GUIDE

STORMSHIELD NETWORK SECURITY

MANUEL D'UTILISATION ET DE CONFIGURATION

Version 4.8.19 LTSB

Dernière mise à jour du document : 24 septembre 2026

Référence : sns-fr-manuel_d'utilisation_et_de_configuration-v4.8.19-LTSB

Table des matières

BIENVENUE 7
Recommandations sur l'environnement d'utilisation 7
Sensibilisation des utilisateurs 13

Prendre en main le firewall SNS 17
Se connecter à l'interface Web d'administration du firewall 17
Comprendre l'interface graphique 17

ACTIVE UPDATE 19
Mettre à jour 19
Mise à jour manuelle des bases de sécurité 19
Configuration avancée 19

ADMINISTRATEURS 20
Onglet Administrateurs 20
Onglet Compte admin 25
Onglet Gestion des tickets 26

AGENT SNMP 27
L'onglet Général 27
L'onglet SNMPv3 28
L'onglet SNMPv1 - SNMPv2c 30
MIB et Traps SNMP 31

ALERTES E-MAIL 34
Onglet Configuration 34
Onglet Destinataires 36
Onglet Modèles 37

ANTISPAM 40
Onglet Général 40
Onglet Domaines en liste blanche 42
Onglet Domaines en liste noire 43

ANTIVIRUS 44
Moteur antiviral 44
Paramètres 44

APPLICATIONS ET PROTECTIONS 46
Nouvelles alarmes 46
Vue par profil d'inspection 46
Vue par contexte 50

AUTHENTIFICATION 51
Onglet Méthodes disponibles 51
Onglet Politique d'authentification 65
Onglet Portail captif 69
Onglet Profils du portail captif 71
Proxy HTTP transparent ou explicite et objets Multi-utilisateur 75

CERTIFICATS ET PKI 78
Les actions possibles 79
Ajouter des autorités et des identités 80
Révoquer une autorité, une sous-autorité ou un certificat 90
Créer, renouveler ou supprimer une CRL 91
Supprimer la clé privée d'une identité (et conserver le certificat) 92
Définir une autorité ou une sous-autorité par défaut 92
Télécharger un certificat 92
Télécharger une identité 93
Télécharger une CRL 93

COMPTES TEMPORAIRES 94
Liste des comptes temporaires 94

CONFIGURATION 97
Onglet Configuration générale 97
Onglet Administration du Firewall 104
Onglet Paramètres réseaux 108

CONFIGURATION DE LA SUPERVISION 110
Intervalles de rafraîchissement 110
La grille de configuration des interfaces, des files d'attente de QoS et des services Web à superviser 110

CONFIGURATION DES ANNUAIRES 112
Fenêtre principale 113
Création d'un LDAP interne 113
Connexion à un annuaire LDAP externe 115
Connexion à un annuaire LDAP externe de type PosixAccount 121
Connexion à un annuaire Microsoft Active Directory 126

CONFIGURATION DES RAPPORTS 131
Général 131
Onglet Liste des rapports 131
Onglet Liste des graphiques historiques 132

CONSOLE CLI 133
Liste des commandes 133
Zone de saisie 133

DHCP 134

Général 134
Service « Serveur DHCP » 134
Service « Relai DHCP » 137

DNS DYNAMIQUE 139
Liste des profils de DNS dynamique 139
Configuration d'un profil 139

DROITS D'ACCÈS 142
Onglet Accès par défaut 142
Onglet Accès détaillé 143
Onglet Serveur PPTP 144

ENREGISTREMENT DES COMMANDES DE CONFIGURATION 146
Enregistrer une séquence de commandes de configuration 146

ENRÔLEMENT 147
La grille 147
Informations de la demande d'enrôlement sélectionnée 147
Configuration avancée 148

ÉVÉNEMENTS SYSTÈME 149
Les actions possibles 149
La liste des événements 149

FILTRAGE ET NAT 151
Evaluation du filtrage et impact du NAT 151
Les politiques 151
L'onglet Filtrage 154
L'onglet NAT 173

FILTRAGE SMTP 184
Les profils 184
Les règles 184

FILTRAGE SSL 187
Les profils 187
Les règles 188

FILTRAGE URL 191
Les profils 191
Les règles 192

HAUTE DISPONIBILITE 195
Étape 1 : Créer ou rejoindre un cluster en Haute Disponibilité 195
Étape 2 : Configuration des interfaces réseaux 196
Étape 3 : Clé pré-partagée du cluster et chiffrement des données 198
Étape 4 : Résumé et finalisation du cluster 199
Écran de la Haute disponibilité 200

INTERFACES 203
La grille des interfaces 203
Les actions possibles 203
Interface Bridge 204
Interface Ethernet 209
Interface Wi-Fi (WLAN) 214
Interface VLAN 216
Agrégat 221
Interface GRETAP 224
Interface modem PPPoE / PPTP 227
Interface USB / Ethernet (pour clé USB / Modem) 229
Modes de configuration réseau 231

INTERFACES VIRTUELLES 233
Créer ou modifier une interface IPsec (VTI) 233
Créer ou modifier une interface GRE 234
Créer ou modifier une interface Loopback 235

LOGS - JOURNAUX D'AUDIT 237
Actions 238
Afficher les détails d'une ligne de log 240
Les interactions 241
Les Journaux 245

LICENCE 247
Firewalls disposant de plusieurs modèles pour une même plate-forme physique 247
L'onglet Général 247
L'onglet Licence locale 249
L'onglet Licence du firewall distant N°_de_série_du_firewall_distant 253

MANAGEMENT DES VULNERABILITES 254
Configuration générale 254
Configuration avancée 256

MAINTENANCE 257
Onglet Mise à jour du système 257
Onglet Sauvegarder 258
Onglet Restaurer 260
Onglet Configuration 261

MESSAGES DE BLOCAGE 263
L'onglet Antivirus 263
L'onglet Page de blocage 264
OBJETS RÉSEAU / TEMPS 266
La barre d'actions 266
Les différents types d'objets 268
OBJETS URL 279
Onglet URL 279
Onglet Noms de certificats (CN) 282
Onglet Base d'URL 283
PORTAIL D'IDENTIFICATION 285
Connexion 285
Le compte « admin », super administrateur 287
Déconnexion 287
PRÉFÉRENCES 288
L'onglet Paramètres 288
L'onglet Affichage 289
L'onglet Liens 290
PROFILS D'INSPECTION 291
Inspection de sécurité 291
PROTOCOLES 293
Recherche 293
Liste des protocoles 293
Les profils 293
Configuration globale des protocoles 294
Live Messenger (MSN) 297
Yahoo Messenger (YMSG) 298
ICMP 298
GIP 298
SCTP 299
TCP-UDP 300
IEC 61850 GOOSE (IPS) 304
MMS / IEC 61850 MMS 304
IEC 61850 SV (IPS) 307
BACnet/IP 307
CIP (onglet IPS - CIP) 309
ETHERNET/IP (onglet IPS) 310
IEC 60870-5-104 (IEC 104) 311
Onglet MODBUS (IPS) 312
Onglet OPC AE (IPS) 314
Onglet OPC DA (IPS) 314
Onglet OPC HDA (IPS) 314
OPC UA 315
PROFINET IO 316
PROFINET-RT 317
S7 317
S7 PLUS 318
Onglet UMAS (IPS) 320
Protocole Microsoft RPC (DCE/RPC) 321
NetBios CIFS (onglet IPS) 324
Onglet NETBIOS EPMAP (IPS) 325
NetBios SSN 325
MGCP (onglet IPS) 325
RTCP (onglet IPS) 326
RTP (onglet IPS) 326
RTSP 327
SIP (onglet IPS) 328
Onglet SOFBUS / LACBUS (IPS) 331
DNS (onglet IPS) 332
FTP 333
HTTP 340
NTP 349
POP3 353
SMTP 356
SNMP (onglet IPS) 361
SSL 363
TFTP (onglet IPS) 370
Autres 371
PROXY CACHE DNS 372
Activer le cache de requête DNS 372
QUALITE DE SERVICE (QoS) 374
L'onglet Files d'attente 374
L'onglet Traffic shapers 378
RAPPORTS 380
Les actions possibles sur les rapports 381
Les rapports disponibles 382
RÈGLES IMPLICITES 389
Règles de filtrage implicites 389
RÉPUTATION DES MACHINES 392
Onglet Configuration 392
Onglet Machines 393
ROUTAGE 394
Onglets Routes statiques IPv4 / IPv6 394
Onglets Routes de retour IPv4 / IPv6 395
ROUTAGE DYNAMIQUE 397
Onglet Général 397

Onglet BIRD v2 398
Onglets BIRD v1 IPv4 et BIRD v1 IPv6 399

ROUTAGE MULTICAST 401
L'onglet Routage Statique 401
L'onglet Routage Dynamique 403

SERVEUR PPTP 408
Configuration générale 408
Configuration avancée 408

SERVICES WEB 410
Onglet Liste des services Web 410
Onglet Groupes 411
Onglet Import de services personnalisés 414

STORMSHIELD MANAGEMENT CENTER 415
Rattachement du firewall au serveur SMC 415
Installer un nouveau package de rattachement sur un firewall SNS 416
Envoyer une demande de rattachement au serveur SMC 416

SUPERVISION 417
Matériel / Haute Disponibilité 419
Système 422
Interfaces 424
QoS 425
Machines 427
Services Web 434
Utilisateurs 435
Connexions 442
SD-WAN 447
Routage multicast dynamique 451
DHCP 455
Tunnels VPN SSL 456
Tunnels VPN IPsec 458
Liste noire / liste blanche 462
Captures réseau 463

SUPPORT IPV6 467
Support IPv6 467
Configuration 470
Bridges et interfaces 471
Interfaces virtuelles 474
Routage 475
DHCP 478
Objets Réseau 482
Filtrage 483

TABLEAU DE BORD 485
Réseau 485
Protections 485
Propriétés 486
Messages 487
Services 487
Indicateurs de santé 488
Pay As You Go 490
Les modules de monitoring et de configuration 491

TRACES - SYSLOG - IPFIX 492
Onglet Stockage local 492
Onglet Syslog 494
Onglet IPFIX 495

TRUSTED PLATFORM MODULE (TPM) 497
Initialiser le module TPM 497
Utiliser des certificats dont la clé privée est protégée par le module TPM 497
Précisions sur les cas d'utilisation avec le module TPM 498

UTILISATEURS 499
Les actions possibles 499
La liste des utilisateurs (CN) 503

VPN IPSEC 505
L'onglet Politique de chiffrement – Tunnels 506
L'onglet Correspondants 516
L'onglet Identification 523
L'onglet Profils de Chiffrement 525

VPN SSL 530
Onglet Configuration générale 531
Onglet Vérification des postes clients (ZTNA) 533

VPN SSL Portail 536
L'onglet Général 537
L'onglet Serveurs web 537
L'onglet Serveurs applicatifs 541
Suppression d'un serveur 542
L'onglet Profils utilisateurs 542
Services VPN SSL sur le portail Web Stormshield Network 544

WI-FI 545

Configuration générale 545
Configuration des canaux 545

Caractères autorisés ou interdits 546

Nom du firewall 546
Identifiant 546
Mot de passe administrateur 546
Bases LDAP 546
PPTP 547
Alertes e-mail 547
Objets de type Nom DNS (FQDN) 547
Certificats et PKI 547
Objets réseau 547
Nom d'interfaces réseau 548
VPN SSL Portail 549
Filtrage et NAT 549
VPN IPsec 549
Qualité de service (QoS) 549
Géolocalisation 550
Services Web - Réputation 550
Mot de passe du TPM 550

Structure d'une base objets au format CSV 551

Machine 551
Plage d'adresses IP 551
Nom DNS (FQDN) 551
Réseau 552
Port 552
Plage de ports 552
Protocole 553
Groupe de machines, d'adresses IP ou de réseaux 553
Groupe de services 553

Structure du fichier d'import de services Web personnalisés (format CSV) 554

Importer / exporter des services Web personnalisés 554
Fichier d'import CSV : structure et limitations 554

BIENVENUE

Bienvenue dans le manuel d'utilisation et de configuration Stormshield Network v4.8.19 LTSB.

Ce guide détaille les fonctionnalités des différents modules de l'interface d'administration web, et vous apporte les informations nécessaires à la configuration d'un Firewall Stormshield Network sur votre réseau.

Les Notes de Version contiennent des informations importantes. Veuillez les consulter avant d'installer ou mettre à jour votre firewall.

Pour toute question ou si vous souhaitez nous signaler une erreur, contactez-nous sur documentation@stormshield.eu.

Produits concernés

SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320,

SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200,

SNi10, SNi20, SNi40, SNi50, SNxr1200,

EVA1, EVA2, EVA3, EVA4 et EVAU.

Copyright © Stormshield 2026. Tous droits réservés.

Toute reproduction, adaptation ou traduction de la présente documentation sans permission préalable est **interdite**.

Le contenu de ce document est relatif aux développements de la technologie Stormshield au moment de sa rédaction. A l'exception des lois obligatoires applicables, aucune garantie sous quelque forme que ce soit, explicite ou implicite, y compris, mais sans s'y limiter, les garanties implicites d'aptitude à la commercialisation et d'adéquation à un usage particulier, n'est accordée quant à la précision, à la fiabilité ou au contenu du document.

Stormshield se réserve le droit de réviser ce document ou de le retirer à n'importe quel moment sans préavis.

Recommandations sur l'environnement d'utilisation

L'installation d'un firewall SNS et d'un serveur SMC s'inscrit dans la mise en place d'une politique de sécurité globale. Pour garantir une protection optimale de vos biens, ressources ou informations, il ne s'agit pas uniquement d'installer le firewall entre votre réseau et l'Internet ou d'installer un serveur SMC pour vous aider à les configurer correctement. En effet, la plupart du temps, les attaques viennent de l'intérieur (accident, personne mécontente de son travail, personne licenciée ayant gardé un accès interne, etc.).

Cette page liste des recommandations de sécurité pour l'utilisation des firewalls SNS et d'un serveur SMC.

IMPORTANT

- Consultez régulièrement les bulletins de sécurité Stormshield sur https://advisories.stormshield.eu et les dernières informations sur la sécurité des produits Stormshield sur https://security.stormshield.eu/.

- Appliquez systématiquement les mises à jour qui corrigent des failles de sécurité sur vos produits Stormshield. Ces mises à jour sont disponibles sur https://mystormshield.eu.

Recommandations

Mesures de sécurité physiques

Les firewalls SNS et le serveur SMC doivent être installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles : local à accès protégé, câbles blindés en paire torsadée, étiquetage des câbles, etc.

Mesures de sécurité organisationnelles

Super administrateur

Un rôle administrateur particulier, le super administrateur, présente les caractéristiques suivantes :

- Il est le seul à être habilité à se connecter via la console locale sur les firewalls SNS, et ce uniquement lors de l'installation du firewall SNS ou pour des opérations de maintenance, en dehors de l'exploitation,
- Il est chargé de la définition des profils des autres administrateurs,
- Tous les accès dans les locaux où sont stockés les firewalls SNS et le serveur SMC se font sous sa surveillance, que l'accès soit motivé par des interventions sur le firewall SNS ou sur d'autres équipements. Toutes les interventions se font sous la responsabilité du super administrateur.

IMPORTANT
Le mot de passe par défaut du super administrateur doit être modifié lors de la première utilisation du firewall SNS.

Mot de passe

Les mots de passe des utilisateurs et des administrateurs doivent être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création et de contrôle de ceux-ci (mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.).

Les administrateurs peuvent modifier leur mot de passe dans l'interface d'administration web :

- Des firewalls SNS dans **Configuration > Système > Administrateur**, onglet **Compte Admin**,
- Du serveur SMC dans **Maintenance > Serveur SMC > Administrateurs**.

Les administrateurs sont sensibilisés à ces bonnes pratiques de par leur fonction et il est de leur responsabilité de sensibiliser tous les utilisateurs à ces bonnes pratiques (voir la section suivante Sensibilisation des utilisateurs).

Bonne politique de contrôle des flux d'informations

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux dits "de confiance" à protéger, de manière :

- **Complète** : les cas d'utilisation standards des équipements ont tous été envisagés lors de la définition des règles et leurs limites autorisées ont été définies,
- **Stricte** : seuls les cas d'utilisation nécessaires des équipements sont autorisés,

- **Correcte** : les règles ne présentent pas de contradiction,
- **Non-ambigüe** : l'énoncé des règles fournit tous les éléments pertinents pour un paramétrage direct du firewall SNS par un administrateur compétent.

Clés cryptographiques

Les clés cryptographiques générées en dehors du firewall SNS et importées sur ce dernier doivent avoir été générées conformément aux recommandations du référentiel général de sécurité (RGS) de l'*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI).

Agents humains

Les administrateurs sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité. Leurs compétences et leur organisation impliquent que :

- Différents administrateurs avec les mêmes droits ne mènent pas des actions d'administration qui se contredisent (modifications incohérentes des politiques de contrôle des flux d'information),
- L'exploitation des journaux et des alarmes dans des délais appropriés.

Environnement de sécurité TI (Technologies de l'Information)

Firewalls SNS

Les firewalls SNS sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. Ils sont dimensionnés en fonction des capacités des équipements adjacents ou alors ces derniers réalisent des fonctions de limitation du nombre de paquets par seconde, positionnées légèrement en deçà des capacités maximales de traitement de chaque firewall SNS installé dans l'architecture réseau.

À part l'application des fonctions de sécurité, les firewalls SNS ne fournissent pas de service réseau autre que le routage et la translation d'adresse (pas de DHCP, DNS, PKI, proxies applicatifs, etc.). Les firewalls SNS ne sont pas configurés pour retransmettre les flux IPX, Netbios, AppleTalk, PPPoE ou IPv6.

Les firewalls SNS ne dépendent pas de services externes en ligne (comme DNS, DHCP, RADIUS, etc.) pour l'application de la politique de contrôle des flux d'information.

L'environnement de sécurité TI fournit :

- Des horodatages NTP fiables,
- Un état à jour de la révocation d'un certificat X.509 pour les correspondants et les administrateurs,
- Un service d'enrôlement fiable.

Serveur SMC

Une politique de contrôle des flux d'informations doit être appliquée au serveur SMC afin de permettre uniquement à ses administrateurs et aux firewalls SNS administrés de s'y connecter.

La machine virtuelle doit être correctement dimensionnée (RAM, CPU, disque) afin de permettre l'administration des firewalls SNS gérés par le logiciel. Le système d'exploitation du serveur SMC ne doit en aucun cas être modifié afin de répondre à des besoins en dehors desquels il a été conçu.

La bande passante disponible entre le serveur SMC et les firewalls SNS doit être suffisante et disponible en permanence afin de réaliser toutes les opérations d'administration. L'administrateur devra configurer voire désactiver certaines fonctionnalités afin de répondre à ce besoin, ou bien devra limiter le nombre de paquets par seconde afin de prioriser les flux d'administration.

La production et la distribution des packages de rattachement, permettant aux firewalls SNS d'être administrés par le serveur SMC, doivent être gérées et confiées à des personnes ayant été sensibilisées à la sécurité. Ces packages ne doivent transiter entre le serveur SMC et les firewalls SNS que via des moyens sécurisés (e-mails chiffrés, clés USB sécurisées, etc.).

Interconnectivité

Les stations d'administration à distance sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elles sont installées dans des locaux à accès protégé et sont exclusivement dédiées à l'administration des firewalls SNS, du serveur SMC et au stockage des sauvegardes.

Les équipements réseau avec lesquels le firewall SNS établit des tunnels VPN sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des firewalls SNS.

Les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des postes clients des réseaux de confiance. Ils sont sécurisés et maintenus à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées.

Configurations et mode d'utilisation des firewalls SNS soumis à l'évaluation

Le mode d'utilisation soumis à l'évaluation présente les caractéristiques suivantes :

- Le cadre de l'évaluation comprend la suite logicielle Stormshield UTM / NG-Firewall installée sur l'ensemble des versions de firewalls Stormshield, allant du SN210 au SN6100, ainsi que les modèles industriels SNi20 et SNi40. Certains modèles ne disposent pas d'un support de stockage conséquent pour les logs et doivent émettre les événements par syslog,
- Les firewalls SNS doivent être stockés dans un local à accès sécurisé. Ces mesures, ainsi que les procédures organisationnelles de l'environnement d'exploitation, doivent garantir que les seuls accès physiques aux firewalls SNS se font sous la surveillance du super-administrateur,
- La console locale n'est pas utilisée en exploitation. Seul le super-administrateur peut s'y connecter, et, par hypothèse, ce genre d'intervention ne se fait que lorsqu'une sortie du cadre de l'exploitation – pour procéder à une maintenance ou à une ré-installation – est décidée,
- Les stations sur lesquelles s'exécutent l'interface Web d'administration sont sécurisées, dédiées à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent,
- Le logiciel Stormshield Network IPsec VPN Client est hors du cadre de l'évaluation. L'utilisateur peut utiliser le client VPN IPsec de son choix ; cependant, ces postes clients doivent être sécurisés avec un niveau de rigueur équivalent à celui des stations d'administration à distance,

- Tout service externe utilisé par le firewall SNS sera hors du cadre de l'évaluation. Néanmoins, ces services doivent être dédiés à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent. Sont considérés comme services externes :
  - Les serveurs de temps NTP,
  - Le serveur d'administration LDAP et le serveur d'annuaire des utilisateurs IPsec,
  - Le serveur Syslog,
  - Le serveur CRL ou OCSP,
  - Le serveur SMC,
  - Le serveur d'enrôlement de certificats EST.
- Les paramétrages usine (défaut) doivent être conservés pour ces modules :
  - CRL : celles-ci sont téléchargées périodiquement depuis un serveur CRL,
  - Horloge interne : synchronisée périodiquement avec des serveurs NTP,
  - Services d'administration NSRPC (port TCP 1300) : limités à la loopback,
  - Fonctionnalité de routage IPv6 : bien que supportée, la fonctionnalité IPv6 est désactivée par défaut et doit le rester pour la durée de l'évaluation,
  - Fenêtres d'anti-rejeu ESP, ré-authentification IKE et PFS (Perfect Forward Secrecy) d'IKE : activés,
  - Durées de vie maximales des SA : 24 heures pour les SA d'IKE et 4 heures pour les SA d'IPsec.
- La certification ne concerne que ces fonctionnalités d'analyse applicative :
  - FTP sur TCP,
  - HTTP sur TCP (extensions WebDAV incluses),
  - SIP sur TCP ou UDP,
  - SMTP sur TCP,
  - DNS sur TCP ou UDP.

  Et ces protocoles industriels :
  - OPC UA sur TCP,
  - MODBUS sur TCP.

  D'autres protocoles ne doivent pas être utilisés dans la configuration de production.
- Les paramètres suivants ne doivent pas être utilisés dans une politique de filtrage dans le but d'associer une règle de filtrage avec :
  - Une inspection applicative (proxies HTTP, SMTP, POP3 et FTP),
  - Une programmation horaire (objet temps),
  - L'action "déchiffrer" (proxy SSL),
  - La réputation d'une machine,
  - Un objet FQDN en source ou en destination (services DNS externes requis).

- Les fonctionnalités suivantes peuvent être utilisées, mais ne sont pas considérées comme des fonctions de sécurité :
  - Translation d'adresses (network address translation ou NAT),
  - Qualité de service,
  - Haute disponibilité,
  - Rapports intégrés,
  - Filtrage par géolocalisation et par réputation d'adresse IP,
  - Filtrage par adresse MAC (couche Ethernet),
  - Active Update.
- Le mode d'utilisation soumis à l'évaluation exclut le fait que le firewall SNS s'appuie sur d'autres services que ceux évoqués auparavant. Les modules que Stormshield fournit en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester. Il s'agit précisément :
  - Des modules permettant la prise en charge des serveurs externes (Kerberos, RADIUS, ...),
  - Du module de routage dynamique,
  - Du module de routage statique multicast,
  - De l'infrastructure à clés publiques (PKI) interne,
  - Du module VPN SSL (Portail et Tunnel) ,
  - Du cache DNS,
  - Des moteurs antivirus,
  - Des serveurs SSH, DHCP, MPD et SNMPD,
  - Du client DHCP,
  - Du relai DHCP,
  - De la connexion Wi-Fi pour les périphériques équipés,
  - De la réputation de machine,
  - Sur les modèles SNi40 et SNi20 : des capacités des composants bypass,
  - De toute signature IPS personnalisée,
  - Des objets FQDN (services DNS externes requis),
  - Des messages IPFIX,
  - De la télémétrie,
  - De Breachfighter (Sandboxing),
  - Du Network Vulnerability Manager (SNVM).

  Les outils d'administration et de supervision fournissent un moyen de vérifier, à tout moment lors de l'exploitation, que ces modules sont bien désactivés.

- Les algorithmes cryptographiques d'IKE et d'IPsec mis en œuvre doivent être :

	Standard IPsec	IPsec DR
Identification	Clé pré-partagée ou certificat avec une clé RSA ou ECDSA (1)	Certificat avec une clé ECDSA ou ECSDSA (2) (3)
Authentification/Intégrité	SHA-2 en 256, 384 ou 512 bits	SHA-2 en 256 bits
Négociation de clé	Groupes Diffie-Hellman 14, 15, 16, 17, 18, 20, 21, 28, 29, 30 (4)	Groupe Diffie-Hellman 19 ou 28
Chiffrement	AES en 128, 192 ou 256 bits en mode CBC, CTR ou GCM	AES en 256 bits en mode GCM ou CTR

(1) : La taille minimale d'une clé RSA doit être de 2048 bits, ou de 3072 bits pour une utilisation au delà de l'année 2030.
(2) : La taille minimale d'une clé doit être de 256 bits.
(3) : Bien que l'usage de RSA soit prohibé dans un environnement DR, un certificat racine RSA peut être utilisé pour signer un certificat intermédiaire, dédié à IPsec par exemple, à partir du moment où l'autorité de certification utilisée comme ancre de confiance sur le firewall est le certificat intermédiaire.
(4) : Pour une utilisation au delà de l'année 2030, le groupe minimal à utiliser doit être le groupe Diffie-Hellman 15.

Ces algorithmes cryptographiques sont nécessaires pour la conformité au Référentiel général de sécurité (RGS) défini par l'ANSSI.

Notez bien que les recommandations sur la mise en œuvre du mode IPsec renforcé, appelé *Diffusion Restreinte (DR)*, en conformité avec le référentiel de l'ANSSI à propos de l'IPsec DR, sont détaillées dans la Note technique SNS "IPsec - mode *Diffusion Restreinte*".

Sensibilisation des utilisateurs

Gestion des accès des administrateurs

L'administrateur de l'appliance firewall-VPN est responsable de la formation des utilisateurs quant à la sécurité du réseau, des équipements qui le composent et des informations qui y transitent.

En effet, la plupart des utilisateurs d'un réseau sont néophytes en informatique et à fortiori en sécurité des réseaux. Il incombe donc à l'administrateur ou au responsable de la sécurité du réseau de mettre en place des sessions de formation ou tout du moins des campagnes de sensibilisation à la sécurité des réseaux.

Lors de ces sessions, il est important d'insister sur la gestion des mots de passe de l'utilisateur et de son environnement de travail et la gestion de leurs accès aux ressources de l'entreprise, comme indiqué dans la section suivante.

Première connexion au boîtier

La première connexion au boîtier nécessite une procédure de sécurisation si celle-ci s'effectue au travers d'un réseau qui ne soit pas de confiance. Cette opération n'est pas nécessaire si la station d'administration est branchée directement au produit.

L'accès au portail d'administration est sécurisé via le protocole SSL/TLS. Cette protection permet d'authentifier le portail via un certificat, assurant ainsi à l'administrateur qu'il est bien connecté au boîtier désiré. Ce certificat peut être le certificat par défaut du boitier ou celui renseigné dans sa configuration (*Authentification* > *Portail captif*).

Le certificat par défaut du boitier a comme nom (CN) le numéro de série du boitier et il est signé par deux autorités dont les noms sont NETASQ - Secure Internet Connectivity ("O") / NETASQ Firewall Certification Authority ("OU") et Stormshield ("O") / Cloud Services ("OU").

Pour valider un accès sécurisé, le navigateur doit faire confiance à l'autorité de certification qui a signé le certificat utilisé, et appartenant à la liste des autorités de certification de confiance du navigateur. Ainsi pour valider l'intégrité du boîtier, il faut donc avant la première connexion, ajouter les autorités NETASQ et Stormshield à la liste des autorités de confiance du navigateur. Ces autorités sont disponibles sur les liens http://pki.stormshieldcs.eu/netasq/root.crt et http://pki.stormshieldcs.eu/products/root.crt. Si le boîtier a configuré un certificat signé par une autre autorité, il faut y ajouter cette autorité à la place de celles de NETASQ et Stormshield.

En conséquence, la connexion initiale au boîtier ne déclenchera plus d'avertissement du navigateur relatif à l'autorité de confiance. En revanche, un message avertit toujours que le certificat n'est pas valide. En effet, le certificat définit le firewall par son numéro de série, et non par son adresse IP. Pour éviter ce dernier avertissement, il faut spécifier au serveur DNS l'association entre le numéro de série et l'IP du firewall.

NOTE
Le mot de passe par défaut de l'utilisateur 'admin' (super administrateur) doit être modifié lors de la première utilisation du produit dans l'interface d'administration web via le module **Administrateur** (menu **Système**), onglet *Compte Admin*.

Ce mot de passe doit être défini selon les bonnes pratiques décrites dans la section suivante, partie *Gestion des mots de passe de l'utilisateur.*

Ce mot de passe ne doit être en aucun cas sauvegardé dans le navigateur Web.

Gestion des mots de passe de l'utilisateur

Au cours de l'évolution des technologies de l'information, de nombreux mécanismes d'authentification ont été inventés et mis en place afin de garantir une meilleure sécurité des systèmes d'information des entreprises. Cette multiplication des mécanismes a entraîné une complexité qui contribue aujourd'hui à détériorer la sécurité des réseaux d'entreprises.

Les utilisateurs (néophytes et non formés) choisissent des mots de passe "simplistes", tirés généralement de leur vie courante et la plupart du temps correspondant à un mot contenu dans un dictionnaire. Ces comportements entraînent, bien entendu, une dégradation notable de sécurité du système d'information.

Il faut prendre conscience que l'attaque par dictionnaire est un "outil" plus que performant. Une étude de 1993 montre déjà cet état de fait. La référence de cette étude est la suivante : (http://www.klein.com/dvk/publications/). Ce qui est le plus frappant dans cette étude est sûrement le tableau présenté ci-dessous (basé sur un mot de passe de 8 caractères) :

Type de mot de passe	Nombre de caractères	Nombre de mots de passe	Temps de Cracking
Lexique anglais 8 caract. et +	spécial	250000	< 1 seconde
casse minuscule uniquement	26	208827064576	9 heures
casse minuscule + 1 majuscule	26/spécial	1670616516608	3 jours

minuscules et majuscules	52	53459728531456	96 jours
Lettres + chiffres	62	218340105584896	1 an
Caractères imprimables	95	6634204312890620	30 ans
Jeu de caractères ASCII 7 bits	128	72057594037927900	350 ans

On peut citer aussi un état de fait qui tend à se résorber mais qui est encore d'actualité : les fameux post-its collés à l'arrière des claviers.

L'administrateur doit mettre en place des actions (formation, sensibilisation, ...) dans le but de modifier et de corriger ces "habitudes".

EXEMPLE

- Incitez vos utilisateurs à choisir des mots de passe de longueur supérieure à 7 caractères,
- Demandez-leur d'utiliser des chiffres et des majuscules,
- De changer souvent de mots de passe,
- Et surtout de ne noter en aucun cas le mot de passe qu'ils auront finalement choisi.

L'une des méthodes classiques pour trouver un bon mot de passe est de choisir une phrase que l'on connaît par cœur (vers d'une poésie, parole d'une chanson) et d'en tirer les premières lettres de chaque mot. Cette suite de caractères peut alors être utilisée comme mot de passe.

EXEMPLE
" **S**tormshield **N**etwork, **1**er **c**onstructeur **f**rançais **d**e **b**oîtiers **F**IREWALL **e**t **V**PN..."
Le mot de passe pourrait être le suivant : **SN1cfdbFeV**.

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) propose à ce titre un ensemble de recommandations permettant de définir des mots de passe suffisamment robustes.

L'authentification d'utilisateurs via le portail captif s'effectue par défaut, par un accès SSL/TLS utilisant un certificat signé par deux autorités non reconnues par les navigateurs. Il est donc nécessaire de déployer ces autorités de certification utilisées par une GPO sur les navigateurs des utilisateurs. Par défaut, ces autorité sont la CA NETASQ et la CA Stormshield, disponibles sur les liens suivants :

- http://pki.stormshieldcs.eu/netasq/root.crt.
- http://pki.stormshieldcs.eu/products/root.crt.

Pour plus de détails, consultez la section précédente **Gestion des administrateurs**, partie *Première connexion au boîtier.*

Environnement de travail

L'espace de travail est souvent un lieu de passage, un croisement pour de nombreuses personnes internes et extérieures à l'entreprise. Il s'agit donc de sensibiliser les utilisateurs au fait que certaines personnes (fournisseurs, clients, ouvriers, ...) peuvent accéder à leur espace de travail et de ce fait recueillir des informations sur l'activité de l'entreprise.

Il est important de faire prendre conscience à l'utilisateur qu'il ne faut pas qu'il divulgue son mot de passe aussi bien par téléphone que par Email (social engineering) et qu'il faut qu'il tape son mot de passe à l'abri des regards indiscrets.

Gestion des accès d'utilisateurs

Pour compléter cette section sur la sensibilisation des utilisateurs à la sécurité des réseaux, l'administrateur doit aborder la gestion des accès utilisateur. En effet le mécanisme d'authentification d'un appliance firewall-VPN Stormshield Network ou d'un serveur SMC (comme beaucoup d'autres systèmes) basé sur un système de login/mot de passe n'implique pas forcément de déloguage à la fermeture de l'application à l'origine de cette authentification (crédit de temps d'authentification). Cet état de fait n'est pas forcément évident pour l'utilisateur néophyte. Ainsi, bien qu'il ait fermé l'application en question, l'utilisateur (qui pense ne plus être connecté) reste authentifié. S'il quitte son poste une personne malintentionnée peut alors usurper son identité et accéder aux informations contenues dans l'application.

Enfin incitez les utilisateurs à verrouiller leurs sessions lorsqu'ils se déplacent et laissent leur poste de travail sans surveillance. Cette tâche qui se révèle parfois fastidieuse peut être facilitée par des mécanismes d'authentification qui automatise le verrouillage (token USB par exemple).

Prendre en main le firewall SNS

Se connecter à l'interface Web d'administration du firewall

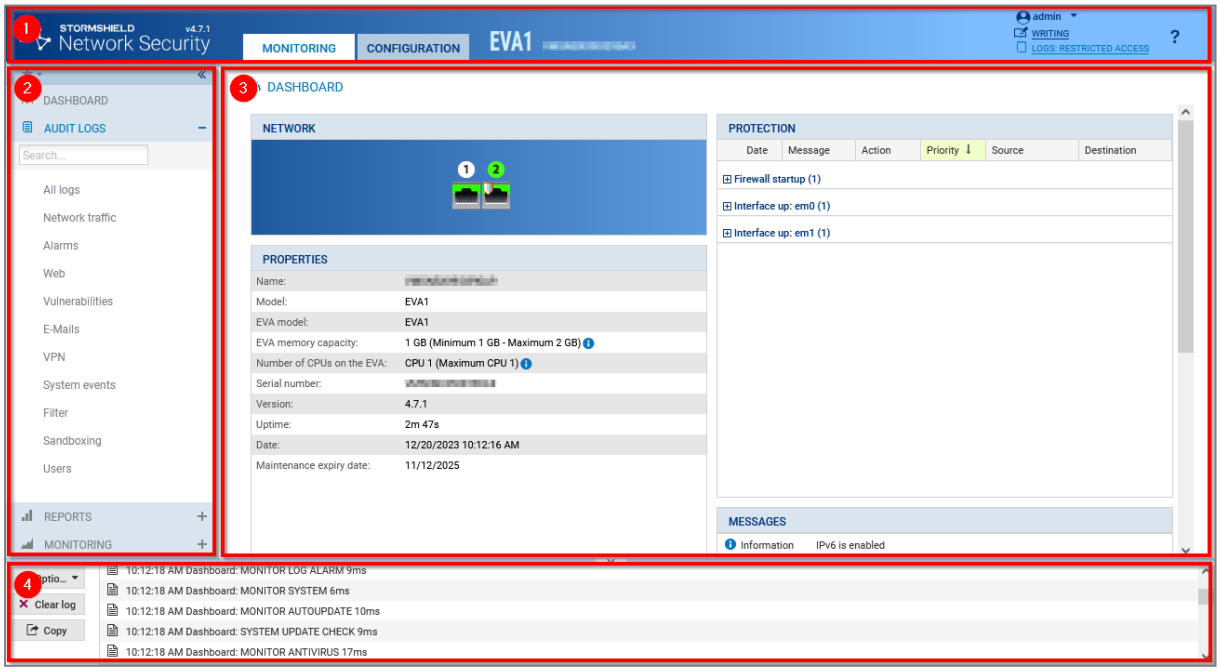
1. Connectez-vous à l'adresse IP (par défaut, 10.0.0.254) du firewall précédée de https:// depuis un navigateur web. Reportez-vous au Product Life Cycle pour connaître la liste des navigateurs web supportés.
2. Connectez-vous à l'interface Web d'administration du firewall en utilisant votre mot de passe et votre identifiant ou l'identifiant et le mot de passe d'administration.

Par défaut, si vous faites quatre erreurs successives lors de l'authentification, vous devez attendre une minute avant de vous identifier à nouveau. Si vous tentez de vous identifier alors que le temps d'attente n'est pas écoulé, celui-ci est allongé d'une minute supplémentaire, dans la limite de dix minutes. Le nombre d'erreurs et le temps d'attente sont configurables. Pour plus d'informations, reportez-vous à la section Onglet Administration du Firewall.

Comprendre l'interface graphique

La fenêtre est composée de 4 zones :

1. Le bandeau supérieur permettant de choisir entre les vues **Monitoring** et **Configuration**, et donnant des informations sur l'état du firewall,
2. Le menu de gauche permettant d'accéder aux différents modules du firewall,
3. La fenêtre active du module sélectionné,
4. La fenêtre inférieure listant les erreurs, les avertissements, les commandes et les notifications.



Bandeau supérieur

Dans le bandeau supérieur, les éléments suivants sont affichés de gauche à droite :

- Le numéro de version de votre firewall,
- Deux onglets permettant d'accéder aux deux vues du firewall : Monitoring et Configuration,
- Le modèle de votre firewall et son nom : survolez le nom pour afficher le numéro de série,
- Un pictogramme clignotant s'affichant si l'état de votre firewall requiert votre attention : survolez le pictogramme pour afficher les éléments surveillés et leur statut,
- Votre nom d'utilisateur : cliquez dessus pour accéder à vos préférences ou vous déconnecter,
- Vos droits de lecture et d'écriture : survolez les droits pour afficher plus d'informations,
- Vos droits d'accès aux logs : si vous êtes en accès restreint, cliquez dessus pour demander un accès complet,
- L'icône permettant d'ouvrir la page du *BIENVENUE* en ligne se rapportant au module que vous consultez.

Menu de gauche

Le menu de gauche permet d'accéder aux différents modules correspondant aux différentes fonctionnalités. Les modules sont classés par catégorie. Vous pouvez :

- Réduire le menu en cliquant sur ,
- Déplier et de réduire les catégories en cliquant dessus,
- Mettre des modules en favori en cliquant sur l'icône qui s'affiche en survolant le nom d'un module,
- Accéder rapidement aux modules favoris en cliquant sur l'icône en haut du menu.

S'il y a des modules grisés dans le menu, cela peut indiquer :

- Qu'ils nécessitent une licence à laquelle vous n'avez pas souscrit, et donc, que vous n'y avez pas accès.
- Que l'utilisateur avec lequel vous êtes connecté n'a pas les privilèges nécessaires pour accéder à ces modules.

Les modules présents dans le menu changent suivant si vous êtes en vue **Monitoring** ou en vue **Configuration**.

Lorsque vous utilisez la barre de recherche, la recherche porte aussi bien sur le nom du module que sur son contenu.

Fenêtre active

Le contenu de cette fenêtre change suivant le module que vous affichez. Les autres sections du *BIENVENUE* décrivent les différents modules et leur contenu.

Fenêtre inférieure

La fenêtre inférieure liste les erreurs, les avertissements, les commandes et les notifications. Vous pouvez :

- Masquer ou afficher cette fenêtre en cliquant sur la flèche au milieu .
- Paramétrer les messages qui s'affichent en cliquant sur **Options**.

ACTIVE UPDATE

Le module **Active Update** se compose d'un écran avec trois parties distinctes :

- **Mettre à jour** : permet de sélectionner pour chaque module si sa mise à jour doit être manuelle, automatique ou désactivée.
- **Mise à jour manuelle des bases de sécurité** : permet la mise à jour des modules paramétrés en mise à jour manuelle. Cette mise à jour est réalisée via un fichier de mises à jour téléchargé sur le site MyStormshield.
- **Configuration avancée** : permet de définir les serveurs utilisés pour les mises à jour automatiques.

Mettre à jour

État	Double cliquez pour sélectionner le type de mise à jour d'un module. Trois choix sont possibles : • Désactivée, • Manuelle (par le biais du fichier de mise à jour téléchargé sur Mystormshield), • Automatique.
Module	Type de données mises à jour (la liste varie selon la licence acquise).

Mise à jour manuelle des bases de sécurité

Pour mettre à jour les données paramétrées en mise à jour manuelle :

1. Téléchargez le fichier de mise à jour (fichier avec extension *.ssp*) sur MyStormshield (menu **Téléchargements** > **Stormshield Network Security** > **Offline Active Update Data**).
2. Sélectionnez ce fichier et cliquez sur le bouton **Mettre à jour**.
   Le fichier contient l'ensemble des données pouvant être mises à jour via Active Update, mais seules les données paramétrées en mise à jour manuelle seront intégrées.

Le lien **Accéder à la supervision système** permet d'accéder au module **Monitoring > Supervision > Système** afin de visualiser l'état de mise à jour et la date de dernière mise à jour des modules.

Configuration avancée

Serveurs de mise à jour des signatures de protection contextuelle personnalisées

Lorsque vous utilisez des signatures de protection contextuelle personnalisées, hébergées sur un ou des serveur(s) interne(s), renseignez la ou les URL d'accès à ce(s) serveur(s) pour bénéficier d'une mise à jour automatique de ces signatures.

Serveurs de mise à jour

Par défaut, les serveurs de mise à jour Stormshield Network sont renseignés; vous pouvez personnaliser ces adresses pour la mise en place de sites miroirs internes. Pour plus d'informations, consultez l'article de la base de connaissances Stormshield *How to create my own autoupdate server for my Stormshield UTMs*.

ADMINISTRATEURS

Ce module est composé de trois onglets :

- **Administrateurs** : il permet de créer des administrateurs en octroyant des droits d'administration aux utilisateurs utilisant une des méthodes d'authentification suivantes : LDAP RADIUS, KERBEROS, ou SSL.
- **Compte admin** : il permet de définir le mot de passe d'authentification du compte admin et d'exporter la clé privée de l'administrateur ou la clé publique.
- **Gestion des tickets** : il permet aux administrateurs gérant les droits d'accès aux données personnelles de créer des tickets temporaires d'accès complet aux logs.

Onglet Administrateurs

Cet onglet se compose d'une grille contenant :

- Une barre des tâches : elle affiche les différentes actions possibles sur un administrateur.
- La liste des utilisateurs et groupes d'utilisateurs répertoriés en tant qu'administrateur et leurs droits.

> **NOTE**
> L'onglet **Administrateurs** est accessible seulement en étant connecté avec le compte *admin*.

Les actions possibles

Certaines actions peuvent également être réalisées en effectuant un clic droit dans la grille des administrateurs.

Ajouter un administrateur	Ajoute un nouvel administrateur sur le firewall. Plusieurs choix sont proposées selon les droits à attribuer au nouvel administrateur. La procédure est détaillée dans la section Ajouter un administrateur.
Supprimer	Supprime l'administrateur sélectionné.
Monter	Place l'administrateur sélectionné au-dessus du précédent dans la liste.
Descendre	Place l'administrateur sélectionné au-dessous du suivant dans la liste.
Copier les droits	Copie les droits de l'administrateur sélectionné.
Coller les droits	Colle les droits copiés à l'administrateur sélectionné.
Donner tous les droits	Attribue tous les droits à l'administrateur sélectionné.
Passer en vue avancée / Passer en vue simple	Modifie l'affichage des droits dans la grille selon deux vues : • **Vue simple** : affichage par défaut comportant plusieurs colonnes représentant les catégories de droits auxquelles un administrateur est affilié ou non. • **Vue avancée** : affiche tous les droits disponibles. Le détail des droits est disponible dans la section Les droits possibles.

Ajouter un administrateur

En cliquant sur le bouton **Ajouter**, plusieurs choix sont proposés :

Administrateur sans droits	Ce type d'administrateur dispose des droits de base, à savoir l'accès au **Tableau de bord** et aux modules suivants : • **Licence,** • **Maintenance,** • **Active Update,** • **Haute disponibilité** (et son assistant), • Console **CLI,** • **Réseau,** • **Routage,** • **DNS dynamique,** • **DHCP,** • **Proxy cache DNS**, • **Objets**, • **Catégories d'URL** (et leurs groupes), • **Certificats et PKI,** • **Authentification** (et son assistant), • **Filtrage URL,** • **Filtrage SSL,** • **Filtrage SMTP,** • **Applications et protections,** • **Profils d'inspection,** • **Antivirus,** • **Antispam,** • **Messages de blocage,** • **Préférences.** Le module **Management des Vulnérabilités** nécessite le droit d'écriture pour être accessible.
Administrateur avec accès en lecture seule	Ce type d'administrateur dispose des mêmes accès de base que l'admin « sans droits » avec en plus des droits supplémentaires : la lecture des logs **SNMP, Alertes e-mails, Evénements système,** ainsi que la lecture du **Filtrage** et du **VPN.**
Administrateur avec tous les droits	Ce type d'administrateur aura accès à tous les modules exceptés ceux où un accès super-administrateur (compte *admin*) est requis. **NOTE** Il n'existe qu'un seul super-administrateur qui présente les caractéristiques suivantes : • Il est le seul à être habilité à se connecter via la console locale sur les Firewalls Stormshield Network, et ce uniquement lors de l'installation du firewall ou pour des opérations de maintenance, en dehors de l'exploitation. • Il est chargé de la définition des profils des autres administrateurs. • Tous les accès dans les locaux où sont stockés les boîtiers firewalls, ainsi que les interventions effectuées se font sous sa surveillance.

Administrateur de comptes temporaires	Ce type d'administrateur peut uniquement gérer les comptes temporaires définis sur le firewall (création, modification, suppression).
Administrateur avec accès aux données personnelles	Ce type d'administrateur peut accéder à l'ensemble des logs en cliquant sur le lien **Logs : accès restreint** afin d'activer le droit **Logs : accès complet (données personnelles)** sans devoir saisir un code d'accès aux données privées.
Administrateur sans accès aux données personnelles	Par souci de conformité avec le règlement européen RGPD (Règlement Général sur la Protection des Données), il est possible de définir un administrateur avec les droits en lecture et écriture sur le firewall mais ne pouvant pas visualiser les données personnelles stockées dans les logs. L'administrateur concerné peut néanmoins demander et obtenir les droits d'accès à ces données personnelles en renseignant un code d'autorisation fourni par son superviseur. Ce code possède une durée de validité limitée définie lors de sa création. Pour activer le droit **Logs : accès complet (données personnelles)**, il doit obligatoirement cliquer sur le lien **Logs : accès restreint** puis saisir le code. Une fois sa tâche terminée, il peut alors relâcher ce droit de visualisation des données personnelles.

Définissez ensuite l'utilisateur ou le groupe d'utilisateurs à ajouter en tant qu'administrateur.

Utilisateur - Groupe présent dans l'annuaire LDAP	Permet d'ajouter en tant qu'administrateur un utilisateur ou un groupe d'utilisateurs présent dans l'annuaire LDAP du firewall. Sélectionnez dans la liste déroulante l'utilisateur ou le groupe d'utilisateurs concerné.
Utilisateur - Groupe provenant d'un autre domaine (annuaire)	Permet d'ajouter en tant qu'administrateur un utilisateur ou un groupe d'utilisateurs provenant d'un autre domaine. Pour ce choix, complétez les informations : • **Utilisateur / Groupe** : définissez si vous souhaitez ajouter un **Utilisateur** ou un **Groupe**. • **Utilisateur - Nom du groupe** : tapez le nom de l'utilisateur ou du groupe concerné. • **Nom de domaine** : tapez le nom de domaine concerné.

Une fois ajouté, l'administrateur apparaît dans la grille dans la colonne **Utilisateur – groupe d'utilisateurs**.

Les droits possibles

L'affichage des droits dans la grille dispose de deux vues :

- **Vue simple** : affichage par défaut comportant plusieurs colonnes représentant les catégories de droits auxquelles un administrateur est affilié ou non. Positionnez votre souris sur le titre d'une colonne pour connaître précisément les droits qu'elle contient.
- **Vue avancée** : affiche tous les droits disponibles.

Utilisez le bouton **Passer en vue avancée / Passer en vue simple** pour modifier l'affichage.

Les icônes de la grille ont la signification suivante :

- ✔ : L'ensemble des droits sont attribués.
- ✖ : L'ensemble des droits ne sont pas accordés.
- ✔✖ : Une partie des droits sont accordés, d'autres non.

Un double clic sur les icônes représentées change l'état des permissions (de « accordé » à « non accordé » par exemple). Un double clic sur l'icône ✔✖ retire les droits attribués.

NOTE
Toute modification des permissions d'un administrateur n'est effective qu'à la prochaine connexion de cet administrateur. Si vous souhaitez qu'une modification soit immédiatement prise en compte, vous devez forcer la déconnexion de l'administrateur concerné (par exemple avec la commande CLI : `monitor flush user`).

Droits en vue simple

Intitulé	Description	Droit attribués
Système	Droits d'effectuer des opérations de maintenance (sauvegardes, restaurations, mises à jour, Firewall arrêt et redémarrage, mise à jour de l'antivirus, modification de la fréquence de mise à jour de l'antivirus et actions relatives au RAID). Droits de modification de la base objet	base, console, contentfilter, globalobject, maintenance, modify, object
Réseau	Droit de modification de la politique de filtrage et du routage (route par défaut, routes statiques et réseaux de confiance)	base, modify, network, route
Utilisateurs	Droit de modification des utilisateurs et de la PKI	base, modify, pki, user
Firewall	Droit de modification de la configuration VPN, de la prévention d'intrusion (IPS) et du management de vulnérabilités	modify, base, filter, vpn, asq, pvm, vpn, read, filter_read, globalfilter
Supervision	Droit de modification de la configuration et modification des traces	modify, mon_write, base, log, log_read, report, report_read, privacy, privacy_read
Comptes temporaires	Droit de gestion des comptes temporaires pour la politique d'authentification "Comptes temporaires"	base, guest_admin

Droits en vue avancée

Intitulé	Description	Droit attribués
Traces (L)	Consultation des traces	base, log_read
Filtrage (L)	Consultation de la politique de filtrage	base, filter_read
VPN (L)	Consultation de la configuration VPN	base, vpn_read
Accès aux données personnelles (L)	Droit de consulter les logs contenant des données personnelles	base, privacy_read
Traces (E)	Droit de modification de la configuration des traces	modify, base, log
Filtrage (E)	Droit de modification de la politique de filtrage	modify, base, filter

VPN (E)	Droit de modification de la configuration VPN	modify, base, vpn
Gestion des accès aux données personnelles	Droit de créer des tickets pour les demandes ponctuelles d'accès aux données personnelles dans les logs.	base, privacy
PKI	Droit de modification de la PKI	base, modify, pki
Monitoring	Permission to view advanced Monitoring	base, modify, mon_write
Filtrage de contenu	Droits pour les politiques de filtrage URL, Mail, SSL et la gestion des antivirus	base, modify, contentfilter
Objets	Droit de modification de la base objet	base, modify, object
Utilisateurs	Droit de modification des utilisateurs	base, modify, user
Réseau	Droit de modification de la configuration réseau (interfaces, bridges, modems, VLANs et configuration du DNS dynamique)	base, modify, network
Routage	Droits de modification du routage (route par défaut, routes statiques and réseaux de confiance)	base, modify, route
Maintenance	Droits d'effectuer des opérations de maintenance (sauvegardes, restaurations, mises à jour, arrêt et redémarrage du firewall, mise à jour de l'antivirus, modification de la fréquence de mise à jour de l'antivirus, configuration de la haute disponibilité et actions relatives au RAID).	base, modify, maintenance
Comptes temporaires	Droit de gestion des comptes temporaires (module **Utilisateurs** > **Comptes temporaires**)	base, guest_admin
Prévention d'intrusion	Droits de modifier la configuration de la prévention d'intrusion (IPS)	base, modify, asq
Management de vulnérabilités	Droit de modifier la configuration de management de vulnérabilités (Stormshield Network Vulnerability Manager)	base, modify, pvm
Objets (global)	Droits d'accès aux objets globaux	base, modify, globalobject
Filtrage (global)	Droits d'accès à la politique de filtrage globale	base, modify, globalfilter
Rapports (E)	Droits de modifier Stormshield Network Activity Report	base, report_read
Rapports (L)	Droits d'accès à Stormshield Network Activity Report	base, report_read
Accès au TPM	Lorsque le firewall est équipé d'un TPM (Trusted Platform Module), ce droit permet d'initialiser le TPM et de manipuler les données protégées par ce TPM (clés privées de certificats du firewall).	base, modify, tpm
Console (SSH)	Droit d'ouvrir une connexion distante en SSH sur le firewall.	base, modify, console

Le droit *base* est systématiquement attribué à tous les utilisateurs. Ce droit permet la lecture de toute la configuration hormis le filtrage, le VPN, les traces et le filtrage de contenu.

Le droit *modify* est affecté à tout utilisateur ayant un droit d'écriture.

L'utilisateur connecté en tant que *admin* obtient le droit *admin*. Seul ce droit permet d'ajouter ou de retirer des droits d'administration aux autres utilisateurs.

Onglet Compte admin

Cet écran permet de définir les données d'authentification du compte administrateur.

NOTES

- Le mot de passe par défaut de l'utilisateur 'admin' (super administrateur) doit être modifié lors de la première utilisation du produit.
- Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur.

Authentification

Ancien mot de passe	Saisissez le mot de passe courant du compte admin afin de pouvoir le changer.
Nouveau mot de passe	Saisissez le nouveau mot de passe du compte admin. Pour connaître les caractères autorisés ou interdits, reportez-vous à la section Noms autorisés ou interdits.
Confirmer le mot de passe	Confirmez le mot de passe du compte admin que vous avez renseigné dans le champ précédent
Robustesse du mot de passe	Cette jauge indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

NOTE

Stormshield Network utilise un système de chiffrement dit « asymétrique », à savoir qu'il utilise une paire composée d'une clé publique, servant à chiffrer les données, et d'une clé privée, servant à déchiffrer. L'intérêt de cette utilisation est qu'elle supprime le problème de transmission sécurisée de la clé, et permet la signature électronique.

Exports

Clé privée de l'administrateur	En cliquant sur ce bouton, vous enregistrerez la clé privée associée au compte admin sur votre machine.
Clé publique du firewall	En cliquant sur ce bouton, vous enregistrerez la clé publique associée au firewall sur votre machine.

Onglet Gestion des tickets

Cette grille permet à un administrateur possédant le droit de gestion des accès aux données personnelles de créer des tickets d'accès temporaires à ces données.

La grille

Cette grille présente l'ensemble des informations relatives aux tickets d'accès aux données personnelles. Elle comporte les colonnes suivantes :

Identifiant du ticket	C'est un identifiant unique généré aléatoirement. Il correspond aux 4 premiers caractères du code d'accès aux données privées.
Début de validité	Date et heure du début de validité du ticket et de son code d'accès aux données privées associé.
Fin de validité	Date et heure d'expiration du ticket et de son code d'accès aux données privées associé.
Code d'accès aux données personnelles	Code généré aléatoirement. Après avoir cliqué sur **Logs : accès restreint** (bandeau supérieur de l'interface Web d'administration), ce code doit être saisi par l'opérateur afin de pouvoir visualiser les données personnelles présentes dans les logs et les rapports.

Les actions possibles

Ajouter un ticket

Pour créer un ticket d'accès temporaire aux données personnelles présentes dans les logs et les rapports, renseignez les dates et heures de début et de fin de validité de ce ticket.

Début de validité	Sélectionnez dans le calendrier le premier jour de validité du code d'accès aux données privées. La valeur proposée par défaut correspond au jour courant. Sélectionnez ensuite l'heure de début de validité (granularité de 30 minutes).
Fin de validité	Sélectionnez dans le calendrier le dernier jour de validité du code d'accès aux données privées. La valeur proposée par défaut correspond au jour courant. Sélectionnez ensuite l'heure de fin de validité (granularité de 30 minutes).

Supprimer

Ce bouton permet de supprimer un ticket :

1. Sélectionnez le ticket à supprimer.
2. Cliquez sur **Supprimer**.

AGENT SNMP

IMPORTANT
Afin de suivre au mieux les recommandations de la RFC2578, et pour résoudre un problème de compatibilité avec certains logiciels de supervision, toutes les tables SNMP pour lesquelles le premier indice était positionné à 0 ont été dupliquées en de nouvelles tables dont le premier indice est positionné à 1.
Les anciennes tables SNMP (indice commençant à 0) continuent d'être utilisées par défaut mais sont marquées comme obsolètes et sont amenées à disparaître dans une future version SNS.

Pour activer les nouvelles tables SNMP (indice commençant à 1) sur le firewall :

1. Connectez-vous au firewall en SSH / Console (compte *admin* ou administrateur avec les droits Console [SSH]),
2. Éditez la section [Config] du fichier de configuration ConfigFiles/snmp et positionnez le jeton de configuration IndexStartAt1 à la valeur "1",
3. Relancez l'agent SNMP à l'aide de la commande *ensnmp*.

L'écran de configuration du service **SNMP** se compose de trois onglets :

- **Général** : onglet qui s'affiche par défaut lorsque l'on clique sur le menu SNMP dans l'arborescence de gauche et qui permet l'activation du module et les notifications alarmes et système qui seront intégrés dans les MIB (Management Information Base) disponibles (en consultation et en envoi de *traps*).
- **SNMPv3 :** Version recommandée car munie d'outils plus sécurisés (outils de sécurité comme l'authentification, le chiffrement, le contrôle du timing…).
- **SNMPv1 – SNMPv2c** : Version dont la requête SNMP contient un nom appelé « Communauté » utilisé comme identifiant et transmis en clair sur le réseau.

L'onglet Général

Cet onglet permet de configurer le système, c'est-à-dire la machine et son administrateur, contient les notifications (alarmes et événements système) qui seront intégrés dans les MIB disponibles.

	Active ou désactive l'agent SNMP.

Il est possible toutefois de configurer les données de cet écran même si le module n'est pas activé.

SNMPv3 (recommandé)	Active la version 3 de SNMP, version recommandée car munie d'outils plus sécurisés (outils de sécurité comme l'authentification, le chiffrement, le contrôle du timing…). Depuis décembre 2002, un nouveau standard existe pour le protocole SNMP, il apporte une avancée significative en matière de sécurité. La configuration requiert les paramètres suivants : SNMPv3 offre des méthodes d'authentification ainsi que des méthodes de chiffrement, et résout certains problèmes de sécurité des versions précédentes.

SNMPv1/v2c	Active les versions v1/v2c de SNMP. V1 est la première version du protocole. La seule vérification faite par cette version concerne la chaîne de caractères « Community ». La version v2c est une version qui améliore les types d'opération de SNMPv2p et utilise la sécurité par chaîne de caractères « Community » de SNMPv1.
SNMPv1/v2c et SNMPv3	Active les trois versions de SNMP.

Configuration des informations MIB-II

Emplacement (sysLocation)	Information alphanumérique de lieu sur l'élément surveillé. La localisation peut indiquer un pays, une ville, une salle serveur, etc. Exemple : France.
Nom	Permet d'affecter un nom significatif à l'agent SNMP du firewall.
Contact (sysContact)	Adresse e-mail, N° de téléphone, etc. de la personne à contacter en cas de problème. Exemple : *admin@compagnie.com*

Envoi des alertes SNMP (*traps*)

Alarmes de prévention d'intrusion	En cochant : • **Ne pas envoyer :** vous ne recevrez pas les alarmes du moteur de prévention d'intrusion. • **Envoyer uniquement les alarmes majeures** : vous recevrez les alarmes ayant la sévérité "majeure" émises par le moteur de prévention d'intrusion. • **Envoyer les alarmes majeures et mineures** : vous recevrez les alarmes ayant les sévérités "mineures" et "majeures" émises par le moteur de prévention d'intrusion.
Événements système	En cochant : • **Ne pas envoyer :** vous ne recevrez pas les événements système du moteur de prévention d'intrusion. • **Envoyer uniquement les alarmes majeures** : vous recevrez les les événements système ayant la sévérité "majeure" émis par le moteur de prévention d'intrusion. • **Envoyer les alarmes majeures et mineures** : vous recevrez les les événements système ayant les sévérités "mineures" et "majeures" émis par le moteur de prévention d'intrusion.

NOTE
SNMP peut être configuré de manière à utiliser le nom du firewall pour SysName, au lieu du numéro de série.

L'onglet SNMPv3

Les options **Activer l'agent SNMPv3 (recommandé)** ou **SNMPv1/v2c et SNMPv3** permettent l'activation du module SNMP v3.

Connexion à l'agent SNMP

Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion et pour la consultation des MIB sur le firewall.

Authentification

Mot de passe	Mot de passe de l'utilisateur qui consultera les MIB. Ce mot de passe devra obligatoirement être en conformité avec la politique générale de mots de passe du firewall, définie dans la section **Politique de mots de passe** du module **Configuration** (onglet *Configuration générale*), et contenir au moins 8 caractères.

Algorithme	L'algorithme actuellement utilisé s'affiche. Une mention précise s'il est obsolète.
	Pour utiliser l'algorithme SHA256, utilisez les commandes CLI / Serverd suivantes :
	`CONFIG SNMP ACCESS USERV3 username=<username> authtype=SHA256 authpass=<passphrase>`
	`CONFIG SNMP ACTIVATE`

Chiffrement (optionnel)

Mot de passe	Les paquets SNMP sont chiffrés en DES ou AES (Advanced Encryption Standard), une clé de chiffrement peut être définie. Par défaut c'est la clé d'authentification qui est utilisée. **AVERTISSEMENT** **Il est vivement recommandé d'utiliser une clé spécifique.**

Algorithme	L'algorithme actuellement utilisé s'affiche. Une mention précise s'il est obsolète.
	Pour utiliser l'algorithme AES-128, utilisez les commandes CLI / Serverd suivantes :
	`CONFIG SNMP ACCESS USERV3 username=<username> authtype=SHA256 authpass=<passphrase> privtype=AES privpass=<passphrase>`
	`CONFIG SNMP ACTIVATE`

Envoi des alertes SNMPv3 (*traps*)

L'envoi des *traps* vers des machines se compose de deux parties avec, à gauche, la liste des machines et à droite le détail d'une machine préalablement sélectionnée.

Liste des serveurs SNMP

Dans cet écran, vous configurez les stations que doit contacter le firewall lorsqu'il veut envoyer un *trap* SNMP (événement). Si aucune station (machine) n'est spécifiée, le firewall n'envoie pas de messages.

Un assistant vous guide dans la configuration des machines.

En cliquant à droite d'un nom de machine, la base d'objets s'affiche vous permettant de sélectionner une machine.

Serveur [Nom du serveur de destination (objet)]

Les paramètres de la configuration des événements de type SNMP v3 sont les suivants :

Port	Port utilisé pour envoyer les données à la machine (*snmptrap* par défaut).
Nom d'utilisateur (securityName)	Nom de l'utilisateur autorisé à envoyer un *trap* sur la station de gestion. Notez que lorsque l'identifiant du serveur ci-dessous n'est pas renseigné (*engineID*), ce nom d'utilisateur (*securityName*) doit être le même que celui utilisé pour la connexion à l'agent SNMP.
Identifiant (engineID)	Chaîne en hexadécimal créée par la station de gestion pour identifier l'utilisateur de manière unique de type 0x0011223344. Le moteur ID doit être composé au minimum de 5 octets et au maximum de 32 octets. Notez que si ce champ est vide, l'agent SNMP doit être configuré pour recevoir un identifiant qui change car celui-ci est auto-généré à chaque redémarrage du service.
Niveau de sécurité	Différents niveaux de sécurité sont disponibles pour la version du protocole SNMP : • **Aucun** : aucune sécurité. Les parties « Security Level : authentification » et « Security level : Chiffrement » sont grisés. • **Authentification, pas de chiffrement** : authentification sans chiffrement des *traps*. • **Authentification et chiffrement** : si le mot de passe chiffrement reste vide on utilise le mot de passe authentification pour le chiffrement.

Paramètres d'authentification

Mot de passe	Mot de passe de l'utilisateur.
Algorithme	Deux types d'authentification sont disponibles, le MD5 (algorithme de hachage qui calcule un condensé de 128 bits) et le SHA1 (algorithme de hachage qui calcule un condensé de 160 bits). Par défaut, l'authentification se fait en MD5.

Paramètres de chiffrement

Mot de passe	Les paquets SNMP sont chiffrés en DES ou AES-128, une clé de chiffrement peut être définie. Par défaut c'est la clé d'authentification qui est utilisée. **AVERTISSEMENT** **Il est vivement recommandé d'utiliser une clé spécifique.**

L'onglet SNMPv1 - SNMPv2c

L'option **Activer SNMPv1/v2c** ou **SNMPv1/v2c et SNMPv3** permet l'activation du module SNMP v1 et v2c.

Connexion à l'agent SNMP

Communauté	Les premières versions du protocole **SNMP** ne sont pas sécurisées. Le seul champ nécessaire est le nom de la communauté. Par défaut le RPV (*Réseau Privé Virtuel*) propose le nom "public". **AVERTISSEMENT** Nous vous conseillons toutefois de ne pas l'utiliser pour des raisons de sécurité. Si vous souhaitez indiquer plusieurs communautés, séparez-les par des virgules.

Envoi des alertes SNMPv2c (*traps*)

Liste des serveurs SNMP

Serveur de destination (objet)	Machine recevant les *traps*, (objet de type « Machine »).
Port	Port utilisé pour envoyer les *traps* à cette machine (objet de type : service). Par défaut, *snmptrap*.
Communauté	Indication de la communauté.

Envoi des alertes SNMPv1 (*traps*)

Par défaut, la liste des machines recevant de *traps* v1 est minimisée pour orienter l'utilisateur vers la version v2c.

Liste des serveurs SNMP

Machine	Machine recevant les *traps*, (objet de type « Machine »).
Port	Port utilisé pour envoyer les *traps* à cette machine (objet de type : service). Par défaut *snmp trap*.
Communauté	Indication de la communauté.

MIB et *Traps* SNMP

Simple Network Management Protocol (SNMP) vous permet de surveiller le parc machine de votre réseau. L'envoi des alertes SNMP (*traps*) et l'écoute des informations (MIB) se paramètrent à l'aide du module **Agent SNMP** de l'interface Web d'administration web du firewall.

Vous pouvez y configurer les stations vers lesquelles le firewall doit envoyer les *traps* et configurer l'accès à celles qui collectent les informations. Ce gestionnaire vous permet de communiquer avec l'agent SNMP d'un firewall et d'obtenir, de gérer et de superviser les données de n'importe quel firewall à travers le réseau. L'agent SNMP autorise l'accès en lecture seule des superviseurs conforme aux versions SNMP v1, v2c, et v3.

Pour la configuration du suivi des informations et pour recevoir les *traps* Stormshield, vous devez au préalable télécharger les MIB (des fichiers au format texte qui décrivent une liste d'objets SNMP utilisés par le superviseur). Ces MIB mettent donc à disposition les informations dont le superviseur a besoin pour interpréter les *traps* SNMP, les événements et les messages de requêtes envoyées au firewall.

Télécharger les MIB

Téléchargez les MIB depuis votre espace personnel MyStormshield (authentification requise) : menu **Téléchargements > Téléchargements > Stormshield Network Security > MIB SNMP** > MIB correspondant à votre version SNS.

MIB Stormshield Network

Voici la liste des MIB Stormshield Network, les commandes CLI / Serverd correspondantes, ainsi que les commandes console.

La MIB *STORMSHIELD-SMI-MIB* est une MIB chapeau de l'ensemble des MIB.
La MIB *STORMSHIELD-VPN-MIB* est une MIB chapeau des MIB *VPNIKESA*, *VPNSA* et *VPNSP*.

MIB Stormshield Network	Contenu	CLI / Serverd	Console
STORMSHIELD-ALARM-MIB	Alarmes déclenchées		sfctl -s log
STORMSHIELD-ASQ-STATS-MIB	Statistiques de l'IPS		sfctl –s stat
STORMSHIELD-AUTHUSERS-MIB	Utilisateurs authentifiés	MONITOR USER	sfctl -s user
STORMSHIELD-AUTOUPDATE-MIB	État des modules mis à jour par Active Update	MONITOR AUTOUPDATE	
STORMSHIELD-HA-MIB	Informations relatives à la haute disponibilité	HA INFO	hainfo
STORMSHIELD-HEALTH-MONITOR-MIB	État de santé du firewall	MONITOR HEALTH	
STORMSHIELD-HOSTS-MIB	Table des machines protégées	MONITOR HOST	sfctl -s host
STORMSHIELD-IF-MIB	État des interfaces vues par l'IPS	MONITOR INTERFACE	sfctl -s global
STORMSHIELD-IPSEC-STATS-MIB	Statistiques IPsec		ipsecinfo
STORMSHIELD-OVPNTABLE-MIB	Clients connectés au VPN SSL	MONITOR OPENVPN LIST	
STORMSHIELD-POLICY-MIB	Politique de filtrage	MONITOR POLICY	slotinfo
STORMSHIELD-PROPERTY-MIB	Informations retournées par la commande "SYSTEM PROPERTY"	SYSTEM PROPERTY SYSTEM IDENT SYSTEM LANGUAGE	

STORMSHIELD-QOS-MIB	Informations sur la QoS	MONITOR QOS	sfctl -s qos
STORMSHIELD-ROUTE-MIB	Table des routeurs	MONITOR ROUTE	sfctl -s route
STORMSHIELD-SERVICES-MIB	État des services du firewall	MONITOR SERVICE	dstat
STORMSHIELD-SYSTEM-MONITOR-MIB	Compteurs d'utilisation des ressources de l'IPS	MONITOR STAT	
STORMSHIELD-VPNIKESA-MIB	Table des SA IKE négociées	MONITOR GETIKESA	
STORMSHIELD-VPNSA-MIB	Table des SA	MONITOR GETSA	showSAD
STORMSHIELD-VPNSP-MIB	Table des SP	MONITOR GETSPD	showSPD

ALERTES E-MAIL

L'écran se compose de 3 onglets :

- **Configuration** : permet de procéder aux réglages de base du module comme le paramétrage du serveur SMTP, la fréquence d'envoi des e-mails (en minutes), les alarmes de prévention d'intrusion et les événements système.
- **Destinataires** : permet de créer les groupes qui seront utilisés dans les politiques de mailing ainsi que dans les modules de configuration où l'envoi d'e-mails peut être configuré.
- **Modèles** : permet de visualiser et de modifier les modèles d'e-mails utilisés lors de l'envoi des notifications aux utilisateurs et aux administrateurs.

Onglet Configuration

Cet onglet regroupe tous les paramètres nécessaires à la configuration des alertes e-mails.

Activer les notifications par e-mail	Cette option active la configuration des messages d'alertes. En cas de désactivation, aucun élément de configuration ne sera accessible car le firewall n'enverra pas de mail. Cette option à cocher est désactivée par défaut. La notification via e-mail nécessite un serveur de messagerie capable de recevoir les e-mails provenant du firewall.

Serveur SMTP

Serveur	Ce champ détermine la machine (serveur SMTP) à laquelle le firewall va envoyer les mails, en la sélectionnant dans la base d'objets. Par défaut, ce champ est vide.
Port	Port du serveur SMTP où seront envoyés les e-mails. Une liste permet de sélectionner un objet, dont la valeur indiquée par défaut est « SMTP ».
Adresse E-mail	Précise l'adresse e-mail de l'émetteur et permet d'assurer la compatibilité avec des services SMTP externes comme Microsoft Office 365. L'adresse e-mail de l'émetteur proposée par défaut débute comme suit : '<nom_du_firewall>@'.
Authentification	Il est maintenant possible de définir un identifiant et un mot de passe pour l'émission des e-mails par le firewall. Cette case à cocher permet d'activer l'authentification du firewall lors de l'envoi des mails d'alertes.
Identifiant	Cette entrée est désactivée si l'option Authentification n'est pas cochée. Ce champ permet la saisie du nom d'utilisateur SMTP (cette entrée doit être renseignée si l'Authentification est activée).
Mot de passe	Cette entrée est désactivée si l'option Authentification n'est pas cochée. Ce champ permet la saisie du mot de passe SMTP (cette entrée doit être renseignée si l'Authentification est activée).
Tester la configuration SMTP	Ce bouton permet d'envoyer un e-mail de test pour vérifier la configuration SMTP du firewall. Après avoir cliqué sur **Tester la configuration SMTP**, renseignez l'adresse destinataire de l'e-mail de test puis cliquez sur **Envoyer**.

Fréquence d'envoi des e-mails (en minutes)

Fréquence d'envoi	Cette option vous permet de spécifier la fréquence d'envoi des rapports. Un rapport contient toutes les alarmes détectées depuis le rapport précédent. Ainsi, la réception de l'e-mail s'effectue par tranche horaire et non par alarme déclenchée. La valeur indiquée par défaut est 15. **EXEMPLE** Avec une fréquence d'envoi de 15 minutes, vous serez averti par e-mail toutes les 15 minutes des alarmes déclenchées durant ce laps de temps sur le firewall.

Alarmes de prévention d'intrusion

Ici, vous pouvez notifier un groupe qui recevra les alarmes de prévention d'intrusion. La liste des alarmes est envoyée dans le corps de l'e-mail au groupe spécifié et selon la fréquence d'envoi des e-mails définie dans le champ **Fréquence d'envoi**.

Ne pas envoyer d'e-mails	Pas d'envoi d'e-mails vers un destinataire spécifique pour les alarmes. Cette option, cochée par défaut, est utilisée pour pouvoir activer les notifications par e-mail afin d'approuver les requêtes de certificats, par exemple, sans pour autant générer d'e-mail pour les alarmes.
Envoyer selon le paramétrage des alarmes et événements	Seuls les alarmes de prévention d'intrusion et les événements système pour lesquels la case **Envoyer un e-mail** a été cochée déclencheront l'envoi d'un e-mail.
Envoyer uniquement les alarmes majeures	En cochant cette option, le groupe sélectionné dans le champ suivant, recevra les alarmes majeures, qui auront une action de notification e-mail configurée (module **Applications et Protections** / colonne *Avancé*).
Envoyer les alarmes majeures et mineures	En cochant cette option, le groupe sélectionné dans le champ suivant recevra les alarmes de prévention d'intrusion majeures et mineures, qui auront l'action de notification e-mail configurée (module **Applications et Protections** / colonne *Avancé*).
Destinataire du message	Choix du groupe qui recevra les alarmes de prévention d'intrusion.

Événements système

Ici, vous pouvez notifier un groupe qui recevra les événements système. La liste des événements est envoyée dans le corps de l'e-mail au groupe spécifié et selon la fréquence d'envoi des e-mails définie dans le champ **Fréquence d'envoi**.

Ne pas envoyer d'e-mails	Pas d'envoi d'e-mails vers un destinataire spécifique pour les événements système. Cette option, cochée par défaut, est utilisée pour pouvoir activer les notifications par e-mail afin d'approuver les requêtes de certificats, par exemple, sans pour autant générer d'e-mail pour les événements système.
Envoyer uniquement les alarmes majeures	En cochant cette option, le groupe sélectionné dans le champ suivant recevra les événements système majeurs, qui auront l'action de notification e-mail configurée (module **Applications et Protections** / colonne *Avancé*).

Envoyer les alarmes majeures et mineures	En cochant cette option, le groupe sélectionné dans le champ suivant recevra les événements système majeurs et mineurs, qui auront l'action de notification e-mail configurée (module **Applications et Protections** / colonne *Avancé*).
Destinataire du message	Choix du groupe qui recevra les événements système.

NOTE
L'état des événements système est visible dans le module **Notifications > Événements système**.

Onglet Destinataires

Dans cet onglet, vous pouvez créer des groupes contenant des destinataires. Chaque destinataire est représenté par une adresse e-mail. Il n'existe aucun groupe pré-configuré. Vous pouvez créer jusqu'à 50 groupes. Le nombre d'adresses e-mails dans un groupe est indéfini.

Une fois un groupe créé, il peut être utilisé dans les politiques de mailing ainsi que dans les modules de configuration où l'envoi d'e-mails peut être configuré.

L'écran se compose de 2 zones :

- Une zone contenant les groupes de destinataires,
- Une zone contenant les membres du groupe de destinataires sélectionné.

NOTE
Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Créer un groupe de destinataires

1. Cliquez sur le bouton **Ajouter**.
2. Saisissez le **Nom** que vous souhaitez donner à votre groupe.
3. Vous pouvez ajouter un commentaire au groupe en complétant le champ prévu à cet effet.
4. Validez en cliquant sur **Appliquer**.

Ajouter un destinataire à un groupe

1. Sélectionnez au préalable le groupe concerné dans la zone de gauche.
2. Dans la zone de droite, cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'affiche, ajoutez le destinataire (utilisateur ou groupe) selon deux possibilités :
   - Si l'utilisateur (ou le groupe) que vous souhaitez ajouter est présent dans l'annuaire LDAP par défaut du firewall, cochez la case **Utilisateur - Groupe présent dans l'annuaire LDAP et** sélectionnez l'utilisateur ou le groupe dans la liste déroulante.
   - Sinon, renseignez directement l'adresse e-mail souhaitée dans le champ **Adresse e-mail**.

Supprimer un groupe

1. Sélectionnez dans la zone de gauche le groupe que vous souhaitez supprimer.
2. Cliquez sur **Supprimer**, puis confirmez la suppression. Si le groupe concerné est utilisé dans la configuration du firewall, vous pouvez : forcer sa suppression, vérifier où il est utilisé, et annuler l'action.

Vérifier si un groupe est utilisé

Le bouton **Vérifier l'utilisation** permet de vérifier si un groupe de destinataires est utilisé dans les différents modules de configuration du firewall.

1. Sélectionnez au préalable le groupe concerné dans la zone de gauche.
2. Cliquez sur **Vérifier l'utilisation** afin d'effectuer la vérification.

Onglet Modèles

Plusieurs modèles sont disponibles contenant chacun un corps qui diffère selon le message que l'on veut envoyer. Ces modèles permettent d'utiliser un courrier type personnalisable pour l'émission des e-mails.

L'écran se compose de 2 zones :

- Les modèles à gauche,
- La zone d'édition à droite.

Modifier un modèle (HTML)

Chaque modèle comporte du contenu appelé "body" (comme pour une page HTML). Ce contenu est un texte au format libre qui peut contenir des balises HTML simples afin de finaliser la mise en forme.

Ces modèles sont modifiables. Ils peuvent contenir des mot-clés qui seront remplacés ensuite par des valeurs. Par exemple, un mot-clé peut afficher de manière automatique le nom de l'utilisateur.

Pour modifier le contenu d'un modèle, sélectionnez ce modèle dans la liste de gauche.

L'écran de modification s'affiche à droite. Il est accompagné d'un bouton **Appliquer le modèle par défaut** permettant de réinitialiser le modèle à sa présentation initiale.

Demande de certificat

- Accepter la demande de certificat : modèle d'e-mail spécifiant que la demande de certificat a été approuvée par l'administrateur.
- Refuser la demande de certificat : modèle d'e-mail spécifiant que la demande de certificat a été rejetée par l'administrateur.

Enrôlement d'un utilisateur

- Accepter la requête utilisateur : modèle d'e-mail spécifiant que la demande d'enrôlement a été approuvée par l'administrateur.
- Refuser la requête utilisateur : modèle d'e-mail spécifiant que la demande d'enrôlement a été rejetée par l'administrateur.

Management des vulnérabilités

- Vulnérabilités détectées (détaillées) : modèle de rapport de vulnérabilités détaillé, appliqué par défaut.
- Vulnérabilités détectées (résumées) : modèle de rapport de vulnérabilités simple, appliqué par défaut.

Modèle de configuration SMTP

- Tester la configuration SMTP : modèle d'e-mail envoyé lors du test de la configuration SMTP et permettant d'informer l'administrateur que la configuration SMTP du firewall pour les notifications est fonctionnelle.

Parrainage

- Demande de parrainage : modèle d'e-mail informant un utilisateur désigné ("parrain") qu'une personne souhaite se connecter au réseau avec son autorisation. Un clic sur le lien inclus dans l'e-mail valide cette demande.

Liste des variables utilisables dans les différents modèles

Modèles de mails dédiés à la détection de vulnérabilités:

- Sujet du message ($Title)
- Sous-titre ($SubTitle)
- Résumé du message ($MailSummary)
- Résumé des vulnérabilités ($VulnsSummary)
- Machines affectées ($HostsByVuln)
- Applications vulnérables ($VulnsByProduct)
- Pied de page du message ($Footer)

Modèles de mails utilisés pour la demande de certificat et l'enrôlement de l'utilisateur:

- Nom de l'utilisateur ($LastName)
- Prénom de l'utilisateur ($FirstName)
- Date de la demande d'enrôlement ($Date)
- Identifiant de l'utilisateur ($UID)
- URL de téléchargement du certificat ($URL)

Exemple de rapport reçu par e-mail pour les alarmes

Type	Minor
Action	Block
Date	2010-10-11 15:08:32
Interface	dmz2
Protocol	tcp

Source	10.2.18.5:55987 (ed:ephemeral_fw_tcp)
Destination	66.249.92.104:80 (www.google.com)
Description	Prévention injection SQL : instruction OR suspecte dans l'URL

ANTISPAM

L'écran de configuration de l'antispam se compose de trois onglets :

- **Général** : configuration de base du module Antispam (activation, paramètres SMTP, Analyse par réputation…),
- **Domaines en liste blanche** : contient la liste des domaines qui doivent être systématiquement considérés comme légitimes,
- **Domaines en liste noire** : contient la liste des domaines qui doivent être systématiquement considérés comme spammeurs.

Onglet Général

L'activation de l'antispam s'effectue en déterminant quelles seront les analyses activées. Deux choix sont disponibles sur le firewall :

Activer l'analyse par réputation (listes noires DNS - RBL)	Cette option permet de valider l'émetteur auprès d'une liste publique de Spams reconnue (DNSBL).
Activer l'analyse heuristique	Cette option permet d'étudier le contenu du mail pour en déterminer la portée.

Paramètres SMTP

Le serveur de confiance concerne le serveur SMTP. En renseignant ce champ, qui est facultatif, les e-mails seront analysés de manière plus fine par le module **Antispam**.

Nom de domaine du serveur SMTP (FQDN)	Cette information facultative permet de définir un domaine dit "de confiance". Les e-mails relayés par un serveur appartenant au domaine indiqué évitent ainsi l'analyse de domaine. Cela peut être défini pour les mails relayés par les serveurs internes, par exemple. Le protocole SMTP permet aux serveurs relayant les mails, de renseigner un champ indiquant leur identité. Si un mail passe par un serveur appartenant au domaine de confiance, les serveurs précédents sont considérés comme légitimes et l'analyse ne s'appliquera qu'aux suivants.
Action	Il existe 4 actions possibles qui permettent au proxy SMTP de répondre au serveur SMTP distant en indiquant un rejet pour cause de spam : • **Marquer comme spam (dans le sujet du message)** : les mails ne sont pas bloqués mais sont marqués comme spams. • **Bloquer tous les spams (niveau 1, 2 ou 3)** : le mail est rejeté quel que soit le seuil de confiance. • **Bloquer les spams de niveau 2 ou 3** : cette option permet de définir qu'à partir du seuil de confiance de niveau 2, un mail sera rejeté. Les seuils sont : 1 – Bas, 2 – Moyen, 3 – Haut. • **Bloquer uniquement les spams de niveau 3** : cette option permet de définir qu'à partir du seuil de confiance 3 (Haut), le mail sera rejeté.

Pour exemple : si vous configurez au niveau de l'analyse heuristique un seuil de 100, les mails seront considérés comme spam à partir de 100. De 100 à 200, le niveau de confiance sera faible, de 200 à 300, il sera modéré, au dessus de 300, il sera élevé. Si vous avez indiqué au niveau de cette option un seuil de confiance modéré, tous les mails de niveau modéré et élevé (donc au dessus de 200) seront rejetés alors que ceux au dessus de 100 à 200 seront gardés.

NOTE
Lorsque plusieurs méthodes d'analyses sont utilisées simultanément, le plus haut niveau de score est attribué.

Configuration avancée

Les messages identifiés comme spam ne sont pas supprimés par le module **Antispam** du firewall. Cependant, il effectue des actions de modifications du message détecté comme spam de façon à permettre un traitement futur par le client de messagerie Web par exemple. Deux actions de marquage sont disponibles :

Insérer les en-têtes X-Spam	En cochant cette option, le module **Antispam** ajoute au message identifié comme spam, un en-tête synthétisant le résultat de son analyse pour ce message. Cet en-tête antispam, au format "spam assassin" peut ensuite être utilisé par le client de messagerie Web pour effectuer les traitements adéquats sur le message marqué.

Analyse par réputation

L'analyse par liste noire DNS (RBL) (*Real time Blackhole List*) permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Les menus suivants permettent de configurer la liste des serveurs RBL qui seront utilisés pour cette analyse ainsi que le niveau de confiance accordé à chacun des serveurs.

Liste des serveurs de listes noires DNS (RBL)

Une grille affiche une liste des serveurs RBL auxquels le firewall envoie ses requêtes pour vérifier qu'un e-mail n'est pas un spam. Cette liste est actualisée par l'**Active Update**. Elle n'est pas modifiable mais vous pouvez toutefois désactiver certains serveurs en cliquant sur la case présente au début de chaque ligne (dans la colonne **Activé**).

Le niveau spécifié dans les colonnes de la grille indique le niveau de confiance accordé à ce serveur.

Vous pouvez aussi configurer vos propres serveurs RBL. Pour ajouter un serveur, cliquez sur le bouton **Ajouter.** Il est possible de définir jusqu'à 50 serveurs RBL.

Spécifiez un nom pour ce serveur (unique pour la liste des serveurs RBL), une cible DNS (Champ : **Nom de domaine** uniquement. Cela doit être un nom de domaine valide), un niveau de confiance (Bas, Moyen, Haut) et enfin un commentaire. L'indication du commentaire est facultative. Puis cliquez sur **Appliquer.**

Pour supprimer un serveur configuré, sélectionnez-le dans la liste puis cliquez sur **Supprimer**.

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des serveurs de listes noires.

NOTE
La différenciation entre les serveurs RBL nativement configurés par le firewall et les serveurs configurés de manière personnalisée s'effectue grâce au cadenas qui indique les serveurs **RBL** nativement configurés.

Analyse heuristique

L'analyse heuristique est basée sur le moteur antispam Vade Secure. Cet antispam délivre, par un algorithme particulier, un degré de légitimité aux messages.

L'antispam effectue le calcul et attribue un score définissant le caractère "non sollicité" d'un message. Les e-mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme Publicité ou Spam.

L'analyse heuristique propose alors d'ajouter un préfixe au sujet de ces mails, ce qui permet par exemple leur isolement dans un dossier dédié du Client Mail.

Publicités

Pour détecter les e-mails publicitaires, activez l'option **Détecter les e-mails correspondant à des publicités**.

Marquage du sujet des publicités (préfixe)	Le sujet des messages identifiés comme publicité sont préfixés par la chaîne de caractères définie. Par défaut cette chaîne est (ADS *) où * représente le niveau de confiance accordé. Ce score peut varier de 1 à 3. Plus ce score est élevé, plus il est probable que le courrier soit de caractère publicitaire. Quelle que soit la chaîne de caractères utilisée, il est indispensable de prévoir l'insertion du niveau de confiance dans cette chaîne en utilisant *. Cet * sera ensuite remplacé par le score. La longueur maximale du préfixe peut être de 128 caractères. Les courriers identifiés comme publicité sont acheminés et non supprimés. Notez bien que les caractères guillemets double ne sont pas autorisés.

Spams

Marquage du sujet des spams (préfixe)	Le sujet des messages identifiés comme spam sont préfixés par la chaîne de caractères définie. Par défaut cette chaîne est (SPAM *) où * représente le niveau de confiance accordé. Ce score peut varier de 1 à 3. Plus ce score est élevé, plus il est probable que le courrier soit du pourriel. Quelle que soit la chaîne de caractères utilisée, il est indispensable de prévoir l'insertion du niveau de confiance dans cette chaîne en utilisant *. Cet * sera ensuite remplacé par le score. La longueur maximale du préfixe peut être de 128 caractères. Les courriers identifiés comme spam sont acheminés et non supprimés. Notez bien que les caractères guillemets double ne sont pas autorisés.
Score minimal de définition d'un spam [1-150]	L'analyse heuristique réalisée par le module **Antispam** effectue le calcul d'une valeur définissant le caractère "non-sollicité" d'un message. Les e-mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme spams. Cette section permet de définir le seuil à appliquer, par défaut le firewall choisit "100". En modifiant le score, la valeur minimale des 3 seuils de confiance est modifiée. De plus, plus cette valeur calculée est élevée plus le niveau de confiance accordé par l'antispam à l'analyse sera élevé. Les seuils de franchissement des niveaux de confiance ne sont pas configurables dans l'interface d'administration Web.

Onglet Domaines en liste blanche

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme **légitimes**.

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à autoriser. Il est possible de définir jusqu'à 256 domaines. Cliquer sur **Ajouter**. La longueur du nom de domaine ne peut excéder 128 caractères. Le domaine ajouté apparaît dans la liste des domaines en liste blanche. Pour supprimer un domaine donné ou la liste complète des domaines, cliquez sur **Supprimer**.

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des domaines en liste blanche.

NOTE
Le filtrage par liste blanche et liste noire prévaut sur les méthodes d'analyses par liste noire DNS et analyse heuristique. Le nom de domaine de l'expéditeur est successivement comparé aux domaines en liste noire et liste blanche.

Onglet Domaines en liste noire

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme spam.

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à bloquer. Il est possible de définir jusqu'à 256 domaines. Cliquer sur **Ajouter**. La longueur du nom de domaine ne peut excéder 128 caractères. Le domaine ajouté apparaît dans la liste des domaines bloqués. Chaque message identifié comme spam du fait de ces domaines en liste noire seront associés au niveau de confiance le plus élevé (à savoir 3). Pour supprimer un domaine donné ou la liste complète des domaines, cliquez sur **Supprimer**.

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des domaines en liste noire.

NOTE
Le filtrage par liste blanche et liste noire prévaut sur les méthodes d'analyses par liste noire DNS et analyse heuristique. Le nom de domaine de l'expéditeur est successivement comparé aux domaines en liste noire et liste blanche.

ANTIVIRUS

L'écran de configuration du service Antivirus comporte trois zones :

- Une zone de choix de l'antivirus
- Une zone de paramètres
- Une zone concernant l'analyse Sandboxing, disponible uniquement pour le moteur antiviral avancé.

Moteur antiviral

La liste déroulante permet de migrer entre solutions Antivirus (ClamAV ou Antivirus avancé). En sélectionnant un antivirus, le message suivant s'affiche :

« *Le changement d'antivirus nécessite le téléchargement complet de la base antivirale. Durant cet intervalle, l'analyse antivirale échouera* ». Cliquez sur **Changer de moteur** pour valider votre choix.

Une fois que la base est téléchargée, l'antivirus est activé.

Paramètres

L'analyse des fichiers ClamAV

Dans ce menu, vous configurez les types de fichiers qui doivent être analysés par le service Antivirus du firewall Stormshield Network.

Analyse des exécutables compressés	Cette option permet d'activer le moteur de décompression (Diet,Pkite, Lzexe, Exepack…).
Analyses des archives	Cette option permet d'activer le moteur d'extraction et d'analyser les archives (zip, arj, lha, rar, cab…)
Bloquer les fichiers chiffrés ou protégés par mot de passe	Cette option permet de bloquer les fichiers chiffrés ou protégés par mot de passe.
Bloquer les formats de fichiers non supportés.	Cette option permet de bloquer les formats de fichiers que l'antivirus ne peut analyser.

L'analyse des fichiers par l'antivirus avancé

Inspecter les archives	Cette option permet d'activer le moteur d'extraction et d'analyser les archives (zip, arj, lha, rar, cab…).
Bloquer les fichiers protégés par mot de passe	Cette option permet de bloquer les fichiers protégés par mot de passe.

Analyse sandboxing

Ce menu n'est disponible (non grisé) que lorsque le moteur antiviral avancé a été sélectionné. Il nécessite également que l'option sandboxing (Breach fighter) ait été souscrite.

Notez qu'il est possible de soumettre manuellement un fichier sur le site https://breachfighter.stormshieldcs.eu/ afin que ce fichier soit analysé.

Après avoir été soumis à l'analyse sandboxing, le fichier se voit attribuer un score (seuil de malveillance) évalué sur une échelle de 1 à 100. Ainsi, un fichier présentant un score de 0 est reconnu comme non dangereux. Un fichier présentant un score de 100 est reconnu comme étant malveillant.

Seuil d'analyse sandboxing à partir duquel les fichiers seront bloqués	Choisissez dans la liste déroulante, le niveau de malveillance à partir duquel les fichiers doivent être impérativement bloqués par le firewall. Quatre niveaux sont disponibles : • Mineur (score entre 1 et 30) • Suspect (score entre 31 et 70) • Potentiellement malveillant (score entre 71 et 99) • Malveillant (score de 100)

APPLICATIONS ET PROTECTIONS

Ce module va vous permettre de gérer la configuration des alarmes générées par les applications et les protections du Firewall.

Notez que l'intitulé des alarmes est affiché dans la langue du firewall (champ **Langue du Firewall** dans l'onglet *Configuration générale* du module **Système** > **Configuration**) et non dans la langue de connexion à l'interface Web d'administration.

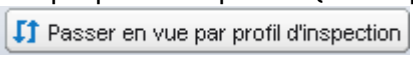
Un **profil d'inspection** (*IPS_00*) est un ensemble de **profils applicatifs** (*default00* – Voir le module **Protocoles**). Un **profil applicatif** contient la configuration des alarmes d'une analyse protocolaire modifiable dans ce module. D'autres éléments de configuration de celle-ci sont accessibles dans le menu «**Protocoles**» correspondant.

Pour configurer les profils d'inspection selon ces profils applicatifs, rendez-vous dans le module **Profils d'inspection** et cliquez sur le bouton *Accéder aux profils*.

Les signatures de ces alarmes sont régulièrement mises à jour via **Active Update** pour les produits sous maintenance (*IPS : signatures de protection contextuelles*) et si cette base est activée dans la configuration d'Active-Update (module **Configuration / Système / Active Update**).

Le déclenchement des alarmes dépend donc de la configuration de ces analyses protocolaires, mais également de la politique de sécurité appliquée.

Dans ce module, la configuration des alarmes est proposée par deux vues par :

- Vue par profil d'inspection (aussi appelé « vue par configuration »)
  

- Vue par contexte (aussi appelé « vue par protocole »)

Nouvelles alarmes

Quand une nouvelle alarme est implémentée, une icône s'affiche dans la colonne *Nouveau* afin d'attirer votre attention.

En cliquant sur *Approuver les nouvelles alarmes*, vous pouvez choisir d'approuver toutes les nouvelles alarmes ou uniquement celles sélectionnées. Les icônes *Nouveau* des alarmes concernées disparaissent.
Notez bien que les nouvelles alarmes sont opérationnelles dès qu'elles sont implémentées : l'approbation sert uniquement à valider le fait que vous avez bien pris connaissance des nouvelles alarmes.

Cette action est applicable aussi bien dans la Vue par profil d'inspection que dans la Vue par contexte.

Vue par profil d'inspection

Sélectionner le profil de configuration

Vous pouvez configurer jusqu'à 10 profils, portant par défaut les noms de « IPS_00 », « IPS_01» etc. Leurs noms ne sont pas modifiables dans le module **Alarmes** mais au sein du menu **Protection applicative** > **Profils d'inspection** (Bouton *Accéder aux profils*) :

1. Sélectionnez une configuration au sein de la liste déroulante.
2. Cliquez sur le bouton **Éditer** et sélectionnez **Renommer**.
3. Changez ensuite le nom du profil dans l'emplacement prévu à cet effet et ajoutez un commentaire si besoin.
4. Cliquez sur **Mettre à jour**.

Vous retrouvez votre profil modifié dans la liste déroulante des configurations du module **Applications et Protections**.

La sélection multiple

La sélection multiple permet d'assigner une même action à plusieurs alarmes. Sélectionnez plusieurs alarmes se succédant à l'aide de touche **Shift** ⇧ ou individuellement avec la touche **Ctrl.** Vous pourrez également soustraire une sélection à une sélection existante, avec la touche **Ctrl.**

Certains intitulés de colonnes affichent l'icône . Par un simple clic, un menu s'affiche et propose d'assigner un même paramètre à plusieurs alarmes sélectionnées (Action, Niveau, Nouveau et Avancé).

Exemple : Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche **Ctrl** puis en cliquant sur **Supprimer**.

Au sein d'un profil, vous pouvez effectuer plusieurs actions :

Appliquer un modèle

Plusieurs modèles permettent de configurer le profil des alarmes en paramétrant leur action (*Autoriser* ou *Interdire*) et leur niveau (*Ignorer*, *Mineur* ou *Majeur)*.

Les modèles BASSE, MOYENNE et HAUTE se différencient essentiellement par l'action des alarmes de type *Protections*, comme les alarmes relatives aux réseaux "peer-to-peer" ou aux messageries instantanées. Par défaut, les alarmes de type *Applications* autorisent le trafic et les alarmes de type *Malwares* le bloquent.

Le modèle INTERNET désactive les alarmes pouvant gêner l'utilisation classique d'Internet, souvent due à de mauvaises pratiques trop répandues pour être interdites. Un exemple est l'alarme levée en cas d'URL contenant des caractères non ASCII.

Par défaut, le profil **(1) IPS_01** est basé sur le modèle INTERNET, étant destiné au trafic dont l'adresse IP source fait partie d'un réseau protégé (Voir **Profils d'Inspection**). Les autres profils sont configurés sur le modèle MOYENNE qui assure un niveau de sécurité standard.

Internet	Cette configuration est adaptée au trafic sortant. La plupart des alarmes sont configurées avec l'action **Autoriser**, quand elles ne présentent pas de danger pour le réseau interne.
Basse	Les alarmes les moins critiques sont configurées avec l'action **Autoriser**.
Moyenne	Ce modèle est un compromis entre sécurité et blocage excessif ; il est appliqué par défaut au trafic entrant.
Haute	La majorité des alarmes sont configurées avec l'action **Bloquer**.

Sélection

Des boutons vous permettent d'effectuer un tri sur les alarmes du profil d'inspection. Les 3 catégories dans lesquelles ces alarmes sont réparties sont **Applications, Protections** et **Malwares**. La sélection s'effectue par les 3 boutons du même nom. Le bouton **Tous** réinitialise la sélection.

Applications	Ce type d'alarme est levé par l'utilisation d'applications courantes. Cette sélection permet l'élaboration d'une **politique de sécurité applicative**.
Protections	Ces alarmes sont levées suite à l'analyse effectuée par le moteur IPS : elles résultent du blocage d'attaques connues ou d'utilisations anormales des protocoles conformément aux **RFC.**
Malwares	Ces alarmes sont basées sur les signatures connues de logiciels malveillants, reconnus par des types d'activité suspects. Il est conseillé d'examiner les machines à l'origine de cette catégorie d'alarmes.

Rechercher

Cet emplacement permet de n'afficher que la ou les alarmes contenant la lettre ou le mot saisi. La recherche est instantanée, afin de filtrer plus facilement les profils et les contextes, sans devoir appuyer sur « Entrée ».

Présélection

Cette liste contient les alarmes générées par un trafic relatif à des familles d'applications. Vous pouvez effectuer un tri et n'afficher que les alarmes faisant partie des catégories suivantes :

Aucune	Toutes les alarmes seront affichées, sans distinction de catégorie.
BYOD	Trafic généré par les appareils mobiles de type téléphone ou tablette électronique pour la pratique qui consiste à utiliser ses équipements personnels (Bring your own device).
Stockage en ligne	Applications proposant l'hébergement de données en ligne.
E-mail	Applications de messagerie en ligne.
Jeu	Applications de jeux en ligne.
Communication	Messagerie instantanée et applications de VOIP ou de visioconférence (Skype, Google talk etc.).
Multimédia	Site d'images, de vidéos ou de musique en ligne.
Peer to peer	Échange direct de fichiers entre utilisateurs.
Accès distant	Contrôle d'ordinateur à distance.
Réseaux sociaux	Sites de communautés en ligne.
Web	Autres applications basées sur les protocoles HTTP / HTTPS.
Protocoles industriels	Alarmes liées au filtrage et à la détection de protocoles industriels (contrôle et fonctionnement d'automates,...)
DoT / DoH	Alarmes liées aux requêtes DNS sur HTTPS (DoH) et sur TLS (DoT).

Cette liste peut être amenée à être modifiée par sa mise à jour via Active Update.

Les différentes colonnes

Pour afficher les colonnes **Signatures, Modèle** et **Profil applicatif,** cliquez sur la flèche apparaissant au survol de l'intitulé d'une colonne et cochez les cases correspondantes proposées dans le menu *Colonnes*.

Signatures	Nombre de variantes de l'attaque ou du trafic que la signature levant l'alarme bloque.
Modèle	Modèle appliqué au profil d'inspection qui configure les alarmes en paramétrant leur action et leur niveau. Consultez la section précédente **Appliquer un modèle**.
Message	Texte décrivant l'alarme et ses caractéristiques. Lors de la sélection d'une alarme, un bouton **Aide** apparaît. Ce lien ouvre une fenêtre d'aide décrivant l'alarme et résumant son action et son niveau.
Profil applicatif	Profil applicatif contenant l'alarme configurée dans ce profil d'inspection.
Action	Lorsqu'une alarme est remontée, le paquet qui a provoqué cette alarme subit l'action associée. Vous pouvez choisir d'**Autoriser ou** d'**Interdire** un trafic qui remonte une alarme.
Niveau	Trois niveaux d'alarmes sont disponibles : **"Ignorer", "Mineur"** et **"Majeur".**
Nouveau	Permet de visualiser les nouvelles alarmes, matérialisées par l'icône .
Contexte : id	Intitulé de l'alarme. L'icône représente les alarmes dites **sensibles**. Référez-vous au paragraphe ci-dessous pour plus d'informations.
Avancé	**Envoyer un e-mail** : un e-mail sera envoyé au déclenchement de l'alarme (cf. module **Alertes e-mails**) avec les conditions suivantes : • **Nombre d'alarmes avant l'envoi**: nombre minimal d'alarmes requises avant le déclenchement de l'envoi, pendant la période fixée ci-après. • **Pendant la période de (secondes)** : délai en secondes pendant lequel les alarmes sont émises, avant l'envoi de l'e-mail. • **Mettre la machine en quarantaine** : la machine responsable de l'alarme sera bloquée avec les paramètres suivants. • **Pour une période de (minutes)** : durée de la mise en quarantaine • **QoS appliquée au flux** : chaque flux applicatif générant une alarme peut désormais se voir appliquer une file d'attente de qualité de service. Cette option permet ainsi d'affecter une limitation de bande passante ou une priorité plus faible au flux à l'origine de l'alarme. • **Capturer le paquet responsable de la remontée de l'alarme** : cette capture pourra être visualisée lors de la consultation des alarmes, grâce à un analyseur de réseau (sniffer) tel que *Wireshark* . • **File d'attente d'acquittement (ACK)** : chaque flux TCP de type ACK peut désormais se voir appliquer une file d'attente d'acquittement (ACK). Cette option permet ainsi d'affecter une limitation de bande passante ou une priorité plus faible au flux à l'origine de l'alarme. Cliquez ensuite sur **Appliquer**.

Pour chacun des 10 profils, vous pouvez effectuer la configuration comme vous le souhaitez, en en modifiant les paramètres décrits ci-avant.

Alarme sensible

L'action Autoriser d'une alarme stoppe l'analyse protocolaire sur le trafic. Il est donc fortement recommandé de dédier aux flux concernés par l'alarme, une règle de filtrage en mode Firewall (ou IDS pour les traces), plutôt que d'Autoriser ce type d'alarme.

Exemple de l'alarme sensible HTTP 47

Microsoft IIS (Internet Information Server) permet la gestion de serveur d'application en utilisant les technologies Microsoft. La gestion de serveurs web propose l'encodage de caractères étendus en utilisant le format "%uXXXX" propriétaire à Microsoft. Cet encodage n'étant pas un standard, les systèmes de détection d'intrusion ne peuvent pas détecter les attaques utilisant cette méthode.

L'accès à un site ayant une URL contenant ce type de caractères encodés, et ne correspondant à aucun caractère valide, lève l'alarme HTTP n°47 - *Encodage en caractère %u invalide dans l'URL* (*Invalid %u encoding char in URL*). Cette alarme considérée comme sensible, bloque l'accès au site.

L'action *Autoriser* appliquée à une alarme bloquant le trafic, stoppe l'analyse protocolaire de cette connexion (incluant les requêtes suivantes).

Afin de maintenir la protection contre ce type d'attaque et dans le même temps, autoriser un accès à ce type de serveur, il est recommandé de dédier une règle de filtrage en mode *Firewall* (ou *IDS* pour les traces), au trafic concerné plutôt que d'*Autoriser* le trafic bloqué par une alarme dite *sensible.* Pour rappel, les modes *Firewall* et *IDS* autorisent l'ensemble du trafic levant des alarmes (avec détection, pour le mode *IDS*).

Vue par contexte

Cette vue présente les alarmes par profils protocolaires. La première liste déroulante, à gauche, permet de sélectionner le contexte protocolaire.

Pour chaque protocole, vous pouvez paramétrer jusqu'à 10 fichiers de configuration, sélectionnables grâce à la seconde liste déroulante (affichant « default »)

Vous pouvez changer le nom du fichier en vous reportant dans le menu **Protection applicative > Protocoles** :

1. Sélectionnez une configuration au sein de la liste déroulante.
2. Cliquez sur le bouton **Éditer** et sélectionnez **Renommer**.
3. Changez ensuite le nom du profil dans l'emplacement prévu à cet effet et ajoutez un commentaire si besoin.
4. Cliquez sur **Mettre à jour**.

Vous retrouvez votre profil modifié dans la liste déroulante des fichiers de configuration du module **Applications et Protections**.

Au sein d'un profil, vous pouvez modifier la politique selon les 4 **modèles** prédéfinis INTERNET, BASSE, MOYENNE et HAUTE, décrits dans la section **« Vue par profil d'inspection »**

AUTHENTIFICATION

La fonction d'authentification permet à l'utilisateur de s'identifier via un login et un mot de passe ou de manière totalement transparente (SSO / certificat). Pour cela, elle peut utiliser une base de données LDAP (*Lightweight Directory Access Protocol*) stockant des fiches utilisateurs et, éventuellement, le certificat numérique x509 qui lui est associé.

Une fois l'authentification réussie, le login de l'utilisateur est associé à la machine à partir de laquelle celui-ci s'est identifié - cela est stocké dans la table utilisateur de l'ASQ - et à tous les paquets IP qui en proviennent, et ce pour la durée spécifiée par l'utilisateur ou l'administrateur selon la méthode utilisée.

Pour être effectives, les méthodes paramétrées (1er onglet) doivent être explicitées dans les règles de la politique d'authentification (2ème onglet).

Le module **Authentification** comporte quatre onglets :

- **Méthodes disponibles** : cet onglet vous propose de choisir une ou plusieurs méthodes d'authentification et de les configurer sur le Firewall pour lui permettre d'appliquer la politique de sécurité. L'authentification peut également être requise par l'administrateur en vue de renseigner l'identité de l'utilisateur de la machine dans les journaux d'audit. Dans cette rubrique, vous pouvez paramétrer plusieurs méthodes car la politique d'authentification autorise l'utilisation de plusieurs de ces méthodes qui seront alors évaluées par ordre, lors du traitement de l'authentification.
- **Politique d'Authentification :** cet onglet permet de spécifier les méthodes selon l'origine de la demande et de définir l'ordre des méthodes d'authentification à appliquer.
- **Portail Captif :** cet onglet permet d'activer l'accès au portail captif depuis différentes interfaces, ainsi que les différentes informations relatives à celui-ci (accès SSL, authentification, proxy). Il vous permet également de personnaliser l'affichage du portail captif.
- **Profils du portail captif** : cet onglet permet de gérer plusieurs profils d'authentification pouvant être utilisés par le portail captif. Ces profils permettent de sélectionner, par exemple, le type de compte utilisé (comptes temporaires, utilisateurs déclarés dans l'annuaire LDAP interne, ...) ou les durées d'authentification autorisées.

NOTE
Le portail captif doit être activé pour toutes les méthodes d'authentification, excepté pour la méthode Agent SSO.

Pour les problématiques liées aux **Objets multi-utilisateur** et les authentifications par **Proxy transparent ou explicite**, référez-vous à la section Proxy HTTP transparent ou explicite et objets multi-utilisateur.

Onglet Méthodes disponibles

Cet écran propose de choisir une ou plusieurs méthodes d'authentification et de les configurer.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des méthodes disponibles :

- Supprimer (la méthode sélectionnée).

Méthodes d'authentification

La colonne de gauche est dédiée à la liste des méthodes d'authentification. La colonne de droite affiche les options de paramétrage de la méthode d'authentification sélectionnée.

Le bouton **Activer une méthode** ouvre une liste déroulante vous proposant de choisir parmi plusieurs méthodes d'authentification, que vous pourrez **Désactiver** si besoin (à l'exception des méthodes LDAP et Agents TS). Ces méthodes sont les suivantes :

- LDAP,
- Certificat (SSL),
- RADIUS,
- Kerberos,
- Authentification transparente (SPNEGO),
- Agent SSO,
- Invités,
- Comptes temporaires,
- Parrainage,
- Mot de passe à usage unique (TOTP),
- Agents TS.

Lorsque la gestion des comptes temporaires est activée sur le firewall, la méthode Comptes temporaires est automatiquement affichée dans la colonne des méthodes d'authentification.

LDAP

La configuration de cette méthode est automatique et nécessite l'implémentation d'une base LDAP. Vous devez vous rendre dans le menu **Utilisateurs** > **Configuration des annuaires** pour y accéder.

Certificat (SSL)

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite, qui présente les éléments suivants :

Liste des autorités de confiance (C.A)

La méthode d'authentification SSL peut accepter l'utilisation de certificats signés par une autorité de certification externe au firewall. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration du firewall de façon à ce que celui-ci accepte tous les certificats effectivement signés par cette autorité.

Si l'autorité de certification est elle-même signée par une autre autorité de certification, il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une "Chaîne de confiance".

Lorsqu'une CA de confiance ou une chaîne de CA de confiance est spécifiée dans la configuration de la méthode d'authentification SSL, elle s'ajoute à la CA interne du firewall implicitement vérifiée dès qu'il existe une autorité racine interne valide sur le firewall.

Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton **Ajouter**, puis sur l'icône s'affichant sur la ligne sélectionnée, on accède à la fenêtre des CA (Cf. *Certificats et PKI*). Si l'autorité de certification à laquelle vous désirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton **Sélectionner** de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les firewalls supportent les **autorités racines multi niveaux** - certificat de l'utilisateur à authentifier signé par une autorité de certification, elle-même signée par une autorité de certification supérieure. Vous pouvez insérer toute la chaine de certification créée par cette autorité racine multi-niveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Supprimer	Supprime l'autorité de certification sélectionnée.

Autorité de certification (C.A) : Ce champ laisse apparaître les certificats auxquels vous faites confiance et que vous serez amenés à utiliser.

Il est possible de modifier le champ du sujet du certificat qui sera utilisé pour rechercher l'utilisateur dans le LDAP. Il est également possible de modifier le champ LDAP utilisé pour la recherche. Par défaut, l'e-mail est utilisé dans les deux cas. Ces paramètres sont configurables en commande CLI.

Configuration avancée

Vous pouvez activer la recherche parmi plusieurs annuaires LDAP.

Différents critères peuvent alors être définis : pour un annuaire donné, il est possible d'indiquer une chaîne de caractères à rechercher dans un champ déterminé du certificat. Cette chaîne est à définir sous forme d'expression régulière.

Activer la recherche dans plusieurs annuaires LDAP	Cocher cette case permet d'activer la recherche des utilisateurs au sein de plusieurs annuaires LDAP et donne accès à la grille des critères de recherche.

Liste des critères de recherche

Chaque critère est défini par un champ de certificat, une expression régulière et un annuaire LDAP.

Vous pouvez **Ajouter**, **Supprimer**, **Monter** ou **Descendre** un critère dans la liste à l'aide des boutons du même nom. Ces critères sont évalués selon l'ordre défini dans la grille.

Champ du certificat	Cette liste déroulante permet de sélectionner le champ du certificat dans lequel les chaînes de caractères sont recherchées.
Expression régulière	Saisissez l'expression régulière définissant les chaînes à rechercher dans le champ du certificat.

Annuaire ou domaine	Sélectionnez l'annuaire LDAP à parcourir pour authentifier les utilisateurs dont le champ de certificat défini contient une chaîne correspondant à l'expression régulière.

RADIUS

RADIUS est un protocole d'authentification standard, fonctionnant en mode client-serveur. Il permet de définir les accès réseau à des utilisateurs distants. Ce protocole est doté d'un serveur relié à une base d'identification (annuaire LDAP etc.). Le firewall peut se comporter comme un client RADIUS et peut alors adresser à un serveur RADIUS externe des demandes d'authentification pour les utilisateurs désirant traverser le firewall. L'utilisateur ne sera authentifié que si le RADIUS accepte la demande d'authentification envoyée par le firewall.

Toutes les transactions RADIUS (communications entre le firewall et le serveur RADIUS) sont elles-mêmes authentifiées par l'utilisation d'un secret pré-partagé, qui n'est jamais transmis sur le réseau. Ce même secret sera utilisé pour chiffrer le mot de passe de l'utilisateur, qui transitera entre le firewall et le serveur RADIUS.

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite.

Accès au serveur

Lorsque la méthode RADIUS est sélectionnée, renseignez les informations relatives à votre serveur RADIUS externe ainsi que d'un éventuel serveur RADIUS de secours.

Serveur	Sélectionnez dans la liste déroulante l'objet représentant le serveur RADIUS. Si cet objet n'existe pas, vous pouvez le créer en cliquant sur l'icône prévue à cet effet. L'authentification RADIUS supporte l'IPv6, l'objet sélectionné peut donc posséder une adresse IPv6 si le firewall est configuré pour utiliser ce protocole.
Port	Port utilisé par le serveur RADIUS. Par défaut, le port 1812 / UDP nommé *RADIUS* est sélectionné. Vous pouvez définir un autre port en le sélectionnant dans la liste déroulante ou en créant un nouvel objet.
Clé pré-partagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur RADIUS.

Serveur de secours

Serveur	Sélectionnez dans la liste déroulante l'objet représentant le serveur de secours. Si cet objet n'existe pas, vous pouvez le créer en cliquant sur l'icône prévue à cet effet. L'authentification RADIUS supporte l'IPv6, l'objet sélectionné peut donc posséder une adresse IPv6 si le firewall est configuré pour utiliser ce protocole.
Port	Port utilisé pour le serveur de secours. Par défaut, le port 1812 / UDP nommé *RADIUS* est sélectionné. Vous pouvez définir un autre port en le sélectionnant dans la liste déroulante ou en créant un nouvel objet.
Clé pré-partagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur de secours.

NOTES

- Par défaut, le délai d'inactivité autorisé pour réaliser une connexion à un serveur RADIUS est de 3000 millisecondes (soit 3 secondes) et le nombre de tentatives de connexion est paramétré à 1.
- Il est possible de configurer de manière avancée le délai d'inactivité et le nombre de tentatives de connexion à un serveur RADIUS principal et de secours en utilisant la commande CLI / Serverd `CONFIG AUTH RADIUS`. Le détail de cette commande est disponible dans le Guide de référence des commandes CLI / Serverd.

Kerberos

Kerberos diffère des autres méthodes d'authentification. Plutôt que de laisser l'authentification avoir lieu entre chaque machine cliente et chaque serveur, Kerberos utilise un chiffrement symétrique, le centre distributeur de tickets (KDC, Key Distribution Center) afin d'authentifier les utilisateurs sur un réseau.

Dans ce processus d'authentification le boîtier agit comme un client qui se substitue à l'utilisateur pour demander une authentification. Cela signifie que même si l'utilisateur est déjà authentifié sur le KDC pour son ouverture de session Windows par exemple, il faut tout de même se ré-authentifier auprès de ce serveur même si les informations de connexion sont identiques, pour traverser le firewall.

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite, qui présente les éléments suivants :

Nom de domaine (FQDN)	Nom de domaine attribué au serveur pour la méthode d'authentification Kerberos. La définition de ce nom de domaine permet de masquer l'adresse IP du serveur et d'en simplifier la recherche. Exemple : www.compagnie.com : **compagnie.com** représente le nom de domaine, plus lisible son adresse IP correspondante : 91.212.116.100.

Accès au serveur

Serveur	Adresse IP du serveur pour la méthode d'authentification Kerberos (*Active Directory* par exemple)
Port	Port utilisé par le serveur. Par défaut, le port 88/UDP nommé Kerberos_udp est sélectionné.

Serveur de secours

Serveur	Adresse IP de rechange du serveur Active Directory pour la méthode d'authentification Kerberos.
Port	Port utilisé par le serveur de secours, si le serveur n'est plus accessible. Par défaut, le port 88/UDP nommé Kerberos_udp est sélectionné.

Authentification transparente (SPNEGO)

La méthode SPNEGO permet le fonctionnement du "Single Sign On" pour l'authentification Web avec un serveur d'authentification externe Kerberos. Cela signifie qu'un utilisateur se connectant à son domaine par une solution basée sur un serveur Kerberos serait automatiquement authentifié sur un firewall Stormshield Network dans le cas d'un accès à

l'Internet (nécessitant une authentification dans la politique de filtrage sur le firewall) grâce à un navigateur Web (Microsoft Edge, Firefox, Mozilla).

Pour mettre en œuvre cette méthode, vous devez au préalable exécuter le script de génération de KEYTAB ***spnego.bat*** sur le contrôleur de domaine. Ce script est disponible dans l'espace personnel MyStormshield (authentification requise), menu **Téléchargements > Téléchargements > Stormshield Network Security > TOOLS**.

REMARQUE
Les paramètres demandés lors de l'exécution du script sont sensibles à la casse et doivent être scrupuleusement respectés car ils ne pourront être modifiés par la suite. En cas d'erreur, il faudra restaurer une sauvegarde du contrôleur de domaine re-procéder à l'installation.

Dans le cas d'un firewall non configuré en haute disponibilité, il est recommandé d'indiquer le numéro de série du firewall plutôt que son nom pour l'identifier (Ce nom correspond au nom indiqué dans le script Stormshield Network livré avec le matériel d'installation). Le *Nom du service* sera le numéro de série précédé de la mention « HTTP/ ». **Exemple :** HTTP/VMSNSXXAZ0000000

Dans le cas d'un firewall en haute disponibilité, l'identifiant devant être commun, il est recommandé d'utiliser le nom du certificat du portail d'authentification (CN) renseigné dans l'onglet *Portail captif* du module **Authentification**.

La configuration de SPNEGO sur le firewall est réalisée grâce aux options expliquées dans le tableau suivant :

Nom du service	Ce champ représente le nom du service Kerberos utilisé par le firewall, obtenu après exécution du script *spnego.bat*
Nom de domaine	Nom de domaine du serveur Kerberos. Il correspond au nom complet du domaine Active Directory et doit être écrit en majuscules.
KEYTAB	Ce champ représente le secret partagé, généré lors de l'utilisation du script sur l'Active Directory. Ce secret doit être fourni au firewall afin qu'il puisse communiquer avec l'Active Directory. Il est également fourni par le script *spnego.bat*

Agent SSO

L'*Authentification Unique* ou *Single Sign-On* (*SSO*) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs services.

La méthode *Agent SSO* requiert l'installation de l'application **Stormshield Network SSO Agent**, service Windows permettant aux Firewalls Stormshield Network de bénéficier de l'authentification sur l'annuaire Windows Active Directory de manière transparente. Pour l'installation de cette application, reportez-vous à la note technique **Stormshield Network SSO Agent - Installation et déploiement.**

Lorsqu'un utilisateur se connecte au domaine Windows par l'ouverture de sa session, celui-ci est automatiquement authentifié sur le Firewall. Le principe est le suivant : l'Agent SSO collecte l'information de l'identification d'un utilisateur sur le domaine en se connectant à distance sur l'observateur d'événements du contrôleur de domaine. L'Agent SSO relaie ensuite ces informations au Firewall par une connexion SSL, qui met à jour sa table des utilisateurs authentifiés.

Depuis la version 3 de firmware, il est possible de déclarer jusqu'à 5 agents SSO, permettant ainsi de gérer l'authentification sur 5 domaines Windows Active Directory dépourvus de relation d'approbation. Ces domaines devront préalablement être déclarés en tant qu'annuaires LDAP externes de type Microsoft Active Directory (module **Utilisateurs** > **Configuration des annuaires**). Les agents SSO supplémentaires seront intitulé Agent SSO 1, Agent SSO 2, ...

Après avoir ajouté cette méthode, vous pouvez saisir les informations relatives à sa configuration.

Agent SSO

Nom de domaine	Sélectionner l'annuaire Microsoft Active Directory correspondant au domaine sur lequel les utilisateurs seront authentifiés. Cet annuaire devra préalablement être paramétré via le module **Configuration des annuaires**.

Agent SSO

Adresse IP	Adresse IP du serveur de la machine hébergeant **Stormshield Network SSO Agent**.
Port	Par défaut, le port "agent_ad" est sélectionné, correspondant au port 1301. Le protocole utilisé est TCP.
Clé pré-partagée.	Cette clé est utilisée pour le chiffrement en SSL des échanges entre l'Agent SSO (machine hébergeant **Stormshield Network SSO Agent**) et le Firewall. Renseignez la **clé pré-partagée** (mot de passe) définie lors de l'installation de l'Agent SSO.
Confirmer la clé pré-partagée	Confirmer la même clé partagée/ mot de passe que dans le champ précédent.
Robustesse du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser des majuscules et des caractères spéciaux.

Agent SSO de secours

Les champs de configuration de l'agent SSO de secours sont les mêmes que décrits précédemment.

Contrôleur de domaine

Vous devez ajouter tous les contrôleurs de domaine régissant le domaine Active Directory sélectionné. Ceux-ci doivent être enregistrés dans la base Objet du Firewall.

Ajouter un contrôleur de domaine	Cliquez pour sélectionner ou créer l'objet correspondant. Vous devez ajouter tous les contrôleurs qui régissent le domaine. Ceux-ci doivent au préalable être enregistrés dans la base Objet du Firewall.

Configuration Avancée

Sélectionnez le mode d'installation utilisé pour l'agent SSO :

- **Mode Windows Active Directory** (agent installé sur un poste ou sur un serveur Windows),
- **Mode serveur Syslog** (agent installé sur une machine Linux Ubuntu).

Champs communs aux Mode Windows Active Directory et Mode serveur Syslog

Durée maximum d'authentification	Définissez la durée maximum de la session d'un utilisateur authentifié. Passé ce délai, le Firewall supprime l'utilisateur de sa table d'utilisateurs authentifiés, déconnectant ainsi l'utilisateur du Firewall. Ce seuil est à définir en secondes ou minutes. Il est par défaut fixé à 36000 secondes, soit 10 heures.
Délai des mises à jour des groupes d'utilisateurs	Si l'annuaire Active Directory est configuré sur le Firewall (Module **Configuration de l'annuaire**), le Firewall consulte les éventuelles modifications apportées aux **groupes de l'annuaire LDAP**. Le Firewall met alors à jour sa configuration de l'annuaire, puis envoie ces informations à l'Agent SSO. Cette durée définie en secondes, minutes ou heures, est fixée par défaut à 3600 secondes, soit 1 heure.

Détection des connexions	Cette option permet de supprimer les utilisateurs authentifiés lorsqu'une machine associée se déconnecte ou lorsqu'une session est fermée. Ce test des machines connectées au Firewall s'effectue soit par la méthode PING, soit par la méthode Base de Registre. Sans l'activation de cette méthode, l'utilisateur ne sera déconnecté uniquement après la durée d'authentification fixée, même en cas de fermeture de sa session.
Méthode de détection	Sélectionnez entre les méthodes de déconnexion **PING** ou **Base de Registre** : • **PING** : l'agent SSO teste l'accessibilité de toutes les machines authentifiées sur le Firewall toutes les 60 secondes par défaut. Dans le cas d'une réponse *host unreachable* ou d'absence de réponse d'une adresse IP après un délai défini ci-après, l'Agent SSO envoie une demande de déconnexion au Firewall. Ce dernier supprime alors l'utilisateur associé à l'adresse IP de sa table d'utilisateurs authentifiés, déconnectant ainsi l'utilisateur du Firewall. • **Base de Registre** : la **Base de registre (BDR)** est une base de données utilisée par le système d'exploitation Windows pour stocker les informations de configuration du système et des logiciels installés. Cette méthode permet par exemple de détecter une session fermée sur une machine toujours allumée. Dans le cas d'une réponse positive au test (PING), l'Agent SSO se connecte à distance sur la machine et vérifie dans la Base de Registre la liste des utilisateurs ayant une session ouverte sur la machine. Cela permet de mettre à jour la table des utilisateurs authentifiés du firewall.
Considérer comme déconnecté après	Si une machine ne répond pas au test d'accessibilité (PING) après ce délai, elle est considérée comme déconnectée. Le Firewall supprime alors l'utilisateur associé à la machine de sa table d'utilisateurs authentifiés. Cette durée est déterminée en secondes, minutes ou heures et est fixée par défaut à 5 minutes.
Détection des connexions	Cette option permet de supprimer les utilisateurs authentifiés lorsqu'une machine associée se déconnecte ou lorsqu'une session est fermée. Ce test des machines connectées au Firewall s'effectue soit par la méthode PING, soit par la méthode Base de Registre. Sans l'activation de cette méthode, l'utilisateur ne sera déconnecté uniquement après la durée d'authentification fixée, même en cas de fermeture de sa session.

Activer la vérification DNS des machines	Cette option permet de gérer les changements d'adresses IP des postes utilisateurs et d'authentifier un utilisateur connecté sur une machine disposant de plusieurs adresses IP.

Comptes d'Administration ignorés	Dans la configuration d'usine du firewall, il existe une liste d'utilisateurs dont l'authentification est ignorée. Cette liste comporte les identifiants usuels dédiés à l'administrateur (Administrator et Administrateur par défaut). Ce mécanisme a été mis en place car le lancement d'un service ou d'une application (fonction Exécuter en tant qu'administrateur, par exemple) est vu par le contrôleur de domaine comme une authentification. Le SN SSO Agent restreignant à une authentification par adresse IP, ce type d'authentification peut potentiellement remplacer l'authentification de l'utilisateur ayant ouvert une session Windows. Cette liste préétablie de « Comptes Administrateur ignorés » permet au SN SSO Agent de ne pas prendre en compte leur authentification. Modifiez-la si nécessaire.

Champs additionnels pour le Mode serveur Syslog

Configuration du serveur Syslog

Adresse IP d'écoute	Indiquez l'adresse IP du serveur syslog.
Port d'écoute	Indiquez le port d'écoute du serveur syslog. L'objet réseau **syslog** est proposé par défaut.
Recherche d'adresse IP (expr. régulière)	Précisez l'expression régulière destinée à rechercher les adresses IP dans les logs hébergés par le serveur syslog. Exemple : ([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s|
Recherche d'utilisateur (expr. régulière)	Précisez l'expression régulière destinée à rechercher les noms d'utilisateurs dans les logs hébergés par le serveur syslog. Exemple : JOHN\\([a-zA-Z0-9\.]*)\s permettra de détecter des entrées du type JOHN\john.doe
Recherche de message (expr. régulière)	Précisez l'expression régulière destinée à rechercher les messages de connexion dans les logs hébergés par le serveur syslog. Exemple : connect|ok permettra de détecter des entrées du type JOHN|connect|ok|sysvol

Configuration du serveur syslog de secours

Il vous est possible de préciser un serveur syslog de secours

Adresse IP d'écoute	Indiquez l'adresse IP du serveur syslog de secours.

Invités

Ce mode permet une identification sans authentification, pour l'accès à un réseau WiFi public, par exemple. Cette méthode déclenche automatiquement l'affichage de conditions d'utilisation d'accès à Internet. Ces conditions sont personnalisables dans l'onglet **Portail captif**. La fréquence de cet affichage validant l'authentification, est par défaut de 18 heures et peut être modifiée dans le paramétrage de cette méthode (*disclaimertime*).

La connexion de ces utilisateurs « invités » est notifiée dans les traces par l'ajout des adresses MAC sources. Cette identification est vérifiée toutes les 4 heures, ce réglage est paramétrable par la commande CLI suivante :

CONFIG AUTH GUEST (exemple : state=1 logontime=14400 disclaimertime= 64800)

NOTE
Dans la politique de sécurité, l'objet Utilisateur à sélectionner pour correspondre à la méthode Invités est **Tous**.

Fréquence d'affichage des Conditions d'utilisation de l'accès à Internet	Avec cette méthode, des Conditions d'utilisation d'accès à Internet - communément appelé Disclaimer - sont systématiquement affichées à l'utilisateur. Une case signifiant son accord est à cocher par l'utilisateur avant d'être s'authentifié. Ces conditions sont personnalisables dans l'onglet « Portail Captif ». Si la fonctionnalité est également activée dans les profils du portail captif, cette fréquence d'affichage est distincte de celle paramétrée pour les autres méthodes.

Comptes temporaires

Ce service permet la gestion de comptes dont la durée de validité est limitée. Ces comptes sont destinés à fournir temporairement un accès Internet public à des personnes externes à l'entreprise. Les comptes temporaires ne sont pas enregistrés dans le ou les annuaire(s) LDAP déclaré(s) sur le firewall.

Durée de validité par défaut d'un nouveau compte (jours)	Ce champ permet de fixer une durée de validité (en jours) qui sera proposée par défaut lors de la création d'un nouveau compte temporaire.

Le lien **Accéder à la liste des comptes temporaires** vous renvoie directement vers le module **Utilisateurs** > **Comptes temporaires** afin de gérer (ajouter, modifier, supprimer) ces comptes.

Parrainage

Ce mode permet une identification sans authentification au travers du portail captif. Elle nécessite la saisie par le filleul de ses nom et prénom, ainsi que de l'adresse e-mail du parrain. Le parrain reçoit alors un e-mail contenant un lien pour valider cette requête. Suite à la validation, le filleul est automatiquement redirigé du portail captif vers la page Web demandée.

Durée minimale d'authentification	Définissez la durée minimale d'une session pour un utilisateur parrainé. Ce seuil est à définir en minutes, heures ou jours. Il est par défaut fixé à 15 minutes.
Durée maximale d'authentification	Définissez la durée maximale d'une session pour un utilisateur parrainé. Passé ce délai, le Firewall déconnecte l'utilisateur. Ce seuil est à définir en minutes, heures ou jours. Il est par défaut fixé à 240 minutes, soit 4 heures.

Cette méthode d'authentification nécessite la configuration d'un serveur SMTP sur le firewall. cliquez sur le lien **Configuration du serveur SMTP** pour accéder au module ALERTES E-MAIL permettant cette configuration.

TOTP (2FA SNS)

La méthode d'authentification 2FA utilisant des mots de passe à usage unique basés sur le temps (TOTP - *Time-based One-time Password*) permet d'accroître la sécurité des authentifications gérées par le firewall.

Cette sécurisation supplémentaire des accès est embarquée sur le firewall et ne nécessite pas la mise en place d'une solution TOTP tierce. Les utilisateurs soumis à l'authentification TOTP SNS n'ont besoin que d'une application sur leur smartphone ou dans leur navigateur Internet pour générer les codes d'authentification TOTP.

Cette méthode peut notamment être activée pour toutes les authentifications : portail captif, tunnels VPN SSL, interface Web d'administration, connexions console ou SSH, tunnels VPN IPsec / Xauth.

NOTE
Cette méthode 2FA étant embarquée sur chaque firewall, un utilisateur devra utiliser autant de codes TOTP que de firewalls sur lesquels il doit se connecter.

NOTE
Stormshield recommande fortement d'activer la synchronisation de temps via NTP pour le firewall en cochant la case Maintenir le firewall à l'heure (NTP) et en précisant des serveurs NTP (module Système > Configuration > onglet Configuration générale).

Mot de passe à usage unique basé sur le temps (TOTP)

Sélectionner les authentifications gérées par le firewall qui seront soumises au TOTP.
Les types d'authentifications possibles sont :

- Portail captif,
- Tunnels VPN SSL,
- Interface Web d'administration,
- SSH / Console,
- IPsec (Xauth / EAP).

Paramètres des codes (TOTP)

Ces informations sont présentées sur le portail captif du firewall lors de l'enrôlement TOTP de l'utilisateur.

Émetteur	Vous pouvez préciser l'émetteur du code TOTP (nom de votre entreprise par exemple). La valeur proposée par défaut est Stormshield Network Security.

Personnaliser le message d'enrôlement des utilisateurs TOTP

Message à afficher (1024 caractères max.)	Vous pouvez définir un message (optionnel) qui sera affiché sur le portail captif du firewall lors de l'enrôlement TOTP de l'utilisateur. Saisissez ce message dans le champ texte en respectant la limite de 1024 caractères.

Configuration avancée

ATTENTION
Si vous utilisez Google Authenticator ou Microsoft Authenticator, la modification de ces paramètres entraîne un dysfonctionnement de l'authentification TOTP.

Durée de vie (s)	Indiquez la durée de vie d'un code TOTP. Un nouveau code sera généré automatiquement par l'application de l'utilisateur un fois ce laps temps écoulé. La valeur proposée par défaut est de 30 secondes.
Taille du code	Indiquez la longueur (nombre de caractères) des codes TOTP générés. La valeur proposée par défaut est 6.
Nombre de codes valides avant et après le code actuel	En cas de légère désynchronisation de temps entre le firewall et l'équipement hébergeant la solution de génération des codes TOTP (smartphone, ordinateur), ou pour permettre un délai raisonnable de saisie du code, cette option permet de préciser combien de codes survenus avant ou devant survenir après le code actuellement valide seront également considérés comme valides et acceptés pour l'authentification.
Algorithme de hachage	Sélectionnez l'algorithme de hachage utilisé lors de la génération des codes TOTP. Les valeurs possibles sont : • SHA1, • SHA256, • SHA512. La valeur proposée par défaut est SHA1.

Les deux boutons présents dans ce cadre permettent de manipuler la base des utilisateurs ayant réalisé leur enrôlement TOTP.

Réinitialiser la base TOTP	En cliquant sur ce bouton, vous pouvez réinitialiser la base complète des utilisateurs ayant réalisé leur enrôlement TOTP. Les utilisateurs devront donc de nouveau suivre la procédure complète d'enrôlement TOTP lors de leur prochaine authentification. Si vous souhaitez réinitialiser la base TOTP complète : 1. Cliquez sur le bouton **Réinitialiser la base TOTP**. Une fenêtre d'avertissement s'affiche. 2. Validez cette action en cliquant sur le bouton **Continuer**. **NOTE** Réinitialiser la base TOTP nécessite d'être connecté avec le compte *admin*.

Afficher les orphelins TOTP	Un utilisateur orphelin est un utilisateur présent dans la base TOTP mais qui est introuvable dans les annuaires LDAP configurés sur le firewall et dont la dernière utilisation de code TOTP remonte à au moins 3 mois. Ce bouton permet d'afficher les utilisateurs orphelins mais aussi de les supprimer de la base TOTP (suppression de **tous** les orphelins TOTP). Si vous souhaitez afficher les utilisateurs orphelins présents dans la base TOTP : 1. Cliquez sur le bouton **Afficher les orphelins TOTP**. Une fenêtre de sélection s'affiche. 2. Sélectionnez dans le calendrier la date de dernière utilisation de code TOTP pour laquelle vous souhaitez afficher les utilisateurs orphelins. La date proposée par défaut est la date remontant 3 mois avant la date du jour. Les utilisateurs correspondant sont affichés. Pour supprimer **tous** les utilisateurs orphelins listés dans cette grille : 1. Cliquez sur le bouton **Supprimer**. 2. Confirmez la suppression de **tous** les utilisateurs orphelins en cliquant sur le bouton **OK**. Pour quitter la grille sans supprimer les utilisateurs orphelins, cliquez sur le bouton **Annuler**.

Agents TS

Cette méthode d'authentification transparente et multi-utilisateurs est destinée aux infrastructures de postes virtuels (Virtual Desktop Infrastructure - VDI).
Elle repose sur des échanges entre le firewall SNS et un ou plusieurs agents nommés SN TS Agents déployés directement sur les serveurs VDI (serveurs Citrix Virtual Apps and Desktops ou Microsoft Remote Desktop Services).

Un firewall SNS peut gérer jusque 100 SNS Agents TS.

Pour plus d'informations, reportez-vous à la **Note Technique** SN TS Agent - Installation et déploiement.

Agents TS

Délai avant désauthentification des utilisateurs déconnectés (sec.)	Il s'agit du délai au bout duquel les utilisateurs déconnectés accidentellement, ou ayant interrompu brutalement une session à distance, seront supprimés de la table des utilisateurs authentifiés dans le moteur de prévention d'intrusion. La valeur proposée par défaut est de 30 secondes. Elle peut être portée au maximum à 300 secondes (5 minutes).

Liste des Agents TS

Il est possible d'**Ajouter** ou de **Supprimer** un Agent TS en cliquant sur les boutons du même nom.

Ajouter un Agent TS

1. Cliquez sur le bouton **Ajouter**.
Une fenêtre présentant les différents paramètres à renseigner s'affiche.
2. A l'aide du curseur, activez (position **ON**) ou non (position **OFF**) l'Agent TS en cours de création.

NOTE
Il est conseillé de créer les Agents TS en les laissant en état inactif afin de ne pas générer d'alarmes et de logs inutiles. Ils seront activés une fois les Agents TS déployés sur les serveurs RDS / Citrix.

3. Renseignez le **Nom de l'Agent TS**.
4. Sélectionnez ou créez directement l'objet correspondant au **Serveur TS** (serveur RDS / Citrix) sur lequel sera installé l'Agent TS.
5. Sélectionnez le **Port** de communication entre le firewall et l'Agent TS.
   L'objet *agent_ts* (TCP/1303) est proposé par défaut.
6. Définissez et confirmez la **Clé pré-partagée** utilisée lors de la communication avec l'Agent TS.
7. Validez la configuration en cliquant sur **Appliquer**.

Supprimer un Agent TS

1. Sélectionnez une ligne de la grille des Agents TS.
2. Cliquez sur **Supprimer**.
3. Confirmer la suppression en cliquant sur **OK**.

Changer l'état d'un Agent TS

Pour modifier l'état (*on* / *off*) d'un Agent TS, double-cliquez dans la colonne **État** de cet Agent TS .

Modifier un Agent TS

Pour modifier un ou plusieurs paramètres d'un Agent TS, double-cliquez dans une colonne autre que la colonne **État** de cet Agent TS.

La grille des Agents TS

État	Indique si la communication avec l'Agent TS est activée (*on*) ou désactivée (*off*).
Nom	Nom de l'Agent TS.
Adresse	Objet correspondant au serveur sur lequel l'Agent TS est installé. En survolant cet objet avec la souris, l'adresse IP du serveur est affichée.
Clé pré-partagée	Le survol de ce champ avec la souris permet d'afficher la clé pré-partagée utilisée lors de la communication avec l'Agent TS.
Port de connexion	Affiche l'objet correspondant au **Port** de communication utilisé entre le firewall et l'Agent TS.

Configuration avancée

Comptes d'Administration ignorés	Il est possible, pour chaque Agent TS configuré, d'exclure des comptes d'administration du mécanisme d'authentification Agent TS. Dans ce cas, les flux initiés par les comptes administrateurs sélectionnés, bien qu'ils puissent correspondre à des règles de filtrage autorisant la méthode Agent TS, sont bloqués par le firewall.

Pour ajouter un compte s'administration ignoré :

1. Dépliez le cadre **Configuration avancée**,
2. Dans la grille **Comptes d'administration ignorés**, cliquez sur **Ajouter**,

3. Sélectionnez un Agent TS précédemment configuré,
4. Saisissez le nom du compte d'administration à ignorer.

Onglet Politique d'authentification

La grille de filtrage vous permet de définir les règles de la politique d'authentification à appliquer à travers le Firewall. Les règles prioritaires sont placées en haut. Le firewall exécute les règles dans l'ordre (règle N°1, 2 et ainsi de suite) et s'arrête dès qu'il trouve une règle correspondant au trafic. Il convient donc de définir les règles dans l'ordre du **plus spécifique au plus général**.

Si aucune règle de la politique n'est définie ou si le trafic ne correspond à aucune règle spécifiée, la *Méthode par défaut* est appliquée. Si celle-ci n'est pas paramétrée ou que le choix est *Interdire*, toute authentification sera alors refusée.

Les actions sur les règles de la politique d'authentification

Recherche par utilisateur...	Ce champ permet la recherche par l'identifiant d'utilisateur. Les règles attribuées à cet utilisateur s'affichent dans la grille. **Exemple** : Si vous saisissez « utilisateur1 » dans le champ, toutes les règles de la politique ayant comme source l'« utilisateur1 » s'affichent dans la grille.

Nouvelle règle	Insérer une ligne prédéfinie ou à définir après la ligne sélectionnée ; 5 choix sont possibles : • **Règle standard** : en la sélectionnant, un assistant d'authentification s'affiche. Voir la section suivante pour les options proposées des écrans. • **Règle Invités :** cet assistant vous propose la création d'une règle d'authentification par la méthode *Invités*. Cette méthode ne peut être combinée avec d'autres méthodes au sein de la même règle, car elle ne requiert pas d'identification. **NOTE** L'objet Utilisateur à sélectionner pour correspondre à la méthode *Guest* est « Tous ». **NOTE** Cette méthode n'est pas compatible avec les objets multi-utilisateurs ; tous les utilisateurs connectés en mode *Guest* doivent avoir des adresses IP différentes. • **Règle Comptes temporaires** : cet assistant vous propose la création d'une règle d'authentification par la méthode des *Comptes temporaires*. Cette méthode ne peut être combinée avec d'autres méthodes au sein de la même règle. • **Règle Parrainage** : cet assistant vous propose la création d'une règle d'authentification par la méthode *Parrainage*. Cette méthode ne peut être combinée avec d'autres méthodes au sein de la même règle, car elle ne requiert pas d'identification. • **Séparateur – regroupement de règles** : Cette option permet d'insérer un séparateur au-dessus de la ligne sélectionnée et contribue à améliorer la lisibilité et la visibilité de la politique d'authentification. Elle peut, par exemple, permettre à l'administrateur de hiérarchiser ses règles. Ou de regrouper celles qui régissent le trafic vers les différents serveurs. Vous pouvez plier et déplier le nœud du séparateur afin de masquer ou afficher le regroupement de règle. Vous pouvez également copier / coller un séparateur d'un emplacement à un autre.
Supprimer	Supprime la règle sélectionnée.
Monter	Ce bouton permet de placer la règle sélectionnée avant la règle directement au-dessus.
Descendre	Ce bouton permet de placer la règle sélectionnée après la règle directement en-dessous.
Couper	Ce bouton permet de couper une règle d'authentification pour la déplacer.
Copier	Ce bouton permet de copier une règle d'authentification dans le but de la dupliquer.
Coller	Ce bouton permet de dupliquer une règle d'authentification, après l'avoir copié.

Menu contextuel

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles d'authentification :

- Nouvelle règle (Règle standard, Règle Invités, Règle Comptes Temporaires, Règle Parrainage, Séparateur - Regroupement de règles),
- Supprimer,
- Couper,
- Copier,
- Coller.

Nouvelle règle

La politique d'authentification permet de créer des règles se basant sur un utilisateur ou des groupes d'utilisateurs. Il est également possible de cibler le trafic en précisant son origine. Cliquer sur le bouton « **Nouvelle règle** » et sélectionner « **Règle standard** », « **Règle Invités** », « **Règle Comptes temporaires** » ou « **Règle Parrainage** » pour exécuter l'assistant.

Étape 1 : Action

Action à appliquer pour cette règle : sélectionnez l'action à appliquer lorsqu'une demande d'authentification correspond à cette règle.

L'action choisie peut être :

- Autoriser,
- Interdire,
- Par défaut (action choisie dans le cadre **Action à appliquer par défaut** sous la grille de la politique d'authentification).

Étape 2 : Authentification d'Utilisateurs

Sélectionnez l'utilisateur, le groupe d'utilisateurs ou laissez la valeur par défaut "Any user@*default_domain*" où *default_domain* représente l'annuaire / domaine défini par défaut sur le firewall.
Cette étape n'est pas proposée pour les règles associées aux méthodes "**Invités**" ou "**Parrainage**".

Étape 3 : Source

Cliquez sur **Ajouter une interface** ou **Ajouter un objet** afin de cibler l'origine (source) du trafic concernée par la règle. Cela peut être l'interface sur laquelle est connecté votre réseau interne (ex : interface *in*) ou l'objet correspondant aux réseaux internes (ex : *Network_internals*).

NOTE
La méthode d'authentification Agent SSO ne peut être appliquée avec comme critère une Interface. En effet, cette méthode se base sur les événements d'authentification collectés par les contrôleurs de domaine, n'indiquant pas l'origine du trafic. Une règle combinant une interface comme origine et la méthode Agent SSO n'est donc pas autorisée.

NOTE
Le choix d'une interface propose l'interface VPN SSL, désignant l'interface sur laquelle sont connectés les utilisateurs d'un tunnel VPN SSL.

Étape 4 : Méthodes d'authentification

Cette étape n'est pas proposée pour les règles associées aux méthodes "**Invités**", "**Comptes temporaires**" ou "**Parrainage**".

Cliquez sur **Activer une méthode** et sélectionnez dans la liste déroulante les méthodes d'authentification souhaitées. La *Méthode par défaut* sélectionnée correspond à la méthode choisie dans l'onglet « **Méthodes disponibles** ».

Il est également possible de sélectionner l'entrée « Interdire », bloquant ainsi toute authentification sur le trafic concerné par la règle.

Mot de passe à usage unique	Si vous souhaitez ajouter l'utilisation d'un mot de passe à usage unique basé sur le temps (TOTP) à cette méthode d'authentification, mettez le curseur en position ON : La colonne **Mot de passe à usage unique** est alors cochée sur la ligne de la règle d'authentification correspondante dans la politique d'authentification.

Les méthodes d'authentification **sont évaluées dans l'ordre de la liste** et du haut vers le bas. La méthode *Agent SSO* étant transparente, elle est par définition, toujours appliquée en priorité.

Pour **activer** la nouvelle règle créée, double cliquez sur *Désactivé* dans la colonne **État** de la grille des règles d'authentification.

Réorganisation des règles

Chaque règle peut être glissée et déplacée pour réorganiser aisément la politique d'authentification. Le symbole ainsi que l'infobulle "Glissez et déplacez pour réorganiser" apparaissent lorsque la souris survole le début de la règle.

Action par défaut

Action à appliquer par défaut	Sélectionnez l'action qui sera appliquée : • Si la demande d'authentification ne correspond à aucune règle définie dans la politique, • Pour les règles dont l'action à appliquer a été positionnée sur **Action par défaut**.

Méthode par défaut

Méthode à appliquer par défaut	Sélectionnez la méthode qui sera appliquée lorsque l'entrée *méthode par défaut* sera choisie dans la politique d'authentification. Les méthodes proposées sont celles ajoutées dans le tableau des méthodes disponibles.

Objets multi-utilisateur

Cette grille permet de sélectionner les objets-réseau permettant plusieurs authentifications depuis une même adresse IP. Cela permet par exemple, d'accéder à des applications et des données depuis un ordinateur distant (serveur TSE) en pratiquant du filtrage par utilisateur.

Vous pouvez **Ajouter** ou **Supprimer** un objet multi-utilisateurs en cliquant sur les boutons du même nom.

NOTE
La méthode SSO ne permet pas l'authentification « **multi utilisateur** ».

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des objets multi-utilisateurs :

- Ajouter,
- Supprimer.

Onglet Portail captif

Afin de renforcer la sécurité, la connexion au portail d'authentification et à l'interface d'administration web se fait en forçant certaines options du protocole SSL. La version SSLv3 est désactivée et les versions TLS activées, conformément aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

L'adresse du portail captif ou d'authentification est hébergée sur le firewall et est accessible à l'adresse : **https://<adresse_ip>/auth**.

Le portail captif doit être activé pour toutes les méthodes d'authentification, mis à part pour l'Agent SSO.

Portail captif

Correspondance entre profil d'authentification et interface

Cette grille permet d'associer un profil du profil du portail captif à une interface du firewall. Il est possible d'**Ajouter** ou de **Supprimer** une règle de correspondance en cliquant sur les boutons du même nom ou en effectuant un clic droit dans la grille.

Interface	Choisissez l'interface réseau sur laquelle associer un profil du portail captif. Il peut s'agir d'une interface Ethernet (in, out ...), d'un modem ou d'une interface IPsec.
Profil	Sélectionnez le profil à associer à l'interface. Si un avertissement apparaît précisant que le portail captif est désactivé, activez-le depuis l'onglet **Profils du portail captif**.
Méthode ou annuaire par défaut	La méthode d'authentification ou l'annuaire associé au profil sélectionné est automatiquement affiché.

Serveur SSL

Certificat (clé privée)	Pour accéder au portail en SSL, le module d'authentification du firewall utilise par défaut sa propre autorité de certification (CA) dont le nom associé est le numéro de série du firewall. Ainsi, lorsqu'un utilisateur contacte le firewall différemment que par son numéro de série, il reçoit un message d'avertissement indiquant une incohérence entre ce que l'utilisateur essaie de contacter et le certificat qu'il reçoit. Vous pouvez choisir d'utiliser un autre certificat d'une autre CA préalablement importé en le choisissant dans la zone de sélection. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module. Par défaut, l'authentification d'utilisateurs via le portail captif s'effectue par un accès SSL/TLS utilisant un certificat signé par deux autorités non reconnues par les navigateurs. Il est donc nécessaire de déployer ces autorités de certification utilisées par une GPO sur les navigateurs des utilisateurs. Ces autorité sont la CA NETASQ et la CA Stormshield, elles sont disponibles sur les liens suivants : • http://pki.stormshieldcs.eu/netasq/root.crt. • http://pki.stormshieldcs.eu/products/root.crt. Pour plus de détails, consultez le chapitre Sensibilisation des utilisateurs, partie **Première connexion au boîtier**.

Conditions d'utilisation de l'accès à Internet

Des conditions d'utilisation peuvent être affichées lorsqu'un utilisateur souhaite accéder à Internet. Vous pouvez définir ces conditions en les important au format HTML ou PDF. L'utilisateur devra alors signifier son accord en cochant une case avant d'accéder à Internet.

Sélectionner les conditions d'utilisation d'accès à Internet au format HTML	Importez votre version au format HTML.
Sélectionner les conditions d'utilisation d'accès à Internet au format PDF	Importez votre version au format PDF.
Réinitialiser la personnalisation des Conditions d'utilisation de l'accès à Internet	Ce bouton permet de réinitialiser la personnalisation des conditions d'utilisation de l'accès à Internet.

ASTUCE
Pensez à activer depuis l'onglet **Profils du portail captif** l'affichage des conditions d'utilisation de l'accès à Internet sur le profil du portail captif où vous souhaitez les afficher.

Configuration avancée

Interrompre les connexions lorsque l'authentification expire	Dès que la durée de vie de l'authentification arrive à échéance, les connexions seront interrompues même si l'utilisateur est en cours de téléchargement.
Fichier de configuration du proxy (.pac)	Ce champ permet d'envoyer au firewall le fichier .PAC à distribuer qui représente le fichier de configuration automatique du proxy (Proxy Auto-Config). L'utilisateur peut récupérer un fichier PAC ou alors vérifier son contenu à l'aide du bouton situé à droite du champ. L'utilisateur peut spécifier dans son navigateur web, le script de configuration automatique qui se situe dans *https://if firewall>/config/wpad.dat*.

Portail captif

Port du portail captif	Cette option vous permet de spécifier un port d'écoute autre que le port TCP/443 (HTTPS) défini par défaut pour le portail captif.
Masquer l'en-tête (logo)	Cette option permet de masquer l'en-tête qui apparaît sur le portail captif. Par défaut, il s'agit du logo Stormshield.
Sélectionnez un logo à afficher (800x50 px)	Vous pouvez personnaliser l'image qui sera affichée dans l'en-tête du portail captif. Par défaut, le format de l'image doit être de 800 x 50 px.
Sélectionnez une feuille de style à appliquer (fichier CSS)	Importez une nouvelle feuille de style au format css qui surchargera la charte graphique du portail captif.
Réinitialiser	Ce bouton permet de réinitialiser la personnalisation du portail captif.

Onglet Profils du portail captif

Cet écran permet de sélectionner un profil du portail captif prédéfini ou personnalisable et d'en modifier la configuration.

La barre d'actions

Champ de sélection du profil	Sélectionnez dans le menu déroulant le profil du portail captif que vous souhaitez configurer.
Renommer	Ce bouton permet de renommer le profil sélectionné.
Date de dernière modification	Survolez l'icône pour afficher la date et l'heure de la dernière modification apportée au profil du portail captif sélectionné.

Authentification

Méthode ou annuaire par défaut	Sélectionnez la méthode d'authentification ou l'annuaire LDAP (pour un firewall ayant défini plusieurs annuaires) affecté par défaut au profil en cours d'édition. Les méthodes proposées sont celles définies dans l'onglet **Méthodes disponibles**. **IMPORTANT** Selon la méthode d'authentification ou l'annuaire par défaut sélectionné, certains champs dans ce module ne sont pas modifiables.
Activer le parrainage	Cette option active la méthode parrainage en plus de la méthode d'authentification choisie par défaut. Cette case est automatiquement cochée et grisée lorsque la méthode **Parrainage** est sélectionnée dans le champ ci-dessus.

Conditions d'utilisation de l'accès à Internet

Activer l'affichage des conditions d'utilisation d'accès à Internet	Cette option affiche des conditions d'utilisation lorsqu'un utilisateur accède à Internet. Il devra alors signifier son accord en cochant une case avant de pouvoir s'authentifier. Personnalisez ces conditions depuis l'onglet **Portail captif**. **NOTE** Cette option n'est pas valide pour la méthode d'authentification transparente Agent SSO car elle ne nécessite pas l'activation du portail d'authentification.
Fréquence d'affichage des Conditions	Définissez la fréquence d'affichage des conditions d'utilisation de l'accès à Internet. Cette fréquence concerne toutes les méthodes d'authentification, sauf la méthode **Invités** dont la fréquence se configure depuis l'onglet **Méthodes disponibles**.

Champs personnalisés du portail captif (méthode Invités uniquement)

Lorsque la méthode **Invités** est sélectionnée, trois champs numérotés sont disponibles. Ils permettent d'ajouter jusqu'à trois zones de saisie au portail captif lors de l'affichage des conditions d'utilisation de l'accès à Internet.

Les valeurs possibles pour ces champs sont les suivantes : Vide (désactive l'affichage du champ sur le portail captif), Prénom, Nom, Téléphone, E-mail, Information et Entreprise.

Durées d'authentification autorisées

Durée minimale	Durée minimale durant laquelle l'utilisateur peut être authentifié.
Durée maximale	Durée maximale durant laquelle l'utilisateur peut être authentifié.
Pour l'authentification transparente	Pour les méthodes de type SPNEGO et Certificats SSL, définissez la durée pendant laquelle aucune demande de réauthentification transparente (ticket Kerberos ou certificat) ne sera réalisée entre le portail captif et le navigateur du client.

Configuration avancée

Activer le portail captif	Cette option autorise l'authentification via un formulaire web depuis les interfaces réseau associées au profil du portail captif. La correspondance entre les interfaces et les profils est consultable depuis l'onglet **Portail captif**.
Activer la page de déconnexion	Cette option active une page de déconnexion distincte de la page d'authentification du portail captif. Lorsque l'utilisateur souhaite accéder à un site Web et qu'il n'est pas encore authentifié, la page d'authentification s'affiche. Une fois authentifié, la page Web demandée s'ouvre alors dans un nouvel onglet tandis que la page de déconnexion s'affiche dans l'onglet courant. Pour se déconnecter, il suffit de cliquer sur le bouton **Déconnexion** affiché dans la page de déconnexion, ou de fermer l'onglet de cette page.
Autoriser l'accès au fichier de configuration du proxy (.pac) pour ce profil	Cette option autorise la publication du fichier .PAC pour les utilisateurs se présentant depuis les interfaces réseau associées au profil d'authentification.
Interdire l'authentification simultanée d'un utilisateur sur plusieurs machines	Cette option permet d'éviter qu'un utilisateur ne s'identifie sur plusieurs postes en même temps. Les requêtes multiples sont automatiquement refusées.
Expiration du 'cookie' HTTP	Cette option permet de paramétrer l'expiration du cookie HTTP : • **A la fin de la période d'authentification** : le cookie est négocié une seule fois pour toute la durée d'authentification. • **A la fermeture de la session** : le cookie est négocié à chaque requête vers le navigateur Web. • **Ne pas utiliser (déconseillé - sauf parrainage)** : le cookie n'expire pas. Ce choix n'est pas recommandé car il dégrade la sécurité de l'authentification. Paramétrer une expiration permet par exemple de se prévenir des attaques par rejeu. Concernant les cookies HTTP, ils sont négociés par navigateur Web. L'authentification réalisée avec un navigateur Web n'est donc pas effective sur un autre. Pour autoriser plusieurs utilisateurs à être authentifiés depuis une même adresse IP, l'utilisation des cookies est indispensable. Les adresses IP concernées sont à renseigner dans la liste des **objets multi-utilisateur** depuis l'onglet **Politique d'authentification**, sauf pour la méthode Agent SSO qui ne supporte pas l'authentification multi-utilisateur.

Page d'authentification

Sélectionner un message personnalisé (fichier HTML)	Cette option permet d'ajouter sous le titre de la page d'authentification un message personnalisé qui peut contenir du texte et des images. Ce message doit être un fichier au format HTML pour pouvoir être chargé sur le firewall.
Réinitialiser la personnalisation de la page d'authentification	En cliquant sur ce bouton, le message personnalisé précédemment ajouté est supprimé de la page d'authentification.

Mots de passe des utilisateurs

Les utilisateurs ne peuvent pas changer leur mot de passe	Cette option ne permet pas aux utilisateurs de modifier leur mot de passe depuis le portail d'authentification.
Les utilisateurs peuvent changer leur mot de passe	Cette option permet aux utilisateurs de modifier leur mot de passe depuis le portail d'authentification, sans contrainte de temps et de validité.
Les utilisateurs doivent changer leur mot de passe	Cette option requiert que les utilisateurs changent leur mot de passe à leur première connexion sur le portail d'authentification puis à chaque fois qu'il expire. La durée de vie d'un mot de passe est spécifiée en jours sans précision d'heure.
Durée de vie (jours)	Ce champ est modifiable si l'option **Les utilisateurs doivent changer leur mot de passe** est sélectionnée. Indiquez le nombre de jours de validité d'un mot de passe. Lorsqu'un mot de passe atteint sa durée de vie maximale, il expire à minuit. **EXEMPLE** Un utilisateur change une première fois son mot de passe le lundi à 14:00 avec une durée de vie paramétrée à 1 jour. Ce mot de passe doit être modifié dès le lendemain à 00:00 et non 24 heures plus tard.

Enrôlement des utilisateurs

Le firewall propose l'enrôlement d'utilisateurs par le Web. Si l'utilisateur qui tente de se connecter ne figure pas dans la base des utilisateurs, il a la possibilité de demander la création de son compte par un enrôlement Web sur le portail captif.

Ne pas permettre l'enrôlement des utilisateurs	Lorsque cette case est cochée, les utilisateurs ne figurant pas dans la base des utilisateurs ne peuvent pas envoyer une demande de création de compte.
Autoriser l'enrôlement web des utilisateurs	Lorsque cette case est cochée, les utilisateurs ne figurant pas dans la base des utilisateurs peuvent demander la création d'un compte en remplissant un formulaire Web. La demande devra être validée ou refusée par un administrateur depuis le module **Configuration > Utilisateurs >** Enrôlement.
Autoriser l'enrôlement web des utilisateurs et créer leur certificat	Lorsque cette case est cochée : • Les utilisateurs ne figurant pas dans la base des utilisateurs peuvent demander la création d'un compte et d'un certificat en remplissant un formulaire web. Deux demandes seront alors envoyées : une pour le compte et une pour le certificat. • Les utilisateurs figurant dans la base des utilisateurs mais ne disposant pas de certificat peuvent demander la création de leur certificat. En effectuant une demande, les utilisateurs définissent le mot de passe de leur certificat. Les demandes devront être validées ou refusées par un administrateur depuis le module **Configuration > Utilisateurs >** Enrôlement. Le certificat sera signé par l'autorité de certification (CA) choisie par défaut dans le module **Configuration > Objets > Certificats et PKI** et créé selon ses paramètres du profil de certificats utilisateurs.
Notification d'un nouvel enrôlement	Cette option permet de définir un groupe d'utilisateurs à notifier lorsqu'une nouvelle demande d'enrôlement est reçue. Par défaut, la liste déroulante affiche qu'aucun e-mail ne sera envoyé. Pour choisir un groupe d'utilisateurs, vous devez au préalable le créer dans le module **Configuration > Notifications > Alertes e-mails**, onglet Destinataires. Une fois créé, il pourra être sélectionné dans la liste déroulante.

Proxy HTTP transparent ou explicite et objets Multi-utilisateur

Objets Multi-utilisateur

La liste de *réseaux des options* permet plusieurs authentifications depuis une même adresse IP (voir l'option **Objets multi-utilisateur**). Cela permet par exemple, d'accéder à des applications et des données depuis un ordinateur distant (serveur TSE) en pratiquant du filtrage par utilisateur. Cette application Multi-utilisateur ne s'applique qu'aux flux HTTP et HTTPS.

Voici ci-dessous, une brève description des mécanismes permettant cette authentification Multi-utilisateur. Ces modes sont détaillés dans les sections suivantes.

Mode Cookie

Le cas d'*objets Multi-utilisateur* est rendu possible grâce au **Mode Cookie**. Lors de la première connexion à chaque nouveau site web interrogé, les informations d'authentification sont enregistrées par le navigateur Web dans un cookie d'authentification possédant plusieurs attributs. Ces informations sont ensuite retransmises dans les requêtes suivantes pour être interceptées par le firewall qui peut ainsi appliquer sa politique.

Seulement dans le cadre d'une connexion non sécurisée HTTP, les navigateurs Web affichent un message d'erreur au lieu du contenu des sites web interrogés car les cookies d'authentification ne peuvent pas utiliser l'attribut "Secure" conjointement à l'attribut "SameSite".
Pour rétablir la navigation sur les sites interrogés en HTTP, une opération manuelle doit être effectuée dans la configuration du navigateur Web :

- Sur Google Chrome :
  - Accédez à chrome://flags/,
  - Passez l'attribut **Cookies without SameSite must be secure** sur **Disabled**,
  - Redémarrez le navigateur.
- Sur Firefox :
  - Accédez à about:config,
  - Passez l'attribut **network.cookie.sameSite.noneRequiresSecure** sur **false**,
  - Redémarrez le navigateur.
- Sur Microsoft Edge :
  - Accédez à edge://flags/,
  - Passez l'attribut **Cookies without SameSite must be secure** sur **Disabled**,
  - Redémarrez le navigateur.

Authentification proposée par le navigateur (HTTP code 407)

Uniquement dans le cas de proxy explicite, la méthode *Proxy-Authorization* - HTTP code 407 peut être utilisée. Le protocole HTTP prévoit un champ dédié à l'authentification. C'est le navigateur qui demande à l'utilisateur de s'authentifier via une fenêtre de message et l'information de connexion est relayée au Firewall via l'entête HTTP. La politique de sécurité pourra ainsi s'appliquer.

L'authentification "Proxy-Authorization" (HTTP 407) par le navigateur n'autorise pas les méthodes SSL (certificats) et SPNEGO, car ces méthodes ne font pas intervenir le portail d'authentification, même si celui-ci doit être activé.

NOTE
Si vous ajoutez ou supprimez un objet dans la liste des *objets Multi-utilisateur*, assurez-vous qu'aucune authentification relative à cet objet n'est enregistrée.

Proxy transparent (implicite)

Le proxy transparent ou implicite permet de filtrer les requêtes des utilisateurs sans aucune configuration sur le poste client (pas de déclaration de proxy dans le navigateur). Ainsi toutes les requêtes seront interceptées par le proxy du Firewall et filtrées pour autoriser ou refuser l'accès à un site internet par exemple.

Ce mode est recommandé car il répond à toutes les demandes souhaitées : authentification de l'utilisateur selon la méthode choisie, Filtrage SSL (blocage de sites internet en HTTPS par exemple), etc. Cette utilisation bénéficie de l'ensemble des fonctionnalités mais ne peut toutefois pas utiliser la méthode d'authentification transparente *Agent SSO*.

Utilisateur unique		Objets Multi-utilisateur (Mode Cookie)	
Méthodes	*Inspections*	*Méthodes*	*Inspections*
Toutes les méthodes	Toutes les inspections	Toutes les méthodes **sauf Agent SSO**	Toutes les inspections

Proxy explicite

Avec un proxy renseigné dans le navigateur du navigateur, deux types d'authentification sont possibles :

- **Mode *Standard* ou *Cookie***

Ce mode est aisé à mettre en place grâce à l'assistant de création *de* **Règle de proxy HTTP explicite**, proposé dans le module **Filtrage**. Deux règles sont générées ; l'une redirige le trafic vers le proxy HTTP explicite, l'autre applique la politique de filtrage. Les prescriptions régissant l'authentification des utilisateurs doivent être stipulées par une règle à placer entre les deux règles générées par l'assistant de création, soit après la redirection vers le proxy HTTP et avant l'autorisation du trafic via *Proxy HTTP explicite*.

- **Authentification proposée par le navigateur (HTTP code 407)**

La fonctionnalité *Proxy-Authorization* - HTTP code 407 s'active en configuration avancée du module *Protocole HTTP* (*onglet Proxy*).accessible par le menu *Protection applicative*.

Ces modes comportent cependant certaines limitations, reprises dans le tableau ci-dessous :

Utilisateur unique				Objets Multi-utilisateur			
Mode standard		**"Proxy-Authorization" code 407**		**Mode Cookie**		**"Proxy-Authorization" code 407**	
Méthodes	*Inspections*	*Méthodes*	*Inspections*	*Méthodes*	*Inspections*	*Méthodes*	*Inspections*

Toutes les méthodes	Toutes les inspections **sauf sur le trafic SSL Filtrage par utilisateur**	• LDAP • Radius • Kerberos • Agent SSO Δ mots de passe en clair (encodé en base 64)	Toutes les inspections **sauf sur le trafic SSL Filtrage par utilisateur**	Toutes les méthodes **sauf Agent SSO**	Toutes les inspections **sauf sur le trafic SSL Filtrage par utilisateur (HTTP uniquement)**	• LDAP • Radius • Kerberos Δ mots de passe en clair (encodé en base 64)	Toutes les inspections **sauf sur le trafic SSL Filtrage par utilisateur**

Le filtrage sur le contenu ne peut se faire que sur le trafic HTTP.
Le filtrage par utilisateur peut se faire sur HTTP et HTTPS, sauf pour les objets Multi-utilisateur en mode *Cookie* (HTTP uniquement).

Le mode explicite implique des flux HTTPS par la méthode CONNECT. Le trafic HTTPS est alors encapsulé en HTTP et la méthode d'envoi des requêtes permet d'établir une relation de confiance entre le client et le serveur.

CERTIFICATS ET PKI

La PKI ou *Public Key Infrastructure* (infrastructure à clés publiques) est un système cryptographique basé sur la cryptographie asymétrique. Elle utilise des mécanismes de signature et certifie des clés publiques qui permettent, par exemple, de chiffrer et de signer des messages ou des flux de données. Elle permet d'assurer confidentialité, authentification, intégrité et non-répudiation.

La PKI Stormshield Network permet de générer ou d'importer des identités numériques d'autorités de confiance (CA : *Certification Authority,* ou « autorité de certification »), de serveurs ou d'utilisateurs. Elle permet également la signature de certificats, ceux-ci contenant une clé publique associée à des informations pouvant appartenir à un utilisateur, un serveur etc. La PKI Stormshield Network a pour objectif d'authentifier ces éléments.

Dans la suite de ce manuel, le terme identité fait référence à la notion d'identité numérique.

Pour l'utilisation de la fonctionnalité VPN SSL, l'autorité de certification « sslvpn-full-default-authority » comprend une identité serveur « openvpnserver » ainsi qu'une identité utilisateur « openvpnclient ». Cela permet au client et au service VPN SSL du firewall Stormshield Network de s'identifier mutuellement sans avoir recours à une autorité externe.

Lorsque le firewall dispose d'un module TPM (Trusted Platform Module) destiné à protéger les clés privées de certificats du firewall et que ce module TPM n'est pas initialisé, une fenêtre d'initialisation du TPM s'affiche à l'ouverture du module **Certificats et PKI**. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module.

L'écran du module **Certificats et PKI** se divise en 3 parties :

- En haut de l'écran, les différentes actions possibles sous formes d'une barre de recherche et de boutons,
- A gauche, la liste des autorités, des identités et des certificats,
- A droite, les détails concernant l'autorité, l'identité ou le certificat sélectionné au préalable dans la liste de gauche, les informations concernant la liste de révocation de certificats (CRL - *Certificate Revocation List*) et, dans le cas d'une autorité ou d'une sous-autorité, les propriétés des certificats signés par cette autorité ou sous-autorité.

L'indicateur de santé du firewall (affiché dans le bandeau supérieur de l'Interface Web d'Administration en cas d'anomalie) dispose de sondes relatives aux dates de validité et à l'état des certificats et des CRL des autorités de certifications utilisées dans la configuration. La couleur de l'indicateur en précise l'état :

- Pour les certificats :
  - **Critique** : le certificat est révoqué (par une autorité de certification) ou expiré,
  - **Non critique** : le certificat va expirer dans moins de 30 jours ou sa date de début de validité n'est pas encore atteinte,
  - **Optimum** : le certificat ne présente aucun caractère critique.
- Pour les CRL :
  - **Critique** : la CRL de la CA est expirée,
  - **Non critique** : le certificat va expirer dans moins de 30 jours ou sa date de début de validité n'est pas encore atteinte,
  - **Optimum** : la CRL ne présente aucun caractère critique.

Les actions possibles

Le champ Entrer un filtre...

Si vous recherchez un certificat, une identité ou une autorité, saisissez son nom dans le champ de recherche.
La liste de tous les certificats, identités et autorités correspondant à la chaîne de caractères saisie s'affiche.

Exemple :

Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous les certificats possédant un « a ».

Le filtre

Ce bouton permet de choisir le type de certificat à afficher et de ne voir que les éléments qui vous intéressent. Un menu déroulant vous propose les choix suivants :

- " **Filtre : Tous** " : affiche dans la liste de gauche toutes les autorités, identités et certificats préalablement créés,
- " **Filtre : Autorités de certification** " : affiche dans la liste de gauche toutes les autorités et sous-autorités,
- " **Filtre : Certificats Utilisateur** " : affiche dans la liste de gauche uniquement les certificats utilisateur et les autorités dont ils dépendent,
- " **Filtre : Certificats Serveur** " : affiche dans la liste de gauche uniquement les certificats serveur et les CA dont ils dépendent.
- " **Filtre : Certificats Smartcard** " : affiche dans la liste de gauche uniquement les certificats Smartcard et les CA dont ils dépendent.

Ajouter

Ce bouton permet d'**Ajouter** différents types d'éléments à la PKI :

- **Autorité racine**,
- **Sous-autorité**,
- **Identité utilisateur**,
- **Identité smartcard**,
- **Identité serveur.**

Et d'**Importer un fichier** contenant des éléments des catégories ci-dessus.

Pour plus d'informations sur ces opérations, consultez les sections Ajouter une autorité racine, Ajouter une Sous-autorité, Ajouter une Identité Utilisateur, Ajouter une Identité Smartcard, Ajouter une Identité Serveur et Importer un fichier.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Révoquer

Ce bouton permet de supprimer une autorité, une sous-autorité, une identité ou un certificat de la PKI.

Pour plus d'informations sur ces opérations, consultez la section Révoquer une autorité, une sous autorité ou un certificat.

Actions

Les actions possibles diffèrent selon le type d'objet sélectionné dans la liste de gauche :

- Autorité ou sous-autorité : **Créer la CRL**, **Renouveler la CRL**, **Supprimer la CRL**, **Définir comme défaut**,
- Certificat utilisateur : **Publication LDAP**,
- Tout type d'identité (sauf identité importée) : **Supprimer la clé privée**, **Protéger avec le TPM**.

Pour plus d'informations sur ces différentes actions, consultez les sections Créer, renouveler ou supprimer une CRL, Supprimer la clé privée (d'une identité), Définir comme défaut et Publier un certificat dans l'annuaire LDAP.

Télécharger

Ce bouton vous permet de télécharger :

- Les certificats d'autorités et de sous-autorités,
- Les CRL d'autorités et de sous-autorités,
- Les certificats utilisateur, certificats Smartcard et certificats serveur,
- Les identités utilisateur, identités Smartcard et identités serveur.

Pour plus d'informations sur ces différentes actions, consultez les sections Télécharger un certificat, Télécharger une identité et Télécharger une CRL.

Vérifier l'utilisation

Vous pouvez rechercher les fonctionnalités ou modules qui utilisent le certificat, la CA ou la sous-autorité sélectionnés.

Ajouter des autorités et des identités

Le bouton **Ajouter** déroule une liste proposant six actions permettant de créer des autorités (et sous-autorités) de certification ainsi que des identités numériques.

Une identité numérique (identité utilisateur, serveur ou Smartcard) est composée :

- Du certificat du porteur : informations d'identité (nom [FQDN pour un serveur], prénom, adresse de messagerie, ...), clé publique du porteur, signature et clé publique de l'autorité de certification émettrice.
- De la clé privée du porteur.

Ajouter une autorité racine ou en afficher les détails

Une autorité racine ou « root CA » est une entité ayant pour objectif de signer, émettre et maintenir les certificats et les CRL (*Certificate Revocation List*, ou « listes de révocations »).

> **NOTE**
> Les informations saisies ne seront plus modifiables après la création de l'autorité.

Ajouter une autorité racine

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Autorité racine**.
3. Renseignez un **CN** (obligatoire).
   Il s'agit d'un nom permettant d'identifier votre autorité racine, dans la limite de 64 caractères. Ce nom peut faire référence à une organisation, un utilisateur, un serveur, une machine etc.
4. Renseignez un **Identifiant** (facultatif).
   Vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande.
5. Renseignez les attributs de l'autorité. Ces informations seront présentes dans le certificat de l'autorité ainsi que dans les certificats qu'elle émettra.
   - **Organisation (O)** : Nom de votre société (ex : Stormshield).
   - **Unité d'organisation (OU)** : "branche" de votre société (ex : Documentation).
   - **Lieu (L)** : Ville dans laquelle est située votre société (ex : Villeneuve d'Ascq).
   - **État ou province (ST)** : Département géographique de votre société (ex : Nord).
   - **Pays (C)** : Choisissez dans la liste le pays de la société (ex : France).
4. Cliquez sur **Suivant**.
5. Saisissez le mot de passe destiné à protéger l'autorité racine et confirmez-le.
   Une jauge indique le degré de robustesse de votre mot de passe. Il est recommandé de combiner les lettres minuscules, majuscules, les chiffres et les caractères spéciaux.
6. Vous pouvez renseigner votre **E-mail** afin de recevoir un message vous confirmant la création de votre autorité.
7. Modifiez éventuellement la **Taille de clé (en bits)**.
   Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celles-ci avec les équipements d'entrée de gamme, pour des raisons de temps de génération.
8. Vous pouvez aussi modifier durée de **Validité (en jours)** de votre autorité.
   Ce champ correspond au nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valides. Cette date influe sur tous les aspects de votre PKI. En effet, une fois ce certificat expiré, tous les certificats utilisateurs le seront également. Cette valeur ne sera pas modifiable par la suite.
   La valeur de ce champ de doit pas excéder 3650 jours.
9. Cliquez sur **Suivant**.
10. Définissez éventuellement les points de distribution des listes de révocation de certificats en cliquant sur **Ajouter** pour définir l'URL d'accès à la CRL.
    Cette information est intégrée à l'autorité générée et permettra aux applications utilisant le certificat de cette autorité de récupérer automatiquement la CRL afin de vérifier la validité du certificat.
    Si plusieurs points de distributions sont définis, ils seront traités dans l'ordre de la liste.
11. Cliquez sur **Suivant**.
    Un résumé des informations saisies vous est présenté.
12. Cliquez sur **Terminer**.

L'autorité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall.

Afficher les détails d'un autorité / modifier les profils de certificats liés à cette autorité

Un clic sur une autorité affiche ses informations détaillées dans la partie droite de l'écran.

Onglet « Détails »

Quatre cadres présentent les données de l'autorité :

- Sa **Validité** : dates d'émission et d'expiration de l'autorité,
- Son destinataire (**Émis pour**) : sujet et détails du certificat de l'autorité,
- Son **Émetteur** : sujet et détails du certificat de l'autorité,
- Ses **Détails** : numéro de série de l'autorité, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé et Extended Key Usage (EKU).

Onglet « Révocation (CRL) »

Il reprend les informations concernant la CRL :

- Sa validité incluant la date des dernière et prochaine mises à jour,
- La grille des certificats signés par cette CA et ayant été révoqués. Sont précisés, pour chacun de ces certificats révoqués : son numéro de série, sa date de révocation et le motif de révocation (facultatif).

Onglet « Profils de certificats »

Cet onglet présente :

- Les points de distribution mettant à disposition la CRL de la CA. Il est possible d'en ajouter de nouveaux ou d'en supprimer depuis cette grille.
- Les valeurs proposées par défaut pour les paramètres intervenant dans la signature d'une nouvelle sous-autorité ou d'un nouveau certificat par l'autorité de certification sélectionnée. Ces valeurs sont modifiables.

NOTE
Si vous modifiez les valeurs de ces paramètres, cela n'affecte pas les sous-autorités ou certificats existants : vous devez les recréer si vous souhaiter utiliser les nouvelles valeurs pour ces éléments.

Ces paramètres sont les suivants :

- **Type de clé** (algorithme de signature) : la valeur proposée par défaut est **SECP**,
- **Taille de clé (bits)** : la valeur proposée par défaut est **256**,
- Durée de **Validité (jours)** : la valeur proposée par défaut est **365** jours par défaut pour un certificat et **3650** jours pour une CA,
- Durée de **Validité de la CRL** (uniquement pour la signature du certificat d'une sous-autorité) : la valeur proposée par défaut est **30** jours (maximum autorisé : 3650 jours),
- **Somme de contrôle** : la valeur utilisée par défaut est **sha256**,

Ajouter une autorité racine ou en afficher les détails

Lorsque vous créez une sous-autorité, les écrans visibles sont similaires à ceux de la création d'une autorité racine. L'assistant de configuration pour une sous-autorité a besoin d'une référence « parente » dont il va reprendre les informations.

Ajouter une sous-autorité

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Sous-Autorité**.

3. Renseignez un **CN** (obligatoire).
   Il s'agit d'un nom permettant d'identifier votre autorité racine, dans la limite de 64 caractères. Ce nom peut faire référence à une organisation, un utilisateur, un serveur, une machine etc.
4. Renseignez un **Identifiant** (facultatif).
   Vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande.
5. Sélectionnez l'autorité parente : l'utilisation d'une sous-autorité n'est possible qu'après identification de son autorité parente.
   L'autorité proposée comme parente pour la nouvelle sous-autorité sera l'autorité par défaut ou, la dernière autorité sélectionnée avant d'avoir cliqué sur **Ajouter > Sous-autorité**.
6. Saisissez le mot de passe de l'autorité parente.
   L'icône vous permet d'afficher le mot de passe en clair pour vérifier qu'il est correct.
7. Cliquez sur **Suivant**.
8. Saisissez le mot de passe destiné à protéger la sous-autorité et confirmez-le.
   Une jauge indique le degré de robustesse de votre mot de passe. Il est recommandé de combiner les lettres minuscules, majuscules, les chiffres et les caractères spéciaux.
9. Vous pouvez renseigner votre **E-mail** afin de recevoir un message vous confirmant la création de votre autorité.
10. Modifiez éventuellement la **Taille de clé (en bits)**.
    Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celles-ci avec les équipements d'entrée de gamme, pour des raisons de temps de génération.
11. Vous pouvez aussi modifier durée de **Validité (en jours)** de votre autorité.
    Ce champ correspond au nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valides. Cette date influe sur tous les aspects de votre PKI, en effet, une fois ce certificat expiré, tous les certificats utilisateurs le seront également. Cette valeur ne sera pas modifiable par la suite.
    La valeur de ce champ de doit pas excéder 3650 jours.
12. Cliquez sur **Suivant**.
13. Définissez éventuellement les points de distribution des listes de révocation de certificats en cliquant sur **Ajouter** pour définir l'URL d'accès à la CRL.
    Cette information est intégrée à l'autorité générée et permettra aux applications utilisant le certificat de cette autorité de récupérer automatiquement la CRL afin de vérifier la validité du certificat.
    Si plusieurs points de distributions sont définis, ils seront traités dans l'ordre de la liste.
14. Cliquez sur **Suivant**.
    Un résumé des informations saisies vous est présenté.
15. Cliquez sur **Terminer**.

La sous-autorité est automatiquement ajoutée à l'arborescence des autorités et certificats définis sur le firewall.

Afficher les détails de la sous-autorité

Un clic sur la sous-autorité affiche ses informations détaillées dans la partie droite de l'écran.

Afficher les détails d'un autorité / modifier les profils de certificats liés à cette autorité

Un clic sur une autorité affiche ses informations détaillées dans la partie droite de l'écran.

Onglet « Détails »

Quatre cadres présentent les données de l'autorité :

- Sa **Validité** : dates d'émission et d'expiration de l'autorité,
- Son destinataire (**Émis pour**) : sujet et détails du certificat de la sous-autorité,
- Son **Émetteur** : sujet et détails du certificat de l'autorité parente,
- Ses **Détails** : numéro de série de la sous-autorité, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé et Extended Key Usage (EKU).

Onglet « Révocation (CRL) »

Il reprend les informations concernant la CRL :

- Sa validité incluant la date des dernière et prochaine mises à jour,
- La grille des certificats signés par cette CA et ayant été révoqués. Sont précisés, pour chacun de ces certificats révoqués : son numéro de série, sa date de révocation et le motif de révocation (facultatif).

Onglet « Profils de certificats »

Cet onglet présente :

- Les points de distribution mettant à disposition la CRL de la CA. Il est possible d'en ajouter de nouveaux ou d'en supprimer depuis cette grille.
- Les valeurs proposées par défaut pour les paramètres intervenant dans la signature d'une nouvelle sous-autorité ou d'un nouveau certificat par l'autorité de certification sélectionnée. Ces valeurs sont modifiables.

NOTE
Si vous modifiez les valeurs de ces paramètres, cela n'affecte pas les sous-autorités ou certificats existants : vous devez les recréer si vous souhaiter utiliser les nouvelles valeurs pour ces éléments.

Ces paramètres sont les suivants :

- **Type de clé** (algorithme de signature) : la valeur proposée par défaut est **SECP**,
- **Taille de clé (bits)** : la valeur proposée par défaut est **256**,
- Durée de **Validité (jours)** : la valeur proposée par défaut est **365** jours par défaut pour un certificat et **3650** jours pour une CA,
- Durée de **Validité de la CRL** (uniquement pour la signature du certificat d'une sous-autorité) : la valeur proposée par défaut est **30** jours (maximum autorisé : 3650 jours),
- **Somme de contrôle** : la valeur utilisée par défaut est **sha256**,

Onglet « Détails »

4 fenêtres présentent les données de la sous-autorité :

- Sa **Validité** : dates d'émission et d'expiration de la sous-autorité,
- Son destinataire (**Émis pour**) : la sous-autorité elle-même,
- Son **Émetteur** : son autorité parente,
- Ses **Détails** : numéro de série de la sous-autorité, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé...

Onglet « Révocation (CRL) »

Il reprend les informations concernant la CRL : la validité incluant la dernière et la prochaine mise à jour, la grille des points de distribution et la grille de certificats révoqués, devant contenir un numéro de série, une date de révocation et un motif de révocation.

Onglet « Profils de certificats »

Cet onglet présente la **Taille de clé (bits)** et la **Validité (jours)** pour l'autorité de certification (avec la **Validité de la CRL en jours** en plus pour l'autorité, dans la limite de 3650 jours), les certificats utilisateur, les certificats Smartcard et les certificats serveurs.

Ces valeurs sont modifiables et sont proposées par défaut lors de la création d'une sous-autorité ou d'un certificat signé par la sous-autorité sélectionnée.

Ajouter une identité utilisateur ou en afficher les détails

Dans l'assistant de configuration, spécifiez les informations relatives à l'utilisateur pour lequel vous souhaitez créer une identité.

Créer une identité utilisateur

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Identité Utilisateur**.
3. Renseignez un **CN** (obligatoire).
   Il s'agit d'un nom permettant d'identifier l'utilisateur dans la limite de 64 caractères.
4. Renseignez un **Identifiant** (facultatif).
   Vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande (exemple : si le CN est un couple Prénom+Nom, l'identifiant peut correspondre aux initiales du CN).
5. Renseignez l'adresse **E-mail** (obligatoire) de l'utilisateur pour lequel vous créez une identité.
6. Cliquez sur **Suivant**.
7. Sélectionnez l'**Autorité parente** destinée à signer le certificat de l'identité.
8. Renseignez le **Mot de passe de l'autorité parente**.
   Les attributs de l'autorité sont automatiquement ajoutés. Ils seront présents dans le certificat utilisateur.
9. Cliquez sur **Suivant**.
10. Lorsque le firewall dispose d'un module TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour que la clé privée de l'identité soit protégée par le TPM.
11. Modifiez éventuellement la durée de **Validité (jours)** du certificat.
    La valeur conseillée est de 365 jours (proposée par défaut).
12. Vous pouvez aussi modifier la **Taille de clé (en bits)** du certificat.
    Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celles-ci avec les équipements d'entrée de gamme, pour des raisons de temps de génération.
13. Si un utilisateur déclaré dans l'annuaire LDAP référence la même adresse e-mail que celle précisée à l'étape 4, vous pouvez associer automatiquement cette identité à l'utilisateur correspondant.
    Ceci n'est cependant possible que si l'autorité utilisée pour générer le certificat est l'autorité par défaut du firewall. Dans ce cas :
    - Cochez la case **Publier cette identité dans l'annuaire LDAP,**
    - Saisissez deux fois un mot de passe destiné à protéger le conteneur PKCS#12 de l'identité.
14. Cliquez sur **Suivant**.
    Un résumé des informations saisies vous est présenté.
15. Cliquez sur **Terminer**.

L'identité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall, sous son autorité parente.

Afficher les détails de l'identité

Un clic sur l'identité affiche ses informations détaillées dans la partie droite de l'écran.

Ces informations sont en lecture seule.

Onglet « Détails »

Plusieurs cadres présentent les données de l'identité :

- Son **Utilisation** : les modules dans lequel le certificat de l'identité est utilisé ainsi que la protection éventuelle de la clé privée de l'identité par le TPM si le firewall en est équipé.
- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**) : sujet et détails du certificat utilisateur (adresse e-mail de l'utilisateur),
- Son **Émetteur** : sujet et détails du certificat de l'autorité parente de l'identité du serveur,
- Ses **Détails** : numéro de série du certificat, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé, types d'usages réservés à cette identité et son certificat (Extended Key Usage - EKU).

Onglet Révocation (CRL)

- Les adresses (URL) des **Points de distribution de CRL** de l'autorité parente,
- Les adresses (URL) des **Serveurs OCSP** si le protocole OCSP est utilisé pour le renouvellement des certificats.

Publier une identité dans l'annuaire LDAP

Si un utilisateur déclaré dans l'annuaire LDAP référence la même adresse e-mail que celle précisée pour un certificat utilisateur, vous pouvez associer cette identité à l'utilisateur si vous ne l'avez pas fait lors de la création de l'identité.

Notez que ceci n'est cependant possible que si l'autorité utilisée pour générer cette identité est l'autorité par défaut du firewall.

Dans ce cas :

1. Sélectionnez l'identité concernée à l'aide d'un simple clic,
2. Cliquez sur le menu **Actions**,
3. Choisissez **Publication LDAP**,
4. Dans la fenêtre pop-up qui s'affiche, saisissez deux fois un mot de passe destiné à protéger le conteneur PKCS#12 de l'identité.
5. Cliquez sur **Publier le certificat**.

Ajouter une identité Smartcard ou en afficher les détails

Une identité SmartCard est liée à un compte Microsoft Windows, donc associée à un utilisateur unique. Le certificat de cet utilisateur est signé par une Autorité de Certification mettant à disposition des CRLDP pour vérifier sa validité, et publié dans un annuaire Active Directory (ou dans un annuaire LDAP). Le firewall étant en mesure de vérifier le compte Windows que l'utilisateur possède par une politique d'authentification, et de valider les informations du certificat correspondant, peut autoriser l'utilisateur ayant connecté sa carte à puce (SmartCard) à accéder aux ressources réseau de votre organisation.

Créer une identité Smartcard

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Identité Smartcard**.
3. Renseignez un **CN** (obligatoire).
   Il s'agit d'un nom permettant d'identifier l'utilisateur dans la limite de 64 caractères.
4. Renseignez un **Identifiant** (facultatif).
   Vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande (exemple : si le CN est un couple Prénom+Nom, l'identifiant peut correspondre aux initiales du CN).
5. Renseignez l'adresse **E-mail** (obligatoire) de l'utilisateur pour lequel vous créez une identité.
6. Dans le champ **Nom principal d'utilisateur (Windows)**, renseignez le nom du compte Active Directory de l'utilisateur.
7. Cliquez sur **Suivant**.
8. Sélectionnez l'**Autorité parente** destinée à signer le certificat.
9. Renseignez le **Mot de passe de l'autorité parente**.
   Les attributs de l'autorité sont automatiquement ajoutés. Ils seront présents dans le certificat Smartcard.
10. Cliquez sur **Suivant**.
11. Lorsque le firewall dispose d'un module TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour que la clé privée de l'identité soit protégée par le TPM.
12. Modifiez éventuellement la durée de **Validité (jours)** du certificat.
    La valeur conseillée est de 365 jours (proposée par défaut).
13. Vous pouvez aussi modifier la **Taille de clé (en bits)** du certificat.
    Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celles-ci avec les équipements d'entrée de gamme, pour des raisons de temps de génération.
14. Cliquez sur **Suivant**.
    Un résumé des informations saisies vous est présenté.
15. Cliquez sur **Terminer**.

Afficher les détails du certificat

Un clic sur l'identité affiche ses informations détaillées dans la partie droite de l'écran.

Ces informations sont en lecture seule.

Onglet « Détails »

Différents cadres présentent les données de l'identité :

- Son **Utilisation** : les modules dans lequel le certificat de l'identité est utilisé ainsi que la protection éventuelle de la clé privée de l'identité par le TPM si le firewall en est équipé.
- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**) : sujet et détails du certificat smartcard (adresse e-mail de l'utilisateur),
- Son **Émetteur** : sujet et détails du certificat de l'autorité parente de l'identité du serveur,
- Ses **Détails** : numéro de série du certificat, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé, types d'usages réservés à cette identité et son certificat (Extended Key Usage - EKU).

Onglet Révocation (CRL)

- Les adresses (URL) des **Points de distribution de CRL** de l'autorité parente,
- Les adresses (URL) des **Serveurs OCSP** si le protocole OCSP est utilisé pour le renouvellement des certificats.

Ajouter une identité serveur ou en afficher les détails

Une identité serveur est destiné à être installée sur un serveur web ou applicatif. Le certificat correspondant à cette identité permet d'authentifier le serveur.

Dans le cas d'un site web, par exemple, le certificat permet de vérifier que l'URL et son nom de domaine (DN - *Domain Name*) appartiennent bien à l'entreprise attendue.

Ajouter une identité serveur

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Identité Serveur**.
3. Renseignez un **Nom de domaine qualifié (FQDN)** (obligatoire).
   La taille limite de ce champ est de 64 caractères. Exemple : myserver.mycompany.com.
4. Renseignez un **Identifiant** (facultatif).
   Vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande.
5. Cliquez sur **Suivant**.
6. Sélectionnez l'**Autorité parente** destinée à signer le certificat de l'identité.
7. Renseignez le **Mot de passe de l'autorité parente**.
   Les attributs de l'autorité sont automatiquement ajoutés. Ils seront présents dans le certificat serveur.
8. Cliquez sur **Suivant**.
9. Lorsque le firewall dispose d'un module TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour que la clé privée de l'identité soit protégée par le TPM.
10. Modifiez éventuellement la durée de **Validité (jours)** du certificat.
    La valeur conseillée est de 365 jours (proposée par défaut).
11. Vous pouvez aussi modifier la **Taille de clé (en bits)** du certificat.
    Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celles-ci avec les équipements d'entrée de gamme, pour des raisons de temps de génération.
12. Cliquez sur **Suivant**.
13. Définissez éventuellement des alias correspondant au serveur. Ces alias sont sous forme de FQDN.
    Exemple : alias1.mycompany.com.
14. Cliquez sur **Suivant**.
    Un résumé des informations saisies vous est présenté.
15. Cliquez sur **Terminer**.

L'identité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall, sous son autorité parente.

Afficher les détails de l'identité

Un clic sur l'identité affiche ses informations détaillées dans la partie droite de l'écran.

Ces informations sont en lecture seule.

Onglet Détails

Différents cadres présentent les données de l'identité :

- Son **Utilisation** : les modules dans lequel le certificat de l'identité est utilisé ainsi que la protection éventuelle de la clé privée de l'identité par le TPM si le firewall en est équipé.
- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**) : sujet et détails du certificat du serveur,
- Son **Émetteur** : sujet et détails du certificat de l'autorité parente de l'identité du serveur,
- Ses **Détails** : numéro de série du certificat, version, algorithmes de chiffrement et de signature utilisés, type de clé, taille de clé, types d'usages réservés à cette identité et son certificat (Extended Key Usage - EKU).
- Ses **Alias** : les FQDN éventuellement ajoutés lors de la création de l'identité.

Onglet Révocation (CRL)

- Les adresses (URL) des **Points de distribution de CRL** de l'autorité parente,
- Les adresses (URL) des **Serveurs OCSP** si le protocole OCSP est utilisé pour le renouvellement des certificats.

Importer un fichier

Il est possible d'importer un fichier contenant un ou plusieurs éléments de la liste suivante :

- Certificat(s),
- Clé(s) privée(s),
- CRL,
- CA,
- Requête(s) de signature de certificat (CSR - Certificate Signing Request).

Importer un fichier

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Importer un fichier**.
3. Pour le champ **Fichier à importer**, cliquez sur l'icône pour parcourir le contenu de votre ordinateur et sélectionner le fichier.
4. Le firewall détecte automatiquement le **Format du fichier**. Si ce n'est pas le cas (extension inconnue), positionnez le sélecteur sur le format adéquat (**P12**, **DER** ou **PEM**).
5. Si le fichier est au format PKCS#12 (extension P12), tapez le **Mot de passe** qui protège le fichier.
6. Indiquez les **Éléments à importer** depuis le fichier (si le fichier contient plusieurs éléments de nature différente, il est possible de n'en sélectionner qu'un seul type).
7. Si les éléments à importer sont déjà présents dans votre PKI, cochez la case **Écraser le contenu existant dans la PKI**.
8. Lorsque le firewall dispose d'un module TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour que la clé privée de l'identité soit protégée par le TPM.
9. Cliquez sur **Importer**.

Si les éléments importés sont des autorités, identités ou certificats, ils sont automatiquement ajoutés à l'arborescence.

Lors du survol de ces éléments à l'aide de la souris, le champ **Type** de l'info-bulle précise qu'il s'agit d'éléments importés.

Révoquer une autorité, une sous-autorité ou un certificat

Le bouton **Révoquer** permet de supprimer de la PKI des autorités, sous-autorités ou d'ajouter des certificats à la CRL d'une autorité pour indiquer que ces certificats ne sont plus de confiance.

Seule l'autorité définie comme autorité par défaut sur le firewall ne peut pas être révoquée.

Si vous révoquez une autorité racine, sa CRL est également supprimée du firewall lors de l'opération.

Si vous révoquez une autorité ou une sous-autorité parente de certificats, tous ces certificats sont révoqués et supprimés lors de l'opération.

Révoquer une autorité

1. Sélectionnez dans la liste de gauche l'autorité à révoquer.
2. Cliquez sur le bouton **Révoquer**.
3. Saisissez le **Mot de passe de la CA** ou de la sous-autorité.
4. Vous pouvez sélectionner la **Raison** de cette révocation dans la liste déroulante.
   Cette raison de révocation sera affichée dans la CRL de l'autorité parente de l'entité révoquée.
5. Choisissez le **Format du fichier d'export de la CRL** :

- Format Base64 (PEM),
- Format binaire (DER).

6. Cliquez sur **Appliquer**.
7. Cliquez sur le lien affiché pour télécharger et enregistrer la CRL sur votre poste de travail.

Révoquer une sous-autorité ou un certificat

1. Sélectionnez dans la liste de gauche la sous-autorité à révoquer.
2. Cliquez sur le bouton **Révoquer**.
3. Saisissez le **Mot de passe de la CA** (mot de passe de la sous-autorité).
4. Saisissez le **Mot de passe de l'autorité racine** parente de la sous-autorité.
5. Vous pouvez sélectionner la **Raison** de cette révocation dans la liste déroulante.
   Cette raison de révocation sera affichée dans la CRL de l'autorité parente de la sous-autorité révoquée.
6. Choisissez le **Format du fichier** d'export de la CRL :
   - Format Base64 (PEM),
   - Format binaire (DER).
6. Cliquez sur **Appliquer**.
7. Cliquez sur le lien présenté pour télécharger et enregistrer la CRL de la sous-autorité sur votre poste de travail.

Révoquer un certificat

1. Sélectionnez dans la liste de gauche le certificat à révoquer.
2. Cliquez sur le bouton **Révoquer**.
3. Saisissez le **Mot de passe de la CA** (mot de passe de l'autorité émettrice du certificat).
4. Vous pouvez sélectionner la **Raison** de cette révocation dans la liste déroulante.
   Cette raison de révocation sera affichée dans la CRL de l'autorité parente de la sous-autorité révoquée.
5. Cochez la case **Exporter la CRL après sa mise à jour** si vous souhaitez conserver une copie de la CRL.
6. Dans ce cas, choisissez le **Format du fichier** d'export de la CRL :
   - Format Base64 (PEM),
   - Format binaire (DER).
6. Cliquez sur **Appliquer**.
7. Si vous avez choisi d'exporter la CRL, une fenêtre vous présente le lien de téléchargement du fichier d'export de la CRL.

Créer, renouveler ou supprimer une CRL

Lorsqu'une autorité ou une sous-autorité est ajoutée à la PKI, sa liste de révocation de certificats (CRL - Certificate Revocation List) doit être créée.

De même, bien qu'une CRL se mette à jour périodiquement de manière automatique, il peut être important de la renouveler manuellement après avoir révoqué des certificats signés par l'autorité propriétaire de la CRL.

Créer une CRL

1. Sélectionnez dans la liste de gauche l'autorité ou la sous-autorité pour laquelle la CRL doit être créée.
2. Cliquez sur **Actions**.
3. Sélectionnez **Créer la CRL**.
   Une boite de dialogue s'ouvre.
4. Renseignez le mot de passe de l'autorité ou de la sous-autorité.
5. Dans le cadre **Exporter la CRL**, cochez ou non la case **Exporter la CRL après sa mise à jour**.
   Si cette case est cochée, choisissez le **Format du fichier** d'export :

- **Format Base64 (PEM)**,
- **Format binaire (DER)**.

6. Cliquez sur **Appliquer**.
7. Si vous avez choisi d'exporter la CRL, une fenêtre vous présente le lien de téléchargement du fichier d'export de la CRL.

Renouveler une CRL

1. Sélectionnez dans la liste de gauche l'autorité ou la sous-autorité pour laquelle la CRL doit être renouvelée.
2. Cliquez sur **Actions**.

3. Sélectionnez **Renouveler la CRL**.
   Une boite de dialogue s'ouvre.
4. Renseignez le mot de passe de l'autorité ou de la sous-autorité.
5. Dans le cadre **Exporter la CRL**, cochez ou non la case **Exporter la CRL après sa mise à jour**.
   Si cette case est cochée, choisissez le **Format du fichier** d'export :

- **Format Base64 (PEM)**,
- **Format binaire (DER)**.

6. Cliquez sur **Appliquer**.
7. Si vous avez choisi d'exporter la CRL, une fenêtre vous présente le lien de téléchargement du fichier d'export de la CRL.

Supprimer une CRL

1. Sélectionnez dans la liste de gauche l'autorité ou la sous-autorité pour laquelle la CRL doit être supprimée.
2. Cliquez sur **Actions**.
3. Sélectionnez **Supprimer la CRL**.
   Une boîte de dialogue s'ouvre.
4. Validez la suppression en cliquant sur **OK**.

Supprimer la clé privée d'une identité (et conserver le certificat)

Après qu'une identité (utilisateur, serveur ou Smartcard) ait été créée sur le firewall et fournie à l'utilisateur final (généralement dans conteneur chiffré PKCS#12), il peut être souhaitable, pour des raisons de sécurité et de confidentialité, de vouloir supprimer la clé privée de l'identité afin de ne pas en garder une copie sur le firewall.

Pour supprimer la clé privée d'une identité :

1. Sélectionnez l'identité dans la liste de gauche.
2. Cliquez sur **Actions**.
3. Sélectionnez **Supprimer la clé privée**.
   Un message confirme la suppression.

Définir une autorité ou une sous-autorité par défaut

Pour définir une autorité ou une sous-autorité comme étant l'autorité par défaut :

1. Sélectionnez dans la liste de gauche l'autorité ou la sous-autorité.
2. Cliquez sur **Actions**.
3. Sélectionnez **Définir comme défaut**.
   Une boîte de dialogue s'ouvre.
4. Validez en cliquant sur **OK**.

Télécharger un certificat

Cette action permet d'exporter le certificat d'une autorité, d'une sous-autorité ou d'une identité.

Le fichier résultant peut être est au format :

- PEM (format ASCII - Encodage des données en Base64),
- DER (format binaire).

Pour télécharger un certificat :

1. Sélectionnez l'autorité, la sous-autorité ou l'identité dans la liste de gauche.
2. Cliquez sur **Télécharger**.
3. Sélectionnez **Certificat** puis le format du fichier.
4. Cliquez sur le lien de téléchargement du fichier contenant le certificat.

Télécharger une identité

Cette action permet de télécharger une identité utilisateur, serveur ou Smartcard.

Le fichier résultant peut être est au format :

- PEM (format ASCII - Encodage des données en Base64),
- DER (format binaire),
- P12 (format binaire chiffré).

Pour télécharger une identité :

1. Sélectionnez l'identité dans la liste de gauche.
2. Cliquez sur **Télécharger**.
3. Sélectionnez **Identité** puis choisissez le format du fichier d'export (PEM, DER ou P12).
4. Définissez le **mot de passe** destiné à protéger la clé privée incluse dans le fichier d'export.
5. **Confirmez** le mot de passe.
   Une jauge indique la robustesse du mot de passe choisi.
6. Cliquez sur **Télécharger le certificat** (format).
7. Cliquez sur le lien de téléchargement du fichier contenant l'identité.

Télécharger une CRL

Cette action permet de télécharger la CRL d'une autorité ou d'une sous-autorité.

Le fichier résultant peut être est au format :

- PEM (format ASCII - Encodage des données en Base64),
- DER (format binaire).

Pour télécharger une CRL :

1. Sélectionnez l'autorité ou la sous-autorité dans la liste de gauche.
2. Cliquez sur **Télécharger**.
3. Sélectionnez **CRL** puis le format du fichier.
4. Cliquez sur le lien de téléchargement du fichier contenant la CRL.

COMPTES TEMPORAIRES

Ce service permet la gestion de comptes dont la durée de validité est limitée. Ces comptes sont destinés à fournir temporairement un accès Internet public à des personnes externes à l'entreprise. Les comptes temporaires ne sont pas enregistrés dans le ou les annuaire(s) LDAP déclaré(s) sur le firewall.

Ces comptes sont caractérisés par les informations suivantes :

- Nom (obligatoire),
- Prénom (obligatoire),
- E-mail (optionnel),
- Société (optionnel),
- Date de début de validité du compte (obligatoire),
- Date de fin de validité du compte (obligatoire),
- Identifiant de connexion automatiquement constitué du prénom et du nom séparés par un point,
- Mot de passe généré de manière automatique.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Le module **Liste des comptes temporaires** permet la gestion (création / modification / suppression) de comptes temporaires.

Liste des comptes temporaires

Lorsque la méthode d'authentification "Comptes temporaires" n'est pas activée, ce module vous invite à vous rendre dans le module **Authentification** afin de procéder à son activation.

Une fois la méthode d'authentification "Comptes temporaires" activée, ce module permet de gérer les comptes temporaires : ajout, suppression, modification, impression des informations, export de la liste des comptes.

La grille

Cette grille présente l'ensemble des informations relatives aux comptes temporaires créés sur le firewall. Elle comporte les colonnes suivantes :

Identifiant	C'est l'identifiant de connexion pour l'utilisateur temporaire. Il est automatiquement formé par la concaténation du prénom et du nom séparés par un point. Exemple: john.doe
Prénom	Prénom associé au compte.
Nom	Nom associé au compte.
E-mail	Adresse e-mail associée au compte temporaire.
Société	Société associée au compte.
Depuis	Il s'agit de la date de début de validité du compte temporaire.
Jusqu'à	Il s'agit de la date de fin de validité du compte temporaire.

Mot de passe	Le mot de passe associé au compte temporaire. Ce mot de passe est généré automatiquement par le firewall.

Les actions possibles

Actualiser

Lorsque plusieurs personnes sont habilitées à créer des comptes temporaires, un clic sur ce bouton permet de rafraîchir la liste des comptes et de visualiser l'ensemble des saisies réalisées.

Ajouter un compte

Pour créer un compte temporaire, renseignez au moins son prénom, son nom ainsi que les dates de début et de fin de validité du compte.

Prénom	Prénom associé au compte.
Nom	Nom associé au compte.
E-mail	Adresse e-mail associée au compte temporaire.
Société	Société associée au compte.
Depuis	Sélectionnez dans le calendrier le premier jour de validité du compte temporaire. La valeur proposée par défaut correspond au jour courant.
Jusqu'à	Sélectionnez dans le calendrier le dernier jour de validité du compte temporaire. La valeur proposée par défaut tient compte de la date de début de validité et de la durée par défaut précisée dans l'onglet *Configuration*.

REMARQUE
L'identifiant associé au compte est automatiquement créé à l'aide du prénom et du nom séparés par un point (exemple: john.doe). C'est identifiant n'est plus modifiable après création du compte.

Afin de valider la création du compte, cliquez sur **Créer le compte**.

La fenêtre suivante présente un résumé des informations du compte ainsi que le mot de passe généré. Il est alors possible d'imprimer ces informations à l'aide du bouton **Imprimer** de cette fenêtre.

Supprimer

Ce bouton permet de supprimer un compte temporaire :

1. Sélectionnez l'utilisateur à supprimer.
2. Cliquez sur **Supprimer**.

Modifier le compte

Ce bouton vous permet de modifier certains paramètres d'un compte temporaire :

- Prénom,
- Nom,
- E-mail,

- Société,
- Date de début de validité,
- Date de fin de validité.

Seuls l'identifiant (définitif après création d'un compte) et le mot de passe du compte ne peuvent être modifiés par ce biais.

1. Sélectionnez le compte que vous souhaitez modifier.
2. Cliquez sur le bouton **Modifier le compte**.
3. Après avoir modifié les paramètres souhaités, cliquez sur le bouton **Appliquer**.
   La fenêtre suivante présente un résumé des informations du compte qu'il est possible d'**Imprimer** sauf si le bénéficiaire du compte temporaire a modifié le mot de passe initial; dans ce cas, seule la réinitialisation du mot de passe permet d'imprimer à nouveau les paramètres du compte.

Générer un nouveau mot de passe

Ce bouton permet de générer un nouveau mot de passe associé au compte temporaire sélectionné.

1. Sélectionnez le compte pour lequel vous souhaitez générer un mot de passe.
2. Cliquez sur le bouton **Générer un nouveau mot de passe**.
   Une fenêtre présente un résumé des informations du compte ainsi que le nouveau mot de passe associé, qu'il est possible d'**Imprimer**.

Exporter

Ce bouton permet d'exporter la liste des comptes temporaires au format CSV. Vous pouvez ensuite ouvrir ce fichier d'export dans un éditeur de texte afin de réaliser une mise en page personnalisée.

Imprimer la sélection

Ce bouton permet d'imprimer les informations d'un compte temporaire, sauf si le bénéficiaire du compte modifié le mot de passe initial; dans ce cas, seule la réinitialisation du mot de passe permet d'imprimer à nouveau les paramètres du compte.

CONFIGURATION

L'écran de configuration se compose de 3 onglets :

- **Configuration générale** : définition des caractéristiques du firewall (nom, langue, clavier) des paramètres cryptographiques et de date et d'heure, de la politique de mots de passe ainsi que des serveurs NTP.
- **Administration du Firewall** : configuration de l'accès à l'interface d'administration du firewall (port d'écoute, protection contre les attaques par force brute) ainsi que de l'accès distant par SSH.
- **Paramètres réseaux** : activation d'IPv6, configuration du serveur proxy et de la résolution DNS.

Onglet Configuration générale

> **NOTE**
> Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Configuration générale

Nom du firewall	Ce nom est affiché sur la fenêtre principale du firewall et est utilisé dans les e-mails d'alarmes envoyés à l'administrateur. Il peut également être utilisé comme nom DNS du portail captif lorsque celui-ci est activé et que l'option **Utiliser le nom du firewall** est sélectionnée. La taille maximale du nom du firewall est de 127 caractères.
Langue du Firewall (traces)	Choix de la langue utilisée par le firewall pour les traces de types log, Syslog et la configuration CLI. Les langues disponibles sont : **Français** et **Anglais**.
Clavier (console)	Type de clavier supporté par le firewall. Les langues disponibles sont : **Anglais**, **Français**, **Italien**, **Polonais**, **Suisse**.

Paramètres cryptographiques

Activer la récupération régulière des listes de révocation de certificats (CRL)	Lorsque cette option est cochée, le firewall vérifie toutes les 6 heures la date de validité de chaque CRL téléchargée depuis les points de distribution spécifiés dans la PKI. Lorsqu'une CRL est proche de son expiration ou expirée, une alarme est alors générée.

Activer le mode de conformité « Diffusion Restreinte (DR) » version 2021

L'option **Activer le mode de conformité « Diffusion Restreinte (DR) » version 2021** impose au firewall de respecter les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) concernant l'usage des coprocesseurs et accélérateurs cryptographiques dans les produits visant une qualification. Elle est impérative sur les réseaux répondant à la classification « Diffusion Restreinte ».
Ce mode repose notamment sur l'utilisation de versions logicielles pour les algorithmes de cryptographie (asymétrique, génération d'aléa et symétrique). Concernant les algorithmes de cryptographie symétrique, les instructions dites "AES-NI", disponibles sur certains produits, bénéficient d'une dérogation car elles sont uniquement constituées d'« instructions simples d'accélération » de certaines opérations cryptographiques.

L'activation du mode « Diffusion Restreinte (DR) » en version SNS 4.8.19 LTSB implique les comportements suivants :

- IPsec : seule l'authentification par certificat est autorisée.
- IPsec : les certificat utilisés (du certificat final jusqu'à la CA de confiance commune) doivent respecter les spécifications suivantes: signature ECDSA ou ECSDSA sur courbe SECP ou Brainpool, SHA256 comme algorithme de hachage et une taille de clé à 256 bits.
- IPsec : vérification que le firewall utilise bien la version 2 du protocole IKE.
- IPsec : vérification que le champ **ID du correspondant** est renseigné.
- IPsec : vérification que les algorithmes de chiffrement utilisés appartiennent bien aux groupes DH19 et DH28 (SECP et Brainpool 256).
- IPsec : vérification que l'algorithme de chiffrement utilisé est soit AES_GCM_16 (AEAD : Authenticated Encryption with Associated DATA. AES_GCM_16 n'est donc associé à aucun algorithme d'authentification), soit AES_CTR, impérativement associé au protocole d'authentification SHA256.
- IPsec : la vérification de révocation des certificats doit être active.
- IPsec : la taille de la fenêtre d'anti-rejeu ne doit pas être nulle.
- IPsec : l'algorithme de Pseudo-Random Function (PRF) doit être SHA256.

> **IMPORTANT**
> Lorsqu'une des conditions énoncées ci-dessus n'est pas respectée, la configuration IPsec non conforme est désactivée et le message suivant est affiché :
> "Le mode 'Diffusion Restreinte' a désactivé la configuration VPN IPsec non conforme".
> Ceci afin d'inciter l'administrateur à modifier la politique IPsec afin de pouvoir l'activer.

- Sur les firewalls équipés de processeurs Intel, le mode « Diffusion Restreinte (DR) » permet l'utilisation des jeux d'instructions cryptographiques matérielles du coprocesseur. Sur les firewalls équipés d'autres types de processeurs, le mode « Diffusion Restreinte (DR) » force la désactivation de ces jeux d'instructions, ce qui entraîne des baisses de performances lors du chiffrement.
- Le mode « Diffusion Restreinte (DR) » restreint les suites de chiffrement utilisables pour le portail d'authentification et le VPN SSL : seules les suites de chiffrement AES, SHA256, SHA384 et GCM sont autorisés.

> **NOTE**
> L'activation du mode « Diffusion Restreinte (DR) » nécessite un redémarrage du firewall.

Politique de mots de passe

Les paramètres indiqués s'appliquent à l'ensemble des mots de passe et clés pré-partagées définis sur le firewall (VPN PPTP, VPN IPsec, annuaire LDAP interne, etc.).

Longueur minimale des mots de passe	Indiquez le nombre minimum de caractères devant être respecté pour chaque mot de passe défini dans le firewall. **NOTE** La valeur définie par défaut est 1 pour des raisons de compatibilité en cas de migration en version 2 de configurations existantes.
Types de caractères obligatoires	Sélectionnez les types de caractères obligatoires à inclure dans chaque mot de passe : • Aucun : le mot de passe n'est soumis à aucune obligation de présence de caractères alphanumériques ou spéciaux, • Alphanumériques : le mot de passe doit contenir au minimum un caractère alphabétique et un chiffre, • Alphabétiques et spéciaux : le mot de passe doit contenir au minimum un caractère alphanumérique et un caractère spécial ('#', '@', etc…)
Entropie minimale	L'entropie est un paramètre permettant de définir le niveau de robustesse à respecter pour définir un mot de passe. Plus elle est élevée, plus la robustesse du mot de passe doit être importante. Lorsqu'elle est définie, elle intervient aussi bien dans le calcul des mots de passe générés aléatoirement (exemple : comptes temporaires) que pour les mots de passe définis manuellement. L'entropie tient compte de la longueur du mot de passe et du nombre de caractères uniques dans le mot de passe. Sa formule de calcul est la suivante : Entropie = (Longueur du mot de passe)*(Log(Nombre de caractères uniques dans le mot de passe)/Log(2)). La valeur proposée par défaut pour l'entropie est : 20. Une valeur de 0 désactive la prise en compte de l'entropie dans la génération automatique ou la définition manuelle des mots de passe.

Paramètres de date et d'heure

Saisie manuelle	Cette option permet de régler manuellement la date et l'heure du firewall.
Synchroniser avec votre machine	Cette option permet de régler la date et l'heure du firewall selon les paramètres de votre machine.
Maintenir le firewall à l'heure (NTP)	Cette option permet de maintenir à jour l'horloge locale du firewall via le réseau par le biais de serveurs NTP (*Network Time Protocol*). Complétez cette configuration en vous reportant sur les grilles **Liste des serveurs NTP** et **Liste des clés NTP**.
Date	Ce champ s'affiche seulement si l'option **Saisie manuelle** est cochée. Choisissez la date souhaitée dans le calendrier.

Heure	Ce champ s'affiche seulement si l'option **Saisie manuelle** est cochée. Saisissez l'heure souhaitée au format *HH:MM:SS*.
Fuseau horaire	Fuseau horaire défini pour le firewall (GMT par défaut). Un changement de fuseau horaire nécessite un redémarrage du firewall.

NOTE
La date et l'heure auxquelles votre firewall Stormshield Network est réglé sont importantes : elles vous permettent de situer dans le temps un événement enregistré dans les fichiers de log. Elles servent également à la programmation horaire des configurations.

Liste des serveurs NTP

IMPORTANT
Les serveurs NTP utilisés doivent être compatibles NTPv4.

Cette grille s'affiche seulement si l'option **Maintenir le firewall à l'heure (NTP)** est cochée.

Serveurs NTP (machine ou groupe-plages d'adresses) (15 max)	Affiche les serveurs NTP utilisés pour maintenir à jour l'horloge locale du firewall. Pour ajouter un serveur NTP, cliquez sur **Ajouter** et sélectionnez dans la liste déroulante l'objet représentant le serveur NTP que vous souhaitez ajouter. Si cet objet n'existe pas, cliquez sur l'icône de création d'objet pour le créer. Pour retirer un serveur NTP de la liste, sélectionnez-le et cliquez sur **Supprimer**.
Identifiant de clé NTP	Vous pouvez renseignez une clé si l'accès à un serveur NTP en nécessite une pour s'authentifier. Sélectionnez dans ce champ un identifiant de clé parmi la liste des clés NTP déjà créées. Chaque identifiant est associé à une valeur représentant la clé NTP. Pour créer un nouvel identifiant de clé ou pour visualiser la liste des clés NTP déjà créées, reportez-vous à la grille **Liste des clés NTP**.

Liste des clés NTP

Cette grille s'affiche seulement si l'option **Maintenir le firewall à l'heure (NTP)** est cochée.

Identifiant de clé NTP	Affiche la liste des identifiants de clé NTP. Ces identifiants peuvent être sélectionnés dans la colonne **Identifiant de clé NTP** de la grille **Liste des serveurs NTP**. Pour ajouter un identifiant de clé NTP, cliquez sur **Ajouter** et définissez-lui un identifiant unique compris entre 1 et 15. Pour supprimer un identifiant de la liste, sélectionnez-le et cliquez sur **Supprimer**.
Valeur	Affiche la valeur des clés NTP. Si vous ajoutez un nouvel identifiant de clé NTP, renseignez la valeur de sa clé dans ce champ (8 catactères maximum). Effectuez un double-clic sur une valeur existante pour la modifier.
Type de clé	Affiche l'algorithme utilisé pour la clé NTP. Vous pouvez le modifier en sélectionnant l'algorithme souhaité dans la liste déroulante.

Configuration avancée

Surveillance d'inactivité (*watchdog*)

Compteur de la surveillance d'inactivité (watchdog)	Ce dispositif teste l'activité du système du firewall. Ce test est réalisé de manière : • Logicielle sur les firewalls virtuels (EVA), • Matérielle et logicielle sur les firewalls physiques. La fréquence de ce test est fixée par ce seuil. En cas d'inactivité du système, ce « chien de garde » (*watchdog*) redémarre le firewall et déclenche un événement système (24). Pour stopper la surveillance, choisissez la valeur **Désactivé**.

Matériel

La zone **Matériel** s'affiche seulement sur les firewalls disposant de la fonction de *bypass*.

La fonction de *bypass* permet, lorsqu'elle est activée (prête à être déclenchée) et en cas de défaillance matérielle ou logicielle critique, de faire passer le trafic réseau au travers du firewall SNS sans qu'aucune analyse ne soit mise en œuvre. Cette fonction permet ainsi d'assurer une continuité de service dans les milieux sensibles.

Activer le mode sûreté	Lorsque vous cochez cette case, vous activez le mode Sûreté du *bypass*. Lorsque ce mode est activé : • Le mécanisme de *bypass* est activé (prêt à être déclenché) sur tous les segments *bypass* configurés pour l'utiliser (interfaces concernées regroupées dans un bridge). Une liste indique les segments *bypass* sur lesquels le mode Sûreté sera activé. • Lorsqu'un événement déclencheur survient (défaillance matérielle ou logicielle critique), le mécanisme de *bypass* est déclenché et le trafic réseau des segments *bypass* concernés passe alors au travers du firewall SNS sans qu'aucune analyse ne soit mise en œuvre. Selon la défaillance rencontrée, le mécanisme de *bypass* est immédiatement déclenché ou après écoulement d'un compte à rebours. • Une fois le mécanisme de *bypass* déclenché, seul un réarmement permet de retrouver un fonctionnement où le firewall SNS effectue de nouveau ses analyses. Vous ne pouvez pas activer le mode Sûreté sur un firewall SNS configuré en haute disponibilité. À noter que tant que le mode Sûreté n'est pas activé, la fonction de *bypass* reste **désactivée** en **permanence**, même si une défaillance critique survient.
Seuil d'inactivité du mode sûreté	Lors d'une défaillance logicielle, notamment lorsque le système d'exploitation du firewall SNS ne répond plus ou est surchargé, le mécanisme de *bypass* se déclenche après écoulement d'un compte à rebours dont le seuil de départ correspond au Seuil d'inactivité du mode sûreté. Sélectionnez le seuil souhaité. Les valeurs proposées vont de 1 minute à 4 minutes.
Réarmement du mode sûreté	Une fois le mécanisme de *bypass* déclenché, seul un réarmement permet de retrouver un fonctionnement où le firewall SNS effectue de nouveau ses analyses. Cliquez sur ce bouton pour réarmer le mécanisme de *bypass*. **IMPORTANT** Après un réarmement manuel, vous devez vérifier le fonctionnement correct des flux réseau. En effet, les connexions initiées pendant la phase active du *bypass* seront interrompues et devront être rétablies à l'initiative des machines distantes.

Pour plus d'informations sur le principe de fonctionnement du *bypass*, sur les firewalls et modules réseau équipés de la fonction de *bypass* et sur la manière de la configurer, reportez-vous à la note technique Gérer le bypass des firewalls SNS.

Portail captif

Redirection vers le portail captif	Cette option permet de choisir la dénomination du firewall utilisée lors de la génération des URI de redirection vers le portail captif. Quatre valeurs sont proposées : • Utiliser l'adresse du firewall. • Utiliser le nom du firewall. Il s'agit du nom indiqué dans le champ **Nom du firewall** de la section **Configuration générale** ou du numéro de série du firewall si aucun nom n'a été précisé dans ce champ. • Utiliser le certificat du portail captif. Il s'agit du nom du firewall précisé dans le certificat du portail. • Préciser un nom de domaine (FQDN).
Nom de domaine (FQDN)	Saisissez un nom DNS pleinement qualifié pour le firewall (ex. : firewall.company.org). Ce champ est accessible seulement si la valeur **Préciser un un nom de domaine (FQDN)** a été sélectionnée dans le champ précédent.

Télémétrie

> **NOTE**
> Lorsque l'administrateur qui consulte ce module est connecté avec un compte autre que *admin* (super-administrateur), ce cadre est grisé et intitulé **Télémétrie (nécessite le compte 'admin')**.

Autoriser l'envoi à Stormshield de données d'utilisation (anonyme)	Lorsque cette case est cochée, votre firewall envoie vers le Cloud Stormshield (sur le port 443) des données d'utilisation à des fins statistiques (liste ci-dessous). En transmettant ces données **parfaitement anonymes**, vous aidez Stormshield à affiner les paramètres de performances du proxy et les tailles et limites des futures versions et plate-formes matérielles SNS.

Liste des données d'utilisation à des fins statistiques :

- Nombre de lignes générées dans chaque fichier de log,
- Taille de chaque fichier de logs,
- Consommation CPU,
- Utilisation mémoire,
- Nombre de connexions prises en charge par le proxy, par protocole,
- Nombre de connexions dégradées prises en charge par le proxy, par protocole,
- Nombre maximal de connexions simultanées prises en charge par le proxy, par protocole,
- Nombre maximal de connexions dégradées simultanées prises en charge par le proxy, par protocole,
- Nombre d'objets dans la base objet, par type,
- Nombre de règles de filtrage et de NAT,
- Nombre de connexions simultanées au travers du firewall,
- Nombre de machines connues du firewall,

- Nombre d'authentifications par type,
- Nombre de contrôles antivirus effectués,
- Nombre d'utilisateurs connectés pour chaque méthode d'authentification,
- Nombre d'Agents TS connectés,
- Statistiques de consommation mémoire des *sockets*,
- Informations d'utilisation de la partition des logs,
- Statistiques de consommation mémoire et CPU des démons,
- Information sur l'utilisation ou non du TPM,
- Statistiques sur la PKI (nombre de CA, de certificats, d'identités et de certificats protégés par le TPM),
- Nombre d'URL correspondant à la catégorie d'URL "URL compromises",
- Information sur l'utilisation ou non de la solution de classification d'URL Extended Web Control (EWC),
- Nombre de requêtes de classification d'URL,
- Nombre de tunnels IPsec site à site configurés et activés dans la politique IPsec active,
- Nombre maximal de tunnels IPsec site à site établis,
- Nombre de tunnels IPsec mobiles configurés et activés dans la politique IPsec active,
- Nombre maximal de tunnels IPsec mobiles établis,
- Nombre de tunnels IPsec IKE v1 configurés dans la politique IPsec active,
- Nombre de tunnels IPsec IKE v2 configurés dans la politique IPsec active,
- Nombre de tunnels IPsec avec authentification par clé pré-partagée configurés dans la politique IPsec active,
- Nombre de tunnels IPsec avec authentification par certificat configurés dans la politique IPsec active,
- Nombre de tunnels IPsec avec authentification par certificat et XAUTH configurés dans la politique IPsec active,
- Nombre de tunnels IPsec avec authentification EAP-GTC configurés dans la politique IPsec active,
- Nombre de tunnels IPsec avec authentification par certificat et EAP-GTC configurés dans la politique IPsec active,
- Nombre d'entrées présentes dans le cache TLS 1.3,
- Nombre d'entrées avec l'erreur de délai d'attente dépassé (*timeout*) présentes dans le cache TLS 1.3,
- Nombre de vidages du cache TLS 1.3 suite à son remplissage,
- Nombre de signaux d'interruption pour fin anormale d'un processus,
- Date de la dernière émission d'un signal d'interruption pour fin anormale d'un processus,
- Nombre d'échecs d'envoi de fichiers vers l'analyse Sandboxing pendant l'intervalle de mesure.

Invite de commande SSH

Nom du nœud système	Ce champ permet de définir un nom additionnel qui sera concaténé au nom du firewall. Ce nom de nœud système est particulièrement utile dans le cadre d'une configuration en haute disponibilité, puisqu'il vous permet d'identifier aisément le membre du cluster sur lequel vous êtes connecté lorsque vous ouvrez une session en mode console via SSH par exemple. Lorsqu'il est configuré, ce nom du nœud système apparaît dans le bandeau supérieur de l'interface Web d'administration, entre parenthèses, derrière le numéro de série du firewall.

Onglet Administration du Firewall

Accès à l'interface d'administration du Firewall

Autoriser le compte 'admin' à se connecter	Le compte *admin* est le seul compte ayant tous les droits. Il peut se connecter sans certificat. Décochez cette case pour désactiver l'accès à l'interface d'administration du firewall au compte *admin*. Il conservera son accès en SSH ou en Console sur le firewall. **IMPORTANT** Ce compte est à considérer comme « dangereux » aux vues de l'étendue des possibilités de configuration et des accès lui étant attribués.
Port d'écoute	Ce champ représente le port sur lequel les administrateurs peuvent accéder à l'interface d'administration (https, tcp/443 par défaut). Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône prévue à cet effet. Ce nouvel objet doit obligatoirement utiliser le protocole « TCP ».
Configurer le certificat SSL du service	Cliquez sur ce lien pour modifier le certificat présenté par l'interface d'administration et le portail d'authentification du firewall.
Délai maximal d'inactivité (tous administrateurs)	Définissez le délai maximal d'inactivité autorisé avant déconnexion pour tous les comptes administrateurs du firewall. Un compte administrateur peut définir dans ses préférences un temps de déconnexion en cas d'inactivité tant qu'il est inférieur au délai maximal paramétré.
Activer la protection contre les attaques par force brute	Les attaques par force brute se définissent par des tentatives de connexion répétées au firewall, en testant toutes les combinaisons de mot de passe possibles. Cette protection concerne l'ensemble des connexions destinées à l'administration du firewall : connexions à l'interface Web d'administration mais aussi connexions SSH. Cochez cette case pour activer cette protection.
Tentatives d'authentification autorisées	Nombre maximum de tentatives de connexion autorisées pour un administrateur avant blocage (erreur d'identifiant ou de mot de passe / sensibilité à la casse par exemple). Les tentatives d'authentification autorisées sont limitées à 3 par défaut. Ce champ est accessible seulement si la case **Activer la protection contre les attaques par force brute** est cochée.

Durée de blocage (minutes)	Temps durant lequel un administrateur ne peut plus se connecter au firewall après le nombre d'échecs spécifié ci-dessus. La durée ne peut excéder 60 minutes. Ce champ est accessible seulement si la case **Activer la protection contre les attaques par force brute** est cochée.

Accès aux pages d'administration du Firewall

Ajouter	Choisissez un objet réseau au sein de la liste déroulante. Celui-ci sera considéré comme un **Poste d'administration autorisé** à se connecter à l'interface d'administration. Cela peut être une machine, un groupe de machines, un réseau ou une plage d'adresses.
Supprimer	Sélectionner la ligne à retirer de la liste et cliquez sur **Supprimer**.

Avertissement pour l'accès à l'interface d'administration

Fichier d'avertissement	Vous pouvez ajouter un texte d'avertissement (*disclaimer*) sur la page de connexion à l'interface Web d'administration du firewall. Il s'affiche alors à droite de la fenêtre d'authentification et nécessite un clic sur le bouton **J'ai compris afin d'activer cette fenêtre d'authentification**. Le fichier contenant ce texte peut-être chargé sur le firewall à l'aide du sélecteur de fichiers .... Pour une mise en forme enrichie, le texte peut être au format HTML mais ne doit pas comporter de JavaScript. Une fois le fichier enregistré sur le firewall, son contenu peut être affiché à l'aide du bouton .
Supprimer le fichier d'avertissement	Ce bouton permet de supprimer le fichier d'avertissement préalablement chargé sur le firewall.

Accès distant par SSH

> **NOTE**
> Pour modifier les paramètres d'accès distant par SSH, vous devez être connecté avec le compte *admin*.

Activer l'accès par SSH	Le SSH (Secure Shell) est un protocole qui permet de se connecter à une machine distante avec une liaison sécurisée. Les données sont chiffrées entre machines. Le SSH permet également d'exécuter des commandes sur un serveur distant. En cochant cette case, vous activez l'accès au firewall par SSH aux comptes déclarés administrateurs du firewall avec le droit "Console (SSH)" ainsi qu'au compte *admin*. En décochant cette case, aucun compte ne peut se connecter au firewall par SSH. Toutes les tentatives de connexion réussies ou échouées par SSH génèrent des logs.

Autoriser l'utilisation de mot de passe	En cochant cette case, tous les comptes déclarés administrateurs du firewall avec le droit "Console (SSH)" ainsi que le compte *admin* peuvent se connecter au firewall par SSH en utilisant leur mot de passe. En décochant cette case, les administrateurs doivent alors utiliser un couple clé privée / clé publique pour s'authentifier. Ce champ est accessible seulement si la case **Activer l'accès par SSH** est cochée. **IMPORTANT** Si le mot de passe d'un ou plusieurs comptes d'administrateurs autorisés à se connecter en SSH contient des caractères non ASCII (exemple : '€', 'à'), il est nécessaire de vous reporter à la procédure Modifier le jeu de caractères pour permettre une connexion SSH avec un mot de passe contenant des caractères non ASCII décrite au bas de cette page.
Utiliser le shell nsrpc pour les administrateurs autres que le compte admin	En cochant cette case, tous les comptes déclarés administrateurs du firewall avec le droit "Console (SSH)" utilisent exclusivement l'interpréteur *shell nsrpc* à l'ouverture d'une session SSH sur le firewall. Cet accès leur permet d'utiliser les commandes *CLI / Serverd* selon les droits dont ils disposent. En décochant cette case, tous les comptes déclarés administrateurs du firewall avec le droit "Console (SSH)" utilisent par défaut l'interpréteur *shell*. Le compte *admin* n'est pas concerné et bénéficie toujours par défaut de l'interpréteur *shell*. **IMPORTANT** L'accès à l'interpréteur *shell* donne des privilèges sans aucune restriction, équivalent à un accès *super-administrateur*. Les commandes utilisées par cet accès ne génèrent pas de logs. Ce champ est accessible seulement si la case **Activer l'accès par SSH** est cochée.
Port d'écoute	Ce champ représente le port sur lequel les administrateurs peuvent accéder au firewall en SSH. ssh, tcp/22 par défaut). Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône prévue à cet effet. Ce nouvel objet doit obligatoirement utiliser le protocole « TCP ». Ce champ est accessible seulement si la case **Activer l'accès par SSH** est cochée.

Recommandations

Sur le firewall

Il est recommandé :

- D'utiliser une clé ECDSA pour s'authentifier,
- Pour une utilisation au delà de l'année 2030, le groupe minimal à utiliser doit être le groupe Diffie-Hellman 15,

- De configurer les suites cryptographiques suivantes dans le fichier ConfigFiles/System :

```
[SSHCiphers]
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
aes256-ctr

[SSHKex]
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256

[SSHMACs]
hmac-sha2-256-etm@openssh.com
```

- De ne pas utiliser les suites cryptographiques de type *Mac-then-Encrypt* :

```
hmac-sha2-256
hmac-sha2-512
```

Sur le poste client qui se connecte au firewall

Il est recommandé de configurer la suite cryptographique ecdsa-sha2-nistp256.

Modifier le jeu de caractères pour permettre une connexion SSH avec un mot de passe contenant des caractères non ASCII

Si votre mot de passe contient des caractères non ASCII (exemple : '€', 'à'), et pour vous connecter via SSH à un firewall en version 4 de SNS, qui utilise par défaut le jeu de caractères ISO-8859-15 pour le stockage des mots de passe, vous devez procéder comme suit.

Option 1 : modifier le jeu de caractères sur le client SSH pour adopter ISO-8859-15

Poste sous Windows utilisant le client SSH *Putty*

1. Sélectionnez la session correspondant à la connexion au firewall.
2. Positionnez-vous dans le menu de gauche **Window** > **Translation**.
3. Pour le champ **Remote Character Set**, sélectionnez la valeur **ISO-8859-15**.

Système Unix utilisant un terminal Gnome

1. Positionnez-vous dans le menu **Preferences** > **Profils**.
2. Cliquez sur le bouton "+" pour ajouter un nouveau profil.
3. Nommez-le (exemple : ISO).
4. Dans l'onglet **Compatibilité** de ce profil, modifiez le champ **Codage** pour **ISO-8859-15**.
5. Dans la fenêtre principale du terminal, faites un clic droit et choisissez **Profils** > *ce nouveau profil* (ISO dans cet exemple) pour l'appliquer,

Système Unix utilisant un terminal UTF-8 quelconque

Après avoir installé l'utilitaire *luit*, lancez la connexion SSH avec la commande suivante :

```
luit -encoding ISO8859-15 ssh <login>@<FW_IP_address>
```

Option 2 : modifier le jeu de caractères sur le firewall (nécessite un redémarrage du firewll)

1. Modifiez temporairement le mot de passe du compte *admin* pour un mot de passe ne comprenant aucun caractère non ASCII.
2. Connectez-vous en SSH au firewall avec ce nouveau mot de passe.
3. Changez le jeu de caractères du firewall à l'aide de la commande : `setconf /usr/Firewall/ConfigFiles/language Language PswdCharset UTF-8`.
4. Redémarrez le firewall.

5. Modifiez de nouveau le mot de passe du compte *admin* en y incluant des caractères non ASCII si vous le souhaitez.
6. Vérifiez qu'une connexion SSH au firewall avec un client SSH utilisant par défaut le jeu de caractères UTF-8.

Onglet Paramètres réseaux

Support IPv6

ON / OFF	Placez le sélecteur sur ON afin d'activer le support d'IPv6 sur le firewall. Pour connaître le champ d'application du support IPv6 et les changements des différents modules de l'interface d'administration, consultez le chapitre SUPPORT IPV6. **IMPORTANT** Cette action étant irréversible, il est donc proposé d'effectuer une sauvegarde de votre configuration avant d'activer ce support. Pour revenir à un support unique de l'adressage IPv4, vous devrez effectuer une remise configuration d'usine avant de pouvoir restaurer la sauvegarde de cette configuration. Cette remise configuration d'usine s'effectue par le bouton dédié si votre équipement en est équipé ou en console, par la commande CLI « defaultconfig ».

Serveur proxy

ON / OFF	Placez le sélecteur sur ON afin d'activer l'utilisation d'un proxy pour l'accès à Internet du firewall pour les services Active Update et Licence Update.
Serveur	Ce champ permet de spécifier l'objet correspondant au serveur utilisé par le firewall comme proxy.
Port	Ce champ permet de spécifier le port utilisé par le firewall pour contacter le proxy.
Identifiant	Ce champ permet de définir un identifiant utilisé par le firewall pour s'authentifier auprès du proxy.
Mot de passe	Définissez un mot de passe que le firewall devra fournir pour accéder au serveur proxy.

Résolution DNS

Liste des serveurs DNS utilisés par le firewall

Les serveurs DNS permettent au firewall de résoudre (connaître son adresse IP à partir d'un nom de machine) les objets ou machines configurés en Résolution DNS « Automatique ».

Ajouter	Lorsque vous cliquez sur **Ajouter**, une ligne vierge s'ajoute à la liste des serveurs DNS. Choisissez alors un objet dans la liste déroulante ou créez-en un nouveau.

Supprimer	Sélectionnez le serveur DNS à retirer et cliquez sur **Supprimer**. Notez que si vous supprimez tous les serveurs DNS définis dans la grille, le firewall utilise alors les serveurs *Root DNS*. Ces serveurs sont renseignés dans le fichier de configuration DNS (*/usr/Firewall/Data/dns*).

CONFIGURATION DE LA SUPERVISION

Les données et courbes de supervision se basent sur les traces enregistrées sur le firewall. Ces traces sont analysées.

L'écran se divise en deux parties :

- En haut : le paramétrage des différents intervalles de rafraîchissement.
- En bas : un tableau listant au sein de deux onglets, les interfaces réseau et files d'attente de Qualité de service à superviser

Intervalles de rafraîchissement

Période maximale affichée (en minutes)	Ce paramètre permet de régler la période de données à afficher pour une courbe. Cette période est exprimée en minutes et peut prendre les valeurs suivantes : 15, 30, 45 ou 60.
Intervalle de rafraîchissement des courbes (en secondes)	Ce paramètre permet de régler l'intervalle de rafraîchissement des courbes de supervision. Cet intervalle s'exprime en secondes et peut prendre les valeurs suivantes : 5, 10, 15 ou 20.
Intervalle de rafraîchissement des grilles (en minutes)	Ce paramètre permet de régler l'intervalle de rafraîchissement des données de supervision présentées dans les grilles. Cet intervalle s'exprime en minutes et peut prendre les valeurs suivantes : 1, 3, 5, 7 ou 10.

La grille de configuration des interfaces, des files d'attente de QoS et des services Web à superviser

Onglet "Configuration des interfaces"

Il est possible d'**Ajouter** ou de **Supprimer** des interfaces à superviser à l'aide des boutons du même nom.

La grille présente les colonnes suivantes :

Nom	Sélectionnez l'interface devant être supervisée. Les interfaces proposées sont les interfaces Ethernet, les agrégats de liens, les VLAN, les interfaces Wi-Fi et les interfaces de type modem (dialup).

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des interfaces supervisées :

- Ajouter,
- Supprimer.

Onglet "Configuration de la QoS"

Il est possible d'**Ajouter** ou de **Supprimer** des files d'attente de QoS à superviser à l'aide des boutons du même nom. Ces files d'attentes doivent être préalablement définies au sein du module **Politique de sécurité** > **Qualité de service**.

La grille présente les colonnes suivantes :

Nom	Sélectionnez dans la liste déroulante la file d'attente de QoS devant être supervisée

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des files d'attente supervisées :

- Ajouter,
- Supprimer.

Onglet "Configuration des services Web"

Il est possible d'**Ajouter** ou de **Supprimer** des services Web (services Web standard ou services Web personnalisés) à superviser à l'aide des boutons du même nom.

La grille présente les colonnes suivantes :

Nom	Sélectionnez dans la liste déroulante le service Web devant être supervisé.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des services Web supervisés :

- Ajouter,
- Supprimer.

CONFIGURATION DES ANNUAIRES

LDAP est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

Les firewalls Stormshield Network embarquent une base LDAP interne. Celle-ci stocke les informations relatives aux utilisateurs devant s'authentifier pour passer au travers du firewall. En plus de cet annuaire interne, il est également possible de connecter le firewall jusqu'à quatre bases LDAP externes qui se trouvent sur des machines distantes.

Le module de Configuration des annuaires (accessible dans le menu **Utilisateurs > Configuration des annuaires**) comporte un assistant de configuration en première page, vous proposant de choisir votre annuaire et de l'initialiser.

- Connexion à un annuaire Microsoft Active Directory,
- Connexion à un annuaire LDAP externe,
- Connexion à un annuaire LDAP externe de type PosixAccount,
- Création d'un LDAP interne.

En fonction de votre choix, l'étape suivante est variable, la configuration d'un LDAP externe réclamant plus de renseignements.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Selon votre modèle de firewall, un nombre maximum détermine l'ensemble des utilisateurs pouvant être authentifiés simultanément. Cette délimitation est indiquée dans la section Utilisateurs.

Chacune des configurations de ces annuaires comporte 3 étapes, sélectionnez la base LDAP choisie en cochant la case correspondante.

Pour pouvoir établir une connexion sécurisée (LDAPS) entre le firewall et l'annuaire, il est nécessaire que le serveur hébergeant l'annuaire externe supporte et utilise l'une des suites de chiffrement suivantes :

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

Avec, pour les suites basées sur ECDHE, des courbes elliptiques appartenant obligatoirement à l'un des groupes listés ci-dessous :

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),

- secp521r1 (0x0019),
- secp384r1 (0x0018).

Fenêtre principale

Ce module contient la liste des différents annuaires configurés sur le firewall.

Il est divisé en 2 zones distinctes :

- A gauche : la liste des annuaires et la barre d'actions,
- A droite : le détail de la configuration et de la structure de l'annuaire sélectionné.

La barre d'actions

Bouton Ajouter un annuaire

Cliquez sur ce bouton pour lancer l'assistant de création d'un nouvel annuaire LDAP.

Liste déroulante Action

Faites dérouler cette liste pour afficher les différentes actions possibles :

- **Supprimer** l'annuaire sélectionné,
- **Définir** l'annuaire sélectionné comme annuaire par **défaut**,
- **Vérifier la connexion** à l'annuaire sélectionné,
- **Vérifier l'utilisation** de l'annuaire sélectionné dans la configuration du firewall.

Création d'un LDAP interne

Ce type d'annuaire est hébergé par votre firewall multifonctions Stormshield Network, vos informations y seront stockées une fois l'annuaire LDAP construit.

Étape 1 : Choix de l'annuaire

Comme précisé ci-dessus, il faut cocher la base LDAP choisie pour valider votre choix. Ceci est la première étape de la configuration d'un annuaire.

Cochez la case **Création d'un annuaire LDAP interne** et cliquez sur **Suivant**.

Étape 2 : Accès à l'annuaire

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous désirez créer. Les informations saisies se retrouveront dans le schéma de l'annuaire LDAP de votre firewall. Le nom de l'annuaire sera automatiquement construit en se basant sur la valeur des champs **Organisation** et **Domaine**.

Organisation	Le nom de votre société (ex : mycompany).
Domaine	L'extension de votre nom de domaine (exemple : fr, eu, org, com...).

Mot de passe	Définition du mot de passe d'administration LDAP.
Confirmer	Confirmation du mot de passe d'administration LDAP, que vous venez de renseigner dans le champ précédent.
Robustesse du mot de passe	Cette jauge indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.
Hachage des mots de passe	Algorithme de chiffrement des mots de passe des utilisateurs.

NOTE
Seuls le mot de passe et la méthode de hachage des mots de passe seront modifiables par la suite, une fois que vous aurez configuré votre LDAP interne.

Cliquez sur **Terminer** pour afficher l'écran de l'annuaire LDAP interne.

Écran de l'annuaire LDAP interne

Une fois la configuration de l'annuaire LDAP effectuée, vous accédez à l'écran du LDAP interne qui présente les éléments suivants :

Configuration

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.
Organisation	Ce champ reprend le nom de votre société, renseigné au préalable.
Domaine	Ce champ reprend le domaine de votre société.
Identifiant	Le login qui vous permet de vous connecter à la base LDAP interne.
Mot de passe	Le mot de passe permettant au firewall de se connecter à l'annuaire. Il est possible de le modifier.
Confirmer	Confirmation du mot de passe d'administration LDAP, que vous venez de renseigner dans le champ précédent.
Robustesse du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Accès au LDAP interne

Activer l'accès non chiffré (PLAIN)	Les données saisies ne seront pas chiffrées, mais affichées en clair.
Activer l'accès SSL. (Certificat SSL présenté par le serveur)	Afin de mettre en place l'accès SSL, vous devrez sélectionner un certificat serveur préalablement généré par votre autorité racine, ou un certificat importé. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module.

Configuration avancée

Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire	Si cette option est cochée, la requête d'authentification est interceptée par le firewall et effectuée avec le compte disposant de tous les droits sur l'annuaire : cn=NetasqAdmin. Dans le cas contraire, la requête est directement effectuée dans l'annuaire.
Autoriser les groupes imbriqués	Cocher cette option vous permet de créer des groupes à l'intérieur d'autres groupes d'utilisateurs.
Hachage des mots de passe	Algorithme de chiffrement des mots de passe des utilisateurs. Une mention précise si l'algorithme est obsolète.

Connexion à un annuaire LDAP externe

Le LDAP externe est un annuaire auquel votre firewall multifonctions Stormshield Network va se connecter.

Etape 1 : Choix de l'annuaire

Sélectionnez la base LDAP correspondant à votre choix. Ceci est la première étape de la configuration de cet annuaire.

Cochez la case **Connexion à un annuaire LDAP externe** et cliquez sur **Suivant**.

Etape 2 : Accès à l'annuaire

Nom de domaine	Nom permettant d'identifier l'annuaire interne lorsque plusieurs annuaires sont définis sur le firewall. Dans une configuration comportant des annuaires multiples, ce nom devra compléter l'identifiant de l'utilisateur pour réaliser une authentification (identifiant@nom_de_domaine). Il est donc fortement conseillé de renseigner un nom de domaine DNS dans ce champ. **EXEMPLE** compagnie.com
Serveur	Vous devez choisir un objet correspondant à votre serveur LDAP au sein de la liste déroulante. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP.
Port	Vous devez renseigner le port d'écoute de votre serveur LDAP. Le port par défaut est : 389.

Domaine racine (Base DN)	Vous devez renseigner le Domaine racine (DN) de votre annuaire. Le DN représente le nom d'une entrée, sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence. Vous pouvez remplir le champ avec le nom du Domaine Racine (DN). **EXEMPLE** Le domaine LDAP est "compagnie.com", le domaine Racine (Base DN) est "dc=compagnie,dc=com".
Accès en lecture seulement	Si cette case est cochée, vous ne pourrez effectuer aucune action d'écriture sur l'annuaire LDAP externe.
Connexion anonyme	Cette option permet de ne pas renseigner d'identifiant et de mot de passe pour se connecter à l'annuaire LDAP externe. Le serveur LDAP doit bien évidemment autoriser les connexions anonymes. Lorsque cette case est cochée, les champs **Identifiant** et **Mot de passe** deviennent inactifs (grisés)
Identifiant	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des modifications (droits en lecture et écriture) sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. **EXEMPLE** cn=id Ce champ est inactif lorsque la case **Connexion anonyme** a été cochée.
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné. Ce champ est inactif lorsque la case **Connexion anonyme** a été cochée.
Hachage des mots de passe	Sélectionnez l'algorithme utilisé pour le hachage des mots de passe utilisateurs.

Cliquez sur **Terminer** pour afficher l'écran de l'annuaire LDAP externe.

Écran de l'annuaire LDAP externe

Une fois que la configuration de l'annuaire LDAP effectuée, vous accédez au LDAP externe qui présente les éléments suivants :

Onglet « Configuration»

La page affichée présente une fenêtre récapitulative des informations saisies pour votre LDAP externe et différents services concernant l'accès à votre annuaire.

Annuaire distant

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.

Serveur	Ce champ reprend le nom du serveur que vous avez préalablement rempli à la page précédente.
Port	Ce champ reprend le port d'écoute que vous avez préalablement sélectionné à la page précédente.
Domaine racine (Base DN)	Le Domaine racine de votre annuaire tel que défini lors de sa création. **EXEMPLE** dc=compagnie,dc=org
Identifiant	L'identifiant permettant au firewall de se connecter sur votre serveur LDAP.
Mot de passe	Le mot de passe créé sur le firewall pour vous connecter sur le serveur LDAP.

Connexion sécurisée (SSL)

Pour pouvoir établir une connexion sécurisée (LDAPS) entre le firewall et l'annuaire, il est nécessaire que le serveur hébergeant l'annuaire externe supporte et utilise l'une des suites de chiffrement suivantes :

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

Avec, pour les suites basées sur ECDHE, des courbes elliptiques appartenant obligatoirement à l'un des groupes listés ci-dessous :

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Activer l'accès en SSL	Cette option permet d'effectuer une vérification de votre certificat numérique généré par l'autorité racine du firewall. Les informations sont chiffrées en SSL. Cette méthode utilise le port 636. L'accès public au LDAP est protégé avec le protocole SSL. **NOTE** Si cette option n'est pas cochée, l'accès est non chiffré.
Vérifier le certificat auprès d'une Autorité racine	Lors d'une connexion à la base LDAP, le firewall vérifie que le certificat a bien été délivré par l'Autorité de certification (CA) spécifiée en-dessous.
Sélectionner une Autorité de certification de confiance	Ce champ permet de sélectionner l'Autorité de certification qui sera utilisée pour vérifier le certificat serveur délivré par le serveur LDAP, afin d'assurer l'authenticité de la connexion à ce serveur. **NOTE** Cette case sera grisée par défaut si les deux options ci-dessus ne sont pas cochées.

Configuration avancée

Serveur de secours	Ce champ permet de définir un serveur de remplacement au cas où le serveur principal serait injoignable. Vous pouvez le sélectionner parmi la liste d'objets proposés dans la liste déroulante.
Port	Renseignez le port d'écoute de votre serveur LDAP de secours. Il peut être différent du port d'écoute du serveur principal. Le port par défaut est : 389 (ldap).
Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire	Lorsque cette case est cochée, le firewall utilise l'identifiant déclaré lors de la création de l'annuaire pour vérifier auprès du serveur LDAP les droits d'un utilisateur lorsque celui-ci s'authentifie. Dans le cas contraire, le firewall utilise le compte de l'utilisateur pour effectuer cette vérification.
Ne pas compléter l'identifiant (ID) par le Domain Name (Base DN)	Cochez cette case si vous ne souhaitez pas que les identifiants utilisateurs récupérés par le firewall depuis cet annuaire prennent la forme identifiant@domaine (exemple john.doe@mydomain.com si l'annuaire sélectionné gère les utilisateurs du domaine mydomain.com).
Autoriser les groupes imbriqués	Cochez cette case si vous souhaitez que les groupes inclus dans d'autres groupes soient importés depuis l'annuaire sélectionné.

Cliquez sur **Appliquer** pour valider votre configuration.

Onglet « Structure»

Accès en lecture

Filtre de sélection des utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = InetOrgPerson*.
Filtre de sélection des groupes d'utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les Groupes d'utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = GroupOfNames*.

L'annuaire est en lecture seule. La création d'utilisateurs et de groupes ne sera pas autorisée : Si cette case est cochée, vous ne pourrez effectuer aucune action d'écriture.

Correspondance d'attributs

Appliquer un modèle : Ce bouton vous propose de choisir parmi 3 serveurs LDAP, celui que vous appliquerez pour définir vos attributs :

- OpenLDAP : serveur LDAP.
- Microsoft Active Directory (AD) : services d'annuaires LDAP pour les systèmes d'exploitation sous Windows.
- Open Directory : répertoire de sites web sous licence Open Directory

Attributs de l'annuaire externe	Cette colonne représente la valeur donnée à l'attribut au sein de l'annuaire externe.

> **EXEMPLES**
> *Cn=COMPAGNIE*
> *telephoneNumber= +33 (0)3 61 96 30*
> *mail* = salesadmin@compagnie.com

Configuration avancée

Hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.

Vous devez choisir la méthode de hash désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.
MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits.

> **REMARQUE**
> Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.

SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.

Branche 'utilisateurs'	Donnez le nom de la branche LDAP pour stocker les utilisateurs. **EXEMPLE** ou=users
Branche 'groupes'	Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. **EXEMPLE** ou=groups
Branche de l'autorité de certification	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. **NOTE** Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL (voir menu **Utilisateurs**\module **Authentification**\onglet **Méthodes disponibles** : il faut ajouter la méthode d'authentification **Certificat (SSL)** et indiquer la CA dans la colonne de droite « Autorités de confiance (C.A) »)

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

Connexion à un annuaire LDAP externe de type PosixAccount

Étape 1 : Choix de l'annuaire

Sélectionnez la base LDAP correspondant à votre choix. Ceci est la première étape de la configuration de cet annuaire.

Cochez la case **Connexion à un annuaire LDAP externe de type PosixAccount** et cliquez sur **Suivant**.

Étape 2 : Accès à l'annuaire

Nom de domaine	Nom permettant d'identifier l'annuaire interne lorsque plusieurs annuaires sont définis sur le firewall. Dans une configuration comportant des annuaires multiples, ce nom devra compléter l'identifiant de l'utilisateur pour réaliser une authentification (identifiant@nom_de_domaine). Il est donc fortement conseillé de renseigner un nom de domaine DNS dans ce champ.
Serveur	Vous devez choisir un objet correspondant à votre serveur LDAP au sein de la liste déroulante. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP.
Port	Vous devez renseigner le port d'écoute de votre serveur LDAP. Le port par défaut est : TCP/389 (objet **ldap**).
Domaine racine (Base DN)	Vous devez renseigner le Domaine racine (DN) de votre annuaire. Le DN représente le nom d'une entrée, sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence. Vous pouvez remplir le champ avec le nom du Domaine AD ou celui du Domaine Racine (DN). **EXEMPLE** Le domaine AD est "compagnie.com", le domaine Racine (Base DN) est "dc=compagnie,dc=com".
Connexion anonyme	En cochant cette case, la connexion à l'annuaire LDAP ne requiert pas l'utilisation d'un identifiant et de son mot de passe associé. Dans ce cas, les champs Identifiant et Mot de passe sont grisés.
Identifiant	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des modifications (droits en lecture et écriture) sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. **EXEMPLE** cn=id
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.
Hachage des mots de passe	Sélectionnez l'algorithme utilisé pour le hachage des mots de passe utilisateurs.

REMARQUE
La connexion à un annuaire externe de type *PosixAccount* est obligatoirement réalisée en lecture seule. Il n'est donc pas possible de créer des utilisateurs ou groupes depuis l'interface d'administration Web du firewall.

Cliquez sur **Terminer** pour afficher l'écran de l'annuaire LDAP externe.

Écran de l'annuaire LDAP externe

Une fois que la configuration de l'annuaire LDAP effectuée, vous accédez au LDAP externe qui présente les éléments suivants :

Onglet « Configuration »

La page affichée présente une fenêtre récapitulative des informations saisies pour votre LDAP externe et différents services concernant l'accès à votre annuaire.

Annuaire distant

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.
Serveur	Ce champ reprend le nom du serveur que vous avez préalablement rempli à la page précédente.
Port	Ce champ reprend le port d'écoute que vous avez préalablement sélectionné à la page précédente.
Domaine racine (Base DN)	Le Domaine racine de votre annuaire tel que défini lors de sa création. **EXEMPLE** dc=compagnie,dc=org
Identifiant	L'identifiant permettant au firewall de se connecter sur votre serveur LDAP.
Mot de passe	Le mot de passe créé sur le firewall pour vous connecter sur le serveur LDAP.

Connexion sécurisée (SSL)

Pour pouvoir établir une connexion sécurisée (LDAPS) entre le firewall et l'annuaire, il est nécessaire que le serveur hébergeant l'annuaire externe supporte et utilise l'une des suites de chiffrement suivantes :

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

Avec, pour les suites basées sur ECDHE, des courbes elliptiques appartenant obligatoirement à l'un des groupes listés ci-dessous :

- x25519 (0x001d),
- secp256r1 (0x0017),
- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Activer l'accès en SSL	Cette option permet d'effectuer une vérification de votre certificat numérique généré par l'autorité racine du firewall. Les informations sont chiffrées en SSL. Cette méthode utilise le port 636. L'accès public au LDAP est protégé avec le protocole SSL. **NOTE** Si cette option n'est pas cochée, l'accès est non chiffré.
Vérifier le certificat auprès d'une Autorité racine	Lors d'une connexion à la base LDAP, le firewall vérifie que le certificat a bien été délivré par l'Autorité de certification (CA) spécifiée en-dessous.
Sélectionner une Autorité de certification de confiance	Cette option permet de sélectionner l'Autorité de certification qui sera utilisée pour vérifier le certificat serveur délivré par le serveur LDAP, afin d'assurer l'authenticité de la connexion à ce serveur. **NOTE** Cette case sera grisée par défaut si les deux options ci-dessus ne sont pas cochées.

Configuration avancée

Serveur de secours	Ce champ permet de définir un serveur de remplacement au cas où le serveur principal tomberait. Vous pouvez le sélectionner parmi la liste d'objets proposés dans la liste déroulante. En cliquant sur le bouton **Tester l'accès à l'annuaire** au-dessous de ce champ, une fenêtre vous précisera si votre serveur principal est opérationnel. Vous pourrez cliquer sur **OK**.
Port	Renseignez le port d'écoute de votre serveur LDAP de secours. Il peut être différent du port d'écoute du serveur principal. Le port par défaut est : 389 (ldap).
Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire	Lorsque cette case est cochée, le firewall utilise l'identifiant déclaré lors de la création de l'annuaire pour vérifier auprès du serveur LDAP les droits d'un utilisateur lorsque celui-ci s'authentifie. Dans le cas contraire, le firewall utilise le compte de l'utilisateur pour effectuer cette vérification.

Ne pas compléter l'identifiant (ID) par le Domain Name (Base DN)	Cochez cette case si vous ne souhaitez pas que les identifiants utilisateurs récupérés par le firewall depuis cet annuaire prennent la forme identifiant@domaine (exemple john.doe@mydomain.com si l'annuaire sélectionné gère les utilisateurs du domaine mydomain.com).
Autoriser les groupes imbriqués	Cochez cette case si vous souhaitez que les groupes inclus dans d'autres groupes soient importés depuis l'annuaire sélectionné.

Cliquez sur **Appliquer** pour valider votre configuration.

Onglet « Structure»

Accès en lecture

Filtre de sélection des utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondant au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = InetOrgPerson*.
Filtre de sélection des groupes d'utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les groupes d'utilisateurs correspondant au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = PosixGroup*.

L'annuaire est en lecture seule. La création d'utilisateurs et de groupes ne sera pas autorisée : la connexion aux annuaires LDAP externes de type POSIX étant obligatoirement en lecture seule, cette case est automatiquement cochée et l'option est grisée.

Correspondance d'attributs

Appliquer un modèle : Ce bouton vous propose de choisir parmi 3 serveurs LDAP, celui que vous appliquerez pour définir vos attributs :

- OpenLDAP : serveur LDAP.
- Microsoft Active Directory (AD) : services d'annuaires LDAP pour les systèmes d'exploitation sous Windows.
- Open Directory : répertoire de sites web sous licence Open Directory

Attributs de l'annuaire externe	Cette colonne représente la valeur donnée à l'attribut au sein de l'annuaire externe. Pour un annuaire LDAP de type *PosixAccount*, l'attribut Stormshield **member** prend la valeur *memberUid*.

Configuration avancée

Hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.

Vous devez choisir la méthode de hachage désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.

MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits. **REMARQUE** Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.
SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.

Branche 'utilisateurs'	Pour un annuaire externe de type *PosixAccount*, ce champ n'est pas disponible.
Branche 'groupes'	Pour un annuaire externe de type *PosixAccount*, ce champ n'est pas disponible.
Branche de l'autorité de certification	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. **NOTE** Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL. (Voir menu **Utilisateurs** >module **Authentification** > onglet **Méthodes disponibles** : il faut ajouter la méthode d'authentification **Certificat (SSL)** et indiquer la CA dans la colonne de droite « Autorités de confiance (C.A) »)

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

Connexion à un annuaire Microsoft Active Directory

A l'instar des annuaires interne et externe, l'Active Directory propose les mêmes fonctionnalités de gestion des utilisateurs développées par Microsoft, et utilisant le système d'exploitation *Windows*.

Étape 1 : Choix de l'annuaire

Sélectionnez l'annuaire correspondant à votre choix. Ceci est la première étape de la configuration de cet annuaire.

Cochez la case **Connexion à un annuaire Microsoft Active Directory** et cliquez sur **Suivant**.

Étape 2 : Accès à l'annuaire

Nom de domaine	Nom permettant d'identifier l'annuaire interne lorsque plusieurs annuaires sont définis sur le firewall. Dans une configuration comportant des annuaires multiples, ce nom devra compléter l'identifiant de l'utilisateur pour réaliser une authentification (identifiant@nom_de_domaine). Il est donc fortement conseillé de renseigner un nom de domaine DNS dans ce champ.
Serveur	Vous devez choisir un objet correspondant à votre serveur LDAP au sein de la liste déroulante. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP.
Port	Vous devez renseigner le port d'écoute de votre serveur LDAP. Le port par défaut est : 389.
Domaine racine (Base DN)	Vous devez renseigner le Domaine racine (DN) de votre annuaire. Le DN représente le nom d'une entrée, sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence. **EXEMPLE** Le domaine AD est "compagnie.com", le domaine Racine (Base DN) est "o=compagnie,dc=com".
Identifiant (user DN)	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des modifications (droits en lecture et écriture) sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. **EXEMPLE** cn=Administrateur,cn=utilisateurs
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.
Hachage des mots de passe	Sélectionnez l'algorithme utilisé pour le hachage du mot de passe d'accès à l'annuaire.

Cliquez sur **Terminer** pour afficher l'écran de l'annuaire Microsoft Active Directory.

Écran de l'annuaire Microsoft Active Directory

Onglet « Configuration »

Une fois que la configuration de l'annuaire effectuée, vous accédez à l'Active Directory qui présente les éléments suivants :

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.
Serveur	Ce champ reprend le nom du serveur que vous avez préalablement rempli à la page précédente.
Port	Ce champ reprend le port d'écoute que vous avez préalablement sélectionné à la page précédente.
Domaine racine (Base DN)	Le Domaine racine de votre annuaire tel que défini lors de sa création. **EXEMPLE** o=compagnie,dc=org
Identifiant	L'identifiant permettant au firewall de se connecter sur votre serveur LDAP. **EXEMPLE** cn=Administrateur,cn=utilisateurs
Mot de passe	Sélectionnez l'algorithme utilisé pour le hachage des mots de passe utilisateurs.

Connexion sécurisée (SSL)

Pour pouvoir établir une connexion sécurisée (LDAPS) entre le firewall et l'annuaire, il est nécessaire que le serveur hébergeant l'annuaire externe supporte et utilise l'une des suites de chiffrement suivantes :

- TLS_AES_128_GCM_SHA256 (0x1301) (TLS1.3),
- TLS_CHACHA20_POLY1305_SHA256 (0x1303) (TLS1.3),
- TLS_AES_256_GCM_SHA384 (0x1302) (TLS1.3),
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b),
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f),
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e),
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9),
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8),
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa),
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c),
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030),
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f),

Avec, pour les suites basées sur ECDHE, des courbes elliptiques appartenant obligatoirement à l'un des groupes listés ci-dessous :

- x25519 (0x001d),
- secp256r1 (0x0017),

- x448 (0x001e),
- secp521r1 (0x0019),
- secp384r1 (0x0018).

Activer l'accès en SSL	Cette option permet d'effectuer une vérification de votre certificat numérique généré par l'autorité racine du firewall. Les informations sont chiffrées en SSL. Cette méthode utilise le port 636. L'accès public au LDAP est protégé avec le protocole SSL. **NOTE** Si cette option n'est pas cochée, l'accès est non chiffré.
Vérifier le certificat auprès d'une Autorité racine	Lors d'une connexion à la base LDAP, le firewall vérifie que le certificat a bien été délivré par l'Autorité de certification (CA) spécifiée en-dessous.
Sélectionner une Autorité de certification de confiance	Cette option permet de sélectionner l'Autorité de certification qui sera utilisée pour vérifier le certificat serveur délivré par le serveur LDAP, afin d'assurer l'authenticité de la connexion à ce serveur. **NOTE** Cette case sera grisée par défaut si les deux options ci-dessus ne sont pas cochées.

Configuration avancée

Serveur de secours	Ce champ permet de définir un serveur de remplacement au cas où le serveur principal serait injoignable. Vous pouvez le sélectionner parmi la liste d'objets proposés dans la liste déroulante.
Port	Renseignez le port d'écoute de votre serveur LDAP de secours. Il peut être différent du port d'écoute du serveur principal. Le port par défaut est : 389 (ldap).
Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire	Lorsque cette case est cochée, le firewall utilise l'identifiant déclaré lors de la création de l'annuaire pour vérifier auprès du serveur LDAP les droits d'un utilisateur lorsque celui-ci s'authentifie. Dans le cas contraire, le firewall utilise le compte de l'utilisateur pour effectuer cette vérification.
Ne pas compléter l'identifiant (ID) par le Domain Name (Base DN)	Cochez cette case si vous ne souhaitez pas que les identifiants utilisateurs récupérés par le firewall depuis cet annuaire prennent la forme identifiant@domaine (exemple john.doe@mydomain.com si l'annuaire sélectionné gère les utilisateurs du domaine mydomain.com).
Autoriser les groupes imbriqués	Cochez cette case si vous souhaitez que les groupes inclus dans d'autres groupes soient importés depuis l'annuaire sélectionné.

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

Onglet « Structure»

Accès en lecture

Filtre de sélection des utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = InetOrgPerson*.
Filtre de sélection des groupes d'utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les Groupes d'utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = GroupOfNames*.

L'annuaire est en lecture seule. La création d'utilisateurs et de groupes ne sera pas autorisée : Si cette case est cochée, vous ne pourrez effectuer aucune action d'écriture.

Correspondance d'attributs

Appliquer un modèle : Ce bouton vous propose de choisir parmi 3 serveurs LDAP, celui que vous appliquerez pour définir vos attributs :

- OpenLDAP
- Microsoft Active Directory (AD)
- Open Directory

Attributs de l'annuaire externe	Cette colonne représente la valeur donnée à l'attribut au sein de l'annuaire externe.

EXEMPLES
Cn= COMPAGNIE
telephoneNumber= +33 (0)3 61 96 30
mail = salesadmin@compagnie.com

Configuration avancée

Hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.

Vous devez choisir la méthode de hash désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.
MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits.

REMARQUE
Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.

SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.
Branche 'utilisateurs'	Donnez le nom de la branche LDAP pour stocker les utilisateurs. **EXEMPLE** ou=users
Branche 'groupes'	Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. **EXEMPLE** ou=groups
Branche de l'autorité de certification	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. **NOTE** Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL. (Voir menu **Utilisateurs** > module **Authentification** > onglet **Méthodes disponibles** : il faut ajouter la méthode d'authentification **Certificat (SSL)** et indiquer la CA dans la colonne de droite « Autorités de confiance (C.A) »)

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

CONFIGURATION DES RAPPORTS

Ce module permet d'activer les rapports statiques ainsi que les courbes historiques du firewall. Ces derniers se basent sur l'ensemble du trafic traité par le firewall, c'est-à-dire toutes les connexions transitant par toutes les interfaces, qu'elles soient internes ou externes.

Général

Rapports statiques	Active les rapports statiques visibles dans le module **Monitoring** > Rapports. Les rapports statiques se basent sur les traces enregistrées sur le firewall. Pour la plupart des rapports, un top 10 des valeurs les plus récurrentes est produit (le reste des valeurs est regroupé dans une valeur "Autres"). Les rapports SD-WAN se basent sur les métriques et les états opérationnels obtenus lors de la supervision des routeurs et de leurs passerelles. L'actualisation des données s'effectue toutes les minutes et comprend un calcul d'un nouveau top 50 des dernières heures et jours afin de mieux représenter les valeurs récurrentes et de ne pas surcharger la base. Les données stockées sur carte SD peuvent être lues par une autre plate-forme équipée du moteur SQLite.
Courbes historiques	Active les courbes historiques visibles dans le module **Monitoring** > Supervision. Les courbes historiques se basent sur les traces enregistrées sur le firewall. Elles proposent quatre échelles de temps : dernière heure, jour, semaine ou mois. Ces plages sont calculées par rapport aux paramètres de date et d'heure du firewall.

Onglet Liste des rapports

Les actions

Rechercher	Filtre la liste des rapports selon ce qui est entré dans le champ de recherche.
Catégories	Filtre la liste des rapports selon la catégorie sélectionnée.
Définir l'état	Active ou désactive le rapport sélectionné au préalable dans la grille.
Réinitialiser la base de données	Réinitialise la base de données.

Les compléments d'information

Rapports actifs	Affiche le nombre de rapports activés.
Taille de la base de données	Indique l'espace disque utilisé par la base de données SQLite.

La grille

État	Active ou désactive le rapport concerné. Certains rapports nécessitent d'avoir souscrit une option spécifique pour être activés. **IMPORTANT** Bien que la génération des rapports ne soit pas prioritaire sur les autres traitements, le nombre de rapports activés ou le type de trafic peut avoir un réel impact sur les performances du firewall.
Catégorie	Indique la catégorie de données à laquelle le rapport est rattaché. Les catégories suivantes sont disponibles : • Web, • Sécurité, • Virus, • Spam, • Vulnérabilité, • Réseau, • Réseau industriel, • Sandboxing, • SD-WAN, • Services Web, • Personnalisé.
Description	Affiche une description du rapport et des données qu'il contient.
Avertissement	Affiche un message d'avertissement si une option ou une fonctionnalité nécessaire à la construction du rapport n'est pas activée.
Données personnelles	Précise grâce à la présence d'un symbole que le rapport contient des données personnelles (adresse IP source, nom de machine, nom d'utilisateur, ...). La visualisation de ces données est possible sous réserve de disposer du droit **Logs : accès complet (données personnelles)**.

NOTE
Ces données peuvent être envoyées via Syslog à destination de la solution Virtual Log Appliance for Stormshield afin de construire des rapports ou d'effectuer leur archivage.

Onglet Liste des graphiques historiques

État	Active ou désactive le graphique historique concerné.
Description	Affiche une description du graphique historique et des données qu'il contient.
Avertissement	Affiche un message d'avertissement si une option nécessaire à la construction du graphique n'est pas activée.

CONSOLE CLI

Les firewalls SNS embarquent une interface en ligne de commandes (CLI) constituée d'un jeu de commandes propriétaire. Les commandes sont accessibles via un shell et permettent de configurer et de superviser toutes les fonctionnalités du firewall.

L'accès au shell CLI se fait via un protocole sécurisé NSRPC (*NETASQ Secure Remote Procedure Call*) en local sur le firewall dans le module **Système > Console CLI** ou à distance à partir d'une machine en utilisant des exécutables dédiés sous Windows et Linux.

Le module **Console CLI** du firewall est composé de deux parties :

- La liste des commandes en haut de l'écran, soit une zone de texte,
- Une zone de saisie des commandes en bas de l'écran.

Les commandes saisies peuvent être enregistrées à l'aide du bouton d'enregistrement situé dans le bandeau supérieur de l'interface Web d'administration. Cette fonctionnalité doit auparavant avoir été activée dans le module Préférences.

Liste des commandes

L'écran affiche par défaut les principales commandes exécutables. Certaines peuvent en impliquer d'autres. Pour visualiser l'ensemble des commandes, exécutez celle de votre choix. La liste affichera les commandes supplémentaires incluses dans celle-ci.

Vous pouvez également utiliser l'argument `HELP` avec une commande pour afficher de l'aide sur ses arguments. Par exemple :

```
CONFIG HELP
```

Pour obtenir l'intégralité des commandes exécutables, consultez le Guide de référence des commandes CLI Serverd (disponible en anglais).

Zone de saisie

Dans la zone de saisie, écrivez la commande que vous souhaitez exécuter.

Vous pouvez naviguer à travers les commandes déjà exécutées avec les touches "Haut" et "Bas" du clavier. L'historique des commandes est stocké et ré-utilisé à chaque fois que l'application web est relancée.

Effacer l'affichage	Ce bouton permet d'effacer l'affichage en cours de la console CLI.
Exécuter	Ce bouton permet de lancer la commande saisie. Vous pouvez également appuyer sur la touche "Entrée" du clavier pour exécuter la commande.
Mode multiligne	Cochez cette case pour exécuter un bloc de commandes. Ce bloc de commandes peut, par exemple, être issu d'un enregistrement de séquence de commandes (bouton **Enregistrement de commandes**).
Arrêt si erreur	Cette case est disponible seulement si le mode multiligne est activé. Cochez cette case pour interrompre à la première erreur rencontrée la séquence de commandes.

DHCP

Le module DHCP se présente en un seul écran, sauf si le support d'IPv6 est activé. Si ce support est activé, le module DHCP se compose de deux onglets distincts et ce paramétrage s'effectue dans l'onglet *DHCPv4*.

Général

	Ce bouton permet d'activer ou de désactiver l'utilisation du protocole DHCP sur le firewall (serveur ou relai).

Serveur DHCP	Envoie différents paramètres réseaux aux clients DHCP.
Relai DHCP	Le mode relai DHCP est à utiliser lorsque l'on souhaite rediriger les requêtes clientes vers un serveur DHCP externe.

Service « Serveur DHCP »

Le service « serveur DHCP » présente 4 zones de configuration :

- **Paramètres par défaut.** Ce menu est réservé à la configuration des paramètres DNS (nom de domaine, serveurs DNS primaire et secondaire) et de la passerelle par défaut envoyés aux clients DHCP.
- **Plage d'adresses**. Par plage, vous spécifiez un groupe d'adresses destinées à être allouées aux utilisateurs. L'adresse est alors allouée pour le temps déterminé dans la configuration avancée.
- **Réservation**. L'adresse allouée par le service est toujours la même pour les machines listées dans la colonne **Réservation**.
- **Configuration avancée.** Ce menu permet d'activer ou non l'envoi du fichier de configuration automatique des proxies pour les machines clientes (WPAD : Web Proxy Autodiscovery Protocol). Il est également possible d'y préciser des serveurs additionnels (WINS, SMTP, POP3, etc.) et de personnaliser la durée d'affectation des adresses IP distribuées par le service DHCP.

Paramètres par défaut

Si l'option serveur DHCP a été cochée, il est possible ici de configurer des paramètres globaux, comme le **nom de domaine**, les **serveurs DNS**, etc. que les machines clientes vont utiliser.

Nom de domaine	Nom de domaine utilisé par les machines clientes DHCP pour leur résolution DNS.
Passerelle	La passerelle par défaut est la machine indiquant les routes à utiliser si l'adresse de destination n'est pas connue du client.
DNS primaire	Sélectionnez le serveur DNS primaire qui sera envoyé aux clients DHCP. Il s'agit d'un objet de type machine. Si aucun objet n'est précisé, c'est le serveur DNS primaire du Firewall qui leur sera transmis.
DNS secondaire	Sélectionnez le serveur DNS secondaire qui sera envoyé aux clients DHCP. Il s'agit d'un objet de type machine. Si aucun objet n'est précisé, c'est le serveur DNS secondaire du Firewall qui leur sera transmis.

Plage d'adresses

Pour qu'un serveur DHCP fournisse des adresses IP, il est nécessaire de configurer une réserve d'adresses dans laquelle il pourra puiser.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des plages d'adresses, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Permet d'ajouter une plage d'adresses. Sélectionnez ou créez une plage d'adresses IPv4 (objet réseau de type **Plage d'adresses IP**).
Supprimer	Permet de supprimer une plage d'adresses, ou plusieurs plages d'adresses simultanément.

La grille affiche les plages d'adresses utilisées par le serveur DHCP pour la distribution d'adresses aux clients.

Plages d'adresses	Sélectionnez un objet réseau de type **Plage d'adresses IP** dans la liste déroulante. Le serveur puisera dans cette réserve pour distribuer des adresses aux clients. Si aucune interface protégée du Firewall n'a d'adresse IP dans le réseau englobant cette plage, un message d'avertissement « Pas d'interface protégée correspondant à cette plage d'adresse » est affiché.
Passerelle	Ce champ permet d'affecter une passerelle par défaut spécifique aux clients DHCP. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **Passerelle par défaut** de la section **Paramètres** qui est utilisée comme passerelle pour les clients DHCP.
DNS primaire	Ce champ permet d'affecter un serveur DNS primaire spécifique aux clients DHCP. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS primaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
DNS secondaire	Ce champ permet d'affecter un serveur DNS secondaire spécifique aux clients DHCP. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS secondaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
Nom de domaine	Ce champ permet d'indiquer un nom de domaine spécifique qui sera utilisé par le client DHCP pour sa résolution DNS. Si aucun nom n'est spécifié, la valeur « Domaine par défaut » est affichée dans cette colonne. C'est alors le nom de domaine indiqué dans le champ **Nom de domaine** de la section **Paramètres par défaut** qui est utilisé pour le client.

AVERTISSEMENTS
Deux plages d'adresses ne peuvent se chevaucher. Une plage d'adresses appartient à un unique bridge/interface.

Réservation

Bien qu'utilisant un serveur distribuant dynamiquement des adresses IP aux clients, il est possible de réserver une adresse IP spécifique pour certaines machines. Cette configuration se rapproche d'un adressage statique, mais rien n'est paramétré sur les postes clients, simplifiant ainsi leur configuration réseau.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des réservations d'adresses, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Permet d'ajouter une réservation d'adresse IP pour un objet réseau spécifique de type machine.
Supprimer	Permet de supprimer une réservation d'adresse IP. Si une réservation est supprimée, la machine concernée se verra attribuer aléatoirement une nouvelle adresse lors de son renouvellement.

La grille affiche les objets machines pour lesquels une réservation d'adresse est effectuée : ces objets seront obligatoirement définis à l'aide d'une adresse IPv4 et de leur adresse MAC. Cette dernière sert en effet d'identifiant unique du client pour l'obtention ou le renouvellement de son adresse IP réservée.

Réservation	Ce champ contient le nom de l'objet réseau (machine) possédant une adresse IPv4 réservée.
Passerelle	Ce champ permet d'affecter une passerelle par défaut spécifique à chaque client DHCP bénéficiant d'une réservation d'adresse. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **Passerelle par défaut** de la section **Paramètres** qui est utilisée comme passerelle pour le client.
DNS primaire	Ce champ permet d'affecter un serveur DNS primaire spécifique à chaque client DHCP bénéficiant d'une réservation d'adresse. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS primaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
DNS secondaire	Ce champ permet d'affecter un serveur DNS secondaire spécifique à chaque client DHCP bénéficiant d'une réservation d'adresse. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS secondaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
Nom de domaine	Ce champ permet d'indiquer un nom de domaine spécifique qui sera utilisé par le client DHCP pour sa résolution DNS. Si aucun nom n'est spécifié, la valeur « Domaine par défaut » est affichée dans cette colonne. C'est alors le nom de domaine indiqué dans le champ **Nom de domaine** de la section **Paramètres par défaut** qui est utilisé pour le client.

Configuration avancée

D'autres types de serveurs à utiliser peuvent être envoyés par le biais du service DHCP aux postes clients.

Filename	Nom du fichier d'amorçage et de configuration que le poste client peut récupérer au démarrage.
Serveur SMTP	Le serveur SMTP est utilisé pour envoyer des e-mails. Une liste déroulante permet de choisir l'objet de type machine correspondant à ce serveur.
Serveur POP3	Le serveur POP3 est utilisé pour recevoir des e-mails. Une liste déroulante permet de choisir l'objet de type machine correspondant à ce serveur.
Next-server	Adresse du serveur hébergeant le fichier d'amorçage et de configuration des postes clients précisé dans le champ **Filename**.
Serveur de News (NNTP)	Ce champ permet d'envoyer l'adresse du serveur de news aux clients DHCP. Ce serveur fournit le service NNTP, qui autorise les clients à lire les nouvelles Usenet.
Serveur TFTP	Le serveur TFTP sert pour le boot à distance des machines. Ce champ (champ option 150 : TFTP server address) peut être utilisé pour le démarrage d'équipements réseaux tels que des routeurs, des X-terminals ou des stations de travail sans disque dur.
Annoncer le fichier de configuration automatique des proxies (WPAD)	Si cette option est cochée, le serveur DHCP distribue aux clients DHCP la configuration d'accès à Internet au travers d'un fichier d'auto-configuration de proxy (PAC : Proxy Auto Configuration) doté d'une extension « .pac ». Ce fichier doit être renseigné dans les paramètres d'authentification (onglet *Portail Captif* du menu **Configuration** > **Utilisateurs** > **Authentification**). Il peut être rendu accessible depuis les interfaces internes et/ou externes (onglets *Interfaces Internes* et *Interfaces Externes* du menu **Configuration** > **Utilisateurs** > **Authentification**).
Mettre à jour les entrées des serveurs DNS	Si cette option est cochée, les serveurs DNS sont dynamiquement mis à jour lorsque les informations contenues par le serveur DHCP sont modifiées.

Durée de bail attribuée

Par défaut (heure)	Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées pour une durée limitée. Il faut donc indiquer ici le temps par défaut pendant lequel les stations garderont la même adresse IP.
Minimum (heure)	Temps minimum pendant lequel les stations garderont la même adresse IP.
Maximum (heure)	Temps maximum pendant lequel les stations garderont la même adresse IP.

Service « Relai DHCP »

Le service « relai DHCP » présente 2 zones de configuration :

- **Paramètres.** Ce menu permet de configurer le ou les serveurs DHCP vers lesquels le firewall relaiera les requêtes DHCP des machines clientes.
- **Interfaces d'écoute et de sortie du service DHCP relai.** La ou les interfaces réseau sur lesquelles le firewall est à l'écoute des requêtes DHCP clientes.

Paramètres

Serveur(s) DHCP	La liste déroulante permet de sélectionner un objet machine, ou un objet groupe contenant des machines. Le Firewall relaiera les requêtes des clients vers ce(s) serveur(s) DHCP.
Adresse IP utilisée pour relayer les requêtes DHCP	L'adresse IP renseignée dans ce champ comme source est alors utilisée pour les requêtes relayées. Cette option permet par exemple aux utilisateurs locaux de bénéficier, au travers d'un tunnel IPsec de la configuration automatique des paramètres IP d'un serveur DHCP distant. Celle-ci doit appartenir à l'extrémité locale de trafic pour pouvoir être prise en compte par le tunnel. Cette option n'est disponible uniquement pour un service DHCPv4 et via un tunnel VPN dont les extrémités de trafic sont paramétrées en IPv4. **NOTE** Ce fonctionnement n'est possible qu'avec un serveur DHCPv4 externe ; il n'est pas possible d'utiliser le service DHCP du firewall. **NOTE** Les extrémités de trafic du tunnel doivent être paramétrées en IPv4 et les extrémités de tunnel peuvent être définies en IPv4 ou en IPv6. Si non renseignée, la sélection de l'adresse est automatique (sélection de l'@IP de l'interface en face du routage)
Relayer les requêtes DHCP pour toutes les interfaces	Si cette case est cochée, le Firewall écoutera les requêtes des clients DHCP sur l'ensemble de ses interfaces réseaux. Dans ce cas, la grille de saisie **Interfaces d'écoute et de sortie du service DHCP relai** est grisée.

Interfaces d'écoute et de sortie du service DHCP Relai

Il s'agit d'indiquer :

- Par quelles interfaces réseaux le Firewall va recevoir les requêtes des clients DHCP,
- Par quelles interfaces réseaux le Firewall va joindre le(s) serveur(s) DHCP externe(s).

Le service de Relai DHCP présent sur le firewall peut également écouter sur l'interface utilisée par le VPN IPsec, afin de relayer les requêtes DHCP au travers ces tunnels.

Les interfaces d'écoute doivent comprendre les interfaces pour l'écoute de la requête côté client ainsi que les interfaces d'écoute de la réponse côté serveur.

Il faudra configurer le serveur DHCP de telle manière qu'il puisse distribuer des adresses IP aux clients qui passent à travers le relai.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des interfaces d'écoute, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Ajoute une ligne dans la grille et ouvre la liste déroulante des interfaces du firewall pour y sélectionner une interface.
Supprimer	Permet de supprimer une ou plusieurs interfaces d'écoute ou de sortie.

DNS DYNAMIQUE

L'écran de configuration du client DNS dynamique se décompose en 2 parties :

- Sur la gauche, la **Liste des profils DNS dynamique**.
- Sur la droite, la **Résolution DNS**, ou configuration du profil préalablement sélectionné.

Liste des profils de DNS dynamique

Le tableau présentant les profils se compose de 2 colonnes :

État	Permet, par un double-clic d'activer ou de désactiver le profil.
Aperçu	Indications du nom du domaine, de l'interface et de l'état de la résolution associées au profil.
Interface associée	Indique l'interface associée au nom de domaine comme sélectionné dans les paramètres du domaine.
Résolution	Indique si une résolution DNS a été effectuée pour ce profil.

- Le bouton **Ajouter** permet d'ajouter un profil.
- Le bouton **Supprimer** permet de supprimer un profil préalablement sélectionné.
- Le bouton **Réinitialiser** permet la réinitialisation de l'état du profil DNS Dynamique.

Configuration d'un profil

Ajouter un profil

1. Cliquez sur **Ajouter**.
2. Sélectionnez le type de profil souhaité : **Fournisseur DynDns** ou **Fournisseur No-IP**.
   Les paramètres de résolution DNS à appliquer à ce nouveau profil s'affichent dans la partie droite de l'écran.
3. Adaptez ces paramètres en suivant les indications de la section **Résolution DNS pour le profil *Nom_du_Profil***.

Modifier un profil

1. Dans la liste des profils située à gauche de l'écran : double-cliquez sur le profil à modifier.
   Les paramètres de résolution DNS à appliquer à ce profil s'affichent dans la partie droite de l'écran.
2. Adaptez ces paramètres en suivant les indications de la section **Résolution DNS pour le profil *Nom_du_Profil***.

Résolution DNS pour le profil *Nom_du_Profil*

Paramètres du domaine

Nom de domaine	Nom de domaine attribué au client DNS dynamique. Par exemple : *monfirewall.dyndns.org*. En utilisant l'option **Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard),** vous pouvez couvrir tous les sous-domaines. **EXEMPLE** Si vous spécifiez **compagnie.dyndns.org** dans le champ **Nom de domaine** et que l'option **Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard)** est sélectionnée, tous les sous-domaines (commerce.compagnie.dyndns.org, labo.compagnie.dyndns.org, etc.) seront associés au client.
Interface associée au nom de domaine	Nom de l'interface réseau dont l'adresse IP est associée au nom de domaine. Notez que : • Une interface ne peut utiliser qu'un seul profil. • Un profil ne peut être utilisé que par une interface. • Le profil ne peut être actif si une interface n'est pas indiquée
Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard)	Active ou désactive la prise en compte des sous-domaines liés au nom de domaine. **NOTE** Une souscription à l'offre Wildcard est nécessaire pour bénéficier de cette fonctionnalité.

Fournisseur du service DNS dynamique

Cette zone vous permet de saisir les informations d'accès à votre fournisseur de service DNS Dynamique.

Fournisseur DNS dynamique	Le nom du fournisseur de services DNS sélectionné à la création du profil est affiché (**DynDns** ou **No-IP**).
Nom d'utilisateur (obligatoire)	Utilisateur indiqué par le fournisseur de services DNS pour l'authentification du client DNS dynamique.
Mot de passe (obligatoire)	Mot de passe indiqué par le fournisseur de services DNS pour l'authentification du client DNS dynamique.
Serveur DNS dynamique (obligatoire)	Serveur du fournisseur de services DNS : • *members.dyndns.org* (proposé par défaut) ou *members.dyndns.com* pour le service **DynDns**. • *dynupdate.no-ip.com* pour le servie **No-IP**.
Service DNS dynamique (obligatoire)	Cette option vous permet d'indiquer le service que vous avez souscrit auprès de votre fournisseur de services DNS : Dynamique", "Statique" ou "Personnalisé".

Configuration avancée

Des paramétrages de configuration avancée sont disponibles en cliquant sur le bouton **Configuration avancée**. Ils permettent notamment de renouveler l'enregistrement du changement d'adresse.

Fréquence de renouvellement (en jours)	Période de renouvellement du service DNS dynamique. Cette période est fixée à 28 jours par défaut par Stormshield Network. **REMARQUE** Ces fournisseurs punissent les renouvellements abusifs (fermeture du compte…). Ainsi un renouvellement survenu avant 26 jours (après le dernier renouvellement) n'est pas permis. De plus sans renouvellement au-delà de 35 jours, le compte est clôturé. Ces informations sont toutefois susceptibles d'être modifiées étant donné qu'il s'agit d'un fonctionnement établi par ces fournisseurs.
Protocole utilisé pour la mise à jour	Protocole utilisé lors de la phase de renouvellement du service DNS dynamique. Les choix possible sont : HTTPS (proposé par défaut) ou HTTP.
Avertir le fournisseur d'accès	Ce service payant chez **DynDns** permet de rediriger les flux à destination de votre réseau vers une page spécifique lorsque votre connexion n'est pas en activité.
Supporter la translation d'adresses (NAT)	Cette option permet au firewall d'utiliser les services de DNS dynamique lorsqu'il se situe derrière un équipement réalisant de la translation d'adresses.

DROITS D'ACCÈS

Ce module se compose de 3 onglets :

- **Accès par défaut** : permet de définir les accès VPN SSL Portail, VPN IPsec, VPN SSL ainsi que la politique de parrainage par défaut.
- **Accès détaillé** : grille de règles correspondant aux accès VPN SSL Portail, VPN IPsec, VPN SSL et aux utilisateurs autorisés à valider les requêtes de parrainage.
- **Serveur PPTP** : permet d'ajouter et de lister les utilisateurs ayant accès au VPN PPTP par leur login et de leur créer un mot de passe pour se connecter.

Onglet Accès par défaut

Accès VPN

Profil VPN SSL Portail	Les profils VPN SSL Portail représentent l'ensemble de serveurs web et applicatifs que vous souhaitez lister afin de les attribuer à vos utilisateurs ou groupes d'utilisateurs. Ce champ permet de définir le profil VPN SSL par défaut pour les utilisateurs. Vous devez avoir restreint au préalable l'accès aux serveurs définis dans la configuration du VPN SSL Portail dans le module **VPN > VPN Portail**, onglet **Profils utilisateurs**. La liste déroulante laisse apparaître les options suivantes : • Interdire : les utilisateurs n'ont pas accès au VPN SSL Portail. • Autoriser : l'utilisateur a accès à tous les profils VPN SSL Portail créés au préalable • <Nom du profil utilisateur1> : l'utilisateur aura uniquement accès à ce profil. • <Nom du profil utilisateur2> : l'utilisateur aura uniquement accès à ce profil.
Politique IPsec	Le **VPN IPsec** permet d'établir un tunnel sécurisé (authentification du correspondant, chiffrement et / ou vérification de l'intégrité des données) entre deux machines, entre une machine et un réseau, ou entre deux réseaux. Ce champ permet d'**Interdire** ou d'**Autoriser** par défaut des utilisateurs à négocier des tunnels VPN IPsec. Selon votre choix, les utilisateurs et les groupes d'utilisateurs pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données.
Politique VPN SSL	Le VPN SSL permet d'établir un tunnel sécurisé (authentification du correspondant, chiffrement et / ou vérification de l'intégrité des données) entre deux machines, entre une machine et un réseau, ou entre deux réseaux. Ce champ permet d'Interdire ou d'Autoriser par défaut des utilisateurs à négocier des tunnels VPN SSL, en cas d'absence de règles spécifiques. Selon votre choix, les utilisateurs et les groupes d'utilisateurs pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données.

Parrainage

Le parrainage permet à un utilisateur externe présent dans l'entreprise de soumettre depuis le portail captif une demande d'accès à Internet pour une durée déterminée.

Politique de parrainage	Le parrainage permet à un utilisateur externe présent dans l'entreprise de soumettre depuis le portail captif une demande d'accès à Internet pour une durée déterminée. Ce champ permet d'Interdire ou d'Autoriser par défaut les utilisateurs à répondre à des requêtes de parrainage établies depuis le portail captif.

Onglet Accès détaillé

Les actions possibles

Certaines actions peuvent également être réalisées en effectuant un clic droit dans la grille.

Rechercher	Permet d'effectuer une recherche par mots ou lettres clés.
Ajouter	Ajoute une nouvelle règle d'accès détaillé. La procédure est expliquée dans la section Ajouter.
Supprimer	Supprime la règle d'accès détaillé sélectionnée.
Monter	Place la règle sélectionnée au-dessus de la précédente dans la liste.
Descendre	Place la règle sélectionnée au-dessous de la suivante dans la liste.

Ajouter

Après avoir cliqué sur le bouton **Ajouter**, définissez l'utilisateur ou le groupe d'utilisateurs pour lequel vous souhaitez créer la règle d'accès détaillé.

Utilisateur - Groupe présent dans l'annuaire LDAP	Permet d'ajouter la règle à un utilisateur ou un groupe d'utilisateurs présent dans l'annuaire LDAP du firewall. Sélectionnez dans la liste déroulante l'utilisateur ou le groupe d'utilisateurs concerné.
Utilisateur - Groupe provenant d'un autre domaine (annuaire)	Permet d'ajouter la règle à un utilisateur ou un groupe d'utilisateurs provenant d'un autre domaine. Pour ce choix, complétez les informations : • **Utilisateur / Groupe** : définissez si la règle concerne un **Utilisateur** ou un **Groupe**. • **Utilisateur - Nom du groupe** : tapez le nom de l'utilisateur ou du groupe concerné. • **Nom de domaine** : tapez le nom de domaine concerné.

Une fois la règle ajoutée, elle apparaît dans la grille et l'utilisateur ou le groupe d'utilisateur concerné est visible dans la colonne **Utilisateur – groupe d'utilisateurs**. Par défaut, une règle ajoutée est désactivée et tous les accès sont définis sur **Interdire** (même si vous les avez configurés différemment dans l'onglet **Accès par défaut**).

La grille Accès détaillé

État	Affiche l'état de la configuration de la règle d'accès détaillé de l'utilisateur ou du groupe d'utilisateurs. Double-cliquez pour modifier l'état. **NOTE** Le firewall évalue les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut vers le bas. Si la règle 1 concerne un groupe d'utilisateur, chaque utilisateur attaché aux règles suivantes et faisant partie de ce même groupe sera soumis à la configuration de la règle 1.
Utilisateur – groupe d'utilisateurs	Affiche l'utilisateur ou le groupe d'utilisateurs concerné par la règle.
VPN SSL Portail	Permet d'attribuer à un utilisateur ou à un groupe d'utilisateurs un profil VPN SSL préalablement configuré dans le module **VPN > VPN SSL Portail**, onglet **Profils utilisateurs**. Si vous choisissez **Interdire**, l'utilisateur ou groupe d'utilisateur n'a accès à aucun profil VPN SSL, à l'inverse de l'option **Autoriser** qui ouvre l'accès à tous les serveurs web et applicatifs activés au sein des profils utilisateurs. L'option **Défaut** prend en compte le profil VPN SSL Portail par défaut saisi dans l'onglet **Accès par défaut**.
IPsec	Permet d'**Interdire** ou d'**Autoriser** des utilisateurs à négocier des tunnels VPN IPsec. L'option **Défaut** prend en compte la politique IPsec par défaut saisi dans l'onglet **Accès par défaut**. Selon votre choix, les utilisateurs et les groupes d'utilisateurs pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données. **NOTE** Le droit IPsec ne concerne que les tunnels : • Avec authentification par clé pré-partagée et des identifiants de type e-mail, ou • Avec authentification par certificat.
VPN SSL	Permet d'**Interdire** ou d'**Autoriser** des utilisateurs à négocier des tunnels VPN SSL.. L'option **Défaut** prend en compte la politique VPN SSL par défaut saisi dans l'onglet **Accès par défaut**. Selon votre choix, les utilisateurs et les groupes d'utilisateurs précisés pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données.
Parrainage	Selon votre choix, les utilisateurs ou groupes d'utilisateurs seront autorisés ou non à valider les requêtes de parrainage reçues depuis le portail captif. L'option **Défaut** prend en compte la politique de parrainage par défaut saisi dans l'onglet **Accès par défaut**.
Description	Commentaire éventuel décrivant l'utilisateur, le groupe d'utilisateurs ou la règle.

Onglet Serveur PPTP

Il permet de lister les utilisateurs ayant accès au **VPN PPTP**, leur donnant accès à une connexion sécurisée et chiffrée pour leur login.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des comptes PPTP :

- Ajouter,
- Supprimer,
- Modifier le mot de passe.

Vous pouvez effectuer les actions suivantes :

Ajouter	Lorsque vous cliquez sur ce bouton, une nouvelle ligne vient s'ajouter au tableau et vous présente la liste déroulante des utilisateurs créés au préalable au sein du menu **Utilisateurs > module Utilisateurs** : Pour que l'opération soit valide, vous devez entrer le mot de passe de l'utilisateur dans la fenêtre qui s'affiche. **NOTE** Il est possible de saisir un utilisateur ne figurant pas dans la base des utilisateurs du firewall, le PPTP étant indépendant du module LDAP.
Supprimer	Sélectionner la ligne contenant l'utilisateur à retirer de la liste des login PPTP, puis cliquer sur **Supprimer**.
Modifier le mot de passe	Sélectionner la ligne contenant l'utilisateur dont vous souhaitez modifier le mot de passe et entrez les nouvelles données dans la fenêtre qui s'affiche.

NOTE
Il est possible de saisir un login uniquement composé de majuscules.

ENREGISTREMENT DES COMMANDES DE CONFIGURATION

Lorsqu'il a été activé dans les préférences, le bouton d'enregistrement des commandes de configuration est affiché dans la partie droite du panneau supérieur de l'interface Web d'administration. Il permet d'enregistrer l'ensemble de commandes envoyées au firewalls lors d'une séquence de configuration afin de pouvoir les réutiliser au sein d'un script par exemple. Cette séquence peut couvrir plusieurs modules de configuration.

Ce bouton peut prendre les deux formes suivantes :

-

: pas d'enregistrement en cours.
- : un enregistrement est en cours.

Enregistrer une séquence de commandes de configuration

1. Cliquez sur le bouton

pour démarrer l'enregistrement,
2. Effectuez toutes les actions de configuration faisant l'objet de l'enregistrement,
3. Arrêtez l'enregistrement en cliquant sur le bouton ,

La fenêtre **Commandes de configuration enregistrées** est affichée. Elle contient la liste de toutes les commandes appliquées séquentiellement au firewall. Cette liste est modifiable.

4. Choisissez l'action à appliquer à la liste de commandes :

- **Copier au presse-papier** : l'ensemble des commandes est mémorisé dans le presse papier du poste de travail afin de pouvoir être collées dans un éditeur de texte,
- **Effacer** : l'ensemble des commandes est effacé sans être mémorisé,
- **Fermer** : ferme la fenêtre **Commandes de configuration enregistrées**.

ENRÔLEMENT

Le service d'enrôlement Web permet à un utilisateur "inconnu" de la base des utilisateurs de demander la création de son compte d'accès (à Internet, au serveur de messagerie, à tous les services qui nécessitent une authentification) et de son certificat.

Ce module requiert au minimum l'utilisation d'un annuaire LDAP pour les requêtes utilisateurs et d'une autorité racine (PKI interne) pour les demandes de certificats utilisateur.

NOTE
Pour que des utilisateurs puissent effectuer des demandes d'enrôlement, le portail captif doit être configuré et l'enrôlement Web des utilisateurs doit y être autorisé. L'activation de l'enrôlement s'effectue depuis le module **Configuration > Utilisateurs > Authentification**, onglet Profils du portail captif.

L'écran se compose de 3 zones :

- Une grille contenant les demandes d'enrôlement des utilisateurs et de certificats,
- Une zone contenant les informations de la demande d'enrôlement sélectionnée,
- Une zone **Configuration avancée**.

La grille

Les actions possibles

Rechercher	Recherche parmi les demandes d'enrôlement reçues.
Actualiser	Actualise la liste des demandes d'enrôlement reçues.
Tout sélectionner	Sélectionne toutes les demandes d'enrôlement reçues.
Approuver	Approuve une demande d'enrôlement utilisateur ou de certificat. Sélectionnez au préalable la ou les lignes des demandes concernées pour les approuver. Lorsque vous validez une demande d'enrôlement utilisateur avec une requête de certificat, vous devez entrer le mot de passe de l'autorité de certification (CA) afin de valider les deux demandes en une seule manipulation.
Rejeter	Rejette une demande d'enrôlement utilisateur ou de certificat. Sélectionnez au préalable la ou les lignes des demandes concernées pour les rejeter. Lorsque vous rejetez une demande d'enrôlement utilisateur avec une requête de certificat, les deux demandes sont rejetées en même temps.

Les demandes d'enrôlement reçues

Type	Type de demande d'enrôlement reçue : **Utilisateur** ou **Certificat**.
Nom	Nom permettant d'identifier l'utilisateur ou le certificat parmi les demandes reçues.

Informations de la demande d'enrôlement sélectionnée

Cette zone affiche les informations de la demande d'enrôlement utilisateur ou de certificat sélectionnée. Pour les demandes de **Certificat**, seul le champ **Adresse e-mail** apparaît.

Identifiant	Identifiant de connexion qui sera créé si l'utilisateur est validé. Vous pouvez modifier le format servant à générer les identifiants dans la zone **Configuration avancée**.
Nom	Nom de l'utilisateur.
Prénom	Prénom de l'utilisateur.
Adresse e-mail	Adresse e-mail de l'utilisateur. Si l'envoi d'un e-mail d'approbation ou de rejet de la demande d'enrôlement est configuré, il est envoyé à cette adresse. La configuration de cet envoi s'effectue dans la zone **Configuration avancée**.
Description	Description de l'utilisateur. Ce champ peut être vide si l'utilisateur ne l'a pas complété lors de sa demande d'enrôlement.
Numéro de téléphone	Coordonnées téléphoniques de l'utilisateur. Ce champ peut être vide si l'utilisateur ne l'a pas complété lors de sa demande d'enrôlement.
Mot de passe	Précise que l'utilisateur a complété son mot de passe lors de sa demande et que ce dernier respecte la politique de mots de passe définie sur le firewall.
Requête de certificat	Précise si une demande de création de certificat a été faite en même temps que la demande d'enrôlement utilisateur.

Configuration avancée

Format de l'identifiant utilisateur

Format de l'identifiant	Définissez le format utilisé pour générer les identifiants de connexion lorsqu'une demande d'enrôlement utilisateur est reçue : • Le format s'écrit sous la forme : `%F.%L`. • La variable **%F** correspond au prénom et la variable **%L** au nom. • Les variables **%f** et **%l** transforment la casse des variables en minuscules. • Les variables peuvent contenir un chiffre afin de définir une limite de caractères. **EXEMPLES** **%F.%L** donne **FIRSTNAME.LASTNAME** **%f1.%l** donne **f.lastname**

Envoyer un e-mail à l'utilisateur

lors de l'approbation / rejet de sa requête d'enrôlement	Cette option permet l'envoi d'un e-mail à l'utilisateur pour l'informer de la validation ou du rejet de sa demande d'enrôlement utilisateur.
lors de l'approbation / rejet de sa requête de certificat	Cette option permet l'envoi d'un e-mail à l'utilisateur pour l'informer de la validation ou du rejet de sa demande de création de certificat.

ÉVÉNEMENTS SYSTÈME

Ce module vous permet de définir le niveau d'alerte des événements système divers pouvant apparaître au sein de vos configurations (attaques, échecs de mises à jour, CRL invalide etc.).

Il est composé d'un unique écran, listant les événements par numéro et par ordre alphabétique, avec la possibilité de rechercher un événement particulier.

Les actions possibles

Vous pouvez dans un premier temps, effectuer deux actions.

Rechercher

Cette zone de saisie permet la recherche par occurrence, lettre ou mot. Vous pouvez ainsi filtrer les éléments de la liste afin de n'afficher que ceux que vous souhaitez.

Exemple

Si vous saisissez « CRL » dans le champ, tous les messages comportant ce terme s'afficheront dans la grille.

Restaurer la configuration par défaut

Ce bouton va permettre d'annuler tous les changements que vous avez effectués au préalable au sein de la configuration des événements systèmes.

Lorsque vous cliquez sur ce bouton, un message de confirmation s'affiche, permettant de valider ou non l'action.

La liste des événements

L'écran est composé de trois colonnes, ainsi que d'une page d'aide disponible en bout de ligne pour chaque type d'événement.

Identifiant	Ce champ affiche le numéro permettant d'identifier l'événement. Il n'est pas éditable.
Niveau	Cette colonne affiche les niveaux d'alertes attribués aux événements par défaut. Il en existe 4, que vous pouvez modifier en sélectionnant le niveau désiré au sein de la liste déroulante, accessible en cliquant sur la flèche de droite : • **Ignorer** : aucune trace de l'événement ne sera conservée au sein des logs. • **Mineur** : dès que l'événement concerné est détecté, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie Traces - Syslog) ou par e-mail (voir module Alertes e-mails). • **Majeur** : dès que l'événement concerné est détecté, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie Traces - Syslog) ou par e-mail (voir module Alertes e-mails). • **Tracer** : le firewall Stormshield Network n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière.

Message (langue dépendante du firewall)	Ce champ affiche le nom de l'événement système et ses caractéristiques et n'est pas éditable. **NOTE** En cliquant sur la flèche de droite en tête de la colonne, vous pouvez inverser l'ordre d'apparition des événements.
Afficher l'aide	Lorsque vous sélectionnez un événement au sein de la liste en positionnant votre curseur dessus, un lien « Afficher l'aide » apparaît. En cliquant sur celui-ci, vous serez renvoyé sur la base de connaissances Stormshield Network, donnant plus de détails sur les informations relatives à l'événement.
Configurer	**Envoyer un e-mail** : un e-mail sera envoyé au déclenchement de l'alarme (cf. module **Alertes e-mails**) avec les conditions suivantes : • **Nombre d'alarme avant l'envoi :** nombre minimal d'alarmes requises avant le déclenchement de l'envoi, pendant la période fixée ci-après. • **Pendant la période de (secondes) :** délai en secondes pendant lequel les alarmes sont émises, avant l'envoi de l'E-mail. **Mettre la machine en quarantaine :** la machine responsable de l'alarme sera temporairement bloquée avec les paramètres suivants : • **Pour une période de (minutes)** : durée de la mise en quarantaine.

NOTE
Lorsque vous modifiez le niveau d'alerte d'un événement, n'oubliez pas de cliquer sur le bouton **Appliquer** en bas de la page, afin de valider votre action.

FILTRAGE ET NAT

Le **Filtrage** et le **NAT** sont réunis en un seul module et font partie du menu **Politique de Sécurité**.

Evaluation du filtrage et impact du NAT

La politique de filtrage est évaluée sur les adresses IP avant modification par le NAT, c'est-à-dire les adresses IP du paquet réseau avant qu'il n'atteigne le firewall. Par exemple, pour autoriser l'accès à un serveur interne depuis un réseau public (Internet par exemple), il faut choisir l'adresse IP publique de ce serveur (ou l'adresse publique du firewall par exemple) dans le champ *Destination* de la règle de filtrage.

Les règles dont l'action est « passer » avec le service HTTP explicite activé, « décrypter » ou « tracer » n'annulent pas l'exécution des règles suivantes. L'évaluation des règles continue. Il est donc possible d'ajouter des règles de filtrage après ce type de règle.

Ce module se compose de 2 onglets, comportant chacun un emplacement réservé aux politiques de filtrage et de NAT, et à leur configuration respective :

- Le **Filtrage** : Il s'agit d'un ensemble de règles qui laissent passer ou bloquent certains trafics réseaux suivant des critères définis.
- Le **NAT** : Il permet de faire de la réécriture (ou translation) d'adresses et de ports source et destination.

Mode « FastPath »

Pour les règles avec une inspection en mode « Firewall », le trafic a été optimisé et les débits multipliés par un mécanisme appelé *FastPath*. Ces règles en mode « Firewall » sont conseillées pour les besoins d'un simple contrôle d'accès, par exemple, pour des flux internes spécifiques. Cela peut être des flux dédiés à la sauvegarde ou à la réplication de données en Datacenter, ou encore réservé à l'accès de sites VPN satellites à un Firewall principal si celui-ci analyse déjà le trafic.

Ce mécanisme permet alors d'alléger une charge importante de traitement du moteur de prévention d'intrusion, en inscrivant ces connexions éligibles au *FastPath,* c'est-à-dire dispensées après contrôle, de passage dans le moteur IPS. Ce mécanisme d'optimisation est automatique pour les règles en mode Firewall appliquées aux flux IPv4, ne réalisant pas de translation (NAT) et sans analyse de protocole utilisant des connexions dynamiques (FTP, SIP, etc). De plus, les règles ne doivent pas avoir les options ou valeurs suivantes :

- La Qualité de service (QoS),
- Un Seuil de connexion : TCP avec ou sans la protection des attaques synflood (synproxy), UDP, ICMP et requêtes applicatives
- DSCP réécrit (valeur DSCP définie),
- Règle avec port de destination non précisé et non conforme au protocole indiqué (onprobe).

Ce mécanisme est compatible avec les options de routage par règle (PBR) et de Load Balancing, Pour assurer une vision complète et cohérente des flux, le suivi des connexions examine la table pour notamment la génération de traces.

Les politiques

Le bandeau vous permet de sélectionner et de manipuler les politiques associés au **Filtrage** d'une part, et au **NAT** d'autre part.

Sélection de la politique de filtrage

Le menu déroulant propose 10 politiques de filtrage pré-configurées numérotées de 1 à 10, de la plus stricte à la plus permissive :

« Block all (1) »	Par défaut, cette politique de filtrage est activée en configuration d'usine. Seuls les ports correspondant à l'administration du firewall sont ouverts (1300/TCP et 443/TCP). Le test d'accessibilité PING à destination de toutes les interfaces du firewall est également autorisé. Toutes les autres connexions sont ensuite bloquées. **NOTE** En sélectionnant cette politique, vous n'aurez accès à l'interface d'administration du firewall uniquement depuis les réseaux internes (interfaces protégées) ; cette restriction dépend de la liste des postes autorisés à administrer le firewall, définie dans le menu **Système**, module **Configuration** (onglet *Administration du Firewall*).
« High (2) »	Si vous choisissez cette politique de filtrage, seuls les trafics web, e-mail, FTP, et les requêtes de type PING (echo request) seront autorisés depuis les réseaux internes.
« Medium (3) »	En choisissant cette politique, la prévention d'intrusion sera effectuée sur les connexions sortantes, dans la mesure où le protocole peut être détecté automatiquement par le moteur de prévention des menaces : Par exemple, le port 80 est généralement utilisé pour faire du HTTP. Tout trafic sur le port 80 sera considéré comme du trafic HTTP par le firewall, car ce port est défini comme port par défaut pour le protocole HTTP (les ports par défaut pour chaque protocole sont définis depuis le menu **Protection applicative** \ **Protocoles**). En revanche, si un autre protocole est utilisé (par exemple un tunnel SSH) à destination du port 80, la connexion sera alors déclarée illégitime et bloquée, car le seul protocole autorisé est l'HTTP. **NOTE** Toutes les connexions sortantes TCP non-analysables (pour lesquelles aucune reconnaissance du protocole n'est possible) seront acceptées.
« Low (4) »	Une analyse des protocoles sera forcée pour les connexions sortantes. **NOTE** Toutes les connexions sortantes non-analysables seront autorisées.
« Filter 05, 06, 07, 08, 09 »	Hormis les 5 politiques configurées par défaut (**Block all, High, Medium, Low, Pass all,** éditables si vous le souhaitez), 5 politiques vides à paramétrer vous-même sont disponibles.
« Pass all (10) »	Cette politique laisse passer l'ensemble du trafic, c'est-à-dire que les connexions sur l'ensemble des protocoles et ports sont autorisées. Les analyses applicatives seront toutefois appliquées. Cette politique ne devrait être utilisée qu'à des fins de test.

NOTE
Vous pouvez **Renommer** ces politiques et modifier leur configuration dès que vous le souhaitez (voir ci-dessous).

Les actions

Activer cette politique	Active immédiatement la politique en cours d'édition: Les paramètres enregistrés écrasent les paramètres en vigueur et la politique est appliquée immédiatement sur le firewall. **IMPORTANT** Les règles de Filtrage et de NAT appartenant à la même politique, elles seront activées simultanément.
Éditer	Cette fonction permet d'effectuer 3 actions sur les politiques : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom de la politique de filtrage d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mettre à jour ». Il est également possible d' « Annuler » la manipulation. • **Réinitialiser** : Permet de rendre à la politique sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier une politique vers une autre, toutes les informations de la politique copiée seront transmises à la politique réceptrice. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure de la dernière modification enregistrée. L'heure affichée est celle du boîtier et non celle du poste client.

La sélection multiple

La sélection multiple permet d'assigner une même action à plusieurs règles. Sélectionnez plusieurs règles se succédant à l'aide de touche **Shift** ⇧ ou individuellement avec la touche **Ctrl.** Vous pourrez également soustraire une sélection à une sélection existante, avec la touche **Ctrl.**

Certains intitulés de colonnes affichent l'icône . Par un simple clic, un menu s'affiche et propose d'assigner un même paramètre à plusieurs règles sélectionnées (*Etat, Action* et *Type d'inspection* pour le filtrage).

EXEMPLE
Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche **Ctrl** puis en cliquant sur **Supprimer**.

Le glisser-déposer (« drag'n'drop »)

Tout au long de votre création et édition de règle, il sera possible de glisser-déposer des objets, des actions et également des règles de filtrage et NAT.

Vous pourrez déplacer n'importe quel objet où vous le souhaitez dans la grille, ainsi qu'en insérer depuis votre barre de navigation à gauche (champ **Objets**), s'ils ont été préalablement créés (vous pouvez également les créer directement depuis chaque champ qui accepte un objet).

Cette fonctionnalité s'applique au champ de recherche.

NOTE
Deux icônes vous permettront de savoir si l'objet ou l'action sélectionnée peut être déplacé au

sein d'une cellule particulière :

- Indique que l'opération est possible,
- Indique que l'objet ne peut être ajouté à la cellule choisie.

L'onglet Filtrage

La technologie de prévention d'intrusion Stormshield Network inclut un moteur de filtrage dynamique des paquets (« stateful inspection ») avec optimisation du traitement des règles permettant une application de la politique de filtrage de manière sûre et rapide.

La mise en œuvre des fonctions de filtrage est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle de la politique de filtrage actif. Le filtrage porte sur tous les paquets sans exception.

En ce qui concerne l'utilisateur ou le groupe d'utilisateurs autorisés par la règle, à partir du moment où un utilisateur s'est identifié et authentifié avec succès à partir d'une machine donnée, le firewall retient ce fait et attribue le nom de l'identifiant de cet utilisateur à tous les paquets IP en provenance de l'adresse de cette machine.

En conséquence, les règles qui spécifient l'authentification des utilisateurs, même sans préciser de contraintes sur les utilisateurs autorisés, ne peuvent s'appliquer qu'à des paquets IP émis d'une machine à partir de laquelle un utilisateur s'est préalablement authentifié. Chaque règle de filtrage peut spécifier une action de contrôle (voir colonne **Action**).

Le **Filtrage** est composé de deux parties. Le bandeau situé en haut de l'écran, permettant de choisir la politique de filtrage, de l'activer, de l'éditer et de visualiser sa dernière modification. La grille de filtrage est dédiée à la création et la configuration des règles.

Vérification en temps réel de la politique

La politique de filtrage d'un firewall est un des éléments les plus importants pour la protection de vos données ou de vos ressources internes. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit conserver une cohérence parfaite afin que des failles n'apparaissent pas dans la protection que propose le firewall.

L'enjeu est d'éviter la création de règles qui en inhiberaient d'autres. Lorsque la politique de filtrage est conséquente, le travail de l'administrateur est d'autant plus fastidieux que ce risque s'accroît. De plus, lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter cela, l'écran d'édition des règles de filtrage des firewalls dispose d'un champ de « **Vérification de la politique** » (situé en dessous de la grille de filtrage), qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles créées.

EXEMPLE

[Règle 2] Cette règle ne sera jamais appliquée car elle est couverte par la règle 1.

Les actions sur les règles de la politique de filtrage

Rechercher	Ce champ permet la recherche par occurrence, lettre ou mot. **EXEMPLE** Si vous saisissez « Network_internals » dans le champ, toutes les règles de filtrage comportant « Network_internals » s'afficheront dans la grille.

Nouvelle règle	Insère une ligne prédéfinie ou à définir après la ligne sélectionnée. 5 choix sont possibles, les règles d'authentification, d'inspection SSL et de proxy HTTP explicite seront définies via un assistant dans une fenêtre à part :

- **Règle simple**: Cette option permet de créer une règle vide laissant à l'administrateur la possibilité de remplir les différents champs de la grille de filtrage.
- **Séparateur – regroupement de règles** : Cette option permet d'insérer un séparateur au-dessus de la ligne sélectionnée.
  Ce séparateur permet de regrouper des règles qui régissent le trafic vers les différents serveurs et contribue à améliorer la lisibilité et la visibilité de la politique de filtrage en y indiquant un commentaire.
  Les séparateurs indiquent le nombre de règles regroupées et les numéros de la première et dernière de ces règles. sous la forme : « *Nom de la règle* (contient *nombre total* règles, de n° *première* à n° *dernière*) ».
  Vous pouvez plier et déplier le nœud du séparateur afin de masquer ou afficher le regroupement de règle. Vous pouvez également copier / coller un séparateur d'un emplacement à un autre.
- **Règle d'authentification** : Cette option a pour but de rediriger les utilisateurs non authentifiés vers le portail captif. En la sélectionnant, un assistant d'authentification s'affiche.
  Vous devrez choisir la **Source** (affichant « Network_internals » par défaut) et la **Destination** (affichant « Internet » par défaut) de votre trafic parmi la liste déroulante d'objets, puis cliquer sur **Terminer.** Le choix du port n'est pas proposé, le port HTTP est choisi automatiquement.
  Vous pouvez spécifier en **Destination**, des catégories ou groupes d'URL dérogeant à la règle, donc accessibles sans authentification (l'objet web *authentication_bypass* contient par défaut les sites de mise à jour Microsoft). L'accès à ces sites sans authentification peut donc bénéficier comme les autres règles des inspections de sécurité du Firewall.
- **Règle d'inspection SSL** : Cet assistant a pour but de créer des règles inspectant le trafic chiffré SSL. Il est fortement conseillé de passer par cet assistant pour la génération des deux règles indispensables au bon fonctionnement du proxy SSL.
  Vous devrez définir la **Politique du trafic à déchiffrer** en indiquant les **Machines sources** (« Network_internals » par défaut), l'**Interface d'entrée** (« any » par défaut), la **Destination** (« Internet » par défaut) et le **Port de destination** (« ssl_srv » par défaut) parmi la liste déroulante d'objets.
  Afin **d'Inspecter le trafic déchiffré** via la seconde zone de la fenêtre de l'assistant, vous pourrez définir la configuration du **Profil d'Inspection**, en choisissant l'une de celles que vous avez définies au préalable ou laisser en mode « Auto ». Ce mode automatique appliquera l'inspection relative à l'origine du trafic (cf **Protection Applicative/ Profils d'inspection**).
  Vous pouvez également activer **l'Antivirus** ou **l'Antispam** et sélectionner des **politiques de filtrage URL, SMTP, FTP ou SSL** (vérification du champ CN du certificat présenté).
- **Règle de proxy HTTP explicite** : Cette option permet d'activer le proxy HTTP explicite et de définir qui peut y accéder. Vous devrez choisir un objet **Machines** et une **Interface d'entrée** via le champ « **Source** ». Définissez ensuite **l'Inspection du trafic relayé** en indiquant si vous souhaitez activer **l'Antivirus** et sélectionner des **politiques de filtrage URL.**

> **NOTE**
> Afin de permettre une politique similaire sur un firewall hébergé dans le Cloud et un firewall physique, le port d'écoute d'un proxy explicite HTTP peut être configuré sur un port différent du port par défaut (8080/TCP).
> Cliquez ensuite sur **Terminer**.

Supprimer	Supprime la ligne sélectionnée.
Monter	Placer la ligne sélectionnée avant la ligne directement au-dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Tout dérouler	Étendre l'arborescence des règles.
Tout fermer	Regrouper l'arborescence des règles.
Couper	Couper une règle de filtrage dans le but de la coller.
Copier	Copier une règle de filtrage dans le but de la dupliquer.
Coller	Dupliquer une règle de filtrage, après l'avoir copié.
Chercher dans les logs	Lorsqu'une règle de filtrage est sélectionnée, cliquez sur ce bouton pour lancer automatiquement une recherche portant sur le nom de la règle dans la vue "Tous les journaux" (module **Logs** > **Journaux d'audit** > **Vues**). Si aucun nom n'a été spécifié pour la règle sélectionnée, un message d'avertissement précise que la recherche est impossible.
Chercher dans la supervision	Lorsqu'une règle de filtrage est sélectionnée, cliquez sur ce bouton pour lancer automatiquement une recherche portant sur le nom de la règle dans le module de supervision des connexions.

Avancé	**Réinitialiser les statistiques des règles**	En cliquant sur ce bouton, vous réinitialisez les compteurs numériques et graphiques d'utilisation des règles de filtrage situés dans la première colonne de la grille.
	Réinitialiser l'affichage des colonnes	Lorsque vous cliquez sur la flèche de droite dans le champ du nom d'une colonne (exemple : **État**), vous avez la possibilité d'afficher des colonnes supplémentaires ou d'en retirer afin qu'elles ne soient pas visibles à l'écran, grâce à un système de coche.

EXEMPLE
Vous pouvez cocher les cases « **Nom** » et « **Port src** » qui ne sont pas affichées par défaut.
En cliquant sur le bouton **réinit. colonnes**, vos colonnes seront remises à leur état initial, avant que vous n'ayez coché de case additionnelle. Ainsi, les cases **Nom** et **Port src** seront de nouveau masquées.

NOTE
Si vous cliquez rapidement 10 fois sur le bouton "Monter", vous distinguez la règle monter visuellement mais la fenêtre d'attente n'apparaît que lorsqu'on ne touche plus au bouton au-delà de 2 ou 3 secondes. Et au final, une seule commande sera passée. Ceci rend le déplacement des règles beaucoup plus fluide.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles de filtrage :

- Nouvelle règle (Règle simple, Séparateur - Regroupement de règles, Règle d'authentification, Règle d'inspection SSL, Règle de proxy HTTP explicite),
- Supprimer,
- Couper,
- Copier,
- Coller,
- Chercher dans les logs,
- Chercher dans la supervision.

Comparaison mathématique

Chaque fois que vous rencontrerez une liste déroulante d'objets au sein des colonnes (exceptées « État » et « Action ») une icône d'opérateur de comparaison mathématique apparaîtra ( ). Elle ne sera utilisable que si un autre objet que « **Any** » est sélectionné.

Vous pourrez ainsi personnaliser les paramètres de votre trafic par le biais de l'icône suivante de 4 manières différentes :

- « = » (ou): la valeur de l'attribut correspond à ce qui est sélectionné.
- « != » (ou) la valeur de l'attribut est différente de ce qui est sélectionné.
- « < » (ou ; utilisable uniquement pour les ports source, ports destination et scores de réputation de machines) : la valeur de l'attribut est inférieure à ce qui est sélectionné.
- « > » (ou ; utilisable uniquement pour les ports source, ports destination et scores de réputation de machines) : la valeur de l'attribut est supérieure à ce qui est sélectionné.

Ajout / modification d'objet

Certaines listes déroulantes de sélection d'objets proposent le bouton qui permet d'accéder à un menu contextuel :

- **Créer un objet** : un nouvel objet peut directement etre créé depuis le module Filtrage/NAT
- **Modifier cet objet** : lorsqu'un objet est présent dans le champ, il peut directement être édité pour modification (changement de nom, d'adresse IP pour une machine, ajout dans un groupe...), à l'exception des objets en lecture seule ("**Any**", "**Internet**", ..).

La grille de filtrage

Elle vous permet de définir les règles de filtrage à appliquer.

Ordonnez-les afin d'avoir un résultat cohérent : le firewall exécute les règles dans l'ordre d'apparition à l'écran (numérotées 1, 2 etc) et s'arrête dès qu'il trouve une règle correspondant au paquet IP.

Il convient donc de définir les règles dans l'ordre du **plus restrictif au plus général**.

Réorganisation des règles

Dans toute politique de sécurité, chaque règle peut être glissée et déplacée pour réorganiser aisément la politique (filtrage ou NAT). Le symbole ainsi que l'infobulle "Glissez et déplacez pour réorganiser" apparaissent lorsque la souris survole le début de la règle.

Statistiques d'usage des règles

Dans la politique de sécurité active, chaque règle activée de filtrage et de NAT affiche également un compteur d'utilisation. Au survol de l'icône, une info-bulle indique le nombre exact d'exécution de la règle. Les 4 niveaux d'utilisations correspondent aux valeurs suivantes, selon le pourcentage du compteur de la règle la plus utilisée :

 0%

 de 0 à 2%

 de 2 à 20% (de 2 à 100% si le compteur est inférieur à 10 000)

 de 20 à 100 %, avec un min. de 10 000 fois (sinon niveau précédent)

Pour obtenir un nouvel indicateur, un bouton **Réinitialiser les statistiques des règles** recommence une nouvelle collecte. Ce compteur est réinitialisé, si :

- L'un des paramètres de la règle est modifié (sauf le commentaire),
- Une autre politique est activée,
- Le firewall est redémarré.

Si aucune icône n'est affichée, cela signifie que l'information est indisponible.

État

Cette colonne affiche l'état **On** / **Off** de la règle. Double-cliquez dessus pour changer l'état : en effectuant cette manipulation une fois, vous activez la règle de filtrage. Renouvelez l'opération pour la désactiver.

Onglet Général

Général

État	Sélectionnez l'état **On** ou **Off** pour respectivement activer ou désactiver la règle en cours d'édition.
Commentaire	Vous pouvez saisir un commentaire : celui-ci sera affiché en toute fin de règle lors de l'affichage de la politique de filtrage.

Configuration avancée

Nom de la règle	Vous pouvez affecter un nom à la règle de filtrage : ce nom est repris dans les logs est facilité l'identification de la règle de filtrage lors d'une recherche dans les logs ou vues (menu **Logs - journaux d'audit**).

Action

Cette zone désigne l'action appliquée sur le paquet remplissant les critères de sélection de la règle de filtrage. Pour définir les différents paramètres de l'action, double-cliquez dans la colonne, une fenêtre contenant les éléments suivants s'affiche :

Onglet Général

Général

Action	Il est possible d'effectuer 5 actions différentes : • **Passer** : Le firewall Stormshield Network laisse passer le paquet correspondant à cette règle de filtrage. Le paquet ne descend plus dans la liste de règles. • **Bloquer** : Le firewall Stormshield Network bloque silencieusement le paquet correspondant à cette règle de filtrage : le paquet est supprimé sans que l'émetteur ne s'en aperçoive. Le paquet ne descend plus dans la liste des règles. • **Déchiffrer** : Cette action permet de déchiffrer le trafic chiffré. Le flux déchiffré continue descend dans la liste des règles. Il sera de nouveau chiffré après l'analyse (si aucune règle ne le bloque). • **Reinit. TCP/UDP**: Cette option concerne surtout les trafics TCP et UDP : Dans le cas d'un trafic TCP, un paquet « TCP reset » sera envoyé à l'émetteur de celui-ci. Dans le cas d'un trafic UDP, une notification ICMP *Destination Unreachable* (*Port Unreachable*) sera envoyée à l'émetteur de celui-ci. En ce qui concerne les autres protocoles IP, le Firewall Stormshield Network bloque simplement le paquet correspondant à cette règle de filtrage. • Si vous vous trouvez en mode d'édition de la politique globale de filtrage, une 5ème possibilité apparaît: « **Déléguer** ». Cette option permet de ne plus confronter le trafic au reste de la politique globale, mais de le confronter directement à la politique locale. Si votre politique contenait des règles avec l'action **Tracer uniquement**, la mention **Tracer uniquement (déprécié)** est affichée lorsque vous éditez ces règles.
Niveau de trace	Par défaut, la valeur est fixée sur **standard (journal de connexions)**, donc aucune trace n'est enregistrée. Plusieurs niveaux de traces sont possibles : • **Standard (journal de connexions)** : Aucune trace n'est conservée dans les logs de filtrage si le paquet correspond à cette règle. En revanche les connexions terminées peuvent être tracées (log des connexions) selon la configuration du protocole associé à la règle, ce qui est le cas en configuration d'usine. Notez que cette option est indisponible si vous avez préalablement choisi l'action « Tracer » au sein du champ précédent. • **Avancé (journal de connexions et journal de filtrage)**: En plus des traces du mode Standard, les traces issues de tous les flux correspondant à cette règle sont enregistrées. Cette option est déconseillée sur une règle de filtrage de type "Deny All" (sauf en cas de débogage) car elle génère alors une quantité de logs très importante. • **Alarme mineure** : Dès que cette règle est appliquée à une connexion, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie **Traces - Syslog - IPFIX**) ou par e-mail (voir module **Alertes e-mails**). • **Alarme majeure** : Dès que cette règle est appliquée à une connexion, une alarme majeure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie **Traces - Syslog - IPFIX**) ou par e-mail (voir module **Alertes e-mails**). Pour désactiver entièrement les traces, il est nécessaire de décocher les cases **Disque**, **Serveur Syslog** et **Collecteur IPFIX** du champ **Destination des traces pour cette règle** (onglet **Configuration avancée** de la boite d'édition de la règle).

Programmation horaire	Sélectionnez ou créez un **Objet Temps**. Vous pourrez ainsi définir la **période**/le **jour de l'année**/le **jour de la semaine**/ l'**heure**/la **récurrence** de validité des règles. La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton

Routage

Passerelle - routeur	Cette option est utile pour spécifier un routeur particulier qui permettra de diriger le trafic correspondant à la règle vers le routeur défini. Le routeur sélectionné peut être un objet de type « machine » ou de type « routeur ». La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton

IMPORTANT
Si des routeurs sont spécifiés dans les règles de filtrage (Policy Based Routing), la disponibilité de ces routeurs est systématiquement testée par l'envoi de messages ICMP *echo request*. Lorsque le routeur détecté comme injoignable est un objet « machine », la passerelle par défaut, renseignée dans le module **Routage,** sera choisie automatiquement. S'il s'agit d'un objet « routeur », le comportement adopté dépendra de la valeur choisie pour le champ **Si aucune passerelle n'est disponible** dans la définition de cet objet (voir la section **Objets Réseau**).
Pour plus d'informations techniques, reportez-vous à la **Base de connaissances - version anglaise** du support technique (article "*How does the PBR hostcheck work ?*").

Cliquer sur **OK** pour valider votre configuration.

Onglet Qualité de service

Le module de **QoS**, intégré au moteur de prévention d'intrusion Stormshield Network est associé au module **Filtrage** pour offrir les fonctionnalités de Qualité de Service.

Dès sa réception ; le paquet est traité par une règle de filtrage puis le moteur de prévention d'intrusion l'affecte à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage.

QoS

File d'attente	Ce champ vous propose de choisir parmi les files d'attente que vous avez définies au préalable au sein du module **Politique de Sécurité** > **Qualité de service**. Cette action n'est pas disponible (grisée) pour les flux transitant par le proxy SSL (menu **Source** > **Configuration avancée** > champ **Via**).
File d'attente d'acquittement (ACK)	Ce champ vous propose de choisir parmi les files d'attente pour les flux TCP de type ACK que vous avez définies au préalable au sein du module **Politique de Sécurité > Qualité de service.** Cette action n'est pas disponible (grisée) pour les flux transitant par le proxy SSL (menu **Source** > **Configuration avancée** > champ **Via**).

Répartition	• **Pas de répartition** : Si vous choisissez cette option, aucune attribution particulière de bande passante ne sera effectuée et chaque utilisateur / machine / connexion l'utilisera en fonction de ses besoins. • **Équité entre les utilisateurs** : la bande passante sera répartie équitablement entre les différents utilisateurs. • **Équité entre les machines** : la bande passante sera répartie équitablement entre les différentes machines. • **Équité entre les connexions** : la bande passante sera répartie équitablement entre les différentes connexions.

Seuil de connexion

Le firewall Stormshield Network peut limiter le nombre maximal de connexions acceptées par seconde pour une règle de filtrage. On peut définir le nombre désiré, pour les protocoles correspondants à la règle (TCP, UDP, ICMP et quelques requêtes applicatives). Cette option vous permet notamment d'éviter le déni de service que pourrait tenter d'éventuels pirates : vous pouvez ainsi limiter le nombre de requêtes par seconde adressées à vos serveurs.

Les paquets reçus une fois cette limite dépassée, seront bloqués et ignorés.

AVERTISSEMENT
La limitation ne s'appliquera qu'à la règle correspondante.

EXEMPLE
Si vous créez une règle FTP, seule la limitation TCP sera prise en compte.

REMARQUE
Si l'option est affectée à une règle contenant un groupe d'objets, la limitation s'applique au groupe dans son ensemble (nombre total de connexions).

Si le seuil est atteint	• **Ne rien faire** : aucune limitation de connexions ou requêtes par seconde (c/s) ne sera établie. • **Protéger des attaques SYN flood**: Cette option permet de protéger les serveurs contre les attaques par saturation de paquets TCP SYN (« SYN flooding ») le proxy SYN répondra à la place du serveur et évaluera la fiabilité de la requête TCP, avant de la transmettre. Vous pourrez limiter le nombre de connexions TCP par secondes pour cette règle de filtrage dans le champ en dessous. • **Déclencher l'alarme associée** : Selon le nombre maximum de connexions par seconde que vous attribuerez aux protocoles ci-dessous, le trafic sera bloqué une fois que le nombre défini sera dépassé. Les identifiants de ces alarmes sont les suivantes : 28 ICMP / 29 UDP / 30 TCP SYN / 253 TCP/UDP.
TCP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole TCP.
UDP (c/s)	Nombre de sessions maximum par seconde autorisé pour le protocole UDP.
ICMP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole ICMP.
SCTP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole SCTP.

Requêtes applicatives (r/s)	Nombre de requêtes applicatives maximum par seconde autorisé pour les protocoles HTTP et DNS.

Cliquer sur **OK** pour valider votre configuration.

DSCP

Le DSCP (*Differentiated Services Code Point)* est un champ dans l'entête d'un paquet IP. Le but de ce champ est de permettre la différentiation de services contenus dans une architecture réseau. Celle-ci spécifie un mécanisme pour classer et contrôler le trafic tout en fournissant de la qualité de service (QoS).

Forcer la valeur	En cochant cette case, vous dégrisez le champ du dessous et libérez l'accès au service DSCP. Cette option permet de réécrire le paquet avec la valeur donnée, afin que le routeur suivant connaisse la priorité à appliquer sur ce paquet.
Nouvelle valeur DSCP	Ce champ permet de définir une différenciation des flux. Via celui-ci, il est possible de déterminer grâce à un code préétabli, l'appartenance d'un trafic à un certain service plutôt qu'à un autre. Ce service DSCP, utilisé dans le cadre de la Qualité de Service, permet à l'administrateur d'appliquer des règles de QoS suivant la différenciation des services qu'il aura définis.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Redirection

Redirection vers le service	• **Aucun** : Cette option implique qu'aucun des deux services suivants ne sera utilisé: l'utilisateur ne passera pas par le proxy HTTP et ne sera pas redirigé vers la page d'authentification. • **Proxy HTTP :** Si vous choisissez cette option, les connexions des utilisateurs seront interceptées par le proxy HTTP qui analysera le trafic. Ce service sera sélectionné lors de création de règles par l'assistant de règle de proxy HTTP explicite. • **Authentification** : Si vous choisissez cette option, les utilisateurs non authentifiés seront redirigés vers le portail captif lors de leur connexion. Ce service sera sélectionné lors de création de règles par l'assistant règle d'authentification.
Redirection d'appels SIP (UDP) entrants	Cette option permet au firewall Stormshield Network de gérer les communications entrantes basées sur le protocole SIP vers des machines internes masquées par de la translation d'adresses (NAT).
URL sans authentification	Ce champ devient accessible si l'option précédente **Service** redirige le flux vers le portail d'authentification (règle d'**authentification**). Il permet de spécifier des catégories ou groupes d'URL dérogeant à l'authentification ; les sites listés deviennent donc accessibles sans authentification, ce qui est par exemple utile pour accéder aux sites de mise à jour. Cet accès peut donc bénéficier des inspections de sécurité du Firewall. Il existe par défaut dans la base objets URL, un groupe d'URL nommé *authentication_bypass* contenant les sites de mise à jour Microsoft.

Traces

Destination des traces pour cette règle	Cette option permet de définir une ou plusieurs méthodes de stockage des traces générées par la règle : • **Disque** : stockage local. • **Serveur Syslog** : le(s) profil(s) Syslog incluant les traces de Politique de filtrage devra(devront) être défini(s) dans l'onglet *SYSLOG* du menu **Notifications** > **Traces - Syslog - IPFIX**. • **Collecteur IPFIX** : le(s) collecteur(s) IPFIX devra(devront) être défini(s) dans l'onglet *IPFIX* du menu **Notifications** > **Traces - Syslog - IPFIX**. Chaque trace comportera le détail des connexions évaluées au travers de la règle.

Configuration avancée

Compter	Si vous cochez cette case, le firewall Stormshield Network comptera le nombre de paquets correspondants à cette règle de filtrage et générera un rapport. Il est ainsi possible d'obtenir des informations de volumétrie sur les flux désirés.
Forcer en IPsec les paquets source	En cochant cette option, et pour cette règle de filtrage, vous obligez les paquets issus du réseau ou des machines sources à emprunter un tunnel IPsec actif pour atteindre leur destination.
Forcer en IPsec les paquets retour	En cochant cette option, et pour cette règle de filtrage, vous obligez les paquets retour (réponses) à emprunter un tunnel IPsec actif pour joindre la machine à l'initiative du flux.
Synchroniser cette connexion entre les firewalls (HA)	Lorsque le firewall est membre d'un cluster, cette option permet d'activer ou non la synchronisation de la connexion correspondant à la règle entre les deux membres du cluster. Cette option est cochée par défaut.

Cliquer sur **OK** pour valider votre configuration.

Source

Ce champ désigne la provenance du paquet traité, il est utilisé comme critère de sélection pour la règle. Un double-clic sur cette zone permettra de choisir la valeur associée dans une fenêtre dédiée.

Celle-ci comporte trois onglets :

Onglet Général

Général

Utilisateur	La règle s'appliquera à l'utilisateur que vous sélectionnerez dans ce champ. Vous pouvez filtrer l'affichage des utilisateurs selon la méthode ou l'annuaire LDAP désiré en cliquant sur l'icône . Seuls les annuaires et méthodes activés (onglet *Méthodes disponibles* du module **Authentification** et annuaires LDAP définis dans le module **Configuration des annuaires**) sont présentés dans cette liste de filtrage. Selon la méthode d'authentification, plusieurs utilisateurs génériques sont proposés : • **« Any user@any»** : désigne tout utilisateur authentifié, quel que soit l'annuaire ou la méthode d'authentification utilisés. • « **Any user@guest_users.local.domain** » : désigne tout utilisateur authentifié par la méthode « Invité ». • « **Any user@voucher_users.local.domain** » : désigne tout utilisateur authentifié par la méthode « Comptes temporaires ». • « **Any user@sponsored_users.local.domain** » : désigne tout utilisateur se présentant via la méthode « Parrainage ». • « **Any user@none** » : désigne tout utilisateur authentifié par une méthode ne reposant pas sur un annuaire LDAP (exemple : méthode Kerberos). • **« Unknown users »** : désigne tout utilisateur inconnu ou non authentifié. **NOTE** Pour que les utilisateurs non authentifiés soient automatiquement redirigés vers le portail captif, il faut définir au moins une règle qui s'applique à l'objet « **Unknown users »**. Cette règle s'appliquera également dès qu'une authentification expire.
Machines sources	La règle s'appliquera à l'objet (créé préalablement au sein de leur menu dédié : **Objets**\module **Objets réseau**) que vous sélectionnerez dans ce champ. La machine source est la machine d'où provient la connexion. Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône . La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton
Interface d'entrée	Interface sur laquelle s'applique la règle de filtrage présentée sous forme de liste déroulante. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source. Il est possible de la modifier pour appliquer la règle sur une autre interface. Cela permet également de spécifier une interface particulière si « Any » a été sélectionnée comme machine source.

Services Web et réputations IP

Sélectionnez un service ou une catégorie de réputation IP

Ce champ permet d'appliquer la règle de filtrage aux machines dont l'adresse IP publique est classifiée dans l'une des catégories ci-dessous :

- **Services Web officiels** (liste mise à jour dynamiquement par le biais du service Stormshield Active Update),
- **Réputations malicieuses** (liste mise à jour dynamiquement par le biais du service Stormshield Active Update) :
  - **anonymiseur** : proxies, convertisseurs IPv4 vers IPv6.
  - **botnet** : machines infectées exécutant des programmes malveillants.
  - **exploit** : adresses IP connues comme étant source d'exploits de vulnérabilités.
  - **malware** : machines distribuant des programmes malveillants
  - **nœud d'entrée tor** : serveurs d'extrémités entrantes du réseau Tor.
  - **nœud de sortie tor** : serveurs d'extrémités sortantes du réseau Tor.
  - **phishing** : serveurs de messagerie compromis.
  - **scanneur** : machines exécutant du balayage de ports (port scanning) ou des attaques par force brute.
  - **spam** : serveurs de messagerie compromis.
  - **suspect** : permet de regrouper des machines et adresses IP présentant peu de gages de confiance et risquant de déclencher de faux positifs. Par défaut, cette catégorie n'est pas incluse dans **bad**.
- **Groupes** :
  - Services Web officiels regroupés par type de fonctionnalité (Accès à distance, Conférence Web ...) ou par fournisseur (Apple, Google ...),
  - **Bad** : regroupe l'ensemble des catégories de réputations malicieuses à l'exception de la catégorie **suspect**,
  - **Malicious** : regroupe **bad** ainsi que deux bases externes d'URL malicieuses.
  - **Nœuds tor** : regroupe les catégories **nœuds d'entrée tor** et **nœud de sortie tor**.

> **NOTE**
> La réputation d'une adresse IP publique pouvant être à la limite de deux catégories (botnet et malware), et ce champ ne permettant de sélectionner qu'une seule catégorie, il est conseillé d'utiliser le groupe "**bad**" pour une protection optimale.

Cliquer sur **OK** pour valider votre configuration.

> **NOTE**
> Les règles de filtrage avec une source de type *user@objet* (sauf *any* ou *unknow@object)*, avec un protocole autre qu'HTTP, ne s'appliquent pas aux **Objets Multi-utilisateurs** (**Authentification > Politique d'authentification**). Ce comportement est inhérent au mécanisme de traitement des paquets effectué par le moteur de prévention d'intrusion.

Onglet Géolocalisation / Réputation

Géolocalisation

Sélectionnez une région	Ce champ permet d'appliquer la règle de filtrage aux machines source dont l'adresse IP publique appartient à des pays, continents ou groupes de régions (groupe de pays et/ou de continents - préalablement définis dans le module **Objets** > **Objets réseau**).

Réputation des machines

Activer le filtrage selon le score de réputation	Cochez cette case afin d'activer le filtrage en fonction du score de réputation des machines du réseau interne. Pour activer la gestion de réputation des machines et définir les machines concernées par le calcul d'un score de réputation, rendez-vous dans le module **Protection applicative** > **Réputation des machines**.
Score de réputation	Ce champ permet de sélectionner le score de réputation au dessus duquel (>) ou au dessous duquel (<) la règle de filtrage s'appliquera aux machines supervisée.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Configuration avancée

Port source	Ce champ permet de préciser le port utilisé par la machine source, si c'est une valeur particulière. Par défaut, le module "Stateful" mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour. La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton
Via	• **Tous** : Cette option implique qu'aucun des trois services suivants ne seront utilisés : la connexion ne passera pas par le proxy HTTP, ne sera pas redirigée vers la page d'authentification et ne passera pas par un tunnel VPN IPsec. • **Proxy HTTP explicite** : Le trafic provient du proxy HTTP. • **Proxy SSL** : Le trafic provient du proxy SSL. • **Tunnel VPN IPsec** : Le trafic provient d'un tunnel VPN IPsec. • **Tunnel VPN SSL** : Le trafic provient d'un tunnel VPN SSL.
DSCP source	Ce champ permet de filtrer en fonction de la valeur du champ DSCP du paquet reçu.

Authentification

Méthode d'authentification	Ce champ permet de restreindre l'application de la règle de filtrage à la méthode d'authentification sélectionnée.

Cliquer sur **OK** pour valider votre configuration.

Destination

Objet destination utilisé comme critère de sélection pour la règle, un double-clic sur cette zone permettra de choisir la valeur associée dans une fenêtre dédiée. Celle-ci comporte deux onglets :

Onglet Général

Général

Machines destinations	Sélectionnez dans la base objets figurant dans la liste déroulante, la machine destinataire du trafic. Vous pouvez **Ajouter** ou **Supprimer** un objet en cliquant sur l'icône . La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton .

Services Web et réputations IP

Sélectionnez un service ou une catégorie de réputation IP	Ce champ permet d'appliquer la règle de filtrage aux machines dont l'adresse IP publique est classifiée dans l'une des catégories ci-dessous : • **Services Web officiels** (liste mise à jour dynamiquement par le biais du service Stormshield Active Update), • **Réputations malicieuses** (liste mise à jour dynamiquement par le biais du service Stormshield Active Update) : ◦ **anonymiseur** : proxies, convertisseurs IPv4 vers IPv6. ◦ **botnet** : machines infectées exécutant des programmes malveillants. ◦ **exploit** : adresses IP connues comme étant source d'exploits de vulnérabilités. ◦ **malware** : machines distribuant des programmes malveillants ◦ **nœud d'entrée tor** : serveurs d'extrémités entrantes du réseau Tor. ◦ **nœud de sortie tor** : serveurs d'extrémités sortantes du réseau Tor. ◦ **phishing** : serveurs de messagerie compromis. ◦ **scanneur** : machines exécutant du balayage de ports (port scanning) ou des attaques par force brute. ◦ **spam** : serveurs de messagerie compromis. ◦ **suspect** : permet de regrouper des machines et adresses IP présentant peu de gages de confiance et risquant de déclencher de faux positifs. Par défaut, cette catégorie n'est pas incluse dans **bad**. • **Groupes** : ◦ Services Web officiels regroupés par type de fonctionnalité (Accès à distance, Conférence Web ...) ou par fournisseur (Apple, Google ...), ◦ **Bad** : regroupe l'ensemble des catégories de réputations malicieuses à l'exception de la catégorie **suspect**, ◦ **Malicious** : regroupe **bad** ainsi que deux bases externes d'URL malicieuses. ◦ **Nœuds tor** : regroupe les catégories **nœuds d'entrée tor** et **nœud de sortie tor**. **NOTE** La réputation d'une adresse IP publique pouvant être à la limite de deux catégories (botnet et malware), et ce champ ne permettant de sélectionner qu'une seule catégorie, il est conseillé d'utiliser le groupe "**bad**" pour une protection optimale.

Cliquer sur **OK** pour valider votre configuration.

Onglet Géolocalisation / Réputation

Géolocalisation

Sélectionnez une région	Ce champ permet d'appliquer la règle de filtrage aux machines destination dont l'adresse IP publique appartient à des pays, continents ou groupes de régions (groupe de pays et/ou de continents - préalablement définis dans le module **Objets** > **Objets réseau**).

Réputation des machines

Activer le filtrage selon le score de réputation	Cochez cette case afin d'activer le filtrage en fonction du score de réputation des machines du réseau interne. Pour activer la gestion de réputation des machines et définir les machines concernées par le calcul d'un score de réputation, rendez-vous dans le module **Protection applicative** > **Réputation des machines**.
Score de réputation	Ce champ permet de sélectionner le score de réputation au dessus duquel (>) ou au dessous duquel (<) la règle de filtrage s'appliquera aux machines destination supervisées.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Configuration avancée

Interface de sortie	Cette option permet de choisir l'interface de sortie du paquet sur laquelle s'applique la règle de filtrage. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP de destination. Il est possible de filtrer en fonction de l'interface de sortie du paquet.

NAT sur la destination

Destination	Si vous souhaitez translater l'adresse IP de destination du trafic, sélectionnez en une parmi les objets de la liste déroulante. Sinon, laissez le champ tel qu'il est : à savoir « **None** » par défaut. **NOTE** Comme ce trafic est déjà translaté par cette option, les autres règles de NAT de la politique courante ne seront pas appliquées à ce flux. La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton .
Publication ARP sur la destination externe (publique)	Cette option permet de pouvoir spécifier une publication ARP, lorsqu'on utilise une règle de filtrage avec du NAT sur la destination. Elle doit être activée si l'adresse IP publique de destination (avant application du NAT) est une IP virtuelle et n'est pas celle de l'UTM. **NOTE** Un autre moyen de mettre en place cette publication consisterait à ajouter l'adresse IP virtuelle à l'interface concernée, depuis le module **Interfaces**.

Cliquer sur **OK** pour valider votre configuration.

Port / Protocole

Le port de destination représente le port sur lequel la machine « source » ouvre une connexion sur une machine de «destination ». Cette fenêtre permet également de définir le protocole sur lequel s'applique la règle de filtrage.

Port

Port destination	Service ou groupe de service utilisé comme critère de sélection pour cette règle. Un double-clic sur cette zone permet de choisir l'objet associé. **EXEMPLES** Port 80 : service HTTP Port 25 : service SMTP Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône La création ou la modification d'un objet directement depuis ce champ peut être réalisée en cliquant sur le bouton .

Protocole

Selon le type de protocole que vous choisissez ici, le champ qui suivra s'affichera différemment :

Type de protocole	Sélectionnez le type de protocole souhaité. Selon votre choix, la valeur des champs suivants sera différente. • Détection automatique du protocole (par défaut), • Protocole applicatif, • Protocole IP, • Protocole Ethernet.
Protocole applicatif	L'intérêt de ce choix est d'appliquer une analyse applicative sur un port différent du port par défaut. Lorsque ce type de protocole est sélectionné : • Protocole applicatif : Choisissez le protocole souhaité dans la liste déroulante. • Protocole IP : le ou les protocoles IP concernés changent selon le protocole applicatif sélectionné.
Protocole IP	Lorsque ce type de protocole est sélectionné : • Protocole applicatif : Aucune analyse applicative. • Protocole IP : Choisissez le protocole souhaité dans la liste déroulante. Des champs supplémentaires peuvent apparaître selon le protocole sélectionné. • Suivi des états (stateful) : Cochez la case pour suivre l'état des connexions IP. Cette option est par défaut activée pour les protocoles TCP, UDP ICMP.
Protocole Ethernet	Lorsque ce type de protocole est sélectionné , choisissez le protocole Ethernet souhaité dans la liste déroulante.

NOTE
Par exemple, vous pouvez activer le suivi d'état (mode « stateful ») des connexions pour le protocole GRE, utilisé dans les tunnels PPTP. Grâce à ce suivi, il est possible de réaliser des opérations de translation sur la source (map), la destination (redirection), ou les 2 (bimap). Toutefois, il est impossible de distinguer 2 connexions qui partagent les mêmes adresses sources et destinations. Concrètement, lorsque le firewall réalise une opération de translation sur la source N -> 1 (map), une seule connexion simultanée vers un serveur PPTP sera possible.

Translation de Port

Cette zone est disponible en cas de **NAT sur la destination** choisie.

Port destination translaté	Port vers lequel est faite la translation. Les paquets réseaux reçus seront redirigés sur un port donné d'une machine ou un équipement réseau vers une autre machine ou équipement réseau. Si vous souhaitez translater le port de destination du trafic, sélectionnez en un parmi les objets de la liste déroulante. Sinon, laissez le champ tel qu'il est : à savoir « **None** » par défaut. Dans ce cas, le champ **Port de destination** restera inchangé.

Inspection de sécurité

Général

Champ Niveau d'inspection

IPS (Détecter et bloquer)	Si vous sélectionnez cette option, l'IPS Stormshield Network (Intrusion Prevention System) détectera et bloquera les tentatives d'intrusion de la couche « réseau » à la couche « applicative » du modèle OSI.
IDS (Détecter)	En sélectionnant cette option, l'IDS Stormshield Network (*Intrusion Detection System*) détectera les tentatives d'intrusion sur votre trafic, mais sans les bloquer.
Firewall (Ne pas inspecter)	Cette option ne donne accès qu'aux fonctions de base de sécurité informatique, et ne fera que filtrer votre trafic sans l'inspecter.

Profil d'inspection

Selon le sens du trafic, IPS_00 à 09	Vous pouvez personnaliser la configuration de votre inspection de sécurité en lui attribuant une politique prédéfinie, celle-ci apparaîtra dans la grille de filtrage. Les configurations numérotées peuvent être renommées dans le menu **Protection applicative** > **Profils d'inspection**. La valeur proposée par défaut (**Selon le sens du trafic**) utilise le profil IPS_00 pour les flux entrants et le profil IPS_01 pour les flux sortants.

Inspection applicative

Antivirus	Les boutons **On** / **Off** vous permettent d'activer ou de désactiver l'Antivirus au sein de votre règle de filtrage. Cette analyse est réalisée uniquement sur les protocoles HTTP, FTP, SMTP, POP3 et leurs variantes en SSL. Elle est paramétrable pour chacun de ces protocoles via le menu **Protection applicative** > **Protocoles**.

Sandboxing	Les boutons **On** / **Off** vous permettent d'activer ou de désactiver l'analyse sandboxing (fichiers malveillants) au sein de votre règle de filtrage. Notez que l'activation de cette option nécessite l'utilisation de l'antivirus avancé. Cette analyse est réalisée uniquement sur les protocoles HTTP, FTP, SMTP, POP3 et leurs variantes en SSL. Elle est paramétrable pour chacun de ces protocoles via le menu **Protection applicative** > **Protocoles**.
Antispam	Les boutons **On** / **Off** vous permettent d'activer ou de désactiver l'Antispam au sein de votre règle de filtrage. Cette analyse est réalisée uniquement sur les protocoles SMTP, POP3 et leurs variantes en SSL. Elle est paramétrable pour chacun de ces protocoles via le menu **Protection applicative** > **Protocoles**.
Filtrage URL	Pour activer ce filtrage, choisissez un profil de filtrage URL au sein des profils proposés.
Filtrage SMTP	Pour activer ce filtrage, choisissez un profil de filtrage SMTP au sein des profils proposés. Le choix d'une politique de filtrage SMTP active également le proxy POP3 dans le cas où la règle de filtrage autorise le protocole POP3.
Filtrage FTP	Les boutons **On** / **Off** vous permettent d'activer ou de désactiver le filtrage FTP au sein de votre règle de filtrage, correspondant aux commandes FTP définies dans le plug-in FTP (module **Protocoles**).
Filtrage SSL	Pour activer ce filtrage, choisissez un profil de filtrage SSL au sein des profils proposés.

Commentaire

Vous pouvez ajouter une description permettant de distinguer plus facilement votre règle de filtrage et ses caractéristiques.

Le commentaire des nouvelles règles indique la date de création et l'utilisateur l'ayant créée si celui-ci n'est pas le compte « admin », sous la forme « Créée le {date}, par {login} ({adresse IP}) ». Ce renseignement automatique peut être désactivé en décochant l'option «Commentaires des règles avec date de création (Filtrage et NAT) - (Comments about rules with creation date (Filtering and NAT) » l'option proposée dans le module Préférences.

L'onglet NAT

Le NAT (*Network Address Translation)* ou la translation d'adresses a pour principe de convertir une adresse IP en une autre lors du passage par le firewall, quelle que soit la provenance de la connexion. Il est également possible par son biais de faire de la translation de ports.

Vérification en temps réel de la politique

La politique de NAT d'un firewall est un des éléments les plus importants pour la sécurité des ressources que le firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit conserver une cohérence parfaite afin que des failles n'apparaissent pas dans la protection que propose le firewall.

L'enjeu est d'éviter la création de règles qui en inhiberaient d'autres. Lorsque la politique de filtrage est conséquente, le travail de l'administrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter cela, l'écran d'édition des règles de filtrage des firewalls dispose d'un champ de « **Vérification de la politique** » (situé en dessous de la grille de filtrage), qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles créées.

EXEMPLE

[Règle 2] Cette règle ne sera jamais appliquée car elle est couverte par la règle 1.

Les actions sur les règles de la politique de NAT

Rechercher	Ce champ permet la recherche par occurrence, lettre ou mot. **EXEMPLE** Si vous saisissez « Any » dans le champ, toutes les règles de NAT comportant « Any » s'afficheront dans la grille.

Nouvelle règle

Insère une ligne à configurer après la ligne sélectionnée, 4 choix sont possibles :

- **Règle simple** : Cette option permet de créer une règle de NAT inactive et qui devra être paramétrée.
- **Règle de partage d'adresse source (masquerading)** : Cette option permet de créer une règle de NAT dynamique de type PAT (Port Address Translation). Ce type de règle permet une conversion d'adresse IP multiples vers une ou N adresses IP. Le port source est également réécrit ; la valeur sélectionnée par défaut est *ephemeral_fw* (correspondant à une plage de ports compris entre 20000 et 59999).
  L'assistant choisit en interface de destination, l'interface correspondant au réseau de cette source après translation.
- **Séparateur-regroupement de règles** : Cette option permet d'insérer un séparateur au-dessus de la ligne sélectionnée.
  Ce séparateur permet de regrouper des règles qui régissent le trafic vers les différents serveurs et contribue à améliorer la lisibilité et la visibilité de la politique de NAT en y indiquant un commentaire.
  Les séparateurs indiquent le nombre de règles regroupées et les numéros de la première et dernière de ces règles. sous la forme : « *Nom de la règle* (contient *nombre total* règles, de n° *première* à n° *dernière*) ».
  Vous pouvez plier et déplier le nœud du séparateur afin de masquer ou afficher le regroupement de règle. Vous pouvez également copier / coller un séparateur d'un emplacement à un autre.
- **Règle de NAT statique (bimap) :** Le principe de la translation d'adresse statique est de convertir une adresse IP (ou N adresses IP, ou adresse publique par exemple) en une autre (ou en N adresses IP privée, par exemple) lors du passage par le firewall, quelle que soit la provenance de la connexion.
  Une fenêtre d'assistant vous permet d'associer une IP privée et une IP publique (virtuelle) en définissant leurs paramètres. Vous devez choisir au sein des listes déroulantes, les **Machines privées** et **virtuelles** pour vos IP, ainsi que l'interface sur laquelle vous souhaitez les appliquer.
  Le champ de **Configuration avancée** permet de restreindre l'application à un port ou un groupe de ports, ainsi que d'activer la Publication ARP. Cette dernière permet de rendre disponible l'IP à publier via l'adresse MAC du firewall.
  Toutefois, il est recommandé de restreindre l'accès à un port ou un groupe de ports par le biais d'une règle de filtrage correspondant à ce flux. Cela permet d'y ajouter d'autres critères afin de rendre ce filtrage plus précis.

Cliquez ensuite sur **Terminer** pour valider votre configuration.

Notez que pour une règle de translation bidirectionnelle (bimap) de N vers N, les plages d'adresses, réseaux ou groupes de machines originaux et translatés doivent être de même taille.

La translation bidirectionnelle est généralement utilisée pour donner accès à un serveur depuis l'extérieur avec une adresse IP publique qui n'est pas l'adresse réelle de la machine.

Les plages d'adresses sont supportées par l'action bidirectionnelle. Les adresses sources et translatées sont utilisées dans l'ordre : la plus "petite" adresse du champ source est translatée vers la plus "petite" adresse du champ translaté.

Lors du choix de l'adresse IP virtuelle, la sélection de l'interface correspondante est automatique. Celle-ci sera utilisée en source pour la règle de redirection et en destination pour les règles de réécriture de la source.

Supprimer	Ce champ permet de supprimer la ligne sélectionnée.
Monter	Placer la ligne sélectionnée avant la ligne directement au-dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Tout dérouler	Étendre l'arborescence des règles.
Tout fermer	Regrouper l'arborescence des règles.
Couper	Couper une règle de NAT dans le but de la dupliquer.
Copier	Copier une règle de NAT dans le but de la dupliquer.
Coller	Dupliquer une règle de NAT, après l'avoir copié.
Chercher dans les logs	Lorsqu'une règle de NAT est sélectionnée, cliquez sur ce bouton pour lancer automatiquement une recherche portant sur le nom de la règle dans la vue "Tous les journaux" (module **Logs** > **Journaux d'audit** > **Vues**). Si aucun nom n'a été spécifié pour la règle sélectionnée, un message d'avertissement précise que la recherche est impossible.
Chercher dans la supervision	Lorsqu'une règle de NAT est sélectionnée, cliquez sur ce bouton pour lancer automatiquement une recherche portant sur le nom de la règle dans le module de supervision des connexions.

Avancé	**Réinitialiser les statistiques des règles**	En cliquant sur ce bouton, vous réinitialisez les compteurs numériques et graphiques d'utilisation des règles de NATsitués dans la première colonne de la grille.
	Réinitialiser l'affichage des colonnes	Lorsque vous cliquez sur la flèche de droite dans le champ du nom d'une colonne (exemple : **État**), vous avez la possibilité d'afficher des colonnes supplémentaires ou d'en retirer afin qu'elles ne soient pas visibles à l'écran, grâce à un système de coche.

EXEMPLE
Vous pouvez cocher les cases « **Nom** » et « **Port src** » qui ne sont pas affichées par défaut.
En cliquant sur le bouton **réinit. colonnes**, vos colonnes seront remises à leur état initial, avant que vous n'ayez coché de case additionnelle.
Ainsi, les cases **Nom** et **Port src** seront de nouveau masquées.

NOTE
Si vous cliquez rapidement 10 fois sur le bouton "Monter", vous distinguez la règle monter visuellement mais la fenêtre d'attente n'apparaît que lorsqu'on ne touche plus au bouton au-delà de 2 ou 3 secondes. Et au final, une seule commande sera passée. Ceci rend le déplacement des règles beaucoup plus fluide.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles de NAT :

- Nouvelle règle (Règle simple, Règle de partage d'adresse source [masquerading], Séparateur - Regroupement de règles, Règle de NAT statique [bimap]),
- Supprimer,
- Couper,
- Copier,
- Coller,
- Chercher dans les logs,
- Chercher dans la supervision.

Comparaison mathématique

Chaque fois que vous rencontrerez une liste déroulante d'objets au sein des colonnes (exceptées **État** et **Action**), une icône d'opérateur de comparaison mathématique apparaîtra ( ). Elle ne sera utilisable que si un autre objet que **Any** est sélectionné.

Vous pourrez ainsi personnaliser les paramètres de votre trafic par le biais de l'icône suivante de 4 manières différentes :

- « = » (ou): la valeur de l'attribut correspond à ce qui est sélectionné.
- « != » (ou) la valeur de l'attribut est différente de ce qui est sélectionné.
- « < » (ou ; utilisable pour les ports source et destination uniquement) : le numéro de port du trafic est inférieur à ce qui est sélectionné.
- « > » (ou ; utilisable pour les ports source et destination uniquement) : le numéro du port du trafic est supérieur à ce qui est sélectionné.

Ajout / modification d'objet

Certaines listes déroulantes de sélection d'objets proposent le bouton qui permet d'accéder à un menu contextuel :

- **Créer un objet** : un nouvel objet peut directement etre créé depuis le module Filtrage/NAT
- **Modifier cet objet** : lorsqu'un objet est présent dans le champ, il peut directement être édité pour modification (changement de nom, d'adresse IP pour une machine, ajout dans un groupe...), à l'exception des objets en lecture seule ("**Any**", "**Internet**", ...).

La grille de NAT

Elle vous permet de définir les règles de NAT à appliquer. Ordonnez-les afin d'avoir un résultat cohérent : le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dès qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et spécifiée et ne continue pas la lecture des règles suivantes.

Il convient donc de définir les règles dans l'ordre **du plus restrictif au plus général**.

La grille du NAT est divisée en deux : elle comporte d'une part, le Trafic original (avant translation), et d'autre part, le Trafic translaté.

Réorganisation des règles

Chaque règle peut être glissée et déplacée pour réorganiser aisément la politique (filtrage ou NAT). Le symbole ainsi que l'infobulle "Glissez et déplacez pour réorganiser" apparaissent lorsque la souris survole le début de la règle.

État

Cette colonne affiche l'état On / Off de la règle. Double-cliquez dessus pour changer l'état : en effectuant cette manipulation une fois, vous activez la règle de NAT. Renouvelez l'opération pour la désactiver.

NOTE
La translation d'adresse source gère les protocoles IP sans état (type GRE) toutefois avec la limitation suivante :
si deux clients passent par le même firewall, ils ne pourront pas se connecter sur un même serveur en même temps. Le moteur de prévention d'intrusion Stormshield Network va bloquer les paquets reçus par le second client.
Au bout de 5 minutes, le moteur de prévention d'intrusion jugera la session trop ancienne et permettra au second client de prendre le relai.

Onglet Général de la fenêtre d'édition de la règle

Général

État	Sélectionnez l'état **On** ou **Off** pour respectivement activer ou désactiver la règle en cours d'édition.
Commentaire	Vous pouvez saisir un commentaire : celui-ci sera affiché en toute fin de règle lors de l'affichage de la politique de translation d'adresses.

Configuration avancée

Nom de la règle	Vous pouvez affecter un nom à la règle de NAT: ce nom est repris dans les logs est facilité l'identification de la règle de NAT lors d'une recherche dans les logs ou vues (menu **Logs - journaux d'audit**).

Source originale (avant translation)

Onglet Général

Général

Utilisateur	La règle s'appliquera à l'utilisateur ou au groupe d'utilisateurs que vous sélectionnerez dans ce champ. Il en existe trois par défaut : • **« No user » :** cette option permet de vider le champ utilisateur et de ne plus y appliquer de critère pour la règle. • **« Any user »** : désigne tout utilisateur authentifié. • **« Unknown users »** : désigne tout utilisateur inconnu ou non authentifié.

Machines sources	La règle s'appliquera à l'objet que vous sélectionnerez dans ce champ. La machine source est la machine d'où provient le paquet traité : elle est l'émetteur du paquet. Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône et **Créer** un objet en cliquant sur l'icône .
Interface d'entrée	Interface sur laquelle s'applique la règle de translation présentée sous forme de liste déroulante. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour appliquer la règle sur une autre interface. Il est possible de la modifier pour appliquer la règle sur une autre interface. Cela permet également de spécifier une interface particulière si « Any » a été sélectionnée comme machine source.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Configuration avancée

Port source	Ce champ permet de préciser le port source utilisé par la machine source. Par défaut, le mode « Stateful » mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
DSCP source	Ce champ désigne le code DSCP source du paquet reçu.

Authentification

Méthode d'authentification	Ce champ permet de restreindre l'application de la règle de filtrage à la méthode d'authentification sélectionnée.

Cliquer sur **OK** pour valider votre configuration.

Destination originale (avant translation)

Onglet Général

Général

Machines destinations	Sélectionnez dans la base objets figurant dans la liste déroulante, la machine destinataire de votre trafic IP.
Port destination	Si vous souhaitez translater le port de destination du trafic, sélectionnez en un parmi les objets de la liste déroulante. L'objet « Any » est sélectionné par défaut.

Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône et **Créer** un objet en cliquant sur l'icône . Cliquer sur **OK** pour valider votre configuration.

NOTE
Des types d'équilibrages de charge autres que le hachage de connexion peuvent être sélectionnés avec une plage de ports de destination.

Onglet Configuration avancée

Configuration avancée

Interface de sortie	Cette option permet de choisir l'interface de sortie du flux translaté. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour restreindre la règle à une interface.
Publication ARP	Cette option permet de rendre disponible l'IP à publier via l'adresse MAC du firewall.

NOTE
L'option de publication ARP est affectée à la destination originale (trafic avant translation), dont l'adresse IP est effectivement publiée, et non à la destination translatée.

Source translatée (après translation)

Onglet Général

Général

Machine source translatée	La règle s'appliquera à l'objet que vous sélectionnerez dans ce champ. La machine source translatée fait référence à la nouvelle adresse IP de la machine source, après sa translation.
Port source translaté	Ce champ permet de préciser le port source utilisé par la machine source après la translation. Par défaut, le mode "Stateful" mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour. La création d'une *règle de partage d'adresse source (masquerading)* assigne la valeur *ephemeral_fw* à ce champ.
Choisir aléatoirement le port source translaté	En cochant cette option, le firewall va sélectionner de manière aléatoire le port source translaté dans la liste (ex : *ephemeral_fw*). Cela permet d'éviter une anticipation des connexions suivantes car les ports sources sont assignés de manière consécutive. Cela renforce ainsi la sécurité.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Répartition de charge

Type de répartition	Cette option permet de répartir les adresses IP sources d'émission du paquet après translation. La méthode de répartition de charge dépend de l'algorithme utilisé. Plusieurs algorithmes de répartition de charge sont disponibles : • **Aucune** : Aucune répartition de charge ne sera effectuée. • **Round-robin** : Cet algorithme permet de répartir équitablement la charge parmi les différentes IP de la plage d'adresses sélectionnée. Chacune de ces adresses IP sources seront utilisées de façon alternée. • **Hachage de l'IP source** : Un hash de l'adresse source est effectué pour choisir l'adresse de la plage à utiliser. Cette méthode permet de garantir qu'une adresse source donnée sera toujours associée avec la même adresse de la plage. • **Hachage de la connexion** : L'utilisateur peut maintenant choisir le hachage par connexion (IP source + port source + adresse IP destination + port destination) comme méthode de répartition de charge (load balancing) dans ses règles de NAT. Cela permet aux connexions d'une source vers un même serveur, d'être réparties en fonction du port source et de l'adresse IP source. • **Aléatoire** : Le firewall sélectionne aléatoirement une adresse parmi la plage d'adresses sélectionnée
Publication ARP	Cette option permet de rendre disponible l'IP à publier via l'adresse MAC du firewall.

Cliquer sur **OK** pour valider votre configuration.

Destination translatée (après translation)

Onglet Général

Général

Machine destination translatée	Ce champ permet de sélectionner la machine destinataire du paquet translaté au sein de la liste déroulante d'objets.
Port destination translaté	Ce champ permet de préciser le port destination utilisé par la machine de destination.

Cliquer sur **OK** pour valider votre configuration.

Onglet Configuration avancée

Des types d'équilibrage de charge autres que le hachage de connexion peuvent être sélectionnés avec une plage de ports de destination.

Répartition de charge

Type de répartition	Cette option permet de répartir la transmission de paquets entre plusieurs adresses IP de destination. La méthode de répartition de charge dépend de l'algorithme utilisé. Plusieurs algorithmes de répartition de charge sont disponibles : • **Aucune** : Aucune répartition de charge ne sera effectuée. • **Round-robin** : Cet algorithme permet de répartir équitablement la charge parmi les différentes IP de la plage d'adresses sélectionnée. Chacune de ces adresses IP sources seront utilisées de façon alternée. • **Hachage de l'IP source** : Un hash de l'adresse source est effectué pour choisir l'adresse de la plage à utiliser. Cette méthode permet de garantir qu'une adresse source donnée sera toujours associée avec la même adresse de la plage. • **Hachage de la connexion** : L'utilisateur peut maintenant choisir le hachage par connexion (IP source + port source + adresse IP destination + port destination) comme méthode de répartition de charge (load balancing) dans ses règles de NAT. Cela permet aux connexions d'une source vers un même serveur, d'être réparties en fonction du port source et de l'adresse IP source. • **Aléatoire** : Le firewall sélectionne aléatoirement une adresse parmi la plage d'adresses sélectionnée
Entre les ports	Cette option permet de répartir la transmission de paquets entre plusieurs ports de destination. La méthode de répartition de charge dépend de l'algorithme utilisé. Les algorithmes de répartition de charge sont les mêmes que ceux décrits que précédemment.

Cliquer sur **OK** pour valider votre configuration.

Protocole

Protocole

Selon le type de protocole que vous choisissez ici, le champ qui suivra s'affichera différemment :

Type de protocole	Sélectionnez le type de protocole souhaité. Selon votre choix, la valeur des champs suivants sera différente. • Détection automatique du protocole (par défaut), • Protocole applicatif, • Protocole IP, • Protocole Ethernet.
Protocole applicatif	L'intérêt de ce choix est d'appliquer une analyse applicative sur un port différent du port par défaut. Lorsque ce type de protocole est sélectionné : • Protocole applicatif : Choisissez le protocole souhaité dans la liste déroulante. • Protocole IP : le ou les protocoles IP concernés changent selon le protocole applicatif sélectionné.
Protocole IP	Lorsque ce type de protocole est sélectionné : • Protocole applicatif : Aucune analyse applicative. • Protocole IP : Choisissez le protocole souhaité dans la liste déroulante. Des champs supplémentaires peuvent apparaître selon le protocole sélectionné.

Protocole Ethernet	Lorsque ce type de protocole est sélectionné , choisissez le protocole Ethernet souhaité dans la liste déroulante.

Options

Niveau de trace	Le traçage des flux permet de faciliter le diagnostic et le dépannage. Ce résultat sera stocké dans les fichiers de traces de type filtrage.
NAT dans le tunnel IPsec (avant chiffrement, après déchiffrement)	Si l'option est cochée, la politique de chiffrement est appliquée sur le trafic translaté. L'opération de NAT est effectuée juste avant le chiffrement par le module IPsec à l'émission et après le déchiffrement des paquets à la réception.

Commentaire

Vous pouvez ajouter une description permettant de distinguer plus facilement votre règle de NAT et ses caractéristiques.

Le commentaire des nouvelles règles indique la date de création et l'utilisateur l'ayant créée si celui-ci n'est pas le compte « admin », sous la forme « Créée le {date}, par {login} ({adresse IP}) ». Ce renseignement automatique peut être désactivé en décochant l'option «Commentaires des règles avec date de création (Filtrage et NAT) - (Comments about rules with creation date (Filtering and NAT) » l'option proposée dans le module Préférences.

FILTRAGE SMTP

Ce module se compose de deux zones :

- Un menu déroulant listant les différents profils,
- Une grille regroupant les règles de filtrage SMTP.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage SMTP.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.

Chaque profil possède par défaut, le nom « MailFilter_ », accompagné de sa numérotation.

EXEMPLES

- (1) MailFilter_00,
- (1) MailFilter_01 ...

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « MailFilter_00 », et choisir le profil voulu.

Par défaut, chaque profil est configuré de la manière suivante :

État	Action	Expéditeur	Destinataire (to,cc,cci)	Commentaire
Activé	Passer	*@*	*@*	default rule (pass all)

Les boutons

Éditer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage SMTP :

1. Sélectionnez un profil dans la liste des profils de filtrage d'URL.
2. La grille de filtrage se présente ainsi qu'un écran d'indication d'erreur.

Les manipulations possibles

Les boutons disponibles sont les suivants :

Ajouter	Insérer une ligne à configurer après la ligne sélectionnée.
Supprimer	Supprimer la ligne sélectionnée.
Monter	Placer la ligne sélectionnée avant la ligne directement au-dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Couper	Enlever la ligne sélectionnée et la placer dans le presse-papier
Copier	Copier la ligne sélectionnée et la placer dans le presse-papier
Coller	Coller la ligne placée dans le presse papier au dessous de la ligne sélectionnée.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles de filtrage :

- Ajouter,
- Supprimer,
- Couper,
- Copier,
- Coller.

La grille

La grille présente les colonnes suivantes :

État	État de la règle : • **Activé**, la règle est utilisée pour le filtrage. • **Désactivé**, la règle n'est pas utilisée pour le filtrage. Lorsque la règle est désactivée, la ligne est grisée afin de refléter la désactivation. Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci passeront automatiquement en **Bloquer** également.
Action	Permet de spécifier le résultat de la règle : **Passer** pour autoriser l'envoi et la réception des mails, **Bloquer** pour les interdire
Expéditeur	Définition de l'émetteur du mail. La sélection de « none » en tant qu'expéditeur est possible.

Destinataire (to, cc, cci)	Définition du destinataire du mail.
Commentaire	Commentaire associé à la règle.

La saisie d'un masque d'e-mails peut comporter la syntaxe suivante :

- * : remplace une séquence de caractères quelconque.

EXEMPLE
*@compagnie.com permet de définir l'ensemble des E-mails domaine Internet de la société COMPAGNIE.

Il est également possible de trouver :

- ? : pour le remplacement d'un caractère
- <none> : Cette valeur ne peut être obtenue que lorsque le champ **Expéditeur** est vide. Elle n'est utilisée que pour le cas des "Mailer Daemon". En effet, lorsqu'un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ **Expéditeur** de ce message d'erreur est vide.

Il est possible de créer une règle avec l'action « bloquer » qui empêchera l'envoi de mail si l'expéditeur n'est pas connu.

Erreurs trouvées dans la politique de filtrage SMTP

L'écran d'édition des règles de filtrage SMTP des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles créées.

Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.

Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée sera automatiquement sélectionnée.

FILTRAGE SSL

Ce module permet de filtrer l'accès aux sites web sécurisés. Il rend possible l'autorisation et l'interdiction des sites web ou des certificats comportant des risques.

Ce module se compose de 2 zones :

- Un menu déroulant listant les différents profils,
- Une grille regroupant les règles de filtrage SSL.

NOTE
Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est à dire de regrouper explicitement les catégories d'URL à interdire dans un groupe d'URL personnalisé auquel est appliqué une règle de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Cette règle est à placer au-dessus de la règle autorisant toutes les autres catégories.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage SSL.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.

Chaque profil possède par défaut, le nom « SSLFilter_ », accompagné de sa numérotation.

EXEMPLES

- (0) SSLFilter_00,
- (1) SSLFilter_01…

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « Default00 », et choisir le profil voulu.

Par défaut, chaque profil est configuré de la manière suivante :

État	Action	URL-CN	Commentaire
Activé	Déchiffrer	any	default rule (decrypt all)

Les boutons

Éditer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.
Fournisseur de base URL	Ce lien redirige vers le module permettant de configurer le fournisseur de Base d'URL (module **Objets** / **URL** / onglet *Base d'URL*)

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage SSL :

1. Sélectionnez un profil dans la liste des profils de filtrage SSL.
2. La grille de filtrage se présente ainsi qu'un écran d'indication d'erreur.

NOTE
Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est à dire de regrouper explicitement les catégories d'URL à interdire dans un groupe d'URL personnalisé auquel est appliqué une règle de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Cette règle est à placer au-dessus de la règle autorisant toutes les autres catégories.

Les manipulations possibles

La sélection multiple permet d'assigner une même action à plusieurs règles. Sélectionnez plusieurs règles se succédant à l'aide de touche **Shift** ⇧ ou individuellement avec la touche **Ctrl.** Vous pourrez également soustraire une sélection à une sélection existante, avec la touche **Ctrl.**

Certains intitulés de colonnes affichent l'icône . Par un simple clic, un menu s'affiche et propose d'assigner un même paramètre à plusieurs règles sélectionnées (*Etat* et *Action*).

EXEMPLE
Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche **Ctrl** puis en cliquant sur **Supprimer**.

Les boutons disponibles sont les suivants :

Ajouter	Insérer une ligne à configurer après la ligne sélectionnée.

Supprimer	Supprimer la ligne sélectionnée.
Monter	Placer la ligne sélectionnée avant la ligne directement au-dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Couper	Enlever la ligne sélectionnée et la placer dans le presse-papier
Copier	Copier la ligne sélectionnée et la placer dans le presse-papier
Coller	Coller la ligne placée dans le presse papier au dessous de la ligne sélectionnée.
Ajouter toutes les catégories prédéfinies	Ce bouton permet en une seule action de créer autant de règles de filtrage que de catégories d'URL existant dans la base d'URL sélectionnée. Toutes les règles ainsi créées sont activées et l'action associée par défaut est *Déchiffrer*.
Nettoyer les règles	Ce bouton est utile pour les politiques de filtrage SSL EWC créées avant la version SNS 4.7.1 EA puis migrées à l'occasion du changement de fournisseur de base d'URL (version SNS 4.7.1 EA ou supérieure) : il permet de supprimer les règles faisant appel à des catégories qui n'ont plus d'équivalent dans la base d'URL du fournisseur en vigueur depuis la version SNS 4.7.1 EA.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles de filtrage :

- Ajouter,
- Supprimer,
- Couper,
- Copier,
- Coller.

La grille

La grille présente les colonnes suivantes :

État	État de la règle : • **Activé**, la règle est utilisée pour le filtrage. • **Désactivé**, la règle n'est pas utilisée pour le filtrage. Lorsque la règle est désactivée, la ligne est grisée afin de refléter la désactivation. **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dès qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci seront considérées **Bloquer** également.

Action	Permet de spécifier l'opération à effectuer : • Si **Passer sans déchiffrer** spécifié, l'accès au CN demandé est autorisé sans analyse SSL préalable. • Si **Bloquer sans déchiffrer** est spécifié, l'accès au CN demandé est refusé, sans qu'aucune analyse SSL ne soit effectuée. La connexion est coupée. • Si **Déchiffrer** est spécifié, l'analyse protocolaire sera appliquée sur le flux déchiffré, ainsi que sur un proxy, si une règle est créée pour cela, • Si BlockPage_XX est spécifié, l'accès au CN demandé est refusé, sans qu'aucune analyse SSL ne soit effectuée. La connexion est coupée et la page de blocage sélectionnée (BlockPage_XX) est affichée à l'utilisateur. Vous pouvez éditer et personnaliser ces pages de blocage dans L'onglet Page de blocage du module MESSAGES DE BLOCAGE.
URL-CN	L'action s'applique en fonction de la valeur de cette colonne, elle peut contenir un groupe ou une catégorie d'URL, ainsi qu'un groupe de noms de certificats.
Commentaire	Commentaire associé à la règle.

Erreurs trouvées dans la politique de filtrage SSL

L'écran d'édition des règles de filtrage SSL des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles créées.

Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.

Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée sera automatiquement sélectionnée.

FILTRAGE URL

Ce module se compose de deux zones :

- Un menu déroulant listant les différents profils,
- Une grille regroupant les règles de filtrage d'URL.

NOTE
Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est à dire de regrouper explicitement les catégories d'URL à interdire dans un groupe d'URL personnalisé auquel est appliqué une règle de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Cette règle doit être placée au-dessus de la règle autorisant toutes les autres catégories.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage URL.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09. Chaque profil possède par défaut, le nom « URLFilter_ », accompagné de sa numérotation.

EXEMPLES
- (0) URLFilter_00,
- (1) URLFilter_01…

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « URLFilter_00 », et choisir le profil voulu. Par défaut, chaque profil est configuré de la manière suivante :

État	Action	Catégorie d'URL ou groupe	Commentaire
Activé	Passer	any	default rule (pass all)

Les boutons

Éditer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. Le profil redevient « actif » sous l'action **Passer**, appliquée à tous les catégories d'URL ou leurs groupes. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.

Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.
Fournisseur de base URL	Ce lien redirige vers le module permettant de configurer le fournisseur de Base d'URL (module **Objets** / **URL** / onglet *Base d'URL*).

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage d'URL :

1. Sélectionnez un profil dans la liste des profils de filtrage d'URL.
2. La grille de filtrage se présente ainsi qu'un écran listant les erreurs présentes dans la politique.

> **NOTE**
> Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est à dire de regrouper explicitement les catégories d'URL à interdire dans un groupe d'URL personnalisé auquel est appliqué une règle de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Cette règle est à placer au-dessus de la règle autorisant toutes les autres catégories.

Les manipulations possibles

La sélection multiple permet d'assigner une même action à plusieurs règles. Sélectionnez plusieurs règles se succédant à l'aide de touche **Shift** ⇧ ou individuellement avec la touche **Ctrl.** Vous pourrez également soustraire une sélection à une sélection existante, avec la touche **Ctrl.**

Certains intitulés de colonnes affichent l'icône . Par un simple clic, un menu s'affiche et propose d'assigner un même paramètre à plusieurs règles sélectionnées (*État* et *Action*).

Exemple : Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche « Ctrl » puis en cliquant sur **Supprimer**.

Les boutons disponibles sont les suivants :

Ajouter	Insérer une ligne à configurer après la ligne sélectionnée.
Supprimer	Supprimer la ligne sélectionnée.
Monter	Placer la ligne sélectionnée avant la ligne directement au-dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Couper	Enlever la ligne sélectionnée et la placer dans le presse-papier
Copier	Copier la ligne sélectionnée et la placer dans le presse-papier
Coller	Coller la ligne placée dans le presse papier au dessous de la ligne sélectionnée.
Ajouter toutes les catégories prédéfinies	Ce bouton permet en une seule action de créer autant de règles de filtrage que de catégories d'URL existant dans la base d'URL sélectionnée. Toutes les règles ainsi créées sont activées et l'action associée par défaut est la redirection vers la page de blocage BlockPage_00.

Nettoyer les règles	Ce bouton est utile pour les politiques de filtrage d'URL EWC créées avant la version SNS 4.7.1 EA puis migrées à l'occasion du changement de fournisseur de base d'URL (version SNS 4.7.1 EA ou supérieure) : il permet de supprimer les règles faisant appel à des catégories qui n'ont plus d'équivalent dans la base d'URL du fournisseur en vigueur depuis la version SNS 4.7.1 EA.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des règles de filtrage :

- Ajouter,
- Supprimer,
- Couper,
- Copier,
- Coller.

La grille

La grille présente les colonnes suivantes :

État	État de la règle : • **Activé**, la règle sera active lorsque cette politique de filtrage sera sélectionnée. • **Désactivé**, la règle ne sera pas opérationnelle. La ligne sera grisée afin de refléter la désactivation. **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dès qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci passeront automatiquement en **Bloquer** également.
Action	Permet de spécifier le résultat de la règle, **Passer** pour autoriser le site, **Bloquer** pour interdire l'accès et clore directement la connexion sans message de blocage. Il est possible de **Bloquer et rediriger vers une page de blocage** pour interdire l'accès et afficher l'une de 4 pages HTML de blocage disponibles. Ces pages sont personnalisables dans le Menu **Notifications**, module **Messages de blocage** et l'onglet *Pages de blocage HTTP*.
Catégorie d'URL ou groupe	Un nom de catégorie d'URL ou de groupe de catégories précédemment créé. En cliquant sur le champ, une liste déroulante vous invite à choisir une catégorie d'URL ou un groupe de catégories, issu de la base objets. Le groupe <Any> correspond à n'importe quelle URL, même si elle ne fait pas partie des catégories d'URL ou de groupes.
Commentaire	Commentaire associé à la règle.

Erreurs trouvées dans la politique de filtrage d'URL

L'écran d'édition des règles de filtrage d'URL des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles créées.

Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.

Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée est automatiquement sélectionnée.

HAUTE DISPONIBILITE

Ce module va vous permettre dans un premier temps, de créer un cluster ou groupe de firewalls. Une fois ceci fait, un autre firewall pourra rejoindre celui que vous venez d'initialiser.

Il est important de noter que seuls des flux liés à la Haute Disponibilité doivent transiter sur les liens HA. L'assistant de création de VLAN ne permet pas, par exemple, de sélectionner des interfaces HA pour supporter les VLAN en cours de création.

La Haute Disponibilité Stormshield Network fonctionne sur le mode « Actif/passif » : un cluster contenant 2 firewalls, si celui considéré comme « actif » tombe, ou qu'un câble est débranché, le second firewall, considéré comme « passif » prend le relai de manière transparente. Ainsi, le firewall « passif » devient « actif ».

Une vidéo de la WebTV Stormshield Network sur YouTube vous guide pas à pas pour la configuration d'un groupe de firewalls Stormshield Network (cluster). Cliquez sur ce lien pour accéder à la vidéo : Configurer un cluster de firewall Stormshield Network.

La configuration de la Haute Disponibilité se déroule en 4 étapes:

- Étape 1 : Créer un groupe de firewalls (cluster) / rejoindre un groupe de firewalls (cluster) existant
- Étape 2 : Configuration des interfaces réseaux : le lien principal et le lien secondaire (facultatif)
- Étape 3 : Définition de la clé pré partagée du cluster
- Étape 4 : Résumé des étapes et application des paramètres configurés

Une fois ces 4 étapes terminées, un nouvel écran s'affichera vous proposant d'effectuer de nouvelles configurations au sein de la HA.

NOTE
Le lien de communication entre les membres d'un cluster doit être établi depuis une interface protégée. La configuration se modifie dans le module **Interfaces**.

Étape 1 : Créer ou rejoindre un cluster en Haute Disponibilité

Créer un groupe de firewalls (cluster)	Lorsque vous cochez cette option, le boîtier se tient prêt à recevoir les autres firewalls et s'ajoute lui-même au cluster.

Rejoindre un groupe de firewalls (cluster)	Lorsque vous cochez cette option, le boîtier va tenter de se connecter à celui renseigné par l'adresse IP définie lors de la création du cluster. Ainsi, ce second firewall va récupérer les infos du premier et se synchroniser à lui. Le cluster est ainsi composé de deux firewalls : si le premier tombe, le second prendra le relai de manière transparente. **NOTE** Un redémarrage du firewall sera effectué à la fin de l'assistant. Une fois ce redémarrage effectué, le boîtier fait partie du cluster, donc n'existe plus en tant qu'entité, mais en tant que membre du cluster. **AVERTISSEMENT** Lorsque vous choisissez de « rejoindre » un cluster, il implique que vous en ayez déjà créé un au préalable, en ayant coché l'autre option « **Créer un groupe de firewalls (cluster)** » et en ayant effectué les configurations nécessaires pour sa mise en place sur un premier firewall.

AVERTISSEMENT
Il est important de ne pas "créer" deux fois de cluster, au quel cas, vous mettriez en place deux clusters HA contenant chacun un firewall, et non un cluster HA contenant 2 firewalls.

NOTE
Il est possible de forcer le passage à l'état actif d'un membre d'un cluster, même si les membres du groupe possèdent différentes versions firmware.

Étape 2 : Configuration des interfaces réseaux

Si vous avez choisi de créer un cluster

Lien principal

Interface	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante.
Définir le nom	Définissez un nom personnalisé pour le lien principal.
Définir l'adresse IP et le masque réseau	Entrez l'adresse IP et le masque réseau dédiés à votre lien principal. Le format est du type adresse / masque.

Lien secondaire (facultatif)

Si le firewall ne reçoit pas de réponse sur le lien principal, il va tenter de se connecter à ce lien secondaire. Cela évite que les deux firewalls passent en mode actif / actif si un problème survient sur le lien principal.

Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster.
Interface	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante.
Définir le nom	Définissez un nom personnalisé pour votre lien secondaire.
Définir l'adresse IP	Entrez l'adresse IP pour votre lien secondaire.

NOTE
Pour qu'un lien fonctionne, les 2 membres du cluster doivent utiliser la même interface.
Si les noeuds du cluster communiquent via une interface Ethernet, celle-ci doit être dédiée à cet usage. L'utiliser comme interface parent d'une interface virtuelle d'un VLAN n'est pas supporté.
L'interface de communication entre les noeuds d'un cluster peut être isolée dans un VLAN. Dans ce cas, certaines fonctionnalités avancées liées à la communication des membres du cluster ne seront pas disponibles.

Si vous avez choisi de rejoindre un cluster

Cette option sous-entend d'un groupe de firewalls ait déjà été créé au préalable, pour que celui-ci puisse le « rejoindre ».
Ainsi, une partie des informations du premier firewall créé seront reprises.

Lien principal

Interface	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Cette interface doit être la même que celle sélectionnée lors de la création du cluster sur le premier firewall.
Définir l'adresse IP et le masque réseau	Adresse IP et masque réseau dédiés à votre lien principal. Le format est du type adresse/masque. Cette adresse doit appartenir au même sous-réseau que celui défini lors de la création du cluster sur le premier firewall.

Lien secondaire (facultatif)

Si le firewall ne reçoit pas de réponse sur le lien principal, il va tenter de se connecter à ce lien secondaire. Cela évite que les deux firewalls passent en mode actif / actif si un problème survient sur le lien principal.

Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster. Cette option ne doit être sélectionnée que si elle l'avait été lors de la création du cluster sur le premier firewall.
Interface	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Cette interface doit être la même que celle sélectionnée lors de la création du cluster sur le premier firewall.

Définir l'adresse IP	Adresse IP pour votre lien secondaire. Cette adresse doit appartenir au même sous-réseau que celui défini lors de la création du cluster sur le premier firewall.

NOTE
Pour qu'un lien fonctionne, les 2 membres du cluster doivent utiliser la même interface.
Si les noeuds du cluster communiquent via une interface Ethernet, celle-ci doit être dédiée à cet usage. L'utiliser comme interface parent d'une interface virtuelle d'un VLAN n'est pas supporté.
L'interface de communication entre les noeuds d'un cluster peut être isolée dans un VLAN. Dans ce cas, certaines fonctionnalités avancées liées à la communication des membres du cluster ne seront pas disponibles.

Étape 3 : Clé pré-partagée du cluster et chiffrement des données

En cas de création de cluster

Clé pré-partagée

Pour sécuriser la connexion entre les membres du cluster, vous devez définir une clé pré partagée.
Celle-ci ne sera utilisée que par les firewalls rejoignant le cluster pour la première fois.

Clé pré-partagée du cluster	Définissez un mot de passe / une clé pré partagée pour votre cluster.
Confirmer	Confirmation du mot de passe / clé pré partagée, que vous venez de renseigner dans le champ précédent.
Robustesse du mot de passe	Cette jauge indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Communication entre les firewalls du groupe de haute disponibilité

Chiffrer la communication entre les firewalls	Par défaut, les communications entre les firewalls ne sont pas chiffrées, partant du principe que le lien utilisé par la HA est un lien dédié. Dans certaines architectures, le lien HA n'est pas dédié, et si on souhaite que les communications inter-cluster soient indéchiffrables, on peut les chiffrer (en AES, par exemple). **AVERTISSEMENTS** 1. Cocher cette option peut dégrader les performances de votre HA. 2. Seules les connexions passent sur le lien HA et non leurs contenus.
Configurer la synchronisation Unicast plutôt que la synchronisation Multicast	Cette option permet de configurer une synchronisation *Unicast* entre les membres d'un cluster lors de sa création. Elle est **nécessaire** pour déployer la haute disponibilité dans un environnement ne supportant pas le protocole *Multicast* comme certaines plate-formes d'hébergement dans le *Cloud*.

Optimisation du basculement

Activer l'agrégation de liens lorsque le firewall est passif	Lorsque l'option est active, dans une configuration utilisant des agrégats de liens (LACP), les agrégats sont activés même sur le membre passif du cluster. Cette case est cochée par défaut.

Cliquez sur **Suivant**.

En cas de cluster existant

Adresse IP du firewall à contacter	Entrez l'adresse IP que vous avez défini dans l'assistant lors de la création du cluster (adresse IP du lien principal ou secondaire).
Clé pré partagée	Entrez le mot de passe / la clé pré partagée que vous avez défini dans l'assistant lors de la création du cluster. Cette icône permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

Étape 4 : Résumé et finalisation du cluster

En cas de création de cluster

Après avoir visualisé le résumé de vos configurations, cliquez sur **Terminer**, le message suivant s'affiche :
Ce firewall est prêt à fonctionner en haute disponibilité. Vous pouvez maintenant configurer un autre firewall pour qu'il rejoigne ce cluster.

Il indique également si la case **Déployer le cluster dans un environnement Cloud** a été cochée.

Votre cluster étant désormais créé, un nouvel écran s'affichera lorsque vous tenterez d'accéder au module.

En cas de cluster existant

Après avoir visualisé le résumé de vos configurations, cliquez sur **Terminer**, le message suivant s'affiche :

Rejoindre le groupe de firewalls nécessite le redémarrage de ce firewall. Êtes-vous sûr de vouloir rejoindre le cluster ?

Pour finaliser la configuration, ce firewall va rejoindre le cluster et réaliser la synchronisation de configuration initiale. Il va ensuite redémarrer afin de l'appliquer. Pour accéder au cluster, vous devrez vous connecter au firewall actif.

NOTE
Cette étape peut être longue sur les modèles d'entrée de gamme. Il ne faut pas débrancher le firewall.

Écran de la Haute disponibilité

Communication entre les firewalls du cluster

Lien principal	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante
Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster.
Lien secondaire	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez parmi les objets figurant au sein de la liste déroulante.

AVERTISSEMENT
Il est conseillé d'utiliser un lien secondaire lorsque l'on souhaite changer l'interface utilisée en tant que lien principal. En effet, le changement de lien peut provoquer une coupure de la communication entre les membres du cluster, pouvant résulter en un cluster non fonctionnel.

Configuration avancée

Modifier la clé pré-partagée entre les firewalls du cluster

Clé pré-partagée du cluster	Ce champ permet de modifier la clé pré-partagée ou le mot de passe défini lors de la création du cluster.
Confirmer	Confirmation du mot de passe / clé pré-partagée, que vous venez de renseigner dans le champ précédent.
Robustesse du mot de passe	Cette jauge indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Indicateur de qualité

Firewall actif en cas d'égalité

Cette option permet de favoriser un firewall comme actif lorsque les 2 ont le même niveau de qualité.

Le but de privilégier un firewall actif est de conserver au maximum les logs sur le même firewall ou de favoriser le trafic sur un firewall spécifique. Si l'actif tombe en panne, ou si un câble se fait débrancher, l'autre passera actif.

Automatique	Si vous choisissez cette option, aucune priorité n'est affectée.
Ce firewall (<son numéro de série>)	En choisissant cette option, vous positionnerez ce firewall comme actif et le second le relaiera si celui tombe en panne ou est débranché.

L'autre firewall (distant) (<son numéro de série>)	En choisissant cette option, vous positionnerez le firewall distant comme actif et celui-ci le relaiera si il tombe en panne ou est débranché. **AVERTISSEMENT** Le choix de cette option va provoquer un swap immédiat, ou basculement de ce firewall en tant que firewall actif, entraînant une déconnexion de l'interface d'administration.

Synchronisation de sessions

Activer la synchronisation selon la durée des connexions	Cette option permet de déclencher la synchronisation des sessions selon la durée de celles-ci. Seules les connexions dont la durée est supérieure ou égale à la valeur précisée dans le champ **Durée minimale des connexions à synchroniser (secondes)** seront synchronisées. Les sessions dont la durée est inférieure à cette valeur seront ignorées lors d'une synchronisation. Cette option permet ainsi d'éviter de synchroniser des connexions très brèves et pouvant être très nombreuses, comme les requêtes DNS par exemple.
Durée minimale des connexions à synchroniser (secondes).	Précisez la durée minimale (en secondes) des connexions devant être synchronisées. La valeur 0 correspond à la désactivation de cette option.

Optimisation du basculement

Cette option accélère notamment la prise en compte de la bascule d'un cluster en mode bridge par les équipements environnants.

Redémarrer toutes les interfaces pendant le basculement (à l'exception des interfaces HA)	Si l'option est active, les interfaces du bridge sont réinitialisées au moment de la bascule pour forcer les commutateurs connectés au firewall à renouveler leur table ARP.
Activer l'agrégation de liens lorsque le firewall est passif	Lorsque l'option est active, dans une configuration utilisant des agrégats de liens (LACP), les agrégats sont activés même sur le membre passif du cluster.
Transmettre périodiquement des requêtes ARP gratuites	En cochant cette case, vous enverrez, à intervalles réguliers, des annonces ARP, afin que les différents éléments du réseau (commutateurs, routeurs, ...) puissent mettre à jour leurs propres tables ARP. **NOTE** Lors du passage actif, le firewall enverra tout de même une annonce ARP, indifféremment de cette option
Fréquence (en secondes)	Ce champ permet de définir la fréquence en secondes des requêtes ARP, dans la limite 9999 secondes maximum.

Forcer la synchronisation des adresses MAC	Cette option permet de choisir si la synchronisation des adresses MAC doit être forcée lors d'une bascule du cluster. L'activation ou la désactivation de cette synchronisation est immédiate. La synchronisation des adresses MAC est activée par défaut sur les firewalls physiques et désactivée par défaut sur les machines virtuelles (EVA). Il peut être nécessaire de désactiver cette option dans des configurations utilisant les agrégats de liens (LACP) par exemple.

Impact de l'indisponibilité d'une interface dans l'indicateur de qualité d'un firewall

Interface	Cette colonne liste toutes les interfaces Ethernet de votre firewall.
Poids [0-9999]	Le poids permet de donner une valeur relative à l'interface. Le nombre « 100 » a été donné par défaut aux interfaces listées. Elles sont donc toutes d'égale importance. Vous pouvez modifier ce critère en sélectionnant la case voulue et spécifier, par exemple, que l'interface « in » est plus importante que l'interface « out » et les autres interfaces en lui attribuant le nombre 150. **NOTE** Il peut être intéressant de placer les interfaces inutilisées à 0, afin qu'elles n'entrent pas en compte dans le calcul de la qualité.

NOTE
Les interfaces réseau désactivées ne sont pas prises en compte dans les calculs de qualité de la haute disponibilité.

Cliquez ensuite sur **Appliquer**

INTERFACES

Le module **Interfaces** permet de gérer, ajouter, supprimer des éléments réseaux appelés "interfaces réseau". Ils représentent des éléments physiques ou non de communication entre les différents réseaux qui transitent par le firewall.

L'écran du module se compose d'une grille contenant :

- La liste des interfaces du firewall et leurs informations.
- Une barre des tâches : elle affiche les différentes actions possibles sur les interfaces.
- Le panneau de configuration d'une interface : il s'affiche lors de l'édition d'une interface.

NOTE
Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

La grille des interfaces

Interface	Nom de l'interface (in, out, dmz1, ...). Au survol avec la souris, une info bulle affiche des informations complémentaires. L'icône signale l'interface par laquelle l'administrateur est connecté. L'icône signale l'interface en cours d'édition (panneau de configuration ouvert).
Port	Numéro de port physique de l'interface. Dans le cas d'un VLAN ou d'un modem, le numéro de port de l'interface parente s'affiche.
Type	Type de l'interface (Bridge, Ethernet, ...). Des informations complémentaires peuvent être affichées avec le type (taux de transfert, identifiant de VLAN, ...).
État	États particuliers d'une interface (désactivée, non connectée, supervisée, ...). Lorsque l'interface est activée et connectée, cette colonne est vide.
Adresse IPv4	Adresse IPv4 de l'interface et son masque, ou DHCP lorsque l'interface est en adressage dynamique.
Adresse IPv6	Adresse IPv6 de l'interface et son masque, ou DHCP lorsque l'interface est en adressage dynamique. Cette colonne est masquée par défaut si l'IPv6 n'est pas activé dans la configuration du firewall.
Adresse MAC	Adresse physique (MAC) de l'interface. Cette colonne est masquée par défaut.
Nom système	Nom de l'interface vue par le système d'exploitation du firewall (em0, vlan0, ...). Cette colonne est masquée par défaut.
Commentaire	Commentaire ajouté lors de la configuration de l'interface (texte libre).

Les actions possibles

Certaines actions peuvent également être réalisées en effectuant un clic droit dans la grille des interfaces. Un glisser-déposer sur une interface modifie sa configuration (ses relations et son adresse IP). Une icône signale si le glisser-déposer est autorisé.

Entrer un filtre	Effectue une recherche parmi les interfaces du firewall.

Tout réduire	Regroupe l'arborescence des interfaces.
Tout déplier	Déplie l'arborescence des interfaces.
Rafraîchir les données affichées	Actualise les informations présentées dans la grille des interfaces.
Éditer	Permet d'éditer l'interface réseau sélectionnée ou l'un des deux profils de modem.
Ajouter	Ajoute une nouvelle interface. Les sections suivantes expliquent comment ajouter une nouvelle interface ou modifier la configuration d'une interface existante.
Supprimer	Supprime l'interface sélectionnée. Certaines interfaces ne peuvent pas être supprimées.
Superviser	Active ou désactive la supervision de l'interface sélectionnée. Les graphiques correspondants sont automatiquement créés dans le module **Monitoring > Supervision > Interfaces**.
Accéder à la supervision	Redirige vers le module **Monitoring > Supervision > Interfaces**.
Vérifier l'utilisation	Affiche dans le menu de gauche les modules où l'interface est utilisée.

Le panneau de configuration d'une interface

Le panneau de configuration d'une interface permet de la configurer. Un double-clic sur une interface permet de l'afficher. Son contenu est différent selon le type d'interface sélectionnée.

- Bridge,
- Interface Ethernet,
- Interface Wi-Fi,
- VLAN,
- Agrégat,
- Interface GRETAP,
- Modem PPPoE / PPTP,
- Interface USB / Ethernet (pour clé USB / Modem).

Interface Bridge

Ajouter un bridge

Ajouter un bridge sans membre

1. Cliquez sur **Ajouter**.
2. Positionnez votre souris sur **Bridge**.
3. Cliquez sur **Sans membre**.
4. Nommez le nouveau bridge et cliquez sur **Appliquer**.
   Le nouveau bridge est ajouté aux interfaces et son panneau de configuration s'affiche.

Ajouter un bridge contenant des interfaces pré-sélectionnées

1. Sélectionnez au préalable les interfaces à inclure dans le nouveau bridge.
2. Cliquez sur **Ajouter**.
3. Positionnez votre souris sur **Bridge**.
4. Cliquez sur **Avec *interface_1*, *interface_2* ...**.
5. Nommez le nouveau bridge et cliquez sur **Appliquer**.
   Le nouveau bridge est ajouté aux interfaces et son panneau de configuration s'affiche.

Panneau de configuration d'un bridge

Pour ouvrir le panneau de configuration d'une interface bridge, faites un double-clic dessus. Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

Paramètres généraux

Nom	Nom de l'interface. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour l'interface.

Plan d'adressage

> **NOTE**
> Les champs **Adresse IPv4** et **Adresse IPv6** comportent les mêmes options à configurer. Le champ **Adresse IPv6** apparaît seulement si l'IPv6 est activé dans la configuration du firewall.

IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Gestion des membres

Vous devez sélectionner au moins deux interfaces qui composeront le bridge. Pour ajouter ou retirer des membres du bridge, déplacez les interfaces d'un cadre à un autre en utilisant les flèches, en effectuant un glisser-déposer ou en double-cliquant sur l'interface.

Onglet Configuration du routage (IPv6 seulement)

NOTE
Cet onglet apparaît seulement si l'IPv6 est activé dans la configuration du firewall.

Sur chaque interface, bridge ou interface agrégée, les messages d'annonces du routeur (*Router Advertisement* - RA) peuvent être envoyés périodiquement à tous les nœuds IPv6 (*multicast*) du segment via l'adresse de la liaison locale ou en réponse à la sollicitation de routeur (*Routeur Sollicitation* - RS) d'une machine du réseau.

Cette annonce permet à un nœud IPv6 d'obtenir les informations suivantes :

- L'adresse du routeur par défaut, en l'occurrence celle du firewall,
- Le(s) préfixe(s) utilisé(s) sur le lien (en 64bits),
- L'indication de l'utilisation de l'auto-configuration sans état (*SLAAC*) ou du DHCPv6 (*Managed*),
- L'indication de récupérer d'autres paramètres via DHCPv6 (*OtherConfig*),
- D'éventuels paramètres DNS (RFC4862).

L'auto-configuration, native dans IPv6 est sans état (*Stateless Address Autoconfiguration* - SLAAC), c'est-à-dire que le serveur ne choisit pas les IPs des clients et n'a pas à les retenir.

Une machine a une adresse de liaison locale dont l'unicité a été vérifiée via NPD DAD (protocole *Neighbor Discovery Protocol - Duplicated Address Detection*) avec succès. La machine reçoit ensuite l'annonce du routeur (RA) périodique ou sollicitée. Si l'information d'auto-configuration sans état est spécifiée, la machine se construit alors une ou plusieurs adresses IPv6 à partir du ou des préfixe(s) annoncé(s) et de son identifiant d'interface (aléatoire ou basé sur l'adresse MAC). L'adresse IP du routeur (celle du firewall) servira alors de passerelle par défaut.

Par défaut, le mode d'émission des annonces de routeur (RA) diffuse le premier préfixe déduit de l'interface. Les serveurs DNS sont par défaut ceux configurés pour le firewall dans le module **Configuration > Système > Configuration**, onglet **Paramètres réseau**.

NOTE
Si les annonces de routeur sont activées sur un bridge, ces annonces sont uniquement diffusées sur les interfaces protégées.

Paramètres d'autoconfiguration

Émettre les RA si DHCPv6 activé	Si le service DHCPv6 est activé sur le firewall (module **Configuration > Réseau > DHCP**), le firewall va émettre automatiquement des annonces (Router Advertisement – RA) sur les interfaces correspondantes, indiquant aux nœuds IPv6 de s'auto-configurer en DHCPv6 (les options Managed et Other config sont alors activées par défaut). Si le firewall fait office de serveur DHCPv6, l'interface configurée doit appartenir à l'une des plages d'adresses renseignées en configuration DHCPv6. Si le firewall sert de relai à un serveur DHCPv6, l'interface configurée doit appartenir à la liste des interfaces d'écoute du service. Si le service DHCPv6 n'est pas actif, l'émission des RA est désactivée.
Émettre les RA	L'adresse du firewall est envoyée comme routeur par défaut. Les informations relayées par cette annonce sont décrites ci-après. Cette configuration est recommandée afin de permettre aux machines directement connectées (lien local) de faire du SLAAC.
Désactiver	Aucune annonce de routeur (RA) n'est diffusée. Cette configuration est recommandée en bridge si un routeur IPv6 est directement connecté (lien local).

Annonces du routeur (RA)

Cette zone est accessible seulement si l'option **Émettre les RA** est sélectionnée.

Annoncer le préfixe déduit de l'interface	Le préfixe annoncé est celui configuré dans le plan d'adressage IPv6 de l'interface dans l'onglet **Configuration générale**. La taille du masque (longueur du préfixe - CIDR) de l'adresse IPv6 configurée doit obligatoirement être de 64 bits.

Configuration avec serveur DHCPv6

Le serveur DHCPv6 délivre les adresses (Managed)	L'annonce indique que les adresses IPv6 sollicitées seront distribuées par le service DHCPv6 activé sur le firewall (module **Configuration > Réseau > DHCP**). Ce service est mis en œuvre par le firewall ou un relai directement connecté (lien local).
Le serveur DHCPv6 délivre des options supplémentaires (Other config)	L'annonce indique que les autres paramètres d'auto-configuration tels que les adresses de serveurs DNS ou un autre type de serveur, seront délivrés par le serveur DHCPv6 (firewall ou relai) directement connecté (lien local).

Configuration avancée

Paramètres DNS

Ce cadre est accessible si l'option **Le serveur DHCPv6 délivre des options supplémentaires (Other config)** n'est pas activée.

Nom de domaine	Nom de domaine par défaut pour joindre un serveur interrogé sans domaine.
Serveur DNS primaire	Adresse IP du serveur DNS primaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).
Serveur DNS secondaire	Adresse IP du serveur DNS secondaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).

Préfixes annoncés

Cette grille est accessible si l'option **Le serveur DHCPv6 délivre les adresses (Managed)** n'est pas activée.

Préfixes	Préfixe à annoncer aux machines. Il est préconisé que le préfixe annoncé soit le même que celui de l'interface. Dans le cas où l'interface en spécifie plusieurs, ce champ précise le préfixe à utiliser.
Autonomous	Instruction d'auto-configuration sans état (SLAAC) : si cette case est cochée, la machine se construit une ou plusieurs adresses IPv6 à partir du préfixe annoncé et d'un identifiant d'interface (aléatoire et/ou basé sur l'adresse MAC).
On link	Cette option précise à la machine que toutes les machines ayant le même préfixe peuvent être joignables directement, sans passer par le routeur. En IPv4, cette information était déduite du masque réseau.
Commentaire	Permet de donner un commentaire au préfixe annoncé.

Onglet Configuration avancée

Autres paramètres

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse MAC	Permet de spécifier une adresse MAC pour le bridge.
Adresse MAC physique	Ce champ n'est pas disponible pour un bridge.

Détection de boucles (Spanning Tree)

Ce cadre permet d'activer l'utilisation d'un protocole de détection des boucles réseau (*Spanning Tree*) sur le bridge. Cette fonctionnalité est uniquement disponible sur les modèles SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200, SNi10, SNi20, SNi40, SNxr1200, EVA1, EVA2, EVA3, EVA4 et EVAU.

Désactiver les protocoles Spanning Tree	Désactive l'utilisation des protocoles Spanning Tree (RSTP et MSTP) au niveau du bridge. Cette case est cochée par défaut.
Activer le protocole Rapid Spanning Tree (RSTP)	Active le protocole Rapid Spanning Tree (RSTP) au niveau du bridge.
Activer le protocole Multiple Spanning Tree (MSTP)	Active le protocole Multiple Spanning Tree (MSTP) au niveau du bridge. En cochant cette case, la zone **Configuration MSTP** apparaît.

Configuration MSTP

Cette zone apparaît seulement si la case **Activer le protocole Multiple Spanning Tree (MSTP)** est cochée. Sur un firewall SNS, une configuration MSTP ne peut définir qu'une seule région.

Nom de la région (MSTP region)	Saisissez le nom de la région MSTP dans laquelle se situe le firewall. Il doit être identique dans la configuration MSTP de tous les équipements réseau appartenant à cette région.

Sélecteur de format	Ce champ précise les informations nécessaires à la définition d'une région. Sa valeur par défaut est 0, indiquant qu'une région est caractérisée par : • Son nom, • Son numéro de révision, • Une empreinte calculée en fonction des numéros d'instances MST et des identifiants de VLAN inclus dans ces instances. Le sélecteur de format doit être identique dans la configuration MSTP de tous équipements réseau appartenant à cette région.
Numéro de révision	Choisissez un numéro de révision pour la région. Le numéro de révision doit être identique dans la configuration MSTP de tous équipements réseau appartenant à cette région. **NOTE** Afin d'assurer un meilleur suivi des modifications, le numéro de révision peut être incrémenté manuellement lorsque la configuration de la région évolue. Dans ce cas, il est impératif que ce changement du numéro de révision soit répété à l'identique sur l'ensemble des équipements de la région concernée.
Common and Internal Spanning Tree (CIST)	Priorité affectée au firewall pour le transit des VLAN qui ne sont pas déclarés dans une instance MSTP (voir la grille **Instances MSTP**).

Instances MSTP

Liste des identifiants des VLANs de l'instance	Indiquez les différents identifiants de VLAN (liste d'identifiants séparés par une virgule) inclus dans l'instance sélectionnée.
Priorité	Définissez la priorité d'une instance MSTP par rapport au pont racine. Le pont racine est celui qui a la priorité la plus basse. **NOTE** Il est déconseillé de déclarer le firewall comme pont racine d'une instance MSTP. Cela pourrait en effet aboutir à un transit réseau important et inutile sur les interfaces du firewall.

Interface Ethernet

Vous pouvez modifier les paramètres de chaque interface Ethernet, mais il n'est pas possible d'en ajouter ou d'en supprimer. Dans le cas où une interface Ethernet est membre d'un :

- Bridge : certains champs du panneau de configuration de l'interface ne sont pas modifiables (grisés) du fait qu'ils sont hérités du bridge.
- Agrégat : seuls les champs **État**, **Nom**, **Commentaire** et **Média** sont visibles. Les autres paramètres sont hérités de la configuration de l'agrégat.

Panneau de configuration d'une interface Ethernet

Pour ouvrir le panneau de configuration d'une interface Ethernet, faites un double-clic dessus. Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface. Désactiver une interface la rend inutilisable. Une interface désactivée (car non utilisée, déployée ultérieurement, ...) est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom	Nom de l'interface. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Plan d'adressage

Plan d'adressage hérité du bridge	En choisissant cette option, l'interface fait partie d'un bridge. Plusieurs paramètres sont alors hérités du bridge (comme le plan d'adressage). Ce choix débloque l'accès au champ **Bridge**. Sélectionnez dans ce champ le bridge parent de l'interface.
Dynamique / Statique	En choisissant cette option, vous indiquez que l'adresse IP de l'interface est dynamique (obtenue par DHCP) ou fixe (statique). Ce choix débloque l'accès au champ **Adresse IPv4** ainsi qu'au champ **Adresse IPv6** si l'IPv6 est activé dans la configuration du firewall. Ils comportent les mêmes options à configurer.

IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.
IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Onglet Configuration du routage (IPv6 seulement)

> **NOTE**
> Cet onglet apparaît seulement si l'IPv6 est activé dans la configuration du firewall.

Sur chaque interface, bridge ou interface agrégée, les messages d'annonces du routeur (*Router Advertisement* - RA) peuvent être envoyés périodiquement à tous les nœuds IPv6 (*multicast*) du segment via l'adresse de la liaison locale ou en réponse à la sollicitation de routeur (*Routeur Sollicitation* - RS) d'une machine du réseau.

Cette annonce permet à un nœud IPv6 d'obtenir les informations suivantes :

- L'adresse du routeur par défaut, en l'occurrence celle du firewall,
- Le(s) préfixe(s) utilisé(s) sur le lien (en 64bits),
- L'indication de l'utilisation de l'auto-configuration sans état (*SLAAC*) ou du DHCPv6 (*Managed*),
- L'indication de récupérer d'autres paramètres via DHCPv6 (*OtherConfig*),
- D'éventuels paramètres DNS (RFC4862).

L'auto-configuration, native dans IPv6 est sans état (*Stateless Address Autoconfiguration* - SLAAC), c'est-à-dire que le serveur ne choisit pas les IPs des clients et n'a pas à les retenir.

Une machine a une adresse de liaison locale dont l'unicité a été vérifiée via NPD DAD (protocole *Neighbor Discovery Protocol - Duplicated Address Detection*) avec succès. La machine reçoit ensuite l'annonce du routeur (RA) périodique ou sollicitée. Si l'information d'auto-configuration sans état est spécifiée, la machine se construit alors une ou plusieurs adresses IPv6 à partir du ou des préfixe(s) annoncé(s) et de son identifiant d'interface (aléatoire ou basé sur l'adresse MAC). L'adresse IP du routeur (celle du firewall) servira alors de passerelle par défaut.

Par défaut, le mode d'émission des annonces de routeur (RA) diffuse le premier préfixe déduit de l'interface. Les serveurs DNS sont par défaut ceux configurés pour le firewall dans le module **Configuration > Système > Configuration**, onglet **Paramètres réseau**.

NOTE
Si les annonces de routeur sont activées sur un bridge, ces annonces sont uniquement diffusées sur les interfaces protégées.

Paramètres d'autoconfiguration

Émettre les RA si DHCPv6 activé	Si le service DHCPv6 est activé sur le firewall (module **Configuration > Réseau > DHCP**), le firewall va émettre automatiquement des annonces (Router Advertisement – RA) sur les interfaces correspondantes, indiquant aux nœuds IPv6 de s'auto-configurer en DHCPv6 (les options Managed et Other config sont alors activées par défaut). Si le firewall fait office de serveur DHCPv6, l'interface configurée doit appartenir à l'une des plages d'adresses renseignées en configuration DHCPv6. Si le firewall sert de relai à un serveur DHCPv6, l'interface configurée doit appartenir à la liste des interfaces d'écoute du service. Si le service DHCPv6 n'est pas actif, l'émission des RA est désactivée.
Émettre les RA	L'adresse du firewall est envoyée comme routeur par défaut. Les informations relayées par cette annonce sont décrites ci-après. Cette configuration est recommandée afin de permettre aux machines directement connectées (lien local) de faire du SLAAC.
Désactiver	Aucune annonce de routeur (RA) n'est diffusée. Cette configuration est recommandée en bridge si un routeur IPv6 est directement connecté (lien local).

Annonces du routeur (RA)

Cette zone est accessible seulement si l'option **Émettre les RA** est sélectionnée.

Annoncer le préfixe déduit de l'interface	Le préfixe annoncé est celui configuré dans le plan d'adressage IPv6 de l'interface dans l'onglet **Configuration générale**. La taille du masque (longueur du préfixe - CIDR) de l'adresse IPv6 configurée doit obligatoirement être de 64 bits.

Configuration avec serveur DHCPv6

Le serveur DHCPv6 délivre les adresses (Managed)	L'annonce indique que les adresses IPv6 sollicitées seront distribuées par le service DHCPv6 activé sur le firewall (module **Configuration > Réseau > DHCP**). Ce service est mis en œuvre par le firewall ou un relai directement connecté (lien local).
Le serveur DHCPv6 délivre des options supplémentaires (Other config)	L'annonce indique que les autres paramètres d'auto-configuration tels que les adresses de serveurs DNS ou un autre type de serveur, seront délivrés par le serveur DHCPv6 (firewall ou relai) directement connecté (lien local).

Configuration avancée

Paramètres DNS

Ce cadre est accessible si l'option **Le serveur DHCPv6 délivre des options supplémentaires (Other config)** n'est pas activée.

Nom de domaine	Nom de domaine par défaut pour joindre un serveur interrogé sans domaine.
Serveur DNS primaire	Adresse IP du serveur DNS primaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).
Serveur DNS secondaire	Adresse IP du serveur DNS secondaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).

Préfixes annoncés

Cette grille est accessible si l'option **Le serveur DHCPv6 délivre les adresses (Managed)** n'est pas activée.

Préfixes	Préfixe à annoncer aux machines. Il est préconisé que le préfixe annoncé soit le même que celui de l'interface. Dans le cas où l'interface en spécifie plusieurs, ce champ précise le préfixe à utiliser.
Autonomous	Instruction d'auto-configuration sans état (SLAAC) : si cette case est cochée, la machine se construit une ou plusieurs adresses IPv6 à partir du préfixe annoncé et d'un identifiant d'interface (aléatoire et/ou basé sur l'adresse MAC).
On link	Cette option précise à la machine que toutes les machines ayant le même préfixe peuvent être joignables directement, sans passer par le routeur. En IPv4, cette information était déduite du masque réseau.
Commentaire	Permet de donner un commentaire au préfixe annoncé.

Onglet Configuration avancée

Autres paramètres

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse MAC	Permet de spécifier une adresse MAC pour l'interface plutôt que d'utiliser l'adresse allouée par le firewall (adresse MAC physique par défaut). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse MAC physique	Adresse MAC matérielle de la carte réseau.

Média

Média	Vitesse de liaison du réseau. Par défaut, le firewall détecte le média automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier en le sélectionnant dans la liste déroulante. **IMPORTANT** Si le firewall est directement connecté à un modem ADSL, Stormshield Network vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.

Routage sans analyse

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Autoriser sans analyser	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).

Routage par interface

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Préserver le routage initial	Cette option demande au firewall de ne pas modifier la destination dans la couche Ethernet lorsqu'un paquet le traverse. Le paquet sera réémis à destination de la même adresse MAC qu'à la réception. Le but de cette option est de faciliter l'intégration des firewalls dans un réseau existant de manière transparente, car elle permet de ne pas avoir à modifier la route par défaut des machines du réseau interne. Cette option doit être activée pour assurer le bon fonctionnement d'un serveur DHCP situé sur l'interface considérée et dont les réponses aux requêtes sont de type unicast. **LIMITATIONS CONNUES** Les fonctionnalités du firewall qui insèrent ou modifient des paquets dans les sessions par le firewall pourraient ne pas fonctionner correctement. Ces fonctionnalités sont : • La réinitialisation des connexions induite par une alarme, • Le proxy SYN (activé dans le filtrage), • La demande de réémission de paquets perdus afin d'accélérer l'analyse, • La réécriture de paquets par les analyses applicatives (SMTP, HTTP et web 2.0, FTP et NAT, SIP et NAT).
Préserver les identifiants de Vlan	Cette option permet la transmission des trames taguées sans que le firewall soit une terminaison du VLAN. Le tag VLAN de ces trames est conservé ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN. Cette option requiert l'activation de l'option précédente "**Préserver le routage initial**".

Interface Wi-Fi (WLAN)

Certains firewalls embarquent une carte Wi-Fi permettant de configurer deux points d'accès WLAN pour la connexion des équipements sans fil sur les bandes de fréquence à 2,4 GHz ou 5 GHz. Vous pouvez modifier les paramètres de chaque interface Wi-Fi, mais il n'est pas possible d'en ajouter ou d'en supprimer.

Panneau de configuration d'une interface Wi-Fi

Pour ouvrir le panneau de configuration d'une interface Wi-Fi, faites un double-clic dessus.

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface. Désactiver une interface Wi-Fi la rend inutilisable même si le réseau Wi-Fi est activé dans la configuration du firewall. À l'inverse, si l'interface Wi-Fi est activée mais que le réseau Wi-Fi est désactivé, le réseau ne sera pas joignable. Assurez-vous de faire coïncider le paramètre d'activation de l'interface Wi-Fi avec le paramètre d'activation du réseau Wi-Fi (module **Configuration** > **Réseau** > Wi-Fi).

Paramètres généraux

Nom	Nom de l'interface. Vous pouvez modifier le nom attribué par défaut si souhaité. Ce nom ne correspond pas au nom du réseau (SSID).
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Wi-Fi

Nom du réseau	Affiche le nom du réseau Wi-Fi (SSID). Vous pouvez le modifier si besoin.
Authentification	Affiche le type de sécurité utilisé pour l'authentification sur le réseau Wi-Fi. Trois choix sont possibles : • **Réseau ouvert** : aucune authentification. Lorsque vous cochez cette case, les champs **Clé de sécurité** sont masqués. • **WPA** (Wi-Fi Protected Access). • **WPA 2** : WPA 2 est une évolution de WPA présentant un niveau de sécurité plus élevé.
Clé de sécurité	Permet de modifier ou d'afficher la clé de sécurité du réseau Wi-Fi. Pour l'afficher, cliquez sur le bouton à droite du champ. Pour modifier la clé, saisissez la nouvelle clé dans ce champ, puis confirmez-la dans le champ **Confirmer la clé de sécurité**. Une jauge indique la robustesse de la clé de sécurité choisie.
Isolation AP	Cette fonctionnalité permet d'interdire à deux équipements connectés au réseau Wi-Fi de dialoguer directement entre eux sans passer par le firewall. Cette option est activée par défaut sur le point d'accès Wi-Fi publique. Elle doit être désactivée dans le cas d'un réseau Wi-Fi privé mettant en lien, par exemple, des postes de travail et une imprimante réseau connectés en Wi-Fi.

Plan d'adressage

Plan d'adressage hérité du bridge	En choisissant cette option, l'interface fait partie d'un bridge. Plusieurs paramètres sont alors hérités du bridge (comme le plan d'adressage). Ce choix débloque l'accès au champ **Bridge**. Sélectionnez dans ce champ le bridge parent de l'interface.
Dynamique / Statique	En choisissant cette option, vous indiquez que l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Interface VLAN

Ajouter un VLAN

Ajouter un VLAN sans membre

1. Cliquez sur **Ajouter**.
2. Positionnez votre souris sur **VLAN**.
3. Cliquez sur **Sans membre**.
   Le nouveau VLAN est ajouté aux interfaces et son panneau de configuration s'affiche.

Ajouter un VLAN contenant des interfaces pré-sélectionnées

1. Sélectionnez au préalable les interfaces à inclure dans le nouveau VLAN.
2. Cliquez sur **Ajouter**.
3. Positionnez votre souris sur **VLAN**.
4. Cliquez sur **Avec *interface_1*, *interface_2* ....**
   Le nouveau VLAN est ajouté aux interfaces et son panneau de configuration s'affiche.

Panneau de configuration d'une interface VLAN

Pour ouvrir le panneau de configuration d'une interface VLAN, faites un double-clic dessus. Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface. Désactiver une interface la rend inutilisable. Une interface désactivée (car non utilisée, déployée ultérieurement, ...) est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom	Nom de l'interface. Vous pouvez modifier le nom attribué par défaut si souhaité.

Commentaire	Permet de donner un commentaire pour l'interface.
Interface parente	Nom physique de l'interface à laquelle est attaché le VLAN.
Identifiant	L'identifiant du VLAN doit être compris entre 1 et 4094 et doit être unique (sauf s'il s'agit d'un VLAN associé à un autre bridge dans un VLAN traversant).
Priorité (CoS)	Cette priorité de type CoS (champ **Classe de Service**) sera forcée sur tous les paquets émis par le VLAN.
Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Plan d'adressage

Plan d'adressage hérité du bridge	En choisissant cette option, l'interface fait partie d'un bridge. Plusieurs paramètres sont alors hérités du bridge (comme le plan d'adressage). Ce choix débloque l'accès au champ **Bridge**. Sélectionnez dans ce champ le bridge parent de l'interface.
Dynamique / Statique	En choisissant cette option, vous indiquez que l'adresse IP de l'interface est dynamique (obtenue par DHCP) ou fixe (statique). Ce choix débloque l'accès au champ **Adresse IPv4** ainsi qu'au champ **Adresse IPv6** si l'IPv6 est activé dans la configuration du firewall. Ils comportent les mêmes options à configurer.
IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Onglet Configuration du routage (IPv6 seulement)

NOTE
Cet onglet apparaît seulement si l'IPv6 est activé dans la configuration du firewall.

Sur chaque interface, bridge ou interface agrégée, les messages d'annonces du routeur (*Router Advertisement* - RA) peuvent être envoyés périodiquement à tous les nœuds IPv6 (*multicast*) du segment via l'adresse de la liaison locale ou en réponse à la sollicitation de routeur (*Routeur Sollicitation* - RS) d'une machine du réseau.

Cette annonce permet à un nœud IPv6 d'obtenir les informations suivantes :

- L'adresse du routeur par défaut, en l'occurrence celle du firewall,
- Le(s) préfixe(s) utilisé(s) sur le lien (en 64bits),
- L'indication de l'utilisation de l'auto-configuration sans état (*SLAAC*) ou du DHCPv6 (*Managed*),
- L'indication de récupérer d'autres paramètres via DHCPv6 (*OtherConfig*),
- D'éventuels paramètres DNS (RFC4862).

L'auto-configuration, native dans IPv6 est sans état (*Stateless Address Autoconfiguration* - SLAAC), c'est-à-dire que le serveur ne choisit pas les IPs des clients et n'a pas à les retenir.

Une machine a une adresse de liaison locale dont l'unicité a été vérifiée via NPD DAD (protocole *Neighbor Discovery Protocol - Duplicated Address Detection*) avec succès. La machine reçoit ensuite l'annonce du routeur (RA) périodique ou sollicitée. Si l'information d'auto-configuration sans état est spécifiée, la machine se construit alors une ou plusieurs adresses IPv6 à partir du ou des préfixe(s) annoncé(s) et de son identifiant d'interface (aléatoire ou basé sur l'adresse MAC). L'adresse IP du routeur (celle du firewall) servira alors de passerelle par défaut.

Par défaut, le mode d'émission des annonces de routeur (RA) diffuse le premier préfixe déduit de l'interface. Les serveurs DNS sont par défaut ceux configurés pour le firewall dans le module **Configuration > Système > Configuration**, onglet **Paramètres réseau**.

NOTE
Si les annonces de routeur sont activées sur un bridge, ces annonces sont uniquement diffusées sur les interfaces protégées.

Paramètres d'autoconfiguration

Émettre les RA si DHCPv6 activé	Si le service DHCPv6 est activé sur le firewall (module **Configuration > Réseau > DHCP**), le firewall va émettre automatiquement des annonces (Router Advertisement – RA) sur les interfaces correspondantes, indiquant aux nœuds IPv6 de s'auto-configurer en DHCPv6 (les options Managed et Other config sont alors activées par défaut). Si le firewall fait office de serveur DHCPv6, l'interface configurée doit appartenir à l'une des plages d'adresses renseignées en configuration DHCPv6. Si le firewall sert de relai à un serveur DHCPv6, l'interface configurée doit appartenir à la liste des interfaces d'écoute du service. Si le service DHCPv6 n'est pas actif, l'émission des RA est désactivée.
Émettre les RA	L'adresse du firewall est envoyée comme routeur par défaut. Les informations relayées par cette annonce sont décrites ci-après. Cette configuration est recommandée afin de permettre aux machines directement connectées (lien local) de faire du SLAAC.
Désactiver	Aucune annonce de routeur (RA) n'est diffusée. Cette configuration est recommandée en bridge si un routeur IPv6 est directement connecté (lien local).

Annonces du routeur (RA)

Cette zone est accessible seulement si l'option **Émettre les RA** est sélectionnée.

Annoncer le préfixe déduit de l'interface	Le préfixe annoncé est celui configuré dans le plan d'adressage IPv6 de l'interface dans l'onglet **Configuration générale**. La taille du masque (longueur du préfixe - CIDR) de l'adresse IPv6 configurée doit obligatoirement être de 64 bits.

Configuration avec serveur DHCPv6

Le serveur DHCPv6 délivre les adresses (Managed)	L'annonce indique que les adresses IPv6 sollicitées seront distribuées par le service DHCPv6 activé sur le firewall (module **Configuration > Réseau > DHCP**). Ce service est mis en œuvre par le firewall ou un relai directement connecté (lien local).
Le serveur DHCPv6 délivre des options supplémentaires (Other config)	L'annonce indique que les autres paramètres d'auto-configuration tels que les adresses de serveurs DNS ou un autre type de serveur, seront délivrés par le serveur DHCPv6 (firewall ou relai) directement connecté (lien local).

Configuration avancée

Paramètres DNS

Ce cadre est accessible si l'option **Le serveur DHCPv6 délivre des options supplémentaires (Other config)** n'est pas activée.

Nom de domaine	Nom de domaine par défaut pour joindre un serveur interrogé sans domaine.
Serveur DNS primaire	Adresse IP du serveur DNS primaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).
Serveur DNS secondaire	Adresse IP du serveur DNS secondaire. Si ce champ n'est pas renseigné, l'adresse envoyée est celle utilisée par le firewall (module **Configuration > Système > Configuration**, onglet **Paramètres réseau**).

Préfixes annoncés

Cette grille est accessible si l'option **Le serveur DHCPv6 délivre les adresses (Managed)** n'est pas activée.

Préfixes	Préfixe à annoncer aux machines. Il est préconisé que le préfixe annoncé soit le même que celui de l'interface. Dans le cas où l'interface en spécifie plusieurs, ce champ précise le préfixe à utiliser.
Autonomous	Instruction d'auto-configuration sans état (SLAAC) : si cette case est cochée, la machine se construit une ou plusieurs adresses IPv6 à partir du préfixe annoncé et d'un identifiant d'interface (aléatoire et/ou basé sur l'adresse MAC).
On link	Cette option précise à la machine que toutes les machines ayant le même préfixe peuvent être joignables directement, sans passer par le routeur. En IPv4, cette information était déduite du masque réseau.
Commentaire	Permet de donner un commentaire au préfixe annoncé.

Onglet Configuration avancée

Autres paramètres

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (sans fragmentation).
Adresse MAC physique	Adresse MAC de l'interface réseau à laquelle appartient le VLAN.

Routage sans analyse

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Autoriser sans analyser	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).

Routage par interface

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Préserver le routage initial	Cette option demande au firewall de ne pas modifier la destination dans la couche Ethernet lorsqu'un paquet le traverse. Le paquet sera réémis à destination de la même adresse MAC qu'à la réception. Le but de cette option est de faciliter l'intégration des firewalls dans un réseau existant de manière transparente, car elle permet de ne pas avoir à modifier la route par défaut des machines du réseau interne. Cette option doit être activée pour assurer le bon fonctionnement d'un serveur DHCP situé sur l'interface considérée et dont les réponses aux requêtes sont de type unicast. **LIMITATIONS CONNUES** Les fonctionnalités du firewall qui insèrent ou modifient des paquets dans les sessions par le firewall pourraient ne pas fonctionner correctement. Ces fonctionnalités sont : • La réinitialisation des connexions induite par une alarme, • Le proxy SYN (activé dans le filtrage), • La demande de réémission de paquets perdus afin d'accélérer l'analyse, • La réécriture de paquets par les analyses applicatives (SMTP, HTTP et web 2.0, FTP et NAT, SIP et NAT).
Préserver les identifiants de Vlan	Cette option permet la transmission des trames taguées sans que le firewall soit une terminaison du VLAN. Le tag VLAN de ces trames est conservé ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN. Cette option requiert l'activation de l'option précédente "**Préserver le routage initial**".

Supprimer un VLAN

Pour supprimer un VLAN :

1. Sélectionnez le VLAN dans l'arborescence des interfaces.
2. Cliquez sur le bouton **Supprimer** de la barre d'outils.
   Le message « Voulez-vous réellement supprimer cette interface ? » s'affiche.
3. Confirmez ou non votre suppression.
   En confirmant la suppression, une vérification de l'utilisation de l'interface (*check*) est faite.

Agrégat

Cette fonctionnalité est uniquement disponible sur les modèles SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200, SNi10, SNi20, SNi40 et SNxr1200. Il existe plusieurs types d'agrégat (LACP, Mode Broadcast et Redondance). Vous pouvez choisir le type souhaité dans l'onglet **Configuration avancée**.

NOTE
L'empilage de commutateurs (*stackable switches*) est recommandé car cela permet la redondance des liens entre les deux équipements.

Ajouter un agrégat

Ajouter un agrégat sans membre

1. Cliquez sur **Ajouter**.
2. Positionnez votre souris sur **Agrégat**.
3. Cliquez sur **Sans membre**.
4. Nommez le nouvel agrégat et cliquez sur **Appliquer**.
   Le nouvel agrégat est ajouté aux interfaces et son panneau de configuration s'affiche.

Ajouter un agrégat contenant des interfaces pré-sélectionnées

1. Sélectionnez au préalable les interfaces à inclure dans le nouvel agrégat.
2. Cliquez sur **Ajouter**.
3. Positionnez votre souris sur **Agrégat**.
4. Cliquez sur **Avec *interface_1*, *interface_2* ...**.
5. Nommez le nouvel agrégat et cliquez sur **Appliquer**.
   Le nouvel agrégat est ajouté aux interfaces et son panneau de configuration s'affiche.

Panneau de configuration d'un agrégat

Pour ouvrir le panneau de configuration d'un agrégat, faites un double-clic dessus. Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'agrégat.

Paramètres généraux

Nom	Nom de l'agrégat. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Plan d'adressage

Plan d'adressage hérité du bridge	En choisissant cette option, l'interface fait partie d'un bridge. Plusieurs paramètres sont alors hérités du bridge (comme le plan d'adressage). Ce choix débloque l'accès au champ **Bridge**. Sélectionnez dans ce champ le bridge parent de l'interface.
Dynamique / Statique	En choisissant cette option, vous indiquez que l'adresse IP de l'interface est dynamique (obtenue par DHCP) ou fixe (statique). Ce choix débloque l'accès au champ **Adresse IPv4**.
IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.
IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Gestion des membres

Pour ajouter ou retirer des membres de l'agrégat, déplacez les interfaces d'un cadre à l'autre en utilisant les flèches, en effectuant un glisser-déposer ou en double-cliquant sur l'interface. Une interface devenant membre d'un agrégat perd ses paramètres de configuration pour hériter de la configuration de l'agrégat (sauf le nom et le réglage Média).

Le nombre maximum de membres que peut contenir un agrégat est différent selon son type :

- **LACP** : 8 membres maximum,
- **Mode Broadcast** : 2 membres maximum,
- **Redondance** : 2 membres (dont 1 membre "*Maître*" à définir).

Le choix du type d'agrégat et du membre *Maître* s'effectuent dans l'onglet **Configuration avancée**.

Onglet Configuration avancée

Autres paramètres

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse physique (MAC)	Permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Si l'interface est contenue dans un bridge, dans ce cas, elle possède la même adresse MAC que lui.

Type d'agrégat

LACP	En sélectionnant ce choix, l'agrégat est de type LACP. La fonction d'agrégation de liens LACP (IEEE 802.3ad - Link Aggregation Control Protocol) permet d'améliorer la bande passante du firewall tout en maintenant un niveau de disponibilité élevé (redondance des liens). Plusieurs ports physiques des firewalls peuvent être regroupés pour être considérés en une unique interface logique. Ainsi, en agrégeant *n* liens, il est possible d'établir une liaison de *n* fois *x* Gbit/s entre deux équipements. **NOTE** Assurez-vous que les équipements distants utilisent le protocole LACP.
Mode Broadcast	En sélectionnant ce choix, l'agrégat est de type Mode Broadcast. Ce mode permet l'émission et la réception de paquets sur l'ensemble des liens inclus dans un agrégat. **NOTE** L'équipement qui est connecté aux interfaces agrégées en mode broadcast du firewall doit supporter ce type de communication : • Soit en ayant une interface active et la seconde passive (principal / secours), • Soit en ignorant les trames provenant d'un des 2 liens.
Redondance	En sélectionnant ce choix, l'agrégat est de type Redondance. La fonction de redondance permet de disposer d'un lien de secours au cas où le lien principal (*Maître*) ne répond plus.
Interface principale	Sélectionnez dans le menu déroulant l'interface principale. Elle apparaît en tant que *Maître* dans la liste des membres de l'agrégat dans l'onglet **Configuration générale**. Ce champ est accessible seulement si l'agrégat est de type **Redondance**.

Interface GRETAP

Les tunnels reposant sur des interfaces GRETAP permettent d'encapsuler du trafic de niveau 2 (Ethernet). Ils peuvent ainsi être utilisés pour relier au travers d'un bridge des sites partageant un même plan d'adressage IP ou pour le transport de protocoles non IP sur un bridge.

Ajouter une interface GRETAP

1. Cliquez sur **Ajouter**.
2. Cliquez sur **Interface GRETAP**.
   L'interface GRETAP est ajoutée aux interfaces et son panneau de configuration s'affiche.

Panneau de configuration d'une interface GRETAP

Pour ouvrir le panneau de configuration d'une interface GRETAP, faites un double-clic dessus. Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface. Désactiver une interface la rend inutilisable. Une interface désactivée (car non utilisée, déployée ultérieurement, ...) est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom	Nom de l'interface. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Adresse du tunnel GRETAP

Source du tunnel	Sélectionnez l'objet réseau correspondant au bridge qui supporte l'interface GRETAP.
Destination du tunnel	Sélectionnez (ou créez) l'objet réseau correspondant à l'adresse publique de l'équipement qui héberge l'interface GRETAP distante.

Plan d'adressage

Plan d'adressage hérité du bridge	En choisissant cette option, l'interface fait partie d'un bridge. Plusieurs paramètres sont alors hérités du bridge (comme le plan d'adressage). Ce choix débloque l'accès au champ **Bridge**. Sélectionnez dans ce champ le bridge parent de l'interface.
Dynamique / Statique	En choisissant cette option, vous indiquez que l'adresse IP de l'interface est dynamique (obtenue par DHCP) ou fixe (statique). Ce choix débloque l'accès au champ **Adresse IPv4**.

IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.
IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Onglet Configuration avancée

Autres paramètres

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse physique (MAC)	Permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Si l'interface est contenue dans un bridge, dans ce cas, elle possède la même adresse MAC que lui.

Routage sans analyse

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Autoriser sans analyser	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).

Routage par interface

Cette zone apparaît seulement si l'option **Plan d'adressage hérité du bridge** est cochée dans le champ **Adressage** de l'onglet **Configuration générale**.

Préserver le routage initial	Cette option demande au firewall de ne pas modifier la destination dans la couche Ethernet lorsqu'un paquet le traverse. Le paquet sera réémis à destination de la même adresse MAC qu'à la réception. Le but de cette option est de faciliter l'intégration des firewalls dans un réseau existant de manière transparente, car elle permet de ne pas avoir à modifier la route par défaut des machines du réseau interne. **LIMITATIONS CONNUES** Les fonctionnalités du firewall qui insèrent ou modifient des paquets dans les sessions par le firewall pourraient ne pas fonctionner correctement. Ces fonctionnalités sont : • La réinitialisation des connexions induite par une alarme, • Le proxy SYN (activé dans le filtrage), • La demande de réémission de paquets perdus afin d'accélérer l'analyse, • La réécriture de paquets par les analyses applicatives (SMTP, HTTP et web 2.0, FTP et NAT, SIP et NAT).
Préserver les identifiants de Vlan	Cette option permet la transmission des trames taguées sans que le firewall soit une terminaison du VLAN. Le tag VLAN de ces trames est conservé ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN. Cette option requiert l'activation de l'option précédente "**Préserver le routage initial**".

Interface modem PPPoE / PPTP

Les interfaces modem sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur votre firewall, via un port Ethernet. Il existe deux types d'interfaces modem :

- Modem PPPoE,
- Modem PPTP.

NOTES

- Le firewall négocie automatiquement l'ouverture de ligne et réinitialise la connexion en cas de coupure. Dans le cas où la connexion n'est pas possible (par exemple dans le cas d'un problème de ligne), le firewall envoie un message d'alarme.
- Si votre modem nécessite d'être branché sur le port USB du firewall, reportez-vous au chapitre Interface USB / Ethernet (pour clé USB / Modem).

Ajouter un modem

1. Cliquez sur **Ajouter**.
2. Positionnez votre souris sur **Modem**.
3. Cliquez sur **PPPoE** ou **PPTP** selon l'interface que vous souhaitez créer.
   L'interface modem est ajoutée aux interfaces et son panneau de configuration s'affiche.

Panneau de configuration d'une interface modem PPPoE

Pour ouvrir le panneau de configuration d'une interface modem, faites un double-clic dessus.
Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface.

Paramètres généraux

Nom	Nom associé au modem. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour le modem.
Type de modem	Rappel du type de modem choisi lors de la création.

Connectivité

Interface parente	Sélectionnez l'interface réseau à laquelle le modem PPPoE est connecté.

Authentification

Identifiant	Saisissez l'identifiant utilisé pour l'authentification.
Mot de passe	Saisissez dans ce champ le mot de passe utilisé pour l'authentification, puis confirmez-le dans le champ **Confirmer**. Une jauge indique la robustesse du mot de passe renseigné.

Onglet Configuration avancée

Autres paramètres

Service	Type de service PPPoE utilisé. Cette option permet de différencier plusieurs modems ADSL. Par défaut, laissez ce champ vide.
Connectivité	Deux choix sont possibles : • **Permanente** : conserve la connexion vers Internet active en permanence. • **En cas de trafic (à la demande)** : la connexion vers Internet s'établit que lorsqu'une demande de connexion émane du réseau interne. Ce mode est plus économique dans le cas d'une liaison payante à la durée.

Panneau de configuration d'une interface modem PPTP

Pour ouvrir le panneau de configuration d'une interface modem, faites un double-clic dessus.
Le panneau de configuration dispose de plusieurs onglets.

Onglet Configuration générale

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer ou désactiver l'interface.

Paramètres généraux

Nom	Nom associé au modem. Vous pouvez le modifier si souhaité.
Commentaire	Permet de donner un commentaire pour le modem.
Type de modem	Rappel du type de modem choisi lors de la création.

Connectivité

Adresse PPTP	Indiquez l'adresse IP interne du modem.

Authentification

Identifiant	Saisissez l'identifiant utilisé pour l'authentification.
Mot de passe	Saisissez dans ce champ le mot de passe utilisé pour l'authentification, puis confirmez-le dans le champ **Confirmer**. Une jauge indique la robustesse du mot de passe renseigné.

Onglet Configuration avancée

Autres paramètres

Connectivité	Deux choix sont possibles : • **Permanente** : conserve la connexion vers Internet active en permanence. • **En cas de trafic (à la demande)** : la connexion vers Internet s'établit que lorsqu'une demande de connexion émane du réseau interne. Ce mode est plus économique dans le cas d'une liaison payante à la durée.

Interface USB / Ethernet (pour clé USB / Modem)

L'interface USB / Ethernet est utilisée dans le cas de connexions distantes lorsque votre modem est branché directement sur le port USB du firewall. Vous pouvez ajouter une seule interface USB / Modem sur votre firewall.

Lorsqu'un modem USB 4G de marque *HUAWEI* supportant la fonctionnalité *HiLink* est connecté sur le firewall puis paramétré, une interface USB / Ethernet est automatiquement créée. Dans le cas où vous utilisez un autre modem USB, la création de l'interface USB / Ethernet nécessite la configuration d'un profil de modem.

> **NOTE**
> Si votre modem nécessite d'être branché sur le port Ethernet ou le port série du firewall (modem PPPoE / PPTP), reportez-vous au chapitre Interface modem PPPoE / PPTP.

Panneau de configuration d'un profil de modem

Pour ouvrir le panneau de configuration d'un profil de modem, cliquez sur **Éditer > Profils de modem**. Deux profils de modem peuvent être définis, sélectionnez l'un des deux profils.

État

ON / OFF	Placez le sélecteur sur ON / OFF pour activer / désactiver le profil de modem.

Paramètres généraux

Nom	Saisissez un nom pour le profil de modem.
Modèle	Saisissez le modèle du modem auquel s'adresse le profil (texte libre).
Identifiant constructeur	Identifiant propre à chaque constructeur de modem (*VendorId* ou *VID*). Il s'agit d'une chaîne hexadécimale.
Identifiant initial de produit	Identifiant du produit (*ProductIdInit*) après avoir été reconnu comme périphérique de stockage USB. Ce paramètre est propre à chaque modèle de modem.
Identifiant cible de produit	Identifiant représentant le produit lorsqu'il est en mode modem (*ProductId* ou *PID*). Ce paramètre est propre à chaque modèle de modem.
Chaîne de passage en mode modem	Il s'agit d'une chaîne de caractères permettant au firewall de détecter le périphérique USB connecté comme étant un modem (*ModeSwitchString*).

Paramètres avancés

Port des commandes de configuration	Il s'agit du numéro du port série dédié pour l'envoi des commandes de configuration (commandes de type "AT") au modem. La valeur la plus courante est 0.
Port des commandes de supervision	Il s'agit du numéro du port série dédié pour l'envoi des commandes de supervision (commandes de type "AT") au modem. La valeur la plus courante est 1.
Chaîne d'initialisation N°1, N°2 et N°3	Ces chaînes sont optionnelles. Elles permettent d'envoyer au modem des commandes de configuration de type "AT" avant son utilisation. **EXEMPLES** *ATZ* : commande de réinitialisation du modem *AT^CURC=0* : commande permettant de désactiver les messages périodiques

Panneau de configuration d'une interface USB / Ethernet (pour clé USB / Modem)

Configurer les profils	Lorsque aucun profil de modem n'est défini ou n'est actif, un message vous invite à configurer un profil de modem. Pour plus d'informations, reportez-vous à la section Panneau de configuration d'un profil de modem.

Paramètres généraux

Nom	Nom de l'interface. Il ne peut pas être modifié.
Commentaire	Permet de donner un commentaire pour l'interface.

Cette interface est	Une interface peut être : • **Interne (protégée)** : en choisissant cette option, vous indiquez le caractère protégé de l'interface (matérialisé par un bouclier). Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le firewall comme le DHCP. • **Externe (publique)** : en choisissant cette option, vous indiquez que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.

Plan d'adressage

IP dynamique (obtenue par DHCP)	En choisissant cette option, l'adresse IP de l'interface est définie par DHCP. Une zone **Configuration DHCP avancée** apparaît avec les paramètres suivants : • **Nom DNS (facultatif)** : vous pouvez indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP. Si ce champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met automatiquement à jour le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et la durée du bail alloué (champ ci-dessous). • **Durée de bail demandée (secondes)** : en complément du nom DNS, indiquez une période de conservation de l'adresse IP avant renégociation. • **Demander les serveurs DNS au serveur DHCP et créer les objets machines** : cochez ce paramètre pour que le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. L'activation de cette option entraîne la création de deux objets : *Firewall_<nom de l'interface>_dns1* et *Firewall_<nom de l'interface>_dns2*. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi, si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.
IP fixe (statique)	En choisissant cette option, l'adresse IP de l'interface est fixe (statique). Une grille apparaît dans laquelle vous devez ajouter l'adresse IP et son masque de sous-réseau. Il est possible d'ajouter plusieurs adresses IP et masques associés (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser le firewall comme un point de routage central. De ce fait, une interface peut être connectée à différents sous-réseaux ayant un adressage différent. Si vous ajoutez plusieurs adresses IP (alias) dans le même plan d'adressage, il est impératif que ces adresses aient toutes le même masque. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Modes de configuration réseau

Il existe plusieurs modes de configuration que vous pouvez réaliser sur votre firewall :

- Mode Bridge,
- Mode avancé (Routeur),
- Mode hybride.

Ces modes n'apparaissent pas visuellement dans l'interface Web d'administration et il n'existe pas d'assistant de configuration pour les mettre en œuvre. Ils représentent des types de configuration que vous pouvez réaliser sur votre firewall. **Au niveau sécurité, tous les modes de fonctionnement sont identiques**.

Mode Bridge

Les interfaces font partie du même plan d'adressage déclaré sur le bridge. Ce mode permet de conserver le même adressage entre les interfaces.

Vous pouvez ensuite filtrer les flux qui le traversent, en utilisant les objets interfaces ou les plages d'adresses suivant vos besoins et donc protéger telle ou telle partie du réseau.

Les avantages de ce mode sont :

- Facilité d'intégration du produit car pas de changement de la configuration des postes client (routeur par défaut, routes statiques...) et aucun changement d'adresse IP sur votre réseau.
- Compatibilité avec IPX (réseau Novell), NetBIOS sous Netbeui, Appletalk ou IPv6.
- Pas de translation d'adresses, donc gain de temps au niveau du traitement des paquets par le firewall.

Ce mode est donc préconisé entre la zone externe et la / les DMZ. Il permet de conserver un adressage public sur la zone externe du firewall et les serveurs publics de la DMZ.

Mode avancé (Routeur)

Le firewall fonctionne comme un routeur entre ses différentes interfaces. Chaque interface activée porte une adresse IP du réseau auquel elle est directement connectée. Cela permet de configurer des règles de translation pour accéder à une autre zone du firewall.

Cela implique certains changements d'adresses IP sur les routeurs ou serveurs lorsque vous les déplacez dans un réseau différent (derrière une interface du firewall différente).

Les avantages de ce mode sont :

- La possibilité de faire de la translation d'adresses entre les différents réseaux.
- Seul le trafic passant d'un réseau à l'autre traverse le firewall (réseau interne vers Internet par exemple). Cela allège considérablement le firewall et fournit de meilleurs temps de réponse.
- Une meilleure distinction des éléments appartenant à chaque zone (interne, externe et DMZ). La distinction se fait par les adresses IP qui sont différentes pour chaque zone. Cela permet d'avoir une vision plus claire des séparations et de la configuration à appliquer pour ces éléments.

Mode hybride

Certaines interfaces possèdent la même adresse IP et d'autres ont une adresse distincte. Le mode hybride utilise une combinaison des deux modes précédents. Ce mode ne peut être employé que pour les produits Stormshield Network possédant plus de deux interfaces réseau. Vous pouvez définir plusieurs interfaces en mode bridge.

EXEMPLE
Zone interne et DMZ, ou zone externe et DMZ, et certaines interfaces dans un plan d'adressage différent. Ainsi vous avez une plus grande flexibilité dans l'intégration du produit.

INTERFACES VIRTUELLES

Le module **Interfaces virtuelles** permet de gérer, ajouter, supprimer des éléments réseaux virtuels. Selon leur nature, ces interfaces virtuelles pourront être utilisées dans une configuration de routage dynamique (interfaces de type loopback), pour établir des tunnels (interfaces GRE) ou des tunnels routés (interfaces IPsec).

L'écran de configuration des interfaces virtuelles se compose de 3 onglets :

- Interfaces IPsec (VTI),
- Interfaces GRE,
- Loopback.

NOTE
Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Créer ou modifier une interface IPsec (VTI)

Ces interfaces permettent d'établir des tunnels IPsec routés. L'interface virtuelle IPsec joue le rôle d'extrémité de trafic et tous les paquets routés vers cette interface sont alors chiffrés. Ce type de configuration peut, par exemple, permettre de faire transiter des flux bénéficiant de QoS au travers d'un tunnel IPsec dédié: les flux prioritaires empruntent alors un tunnel spécifique, tandis que les autres flux passent par un second tunnel.

Pour créer ou modifier une interface virtuelle IPsec, cliquez sur l'onglet *Interfaces IPsec (VTI)*.

Présentation de la barre de boutons

Recherche	Recherche qui porte sur une interface.
Ajouter	Ajoute une nouvelle interface. L'ajout de l'interface (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Nom, Adresse IP, Masque** remplis.
Supprimer	Supprime une ou plusieurs interfaces préalablement sélectionnée(s). Utiliser les touches **Ctrl**/**Shift** + **Supprimer** pour la suppression de plusieurs interfaces
Vérifier l'utilisation	Matérialisé par l'icône, ce bouton vous renseigne sur l'utilisation de l'interface sélectionnée dans le reste de la configuration.
Appliquer	Envoie la configuration des interfaces IPsec.
Annuler	Annule la configuration des interfaces IPsec.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des interfaces IPsec virtuelles :

- Ajouter,
- Supprimer,

- Vérifier l'utilisation.

Présentation de la grille

La grille présente cinq informations :

État	État des interfaces : • Activé : Double-cliquez pour activer l'interface créée. • Désactivé : L'interface n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.
Nom (obligatoire)	Affectez un nom à l'interface IPsec. **NOTE** Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.
Adresse IPv4 (obligatoire)	Renseignez l'adresse IP affectée à l'interface virtuelle créée.
Masque IPv4 (obligatoire)	La valeur proposée par défaut est 255.255.255.252. En effet, les interfaces virtuelles IPsec étant destinées à établir des tunnels point à point, un réseau permettant d'affecter deux adresses est théoriquement suffisant. Cette valeur peut cependant être personnalisée.
Protégée	Double-cliquez sur cette cellule pour modifier le type de l'interface : • Protégée • Publique
Commentaire (optionnel)	Texte libre.

Créer ou modifier une interface GRE

Le protocole GRE permet d'encapsuler des flux IP dans un tunnel IP point à point. Cela permet, par exemple, de router des réseaux d'un site vers un autre via un tunnel GRE sans devoir déclarer ce routage sur l'ensemble des routeurs intermédiaires.

Un tunnel GRE n'est pas chiffré nativement: il ne fait que de l'encapsulation. Il est cependant possible de faire transiter le trafic GRE au travers d'un tunnel IPsec.

Pour créer ou modifier une interface virtuelle GRE, cliquez sur l'onglet *Interfaces GRE*.

Présentation de la barre de boutons

Recherche	Recherche qui porte sur une interface.
Ajouter	Ajoute une nouvelle interface. L'ajout de l'interface (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Nom, Adresse IP, Masque, Source du tunnel et Destination du tunnel** remplis.

Supprimer	Supprime une ou plusieurs interfaces préalablement sélectionnée(s). Utiliser les touches **Ctrl**/**Shift** + **Supprimer** pour la suppression de plusieurs interfaces
Vérifier l'utilisation	Matérialisé par l'icône, ce bouton vous renseigne sur l'utilisation de l'interface sélectionnée dans le reste de la configuration.

Appliquer	Envoie la configuration des interfaces IPsec.
Annuler	Annule la configuration des interfaces IPsec.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des interfaces GRE :

- Ajouter,
- Supprimer,
- Vérifier l'utilisation.

Présentation de la grille

La grille présente sept informations :

État	État des interfaces : • Activé : Double-cliquez pour activer l'interface créée. • Désactivé : L'interface n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.
Nom (obligatoire)	Affectez un nom à l'interface GRE.
Adresse IPv4 (obligatoire)	Renseignez l'adresse IP affectée à l'interface virtuelle créée.
Masque IPv4 (obligatoire)	La valeur proposée par défaut est 255.255.255.252. En effet, les interfaces virtuelles GRE étant destinées à établir des tunnels point à point, un réseau permettant d'affecter deux adresses est théoriquement suffisant. Cette valeur peut cependant être personnalisée.
Source du tunnel (obligatoire)	Sélectionnez l'interface de sortie des flux empruntant le tunnel. Il s'agit en général de l'interface « out » ou d'un bridge du firewall.
Destination du tunnel (obligatoire)	Sélectionnez l'objet représentant l'extrémité distante du tunnel. Il s'agit d'un objet machine présentant l'adresse IP publique du firewall distant.
Commentaire (optionnel)	Texte libre.

Créer ou modifier une interface Loopback

Les interfaces loopback peuvent être utilisées, par exemple, dans une configuration de routage dynamique.

Pour créer ou modifier une interface loopback, cliquez sur l'onglet *Loopback*.

Présentation de la barre de boutons

Recherche	Recherche qui porte sur une interface.
Ajouter	Ajoute une nouvelle interface. L'ajout de l'interface (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Nom et Adresse IP** remplis.
Supprimer	Supprime une ou plusieurs interfaces préalablement sélectionnée(s). Utiliser les touches **Ctrl** / **Shift** + **Supprimer** pour la suppression de plusieurs interfaces.
Vérifier l'utilisation	Matérialisé par l'icône, ce bouton vous renseigne sur l'utilisation de l'interface sélectionnée dans le reste de la configuration.
Appliquer	Envoie la configuration des interfaces IPsec.
Annuler	Annule la configuration des interfaces IPsec.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des interfaces loopback :

- Ajouter,
- Supprimer,
- Vérifier l'utilisation.

Présentation de la grille

La grille présente quatre informations :

État	État des interfaces : • Activé : Double-cliquez pour activer l'interface créée. • Désactivé : L'interface n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.
Nom (obligatoire)	Affectez un nom à l'interface loopback.
Adresse IPv4 (obligatoire)	Renseignez l'adresse IP affectée à l'interface loopback créée.
Commentaire (optionnel)	Texte libre.

LOGS - JOURNAUX D'AUDIT

Ce menu n'est pas disponible sur les firewalls ne disposant pas de support de stockage.

Le module Logs - Journaux d'audit vous permet de consulter les traces (logs) générées par les équipements et stockées localement. Ces logs sont regroupés sous forme de vues de type alarmes, connexions, traces WEB, … Des filtres avancés permettent une analyse approfondie des traces.

Données personnelles

Par souci de conformité avec le règlement européen RGPD (Règlement Général sur la Protection des Données), les données sensibles (nom d'utilisateur, adresse IP source, nom de la source, adresse MAC source) ne sont pas affichées dans les logs et rapports et sont remplacées par la mention "Anonymized".

Pour visualiser ces données sensibles, l'administrateur doit alors activer le droit "Logs : accès complet (données personnelles)" en cliquant sur **Logs : accès restreint** dans le bandeau supérieur de l'interface Web d'administration, puis en saisissant un code d'autorisation obtenu auprès de son superviseur (voir la section **Administrateurs** > **Gestion des tickets**). Ce code possède une durée de validité limitée définie lors de sa création.

Pour relâcher ce droit, l'administrateur doit ensuite cliquer sur la mention **Logs : accès complet (données personnelles)** présente dans le bandeau supérieur de l'interface Web d'administration puis cliquer sur le bouton **Libérer** de la boite de dialogue affichée.

Après avoir obtenu ou relâché ce droit, il est nécessaire de rafraîchir les données affichées.

Notez que chaque action d'obtention ou de libération du droit "Logs : accès complet (données personnelles)" génère une entrée dans les logs.

Collaborative security

Pour une sécurité plus collaborative, à partir des vues, il est maintenant possible d'augmenter le niveau de protection d'une machine en un clic. Une interaction vous permet en effet d'ajouter les machines à un groupe préalablement établi et se voir attribuer un profil de protection renforcée ou des règles de filtrage spécifiques (zones de mise en quarantaine, accès limité, etc.).

Pour plus d'informations, reportez-vous à la Note Technique **Sécurité collaborative**.

Support de stockage : cartes SD / microSD

Pour les modèles SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 et SNi20, vous pouvez bénéficier de l'ensemble de la fonctionnalité en utilisant un support de stockage externe de type :

- Carte SD pour les modèles SN160(W), SN210(W), SN310 et SNi20,
- Carte microSD pour les modèles SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 et SNi10.

Ces supports externes doivent respecter les caractéristiques suivantes :

Carte SD	Carte microSD
Classe 10 (C10) UHS Classe 1 (U1) ou **App Performance (A2)** et de standard **SDHC** ou **SDXC**. La carte mémoire doit être de préférence au format physique SD "full-size". Seuls les adaptateurs fournis avec la carte doivent être utilisés.	**Classe 10 (C10) UHS Classe 1 (U1)** ou **App Performance 2 (A2)** et de standard SDHC ou SDXC.
Stormshield recommande l'utilisation de cartes de gamme haute endurance / industrielle ou embarquant de préférence de la flash de type **MLC**, issues des majors du secteur (ex : SanDisk, Western Digital, Innodisk, Transcend, etc.) et de **taille minimale 32 Go**. La taille mémoire **maximale** supportée est de **2 To**.	

NOTE
Le stockage sur support externe s'effectue uniquement sur carte SD ou microSD. Ce service n'est pas compatible avec d'autres supports de stockage comme une clé USB ou un disque dur externe.

Pour plus d'information, consultez le Guide **PRÉSENTATION ET INSTALLATION DES PRODUITS STORMSHIELD NETWORK Gamme SN** disponible sur le site de Documentation Technique Stormshield.

Actions

Barre d'outils N°1 : période

Échelle de temps	Ce champ permet le choix de l'échelle de temps : Dernière heure, Aujourd'hui, 7 derniers jours, 30 derniers jours et plage personnalisée. • La dernière heure est calculée jusqu'à la minute précédant celle en cours. • La vue Aujourd'hui couvre la journée en cours, depuis la veille à minuit jusqu'à la minute précédant l'actualisation des données. • La vue Hier couvre la journée précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. • La plage personnalisée permet de définir une période déterminée, qui couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. Le bouton est un raccourci permettant de choisir **une plage personnalisée**.
Actualiser	Ce bouton permet de rafraîchir les données affichées.

Barre d'outils N°2 : recherche simple ou avancée

Changez de mode de Recherche par le bouton "**Recherche simple**" / "**Recherche avancée**".

Mode Recherche simple

Par ce mode de recherche par défaut, le boîtier recherche la valeur saisie dans tous les champs des fichiers de traces affichés.

Cette recherche ne porte que sur les valeurs des champs, et non sur les noms des champs. Par exemple, pour filtrer les connexions bloquées, il faut entrer la valeur « block » dans le champ de recherche, et non « action=block ». Pour les pays source ou destination, utilisez le code pays (exemple : fr, en, us...).

(Champ de saisie de la valeur recherchée)	Pour créer la recherche, vous pouvez saisir un texte dans le champ de saisie ou y glisser la valeur depuis un champ des résultats. Il est également possible de glisser le nom d'un objet directement dans ce champ depuis le module **Objets réseau**.

Mode Recherche avancée

En mode avancé, vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (Nouveau filtre) permet de réinitialiser le filtre en supprimant la sélection de critères.
Enregistrer	Enregistrez en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après. Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
Supprimer	Supprimez un filtre personnalisé, enregistré précédemment.

Panneau FILTRAGE

Vous pouvez ajouter un critère de recherche soit en cliquant sur le bouton **Ajouter un critère,** soit en glissant la valeur depuis un champ des résultats dans le panneau.

La fenêtre de création propose soit **d'appliquer**, soit **d'ajouter** le critère défini. Le bouton **Ajouter** conserve la fenêtre ouverte afin de définir successivement plusieurs critères avant de lancer la recherche.

Ajouter un critère	Pour ajouter un critère de recherche, cliquez sur ce bouton pour ouvrir la fenêtre de d'édition d'un critère, proposant les 3 éléments suivants à renseigner : • Un **Champ** à sélectionner dans lequel la valeur va être recherchée. Le choix any permet une recherche dans l'ensemble des valeurs contenues dans les traces. • On retrouve dans cette liste le nom traduit du champ et entre parenthèses, le nom d'origine (token). Les champs principaux sont affichés en noir et les champs secondaires en gris, correspondant à l'affichage du bouton **Afficher / Résumer tous les éléments**. • Un **Critère** de tri qui sera associé à la valeur recherchée. Ces opérateurs sont : égal à, différent de, contient, ne contient pas, commence par et termine par. • Une **Valeur** à rechercher selon les critères précédemment choisis. Pour les pays source ou destination, utilisez le code pays (exemple : fr, en, us...).

Une fois le critère crée, il est ajouté dans ce panneau **Filtrage**. Ce critère ajouté permet :

- Sa suppression via l'icône . La suppression d'un critère relance automatiquement la recherche du filtre modifié, sans ce critère.
- Son édition par une fenêtre identique à sa création, via l'icône . La fenêtre d'édition ne propose que d'appliquer la recherche.

Barre d'outils N°3 : actions

Afficher tous les éléments / Résumer les éléments	Affichage de l'ensemble des champs ou uniquement des champs principaux.
Exporter les données	Matérialisé par le symbole , ce bouton permet de télécharger les données au format CSV. Les valeurs sont séparées par des virgules et enregistrées dans un fichier texte. Cela permet la réouverture du fichier dans un logiciel tableur comme *Microsoft Excel.*
Imprimer	Matérialisé par le symbole , ce bouton permet d'accéder à la fenêtre d'aperçu pour l'impression des traces contenues dans le journal. Le bouton *Imprimer* envoie le fichier au module d'impression du navigateur qui permet de choisir entre l'impression ou la génération d'un fichier PDF.
Réinitialiser l'affichage des colonnes	Affiche uniquement les colonnes proposées par défaut lors de la première consultation de la trace ou de la vue concernée, ou annule les modifications de largeur des colonnes.

Informations

Au-dessus de la grille présentant les traces est affichée la période interrogée, selon la valeur choisie dans le menu déroulant de la 1ère barre d'outils. Cette période est affichée sous la forme :

RECHERCHE DU - DD/MM/AAAA HH:MM:SS - AU - DD/MM/AAAA HH:MM:SS

Sous la grille des traces sont indiquées les informations suivantes :

- Numéro de la page affichée,
- Nombre de traces affichées dans la page,
- Période couverte par les traces affichées dans la page,
- Date et Heure de l'UTM (information utile dans le cas où le poste de l'administrateur n'a pas les mêmes paramètres).

Afficher les détails d'une ligne de log

Un clic sur une ligne de log affiche automatiquement le détail de cette ligne dans une fenêtre à droite de la grille. Un bouton permet de masquer ( ) ou d'afficher ( ) cette fenêtre.

Au sein de cette fenêtre, cliquez sur les boutons **Précédent** ou **Suivant** afin d'afficher automatiquement les détails de la ligne précédente ou de la ligne suivante de log.

Le bouton **Copier** permet de copier directement l'ensemble des champs / valeurs d'une ligne de log dans le presse-papier.

Les interactions

Quel que soit le mode d'affichage (ligne / grille), les valeurs affichées dans la fenêtre de consultation des traces proposent des interactions classées en deux catégories : ACTION et CONFIGURATION. Par un clic droit, un menu propose les actions suivantes :

Mode Recherche simple

- **Ajouter cette valeur comme critère de recherche :** raccourci pour créer un critère recherchant la valeur dans le champ correspondant et dans l'ensemble de la vue Ce type de recherche est identique au glisser/déposer de la valeur.
- **Accéder à la règle de sécurité correspondante** : raccourci pour ouvrir le module Filtrage et NAT et surligner la règle de sécurité correspondant à la ligne de trace sélectionnée.
- **Copier la ligne sélectionnée dans le presse-papier** : raccourci pour copier les données de la ligne de logs sélectionnée dans le presse-papier. Cette action est identique à celle déclenchée par un clic sur le bouton **Copier** disponible sous la fenêtre d'affichage des détails de la ligne sélectionnée.

Mode Recherche avancée

- **Ajouter un critère pour ce champ / valeur** : raccourci pour créer un critère recherchant la valeur dans le champ correspondant et dans l'ensemble de la vue affichée. Pour éviter la répétition de la valeur recherchée, la colonne correspondante est alors automatiquement masquée en mode d'affichage par grille. Ce type de recherche est identique au glisser / déposer de la valeur.
- **Ajouter un critère de différence à cette valeur** : raccourci pour créer un critère recherchant toute valeur différente de celle sélectionnée dans le champ correspondant et dans l'ensemble de la vue affichée.
- **Accéder à la règle de sécurité correspondante** : raccourci pour ouvrir le module Filtrage et NAT et surligner la règle de sécurité correspondant à la ligne de trace sélectionnée.

Adresses IP et objets machine

- **Rechercher cette valeur dans la vue "Tous les journaux"** : raccourci pour ouvrir la vue "Tous les journaux" avec un filtre sur la valeur sélectionnée.
- **Vérifier cette machine** : indique dans quelles règles de filtrage ou de NAT cette machine est utilisée.
- **Afficher les détails de la machine** : ouvre une fenêtre présentant un certains nombre d'informations complémentaires sur la machine sélectionnée. Ces informations sont les suivantes :

- Réputation de l'adresse IP publique,
- Géolocalisation,
- Réputation de la machine,
- Classification de l'URL (à laquelle s'est connectée la machine),
- Vulnérabilités,
- Applications (navigateurs Internet, clients de messagerie ...),
- Services,

- Informations (Système d'exploitation détecté,...),
- Délai de réponse au Ping et chemin réseau (Traceroute) pour joindre la machine.
  - **Réinitialiser le score de réputation de cet objet** : en cliquant sur ce menu, le score de réputation de l'objet sélectionné est remis à zéro.
  - **Placer cet objet en liste noire** : permet de positionner une machine, une plage d'adresses IP ou un réseau en liste noire (quarantaine). Les objets ainsi sélectionnés sont rejetés par le firewall pendant une durée choisie dans le sous-menu de cette action :
  - Pour 1 minute,
  - Pour 5 minutes,
  - Pour 30 minutes,
  - Pour 3 heures.
    Une fois ce délai de quarantaine écoulé, l'objet considéré est de nouveau autorisé à traverser le firewall en respect de la politique de sécurité active.
  - **Afficher les IoC** : un clic sur ce menu vous dirige sur le site Stormshield Security et affiche les détails de sécurité de l'objet sélectionné :
  - Adresse IP,
  - Pays d'origine,
  - FQDN
  - Catégorie de réputation ou service Web de rattachement s'ils sont définis sur le firewall.
  - **Ajouter la machine à la base objet et / ou l'ajouter à un groupe :** cette option permet de créer une machine et/ou de l'ajouter à un groupe depuis un fichier de traces. Ainsi, une machine identifiée comme vulnérable peut par exemple, être ajoutée à un groupe ayant un profil de protection renforcé (cf. Note Technique **Sécurité collaborative**).
    Cette option apparaît sur les champs contenant des adresses IP (source, destination) ou des noms d'objet (nom de la source, nom de la destination). Une fenêtre s'affiche, permettant :
  - d'enregistrer l'objet dans la base s'il s'agit d'une adresse IP,
  - de sélectionner l'objet approprié si l'adresse IP correspond à plusieurs objets,
  - de l'ajouter à un groupe existant. Ce groupe peut correspondre à une mise en quarantaine d'objets vulnérables préétablie.

En plus des interactions listées ci-dessus, le survol d'une adresse IP source ou du nom d'une machine source entraîne l'affichage d'une info-bulle reprenant les informations suivantes (si l'administrateur a acquis le droit "Logs : accès complet (données personnelles)") :

- Nom de la machine si celle-ci est définie dans la base objets,
- Adresse IP de la machine,
- Système d'exploitation de la machine,
- Nombre de vulnérabilités détectées pour la machine.

URL

- **Rechercher cette valeur dans la vue "Tous les journaux"** : raccourci pour ouvrir la vue "Tous les journaux" avec un filtre sur la valeur sélectionnée.
- **Afficher les détails de la machine** : ouvre une fenêtre présentant un certains nombre d'informations complémentaires sur la machine sélectionnée. Ces informations sont les suivantes :

- Réputation de l'adresse IP publique,
- Géolocalisation,
- Réputation de la machine,
- Classification de l'URL (à laquelle s'est connectée la machine),
- Vulnérabilités,
- Applications (navigateurs Internet, clients de messagerie ...),
- Services,
- Informations (Système d'exploitation détecté,...),
- Délai de réponse au Ping et chemin réseau (Traceroute) pour joindre la machine.

- **Réinitialiser le score de réputation de cet objet** : en cliquant sur ce menu, le score de réputation de l'objet sélectionné est remis à zéro.
- **Placer cet objet en liste noire** : permet de positionner une machine, une plage d'adresses IP ou un réseau en liste noire (quarantaine). Les connexions issues ou à destination de l'objet ainsi sélectionné sont rejetées par le firewall pendant une durée choisie dans le sous-menu de cette action :

- Pour 1 minute,
- Pour 5 minutes,
- Pour 30 minutes,
- Pour 3 heures.
  Une fois ce délai de quarantaine écoulé, l'objet considéré est de nouveau autorisé à émettre des connexions ou en être destinataire en respect de la politique de sécurité active.

- **Afficher les IoC** : un clic sur ce menu vous dirige sur le site Stormshield Security et affiche les détails de sécurité de l'objet sélectionné :

- Adresse IP,
- Pays d'origine,
- FQDN
- Catégorie de réputation ou service Web de rattachement s'ils sont définis sur le firewall.

- **Ajouter la machine à la base Objet et/ou l'ajouter à un groupe :** cette option permet de créer une machine et/ou de l'ajouter à un groupe depuis un fichier de traces. Ainsi, une machine identifiée comme vulnérable peut par exemple, être ajoutée à un groupe ayant un profil de protection renforcé (cf. Note Technique **Sécurité collaborative**).
  Cette option apparaît sur les champs contenant des adresses IP (source, destination) ou des noms d'objet (nom de la source, nom de la destination). Une fenêtre s'affiche, permettant :

- d'enregistrer l'objet dans la base s'il s'agit d'une adresse IP,
- de sélectionner l'objet approprié si l'adresse IP correspond à plusieurs objets,
- de l'ajouter à un groupe existant. Ce groupe peut correspondre à une mise en quarantaine d'objets vulnérables préétablie.

- **Ajouter l'URL à un groupe :** cette option permet d'ajouter l'URL à un groupe depuis un fichier de traces. Ainsi, une URL identifiée comme malicieuse ou indésirable peut, par exemple, être ajoutée à un groupe personnalisé faisant l'objet de filtrage d'URL.
  Cette option apparaît sur les champs contenant des URL (nom de la destination). Une fenêtre s'affiche, permettant :

- d'ajouter l'URL à un groupe existant. Ce groupe peut, par exemple, correspondre à une catégorie d'URL interdites.

En plus des interactions listées ci-dessus, le survol d'une URL destination entraîne l'affichage d'une info-bulle reprenant les informations suivantes (si l'administrateur a acquis le droit "Logs : accès complet (données personnelles)") :

- Nom du domaine,
- Adresse IP correspondante.

Ports

- **Ajouter le service à la base objet et/ou l'ajouter à un groupe :** cette option permet de créer un service et/ou de l'ajouter à un groupe depuis un fichier de traces. Ainsi, un service identifié comme vulnérable ou indésirable peut par exemple, être ajouté à un groupe de services interdits dans les règles de filtrage.
  Cette option apparaît sur les champs contenant des numéros de ports ou des noms de services (port source, port destination, nom du port source, nom du port dest.). Une fenêtre s'affiche, permettant :
  - d'enregistrer l'objet dans la base s'il s'agit d'un numéro de port,
  - de l'ajouter à un groupe existant. Ce groupe peut correspondre à un groupe de services interdits.

En plus des interactions listées ci-dessus, le survol d'un nom de port entraîne l'affichage d'une info-bulle reprenant les informations suivantes (si l'administrateur a acquis le droit "Logs : accès complet (données personnelles)") :

- Nom de l'objet port,
- Numéro ou plage de ports correspondants,
- Protocole,
- Commentaire éventuel défini dans l'objet port.

Paquets réseau

- **Exporter le paquet** : cette option permet d'exporter au format *pcap* le paquet capturé afin de l'analyser à l'aide d'outils comme Wireshark. Pour provoquer la capture d'un paquet, la case **Capturer le paquet responsable de la remontée de l'alarme** doit avoir été cochée dans la configuration de l'alarme concernée (module **Protection applicative** > **Applications et protections** > colonne **Avancé** > clic sur **Configurer**).

Vue Alarmes

- **Configurer l'alarme** : raccourci pour ouvrir le module **Application et Protections - Par profil d'inspection** avec sélection automatique de l'alarme concernée.

Vue Événements système

- **Configurer l'événement système** : raccourci pour ouvrir le module **Événements système** avec sélection automatique de l'événement concerné.

Les Journaux

La liste des logs (utilisés dans les vues à but thématique) et le nom du fichier de traces correspondant sur le firewall sont disponibles dans la Note Technique "Description des journaux d'Audit".

Les vues disponibles sont les suivantes :

- Tous les journaux

Cette vue affiche l'ensemble des journaux : **Administration, Alarmes, Authentification, Connexions réseaux, Filtrage, Proxy FTP, VPN IPsec, Connexions applicatives, Proxy POP3, Proxy SMTP, Proxy SSL, Événements système, Vulnérabilités, Proxy HTTP** et **VPN SSL.**

> NOTE
> Si l'utilisateur n'a pas le droit *admin*, le journal **Administration** ne sera pas comptabilisé dans cette vue.

- Trafic réseau

Cette vue affiche les journaux **Connexions réseaux, Filtrage, Proxy FTP, Connexions applicatives, Proxy POP3, Proxy SMTP, Proxy SSL, Proxy HTTP** et **VPN SSL.**

Deux filtres prédéfinis sont proposés recherchant le trafic IPv4 et le trafic IPv6.

- Routage

Cette vue affiche le journal **Routage** correspondant au routage unicast.

- Alarmes

Cette vue affiche le journal **Alarmes** selon une certaine catégorisation; ce journal affiche uniquement les traces dont la catégorie d'appartenance de l'alarme n'est pas *filter*.

Trois filtres prédéfinis sont proposés recherchant les vulnérabilités de type Application (classification=1), Malware (classification=2) ou Protection (classification=0).

- Web

Cette vue affiche les journaux **Connexions réseaux, Connexions applicatives** et **Proxy HTTP** selon certaines catégorisations :

- Le journal de Connexions réseaux affiche uniquement les traces dont le service standard correspondant au port de destination est HTTP, HTTPS ou HTTP_PROXY.
- Le journal de Connexions applicatives affiche uniquement les traces dont le nom du plugin associé est HTTP ou HTTPS.

Un filtre prédéfini est proposé recherchant les Virus détectés.

- Vulnérabilités

Cette vue affiche le journal **Vulnérabilités.**

Deux filtres prédéfinis sont proposés recherchant les Vulnérabilités de type Client (targetclient=1) et de type Serveur (targetserver=1)

- E-mails

Cette vue affiche les journaux **Connexions réseaux, Connexions applicatives, Proxy POP3** et **Proxy SMTP** selon certaines catégorisations :

- Le journal de Connexions réseaux affiche uniquement les traces dont le service standard correspondant au port de destination est SMTP, SMTPS, POP3, POP3S, IMAP ou IMAPS.

- Le journal de Connexions applicatives affiche uniquement les traces dont le nom du plugin associé est SMTP, SMTPS, POP3, POP3S, IMAP ou IMAPS.

Deux filtres prédéfinis sont proposés recherchant les Virus détectés (virus=infected) et les Spam détectés (spamlevel renseigné et différent de 0)

- VPN

Cette vue affiche les journaux **VPN IPsec, Événements système** et **VPN SSL** selon une certaine catégorisation ; le journal **Événements système** affiche uniquement les traces dont le message de référence à l'action est PPTP.

- Événements système

Cette vue affiche les journaux **Alarmes** et **Événements système** selon une certaine catégorisation ; le journal **Alarmes** affiche uniquement les traces dont la catégorie d'appartenance de l'alarme est *system*.

Deux filtres prédéfinis sont proposés recherchant les niveaux Mineur (pri = 4) ou Majeur (pri = 1).

- Filtrage

Cette vue affiche les journaux **Alarmes** et **Filtrage** selon une certaine catégorisation ; le journal **Alarmes** affiche uniquement les traces dont la catégorie d'appartenance de l'alarme est *filter*.

- Analyse sandboxing

Cette vue affiche le journal **Sandboxing.**

- Utilisateurs

Cette vue affiche le journal **Authentification.**

- Routage multicast dynamique

Cette vue affiche le journal **Routage multicast dynamique**.

LICENCE

L'écran de Licence se décompose en plusieurs parties :

- L'onglet **Général** : installation manuelle ou automatique d'une licence et consultation des principales informations.
- L'onglet **Licence locale** (ou indication du N° de série type Licence Locale SN210XX8E4545A5 pour différencier le firewall actif d'un firewall passif) : détail de toutes les options de la licence et de leur valeur active sur le firewall.
- Un onglet supplémentaire **Licence du firewall distant *N° de série du firewall distant*** pour le firewall passif dans le cadre de la Haute Disponibilité.

Firewalls disposant de plusieurs modèles pour une même plate-forme physique

Pour les firewalls disposant de plusieurs modèles pour une même plate-forme physique (firewalls SN-XS-Series-170 / SNi10, SN-S-Series-220 / SN-S-Series-320, SN-M-Series-720 / SN-M-Series-920, SN-L-Series-2200 / SN-L-Series-3200 et SN-XL-Series-5200 / SN-XL-Series-6200), l'évolution d'un modèle vers l'autre s'effectue via l'installation d'une licence suivie d'un redémarrage du firewall.

Pour en savoir plus, consultez le Guide de présentation et d'installation produits.

L'onglet Général

Cet onglet vous permet d'installer une licence de manière automatique ou manuelle.

Il existe 2 manières d'installer une licence en manuel :

- En injectant le **Fichier de licence** dans le champ adapté. Possibilité de configurer en automatique.
- En recherchant une nouvelle licence.

Les boutons

- **Rechercher une nouvelle licence** : Ce bouton sert à la recherche d'une nouvelle licence ou actualise la date de dernière vérification de licence.
  En cliquant sur ce bouton, une demande de recherche de licence est faite au boîtier. Si une licence est trouvée, une notification s'affiche au niveau des informations de l'onglet *Général* et l'utilisateur a alors accès au bouton **Installer la nouvelle licence**. La recherche de licence se fait manuellement. Si vous souhaitez une recherche de licence automatique, dans ce cas, il faudra paramétrer la configuration avancée dans cet onglet.
- **Installer la nouvelle licence** : Si le firewall a trouvé une licence par le biais du bouton **Rechercher une nouvelle licence**, le bouton **Installer la nouvelle licence** apparaît en clair. En cliquant dessus, un téléchargement est réalisé. Puis il suffit de confirmer ou non ce téléchargement.

Les dates

- **Date locale sur le firewall** : cette date permet de confirmer que le firewall est à la bonne date. Les dates d'expirations sont calculées selon la date indiquée ici.
- **Dernière vérification d'une mise à jour de licence effectuée le** : dernière date à laquelle une demande de recherche de licence a été faite manuellement ou automatiquement.

Le firewall Stormshield Network est livré par défaut avec l'ensemble de ses fonctionnalités. Cependant, certaines fonctionnalités (filtrage URL, Haute Disponibilité...) sont optionnelles et ne sont pas activées. D'autres part certaines options, comme la mise à jour, sont limitées dans le temps. Si la date d'expiration est dépassée, certaines options sont désactivées sur le firewall.

Les informations importantes sur la licence

L'écran de configuration de la licence vous donne la version de votre firewall, des informations sur le matériel et les différentes options avec leur date d'expiration s'il y en a une.

Des icônes et des couleurs vous indiquent si une option est proche de l'expiration ou expirée.

Installation à partir d'un fichier

Ici, vous pouvez installer votre première licence si vous n'avez pas d'accès à Internet où si vous souhaitez gérer les licences vous-même.

Si vous choisissez d'utiliser de nouvelles fonctionnalités ou renouveler certaines options, veuillez contacter votre revendeur. Un nouveau fichier chiffré sera alors disponible dans votre espace privé, sur le site Web de Stormshield Network.

Fichier de licence	Ce champ vous permet d'insérer votre licence préalablement récupérée sur le site web Stormshield Network et ainsi activer la configuration de votre firewall. Le bouton **Installer** valide l'installation du fichier de licence sur le firewall. Les informations concernant votre firewall sont modifiées et les nouvelles options sont activées sur le firewall.
Installer la licence sur	Ce champ n'est disponible que sur le firewall actif dans le cas d'une configuration en haute disponibilité. Il permet de sélectionner sur quel membre du cluster le nouveau fichier de licence doit être installé. Le bouton **Installer** valide l'installation du fichier de licence sur le firewall sélectionné. Les informations concernant ce firewall sont modifiées et les nouvelles options sont activées sur le firewall.

REMARQUE
Les options nécessitant un redémarrage du firewall sont les changements de puissance de chiffrement et les cas d'ajout ou de retrait de cartes d'interfaces réseaux.
Pour être accessibles, ces modules même physiquement installés nécessitent l'installation de la licence appropriée, suivie d'un redémarrage.

Configuration avancée

Ici, vous définissez la fréquence de recherche de mise à jour ainsi que le type d'installation (manuelle ou automatique).

Rechercher les mises à jour de licence	Indication de la fréquence de recherche. Si une licence est trouvée, dans ce cas une notification est indiquée dans le panneau d'informations de l'onglet *Général*, de type « ! Une nouvelle licence est disponible pour U30XXA32100950 ».

Installation de la licence après téléchargement	• Si vous sélectionnez **toujours manuelle** (via le bouton **« installer une nouvelle licence »**), le bouton **Installer la nouvelle licence** s'affiche dès qu'une licence est proposée. Il est alors possible de comparer la nouvelle licence avec la licence actuelle dans l'onglet *Détails de la licence*. Si la licence vous convient, il suffit de cliquer sur **Installer la nouvelle licence**. Un message de notification s'affiche en vous indiquant que la licence actuelle est à jour. • Si vous sélectionnez **automatique lorsque c'est possible (pas de redémarrage requis)**, le boîtier installe la licence. Notez qu'il existe différents messages de notification : ◦ « *Licence Update : une nouvelle licence est disponible* » sera affiché, lorsque tel sera explicitement le cas. Chaque message est associé à une alarme (ici *68*). ◦ Il est également possible de trouver : *69*= « *Licence Update: Licence temporaire, enregistrement nécessaire* » ou encore *71*= « Licence Update: Une nouvelle licence a été installée » Ces messages sont visibles dans les alertes SNMP ou syslog. Afin d'activer l'envoi de ces messages, vous pouvez vous rendre dans le menu **Notifications,** Écran **Traces-Syslog** ou **Agent SNMP**.

L'onglet Licence locale

Cet onglet affiche la licence en vigueur du firewall sur lequel vous êtes connecté (firewall actif dans le cas d'une configuration en haute disponibilité). Il permet également la recherche et l'installation d'un nouveau fichier de licence pour ce firewall.

Les boutons

Rechercher une nouvelle licence	Ce bouton sert à la recherche d'une nouvelle licence ou actualise la date de dernière vérification de licence. **NOTE** Dans cet onglet, le bouton permet une recherche de licence de tous les firewalls du cluster HA.
Installer la nouvelle licence	Si le firewall a trouvé une licence par le biais du bouton **Rechercher une nouvelle licence**, le bouton **Installer la nouvelle licence** apparaît en clair. En cliquant dessus, un téléchargement est réalisé. Puis il suffit de confirmer ou non ce téléchargement. **NOTE** Dans cet onglet, le bouton permet l'installation de la licence pour le firewall indiqué.
Tout fermer	Rétracte l'arborescence des fonctionnalités de la licence.
Tout dérouler	Déploie l'arborescence des fonctionnalités de la licence.

La grille

Fonctionnalité	Indication des fonctionnalités et des options de chaque fonctionnalité que propose le firewall. Les fonctionnalités sont : « Administration », « Date d'expiration », « Options », « Global », « Matériel », « Limites », « Réseau », « Proxy », « Services » et « VPN ».
En cours (licence actuelle)	Indication, pour la licence installée, de l'activation ou non des options pour chaque fonctionnalité, ou de l'état d'expiration. Un symbole explicite indique l'activation de la fonctionnalité, un autre symbole la désactivation d'une option. Des symboles et couleurs font la différence entre une option bientôt expirée (moins de 90 jours de la date d'expiration), une option expirée et une option en cours de validité.
Nouvelle licence	Cette colonne ne s'affiche que si une nouvelle licence est disponible mais pas encore installée, et qu'un redémarrage est nécessaire (en d'autres termes, cette colonne ne s'affichera jamais si vous avez coché dans la configuration avancée de l'onglet *Général* l'option **Installation de la licence après téléchargement automatique lorsque c'est possible (pas de redémarrage requis)**. Lorsqu'une nouvelle licence est disponible, cette colonne présente les nouvelles valeurs en comparaison des valeurs de la licence actuelle indiquées dans la colonne « En cours (licence actuelle)». Des symboles et des couleurs indiquent une amélioration de valeur par rapport à la valeur de la licence actuelle ou une régression. Si l'option n'a pas changé, rien n'est indiqué.
Manager	Administration possible via l'interface Web. (Valeur par défaut : 1).
Monitor	Monitoring possible via Stormshield Network REALTIME MONITOR (Valeur par défaut : 1).
Antispam listes noires DNS (RBL)	Date limite de mise à jour des bases de spams DNSBL.
Antivirus ClamAV	Date limite de mise à jour des bases virales ClamAV.
Garantie Express	Date limite pour la Garantie Express. Cela permet de limiter l'attente du client dans la réparation de son produit.
Industriel	Date limite de l'option permettant l'analyse des protocoles industriels.
Fin de validité de la licence	Date d'expiration de la licence.
Signatures de protection contextuelle	Date limite de mise à jour des signatures de protection contextuelle (moteur de prévention d'intrusion).
Antispam : moteur heuristique	Date limite de mise à jour du moteur heuristique de filtrage des spams.
Sandboxing Breach Fighter	Date limite d'analyse de fichiers via le sandboxing.
Bases d'URL embarquées	Date limite de mise à jour des bases de filtrage d'URL Stormshield Network.

Bases d'URL Extended Web Control	Date limite de mise à jour des bases de filtrage d'URL Stormshield Network Extended Web Control.
Mise à jour	Date limite de mise à jour du boîtier.
Antivirus avancé	Date limite de mise à jour des bases virales avancées.
Management de vulnérabilités	Date limite de mise à jour des vulnérabilités SEISMO.
Garantie	Date limite pour la garantie.

Signatures de protection contextuelle personnalisées	Permet la création de signatures personnalisées pour le moteur de prévention d'intrusion.
Garantie Express	Garantie express qui permet de limiter l'attente du client dans la réparation de son produit.
Annuaire externe (LDAP)	Active ou désactive l'utilisation d'un annuaire LDAP (Valeur par défaut : 1*)
Haute Disponibilité	Permet de définir un boîtier maître et un esclave dans un cluster HA. (Master/Slave/None).
Industriel	Active ou désactive l'option permettant l'analyse des protocoles industriels.
PKI	Active ou désactive la PKI interne. (Valeur par défaut : 1)
Management de vulnérabilités	Active ou désactive SEISMO. (Valeur par défaut : 0)

Commentaire	Commentaire.
Id	Identifiant unique.
Temporaire	Licence temporaire (tant que le boîtier n'a pas été enregistré) ou non. Valeur par défaut : 1 (en sortie d'usine), 0 une fois le produit enregistré.
Version	Version de la licence (vérifie la compatibilité format de licence/version du Firmware). La valeur par défaut est 9.

Carte de calculs cryptographiques	Présence d'une carte optionnelle de cryptographie. (Valeur par défaut : dépend du modèle).
Stockage externe	Présence d'une carte SD pour le stockage des logs
Interfaces réseau	Nombre maximum d'interfaces physiques. (Valeur par défaut : dépond du modèle).
RAID	Permet d'acheminer les données d'un disque dur à un autre lorsque l'un d'entre eux tombe.

Connexions	Nombre maximum de connexions passant par l'ASQ. (Valeur par défaut : 0 (= pas de limite)).
Réseau	Nombre maximum de réseaux gérés par l'ASQ. (Valeur par défaut : 0 (= pas de limite)).
Utilisateurs	Nombre maximum d'utilisateurs qui peuvent s'authentifier sur le boîtier. (Valeur par défaut : 0 (= pas de limite)).
Haute disponibilité de modems (dialup)	Active ou désactive la possibilité d'utiliser les dialups pour réaliser le/les lien(s) HA. (Valeur par défaut : 1).
Routage par interface	Permet de faire du routage par interface. Cette option est activée par défaut.
Répartition de charge des modems (dialup)	Active ou désactive le load-balancing sur les dialups. (Valeur par défaut : 1).
QoS	Active ou désactive la QoS. (Valeur par défaut : 1).
Antispam listes noires DNS (RBL)	Active ou désactive le filtrage des spams via DNSBL dans le proxy. (Valeur par défaut : 1).
Antivirus ClamAV	Active ou désactive l'antivirus ClamaV dans le proxy. (Valeur par défaut : 1).
Proxy FTP	Active ou désactive le proxy FTP. (Valeur par défaut : 1**).
Proxy HTTP	Active ou désactive le proxy http (Valeur par défaut : 1).
ICAP (URL)	Active ou désactive l'ICAP ReqMod. (Valeur par défaut : 1).
ICAP (Virus)	Active ou désactive l'ICAP RespMod. (Valeur par défaut : 1).
Proxy POP3	Active ou désactive le proxy POP3. (Valeur par défaut : 1).
Proxy SMTP	Active ou désactive le proxy SMTP. (Valeur par défaut : 1).
Sandboxing Breach Fighter	Active ou désactive l'analyse de fichiers via le sandboxing au travers du proxy.
Antispam : moteur heuristique	Active ou désactive le moteur heuristique de filtrage des spams. (Valeur par défaut : 0).
Bases d'URL embarquées	Active ou désactive le filtrage d'URL via la base Stormshield Network dans le proxy. (Valeur par défaut : 1).
Bases d'URL Extended Web Control	Active ou désactive le filtrage d'URL via la base Stormshield Network Extended Web Control dans le proxy. (Valeur par défaut : 0).
Antivirus avancé	Active ou désactive l'antivirus avancé dans le proxy. (Valeur par défaut : 0).
Authentication	Active ou désactive l'interface d'authentification utilisateur.
DHCP	Active ou désactive le service DHCP serveur/relai (Valeur par défaut : 1).
DNS	Active ou désactive le service DNS cache. (Valeur par défaut : 1).

DNS dynamique	Active ou désactive le client DynDNS de mise à jour de serveur DNS.
Enrôlement	Active ou désactive l'enrôlement. (Valeur par défaut : 1).
Base LDAP interne	Active ou désactive la base LDAP interne (Valeur par défaut : 1).
NTP	Active ou désactive la synchronisation de temps NTP (Valeur par défaut : 1).
Annuaire public (LDAP)	Active ou désactive l'accès public au LDAP interne (Valeur par défaut : 1*).
SNMP	Active ou désactive l'agent SNMP. (Valeur par défaut : 1*).

Tunnels VPN IPsec anonymes	Active ou désactive la possibilité de monter des tunnels anonymes. (Valeur par défaut : 1*).
PPTP	Active ou désactive les tunnels PPTP. (Valeur par défaut : 1*).
VPN SSL	Active ou désactive le VPN SSL.
Chiffrement fort	Active ou désactive le support d'algorithmes forts pour l'encryptage dans les tunnels IPsec. (Valeur par défaut : 1*).
Nombre de tunnels VPN IPsec	Nombre maximal de tunnels IPsec. (Valeur par défaut : 0 (=pas de limite)).

L'onglet Licence du firewall distant *N° de série du firewall distant*

Cet onglet n'est présent que pour une configuration en haute disponibilité (*cluster*).

Il possède exactement les mêmes caractéristiques que L'onglet Licence du firewall local et permet la recherche et l'installation d'un nouveau fichier de licence sur le firewall distant.

MANAGEMENT DES VULNERABILITES

Ce menu vous permet de configurer votre politique de management des vulnérabilités susceptibles d'apparaître sur votre réseau.

Vous pouvez assigner un profil de supervision à une machine, un réseau, un groupe ou une plage d'adresses. Il en existe 12 pré-configurés par défaut.

La configuration du management des vulnérabilités consiste donc simplement à :

- Effectuer le lien entre objets réseau et profils de supervision,
- Décider des destinataires qui recevront les rapports de vulnérabilités.

L'écran de configuration de **Management des vulnérabilités** se divise en 2 zones :

- Une zone de **Configuration générale** : elle comporte une case d'activation du module et des éléments de configuration générale.
- **Configuration avancée :** une zone pour déterminer la durée de vie d'une information et pour les objets exclus.

AVERTISSEMENT
L'index des applications est basé sur l'adresse IP de la machine initiant le trafic.
Une même adresse IP partagée par plusieurs utilisateurs peut entraîner une charge importante sur le module. Ces cas sont par exemple, l'usage d'un proxy HTTP, d'un serveur TSE ou d'un routeur réalisant du NAT dynamique de la source. Il est donc conseillé de mettre ces adresses IP partagées dans la liste d'exclusion.

Configuration générale

Activer la détection d'applications et de vulnérabilités	En cochant cette option, la détection des vulnérabilités est activée et les informations seront visibles depuis le module **Monitoring** > **Supervision** > **Machines**. Notez que lors de la mise à jour (et si vous avez acquis la licence), le module Management de Vulnérabilités sera activé par défaut. La remontée d'alertes se fera en fonction de la configuration par défaut : surveiller l'ensemble des vulnérabilités pour toutes les machines internes. Pensez à mettre à jour la base de vulnérabilités dans **Système** > **Active Update**. Sans une base à jour, le service ne peut fonctionner correctement. La détection des vulnérabilités repose sur l'analyse du trafic réseau. Cela permet de détecter une application et / ou une faille, dès la première activité de l'utilisateur.
Envoyer les rapports simples à	Groupe d'adresses e-mail à qui seront envoyés des rapports synthétiques. Ces rapports sont succincts et comportent un résumé des vulnérabilités par produit et des machines affectées.
Envoyer les rapports détaillés à	Groupe d'adresses e-mail à qui seront envoyés les rapports complets. Les rapports détaillés comportent un résumé des vulnérabilités, ainsi que leur description détaillée (famille, client, possibilité d'exploitation à distance), ainsi qu'un lien vers sa référence dans la base de connaissances Stormshield Network, qui inclut généralement des indications sur le correctif à appliquer.

REMARQUE
Les groupes d'adresses e-mail se configurent le menu : **Notifications** > **Alertes e-mail** > onglet **Destinataires**.

Liste des éléments réseaux sous surveillance

Dans la grille, se trouve la liste des objets surveillés avec le profil de supervision qui leur est associé.

Élément réseau (machine ou groupe – réseau – plage d'adresses)	Choix de l'objet réseau pour lequel s'applique la surveillance. Cet objet est analysé par le moteur Stormshield Network Vulnerability Manager qui se basera sur les règles contenues dans le profil de supervision associé. L'objet lié au profil ne peut être qu'une machine, un groupe de machines, un réseau ou une plage d'adresses. La liste des éléments surveillés est prise en compte de manière ordonnée. Cela signifie que si un élément réseau est présent plusieurs fois dans cette liste, seul le premier profil de supervision s'appliquera. Il est possible de créer un objet au sein de la colonne à l'aide du bouton
Profil de supervision	Permet de choisir un profil pour restreindre les applications à surveiller. La sélection du profil se fait dans la liste déroulante de la colonne, qui s'affiche en cliquant sur la flèche de droite, lorsque vous ajoutez une ligne au tableau (voir bouton **Ajouter** ci-dessous).

Vous pouvez réaliser différentes actions à partir de cette grille :

Ajouter	Ce bouton permet d'ajouter un objet réseau et un profil associé à cet objet à la liste des éléments supervisés. En cliquant sur ce bouton, une ligne vide s'affiche dans le tableau.
Supprimer	Sélectionnez l'association objet –profils à supprimer puis cliquez sur le bouton. Attention : aucun message ne vous demande de confirmer la suppression du profil.
Monter	Permet d'élever la priorité de l'association entre un élément réseau et un profil.
Descendre	Permet de réduire la priorité de l'association entre un élément réseau et un profil.

Voici la liste des profils et des familles de vulnérabilités qui vont être détectés et signalés :

SERVEURS	APPLICATIONS CLIENTES ET SYSTEMES D'EXPLOITATION	CLIENTS	OUTILS
Serveurs : Serveurs SSH – Serveurs HTTP / Web – Serveurs de Bases de Données – Serveur FTP – Serveurs Mail et Systèmes d'Exploitations **Serveurs - failles critiques** : SSH-Web-Apps-DB-DNS-Web Server-FTP Server-Misc-Mail Server-P2P-OS	**Applications clientes et systèmes d'exploitation (OS)** **Applications clientes et des systèmes d'exploitation (OS) – failles critiques**	**Client mail** : Client, Mail (Thunderbird, Outlook, e-mail …)	**Outils de sécurité** : Antivirus, Outils de Sécurisation et Scanner de vulnérabilités ou de réseaux

Serveurs FTP	**Navigateurs et autres clients web** : Clients web, lecteurs de flux RSS	**Outils d'administration** : Client d'administration FTP, SSH etc.
Serveurs de mail		
Serveurs web : serveurs de contenu web/HTTP		
Serveurs base de données (SQL)		

Le profil « Toutes les applications connues »

Il permet d'attribuer à un objet (machine, groupe, réseau ou plage d'adresses), la détection de toutes les vulnérabilités clientes / serveurs et systèmes d'exploitation détectées par Stormshield Network Vulnerability Manager.

Configuration avancée

Durée de vie d'une information (jours) [1 – 30] : Durée de rétention de l'information (application, vulnérabilité) sans trafic ou sans mise à jour détecté.

Liste d'exclusion (éléments non supervisés)

Élément surveillé (machine ou groupe – réseau – plage d'adresses)	Une fois les objets associés à un profil, il est possible d'exclure un ou plusieurs objet (s) de l'analyse. Ainsi, quelle que soit la configuration des éléments supervisés, les membres de cette liste d'exclusion ne seront pas surveillés. Le choix des objets à exclure s'effectue à partir de cette grille en cliquant sur le bouton **Ajouter**.

AVERTISSEMENT
L'inventaire d'applications réalisé par Stormshield Network Vulnerability Manager se base sur l'adresse IP de la machine initiant le trafic pour indexer les applications.
Le cas de machines ayant une adresse IP partagée par plusieurs utilisateurs, par exemple un proxy HTTP, un serveur TSE ou encore un routeur réalisant du NAT dynamique de la source, peuvent entraîner une charge important sur le module. Il est donc conseillé de mettre les adresses de ces machines dans la liste d'exclusion (éléments non supervisés).

MAINTENANCE

Le module **Maintenance** va vous permettre d'effectuer les réglages et les contrôles de vérification nécessaires au bon fonctionnement de votre équipement.

Via l'interface, il est possible d'établir une configuration sécurisée de votre firewall, de procéder à des sauvegardes et des mises à jour de votre système, comme l'indiquent les 4 onglets suivants :

- **Mise à jour du système**,
- **Sauvegarder**,
- **Restaurer**,
- **Configuration**.

Onglet Mise à jour du système

> **NOTE**
> Dans le cas d'un cluster de firewalls en haute disponibilité (HA), la procédure à suivre est spécifique et doit respecter les étapes décrites dans la section Mise à jour logicielle d'un cluster de la note technique *Haute disponibilité sur SNS*.

Mises à jour disponibles

Si une mise à jour est disponible, elle s'affiche dans la zone **Mises à jour disponibles**.

Dans le cas où l'accès au serveur de mise à jour est impossible ou si vous souhaitez installer une autre version, téléchargez-la depuis votre espace personnel MyStormshield en vous reportant à la procédure Télécharger la dernière version disponible pour un produit.

Télécharger cette mise à jour	Ce lien n'apparaît que si une nouvelle mise à jour est disponible. Il permet de télécharger la mise à jour (fichier *maj*).
Notes de version	Ce lien n'apparaît que si une nouvelle mise à jour est disponible. Il permet de télécharger les Notes de version applicables à la version du firmware proposée au téléchargement.
sha1	Ce lien n'apparaît que si une nouvelle mise à jour est disponible. Il permet d'afficher l'empreinte SHA1 du fichier de mise à jour.
Rechercher de nouvelles mises à jour	Le firewall effectue une recherche des nouvelles mises à jour du système sur les serveurs *update* (**Objets > Objets réseau**) et les affiche à l'écran.

Mise à jour du système

Sélectionner la mise à jour	Cliquez sur le bouton ... et sélectionnez la mise à jour à installer.

Mettre à jour le firewall	Appliquez la mise à jour sélectionnée sur votre firewall en cliquant sur ce bouton.

> **NOTE**
> Effectuer une mise à jour vers une version précédente n'est pas supporté et peut causer des instabilités. Une remise à zéro du produit sera nécessaire.

Configuration avancée

Action

Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le Firewall	En cochant cette option, vous sauvegardez la partition principale de votre système sur la partition de secours, afin d'en conserver une trace. En effet, le firewall va redémarrer à la fin du processus de mise à jour.
Télécharger le firmware et l'activer	Cette option permet d'envoyer le fichier de mise à jour (.maj) et de l'activer.
Télécharger le nouveau firmware	Cette option permet d'envoyer le fichier de mise à jour sans l'activer. Il est ensuite possible de l'activer via l'option ci-dessous **Activer le firmware précédemment téléchargé**.
Activer le firmware précédemment téléchargé	Si un fichier se trouve sur le firewall, cette option permet de l'activer. La version indiquée est présente dans le champ **Mise à jour présente sur le firewall**.

Version actuelle du système

Ce champ affiche la version logicielle actuelle de votre produit.

Mise à jour présente sur le firewall

Ce champ affiche la mise à jour que vous avez sélectionnée préalablement en haut de cet écran.

Onglet Sauvegarder

Via cet écran, vous pouvez effectuer une sauvegarde manuelle ou programmer une sauvegarde automatique de la configuration du firewall.

Sauvegarde de configuration

Nom donné à la sauvegarde	Par défaut, le nom de la sauvegarde proposé est **<numéro de série du firewall>_jour_mois_année.na**. Vous pouvez modifier ce nom si besoin.
Télécharger la sauvegarde de configuration	Cliquez sur ce bouton pour enregistrer la sauvegarde. Le fichier sera sauvegardé au format *.na*.

Configuration avancée

Mot de passe / Confirmer	Définissez un mot de passe pour protéger votre sauvegarde. Il est fortement recommandé de protéger le fichier de sauvegarde par un mot de passe robuste. Conservez-le soigneusement., toute restauration sera impossible sans ce dernier et il n'est pas possible de le changer ni de le réinitialiser. Notre support technique n'a pas la possibilité de le récupérer ni de le réinitialiser.
Robustesse du mot de passe	Cette jauge indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser des combinaisons de lettres minuscules et majuscules, des chiffres ainsi que des caractères spéciaux.
Mot de passe du TPM	Lorsque le firewall dispose d'un TPM et que celui-ci a été initialisé, il est nécessaire de saisir le mot de passe du TPM pour réaliser une sauvegarde de configuration. La sauvegarde contient toutes les clés privées de certificats du firewall, mais celles protégées par le TPM sont incluses déchiffrées. Pour plus d'informations, reportez-vous à la section Trusted Platform Module.

Sauvegarde automatique de configuration

La sauvegarde automatique de configuration est effectuée de manière périodique et sécurisée. Les informations concernant la dernière sauvegarde sont disponibles sur le **Tableau de bord** du firewall, widget **Services**.

> **NOTE**
> Pour bénéficier de ce service, le firewall doit être sous maintenance.

Lorsque le firewall dispose d'un TPM et que celui-ci a été initialisé, la sauvegarde contient toutes les clés privées de certificats du firewall, et celles protégées par le TPM sont incluses chiffrées. Pour plus d'informations, reportez-vous à la section Trusted Platform Module.

ON / OFF	Positionnez le sélecteur sur ON pour activer l'envoi périodique d'une sauvegarde de configuration du firewall.
Configuration	• **Cloud backup** : ces sauvegardes sont stockées sur au sein de l'infrastructure de services Cloud par communication chiffrée. • **Serveur personnalisé** : ces sauvegardes sont stockées sur un serveur personnalisé (HTTP/HTTPS local ou externalisé), selon les critères choisis ci-après.

Configuration avancée

Fréquence des sauvegardes	La sauvegarde automatique peut être effectuée tous les jours, tous les 7 jours ou tous les 30 jours.
Mot de passe du fichier de sauvegarde	Il est fortement recommandé de protéger le fichier de sauvegarde par un mot de passe robuste. Conservez-le soigneusement., toute restauration sera impossible sans ce dernier et il n'est pas possible de le changer ni de le réinitialiser. Notre support technique n'a pas la possibilité de le récupérer ni de le réinitialiser.

Serveur personnalisé

Si vous avez sélectionné une sauvegarde sur un serveur personnalisé, vous devez renseigner sa configuration :

URL du serveur	Emplacement utilisé pour le dépôt des sauvegardes. Cette URL est définie lorsque les champs **Serveur de sauvegarde**, **Port du serveur**, **Protocole de communication** et **Chemin d'accès** sont complétés.
Serveur de sauvegarde	Sélection d'un serveur personnalisé. Assurez-vous que la résolution du serveur sélectionné soit conforme à celle escomptée.
Nom donné à la sauvegarde	Indiquez le nom attribué au fichier de sauvegarde.
Port du serveur	Port d'écoute du serveur pour la réception des sauvegardes.
Protocole de communication	Choix du protocole utilisé pour l'émission des sauvegardes entre HTTP et HTTPS. Le protocole HTTPS nécessite de renseigner un certificat afin que le firewall puisse s'assurer de l'identité du serveur avant de lui transmettre la sauvegarde.
Certificat du serveur	Dans le cas du choix d'un protocole en HTTPS, importez puis sélectionnez le certificat du serveur dans ce champ, afin que le firewall puisse l'authentifier.
Chemin d'accès	Selon la méthode d'envoi sélectionnée ci-dessous, le chemin d'accès peut être un dossier (*/directory/*) pour les méthodes WebDAV (auth) ou un script (*/upload.php*) pour la méthode POST.
Méthode d'envoi	Les modes *Basic* et *Digest* (RFC 2617) sont des modes permettant l'identification du firewall sur le serveur à l'aide d'un identifiant et d'un mot de passe : • **auth basic** : ce mode transmet le mot de passe encodé mais en clair. Il est donc préconisé de l'utiliser avec une communication HTTPS. • **auth digest** : ce mode permet une identification sans transmettre le mot de passe en clair ; ce mode est plus sécurisé que le mode *basic*. Il est préconisé lors de l'utilisation d'une communication HTTP. • **POST** : l'identification par cette méthode n'étant pas géré, il est donc conseillé de l'employer avec une communication HTTPS.
Identifiant	En cas d'utilisation d'une méthode d'envoi avec identification (*auth basic* ou *auth digest*), cet identifiant permet l'authentification du firewall par le serveur.
Mot de passe de la sauvegarde	En cas d'utilisation d'une méthode d'envoi avec identification (*auth basic* ou *auth digest*), ce mot de passe permet l'authentification du firewall par le serveur.
POST - control name	En cas d'utilisation de la méthode d'envoi POST, ce champ indique le nom de contrôle présent dans l'en-tête des paquets HTTP.

Onglet Restaurer

Cet écran permet de restaurer une sauvegarde précédemment effectuée.

Restauration de configuration

Sauvegarde à restaurer	Sélectionnez dans ce champ le fichier de sauvegarde au format *.na* à restaurer. De manière générale, une sauvegarde contenant des clés privées de certificats protégées par le TPM ne peut être restaurée que sur le firewall source. Pour plus d'informations, reportez-vous à la section Trusted Platform Module.

Restaurer la configuration à partir du fichier de sauvegarde	Cliquez sur ce bouton pour restaurer la configuration du firewall à partir du fichier sélectionné. Vous pouvez être amené à redémarrer le firewall selon la sauvegarde restaurée. Si un redémarrage est nécessaire, il est proposé de redémarrer maintenant ou plus tard.

Configuration avancée

Mot de passe de la sauvegarde	Si vous avez protégé la sauvegarde sélectionnée par un mot de passe, saisissez-le dans ce champ. Sans celui-ci, toute restauration sera impossible.
Modules à restaurer	Il est possible d'effectuer une restauration totale ou partielle de la configuration de votre firewall. La case **Restaurer tous les modules du fichier de sauvegarde** est cochée par défaut. Elle permet de restaurer l'intégralité des modules contenus dans le fichier de sauvegarde. Si vous souhaitez restaurer une partie des modules du fichier de sauvegarde, décochez la case **Restaurer tous les modules du fichier de sauvegarde** puis cochez les modules dont vous souhaitez restaurer la configuration.

Restauration de sauvegarde automatique

Date de la dernière sauvegarde	Date de la dernière sauvegarde effectuée de votre configuration, disponible sur le serveur local ou externalisé.
Restaurer la configuration à partir de la sauvegarde automatique	Cliquez sur ce bouton afin de procéder à la restauration de la configuration du firewall, via le fichier sélectionné ci-dessus. Vous pouvez être amené à redémarrer le firewall selon la sauvegarde restaurée. Si un redémarrage est nécessaire, il est proposé de redémarrer maintenant ou plus tard.

Configuration avancée

Mot de passe de la sauvegarde	Si vous avez protégé la sauvegarde sélectionnée par un mot de passe, saisissez-le dans ce champ. Sans celui-ci, toute restauration sera impossible.

Onglet Configuration

Disque système

Vous utilisez actuellement la partition	Le disque système de votre firewall est découpé en deux partitions permettant de sauvegarder vos données. Cette section indique la partition sur laquelle le produit a démarré.
Partition principale	Version de firmware installée sur la partition principale.
Partition de secours	Version de firmware installée sur la partition de secours.

Au démarrage, utiliser la partition	Choisissez la partition de démarrage du produit : la partition principale ou de secours. • **Partition principale** : si vous cochez cette option, votre firewall utilisera cette partition au démarrage. • **Partition de secours** : la partition de secours représente votre dernière partition sauvegardée. Si vous cochez cette option, votre firewall utilisera cette partition au démarrage.
Sauvegarder la partition active	Ce bouton permet de sauvegarder la partition active (celle indiquée par **Vous utilisez actuellement la partition**) sur l'autre partition.

Maintenance

Redémarrer le firewall	Cliquez sur ce bouton pour redémarrer directement votre firewall.
Arrêter le firewall	Cliquez sur ce bouton si vous souhaitez éteindre votre firewall.

Haute disponibilité

Forcer un firewall à rester actif	Dans le cas où les deux firewalls de votre groupe HA se retrouvent dans l'état actif ou démarrent en même temps, cette option permet de désigner l'un des membres comme prioritaire pour rester actif. **NOTE** Avant de définir un firewall distant comme prioritaire, vérifiez que vos firewalls sont synchronisés. En effet, les modifications de configuration en cours sur votre firewall actif seraient alors perdues lors de la bascule.

Rapport système (sysinfo)

Télécharger le rapport système	Ce bouton permet d'obtenir des informations diverses sur votre firewall au format *sysinfo*. Il est possible de connaître par son biais : le modèle du firewall, son numéro de série, son état de fonctionnement actuel, l'état de sa mémoire, etc.

MESSAGES DE BLOCAGE

L'écran de configuration du module **Messages de blocage** est composé de deux parties :

- L'onglet **Antivirus** : détection d'un virus attaché aux documents, pouvant intervenir au cours de l'envoi et de la réception de mails (POP3, SMTP) ou via le transfert de fichiers (protocole FTP).
- L'onglet **Pages de blocage** : page affichée lors d'une tentative d'accès à un site (HTTP / HTTPS) non autorisé par les règles de filtrage URL et de filtrage SSL.

L'onglet Antivirus

Protocole POP3

Contenu de l'e-mail

Ce champ permet de modifier le texte du message reçu si un virus est détecté dans un mail.

> **EXEMPLE**
> Le firewall Stormshield Network a détecté un virus dans cet e-mail, il a été extrait par l'antivirus intégré, les pièces jointes infectées ont été supprimées.

Protocole SMTP

Code d'erreur SMTP

Limité à 3 chiffres, ce champ permet de définir le code d'erreur que le serveur SMTP recevra si un virus est détecté dans un mail envoyé.

> **EXEMPLE**
> 554

Message associé

Ce champ contient le message informationnel qui sera envoyé au serveur SMTP en cas de détection d'un virus.

> **EXEMPLE**
> 5.7.1 Virus détecté.

Protocole FTP

Code d'erreur FTP

Limité à 3 chiffres, ce champ contient le code d'erreur que l'utilisateur ou le serveur FTP recevra si un virus est détecté dans un fichier transféré.

> **EXEMPLE**
> 425

Message associé	Cet emplacement est réservé au message informationnel qui sera envoyé avec le code d'erreur lors de la détection d'un virus au sein de l'envoi / de la réception d'un fichier vers / depuis un serveur FTP. **EXEMPLE** Virus détecté. Transfert interrompu.

L'onglet Page de blocage

Cette fenêtre présente par défaut la page de blocage HTTP / HTTPS qui est affichée lors d'une tentative d'accès à un site bloqué par les règles de filtrage URL ou de filtrage SSL. Dans une règle de filtrage, le choix est donné entre 4 versions de pages de blocage.

Une page de blocage se compose par défaut d'une icône et d'un message explicite permettant de comprendre pourquoi la page est bloquée, et de savoir par exemple, à quelle catégorie d'URL appartient le site web non autorisé.

EXEMPLE
Cette page n'est pas autorisée par la politique de la société. Elle fait partie de la catégorie : « Jeux ».

La page de blocage est totalement personnalisable : il s'agit d'une page au format HTML/CSS. Vous pouvez décider d'afficher un logo seul, une phrase seule, ou la combinaison des deux. Chaque champ présent dans la page peut être modifié: le logo, la police de caractères, sa taille ou encore sa couleur.

Chacune des 4 pages HTML personnalisables supportent le multi-langage, c'est-à-dire que le message affiché peut être décliné en différentes langues. La version du texte affiché lors du blocage sera choisie en fonction de la langue par défaut du navigateur.

Enfin, une notification e-mail à l'administrateur peut y être associée pour demander le déblocage de l'accès à un site Web.

Onglets des pages de blocage

Chacune des 4 pages de blocage est directement éditable depuis l'interface Web d'administration. Il est également possible de leur appliquer l'une des actions suivantes :

Renommer	Permet de personnaliser le nom de la page de blocage courante.
Réinitialiser	Permet de rétablir les données de la page de blocage proposée par défaut.
Copier vers	Permet de copier les paramètres de la page de blocage courante et d'appliquer ce modèle à l'une des 3 autres pages de blocage.

L'édition des pages de blocage

Vous pouvez personnaliser la page par le remplacement de l'image affichée dans la page. La page HTML propose également la gestion de plusieurs langues.

Selon la langue, il est possible de personnaliser le message affiché lors du blocage, ainsi qu'un éventuel e-mail de notification à l'administrateur pour une demande de catégorisation ou de déblocage d'accès au site Web bloqué.

La page est déclinée en plusieurs langues par défaut et offre la possibilité d'en ajouter de nouvelles

Des variables existent, permettant de rendre dynamiques les informations contenues, comme les catégories auxquelles appartiennent les sites bloqués.

Ces variables sont les suivantes :

$host	Nom de domaine interrogé (ex : www.google.com)
$url	Page du domaine interrogé
$protected_url	Page du domaine interrogé – encodée dans un format manipulable par le navigateur ou le client mail
$user	Nom de l'utilisateur authentifié (s'il est connu)
$src	Nom de la source ou son adresse IP
$url_group	Nom du groupe de catégorie
$protected_url_group	Nom du groupe de catégorie - encodée dans un format manipulable par le navigateur ou le client mail
$cat_group	Nom de la catégorie URL
$protected_cat_group	Nom de la catégorie - encodée dans un format manipulable par le navigateur ou le client mail
$url_rule	Numéro de la règle de blocage de la politique de filtrage URL
$url_policy	Numéro de la politique de filtrage URL

Pour afficher l'URL complète, il faut concaténer les 2 variables comme suit : **$host$url**

OBJETS RÉSEAU / TEMPS

Ce module regroupe les objets réseau et les objets temps. Il est divisé en deux parties :

- La barre d'actions en haut, permettant de trier et de manipuler les objets.
- Deux colonnes dédiées aux objets : l'une les listant par catégorie, et l'autre affichant leurs propriétés.

NOTE
La création d'objets permet de déclarer un objet en mode Global, uniquement si l'option "Afficher les politique globales (Filtrage, NAT et VPN IPsec)" est activée dans le module **Préférences**.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Caractères autorisés ou interdits.

La barre d'actions

Rechercher

Si vous recherchez un objet en particulier, saisissez son nom.
Le champ de recherche vous permet de lister tous les objets réseau dont les propriétés correspondent au(x) mot(s) ou lettre(s) clé(s) saisie(s).

EXEMPLE
Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous objets possédant un « a » dans leur nom ou dans leur description.

Vous pouvez également affiner la recherche en fonction du « filtre » listant les différents types d'objets (voir bouton « Filtre » ci-après).

NOTE
L'icône croix dans le champ de recherche permet de supprimer la saisie et lister tous les objets en fonction du filtre courant.

NOTE
Lorsque vous vous rendez au sein de l'onglet *Objets* dans l'arborescence de gauche, le focus est désormais directement placé dans le champ dédié à la recherche.

Ajouter	Lorsque vous cliquez sur ce bouton, une boîte de dialogue s'affiche et vous propose de créer un objet, en indiquant son type et les informations lui étant relatives dans les champs appropriés. **REMARQUE** L'objet peut être défini comme « global » au moment de sa création si vous cochez l'option « *Cet objet est global* » au sein de la boîte de dialogue. Il apparaîtra lorsque vous opterez pour le filtre « Tous les objets » ou « Réseau » (voir ci-dessous) et sera matérialisé par l'icône suivante.
Supprimer	Sélectionnez l'objet à retirer de la liste et cliquez sur **Supprimer**.
Vérifier l'utilisation	Si vous cliquez sur ce bouton après avoir sélectionné un événement, le résultat s'affiche dans l'arborescence des modules.
Exporter	Lorsque vous cliquez sur ce bouton (matérialisé par l'icône), une fenêtre vous présente le lien de téléchargement de la base objets au format CSV. Cliquez sur ce lien pour enregistrer le fichier d'export sur votre ordinateur.
Importer	Lorsque vous cliquez sur ce bouton (matérialisé par l'icône), une fenêtre vous permet de sélectionner une base objets sous la forme d'un fichier CSV afin de l'importer dans le firewall. Les champs constituant une ligne type d'un fichier CSV sont détaillées dans la section Structure d'une base objets au format CSV. Une jauge vous permet de visualiser l'avancement du transfert de la base vers le firewall. NOTE Les objets déjà existants sur le firewall seront remplacés par les objets transférés correspondants.
Tout fermer	Ce bouton permet d'étendre l'arborescence des objets.
Tout dérouler	Ce bouton permet de regrouper l'arborescence des objets.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des objets réseau :

- **Supprimer** (l'objet sélectionné),
- **Vérifier l'utilisation** (de l'objet sélectionné).

Le filtre

Ce bouton permet de choisir le type d'objets à afficher. Un menu déroulant vous propose les choix suivants :

Tous les objets	Matérialisée par l'icône , cette option permet d'afficher dans la liste des objets à gauche, tous les types d'objets réseau.

Machine	Matérialisée par l'icône , cette option permet d'afficher uniquement les objets de type « machine » dans la colonne de gauche.
Nom DNS (FQDN)	Matérialisée par l'icône , cette option permet d'afficher uniquement les objets de type « Nom DNS (FQDN) » dans la colonne de gauche.
Réseau	Matérialisée par l'icône , cette option permet d'afficher uniquement les objets de type réseaux.
Plage d'adresses	Matérialisée par l'icône , cette option permet d'afficher uniquement les plages d'adresses IP et les plages d'adresses MAC.
Routeur	Matérialisée par l'icône , cette option permet d'afficher uniquement les objets de type routeur.
Groupe	Matérialisée par l'icône , cette option permet d'afficher uniquement les groupes de réseaux.
Protocole IP	Matérialisée par l'icône , cette option permet d'afficher uniquement les protocoles IP.
Port – plage de ports	Matérialisée par l'icône , cette option permet d'afficher les ports et les plages de ports.
Groupe de ports	Matérialisée par l'icône , cette option permet d'afficher uniquement les groupes de ports.
Objet temps	Matérialisée par l'icône , cette option permet d'afficher uniquement les objets temps.
Groupe de régions	Matérialisée par l'icône , cette option permet d'afficher uniquement les groupes géographiques.

Les différents types d'objets

Cette section détaille les différents types d'objets qui peuvent être définis sur le firewall.

Machine

Sélectionnez une machine pour visualiser ou éditer ses propriétés. Chacune d'entre elles possèdent par défaut un nom, une IP et une résolution DNS (« Automatique » ou « Aucune (IP statique »).

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer** » et « **Sauvegarder** » pour enregistrer le changement. L'icône à droite de la case permet d'obtenir l'IP de l'objet, visible au sein du champ « Adresse IP ». Pour cela, il faut avoir saisi l'url complète de l'objet.
Adresse IPv4	Adresse IP de la machine sélectionnée.

Résolution DNS	La résolution DNS (Domain Name System) associe des adresses IP et un nom de domaine. Deux choix sont possibles : • **Aucune (IP statique)** : L'objet sélectionné possède une adresse IP fixe qui sera utilisé systématiquement. • **Automatique** : Si vous cochez cette case, le firewall effectuera une requête DNS toutes les 5 minutes afin de déterminer l'adresse IP de l'objet sélectionné.
Adresse MAC	Media Access control adress. Elle correspond à l'adresse physique d'une interface réseau ou d'une carte réseau, permettant d'identifier une machine sur un réseau local. **EXEMPLE** 5E:FF:56:A2:AF:15.
Commentaire	Description associée à la machine sélectionnée.

Nom DNS (FQDN)

Les objets de type Nom DNS sont des objets dynamiques représentant des noms DNS (FQDN) pouvant être résolus sur plusieurs adresses IP. Ces objets peuvent être définis en IPv4 ou IPv6 et sont utilisables uniquement en source ou destination d'une règle de filtrage. Ils ne peuvent pas être inclus dans un groupe.

Sélectionnez un nom DNS pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable. cliquez sur « **Appliquer** » ou « **Sauvegarder** » pour enregistrer le changement.
Adresse IP par défaut	Adresse IP de l'objet sélectionné.
Commentaire	Description associée au nom DNS sélectionné.

Réseau

Sélectionnez un réseau pour visualiser ou éditer ses propriétés. Ils possèdent chacun un nom, une IP et un masque réseau. Ces objets peuvent être définis en IPv4 ou IPv6.

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer** » ou « **Sauvegarder** » pour enregistrer le changement.
Adresse IP	Adresse IP du réseau sélectionné. L'adresse est suivie du symbole "/" et du masque de réseau associé.
Commentaire	Description associée au réseau sélectionné.

Plage d'adresses

Sélectionnez une plage d'adresses pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer** » ou « **Sauvegarder** » pour enregistrer le changement.

Adresses IPv4

Début	Première adresse IP associée à la plage.
Fin	Dernière adresse IP associée à la plage.

Adresses MAC

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer** » ou « **Sauvegarder** » pour enregistrer le changement.
Début	Première adresse MAC associée à la plage.
Fin	Dernière adresse MAC associée à la plage.
Commentaire	Description associée à la plage d'adresses MAC sélectionnée.

Routeur

Les objets routeurs peuvent être utilisés :

- Comme passerelle par défaut pour le firewall,
- Comme passerelle dans des routes statiques (sauf pour les objets routeurs caractérisés par du partage de charge),
- Pour spécifier du routage au sein des règles de filtrage (PBR : Policy Based Routing).

Un objet routeur est défini par un nom et au minimum une passerelle utilisée. Il peut comporter une ou plusieurs passerelles utilisées et passerelles de secours. Un mécanisme de test de disponibilité de ces passerelles permet alors une notion de redondance : en cas de défaut de réponse d'une ou plusieurs passerelles principales, une ou plusieurs passerelles de secours prennent alors le relai. Une fois la passerelle principale redevenue active, la bascule depuis la passerelle de secours vers la passerelle principale est automatique.

Sélectionnez un routeur pour visualiser ou éditer ses propriétés.

Propriétés

Nom de l'objet	Nom donné à l'objet routeur lors de sa création.
Commentaire	Description associée à l'objet routeur.

Supervision

Les champs du cadre **Supervision** permettent de définir la méthode et les paramètres à utiliser pour vérifier la disponibilité des passerelles de l'objet routeur.

Méthode de détection	Deux méthodes de détection de l'état des passerelles peuvent être sélectionnées : • ICMP : la détection est basée sur l'envoi de requêtes ICMP (*ping*) et la réponse ou non des passerelles testées. • TCP Probe : la détection est basée sur la connexion à un service TCP hébergé par les passerelles composant l'objet routeur. Le choix de cette méthode provoque l'affichage d'un champ supplémentaire correspondant au port TCP du service à tester (HTTPS par défaut).

Port	Ce champ n'est affiché que si la méthode de détection TCP Probe a été choisie. Sélectionnez le port TCP à tester sur les passerelles constituant l'objet routeur. Le port *https* est proposé par défaut.
Délai d'expiration (s)	Indiquez le délai (en secondes) au delà duquel une requête n'ayant pas obtenu de réponse est considérée comme un échec.
Intervalle de tests (s)	Indiquez l'intervalle de temps (en secondes) entre deux requêtes.
Échecs avant dégradation	Indiquez le nombre de requêtes devant être en échec avant de déclarer le lien comme dégradé ou la passerelle comme injoignable.

SLA SD-WAN (seuils)

Cochez cette case pour afficher les contraintes sur des métriques réseau (latence, gigue, perte de paquets...) que doivent respecter les passerelles composant l'objet routeur pour assurer l'engagement de SLA lié au routeur.
Le respect ou non de ces valeurs détermine le statut des passerelles composant l'objet routeur, et donc le statut de l'objet routeur lui même. Ces statuts sont affichés dans le tableau de bord, le module de supervision SD-WAN et le module de supervision des Connexions.

Latence (ms)	Cette métrique représente le temps nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau. Par abus de langage, on parle du temps de latence lors du résultat en ms d'un *ping* vers la destination. Indiquez la latence maximale acceptée (en millisecondes) pour les passerelles composant l'objet routeur. Cette valeur doit être comprise entre 0 et 60000 millisecondes.
Gigue (ms)	Cette métrique représente l'évolution de la latence au fil du temps. Indiquez la gigue maximale acceptée (en millisecondes) pour les passerelles composant l'objet routeur. Cette valeur doit être comprise entre 0 et 30 millisecondes.
Taux de perte de paquets (%)	Cette métrique représente le pourcentage de perte que peut subir un message (envoi sans réponse). Cette valeur doit être comprise entre 0 et 100.
Taux d'indisponibilité (%)	Cette métrique représente le pourcentage de temps pendant lequel une passerelle a été hors-service ou inactive sur la période de mesure. Ce paramètre existe principalement afin d'afficher des statistiques concernant la disponibilité des passerelles.

NOTE
Avant d'activer un basculement en cas de non respect d'un des seuils SLA, il est recommandé de vérifier au préalable que ces seuils ne déclencheront pas à tort un basculement. Pour le vérifier, créez un objet routeur avec les seuils SLA souhaités et ajoutez-le en fin de votre politique de sécurité dans une règle qui ne sera jamais utilisée. L'objet apparaîtra alors dans le module **Supervision** et vous pourrez ainsi vous assurer que les seuils SLA sont correctement choisis.
Nous recommandons d'autant plus cette vérification dans le cas où la gigue est utilisée comme seuil SLA du fait que sa mesure est sensible aux éventuels micro-changements.

Grilles des passerelles utilisées et des passerelles de secours

Présentation de la barre de boutons

Ajouter	Ajoute une passerelle.
Supprimer	Supprime la passerelle sélectionnée.
Déplacer dans la liste de secours / Déplacer dans la liste principale	Permet de basculer une passerelle de la grille principale à la grille de secours ou de la grille de secours à la grille principale.

Les deux grilles comportent les colonnes ci-dessous :

Passerelle	Un clic dans une ligne de cette colonne ouvre la base d'objets afin de sélectionner une machine composant le routeur.
Poids	Permet d'affecter une priorité entre les différentes passerelles pour le mécanisme de répartition de charge. Une passerelle ayant un poids supérieur sera ainsi utilisée plus souvent lors de la répartition de charge des flux.
Cible(s) des tests	Machine ou groupe de machines à tester afin de définir la connectivité de la passerelle. La valeur sélectionnée peut être la passerelle elle-même (**Tester directement la passerelle**), une machine ou un groupe de machines tierces. Le test de disponibilité peut être désactivé pour la passerelle sélectionnée en choisissant la valeur **Pas de test de disponibilité.**
Commentaire	Texte libre.

NOTE
Il est fortement recommandé d'utiliser un groupe de machine comme cible des tests.

NOTE
Si la valeur **Pas de test de disponibilité** est sélectionnée pour l'ensemble des passerelles, la fonction de bascule vers les passerelles de secours est alors désactivée.

NOTE
Les paramètres définissant le délai entre deux tests de disponibilité (« frequency »), le délai d'attente maximum pour une réponse (« wait ») et le nombre de tests à réaliser avant de déclarer la passerelle injoignable (« tries ») sont exclusivement paramétrables via une commande CLI :

```
CONFIG OBJECT ROUTER NEW name=<router name> [tries=<int>]
[wait=<seconds>] [frequency=<seconds>] update=1.
```

Les valeurs recommandées sont de 15 secondes pour le paramètre « frequency », de 2 secondes pour le paramètre « wait » et de 3 pour le paramètre « tries ».

Configuration avancée

Répartition de charge	Le firewall permet d'effectuer un routage réparti entre les différentes passerelles utilisées selon plusieurs méthodes. • **Aucune répartition** : seule la première passerelle définie dans les grilles "Passerelles utilisées" et "Passerelles de secours" est utilisée pour le routage. • **Par connexion** : toutes les passerelles définies dans la grille "Passerelles utilisées" sont utilisées. L'algorithme de répartition de charge se base sur la source (adresse IP source, port source) et sur la destination (adresse IP destination, port destination) du trafic. Le taux d'utilisation des différentes passerelles sera lié à leur poids respectif. • **Par adresse IP source :** toutes les passerelles définies dans la grille "Passerelles utilisées" sont utilisées. Un algorithme permet de répartir le routage en fonction de la source qui est à l'origine du trafic routé. Le taux d'utilisation des différentes passerelles sera lié à leur poids respectif.
Activation des passerelles de secours	• **Lorsque toutes les passerelles sont injoignables** : la ou les passerelles de secours ne sont activées que lorsque toutes les passerelles utilisées sont injoignables. • **Lorsqu'au moins une passerelle est injoignable** : la ou les passerelles de secours sont activées dès qu'une passerelle utilisée est injoignable. Cette option est grisée lorsqu'une seule passerelle est renseignée dans la grille des passerelles utilisées. • **Lorsque le nombre de passerelles joignables est inférieur à** : la ou les passerelles de secours sont activées dès que le nombre de passerelles utilisées joignables devient inférieur au nombre indiqué. Cette option est grisée lorsqu'une seule passerelle est renseignée dans la grille des passerelles utilisées.
Activer toutes les passerelles de secours en cas d'indisponibilité	Lorsque cette case est cochée, toutes les passerelles de secours sont activées dès que la condition d'activation est remplie. Si elle est décochée, seule la première passerelle de secours listée sera activée.
Si aucune passerelle n'est disponible	Sélectionnez le comportement que le firewall doit adopter si toutes les passerelles définies au sein de l'objet routeur sont injoignables : • **Routage par défaut** : les routes (statiques ou dynamiques) définies dans la table de routage du firewall sont appliquées. • **Ne pas router** : les paquets ne sont pas pris en charge par le firewall.

Appliquer	Valide la configuration du routeur.
Copier	Permet de créer par duplication un nouvel objet routeur reprenant les mêmes caractéristiques.
Annuler	Annule la configuration du routeur.

Groupe

Cet écran va vous permettre d'agréger vos objets selon votre topologie réseau, par exemple.

Nom de l'objet	Nom donné au groupe d'objets lors de sa création. Les objets en « lecture seule » seront grisés et ne pourront pas être modifiés.

Commentaire	Description associée au groupe d'objets.
Éditer ce groupe	Un clic sur ce bouton déclenche l'affichage une boîte de dialogue d'ajout d'objet(s) au sein du groupe. **Nom de l'objet** : saisissez le nouveau nom du groupe si vous souhaitez le modifier. Deux colonnes sont affichées : • Celle de gauche comporte la liste de tous les objets réseau que vous pouvez ajouter à votre groupe, • La colonne de droite comporte les objets qui figurent déjà dans le groupe. Pour ajouter un objet dans le groupe, vous devrez le faire passer d'une colonne à une autre : 1. Sélectionnez le ou les éléments à ajouter. 2. Cliquez sur cette flèche-ci , l'objet bascule dans la colonne de droite et intègre votre groupe (en tête de la liste). Pour retirer un objet du groupe : 1. Sélectionnez-le dans la colonne de droite. 2. Cliquez sur cette flèche . **NOTE** En cliquant sur le bouton « Éditer ce groupe », vous pouvez, d'une part, changez le nom du groupe et lui attribuer un commentaire, et d'autre part, effectuer une recherche d'objet(s) et en inclure de nouveaux au sein du groupe.
Objets dans ce groupe	Vous visualisez les objets réseau figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

Protocole

Nom de l'objet	Nom du protocole sélectionné. Ce champ est grisé et non modifiable.
Numéro du protocole	Nombre ou chiffre associé au protocole sélectionné et fourni par l'IANA (Internet Assigned Numbers Authority).
Commentaire	Description associée au protocole sélectionné.

Port – plage de ports

Sélectionnez un port ou une plage de ports pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom du service utilisé. Ce champ est grisé et non modifiable.
Port	Numéro du port associé au service sélectionné.
Plage de ports	En cochant cette case, vous attribuerez une plage de ports au service sélectionné et dégrisez les deux cases du dessous.

Depuis	Si la case Plage de ports est cochée, ce champ est dégrisé. Il correspond au premier port inclus dans la plage de port sélectionnée.
Jusqu'à	Si la case Plage de ports est cochée, ce champ est dégrisé. Il correspond au dernier port inclus dans la plage de port sélectionnée.
Protocole	Choisissez le protocole IP utilisé par votre service : • **TCP** : Transmission Control Protocol. Protocole de transport fonctionnant en mode connecté et composé de trois phases : l'établissement de la connexion, le transfert des données, la fin de la connexion. • **UDP :** User Datagram Protocol. Ce protocole permet de transmettre les données de manière simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. • **SCTP** : Stream Control Transmission Protocol est un protocole défini dans la RFC 4960 (un texte d'introduction est fourni dans la RFC 3286). En tant que protocole de transport, SCTP est équivalent dans un certain sens à TCP ou à UDP. Alors que TCP est orienté flux (la séquence d'octets contenue dans un paquet n'a pas conceptuellement de début ou de fin, elle fait partie du flux constitué par la connexion), SCTP est, comme UDP, orienté message (au sein d'un flux, il transmet des messages avec un début et une fin, qui peuvent éventuellement être fragmentés sur plusieurs paquets). • **Tout protocole** : N'importe quel protocole IP pourra être utilisé par le service sélectionné.
Commentaire	Description associée au port ou à la plage de ports sélectionnés.

Si vous souhaitez ajouter un port pouvant être porté par UDP et TCP :

1. Créez un premier objet de type port basé sur TCP (exemple : MyTCPport = TCP/1234),
2. Créez un second objet de type port basé cette fois sur UDP (exemple : MyUDPport = UDP/1234),
3. Regroupez ces deux objets dans un objet de type Groupe de ports que vous pourrez utiliser dans votre configuration de firewall (exemple : MyPortGroup incluant MyTCPport et MyUDPport).

Groupe de ports

Cet écran va vous permettre d'agréger vos ports par catégorie.

Exemple

Un groupe « **mail** » regroupant les ports « imap », « pop3 » et « smtp ».

Nom de l'objet	Nom donné au groupe de ports lors de sa création.
Commentaire	Description associée au groupe de ports.

Éditer ce groupe	Un clic sur ce bouton déclenche l'affichage une boîte de dialogue d'ajout d'objet(s) au sein du groupe. **Nom de l'objet** : saisissez le nouveau nom du groupe si vous souhaitez le modifier. Deux colonnes sont affichées : • Celle de gauche comporte la liste de tous les objets réseau que vous pouvez ajouter à votre groupe, • La colonne de droite comporte les objets qui figurent déjà dans le groupe. Pour ajouter un objet dans le groupe, vous devrez le faire passer d'une colonne à une autre : 1. Sélectionnez le ou les éléments à ajouter. 2. Cliquez sur cette flèche-ci, l'objet bascule dans la colonne de droite et intègre votre groupe (en tête de la liste). Pour retirer un objet du groupe : 1. Sélectionnez-le dans la colonne de droite. 2. Cliquez sur cette flèche. **NOTE** En cliquant sur le bouton « Éditer ce groupe », vous pouvez, d'une part, changez le nom du groupe et lui attribuer un commentaire, et d'autre part, effectuer une recherche d'objet(s) et en inclure de nouveaux au sein du groupe.
Objet dans ce groupe	Vous visualisez les objets réseau figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

Groupe de régions

Cet écran va vous permettre d'agréger des pays ou continents au sein d'un groupe.

Nom de l'objet	Nom donné au groupe de régions lors de sa création.
Commentaire	Description associée au groupe de régions.

Éditer ce groupe	Ce bouton comporte une boite de dialogue permettant d'ajouter des pays ou continents au sein du groupe. Lorsque vous cliquez dessus, vous pouvez, d'une part, changer le nom du groupe et lui attribuer un commentaire, et d'autre part, effectuer une recherche de pays ou continents et en inclure de nouveaux au sein du groupe. Deux colonnes apparaissent : • Celle de gauche comporte la liste de tous les pays et continents que vous pouvez ajouter à votre groupe. • La colonne de droite comporte les pays et continents qui figurent déjà dans le groupe. Pour ajouter un pays ou un continent dans le groupe, vous devrez le faire passer d'une colonne à une autre : 1. Sélectionnez le ou les éléments à ajouter. 2. Cliquez sur cette flèche-ci, l'objet bascule dans la colonne de droite et intègre votre groupe (en tête de la liste). Pour retirer un objet du groupe : 1. Sélectionnez-le dans la colonne de droite. 2. Cliquez sur cette flèche.
Objet dans ce groupe	Vous visualisez les pays et continents figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

Objet temps

Nom de l'objet	Nom donné au groupe de ports lors de sa création.
Commentaire	Description associée au groupe de ports.
Description	Ce champ dynamique est renseigné automatiquement en fonction des paramètres choisis pour définir l'objet temps.

Événement ponctuel

Ce champ permet de préciser « Depuis » quand l'événement a lieu et jusque quand il se tiendra. Il faut définir un jour au sein du calendrier présenté.

Vous devez également définir une heure en remplissant le champ vide marqué « à ».

Jour de l'année

Par défaut, ce champ indique la date du 01: 01, vous pouvez cliquez sur **Ajouter une plage de dates** et saisir une date de début et une date de fin pour votre événement, en choisissant le mois et le jour.

Jour(s) de la semaine

Les jours concernés par l'événement sont marqués par cette icône . Si vous souhaitez en retirer un, cliquez une fois dessus. Si vous souhaitez en appliquer un supplémentaire, comme le samedi par exemple, cliquez une fois sur la case « Sam ». Celle-ci sera alors marquée par l'icône décrite ci-dessus et ce jour sera concerné par votre événement.

Plage(s) horaire(s)

Vous pouvez définir la / les plage(s) horaire(s) à l'aide de ces boutons :

- **Ajouter une plage horaire**, pour ainsi effectuer l'action citée et paramétrer l'heure de début et de clôture de votre événement.
- Pour la supprimer.

Les nouvelles informations concernant la / les plage(s) horaire(s) s'afficheront dans le champ **Description**.

OBJETS URL

Ce module propose de :

- Créer des catégories personnalisées d'URL et des groupes personnalisés de catégories d'URL,
- Créer des catégories personnalisées de noms de certificats (CN) et des groupes personnalisés de CN,
- Définir le fournisseur de Base d'URL utilisé mettant à disposition les catégories d'URL dynamiques.

Par exemple, pour la catégorie "*banks*" dans laquelle sont rassemblées les URL des banques les plus consultées, il est possible de créer une règle dans le module **Configuration > Politique de sécurité > Filtrage URL** pour en bloquer l'accès. Ainsi, lors d'une tentative de connexion sur un site web concerné, une page de blocage s'affiche avec un message d'erreur.
La page de blocage peut être personnalisée dans le module **Configuration > Notifications > Messages de blocage**, onglet **Page de blocage HTTP**.

NOTE
Dans les politiques de filtrage, il est préférable d'utiliser les catégories dynamiques fournis par les bases d'URL, celles-ci sont plus riches et plus performantes que les listes d'URL personnalisées.

Ce module se compose de trois onglets :

- **URL** : permet de rassembler les URL par catégorie (exemples : *shopping*, *pornography*, *videogames*). Chacune de ces catégories réunit un certain nombre d'URL de sites web, qui pourront être bloquées, ou autorisées, en fonction de l'action souhaitée. Permet également de créer des groupes de catégories d'URL parmi les catégories personnalisées ou dynamiques (Base d'URL).
- **Nom de certificat (CN)** : permet la création de catégories pour reconnaître les certificats attribués aux sites web sécurisés, en vue d'une utilisation par le filtrage SSL. Permet également de créer des groupes de catégories de CN.
- **Base d'URL** : permet de définir le fournisseur de base URL utilisé. Le **Moteur interne de filtrage d'URL (aucune mise à jour de base de données)** est sélectionné par défaut.
  Vous devez associer ce moteur à des catégories d'URL personnalisées ou à des bases d'URL maintenues par des tiers, par exemple :
  - Base de filtrage d'URL française fournie par le Rectorat de Toulouse (Académie de Toulouse), en suivant la méthode décrite dans la Base de connaissances Stormshield (authentification requise),
  - Base de filtrage d'URL polonaise fournie par Dagma, en suivant la méthode suivante : https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku).

  Stormshield ne garantit pas la disponibilité de ces bases et ne les maintient pas.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Onglet URL

Cet onglet donne une vue d'ensemble :

- Des catégories prédéfinies d'URL telles que *antivirus_bypass* et *authentication_bypass*,
- Des catégories personnalisées d'URL,
- Des groupes de catégories d'URL.

Les actions

Entrer un filtre	Tapez une suite de caractères dans ce champ : seuls les éléments contenant cette suite de caractères sont affichés dans les grilles **Catégories d'URL** et **Groupe de catégories d'URL**. Effacez la suite de caractère pour ré-afficher l'ensemble des éléments.
Tout sélectionner	Sélectionner toutes les catégories d'URL et tous les groupes de catégories d'URL afin de leur appliquer l'action **Supprimer**.
Ajouter	Crée une nouvelle catégorie d'URL ou un nouveau groupe de catégories d'URL. En sélectionnant un de ces deux éléments dans le menu déroulant, une nouvelle ligne s'affiche dans la grille correspondante, vous permettant d'indiquer le nom de la catégorie ou du groupe de catégories et un éventuel commentaire.
Supprimer	Supprime l'élément (catégorie d'URL ou groupe de catégories) sélectionné. Si cet élément est utilisé dans la configuration du firewall, un message d'avertissement vous demande de confirmer l'action.
Vérifier l'utilisation	Vérifie si l'élément sélectionné est utilisé dans la configuration du firewall. Le résultat de la vérification s'affiche au niveau de l'arborescence des modules.
Vérifier la classification d'une URL	Vérifie si une URL appartient à une catégorie d'URL définie. La recherche s'effectue dans les catégories personnalisées et dynamiques. Cela permet de déterminer s'il est nécessaire d'ajouter l'URL à une catégorie. Renseignez dans la zone de texte l'URL souhaitée, puis appuyez sur la touche **Entrée** du clavier. Un panneau **Catégories d'URL** apparaît et affiche les catégories qui contiennent cette URL.

Grille des catégories d'URL

La grille présente les éléments indiqués ci-dessous :

Catégorie d'URL	Nom de la catégorie d'URL.
Utilisation	• Un symbole ● indique que cette catégorie d'URL est utilisée dans la configuration du firewall (Filtrage URL / SSL ou Filtrage), • Un symbole ● indique que cette catégorie d'URL n'est pas utilisée dans la configuration du firewall.
Nombre d'éléments	Indique le nombre d'URL incluses dans la catégorie 'URL.
Commentaire	Affiche le commentaire éventuellement ajouté lors de la création de la catégorie d'URL.

NOTE
Le nombre de caractères pour une catégorie d'URL est limité à 255.

Éditer une catégorie d'URL

En double-cliquant sur une catégorie d'URL, son contenu s'affiche dans la partie droite de l'écran.

Vous pouvez y effectuer les actions suivantes :

Nom du groupe	Modifier le nom de la catégorie d'URL.
Commentaire	Ajouter ou modifier le commentaire associé à cette catégorie d'URL
Entrer un filtre	Tapez une suite de caractères dans ce champ : seuls les éléments contenant cette suite de caractères sont affichés dans la grille. Effacez la suite de caractère pour ré-afficher l'ensemble des éléments.
Tout sélectionner	Permet de sélectionner toutes les URL d'une catégorie afin de leur appliquer l'action **Supprimer**.
Ajouter	Ajoute une URL à une catégorie. En cliquant sur le bouton, une nouvelle ligne s'affiche vous permettant d'indiquer l'URL et un éventuel commentaire. L'URL peut contenir les méta-caractères (wildcard) * et ?.
Supprimer	Supprime une URL d'une catégorie. Sélectionnez l'URL concernée, puis cliquez sur le bouton.

La grille présente les éléments indiqués ci-dessous :

URL	Nom de l'URL. Il peut contenir les méta-caractères (wildcard) * et ?.
Commentaire	Vous avez la possibilité d'ajouter un commentaire pour décrire chaque URL listée.

La liste des **Caractères autorisés** et les indications de syntaxe sont valables uniquement pour les URL. Les méta-caractères (wildcard) suivants peuvent être utilisés :

*	Remplace une séquence de caractères quelconque. **EXEMPLES** ***.compagnie.com/*** permet d'inclure tous les sous-domaines de compagnie.com (comme mail.compagnie.com, www.compagnie.com) ainsi que tous les éléments après la barre oblique "/". ***.exe** permet d'inclure toutes les URL se terminant par ".*exe*".
?	Remplace un caractère unique. **EXEMPLE** **???**.compagnie.com inclut **www**.compagnie.com ou **ftp**.compagnie.com mais pas **www1**.compagnie.com.

Grille des groupes de catégories d'URL

La grille présente les éléments indiqués ci-dessous :

Groupe de catégories d'URL	Nom du groupe de catégories d'URL.
Utilisation	• Un symbole ● indique que ce groupe de catégories d'URL est utilisé dans la configuration du firewall (Filtrage URL / SSL ou Filtrage), • Un symbole ● indique que ce groupe de catégories d'URL n'est pas utilisé dans la configuration du firewall.
Nombre d'éléments	Indique le nombre de catégories d'URL incluses dans le groupe .
Commentaire	Affiche le commentaire éventuellement ajouté lors de la création du groupe.

NOTE
Le nombre de caractères pour un groupe de catégories d'URL est limité à 255.

Éditer un groupe de catégories d'URL

En double-cliquant sur un groupe de catégories d'URL, son contenu s'affiche dans la partie droite de l'écran.

Vous pouvez y effectuer les actions suivantes :

Nom du groupe	Modifier le nom du groupe de catégories d'URL.
Commentaire	Ajouter ou modifier le commentaire associé à ce groupe
Entrer un filtre	Tapez une suite de caractères dans ce champ : seuls les éléments contenant cette suite de caractères sont affichés dans la grille. Effacez la suite de caractère pour ré-afficher l'ensemble des éléments.
Tout sélectionner	Permet de sélectionner toutes les catégories d'un groupe afin de leur appliquer l'action **Supprimer**.
Ajouter	Ajoute une catégorie d'URL au groupe. En cliquant sur le bouton, une nouvelle ligne s'affiche vous permettant de sélectionner la catégorie d'URL.
Supprimer	Supprime une catégorie d'URL du groupe. Sélectionnez la catégorie d'URL concernée, puis cliquez sur le bouton.

La grille présente les éléments indiqués ci-dessous :

Objets dans ce groupe	Nom des catégories d'URL composant le groupe.

Onglet Noms de certificats (CN)

Cet écran propose de créer des catégories personnalisées de noms de certificat, ce qui peut s'avérer utile pour le filtrage SSL (module **Configuration > Politique de sécurité > Filtrage SSL**).

L'écran se décompose en 2 parties : une pour les catégories personnalisées de noms de certificat, une seconde pour les noms de certificat ajoutés à une catégorie.

Grille des catégories personnalisées de noms de certificat

Vous pouvez effectuer les actions suivantes :

Ajouter une catégorie personnalisée	Crée une nouvelle catégorie. En cliquant sur le bouton, une nouvelle ligne s'affiche vous permettant d'indiquer le nom de la catégorie et un éventuel commentaire.
Supprimer	Supprime une catégorie existante. Sélectionnez la catégorie concernée, puis cliquez sur le bouton. Si la catégorie est utilisée, un message d'avertissement vous demande de confirmer l'action.
Vérifier l'utilisation	Vérifie si une catégorie est utilisée dans une configuration. Sélectionnez la catégorie concernée, puis cliquez sur le bouton. Le résultat de la vérification s'affiche au niveau de l'arborescence des modules.

La grille présente les éléments indiqués ci-dessous :

Catégorie de noms de certificat (CN)	Nom de la catégorie.
Commentaire	Description de la catégorie.

NOTE
Le nombre de caractères pour une catégorie de noms de certificat est limité à 255.

Grille des noms de certificat d'une catégorie

Le contenu de la grille des noms de certificat (à droite) s'actualise en sélectionnant une catégorie personnalisée de noms de certificat (dans la grille à gauche).

Vous pouvez y effectuer les actions suivantes :

Ajouter un nom de certificat	Ajoute un nom de certificat à une catégorie. En cliquant sur le bouton, une nouvelle ligne s'affiche vous permettant d'indiquer le nom de certificat et un éventuel commentaire. Le nom peut contenir le méta-caractère (wildcard) * tant qu'il est placé en début d'URL et suivi d'un point.
Supprimer	Supprime un nom de certificat à une catégorie. Sélectionnez le nom de certificat concerné, puis cliquez sur le bouton.

La grille présente les éléments indiqués ci-dessous :

Nom de certificat (CN)	Nom du nom de certificat. Il peut contenir le méta-caractère (wildcard) * tant qu'il est placé en début d'URL et suivi d'un point.
Commentaire	Vous avez la possibilité d'ajouter un commentaire pour décrire chaque nom.

La liste des **Caractères autorisés** et les indications de syntaxe sont valables uniquement pour les noms de certificat. Le méta-caractère (wildcard) * peut être utilisé pour remplacer une séquence de caractères quelconque mais doit être placé en début d'URL et suivi d'un point.

EXEMPLE
***.compagnie.com** permet d'inclure tous les sous-domaines de compagnie.com (comme mail.compagnie.com, www.compagnie.com).

Onglet Base d'URL

Cet onglet permet de modifier le fournisseur de base d'URL utilisé. Il en existe deux :

- **Moteur interne de filtrage d'URL (aucune mise à jour de base de données)** : moteur de filtrage d'URL sélectionné par défaut.
  Vous devez associer ce moteur à des catégories d'URL personnalisées ou à des bases d'URL maintenues par des tiers, par exemple :
  - Base de filtrage d'URL française fournie par le Rectorat de Toulouse (Académie de Toulouse), en suivant la méthode décrite dans la Base de connaissances Stormshield (authentification requise),
  - Base de filtrage d'URL polonaise fournie par Dagma, en suivant la méthode suivante : https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku).

  Stormshield ne garantit pas la disponibilité de ces bases et ne les maintient pas.
- **Extended Web Control** : fournisseur accessible si vous avez souscrit une option supplémentaire. Il propose une base d'URL hébergée « dans le Cloud ». Ce filtrage d'URL a l'avantage d'avoir une qualité supérieure à la solution embarquée.

Vous pouvez effectuer l'action suivante :

Fournisseur de base d'URL	Sélectionnez le fournisseur de base d'URL que vous souhaitez utiliser. Vous pourrez ainsi choisir ses catégories d'URL dans le module Filtrage URL. Dans le cas d'un changement de fournisseur, un message d'avertissement s'affiche signalant que toute politique de filtrage URL qui utilise une catégorie du fournisseur actuel cessera de fonctionner. Pendant la migration, il est conseillé d'appliquer une politique de filtrage URL qui ne fait pas appel aux catégories d'URL destinées à être supprimées. Cela est dû aux noms de catégories différents selon les bases d'URL. Par exemple, le cas d'une politique de filtrage URL antérieure avec des règles comprenant des catégories **Extended Web Control** devra être réécrite avec les catégories de la base d'URL associée au moteur interne de filtrage d'URL.

Un encadré situé sous le choix du fournisseur de base d'URL affiche des informations concernant les catégories d'URL du fournisseur en cours d'utilisation (noms des catégories et leur description).

Concernant le téléchargement des mises à jour des bases d'URL :

- **Moteur interne de filtrage d'URL** : la mise à jour s'effectue selon la procédure mise en place par le fournisseur de la base de données d'URL sélectionnée.
- **Extended Web Control** : cette base d'URL étant hébergée « dans le Cloud », le téléchargement est réalisé dynamiquement et de manière transparente.

Si les serveurs sont temporairement inaccessibles, une page indique que la mécanique d'interrogation pour la classification du site est automatiquement relancée.

PORTAIL D'IDENTIFICATION

Afin de renforcer la sécurité, la connexion au portail d'authentification et à l'interface d'administration web se fait en forçant certaines options du protocole SSL. La version SSL v3 est désactivée et les versions TLS activées, conformément aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Connexion

Pour pouvoir configurer votre firewall Stormshield Network, il faut vous connecter à l'interface d'administration web.

La configuration d'un firewall n'est accessible qu'aux administrateurs du produit.
L'attribution des droits aux utilisateurs et / ou aux groupes d'utilisateurs est effectuée dans le menu **Système** > **Administrateurs** par le « super admin » ou l'administrateur qui dispose de tous les droits.

Présentation de l'écran

Le module de connexion se décompose en 2 parties :

- Une partie fixe
- Une partie rétractable : Options

Un troisième volet optionnel est affiché lorsqu'un **Avertissement pour l'accès à l'interface d'administration** a été configuré sur le firewall (voir la section **Configuration** > onglet Administration du Firewall).

Les indications à fournir varient selon qu'il s'agit d'une première connexion au firewall ou pas.

Identifiant	Champ réservé au login utilisateur disposant au minimum des droits base.
Mot de passe	Mot de passe de l'utilisateur, qui sera invité à en saisir un s'il s'agit de sa première connexion. Pour une configuration par défaut, il n'y a pas de mot de passe (champ vide).
S'authentifier en utilisant un certificat SSL	Lorsque cette case est activée, les champs **Utilisateur** et **Mot de passe** ne sont plus nécessaires, donc grisés. Le message suivant s'affiche : « *L'utilisation de certificat vous permet de vous authentifier automatiquement. Voulez-vous activer l'authentification automatique ?* ». Sélectionnez **Authentification automatique** ou **Authentification manuelle**. **REMARQUE** L'option de connexion automatique peut être activée automatiquement dans l'écran des **Préférences > Paramètres de connexion >** *Se connecter automatiquement en utilisant un certificat SSL.*
Se connecter	Un clic sur ce bouton ou appuyer sur la touche « Entrée » permet d'envoyer les informations de connexion au firewall.

AVERTISSEMENT
Le firewall Stormshield Network est sensible à la casse, il fait donc la différence entre les majuscules et les minuscules, aussi bien pour le nom d'utilisateur que pour le mot de passe.

Options

Langue	Langue de l'interface Web d'administration. Lorsque l'utilisateur choisit une nouvelle langue pour l'IHM Web, la page d'authentification se recharge dans la langue choisie. Les langues disponibles sont l'anglais, le français, le polonais, le hongrois et l'allemand.
Lecture seule	Permet une connexion en mode "lecture". Ainsi vous pouvez vous connecter au firewall sans droits de modifications au moyen d'un compte possédant habituellement ces droits. Ceci permet de ne pas utiliser les droits de modifications si cela n'est pas nécessaire.

REMARQUES

- Les options sont contenues dans un cookie. L'utilisateur conserve donc sur son navigateur ses préférences de connexion.
- Si, lors de la connexion sur la page d'authentification, l'option « Lecture seule » se trouve activée dans le cookie, la partie des options sera présentée déployée à l'utilisateur afin d'éviter toute confusion.

Notifications d'erreurs

Lorsqu'un champ est vide

Si l'utilisateur tente de s'authentifier alors qu'il n'a pas renseigné le champ **Utilisateur** ou **Mot de passe**, l'authentification n'est pas lancée et le message « Ce champ doit être renseigné » s'affiche.

Lorsque la touche « Verrouillage majuscules » est activée

Si cette touche est activée lorsque l'utilisateur renseigne son mot de passe, une icône d'avertissement s'affiche « la touche Verrouillage Majuscule est active ».

Échec d'authentification

Lorsqu'il y a échec d'authentification, le message suivant « *L'authentification a échoué* » s'affiche en rouge.

REMARQUE
Protection contre les attaques par force brute :
Lorsqu'un trop grand nombre de requête est effectué avec un mot de passe incorrect, le message suivant s'affiche : « La protection de l'authentification contre les attaques par force brute a été activée. La prochaine tentative d'authentification sera possible dans <nombre de secondes>.

Lorsque l'authentification TOTP est activée

Lorsque la méthode d'authentification TOTP est activée pour l'accès à l'interface Web d'administration, la saisie correcte d'un identifiant d'administrateur (autre que le compte super administrateur *admin*) et de son mot de passe est suivie de l'apparition d'une seconde fenêtre composée de deux champs :

- Un premier cadre comporte un message invitant l'administrateur à réaliser son enrôlement TOTP via la page d'enrôlement du portail captif si cette action n'a pas encore été réalisée.
- Un champ de saisie du code TOTP pour valider entièrement l'authentification de l'administrateur ayant réalisé son enrôlement TOTP.

Le compte « admin », super administrateur

Par défaut, il n'existe qu'un seul utilisateur possédant des droits d'administration des produits Stormshield Network, le compte "admin". Cet administrateur possède tous les droits. Il peut effectuer certaines opérations comme modifier la méthode d'authentification d'un utilisateur par exemple.

AVERTISSEMENT
Par défaut, le compte administrateur a la valeur "admin" comme identifiant **et** comme mot de passe.

REMARQUE
Étant donné les droits du compte "admin", Stormshield Network conseille de n'utiliser ce compte qu'en test ou dans le cas d'une maintenance.
Seul l' « admin » peut attribuer des droits d'administration à d'autres utilisateurs.

Déconnexion

Pour vous déconnecter d'un firewall, suivez la procédure suivante :

1. Dans le menu déroulant portant le nom de l'utilisateur connecté (en haut à droit de l'interface), sélectionnez Se déconnecter.
2. Cliquez ensuite sur **Quitter** pour confirmer la déconnexion.
   L'interface d'administration revient à l'écran de connexion.
   Si vous cliquez sur **Annuler**, l'interface revient à l'écran principal, sans conséquence pour la suite de l'exécution du programme.

PRÉFÉRENCES

Le module **Préférences** vous permet de gérer les paramètres de l'interface web d'administration du firewall et de gagner en ergonomie et rapidité selon vos choix d'options.

Il est accessible en haut à droite via le menu déroulant portant l'identifiant de l'administrateur connecté.

Pour ouvrir ce module :

1. Cliquez sur le nom de l'administrateur connecté (partie supérieure droite de l'écran).
2. Cliquez sur **Préférences**.

Restaurer les paramètres par défaut	Ce bouton permet de réinitialiser toutes les préférences utilisateur. Ceci inclut les éléments du module **Préférences** ainsi que les préférences d'affichage des modules de configuration (colonnes affichées, ordre, etc.).

L'écran des préférences se compose de 3 onglets :

- **Paramètres**,
- **Affichage**,
- **Liens**.

L'onglet Paramètres

Paramètres de connexion

Se connecter automatiquement en utilisant un certificat SSL	En cochant cette option, vous n'aurez plus besoin de vous identifier, vous serez directement reconnu grâce à votre certificat SSL.
Déconnexion en cas d'inactivité	Il est possible de fixer un délai pour la déconnexion de votre interface web : • 5 minutes, • 15 minutes, • 30 minutes, • 1 heure, • Toujours rester connecté. **NOTE** Si le super-administrateur a défini un délai maximal d'inactivité pour tous les comptes administrateurs, les délais supérieurs à celui-ci n'apparaîtront pas dans le menu déroulant.

Paramètres de l'interface de management

Vérifier tous les champs d'un objet lors d'une recherche	Lorsque vous effectuez une recherche par lettre ou par mot dans les champs dédiés, le moteur va aussi bien vérifier les noms que les commentaires, tout ce qui concerne le sujet de la recherche.
Désactiver les diagnostics en temps réel de la politique de sécurité	Lorsque vous créez une règle au sein de la politique de sécurité, le moteur de diagnostic va automatiquement vérifier si des règles se chevauchent, si des erreurs sont repérées. En cochant cette case, vous suggérerez une recherche manuelle de ces possibles erreurs.
La semaine commence le dimanche	En cochant cette case, les Objets temps figurant dans le menu Objets démarreront leur semaine le dimanche.
Confirmer avant d'appliquer les modifications	Cette option va permettre d'annuler vos actions si vous avez effectué une fausse manipulation ou si vous décidez de ne pas poursuivre votre configuration. En effet, une fenêtre de confirmation s'affichera, permettant de valider ou non votre action.

L'onglet Affichage

Paramètres de l'application

Toujours afficher les éléments de configuration avancée	Les éléments de configuration avancée peuvent être déroulés au sein de chaque module qui en comportent, mais ils sont masqués par défaut. En cochant cette case, vous les rendrez visibles à l'écran sans avoir besoin de les dérouler.
Afficher le bouton d'enregistrement des commandes	En cochant cette case, le bouton d'enregistrement des commandes est affiché dans le bandeau supérieur de l'interface Web d'administration. Il est ainsi disponible quel que soit le module de configuration sélectionné.
Afficher les utilisateurs dès l'accès au module	En cochant cette option, tous les utilisateurs seront affichés au sein de l'arborescence de gauche.
Afficher les objets réseau dès le lancement du module	En cochant cette option, tous les objets réseau seront affichés au sein de l'arborescence de gauche.
Afficher les politiques globales (Objets réseau, Certificats, Filtrage, NAT et VPN IPsec)	En cochant cette case, lors de la connexion aux modules **Filtrage et NAT (Politique de Sécurité), VPN IPsec (VPN) et Objets,** l'écran affichera un menu déroulant proposant le choix entre les politiques locales et globales. La politique de sécurité locale en vigueur est affichée par défaut.
Appliquer un commentaire par défaut aux règles (Filtrage, NAT et IPsec)	En cochant cette case, les commentaires créés pour les règles de filtrage et de NAT intégreront automatiquement la date et l'heure de création. Cette option s'applique à l'affichage des politiques de Filtrage, de NAT et IPsec.

Nombre de règles par page (Filtrage, NAT et IPsec)	Selon le nombre de règles existantes, vous pouvez choisir d'en afficher : • 100 règles par page • 200 règles par page • 500 règles par page • 1000 règles par page En choisissant « Automatique », le moteur Stormshield Network essaiera de déduire le nombre de règles par page, en fonction de votre configuration. Cette option s'applique à l'affichage des politiques de Filtrage, de NAT et IPsec.

Paramètres des traces (logs)

Nombre de lignes affichées par page	Selon le nombre de lignes existantes dans les fichiers de traces, vous pouvez choisir d'en afficher : • 200 lignes par page • 400 lignes par page • 600 lignes par page • 800 lignes par page • 1000 lignes par page
Nombre de caractères minimum pour lancer la recherche (0 pour désactiver)	Indiquez le nombre de caractères devant être saisis dans le champ de recherche afin de filtrer automatiquement les données sur cette valeur.

L'onglet Liens

Liens externes

URL d'accès à l'aide en ligne	Cette URL vous rappelle l'adresse d'accès à l'aide en ligne Stormshield Network : vous y trouverez l'arborescence des modules par ordres alphabétique. Cliquez sur le module de votre choix afin d'afficher la page correspondante.
URL d'accès à la documentation des alarmes	Cette adresse vous permettra d'accéder à un document d'aide à la compréhension du module Alarmes, figurant dans la base de connaissances Stormshield Network.

PROFILS D'INSPECTION

Le module de profils d'inspection se compose de 2 écrans :

- Une zone dédiée à la configuration par défaut et un menu rétractable pour le mode avancé.
- Une zone de configuration pour l'association des profils protocolaires, accessible via le bouton **Accéder au profils**.

Inspection de sécurité

Configuration globale

Profils d'inspection par défaut

Profil pour le trafic entrant	Définissez le profil à appliquer pour le trafic entrant du réseau via le firewall SNS. Le trafic entrant représente le trafic d'une interface non protégée (comme Internet) vers une interface protégée (votre réseau local/interne).
Profil pour le trafic sortant	Définissez le profil à appliquer pour le trafic sortant du réseau via le firewall SNS. Le trafic sortant représente le trafic d'une interface protégée vers une interface non protégée.

Nouvelles alarmes

Appliquer le modèle par défaut aux nouvelles alarmes	Cette option est liée au module **Protection Applicative > Applications et protections**. En la cochant, les nouvelles alarmes se mettront à jour automatiquement et seront livrées avec la signature SNS. Les options suivantes seront alors grisées. Si vous souhaitez les appliquer vous-même, décochez la case pour les modifier.
Action	Lorsqu'une alarme est remontée, le paquet qui a provoqué cette alarme subit l'action associée. Vous pouvez choisir de laisser **Passer** ou de **Bloquer** les nouvelles alarmes. Vous pourrez constater l'état que vous avez appliquez au sein du module **Protection Applicative > Applications et protections**. Les nouvelles alarmes se trouvent dans la colonne "**Nouveau**".
Niveau	Trois niveaux d'alarmes sont disponibles, "Ignorer", "Mineur" et "Majeur".
Capture du paquet	En cochant cette option, le paquet responsable de la remontée de l'alarme sera capturé.

En cas de saturation du service de gestion des logs

Bloquer les paquets générant une alarme	Cette option permet, lorsque le firewall n'est plus en mesure de tracer les événements du fait que son service de gestion des logs est saturé, de bloquer les paquets générant une alarme. En désactivant cette option, les paquets concernés ne sont pas bloqués et ne sont plus tracés.
Bloquer les paquets traversant une règle de filtrage configurée en mode "Tracer (journal de filtrage)"	Cette option permet, lorsque le firewall n'est plus en mesure de tracer les événements du fait que son service de gestion des logs est saturé, de bloquer les paquets traversant une règle de filtrage configurée pour tracer un événement. En désactivant cette option, les paquets concernés ne sont pas bloqués et ne sont plus tracés.

Configuration avancée

Considérer les interfaces IPsec (sauf interfaces IPsec virtuelles) comme internes. S'applique à tous les tunnels : les réseaux distants devront être explicitement légitimés.	En cochant cette case, les interfaces IPsec deviennent des interfaces internes et donc protégées. Tous les réseaux pouvant se présenter au travers des tunnels IPsec doivent alors être légitimés et les routes statiques permettant de les joindre doivent être déclarées. Dans le cas contraire, le trafic IPsec sera rejeté par le firewall. **IMPORTANT** Lorsque cette case est cochée, l'option s'applique à **l'ensemble** des tunnels IPsec définis sur le firewall.

PROTOCOLES

Ce module contient la liste des divers protocoles configurables depuis votre interface web.

Il est divisé en 2 zones distinctes :

- La liste des protocoles (colonne de gauche). Certains protocoles sont regroupés par thématique :
  - Messageries instantanées,
  - Protocoles IP (ICMP, IP, SCTP et TCP-UDP),
  - Protocoles industriels,
  - Protocoles Microsoft,
  - VoIP / Streaming.
- Les profils attribuables aux protocoles et leur configuration (colonne de droite). Cette zone est activée après avoir sélectionné un protocole dans la colonne de gauche.

Recherche

La barre de recherche permet de retrouver le protocole à configurer en saisissant les premières lettres de son nom. Il est possible de travailler directement avec le protocole voulu en cliquant dessus.

Liste des protocoles

Choisissez le protocole que vous souhaitez paramétrer au sein de la liste affichée. Une fois le protocole choisi, la configuration de celui-ci peut démarrer.

Les profils

Sélection du profil applicatif

Ces **profils applicatifs** sont la configuration de l'analyse protocolaire, pouvant lever des alarmes. Un **profil d'inspection** est constitué de la somme d'un profil applicatif par protocole. Par défaut, le profil d'inspection *IPS_00* contient les **profils applicatifs** *protocole_00*, et ainsi de suite. Ce sont ces **profils d'inspection** qui seront appliqués dans la politique de filtrage.

Pour information, en configuration d'usine, le profil d'inspection *IPS_00* est destiné aux **interfaces internes**, appliqué donc au trafic entrant. Le profil destiné aux **interfaces publiques** appliqué au trafic sortant est le profil *IPS_01*.

Le menu déroulant propose 10 profils, numérotés de 00 à 09.

Chaque profil possède par défaut, le nom du protocole, accompagné de sa numérotation.

EXEMPLES

- http_00
- http_01…

Les boutons

Éditer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Éditer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Si le profil sélectionné possède un commentaire, celui-ci sera affiché au sein d'une info-bulle.
Accéder à la configuration globale	Cette option contient la liste des ports TCP par défaut. Cette option est présente dans chaque protocole sauf : IP, ICMP, RTP, RTCP. Il est possible d'**Ajouter** ou de **Supprimer** des ports en cliquant sur les boutons du même nom. Consultez la section suivante pour connaître les paramètres proposés en configuration globale. **NOTE** Les configurations globales des **Protocoles SSL et TCP/UDP** se paramètrent de manière différente. Elles sont décrites dans une sous-section de la partie **Configuration globale des protocoles.**

Configuration globale des protocoles

Le bouton « Accéder à la configuration globale » s'applique à l'ensemble des profils du protocole sélectionné.

Cette option est proposée pour chaque protocole sauf pour les protocoles IP, RTP, RTCP et S7.

Protocole : liste des ports TCP - ou UDP - par défaut

Cette option définit la liste des ports (TCP ou UDP) analysés par défaut par le plugin du protocole que l'on paramètre. Il est possible d'**Ajouter** ou de **Supprimer** des ports en cliquant sur les boutons du même nom.

Protocole over SSL : liste des ports TCP par défaut

Les ports ajoutés dans la liste des protocoles sécurisés seront au préalable analysés par le plugin SSL, puis par le plugin du protocole paramétré si le trafic est déchiffré. Il est possible d'**Ajouter** ou de **Supprimer** des ports en cliquant sur les boutons du même nom.

Cette sélection est proposée pour les protocoles *HTTPS*, *SMTPS*, *FTPS*, *POP3S*, *OSCAR over SSL*, *NetBios CIFS over SSL*, *NetBios SSN over SSL* et *SIP over SSL*.

EXEMPLE
Le choix du port HTTPS dans la liste "HTTPS : liste des ports TCP par défaut" entrainera deux temps d'analyse :

- Le trafic HTTPS sera analysé par le plugin SSL.
- Le trafic déchiffré par le proxy SSL sera analysé par le plug-in HTTP.

Proxy

Cette option s'active en configuration globale des protocoles HTTP, SMTP, POP3 et SSL. Elle s'applique à l'ensemble des profils d'inspection.

Appliquer la règle de NAT sur le trafic analysé	Par défaut, le trafic analysé par un proxy implicite est réémis avec l'adresse de l'interface de sortie du Firewall. Dans le cas d'une politique de NAT et en cochant cette option, la translation d'adresse est appliquée sur ce trafic sortant de l'analyse du proxy. Cette option n'est pas appliquée pour une translation sur la destination.

Configuration globale du protocole TCP/UDP

Onglet IPS

Déni de Service (DoS)

Nb max. ports par seconde	Afin d'éviter le scan de ports, cette valeur est la limite du nombre de ports différents (compris entre 1 et 1024) accessibles en 1 seconde pour une destination protégée donnée. Ce nombre doit être compris entre 1 et 16 ports.
Fréquence de purge table de session (secondes)	Une fois la table de connexions / sessions saturée, un mécanisme de purge des connexions inactives est programmé. Définissez le temps minimum entre deux purges des tables de sessions compris entre 10 et 172800 secondes, afin de ne pas surcharger le boîtier.

Connexion

Autoriser les connexions semi-ouvertes (RFC 793, section 3.4)	Cette option permet d'éviter le déni de service pouvant opérer au sein des connexions dites « normales ».

http://tools.ietf.org/html/rfc793#section-3.4

Support

Tracer chaque connexion TCP	Option pour activer la génération de log pour les connexions TCP.
Tracer chaque pseudo-connexion UDP	Option pour activer la génération de log pour les connexions UDP.

Configuration globale du protocole SSL

Onglet Proxy

Génération des certificats pour émuler le serveur SSL

C.A (signe les certificats)	Choisissez la Sous-autorité utilisée pour signer les certificats générés par le proxy SSL. Vous devez l'avoir importée au préalable dans le module **Certificat** (menu **Objet**).
Mot de passe de l'autorité	Renseignez le mot de passe de l'autorité de certification choisie.
Durée de vie du certificat (jours)	Ce champ précise la **Validité (jours)** des certificats générés par le proxy.

SSL : liste des ports TCP par défaut

Cette option est proposée pour la liste des ports TCP par défaut. Les ports par défaut des protocoles ajoutés seront analysés par le plugin SSL.

Proxy

Cette option s'applique à l'ensemble des profils d'inspection. Cette option n'est pas appliquée pour la translation sur la destination.

Appliquer la règle de NAT sur le trafic analysé	Par défaut, le trafic analysé par un proxy implicite obtient en sortie, l'adresse de l'interface de sortie du Firewall. Dans le cas d'une politique de NAT et en cochant cette option, la translation d'adresse est appliquée sur ce trafic sortant de l'analyse du proxy. Cette option n'est pas appliquée pour une translation sur la destination.

Onglet Autorités de certification personnalisées

Ajouter la liste de C.A personnalisée aux autorités de confiance	Cette option permet d'activer la fonctionnalité d'import d'autorités de certifications non publiques. Ces C.A. seront considérées comme autorité de confiance. Les certificats délivrés par ces C.A. personnalisées seront donc considérés comme digne de confiance.

Il est possible d'**Ajouter** ou de **Supprimer** des autorités de certifications en cliquant sur les boutons du même nom.

Onglet Autorités de certification publiques

Il est possible de désactiver une autorité de certification publique par double-clic sur l'icône d'état, par défaut activée. Vous pouvez également choisir de **Tout activer** ou de **Tout désactiver** ces C.A. publiques en cliquant sur les boutons du même nom.

Afin d'améliorer le contrôle, ces autorités de certification racines de confiance sont maintenues à jour dans la liste du firewall via **Active-Update**.

Onglet Certificats de confiance

Il s'agit d'une liste blanche de certificats pour lesquels les traitements d'inspection de contenu (certificats auto-signés, certificats expirés, etc.), définis dans l'onglet *Proxy* de la configuration des profils SSL, ne seront pas appliqués.

Cette fenêtre permet d'**Ajouter** ou de **Supprimer** des certificats de confiance en cliquant sur les boutons du même nom.

Onglet IPS

Analyse des certificats

Délai de conservation des certificats dans le cache (TTL)	Pour optimiser les performances d'analyse des certificats serveur, un mécanisme de cache a été implémenté afin de ne pas déclencher la récupération d'un certificat lorsque celui-ci est déjà connu du moteur de prévention d'intrusion. Ce mécanisme définit ainsi un délai de conservation des entrées du cache, exprimé en secondes. Lorsque cette durée maximale de conservation est atteinte par un certificat présent dans le cache, l'entrée correspondante est automatiquement supprimée.

Configuration globale du protocole ICMP

Onglet IPS

IPS

Taux global maximum de paquets d'erreurs ICMP (paquets par seconde et par coeur)	Lorsque le nombre de paquets d'erreur ICMP dépasse cette limite (25000 par défaut), les paquets supplémentaires sont ignorés par le firewall avant d'appliquer les règles de filtrage. Cette option permet de protéger le firewall contre des attaques de type Blacknurse.

Live Messenger (MSN)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole Live Messenger (MSN) sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête Live Messenger	Active ou désactive les logs permettant de tracer les requêtes Live Messenger.

Yahoo Messenger (YMSG)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole Yahoo Messenger sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête Yahoo Messenger	Active ou désactive la remontée des logs relatifs au protocole Yahoo Messenger.

ICMP

Onglet « IPS »

Paramètres de session (en secondes)

Expiration d'une session	Cette valeur doit être comprise entre 2 et 60 secondes.

Support

Ignorer les notifications ICMP (suivi d'état TCP/UDP)	En cochant cette option, vous ne prendrez pas en compte les messages d'erreur pouvant intervenir au sein des protocoles, comme l'inaccessibilité d'un service ou d'un hôte, par exemple.

GIP

Onglet « IPS »

MTU

Imposer une limite MTU (force la fragmentation)	Le MTU (Maximum Transmission Unit) représente la taille maximale d'un paquet IP. En cochant cette option, vous dégriserez la suivante et pourrez définir votre limite.
Valeur maximale du MTU	Définissez la valeur maximale du datagramme IP, comprise entre 140 et 65535 octets.

Fragmentation

Taille minimum d'un fragment (octets)	Le fragment doit être compris entre 28 et 65535 octets. La valeur par défaut est 140 octets.
Expiration d'une session (en secondes)	Cela doit être compris entre 2 et 30 secondes.

Mode furtif

Activer le mode furtif	Le mode furtif est un mode dans lequel le firewall ne répond pas aux tentatives de détection (requêtes ICMP notamment) afin de le rendre invisible. Le mode furtif est activé par défaut et peut être désactivé en décochant cette case. **NOTE** La désactivation du mode furtif (*stealth* mode) impacte les performances de traitement des paquets. En effet, pour être en mesure de répondre à un message d'erreur ICMP, le firewall doit garder une trace de chacun des paquets. Le mode furtif permet donc au firewall de faire l'économie de toutes ces traces de paquets.

NOTE
Le protocole IP ne dispose pas de profil.

SCTP

SCTP, ou Stream Control Transmission Protocol est un protocole défini dans la RFC 4960 (un texte d'introduction est fourni dans la RFC 3286).

En tant que protocole de transport, SCTP est équivalent dans un certain sens à TCP ou à UDP.

Alors que TCP est orienté flux (la séquence d'octets contenue dans un paquet n'a pas conceptuellement de début ou de fin, elle fait partie du flux constitué par la connexion), SCTP est, comme UDP, orienté message (au sein d'un flux, il transmet des messages avec un début et une fin, qui peuvent éventuellement être fragmentés sur plusieurs paquets).

Onglet « IPS »

Configuration spécifique

Nombre max. d'adresses IP par extrémité [1-8]	Ce paramètre définit le nombre maximum d'adresses IP autorisées pour une extrémité d'association SCTP (*multi-homing*).

Expiration (en secondes)

Délai de négociation d'une association [2-60]	Temps maximum autorisé pour l'établissement complet d'une association SCTP (exprimé en secondes). Cette valeur doit être comprise entre 2 et 60 secondes (valeur par défaut : 20 secondes).
Inactivité [30-604800]	Temps maximum de conservation de l'état d'une association SCTP sans activité (exprimé en secondes). Cette valeur doit être comprise entre 30 et 604800 secondes (valeur par défaut : 3600 secondes).
Fermeture d'une association [2-60]	Temps maximum admis pour la phase de fermeture d'une association SCTP (exprimé en secondes). Cette valeur doit être comprise entre 2 et 60 secondes (valeur par défaut : 20 secondes).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole SCTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête SCTP	Active ou désactive les logs permettant de tracer les requêtes SCTP.

TCP-UDP

Le protocole TCP assure le contrôle des données lors de leur transfert. Il a pour rôle de vérifier que les paquets IP envoyés sont bien reçus en l'état, sans aucune perte ou changement sur le plan de leur intégrité.

Le protocole UDP peut remplacer le TCP en cas de problème mineur, il assure un transfert plus fluide car il ne contrôle pas chacune des étapes de la transmission. Il convient par exemple à des applications de streaming (diffusion audio/vidéo) pour lesquelles la perte de paquets n'est pas vitale. En effet, lors de ces transmissions, les paquets perdus seront ignorés.

L'écran des profils

Onglet IPS-Connexion

Inspection

Imposer une limite MSS	Cette case permet d'imposer une limite MSS (Maximum Segment Size) pour l'inspection du profil. **NOTE** Le MSS désigne la quantité de données en octets qu'un ordinateur ou tout équipement de communication peut contenir dans un paquet seul et non fragmenté. En cochant cette option, vous dégriserez le champ suivant qui vous permettra d'établir votre limite.
Limite MSS (en octets)	Définissez votre limite MSS, comprise entre 100 et 65535 octets.

Réécrire les séquences TCP avec un aléa fort (arc4)	En cochant cette case, les numéros de séquence TCP générées par le client et le serveur seront écrasés et remplacés par le moteur de prévention d'intrusion Stormshield Network, qui produira des numéros de séquence aléatoires.
Protéger contre l'envoi répété de paquets ACK	En cochant cette option, vous vous protégez contre le vol de session, ou attaque de type « ACK ».
Activer l'ajustement automatique de la mémoire dédiée au suivi de données	En cochant cette option, vous autorisez le firewall à ajuster dynamiquement la mémoire allouée au suivi de données (data tracking). La valeur maximale de la mémoire allouée dynamiquement est égale à la taille de la fenêtre TCP divisée par la limite MSS. Lorsque la case est décochée, cette valeur maximale est de 256.
Activer le suivi d'applications	Cette option permet de consigner les identifiants d'applications dans les logs d'alarmes et de connexions afin de générer un rapport basé sur ces identifiants d'applications.

Protection contre le déni de service

Limites de connexions

Nombre maximal de connexions TCP par adresse IP source (0 désactive cette protection)	Cette option permet de limiter le nombre de connexions TCP pour une même adresse IP source. Lorsque la valeur choisie vaut 0, aucune restriction n'est appliquée. **IMPORTANT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.
Nombre maximal de sessions UDP par adresse IP source (0 désactive cette protection)	Cette option permet de limiter le nombre de sessions UDP pour une même adresse IP source. Lorsque la valeur choisie vaut 0, aucune restriction n'est appliquée. **IMPORTANT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.

Fréquences limites de réception de premiers paquets TCP / UDP

Nombre max. de SYN reçus dans l'intervalle de temps de référence pour une adresse source (0 désactive cette protection)	Cette option permet de fixer le nombre maximal de demandes d'établissement de connexions TCP (paquets SYN) reçues depuis une même adresse IP source pendant la période de référence définie dans le cadre **Intervalles de temps de référence pour les fréquences limites de réception de premiers paquets TCP / UDP**. Elle permet de protéger le firewall contre des attaques de type SYN flood (DDoS).

Nombre max. de nouvelles sessions UDP dans l'intervalle de temps de référence pour une adresse source (0 désactive cette protection)	Cette option permet de fixer le nombre maximal de demandes d'établissement de sessions UDP reçues depuis une même adresse IP source pendant la période de référence définie dans le cadre **Intervalles de temps de référence pour les fréquences limites de réception de premiers paquets TCP / UDP**. Elle permet de protéger le firewall contre des attaques de type UDP flood (DoS).

Intervalles de temps de référence pour les fréquences limites de réception de premiers paquets TCP / UDP

Intervalle de temps pendant lequel les nouvelles connexions TCP venant d'une même adresse source sont comptées jusqu'à atteindre le seuil défini dans le calcul de fréquence limite de réception de premiers paquets TCP	Cette option permet de fixer le temps de référence pour le calcul des fréquences limites de nouvelles connexions TCP (paquets SYN) pour une même adresse IP source. **IMPORTANT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.

Intervalle de temps pendant lequel les nouvelles sessions UDP venant d'une même adresse source sont comptées jusqu'à atteindre le seuil défini dans le calcul de fréquence limite de réception de premiers paquets UDP	Cette option permet de fixer le temps de référence pour le calcul des fréquences limites de nouvelles sessions UDP pour une même adresse IP source. **IMPORTANT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.

NOTE
Pour suivre les valeurs des compteurs de connexions simultanées, vous devez utiliser la commande : `sfctl -s host -v`.

Expiration (en secondes)

Délai d'ouverture d'une connexion (SYN)	Temps maximum, exprimé en secondes, autorisé pour l'établissement complet de la connexion TCP (SYN / SYN+ACK / ACK). Ce temps est compris entre 10 et 60 secondes (valeur par défaut : 20 secondes).
Connexion TCP	Temps maximum en secondes, de conservation de l'état d'une connexion TCP sans activité. Ce temps est compris entre 30 et 604800 secondes (valeur par défaut : 3600 secondes).
Session UDP	Temps maximum, exprimé en secondes, de conservation de l'état d'une pseudo-connexion UDP sans activité. Ce temps est compris entre 30 et 604800 secondes (valeur par défaut : 120 secondes).
Fermeture d'une connexion (FIN)	Temps maximum, exprimé en secondes, admis pour la phase de fermeture d'une connexion TCP (FIN+ACK / ACK / FIN+ACK / ACK). Cette valeur doit être comprise entre 10 et 3600 secondes (valeur par défaut : 480 secondes).
Connexions closes	Délai, en secondes, de conservation d'une connexion clôturée (état *closed*). Ce délai est compris entre 2 et 60 secondes (valeur par défaut : 2 secondes).
Petite fenêtre TCP	Pour éviter les attaques par déni de service, ce compteur détermine la durée de vie maximum d'une connexion avec une petite fenêtre TCP (inférieure à 100 octet). Ce compteur est initialisé lors de la réception de la première annonce de petite fenêtre. Si aucun message d'augmentation de fenêtre n'est reçu avant l'expiration de ce compteur, la connexion TCP est coupée.

Support

Désactiver le proxy SYN	En cochant cette case, vous ne serez plus protégé contre les attaques de type « SYN », car le proxy ne filtrera plus les paquets. Il est recommandé de ne désactiver cette option qu'à des fins de diagnostic.

IEC 61850 GOOSE (IPS)

Le standard IEC61850 est une norme de communication utilisée par les systèmes de protection des sous-stations dans le secteur de la production d'énergie électrique.

La norme de communication IEC 61850 est spécifiquement utilisée pour la communication entre les dispositifs électroniques intelligents localisés au niveau des postes de distribution d'un réseau électrique. Les dispositifs électroniques intelligents, également appelés IED, sont composés essentiellement de relais de protection basés sur microprocesseur, de dispositifs de mesure, de contrôleurs logiques programmables, d'enregistreurs de défauts et d'événements. Ils permettent la surveillance en temps réel du réseau électrique et constituent «l'intelligence» de la sous-station.

Paramètres généraux

Durée max. d'une connexion Ethernet en secondes [2-604800]	Ce délai fixe une limite au-delà de laquelle les connexions IEC 61850 GOOSE restées sans réponse sont supprimées. Cette valeur doit être comprise entre 2 et 604800 secondes. La valeur par défaut est de 60 secondes.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole IEC 61850 GOOSE sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête IEC 61850 GOOSE	Active ou désactive les logs permettant de tracer les requêtes IEC 61850 GOOSE.

MMS / IEC 61850 MMS

Onglet MMS

Gestion des services MMS

Interdire les services réservés	En cochant cette option, vous bloquez un service avec confirmation particulier : le service labellisé *Reserved service* et rattaché à l'identifiant n°79 dans les spécifications du protocole IEC61850.

Onglet "Services avec confirmation"

Cette grille recense les services MMS standards avec confirmation (services nécessitant une réponse) prédéfinis dans le firewall. Ils sont classifiés par jeu de services :

- VMD Support,
- Variable Access,
- Semaphore Management,
- Scattered Access
- Program Invocation Management,
- Operator Communication,
- Journal management,
- File Management,
- Event Management,
- Event Enrollment,
- Event Condition,
- Event Action,
- Domain Management,
- Data Exchange,
- Access Control.

Les services MMS standards avec confirmation prédéfinis sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux. Les boutons **Interdire par jeu de services**, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services listés dans la grille.

Onglet "Services additionnels avec confirmation"

Cette grille recense les services MMS additionnels avec confirmation (services nécessitant une réponse) prédéfinis dans le firewall. Ils sont classifiés par jeu de services :

- VMD Support,
- Unit Control,
- Program Invocation Management,
- Event Condition.

Les services MMS additionnels prédéfinis sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux. Le bouton **Modifier tous les services** permet de modifier l'action (*Autoriser / Interdire*) appliquée à l'ensemble des services listés dans la grille.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole MMS sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Détecter et inspecter automatiquement le protocole	Si le protocole MMS est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Onglet IEC 61850 MMS (IPS)

Le standard IEC61850 est une norme de communication utilisée par les systèmes de protection des sous-stations dans le secteur de la production d'énergie électrique.

La norme de communication IEC 61850 est spécifiquement utilisée pour la communication entre les dispositifs électroniques intelligents localisés au niveau des postes de distribution d'un réseau électrique. Les dispositifs électroniques intelligents, également appelés IED, sont composés essentiellement de relais de protection basés sur microprocesseur, de dispositifs de mesure, de contrôleurs logiques programmables, d'enregistreurs de défauts et d'événements. Ils permettent la surveillance en temps réel du réseau électrique et constituent «l'intelligence» de la sous-station.

Gestion des services IEC 61850

Cette grille recense les services IEC61850 MMS prédéfinis dans le firewall. Ils sont classifiés par jeu de services :

- Setting Group Control Block,
- Server,
- Report Control Block,
- Logical Node,
- Logical Device,
- Log Control Block,
- GSSE,
- GOOSE,
- File transfert,
- Data Set,
- Data,
- Control.

Les services IEC61850 MMS sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux. Les boutons **Interdire par jeu de services**, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services listés dans la grille.

Liste blanche des Logical Nodes

Cette grille recense les services ne devant pas être soumis à l'analyse protocolaire IEC61850 MMS.

Activer la liste blanche	En cochant cette case, vous rendez active la liste blanche afin d'y ajouter des services MMS à exclure de l'analyse.

Il est possible d'**Ajouter** ou de **Supprimer** un service MMS à cette liste blanche à l'aide des boutons du même nom.

Le bouton **Tout sélectionner** permet de sélectionner l'ensemble des services présent dans la liste blanche afin de les **Supprimer** en une seule opération.

IEC 61850 SV (IPS)

Le standard IEC61850 est une norme de communication utilisée par les systèmes de protection des sous-stations dans le secteur de la production d'énergie électrique.

La norme de communication IEC 61850 est spécifiquement utilisée pour la communication entre les dispositifs électroniques intelligents localisés au niveau des postes de distribution d'un réseau électrique. Les dispositifs électroniques intelligents, également appelés IED, sont composés essentiellement de relais de protection basés sur microprocesseur, de dispositifs de mesure, de contrôleurs logiques programmables, d'enregistreurs de défauts et d'événements. Ils permettent la surveillance en temps réel du réseau électrique et constituent «l'intelligence» de la sous-station.

Paramètres généraux

Durée max. d'une connexion Ethernet en secondes [2-604800]	Ce délai fixe une limite au-delà de laquelle les connexions IEC 61850 SV restées sans réponse sont supprimées. Cette valeur doit être comprise entre 2 et 604800 secondes. La valeur par défaut est de 60 secondes.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole IEC 61850 SV sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête IEC 61850 SV	Active ou désactive les logs permettant de tracer les requêtes IEC 61850 SV.

BACnet/IP

Gestion des services

Gestion des services avec confirmation

Onglet "Services avec confirmation"

Cette grille recense les identifiants et services avec confirmation BACnet/IP associés (services nécessitant une réponse) prédéfinis dans le firewall. Ces codes sont classifiés par jeu de services (*Service choice*) :

- Alarm and Event,
- File Access,
- Security,
- Object Access,
- Remote Device Management,
- Virtual Terminal.

Les services avec confirmation BACnet/IP prédéfinis sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux. Les boutons **Interdire par jeu de services**, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services BACnet/IP listés dans la grille.

Onglet Autres services avec confirmation

Cette liste permet d'autoriser des identifiants de services avec confirmation BACnet/IP additionnels bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Gestion des services sans confirmation

Onglet "Services sans confirmation"

Cette grille recense les identifiants et services sans confirmation BACnet/IP associés (services ne nécessitant pas de réponse) prédéfinis dans le firewall.

Les services sans confirmation BACnet/IP prédéfinis sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux. Le bouton **Tout sélectionner** permet de modifier l'action (*Autoriser / Interdire*) appliquée à l'ensemble des services BACnet/IP listés dans la grille.

Onglet Autres services sans confirmation

Cette liste permet d'autoriser des identifiants de services sans confirmation BACnet/IP additionnels bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Fonctions BVLL

Gestion des fonctions BVLL

Onglet "Fonctions BVLL"

Cette grille recense les identifiants et services prédéfinis dans le firewall autorisés sur la couche BVLL, ce qui correspond à la couche IP.

Les services sont autorisés par défaut (action *Autoriser*) et cette action peut être modifiée pour chacun d'entre eux (action *Interdire*).

Onglet "Autres fonctions BVLL autorisées"

Cette liste permet d'autoriser des identifiants de services bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Fonctions NPDU

Gestion des fonctions NPDU

Onglet "Fonctions NPDU"

Cette grille recense les identifiants et services prédéfinis dans le firewall autorisés sur la couche NPDU, ce qui correspond à la couche réseau.

Onglet "Autres fonctions NPDU autorisées"

Cette liste permet d'autoriser des identifiants de services bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole BACnet/IP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête BACnet/IP	Active ou désactive les logs permettant de tracer les requêtes BACnet/IP.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

CIP (onglet IPS - CIP)

Paramètres

Nombre maximal de services CIP dans un paquet	Le code de service CIP Multiple_Service_Packet permet d'encapsuler plusieurs commandes CIP dans un même paquet réseau. Ce champ permet de définir le nombre de commandes pouvant être regroupées dans un seul paquet. Cette valeur doit être comprise entre 1 et 65535 (valeur par défaut: 65535).

Gestion des services

Onglet Services standards

Cette liste recense les identifiants de services et les services CIP standards associés que le firewall autorise par défaut. L'action (*Autoriser / Interdire*) appliquée à chaque service peut être modifiée en cliquant dans la colonne **Action**. Le bouton **Tout sélectionner** permet de modifier l'action (*Autoriser / Interdire*) qui est appliquée à l'ensemble des services.

Onglet Services spécifiques

Cette liste recense les identifiants de services , les services CIP spécifiques et les identifiants de classes associés que le firewall autorise par défaut. Ces services sont autorisés par défaut (action *Autoriser*). Ces services sont classifiés par groupe de services :

- Acknowledge Handler Object,
- Assembly Object,
- Connection Manager Object,
- Connection Object,
- Connection Configuration Object,
- File Object,
- Message Router Object,
- Motion Axis Object,
- Parameter Object,
- S-Analog Sensor Object,
- S-Device Supervisor Object,

- S-Gas Calibration Object,
- S-Partial Pressure Object,
- S-Sensor Calibration Object,
- S-Single Stage Controller Object,
- Time Sync Object.

Les boutons **Interdire par jeu de services**, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services CIP listés dans la grille.

Classes et services personnalisés

Cette liste permet de filtrer pour des identifiants de classe sélectionnés (compris entre 0 et 65535, séparés par des virgules, ou par un tiret pour définir une plage), les identifiants de services CIP à autoriser (compris entre 0 et 127, séparés par des virgules, ou par un tiret pour définir une plage). Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

ETHERNET/IP (onglet IPS)

Paramètres

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session EtherNet/IP. Cette valeur doit être comprise entre 1 et 512 (valeur par défaut: 10).
Durée max. d'une requête (en secondes)	Ce délai fixe une limite au-delà de laquelle les requêtes EtherNet/IP restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 3600 (valeur par défaut: 10).
Taille max. d'un message (en octets)	Cette valeur permet de limiter la taille autorisée d'un message EtherNet/IP. Elle doit être comprise entre 24 et 65535 (valeur par défaut: 65535).

Gestion des commandes

Onglet Commandes publiques

Cette liste recense les commandes EtherNet/IP publiques autorisées par défaut par le firewall. L'action (*Autoriser / Interdire*) appliquée à chaque commande peut être modifiée en cliquant dans la colonne **Action**. Le bouton **Modifier toutes les commandes** permet de modifier l'action (*Autoriser / Interdire*) qui est appliquée à l'ensemble des commandes.

Onglet Autres commandes autorisées

Cette liste permet d'autoriser des commandes EtherNet/IP additionnelles bloquées par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole EtherNet/IP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête	Active ou désactive les logs permettant de tracer les requêtes EtherNet/IP.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

IEC 60870-5-104 (IEC 104)

Paramètres

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session. Cette valeur doit être comprise entre 1 et 32768 (valeur par défaut: 12).
Durée max. d'une requête (en secondes)	Ce délai fixe une limite au-delà de laquelle les requêtes restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 255 (valeur par défaut: 10).
Taille max. d'un message (en octets)	Cette valeur permet de limiter la taille autorisée d'un message. Elle doit être comprise entre 12 et 255 (valeur par défaut: 255).

Redondance

Le protocole IEC 104 intègre une notion de redondance : une machine cliente établit un certain nombre de connexions avec son serveur, une seule de ces connexions étant active à l'instant T. Cet ensemble de connexion est appelé "groupe de redondance". Lorsque la connexion active est interrompue, une des connexions déjà établies prend alors immédiatement le relais.

Nombre max. de groupes de redondance	Il s'agit du nombre maximal de groupes de redondance autorisé par serveur.
Nombre max. de connexions redondantes	Il s'agit du nombre maximal de connexions à établir au sein d'un groupe de redondance.

Gestion des ASDU

Identifiants de type publiques

Cette grille recense les *ASDU (Application Service Data Units)* prédéfinies dans le firewall. Les ASDU, représentées par leur identifiant, sont classées par *Type Id*: Transferts de fichier, Paramètres, Processus d'information et Informations système, .

Ces identifiants de type publiques sont autorisés par défaut (action *Autoriser*). Les boutons **Interdire par jeu de Type Id**, **Autoriser par jeu de Type Id** et **Modifier tous les Type ID** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu d'*ASDU* sélectionné ou à l'ensemble des *ASDU* listées dans la grille.

Autres identifiants de type autorisés

Cette liste permet d'autoriser des identifiants supplémentaires. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête IEC 60870-5-104	Active ou désactive les logs permettant de tracer les requêtes.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Paramètres avancés

Cause additionnelle

Le champ Cause de transmission (COT - Cause Of Transmission) d'un paquet IEC104 permet de spécifier la raison pour laquelle ce paquet a été transmis.
En plus de la liste de COT prédéfinis dans la norme du protocole IEC104, cette grille permet d'**Ajouter** (à l'aide du bouton du même nom) des **Causes additionnelles** qui seront analysées par le moteur de d'analyse protocolaire IEC 60870-5-104.

Onglet MODBUS (IPS)

Paramètres généraux

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session. Cette valeur doit être comprise entre 1 et 512 (valeur par défaut: 10).
Durée max. d'une requête (en secondes)	Ce délai fixe une limite au-delà de laquelle les requêtes restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 3600 secondes (valeur par défaut: 10).
Supporter les passerelles série	En cochant cette case, vous autorisez l'analyse protocolaire pour le trafic Modbus à destination d'une passerelle Modbus TCP vers port série (les messages Modbus ayant dans ce cas des champs comportant des valeurs particulières).

Unit ID autorisés

Cette liste recense les Unit Id autorisés. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Paramètres Modbus

Taille max. d'un message (en octets)	Cette valeur permet de limiter la taille autorisée d'un message. Elle doit être comprise entre 8 et 4096 (valeur par défaut: 260).
Numéro max. de fichier	Ce champ permet de fixer le numéro maximum de fichier autorisé pour les opérations de type "Read File Record" et "Write File Record" afin de protéger certains types d'automates vulnérables au delà d'une valeur définie de numéro de fichier.

Gestion des codes de fonction Modbus

Opérations publiques

Cette liste recense les fonctions publiques autorisées par défaut par le firewall. Les boutons **Modifier les opérations d'écriture** et **Modifier toutes les opérations** permettent de modifier l'action (*Autoriser / Interdire*) qui est appliquée à la fonction sélectionnée ou à l'ensemble des fonctions.

Autres opérations autorisées

Cette liste permet d'autoriser des codes de fonction additionnels bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Gestion des adresses Modbus

Ce panneau permet de filtrer les droits d'accès des codes fonction Modbus aux adresses mémoire des automates. Par défaut, tous les codes de fonction Modbus en lecture et en écriture (1,2,3,4,5,6,15,16,22,23,24) sont autorisés à accéder à toutes les plages mémoire des automates (0-65535). Il est possible d'**Ajouter** ou de **Supprimer** des règles d'accès dans cette liste en cliquant sur les boutons du même nom.

Cette protection ajoutée dans le firewall permet ainsi de définir un profil Modbus précisant les plages mémoire de l'automate dans lesquelles il est possible d'écrire des données Modbus.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête Modbus	Active ou désactive les logs permettant de tracer les requêtes.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Onglet OPC AE (IPS)

Paramètres généraux OPC AE

Cette grille recense les services OPC AE (OPC Alarms and Events) prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Events,
- OPC Type Library.

Les services OPC AE prédéfinis sont autorisés (analysés) par défaut (action *Autoriser*). Les boutons **Interdire par jeu de service**s, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC AE listés dans la grille.

Onglet OPC DA (IPS)

La grille des opérations et des groupes d'opérations

Cette grille recense les opérations OPC DA prédéfinies dans le firewall. Les différentes informations pur chaque opération / groupe d'opérations sont les suivantes :

- **Nom** : nom de l'opération ou du groupe d'opérations.
- **N° d'opération** : identifiant numérique de l'opération dans son groupe.
- **Action** : action appliquée au paquet réseau correspondant à l'opération (*Autoriser* / *Interdire*)
- **Type** : indique s'il s'agit d'une opération en *Lecture* ou en *Écriture*.

Les actions possibles

Les opérations OPC DA prédéfinies sont autorisées par défaut (action *Autoriser*). Les boutons **Interdire la sélection**, **Autoriser la sélection** et **Modif. toutes op. en écriture** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée à l'opération sélectionnée, au jeu d'opérations sélectionné ou à l'ensemble des opérations OPC DA en écriture listées dans la grille.

Onglet OPC HDA (IPS)

Paramètres généraux OPC HDA

Cette grille recense les services OPC HDA (OPC Historical Data Access) prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Browser,
- OPC Client,
- OPC Server
- OPC Type Library.

Les services OPC HDA prédéfinis sont autorisés (analysés) par défaut (action *Autoriser*). Les boutons **Interdire par jeu de service**s, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC HDA listés dans la grille.

OPC UA

Paramètres OPC UA

Taille max. d'un message client (en octets)	Cette valeur permet de limiter la taille autorisée émise par un client OPC UA. Elle doit être comprise entre 8192 et 2147483647 (valeur par défaut: 65535).
Taille max. d'un message serveur (en octets)	Cette valeur permet de limiter la taille autorisée émise par un serveur OPC UA. Elle doit être comprise entre 8192 et 2147483647 (valeur par défaut: 65535).
Interdire le mode de sécurité "None"	En cochant cette case, vous empêchez la circulation du trafic OPC UA non chiffré et non signé.

Gestion des services OPC UA

Services publiques

Cette grille recense les codes et les services OPC UA associés, prédéfinis dans le firewall. Ces codes sont classifiés par jeu d'opération: Attribute, Discovery, Method, Monitored Item, Node Management, Query, Secure Channel, Session, Subscription et View.

Les services OPC UA prédéfinis sont autorisés par défaut (action *Autoriser*). Les boutons **Interdire par jeu de services**, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC UA listés dans la grille.

Autres services autorisés

Cette liste permet d'autoriser des codes de fonction OPC UA additionnels bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole OPC UA sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête OPC UA	Active ou désactive les logs permettant de tracer les requêtes OPC UA.

PROFINET IO

A l'instar du protocole FTP, le protocole PROFINET IO peut être amené à établir plusieurs connexions pour un même flux : une connexion mère du client vers le serveur sur le port dédié au service, suivie d'une ou plusieurs connexions filles sur des ports aléatoires pour l'échange des données.

Lors de l'analyse du protocole PROFINET IO, le firewall extrait de la connexion mère les données nécessaires à la création des connexions filles (ports aléatoires à autoriser) afin de créer un squelette de connexion permettant le dialogue.

Paramètres des squelettes de connexion

Autoriser la création de squelettes	En cochant cette case, le moteur d'analyse PROFINET IO autorise la création de connexions mère et filles.
Autoriser la création de squelettes EPMAP	En cochant cette case, le moteur d'analyse PROFINET IO autorise la création de connexions mère et filles pour les transactions basées sur EPMAP.
Délai d'expiration d'un squelette	Ce paramètre définit le délai au terme duquel un squelette créé par une connexion PROFINET IO devenue inactive doit être supprimé. Par défaut il est établi à 60 secondes.

Gestion des UUID

Cette grille vous propose de gérer l'action (*Autoriser / Interdire*) appliquée aux catégories de service PROFINET IO prédéfinis sur le firewall.

Cette catégories de services sont identifiée par un UUID (Universal Unique Identifier) de 16 octets. Une info-bulle affiche l'UUID (Universal Unique Identifier) de chaque catégorie au survol de celle-ci.

Vous pouvez assigner une action à une catégorie de services, ou à toutes les catégories de services renseignées dans la grille (bouton "**Modifier tous les services**").

Gestion des numéros d'opérations

Cette grille vous propose de gérer l'action (*Autoriser / Interdire*) appliquée aux opération PROFINET IO (opérations en lecture ou écriture) prédéfinies sur le firewall et repérées par un numéro d'opération.

Vous pouvez assigner une action à une opération, à toutes les opérations (bouton "**Modifier toutes les opérations**"), ou à toutes les opérations en écriture renseignées dans la grille (bouton "**Modifier les opérations d'écriture**").

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole PROFINET IO sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête PROFINET IO	Active ou désactive le traçage des requêtes PROFINET IO

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

PROFINET-RT

Paramètres

Durée max. d'une connexion Ethernet en secondes [2-604800]	Ce délai fixe une limite au-delà de laquelle les connexions Ethernet inactives sont supprimées. Cette valeur doit être comprise entre 2 et 604800 (valeur par défaut: 60).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole PROFINET-RT sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête Ethernet	Active ou désactive les logs permettant de tracer les requêtes Ethernet.

S7

Paramètres

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session. Cette valeur doit être comprise entre 1 et 512 (valeur par défaut: 10).
Durée max. d'une requête (en secondes)	Ce délai fixe une limite au-delà de laquelle les requêtes restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 3600 (valeur par défaut: 10).
Taille max. d'un message (en octets)	Cette valeur permet de limiter la taille autorisée d'un message. Elle doit être comprise entre 11 et 3837 (valeur par défaut: 960).

Gestion des codes de fonction

Opérations prédéfinies

Cette grille recense les codes et les opérations S7 associées, prédéfinis dans le firewall. Ces codes sont classifiés par jeu d'opération: JOB et USERDATA (de différents groupes).

Les opérations S7 prédéfinies sont autorisés par défaut (action *Autoriser*). Les boutons **Interdire par jeu d'opérations**, **Autoriser par jeu d'opérations** et **Modifier toutes les opérations** permettent de modifier l'action (*Autoriser / Interdire*) appliquée au jeu d'opérations sélectionné ou à l'ensemble des opérations S7 listées dans la grille.

Autres opérations

Autres JOBS bloqués

Cette liste permet d'interdire des codes ou des plages de codes de fonctions S7 supplémentaires appartenant au jeu d'opérations de type JOB. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Autres groupes USERDATA bloqués

Cette liste permet d'interdire des jeux complets ou des plages de jeux complets d'opérations de type USERDATA. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole S7 sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête S7	Active ou désactive les logs permettant de tracer les requêtes S7.

S7 PLUS

Version de protocole

Autoriser le protocole v2	En cochant cette case, vous autorisez l'analyse de paquets S7 Plus v2. Si cette case est décochée, les paquets S7 Plus v2 seront systématiquement rejetés.
Autoriser le protocole v3	En cochant cette case, vous autorisez l'analyse de paquets S7 Plus v3. Si cette case est décochée, les paquets S7 Plus v3 seront systématiquement rejetés.

Configuration des opérations

Démarrer le PLC	Lorsque cette case est cochée, toute requête S7 Plus de démarrage de PLC sera automatiquement acceptée par le firewall.
Régler la date et l'heure	Lorsque cette case est cochée, toute requête S7 Plus de réglage de date et heure de PLC sera automatiquement acceptée par le firewall.
Arrêter le PLC	Lorsque cette case est cochée, toute requête S7 Plus d'arrêt de PLC sera automatiquement acceptée par le firewall.
Télécharger un programme	Lorsque cette case est cochée, toute requête S7 Plus de téléchargement de programme pour un PLC sera automatiquement acceptée par le firewall.
Envoyer un programme	Lorsque cette case est cochée, toute requête S7 Plus d'envoi de programme pour un PLC sera automatiquement acceptée par le firewall.

Gestion des fonctions S7 Plus

Onglet Services classiques

Cette grille recense les codes et les fonctions S7 Plus correspondants prédéfinis dans le firewall.

Code	Numéro de code S7 Plus selon la nomenclature définie par Siemens.
Nom du service	Nom de service affecté au code S7 Plus selon la nomenclature définie par Siemens.
Action	Indique l'action appliquée au code S7 Plus. Cette action peut être **Autoriser** ou **Interdire**.

Les actions possibles

Entrer un filtre...	Saisissez des caractères numériques pour filtrer la liste des codes ou des caractères alphabétiques pour filtrer la liste des noms de services classiques affichés dans la grille.
Tout sélectionner	Permet de sélectionner l'ensemble des lignes affichées dans la grille afin de leur attribuer une action commune (**Autoriser** / **Interdire**) en cliquant sur le bouton du même nom.
Autoriser la sélection	Permet d'attribuer l'action **Autoriser** à la ligne sélectionnée (ou à l'ensemble des lignes si le bouton **Tout sélectionner** a été utilisé).
Interdire	Permet d'attribuer l'action **Interdire** à la ligne sélectionnée (ou à l'ensemble des lignes si le bouton **Tout sélectionner** a été utilisé).

Onglet Services personnalisés

Cette grille permet de gérer des codes et fonctions S7 Plus personnalisés qui seront automatiquement acceptés par le firewall.

Les actions possibles

Entrer un filtre...	Saisissez des caractères numériques pour filtrer la liste des codes de services personnalisés affichés dans la grille.
Tout sélectionner	Permet de sélectionner l'ensemble des lignes affichées dans la grille afin de les **Supprimer** en une seule action en cliquant sur le bouton du même nom.
Ajouter	Permet d'ajouter un code de service S7 Plus personnalisé dans la grille.
Supprimer	Permet de supprimer le code de service S7 Plus personnalisé sélectionné ou l'ensemble des codes si le bouton **Tout sélectionner** a été utilisé.

Configuration S7 Plus

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session. Cette valeur doit être comprise entre 1 et 512 (valeur par défaut: 50).
Durée max. d'une requête (s)	Ce délai fixe une limite au-delà de laquelle les requêtes restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 3600 (valeur par défaut: 10).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole S7 Plus sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête S7 Plus	Active ou désactive les logs permettant de tracer les requêtes S7 Plus.

Onglet UMAS (IPS)

Le protocole UMAS (Unified Messaging Application Services) est la propriété intellectuelle de la société Schneider Electric. Pour assurer le dialogue entre les automates et les logiciels Schneider Electric, activez en ligne de commande l'option sysctl net.link.ether.handle802_3=1 sur les firewalls installés entre ces différents éléments.

Paramètres UMAS

Taille max. d'un message (en octets)	Cette valeur permet de limiter la taille autorisée d'un message. Elle doit être comprise entre 10 et 4096 (valeur par défaut: 1480).
Durée de vie max. d'une réservation (en secondes, 0 pour une durée infinie)	Le mécanisme de réservations permet d'éviter que certaines requêtes modifiant le comportement d'un automate ne soient exécutées de manière concurrente. Il est basé sur un identifiant de réservation défini aléatoirement par le serveur et retourné dans la réponse de Umas_takePlcReservation, puis utilisé dans le champ 'Reservation ID' des commandes envoyées par le client dans le cadre de cette réservation. Lorsqu'un serveur est réservé par un client, les demandes de réservation provenant d'autres clients sont rejetées. Selon les spécifications du protocole, une réservation non utilisée est désactivée au bout de 50 secondes. Une fois allouée, une réservation peut être utilisée par des requêtes UMAS provenant de connexions TCP différentes. En outre, la réservation continue de vivre après la fermeture d'une connexion TCP l'ayant utilisée, et ce jusqu'à son expiration (50 secondes). La valeur spécifiée dans ce champ permet donc de diminuer cette durée de vie de 50 secondes fixée par les spécifications.

Gestion des codes de fonction UMAS

Opérations publiques

Cette grille recense les codes et les fonctions UMAS associées, prédéfinis dans le firewall. Ces fonctions sont classifiées par groupe de fonctions : Application Management, Application download to PLC, Application upload from PLC, Configuration Information requests, Connection Information requests, Debugging, PLC Status commands, PLC Status requests, Read commands, Reservation requests et Write commands.

Les boutons **Interdire par groupe de fonctions** et **Autoriser par groupe de fonctions** permettent de modifier l'action (*Autoriser* / *Interdire*) qui est appliquée au groupe de fonctions sélectionné.

Autres opérations autorisées

Cette liste permet d'autoriser des codes de fonction additionnels bloqués par défaut par le firewall. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.

Protocole Microsoft RPC (DCE/RPC)

Afin de sécuriser le trafic Microsoft RPC, basé sur le standard DCE/RPC, ce module propose d'autoriser ou non chaque flux utilisant ce protocole, détaillé par service Microsoft (Microsoft Exchange, par exemple).

Onglet DCE/RPC (IPS)

A l'instar du protocole FTP, le protocole DCE-RPC peut être amené à établir plusieurs connexions pour un même flux : une connexion mère du client vers le serveur sur le port dédié au service, suivie d'une ou plusieurs connexions filles sur des ports aléatoires pour l'échange des données.

Lors de l'analyse du protocole DCE/RPC, le firewall extrait de la connexion mère les données nécessaires à la création des connexions filles (ports aléatoires à autoriser) afin de créer un squelette de connexion permettant le dialogue.

Paramètres des squelettes de connexion

Autoriser la création de squelettes	En cochant cette case, le moteur d'analyse mécanisme DCE-RPC autorise la création de connexions mère et filles.
Délai d'expiration d'un squelette	Ce paramètre définit le délai au terme duquel un squelette créé par une connexion DCE/RPC devenue inactive doit être supprimé. Par défaut il est établi à 60 secondes.
Nombre de squelettes créés par adr. IP	Il est possible de limiter le nombre de squelettes DCE/RPC créés par une même adresse IP source.

Authentification

Vérifier la légitimité de l'utilisateur	En cochant cette case, vous activez l'authentification des utilisateurs DCE/RPC. Le moteur d'analyse DCE/RPC est ainsi capable d'extraire l'utilisateur et de le comparer à la liste des utilisateurs authentifiés dans le firewall. Lorsque aucun utilisateur authentifié ne correspond à l'utilisateur présenté par la requête DCE/RPC, le paquet est bloqué.

Microsoft Appel de procédure à distance (RPC)

Onglet "Services MS-RPC prédéfinis"

Le protocole DCE/RPC permet le lancement des procédures hébergées à distance. Ces services dits MS-RPC, prédéfinis pour les principales Applications Microsoft, sont par défaut autorisés.

Ces services classés par catégories peuvent être autorisés (analysés) / interdits individuellement ou par groupe en sélectionnant plusieurs catégories à l'aide de la touche *Shift* et à l'aide des boutons proposés dans le menu *Action*. Le bouton "Modifier toutes les opérations" permet d'assigner l'action à l'ensemble des catégories de services. Les boutons "Interdire par groupe de services" et "Autoriser par groupe de services" permettent de modifier l'action affectée à un groupe complet de services. Les services interdits lèveront l'alarme « Service DCERPC interdit».

Une info-bulle affiche l'UUID (Universal Unique Identifier) de chaque service au survol de celui-ci.

Ces principales Applications Microsoft ayant des services MS-RPC prédéfinis, sont les suivants :

- Distributed File System Replication,
- Microsoft Active Directory,
- Microsoft DCOM,
- Microsoft Distributed Transaction Coordinator service,
- Microsoft Exchange,
- Microsoft File Replication service,
- Microsoft IIS,
- Microsoft Inter-site Messaging,
- Microsoft Messenger,
- Microsoft Netlogon,
- Microsoft Scheduler,
- Microsoft RPC services,
- Windows Management Instrumentation Remote Protocol.

Onglet "Services MS-RPC personnalisés"

Cette grille vous propose de renseigner l'Identifiant universel unique (UUID) de services MS-RPC qui ne seraient pas renseignés dans la liste des services MS-RPC prédéfinis. De la même manière que pour le premier onglet, vous pouvez assigner une action à un service, à un ensemble de services (boutons "Interdire par groupe de services" et "Autoriser par groupe de services") ou à tous les services renseignés (bouton "Modifier toutes les opérations").

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole MS-RPC sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête DCE-RPC	Active ou désactive le traçage des requêtes MS-RPC.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Onglet NETBIOS EPMAP (IPS)

Ce protocole permet l'amorçage des procédures hébergées à distance (bootstrap) par la distribution de l'adresse IP et du protocole d'un service MS-RPC. Les options de ce module peuvent restreindre ces relais. Les ouvertures de connexions dynamiques sur EPMAP (portmapper) sont supportées.

Squelettes

Ce protocole servant à relayer les accès aux services Microsoft, les options suivantes permettent de restreindre les services et options relayés par le serveur EPMAP.

Les squelettes peuvent uniquement être créés si l'adresse retournée dans la réponse DCE/RPC est identique à l'adresse du serveur	Cochez cette case pour autoriser les services EPMAP à créer des squelettes de connexion. Elle est cochée par défaut.
Les squelettes peuvent uniquement être créés pour les UUID Microsoft Exchange	Si l'option est cochée, seuls les services **Microsoft Exchange** pourront créer des squelettes de connexion.

Onglet OPC AE (IPS)

Paramètres généraux OPC AE

Cette grille recense les services OPC AE (OPC Alarms and Events) prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Events,
- OPC Type Library.

Les services OPC AE prédéfinis sont autorisés (analysés) par défaut (action *Autoriser*). Les boutons **Interdire par jeu de service**s, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC AE listés dans la grille.

Onglet OPC DA (IPS)

La grille des opérations et des groupes d'opérations

Cette grille recense les opérations OPC DA prédéfinies dans le firewall. Les différentes informations pur chaque opération / groupe d'opérations sont les suivantes :

- **Nom** : nom de l'opération ou du groupe d'opérations.
- **N° d'opération** : identifiant numérique de l'opération dans son groupe.
- **Action** : action appliquée au paquet réseau correspondant à l'opération (*Autoriser* / *Interdire*)
- **Type** : indique s'il s'agit d'une opération en *Lecture* ou en *Écriture*.

Les actions possibles

Les opérations OPC DA prédéfinies sont autorisées par défaut (action *Autoriser*). Les boutons **Interdire la sélection**, **Autoriser la sélection** et **Modif. toutes op. en écriture** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée à l'opération sélectionnée, au jeu d'opérations sélectionné ou à l'ensemble des opérations OPC DA en écriture listées dans la grille.

Onglet OPC HDA (IPS)

Paramètres généraux OPC HDA

Cette grille recense les services OPC HDA (OPC Historical Data Access) prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Browser,
- OPC Client,
- OPC Server
- OPC Type Library.

Les services OPC HDA prédéfinis sont autorisés (analysés) par défaut (action *Autoriser*). Les boutons **Interdire par jeu de service**s, **Autoriser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Autoriser* / *Interdire*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC HDA listés dans la grille.

NetBios CIFS (onglet IPS)

NetBios est un protocole utilisé pour le partage de fichiers/imprimantes, généralement par les systèmes Microsoft.

NetBIOS CIFS : Taille maximale des éléments (en octets)

Nom des fichiers (format SMB2)	Ce nombre doit être compris entre 1 et 65536 octets. Cette taille de nom de fichier (**SMB2 - ioctl referral request**) est fixée par défaut à 61640 pour protéger de la vulnérabilité *CVE 2009-2526*.

Microsoft RPC (DCE/RPC)

Inspecter le protocole Microsoft RPC (DCE/RPC)	Le protocole DCE/RPC pouvant être encapsulé dans ce protocole, cette option permet d'activer ou de désactiver son inspection.

Authentification

Vérifier la légitimité de l'utilisateur	En cochant cette case, vous activez l'authentification des utilisateurs via l'entête CIFS. Le plugin CIFS est ainsi capable d'extraire l'identifiant de l'utilisateur et de le comparer à la liste des utilisateurs authentifiés dans le firewall. Lorsqu'aucun utilisateur authentifié ne correspond, le paquet est alors bloqué.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole NetBios CIFS sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Onglet NETBIOS EPMAP (IPS)

Ce protocole permet l'amorçage des procédures hébergées à distance (bootstrap) par la distribution de l'adresse IP et du protocole d'un service MS-RPC. Les options de ce module peuvent restreindre ces relais. Les ouvertures de connexions dynamiques sur EPMAP (portmapper) sont supportées.

Squelettes

Ce protocole servant à relayer les accès aux services Microsoft, les options suivantes permettent de restreindre les services et options relayés par le serveur EPMAP.

Les squelettes peuvent uniquement être créés si l'adresse retournée dans la réponse DCE/RPC est identique à l'adresse du serveur	Cochez cette case pour autoriser les services EPMAP à créer des squelettes de connexion. Elle est cochée par défaut.
Les squelettes peuvent uniquement être créés pour les UUID Microsoft Exchange	Si l'option est cochée, seuls les services **Microsoft Exchange** pourront créer des squelettes de connexion.

NetBios SSN

Les écrans sont les mêmes que pour le protocole précédent, à ceci près qu'ils permettent la configuration du protocole NetBios SSN, rendant possible l'échange de messages en mode connecté.

MGCP (onglet IPS)

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Paramètres de session MGCP

Taille max. d'une commande (octets)	Une commande peut comporter entre 32 et 1024 octets.
Nb max. de paramètres par commande	Le nombre de paramètres pouvant figurer au sein d'une commande doit être compris entre 32 et 1024 octets.
Taille max. du paramètre SDP (octets)	Le paramètre SDP valide automatiquement le lancement des applications dans une session depuis le www du client ou par la messagerie. Sa taille doit être comprise entre 32 et 1024 octets.
Durée d'inactivité max. (secondes)	La durée d'inactivité maximale d'une session doit être comprise entre 60 et 604800 octets.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole MGCP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.

RTCP (onglet IPS)

Commandes RTCP

Onglet Commandes RTCP autorisées

Il est possible de définir des commandes RTCP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 115 caractères. La suppression est également autorisée.

Onglet Commandes RTCP interdites

Il est possible d'interdire des commandes RTCP au sein de la prévention d'intrusion, dans la limite de 115 caractères.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole RTCP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.

RTP (onglet IPS)

Liste des codecs RTP supportés

Cette liste contient les codecs RTP supportés par défaut.

Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole RTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête RTP	Active ou désactive les logs permettant de tracer les requêtes RTP.

RTSP

RTSP est un protocole de communication de niveau applicatif destiné aux systèmes de streaming média. Il permet de contrôler un serveur de média à distance, offrant des fonctionnalités typiques d'un lecteur audio/vidéo telles que « lecture » et « pause », et permettant un accès en fonction de la position temporelle.

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Commandes RTSP

Onglet Commandes RTSP autorisées

Ajouter	Insérer dans la liste des commandes additionnelles qui nécessitent une autorisation.
Supprimer	Sélectionnez la commande à retirer de la liste et cliquez sur **Supprimer**.

Onglet Commandes RTSP interdites

Ajouter	Insérer dans la liste des commandes additionnelles qui ne sont pas autorisées.
Supprimer	Sélectionnez la commande à retirer de la liste et cliquez sur **Supprimer**.

Taille maximale des éléments (en octets)

Requêtes RTSP	Taille maximale de la requête et de la réponse. Permet de gérer le débordement de mémoire.
En-tête RTSP	Taille maximale de l'en-tête. Permet de gérer le débordement de mémoire.
Protocole SDP	Taille maximale d'une ligne SDP. Permet de gérer le débordement de mémoire.
Content-Type	Taille maximale de l'en-tête « Content-Type ».

Paramètres de session RTSP

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponses sur une même session RTSP.
Durée de session (secondes)	Temps en secondes d'une session RTSP.
Durée d'une requête (secondes)	Temps en secondes d'une requête RTSP

Fonctionnalités RTSP

Activer le support de l'entrelacement	En cochant cette case, vous autorisez le protocole RTSP à encapsuler dans sa propre connexion TCP les protocoles RTP/RTCP utilisés pour le transport des médias et habituellement basés sur UDP. Cela peut être nécessaire lorsque les flux UDP sont refusés.
Autoriser les messages d'erreur avec contenu	Cette option permet d'accepter les messages d'erreur comportant du contenu complémentaire, généralement de type HTML.
Autoriser la renégociation des paramètres de transport des médias	En cochant cette case, le firewall autorise la mise à jour des paramètres de transport RTP/RTCP au cours d'une session.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole RTSP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête RTSP	Active ou désactive les logs permettant de tracer les requêtes SIP

SIP (onglet IPS)

Le protocole SIP assure l'analyse protocolaire ainsi que l'autorisation dynamique des connexions secondaires. L'analyse des connexions est réalisée ligne par ligne: la ligne doit être complète avant le lancement de l'analyse. Pour chaque ligne d'en-tête une vérification est réalisée en fonction de l'état de l'automate.

- Pour les requêtes et les réponses : vérification de la version SIP et de l'opération, validation de l'URI qui doit être encodée en UTF-8.

  - Analyse de l'en-tête ligne par ligne: validation des champs de l'en-tête et extraction d'information (nom de l'appelant et de l'appelé ...), protection contre les attaques (encodage, débordement de tampons, présence et ordre des champs obligatoires, format des lignes ...).

  - Analyse et validation des données présentes dans le SDP (encodage, débordement de tampons, conformité à la RFC, présence et ordre des champs obligatoires, format des lignes ...).

- Pour les réponses (en plus des vérifications précédentes): cohérence générale de la réponse et cohérence par rapport à la requête.
  La fonction d'audit est agrémentée d'un identifiant de groupe de session permettant de retrouver toutes les connexions d'une conversation, les noms de l'appelant et de l'appelé et le type de média utilisé (audio, vidéo, application, donnée, contrôle ...).

Détecter et inspecter automatiquement le protocole	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage.

Méthodes SIP

Onglet Méthodes SIP autorisées

Ajouter	Insérer dans la liste des méthodes additionnelles qui nécessitent une autorisation.
Supprimer	Sélectionnez la méthode à retirer de la liste et cliquez sur **Supprimer**.

Onglet Méthodes SIP interdites

Ajouter	Insérer dans la liste des méthodes additionnelles qui ne sont pas autorisées.
Supprimer	Sélectionnez la méthode à retirer de la liste et cliquez sur **Supprimer**.

Taille maximale des éléments (en octets)

Requête SIP [64-4096]	Taille maximale de la requête et de la réponse. Permet de gérer le débordement de mémoire.
En-tête SIP [64-4096]	Taille maximale de l'en-tête. Permet de gérer le débordement de mémoire.
Protocole SDP [64-604800]	Taille maximale d'une ligne SDP. Permet de gérer le débordement de mémoire.

Paramètres de session SIP

Nombre maximum de requêtes en attente [1-512]	Nombre maximum de requêtes sans réponses sur une même session SIP.
Durée de session (secondes) [60-604800]	Temps en secondes d'une session SIP.

Extension du protocole SIP

Activer l'extension INFO (RFC2976)	L'extension INFO permet d'échanger des informations lors d'un appel en cours. **EXEMPLE** La puissance du signal wifi de l'un des deux correspondants. Cochez la case pour activer l'extension.
Activer l'extension PRACK (RFC3262)	Il existe deux types de réponses définies par SIP : les provisoires et les définitives. L'extension PRACK permet de fournir un système de reconnaissance fiable et de garantir une livraison ordonnée des réponses provisoires dans SIP. Cochez la case pour activer l'extension.
Activer l'extension SUSCRIBE, NOTIFY (RFC3265)	Le protocole SIP inclut un mécanisme normalisé pour permettre à n'importe quel client (un téléphone en VoIP étant un exemple de client SIP) de surveiller l'état d'un autre dispositif. Si un dispositif A client veut être informé des changements de statut d'un dispositif B, il envoie une requête SUBSCRIBE (de Souscription) directement au dispositif B ou à un serveur qui rend compte de l'état du dispositif B. Si la requête SUBSCRIBE est réussie, chaque fois que le dispositif B changera d'état, le dispositif A recevra un SIP NOTIFY, message indiquant le changement du statut ou présentant des informations sur l'événement. Lorsqu'un dispositif s'enregistre sur un autre, il sera informé dès qu'un événement survient. **EXEMPLE** La mise en ligne des contacts qu'ils recherchent. Cochez la case pour activer l'extension.
Activer l'extension UPDATE (RFC3311)	L'extension UPDATE permet à un client de mettre à jour les paramètres d'une session avant qu'elle soit établie, comme l'ensemble des flux de médias et de leurs codecs. Cochez la case pour activer l'extension.
Activer l'extension MESSAGE (RFC3428)	L'extension MESSAGE est une prolongation du protocole SIP, permettant le transfert des messages instantanés. Puisque la requête MESSAGE est une prolongation au SIP, elle hérite de tous dispositifs de cheminement et de sécurité inclus dans ce protocole. Les requêtes MESSAGE portent le contenu au format de type MIME. Cochez la case pour activer l'extension.
Activer l'extension REFER (RFC3515)	L'extension REFER est utilisée notamment pour le transfert ou la redirection d'appels. Si un correspondant A essaie de joindre B et que ce dernier est indisponible, A sera redirigé vers un correspondant C, qui fait office de « référent » pour B. Cochez la case pour activer l'extension.
Activer l'extension PUBLISH (RFC3903)	L'extension PUBLISH permet de publier l'état des événements vers un destinataire. Cochez la case pour activer l'extension.
Activer le support pour le protocole PINT	Cette extension permet de faire coexister des téléphones SIP avec des services non IP (fax, etc.). Cochez la case pour activer l'extension.

Activer le support pour Microsoft Messenger (MSN)	Cette option permet d'activer le support de Microsoft Windows Messenger.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole SIP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête SIP	Active ou désactive les logs permettant de tracer les requêtes SIP.

Onglet SOFBUS / LACBUS (IPS)

Les protocoles SOFBUS / LACBUS sont la propriété intellectuelle de LACROIX Sofrel.

SOFBUS / LACBUS sont des protocoles applicatifs industriels principalement utilisés dans les infrastructures de gestion des eaux pour faire de la télégestion, qui consiste à surveiller et contrôler des sites industriels à distance.

Ces protocoles sont encapsulés dans le protocole MODBUS, qui est également un protocole applicatif industriel utilisant TCP comme protocole de transport.

Activer l'analyse SOFBUS / LACBUS dans les paquets MODBUS	Permet d'activer ou de désactiver l'analyse des protocoles SOFBUS / LACBUS dans les paquets MODBUS. La configuration par défaut de l'analyse SOFBUS / LACBUS dans le firewall respecte les spécifications de LACROIX Sofrel.

Gestion des Unités d'Information (U.I.) et des blocs SOFBUS ou LACBUS

La grille recense les Unités d'Information (U.I.) et les blocs SOFBUS ou LACBUS. Une U.I. peut contenir plusieurs blocs. Chaque élément dispose d'un nom, d'une lettre, d'une action et d'un type.

Des U.I. et des blocs sont créés par défaut dans la configuration. Ils sont identifiables selon leur type : *U.I. par défaut* ou *Bloc par défaut*. Ces derniers sont présents dans les caractéristiques techniques fournies par LACROIX Sofrel et constituent donc la configuration par défaut. Ils ne peuvent pas être renommés, déplacés ni supprimés, mais l'action associée peut être modifiée pour : *Autoriser* ou *Interdire*.

Si nécessaire, il est possible de personnaliser la configuration par défaut. Le bouton **Ajouter une U.I. ou un bloc** permet d'ajouter une *U.I. personnalisée* ou un *Bloc personnalisé* à une U.I. existante. Des règles existent concernant l'utilisation des lettres :

- Lettre d'U.I. : elle doit être majuscule. Deux U.I. ne peuvent pas porter la même lettre.
- Lettre de bloc : elle peut être majuscule ou minuscule. Deux blocs dans une même U.I. ne peuvent pas porter la même lettre majuscule ou minuscule (sensible à la casse).

Les U.I. et blocs personnalisés peuvent être renommés et déplacés tant que les règles d'utilisation des lettres sont respectées, mais l'action associée ne peut pas être modifiée.

Le bouton **Supprimer** permet de supprimer une *U.I. personnalisée* ou un *Bloc personnalisé*. Il n'est pas possible de supprimer une *U.I. par défaut* ou un *Bloc par défaut*

DNS (onglet IPS)

Taille maximale des champs DNS (en octets)

Nom DNS (requête)	Ce champ doit être compris entre 10 et 2048 octets.

Taille des messages DNS

Activer la détection des messages de grande taille	Cette case à cocher permet d'activer l'option vérifiant la longueur des messages DNS afin de générer une alarme en cas de dépassement d'un seuil précisé.
Seuil de déclenchement de l'alarme "Message DNS trop grand" [0-65535] (en octets)	Indiquez la taille à partir de laquelle un message DNS est considéré comme potentiellement suspect et déclenche l'alarme "Message DNS trop grand". Cette taille est spécifiée en octets.

Paramètres de requête DNS (en secondes)

Durée max. d'une requête	Ce délai fixe une limite au-delà duquel on supprime les requêtes DNS restées sans réponse. Cette durée de 3 secondes par défaut, peut varier de 1 à 60 secondes.

Liste blanche de domaines DNS (DNS rebinding)

Liste des noms de domaines

Cette liste contient les noms de domaines autorisés (de type <*www.nomdedomaine.fr*>, par exemple) à être résolus par un serveur se trouvant sur une interface non-protégée.

Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur **Supprimer**.

Afin d'éviter des cas de faux positifs, cette liste contient par défaut le nom de domaine du service DNS Windows (msftncsi.com).

Types d'enregistrements DNS

Onglet Types connus à interdire

Cette liste recense les types DNS connus (A, A6, AAAA, CNAME, ...) ainsi que leurs codes associés. Ces types DNS sont, par défaut, autorisés et analysés par le firewall.

L'action (*Autoriser* / *Interdire*) appliquée à un type DNS peut être modifiée en cliquant dans la colonne *Action* correspondant à ce type.

Le bouton **Tout sélectionner** permet de modifier l'action (*Autoriser* / *Interdire*) appliquée à l'ensemble des types DNS.

Onglet Types additionnels à interdire

Cette liste permet d'interdire des types DNS additionnels (identifiés par leur code). Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole DNS sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.

FTP

Le protocole FTP supporte la RFC principale [RFC959] ainsi que de nombreuses extensions.

L'activation de ce protocole permet de prévenir des grandes familles d'attaques applicatives basées sur le protocole FTP. Ce protocole effectue diverses analyses comme l'analyse de conformité aux RFC, la vérification de la taille des paramètres des commandes FTP ou les restrictions sur le protocole (SITE EXEC par exemple). Ces analyses, permettent ainsi de stopper les attaques comme FTP Bounce, FTP PASV DoS, Buffer Overflow… Ce protocole est indispensable pour permettre au trafic FTP de traverser le firewall et de gérer dynamiquement les connexions de données du protocole FTP.

Onglet IPS

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Authentification

Autoriser l'authentification SSL	Activation du support de l'authentification SSL pour le protocole (FTP uniquement). En cochant cette option, les données personnelles comme le login et le mot de passe pourront être chiffrées, et donc, protégées.
Ne pas analyser la phase d'authentification FTP	Aucune vérification des données ne sera effectuée

Taille des éléments (en octets)

La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

Nom d'utilisateur	Nombre maximum de caractères que peut contenir un nom d'utilisateur : Celui-ci est compris entre 10 et 2048 octets.
Mot de passe utilisateur	Nombre maximum de caractères pour le mot de passe FTP. Il doit être compris entre 10 et 2048 octets.
Chemin (répertoire + nom de fichier)	Nombre maximum de caractères que peut contenir le parcours suivi par l'exécution du programme, soit le circuit emprunté dans l'arborescence pour parvenir au fichier FTP. Ce nombre est compris entre 10 et 2048 octets.

Commande SITE	Nombre maximum de caractères que peut contenir la commande SITE (entre 10 et 2048 octets).
Autres commandes	Nombre maximum de caractères que peut contenir les commandes supplémentaires (entre 10 et 2048 octets)

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole FTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête FTP	Activation ou désactivation de la remontée des logs concernant le protocole FTP.

Onglet Proxy

Filtrer la bannière d'accueil envoyée par le serveur FTP	En cochant cette option, la bannière du serveur ne sera plus envoyée lors d'une connexion FTP.
Interdire les rebonds (FTP bounce)	Permet d'éviter le spoofing, ou usurpation d'adresse IP. Une machine extérieure, en exécutant la commande PORT et en spécifiant une adresse IP interne, pourrait accéder à des données confidentielles, en exploitant les failles d'un serveur FTP ou d'une machine vulnérables par « rebond ».

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Modes de transfert autorisés

Entre le client et le proxy	Lorsque le client FTP envoie une requête au serveur, celle-ci est d'abord interceptée par le proxy qui l'analyse. Du point de vue du « client » FTP, le proxy correspond au serveur. Cette option permet de définir le mode de transfert autorisé : • Si **Actif uniquement** est spécifié, le client FTP détermine le port de connexion à utiliser pour transférer les données. Le serveur FTP initialisera la connexion de son port de données (port 20) vers le port spécifié par le client. • Si **Passif uniquement** est spécifié, le serveur FTP détermine lui-même le port de connexion à utiliser afin de transférer les données (data connexion) et le transmet au client. • Si **Actif et passif** est spécifié, le client FTP aura le choix entre les deux modes de transfert au moment de la configuration du firewall.
Entre le proxy et le serveur	Lorsque le proxy a terminé l'analyse de la requête cliente, il la transfère au serveur FTP. Ce dernier interprète le proxy comme le client FTP, puisque le proxy a un rôle intermédiaire, il est transparent. Les modes de transfert autorisés sont les mêmes que pour l'option précédente.

Onglet Commandes FTP

Proxy

Onglet Commandes principales

Commande	Nom de la commande.
Action	3 autorisations possibles entre « Autoriser sans analyser », « Autoriser » et « Interdire ».
Type de commande	Indication du type de commande. Les commandes FTP dites «d'écriture» définies dans les RFC sont des commandes pouvant entraîner des modifications au niveau du serveur comme, par exemple, la suppression de données ou encore la création de répertoires. Le fonctionnement de ces commandes est identique aux commandes dites « génériques » : en effet, vous pouvez autoriser une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Onglet Autres commandes autorisées

Il est possible d'**Ajouter** des commandes supplémentaires, dans la limite de 21 caractères, et de les **Supprimer** si besoin.

IPS

Onglet Commandes FTP autorisées

Il est possible de définir des commandes FTP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 115 caractères. La suppression est également autorisée.

Onglet Commandes FTP interdites

Il est possible d'interdire des commandes FTP au sein de la prévention d'intrusion, dans la limite de 115 caractères.

Liste des commandes génériques FTP et détail du filtrage

- **ABOR** : Commande qui interrompt le transfert en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **ACCT** : Commande qui spécifie le compte à utiliser pour se connecter. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **ADAT** : Commande qui envoie des données de sécurité pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **AUTH** : Commande qui sélectionne le mécanisme de sécurité pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **CCC** : Commande qui autorise le message non protégé.
- **CDUP** : Commande qui modifie le répertoire de travail au parent. Cette commande n'accepte pas d'argument. . Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **CONF** : Commande qui spécifie le message « confidentiel » utilisé pour l'authentification.
- **CWD** : Cette commande modifie le répertoire de travail. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.

- **ENC** : Cette commande spécifie le message « privé » utilisé pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **EPRT** : Cette commande active le mode de transfert actif étendu. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **EPSV** : Cette commande sélectionne le mode de transfert passif étendu. Cette commande doit être passée avec au plus un argument. Cette commande est bloquée par défaut.
- **FEAT** : Cette commande affiche les extensions supportées par le serveur. Elle n'accepte pas d'argument. Le résultat de cette commande est filtré par le proxy si on demande le filtrage de la commande FEAT.
- **HELP** : Cette commande retourne les détails pour une commande donnée. Cette commande doit être passée avec au plus un argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **LIST** : Cette commande liste le contenu d'une localisation donnée d'une manière amicale.
- **MDTM** : Cette commande affiche le dernier temps de modification pour un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MIC** : Cette commande spécifie le message « sain » utilisé pour l'authentification. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MLSD** : Cette commande affiche le contenu du dossier normalisé. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MLST** : Cette commande affiche l'information du fichier normalisé. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **MODE** : Cette commande spécifie le mode de transfert. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les arguments S, B, C et Z. Si l'analyse antivirale est activée, seul l'argument S est autorisé.
- **NLST** : Cette commande liste le contenu d'une localisation donnée de l'ordinateur de manière amicale. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **NOOP** : Cette commande ne fait rien. Elle n'accepte pas d'arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **OPTS** : Cette commande spécifie les options d'état pour la commande donnée. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PASS** : Cette commande spécifie le mot de pass utilisé pour la connexion. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PASV** : Cette commande sélectionne le mode de transfert passif. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PBSZ** : Cette commande spécifie la taille des blocs encodés. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PORT** : Cette commande sélectionne le mode de transfert actif. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **PROT** : Cette commande spécifie le niveau de protection. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. En effet, seuls les arguments C, S E et P sont acceptés.

- **PWD** : Cette commande affiche le dossier de travail en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **QUIT** : Cette commande termine la session en cours et la connexion. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **REIN** : Cette commande termine la session en cours (initialisée avec l'utilisateur). Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **REST** : Cette commande spécifie l'offset par lequel le transfert doit être repris. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. En effet, elle est interdite en cas d'analyse antivirale. Dans le cas contraire, le proxy vérifie qu'un seul argument est présent.
- **RETR** : Cette commande récupère un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC
- **SITE** : Cette commande exécute une commande spécifique du serveur. Cette commande n'accepte qu'un seul argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **SIZE** : Cette commande affiche la taille de transfert pour un fichier donné. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **SMNT** : Cette commande modifie la structure de données du système en cours. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **STAT** : Cette commande affiche l'état en cours. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **STRU** : Cette commande spécifie la structure des données transférées. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les arguments F, R et P. Si l'analyse antivirale est activée, alors seul l'argument F est autorisé.
- **SYST** : Cette commande affiche l'information à propos du système d'opération du serveur. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **TYPE** : Cette commande spécifie le type des données transférées. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC. Cette commande fait l'objet d'un filtrage plus important. Elle n'est autorisée qu'avec les commandes ASCII, EBCDIC, IMAGE, I, A, E, L. Si l'analyse antivirale est activée, seuls les arguments ASCII, IMAGE, I et A sont autorisés. L'option L peut être suivie d'un argument numérique. L'option L peut être suivie d'un argument numérique. Les options E, A, EBCDIC et ASCII acceptent les arguments suivants : N, C et T.
- **USER** : Cette commande spécifie le nom de l'utilisateur utilisé pour se connecter.
- **XCUP** : Cette commande modifie le dossier de travail au parent. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **XCWD** : Cette commande modifie le dossier de travail. Cette commande accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.
- **XPWD** : Cette commande affiche le dossier de travail en cours. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC.

Liste des commandes de modification FTP et détail du filtrage

- **ALLO** : Cette commande alloue de l'espace de stockage sur ce serveur. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **APPE** : Cette commande ajoute (ou crée) à la localisation donnée. Cette commande fait l'objet d'un filtrage plus important. En effet, cette commande est interdite lorsque l'analyse antivirale est activée (risque de contournement). Dans le cas contraire, on vérifie qu'au moins un argument est présent.
- **DELE** : Cette commande supprime un fichier donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **MKD** : Cette commande crée un nouveau répertoire. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RMD** : Cette commande supprime le répertoire donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RNFR** : Cette commande sélectionne un fichier qui doit être renommé. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **RNTO** : Cette commande spécifie le nouveau nom du fichier sélectionné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **STOR** : Cette commande conserve un fichier donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **STOU** : Cette commande conserve un fichier donné avec un nom unique. Cette commande n'accepte pas d'argument. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **XMKD** : Cette commande créée un nouveau répertoire. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.
- **XRMD** : Cette commande supprime le répertoire donné. Elle accepte un ou plusieurs arguments. Par défaut, une analyse est faite afin de vérifier la conformité à la RFC si l'option « Activer les commandes de modification » est activée. Sinon, la commande est bloquée.

Onglet Utilisateurs FTP

Liste des utilisateurs

Onglet Utilisateurs autorisés

Il est possible de définir des utilisateurs FTP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 127 caractères. La suppression est également autorisée.

Onglet Utilisateurs refusés

Il est possible d'interdire des utilisateurs FTP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 127 caractères. La suppression est également autorisée.

Onglet Analyse des fichiers

Taille max. pour l'analyse antivirale et sandboxing (Ko)	Il est possible ici de déterminer la taille maximale utilisée pour l'analyse des fichiers. Vous pouvez également configurer l'action à entreprendre si le fichier est supérieur à la taille autorisée. **AVERTISSEMENT** Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur FTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps. Cette option correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. La taille par défaut dépend du modèle de firewall : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 et EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 et EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 et EVAU : 16000 Ko.
Analyser les fichiers	Cette option permet de choisir le type de fichier devant être analysé : les fichiers « téléchargés et envoyés » ; les fichiers « téléchargés uniquement » ou les fichiers « envoyés uniquement ».

Actions sur les fichiers

Lorsqu'un virus est détecté	Cette option propose deux actions : « Autoriser » et « Interdire ». En sélectionnant « Bloqué », le fichier analysé n'est pas transmis. En sélectionnant « Autoriser », l'antivirus transmet le fichier en cours d'analyse.
Lorsque l'antivirus ne peut analyser	Cette option définit l'état de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **EXEMPLE** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.
Lorsque la collecte des données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible d'**Interdire** le trafic en cas d'échec de la récupération des informations, ou de l'**Autoriser sans analyser**

Onglet Analyse sandboxing (Breach Fighter)

Sandboxing

État	Cette colonne affiche l'état (**Activé**/**Désactivé**) de l'analyse sandboxing pour le type de fichier correspondant. Double-cliquez dessus pour changer l'état.
Type de fichiers	L'option sandboxing propose l'analyse de différents types de fichiers : • **Archive** : sont inclus les principaux types d'archives (zip, .tar, .rar, .gz, .gzip, .bz2, .7z, ...). • **Fichier HTML**. • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous Windows (.exe, .bat, .cmd , .scr, ...). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar"). • **Scripts** : PowerShell, Javascript, VBScript, Batch, Python. • **E-mail avec pièce jointe**. • **Image**. • **Autre**.
Taille max. des fichiers analysés (Ko)	Ce champ permet de définir la taille maximale des fichiers devant être soumis à l'analyse sandboxing. Par défaut, cette valeur est égale à celle du champ **Taille max. pour l'analyse antivirale et sandboxing (Ko)** présent dans l'onglet *Analyse des fichiers*. Elle ne peut l'excéder.

Limites

- Taille maximale du fichier à analyser : 10 Mo.
- Nombre maximal de fichiers au sein d'un même mail ou d'une même archive : 10.
- Nombre maximal de niveaux d'imbrication au sein d'une même archive : 10.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. En sélectionnant « Interdire », le fichier analysé n'est pas transmis. En sélectionnant « Autoriser », le fichier est transmis dans son état.
Lorsque sandboxing ne peut analyser	Cette option définit le comportement de l'option sandboxing si l'analyse du fichier échoue : • Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. • Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

HTTP

L'activation de ce protocole permet la prévention de grandes familles d'attaques applicatives basées sur le protocole HTTP. Les différentes analyses effectuées par ce protocole (notamment la vérification de la conformité aux RFC), la validation de l'encodage utilisé dans l'URL ou la vérification de la taille de l'URL et du corps de la requête, vous permettent de stopper des attaques telles que Code RED, Code Blue, NIMDA, HTR, Buffer Overflow ou encore Directory Traversal.

La gestion des débordements de tampons (ou Buffer Overflow) est primordiale chez Stormshield Network, c'est pourquoi la définition des tailles maximales permises pour les tampons dans le cadre du protocole HTTP est particulièrement développée.

Onglet IPS

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Options des moteurs de recherche

Activer le filtrage des moteurs de recherche (Safesearch)	Ce mécanisme permet d'exclure des sites web, les documents ou images manifestement inappropriés ou indésirables des résultats d'une recherche effectués sur les principaux moteurs de recherche (Google, Bing, Yahoo)
Limitation du contenu YouTube	Ce champ permet de sélectionner le type de limitations qui seront appliquées aux résultats d'une recherche de vidéos lors d'une recherche sur la plate-forme YouTube : • le choix "stricte" permet de filtrer les vidéos non appropriées, • le choix "modérée" présente les résultats les plus pertinents et peut donc peut laisser passer des vidéos inappropriées.
Services et comptes Google autorisés	Cette option permet de restreindre l'accès aux services et comptes Google en renseignant dans cette liste, les seuls domaines autorisés. Renseignez dans cette liste le domaine avec lequel vous vous êtes inscrit à Google Apps, ainsi que les éventuels domaines secondaires que vous y avez ajoutés. L'accès aux services Google à partir d'un compte non autorisé sont redirigés une page de blocage de Google. Le principe est que le firewall intercepte le trafic SSL à destination de Google et y ajoute l'en-tête HTTP « X-GoogApps-Allowed-Domains », dont la valeur est la liste des noms de domaine autorisés, séparés par des virgules. Pour plus d'informations, consultez le lien suivant : FR https://support.google.com/a/answer/1668854?hl=fr EN https://support.google.com/a/answer/1668854?hl=en **NOTE** Cette fonctionnalité nécessite d'activer l'inspection SSL dans la politique de filtrage.

Analyses HTML/JavaScript

Inspecter le code HTML	Toute page contenant du contenu HTML susceptible d'être malveillant sera bloquée.
Longueur max. d'un attribut HTML (octets)	Nombre maximum d'octets pour un attribut d'une balise HTML (Min : 128 ; Max : 65536)..

Inspecter le code JavaScript	Afin d'éviter que des contenus malveillants ne viennent endommager les pages web dynamiques et interactives que fournit le langage de programmation JavaScript, une analyse est effectuée afin de les détecter. De la même façon que l'option **Inspecter le code HTML**, si cette case est cochée, une page contenant du contenu JavaScript susceptible d'être malveillant sera bloquée.
Supprimer automatiquement les contenus malveillants	Plutôt que d'interdire la connexion TCP, l'analyse efface le contenu malveillant (ex: attribut, balise HTML) et laisse passer le reste de la page HTML. **EXEMPLE D'ACTION MALVEILLANTE** Toute redirection à votre insu, vers un site web non souhaité. **NOTE** Cocher cette case désactive l'option **Activer la décompression à la volée des données**.
Activer la décompression à la volée des données	Lorsque les serveurs HTTP présentent des pages compressées, activer cette option permet de décompresser les données et de les inspecter au fur et à mesure de leur passage par le firewall. Aucune réécriture de données n'étant effectuée, cette opération n'induit donc aucun délai supplémentaire. **NOTE** Cocher cette case désactive l'option **Supprimer automatiquement les contenus malveillants**.

Liste d'exclusion de la suppression automatique de code malveillant (User-Agent)

Celle-ci regroupe les navigateurs et leurs données qui ne seront pas supprimés automatiquement par l'option cité ci-dessus. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Authentification

Vérifier la légitimité de l'utilisateur	En cochant cette case, vous activez l'authentification des utilisateurs via l'entête HTTP "Authorization". Le plugin HTTP est ainsi capable d'extraire l'utilisateur et de le comparer à la liste des utilisateurs authentifiés dans le firewall. Lorsqu'aucun utilisateur authentifié ne correspond, le paquet est alors bloqué.

Configuration avancée

URL : taille maximale des éléments (en octets)

La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

URL (domaine + chemin)	Taille maximum d'une URL, nom de domaine et chemin compris [128 – 4096 octets]
Par paramètre (après le '?' [argument])	Taille maximum d'un paramètre dans une URL [128 – 4096 (octets)]
Requête complète (URL+ paramètres)	Nombre maximal d'octets pour la requête entière : http://URLBuffer ?QueryBuffer [128 – 4096] (octets)]

URL

Nombre maximum de paramètres (après le '?')	Nombre maximum de paramètres dans une URL (Min :0 ; Max : 512).

Format des entêtes HTTP (en octets)

Nombre de lignes par requête cliente	Nombre maximum de lignes (ou headers) que peut contenir une requête, du client vers le serveur (Min :16 ; Max : 512).
Nombre de plages par requête cliente	Nombre maximum de plages de données (ou range) que peut contenir une requête, du client vers le serveur (Min : 0 ; Max : 1024).
Nombre de lignes par réponse serveur	Nombre maximum de lignes (ou headers) que peut contenir une réponse du serveur vers le client (Min : 16 ; Max : 512).

Taille maximale des champs HTTP (en octets)

Champ AUTHORIZATION	Nombre maximum d'octets pour le champ AUTHORIZATION incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ CONTENTTYPE	Nombre maximum d'octets pour le champ CONTENTTYPE incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ HOST	Nombre maximum d'octets pour le champ HOST incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ COOKIE	Nombre maximum d'octets pour le champ COOKIE incluant les attributs de formatage. (Min : 128 ; Max : 8192).
Autres champs	Nombre maximum d'octets pour les autres champs incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ Authorization (NTLM)	Nombre maximum d'octets pour le champ AUTHORIZATION (NTLM) incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ Content-Security-Policy	Nombre maximum d'octets pour le champ CONTENT-SECURITY-POLICY incluant les attributs de formatage. (Min : 128 ; Max : 65535).

Paramètres de sessions HTTP (en secondes)

Durée max. d'une requête	Programmée à 30 secondes par défaut (Max : 600 secondes).

Extensions du protocole HTTP

Autoriser le protocole Shoutcast	Cette option autorise le transport de son à travers le protocole HTTP. **EXEMPLES** Webradio, webtv.
Autoriser les connexions WebDAV (lecture et écriture)	Cette option permet d'ajouter des fonctionnalités d'écriture et de verrou au protocole HTTP, ainsi que de sécuriser plus facilement les connexions HTTPS.

Commandes HTTP autorisées

Liste des commandes HTTP autorisées (au format CSV). Toutes les commandes incluses ne peuvent excéder 126 caractères. Il est possible d'**Ajouter** ou de **Supprimer** des commandes via les boutons du même nom.

Commandes HTTP interdites

Liste des commandes HTTP interdites (au format CSV). Toutes les commandes incluses ne peuvent excéder 126 caractères. Il est possible d'**Ajouter** ou de **Supprimer** des commandes via les boutons du même nom.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole HTTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête HTTP	Active ou désactive les logs permettant de tracer les requêtes HTTP.

Onglet Proxy

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Filtrage URL (base Extended Web Control uniquement)

Lorsque l'URL n'a pas pu être classifiée	Le choix est l'action **Autoriser** ou **Interdire.** Si une URL n'est pas répertoriée dans une catégorie d'URL, cette action détermine si l'accès au site est autorisé.
Autoriser les adresses IP dans les URL	Une option permet d'autoriser ou non l'usage d'adresse IP dans l'URL, c'est-à-dire l'accès à un site par son adresse IP et non par son nom de domaine. En effet, cet usage peut être une tentative de contournement du filtrage URL. Si l'option est décochée et que l'URL interrogée (contenant une adresse IP) ne peut être classifiée par le système de Filtrage URL, son accès sera bloqué. Cependant, cette option est conçue pour s'appliquer après l'évaluation du filtrage. En conséquence, un serveur interne joint par son adresse IP, ne sera pas bloqué si son accès est explicitement autorisé dans la politique de filtrage (politique différente de pass all). Cet accès peut être autorisé via les objets Réseau de base du firewall (RFC5735) ou le groupe « Private IP » de la Base URL EWC.

NOTE
Que l'option précédente soit activée ou non, une adresse IP écrite dans un format différent du type *a.b.c.d*, est systématiquement bloquée.

Extensions du protocole HTTP

Autoriser les connexions WebDAV (lecture et écriture)	WebDAV est un ensemble d'extensions au protocole HTTP concernant l'édition et la gestion collaborative de documents. Si cette option est cochée, le protocole WebDav est autorisé au travers du firewall Stormshield Network.
Autoriser les tunnels TCP (méthode CONNECT)	La **méthode CONNECT** permet de réaliser des tunnels sécurisés au travers de serveurs proxies. Si cette option est cochée la méthode **CONNECT** est autorisée au travers du firewall Stormshield Network.

Tunnels TCP : Liste des ports de destinations autorisés

Cette zone sert à spécifier quels types de service peuvent utiliser la méthode **CONNECT**.

Port de destination (objet service)	Le bouton **Ajouter** vous permet d'ajouter des services via la base d'objets. Pour **modifier** un service, sélectionnez la ligne à modifier puis faites votre nouvelle sélection. Le bouton **Supprimer** vous permet de supprimer le service sélectionné.

Configuration avancée

Qualité de la protection

Vérifier l'encodage de l'URL	En cochant cette option, la politique de filtrage ne peut être contournée.

Trafic émis vers le serveur

Ajouter l'utilisateur authentifié dans l'en-tête HTTP	Si le proxy HTTP externe nécessite une authentification des utilisateurs, l'administrateur peut cocher cette option pour envoyer au proxy externe les informations concernant l'utilisateur recueilli par le module d'authentification du firewall.

Proxy explicite

Le proxy explicite permet de référencer le proxy du firewall dans le navigateur et de lui transmettre directement les requêtes HTTP.

Activer l'authentification "Proxy-Authorization" (HTTP 407)	Le navigateur demande à l'utilisateur de s'authentifier via une fenêtre de message et l'information de connexion est relayée au Firewall via l'entête HTTP. **NOTE** L'authentification "Proxy-Authorization" (HTTP 407) par le navigateur n'autorise pas les méthodes SSL (certificats) et SPNEGO, car ces méthodes ne font pas intervenir le portail d'authentification, même si celui-ci doit être activé. Pour plus d'informations, consultez l'aide du module **Authentification**, section « Proxy HTTP transparent ou explicite et objets Multi-utilisateur »

Onglet ICAP

Réponse HTTP (reqmod)

Les contenus Web et Mail sont principalement visés par le protocole ICAP. Il fournit une interface aux proxies HTTP (pour le web) et aux relais SMTP (pour les mails).

Transmettre les requêtes HTTP au serveur ICAP	Chaque requête cliente vers un site web est transmise au serveur ICAP.

Serveur ICAP

Serveur	Indication du serveur ICAP.
Port ICAP	Indication du port ICAP.
Nom du service ICAP	Indication du nom du service à mettre en place. Cette information est différente suivant la solution utilisée, le serveur ICAP ainsi que le port utilisé.

Authentification sur le serveur ICAP

On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP.

Exemple

Il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP.

Transmettre le nom d'utilisateur / le groupe	Cette option permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié).
Transmettre l'adresse IP du client	Cette option permet de se servir des adresses IP des clients HTTP effectuant la requête à Adapter (objet utilisé pour faire la traduction entre le format ICAP et le format demandé).

Configuration avancée

Liste blanche (pas de transmission au serveur ICAP)

Serveur HTTP (Machine – Réseau – Plage d'adresse)	Permet d'ajouter des machines, des réseaux ou des plages d'adresses dont les informations ne seront pas transmises au serveur ICAP. Ceux-ci peuvent être supprimés de la liste à tout moment.

Onglet Analyse des fichiers

Transfert de fichiers

Téléchargement partiel	Par exemple lorsqu'on télécharge un fichier via HTTP si le téléchargement ne s'effectue pas jusqu'au bout (erreur de connexion par exemple), il est possible de relancer le téléchargement à partir de là où a surgi l'erreur plutôt que de devoir tout télécharger de nouveau. Il s'agit dans ce cas d'un téléchargement partiel (le téléchargement ne correspond pas à un fichier complet). L'option **Téléchargement partiel** permet de définir le comportement du proxy HTTP du firewall vis-à-vis de ce type de téléchargement. • **Interdire** : le téléchargement partiel est interdit • **Interdire si analyse de fichiers active** : le téléchargement partiel est autorisé sauf si le flux correspond à un trafic inspecté par une règle avec analyse antivirale. • **Autoriser** : le téléchargement partiel est autorisé mais il n'y a pas d'analyse antivirale effectuée.
Taille maximale d'un fichier (Ko)	Lorsque les fichiers téléchargés sur l'Internet, via HTTP, sont trop imposants, ils peuvent dégrader la bande passante du lien Internet et cela pour une durée parfois très longue. Pour éviter cela, indiquez la taille maximum en Ko pouvant être téléchargée par le protocole HTTP.
URL exclues de l'analyse antivirale	Une catégorie d'URL ou groupe de catégorie peut être exclue de l'analyse antivirale. Par défaut, il existe dans la base Objet, un groupe d'URL nommé *antivirus_bypass* contenant les sites de mise à jour Microsoft.

Filtrage des fichiers (par type MIME)

État	Indique l'état actif ou inactif du fichier. 2 positions sont disponibles : « Activé » ou « Désactivé »
Action	Indique l'action à mettre en place pour le fichier en question, il existe 3 possibilités : • **Détecter et bloquer les virus** : Le fichier est analysé afin de détecter les virus pouvant s'y être glissé, ceux-ci seront bloqués. • **Autoriser sans analyse des fichiers** : Le fichier peut être téléchargé librement, aucune analyse antivirale n'est effectuée. • **Interdire** : Le téléchargement du fichier est interdit.
Type MIME	Indique de quel type de contenu de fichier il s'agit. Cela peut être du texte, de l'image ou de la vidéo, à définir dans ce champ. **EXEMPLES** « text/plain* » « text/* » « application/* »

Taille max. pour l'analyse antivirale et Sandboxing (Ko)	Cette option correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. La taille par défaut dépend du modèle de firewall : • SN160(W), SN210(W), SN310 et EVA1 : 4000 Ko. • SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA2 et EVA3 : 8000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 et EVA4 : 16000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 et EVAU : 32000 Ko.

Actions sur les fichiers

Lorsqu'un virus est détecté	Ce champ contient 2 options. En sélectionnant « Interdire », le fichier analysé n'est pas transmis. En sélectionnant « Autoriser », l'antivirus transmet le fichier dans son état.
Lorsque l'antivirus ne peut analyser	Cette option définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **EXEMPLE** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.
Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible d'**Interdire** le trafic en cas d'échec de la récupération des informations, ou de l'**Autoriser sans analyser**. **EXEMPLE** Si le disque dur est plein, le téléchargement des informations ne pourra pas être effectué.

Onglet Analyse sandboxing (Breach Fighter)

Sandboxing

État	Cette colonne affiche l'état (**Activé**/**Désactivé**) de l'analyse sandboxing pour le type de fichier correspondant. Double-cliquez dessus pour changer l'état.

Type de fichiers	L'option sandboxing propose l'analyse de différents types de fichiers : • **Archive** : sont inclus les principaux types d'archives (zip, .tar, .rar, .gz, .gzip, .bz2, .7z, ...). • **Fichier HTML**. • **Document bureautique (logiciels Office)** : tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable** : fichiers exécutables sous Windows (.exe, .bat, .cmd , .scr, ...). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar"). • **Scripts** : PowerShell, Javascript, VBScript, Batch, Python. • **E-mail avec pièce jointe**. • **Image**. • **Autre**.
Taille max. des fichiers analysés (Ko)	Ce champ permet de définir la taille maximale des fichiers devant être soumis à l'analyse sandboxing. Par défaut, cette valeur est égale à celle du champ **Taille max. pour l'analyse antivirale et sandboxing (Ko)** présent dans l'onglet *Analyse des fichiers*. Elle ne peut l'excéder.

Limites

- Taille maximale du fichier à analyser : 10 Mo.
- Nombre maximal de fichiers au sein d'un même mail ou d'une même archive : 10.
- Nombre maximal de niveaux d'imbrication au sein d'une même archive : 10.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options : • En sélectionnant **Interdire**, le fichier analysé n'est pas transmis. • En sélectionnant **Autoriser**, le fichier est transmis dans son état.
Lorsque sandboxing ne peut analyser	Cette option définit le comportement de l'option sandboxing si l'analyse du fichier échoue. • Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. • Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

NTP

Network Time Protocol (« protocole d'heure réseau ») ou NTP est un protocole qui permet de synchroniser, via le réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.

Dès le début, ce protocole fut conçu pour offrir une précision de synchronisation meilleure que la seconde. Par rapport au service « Time Protocol » qui offre un service d'heure sans proposer une infrastructure, le projet NTP propose une solution globale et universelle de synchronisation qui est utilisable dans le monde entier.

Onglet IPS

Versions autorisées

Cochez les cases correspondant aux versions du protocole NTP que vous souhaitez analyser. Les paquets correspondant aux versions non cochées provoqueront la levée de l'alarme "NTP : version refusée" et seront bloqués par le firewall.

Version 1	En cochant cette case, vous activez l'analyse de prévention d'intrusion pour la version 1 du protocole NTP.
Version 2	En cochant cette case, vous activez l'analyse de prévention d'intrusion pour la version 2 du protocole NTP.
Version 3	En cochant cette case, vous activez l'analyse de prévention d'intrusion pour la version 3 du protocole NTP.
Version 4	En cochant cette case, vous activez l'analyse de prévention d'intrusion pour la version 4 du protocole NTP.

Paramètres généraux

Nombre max. de requêtes en attente	Nombre maximum de requêtes sans réponse sur une même session NTP. Cette valeur doit être comprise entre 1 et 512 (valeur par défaut: 10).
Durée max. d'une requête (en secondes)	Ce délai fixe une limite au-delà de laquelle les requêtes NTP restées sans réponse sont supprimées. Cette valeur doit être comprise entre 1 et 3600 (valeur par défaut: 10).

Protection contre les attaques de type Time Poisoning

Seuil de décalage d'horloge autorisé (minutes)	Ce paramètre indique la limite de décalage d'horloge susceptible d'être envoyée par un serveur NTP vers un client NTP. Au delà de la valeur indiquée (20 minutes par défaut), la machine cliente émettant les requêtes NTP sera considérée comme étant la cible d'une attaque de type Time Poisoning et déclenchera l'alarme ntp:463 "NTP : possible attaque de type poisoning" (alarme bloquante par défaut) . Cette protection est basée sur l'horloge interne du firewall. Assurez-vous que l'horloge du firewall est correctement configurée (voir le module Configuration > Paramètres de date et d'heure). La valeur "0" désactive cette protection.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole NTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête du mode client NTP	Active ou désactive les logs permettant de tracer les requêtes NTP.

Onglet IPS - NTP v1

Configuration de base

Taille maximale des paquets (octets)	Renseignez la taille maximale autorisée pour les paquets NTP v1 (valeur par défaut: 72 octets).

Modes NTP

Cette liste recense les modes NTP v1 connus (symétrique actif, symétrique passif, client et serveur) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement un mode en cliquant sur son action associée,
- De sélectionner tous les modes avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Configuration avancée

***Reference ID* interdites**

Cette liste permet d'interdire des *Reference ID* NTP additionnelles (LOCL, LCL, ...) :

- Cliquez sur le bouton **Ajouter** et précisez le nom de la *Reference ID*,
- Sélectionnez une *Reference ID* ou toutes les *Reference ID* avec le bouton **Tout sélectionner** et cliquez sur le bouton **Supprimer**.

Onglet IPS - NTP v2

Configuration de base

Taille maximale des paquets (octets)	Renseignez la taille maximale autorisée pour les paquets NTP v2 (valeur par défaut: 72 octets).

Modes NTP

Cette liste recense les modes NTP v2 connus (réservé, symétrique actif, symétrique passif, client, serveur, broadcast, messages de contrôle NTP, utilisation privée) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement un mode en cliquant sur son action associée,
- De sélectionner tous les modes avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Configuration avancée

***Reference ID* interdites**

Cette liste permet d'interdire des *Reference ID* NTP additionnelles (LOCL, LCL, ...) :

- Cliquez sur le bouton **Ajouter** et précisez le nom de la *Reference ID*,
- Sélectionnez une *Reference ID* ou toutes les *Reference ID* avec le bouton **Tout sélectionner** et cliquez sur le bouton **Supprimer**.

Onglet IPS - NTP v3

Configuration de base

Taille maximale des paquets (octets)	Renseignez la taille maximale autorisée pour les paquets NTP v3 (valeur par défaut: 120 octets).

Modes NTP

Cette liste recense les modes NTP v3 connus (réservé, symétrique actif, symétrique passif, client, serveur, broadcast, messages de contrôle NTP, utilisation privée) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement un mode en cliquant sur son action associée,
- De sélectionner tous les modes avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Configuration avancée

Reference ID interdites

Cette liste permet d'interdire des *Reference ID* NTP additionnelles (LOCL, LCL, ...) :

- Cliquez sur le bouton **Ajouter** et précisez le nom de la *Reference ID*,
- Sélectionnez une *Reference ID* ou toutes les *Reference ID* avec le bouton **Tout sélectionner** et cliquez sur le bouton **Supprimer**.

Onglet IPS - NTP v4

Configuration de base

Taille maximale des paquets (octets)	Renseignez la taille maximale autorisée pour les paquets NTP v4 (valeur par défaut: 72 octets).

Modes NTP

Cette liste recense les modes NTP v4 connus (réservé, symétrique actif, symétrique passif, client, serveur, broadcast, messages de contrôle NTP, utilisation privée) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement un mode en cliquant sur son action associée,
- De sélectionner tous les modes avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Configuration avancée

Gestion des *Reference ID*

Onglet *Reference ID* prédéfinies

Cette liste recense les *Reference ID* par défaut (définies dans la RFC) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement une *Reference ID* en cliquant sur son action associée,
- De sélectionner toutes les *Reference ID* avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Onglet *Reference ID* personnalisée

Cette liste permet d'ajouter ou de supprimer des *Reference ID* :

- Cliquez sur le bouton **Ajouter** et précisez le nom de la *Reference ID*,
- Sélectionnez une *Reference ID* ou toutes les *Reference ID* avec le bouton **Tout sélectionner** et cliquez sur le bouton **Supprimer**.

Paquets *Kiss of death*

Onglet *Reference ID* prédéfinies

Cette liste recense les *Reference ID* par défaut (définies dans la RFC) pouvant être impliquées dans les attaques de type *Kiss of Death* (DENY, RSTR, RATELCL, ...) et l'action appliquée à chacun d'entre eux.

Il est possible :

- D'autoriser ou d'interdire unitairement une *Reference ID* en cliquant sur son action associée,
- De sélectionner toutes les *Reference ID* avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Onglet *Reference ID* personnalisée

Cette liste permet d'ajouter ou de supprimer des *Reference ID* pouvant être impliquées dans les attaques de type *Kiss of Death* :

- Cliquez sur le bouton **Ajouter** et précisez le nom de la *Reference ID*,
- Sélectionnez une *Reference ID* ou toutes les *Reference ID* avec le bouton **Tout sélectionner** et cliquez sur le bouton **Supprimer**.

POP3

Le protocole POP3 a pour objectif de détecter les connexions entre un client et un serveur e-mail utilisant le protocole POP3.

Onglet IPS - PROXY

Ces deux fonctionnalités ont été réunies en un seul onglet par souci d'ergonomie.

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Proxy

Le trafic Mail n'est pas seulement basé sur le protocole SMTP mais aussi sur POP3. Ce protocole va permettre à l'utilisateur d'un logiciel de messagerie, de récupérer sur son poste des mails stockés sur un serveur distant. Ce serveur de mail distant pouvant être situé à l'extérieur du réseau local ou sur une interface distincte, le flux POP3 transite au travers du firewall lui permettant de réaliser son analyse.

Filtrer la bannière d'accueil envoyée par le serveur	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion POP3. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole POP3 sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête POP3	Active ou désactive les logs permettant de tracer les requêtes HTTP.

Onglet Commandes POP3

Proxy

Onglet Commandes principales

Ce menu vous permet d'autoriser ou de rejeter les commandes POP3 définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Bouton **Tout sélectionner :** Permet d'**Autoriser sans analyser**, d'**Interdire** ou d'analyser toutes les commandes (**Autoriser**).

Commande	Indication du nom de la commande
Action	Cela permet de définir le comportement attribué à la commande.3 possibilités sont disponibles. Il faut cliquer sur l'action de la commande pour pouvoir la modifier : • **Autoriser** : les données liées à la commande sont analysées en conformité avec les RFC, et bloquées si nécessaire. **EXEMPLE** Si le nom de la commande USER n'est pas conforme aux RFC, le paquet ne sera pas transmis au serveur. • **Autoriser sans analyser** : la commande est autorisée, sans vérification. • **Interdire** : la commande est bloquée d'office, une alarme sera remontée pour le stipuler.

Onglet Autres commandes autorisées

Commande	Ce champ permet d'ajouter des commandes personnelles supplémentaires à **Analyser**.

Onglet Analyse des fichiers

Taille max. pour l'analyse antivirale et sandboxing (Ko)	Cette option correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. La taille par défaut dépend du modèle de firewall : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 et EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 et EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 et EVAU : 16000 Ko.

AVERTISSEMENT
Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur POP3 est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

Action sur les messages

Cette zone décrit le comportement de l'antivirus face à certains événements.

Lorsqu'un virus est détecté	Ce champ contient 2 options. En sélectionnant **Interdire**, le fichier analysé n'est pas transmis. En sélectionnant **Autoriser**, l'antivirus transmet le fichier dans son état.
Lorsque l'antivirus ne peut analyser	Cette option définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Autoriser sans analyser** est spécifié, le fichier est transmis sans vérification.
Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible d'**Interdire** le trafic en cas d'échec de la récupération des informations, ou de l'**Autoriser sans analyser**.

Onglet Analyse sandboxing (Breach Fighter)

Sandboxing

État	Cette colonne affiche l'état (**Activé**/ **Désactivé**) de l'analyse sandboxing pour le type de fichier correspondant. Double-cliquez dessus pour changer l'état.

Type de fichiers	L'option sandboxing propose l'analyse de différents types de fichiers : • **Archive** : sont inclus les principaux types d'archives (zip, .tar, .rar, .gz, .gzip, .bz2, .7z, ...). • **Fichier HTML**. • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous Windows (.exe, .bat, .cmd , .scr, ...). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar"). • **Scripts** : PowerShell, Javascript, VBScript, Batch, Python. • **E-mail avec pièce jointe**. • **Image**. • **Autre**.
Taille max. d'un e-mail soumis à l'analyse sandboxing (Ko)	Ce champ permet de définir la taille maximale d'un e-mail devant être soumis à l'analyse sandboxing. Par défaut, cette valeur est égale à celle du champ **Taille max. pour l'analyse antivirale et sandboxing (Ko)** présent dans l'onglet *Analyse des fichiers*. Elle ne peut l'excéder.

Limites

- Taille maximale du fichier à analyser : 10 Mo.
- Nombre maximal de fichiers au sein d'un même mail ou d'une même archive : 10.
- Nombre maximal de niveaux d'imbrication au sein d'une même archive : 10.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. • En sélectionnant **Interdire**, le fichier analysé n'est pas transmis. • En sélectionnant **Autoriser**, le fichier est transmis dans son état.
Lorsque sandboxing ne peut analyser	Cette option définit le comportement de l'option sandboxing si l'analyse du fichier échoue : • Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. • Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

SMTP

Le protocole SMTP a pour objectif de détecter les connexions entre un client et un serveur e-mail ou entre deux serveurs e-mails utilisant le protocole SMTP. Il permet d'envoyer des e-mails. Il est utilisé par Stormshield Vulnerability Manager pour détecter la version du client et / ou du serveur e-mail afin de remonter d'éventuelles vulnérabilités.

Onglet IPS

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Extensions du protocole SMTP

Filtrer l'extension CHUNKING	Permet de filtrer les données transférées d'une adresse mail à une autre. **EXEMPLE** Les pièces jointes incluses dans un mail.
Filtrer les extensions spécifiques à Microsoft Exchange Server	Permet de filtrer les commandes additionnelles provenant du serveur de mails Microsoft Exchange Server.
Filtrer la demande modification de sens de connexion ATRN et ETRN	Permet de filtrer les données contenues dans la demande de modification de sens de connexion, du client vers le serveur, ou du serveur vers le client. Lors d'une communication SMTP, l'utilisation des commandes ATRN et ETRN permet d'échanger les rôles client/serveur.

Taille maximale des éléments (octets)

La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

En-tête du message	Nombre maximum de caractères que peut contenir l'en-tête d'un e-mail (adresse mail de l'expéditeur, date, type de codage utilisé etc.). Les valeurs autorisées sont comprises entre 64 et 4096.
Ligne de réponse serveur	Nombre maximum de caractères que peut contenir la ligne de réponse du serveur SMTP. Les valeurs autorisées sont comprises entre 64 et 4096.
Données Exchange (XEXCH50)	Taille maximale des données lors d'un transfert de fichier au format MBDEF (Message Database Encoding Format). Les valeurs autorisées sont comprises entre 102400 et 1073741824.
En-tête de l'extension BDAT	Taille maximale des données transmises via la commande BDAT. Les valeurs autorisées sont comprises entre 102400 et 10485760.
Ligne de commande	Taille maximale des données que peut contenir une ligne de commande (en dehors de la commande DATA). Les valeurs autorisées sont comprises entre 64 et 4096.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole SMTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.

Tracer chaque requête SMTP	Active ou désactive les logs permettant de tracer les requêtes SMTP.

Onglet Proxy

Filtrer la bannière d'accueil	Lorsque cette option est cochée, la bannière du serveur est anonymisée lors d'une connexion SMTP.

Commande HELO

Remplacer le nom de domaine du client par son adresse IP	Lors d'une identification basique, le client renseigne son nom de domaine en exécutant la commande HELO. En cochant cette case, le nom de domaine sera remplacé par l'adresse IP.

Filtrage du nom de domaine

Activer le filtrage du nom de domaine du serveur	Cette option permet de supprimer le nom de domaine que le serveur SMTP inclut dans sa réponse à une commande HELO. Ce filtrage est activé par défaut.

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Limites lors de l'envoi d'un e-mail

Par défaut, la limite de taille des données du message de mails sortants (text line) est activée. Elle est fixée à 1000 caractères maximum conformément à la norme RFC 2821.

Limiter la taille des lignes de message	Active une limite sur la longueur des lignes d'un message sortant.
Longueur maximale de ligne [1000-2048 (Ko)]	Ce champ indique la longueur maximale de la ligne lors de l'envoi d'un message. **REMARQUE** La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).
Nombre max. de destinataires	Indique le nombre maximum de destinataires que peut contenir un message. Les messages dont le nombre de destinataires est excessif seront refusés par le firewall (le refus sera marqué par un message d'erreur SMTP). Cela permet de limiter le spam d'e-mails.
Taille max. du message (Ko)	Indique la taille maximale que peut prendre un message passant par le firewall Stormshield Network. Les messages dont la taille est excessive seront refusés par le firewall. Les valeurs autorisées sont comprises entre 0 et 2147483647.

Onglet Commandes SMTP

Ce menu vous permet d'autoriser ou de rejeter les commandes SMTP définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Proxy

Onglet Commandes principales

Bouton **Tout sélectionner** : permet d'**Autoriser sans analyser**, d'**Interdire** ou d'analyser toutes les commandes (**Autoriser**).

Commande	Indication du nom de la commande.
Action	Indication de l'action effectuée.

Onglet Autres commandes autorisées

Commande	Par défaut, toutes les commandes non définies dans les RFC sont interdites. Cependant, certains systèmes de messagerie utilisent des commandes supplémentaires non standardisées. Vous pouvez donc ajouter ces commandes afin de les laisser passer au travers du firewall. Les boutons d'actions **Ajouter** et **Supprimer** permettent d'agir sur la liste de commandes.

IPS

Onglet Commandes SMTP autorisées

Liste des commandes SMTP supplémentaires autorisées. Il est possible d'en **Ajouter** ou d'en **Supprimer**.

Onglet Commandes SMTP interdites

Liste des commandes SMTP interdites. Il est possible d'en **Ajouter** ou d'en **Supprimer**.

Onglet Analyse des fichiers

Taille max. pour l'analyse antivirale et sandboxing (Ko)	Cette option correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. La taille par défaut dépend du modèle de firewall : • SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40, EVA1, EVA2 et EVA3 : 4000 Ko. • SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SNxr1200 et EVA4 : 8000 Ko. • SN1100, SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200 et EVAU : 16000 Ko.

AVERTISSEMENT
Lorsque vous définissez une taille limite de données analysées manuellement, veillez à

conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille totale, aucun autre fichier ne pourra être analysé en même temps.

Action sur les messages

Cette zone décrit le comportement de l'antivirus face à certains événements.

Lorsqu'un virus est détecté	Ce champ contient 2 options : **Autoriser** et **Interdire**. • En sélectionnant **Interdire**, le fichier analysé n'est pas transmis. • En sélectionnant **Autoriser**, l'antivirus transmet le fichier même s'il est détecté comme infecté.
Lorsque l'antivirus ne peut analyser	L'option **Autoriser sans analyser** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. • Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. • Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.
Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. **EXEMPLES** Si le disque dur est plein, le téléchargement des informations ne pourra pas être effectué. La taille maximale que le fichier peut atteindre pour l'analyse antivirale est restreinte (1000Ko).

Onglet Analyse sandboxing (Breach Fighter)

Sandboxing

État	Cette colonne affiche l'état (**Activé**/ **Désactivé**) de l'analyse sandboxing pour le type de fichier correspondant. Double-cliquez dessus pour changer l'état.
Type de fichiers	L'option sandboxing propose l'analyse de différents types de fichiers : • **Archive** : sont inclus les principaux types d'archives (zip, .tar, .rar, .gz, .gzip, .bz2, .7z, ...). • **Fichier HTML**. • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous Windows (.exe, .bat, .cmd , .scr, ...). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar"). • **Scripts** : PowerShell, Javascript, VBScript, Batch, Python. • **E-mail avec pièce jointe**. • **Image**. • **Autre**.

Taille max. d'un e-mail soumis à l'analyse sandboxing (Ko)	Ce champ permet de définir la taille maximale d'un e-mail devant être soumis à l'analyse sandboxing. Par défaut, cette valeur est égale à celle du champ **Taille max. pour l'analyse antivirale et sandboxing (Ko)** présent dans l'onglet *Analyse des fichiers*. Elle ne peut l'excéder.

Limites

- Taille maximale du fichier à analyser : 10 Mo.
- Nombre maximal de fichiers au sein d'un même mail ou d'une même archive : 10.
- Nombre maximal de niveaux d'imbrication au sein d'une même archive : 10.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options : • En sélectionnant **Interdire**, le fichier analysé n'est pas transmis. • En sélectionnant **Autoriser**, le fichier est transmis dans son état.
Lorsque sandboxing ne peut analyser	Cette option définit le comportement de l'option sandboxing si l'analyse du fichier échoue. • Si **Interdire** est spécifié, le fichier en cours d'analyse n'est pas transmis. • Si **Autoriser sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

SNMP (onglet IPS)

Versions autorisées

SNMPv1	En cochant cette case, les paquets correspondant à la version 1 du protocole SNMP sont autorisés par le firewall.
SNMPv2c	En cochant cette case, les paquets correspondant à la version 2c du protocole SNMP sont autorisés par le firewall.
SNMPv3	En cochant cette case, les paquets correspondant à la version 3 du protocole SNMP sont autorisés par le firewall.

Champs vides autorisés

Communauté	En cochant cette case, vous autorisez les requêtes SNMP présentant une communauté vide (SNMPv1 - SNMPv2c).
Identifiant	En cochant cette case, vous autorisez les requêtes SNMP présentant un identifiant vide (SNMPv3).

Gestion des commandes SNMP

Opérations SNMP

Cette liste recense les commandes SNMP autorisées par défaut par le firewall. L'action (*Autoriser / Interdire*) appliquée à chaque commande peut être modifiée en cliquant dans la colonne **Action**. Le bouton **Modifier toutes les commandes** permet de modifier l'action appliquée à l'ensemble des commandes.

Communautés

Onglet Liste noire

Cette grille permet de lister les communautés pour lesquelles les paquets SNMP seront systématiquement bloqués. Il est possible d'**Ajouter** ou de **Supprimer** des communautés en cliquant sur les boutons du même nom.

Onglet Liste blanche

Cette grille permet de lister les communautés pour lesquelles les paquets SNMP ne seront pas soumis aux traitements d'inspection de contenu. Il est possible d'**Ajouter** ou de **Supprimer** des communautés en cliquant sur les boutons du même nom.

Boutons → et ←

Ces boutons permettent de déplacer une communauté d'une grille à l'autre.

Identifiants

Onglet Liste noire

Cette grille permet de lister les identifiants pour lesquels les paquets SNMP seront systématiquement bloqués. Il est possible d'**Ajouter** ou de **Supprimer** des identifiants en cliquant sur les boutons du même nom.

Onglet Liste blanche

Cette grille permet de lister les identifiants pour lesquels les paquets SNMP ne seront pas soumis aux traitements d'inspection de contenu. Il est possible d'**Ajouter** ou de **Supprimer** des identifiants en cliquant sur les boutons du même nom.

Boutons → et ←

Ces boutons permettent de déplacer un identifiant d'une grille à l'autre.

OID

Onglet Liste noire

Cette grille permet de lister les OID (Objects Identifiers) pour lesquels les paquets SNMP seront systématiquement bloqués. Il est possible d'**Ajouter** ou de **Supprimer** des OID en cliquant sur les boutons du même nom.

Lorsqu'un OID est précisé dans cette grille, tous les OID qui en découlent sont également bloqués.

Exemple : ajouter l'OID 1.3.6.1.2.1 dans cette grille implique que les OID 1.3.6.1.2.1.1, 1.3.6.1.2.1.2, etc... seront également bloqués.

Onglet Liste blanche

Cette grille permet de lister les OID pour lesquels les paquets SNMP ne seront pas soumis aux traitements d'inspection de contenu. Il est possible d'**Ajouter** ou de **Supprimer** des OID en cliquant sur les boutons du même nom.

Lorsqu'un OID est précisé dans cette grille, tous les OID qui en découlent ne sont pas soumis aux traitements d'inspection de contenu.

Exemple : ajouter l'OID 1.3.6.1.2.1 dans cette grille implique que les OID 1.3.6.1.2.1.1, 1.3.6.1.2.1.2, etc... seront également en liste blanche.

Boutons → et ←

Ces boutons permettent de déplacer un OID d'une grille à l'autre.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole SNMP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête SNMP	Active ou désactive les logs permettant de tracer les requêtes SNMP.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

SSL

Le protocole SSL (Secure Sockets Layer), devenu Transport Layer Security (TLS) en 2001, est supporté en version 3 (1996). Les sites utilisant une version antérieure (présentant des défauts de sécurité) ou ne supportant pas un début de négociation en TLS seront bloqués.

La validation par un serveur ICAP des requêtes HTTPS déchiffrées par le proxy SSL n'est pas supportée.

Onglet IPS

Cet écran va permettre valider le fonctionnement du protocole SSL à travers le firewall.

Certaines options permettent de renforcer la sécurité de ce protocole. Par exemple, il est possible d'interdire des négociations d'algorithmes cryptographiques considérés comme faibles, de détecter des logiciels utilisant le SSL pour passer outre les politiques de filtrage (SKYPE, proxy HTTPS,...).

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

TLS v1.3

Autoriser le mécanisme 0-RTT	En cochant cette case, le moteur d'analyse IPS autorise les requêtes TLS utilisant le mécanisme 0-RTT (Zero Round Trip Time - Temps Aller Retour Zero) qui réduit le *Handshake* (poignée de mains) à zéro échange afin d'augmenter les performances pour les flux TLS. Le mécanisme 0-RTT permet au client d'envoyer des données applicatives dès le premier échange lorsque le client et le serveur partagent une clé pré-partagée, importée manuellement ou calculée lors d'un précédent *Handshake*.
Valeurs / Extensions inconnues	Sélectionnez dans la liste le type de valeurs ou extensions TLS à autoriser : • Valeurs / extensions RFC TLS 1.3, GREASE (Generate Random Extensions And Sustain Extensibility) ou inconnues, • Valeurs / extensions RFC TLS 1.3 et GREASE, • Valeurs / extensions RFC TLS 1.3 et inconnues (sauf GREASE), • Valeurs / extensions RFC TLS 1.3 uniquement.
Activer l'analyse de certificats serveur	Lorsque vous sélectionnez cette option, le moteur de prévention d'intrusion tente de récupérer le certificat serveur pour chaque flux TLS 1.3 traversant le firewall, afin d'analyser les éventuelles failles de sécurité liées à ce certificat. **NOTE** Afin d'optimiser les performances de l'analyse de certificats serveur, un mécanisme de cache permet ne pas déclencher la récupération d'un certificat lorsque celui-ci est déjà connu du moteur de prévention d'intrusion. Configurez ce mécanisme dans la Configuration globale du protocole SSL, onglet **IPS**.
Lorsque le type de certificat est incorrect	Sélectionnez l'action appliquée au flux TLS analysé lorsque le certificat serveur récupéré présente une anomalie : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : le certificat est rejeté, le firewall génère une alarme et bloque le flux TLS 1.3 concerné en fermant la connexion.
Lorsque le SNI est absent	Sélectionnez l'action appliquée au flux TLS analysé lorsque le certificat ne comporte pas de SNI (Server Name Indication) : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : le certificat est rejeté, le firewall génère une alarme et bloque le flux TLS 1.3 concerné en fermant la connexion.

Lorsque la CA n'est pas de confiance	Sélectionnez l'action appliquée au flux TLS lorsque la CA ayant signé le certificat serveur n'est pas définie dans la liste des CA de confiance : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : le certificat est rejeté, le firewall génère une alarme et bloque le flux TLS 1.3 concerné en fermant la connexion.
Lorsque le certificat est auto-signé	Ces certificats sont à usage interne et signés par votre serveur local. Ils permettent de garantir la sécurité de vos échanges, et, entre autres, d'authentifier les utilisateurs. Sélectionnez l'action à effectuer lorsque vous rencontrez des certificats auto-signés : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Lorsque la date de validité est incorrecte	Les certificats concernés par ce champ de configuration ont une date de validité antérieure ou postérieure à la date en cours et ne sont donc pas "valide". Sélectionnez l'action à effectuer lorsque vous rencontrez des certificats dont la date de validité n'est pas conforme : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Lorsque la vérification de la CRL échoue	Sélectionnez l'action à effectuer lorsque la vérification automatique de la CRL n'a pas pu aboutir : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Lorsque la CRL est invalide	Sélectionnez l'action à effectuer lorsque la CRL à vérifier est expirée : • **Continuer l'analyse** : le moteur de prévention d'intrusion poursuit l'analyse du certificat et les analyses protocolaires sur le flux TLS 1.3 concerné. • **Interdire le trafic** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Adresse utilisée pour la vérification des certificats	Sélectionnez l'objet représentant l'adresse IP du firewall à utiliser pour réaliser les requêtes de vérification des certificats. Si aucun objet n'est sélectionné, l'adresse IP de l'interface *Firewall_out* est utilisée.

Négociation SSL

Autoriser les chiffrements non supportés	Cochez cette case si l'algorithme de chiffrement que vous souhaitez utiliser n'est pas supporté par le protocole SSL.

Autoriser les données non chiffrées après une négociation SSL	Cette option permet de transmettre les données en clair après une négociation SSL. **AVERTISSEMENT** Laisser transiter les données en clair représente un risque de sécurité.
Autoriser les algorithmes cryptographiques de signalement (SCSV)	Les attaques par repli consistent à intercepter une communication et à imposer une variante cryptographique la plus faible possible. En activant cette option, le firewall annoncera un pseudo-algorithme cryptographique permettant de signaler une tentative d'attaque par repli (RFC 7507).
Niveaux de chiffrements autorisés	Plus l'algorithme de chiffrement utilisé est fort, et le mot de passe complexe, plus le niveau est considéré comme « haut ». **EXEMPLE** L'algorithme de chiffrement AES doté d'une force de 256 bits, associé à un mot de passe d'une dizaine de caractères fait de lettres, de chiffres et de caractères spéciaux. Trois choix sont proposés, vous pouvez autoriser les niveaux de chiffrement : • **Bas, moyen et haut** : par exemple, DES (force de 64 bits), CAST128 (128 bits) et AES. Quel que soit le niveau de sécurité du mot de passe, le niveau de chiffrement sera autorisé. • **Moyen et haut** : Seuls les algorithmes de moyenne et haute sécurité seront tolérées. • **Haut uniquement** : Seuls les algorithmes forts et les mots de passe dotés d'un haut niveau de sécurité seront tolérés.

Gestion des extensions SSL

Onglet Extensions nommées

Cette grille permet d'autoriser / interdire les extensions nommées du protocole TLS v1.3. Toutes les extensions nommées connues (cf. la liste des extensions TLS de l'IANA) sont listées par défaut : une ligne de la grille comprend ainsi l'identifiant (compris entre 0 et 56), le nom de l'extension et l'action qui lui est appliquée.

Il est possible :

- D'autoriser ou d'interdire unitairement une extension en cliquant sur son action associée,
- D'autoriser ou d'interdire une sélection d'extensions (touche Maj. enfoncée et sélection de lignes contiguës ou touche Ctrl. enfoncée et sélection de lignes non contiguës) et de leur appliquer une action commune à l'aide des boutons **Autoriser la sélection** et **Interdire la sélection**,
- De sélectionner toutes les extensions avec le bouton Tout sélectionner et de leur appliquer une action commune à l'aide des boutons **Autoriser la sélection** et **Interdire la sélection**.

Un champ de recherche permet également de filtrer l'affichage des extensions.

Onglet Plages d'extensions en liste noire

Cette grille est destinée à interdire les extensions connues du protocole TLS v1.3 autres que celles définies dans l'onglet **Extensions nommées**. L'identifiant de ces extensions doit être compris entre 57 et 65535).

Il est possible d'y ajouter (bouton **Ajouter**) ou d'en supprimer (bouton **Supprimer** après sélection de la ligne concernée) des extensions définies unitairement à l'aide de leur identifiant (exemple : 59) ou des plages d'extensions (exemples : 59-62, 92-1001).

Un champ de recherche permet également de filtrer l'affichage des identifiants placés en liste noire.

Détection des données non chiffrées (trafic en clair)

Méthode de détection	• **Ne pas détecter** : les données non chiffrées ne seront pas analysées. • **Inspecter tout le flux** : tous les paquets reçus seront analysés par le protocole SSL afin de détecter du trafic en clair • **Échantillonnage (7168 octets)** : Seuls les 7168 premiers octets du flux seront analysés afin de détecter du trafic en clair.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole SSL sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête SSL	Active ou désactive les logs permettant de tracer les requêtes SMTP.

Application-Layer Protocol Negotiation (ALPN)

Application-Layer Protocol Negotiation (ALPN) est une extension du protocole Transport Layer Security (TLS) permettant la négociation du protocole de la couche applicative lors de la poignée de mains TLS.

Onglet ALPN IANA

Cette grille permet d'autoriser / interdire les protocoles enregistrés auprès de l'IANA et inclus dans l'extension ALPN telle que décrite dans la RFC 7301.

Il est possible :

- D'autoriser ou d'interdire unitairement un protocole en cliquant sur son action associée,
- De sélectionner tous les protocoles avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Un champ de recherche permet également de filtrer l'affichage des protocoles.

Onglet ALPN A NE PAS ANALYSER

Cette grille permet de définir les protocoles de l'extension ALPN devant être exclus de l'analyse protocolaire SSL/TLS.

Il est possible :

- D'ajouter un protocole à exclure à l'aide du bouton **Ajouter**.
- De sélectionner tous les protocoles exclus et de les supprimer de la grille à l'aide des boutons **Tout sélectionner** puis **Supprimer**.

Un champ de recherche permet également de filtrer l'affichage des protocoles.

Onglet Proxy

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Inspection de contenu

Certificats auto-signés	Ces certificats sont à usage interne et signés par votre serveur local. Ils permettent de garantir la sécurité de vos échanges, et, entre autres, d'authentifier les utilisateurs. Cette option détermine l'action à effectuer lorsque vous rencontrez des certificats auto-signés : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Continuer l'analyse** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent et sont analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Certificats expirés	Les certificats expirés sont antérieurs ou postérieurs à la date en cours et ne sont donc pas « valides ». Pour y remédier, ils doivent être renouvelés par une autorité de certification. **AVERTISSEMENT** Les certificats expirés peuvent présenter un risque de sécurité. Après expiration d'un certificat, la CA l'ayant émis n'est plus responsable d'une utilisation malveillante de celui-ci. Cette option détermine l'action à effectuer lorsque vous rencontrez des certificats expirés : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Continuer l'analyse** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent et sont analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.

Certificats inconnus	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats inconnus : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Ne pas déchiffrer** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent transitent sans être analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Type de certificat incorrect	Ce test valide le type du certificat. Un certificat est considéré conforme s'il est utilisé dans le cadre défini par sa signature. Ainsi, un certificat utilisateur employé par un serveur est non conforme. Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats non conformes : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Continuer l'analyse** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent et sont analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Certificat avec FQDN incorrect	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats dont le format du nom de domaine (FQDN) est invalide : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Continuer l'analyse** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent et sont analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.
Lorsque le FQDN du certificat diffère du nom de domaine SSL	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats dont le nom de domaine (FQDN) est différent du nom de domaine SSL attendu : • **Déléguer à l'utilisateur** : cette action provoque une alerte de sécurité dans l'explorateur Web du client. Le client décide alors de poursuivre ou non la connexion vers le serveur concerné. Une alarme est générée et l'action du client est enregistrée dans le fichier de logs l_alarm. • **Continuer l'analyse** : ces certificats sont acceptés sans générer d'alerte de sécurité dans l'explorateur Web du client. Les flux transitent et sont analysés par le moteur de prévention d'intrusion. • **Interdire** : ces certificats sont refusés par le firewall et les flux correspondant sont bloqués.

Autoriser les adresses IP dans les noms de domaine SSL	Cette option permet d'autoriser ou non l'accès à un site par son adresse IP et non par son nom de domaine SSL.

Support

Si le déchiffrement échoue	Cette option va déterminer l'action à effectuer lorsque le déchiffrement échoue: vous pouvez choisir de **Interdire le trafic** ou de **Ne pas déchiffrer**. En choisissant cette deuxième possibilité, le trafic ne sera pas inspecté.
Lorsque le certificat n'a pas pu être classifié	Le choix est l'action **Autoriser sans déchiffrer** ou **Interdire sans déchiffrer**. Si un certificat n'est pas répertorié dans une catégorie de certificat, cette action détermine si le trafic est autorisé ou non.

Application-Layer Protocol Negotiation (ALPN)

Application-Layer Protocol Negotiation (ALPN) est une extension du protocole Transport Layer Security (TLS) permettant la négociation du protocole de la couche applicative lors de la poignée de mains TLS.

Onglet ALPN IANA

Cette grille permet d'autoriser / interdire les protocoles enregistrés auprès de l'IANA et inclus dans l'extension ALPN telle que décrite dans la RFC 7301.

Il est possible :

- D'autoriser ou d'interdire unitairement un protocole en cliquant sur son action associée,
- De sélectionner tous les protocoles avec le bouton **Tout sélectionner** et de leur appliquer une action commune à l'aide des boutons **Autoriser** ou **Interdire**.

Un champ de recherche permet également de filtrer l'affichage des protocoles.

Onglet ALPN A NE PAS ANALYSER

Cette grille permet de définir les protocoles de l'extension ALPN devant être exclus de l'analyse protocolaire SSL/TLS.

Il est possible :

- D'ajouter un protocole à exclure à l'aide du bouton **Ajouter**.
- De sélectionner tous les protocoles exclus et de les supprimer de la grille à l'aide des boutons **Tout sélectionner** puis **Supprimer**.

Un champ de recherche permet également de filtrer l'affichage des protocoles.

TFTP (onglet IPS)

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, cette option permet à un trafic correspondant détecté et autorisé par une règle de filtrage avec un niveau d'inspection IPS ou IDS et qui n'utilise pas le port par défaut d'être inspecté au niveau applicatif. Si cette option n'est pas sélectionnée, l'analyse protocolaire se limite à la couche transport (TCP/UDP).

Taille maximale des éléments (en octets)

Nom de fichier	Ce nombre doit être compris entre 64 et 512 octets.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'analyse du protocole TFTP sera désactivée et le trafic sera autorisé si la politique de filtrage le permet.
Tracer chaque requête TFTP	Active ou désactive permettant de tracer les requêtes TFTP.

L'analyse de l'option « utimeout » est ajoutée à celle du protocole TFTP.

Autres

Cette partie est dédiée au « reste » des protocoles que vous pouvez rencontrer et non cités ci-avant.

L'écran est divisé en cinq colonnes :

Nom du protocole	Le nom donné au protocole.
Port par défaut	Le nom du port affecté par défaut. Il est possible de créer un nouveau port en cliquant sur l'icône à droite de la colonne.
Port SSL par défaut	Nom du port attribué au protocole par défaut.
Détection automatique	Vous pouvez choisir d'activer ou non la détection automatique du protocole. Tous les protocoles étant activés par défaut, double-cliquez sur la colonne pour désactiver la détection automatique du protocole concerné.
État	Vous pouvez choisir d'activer ou non le protocole sélectionné. Les protocoles étant activés par défaut, double-cliquez dans la colonne pour désactiver le protocole concerné. Répétez l'opération lorsque vous souhaitez le réactiver.

Cliquez sur le bouton **Appliquer** pour conserver vos modifications.

PROXY CACHE DNS

Lorsque vous effectuez une requête DNS vers votre navigateur ou vers une adresse mail, le serveur DNS transforme le nom de domaine connu (par exemple *www.compagnie.com* ou *smtp.compagnie.com*) en adresse IP et vous la communique.

Le Proxy cache DNS permet de stocker dans la mémoire du firewall, la réponse et l'adresse IP communiquée par le serveur au préalable. Ainsi, dès qu'une requête similaire sera effectuée, le firewall répondra à la place du serveur plus rapidement, et fournira l'adresse IP souhaitée et conservée.

L'écran du **Proxy cache DNS** se compose d'un écran unique, divisé en deux parties :

- Un tableau listant les clients DNS autorisés à utiliser le cache.
- Un menu déroulant permettant de définir les paramètres de la configuration avancée.

Activer le cache de requête DNS

Cette option permet de faire fonctionner le **Proxy cache DNS** : lorsqu'une requête DNS est envoyée au firewall, celle-ci est traitée par le cache DNS.

Liste des clients DNS autorisés à utiliser le cache

Client DNS [machine, réseau, plage, groupe] :

Les clients renseignés au sein de la liste peuvent émettre des requêtes DNS au travers du firewall.

Ajouter	En cliquant sur ce bouton, une nouvelle ligne vient se positionner en tête du tableau. La flèche située à droite du champ présenté vide permet d'ajouter un client DNS. Vous pouvez le sélectionner dans la base d'objets qui s'affiche. Cela peut être une machine, un réseau, une plage d'adresse ou encore un groupe.
Supprimer	Sélectionnez d'abord le client DNS que vous souhaitez retirer de la liste. Une fenêtre de confirmation s'affiche avec le message suivant : « **Supprimer le client DNS sélectionné** ? ». Vous pouvez valider la suppression ou **Annuler** l'action.

NOTE
En mode transparent, les clients sélectionnés bénéficieront du Proxy cache DNS, les autres demandes seront soumis au filtrage.

Configuration avancée

Taille du cache (octets) :

La taille maximale allouée au cache DNS dépend du modèle de votre firewall.

Mode transparent (intercepte toutes les requêtes DNS émise par les clients autorisées)	Comme son nom l'indique cette option vise à rendre transparent le service DNS du firewall Stormshield Network. Ainsi lorsque cette option est activée la redirection des flux DNS vers le cache DNS est invisible aux utilisateurs qui pensent accéder à leur serveur DNS. En mode transparent, toutes les requêtes sont interceptées, même si celles-ci sont à destination d'autres serveurs DNS que le firewall. Les réponses sont gardées un certain temps en mémoire pour éviter de retransmettre des demandes déjà connues.
Interrogation aléatoire des serveurs DNS	En cochant cette option, le firewall va sélectionner au hasard le serveur DNS dans la liste. (voir menu **Système**/module **Configuration**/onglet *Paramètres Réseaux*/panneau **Résolution DNS**).

QUALITE DE SERVICE (QoS)

Le paramétrage de la QoS ayant évolué avec la version SNS 4.3.0, la mise à jour en version SNS 4.3.0 (ou supérieure) d'une configuration utilisant de la QoS entraîne l'affichage d'un message d'avertissement indiquant que "La configuration de la QoS doit être complétée".

IMPORTANT

Cette fonctionnalité est en accès anticipé dans SNS 4.8

Veuillez impérativement consulter les Problèmes connus et les Limitations et précisions sur les cas d'utilisation des Notes de version SNS 4.8 avant d'activer cette fonctionnalité ou de mettre à jour une configuration QoS existante vers une version SNS 4.8

Si vous avez mis à jour en version SNS 4.8 une configuration QoS existante, notez que cette configuration n'est pas automatiquement validée.
La configuration après mise à jour nécessite en effet le paramétrage des *Traffic shapers* pour pouvoir être activée.

Le paramétrage de la QoS est réalisé au travers de deux onglets :

- L'onglet **Files d'attente** : définition des *Traffic shapers* et des files d'attente,
- L'onglet **Traffic shapers** : affectation de *Traffic shapers* et de files d'attente aux interfaces réseau concernées par la QoS.

L'onglet Files d'attente

Files d'attente

Le module de QoS, intégré au moteur de prévention d'intrusion Stormshield Network est associé au module Filtrage pour offrir les fonctionnalités de Qualité de Service.

Dès sa réception, le paquet est traité par une règle de filtrage puis le moteur de prévention d'intrusion l'affecte à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage.

Il existe trois types de file d'attente sur le firewall. Deux sont directement associés aux algorithmes de QoS : PRIQ (Priority Queuing) et CBQ (Class-Based Queuing). Le troisième type permet le monitoring du trafic.

File d'attente par classe d'application ou d'affectation (CBQ)

Il est possible de choisir une classe d'ordonnancement pour chacune des règles de filtrage et de lui associer une garantie de bande passante ainsi qu'une limite.

Par exemple : vous pouvez associer une classe d'ordonnancement aux flux HTTP en associant une queue CBQ à la règle de filtrage correspondante.

Les files d'attente par classe d'application ou d'affectation induisent la façon dont les trafics affectés par ces règles de QoS seront gérés sur le réseau. Les mécanismes de réservation et de limitation de la bande passante de ce type de files d'attente permettent dans le premier cas, la garantie d'un service minimum et dans le deuxième cas, la préservation de la bande passante vis-à-vis d'applications coûteuses en ressources.

Ajout d'une file d'attente par classe d'application ou d'affectation

Pour ajouter une file d'attente par classe d'application ou d'affectation :

1. Cliquez sur le bouton **Ajouter.**
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ).**
   Une fenêtre s'affiche pour configurer les différentes propriétés de la file d'attente : Nom, Type, Commentaire éventuel, Contraintes de bande passante.

Le détail des propriétés d'une file d'attente de type **Réservation ou limitation de bande passante (CBQ)** est décrit ci-dessous.

Modification d'une file d'attente par classe d'application ou d'affectation

Nom	Nom de la file d'attente à configurer.
Type	Pour une file d'attente de type réservation / limitation de bande passante, il est indiqué **Réservation / limitation de bande passante (CBQ)**.
Commentaire	Commentaire associé (facultatif).

Contraintes de bande passante

Bp garantie	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s, Mbit/S, Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s. **REMARQUE** Par défaut, cette option est synchronisée avec l'option **Bp inv. garantie**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Bp inv. garantie**. En modifiant la valeur de **Bp inv. garantie**, les valeurs sont différentes et donc désynchronisées.
Bp max	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, Mbits/s, Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 500Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 500Kbits/s. **REMARQUE** Par défaut, cette option est synchronisée avec l'option **Bp inv. max**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Bp inv. max**. En modifiant la valeur de **Bp inv. max**, les valeurs sont différentes et donc désynchronisées.

Bp inv. garantie	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert descendant. Configurée en Kbits/s, Mbits/s, Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s. **REMARQUE** Si vous saisissez une valeur supérieure à **Bp inv. max**, dans ce cas le message suivant s'affiche : « trafic descendant : La bande passante minimale garantie doit être inférieure ou égale à la bande passante maximale ».
Bp inv. max	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic descendant affecté par ces files d'attente. Configurée en Kbits/s, Mbits/s, Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 500Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 500Kbits/s.

REMARQUE
Lorsque vous sélectionnez **Aucun** dans la colonne **Bp garantie** et **Illimité** dans la colonne **Bp max**, aucune contrainte n'est imposée sur le trafic. Dans ce cas, un message s'affiche dans lequel l'application vous propose de transformer votre file d'attente en une file de surveillance.

La grille du menu **Files d'attente** affiche les différentes files d'attente qui ont été configurées. Un clic sur le bouton **Vérifier l'utilisation** permet d'afficher la liste des règles de filtrage dans lesquelles la file d'attente sélectionnée est utilisée.

Suppression d'une file d'attente par classe d'application ou d'affectation

Sélectionnez la ligne de file d'attente à supprimer puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

Surveillance du trafic (monitoring)

Les files d'attente de monitoring n'affectent pas la manière dont sont traités les trafics qui sont associés à ces règles de QoS.

Elles permettent l'enregistrement d'informations de débit et de bande passante qui peuvent être visualisées dans le module **Supervision de la QoS** (après avoir été sélectionnées dans l'onglet **Configuration de la QoS** du module **Configuration de la supervision**).

Les différentes options de la configuration d'une file d'attente du type Monitoring sont présentées ci-dessous :

Ajout d'une surveillance du trafic

Pour ajouter une surveillance du trafic :

1. Cliquez sur le bouton **Ajouter.**
2. Sélectionnez **Surveillance du trafic (MONQ)**.
   Une fenêtre s'affiche pour configurer les différentes propriétés de la file d'attente : Nom, Type, Commentaire éventuel.

Le détail des propriétés d'une file d'attente de type **Surveillance du trafic (MONQ)** est décrit ci-dessous.

Modification d'une surveillance du trafic

Nom	Nom de la file d'attente à configurer.
Type	Pour une file d'attente de type surveillance du trafic, il est indiqué **Surveillance du trafic (MONQ)**.
Commentaire	Commentaire associé (facultatif).

Suppression d'une surveillance du trafic

Sélectionnez la ligne concernée dans la grille de surveillance de trafic puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

File d'attente par priorité

Il existe 7 niveaux de priorité. Les paquets seront traités en fonction des priorités paramétrées.

Il est possible d'associer une priorité élevée aux requêtes DNS en créant une règle de filtrage et en lui associant une queue PRIQ.

Les files d'attente par priorité induisent une priorisation des paquets dans leur traitement. Les paquets qui sont associés à une règle de filtrage avec une file d'attente du type **PRIQ** sont traités avant les autres.

Les priorités s'échelonnent entre 0 et 7. La priorité 0 correspond aux trafics les plus prioritaires parmi les files d'attente **PRIQ**. La priorité 7 correspond aux trafics les moins prioritaires parmi les files d'attente **PRIQ**.

Les flux sans règles de QoS seront traités avant toutes files d'attente du type **PRIQ** ou **CBQ**

Les différentes options de la configuration d'une file d'attente du type PRIQ sont présentées ci-dessous.

Ajout d'une file d'attente par priorité

Pour ajouter une file d'attente par priorité :

1. Cliquez sur le bouton **Ajouter**.
2. Sélectionnez **Traitement par priorité (PRIQ).**
   Une fenêtre s'affiche pour configurer les différentes propriétés de la file d'attente : Nom, Type, Priorité, Commentaire éventuel.

Le détail des propriétés d'une file d'attente de type **Traitement par priorité (PRIQ)** est décrit ci-dessous.

Modification d'une file d'attente par priorité

La grille affiche les différentes files d'attente qui ont été configurées. Il est possible de vérifier si ces règles sont utilisées dans une règle de filtrage en cliquant sur le bouton **Vérifier l'utilisation**. Dans ce cas, un menu apparaît dans la barre de navigation en affichant les règles.

Nom	Nom de la file d'attente à configurer.
Type	Pour une file d'attente de type traitement par priorité, il est indiqué **Traitement par priorité PRIQ**.

Priorité	Permet de choisir le niveau de priorité du trafic affecté à la queue. Les cellules de cette colonne ne sont éditables que pour les queues de type PRIQ. Il est possible de sélectionner une valeur allant de 7 (priorité la plus basse) à 0 (priorité la plus haute).
Commentaire	Commentaire associé (facultatif).

Suppression d'une file d'attente par priorité

Sélectionnez la ligne concernée dans la grille de file d'attente par priorité puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

Files d'attente disponibles

A la fin de la grille des files d'attente est indiqué le nombre de files d'attentes disponibles pour un modèle de firewall donné. Ces valeurs sont les suivantes :

SN160(W), SN210(W), SN310	EVA1, EVA2, EVA3, EVA4, EVAU (16G) SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 SN510, SN-M-Series-520 SN710, SN-M-Series-720 SN910, SN-M-Series-920 SN1100, SNxr1200 SNi10 SNi20 SNi40	EVAU (32G), EVAU (64G) SN2100, SN-L-Series-2200, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6100, SN-XL-Series-6200
20	100	255

L'onglet Traffic shapers

Traffic shaper

Cette grille liste les *Traffic shapers* qui pourront être affectés aux interfaces réseau faisant l'objet de QoS.

DEFINITION
Le *Traffic shaping* (régulation de flux) est le contrôle du volume des échanges sur un réseau informatique dans le but d'optimiser ou de garantir les performances, une latence plus faible ou d'augmenter la bande passante utilisable en retardant les paquets qui correspondent à certains critères. Plus particulièrement, le *Traffic shaping* désigne toute action sur un flux réseau qui impose un délai supplémentaire à ces paquets pour qu'ils se conforment à une contrainte prédéterminée (contractuelle ou liée à un certain type de trafic).

Les actions

Il est possible d'**Ajouter** ou de **Supprimer** des *Traffic shapers*. Si vous souhaitez supprimer un *Traffic shaper* utilisé par une interface réseau, un message d'avertissement vous invite à modifier la configuration de la QoS avant de le supprimer.

Il est également possible de filtrer l'affichage des *Traffic shapers* selon une chaîne de caractères saisie dans le champ de filtrage.

La grille

Nom	Nom donné au *Traffic shaper*.
Bande passante sortante	Indiquez la bande passante sortante maximale réservée au *Traffic shaper*. Lors de la définition d'un *Trafic shaper* destiné à l'interface en lien avec le routeur d'accès Internet, il est conseillé de positionner cette valeur à 95% de la bande passante maximale du lien Internet.
Unité	Sélectionnez l'unité de bande passante sortante affectée au *Traffic shaper* : • Kbit/s, • Mbit/s, • Gbit/s.
Bande passante entrante	Indiquez la bande passante entrante maximale réservée au *Traffic shaper*. Lors de la définition d'un *Trafic shaper* destiné à l'interface en lien avec le routeur d'accès Internet, il est conseillé de positionner cette valeur à 95% de la bande passante maximale du lien Internet.
Unité	Sélectionnez l'unité de bande passante entrante affectée au *Traffic shaper* : • Kbit/s, • Mbit/s, • Gbit/s.

Interfaces avec QoS

Cette grille permet de définir les interfaces concernées par la QoS, ainsi que le *Traffic shaper*, la file d'attente ou la file d'attente d'acquittement (ACK - pour les flux TCP) à utiliser pour chacune de ces interfaces.

Les actions

Il est possible d'**Ajouter** ou de **Supprimer** des associations Interface / *Traffic shaper* / File d'attente / File d'attente de d'acquittement (ACK).

La grille

Interface	Sélectionnez l'interface à laquelle vous souhaitez affecter de la QoS.
Traffic shaper	Sélectionnez l'un des *Traffic shapers* définis sur le firewall.
File d'attente par défaut	Sélectionnez l'une des files d'attente définies sur le firewall. Si vous ne souhaitez pas affecter de file d'attente particulière, sélectionnez *Bypass*.
File d'attente d'acquittement (ACK) par défaut	Sélectionnez l'une des files d'attente définies sur le firewall. Si vous ne souhaitez pas affecter de file d'attente d'acquittement (ACK) particulière, sélectionnez *Bypass*.

RAPPORTS

Le module **Rapports** propose des rapports statiques qui se basent sur les traces enregistrées sur le firewall. Ils sont répartis en plusieurs catégories : Web, Sécurité, Virus, Spam, Vulnérabilité, Réseau, Réseau industriel, Sandboxing, SD-WAN et Services Web.

La plupart des rapports présentent des "Top 10" des valeurs les plus récurrentes (Top des sites Web les plus bloqués par exemple), le reste des valeurs étant regroupé dans une valeur "Autres". Les rapports SD-WAN se basent sur les métriques et les états opérationnels obtenus lors de la supervision des routeurs et de leurs passerelles.

NOTE
Les rapports de chaque catégorie s'affichent uniquement s'ils sont activés dans le module **Configuration > Traces - Syslog - IPFIX >** Configuration des rapports). Si aucun rapport n'est activé dans la configuration, le module **Rapports** est alors non visible.

Données personnelles

Par souci de conformité avec le règlement européen RGPD (Règlement Général sur la Protection des Données), les données sensibles (nom d'utilisateur, adresse IP source, nom de la source, adresse MAC source) ne sont pas affichées dans les logs et rapports et sont remplacées par la mention "Anonymized".

Pour visualiser ces données sensibles, l'administrateur doit alors activer le droit "Logs : accès complet (données personnelles)" en cliquant sur **Logs : accès restreint** dans le bandeau supérieur de l'interface Web d'administration, puis en saisissant un code d'autorisation obtenu auprès de son superviseur (voir la section **Administrateurs** > **Gestion des tickets**). Ce code possède une durée de validité limitée définie lors de sa création.

Pour relâcher ce droit, l'administrateur doit ensuite cliquer sur la mention **Logs : accès complet (données personnelles)** présente dans le bandeau supérieur de l'interface Web d'administration puis cliquer sur le bouton **Libérer** de la boite de dialogue affichée.

Après avoir obtenu ou relâché ce droit, il est nécessaire de rafraîchir les données affichées.

Notez que chaque action d'obtention ou de libération du droit "Logs : accès complet (données personnelles)" génère une entrée dans les logs.

NOTE
Pour les modèles SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 et SNi20, vous pouvez bénéficier de l'ensemble de la fonctionnalité en utilisant un support de stockage externe de type :

- Carte SD pour les modèles SN160(W), SN210(W), SN310 et SNi20,
- Carte microSD pour les modèles SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 et SNi10.

Les caractéristiques que doivent respecter ces supports sont précisées dans la partie LOGS - JOURNAUX D'AUDIT de ce guide.

Sécurité collaborative

Pour une sécurité plus collaborative, à partir des rapports de vulnérabilités remontés par Vulnerability Manager, il est maintenant possible d'augmenter le niveau de protection d'une machine identifiée comme vulnérable en un clic. Ainsi, en cas de détection de vulnérabilités critiques, une nouvelle interaction vous permet d'ajouter les machines concernées à un groupe préalablement établi et se voir attribuer un profil de protection renforcée ou des règles de filtrage spécifiques (zones de mise en quarantaine, accès limité, etc.).

Pour plus d'informations, reportez-vous à la Note Technique **Sécurité collaborative**.

Les actions possibles sur les rapports

Échelle de temps	Modifie l'échelle de temps du rapport. Plusieurs choix sont possibles : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. À noter que : • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit.
Rafraîchir les données	Actualise les données affichées.
Afficher le	Ce champ est accessible seulement si l'échelle de temps sélectionnée est **Vue par jour**. Choisissez alors dans le calendrier la date souhaitée.
Imprimer le rapport	Ouvre la fenêtre d'aperçu pour l'impression du rapport. Un champ commentaire peut être ajouté au rapport mis en page pour l'impression. Le bouton **Imprimer** envoie le fichier au module d'impression du navigateur qui permet de choisir entre l'impression ou la génération d'un fichier PDF.
Télécharger les données au format CSV	Permet de télécharger les données au format CSV.
Vue par histogramme horizontal	Affiche les données sous forme d'histogramme horizontal.
Vue par histogramme vertical	Affiche les données sous forme d'histogramme vertical.
Vue par diagramme circulaire	Affiche les données sous forme de diagramme circulaire.
Afficher / Masquer la légende	Affiche ou masque la légende du rapport. La légende se compose : • D'une couleur pour chaque valeur du rapport, • Une numérotation précisant le classement des valeurs du rapport, • Le nom des valeurs, • La quantité des valeurs, • Le pourcentage que la valeur représente dans ce rapport. Selon les rapports, des informations ou des interactions supplémentaires peuvent être ajoutées à la légende (exemple : action d'une alarme).

Un clic gauche sur une valeur présentée dans un rapport affiche un menu proposant plusieurs interactions. Celles-ci peuvent par exemple donner des informations supplémentaires sur la valeur, modifier un paramètre du profil de configuration ou encore lancer une recherche dans les traces du firewall. Certaines interactions sont accessibles seulement sur certaines valeurs de certains rapports.

Les rapports disponibles

Rapports Web

L'activité analysée dans la catégorie Web concerne la totalité des sites interrogés, soit ceux appartenant aux réseaux internes de l'entreprise ou ceux hébergés sur internet. Ces rapports concernent les trafics effectués avec les protocoles HTTP et HTTPS.

Pour les rapports relatifs aux *Sites*, les interactions avec les éléments et la légende sont l'interrogation de la catégorie d'une URL ainsi que l'accès direct à l'URL. Le *Top des recherches Web* permet quant à lui, de relancer la recherche via le moteur Google.

Sites Web visités	Top des sites Web les plus visités. Ces valeurs sont évaluées par le nombre de requêtes (hits) effectués au serveur HTTP, pour le téléchargement des fichiers nécessaires à l'affichage des pages web.
Domaines Web visités	Top des domaines Web les plus visités. Par un mécanisme d'agrégation du nombre de *Sites Web* interrogés, le rapport précédent est établi en fonction des *Domaines Web*, ce qui permet d'éviter leur fractionnement.
Catégories Web consultées	Top des catégories Web les plus consultées. Pour ce rapport, l'activation du module **Filtrage URL** est requise. Pour rappel, les sites interrogés comprennent ceux appartenant au réseau interne (catégorie *Private IP Addresses*).
Sites Web par volume	Top des sites Web par volume échangé. Ce rapport se base sur les volumes de données échangées, en émission comme en réception.
Domaines Web par volume	Top des domaines Web par volume échangé. Par un mécanisme d'agrégation du nombre de *Sites Web* interrogés, le rapport précédent est établi en fonction des *Domaines Web*, ce qui permet d'éviter leur fractionnement.
Catégories Web par volume	Top des catégories Web par volume échangé. Le trafic est analysé sur les règles avec un **Filtrage URL** appliqué (*Inspection de sécurité*). Il concerne les volumes de données échangées, en émission comme en réception.
Utilisateurs par volume	Top des utilisateurs par volume échangé. L'Authentification doit être configurée (voir la section Authentification de ce Guide). Il concerne les volumes de données échangées, en émission comme en réception. Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Sites Web bloqués	Top des sites Web les plus bloqués. Ce rapport est relatif aux sites bloqués par le moteur ASQ ou par le **Filtrage URL** s'il est activé (*Inspection de sécurité*).

Domaines Web bloqués	Top des domaines Web les plus bloqués. Par un mécanisme d'agrégation du nombre de *Sites Web* interrogés, le rapport précédent est établi en fonction des *Domaines Web*, ce qui permet d'éviter leur fractionnement.
Catégories Web bloquées	Top des catégories Web les plus bloquées. L'inspection **Filtrage URL** est requise pour obtenir les catégories. Ce rapport est relatif aux sites bloqués par le moteur ASQ ou par le **Filtrage URL** s'il est activé (*Inspection de sécurité*).
Recherches Web	Top des recherches Web. Les valeurs concernent les requêtes effectuées sur les moteurs de recherche sur Google, Bing et Yahoo. Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.

Rapports Sécurité

Les rapports *Alarmes* se basent sur les alarmes du module **Configuration > Protection applicative > Applications et protections** et les événements système du module **Configuration > Notifications > Evénements système**).

Pour les rapports relatifs aux alarmes, vous pouvez modifier l'action, changer le niveau d'alerte et accéder à l'aide de l'alarme sélectionnée. Ces modifications sont effectuées sur le profil concerné par le flux ayant généré l'alarme.

Alarmes	Top des alarmes les plus fréquentes. Ce rapport affiche les alarmes les plus fréquentes levées lors de l'analyse du trafic par le firewall.
Alarmes par machine	Top des machines à l'origine des alarmes. Les machines générant le plus d'alarmes sont identifiées par le nom DNS (fqdn) ou à défaut l'adresse IP. Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Sessions Administrateur	Ce rapport recense les plus grands nombres de sessions à l'interface d'administration du Firewall - quel que soit les droits. Ce nombre de sessions est comptabilisé par rapport à l'identifiant du compte *Administrateur* et par rapport à l'adresse IP de la machine s'étant connectée. Ainsi une même adresse IP pourrait être citée plusieurs fois si différents comptes ont été utilisés pour se connecter au firewall depuis une même machine.
Alarmes par pays	Top des pays générant des alarmes. Ce rapport présente les pays générant le plus d'alarmes, qu'ils soient en source ou en destination du trafic réseau.
Réputation des machines	Top des machines présentant les scores de réputation les plus élevés. Ce rapport présente les machines du réseau interne présentant les scores de réputation les plus élevés, qu'elles soient en source ou en destination du trafic réseau. Ce rapport nécessite que la gestion de réputation des machines soit activée. Il contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Taux de détection par moteur d'analyse (Sandboxing, Antivirus, AntiSpam)	Ce rapport présente la répartition des analyses réalisées sur les fichiers entre l'analyse sandboxing, l'antivirus et l'antispam.

Rapports Virus

L'inspection **Antivirus** est requise pour ces analyses.

Virus Web	Top des virus Web. Ce rapport liste les virus détectés sur le trafic web (protocoles HTTP et HTTPS si l'inspection SSL est activée). Une interaction sur le graphique permet de pointer sur une description du virus en ligne (securelist.com).
Virus par e-mails	Top des virus par e-mails. Ce rapport liste les virus détectés sur le trafic mail (protocoles POP3, SMTP et POP3S, SMTPS si l'inspection SSL est activée). Une interaction sur le graphique permet de pointer sur une description technique du virus en ligne (securelist.com).
Émetteurs de virus par e-mail	Top des émetteurs de virus par e-mail. Les virus par e-mail détectés sur le trafic mail des réseaux internes (protocoles SMTP et SMTPS si l'inspection SSL est activée) sont listés par émetteurs. Les expéditeurs sont identifiés selon leur identifiant d'utilisateur authentifiés. L'Authentification doit donc être configurée (voir la section **Authentification** de ce Guide). Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.

Rapports Spam

Le module **Antispam** doit être activé. Ces données sont comptabilisées par destinataire de spam reçus, en analysant le trafic SMTP, POP3 et SMTPS, POP3S si l'analyse SSL est activée.

Utilisateurs spammés	Top des utilisateurs les plus spammés. Ce rapport comptabilise les spams quel que soit le seuil de confiance (niveau 1-Bas, 2-Moyen et 3-Haut) L'utilisateur est identifié par l'identifiant de son adresse électronique (sans le caractère @ et le nom du domaine). Il contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Taux de spam	Taux de spam dans les e-mails reçus. Ce rapport est un ratio. Sur la totalité d'e-mails reçus et analysés par le module **Antispam**, trois pourcentages sont remontés. La proportion de spams quel que soit le seuil de confiance (niveau 1-Bas, 2-Moyen et 3-Haut), celle des e-mails scannés mais avec échec de l'analyse et enfin, la part des mails n'étant pas considérés comme spams.

Rapports Vulnérabilité

Vous pouvez lister des vulnérabilités par machine. Le module **Management des vulnérabilités** doit être activé.

Par défaut, ces rapports concernent les vulnérabilités détectées sur les réseaux internes, car par défaut, l'objet *network_internals* est défini dans la liste des éléments réseaux sous surveillance. L'analyse porte donc sur les machines appartenant aux réseaux internes, identifiées par le nom DNS (fqdn) ou à défaut l'adresse IP. À noter qu'une vulnérabilité remontée à un instant donné peut avoir été résolue au moment de la consultation du rapport.

Pour plus d'informations sur les profils et les familles de vulnérabilités, reportez-vous sur la section Management des vulnérabilités.

Machines vulnérables	Top des machines les plus vulnérables. Ce rapport remonte la liste des machines les plus vulnérables du réseau par rapport au nombre de vulnérabilités détectées sans tenir compte de leur gravité. Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Vulnérabilités Client	Top des vulnérabilités Client. Ce rapport remonte toutes les vulnérabilités détectées avec une cible *Client,* qui ont un degré de sévérité « 3 » (Elevé) ou « 4 » (Critique). Celles-ci incluent les vulnérabilités qui ont à la fois des cibles *Client* et *Serveur*.
Vulnérabilités Serveur	Top des vulnérabilités Serveur. Ce rapport remonte toutes les vulnérabilités détectées avec une cible *Serveur,* qui ont un degré de sévérité « 2 » (Moyen), « 3 » (Élevé) ou « 4 » (Critique). Celles-ci incluent les vulnérabilités qui ont à la fois des cibles *Client* et *Serveur*.
Applications vulnérables	Top des applications les plus vulnérables. Ce rapport affiche le top de 10 des vulnérabilités les plus détectées sur le réseau, par produit quelle que soit la gravité.

Rapports Réseau

L'activité analysée dans la catégorie Réseau concerne la totalité des flux transitant par le firewall, soit la totalité des protocoles. Les volumes sont calculés sur les données échangées en émission et en réception.

Machines par volume	Top des machines par volume échangé. Ce volume de données concerne toutes les machines, qu'elles appartiennent aux réseaux internes ou externes. Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Protocoles par volume	Top des protocoles par volume échangé. Ce rapport présente les protocoles les plus utilisés sur la totalité des volumes échangés par toutes les machines, qu'elles appartiennent aux réseaux internes ou externes.
Utilisateurs par volume	Top des utilisateurs par volume échangé. Le volume de données concerne les utilisateurs authentifiés. L'Authentification doit être configurée (voir la section **Authentification** de ce Guide). Ce rapport contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Protocoles par connexion	Top des protocoles les plus utilisés par connexion. Les protocoles concernent uniquement les protocoles de la couche Application du modèle OSI. Ce rapport présente les protocoles les plus utilisés sur la totalité des connexions pendant la période donnée.
Pays sources	Top des pays identifiés comme source du trafic réseau. Ce rapport présente les pays les plus fréquemment identifiés comme étant à la source du trafic réseau traversant le firewall.
Pays destinations	Top des pays identifiés comme destination du trafic réseau. Ce rapport présente les pays les plus fréquemment identifiés comme étant destinataires du trafic réseau traversant le firewall.

Applications clientes détectées	Top des applications clientes détectées. Ce rapport présente les applications les plus détectées côté client par le moteur de prévention d'intrusion pendant la période donnée.
Applications serveur détectées	Top des applications serveur détectées. Ce rapport présente les applications les plus détectées côté serveur par le moteur de prévention d'intrusion pendant la période donnée.
Applications clientes par volume échangé	Top des applications clientes par volume échangé. Ce rapport présente les applications clientes les plus utilisés sur la totalité des volumes échangés par toutes les machines pendant la période donnée.
Applications serveur par volume échangé	Top des applications serveur par volume échangé. Ce rapport présente les applications serveur les plus utilisés sur la totalité des volumes échangés par toutes les machines pendant la période donnée.

Rapports Réseau industriel

L'activité analysée dans la catégorie Réseau industriel concerne la totalité des flux de type protocoles industriels transitant par le firewall. Les volumes sont calculés sur les données échangées en émission et en réception.

Serveurs MODBUS par volume	Top des serveurs Modbus par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel MODBUS.
Serveurs UMAS par volume	Top des serveurs UMAS par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel UMAS.
Serveurs S7 par volume	Top des serveurs S7 par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel S7.
Serveurs OPC UA par volume	Top des serveurs OPC UA par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel OPC UA.
Serveurs EtherNet/IP par volume	Top des serveurs Ethernet/IP par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel Ethernet/IP.
Serveurs IEC 60870-5-104 par volume	Top des serveurs IEC 60870-5-104 par volume échangé. Ce rapport présente les serveurs les plus utilisés sur la totalité des volumes échangés pour le protocole industriel IEC 60870-5-104.

Rapports Analyse Sandboxing

L'option **Sandboxing** doit être activée. Les données sont comptabilisées en analysant le trafic HTTP, SMTP, POP3, FTP et HTTPS, SMTPS, POP3S si l'analyse SSL est activée.

Fichiers malveillants détectés	Top des fichiers malveillants détectés suite à l'analyse sandboxing. Ce rapport présente les fichiers malveillants les plus souvent détectés par l'analyse sandboxing.

Fichiers malveillants bloqués	Top des fichiers malveillants détectés et bloqués par une requête sandboxing. Ce rapport présente les fichiers malveillants les plus souvent bloqués par l'analyse sandboxing.
Types de fichiers les plus fréquemment analysés	Top des types de fichiers les plus fréquemment analysés. Ce rapport présente les types de fichiers les plus souvent envoyés pour une analyse sandboxing.
Machines ayant soumis le plus de fichiers à l'analyse Sandboxing	Top des machines ayant soumis des fichiers à l'analyse Sandboxing. Ce rapport présente les machines du réseau ayant provoqué le plus d'analyses sandboxing. Il contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.
Protocoles ayant le plus recours à l'analyse Sandboxing	Top des protocoles ayant recours à l'analyse Sandboxing. Ce rapport présente les protocoles réseau (HTTP, SSL, SMTP, FTP) ayant provoqué le plus d'analyses sandboxing.
Utilisateurs ayant soumis le plus de fichiers à l'analyse Sandboxing	Top des utilisateurs ayant soumis des fichiers à l'analyse Sandboxing. Ce rapport présente les utilisateurs ayant provoqué le plus d'analyses sandboxing. Il contient des données personnelles et nécessite donc l'obtention du droit **Logs : accès complet (données personnelles)** pour être visualisé.

Rapports SD-WAN

L'activité analysée dans la catégorie SD-WAN concerne les métriques et les états opérationnels obtenus lors de la supervision des routeurs et de leurs passerelles, qu'ils soient utilisés ou non dans la configuration du firewall (objets routeurs, passerelle par défaut, routeurs configurés dans des règles de filtrage, routes de retour).

Latence	Routeurs et passerelles présentant la latence la plus élevée. Ce rapport présente les passerelles des objets routeurs présentant la latence (en ms) la plus élevée. Les routeurs et les passerelles inaccessibles n'apparaissent pas dans ce rapport.
Gigue	Routeurs et passerelles présentant la gigue la plus élevée. Ce rapport présente les passerelles des objets routeurs présentant la gigue (en ms) la plus élevée. Les routeurs et les passerelles inaccessibles n'apparaissent pas dans ce rapport.
Perte de paquets	Routeurs et passerelles présentant le taux de perte de paquets le plus élevé. Ce rapport présente les passerelles des objets routeurs présentant le taux de perte de paquets le plus élevé.
Indisponibilité	Routeurs et passerelles présentant le taux d'indisponibilité le plus élevé. Ce rapport présente les passerelles des objets routeurs présentant le taux d'indisponibilité le plus élevé.
État opérationnel	Routeurs et passerelles présentant le taux d'état opérationnel le plus élevé. Ce rapport présente les passerelles des objets routeurs présentant le taux d'état opérationnel le plus élevé.
État injoignable	Routeurs et passerelles présentant le taux d'état injoignable le plus élevé. Ce rapport présente les passerelles des objets routeurs présentant le taux d'état injoignable le plus élevé.
État dégradé	Routeurs et passerelles présentant le taux d'état dégradé le plus élevé. Ce rapport présente les passerelles des objets routeurs présentant le taux d'état dégradé le plus élevé.

Rapports Services Web

L'activité analysée dans la catégorie Services Web concerne les flux liés aux services Web du marché définis dans la configuration du firewall ainsi qu'aux services Web personnalisés.

Services Web par volume échangé	Top des services Web par volume échangé. Ce rapport présente les services Web présents dans la configuration du firewall et pour lesquels le trafic est le plus important en termes de volume de données.
Services Web par nombre de connexions	Top des services Web par nombre de connexions. Ce rapport présente les services Web présents dans la configuration du firewall et pour lesquels le nombre de connexions relevées est le plus important.

RÈGLES IMPLICITES

Règles de filtrage implicites

Cet écran vous informe qu'il est possible de générer automatiquement différentes règles de filtrage IP pour autoriser l'utilisation des services du firewall. Si vous activez un service, le firewall crée de lui-même les règles de filtrage nécessaires, sans avoir besoin de créer des règles « explicites » dans la politique de filtrage.

Pour détecter et bloquer les attaques de type SYN Flood contre les services internes du firewall, les règles implicites à destination des services internes du firewall doivent être désactivées et remplacées par des règles explicites équivalentes. Dans ce cas, le firewall génère des logs spécifiques permettant de tracer les tentatives de déni de service via ce type d'attaques.

La grille de règles

La grille présente les colonnes suivantes :

Activé	Affiche l'état de la règle. Effectuez un double-clic pour activer / désactiver la règle implicite.
Nom	Affiche le nom de la règle implicite. Celui-ci n'est pas modifiable.

Les règles suivantes figurent dans la colonne **Nom** :

- **Autoriser l'accès au serveur PPTP** : les utilisateurs peuvent contacter le firewall via le protocole PPTP pour accéder au serveur, s'il est activé.
- **Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster HA)** : cela permet aux différents membres du cluster HA de communiquer entre eux.
- **Autoriser ISAKMP (port 500 UDP) et le protocole ESP pour les correspondants VPN IPsec site à site** : les correspondants VPN IPsec pourront contacter le firewall via ces deux protocoles permettant de sécuriser les données circulant sur le trafic IP.
- **Autoriser l'accès au service DNS (port 53) du Firewall pour les interfaces protégées** : les utilisateurs peuvent joindre le service DNS, et donc utiliser le proxy cache DNS, si ce dernier est activé.
- **Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces modems (dialup)**.
- **Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces ethernet**.
- **Autoriser l'accès au serveur d'administration (port 1300) du firewall pour les interfaces protégées (Serverd)** : les administrateurs pourront se connecter via les réseaux internes sur le port 1300 du firewall. Ce service est utilisé notamment par des outils annexes Stormshield (exemple : Stormshield Network Centralized Management).
- **Autoriser l'accès au port ssh du Firewall pour les interfaces protégées** : permet d'ouvrir l'accès au firewall par SSH afin de pouvoir se connecter dessus en lignes de commande à partir d'une machine située sur les réseaux internes.

- **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces associées aux profils d'authentification (Authd)** : une règle autorisant l'accès au service https (port 443) est créée pour chaque interface associée à un profil d'authentification ayant activé le portail captif. Les utilisateurs peuvent donc s'authentifier et accéder au VPN SSL depuis les réseaux correspondant à ces interfaces.
- **Autoriser l'accès au serveur d'administration web du firewall (WebAdmin) :** les administrateurs pourront se connecter à l'interface d'administration web.

> **NOTE**
> Cette règle autorise l'accès au portail captif, et donc à l'interface d'administration web pour tous les utilisateurs connectés depuis une interface protégée. Pour restreindre l'accès à l'administration web (répertoire */admin/*), il faut indiquer une ou plusieurs machines depuis le module **Système > Configuration** onglet **Administration du Firewall**. Un tableau permet de restreindre l'accès à ces pages au niveau applicatif web.

- **Autoriser les requêtes "Bootp" avec une adresse IP spécifiée pour relayer les requêtes DHCP** : les requêtes du service BOOTP (Bootstrap Protocol) vers un serveur DHCP relayé par le firewall sont autorisées lorsqu'elles utilisent une adresse IP spécifiée dans la configuration du relai DHCP (option « adresse IP utilisée pour relayer les requêtes DHCP »). Cette option est utilisée pour relayer les requêtes DHCP d'utilisateurs distants au travers d'un tunnel IPsec vers un serveur interne.
- **Autoriser les clients à joindre le service VPN SSL du firewall sur les ports TCP et UDP** : les connexions relatives à l'établissement de tunnel VPN SSL sont autorisées sur les ports TCP et UDP.
- **Autoriser les sollicitations de routeur (RS) en multicast ou à destination du firewall** : si le support d'IPv6 est activé sur le Firewall, les nœuds IPv6 peuvent envoyer des sollicitations de routeur (RS) en multicast ou au firewall.
- **Autoriser les requêtes au serveur DHCPv6 et les sollicitations multicast DHCPv6** : si le support d'IPv6 est activé sur le Firewall, les clients DHCPv6 peuvent émettre des requêtes de sollicitations au serveur ou relai DHCPv6 présent sur le firewall.
- **Ne pas tracer les paquets IPFIX dans le trafic IPFIX** : cette règle permet de ne pas inclure les paquets nécessaires au fonctionnement du protocole IPFIX dans les traces envoyées vers le(s) collecteur(s) IPFIX.
- **Autoriser la réception de paquets IGMP et PIM pour le fonctionnement du routage multicast dynamique** : cette règle permet de ne pas rejeter les paquets IGMP et PIM à destination du firewall lorsque vous configurez du routage multicast dynamique.
- **Autoriser l'envoi des requêtes d'analyse de certificats vers une autre interface. Utile pour TLS 1.3** : cette règle permet de transférer les requêtes d'analyse de certificats d'une interface du firewall vers une autre.
- **Autoriser l'accès aux ressources Extended Web Control** : cette règle autorise les requêtes du firewall vers le fournisseur de base de données de classification d'URL.

> **IMPORTANT**
> Deux cas peuvent être dangereux :
>
> - **Désactiver la règle « Serverd »** : peut amener, en cas d'absence de règle explicite, à ne plus avoir d'accès avec les outils annexes Stormshield utilisant le port 1300 (exemple : Stormshield Network Centralized Management).
> - **Désactiver la règle « WebAdmin »** : vous n'aurez plus accès à l'interface d'administration web, sauf si une règle explicite l'autorise.

Configuration avancée

Inclure les règles implicites de sortie des services hébergés (indispensable)	Cette case, cochée par défaut, active les règles implicites de sortie pour les services hébergés par le firewall. Cette fonctionnalité, qui était présente dans les versions antérieures de firmware, ne pouvait jusqu'à présent être modifiée qu'à l'aide d'une commande CLI. **IMPORTANT** Ces règles sont indispensables au bon fonctionnement du firewall. Elles devront être explicitement définies dans la politique de filtrage si cette case a été décochée.

RÉPUTATION DES MACHINES

Cette fonctionnalité, qui peut être combinée à la géolocalisation, permet de limiter le risque d'attaques subies par une entreprise.

Via sa politique de sécurité, l'administrateur peut bloquer les connexions des machines ayant une mauvaise réputation.

Trois critères entrent en compte dans le calcul de réputation d'une machine :

- Les alarmes mineures et majeures générées par la machine,
- Les résultats d'analyse sandboxing des fichiers échangés par la machine,
- Les résultats d'analyse antivirale des fichiers hébergés et transitant par la machine.

Onglet Configuration

Cette onglet permet d'activer la gestion de réputation des machines et de définir le poids respectif des différents critères entrant dans le calcul d'une réputation.

Général

	Ce bouton permet d'activer ou de désactiver la gestion de réputation des machines.

Alarmes

Majeur [0-20]	Réglez le curseur afin de définir le poids des alarmes majeures émises par une machine dans le calcul de sa réputation.
Mineur [0-20]	Réglez le curseur afin de définir le poids des alarmes mineures émises par une machine dans le calcul de sa réputation.

Antivirus

Infectés [0-100]	Réglez le curseur afin de définir le poids des fichiers infectés détectés pour une machine dans le calcul de réputation de cette machine.
Inconnus [0-20]	Réglez le curseur afin de définir le poids dans le calcul de réputation d'une machine des fichiers n'ayant pas pu être analysés (fichiers chiffrés, fichiers protégés par mot de passe,...).
Analyse échouée [0-20]	Réglez le curseur afin de définir le poids des fichiers dont l'analyse antivirale a échoué dans le calcul de réputation d'une machine (fichier corrompu, base antivirale corrompue...).

Sandboxing

Malveillant [0-100]	Réglez le curseur afin de définir le poids des fichiers malveillants détectés pour une machine dans le calcul de réputation de cette machine.
Suspect [0-100]	Réglez le curseur afin de définir le poids des fichiers suspects détectés pour une machine dans le calcul de réputation de cette machine.

Analyse échouée [0-20]	Réglez le curseur afin de définir le poids des fichiers dont l'analyse sandboxing a échoué dans le calcul de réputation d'une machine (fichier corrompu,...).

Statistiques

Réinitialiser le score de toutes les machines dans la base de données	En cliquant sur ce bouton, vous effacez les scores de réputation de toutes les machines contenues dans la base de données de réputation. Toutes ces machines bénéficieront alors de nouveau d'un score de réputation nul et qui évoluera selon les paramètres choisis dans les catégories **Alarmes**, **Antivirus** et **Sandboxing**. Si des règles de filtrage bloquantes sont appliquées selon le score de réputation, les machines ne seront donc bloquées qu'après que leur score de réputation ait augmenté.

Onglet Machines

Cette onglet permet de sélectionner les machines du réseau interne pour lesquelles une réputation doit être calculée.

Machines supervisées

Cette grille permet de définir les machines pour lesquelles une réputation doit être calculée. Il est possible d'**Ajouter** ou de **Supprimer** des machines, groupes de machines, réseaux, plages d'adresses IP à l'aide des boutons du même nom.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des machines supervisées :

- **Ajouter**,
- **Supprimer**.

Configuration avancée

Machines exclues

Cette grille permet de définir les machines à exclure du calcul de réputation. Il est possible d'**Ajouter** ou de **Supprimer** des machines, groupes de machines, réseaux, plages d'adresses IP à l'aide des boutons du même nom.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des machines exclues :

- **Ajouter**,
- **Supprimer**.

ROUTAGE

Le fonctionnement du routage est segmenté en plusieurs onglets. Ceux IPv6 sont accessibles seulement si l'IPv6 est activé dans la configuration du firewall.

- Routes statiques IPv4 / IPv6 : permet la définition des routes statiques. Le routage statique représente un ensemble de règles définies par l'administrateur ainsi qu'une route par défaut.
- Routage dynamique IPv4 / IPv6 : permet de configurer les protocoles de routage dynamique (RIP, OSPF, BGP) au sein du moteur BIRD afin de permettre au firewall d'apprendre des routes gérées par d'autres équipements.
- Routes de retour IPv4 / IPv6 : lorsque plusieurs passerelles sont utilisées pour réaliser du partage de charge, cet onglet permet de définir la passerelle par laquelle les paquets retour doivent impérativement transiter afin de garantir la cohérence des connexions.

Ces parties fonctionnent simultanément, le routage statique étant prioritaire sur tout le reste lors de l'acheminement d'un paquet sur le réseau.

Onglets Routes statiques IPv4 / IPv6

Ces onglets correspondent à la liste des routes statiques dont le nombre maximum varie selon le modèle de firewall. Retrouvez cette information en consultant sa fiche produit disponible sur le site www.stormshield.com.

L'onglet **Routes statiques IPv6** est accessible seulement si l'IPv6 est activé dans la configuration du firewall.

Configuration générale

Passerelle par défaut (routeur)	Le routeur par défaut est généralement l'équipement qui permet l'accès de votre réseau à Internet. C'est à cette adresse que le firewall envoie les paquets qui doivent sortir sur le réseau public. Bien souvent le routeur par défaut est connecté à Internet. Si vous ne configurez pas le routeur par défaut, le firewall ne sait pas laisser passer les paquets possédant une adresse de destination différente de celles directement reliées au firewall. Vous pourrez ainsi communiquer entre les machines sur les réseaux internes, externes ou DMZ, mais aucun autre réseau (dont Internet). Pour définir le routeur par défaut, sélectionnez dans le menu déroulant l'objet (Machine ou Routeur) le représentant. Si cet objet n'existe pas, cliquez sur le bouton de création d'un objet pour le créer. Une fois la sélection faite, le nom de la machine réapparaît sur l'écran. Cette option peut être grisée dans le cas où plusieurs passerelles principales sont définies.

Routes statiques

Les actions possibles

Certaines actions peuvent également être réalisées en effectuant un clic droit dans la grille.

Rechercher...	Recherche qui porte sur un objet machine, un réseau ou un groupe.

Ajouter	Ajoute une ligne vide dans la grille. L'ajout de la route (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Réseau de destination (objet machine, réseau ou groupe)** et **Interface** complétés.
Supprimer	Supprime une route ou plusieurs routes préalablement sélectionnée(s).

Une fois les modifications réalisées :

Appliquer	Envoie la configuration des routes statiques.
Annuler	Annule la configuration des routes statiques.

La grille des routes statiques

État	Précise l'état de la configuration des routes statiques. Double-cliquez pour activer ou désactiver une route.
Réseau de destination (objet machine, réseau ou groupe)	Un clic dans cette colonne ouvre la base d'objets afin de sélectionner une machine, un réseau ou encore un groupe. Si l'objet n'existe pas, cliquez sur le bouton de création d'un objet pour le créer. Ce champ est obligatoire.
Interface	Une liste déroulante permet de sélectionner l'interface de sortie permettant de joindre le réseau distant. Ce champ est obligatoire.
Plan d'adressage	Cette colonne affiche l'adresse IP ou le groupe d'adresses liés aux éléments de la colonne **Réseau de destination (objet machine, réseau ou groupe)**.
Protégée	Cette colonne vous informe de la nature protégée ou pas de la route. Une route protégée est ajoutée à l'objet *Network internals*. Le comportement de la configuration de sécurité prendra en compte ce paramètre. Les machines joignables par cette route seront mémorisées dans le moteur de prévention d'intrusion.
Passerelle	Un clic dans cette colonne ouvre la base d'objets pour sélectionner un objet machine ou un objet routeur (ne faisant pas l'objet de répartition de charge). Si l'objet souhaité n'existe pas, cliquez sur le bouton de création d'un objet pour le créer. Ce champ est optionnel. **NOTE** La répartition de charge n'est pas compatible avec la définition de routes statiques. Si vous sélectionnez un routeur faisant l'objet de répartition de charge, un message d'avertissement vous indique que cette route ne peut pas être activée.
Commentaire	Champ optionnel pour insérer un texte libre.

Onglets Routes de retour IPv4 / IPv6

Lorsque plusieurs passerelles sont utilisées pour réaliser du partage de charge, cet onglet permet de définir la passerelle par laquelle les paquets retour doivent impérativement transiter afin de garantir la cohérence des connexions.

L'onglet **Routes de retour IPv6** est accessible seulement si l'IPv6 est activé dans la configuration du firewall.

Routes de retour

Les actions possibles

Certaines actions peuvent également être réalisées en effectuant un clic droit dans la grille.

Rechercher...	Recherche qui porte sur un objet machine, un réseau ou un groupe.
Ajouter	Ajoute une ligne vide dans la grille. L'ajout de la route (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Passerelle** et **Interface** complétés.
Supprimer	Supprime une route ou plusieurs routes préalablement sélectionnée(s).

Une fois les modifications réalisées :

Appliquer	Envoie la configuration des routes de retour.
Annuler	Annule la configuration des routes de retour.

La grille des routes de retour

État	Précise l'état de la configuration des routes de retour. Double-cliquez pour activer ou désactiver une route.
Passerelle	Un clic dans cette colonne ouvre la base d'objets afin de sélectionner une machine ou une interface virtuelle (IPsec). S'il s'agit d'un objet de type "machine", il devra impérativement préciser une adresse MAC. Ce champ est optionnel.
Interface	Une liste déroulante permet de sélectionner l'interface de sortie pour la route de retour. Ce champ est obligatoire.
Commentaire	Champ optionnel pour insérer un texte libre.

ROUTAGE DYNAMIQUE

BIRD prend en charge les versions suivantes de protocoles de routage dynamique :

- Rip v2,
- OSPF v2 pour IPv4 et OSPF v3 pour IPv6,
- BGP v4 pour IPv4 et IPv6.

En version SNS 4.8 ou supérieure, le firewall peut exécuter au choix le moteur de routage dynamique BIRD en version 1 (obsolète) ou en version 2.

Ceci permet de réaliser la migration d'une configuration d'origine BIRD v1 vers la version BIRD v2 sans risque.

Le module **Routage dynamique** est organisé en 3 ou 4 onglets selon que la configuration du routage dynamique s'applique à IPv6 ou non :

- L'onglet **Général**,
- L'onglet nommé **BIRD v2** ou **BIRD v2 (INACTIF)** selon que BIRD v2 est activé ou non,
- L'onglet nommé **BIRD v1 IPv4** ou **BIRD v1 IPv4 (INACTIF)** selon que BIRD v1 IPv4 est activé ou non,
- L'onglet nommé **BIRD v1 IPv6** ou **BIRD v1 IPv6 (INACTIF)** selon que BIRD v1 IPv6 est activé ou non.

Onglet Général

Cet onglet permet d'activer l'une ou l'autre des versions de BIRD et de paramétrer le comportement du routage dynamique, notamment dans le cas d'une configuration en haute disponibilité.

Configuration générale

BIRD v2	Active ou désactive l'utilisation du moteur de routage dynamique BIRD v2.
BIRD v1 IPv4	Active ou désactive l'utilisation du moteur de routage dynamique BIRD v1 pour les routes IPv4 uniquement.
BIRD v1 IPv6	Active ou désactive l'utilisation du moteur de routage dynamique BIRD v1 pour les routes IPv6 uniquement.
BIRD v1 IPv4 et IPv6	Active ou désactive l'utilisation du moteur de routage dynamique BIRD v1 pour les routes IPv4 et IPv6.

Configuration avancée

Redémarrer le routage dynamique lorsque le firewall devient actif (Haute Disponibilité)	Au sein d'un cluster mettant en œuvre le protocole de routage dynamique OSPF, le firewall actif tient le rôle de routeur OSPF référent (DR : Designated Router). Cette option permet d'éviter qu'au cours d'une bascule, le nouveau firewall actif ne détecte pas qu'il hérite de ce rôle de Designated Router OSPF. Elle est activée par défaut. Ce champ est accessible seulement dans l'onglet **Routage dynamique IPv4**.

Ajouter les réseaux IPv4 distribués par le routage dynamique dans la table des réseaux protégés	Cette option permet d'injecter automatiquement dans la table des réseaux protégés du moteur de prévention d'intrusion les réseaux propagés par le moteur de routage dynamique IPv4.
Ajouter les réseaux IPv6 distribués par le routage dynamique dans la table des réseaux protégés	Cette option permet d'injecter automatiquement dans la table des réseaux protégés du moteur de prévention d'intrusion les réseaux propagés par le moteur de routage dynamique IPv6.

Onglet BIRD v2

> **NOTE**
> Le suffixe "**(Inactif)**" est ajouté au nom de l'onglet **BIRD v2** lorsque la version 2 de BIRD n'est pas activée dans l'onglet **Général**.

Présentation de l'écran

Cet écran a été conçu pour faciliter la migration de BIRD v1 vers BIRD v2.

Il comporte 3 éléments :

- Dans la partie supérieure gauche de l'écran : la fenêtre de saisie de la configuration de BIRD v2, sa barre d'outils et le bouton de vérification de configuration,
- Dans la partie supérieure droite de l'écran : la fenêtre d'affichage de la configuration de BIRD v1,
- Dans la partie inférieure de l'écran : la console de vérification de la configuration.

La fenêtre de saisie de la configuration BIRD v2

Cette fenêtre permet de saisir les modifications de la configuration du moteur de routage dynamique BIRD.

Vérifier la configuration	En cliquant sur ce bouton, vous déclenchez une vérification de la configuration : si des erreurs de syntaxe sont présentes, elles sont référencées dans la console de vérification (ligne et colonne de l'erreur). Cette opération de vérification est obligatoire pour pouvoir enregistrer les modifications apportées à la configuration.

Les actions possibles : la barre d'outils

Rechercher	Ce champ permet de rechercher une chaîne de caractères dans la configuration de BIRD v2. Vous pouvez rendre cette recherche sensible / insensible à la casse à l'aide du bouton **Aa**.
Aa	Ce bouton permet de rendre la recherche sensible / insensible à la casse.

Revenir à la configuration enregistrée	Si les modifications apportées à la configuration de BIRD ne conviennent pas, ce bouton permet de revenir à la version de la configuration précédemment enregistrée. Pour bénéficier pleinement de cette fonctionnalité, il est important d'enregistrer régulièrement les modifications apportées à la configurations (bouton **Appliquer**).
Copier dans le presse-papier	Ce bouton permet de copier le texte sélectionné dans le presse papier afin de le coller dans un document externe par exemple.
Revenir à la configuration proposée par défaut	Ce bouton permet de supprimer toutes les modifications apportées à la configuration de BIRD v2 en restaurant la configuration minimale proposée sur un firewall en configuration d'usine.

La fenêtre d'affichage de la configuration BIRD v1 (IPv4 et / ou IPv6)

Lorsqu'une configuration de routage dynamique BIRD v1 est présente sur le firewall, elle est affichée dans cette fenêtre qui propose un ou deux onglets selon les versions d'IP configurées dans BIRD v1 : IPv4 et / ou IPv6.

L'objectif de cette fenêtre est de faciliter la migration de BIRD v1 vers BIRD v2 en offrant la possibilité d'effectuer directement des opérations de copier / coller d'éléments de configuration tout en vérifiant qu'aucun élément n'a été oublié.

La console de vérification

Après avoir cliqué sur le bouton **Vérifier la configuration**, cette console affiche les lignes / colonnes des éventuelles erreurs de syntaxe présentes dans la configuration de BIRD v2.

Il est obligatoire de les corriger pour pouvoir enregistrer la configuration.

Enregistrer / Appliquer la configuration

Cliquez sur **Appliquer** puis **Sauvegarder** pour enregistrer la configuration : cette opération n'est possible que si la configuration est valide (sans erreurs de syntaxe).

Si le protocole BIRD v2 est actif, la configuration sauvegardée est automatiquement appliquée.

Onglets BIRD v1 IPv4 et BIRD v1 IPv6

> **NOTE**
> Le suffixe "**(Inactif)**" est ajouté au nom des onglets **BIRD v1 IPv4** et **BIRD v1 IPv6** lorsque la version de BIRD correspondante n'est pas activée dans l'onglet **Général**.

Présentation de l'écran

L'écran comporte 2 éléments :

- Dans la partie supérieure de l'écran : la fenêtre de saisie de la configuration de BIRD v1, sa barre d'outils et le bouton de vérification de configuration,
- Dans la partie inférieure de l'écran : la console de vérification de la configuration.

La fenêtre de saisie de la configuration BIRD v1

Cette fenêtre permet de saisir les modifications de la configuration du moteur de routage dynamique BIRD.

Vérifier la configuration	En cliquant sur ce bouton, vous déclenchez une vérification de la configuration : si des erreurs de syntaxe sont présentes, elles sont référencées dans la console de vérification (ligne et colonne de l'erreur). Cette opération de vérification est obligatoire pour pouvoir enregistrer les modifications apportées à la configuration.

Les actions possibles : la barre d'outils

Rechercher	Ce champ permet de rechercher une chaîne de caractères dans la configuration de BIRD v1. Vous pouvez rendre cette recherche sensible / insensible à la casse à l'aide du bouton **Aa**.
Aa	Ce bouton permet de rendre la recherche sensible / insensible à la casse.
Revenir à la configuration enregistrée	Si les modifications apportées à la configuration de BIRD ne conviennent pas, ce bouton permet de revenir à la version de la configuration précédemment enregistrée. Pour bénéficier pleinement de cette fonctionnalité, il est important d'enregistrer régulièrement les modifications apportées à la configurations (bouton **Appliquer**).
Copier dans le presse-papier	Ce bouton permet de copier le texte sélectionné dans le presse papier.
Revenir à la configuration proposée par défaut	Ce bouton permet de supprimer toutes les modifications apportées à la configuration de BIRD v1 en restaurant la configuration minimale proposée sur un firewall en configuration d'usine.

La console de vérification

Après avoir cliqué sur le bouton **Vérifier la configuration**, cette console affiche les lignes / colonnes des éventuelles erreurs de syntaxe présentes dans la configuration.

Il est obligatoire de les corriger pour pouvoir enregistrer la configuration.

Enregistrer / Appliquer la configuration

Cliquez sur **Appliquer** puis **Sauvegarder** pour enregistrer la configuration : cette opération n'est possible que si la configuration est valide (sans erreurs de syntaxe).

Si le protocole BIRD v1 est actif, la configuration sauvegardée est automatiquement appliquée.

ROUTAGE MULTICAST

Le routage multicast est une technologie dont l'objectif est de préserver la bande passante en délivrant un flux unique d'information à plusieurs destinataires, potentiellement en très grand nombre (plusieurs milliers).
Le multicast IP permet de délivrer des contenus simultanés en utilisant le moins de bande passante possible mais aussi sans surcharger ni l'émetteur ni les récepteurs.

Cette méthode de distribution est intéressante pour des applications de type vidéo-conférence, e-learning, cotations boursières, vidéo *on demand*.

NOTE
Le routage multicast (statique ou dynamique) est prioritaire sur tous les autres types de routage (routage statique, routage dynamique, routage au sein d'un bridge, routage par politique, ...).

	Cet interrupteur permet d'activer ou de désactiver le routage multicast. Il est ensuite impératif de sélectionner le routage statique **ou** le routage dynamique **IMPORTANT** Le routage multicast statique et le routage multicast dynamique ne peuvent pas être activés simultanément.
Routage statique	Ce bouton radio permet d'activer le routage multicast statique et son onglet de paramétrage.
Routage dynamique	Ce bouton radio permet d'activer le routage multicast dynamique et son onglet de paramétrage.

L'onglet Routage Statique

Les actions sur les règles de la politique de routage multicast statique

La grille permet de définir les règles de la politique de routage multicast à appliquer sur le Firewall. Les règles prioritaires sont placées en haut. Le firewall exécute les règles dans l'ordre (règle n°1, 2 et ainsi de suite) et s'arrête dès qu'il trouve une règle correspondant au trafic.

Ajouter	Ce bouton permet d'insérer une ligne après la ligne sélectionnée ; un assistant de création de règle de routage se lance alors automatiquement.
Supprimer	Supprime la règle sélectionnée.
Monter	Ce bouton permet de placer la règle sélectionnée avant la règle directement au-dessus.
Descendre	Ce bouton permet de placer la règle sélectionnée après la règle directement en-dessous.
Couper	Ce bouton permet de couper une règle de routage pour la déplacer.
Copier	Ce bouton permet de copier une règle de routage dans le but de la dupliquer.
Coller	Ce bouton permet de dupliquer une règle de routage, après l'avoir copiée.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des routes statiques multicast :

- Ajouter,
- Supprimer,
- Monter,
- Descendre,
- Couper,
- Copier,
- Coller.

Nouvelle règle

Étape 1 : sélection du groupe multicast et de l'interface source

Sélectionnez l'objet multicast contenant les adresses IP multicast autorisées, ainsi que l'origine (interface source) du trafic multicast pour cette règle de routage.

Le groupe multicast doit contenir une machine, un réseau, une plage d'adresses IP ou un groupe comportant exclusivement des adresses IP multicast (comprises dans plage 224.0.0.0 - 239.255.255.255).

Étape 2 : sélection des interfaces destination

Cliquez sur **Ajouter** afin de cibler la destination du trafic concernée par la règle de routage multicast. Vous pouvez ajouter autant d'interfaces destinations que nécessaire dans la règle.

Un paquet multicast correspondant à la règle (paquet provenant d'une adresse contenue dans le groupe multicast et se présentant par l'une des interfaces sources déclarées) sera transmis à l'ensemble des interfaces de destination.

La grille

La grille présente la liste des règles de routage statique multicast ainsi que leur état :

État	État de la route statique multicast : • on : La route est opérationnelle. • off : La route n'est pas opérationnelle. Double-cliquez pour activer la route.
Interface Source	Affiche le groupe multicast et l'interface source associée sous la forme : groupe_multicast@interface_source.
Interfaces de destination	Affiche la liste des interfaces de destination du flux multicast précisées dans l'assistant de création de la règle de routage.
Commentaire	Affiche le commentaire éventuellement renseigné lors de l'ajout de la règle.

L'onglet Routage Dynamique

Définitions

- Source multicast : émetteur de la source (caméra vidéo par exemple).
- Receiver multicast : récepteur du flux multicast (abonné au groupe multicast).
- Groupe multicast : adresse multicast (privée, publique, SSM).
- (S,G) - (Source, Groupe) multicast : couple adresse IP de la source, adresse du groupe multicast.
- IGMP (*Internet Group Management Protocol*) : protocole utilisé par un récepteur multicast pour s'abonner ou se désabonner à un groupe multicast.
- PIM (*Protocol Independent Multicast*) : famille de protocoles de routages IP multicast.
- PIM-SM (*PIM Sparse Mode*) : version de PIM qui construit un arbre de distribution. C'est une version évolutive du protocole qui permet de gérer de multiples sources. L'arbre de distribution peut être :
  - En mode partagé en passant par un Rendez-vous Point (Shared Tree ou RPT),
  - Établi en recalculant un chemin le plus court possible appelé SPT (Shortest Path Tree), grâce au routage unicast.
- PIM-SSM (*PIM Source-Specific Multicast*) : version de PIM où la source est connue des receveurs. Lorsque le receveur s'abonne, le couple adresse IP de la source et adresse du groupe multicast est formé directement. Ce protocole est plus simple à mettre en œuvre que PIM-SM (absence de RP), mais nécessite IGMPv3 et se destine à un type d'applications plus limité.
- RP (*Rendez-vous Point*) : rôle tenu par un routeur PIM-SM. Le RP est sollicité pour indiquer où se trouve la source multicast.
  Le firewall SNS peut jouer ce rôle.
- BSR (*BootStrap Router*) : rôle tenu par un routeur PIM. Le BSR est élu parmi une liste de candidats. Une fois élu, il récolte les candidatures pour le rôle de RP, puis diffuse aux autres routeurs la table des associations groupes multicast / RP.
  Le firewall SNS peut jouer ce rôle.

Interfaces & candidats Rendez-vous Points (RP dynamiques)

Il s'agit de définir toutes les interfaces participant au routage multicast dynamique :

- Les interfaces source et / ou destination utilisant le protocole IGMP,
- Les versions de protocole IGMP que peuvent accepter ces interfaces pour les annonces de sources ou d'abonnement et désabonnement des récepteurs,
- Les interfaces utilisées par un firewall candidat à un rôle de Rendez-vous Point (RP) dynamique et les groupes multicast associés,
- Les interfaces utilisées par un firewall candidat à un rôle de Bootstrap Router (BSR).

Pour autoriser les paquets issus de ces protocoles à destination des interfaces du firewall, il est impératif que la règle de filtrage implicite **Autoriser la réception de paquets IGMP et PIM pour le fonctionnement du routage multicast dynamique** soit activée. Elle est activée par défaut.

Les actions possibles

Tout sélectionner	Ce bouton permet de sélectionner toutes les lignes de la grille afin de les supprimer en une seule action.
Ajouter	Ce bouton permet d'insérer une ligne après la ligne sélectionnée pour ajouter une interface.
Supprimer	Ce bouton permet de supprimer la ligne sélectionnée.
Éditer la sélection	Ce bouton permet de modifier la ligne sélectionnée.

La grille

Interface	Interface participant au multicast : • Interface utilisée pour les annonces IGMP (demandes d'abonnement ou de désabonnement de récepteurs multicast). Exemple : l'interface *in* et l'interface *out* du firewall. • Interfaces utilisées pour les candidatures RP (C-RP). Il est recommandé d'utiliser des interfaces de boucle locale (*loopback*) définies à cet effet. Ces interfaces doivent avoir une adresse IP "routable".
Version IGMP	Versions du protocole IGMP que peut accepter cette interface pour les demandes d'abonnement ou de désabonnement de récepteurs multicast. Les choix possibles sont : • **IGMP v2 uniquement**, • **IGMP v2 et IGMP v3.**
Priorité du DR	Le *Designated Router* (DR) est le routeur de bordure (dernier routeur rencontré avant une source multicast ou un récepteur multicast) chargé de transmettre les demandes d'abonnements au RP. Il est élu. Indiquez la priorité accordée à la candidature du firewall pour jouer ce rôle pour un groupe multicast donné. **IMPORTANT** L'interface présentant le numéro de priorité le **moins élevé** sera la plus prioritaire parmi tous les candidats. A égalité de priorité, c'est l'interface présentant l'adresse IP la plus élevée qui sera prioritaire.
C-RP (Candidat Rendez-vous Point)	Cochez cette case pour activer la candidature du firewall au rôle de RP pour le groupe multicast associé.
Priorité C-RP (Candidat Rendez-vous Point)	**IMPORTANT** L'interface présentant le numéro de priorité le **moins élevé** sera la plus prioritaire parmi tous les candidats. A égalité de priorité, c'est l'interface présentant l'adresse IP la plus élevée qui sera prioritaire.
Groupes Multicast	Précisez le groupe multicast associé au C-RP.

Ajouter une interface

> **NOTE**
> Les bridges et interfaces appartenant à des bridges ne peuvent pas être sélectionnés comme interfaces multicast.

Pour ajouter une interface à la liste des interfaces participant au routage multicast dynamique :

1. Sélectionnez la ligne de la grille sous laquelle vous souhaitez créer une nouvelle entrée.
2. Cliquez sur **Ajouter**.
3. Sélectionnez l'interface.
4. Sélectionnez la version de protocole IGMP autorisée pour cette interface : **IGMP v2 uniquement** ou **IGMP v2 et IGMP v3**.

   > **NOTE**
   > Si vous souhaitez utiliser le protocole PIM-SSM, il est impératif de choisir **IGMP v2 et IGMP v3** car seul IGMP v3 est compatible avec ce protocole.

5. Précisez la priorité affectée à cette interface.
   Cette notion de priorité est importante dans une architecture à accès multiples où plusieurs firewalls SNS ou routeurs gèrent du routage multicast dynamique sur le même réseau local. En effet, la priorité permettra l'élection du Designated Router (DR) qui sera en charge de l'envoi des requêtes auprès du RP via l'interface la plus prioritaire.

   > **NOTE**
   > L'interface présentant le numéro de priorité le plus bas sera la plus prioritaire pour le routage des flux multicast.
   > A égalité de priorité, c'est l'interface présentant l'adresse IP la plus élevée qui sera prioritaire.

6. Si vous souhaitez que le firewall participe aux élections de RP avec cette interface, cochez la case **Être candidat au rôle de Rendez-vous Point (RP)**. Dans ce cas, complétez la configuration en sélectionnant :
   - Une priorité C-RP (Candidate Rendez-vous Point),
   - Un ou plusieurs groupes multicast pour lesquels le firewall jouera le rôle de RP s'il est élu à ce rôle.

Les interactions possibles

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des interfaces :

- Ajouter,
- Supprimer,
- Éditer la sélection.

Paramètres PIM-SM

Être candidat au rôle de Bootstrap Router (BSR)

La présence d'un Bootstrap Router (BSR) est indispensable dans une configuration utilisant les Rendez-vous Points (RP) dynamiques car il gère le processus des élections des RP :

- Il récolte les candidatures issues des C-RP,
- Procède à l'élection de RP pour chaque groupe multicast,
- Annonce les RP en charge des différents groupes multicast.

Lorsqu'un un BSR est déjà configuré sur le réseau, le firewall SNS peut ne pas être candidat à cette fonction.

Si vous souhaitez que le firewall SNS puisse être élu en tant que BSR, utilisez cette grille :

Adresse	Sélectionnez l'interface réseau du firewall qui servira d'identifiant au firewall dans le mécanisme d'élections. Il peut s'agir d'une interface du firewall (exemple : *Firewall_out*) mais il est conseillé d'utiliser des adresses IP de boucle locale (*loopback*) spécifiquement définies pour cet usage, car elles ne dépendent pas d'interfaces physiques dont l'état peut varier. Cette interface doit avoir été déclarée dans les interfaces participant au multicast. Les interfaces *loopback* peuvent être définies dans le module **Réseau** > **Interfaces virtuelles** > onglet **Loopback**. Plus d'informations sur la création d'interfaces *loopback*.
Priorité	Cette notion de priorité est importante dans une architecture pour laquelle plusieurs équipements sont candidats pour être BSR : l'équipement dont l'interface est la plus prioritaire sera élu. **IMPORTANT** L'interface présentant le numéro le **plus élevé** sera la plus prioritaire. A égalité de priorité, c'est l'interface présentant l'adresse IP la plus élevée qui sera prioritaire.

Rendez-vous Points (RP) statiques

NOTE
Il est nécessaire d'être très rigoureux dans la gestion des groupes multicast (aucun recouvrement d'adresses toléré) pour utiliser simultanément le mécanisme d'élections de RP et la définition de RP statiques.

Si vous souhaitez définir de manière statique (sans passer par un mécanisme d'élections) les Rendez-vous Points, utilisez cette grille.

Les actions possibles :

- Pour ajouter une définition statique de RP, cliquez sur **Ajouter** puis remplissez les deux champs suivants :

Plage	Plage d'adresses multicast (groupe multicast) qui sera gérée par le RP statique. Il peut s'agir par exemple d'un groupe d'adresses ou d'une plage incluant les adresses IP multicast des caméras de vidéo-surveillance. Cette plage peut être une plage personnalisée existante définie dans les objets réseau du firewall ou peut être créée directement depuis cette grille.

Adresse	Adresse IP du RP en charge du groupe multicast précisé. Il peut s'agir d'une interface du firewall (exemple : *Firewall_out*) mais il est conseillé d'utiliser des adresses IP de boucle locale (*loopback*) spécifiquement définies pour cet usage, car elles ne dépendent pas d'interfaces physiques dont l'état peut varier. Cette interface doit avoir été déclarée dans les interfaces participant au multicast. Les interfaces *loopback* peuvent être définies dans le module **Réseau** > **Interfaces virtuelles** > onglet **Loopback**. Plus d'informations sur la création d'interfaces *loopback*.

IMPORTANT
Chaque entrée (adresse IP) de RP statique doit être renseignée à l'identique sur l'ensemble des équipements participant au routage multicast de la plage considérée.

- Pour supprimer une définition statique de RP, sélectionnez la ligne correspondante puis cliquez sur **Supprimer**.
- Pour supprimer toutes les définitions statiques de RP, cliquez sur **Tout sélectionner** puis sur **Supprimer**.

NOTE
L'utilisation de RP statiques présente un inconvénient : il n'y a pas de redondance en cas de perte du RP en charge du groupe multicast précisé.

Paramètres avancés

Intervalle entre deux Hello	Intervalle de temps (en secondes) entre deux envois de paquets Hello à destination des autres équipements gérant le protocole PIM. La valeur proposée par défaut est de 30 secondes.
Intervalle entre deux requêtes IGMP	Intervalle de temps (en secondes) entre deux requêtes destinées à recueillir les demandes d'abonnements de récepteurs multicast ou de détecter au contraire les fins d'abonnements. La valeur proposée par défaut est de 5 secondes.

SERVEUR PPTP

IMPORTANT
La fonctionnalité Serveur PPTP est obsolète et sera supprimée dans une version SNS à venir.

L'écran de configuration du **serveur PPTP** se divise en 2 zones :

- **Configuration générale** : Activation du serveur PPTP, choix du pool d'adresses.
- **Configuration avancée** : Chiffrement du trafic.

La mise en place est très simple et rapide et se déroule en trois étapes :

- Les adresses IP des clients PPTP (objet).
- Les paramètres de chiffrement.
- Le Serveur DNS et le serveur WINS.

Configuration générale

Activer le serveur PPTP	Activation / Configuration du serveur **PPTP** sur le firewall. Cela est réalisé en cochant **Activer le serveur PPTP**.
Adresses IP des clients PPTP (objet) (Obligatoire)	Une fois le serveur PPTP activé, il faut obligatoirement créer un pool d'adresses IP privées. Le firewall affecte au client qui vient se connecter en **PPTP** une adresse IP disponible dans le pool. Il faut créer un groupe de machines contenant les adresses réservées, ou une plage d'adresses provenant de la base objets.

Paramètres transmis aux clients PPTP

Serveur DNS	Le champ **Serveur DNS** permet d'envoyer l'adresse IP du serveur DNS au client.
Serveur WINS	Le champ **Serveur WINS** permet d'envoyer au client l'adresse IP du serveur WINS du site.

REMARQUE
Les caractères « _ », « - », et « . » sont autorisés pour les noms des utilisateurs PPTP.

Configuration avancée

Chiffrement du trafic

Les paramètres de chiffrement possibles sont :

Ne pas chiffrer	Désactive le champ **Accepter uniquement le trafic chiffré et autoriser les algorithmes suivants** ainsi que les MPPE proposés.

Accepter uniquement le trafic chiffré et autoriser les algorithmes suivants	Autorise la connexion uniquement si le client chiffre les données.
MPPE40 bits	Autorise l'utilisation du protocole de chiffrement MPPE 40 bits.
MPPE56 bits	Autorise l'utilisation du protocole de chiffrement MPPE 56 bits.
MPPE128 bits	Autorise l'utilisation du protocole de chiffrement MPPE 128 bits.

SERVICES WEB

Ce module présente les services Web définis sur le firewall. Ils sont destinés à être utilisés au sein de la politique de filtrage. Il en existe deux types :

- Les services Web officiels (onglet **Liste des services Web**) : ils sont téléchargés automatiquement via le module Active Update. Ce sont les services Web des principaux éditeurs du marché (exemple : Google Drive, Logmein, Microsoft Azure...). Ils peuvent être regroupés au sein de groupes prédéfinis et personnalisés (onglet **Groupes**).
- Les services Web personnalisés (onglet **Liste des services Web**) : ils sont définis par l'administrateur et importés sur le firewall par le biais d'un fichier au format CSV (onglet **Import de services personnalisés**). Ils peuvent être regroupés au sein de groupes personnalisés (onglet **Groupes**).

Onglet Liste des services Web

Cet onglet donne une vue d'ensemble des services Web définis sur le firewall. La grille des services Web comporte deux sections :

- La liste des services Web distribués par Stormshield,
- La liste des services Web personnalisés.
  Cette liste apparaît seulement si une base personnalisée a été importée.

Services Web distribués par Stormshield

Ce sont les services Web en ligne les plus répandus (Microsoft Office 365, Logmein, Sharepoint, Webex ...).
Ils sont automatiquement importés et mis à jour via le mécanisme Active Update.

Chaque service Web est composé d'adresses IP publiques et / ou de FQDN.

Les caractéristique d'un service Web sont les suivantes :

Nom	Nom donné au groupe.
Utilisation	La pastille de couleur : • Verte : indique que le service Web correspondant appartient à un groupe de services ou est utilisé dans la configuration du firewall. • Noire : indique que le groupe correspondant n'appartient à aucun groupe de services et n'est pas utilisé dans la configuration du firewall.

En survolant l'un de ces services Web, une infobulle en présente les caractéristiques :

- **Nom** : le nom du service Web (exemple : Microsoft Office 365),
- **Description** : le contenu du service (exemple : adresses IP et domaines pour joindre les services en ligne de Microsoft Office 365),
- **En lecture seule** : indique si le service est modifiable ou peut être supprimé. Un service Web distribué par Stormshield est toujours en lecture seule,
- **Numéro de révision** : ce numéro s'incrémente à chaque fois qu'Active Update récupère une nouvelle version du contenu du service Web concerné,
- **Date de révision** : il s'agit de la date de dernière récupération par Active Update d'une mise à jour du contenu du service Web concerné,

- **URL** : précise les adresses permettant de consulter les listes de FQDN ou d'adresses IP publiques du service chez le fournisseur.

Services Web personnalisés

Cette liste n'est affichée que lorsque des services Web personnalisés ont été importés via un fichier au format CSV (onglet **Import de services personnalisés**).

En survolant l'un de ces services Web, une infobulle en présente les caractéristiques :

- **Nom** : le nom du service Web (exemple : MonServiceWebPersonnalisé),
- **Description** : correspond au commentaire optionnel précisé pour le service dans le fichier d'import,
- **En lecture seule** : indique si le service est modifiable ou peut être supprimé. Un service personnalisé est toujours en lecture seule. Seule la base complète de services Web personnalisés peut être supprimée,
- **Numéro de révision** : ce numéro est précisé manuellement dans le fichier CSV d'import,
- **Date de révision** : cette date est précisée manuellement dans le fichier CSV d'import,
- **Nombre d'adresses IPv4** : indique par combien d'adresses IPv4 est défini le service Web,
- **Nombre d'adresses IPv6** : indique par combien d'adresses IPv6 est défini le service Web,
- **Nombre de FQDN** : indique par combien de FQDN est défini le service Web.

Les actions possibles

Entrer un filtre...	Saisissez une séquence de lettres présente dans le nom des services Web recherchés pour limiter l'affichage à ces services.
Exporter la base personnalisée	Cliquez sur ce bouton pour exporter tous les services Web personnalisés dans un fichier au format CSV qu'il vous est proposé de télécharger.
Supprimer la base personnalisée	Cliquez sur ce bouton pour supprimer l'intégralité de la base de services Web personnalisés.
Vérifier l'utilisation	Cliquez sur ce bouton pour vérifier si l'un des services web listé dans la grille est utilisé dans la configuration du firewall : 1. Sélectionnez le service Web. 2. Cliquez sur **Vérifier l'utilisation**. Les modules de configuration utilisant ce service Web sont affichés dans le menu de gauche.

Onglet Groupes

Cet onglet est composé de deux parties distinctes :

- La liste des groupes de services Web sur la gauche de l'écran,
- Les propriétés et les membres du groupe sélectionné sur la droite de l'écran.

La grille Liste des groupes

Cette grille contient :

- Les groupes prédéfinis contenant les services Web officiels (Cloud Computing, Microsoft...),

- Les éventuels groupes personnalisés destinés à contenir des services Web officiels et personnalisés. Ces groupes sont créés manuellement par l'administrateur.

Les caractéristique d'un groupe sont les suivantes :

Nom	Nom donné au groupe.
Utilisation	Une pastille de couleur : • Verte indique que le groupe correspondant est utilisé dans la configuration du firewall. • Noire indique que le groupe correspondant n'est pas utilisé dans la configuration du firewall.
Nombre de membres	Affiche le nombre de services Web composant le groupe.
Commentaire	Affiche le commentaire optionnel défini lors de la création ou la modification du groupe (uniquement pour les groupes personnalisés).

En survolant l'un de ces groupes, une infobulle en présente les caractéristiques :

- **Nom** : le nom du groupe (exemple : Microsoft),
- **En lecture seule** : indique si le groupe peut être renommé ou supprimé. Un groupe de services Web officiels est toujours en lecture seule,
- **Membres du groupe** : liste les services Web inclus dans le groupe.

Les actions possibles sur la grille Liste des groupes

Entrer un filtre...	Saisissez une séquence de lettres présente dans le nom des groupes de services Web recherchés pour limiter l'affichage à ces groupes.
Tout sélectionner	En cliquant sur le bouton, tous les groupes de services présents dans la grille sont sélectionnés.
Ajouter	Ce bouton permet de créer un nouveau groupe personnalisé vide : 1. Cliquez sur **Ajouter**. 2. Saisissez le **Nom du groupe** (ce nom ne peut pas contenir d'espaces). 3. Ajoutez un éventuel **Commentaire**. 4. Cliquez sur **Appliquer**.
Renommer	Cette action n'est possible que pour les groupes personnalisés. 1. Sélectionnez le groupe personnalisé que vous souhaitez renommer. 2. Cliquez sur **Renommer**. 3. Saisissez le nouveau **Nom du groupe**. 4. Cliquez sur **Appliquer**.
Supprimer	Cette action n'est possible que pour les groupes personnalisés. 1. Sélectionnez le ou les groupes personnalisés que vous souhaitez supprimer (sélection multiple avec la touche [Ctrl]). 2. Cliquez sur **Supprimer**. 3. Validez la suppression en cliquant sur **OK**.

Vérifier l'utilisation	Ce bouton permet de vérifier si l'un groupe de services web listé dans la grille est utilisé dans la configuration du firewall : 1. Sélectionnez le groupe. 2. Cliquez sur **Vérifier l'utilisation**. Les modules de configuration utilisant ce groupe sont affichés dans le menu de gauche.

Éditer les propriétés et les membres d'un groupe de services

Double cliquez sur le groupe à éditer. Seuls les groupes personnalisés peuvent être modifiés.

Les propriétés et les membres du groupe sélectionné s'affichent sur la droite de l'écran.

Propriétés du groupe

Commentaires	Saisissez le commentaire souhaité pour le groupe. La prise en compte de ce commentaire est immédiate (il s'affiche automatiquement dans la grille des groupes de services).

Grille Membres du groupe

Entrer un filtre...	Saisissez une séquence de lettres présente dans le nom des membres du groupe de services Web recherchés pour limiter l'affichage à ces membres.
Tout sélectionner	En cliquant sur le bouton, tous les membres présents dans le groupe sont sélectionnés afin de leur appliquer une action commune (**Supprimer**).
Ajouter	Ce bouton permet d'ajouter des services Web (officiels et personnalisés) ou des groupes de services Web dans le groupe personnalisé en cours d'édition : 1. Cliquez sur **Ajouter**. La liste des services Web et des groupes de services définis sur le firewall s'affiche. Les services déjà présents dans le groupe sont surlignés en jaune et la case précédant leur nom est cochée. **NOTE** Il n'est pas possible d'ajouter un groupe contenant un service déjà présent dans le groupe en cours d'édition. 2. Cochez les cases des services Web ou des groupes que vous souhaitez ajouter. La prise en compte des modifications est immédiate.
Supprimer	Cette action n'est possible que pour les groupes personnalisés. 1. Sélectionnez les services Web ou groupes de services Web que vous souhaitez supprimer du groupe en cours d'édition (sélection multiple avec la touche [Ctrl]). 2. Cliquez sur **Supprimer**. La prise en compte des modifications est immédiate.

Onglet Import de services personnalisés

Cet onglet est destiné à importer des services Web personnalisés depuis un fichier au format CSV.
La structure à respecter pour ce fichier au format CSV est décrite dans la section Structure du fichier d'import de services Web personnalisés (format CSV).

Importer

IMPORTANT
L'import réussi d'une base personnalisée **supprime et remplace** la base personnalisée existante. Dans ce cas, assurez-vous au préalable que le fichier d'import utilisé contienne tous les services Web personnalisés que vous souhaitez conserver, sinon ils seront perdus.

1. Utilisez le champ **Sélectionner la base à importer (fichier CSV)** pour choisir un fichier d'import stocké sur votre poste de travail.
2. Cliquez ensuite sur le bouton **Importer la base**.
   Selon le résultat de l'import, des informations additionnelles sont affichées dans ce cadre :
   - En cas de succès : le message "La liste personnalisée de services Web importée est entièrement opérationnelle",
   - En cas d'échec :
     - La raison de l'échec (exemple : "La génération de fichiers bitgraphs issus de l'import CSV a échoué : le format de certaines données du fichier CSV est invalide"),
     - Le N° de la ligne incriminée dans le fichier CSV et le contenu de cette ligne (exemple : "Une erreur est survenue à la ligne 1 : MyWebService1,,2022/01/19,12.2,My first Web service").

Informations au sujet du dernier import

Après un import réussi, ce cadre présente un résumé des données importées :

Dernier import de services Web personnalisés	Date et heure du dernier import réalisé avec succès.
Nombre de services Web personnalisés	Nombre de services Web importés via le fichier CSV.
Total d'adresses IPv4	Nombre d'enregistrements importés et caractérisés par une adresse IPv4.
Total d'adresses IPv6	Nombre d'enregistrements importés et caractérisés par une adresse IPv6.
Total de FQDN	Nombre d'enregistrements importés et caractérisés par un FQDN.

STORMSHIELD MANAGEMENT CENTER

Si vous disposez du serveur d'administration centralisée Stormshield Management Center, ce panneau vous permet d'installer le package de rattachement afin de connecter votre firewall au serveur SMC.

IMPORTANT
Lorsque vous êtes connecté via l'interface Web d'administration à un firewall rattaché à un serveur SMC, la mention "**Managed by SMC**" est affichée dans le panneau supérieur. Le compte utilisé ne dispose par défaut que des droits d'accès en lecture.
Il est fortement déconseillé de modifier directement la configuration d'un firewall administré par un serveur SMC, sauf en cas d'urgence (serveur SMC non joignable par exemple).
En effet, toute modification de configuration réalisée directement via l'interface Web d'administration sur un firewall rattaché à un serveur SMC est susceptible d'être écrasée par l'envoi d'une nouvelle configuration depuis le serveur SMC.
Pour plus d'informations sur la mise en œuvre de SMC, consultez le Guide d'installation SMC et le Guide d'administration SMC.

Rattachement du firewall au serveur SMC

Sélectionner le package de rattachement	Choisissez le package de rattachement SMC issu du serveur d'administration centralisée.

Les boutons

Installer le package: lorsqu'un package de rattachement a été sélectionné, ce bouton permet de le télécharger et de l'installer sur le firewall.

Paramètres de rattachement

Une fois le package installé, les informations de rattachement au serveur sont alors affichées (adresse IPv4/IPv6 du serveur, durée de validité de la connexion, fréquence de vérification de cette connexion, délai d'attente de réponse du serveur, délai d'attente avant reconnexion).

NOTE
Pour plus d'informations sur l'administration centralisée Stormshield Management Center, veuillez-vous référer au Guide d'installation SMC et au Guide d'administration SMC.

TPM

Lorsque le firewall est équipé d'un TPM, ce cadre permet d'activer la protection de la clé privée du certificat utilisé pour les communications avec le serveur SMC. Pour activer cette protection, cliquez sur le bouton **Protéger l'agent SMC**.

Si le firewall est déjà rattaché à un serveur SMC lors de l'initialisation du TPM, la clé privée du certificat utilisé pour les communications avec le serveur SMC est protégée automatiquement.

Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module.

Installer un nouveau package de rattachement sur un firewall SNS

Lorsqu'un firewall SNS est déjà rattaché à SMC, si vous souhaitez remplacer le package de rattachement, procédez comme suit.

Assurez-vous auparavant qu'aucun déploiement de configuration ou de mise à jour de SMC n'est en cours d'exécution.

1. Depuis SMC, générez un nouveau package de rattachement depuis le menu **Système** > **Configuration** du firewall.
2. Sur le firewall, exécutez la commande `CLI CONFIG RESTORE list=fwadmin,network < /tmp/mon_fichier.pack` en fournissant le package (*.pack*).

Envoyer une demande de rattachement au serveur SMC

Cette méthode permet de rattacher manuellement un firewall au serveur SMC, sans installation de package de rattachement.

> **NOTE**
> Pour que cette méthode de rattachement fonctionne, le firewall doit avoir été déclaré au préalable sur le serveur SMC.

Adresse du serveur SMC	Saisissez l'adresse IP du serveur SMC auquel vous souhaitez rattacher le firewall.
Empreinte numérique du serveur SMC	Saisissez l'empreinte numérique SHA-256 du certificat présenté par le serveur SMC auquel vous souhaitez rattacher le firewall.

Les boutons

Envoyer la demande: lorsque les informations concernant le serveur SMC ont été renseignées, ce bouton permet d'envoyer la demande de rattachement au serveur SMC et de déclencher le processus de rattachement.

SUPERVISION

Le module **Supervision** propose des données en temps réel ainsi que des courbes historiques (si cette option a été activée dans le module **Configuration des rapports**) concernant :

- L'état du matériel et de la haute disponibilité,
- L'utilisation des ressources système du firewall,
- Le niveau d'utilisation des interfaces réseaux,
- Le niveau d'utilisation des files d'attente de la QoS,
- Les machines ayant traversé le firewall,
- Les utilisateurs authentifiés sur le firewall,
- Les connexions réalisées au travers du firewall,
- L'état des routeurs, routeurs SD-WAN et passerelles réseau définis sur le firewall,
- L'état du routage multicast dynamique : rôle du firewall, routes et groupes multicast connus...
- Le service DHCP,
- Les tunnels VPN SSL établis,
- Les tunnels VPN IPsec établis,
- Les listes blanches / noires du firewall,
- Les captures du trafic réseau traversant le firewall.

Ces données sont présentées sous forme de courbes ou de grilles. Les courbes historiques proposent quatre échelles de temps: dernière heure, jour, semaine ou mois. Ces plages sont calculées par rapport aux paramètres de date et d'heure du firewall.

Données personnelles

Par souci de conformité avec le règlement européen RGPD (Règlement Général sur la Protection des Données), les données sensibles (nom d'utilisateur, adresse IP source, nom de la source, adresse MAC source) ne sont pas affichées dans les logs et rapports et sont remplacées par la mention "Anonymized".

Pour visualiser ces données sensibles, l'administrateur doit alors activer le droit "Logs : accès complet (données personnelles)" en cliquant sur **Logs : accès restreint** dans le bandeau supérieur de l'interface Web d'administration, puis en saisissant un code d'autorisation obtenu auprès de son superviseur (voir la section **Administrateurs** > **Gestion des tickets**). Ce code possède une durée de validité limitée définie lors de sa création.

Pour relâcher ce droit, l'administrateur doit ensuite cliquer sur la mention **Logs : accès complet (données personnelles)** présente dans le bandeau supérieur de l'interface Web d'administration puis cliquer sur le bouton **Libérer** de la boite de dialogue affichée.

Après avoir obtenu ou relâché ce droit, il est nécessaire de rafraîchir les données affichées.

Notez que chaque action d'obtention ou de libération du droit "Logs : accès complet (données personnelles)" génère une entrée dans les logs.

NOTE
Pour les modèles SN160(W), SN-XS-Series-170, SN210(W), SN-S-Series-220, SN310, SN-S-Series-320, SNi10 et SNi20, vous pouvez bénéficier de l'ensemble de la fonctionnalité en utilisant un support de stockage externe de type :

- Carte SD pour les modèles SN160(W), SN210(W), SN310 et SNi20,
- Carte microSD pour les modèles SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320 et SNi10.

Les caractéristiques que doivent respecter ces supports sont précisées dans la partie LOGS - JOURNAUX D'AUDIT de ce guide.

La grille

Recherche	Ce champ permet la recherche de graphiques ou grilles de supervision par mot clé.

Les info-bulles

Le survol à la souris de certains types d'objets permet d'en afficher les propriétés dans une info-bulle. Ceci offre l'avantage, par exemple, de limiter le nombre de colonnes à afficher dans une grille.

Lorsque l'administrateur dispose du droit d'accès complet aux logs, les propriétés affichées dans l'info-bulle sont les suivantes :

Machine ou adresse IP

- Nom de la machine si celle-ci est définie dans la base objets,
- Adresse IP de la machine,
- Système d'exploitation de la machine (machine interne uniquement),
- Nombre de vulnérabilités détectées pour la machine,
- Score de réputation de la machine (machine interne uniquement),
- Pays d'hébergement de la machine (machine externe uniquement),
- Nombre de paquets émis,
- Nombre de paquets reçus,
- Bande passante sortante utilisée,
- Bande passante entrante utilisée,
- Interface du firewall par laquelle cette machine est vue,
- Adresse MAC de la machine (machine interne uniquement).

Grilles concernées :

- Supervision des machines : vue "Machines", vue "Connexions",
- Supervision des utilisateurs : vue "Utilisateurs", vue "Connexions",
- Supervision des connexions.

Port destination

- Nom de l'objet correspondant au port,
- Numéro de port,
- Protocole,
- Commentaire éventuel défini dans l'objet Port.

Grilles concernées :

- Supervision des machines : vue "Machines", vue "Connexions",
- Supervision des utilisateurs : vue "Connexions",
- Supervision des connexions.

Utilisateur

- Description éventuelle,
- Identifiant de connexion,
- Domaine (annuaire),
- E-mail,
- Téléphone,
- Adresse IP de la machine de connexion et nom de l'objet machine correspondant s'il est défini dans la base objets,
- Interface du firewall par laquelle cette machine est vue,
- Bande passante entrante utilisée,
- Bande passante sortante utilisée.

Grilles concernées :

- Supervision des utilisateurs : vue "Utilisateurs",
- Supervision des connexions.

Interface

- Nom,
- Interface protégée ou non,
- Bridge auquel est éventuellement rattachée l'interface,
- Bande passante entrante utilisée,
- Bande passante sortante utilisée.

Grilles concernées :

- Supervision des machines : vue "Machines",
- Supervision des utilisateurs : vue "Connexions",
- Supervision des connexions.

Matériel / Haute Disponibilité

L'onglet "Matériel"

Ce module présente différents indicateurs de fonctionnement du firewall ou des membres du cluster sous forme de graphiques ou de grilles :

- Courbe de température CPU,
- Informations et tests S.M.A.R.T des disques,
- État du RAID éventuel,
- État des alimentations,
- État des ventilateurs,
- Modems 3G/4G connectés au firewall.

Les interactions

Pour la courbe :

- Un clic gauche sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique,
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.

Pour la grille des informations S.M.A.R.T. :

- En survolant la référence d'un disque à l'aide de la souris, le détail des tests S.M.A.R.T. réalisés et leurs résultats sont affichés dans une info-bulle.

L'onglet "Détails du cluster"

Cet onglet n'est accessible que lorsque la Haute Disponibilité est configurée et activée. Il regroupe des données sur l'état de la haute disponibilité pour chacun des membres du cluster.

La colonne **Firewall local** présente la valeur d'un indicateur pour le firewall sur lequel l'administrateur est connecté. La colonne **Firewall distant** présente la valeur de cet indicateur pour le membre distant du cluster.

Indicateurs

N° de série	Ce champ indique le N° de série des deux membres du cluster.
État	Ce champ indique si le firewall concerné est Actif ou Passif.
Version de firmware	Indique la version du firmware sur chacun des membres du cluster.
État forcé	L'état *Actif* est forcé sur l'un des membres du cluster lorsque vous sélectionnez "Ce firewall (N° de série)" ou "L'autre firewall (N° de série)" pour le champ **Indicateur de qualité** (menu **Système** > **Haute disponibilité** > **Configuration avancée**).
Indicateur de qualité	Précise l'indicateur de qualité calculé pour la haute disponibilité. Cet indicateur tient notamment compte du poids affecté aux interfaces réseau en cas d'indisponibilité accidentelle de l'une d'entre elles. Un voyant dont la couleur varie du vert au rouge accompagne la valeur de l'indicateur.
Priorité	Indique la priorité affectée au firewall sur lequel l'administrateur est connecté. Cette priorité peut être fixée dans le menu : **Haute Disponibilité** > **Indicateur de qualité** > **Firewall actif en cas d'égalité**. Si l'un des firewalls est sélectionné, il possède alors une priorité de 50 tandis que l'autre membre du cluster se voit attribuer une priorité de 0.
État de la synchronisation	Indique si les configurations des deux membres du cluster sont identiques. Valeurs possibles : *Synchronisé* ou *Désynchronisé*. Un voyant vert ou rouge accompagne cette valeur.
État du lien HA	Affiche l'état du lien physique principal entre les membres du cluster : • OK : le lien est opérationnel • KO : le lien n'est pas opérationnel (câble débraché,...). • UNKNOWN : l'état du lien ne peut pas être récupéré.

État du lien HA de secours	Affiche l'état du lien physique de secours (secondaire) entre les membres du cluster : • OK : un lien de secours est défini et opérationnel. • KO : un lien de secours est défini mais n'est pas opérationnel (câble débraché,...). • UNKNOWN : l'état du lien ne peut pas être récupéré. • N/A: aucun lien de secours n'est défini dans la configuration de la HA.

Indicateurs avancés

Récupération des informations HA	Indique sous la forme d'un voyant vert ou rouge si le firewall a répondu à la requête permettant de récupérer les données concernant la Haute Disponibilité.
Modèle de firewall	Précise le modèle de firewall (SN200, SN6000...).
Superviseur	Dans un cluster, l'un des deux firewalls assure le rôle de superviseur afin de décider d'une synchronisation de fichiers par exemple. Ce champ indique lequel des deux firewalls assure ce rôle.
Numéro de version (données)	Ce numéro de version est associé aux données issues du moteur de prévention d'intrusion et synchronisées entre les deux firewalls. Il permet de détecter les incompatibilités quand le cluster regroupe deux firewalls dont la version diffère.
Numéro de version (connexions)	Ce numéro de version est associé au protocole (et non aux données) utilisé pour la synchronisation des données issues du moteur de prévention d'intrusion.
Numéro de version (état)	Numéro de version de l'algorithme servant à déterminer l'état (actif / passif) des membres du cluster.
Licence	Précise le type de licence liée à la HA (Master / Slave / None).
Actuellement connecté sur	Indique sur quel membre du cluster l'administrateur est connecté.
Partition de boot	Indique quelle partition est utilisée en cas de démarrage du firewall (Principale / Secours).
Version de la partition de secours	Précise la version de firmware installé sur la partition de secours.
Date de la partition de secours	Indique la date de dernière mise à jour de la partition de secours.
Dernier démarrage du firewall	Indique la date du dernier démarrage du firewall (format: AAAA-MM-JJ HH:MM:SS).
Dernière synchronisation	Indique la date de la dernière synchronisation au sein du cluster (format: AAAA-MM-JJ HH:MM:SS).
Dernier changement d'état	Indique la date du dernier changement d'état (Actif / Passif) du firewall (format: AAAA-MM-JJ HH:MM:SS).

Service HA	Il s'agit de l'état interne du service de gestion de la HA sur les membres du cluster. Les valeurs possibles sont les suivantes: • Starting : état initial du service lorsque le firewall vient de redémarrer. • Waiting peer : lors du redémarrage, le firewall se met en passif et tente de joindre l'autre membre du cluster. • Synchronizing : lorsqu'un firewall a redémarré puis a réussi à contacter l'autre membre du cluster, une synchronisation des connexions est lancée. • Running : le firewall est Actif. • Ready : le firewall est Passif et prêt à passer en Actif si nécessaire. • Reboot : avant son redémarrage, le firewall en informe l'autre membre du cluster puis devient passif. Son service est alors vu en état Reboot. • Down : avant d'etre arrêté, le firewall en informe l'autre membre du cluster. Son service est alors vu en état Down.
Adresse IP du lien HA	Adresse IP du firewall portée par l'interface dédiée au lien HA principal.
Changement d'état du lien HA	Indique la date du dernier changement d'état du lien HA principal (format: AAAA-MM-JJ HH:MM:SS).
Adresse IP du lien HA de secours	Adresse IP du firewall portée par l'interface dédiée au lien HA de secours (N/A si aucun lien de secours n'est défini dans le cluster).
Changement d'état du lien HA de secours	Indique la date du dernier changement d'état du lien HA de secours (format: AAAA-MM-JJ HH:MM:SS).
N° du dernier déploiement SMC	Indique le n° de révision du dernier déploiement de configuration réalisé via Stormshield Management Center (N/A si les firewalls ne sont pas gérés par un serveur SMC).

Système

L'onglet "Temps réel"

Ce module présente différents indicateurs de fonctionnement du firewall sous forme de graphiques ou de grilles :

- Consommation CPU (espace utilisateur, interruptions et système).
- Utilisation mémoire par hôtes internes, paquets fragmentés, état ICMP, sessions TCP / UDP, suivi de données IPS, services actifs et *sockets* réseau.
- Consommation CPU de chacun des services activés sur le firewall.
- Informations système : date et heure du système, durée de fonctionnement depuis le dernier redémarrage.
- Active Update : nom, état (**Jamais utilisé** / **Échec** / **Désactivé** / **Mis à jour manuellement** / **A jour** / **En cours**) et date de dernière mise à jour des base de sécurité du firewall.
  Il est possible de relancer une mise à jour de l'ensemble des modules paramétrés pour être actualisés automatiquement (bouton **Relancer toutes les mises à jour automatiques**). Dans le cas d'un module configuré en mise à jour manuelle (mention **Mis à jour manuellement**), il s'agit de la date du dernière fichier *.ssp* importé.
- Agents SSO : nom, état (Activé / Désactivé) de l'agent principal et de l'agent de secours pour chaque méthode Agent SSO configurée (module **Configuration > Utilisateurs > Authentification**).

- NTP : nom du serveur, état, raison de l'alarme éventuelle, date de dernière connexion du firewall au serveur et niveau de strate du serveur par rapport à l'horloge atomique pour chaque serveur NTP configuré (module **Configuration** > **Configuration** > onglet **Configuration générale**).
- Serveurs syslog : nom, état (Activé / Désactivé), protocole utilisé pour chaque serveur syslog configuré (module **Configuration > Notifications > Traces - Syslog - IPFIX**).
- Radius : nom, état, port du serveur principal et du serveur de secours (module **Configuration > Utilisateurs > Authentification**).
- Agents TS : nom, nombre d'utilisateur connectés via l'agent, état et temps écoulé depuis la dernière connexion du firewall à l'agent pour chaque Agent TS configuré (module **Configuration > Utilisateurs > Authentification**).

Les actions

Tout réduire	Replie l'ensemble des graphiques de la page en une seule action.
Tout déplier	Déplie l'ensemble des graphiques de la page en une seule action.
Ajouter une colonne	Augmente le nombre de colonnes d'affichage des courbes et informations.
Enlever une colonne	Réduit le nombre de colonnes d'affichage des courbes et informations.
Accéder à la configuration de la supervision	Redirige vers le module de configuration de la supervision (intervalles de rafraîchissement).

Les interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info-bulle.
- Des boutons permettent d'accéder directement à la fenêtre de configuration de certains modules.

L'onglet "Historique"

Cet onglet présente un graphique historique de la consommation CPU du firewall (espace utilisateur, interruptions et système).

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.
Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.

Les interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.
- Un clic sur le bouton présent à droite de chaque graphique met en page les données du graphique pour un envoi en impression. Un commentaire peut être ajouté avant de confirmer l'impression (bouton **Imprimer**).

Interfaces

L'onglet "Temps réel"

Ce module présente deux indicateurs graphiques pour chaque interface / agrégat d'interfaces sélectionné dans le module **Configuration** > **Configuration de la supervision** :

- Utilisation de la bande passante (débit entrant, débit sortant),
- Nombre de connexions (TCP, UDP).

Les actions

Tout fermer	Le bouton permet de replier l'ensemble des graphiques de la page en une seule action.
Tout dérouler	Le bouton permet de déplier l'ensemble des graphiques de la page en une seule action.
Ajouter une colonne	Ce bouton permet d'augmenter le nombre de colonnes d'affichage des courbes et informations. Il offre ainsi un regroupement d'informations dans une même colonne pour chaque interface active.
Enlever une colonne	Ce bouton permet de réduire le nombre de colonnes d'affichage des courbes et informations.
Configurer les interfaces réseau	Ce lien permet de se rendre directement dans le module de configuration des interfaces réseau (module **Configuration** > **Réseau** > **Interfaces**).
Accéder à la configuration de la supervision	Ce lien permet de se rendre directement dans le module de configuration des interfaces réseau à superviser.

Les interactions

- Un clic gauche sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.

L'onglet "Historique"

Cet onglet présente des graphiques historiques d'utilisation de la bande passante et du nombre de paquets acceptés / bloqués pour chacune des interfaces supervisées (à l'exception des VLAN).

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.
Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.
Réduire	Le bouton permet de replier l'ensemble des graphiques de la page en une seule action.
Développer	Le bouton permet de déplier l'ensemble des graphiques de la page en une seule action.
Ajouter une colonne	Ce bouton permet d'augmenter le nombre de colonnes d'affichage des courbes et informations. Il offre ainsi un regroupement d'informations dans une même colonne pour chaque interface active.
Enlever une colonne	Ce bouton permet de réduire le nombre de colonnes d'affichage des courbes et informations.

Les Interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.
- Un clic sur le bouton présent à droite de chaque graphique met en page les données du graphique pour un envoi en impression. Un commentaire peut être ajouté avant de confirmer l'impression (bouton **Imprimer**).

QoS

L'onglet "Temps réel"

Pour chacune des files d'attentes de QoS sélectionnées dans le module **Configuration** > **Configuration de la supervision**, ce module présente l'utilisation de bande passante (débit entrant, débit sortant) sous forme de graphique.

Les actions

Réduire	Le bouton permet de replier l'ensemble des graphiques de la page en une seule action.

Développer	Le bouton permet de déplier l'ensemble des graphiques de la page en une seule action.
Ajouter une colonne	Ce bouton permet d'augmenter le nombre de colonnes d'affichage des courbes et informations. Il offre ainsi un regroupement d'informations dans une même colonne pour chaque file d'attente active.
Enlever une colonne	Ce bouton permet de réduire le nombre de colonnes d'affichage des courbes et informations.
Accéder à la configuration de la QoS	Ce lien permet de se rendre directement dans le module de configuration de la QoS (module **Configuration** > **Politique de sécurité** > **Qualité de service**).
Accéder à la configuration de la supervision	Ce lien permet de se rendre directement dans le module de configuration des files d'attente de QoS à superviser.

Les interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.

L'onglet "Historique"

Cet onglet présente des graphiques historiques d'utilisation de bande passante pour chacune des files d'attente de QoS supervisées.

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.
Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.
Réduire	Le bouton permet de replier l'ensemble des graphiques de la page en une seule action.
Développer	Le bouton permet de déplier l'ensemble des graphiques de la page en une seule action.
Ajouter une colonne	Ce bouton permet d'augmenter le nombre de colonnes d'affichage des courbes et informations. Il offre ainsi un regroupement d'informations dans une même colonne pour chaque file d'attente active.

Enlever une colonne	Ce bouton permet de réduire le nombre de colonnes d'affichage des courbes et informations.

Les Interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.
- Un clic sur le bouton présent à droite de chaque graphique met en page les données du graphique pour un envoi en impression. Un commentaire peut être ajouté avant de confirmer l'impression (bouton **Imprimer**).

Machines

L'onglet "Temps réel"

L'écran se compose de 2 vues :

- Une vue qui liste les machines.
- Une vue qui liste les Connexions, Vulnérabilités, Applications, Services, Informations, et Historique de réputation en rapport avec la machine sélectionnée.

Vue « Machines »

Cette vue permet de visualiser toutes les machines détectées par le firewall. Une ligne représente une machine.

Les données de la vue « Machines » sont les suivantes :

Nom	Nom de la machine émettrice (si déclarée dans les objets) ou adresse IP de la machine (dans le cas contraire).
Adresse IP	Adresse IP de la machine.
Adresse MAC	Adresse MAC de la machine.
Interface	Interface à laquelle est rattaché l'utilisateur.
Réputation	Score de réputation de la machine. Cette colonne ne contient des données que lorsque la gestion de réputation des machines est activée et que la machine sélectionnée appartient aux machines supervisées.
Paquets	Nombre de paquets échangés par la machine sélectionnée.
Octets entrants	Nombre d'octets ayant transité par le firewall à partir de la machine émettrice depuis le démarrage du firewall.
Octets sortants	Nombre d'octets ayant transité par le firewall à destination de la machine émettrice depuis le démarrage du firewall.
Débit entrant	Débit réel des flux émis par la machine source et transitant par le firewall.
Débit sortant	Débit réel des flux vers la machine destination et transitant par le firewall.

Protégée	Indique si l'interface sur laquelle la machine a été détectée est une interface protégée.
Continent	Si la case **Voir toutes les machines (affiche également les machines derrière les interfaces non protégées)** a été cochée dans le filtre, le continent d'origine de la machine externe est affiché.
Pays	Si la case **Voir toutes les machines (affiche également les machines derrière les interfaces non protégées)** a été cochée dans le filtre, le pays d'origine de la machine externe est affiché.
Catégorie de réputation	Indique la catégorie de réputation de la machine externe si celle-ci est classifiée. **EXAMPLE** SPAM, Phishing...

Menu contextuel

Un clic droit sur le nom ou l'adresse IP d'une machine donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Vérifier (l'utilisation de) cette machine,
- Afficher les détails de la machine,
- Réinitialiser le score de réputation de cet objet,
- Placer cet objet en liste noire (Pour 1 minute, Pour 5 minutes, Pour 30 minutes ou Pour 3 heures),
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

La barre d'actions

Vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (Nouveau filtre) permet de réinitialiser le filtre en supprimant la sélection de critères.

Filtrer	Cliquez sur ce bouton pour :
	• Sélectionner des critères de filtrage (**Critère de recherche**). Pour la vue "**machines**", ces critères sont les suivants :
	  • Par plage d'adresses ou par adresse IP.
	  • Par interface.
	  • Si le score de réputation est supérieur à la valeur précisée à l'aide du curseur.
	  • Si la case **Voir toutes les machines (affiche également les machines derrière les interfaces non protégées)** est cochée, l'ensemble des machines détectées sera affiché dans la grille.
	• Enregistrer en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après (**Enregistrer le filtre courant**). Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
	• **Supprimer le filtre courant**.

Réinitialiser	Ce bouton permet d'annuler l'action du filtre en cours d'utilisation. S'il s'agit d'un filtre personnalisé enregistré, cette action ne supprime pas le filtre .
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille. Lorsqu'un filtre est appliqué, seuls les résultats correspondant à ce filtre sont exportés.
Réinitialiser l'affichage des colonnes	Ce bouton permet de réinitialiser la largeur des colonnes et de n'afficher que les colonnes proposées par défaut à la première ouverture de cette fenêtre de supervision.

Panneau « FILTRAGE SUR »

Vous pouvez ajouter un critère en glissant la valeur depuis un champ des résultats dans le panneau.

Vue « Connexions »

Cette vue permet de visualiser toutes les connexions détectées par le firewall. Une ligne représente une connexion. Les données disponibles pour la vue « **Connexions** » sont les suivantes :

Date	Indication de la date et de l'heure de connexion de l'objet.
Connexion	Identifiant de la connexion
Connexion parente	Certains protocole peuvent générer des connexions "filles" (exemple : FTP) et, dans ce cas de figure, cette colonne référence l'identifiant de la connexion parente.
Protocole	Protocole de communication utilisé pour la connexion.
Utilisateur	Utilisateur connecté sur la machine (s'il existe).
Source	Adresse IP de la machine à l'origine de la connexion.
Nom de la source	Nom de l'objet (s'il existe) correspondant à la machine source.

Adresse MAC source	Adresse MAC de l'objet à l'origine de la connexion.
Port source	Indication du n° de port source utilisé pour la connexion.
Nom du port source	Nom de l'objet correspondant au port source.
Destination	Adresse IP de la machine vers laquelle la connexion a été établie.
Nom de destination	Nom de l'objet (s'il existe) vers lequel une connexion a été établie.
Port de destination	Indication du n° de port de destination utilisé pour la connexion.
Nom du port dest.	Nom de l'objet correspondant au port destination.
Interf. source	Nom de l'interface du firewall sur laquelle la connexion s'est établie.
Interf dest.	Nom de l'interface de destination utilisée par la connexion sur le firewall.
Débit moyen	Valeur moyenne de bande passante utilisée par la connexion sélectionnée.
Envoyé	Nombre d'octets envoyés au cours de la connexion.
Reçu	Nombre d'octets reçus au cours de la connexion.
Durée	Temps de la connexion.
Dernière utilisation	Temps écoulé depuis le dernier échange de paquets pour cette connexion.
Routeur	Identifiant attribué par le firewall au routeur utilisé par la connexion
Nom du routeur	Nom du routeur enregistré dans la base objet et utilisé par la connexion
Type de règle	Indique s'il s'agit d'une règle locale, globale ou implicite.
Règle	Le nom de l'identifiant de la règle autorisant la connexion
État	Ce paramètre indique le statut de la connexion correspondant par exemple, à son initiation, son établissement ou sa fermeture.
Nom de file d'attente	Nom de la file d'attente QoS utilisée par la connexion.
Nom de la règle	Lorsqu'un nom a été donné à la règle de filtrage par laquelle transite la connexion, ce nom est affiché dans la colonne.
Profil IPS	Affiche le N° du profil d'inspection appelé par la règle ayant filtré la connexion.
Géolocalisation	Affiche le drapeau correspondant au pays de la destination.
Catégorie de réputation	Indique la catégorie de réputation de la machine externe si celle-ci est classifiée. **EXEMPLE** SPAM, Phishing...
Argument	Information complémentaire pour certains protocoles exemple : HTTP).
Opération	Information complémentaire pour certains protocoles exemple : HTTP).

Menu contextuel

Un clic droit sur une ligne de cette vue donne accès au menu contextuel suivant :

- Accéder à la règle de sécurité correspondante.

La barre d'actions

Vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (Nouveau filtre) permet de réinitialiser le filtre en supprimant la sélection de critères.

Filtrer	Cliquez sur ce bouton pour :
	• Sélectionner des critères de filtrage (**Critère de recherche**). Pour la vue "**connexions**", ces critères sont les suivants :
	  • Par plage d'adresses ou par adresse IP (grisé si une machine a été sélectionnée dans la vue "machines").
	  • Par interface.
	  • Par interface source.
	  • Par interface destination.
	  • Par port destination.
	  • Par protocole.
	  • Par utilisateur.
	  • Pour une valeur de données échangées supérieure à la valeur précisée à l'aide du curseur.
	  • Selon la dernière utilisation de la connexion (seuls les enregistrement dont la dernière utilisation est inférieure à la valeur précisée sont affichés).
	  • Par nom de règle de filtrage.
	  • Par profil IPS.
	  • Par origine ou destination géographique.
	  • Si la case **Voir toutes les connexions (connexions closes, réinitialisées, ...)** est cochée, l'ensemble des connexions sera affiché dans la grille, quel que soit leur état.
	• Enregistrer en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après (**Enregistrer le filtre courant**). Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
	• **Supprimer le filtre courant**.

Réinitialiser	Ce bouton permet d'annuler l'action du filtre en cours d'utilisation. S'il s'agit d'un filtre personnalisé enregistré, cette action ne supprime pas le filtre .
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille. Lorsqu'un filtre est appliqué, seuls les résultats correspondant à ce filtre sont exportés.
Réinit. colonnes	Ce bouton permet de ne réafficher que les colonnes proposées par défaut à l'ouverture de la fenêtre de supervision des machines.

Panneau « FILTRAGE SUR »

Vous pouvez ajouter un critère en glissant la valeur depuis un champ des résultats dans le panneau.

Vue « Vulnérabilités »

Cet onglet décrit, pour une machine sélectionnée, les vulnérabilités décelées. Il est possible ensuite de visualiser en détail une vulnérabilité. En survolant une vulnérabilité à l'aide de la souris, un lien vers une page de description de cette vulnérabilité est proposé.

Les données de la vue « Vulnérabilités » sont les suivantes :

Identifiant	Identifiant de la vulnérabilité.
Nom	Indication du nom de la vulnérabilité.
Famille	Nombre de machines affectées.
Sévérité	Indication du niveau de sévérité de la vulnérabilité. Il existe 4 niveaux de sévérité : "**Faible**", "**Modéré**", "**Elevé**", "**Critique**".
Exploit	L'accès peut s'effectuer en local ou à distance (par le réseau). Il permet d'exploiter la vulnérabilité.
Solution	Indique si oui ou non il y a une solution proposée.
Niveau	Indique le niveau de l'alarme associée à la découverte de cette vulnérabilité.
Port	Indique le port réseau sur lequel la machine est vulnérable (exemple : 80 pour un serveur Web vulnérable).
Service	Indique le nom du programme vulnérable (exemple : lighthttpd_1.4.28)
Détecté	Indique la date à laquelle la vulnérabilité a été détectée sur la machine
Détails	Donne un complément d'information sur la vulnérabilité.

Menu contextuel

Un clic droit sur le nom de la vulnérabilité donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

Vue « Applications»

Cet onglet décrit, pour une machine sélectionnée, les applications détectées.

Les données de la vue « **Applications** » sont les suivantes :

Nom du produit	Nom de l'application.
Famille	Famille de l'application (exemple : Web client).
Détails	Nom complet de l'application incluant son numéro de version.

Menu contextuel

Un clic droit sur le nom du produit donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

Vue « Services»

Cet onglet décrit, pour une machine sélectionnée, les services détectés.

Les données de la vue « **Services** » sont les suivantes :

Port	Indique le port et le protocole utilisés par le service (exemple : 80/tcp).
Nom du service	Indique le nom du service (exemple : lighthhtpd).
Service	Indique le nom du service en incluant son numéro de version (exemple : lighthhtpd_1.4.28).
Détails	Donne un complément d'information sur le service détecté.
Famille	Famille du service (exemple : Web server).

Vue « Informations»

Cet onglet décrit les informations liées à une machine donnée.

Les données de la vue « **Informations** » sont les suivantes :

Id	Identifiant unique du logiciel ou du système d'exploitation détecté.
Nom	Nom du logiciel ou du système d'exploitation détecté.
Famille	Famille à laquelle est attaché le logiciel détetcé (Exemple : Operating System).
Niveau	Indique le niveau de l'alarme associée à la dévouverte de ce logiciel.
Détecté	Date et heure de détection du logiciel ou du système d'exploitation.
Détails	Nom et version du logiciel ou du système d'exploitation détecté (exemple : Microsoft_Windows_Seven_SP1).

Menu contextuel

Un clic droit sur le nom donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

Vue « Historique des réputations»

Cette vue présente sous forme graphique l'évolution de réputation de la machine sélectionnée et l'impact des différents critères entrant dans le calcul de ce score (alarmes, résultats d'analyse sandboxing et d'analyse antivirale).

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.

Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.

Les Interactions

Un clic gauche sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.

En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.

L'onglet "Historique"

Cette vue présente sous forme graphique l'évolution de réputation de la machine sélectionnée (réputation moyenne et réputation maximum).

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.
Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.
Imprimer	Ce bouton permet d'afficher la courbe en plein écran afin de l'envoyer en impression (bouton **Imprimer**).

Les Interactions

Un clic gauche sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.

En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.

Services Web

L'onglet "Nombre de connexions par service Web"

Cette courbe présente l'évolution sur les 10 dernières minutes du nombre de connexions réalisées pour chacun des services Web utilisés dans la configuration du firewall.

L'onglet "Débit entrant par service Web"

Cette courbe présente l'évolution sur les 10 dernières minutes de la bande passante entrante consommée par chacun des services Web utilisés dans la configuration du firewall.

L'onglet "Débit sortant par service Web"

Cette courbe présente l'évolution sur les 10 dernières minutes de la bande passante sortante consommée par chacun des services Web utilisés dans la configuration du firewall.

Utilisateurs

L'onglet "Temps réel"

L'écran se compose de 2 vues :

- Une vue qui liste les utilisateurs authentifiés sur le firewall.
- Une vue qui liste les Connexions, Vulnérabilités, Applications, Services et Informations en rapport avec l'utilisateur sélectionné.

Vue « Utilisateurs»

Cette vue permet de visualiser tous les utilisateurs authentifiés sur le firewall. Une ligne représente un utilisateur.

Les données de la vue « **Utilisateurs** » sont les suivantes :

Nom	Nom de l'utilisateur.
Adresse IP	Adresse IP de la machine sur laquelle est connecté l'utilisateur.
Annuaire	Nom de l'annuaire LDAP utilisé pour authentifier l'utilisateur.
Groupe	Liste des groupes auxquels appartient l'utilisateur.
Délai d'expiration	Durée d'authentification restante pour la session de l'utilisateur
Méthode d'auth.	Méthode ayant servi à l'authentification de l'utilisateur (Exemple : SSL)
Vérification des postes clients (ZTNA)	Cette colonne indique le statut du client par rapport à la politique de vérification des machines / utilisateurs. Quatre valeurs sont possibles : • **N/A** : lorsque la méthode d'authentification n'est pas liée au VPN SSL, • **Désactivé** : lorsqu'aucune politique de vérification du poste client / utilisateur n'est définie, • **Non vérifié** : cette valeur est affichée lorsque le mode permissif a été activé (case **Autoriser l'établissement de tunnels pour des clients non compatibles avec ZTNA** cochée) et que le client VPN SSL utilisé pour établir le tunnel n'est pas compatible avec la vérification du poste client / utilisateur (client VPN SSL tiers ou version SN SSL VPN Client non compatible), • **Conforme** : lorsque le poste client est conforme aux critères définis dans la politique de vérification du poste client / utilisateur.
Mot de passe à usage unique	Une coche verte indique que l'utilisateur a utilisé un mot de passe TOTP.
Multi-utilisateur	Indique si la machine sur laquelle est connecté l'utilisateur est une machine de type multi-utilisateur (exemple : un serveur TSE).

Administrateur	Précise si l'utilisateur a des droits d'administration sur le firewall.
Parrain	Lorsque l'utilisé s'est connecté par la méthode Parrainage, cette colonne indique le nom de la personne ayant validé la demande de connexion.
VPN SSL Portail	Une coche verte dans cette case indique que l'utilisateur est autorisé à se connecter au portail VPN SSL pour accéder à des serveurs Web.
VPN SSL Portail (Applet Java)	Une coche verte dans cette case indique que l'utilisateur est autorisé à se connecter au portail VPN SSL pour accéder à des serveurs applicatifs via un applet Java.
VPN SSL	Une coche verte dans cette case indique que l'utilisateur est autorisé à établir un tunnel VPN SSL à l'aide de SN SSL VPN Client.
VPN IPsec	Une coche verte dans cette case indique que l'utilisateur est autorisé à établir un ou des tunnels VPN IPsec.

Menu contextuel

Un clic droit sur le nom d'utilisateur donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Déconnecter cet utilisateur,
- Afficher les détails de la machine.

La barre d'actions

Vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (Nouveau filtre) permet de réinitialiser le filtre en supprimant la sélection de critères.

Filtrer	Cliquez sur ce bouton pour :
	• Sélectionner des critères de filtrage (**Critère de recherche**). Pour la vue "**utilisateurs**", ces critères sont les suivants :
	  ◦ Par plage d'adresses ou par adresse IP (grisé si un utilisateur a été sélectionnée dans la vue "utilisateurs").
	  ◦ Par annuaire (permet d'affiner le filtrage lorsque plusieurs annuaires LDAP sont définis sur le firewall).
	  ◦ Par méthode d'authentification.
	  ◦ Par utilisation de mot de passe à usage unique en choisissant **Code TOTP utilisé** ou **Pas de code TOTP utilisé**.
	• Enregistrer en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après (**Enregistrer le filtre courant**). Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
	• **Supprimer le filtre courant**.

Réinitialiser	Ce bouton permet d'annuler l'action du filtre en cours d'utilisation. S'il s'agit d'un filtre personnalisé enregistré, cette action ne supprime pas le filtre .
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille. Lorsqu'un filtre est appliqué, seuls les résultats correspondant à ce filtre sont exportés.
Configurer l'authentification	Ce lien permet d'accéder directement à la configuration de l'authentification (module **Configuration** > **Utilisateurs** > **Authentification**).
Réinitialiser l'affichage des colonnes	Ce bouton permet de réinitialiser la largeur des colonnes et de n'afficher que les colonnes proposées par défaut à la première ouverture de cette fenêtre de supervision.

Panneau « FILTRES »

Vous pouvez ajouter un critère en glissant la valeur depuis un champ des résultats dans le panneau.

Vue « Connexions »

Cette vue permet de visualiser toutes les connexions détectées par le firewall pour un utilisateur sélectionné. Une ligne représente une connexion. Les données disponibles pour la vue « **Connexions** » sont les suivantes :

Date	Indication de la date et de l'heure de connexion de l'objet.
Connexion	Identifiant de la connexion
Connexion parente	Certains protocole peuvent générer des connexions "filles" (exemple : FTP) et, dans ce cas de figure, cette colonne référence l'identifiant de la connexion parente.
Protocole	Protocole de communication utilisé pour la connexion.
Utilisateur	Utilisateur connecté sur la machine (s'il existe).
Source	Adresse IP de la machine à l'origine de la connexion.
Nom de la source	Nom de l'objet (s'il existe) correspondant à la machine source.
Adresse MAC source	Adresse MAC de l'objet à l'origine de la connexion.
Port source	Indication du N° de port source utilisé pour la connexion.
Nom du port source	Nom de l'objet correspondant au port source.
Destination	Adresse IP de la machine vers laquelle la connexion a été établie.
Nom de destination	Nom de l'objet (s'il existe) vers lequel une connexion a été établie.
Port de destination	Indication du N° de port de destination utilisé pour la connexion.
Nom du port dest.	Nom de l'objet correspondant au port destination.
Interf. source	Nom de l'interface du firewall sur laquelle la connexion s'est établie.
Interf. dest.	Nom de l'interface de destination utilisée par la connexion sur le firewall.

Débit moyen	Valeur moyenne de bande passante utilisée par la connexion sélectionnée.
Envoyé	Nombre d'octets envoyés au cours de la connexion.
Reçu	Nombre d'octets reçus au cours de la connexion.
Durée	Temps de la connexion.
Dernière utilisation	Temps écoulé depuis le dernier échange de paquets pour cette connexion.
Routeur	Identifiant attribué par le firewall au routeur utilisé par la connexion
Nom du routeur	Nom du routeur enregistré dans la base objet utilisé par la connexion
Type de règle	Indique s'il s'agit d'une règle locale, globale ou implicite.
Règle	Le nom de l'identifiant de la règle autorisant la connexion
État	Ce paramètre indique le statut de la connexion correspondant par exemple, à son initiation, son établissement ou sa fermeture.
Nom de file d'attente	Nom de la file d'attente QoS utilisée par la connexion.
Nom de la règle	Lorsqu'un nom a été donné à la règle de filtrage par laquelle transite la connexion, ce nom est affiché dans la colonne.
Profil IPS	Affiche le N° du profil d'inspection appelé par la règle ayant filtré la connexion.
Géolocalisation	Affiche le drapeau correspondant au pays de la destination.
Catégorie de réputation	Indique la catégorie de réputation de la machine externe si celle-ci est classifiée. **EXEMPLE** SPAM, Phishing...
Argument	Information complémentaire pour certains protocoles exemple : HTTP).
Opération	Information complémentaire pour certains protocoles exemple : HTTP).

Menu contextuel

Un clic droit sur le nom de la machine source ou de la destination donne accès aux menus contextuels suivants :

- Accéder à la règle de sécurité correspondante.

La barre d'actions

Vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (**Nouveau filtre**) permet de réinitialiser le filtre en supprimant la sélection de critères.

Filtrer	Cliquez sur ce bouton pour :
	• Sélectionner des critères de filtrage (**Critère de recherche**). Pour la vue "**connexions**", ces critères sont les suivants :
	  ◦ Par plage d'adresses ou par adresse IP.
	  ◦ Par interface.
	  ◦ Par interface source.
	  ◦ Par interface destination.
	  ◦ Par port destination.
	  ◦ Par protocole.
	  ◦ Par utilisateur (grisé si une machine a été sélectionnée dans la vue "machines").
	  ◦ Pour une valeur de données échangées supérieure à la valeur précisée à l'aide du curseur.
	  ◦ Selon la dernière utilisation de la connexion (seuls les enregistrement dont la dernière utilisation est inférieure à la valeur précisée sont affichés).
	  ◦ Par nom de règle.
	  ◦ Par profil IPS.
	  ◦ Par origine ou destination géographique.
	  ◦ Si la case **Voir toutes les connexions (connexions closes, réinitialisées, ...)** est cochée, l'ensemble des connexions sera affiché dans la grille, quel que soit leur état.
	• Enregistrer en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après (**Enregistrer le filtre courant**). Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
	• **Supprimer le filtre courant**.

Réinitialiser	Ce bouton permet d'annuler l'action du filtre en cours d'utilisation. S'il s'agit d'un filtre personnalisé enregistré, cette action ne supprime pas le filtre .
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille. Lorsqu'un filtre est appliqué, seuls les résultats correspondant à ce filtre sont exportés.
Réinit. colonnes	Ce bouton permet de ne réafficher que les colonnes proposées par défaut à l'ouverture de la fenêtre de supervision des machines.

Panneau « FILTRAGE SUR »

Vous pouvez ajouter un critère en glissant la valeur depuis un champ des résultats dans le panneau.

Vue « Vulnérabilités »

Cet onglet décrit les vulnérabilités détectées sur la machine de connexion de l'utilisateur sélectionné.

Les données de la vue « **Vulnérabilités** » sont les suivantes :

Identifiant	Identifiant de la vulnérabilité.
Nom	Indication du nom de la vulnérabilité.
Famille	Nombre de machines affectées.
Sévérité	Indication du niveau de sévérité de la/les machine(s) concernée(s) par la vulnérabilité. Il existe 4 niveaux de sévérité : "**Faible**", "**Modéré**", "**Elevé**", "**Critique**".
Exploit	L'accès peut s'effectuer en local ou à distance (par le réseau). Il permet d'exploiter la vulnérabilité.
Solution	Indique si oui ou non il y a une solution proposée.
Niveau	Indique le niveau de l'alarme associée à la découverte de cette vulnérabilité.
Port	Indique le port réseau sur lequel la machine est vulnérable (exemple : 80 pour un serveur Web vulnérable).
Service	Indique le nom du programme vulnérable (exemple : lighthttpd_1.4.28)
Détecté	Indique la date à laquelle la vulnérabilité a été détectée sur la machine
Détails	Donne un complément d'information sur la vulnérabilité.

Menu contextuel

Un clic droit sur le nom de la vulnérabilité donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

Vue « Applications»

Cet onglet décrit les applications détectées sur la machine de connexion de l'utilisateur sélectionné.

Les données de la vue « **Applications** » sont les suivantes :

Nom du produit	Nom de l'application.
Famille	Famille de l'application (exemple : Web client).
Détails	Nom complet de l'application incluant son numéro de version.

Menu contextuel

Un clic droit sur le nom du produit donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

Vue « Services»

Cet onglet décrit les services détectés sur la machine de connexion de l'utilisateur sélectionné.

Les données de la vue « **Services** » sont les suivantes :

Port	Indique le port et le protocole utilisés par le service (exemple : 80/tcp).

Nom du service	Indique le nom du service (exemple : lighthhtpd).
Service	Indique le nom du service en incluant son numéro de version (exemple : lighthhtpd_1.4.28).
Détails	Donne un complément d'information sur le service détecté.
Famille	Famille du service (exemple : Web server).

Vue « Informations»

Cet onglet décrit les informations liées à la machine sur laquelle l'utilisateur sélectionné est connecté.

Les données de la vue « **Informations** » sont les suivantes :

Id	Identifiant unique du logiciel ou du système d'exploitation détecté.
Nom	Nom du logiciel ou du système d'exploitation détecté.
Famille	Famille à laquelle est attaché le logiciel détecté (Exemple : Operating System).
Niveau	Indique le niveau de l'alarme associée à la découverte de ce logiciel.
Détecté	Date et heure de détection du logiciel ou du système d'exploitation.
Détails	Nom et version du logiciel ou du système d'exploitation détecté (exemple : Microsoft_Windows_Seven_SP1).

Menu contextuel

Un clic droit sur le nom du produit donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe.

L'onglet "Historique"

Cet onglet présente des graphiques historiques sur la répartition des authentifications selon leur type :

- Total,
- Portail captif,
- Console,
- IPsec,
- SSL VPN,
- TOTP,
- Interface Web d'administration.

Les actions

Échelle de temps	Ce champ permet le choix de l'échelle de temps : dernière heure, vue par jour, 7 derniers jours et les 30 derniers jours. • La dernière heure est calculée depuis la minute précédant celle en cours. • La vue par jour couvre la journée entière, sauf pour le jour en cours où les données courent jusqu'à la minute précédente. • Les 7 et les 30 derniers jours concernent la période achevée la veille à minuit. Le bouton permet de rafraîchir les données affichées.
Afficher le	Dans le cas d'une vue par jour, ce champ propose un calendrier permettant de choisir la date.

Les Interactions

- Un clic sur l'un des indicateurs référencés dans la légende permet de masquer / afficher les données correspondantes sur le graphique.
- En survolant une courbe à l'aide de la souris, la valeur de l'indicateur et l'heure de mesure correspondante sont affichées dans une info bulle.
- Un clic sur le bouton présent à droite de chaque graphique met en page les données du graphique pour un envoi en impression. Un commentaire peut être ajouté avant de confirmer l'impression (bouton **Imprimer**).

Connexions

La grille "Temps réel"

Cette vue permet de visualiser toutes les connexions détectées par le firewall. Une ligne représente une connexion. Les données disponibles pour la vue « **Connexions** » sont les suivantes :

Date	Indication de la date et de l'heure de connexion de l'objet.
Connexion	Identifiant de la connexion
Connexion parente	Certains protocole peuvent générer des connexions "filles" (exemple : FTP) et, dans ce cas de figure, cette colonne référence l'identifiant de la connexion parente.
Protocole	Protocole de communication utilisé pour la connexion.
Protocole Ethernet	Lorsque le protocole de communication appartient à la liste suivante : • PROFINET-RT, • IEC61850-GOOSE, • IEC61850-SV.
Utilisateur	Utilisateur connecté sur la machine (s'il existe).
Source	Adresse IP de la machine à l'origine de la connexion.
Nom de la source	Nom de l'objet (s'il existe) correspondant à la machine source.

Adresse source multi-homing (SCTP)	Adresse IP présentée par la machine à l'origine d'une connexion SCTP. Pour rappel, un équipement dialoguant en SCTP peut disposer de plusieurs adresses IP (*multi-homing*).
Adresse MAC source	Adresse MAC de l'objet à l'origine de la connexion.
Port source	Indication du N° de port source utilisé pour la connexion.
Nom du port source	Nom de l'objet correspondant au port source.
Destination	Adresse IP de la machine vers laquelle la connexion a été établie.
Nom de destination	Nom de l'objet (s'il existe) vers lequel une connexion a été établie.
Adresse MAC destination	Adresse MAC de la machine vers laquelle la connexion a été établie .
Adresse dest. multi-homing (SCTP)	Adresse IP de la machine destinataire d'une connexion SCTP. Pour rappel, un équipement dialoguant en SCTP peut disposer de plusieurs adresses IP (*multi-homing*).
Port destination	Indication du N° de port de destination utilisé pour la connexion.
Nom du port dest.	Nom de l'objet correspondant au port destination.
Interf. source	Nom de l'interface du firewall sur laquelle la connexion s'est établie.
Interf. dest.	Nom de l'interface de destination utilisée par la connexion sur le firewall.
Débit moyen	Valeur moyenne de bande passante utilisée par la connexion sélectionnée.
Envoyé	Nombre d'octets envoyés au cours de la connexion.
Reçu	Nombre d'octets reçus au cours de la connexion.
Durée	Temps de la connexion.
Dernière utilisation	Temps écoulé depuis le dernier échange de paquets pour cette connexion.
ID de routeur	Identifiant attribué par le firewall au routeur utilisé par la connexion.
Nom de passerelle	Nom de la passerelle (composant le routeur dont l'identifiant est précisé dans la colonne précédente) utilisée par la connexion.
Statut de passerelle	État actuel de la passerelle utilisée pour la connexion.
Type de règle	Indique s'il s'agit d'une règle locale, globale ou implicite.
Règle	Le nom de l'identifiant de la règle autorisant la connexion.
État	Ce paramètre indique le statut de la connexion correspondant par exemple, à son initiation, son établissement ou sa fermeture.
Nom de file d'attente	Nom de la file d'attente QoS utilisée par la connexion.
Nom de la règle	Lorsqu'un nom a été donné à la règle de filtrage par laquelle transite la connexion, ce nom est affiché dans la colonne.
Profil IPS	Affiche le N° du profil d'inspection appelé par la règle ayant filtré la connexion.
Géolocalisation	Affiche le drapeau correspondant au pays de la destination.

Catégorie de réputation	Indique la catégorie de réputation de la machine externe si celle-ci est classifiée. **EXEMPLE** SPAM, Phishing...
Argument	Information complémentaire pour certains protocoles (exemple : HTTP).
Opération	Information complémentaire pour certains protocoles (exemple : HTTP).

Menu contextuel

Un clic droit sur le nom ou l'adresse IP d'une machine source ou destination donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Afficher les détails de la machine,
- Réinitialiser son score de réputation,
- Ajouter la machine à la base Objet et / ou l'ajouter dans un groupe.

Un clic droit sur le nom d'utilisateur donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Déconnecter cet utilisateur,
- Afficher les détails de la machine.

Un clic droit sur le nom de la source ou le nom de destination donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Afficher les détails de la machine,
- Réinitialiser le score de réputation de cet objet,
- Placer cet objet en liste noire (Pour 1 minute, Pour 5 minutes, Pour 30 minutes ou Pour 3 heures),
- Ajouter la machine à la base Objet et/ou l'ajouter dans un groupe,
- Accéder à la règle de sécurité correspondante.

Un clic droit sur le nom de la source ou le nom de destination donne accès aux menus contextuels suivants :

- Accéder à la règle de sécurité correspondante,
- Ajouter le service à la base Objet et/ou l'ajouter dans un groupe.

Un clic droit sur les autres colonnes donne accès au menu contextuel suivant :

- Accéder à la règle de sécurité correspondante.

La barre d'actions

Vous pouvez combiner plusieurs critères de recherche. Ces critères doivent être remplis conjointement pour être affichés, car les critères de recherche se cumulent.

Cette combinaison de critères de recherche peut alors être enregistrée en tant que « filtre ». Ceux-ci sont gardés en mémoire et peuvent être réinitialisés via le module **Préférences** de l'interface d'administration.

(menu déroulant Filtres)	Sélectionnez un filtre pour lancer la recherche correspondante. La liste propose les filtres enregistrés au préalable et pour certaines Vues, des filtres prédéfinis. La sélection de l'entrée (Nouveau filtre) permet de réinitialiser le filtre en supprimant la sélection de critères.

Filtrer	Cliquez sur ce bouton pour :
	• Sélectionner des critères de filtrage (**Critère de recherche**). Pour la vue "**connexions**", ces critères sont les suivants :
	  ◦ Par plage d'adresses, par adresse IP ou par machine source.
	  ◦ Par interface.
	  ◦ Par nom de passerelle.
	  ◦ Par état de passerelle.
	  ◦ Par interface source.
	  ◦ Par interface destination.
	  ◦ Par port destination.
	  ◦ Par protocole.
	  ◦ Par utilisateur (grisé si une machine a été sélectionnée dans la vue "machines").
	  ◦ Pour une valeur de données échangées supérieure à la valeur précisée à l'aide du curseur.
	  ◦ Selon la dernière utilisation de la connexion (seuls les enregistrement dont la dernière utilisation est inférieure à la valeur précisée sont affichés).
	  ◦ Par nom de règle.
	  ◦ Par profil IPS.
	  ◦ Par origine ou destination géographique.
	  ◦ Lorsque la case **Afficher toutes les connexions TCP/UDP (connexions fermées, réinitialisées ...)** est cochée seule, le filtre affiche l'ensemble des connexions, quel que soit leur état, ainsi que les associations en cours d'utilisation.
	  ◦ Lorsque la case **Afficher toutes les associations SCTP (initialisées, en cours d'utilisation, en cours de fermeture et fermées)** est cochée seule, le filtre affiche l'ensemble des associations SCTP, quel que soit leur état, ainsi que les connexions en cours d'utilisation.
	  ◦ Lorsque les deux cases **Afficher toutes les connexions TCP/UDP (connexions fermées, réinitialisées ...)** et **Afficher toutes les associations SCTP (initialisées, en cours d'utilisation, en cours de fermeture et fermées)** sont cochées, le filtre affiche l'ensemble des connexions et associations connues du firewall, quel que soit leur état.
	  ◦ Lorsque aucune des deux cases **Afficher toutes les connexions TCP/UDP (connexions fermées, réinitialisées ...)** et **Afficher toutes les associations SCTP (initialisées, en cours d'utilisation, en cours de fermeture et fermées)** n'est cochée, le filtre affiche uniquement les connexions et associations en cours d'utilisation.
	• Enregistrer en tant que filtre personnalisé, les critères définis dans le panneau Filtrage décrit ci-après (**Enregistrer le filtre courant**). Vous pouvez enregistrer un nouveau filtre par le bouton "Enregistrer sous" sur la base d'un filtre existant ou d'un filtre prédéfini proposé dans certaines Vues. Une fois un filtre enregistré, il est automatiquement proposé dans la liste des filtres.
	• **Supprimer le filtre courant**.

Réinitialiser	Ce bouton permet d'annuler l'action du filtre en cours d'utilisation. S'il s'agit d'un filtre personnalisé enregistré, cette action ne supprime pas le filtre .
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.

Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille. Lorsqu'un filtre est appliqué, seuls les résultats correspondant à ce filtre sont exportés.
Réinitialiser l'affichage des colonnes	Ce bouton permet de réinitialiser la largeur des colonnes et de n'afficher que les colonnes proposées par défaut à la première ouverture de cette fenêtre de supervision.

Panneau « FILTRAGE SUR »

Vous pouvez ajouter un critère en glissant la valeur depuis un champ des résultats dans le panneau.

SD-WAN

L'onglet "Temps réel"

Cette grille reprend la liste des routeurs utilisés dans la configuration du firewall : objets routeurs, passerelle par défaut, routeurs configurés dans des règles de filtrage (PBR : Policy Based Routing) et routes de retour.

La barre d'actions

- Le champ **Rechercher...** permet de filtrer la grille sur le nom d'un routeur ou d'une passerelle. Lorsque le filtrage est réalisé sur le nom d'une passerelle, le routeur utilisant cette passerelle est affiché dans la grille.
- Le bouton permet de masquer toutes les passerelles composant les objets routeurs utilisés dans la configuration et de n'afficher que les informations concernant ces routeurs.
- Le bouton permet d'afficher toutes les passerelles qui composent les objets routeurs ainsi que l'ensemble des informations liées aux routeurs et aux passerelles.
- Le bouton **Actualiser** permet de rafraîchir les données affichées dans la grille.
- Le bouton **Exporter les résultats** permet de télécharger un fichier au format CSV contenant l'ensemble de ces informations.
- Le lien **Configurer le routage** permet d'accéder directement à la configuration du routage (module **Configuration** > **Réseau** > **Routage**).
- Le bouton **Réinitialiser l'affichage des colonnes** permet de réinitialiser la largeur des colonnes et de n'afficher que les colonnes proposées par défaut à la première ouverture de cette fenêtre de supervision.

La grille

Les données disponibles pour la grille **Temps Réel** sont les suivantes :

Routeurs / Passerelles	Concerne les routeurs et les passerelles. Nom du routeur ou d'une passerelle entrant dans la composition d'un routeur.

Type	Concerne uniquement les passerelles. Indique dans quel type de route une passerelle est utilisée. Les valeurs possibles sont : • **Routage par politique**, • **Route par défaut**.
État	Concerne les routeurs et les passerelles. L'état d'un routeur est déterminé par l'état de ses passerelles. Les valeurs possibles pour une passerelle principale sont les suivantes : • **Actif** : passerelle en état optimal et en cours d'utilisation, • **Actif** : passerelle principale en état dégradé et en cours d'utilisation, • **Injoignable** : passerelle principale ne répondant pas aux tests de connexion, • **Non supervisé** : aucun test de connexion n'a encore été effectué pour cette passerelle. Les valeurs possibles pour une passerelle de secours sont les suivantes : • **En veille** : la passerelle de secours est en état optimal ou en état dégradé, • **Injoignable** : la passerelle de secours ne répond pas aux tests de connexion, • **Non supervisé** : aucun test de connexion n'a encore été effectué pour cette passerelle. Les valeurs possibles pour un routeur sont les suivantes : • **Opérationnel** : toutes ses passerelles sont en état **Actif**, • **Opérationnel** : ◦ Au moins l'un de ses passerelles est en état **Actif** et toutes les autres en état **En veille**, ◦ Au moins l'un de ses passerelles est en état **Actif** et toutes les autres dans n'importe quel état, ◦ Toutes ses passerelles sont en état **Actif** ou en état **En veille**, ◦ Au moins une de ses passerelle est en état **En veille.** • **En veille** : toutes les autres combinaisons d'états de passerelles composant le routeur .
Version d'IP	Concerne uniquement les passerelles. Version du protocole IP utilisé sur la passerelle. Les valeurs possibles sont : • [IPv]**4**, • [IPv]**6**.
Adresse IP	Concerne uniquement les passerelles. Adresse IP de la passerelle (n'existe pas pour un routeur).
SLA SD-WAN	Concerne uniquement les routeurs. Indique si un engagement SLA est défini pour le routeur. Les valeurs possibles sont : • **Actif**, • **Inactif**.

Méthode de détection	Concerne uniquement les routeurs. Affiche le type de tests de connexion pour établir l'état d'un routeur. Les valeurs possibles sont : • **ICMP**, • **TCP Probe (*protocole utilisé*)**.
Principal / secours	Concerne uniquement les passerelles. Indique si la passerelle est définie comme passerelle principale ou passerelle de secours au sein du routeur.
Dernière vérification	Concerne uniquement les passerelles. Date et heure du dernier test de connexion de la passerelle.
Latence (ms)	Concerne les routeurs et les passerelles. Pour un routeur : indique le seuil paramétré dans l'objet. Pour une passerelle, indique la latence mesurée lors du dernier test de connexion.
Gigue (ms)	Concerne les routeurs et les passerelles. Pour un routeur : indique le seuil paramétré dans l'objet. Pour une passerelle, indique la gigue mesurée sur une période glissante de 10 minutes.
Perte de paquets	Concerne les routeurs et les passerelles. Pour un routeur : indique le seuil paramétré dans l'objet. Pour une passerelle, indique le taux de perte de paquets mesuré pour une passerelle sur une période glissante de 10 minutes.
Taux d'indisponibilité	Concerne les routeurs et les passerelles. Pour un routeur : indique le seuil paramétré dans l'objet. Pour une passerelle, indique le pourcentage de temps passé en état inactif ou injoignable sur une période glissante de 10 minutes.

Statut SLA	Concerne les routeurs et les passerelles. Indique si l'engagement SLA SD-WAN défini (lorsqu'il est activé dans la définition de l'objet routeur) est respecté pour les passerelles le routeur. L'état SLA d'un routeur est déterminé par l'état SLA de ses passerelles. Les valeurs possibles pour une passerelle sont les suivantes : • **Bon** : la passerelle respecte tous les seuils SLA définis, • **Dégradé** : la passerelle ne respecte pas au moins un des seuils SLA définis, • **Injoignable** : la passerelle ne répond pas aux tests de connexion (ICMP ou TCP Probe selon la Méthode de détection choisie). • **Non supervisé** : aucun test de connexion n'a encore été effectué pour cette passerelle. **NOTE** Lorsque vous survolez l'état SLA d'une passerelle avec votre souris, une fenêtre reprenant les valeurs des différentes métriques mesurées et des seuils définis s'affiche. Associées à un code couleur, les valeurs affichées permettent ainsi d'identifier les métriques responsables de l'état de la passerelle. Les valeurs possibles pour un routeur sont les suivantes : • **Bon** : toutes ses passerelles ont un statut SLA **Bon**. • **Dégradé** : au moins une de ses passerelles a un statut SLA **Dégradé**, quel que soit le statut SLA de ses autres passerelles. • **Injoignable** : toutes les passerelles du routeur ont le statut SLA **Injoignable**. • **Non supervisé** : aucun test de connexion n'a encore été effectué sur les passerelles de ce routeur.
Dernier changement d'état	Concerne uniquement les passerelles. Heure du dernier changement d'état et délai écoulé depuis le dernier changement d'état de la passerelle.
Disponible depuis	Concerne les routeurs et les passerelles. Délai écoulé depuis le dernier changement de disponibilité de la passerelle ou du routeur.
Id. de routeur	Concerne uniquement les passerelles. Identifiant unique de la passerelle.
Répartition	Concerne uniquement les passerelles. Pourcentage d'utilisation de la passerelle au sein de l'objet routeur lorsque de la répartition de charge est définie.

L'onglet "Graphe temps réel"

Lors du premier accès à l'onglet **Historique**, aucune courbe n'est affichée par défaut : sélectionnez une passerelle dans la liste déroulante **Choisir une passerelle** pour afficher ses graphes.

Deux graphes sont affichés pour la passerelle sélectionnée :

- Latence mesurée lors des 10 dernières minutes,
- État sur la même période.

L'onglet "Historique"

Lors du premier accès à l'onglet **Historique**, aucune courbe n'est affichée par défaut.

1. Sélectionnez un routeur dans la liste déroulante **Choisir un routeur**
   La première passerelle (par ordre alphabétique) composant ce routeur est alors automatiquement sélectionnée et les courbes relatives aux métriques de cette passerelle sont affichées.
2. Si vous souhaitez afficher les courbe d'une autre passerelle, ou afficher les courbe d'une autre passerelle en plus de celle sélectionnée par défaut, utilisez la liste déroulante **Choisir des passerelles (max. 10)**.
   Un maximum de 10 passerelles peuvent être sélectionnées simultanément.

Trois graphes sont affichés pour chaque passerelle sélectionnée :

- Gigue et latence,
- Taux de perte de paquets et taux d'indisponibilité,
- Répartition des états pour la passerelle : pourcentage de temps passé dans chacun des états possibles (Opérationnel, Dégradé et Injoignable).

Routage multicast dynamique

Selon son positionnement dans l'infrastructure multicast, le firewall peut être identifié en tant que :

- *First Hop Router* (*FHR*) : le firewall est connecté à une source multicast et envoie son flux multicast vers le RP (PIM-SM) ou vers la destination (PIM-SSM).
- *Middle Hop Router* (*MHR*) : le firewall joue un rôle intermédiaire et transmet le flux multicast.
- *Last Hop Router* (*LHR*) : le firewall est connecté à des récepteurs multicast et envoie au RP les demandes d'abonnement / désabonnement de ces récepteurs.

Les informations affichées dans les grilles décrites ci-dessous diffèrent selon le positionnement du firewall pour un flux multicast donné.

Le firewall peut également être amené à jouer des rôles spécifiques dans l'infrastructure multicast :

- *Rendez-vous Point* (RP) : le RP est sollicité pour établir la route jusqu'à la source multicast (*upstream*), puis transférer les flux reçus vers les récepteurs (*downstream*).
- *BootStrap router*) (BSR) : le BSR est élu parmi tous les candidats BSR. Une fois élu, il récolte les candidatures pour le rôle de RP, puis diffuse aux autres routeurs la table des associations groupes multicast / RP.

Pour plus d'informations sur ces rôles et les mécanismes d'élections, veuillez consulter module de configuration du Routage Multicast Dynamique.

La barre d'actions

- : cliquez sur ce bouton pour rafraîchir les données affichées dans les grilles de supervision du routage multicast dynamique.
- : cliquez sur ce bouton pour modifier la fréquence de rafraîchissement (en secondes) des informations affichées dans les grilles de supervision du routage multicast dynamique. La valeur par défaut est de 30 secondes.

- : cliquez sur ce bouton pour réduire toutes les grilles de supervision présentes sur l'écran.
- : cliquez sur ce bouton pour déplier toutes les grilles de supervision présentes sur l'écran.
- : cliquez sur ce bouton pour accéder directement au module de configuration du routage multicast dynamique (**Configuration** > **Réseau** > **Routage Multicast**).

Les grilles

Routes Multicast

Cette grille affiche la table de routage multicast apprise par le firewall. Toutes les routes listées dans cette grille ne sont pas nécessairement utilisées par le firewall.

Source	Ce champ précise l'adresse IP ou l'objet machine représentant l'adresse de la source du flux multicast pour la route affichée. La valeur de cette source est précisée lorsque le firewall remplit une des conditions suivantes : • Il est placé en position de FHR par rapport à la source, • Il est élu dans le rôle de RP (PIM-SM), • Il est positionné sur la route du *Shortest Path Tree* (*SPT*)lorsque cette route est établie. La valeur *any* est affichée lorsque le firewall remplit une des conditions suivantes : • Il est RP pour le groupe multicast et il est informé d'une demande d'abonnement, • Il est positionné en LHR d'un récepteur (PIM-SM), • Il est placé sur la route entre le LHR et le RP.
Groupe	Précise l'adresse IP ou l'objet machine représentant l'adresse IP du groupe multicast concerné par la route.
Adresse du RP	Protocole PIM-SM : Précise l'adresse ou l'objet machine représentant l'adresse IP du RP en charge de cette route multicast. Ce nom est affiché en gras lorsque le routeur supervisé est lui-même élu RP de la route multicast sélectionnée. Protocole PIM-SSM : Aucune adresse n'est précisée car le rôle de RP n'existe pas dans ce protocole.

Drapeaux	Plusieurs valeurs sont possibles : • SG : lorsque la source est identifiée pour la route multicast, • CACHE : lorsque la route est activée sur le firewall supervisé, • SPT (uniquement en PIM-SM) : ◦ Lorsque le firewall est RP, ce drapeau indique alors que la SPT est disponible, ◦ Lorsque le firewall est positionné comme LHR : ce drapeau indique que le flux emprunte la SPT, • WC-RPT: lorsque le firewall est positionné sur la route du LHR (inclus) vers le RP (inclus), • ASSERTED : lorsque le firewall gagne le mécanisme de *PIM assert* permettant d'éliminer les duplications de flux sur un segment partagé. Notez que ces différentes valeurs peuvent être combinées entre elles.
Détails	En survolant cette zone, vous affichez les délais d'expiration en cours pour les mécanismes caractéristiques du protocole PIM SM. Les délais affichés (expiration de la route [*expiry timer*], fin de la transmission d'un flux lorsque celui-ci n'a plus de récepteurs déclarés [*register suppression*]...) dépendent de la position du firewall dans l'infrastructure multicast (*First Hop*, *Middle Hop*, *Last Hop*) et de son ou ses rôles (RP, BSR). La RFC 4601 présente le détail de ces délais d'expiration.

Cliquez sur le symbole "+" d'une route multicast pour obtenir plus de détails :

Interface	Cette colonne liste les interfaces participant à la route multicast sélectionnée.
Incoming(IIF)	Pour une route multicast donnée, l'interface présentant une coche est l'interface par laquelle le flux multicast arrive sur le firewall.
Liste des interfaces sortantes (OIL)	• Joined : une coche indique que cette interface est intervenue pour une demande d'abonnement au flux multicast. • Pruned : une coche indique que cette interface est intervenue pour une demande de désabonnement au flux multicast. • Leaf : une coche indique que cette interface est directement connectée à un récepteur. • Asserted : une coche indique que cette interface intervient dans le mécanisme de *PIM assert*. • Outgoing : une coche indique que cette interface est utilisée pour transmettre le flux multicast.

Membres des groupes IGMP

NOTE
Des informations sont affichées dans cette grille uniquement lorsque le firewall se situe en tant que *Last Hop Router* pour un flux multicast.

Un clic sur le titre d'une colonne permet de classer les informations de la grille selon cette valeur.

Cliquez sur le symbole "+" d'un groupe multicast pour obtenir la liste des récepteurs composant ce groupe:

Groupe	Adresse ou objet machine représentant l'adresse IP du groupe pour lequel la requête IGMP a été initiée.
Source	Adresse ou objet machine représentant l'adresse IP de la source du flux multicast pour le groupe considéré.
Récepteur	Adresse ou objet machine représentant l'adresse IP de l'initiateur de la requête IGMP.
Interface	Affiche l'interface par laquelle le firewall a reçu la requête IGMP.
Délai d'expiration	Lorsque cette valeur est atteinte, cela signifie que le récepteur concerné n'est plus à l'écoute du flux IGMP.

Interfaces / Voisins

Cette grille recense l'ensemble des interfaces du firewall participant au routage multicast ainsi que les voisins de ces interfaces. Un voisin est un autre équipement réseau (routeur, firewall) utilisant le protocole PIM et directement connecté à l'interface listée.

Certaines informations ne sont disponibles que pour les interfaces, d'autres pour les interfaces et ses voisins.

Interface / Voisin	Affiché uniquement pour l'interface. Nom de l'interface du firewall participant au routage multicast. Le nombre de voisins de cette interface est précisé entre parenthèses. Un clic sur le symbole "+" de l'interface permet d'obtenir le détail de ses voisins.
État	Affiché uniquement pour l'interface. Indique si l'interface est active ou non.
Groupe	Affiché uniquement pour l'interface. Nombre de groupes multicast distincts sollicités par des récepteurs rattachés à l'interface.
Adresse	Affiché pour l'interface et pour ses voisins. Adresse ou objet machine représentant l'adresse IP de l'interface ou du voisin de l'interface.
Priorité du DR	Affiché pour l'interface et pour ses voisins. Indique la priorité affectée à l'interface ou à son voisin dans le cadre de l'élection en tant que DR.
DR	Affiché pour l'interface et pour ses voisins. Indique si l'interface ou le voisin de l'interface est élu comme DR. Lorsque la coche est suivi d'un astérisque, il s'agit d'une interface du routeur supervisé qui est élue DR.
Demandeur IGMP	Affiché pour l'interface et pour ses voisins. Une coche indique que l'interface ou son voisin joue le rôle de demandeur IGMP, chargé de contacter les récepteurs afin de savoir s'ils sont encore à l'écoute de certains flux multicast.
Depuis	Indique le temps écoulé depuis la découverte du voisin.
Expire dans	Temps restant avant la disparition du voisin si celui-ci n'a pas envoyé de message HELLO.

Rendez-vous Points (RP) / Candidats (C-RP)

> **NOTE**
> Cette grille n'affiche des données que lorsque le protocole PIM SM est utilisé (la notion de RP n'existant pas dans le protocole PIM SSM).

Groupe Multicast	Indique l'adresse ou l'objet machine / réseau représentant l'adresse IP du groupe multicast géré par le RP. Lorsque le RP associé est un RP dynamique, le nombre de candidats à l'élection de RP est indiqué entre parenthèses.
Adresse du RP > C-RP	Sur une ligne principale, ce champ indique l'adresse ou l'objet machine représentant l'adresse IP du RP désigné (RP statique) ou élu (RP dynamique) pour le groupe multicast affiché. Dans le cas d'un RP dynamique, un clic sur le symbole "+" affiche la liste des candidats à l'élection de RP pour le groupe multicast considéré.
Type	Indique s'il s'agit d'un RP statique ou dynamique (élu).
Priorité	Affiche la priorité attribuée au RP ou au candidat RP.
Hold-time	Intervalle de temps entre deux annonces du candidat RP à destination du BSR.
Expire dans	Délai d'expiration de la candidature si le candidat n'émet plus d'annonce à destination du BSR.

Routeurs Bootstrap (BSR) / Candidats voisins (C-BSR)

> **NOTE**
> Cette grille n'affiche des données que lorsque le protocole PIM SM est utilisé, la notion de BSR n'existant pas dans le protocole PIM SSM.

Adresse du BSR / C-BSR	Référence l'adresse ou l'objet machine représentant l'adresse IP du BSR ainsi que les candidats (C-BSR) annoncés par les voisins du firewall.
Priorité	Affiche la priorité affectée au C-BSR pour l'élection.
Longueur du masque de hachage	Affiche la taille (nombre de bits significatifs) utilisée pour la répartition des groupes multicast entre les DR en cas de recouvrement. Le masque est positionné à 30 par défaut.
Expire dans	Il s'agit du temps restant jusqu'à une prochaine élection en cas de perte du BSR. Cette valeur n'est affichée que pour le BSR élu.

DHCP

La grille "Temps réel"

Cette grille permet de visualiser l'ensemble des machines ayant obtenu une adresse IP par le serveur DHCP du firewall. Pour chaque machine, les données disponibles pour la vue « **Supervision DHCP** » sont les suivantes :

Adresse IP	Indique l'adresse IP attribuée à la machine. Cette adresse est issue de l'une des plages d'adresses déclarées dans le module **Réseau** > **DHCP**.
État	Indique si l'adresse IP référencée dans la grille est utilisée (active) ou libre (free) au sein de la plage DHCP.
Début du bail	Indique la date et l'heure à laquelle la machine s'est vue attribuer une adresse par le serveur DHCP. Cette information est au format AAAA-MM-JJ HH:MM:SS.
Fin du bail	Indique la date et l'heure à laquelle l'adresse IP attribuée par le serveur DHCP du firewall deviendra de nouveau disponible si aucune demande de renouvellement de bail n'a été effectuée par la machine. La durée du bail peut être personnalisée dans le module **Réseau** > **DHCP** > **Configuration avancée** > **Durée de bail attribuée**. Cette information est au format AAAA-MM-JJ HH:MM:SS.
Adresse MAC	Indique l'adresse MAC de la carte réseau portant l'adresse IP attribuée par le serveur DHCP du firewall.
Nom de machine	Indique le nom de la machine à laquelle l'adresse IP a été attribuée.

Menu contextuel

Un clic droit sur le nom ou l'adresse IP d'une machine source ou destination donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Vérifier cette machine,
- Afficher les détails de la machine,
- Réinitialiser son score de réputation,
- Placer cet objet en liste noire (Pour 1 minute, Pour 5 minutes, Pour 30 minutes ou Pour 3 heures),
- Ajouter la machine à la base Objet et / ou l'ajouter dans un groupe.

La barre d'actions

Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille.
Configurer le service DHCP	Ce lien permet d'accéder directement à la configuration du service DHCP (module **Configuration** > **Réseau** > **DHCP**).
Réinitialiser l'affichage des colonnes	Ce bouton permet de n'afficher que les colonnes proposées par défaut à l'ouverture de la fenêtre de supervision.

Tunnels VPN SSL

La grille "Temps réel"

Cette grille permet de visualiser l'ensemble des machines connectées au firewall par le biais d'un tunnel VPN SSL. Pour chaque machine, les données disponibles pour la vue « **Supervision des tunnels VPN SSL** » sont les suivantes :

Utilisateur	Identifiant de connexion utilisé pour établir le tunnel VPN SSL référencé.
Annuaire	Annuaire dans lequel est défini l'utilisateur connecté.
Adresse IP du client	Adresse IP affectée au poste client pour établir le tunnel VPN SSL (cette adresse appartient au réseau défini dans le module **VPN** > **VPN SSL** > champ **Réseau assigné aux clients (TCP)** ou **champ Réseau assigné aux clients (UDP)**.
Version du client	Cette colonne indique la version de SN SSL VPN Client utilisée pour établir le tunnel affiché. La valeur indiquée pour un client VPN SSL tiers ou non compatible est N/A.
Vérification des postes clients (ZTNA)	Cette colonne indique le statut du client par rapport à la politique de vérification des machines / utilisateurs. Trois valeurs sont possibles : • **Désactivé** : lorsqu'aucune politique de vérification du poste client / utilisateur n'est définie, • **Non vérifié** : cette valeur est affichée lorsque le mode permissif a été activé (case **Autoriser l'établissement de tunnels pour des clients non compatibles avec ZTNA** cochée) et que le client VPN SSL utilisé pour établir le tunnel n'est pas compatible avec la vérification du poste client / utilisateur (client VPN SSL tiers ou version SN SSL VPN Client non compatible), • **Conforme** : lorsque le poste client est conforme aux critères définis dans la politique de vérification du poste client / utilisateur.
Adresse IP réelle	Adresse IP affectée au réseau local du poste client connecté.
Reçu	Nombre d'octets reçus par le serveur VPN SSL (firewall) dans le tunnel considéré.
Envoyé	Nombre d'octets émis par le serveur VPN SSL. (firewall) dans le tunnel considéré.
Durée	Temps écoulé depuis l'établissement du tunnel. Cette valeur est exprimée en hh:mm:ss.
Port	Port utilisé par le client pour établir le tunnel.

Menu contextuel

Un clic droit sur le nom d'utilisateur donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans les traces,
- Déconnecter cet utilisateur.

Un clic droit sur l'adresse IP du client VPN ou sur l'adresse IP réelle d'une machine donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Afficher les détails de la machine,
- Réinitialiser le score de réputation de cet objet,
- Placer cet objet en liste noire (Pour 1 minute, Pour 5 minutes, Pour 30 minutes ou Pour 3 heures).

La grille "Informations"

Cette grille liste le nombre de tunnels établis :

- Nombre total de tunnels (UDP + TCP)
- Nombre de tunnels UDP
- Nombre de tunnels TCP

Un message d'avertissement est affiché lorsque le nombre de tunnels établis approche du nombre maximum de tunnels simultanés autorisé (information disponible dans le module VPN SSL).

La barre d'actions

Réinitialiser ce tunnel	Ce bouton permet de forcer la renégociation du tunnel sélectionné. Le client distant est alors déconnecté puis se reconnecte automatiquement.
Actualiser	Ce bouton permet d'actualiser les données présentées à l'écran.
Exporter les résultats	Ce bouton permet de télécharger un fichier au format CSV contenant les informations de la grille.
Configurer le service VPN SSL	Ce lien permet d'accéder directement à la configuration du service VPN SSL (module **Configuration** > **VPN** > **VPN SSL**).
Réinitialiser l'affichage des colonnes	Ce bouton permet de n'afficher que les colonnes proposées par défaut à l'ouverture de la fenêtre de supervision des tunnels.

Tunnels VPN IPsec

Ce module permet de visualiser les tunnels de la politiques IPsec active sur le firewall (tunnels définis à l'aide de l'interface IPsec native ou d'interfaces IPsec virtuelles).

La barre d'actions

Actualiser	Ce bouton permet de rafraîchir les informations affichées dans les grilles.
Configurer le service VPN IPsec	Ce lien permet d'accéder directement à la configuration du service VPN IPsec (module **Configuration** > **VPN** > **VPN IPsec**).

La grille « Politiques »

Les données affichées dans la grille « Politiques » sont classées suivant le type de politique :

- Tunnels site à site,
- Tunnels mobiles,
- Politiques d'exception (bypass).

Ces données sont les suivantes :

Type	Il s'agit du type de politique IPsec : Tunnels site à site, Tunnels mobiles et Politiques d'exception (bypass).
État	Un voyant vert accompagné de la mention OK, ou rouge accompagné de la mention KO, indique l'état des tunnels de la politique concernée.

Nom de règle	Nom donné à la règle IPsec (boite d'édition de la règle > **Paramètres généraux** > **Configuration avancée** > **Nom**).
Source	Nom de l'objet correspondant au réseau local.
Adresse source	Réseau des machines ayant initié le trafic traversant le tunnel IPsec sélectionné (extrémité de trafic).
Masque	Masque réseau associé à l'adresse source.
Passerelle locale	Nom de l'objet correspondant à la passerelle IPsec locale (extrémité locale du tunnel).
Adresse IP passerelle locale	Adresse IP présentée par le firewall local pour établir le tunnel.
Local ID	Identifiant (optionnel) local précisé lors de la création du correspondant. Si rien n'est précisé, il s'agit de l'adresse IP de la passerelle locale.
Passerelle distante	Nom de l'objet correspondant à la passerelle IPsec distante (extrémité distante du tunnel).
Adresse IP passerelle distante	Adresse IP présentée par le firewall distant pour établir le tunnel avec le firewall local.
Correspondant	Nom du correspondant ayant servi à établir le tunnel.
ID du correspondant	Identifiant (optionnel) attribué au correspondant. Si rien n'est précisé, il s'agit de l'adresse IP de la passerelle distante.
Extrémité de trafic distante	Nom de l'objet correspondant au réseau de la machine distante avec laquelle le trafic est échangé au sein du tunnel.
Adresse distante	Réseau des machines distantes dialoguant au travers du tunnel sélectionné (extrémité de trafic).
Masque réseau distant	Masque réseau associé à l'adresse distante.
Politique	Type de politique IPsec. Ce champ peut prendre deux valeurs : • *tunnel*, • *pass*.
Encapsulation	Protocole utilisé pour l'encapsulation des données du tunnel.
Version IKE	Version (1 ou 2) du protocole IKE utilisé pour l'établissement du tunnel.
Durée de vie	Durée de vie maximale du tunnel avant renégociation des clés.
Protection par PPK	Indique si l'option **PPK requise** a été cochée pour ce correspondant. Les valeurs affichées possibles sont : • Obligatoire (option cochée), • Non requise (option non cochée).

Menu contextuel

Un clic droit sur les champs **Type**, **État**, **Nom de la règle**, **Masque du réseau source**, **Local ID**, **Correspondant**, **ID du correspondant**, **Masque du réseau distant**, **Type de politique**, **Encapsulation**, **Version IKE** ou **Durée de vie** donne accès aux menus contextuels suivants :

- Accéder aux logs de cette politique IPsec,
- Copier la ligne sélectionnée dans le presse-papier,
- Accéder à la configuration de cette politique IPsec,
- Accéder à la configuration de ce correspondant.

Un clic droit sur les champs **Passerelle locale**, **Adresse IP de la passerelle locale**, **Passerelle distante** ou **Adresse IP de la passerelle distante** donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Afficher les détails de la machine,
- Placer cet objet en liste noire (pour 1 minute, pour 5 minutes, pour 30 minutes ou pour 3 heures),
- Accéder aux logs de cette politique IPsec,
- Copier la ligne sélectionnée dans le presse-papier,
- Accéder à la configuration de cette politique IPsec,
- Accéder à la configuration de ce correspondant.

Un clic droit sur les champs **Source**, **Adresse de la source**, **Extrémité de trafic distante** ou **Adresse distante** donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Afficher les détails de la machine,
- Placer cet objet en liste noire (pour 1 minute, pour 5 minutes, pour 30 minutes ou pour 3 heures),
- Accéder aux logs de cette politique IPsec,
- Copier la ligne sélectionnée dans le presse-papier,
- Ajouter la machine à la base Objet et / ou l'ajouter dans un groupe,
- Accéder à la configuration de cette politique IPsec,
- Accéder à la configuration de ce correspondant.

Détails complémentaires d'un tunnel

La sélection d'une ligne de tunnel permet l'affichage de détails complémentaires dans les grilles suivantes :

- Associations de sécurité (SA) IKE,
- Associations de sécurité (SA) IPsec.

La grille « Associations de sécurité (SA) IKE »

Nom de règle	Nom (optionnel) donné à la règle VPN IPsec correspondant au tunnel établi. Pour rappel, ce nom permet une recherche dans les logs IPsec des événements liés au tunnel.
IKE	Indique la version du protocole IKE pour le tunnel concerné.
Passerelle locale	Nom de l'objet correspondant à la passerelle locale (extrémité locale du tunnel).
Adresse passerelle locale	Adresse IP présentée par la passerelle locale pour établir le tunnel IPsec concerné.
Passerelle distante	Nom de l'objet correspondant à la passerelle distante (extrémité distante du tunnel).

Adresse passerelle distante	Adresse IP présentée par la passerelle distante pour établir le tunnel IPsec concerné.
État	Indique l'état de la SA IKE (exemple: *established*).
Rôle	Rôle de la passerelle locale dans l'établissement du tunnel (*initiator* ou *responder*).
Cookie initiateur	Marqueur d'identité temporaire de l'initiateur de la négociation. Exemple : « 0xae34785945ae3cbf ».
Cookie réception	Marqueur d'identité temporaire du correspondant de la négociation. Exemple : « 0x56201508549a6526 ».
Local ID	Identifiant (optionnel) local précisé lors de la création du correspondant. Si rien n'est précisé, il s'agit de l'adresse IP de la passerelle locale.
ID du correspondant	Identifiant (optionnel) attribué au correspondant. Si rien n'est précisé, il s'agit de l'adresse IP de la passerelle distante.
NAT-T	Indique si le NAT-T (Nat Traversal - Passage du protocole IPsec au travers d'un réseau réalisant de la translation d'adresses dynamique) est activé pour ce tunnel.
Authentification	Algorithme d'authentification utilisé pour la phase IKE du tunnel.
Chiffrement	Algorithme de chiffrement utilisé pour la phase IKE du tunnel.
PRF	PseudoRandom Function négociée et utilisée pour la dérivation des clés.
DH	Profil Diffie-Hellman utilisé pour le tunnel.
Durée de vie	Durée de vie écoulée de la SA (Security Association) IKE pour le tunnel concerné.

La grille « Associations de sécurité (SA) IPsec »

État	Indique l'état de la SA IPsec (exemple: *installed* / *rekeying*).
Passerelle locale	Nom de l'objet correspondant à la passerelle locale (extrémité locale du tunnel).
Passerelle distante	Nom de l'objet correspondant à la passerelle distante (extrémité distante du tunnel).
Octets entrants	Quantité de données (en octets) ayant transité dans le tunnel à destination de l'extrémité locale de trafic.
Octets sortants	Quantité de données (en octets) ayant transité dans le tunnel à destination de l'extrémité distante de trafic.
Chiffrement	Algorithme de chiffrement utilisé pour la phase IPsec du tunnel.
Authentification	Algorithme d'authentification utilisé pour la phase IPsec du tunnel.
Durée de vie écoulée	Durée de vie écoulée de la SA IPsec pour le tunnel concerné.
ESN	Indique si l'option ESN (Extended Sequence Number) est activée. Cette option n'est disponible que pour IKEv2.

Encapsulation UDP	Indique si l'encapsulation UDP des paquets ESP est activée. Cette encapsulation est automatiquement forcée lorsque le mode DR est activé (**Configuration** > **Système** > **Configuration** > onglet **Configuration Générale** > **Activer le mode "Diffusion Restreinte (DR)"**). Sur un firewall non configuré en mode DR, cette option est activable à l'aide du jeton `natt=<auto|force>` des commandes CLI / Serverd `CONFIG.IPSEC.PEER.NEW` et `CONFIG.IPSEC.PEER.UPDATE`. Pour plus de détails sur ces commandes, veuillez vous référer au Guide de référence des commandes CLI / Serverd.

Liste noire / liste blanche

La grille "Temps réel"

Liste noire

Cette vue reprend la liste des machines ajoutées en quarantaine. Cette mise en quarantaine est possible depuis :

- Le menu contextuel disponible dans certains modules de logs et de supervision,
- La configuration des alarmes.

Les actions possibles :

Supprimer de la liste noire	Ce bouton permet de supprimer de la liste noire l'entrée sélectionnée dans la grille.

Les données disponibles pour la vue « **Liste noire** » sont les suivantes :

Machine / Plage d'adresses	Référence l'adresse IP, le nom (si la machine est déclarée dans la base Objets) ou la plage d'adresses IP mise en liste noire (quarantaine).
Destination bloquée	Indique vers quelle destination (machine, réseau, sous-réseau, plage d'adresses) les flux de la machine en quarantaine sont bloqués.
Délai d'expiration	Indique la date de sortie de la quarantaine pour la machine ou la plage d'adresses concernée.

Liste blanche

Cette vue reprend la liste des machines autorisées à traverser le firewall sans aucune action de celui-ci (pas de filtrage, pas d'analyse IPS). Cette mise en liste blanche n'est possible que depuis la ligne de commande et est destinée à ne pas bloquer des machines de production dans le cadre d'une analyse approfondie d'un comportement non souhaité du firewall. Les données disponibles pour la vue « **Liste blanche** » sont les suivantes :

Machine / Plage d'adresses	Référence l'adresse IP, le nom (si la machine est déclarée dans la base Objets) ou la plage d'adresses IP déclarée en liste blanche.
Destination bloquée	Indique vers quelle destination (machine, réseau, sous-réseau, plage d'adresses) les flux de la machine mise en liste blanche sont bloqués.
Délai d'expiration	Indique la date de sortie de la liste blanche pour la machine ou la plage d'adresses concernée.

Captures réseau

L'outil de captures réseau est basé sur l'analyseur de paquets en ligne de commande tcpdump. Le module se compose de deux grilles :

- Grille **Captures en cours** : permet de lancer des captures réseau, de lister celles en cours, de les stopper et de copier leurs filtres TCPDump,
- Grille **Captures terminées** : permet de lister les captures passées, de télécharger leurs fichiers PCAP et métadonnées, de les supprimer et de copier leurs filtres TCPDump.

> **NOTE**
> L'accès à ce module est possible seulement si le firewall possède un support de stockage sur lequel enregistrer les captures (stockage interne ou carte SD par exemple). De plus, les administrateurs doivent disposer du droit d'écriture ainsi que du droit "**Logs : accès complet (données personnelles)**" ou d'un ticket d'accès temporaire aux données personnelles.

Informations sur le stockage local

Les captures réseau sont conservées sur le stockage local du firewall dans la limite du quota d'espace disque alloué aux captures réseau. Si aucun quota n'est alloué ou activé, le module n'est pas utilisable et un message d'avertissement s'affiche accompagné de deux boutons :

- **Configurer l'espace disque alloué** : ouvre le module Traces - Syslog - IPFIX où il est possible d'allouer et d'activer un quota d'espace disque aux captures réseau,
- **Recharger le module** : recharge le module après avoir alloué ou activé de l'espace disque aux captures réseau.

Les interactions

Les actions listées dans la barre des tâches des deux grilles peuvent être réalisées en effectuant un clic droit dans la grille correspondante. Pour certaines actions, une ligne de la grille doit être sélectionnée au préalable.

La grille Captures en cours

Les actions

Rafraîchir la liste de captures	Permet de rafraîchir la liste des captures en cours et leurs informations.
Créer une capture	Crée une nouvelle capture. La procédure est détaillée dans la section suivante.
Arrêter la capture	Arrête une capture en cours. Sélectionnez au préalable la capture concernée.
Redémarrer la capture	Permet de rejouer une capture en pré-remplissant ses paramètres dans la fenêtre de création d'une nouvelle capture. Sélectionnez au préalable la capture concernée.
Copier le filtre	Copie le filtre TCPDump d'une capture. Sélectionnez au préalable la capture concernée. Ce filtre peut ensuite être utilisé pour créer une nouvelle capture.

Créer une capture

Vous pouvez lancer jusqu'à 5 captures simultanément mais une seule à la fois par interface. À noter que les performances du firewall peuvent être affectées pendant l'exécution des captures réseau. Si l'espace disque utilisé par les captures est égal ou supérieur à 95 %, il n'est plus possible de lancer une nouvelle capture. Lorsque ce seuil est atteint, toutes les captures en cours s'arrêtent automatiquement.

Pour créer une capture, cliquez sur **Créer une capture** et choisissez parmi :

- **Filtre TCPDump** : permet de créer une capture en renseignant manuellement le filtre. Vous devez connaître le format des filtres TCPDump ou être déjà en possession du filtre.
- **Assistant de création de filtre** : permet de créer une capture par le biais d'un assistant de création afin de construire pas à pas le filtre TCPDump.

Une fois la fenêtre de création ouverte, complétez les informations :

Interface	Choisissez l'interface où capturer le trafic réseau. Notez que les interfaces de type loopback ne peuvent pas être sélectionnées pour une capture réseau, ceci afin de ne pas permettre la capture de flux déchiffrés par le proxy SSL.
Durée max. (sec)	Précisez la durée maximale durant laquelle la capture peut capturer des paquets. Cette valeur ne peut pas excéder 172 800 secondes (soit 48 heures). La capture s'arrête automatiquement après avoir atteint la durée maximale, sauf si la capture est arrêtée avant par un autre paramètre.
Nombre max. de paquets	Précisez le nombre maximal de paquets que la capture peut capturer. Cette valeur ne peut pas excéder 2 147 483 647. La capture s'arrête automatiquement si ce nombre est atteint, sauf si la capture est arrêtée avant par un autre paramètre.
Taille limite de paquet	Vous pouvez définir une limite concernant la taille des paquets capturés. Ceux dépassant cette taille seront tronqués. La valeur 0 permet de capturer les paquets complets. Cette valeur ne peut pas excéder 262 144.
Filtre TCPDump	**Si vous avez sélectionné Filtre TCPDump**, seul le champ **Filtre TCPDump** apparaît. Renseignez-y le filtre. **Si vous avez sélectionné Assistant de création de filtre**, plusieurs champs apparaissent. Complétez uniquement ceux nécessaires à votre capture. • **Protocoles de transport** : renseignez les protocoles de transport (tcp, udp, icmp, ...) concernés par la capture. • **Protocoles réseau** : renseignez les protocoles réseau (ip, ip6, arp, ...) concernés par la capture. • **Bi-directionnel** : cette case cochée par défaut permet d'appliquer les mêmes valeurs **Machines**, **Adresses MAC** et **Ports** en source et en destination. Décochez cette case pour accéder aux onglets **Source** et **Destination**. ◦ **Machines** : entrez les adresses IP des machines concernées par la capture. ◦ **Adresses MAC** : entrez les adresses MAC concernées par la capture. ◦ **Ports** : entrez les ports concernés par la capture. **NOTE** Utilisez l'attribut **Égal à** ou **Différent de** selon ce que vous souhaitez capturer ou non. Cliquez sur l'icône à côté de la zone de texte pour modifier l'attribut.

Une fois les informations complétées, cliquez sur **Démarrer** pour lancer la capture. Durant son exécution, vous pouvez quitter le module **Captures réseau** et y revenir plus tard.

NOTE
Dans une configuration en Haute Disponibilité (HA), les captures réseau peuvent être arrêtées seulement depuis le firewall qui les a lancées. Lors du basculement du firewall actif en passif, les captures en cours continuent de s'exécuter jusqu'à s'arrêter automatiquement selon la valeur du paramètre **Durée max. (sec)**.

La grille

Interface	Interface sur laquelle la capture est en cours.
Filtre TCPDump	Filtre TCPDump de la capture.
Durée max. de capture	Durée maximale durant laquelle la capture peut capturer des paquets.
Taille limite de paquet	Taille limite de paquet définie pour la capture.
Nombre de paquets	Nombre de paquets actuellement capturés dans la capture. La valeur de cette colonne ne s'actualise pas en temps réel. Utilisez le bouton **Rafraîchir la liste de captures** pour actualiser les informations de la grille.
Nombre max. de paquets	Nombre maximal de paquets que la capture peut capturer.

La grille Captures terminées

Les actions

Rafraîchir la liste de captures	Permet de rafraîchir la liste des captures terminées.
Tout sélectionner	Sélectionne toutes les captures de la grille.
Supprimer	Supprime les captures sélectionnées.
Télécharger le fichier PCAP	Télécharge le fichier PCAP d'une capture. Sélectionnez au préalable la capture concernée, puis cliquez sur le lien pour télécharger le fichier. Depuis l'interface, il n'est pas possible de télécharger plusieurs fichiers PCAP en une seule manipulation. Les fichiers PCAP sont nommés selon le format : *serial_ifname_timestamp.pcap*. Ils sont stockés sur le firewall dans le répertoire */log/capture*.
Télécharger les métadonnées de capture	Télécharge les métadonnées d'une capture. Sélectionnez au préalable la capture concernée, puis cliquez sur le lien pour télécharger le fichier. Depuis l'interface, il n'est pas possible de télécharger les métadonnées de plusieurs captures en une seule manipulation. Les fichiers contenant les métadonnées sont nommés selon le format : *serial_ifname_timestamp.txt*. Ils sont stockés sur le firewall dans le répertoire */log/capture*.
Rejouer la capture	Permet de rejouer une capture en pré-remplissant ses paramètres dans la fenêtre de création d'une nouvelle capture. Sélectionnez au préalable la capture concernée.

Copier le filtre	Copie le filtre TCPDump d'une capture. Sélectionnez au préalable la capture concernée. Ce filtre peut ensuite être utilisé pour créer une nouvelle capture.

NOTE
Dans une configuration en Haute Disponibilité (HA), les fichiers d'une capture réseau peuvent être téléchargés ou supprimés seulement depuis le firewall qui a lancé la capture.

La grille

Nom	Nom du fichier PCAP de la capture.
Interface	Interface sur laquelle la capture a été réalisée.
Filtre TCPDump	Filtre TCPDump de la capture.
Taille limite de paquet	Taille limite de paquet définie pour la capture. Cette colonne est masquée par défaut.
Taille de capture	Taille du fichier PCAP de la capture.
Durée de capture	Durée pendant laquelle la capture a capturé des paquets. Cette durée peut être inférieure à la **Durée max. de capture** si le **Nombre max. de paquets** a été atteint avant ou si la capture a été stoppée manuellement.
Durée max. de capture	Durée maximale définie pour la capture.
Début de capture	Date et heure de démarrage de la capture. Cette colonne est masquée par défaut.
Fin de capture	Date et heure de fin de la capture. Cette colonne est masquée par défaut.
Nombre de paquets	Nombre de paquets capturés par la capture. Ce nombre peut être inférieur au **Nombre max. de paquets** si la **Durée max. de capture** a été atteinte avant ou si la capture a été stoppée manuellement.
Paquets rejetés par le noyau	Nombre de paquets rejetés par le noyau pendant la capture. Des paquets sont rejetés par le noyau lorsqu'il n'est pas en mesure de tous les capturer, par exemple lorsqu'il reçoit un trop grand nombre de paquets à traiter.
Paquets rejetés par l'interface	Nombre de paquets rejetés par l'interface ou son pilote pendant la capture. Cette colonne est masquée par défaut.
Nombre max. de paquets	Nombre maximal de paquets que la capture pouvait capturer.

SUPPORT IPV6

Le support d'IPv6, proposé dans cette version, permet aux Firewalls d'être intégrés dans des infrastructures IPv4 et/ou IPv6. Les fonctions de Réseau (interfaces et routage), Filtrage, VPN et Administration sont compatibles IPv6. Ce support est optionnel et activable dans le module **Configuration**.

L'interface d'administration web est alors accessible indifféremment en IPv6 ou IPv4 car les interfaces réseau du Firewall peuvent disposer d'une adresse IPv6 fixe seule ou en complément d'une adresse IPv4 (double pile). Les routes statiques et passerelles peuvent désormais être renseignées en IPv6 ; de plus, le routage dynamique embarqué sur les Firewalls Stormshield Network (Bird6) est également compatible.

Le mécanisme SLAAC (StateLess Address AutoConfiguration) est implémenté sur le Firewall Stormshield Network afin de générer des Annonces Routeur (RA - Router Advertisements). Celles-ci permettent l'auto-configuration des machines du réseau par la distribution des préfixes IPv6 à utiliser. Ces annonces permettent également de communiquer des paramètres DNS (Support du RDNSS - RFC 6106) et de définir le Firewall comme passerelle par défaut. Ce mécanisme peut être complété par le service de serveur ou relai DCHPv6 du firewall, pour bénéficier par exemple de la réservation d'adresses en IPv6.

Les objets réseau (machines, réseaux et plages d'adresses IP) peuvent être adressés en IPv6, ou de manière hybride. Les politiques de filtrage sont ainsi applicables aux objets IPv6 et peuvent faire appel à l'inspection de sécurité (profils d'inspection personnalisables). En revanche, les fonctions d'inspections applicatives (Antivirus, Antispam et filtrages URL, SMTP, FTP et SSL) ne sont pas disponibles dans cette version. De même, il n'est pas possible de réaliser de la translation d'adresses (NAT) sur des objets IPv6.

NOTE
Pour chacune des interfaces définies en mode IPv6 et appartenant à un bridge, il est nécessaire de désactiver l'option de **routage sans analyse** du protocole IPv6 (onglet *configuration avancée* du module **Réseau** > **Interfaces**), afin d'autoriser le filtrage de ce trafic.

Les tunnels IPsec sont également compatibles IPv6 ; il est ainsi possible d'établir des tunnels entre deux extrémités IPv6 et d'y faire transiter indifféremment des flux IPv4 ou IPv6. Inversement, les flux IPv6 peuvent emprunter des tunnels IPsec IPv4.

Support IPv6

Détail des fonctionnalités supportées

Système

ACL

Un réseau interne IPv6 est automatiquement intégré au groupe « Network_internals ».

Configuration : NTP

Un firewall peut synchroniser son horloge avec un serveur de temps (serveur NTP) paramétré en IPv6.

Serveur d'administration IPv4/IPv6

L'administration d'un firewall peut être réalisée indifféremment depuis une machine distante adressée en IPv4 ou IPv6 (administration Web et connexions SSH). Pour ce faire, le serveur doit écouter sur les deux protocoles.

Active Update

Les fonctions de protection applicative prises en charge par Active Update (Antispam, Antivirus, etc.) peuvent récupérer leurs mises à jour depuis un serveur miroir disposant d'une adresse IPv6.

Haute disponibilité (HA)

Le transfert de sessions établies en IPv4 ou IPv6 peut être réalisé sur un lien HA en IPv4.

Commandes CLI

Les commandes IPv6 sont accessibles depuis le module **Configuration** > **Commandes CLI** de l'interface web d'administration du firewall.

Réseau

Interfaces : double pile

Une interface du firewall peut posséder simultanément une adresse IPv4 et une adresse IPv6 (double pile).

Interfaces : adressage IPv6 unique

Il est possible de paramétrer un firewall (ou simplement l'une de ses interfaces) en IPv6 seul.

Interfaces : annonces de routeur (RA)

Le firewall peut émettre des messages d'annonces de routeurs et de préfixes (RA : Router Advertisement).

Routage statique

Des routes statiques IPv6 peuvent être définies sur le firewall.

Routage dynamique

Le moteur de routage dynamique prend en charge les routes IPv6 (protocoles RIP / BGP / OSPF).

DHCPv6

Le firewall peut jouer le rôle d'un serveur ou d'un relai DHCPv6.

Objets

Objets réseau

Un objet réseau peut avoir une adresse IPv4 seule, une adresse IPv6 seule ou les deux (double pile).

Utilisateurs

Authentification

La connexion au portail web d'authentification peut être réalisée indifféremment depuis une machine distante adressée en IPv4 ou IPv6.

Politique de sécurité

Filtrage

Une règle de filtrage peut contenir simultanément des objets IPv4, des objets IPv6 et des objets IPv4 et IPv6 (double pile).

Filtrage : vérificateur de cohérence des règles

Le vérificateur de cohérence s'applique également aux règles incluant des objets IPv6.

Filtrage : IPS

L'analyse protocolaire est applicable aux protocoles de niveau 7 transportés sur IPv6 (exemple : HTTP, SMTP, etc.).

Qualité de service

Des traitements de qualité de service peuvent être appliqués aux flux IPv6.

Règles implicites IPv6

Des règles implicites propres aux services IPv6 (Annonces de routeur, DHCPv6) ont été ajoutées (ces règles sont listées dans le paragraphe **Généralités** > **Règles implicites**).

Supervision

Alarmes / Traces

Les événements déclenchés par des flux IPv6 (alarmes, etc.) sont enregistrés dans les fichiers de traces.

VPN

IPsec IKEv1

Des flux IPv4 et/ou IPv6 peuvent transiter dans des tunnels IPsec établis :

- Entre des extrémités de tunnel IPv6,
- Entre des extrémités de tunnel IPv4.

Notifications

Syslog

Les traces peuvent être envoyées à destination de serveurs syslog adressés en IPv6.

Serveur SNMP

Le serveur SNMP intègre la MIB-2 IPv6. Il peut également générer des Traps en IPv6.

Fonctionnalités non supportées

En version SNS 4, voici les principales fonctionnalités non disponibles pour le trafic IPv6 :

- Le trafic IPv6 au travers de tunnels IPsec basés sur des interfaces IPsec virtuelles (VTI),
- La translation d'adresses IPv6 (NATv6),
- Inspections applicatives (Antivirus, Antispam, Filtrage URL, Filtrage SMTP, Filtrage FTP, Filtrage SSL),
- L'utilisation du proxy explicite,
- Le cache DNS,
- Les tunnels VPN SSL portail,
- Les tunnels VPN SSL,

- L'authentification via Kerberos,
- Le Management de Vulnérabilités,
- Les interfaces modems (en particulier les modems PPPoE).

Généralités

Active Update

Le service Active Update du Firewall peut désormais s'adresser à des serveurs de mise à jour configurés en IPv6. Dans ce cas, il est nécessaire d'installer un serveur miroir de mises à jour configuré en double pile (IPv4 / IPv6) : ce dernier pourra se synchroniser en IPv4 avec les serveurs Active Update de Stormshield, et mettre à disposition ses mises à jour aux firewalls en IPv6.

Haute Disponibilité

Dans le cas où un Firewall est en Haute Disponibilité et a activé la fonctionnalité IPv6, les adresses MAC des interfaces portant de l'IPv6 (autres que celles du lien HA) doivent impérativement être définies en configuration avancée. En effet, les adresses de lien local IPv6 étant dérivées de l'adresse MAC, ces adresses seront différentes, entrainant des problèmes de routage en cas de bascule.

Protocoles

L'activation du support IPv6 ne modifie pas les éléments de configuration du protocole IP (module Protection Applicative > Protocoles).

Règles implicites

Des règles implicites propres à l'utilisation des services IPv6 ont été ajoutées et peuvent être activées ou désactivées. Ces règles sont les suivantes:

- Autoriser les sollicitations de routeur (RS) en multicast ou à destination du firewall,
- Autoriser les requêtes au serveur DHCPv6 et les sollicitations multicast DHCPv6.

Configuration

L'activation générale d'IPv6 sur les Firewalls Stormshield Network est réalisée au travers de l'onglet *Paramètres Réseaux* du module **Configuration**.

Onglet Paramètres Réseaux

Activer le support du protocole IPv6 sur ce Firewall	Cliquer sur ce bouton active les couches réseaux IPv6 du Firewall, rendant ainsi accessibles les paramètres IPv6 de différents modules de configuration (Interfaces, DHCP, Routage, etc.). L'activation d'IPv6 nécessite un redémarrage du Firewall.

AVERTISSEMENT
Cette action étant irréversible, il est donc proposé d'effectuer une sauvegarde de votre configuration avant d'activer le support IPv6. Pour revenir à un support unique de l'adressage IPv4, vous devrez effectuer une réinitialisation en configuration d'usine du Firewall avant de pouvoir restaurer la sauvegarde de cette configuration. Cette remise en configuration d'usine s'effectue par le bouton dédié si votre équipement en est équipé, ou en console, par la commande CLI « defaultconfig ».

NOTE
De même, pour chacune des interfaces possédant une adresse IPv6 et appartenant à un bridge, il est nécessaire de désactiver l'option de **routage sans analyse** du protocole IPv6 (onglet *configuration avancée* du module **Réseau** > **Interfaces**) afin d'autoriser le filtrage de ce trafic.

Bridges et interfaces

Bridge

Onglet « Configuration générale »

Plan d'adressage

Adresse IPv6

IP fixe (statique)	En cochant cette option, le bridge dispose d'une adresse IPv6 fixe.
Adresse / Masque	Adresse IP affectée au bridge (toutes les interfaces contenues dans un bridge possèdent la même adresse IP). Renseignez cette adresse et son masque de réseau associé, en notation CIDR (exemple : 2001:db8::70/32), dans le champ situé sous la case à cocher.
Commentaire	Permet de spécifier un commentaire pour l'adressage du bridge.

Plusieurs adresses IP et masques associés peuvent être définis pour un même bridge (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser ce Firewall Stormshield Network comme un point de routage central. De ce fait, un bridge peut être connecté à différents sous-réseaux ayant un adressage différent. Pour les ajouter ou les retirer, il suffit d'utiliser les boutons d'action **Ajouter** et **Supprimer** situés au-dessus des champs du tableau.

Il est possible d'ajouter plusieurs adresses IP (alias) dans le même plan d'adressage sur une interface. Dans ce cas, il est impératif que ces adresses aient toutes le même masque.

Onglet « Configuration du routage »

Sur chaque interface, bridge ou interface agrégée, les messages d'annonces du routeur (*Router Advertisement* - RA) peuvent être envoyés périodiquement à tous les nœuds IPv6 (*multicast*) du segment via l'adresse de la liaison locale ou en réponse à la sollicitation de routeur (*Routeur Sollicitation* - RS) d'une machine du réseau.

Cette annonce permet à un nœud IPv6 d'obtenir les informations suivantes :

- L'adresse du routeur par défaut, en l'occurrence celle du firewall,
- Le(s) préfixe(s) utilisé(s) sur le lien (en 64bits),
- l'indication de l'utilisation de l'auto-configuration sans état (*SLAAC*) ou du DHCPv6 (*Managed*)
- L'indication de récupérer d'autres paramètres via DHCPv6 (*OtherConfig*),
- D'éventuels paramètres DNS (RFC4862).

L'auto-configuration, native dans IPv6 est sans état (*Stateless Address Autoconfiguration* - SLAAC), c'est-à-dire que le serveur ne choisit pas les IPs des clients et n'a pas à les retenir.

Une machine a une adresse de liaison locale dont l'unicité a été vérifiée via NPD DAD (protocole *Neighbor Discovery Protocol - Duplicated Address Detection*) avec succès. La machine reçoit ensuite l'annonce du routeur (RA) périodique ou sollicitée. Si l'information d'auto-configuration sans état est spécifiée, la machine se construit alors une ou plusieurs adresses IPv6 à partir du ou des préfixe(s) annoncé(s) et de son identifiant d'interface (aléatoire ou basé sur l'adresse MAC). L'adresse IP du routeur (celle du firewall) servira alors de passerelle par défaut.

Par défaut, le mode d'émission des annonces de routeur (RA) diffuse le premier préfixe déduit de l'interface. Les serveurs DNS sont par défaut ceux configurés pour le firewall (**Système** > module **Configuration**).

NOTE
Si les annonces de routeur sont activées sur un bridge, ces annonces sont uniquement diffusées sur les interfaces protégées.

Paramètres d'autoconfiguration

Émettre les RA si DHCPv6 activé	Si le service DHCPv6 est activé sur le firewall (**Réseau > DHCP**), le firewall va émettre automatiquement des annonces (Router Advertisement – RA) sur les interfaces correspondantes, indiquant aux nœuds IPv6 de s'auto-configurer en DHCPv6 (les options Managed et Other config sont alors activées par défaut). Si le firewall fait office de serveur DHCPv6, l'interface configurée doit appartenir à l'une des plages d'adresses renseignées en configuration DHCPv6. Si le firewall sert de relai à un serveur DHCPv6, l'interface configurée doit appartenir à la liste des interfaces d'écoute du service. Si le service DHCPv6 n'est pas actif, l'émission des RA est désactivée.
Émettre les RA	L'adresse du firewall est envoyée comme routeur par défaut. Les informations relayées par cette annonce sont décrits ci-après. Cette configuration est recommandée afin de permettre aux machines directement connectées (lien local) de faire du SLAAC.
Désactiver	Aucune annonce de routeur (RA) n'est diffusée. Cette configuration est recommandée en bridge si un routeur IPv6 est directement connecté (lien local).

Annonces du routeur (RA)

Annoncer le préfixe déduit de l'interface	Le préfixe annoncé est celui configuré dans le plan d'adressage IPv6 de l'interface (onglet *Configuration*). La taille du masque (longueur du préfixe - CIDR) de l'adresse IPv6 configurée doit obligatoirement être de 64 bits.

Configuration avec serveur DHCPv6

Le serveur DHCPv6 délivre les adresses (Managed)	L'annonce indique que les adresses IPv6 sollicitée seront distribuées par le service DHCPv6 activé sur le firewall (**Réseau > DHCP**). Ce service est mis en œuvre par le firewall ou un relai directement connecté (lien local).
Le serveur DHCPv6 délivre des options supplémentaires (Other config)	L'annonce indique que les autres paramètres d'auto-configuration telles que les adresses de serveurs DNS ou un autre type de serveur, seront délivrées par le serveur DHCPv6 (firewall ou relai) directement connecté (lien local).

Configuration avancée

Paramètres DNS

Nom de domaine	Nom de domaine par défaut pour joindre un serveur interrogé sans domaine.
Serveur DNS primaire	Adresse IP du serveur DNS primaire. Si ce champ n'est pas renseigné, l'adresse envoyée sera celle utilisés par le Firewall (**Système > Configuration**)
Serveur DNS secondaire	Adresse IP du serveur DNS secondaire. Si ce champ n'est pas renseigné, l'adresse envoyée sera celle utilisés par le Firewall (**Système > Configuration**)

Préfixes annoncés

Comme il est préconisé que le préfixe annoncé soit le même que celui de l'interface, dans le cas où l'interface en spécifie plusieurs, ce champ précise le préfixe à utiliser.

Préfixes	Préfixe à annoncer aux machines
Autonomous	Instruction d'auto-configuration sans état (SLAAC) : si cette case est cochée, la machine se construit une ou plusieurs adresses IPv6 à partir du préfixe annoncé et d'un identifiant d'interface (aléatoire et/ou basé sur l'adresse MAC).
On link	Cette option précise à la machine que toutes les machines ayant le même préfixe peuvent être joignables directement, sans passer par le routeur. **NOTE** En IPv4, cette information était déduite du masque réseau.
Commentaire	Permet de donner un commentaire au préfixe annoncé.

Paramètres optionnels

Certains paramètres spécifiques des Annonces de routeur sont configurables via commande CLI, comme la taille maximale d'un paquet transmis (MTU) sur le lien, la durée de validité de(s) préfixe(s) utilisé(s) sur le lien ou le champ *Router Lifetime*.

Pour consulter le détail et les valeurs possibles de ces paramètres, reportez-vous au guide « CLI serverd commands reference – V1.0 » disponible dans votre espace client.

Interface Ethernet en mode Bridge

Onglet « Configuration avancée »

Routage sans analyse

Autoriser sans analyser	Permet de laisser passer les paquets IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est alors réalisé sur ce protocole.

IMPORTANT
Pour chacune des interfaces incluses dans un bridge, il est nécessaire de décocher la case **Autoriser sans analyser** pour le protocole IPv6 afin de bénéficier du filtrage de ces flux.

Interface Ethernet en mode avancé

Onglet « Configuration générale »

Pour configurer une interface dans un réseau ne faisant pas partie d'un bridge, il suffit de la sortir de l'arborescence du bridge en la glissant avec la souris.

Lors du détachement, l'écran de plan d'adressage s'affiche.

Adressage IPv4	En cochant cette option, l'interface dispose d'une adresse IPv4. Si celle-ci est statique, il faut l'indiquer (suivie de son masque de réseau) dans le champ situé sous la case à cocher. Par défaut, une adresse dynamique lui est adressée via DHCP.
Adressage IPv6	En cochant cette option, l'interface dispose d'une adresse IPv6 fixe. Renseignez cette adresse et son masque de réseau associé, en notation CIDR (exemple : 2001:db8::70/32), dans le champ situé sous la case à cocher.

Une fois l'interface hors du bridge, vous avez accès aux paramètres de l'interface décrits dans la section **Interface Ethernet en mode Bridge**.

VLAN

Onglet « Configuration générale »

Plan d'adressage

Adresse IPv6

IP fixe (statique)	En cochant cette option, le VLAN dispose d'une adresse IPv6 fixe.
Adresse / Masque	Adresse IP affectée au VLAN. Renseignez cette adresse et son masque de réseau associé, en notation CIDR (exemple : 2001:db8::70/32), dans le champ situé sous la case à cocher.
Commentaire	Permet de spécifier un commentaire pour l'adressage du VLAN.

Onglet « Configuration du routage »

Pour les options concernant les **Paramètres d'autoconfiguration** et les **Annonces du routeur**, reportez-vous à la section **Onglet « Annonces du Routeur (RA) »** du menu **Bridge**.

Interfaces virtuelles

Onglet « Interfaces IPsec (VTI) »

Adresse IPv6	Indiquez l'adresse IPv6 attribuée à l'interface IPsec.
Préfixe IPv6	Indiquez le préfixe IPv6 associé à l'adresse de l'interface IPsec.

Onglet « Loopback »

Adresse IPv6	Indiquez l'adresse IPv6 attribuée à la loopback.

Routage

Le paramétrage du routage IPv6 est segmenté en deux parties :

- Routage statique IPv6: Permet la définition des routes statiques pour les paquets IPv6. Le routage statique représente un ensemble de règles définies par l'administrateur ainsi qu'une route par défaut.
- Routage dynamique BIRD IPv6: Permet de configurer les protocoles de routage dynamique (RIP, OSPF, BGP) au sein du moteur BIRD IPv6, afin de permettre au firewall d'apprendre des routes gérées par d'autres équipements.

AVERTISSEMENT
Le moteur de routage dynamique BIRD6 est dédié au routage dynamique IPv6. Cette configuration est à paramétrer en console dans les fichiers :
/usr/Firewall/ConfigFiles/Bird/global (section [bird6])/usr/Firewall/ConfigFiles/Bird/bird6.conf
Pour plus d'information sur la configuration du routage dynamique, reportez-vous à la Note Technique **Routage Dynamique BIRD**, disponible sur le site de Documentation Technique Stormshield.

Le routage statique et le routage dynamique fonctionnent simultanément; le routage statique reste cependant prioritaire pour l'acheminement des paquets sur le réseau.

L'onglet « Routes statiques IPv6 »

Passerelle par défaut (routeur)	Le routeur par défaut est généralement l'équipement qui permet l'accès de votre réseau à Internet. C'est à cette adresse que le Firewall envoie les paquets qui doivent sortir sur le réseau public. Si vous ne configurez pas le routeur par défaut, le Firewall ne sait pas diriger les paquets possédant une adresse de destination différente des réseaux qui lui sont directement reliés. Les machines ne pourront alors accéder à aucun autre réseau que le leur. Cliquez sur le bouton pour accéder à la base d'objets et sélectionnez une machine. Le champ Passerelle par défaut est grisé lorsqu'une une liste de passerelle est définie dans la zone de configuration avancée.

Présentation de la barre de boutons

Recherche	Recherche qui porte sur un objet machine, un réseau ou un groupe.
Ajouter	Ajoute une route statique "vide". L'ajout de la route (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Réseau de destination (objet machine, réseau ou groupe)** et **Interface** remplis.
Supprimer	Supprime une route ou plusieurs routes préalablement sélectionnée(s). Utiliser les touches **Ctrl**/**Shift** + **Supprimer** pour la suppression de plusieurs routes.

Appliquer	Envoie la configuration des routes statiques.
Annuler	Annule la configuration des routes statiques.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des routes statiques IPv6 :

- Ajouter,
- Supprimer.

Présentation de la grille

La grille présente six informations :

État	État de la configuration des routes statiques : • **Activé** : Double-cliquez pour activer la route créée. • **Désactivé** : La route n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.
Réseau de destination (objet machine, réseau ou groupe)(Obligatoire)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine, un réseau ou un groupe.
Plan d'adressage	Adresse IP ou groupe d'adresses liés aux éléments sélectionnés dans la colonne « Réseau de destination (objet machine, réseau ou groupe) ». Ce champ est renseigné automatiquement.
Interface(Obligatoire)	Une liste déroulante permet de sélectionner l'interface de sortie pour joindre le réseau de destination. Cet objet peut être une interface Ethernet, un Vlan ou un modem (dialup).
Protégée	Cette colonne vous informe de la nature protégée ou non de la route. Une route protégée est ajoutée à l'objet Network_internals. Le comportement de la configuration de sécurité prendra en compte ce paramètre. Les machines joignables par cette route seront mémorisées dans le moteur de prévention d'intrusion.
Passerelle (Optionnel)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine (routeur).
Commentaire (Optionnel)	Texte libre.

L'onglet « Routage dynamique IPv6 »

Cet onglet permet d'activer et de configurer le moteur de routage dynamique BIRD pour IPv6 (Bird6).

Activer le routage dynamique BIRD	Cette case permet d'activer l'utilisation du moteur de routage dynamique BIRD pour IPv6.

La fenêtre située sous la case d'activation de Bird6 permet de saisir directement la configuration du moteur de routage dynamique Bird6.

Pour plus d'information sur la configuration du routage dynamique ou sur la migration de ZebOS vers BIRD, reportez-vous à la Note technique Routage Dynamique BIRD, disponible sur le site de Documentation Technique Stormshield.

Configuration avancée

Ajouter les réseaux IPv6 distribués par le routage dynamique dans la table des réseaux protégés	Cette option permet d'injecter automatiquement dans la table des réseaux protégés du moteur de prévention d'intrusion les réseaux propagés par le moteur de routage dynamique.

Envoi de la configuration

Les modifications effectuées sur cet écran sont validées à l'aide du bouton Appliquer.

AVERTISSEMENT
Aucune vérification syntaxique n'est effectuée lors de l'envoi de la configuration du moteur de routage dynamique.

L'onglet « Routes de retour IPv6 »

Lorsque plusieurs passerelles sont utilisées pour réaliser du partage de charge, cet onglet permet de définir la passerelle par laquelle les paquets retour doivent impérativement transiter afin de garantir la cohérence des connexions.

REMARQUE
Si la passerelle sélectionnée dans la liste déroulante est un objet de type « machine », cet objet devra impérativement préciser une adresse MAC.

Présentation de la barre de boutons

Ajouter	Ajoute une route de retour "vide". L'ajout de la route (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Passerelle** et **Interface** remplis.
Supprimer	Supprime une route préalablement sélectionnée.
Appliquer	Envoie la configuration des routes de retour.
Annuler	Annule la configuration des routes de retour.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des routes de retour IPv6 :

- Ajouter,
- Supprimer.

Présentation de la grille

La grille présente quatre informations :

État	État de la configuration des routes de retour : • Activé : Double-cliquez pour activer la route créée. • Désactivé : La route n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.
Interface (Obligatoire)	Une liste déroulante permet de sélectionner une interface parmi Loopback, Ethernet, Vlan, Dialup, GRE, GRETAP.
Passerelle (Optionnel)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine ou une interface virtuelle (IPsec). S'il s'agit d'un objet de type « machine », il devra impérativement préciser une adresse MAC.
Commentaire (Optionnel)	Texte libre.

DHCP

Les paramètres du service DHCP sont regroupés au sein de l'onglet DHCP IPv6.

Général

Activer le service : permet d'activer le service DHCP selon 2 modes spécifiques : serveur ou relai.

Serveur DHCP	Envoie différents paramètres réseaux aux clients DHCP.
Relai DHCP	Le mode relai DHCP est à utiliser lorsque l'on souhaite rediriger les requêtes clientes vers un serveur DHCP externe.

Service « Serveur DHCP »

Le service « serveur DHCP » présente 4 zones de configuration :

- **Paramètres par défaut.** Ce menu est réservé à la configuration des paramètres DNS envoyés aux clients DHCP (nom de domaine, serveurs DNS primaire et secondaire)
- **Plage d'adresses**. Par plage, vous spécifiez un groupe d'adresses destinées à être allouées aux utilisateurs. L'adresse allouée l'est alors pour le temps déterminé dans la configuration avancée.
- **Réservation**. L'adresse allouée par le service est toujours la même pour les machines listées dans la colonne **Réservation**.
- **Configuration avancée.** Ce menu permet d'activer ou non l'envoi du fichier de configuration automatique des proxies pour les machines clientes (WPAD : Web Proxy Autodiscovery Protocol). Il est également possible d'y personnaliser la durée d'affectation des adresses IP distribuées par le service DHCP.

NOTE
Le DHCPv6 ne peut fonctionner qu'avec le mécanisme d'Annonces de Routeur (RA) paramétré sur une interface ou un bridge dans le module **Réseau** > **Interfaces**. Ces annonces de routeur induisent que le firewall se présente comme le routeur par défaut.

Paramètres par défaut

Si l'option serveur DHCP a été cochée, il est possible ici de configurer des paramètres globaux, comme le **nom de domaine**, les **serveurs DNS**, etc. que les machines clientes vont utiliser.

Nom de domaine	Nom de domaine utilisé par les machines clientes DHCP pour leur résolution DNS.
Serveur DNS primaire	Sélectionnez le serveur DNS primaire qui sera envoyé aux clients DHCP. Il s'agit d'un objet de type machine. Si aucun objet n'est précisé, c'est le serveur DNS primaire du Firewall qui leur sera transmis.
Serveur DNS secondaire	Sélectionnez le serveur DNS secondaire qui sera envoyé aux clients DHCP. Il s'agit d'un objet de type machine. Si aucun objet n'est précisé, c'est le serveur DNS secondaire du Firewall qui leur sera transmis.

Plage d'adresses

Pour qu'un serveur DHCP fournisse des adresses IP, il est nécessaire de configurer une réserve d'adresses dans laquelle il pourra puiser.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des plages d'adresses, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Permet d'ajouter une plage d'adresses. Sélectionnez ou créez une plage d'adresses IPv6 (objet réseau de type **Plage d'adresses IP**).
Supprimer	Permet de supprimer une plage d'adresses, ou plusieurs plages d'adresses simultanément.

La grille affiche les plages d'adresses utilisées par le serveur DHCP pour la distribution d'adresses aux clients.

Plages d'adresses	Sélectionnez un objet réseau de type **Plage d'adresses IP** dans la liste déroulante. Le serveur puisera dans cette réserve pour distribuer des adresses aux clients. Si aucune interface protégée du Firewall n'a d'adresse IP dans le réseau englobant cette plage, un message d'avertissement « Pas d'interface protégée correspondant à cette plage d'adresse » est affiché.
DNS primaire	Ce champ permet d'affecter un serveur DNS primaire spécifique aux clients DHCP. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS primaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
DNS secondaire	Ce champ permet d'affecter un serveur DNS secondaire spécifique aux clients DHCP. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS secondaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
Nom de domaine	Ce champ permet d'indiquer un nom de domaine spécifique qui sera utilisé par le client DHCP pour sa résolution DNS. Si aucun nom n'est spécifié, la valeur « Domaine par défaut » est affichée dans cette colonne. C'est alors le nom de domaine indiqué dans le champ **Nom de domaine** de la section **Paramètres par défaut** qui est utilisé pour le client.

AVERTISSEMENT
Deux plages ne peuvent se chevaucher. Une plage d'adresses appartient à un unique bridge/interface.

Réservation

Bien qu'utilisant un serveur distribuant dynamiquement des adresses IP aux clients, il est possible de réserver une adresse IP spécifique pour certaines machines. Cette configuration se rapproche d'un adressage statique, mais rien n'est paramétré sur les postes clients, simplifiant ainsi leur configuration réseau.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des réservations d'adresses, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Permet d'ajouter une réservation d'adresse IP pour un objet spécifique réseau de type machine.
Supprimer	Permet de supprimer une réservation d'adresse IP. Si une réservation est supprimée, la machine concernée se verra attribuer aléatoirement une nouvelle adresse lors de son renouvellement.

La grille affiche les objets machines pour lesquels une réservation d'adresse est effectuée (chaque objet contenant obligatoirement l'adresse IPv6 réservée), ainsi que leur identifiant unique associé (DUID : DHCP Unique Identifier). Le DUID est obligatoire : il permet d'identifier la machine cliente lors d'une attribution ou d'un renouvellement d'adresse IP, afin de lui affecter l'adresse réservée ; il joue un rôle similaire à celui de l'adresse MAC en DHCP IPv4.

Réservation	Ce champ contient le nom de l'objet réseau (machine) possédant une adresse IPv6 réservée.
Identifiant unique DHCP (DUID)	Ce champ contient l'identifiant unique de la machine. Celui-ci permet au Firewall d'identifier le client et de lui réattribuer l'adresse IP réservée. Sur un poste client Windows, cet UUID est renseigné dans la clé de registre suivante : HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TCPIP6\Parameters\Dhcpv6DUID
DNS primaire	Ce champ permet d'affecter un serveur DNS primaire spécifique à chaque client DHCP bénéficiant d'une réservation d'adresse. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS primaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
DNS secondaire	Ce champ permet d'affecter un serveur DNS secondaire spécifique à chaque client DHCP bénéficiant d'une réservation d'adresse. Sélectionnez un objet réseau de type « machine » dans la liste déroulante. Si aucun objet n'est sélectionné, la valeur « default » est affichée dans cette colonne. C'est alors la machine choisie dans le champ **DNS secondaire** de la section **Paramètres par défaut** qui est utilisée comme serveur DNS pour le client.
Nom de domaine	Ce champ permet d'indiquer un nom de domaine spécifique qui sera utilisé par le client DHCP pour sa résolution DNS. Si aucun nom n'est spécifié, la valeur « Domaine par défaut » est affichée dans cette colonne. C'est alors le nom de domaine indiqué dans le champ **Nom de domaine** de la section **Paramètres par défaut** qui est utilisé pour le client.

Configuration avancée

Serveur TFTP	Le serveur TFTP sert pour le boot à distance des machines. Ce champ (champ option 150 : TFTP server address) peut être utilisé pour le démarrage d'équipements réseaux tels que des routeurs, des X-terminals ou des stations de travail sans disque dur. Seuls les serveurs disposant d'une IPv6 seront présentés dans la liste.
Annoncer le fichier de configuration automatique des proxies (WPAD)	Si cette option est cochée, le serveur distribue aux clients DHCP la configuration d'accès à Internet au travers d'un fichier d'auto-configuration de proxy (PAC : Proxy Auto Configuration). Ce fichier, doté d'une extension « .pac », doit être renseigné dans les paramètres d'authentification (onglet *Portail Captif* du menu **Configuration** > **Utilisateurs** > **Authentification**). Il peut être rendu accessible depuis les interfaces internes et/ou externes (onglets *Interfaces Internes* et *Interfaces Externes* du menu **Configuration** > **Utilisateurs** > **Authentification**).

Durée de bail attribuée

Par défaut (heure)	Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées pour une durée limitée. Il faut donc indiquer ici le temps par défaut pendant lequel les stations garderont la même adresse IP.
Minimum (heure)	Temps minimum pendant lequel les stations garderont la même adresse IP.
Maximum (heure)	Temps maximum pendant lequel les stations garderont la même adresse IP.

Service « Relai DHCP »

Le service « relai DHCP » présente 3 zones de configuration :

- **Paramètres.** Ce menu permet de configurer le ou les serveurs DHCP vers le(s)quel(s) le firewall relaiera les requêtes DHCP des machines clientes.
- **Interfaces d'écoute des requêtes DHCP**. Les interfaces réseau sur lesquelles le Firewall est à l'écoute des requêtes DHCP clientes.
- **Interfaces de sortie du relai DHCP**. Il s'agit de préciser les interfaces par lesquelles le Firewall enverra les requêtes vers le(s) serveur(s) DHCP précédemment indiqués.

Paramètres

Serveur(s) DHCP	La liste déroulante permet de sélectionner un objet machine, ou un objet groupe contenant des machines. Le Firewall relaiera les requêtes des clients vers ce(s) serveur(s) DHCP.

Interfaces d'écoute des requêtes DHCP

Il s'agit d'indiquer par quelles interfaces réseaux le Firewall va recevoir les requêtes des clients DHCP.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des interfaces d'écoute, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Ajoute une ligne dans la grille et ouvre la liste déroulante des interfaces du firewall pour y sélectionner une interface.
Supprimer	Permet de supprimer une ou plusieurs interfaces d'écoute.

Interfaces de sortie du relai DHCP

Il s'agit d'indiquer par quelles interfaces réseaux le Firewall pourra joindre le(s) serveur(s) DHCP afin de transmettre les requêtes des clients DHCP.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des interfaces de sortie, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Ajoute une ligne dans la grille et ouvre la liste déroulante des interfaces du firewall pour y sélectionner une interface.
Supprimer	Permet de supprimer une ou plusieurs interfaces de sortie.

Objets Réseau

Ce module est divisé en deux parties :

- La barre d'actions, en haut de l'écran, permettant de trier et de manipuler les objets.
- Deux colonnes dédiées aux objets : l'une les listant, et l'autre affichant leurs propriétés.

> **NOTE**
> La création d'objets ne permet de déclarer un objet en mode Global que si l'option "Afficher les politique globales (Filtrage, NAT et VPN IPsec)" est activée dans le module **Préférences**.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

La barre d'actions

Version IP

Ce bouton complète la fonctionnalité du filtre et permet de choisir le type d'objets à afficher en fonction de la version d'IP qu'ils utilisent. Un menu déroulant vous propose les choix suivants :

IPv4 et IPv6	Cette option permet d'afficher dans la liste des objets à gauche, tous les objets réseau du type choisi (Machine, Réseau, Plage d'adresses IP), quelle que soit la version d'IP utilisée pour leur adressage.
IPv4	Cette option permet d'afficher dans la liste des objets à gauche, tous les objets réseau du type choisi (Machine, Réseau, Plage d'adresses IP) et adressés exclusivement en IPv4.
IPv6	Cette option permet d'afficher dans la liste des objets à gauche, tous les objets réseau du type choisi (Machine, Réseau, Plage d'adresses IP) et adressés exclusivement en IPv6.

Les différents types d'objets

Machine

Sélectionnez une machine pour visualiser ou éditer ses propriétés. Chaque objet de ce type est obligatoirement caractérisé par un nom et une méthode de résolution DNS : « Automatique » si la machine est paramétrée en adressage IP dynamique ; « Aucune (IP statique) » si la machine est paramétrée en adressage statique).

Adresse IPv6

L'adresse IPv6 de la machine sélectionnée.

> **EXAMPLE**
> 2001:db8:11a::10

Afin de simplifier la saisie de l'adresse IPv6, une liste déroulante propose l'ensemble des préfixes globaux renseignés sur le Firewall.

Réseau

Sélectionnez un réseau pour visualiser ou éditer ses propriétés. Chaque objet de ce type est obligatoirement caractérisé par un nom, une adresse de réseau et son masque associé.

Adresse IPv6

L'adresse IPv6 du réseau sélectionné et son masque associé, en notation CIDR.

> **Exemple**
> 2001:db8::/32

Afin de simplifier la saisie de l'adresse IPv6, une liste déroulante propose l'ensemble des préfixes globaux renseignés sur le Firewall.

Filtrage

Les objets réseau (machines, réseaux et plages d'adresses IP) peuvent être adressés en IPv6, ou de manière hybride (IPv4 et IPv6). Les politiques de filtrage sont ainsi applicables aux objets IPv6 et peuvent faire appel à l'inspection de sécurité (profils d'inspection personnalisables).

En revanche, les fonctions d'inspections applicatives (Antivirus, Antispam, filtrages URL, SMTP, FTP et SSL) et de translation d'adresses (NAT) ne sont pas disponibles pour les objets IPv6 dans cette version (l'onglet *NAT* est renommé en *NAT IPv4* lors de l'activation d'IPv6).

L'onglet « Filtrage »

Le **Filtrage** est composé de deux parties. Le bandeau situé en haut de l'écran, permettant de choisir la politique de filtrage, de l'activer, de l'éditer et de visualiser sa dernière modification. La grille de filtrage est dédiée à la création et la configuration des règles.

Les actions sur les règles de la politique de filtrage

Les actions disponibles sont identiques pour des règles incluant des objets IPv4 ou IPv6.

REMARQUE
Les flux liés au protocole NDP (Neihgbour Discovery Protocol) ne sont jamais bloqués, même dans le cas d'une politique de filtrage de type « block all ». Cela concerne les messages de type NS (Neighbour Sollicitation) et NA (Neighbour Advertisement).

Certaines actions ne pouvant s'appliquer qu'au trafic IPv4 génèreront des avertissements (icône) ou des erreurs (icône) dans le champ « Vérification de la politique », si des objets IPv6 sont inclus dans les règles de filtrage.

Règle standard incluant des objets ayant des versions d'IP différentes en source et destination	[Règle X] Les objets Source et Destination n'utilisent pas la même version d'adressage IP (IPv4/IPv6).
Règle d'authentification incluant des objets IPv6	[Règle X] La redirection vers les services s'effectuera uniquement sur le trafic IPv4.
Règle d'inspection SSL incluant des objets IPv6	[Règle X] L'action « déchiffrer » s'appliquera uniquement sur le trafic IPv4.
Règle de proxy HTTP explicite incluant des objets IPv6	[Règle X] Cannot apply proxy nor NAT on IPv6 traffic.
Règle avec NAT sur la destination incluant des objets IPv6	[Règle X] Le NAT sur la destination s'appliquera uniquement sur le trafic IPv4
Règle incluant des objets IPv6 et faisant appel aux inspections applicatives (Antivirus, Antispam, filtrage URL, filtrage SMTP, filtrage FTP ou filtrage SSL)	[Règle X] Les inspections applicatives s'appliqueront uniquement sur le trafic IPv4.

TABLEAU DE BORD

Le tableau de bord présente une vue d'ensemble des informations concernant le firewall. Il est accessible à n'importe quel moment pendant la configuration du firewall en cliquant sur l'onglet **Monitoring** dans le bandeau supérieur, puis sur **Tableau de bord** dans le menu de gauche.

Le tableau de bord se compose de plusieurs widgets.

Réseau

Le widget **Réseau** contient une représentation graphique des interfaces du firewall SNS :

- Le nombre d'interfaces disponibles sur le firewall est représenté (32 maximum),
- Les interfaces utilisées apparaissent en vert,
- Lorsque le mode Sûreté est activé (mécanisme de *bypass* prêt à être déclenché), le numéro des interfaces des segments *bypass* apparaît dans un cercle orange,
- Lorsque le mécanisme de *bypass* a été déclenché, les interfaces des segments *bypass* apparaissent en orange avec une flèche bidirectionnelle les reliant.

Une info bulle contenant les informations de chacune des interfaces est disponible.

Ces informations sont les suivantes :

Interface	Nom de l'interface utilisée (de type « in », « out » ou « dmz »).
Adresse	Adresse(s) IP et masque de sous-réseau.
Paquets réseau	Le nombre de paquets Accepté, Bloqué, Fragmenté, TCP, UDP et ICMP.
Bloqués	Le nombre de paquets bloqués issus de cette interface.
Trafic reçu	La totalité et le détail des paquets TCP, UDP et ICMP reçus.
Trafic émis	La totalité et le détail des paquets TCP, UDP et ICMP émis.
Débit entrant actuel	Le débit entrant actuel.
Débit sortant actuel	Le débit sortant actuel.
Mode (Sûreté / Bypass) activé	Cette valeur n'est disponible que pour les firewalls disposant de la fonction de *bypass* et est affichée que lorsque le mode Sûreté du *bypass* est activé. Les valeurs possibles sont « Mode Sûreté activé » (mécanisme de *bypass* non déclenché) ou « Mode Bypass activé » (mécanisme de *bypass* déclenché).

Protections

Cette fenêtre contient la liste des dernières alarmes (ou événements systèmes) levées par le firewall. Certaines colonnes peuvent être masquées par défaut.

Date	La date et l'heure des dernières alarmes remontées, classée de la plus à la moins récente.

Message	Commentaire associé à l'alarme sélectionnée. **Exemples de messages possibles** « Message ICMP invalide (no TCP/UDP linked entry) » (priorité type mineur). « Usurpation d'adresse IP (type=1) » (priorité type majeur).
Action	Lorsqu'une alarme est remontée le paquet qui a provoqué cette alarme subit l'action associée. Les actions sont « Bloquer » ou « Passer ».
ID	Identifiant unique de l'alarme.
Classe	Classe liée à l'alarme.
Priorité	3 niveaux de priorités sont possibles et configurables au sein du module Protection Applicative/ Applications et Protections.
Interface source	Interface d'entrée des paquets ayant déclenché l'alarme.
Port source	Port d'origine des paquets ayant déclenché l'alarme.
Source	Adresse IP à l'origine du déclenchement de l'alarme. Par souci de conformité avec le règlement européen RGPD (Règlement Général sur la Protection des Données), les adresses IP sont remplacées par le terme "Anonymized". Pour les afficher, il est nécessaire d'obtenir le droit "Logs : accès complet (données personnelles)" en cliquant sur le lien **Logs : accès restreint** puis en rafraîchissant les données du widget.
Port destination	Port destination utilisé par les paquets ayant déclenché l'alarme.
Destination	Adresse de la machine destinataire du paquet ayant déclenché l'alarme.

Un clic droit sur une ligne d'alarme (ou d'événement système) permet d'accéder à la configuration ou à la page d'aide de l'alarme (ou de l'événement système) :

Accéder à la configuration des alarmes	Ce bouton affiche l'alarme dans le module **Applications et Protections**. La colonne *Avancée* de la ligne sélectionnée propose le bouton **Options avancées**. Cette action permet d'envoyer un e-mail au déclenchement de l'alarme, de mettre la machine responsable de l'alarme en quarantaine ou de capturer le paquet bloqué.
Accéder à la configuration des événements système	Ce bouton affiche l'événement système dans le module **Notifications > Événements système**. La colonne *Avancée* de la ligne sélectionnée propose le bouton **Configurer**. Cette action permet d'envoyer un e-mail au déclenchement de l'alarme, de mettre la machine responsable de l'alarme en quarantaine ou de capturer le paquet bloqué.
Ouvrir la page d'aide pour visualiser les détails de cette alarme	Sélectionnez l'alarme voulue, et cliquez sur ce lien qui vous mènera à une page d'aide concernant le message (voir ci-dessus).

Propriétés

Cette fenêtre affiche les données relatives à votre modèle de firewall ainsi qu'à la version de firmware installée sur votre firewall ou cluster de firewalls.

Nom	Nom donné au firewall (module **Configuration > Système > Configuration**, onglet **Configuration générale**). Par défaut, ce nom correspond au numéro de série du firewall.
Modèle	Modèle physique du firewall (exemple : SN 210).
Modèle EVA	Ce champ n'apparaît que sur les firewalls virtuels. Il indique le modèle de firewall virtuel correspondant aux ressources physiques affectées à la machine (EVA1, EVA2, EVA3, EVA4 ou EVAU).
Capacité mémoire de l'EVA	Ce champ n'apparaît que sur les firewalls virtuels. Cette entrée précise la quantité de mémoire actuellement alloués à la machine virtuelle. Les valeurs minimales et maximales de mémoire appliquables à ce modèle sont également précisées entre parenthèses.
Nombre de CPU de l'EVA	Ce champ n'apparaît que sur les firewalls virtuels. Cette entrée précise le nombre de processeurs virtuels (vCPU) actuellement alloués à la machine virtuelle. Les nombres minimum et maximum de processeurs virtuels appliquables à ce modèle sont également précisées entre parenthèses.
Numéro de série	Référence de votre Firewall Stormshield Network.
Version	Version de firmware installée sur la partition active du firewall.
Version (firewall passif)	Ce champ n'apparaît que lorsque la HA est activée. Version de firmware installée sur la partition active du firewall passif.
Durée de fonctionnement (uptime)	Temps depuis lequel le firewall tourne sans interruption.
Date	Date et heure du firewall en temps réel.
Date d'expiration de la maintenance	Date de fin de validité de la maintenance du firewall.
Date d'expiration de la maintenance (firewall passif)	Ce champ n'apparaît que lorsque la HA est activée. Date de fin de validité de la maintenance du firewall passif.

Messages

Cette fenêtre liste les avertissements et alertes liées au système.

Services

Cette fenêtre présente l'état de certains services du firewall. De manière générale, la couleur de l'icône indique l'état du service :

- Couleur grise : service non disponible ou non activé sur le firewall,
- Couleur verte : état normal du service,
- Couleur orange : l'état du service requiert votre attention,
- Couleur rouge : état critique du service.

Les indicateurs pris en compte pour chacun des indicateurs de santé sont les suivants :

Management Center	État de la connexion entre le firewall et le serveur Stormshield Management Center.
Active Update	Date de mise à jour du module Active Update.
Sandboxing	État de la connexion aux serveurs Sandboxing.
Cloud Backup	État de la connexion à l'infrastructure Cloud Backup lorsque les sauvegardes automatiques sont activées.
Antivirus	Date de mise à jour des définitions virales. La couleur orange indique une mise à jour en cours de la base antivirale allégée.
Rapports	Activation des rapports Activation des graphiques historiques
Serveur syslog	État de la connexion aux serveurs syslog configurés sur le firewall. Si aucun serveur syslog n'est configuré, un clic sur ce service vous dirige vers le module de configuration correspondant (**Configuration** > **Notifications** > onglet **Syslog**).
Agent SSO	État de la connexion aux agents SSO configurés sur le firewall. Si aucun agent SSO n'est configuré, un clic sur ce service vous dirige vers le module de configuration des méthodes d'authentification.
RADIUS	État de la connexion aux serveurs RADIUS configurés sur le firewall. Si aucun serveur RADIUS n'est configuré, un clic sur ce service vous dirige vers le module de configuration des méthodes d'authentification.
Agents TS	État de la connexion aux Agents TS configurés sur le firewall. Si aucun Agent TS n'est configuré, un clic sur ce service vous dirige vers le module de configuration des méthodes d'authentification.
NTP	État de la connexion aux serveurs NTP référencés sur le firewall. Si le protocole NTP n'est pas utilisé, un clic sur ce service vous dirige vers le module de configuration des paramètres de date et d'heure.
Télémétrie	État du service de télémétrie. Si le service de télémétrie n'est pas actif, un clic sur ce service vous dirige vers le module de configuration générale du firewall.
Hostchecking (ZTNA)	État du service de vérification de la conformité des postes établissant des tunnels VPN (ZTNA). Trois états sont possibles : • Gris : le service ZTNA est désactivé. • Vert : le service ZTNA est activé et configuré. • Orange : le service ZTNA est activé et configuré en mode permissif. Un clic sur cette icône vous dirige vers l'onglet Vérification des postes clients (ZTNA) du module de configuration VPN SSL.

Indicateurs de santé

Cette fenêtre présente l'état des ressources matérielles du firewall. Un code couleur indique de manière visuelle cet état :

- Gris : ce module n'est pas disponible, installé ou activé sur votre firewall,
- Vert : les indicateurs de santé du module sont optimaux,
- Orange : la valeur d'un ou plusieurs indicateurs du module requiert votre attention,
- Rouge : la valeur d'un ou plusieurs indicateurs de santé du module est critique.

Cliquez sur un indicateurs de santé pour accéder directement au module de supervision ou de configuration correspondant.

Les indicateurs pris en compte pour chacun des indicateurs de santé sont les suivants :

Lien HA	État du lien dédié à la HA.
Alimentation	État des modules d'alimentation lorsque le firewall en est équipé. Les valeurs possibles sont les suivantes : « Alimenté », « Non alimenté » ou « Non détecté » (module absent ou défectueux).
Ventilateur	État du ventilateur lorsque le firewall en est équipé.
CPU	Pourcentage d'utilisation de votre processeur.
Mémoire	État de la mémoire utilisée par le firewall. Différents types de mémoire sont analysés : • **Machine** : pourcentage de la mémoire allouée au traitement d'une machine. • **Fragmenté** : pourcentage de la mémoire allouée pour le traitement des paquets fragmentés. • **Connexion** : pourcentage de la mémoire allouée pour le traitement des connexions. • **ICMP** : pourcentage de la mémoire allouée pour le protocole ICMP. • **Traces** : pourcentage de la mémoire utilisée pour le suivi des données (*Data Tracking*). • **Dynamique** : pourcentage de mémoire dynamique du moteur de prévention d'intrusion.
Disque	État du périphérique de stockage interne du firewall.
RAID	État de la redondance de données entre les disques physique du firewall.
Température	Température du firewall. Cet indicateur n'est pas disponible sur machine virtuelle.
Certificats	Dates de validité des certificats et CRL : • Certificat expirant dans moins de 30 jours, • Certificat dont la date de début de validité n'est pas encore atteinte, • Certificat expiré, • Certificat révoqué, • CRL d'une CA ayant atteint plus de la moitié de sa durée de vie ou l'atteignant dans moins de 5 jours, • CRL d'une CA expirée.

TPM	État du module TPM lorsque le firewall en est équipé. Les valeurs possibles sont les suivantes : • État en gris : le module TPM n'est pas initialisé. • État en vert : le module TPM est initialisé, opérationnel et protège au moins une clé privée. • État en orange : ◦ Le module TPM est initialisé, mais ne protège aucune clé privée. La valeur « *Le TPM est initialisé mais n'est pas utilisé* » confirme cet état. ◦ La politique de scellement du module TPM a été modifiée. Pour l'appliquer, vous devez sceller de nouveau le module TPM. La valeur « *Scellement du TPM requis pour appliquer la nouvelle politique de scellement du TPM* » confirme cet état. • État en rouge : ◦ Les tests sur le module TPM ne sont pas fonctionnels (celui-ci ne répond plus). ◦ L'accès au module TPM n'est plus possible car la valeur des empreintes des PCR de confiance a été modifiée. Pour les actualiser, vous devez sceller de nouveau le module TPM. La valeur « *Scellement du TPM requis pour retrouver l'accès au TPM* » confirme cet état. ◦ La fonctionnalité Secure Boot est désactivée. Un avertissement dans le widget **Messages** du **Tableau de bord** confirme que la fonctionnalité est désactivée. Un clic sur cet indicateur vous dirige dans le module Certificats et PKI. Pour plus d'informations sur comment sceller le module TPM, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.
SD-WAN	État de l'ensemble des objets routeurs du firewall et de leurs passerelles. Si aucun objet routeur ne supervise l'état de ses passerelles, un clic sur cet indicateur vous dirige dans le module de configuration des objets réseau.

Pay As You Go

Cet encadré n'est affiché que sur les firewalls virtuels EVA fonctionnant selon le modèle de licence Pay As You Go (facturation selon l'utilisation).

Ce modèle de licence peut être utilisé :

- De manière autonome si vous gérez votre firewall virtuel au sein de votre espace privé Mystormshield,
- Par intermédiaire d'un partenaire agréé qui gère alors votre firewall virtuel dans son propre espace Mystormshield.

Enrôlement de la machine virtuelle	Cette entrée précise si le firewall virtuel s'est correctement connecté au service Cloud Pay As You Go afin de récupérer son identité, son certificat et sa licence (.
Date d'expiration	Date de fin de validité de la licence Pay As You Go.
Code Web	Lorsque la machine est gérée en mode autonome, ce code Web vous permet de l'enregistrer dans votre espace privé Mystormshield.
Identifiant client	Cette entrée peut afficher un identifiant optionnel choisi lors de l'import de l'image d'installation ou lors de la création de cette image par le partenaire afin d'identifier le propriétaire de l'EVA.

Les modules de monitoring et de configuration

Les onglets **Monitoring** et **Configuration** du bandeau supérieur permettent d'accéder respectivement aux modules de monitoring et de configuration du firewall. Une fois un onglet ouvert, le menu situé à gauche permet d'accéder aux différents modules.

Le menu des modules se présente sous forme d'une colonne rétractable (bouton «) et propose plusieurs rubriques déroulantes ainsi qu'une liste des modules favoris.

Les modules favoris

Les modules favoris sont listés dans le menu déroulant situé sous l'icône ★.

Pour ajouter un module à la liste des favoris, cliquez sur l'icône ☆ située à droite de l'intitulé de ce module.

Accès aux modules

Pour accéder à un module, cliquez dessus. L'affichage au centre de la page s'actualise alors avec le contenu du module ouvert.

Si vous rencontrez des modules grisés dans les menus, cela peut indiquer :

- Qu'ils nécessitent une licence à laquelle vous n'avez pas souscrit, et donc, que vous n'y avez pas accès.
- Que l'utilisateur avec lequel vous êtes connecté n'a pas les privilèges nécessaires à l'accès de ces modules.

TRACES - SYSLOG - IPFIX

L'écran de configuration des traces se compose de 3 onglets :

- **Stockage local**,
- **Syslog**,
- **IPFIX**.

Onglet Stockage local

La configuration des traces permet d'allouer de l'espace disque pour chaque famille de traces du firewall. Ce menu permet également d'activer ou de désactiver l'enregistrement de ces traces sur le firewall.

	Active ou désactive l'enregistrement des traces sur le firewall. L'enregistrement est par défaut désactivé si le firewall ne possède pas de support de stockage.

Support de stockage

Support de stockage	Choisissez le support de stockage sur lequel enregistrer les traces : • Support de stockage interne du firewall, • Carte SD pour les firewalls disposant d'un support de stockage externe. **NOTE** Pour plus d'informations, reportez-vous au Guide de présentation et d'installation SNS, chapitre **Annexe B : stockage des traces**.
Actualiser	Actualise la liste des supports de stockage.
Formater	Formate le support de stockage.

NOTE
Dans une configuration en Haute Disponibilité (HA), les actions relatives à la carte SD ne sont valables que pour la carte insérée dans le firewall actif. Pour manipuler la carte SD du firewall passif, vous devez au préalable le basculer de passif à actif via le module **Maintenance**.

Configuration de l'espace réservé pour les traces

Il existe plusieurs familles pour lesquelles le firewall enregistre des traces d'événements détectés par les fonctions de journalisation ainsi que des données liées à des fonctionnalités de capture.

Les familles partagent un espace de stockage commun. Vous pouvez activer ou désactiver l'enregistrement des traces d'une famille ainsi que modifier son quota d'espace disque disponible en lui attribuant un pourcentage.

La grille

Activé	Affiche l'état d'activation de l'enregistrement des traces d'une famille. Effectuez un double-clic pour changer l'état d'activation.
Famille	Précise le nom de la famille de traces.
Pourcentage	Affiche le pourcentage d'espace disque attribué à la famille. Effectuez un double-clic pour le modifier. L'espace total réservé pour toutes les familles est affiché en bas de la grille. S'il dépasse 100 %, un message d'avertissement s'affiche. Les modifications sont toutefois autorisées. En cas de saturation du support de stockage, les traces les plus récentes effacent les traces les plus anciennes.
Quota d'espace disque	Affiche la proportion d'espace disque qu'occupe chaque famille sur le support de stockage. Cette valeur varie selon le pourcentage attribué.

Les boutons **Tout activer** et **Tout désactiver** permettent d'activer ou de désactiver en une seule action l'enregistrement des traces de toutes les familles.

Validez les modifications en cliquant sur **Appliquer**. Si l'espace total réservé dépasse 100 %, vous devez confirmer l'enregistrement des modifications.

Les familles de traces

Administration (serverd)	Événements liés au serveur d'administration des firewalls (serverd).
Authentification	Événements liés à l'authentification des utilisateurs.
Connexions réseau	Événements liés aux connexions autorisées à travers et à destination du firewall. Le log est écrit à la fin de la connexion.
Evénements système	Événements liés directement au système : arrêt et démarrage du firewall, erreur système, etc. L'arrêt et le démarrage des fonctions de journalisation correspondent à l'arrêt et au démarrage des démons qui génèrent les traces.
Alarmes	Événements liés à l'application des fonctions de prévention des intrusions.
Proxy HTTP	Événements liés au trafic HTTP.
Connexions applicatives (plugin)	Événements liés au traitement des plugins de l'ASQ.
Proxy SMTP	Événements liés au trafic SMTP.
Politique de filtrage	Événements liés à l'application des fonctions de filtrage.
VPN IPsec	Événements liés à l'établissement des SA.
VPN SSL	Événements liés à l'établissement du VPN SSL.
Proxy POP3	Événements liés à l'envoi des messages.
Statistiques	Événements liés au monitoring temps réel.
Management des vulnérabilités	Événements liés à l'application de consultation des vulnérabilités sur le réseau Stormshield Network Vulnerability Manager.
Proxy FTP	Événements liés au trafic FTP.
Proxy SSL	Événements liés au trafic SSL.

Sandboxing	Événements liés à l'analyse sandboxing des fichiers lorsque cette option a été souscrite et activée.
Captures réseau	Données issues des captures réseau déclenchées depuis le firewall.
Statistiques des routeurs	Données issues des statistiques des routeurs et de leurs passerelles.

Onglet Syslog

L'onglet *Syslog* permet de configurer jusqu'à 4 profils d'envoi de traces vers des serveurs Syslog.

Afin de renforcer la sécurité des traces transmises, les serveurs Syslog doivent être configurés avec des algorithmes conformes au RGS.

Les Syslog sont au format UTF-8 et respectent le standard WELF. Le format WELF est une suite d'éléments, écrits sous la forme champ=valeur et séparés par des espaces. Les valeurs sont éventuellement délimitées par des guillemets doubles.

Une trace correspond à une ligne terminée par un retour chariot (CRLF).

Profils Syslog

État	Active ou désactive le profil Syslog grâce à un double-clic.
Nom	Affiche le nom du profil Syslog.

Détails

Cette zone permet de visualiser ou de modifier la configuration du profil Syslog sélectionné dans la grille de gauche.

Nom	Nom attribué au profil Syslog.
Commentaire	Ce champ permet de rédiger un commentaire libre.
Serveur Syslog	Sélectionnez ou créez un objet machine correspondant au serveur Syslog. Il n'est pas possible de sélectionner un groupe.
Protocole	Sélectionnez le protocole utilisé pour l'envoi des traces vers le serveur : • UDP (perte de messages possible - messages envoyés en clair), • TCP (fiable - messages envoyés en clair), • TLS (fiable - messages cryptés). **NOTE** Il est recommandé de sélectionner TLS.
Port	Port utilisé par le serveur Syslog.
Autorité de certification	Ce champ n'est actif que lorsque le protocole TLS a été choisi. Indiquez l'autorité de certification (CA) ayant signé les certificat que présenteront le firewall et le serveur pour s'authentifier mutuellement.

Certificat serveur	Ce champ n'est actif que lorsque le protocole TLS a été choisi. Sélectionnez le certificat que doit présenter le serveur Syslog pour s'authentifier auprès du firewall. Vous ne pouvez pas sélectionner un certificat dont la clé privée est protégée par le module TPM.
Certificat client	Ce champ n'est actif que lorsque le protocole TLS a été choisi. Sélectionnez le certificat que doit présenter le firewall pour s'authentifier auprès du serveur Syslog. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module. Assurez-vous que le serveur Syslog dispose bien du certificat client sélectionné. Vous pouvez exporter le certificat au format P12 dans **Configuration > Objets > Certificats et PKI**.
Format	Choisissez le format Syslog à utiliser : • LEGACY (format limité à 1024 caractères par message Syslog), • LEGACY-LONG (pas de limite pour la longueur des messages), • RFC5424 (format respectant la RFC 5424).

Configuration avancée

Serveur de secours	Ce champ n'est actif que lorsque le protocole TLS ou TCP a été choisi. Sélectionnez ou créez un objet machine correspondant au serveur Syslog de secours. Il n'est pas possible de sélectionner un groupe.
Port de secours	Ce champ n'est actif que lorsque le protocole TLS ou TCP a été choisi. Port utilisé par le serveur Syslog de secours.
Catégorie (facility)	Permet d'associer à un système applicatif les logs envoyés au serveur Syslog.
Sekoia Intake Key	Si vous disposez d'un abonnement pour envoyer vos données vers les serveurs sekoia.io, entrez la clé d'authentification que vous a fournie Sekoia. Cette clé se compose de 32 caractères. Effacez la clé renseignée dans ce champ et validez la configuration pour désactiver ce service. **NOTE** Ce champ n'est affiché que lorsque le format syslog RFC 5424 et le protocole TLS ont été choisis.

Traces activées

Cette grille permet de sélectionner les traces devant être envoyées au serveur Syslog.

État	Active ou désactive l'envoi du fichier de traces sélectionné. Double-cliquez pour changer l'état.
Nom	Type de traces à envoyer (Alarme, Connexion, Web, Filtrage…).

Onglet IPFIX

Le protocole IPFIX (IP Flow Information Export), dérivé de Netflow, est un protocole de supervision de réseau permettant de collecter les informations sur les flux IP.

Ces flux sont caractérisés par l'envoi d'un patron (*template*) décrivant le type d'informations envoyées au collecteur. Pour un flux IPFIX basé sur le protocole TCP, ce patron est transmis uniquement lors de l'établissement de la connexion. Lorsque le flux IPFIX est basé sur le protocole UDP, le patron est envoyé régulièrement.

	Ce bouton permet d'activer ou de désactiver l'envoi des traces vers un collecteur IPFIX.
Collecteur IPFIX	Sélectionnez ou créez un objet machine correspondant au collecteur IPFIX. Il n'est pas possible de sélectionner un groupe.
Protocole	Sélectionnez le protocole sur lequel seront basés les flux IPFIX (TCP ou UDP).

Configuration avancée

Port	Choisissez un objet correspondant au port de communication entre le firewall et le collecteur IPFIX. La valeur proposée par défaut est **ipfix** (port 4739).
Collecteur IPFIX de secours	Ce champ n'est actif que lorsque le protocole sélectionné est TCP. Il est dans ce cas possible de préciser un collecteur vers lequel sont envoyés les messages IPFIX en cas d'indisponibilité du collecteur nominal. 10 minutes après avoir basculé ses flux vers le collecteur de secours, le firewall tente à nouveau de joindre le collecteur nominal. En cas d'échec, le firewall continue d'envoyer ses flux vers le collecteur de secours tout en réessayant régulièrement de joindre le collecteur nominal.
Port de secours	Ce champ n'est actif que lorsque le protocole sélectionné est TCP. Il s'agit du port d'écoute du collecteur IPFIX de secours

TRUSTED PLATFORM MODULE (TPM)

Le module TPM (*Trusted Platform Module*) présent sur certains firewalls SNS offre un stockage matériel renforçant le niveau de sécurité des certificats stockés sur le firewall SNS.

Si le firewall SNS dispose d'un module TPM, un indicateur "TPM" est présent dans le widget Indicateurs de santé du **Tableau de bord**. Retrouvez tous les modèles disposant d'un module TPM sur la page Nos firewalls Stormshield Network Security du site de Stormshield.

Pour utiliser le module TPM et protéger des clés privées de certificats, celui-ci doit être au préalable initialisé.

Initialiser le module TPM

Pour initialiser le module TPM, l'administrateur doit posséder le droit **Accès au TPM (E)**. Seul le compte *admin* peut attribuer ce droit dans le module **Configuration > Système > Administrateurs**, onglet Administrateurs, bouton **Passer en vue avancée**.

Pour initialiser le module TPM :

1. Rendez-vous dans le module **Configuration > Objets > Certificats et PKI**.
2. Cliquez sur **Init. TPM**.
3. Si la fonctionnalité Secure Boot n'est pas activée, un avertissement s'affiche. Il est recommandé d'activer la fonctionnalité Secure Boot avant d'initialiser le module TPM, mais vous pouvez le faire plus tard. Notez toutefois que la protection assurée par le module TPM sera incomplète tant que la fonctionnalité Secure Boot ne sera pas activée.
4. Dans la fenêtre **Définir le mot de passe**, définissez le mot de passe d'administration du module TPM :
   - Il doit respecter la politique de mots de passe définie sur le firewall SNS,
   - Il est recommandé de le générer aléatoirement avec une longueur d'au moins 64 caractères.
   - **Il doit être conservé dans un espace sécurisé et sauvegardé.** En cas de perte, il n'est pas possible de le réinitialiser et Stormshield n'est pas en mesure de le retrouver.
5. Sélectionnez les fonctionnalités pour lesquelles vous souhaitez protéger les clés privées de certificats utilisés. Les fonctionnalités qui n'utilisent pas de certificat dans leur configuration ne peuvent pas être sélectionnées. Vous pouvez également laisser toutes les cases décochées et protéger les clés privées de certificats du firewall SNS plus tard.
6. Cliquez sur **Terminer**.

Le module TPM est initialisé et le mécanisme de dérivation de la clé symétrique est utilisé pour générer la clé symétrique, que le firewall SNS soit membre d'un cluster en haute disponibilité ou non. Si le firewall SNS est membre d'un cluster en haute disponibilité, le module TPM du firewall passif est initialisé automatiquement.

Pour plus d'informations sur l'initialisation du module TPM, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.

Utiliser des certificats dont la clé privée est protégée par le module TPM

Le mécanisme de sécurisation par le module TPM s'applique aux certificats dans les cas ci-dessous. Reportez-vous aux sections de ces modules pour utiliser dans la configuration du firewall SNS des certificats dont la clé privée est protégée.

Dans ces modules, l'icône indique les certificats dont la clé privée est protégée par le module TPM.

- VPN IPsec (module Configuration > VPN > VPN IPsec),
- VPN SSL (module Configuration > VPN > VPN SSL),
- Déchiffrement SSL/TLS pour l'interface Web d'administration et le portail captif (module Configuration > Utilisateurs > Authentification),
- Communications avec le serveur SMC (module Configuration > Système > Management Center),
- Envois de logs vers un serveur syslog (module Configuration > Notifications > Traces - Syslog - IPFIX),
- LDAP interne (module Configuration > Utilisateurs > Configuration des annuaires).

Pour plus d'informations sur la protection par le module TPM des clés privées de certificats, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.

Précisions sur les cas d'utilisation avec le module TPM

- Des spécificités existent concernant l'état de chiffrement des clés privées protégées incluses dans le fichier de sauvegarde de configuration (module Configuration > Maintenance > Sauvegarde) :
  - Pour une sauvegarde manuelle, les clés privées protégées sont incluses déchiffrées car le mot de passe du TPM doit être renseigné,
  - Pour une sauvegarde automatique, les clés privées sont incluses, mais restent chiffrées.
- Une sauvegarde contenant des clés privées chiffrées ne peut être restaurée **que** sur le firewall d'origine. Sur un autre firewall SNS, les clés privées chiffrées ne peuvent pas être déchiffrées car la clé symétrique est supposément différente.
- Lors d'une configuration initiale d'un firewall SNS par clé USB, les opérations initTPM et p12import permettent d'interagir avec le module TPM.
- L'état du module TPM peut être pris en compte dans le calcul du facteur de qualité de la haute disponibilité (HA).

Pour plus d'informations sur ces cas d'utilisation, reportez-vous à la section Précisions sur les cas d'utilisation une fois le module TPM initialisé de la note technique *Configurer le module TPM et protéger les clés privées de certificats du firewall SNS*.

UTILISATEURS

Le service d'authentification des utilisateurs nécessite la création de comptes utilisateurs au niveau du firewall. Pour accéder aux fonctionnalités de ce module, vous devez avoir, au préalable, créé ou configuré votre base LDAP (voir la section CONFIGURATION DES ANNUAIRES).

Les comptes contiennent l'ensemble des informations relatives à ces utilisateurs :

- Identifiant de connexion,
- Nom,
- Prénom,
- Adresse e-mail (optionnel),
- Téléphone (optionnel),
- Description (optionnel).

L'écran des **Utilisateurs** se décompose en trois parties :

- Dans la partie supérieure, une barre d'outils affichant les différentes actions possibles,
- Dans la colonne de gauche, la liste des utilisateurs. Elle se compose de une à trois colonnes :
  - La colonne **CN** (affichée par défaut) qui reprend le nom des utilisateurs sous la forme *identifiant@annuaire*,
  - La colonne **DN** (masquée par défaut) qui affiche le *Distinguished Name* de l'utilisateur (champs CN, OU, O et DC caractérisant l'utilisateur dans son annuaire de référence),
  - La colonne **TOTP** (masquée par défaut) qui contient une coche verte pour chaque utilisateur authentifié par une méthode TOTP (*Time-based One Time Password* - Mot de passe à usage unique basé sur le temps).
- Dans la colonne de droite, le détail des caractéristiques de l'utilisateur sélectionné réparti dans trois onglets :
  - L'onglet **Compte** qui affiche les informations du compte listées ci-dessus,
  - L'onglet **Certificat** qui expose le détail du certificat de l'utilisateur lorsqu'il possède une identité dans la PKI du firewall,
  - L'onglet **Membre des groupes** qui liste les groupes de l'annuaire auxquels appartient l'utilisateur sélectionné.

Pour connaître les caractères autorisés ou interdits des différents champs à renseigner, reportez-vous à la section Noms autorisés.

Les actions possibles

La barre de recherche

Si vous recherchez un utilisateur ou un groupe d'utilisateurs en particulier, saisissez son nom.

Le champ de recherche vous permet de lister tous les utilisateurs et / ou groupes d'utilisateurs dont le nom, le prénom, et / ou l'identifiant (login) correspondent aux mots-clés saisis.

EXEMPLE
Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous les utilisateurs ou groupes d'utilisateurs possédant un « a » dans leur nom et / ou prénom.

Le filtre

Ce bouton permet de choisir le type de CN à afficher. Un menu déroulant vous propose les choix suivants :

Groupes et utilisateurs	Matérialisé par l'icône , cette option permet d'afficher dans la liste des CN à gauche, les utilisateurs et les groupes d'utilisateurs.
Utilisateurs	Matérialisé par l'icône , cette option permet d'afficher uniquement les utilisateurs dans la colonne de gauche.
Groupes	Matérialisé par l'icône , cette option permet d'afficher uniquement les groupes d'utilisateurs dans la colonne de gauche.

Ajouter un utilisateur

Pour créer un utilisateur, renseignez au moins son identifiant et son nom. Pour lui associer un certificat, vous devrez indiquer une adresse e-mail valide.

Identifiant (login)	Identifiant de connexion de l'utilisateur
Nom	Nom de l'utilisateur
Prénom	Prénom de l'utilisateur
Mail	Adresse e-mail de l'utilisateur. Celle-ci sera utile pour la création d'un certificat.
Téléphone	Numéro de téléphone de l'utilisateur.
Description	Description indicative à l'utilisateur.

NOTE
Les champs « Identifiant », « Nom » et « Prénom » ne seront plus modifiables après leur création.

Afin de valider la création de votre utilisateur et de ne perdre aucune modification apportée, cliquez sur **Appliquer**.

Une fenêtre proposant la création d'un mot de passe pour cet utilisateur s'affiche alors :

Mot de passe	Saisissez le mot de passe de l'utilisateur.
Confirmez le mot de passe	Confirmez le mot de passe.
Robustesse du mot de passe	Une jauge indiquant la robustesse du mot de passe choisi est affichée.

Cliquez sur le bouton **Appliquer** de cette fenêtre pour valider la création du mot de passe.

NOTE
La création du mot de passe utilisateur n'est pas obligatoire. Il suffit de cliquer sur le bouton **Annuler** de la fenêtre pour passer cette étape.

Ajouter un groupe

L'écran du module **Utilisateurs** vous propose, dans la colonne de droite, de renseigner les informations du groupe que vous souhaitez créer.

Nom du groupe	Donner un nom à votre groupe afin de l'identifier dans la liste des CN. **NOTE** Vous ne pourrez plus changer le nom de votre groupe une fois ce dernier créé.
Description	Vous pouvez décrire le groupe et modifier le contenu de sa description dès que vous le souhaitez. Remplir ce champ reste facultatif mais néanmoins recommandé.

CN

Filtrer (barre de recherche)	Vous pouvez saisir une chaîne de caractères afin de filtrer la liste des membres, ou vider ce champ pour afficher la liste complète.
Ajouter	Il est possible d'ajouter un utilisateur au groupe de 2 manières différentes : • Lorsque vous cliquez sur le bouton **Ajouter**, une ligne vide vient se positionner en haut du tableau. Déroulez la liste des utilisateurs existants à l'aide de la flèche de droite et sélectionnez celui que vous désirez inclure au groupe. • Vous pouvez également effectuer un 'glisser-déposer' en important un utilisateur depuis la liste des CN, dans la colonne de gauche.
Supprimer	Pour retirer un membre du groupe, sélectionnez-le et cliquez sur le bouton **Supprimer**. Lorsqu'un utilisateur est supprimé, la révocation de son certificat est proposée à l'administrateur.

Afin de valider la création de votre groupe et de ne perdre aucune modification apportée, cliquez sur **Appliquer**.

Supprimer un utilisateur sans certificat

Ce bouton permet de supprimer un utilisateur ou un groupe.

Pour un groupe ou un utilisateur ne possédant pas de certificat issu de la PKI du firewall

1. Sélectionnez l'utilisateur ou le groupe à supprimer.
2. Cliquez sur **Supprimer.**
   Une fenêtre affichant le message « *Confirmez-vous l'effacement de l'utilisateur <nom de l'utilisateur>* » s'affiche.
3. Cliquez sur **Oui**.

Pour un utilisateur possédant un certificat issu de la PKI du firewall

1. Sélectionnez l'utilisateur à supprimer.
2. Cliquez sur **Supprimer.**
   Une fenêtre affichant le message « *Confirmez-vous l'effacement de l'utilisateur <nom de l'utilisateur>* » s'affiche.
3. Saisissez le **Mot de passe de la CA** (mot de passe de l'autorité émettrice du certificat).

4. Cochez la case **Exporter la CRL après sa mise à jour** si vous souhaitez conserver une copie de la CRL.
5. Dans ce cas, choisissez le **Format du fichier** d'export de la CRL :
   - Format Base64 (PEM),
   - Format binaire (DER).
6. Cliquez sur **Appliquer**.
7. Si vous avez choisi d'exporter la CRL, une fenêtre vous présente le lien de téléchargement du fichier d'export de la CRL.

Vérifier l'utilisation

Matérialisé par l'icône , ce bouton vous renseigne sur les groupes dont vos utilisateurs font partie, ainsi que sur l'utilisation de l'utilisateur ou du groupe dans le reste de la configuration.

EXEMPLE
Le filtrage :

1. Sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez vérifier l'utilisation.
2. Cliquez sur le bouton **Vérifier l'utilisation**.
   L'arborescence des menus de gauche vous présente votre utilisateur / groupe (par son identifiant) au sein de l'onglet *User ans groups*, et affiche la liste des groupes dont celui-ci fait partie, ainsi que son utilisation dans la configuration du firewall.

Réinitialiser l'enrôlement TOTP de l'utilisateur

Ce bouton n'est disponible que lorsque l'utilisateur sélectionné s'est authentifié sur le firewall via la méthode TOTP.

En cliquant sur ce bouton, vous réinitialisez l'enrôlement TOTP de l'utilisateur : à la prochaine connexion aux services du firewall soumis à l'authentification TOTP, cet utilisateur devra donc de nouveau suivre la procédure complète d'enrôlement TOTP.

NOTE
Il n'est pas possible du supprimer de la base TOTP un utilisateur ayant les droits d'administration.

Les interactions

Certaines opérations, listées dans la barre des tâches, peuvent être réalisées en effectuant un clic droit sur la grille des utilisateurs / groupes (grille CN) :

- Ajouter un utilisateur,
- Ajouter un groupe,
- Supprimer (l'utilisateur ou le groupe sélectionné),
- Vérifier l'utilisation (de l'utilisateur ou du groupe sélectionné),
- Réinitialiser l'enrôlement TOTP de l'utilisateur sélectionné.

La liste des utilisateurs (CN)

Lorsque vous souhaitez accéder aux données d'un utilisateur, sélectionnez-le dans la liste des CN de gauche, et les informations le concernant apparaissent dans la colonne de droite.

Onglet Compte

Créer ou modifier le mot de passe	En cliquant sur cette option, vous pouvez créer le mot de passe d'authentification de l'utilisateur dans une fenêtre spécifique, affichant également le niveau de sécurité. **NOTE** Pour autoriser l'utilisateur à modifier son mot de passe lui-même, il faut vous rendre dans le module **Utilisateurs > Authentification**, onglet **Profils du portail captif**, zone **Configuration avancée > Mot de passe des utilisateurs**.
Droits d'accès	Ce raccourci permet d'afficher directement les droits d'accès de l'utilisateur situés dans le module **Utilisateurs** > **Droits d'accès**.
Id (non modifiable)	L'identifiant de connexion de l'utilisateur sélectionné.
Nom (non modifiable)	Le nom de l'utilisateur sélectionné.
Prénom (non modifiable)	Le prénom de l'utilisateur sélectionné.
E-mail	Indique l'adresse e-mail de l'utilisateur sélectionné.
Téléphone	Le numéro de téléphone de l'utilisateur sélectionné.
Description	Description relative à l'utilisateur sélectionné.

TOTP

Ce cadre n'est affiché que lorsque l'utilisateur sélectionné s'est authentifié sur le firewall via la méthode TOTP.

Code TOTP à vérifier	Ce champ permet de vérifier la validité d'un code TOTP utilisé pour se connecter aux services du firewall soumis à l'authentification TOTP.
Réinitialiser l'enrôlement	En cliquant sur ce bouton, vous réinitialisez l'enrôlement TOTP de l'utilisateur : à la prochaine connexion aux services du firewall soumis à l'authentification TOTP, cet utilisateur devra donc de nouveau suivre la procédure complète d'enrôlement TOTP. **NOTE** Il n'est pas possible du supprimer de la base TOTP un utilisateur ayant les droits d'administration.

Onglet Certificat

Cet onglet vous permet de gérer le certificat x509 de l'utilisateur.

La PKI ne possédant pas d'Autorité de certification pas défaut, vous devez en créer une afin de gérer les certificats des utilisateurs : il faut vous rendre dans le module **Objets > Certificats et PKI**, bouton **Ajouter > Ajouter une autorité racine**.

Ce certificat peut servir dans deux cas : authentification via SSL et accès en VPN au firewall avec un client mobile IPsec. Ce certificat peut aussi être utilisé par d'autres applications.

Onglet Membres des groupes

Il permet d'inclure l'utilisateur dans un ou plusieurs groupes :

1. Cliquez sur le bouton **Ajouter**.
   Une ligne vierge vient s'ajouter au tableau des groupes.
2. Sélectionnez la flèche à droite du champ.
   Un menu déroulant vous propose une liste de groupes existants.
3. Cliquez sur le groupe de votre choix.
   Celui-ci vient s'ajouter à votre tableau.

Pour retirer un groupe, sélectionnez-le et cliquez sur le bouton **Supprimer**.

Par exemple, une personne, rattachée à de nombreux services peut appartenir à de nombreux groupes différents. Le nombre maximum est maintenant de 50 groupes par utilisateur.

VPN IPSEC

Protocole standard, l'IPsec (IP Security) permet la création de tunnels VPN entre deux machines, entre une machine et un réseau, entre deux réseaux et tout type d'objet supportant le protocole.

Les services proposés par l'IPsec Stormshield Network offrent le contrôle d'accès, l'intégrité en mode non connecté, l'authentification de l'origine des données, la protection contre le rejeu, la confidentialité au niveau du chiffrement et sur le flux de trafic. Vous pouvez par exemple créer un tunnel entre deux firewalls ou entre le firewall et des clients mobiles sur lesquels seraient installés des clients VPN.

Recommandations

Lorsqu'un VPN IPsec est configuré, il est recommandé de :

- Configurer une route statique à destination de la boucle locale (*blackholing*) pour joindre les réseaux distants accessibles au travers de tunnels VPN IPsec,
- S'assurer que la politique IPsec n'est jamais désactivée y compris lors de phases transitoires,
- S'assurer que les règles de filtrage sont toujours plus spécifiques que les règles de NAT avant IPsec,
- S'assurer que les flux (adresse IP source et destination) après la translation (NAT) correspondent à la politique IPsec,
- S'assurer qu'en l'absence de règles de NAT, les règles de filtrage sont toujours plus spécifiques que la politique IPsec.

Mécanisme d'optimisation des opérations de chiffrement et déchiffrement

Le service IPsec bénéficie d'un mécanisme destiné à optimiser la répartition des opérations de chiffrement et de déchiffrement. Son but est d'améliorer de manière notable les débits IPsec notamment dans le cas d'une configuration comportant un seul tunnel IPsec.

Il dispose de 3 modes de configuration :

Mode Automatique (auto)	Il s'agit du mode par défaut. Il permet au mécanisme d'optimisation de s'enclencher automatiquement et de manière transparente dans le cas où les deux conditions suivantes sont remplies : • La politique IPsec active possède un seul tunnel VPN actif. • Le modèle de firewall supporte le mode **Automatique**. Les modèles qui supportent le mode **Automatique** sont : SN510, SN710, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100 et SNi40. Pour les autres, seul le mode **Activé** permet d'enclencher le mécanisme d'optimisation.
Mode Activé (1)	Il permet d'enclencher de manière permanente et sans condition particulière le mécanisme d'optimisation. Il peut être paramétré sur tous les modèles de firewalls. Son utilisation n'est pas recommandée dans le cas où une politique IPsec possède un nombre important de tunnels VPN actifs. De manière générale, assurez-vous que l'utilisation du mode **Activé** n'affecte pas la qualité de votre service.
Mode Désactivé (0)	Il permet de désactiver de manière permanente le mécanisme d'optimisation.

La configuration du mode s'effectue uniquement à l'aide de la commande CLI / Serverd suivante :

```
CONFIG IPSEC UPDATE slot=<n> CryptoLoadBalance=<0|1|auto>
```

Le détail de cette commande est disponible dans le Guide de référence des commandes CLI / Serverd.

Écran du module VPN IPsec

L'écran du module VPN IPsec est composé de quatre onglets :

- **Politique de chiffrement – Tunnels** : créez des tunnels IPsec entre deux firewalls (**Site à site – Gateway- Gateway**) ou entre un firewall multifonctions Stormshield Network et un utilisateur mobile (**Mobile – Utilisateurs nomades**).
  10 profils de chiffrement vierges peuvent être configurés, activés et édités. La politique mobile permet aussi de configurer des tunnels avec un autre firewall, mais qui ne dispose pas d'une adresse IP fixe. Il a alors la même contrainte qu'un client mobile "classique": une adresse IP non prévisible.
- **Correspondants** : créez de nouveaux correspondants (site distant ou correspondant mobile) en renseignant notamment leur **profil IKE**, leur méthode de négociation, ainsi que les paramètres spécifiques à chaque méthode de négociation.
- **Identification** : listez vos autorités de certification acceptées dans les tunnels utilisant les méthodes PKI, ainsi que les clés pré-partagées (PSK) de vos tunnels mobiles.
- **Profils de chiffrement** : définissez vos profils de chiffrement IKE (phase 1) et IPsec (phase 2), ajoutez-en de nouveaux, établissez leur durée de vie maximum (en secondes). Vous pouvez également définir les propositions de négociation au niveau des algorithmes d'authentification et de chiffrement.

NOTES

- Les politiques VPN IPsec proposent d'éditer leur configuration en mode Global. Pour activer l'option, sélectionnez "Afficher les politiques globales" dans le module Préférences.
- Il n'existe pas de droit spécifique au "vpn global".

L'onglet Politique de chiffrement – Tunnels

Une politique IPsec peut regrouper des correspondants utilisant des versions différentes du protocole IKE avec des limitations dans l'utilisation du protocole IKEv1 (cf. section ***Précisions sur les cas d'utilisation*** des ***Notes de Version v4***).

La barre des profils	Le menu déroulant propose 10 profils IPsec numérotés de (01) à (10). Pour sélectionner un profil afin d'établir une configuration, cliquez sur la flèche à droite du champ.
Activer cette politique	Active immédiatement la politique IPsec sélectionnée : les paramètres enregistrés dans cette politique écrasent les paramètres en vigueur.

Actions	Cette fonction permet d'effectuer 3 actions sur les profils : • **Éditer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mettre à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Suppression de toutes les modifications apportées au profil. La configuration sera alors perdue. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure de la dernière modification effectuée. L'heure affichée est celle du boîtier et non celle de votre poste.
Désactiver la politique	Ce bouton permet de désactiver immédiatement la politique IPsec sélectionnée.

Site à site (Gateway - Gateway)

Cet onglet permet de créer un tunnel VPN entre deux éléments réseaux supportant la norme IPsec. On appelle également ce type de procédé : *Tunnel VPN passerelle à passerelle* ou *tunnel Gateway to Gateway*.

Plusieurs tutoriels vous guident pas à pas pour la configuration d'une connexion sécurisée entre vos sites. Cliquez sur l'un des liens pour y accéder :

- VPN IPsec : Authentication par clé pré-partagée,
- VPN IPsec : Authentification par certificats,
- VPN IPsec : Configuration Hub and Spoke.

Rechercher	La recherche s'effectuera sur le nom de l'objet et de ses différentes propriétés, sauf si vous avez spécifié dans les préférences de l'application de restreindre cette recherche aux noms d'objet.
Ajouter	Le bouton **Ajouter** est détaillé dans la section suivante.
Supprimer	Sélectionnez le tunnel VPN IPsec à retirer de la grille et cliquez sur ce bouton.
Monter	Placer la ligne sélectionnée avant celle du dessus.
Descendre	Placer la ligne sélectionnée après celle du dessous.
Couper	Couper la ligne dans le but de la coller.
Copier	Copier la ligne dans le but de la dupliquer.
Coller	Dupliquer la ligne après l'avoir copiée.

Afficher les détails	Pour faciliter la configuration du tunnel avec un équipement distant (passerelle ou client mobile), un clic sur cette icône affiche les différentes informations de la politique IPsec : • **Résumé** : ◦ Type de règle : Passerelle, ◦ Version IKE, ◦ Correspondant, ◦ Passerelle distante, ◦ Réseau local, ◦ Réseau distant. • **Authentification** : ◦ Mode : Auto, ◦ Type : Certificat ou Clé pré-partagée (PSK), • **Profils IKE (phase 1)** : ◦ DH par défaut, ◦ Durée de vie, ◦ Propositions. • **Profil IPsec (phase2)** : ◦ Durée de vie, ◦ Authentification, ◦ Chiffrement, ◦ PFS.
Chercher dans les logs	Lorsque un nom a été attribué à la règle IPsec, un clic sur ce bouton lance la recherche du nom de la règle dans le log VPN IPsec et affiche le résultat.
Chercher dans la supervision	Un clic sur ce bouton ouvre directement l'écran de supervision des tunnels IPsec (onglet **Monitoring** > module **Supervision** > **Tunnels VPN IPsec**).

REMARQUE
Un clic droit depuis n'importe quelle zone de la grille affiche un menu contextuel proposant les actions suivantes :

- **Ajouter**,
- **Copier**,
- **Couper**,
- **Coller**,
- **Afficher les détails**,
- **Supprimer**,
- **Chercher dans les logs**,
- **Chercher dans la supervision**.

Ajouter

Afin de réaliser la configuration du tunnel, sélectionnez la politique VPN dans laquelle vous désirez réaliser le tunnel. L'assistant de politique VPN IPsec vous aiguille alors dans la configuration.

Tunnel site à site simple

Vous allez ici définir chacune des extrémités de votre tunnel ainsi que le correspondant.

Ressources locales	Machine, groupe de machines, réseau ou groupe de réseaux qui vont être accessibles via le tunnel VPN IPsec.
Choix du correspondant	Ceci est l'objet correspondant à l'adresse IP publique de l'extrémité du tunnel, soit, du correspondant VPN distant. La liste déroulante affiche par défaut « None ». Vous pouvez créer un correspondant via l'option suivante ou en choisir un dans la liste de ceux qui existent déjà.
Créer un correspondant	Définissez les paramètres de votre correspondant, plusieurs étapes sont nécessaires : Étape 1 : Sélectionner la passerelle. 1. **Passerelle distante** : choisissez l'objet correspondant à l'adresse IP de l'extrémité du tunnel au sein de la liste déroulante. Vous pouvez également en ajouter à l'aide du bouton . 2. **Nom** : vous pouvez spécifier un nom pour votre passerelle ou conserver le nom d'origine du correspondant, qui sera précédé de la mention « Site_ » (« Site_<nom de l'objet> »). Un choix de correspondant *None* permet de générer des politiques sans chiffrement. L'objectif est de créer une exclusion aux règles suivantes de la politique de chiffrement. Le trafic de cette règle sera régit par la politique de routage. 3. **Version IKE** : sélectionnez IKEv1 ou IKEv2 selon le version du protocole IKE utilisée par le correspondant. 4. Cliquez sur **Suivant**. Étape 2 : Identification du correspondant. 2 choix sont possibles : • **Certificat** • **Clé pré-partagée (PSK** – Pre-Shared Key**)**. 1. Cochez l'option voulue. 2. Si vous optez pour le **Certificat**, vous devrez le sélectionner parmi ceux que vous avez créé préalablement au sein du module Certificats et PKI. Le certificat à renseigner ici est celui présenté par le firewall et non celui présenté par le site distant. Il est également possible d'ajouter une autorité de certification. 3. Si vous optez pour la **Clé pré partagée (PSK),** il vous faudra définir le secret que partageront les deux correspondants du tunnel VPN IPsec, sous forme d'un mot de passe à confirmer dans un second champ. Vous pouvez **Saisir la clé en caractères ASCII** (chaque caractère d'un texte en ASCII est stocké dans un octet dont le 8e bit est 0.) en cochant la case correspondante. Décochez la case pour afficher la clé en caractères hexadécimaux (dont le principe repose sur 16 signes : les lettres de A à F et les chiffres de 0 à 9). **NOTE** Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur.

4. Cliquez sur **Suivant.**
   L'écran vous présente une fenêtre récapitulative de la configuration effectuée, les **Paramètres du site distant** et la **Clé pré partagée**.
   Vous pouvez également ajouter un correspondant de secours en cliquant sur le lien joint. Vous devrez renseigner la passerelle distante.
5. Cliquez sur **Terminer**.

Réseaux distants	Machine, groupe de machines, réseau ou groupe de réseaux accessibles via le tunnel IPsec avec le correspondant.

Séparateur (regroupement de règles)

Cette option permet d'insérer un séparateur au-dessus de la ligne sélectionnée. Cela peut permettre à l'administrateur de hiérarchiser ses tunnels comme il le souhaite.

La grille

Ligne	Cette colonne indique le numéro de la ligne (1,2,3…) traitée par ordre d'apparition à l'écran.
État	Cette colonne affiche l'état on / off du tunnel. Lorsque vous créez un tunnel, celui-ci s'active par défaut : cliquez deux fois dessus pour le désactiver.
Nom	Il vous est possible d'attribuer un nom à cette règle IPsec afin de faciliter la recherche des événements propres à cette règle dans les logs.
Réseau local	Choisissez votre machine, groupe de machines, réseau ou groupe de réseaux qui sera accessible via le tunnel VPN IPsec, au sein de la liste déroulante d'objets.
Correspondant	Configuration de correspondant, visible au sein de l'onglet du même nom dans le module VPN IPsec.
Réseau distant	Choisissez parmi la liste déroulant d'objets, votre machine, groupe de machines, réseau ou groupe de réseaux accessibles via le tunnel IPsec avec le correspondant.
Protocole	Cette option permet de limiter l'établissement du tunnel IPsec aux flux basés sur un protocole particulier : • TCP • UDP • ICMP • GRE • Tous
Profil de chiffrement	Cette option permet de choisir le modèle de protection de Phase 2 associé à votre politique VPN, parmi les 3 profils pré-configurés : **StrongEncryption, GoodEncryption et Mobile.** Il est possible de créer ou de modifier d'autres profils au sein de l'onglet *Profils de chiffrement*.

Keepalive	L'option supplémentaire **Keepalive** permet de maintenir les tunnels montés de façon artificielle. Cette mécanique envoie des paquets initialisant et forçant le maintien du tunnel. Cette option est désactivée par défaut pour éviter une charge inutile, dans le cas de configuration contenant de nombreux tunnels, montés en même temps sans réel besoin. Pour activer cette option, affectez une valeur différente de 0, correspondant à l'intervalle en seconde, entre chaque envoi de paquet UDP.
Commentaire	Description associée à la politique VPN.

Vérification en temps réel de la politique

L'écran d'édition des règles de politique IPsec dispose d'un champ de « **Vérification de la politique** » (situé en dessous de la grille), qui prévient l'administrateur en cas d'incohérence ou d'erreur sur une des règles créées.

Utilisateurs mobiles (nomades)

Le VPN IPsec comporte deux extrémités : l'extrémité de tunnel, et l'extrémité de trafic. Pour les utilisateurs mobiles, l'adresse IP d'extrémité de tunnel n'est pas connue à l'avance.

L'adresse IP d'extrémité de trafic, quant à elle, peut être soit choisie par le correspondant (cas « classique »), ou distribuée par la passerelle (« Mode Config »).

Il est possible de construire une politique IPsec mobile contenant plusieurs correspondants dès lors qu'ils utilisent le même profil de chiffrement IKE. En cas d'authentification par certificats, les certificats des différents correspondants doivent être issus d'une même CA.

Ajouter

Sélectionnez la politique VPN dans laquelle vous désirez réaliser le tunnel. Des assistants de création de politique vous aiguillent dans cette configuration. Si vous souhaitez créer le correspondant mobile par l'assistant, reportez-vous à la section **« Création de correspondant mobile »** ci-dessous.

Pour les utilisateurs mobiles, il est possible de définir des paramètres clients VPN (Mode Config) par l'assistant de création de *politique Mode Config*.

Nouvelle politique mobile simple

Cette politique rend accessible via un tunnel IPsec, les réseaux locaux aux utilisateurs autorisés. Dans cette configuration, les utilisateurs distants se connectent avec leur propre adresse IP.

Renseignez le correspondant mobile à utiliser. Puis, ajoutez dans la liste, les ressources locales accessibles.

Nouvelle politique Mode Config

Cette politique avec Mode Config rend accessible via un tunnel IPsec, un unique réseau local aux utilisateurs autorisés. Avec Mode Config, les utilisateurs distants se connectent avec une adresse IP attribuée dans un ensemble défini en tant que "Réseau mobile".

Une fois créée, la cellule correspondant à la colonne Mode Config propose un bouton **Éditer le mode Config (sélection)**, vous permettant de renseigner les paramètres du Mode Config IPsec, décrits dans la section **« La grille ».**

Vous pouvez renseigner un serveur DNS particulier et spécifier les domaines d'utilisation de ce serveur. Ces indications sont par exemple, indispensables en cas d'utilisation d'un client mobile Apple® (iPhone, iPad). Cette fonctionnalité est couplée au mode Config, et n'est pas utilisée par tous les clients VPN du marché.

Création de correspondant mobile

La procédure à suivre pour créer un correspondant par ces assistants, est décrite ci-dessous. Vous pouvez également le créer directement depuis l'onglet *Correspondant*.

1. Cliquez sur le bouton « **Ajouter** » une « **Nouvelle Politique** » VPN, puis sur « **Créer un correspondant mobile** » via l'assistant de politique VPN IPsec mobile.
2. Donnez un **Nom** à votre configuration mobile.
3. Choisissez la **Version** (du protocole) **IKE** utilisée par le correspondant.
4. Cliquez sur **Suivant**.
5. Choisissez la méthode d'authentification du correspondant.

Certificat	Si vous optez pour cette méthode d'authentification, vous devrez ensuite choisir votre **Certificat** (serveur) à présenter au correspondant, parmi la liste de ceux que vous avez créés au préalable (**Module Certificats et PKI**). Vous pourrez également fournir l'« **Autorité de confiance** » (CA) ayant signé le certificat de votre correspondant afin qu'elle soit automatiquement ajoutée à la liste des autorités de confiance.
Clé pré-partagées	Si vous optez pour cette méthode d'authentification, vous devrez éditer votre clé dans un tableau, en fournissant son ID, et sa valeur à confirmer. Pour cela, cliquez sur **Ajouter**. L'ID peut-être au format IP (X.Y.Z.W), FQDN (monserveur.domain.com), ou e-mail (prenom.nom@domain.com). Il occupera ensuite la colonne « Identité » du tableau et la PSK occupera une colonne du même nom avec sa valeur affichée en hexadécimal. **NOTE** Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur.
EAP-Generic Token Card (GTC)	La méthode EAP-GTC (Extensible Authentication Protocol - Generic Token Card) est décrite dans la RFC 3748. Elle n'est disponible que pour les correspondants mobiles en version IKEv2. Elle est destinée à être utilisée avec les cartes supportant les vérifications de type *challenge / response*. Si vous optez pour cette méthode d'authentification, vous devrez ensuite choisir le **Certificat** (serveur) que le firewall doit présenter au correspondant pour s'authentifier. Vous pourrez également fournir l'« **Autorité de confiance** » (CA) ayant signé le certificat de votre correspondant afin qu'elle soit automatiquement ajoutée à la liste des autorités de confiance. La grille **Groupes** vous permet d'ajouter directement des groupes d'utilisateurs à rattacher à ce profil de correspondant. Ces groupes peuvent être issus de l'annuaire LDAP par défaut ou d'un autre annuaire (domaine).

Certificat et EAP-Generic Token Card (GTC)	La méthode EAP-GTC (Extensible Authentication Protocol - Generic Token Card) est décrite dans la RFC 3748. Elle n'est disponible que pour les correspondants mobiles en version IKEv2. Elle est destinée à être utilisée avec les cartes supportant les vérifications de type *challenge / response*. Si vous optez pour cette méthode d'authentification, vous devrez ensuite choisir le **Certificat** (serveur) vous devrez ensuite choisir le **Certificat** (serveur) que le firewall doit présenter au correspondant pour s'authentifier. Vous pourrez également fournir l'« **Autorité de confiance** » (CA) ayant signé le certificat de votre correspondant afin qu'elle soit automatiquement ajoutée à la liste des autorités de confiance. La grille **Groupes** vous permet d'ajouter directement des groupes d'utilisateurs à rattacher à ce profil de correspondant. Ces groupes peuvent être issus de l'annuaire LDAP par défaut ou d'un autre annuaire (domaine).

6. Cliquez sur **Suivant**.
7. Vérifiez l'écran de résumé de votre configuration mobile et cliquez sur **Terminer**.
8. Renseignez ensuite la ressource locale, ou « **réseau local** » auquel l'utilisateur mobile aura accès.

Vous pouvez également effectuer d'autres actions :

Rechercher	La recherche s'effectuera sur le nom de l'objet et de ses différentes propriétés, sauf si vous avez spécifié dans les préférences de l'application de restreindre cette recherche aux noms d'objet.
Supprimer	Sélectionnez le tunnel VPN IPsec à retirer de la grille et cliquez sur ce bouton.
Monter	Placer la ligne sélectionnée avant celle du dessus.
Descendre	Placer la ligne sélectionnée après celle du dessous.
Couper	Couper la ligne dans le but de la coller.
Copier	Copier la ligne dans le but de la dupliquer.
Coller	Dupliquer la ligne après l'avoir copiée.

Afficher les détails	Pour faciliter la configuration du tunnel avec un équipement distant (passerelle ou client mobile), un clic sur cette icône affiche les différentes informations d'une règle sélectionnée dans la politique IPsec : • **Résumé** : ◦ Type de règle : Correspondants mobiles, ◦ Version IKE, ◦ Correspondant, ◦ Passerelle distante : *Any* dans le cas d'un correspondant mobile, ◦ Réseau local, ◦ Réseau distant. • **Authentification** : ◦ Mode : Auto, ◦ Type : Certificat, Clé pré-partagée (PSK), EAP-Generic Token Card (GTC) ou Certificat et EAP-Generic Token Crd (GTC). • **Profils IKE (phase 1)** : ◦ DH par défaut, ◦ Durée de vie, ◦ Propositions. • **Profil IPsec (phase2)** : ◦ Durée de vie, ◦ Authentification, ◦ Chiffrement, ◦ PFS.
Chercher dans les logs	Lorsque un nom a été attribué à la règle IPsec, un clic sur ce bouton lance la recherche du nom de la règle dans le log VPN IPsec et affiche le résultat.
Chercher dans la supervision	Un clic sur ce bouton ouvre directement l'écran de supervision des tunnels IPsec (onglet **Monitoring** > module **Supervision** > **Tunnels VPN IPsec**).

REMARQUE
Un clic droit depuis n'importe quelle zone de la grille affiche un menu contextuel proposant les actions suivantes :

- **Ajouter**,
- **Copier**,
- **Couper**,
- **Coller**,
- **Afficher les détails**,
- **Supprimer**,
- **Chercher dans les logs**,
- **Chercher dans la supervision**.

La grille

Ligne	Cette colonne indique le numéro de la ligne (1,2,3…) traitée par ordre d'apparition à l'écran
État	Cette colonne affiche l'état on / off du tunnel. Lorsque vous créez un tunnel, celui-ci s'active par défaut : cliquez deux fois dessus pour le désactiver.
Nom	Il vous est possible d'attribuer un nom à cette règle IPsec afin de faciliter la recherche des événements propres à cette règle dans les logs.
Réseau local	Choisissez votre machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux qui sera accessible via le tunnel VPN IPsec, au sein de la liste déroulante d'objets.
Correspondant	Configuration de correspondant, visible au sein de l'onglet du même nom dans le module VPN IPsec.
Réseau distant	Choisissez parmi la liste déroulant d'objets, votre machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux accessibles via le tunnel IPsec avec le correspondant. **NOTE** Lorsque vous créez une nouvelle politique VPN IPsec mobile via l'assistant, il vous est demandé de fournir le réseau local, et non le réseau distant, puisque l'adresse IP n'est pas connue. L'objet « Any » sera donc choisi par défaut.
Nom de domaine	Cette option permet de préciser le domaine (annuaire LDAP) sur lequel le correspondant mobile doit être authentifié. Un même utilisateur peut ainsi établir simultanément plusieurs tunnels VPN IPsec et accéder à des ressources distinctes en s'authentifiant sur des annuaires différents.
Groupe	Cette option permet de préciser le groupe de l'utilisateur au sein du domaine d'authentification. Un même utilisateur peut alors établir simultanément plusieurs tunnels VPN IPsec en s'authentifiant sur un ou plusieurs domaines, et accéder à des ressources distinctes en se voyant attribuer les droits propres au groupe précisé. Cette option nécessite de préciser le **Nom de domaine**.
Protocole	Cette option permet de limiter l'établissement du tunnel IPsec aux flux basés sur un protocole particulier : • TCP • UDP • ICMP • GRE • Tous
Profil de chiffrement	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils pré-configurés : **StrongEncryption, GoodEncryption** et **Mobile**. Il est également de créer et de modifier d'autres profils au sein de l'onglet *Profils de chiffrement*.

Mode Config	Cette colonne rend possible l'activation du « Mode Config », désactivé par défaut. Ce mode permet de distribuer l'adresse IP d'extrémité de trafic au correspondant. **NOTES** 1. Si vous choisissez d'activer ce mode, vous devrez sélectionner un objet autre qu'« Any » en tant que réseau distant. 2. Avec le mode config, une seule politique peut être appliquée par profil. Le bouton **Éditer le mode Config** permet de renseigner les paramètres du Mode Config IPsec, qui sont les suivants : • **Serveur DNS utilisé** : ce champ détermine la machine (serveur DNS) qui sera utilisée par les clients mobiles, pour réaliser les résolutions DNS. Vous pouvez la sélectionner ou la créer dans la base d'objets. Par défaut, ce champ est vide. • **Domaines utilisés en Mode config** : le client utilisera le serveur DNS sélectionné précédemment, uniquement pour les domaines spécifiés dans cette grille. Pour les autres domaines, le client continuera à utiliser son / ses serveur(s) DNS système. Il s'agira donc généralement de noms de domaines internes. **EXEMPLE** Dans le cas du choix du domaine "compagnie.com", un iPhone par exemple, en joignant "www.compagnie.com" ou "intranet.compagnie.com" utilisera le serveur DNS spécifié plus haut. Cependant, s'il tente de joindre de joindre "www.google.fr", il continuera à utiliser ses anciens serveurs DNS.
Commentaire	Description associée à la politique VPN.
Keepalive	L'option supplémentaire **Keepalive** permet de maintenir les tunnels montés de façon artificielle. Cette mécanique envoie des paquets initialisant et forçant le maintien du tunnel. Cette option est désactivée par défaut pour éviter une charge inutile, dans le cas de configuration contenant de nombreux tunnels, montés en même temps sans réel besoin. Pour activer cette option, affectez une valeur différente de 0, correspondant à l'intervalle en seconde, entre chaque envoi de paquet UDP.

NOTE
Vous ne pourrez utiliser et créer qu'une seule configuration mobile (« roadwarrior ») par profil IPsec. Les correspondants sont applicables à tous les profils. Par conséquent, un seul type d'authentification peut être utilisé à la fois pour la configuration mobile.

Vérification en temps réel de la politique

L'écran d'édition des règles de politique IPsec dispose d'un champ de « **Vérification de la politique** » (situé en dessous de la grille), qui prévient l'administrateur en cas d'incohérence ou d'erreur sur une des règles créées.

L'onglet Correspondants

Cet onglet est divisé en deux écrans :

- À gauche : la liste des correspondants VPN IPsec site à site (**Passerelles distantes**) et VPN IPsec mobiles (**Correspondants mobiles**).
- À droite : les informations du correspondant sélectionné.

La liste des correspondants

Entrer un filtre...	Ce champ permet d'effectuer une recherche sur le nom de l'objet et ses différentes propriétés, par occurrence, lettre ou mot.
Ajouter	Il est possible d'ajouter des correspondants à cet endroit précis. Pour cela, choisissez parmi la liste déroulante le type de correspondant à créer : • **Nouvelle passerelle distante** (pour un tunnel site à site), • **Nouveau correspondant mobile**.
Action	Lorsque vous sélectionnez un correspondant dans la liste, déroulez le menu **Action** pour : • **Dupliquer** ce correspondant, • **Renommer** ce correspondant, • **Supprimer** ce correspondant, • **Vérifier l'utilisation** de ce correspondant dans la configuration du firewall.

Les informations des correspondants de type « passerelle »

Sélectionnez un correspondant dans la liste pour en afficher les informations.

Commentaire	Description associée au correspondant local.
Passerelle distante	Objet sélectionné pour caractériser l'adresse IP distante lors de la création du correspondant via l'assistant.
Adresse locale	Ce champ permet de sélectionner l'interface externe présentée pour établir le tunnel avec le correspondant affiché.
Profil IKE	Cette option permet de choisir le modèle de protection associé à la phase 1 de votre politique VPN, parmi les 3 profils pré-configurés : **StrongEncryption**, **GoodEncryption**, **Mobile**. Il est possible de créer ou de modifier d'autres profils au sein de l'onglet *Profils de chiffrement*.
Version IKE	Cette option permet de choisir la version du protocole IKE (IKEv1 ou IKEv2) utilisée par le correspondant.

Identification

Méthode d'authentification	Ce champ affichera la méthode d'authentification choisie lors de la création de votre correspondant via l'assistant. Vous pouvez modifier votre choix en sélectionnant une autre méthode d'authentification présente dans la liste déroulante. **NOTE** Pour un correspondant de type « passerelle », vous avez le choix entre **Certificat** ou **Clé pré-partagée (PSK)**.

Certificat	Si vous avez choisi la méthode d'authentification par certificat, ce champ affiche le certificat à présenter au correspondant pour établir le tunnel IPsec. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module. Si vous avez opté pour la clé pré-partagée, ce champ n'est pas affiché.
Local ID (Optionnel)	Ce champ représente une extrémité du tunnel VPN IPsec, partageant le « secret » ou la PSK avec le « Peer ID », autre extrémité. Le « Local ID » vous représente. Cet identifiant doit avoir la forme d'une adresse IP, d'un nom de domaine (FQDN ou Full Qualified Domain Name) ou d'une adresse e-mail (user@fqdn).
ID du correspondant (optionnel)	Ce champ représente une extrémité du tunnel VPN IPsec, partageant le « secret » ou la PSK avec le « Local ID », autre extrémité. Le « Peer ID » représente votre correspondant. Le format est analogue au champ précédent.
Clé pré-partagée (ASCII)	Dans ce champ apparaît votre PSK sous le format que vous avez choisi précédemment lors de la création du correspondant via l'assistant : caractères ASCII ou hexadécimaux (case à cocher au bas du champ si vous souhaitez en changer).
Éditer	Ce bouton permet de modifier directement la clé pré-partagée servant à établir le tunnel IPsec avec ce correspondant.

Clés pré-partagées post-quantiques (PPK)

La puissance de calcul d'un ordinateur quantique pourra très probablement à l'avenir lui permettre de déchiffrer des clés négociées via les méthodes Diffie-Hellman (DH) et Elliptic Curve Diffie-Hellman (ECDH), et mettre en danger la sécurité du protocole IKEv2.

Un utilisateur malveillant pourrait dès à présent réaliser une attaque de type "stocker maintenant, déchiffrer plus tard" : intercepter des communications IPsec et les stocker afin de les déchiffrer ultérieurement à l'aide d'un ordinateur quantique.

Pour les clients qui souhaitent dès à présent se protéger de telles attaques, il est déjà possible d'utiliser des clés pré-partagées post-quantiques (PPK) destinées à protéger les échanges des clés de chiffrement des données.

Pour en savoir plus sur l'utilisation de clés pré-partagées post-quantiques pour le protocole IKEv2, nous vous invitons à consulter la RFC 8784.

Afin de suivre ces recommandations, les version SNS 4.8 et supérieures offrent la possibilité de définir des clés pré-partagées post-quantiques pour les correspondants utilisant le protocole IKEv2 avec authentification par certificats.

NOTE
Pour être efficaces, ces PPK doivent respecter une entropie suffisamment élevée (256 bits minimum selon la RFC 8784).

Identifiant de PPK	Cet identifiant doit avoir la forme d'une adresse IP, d'un nom de domaine (FQDN ou Full Qualified Domain Name) ou d'une adresse e-mail (user@fqdn). Si cet identifiant correspond à celui d'une PPK déjà définie sur le firewall (onglet Identification du module VPN IPsec), cette PPK sera automatiquement utilisée. Il n'est pas nécessaire dans ce cas d'utiliser le champ **Mot de passe de la PPK**. Ce champ doit être obligatoirement renseigné si la case **PPK requise** est cochée.

Mot de passe de la PPK	Si l'Identifiant de PPK précédemment renseigné ne correspond à aucune PPK définie sur le firewall (onglet **Identification** du module VPN IPsec), un clic sur le bouton **Éditer** ouvre la boite de dialogue destinée à renseigner le mot de passe (aussi appelé *secret*) pour cette nouvelle PPK. Ce mot de passe peut être renseigné en caractères ASCII ou en caractères hexadécimaux.
PPK requise	En cochant cette case, vous indiquez qu'il est obligatoire d'utiliser une PPK pour établir un tunnel avec le correspondant.

Configuration avancée

Ne pas initier le tunnel (Responder-only) :	Si vous cochez cette option, le serveur IPsec sera mis en attente. Il ne prendra pas l'initiative de négociation du tunnel. Cette option est utilisée dans le cas où le correspondant est un mobile.
Fragmentation IKE	Cette case permet d'activer la fragmentation IKE lorsque les paquets IKE dépassent la taille standard de paquets paramétrée sur le firewall.
DPD	Ce champ permet de configurer la fonctionnalité VPN dite de DPD (*Dead Peer Detection*). Celui-ci permet de vérifier qu'un correspondant est toujours opérationnel. Quand le DPD est activé sur un correspondant, des requêtes de test de disponibilité (*R U there*) sont envoyées à l'autre correspondant. Ce dernier devra acquitter la requête pour valider sa disponibilité (*R U there ACK*). Ces échanges sont sécurisés via les SAs (*Security Association*) ISAKMP (Internet Security Association and Key Management Protocol). Si on détecte qu'un correspondant ne répond plus, les SAs négociées sont détruites. **IMPORTANT** Cette fonctionnalité apporte une stabilité au service VPN sur les Firewalls Stormshield Network, à la condition que le DPD soit correctement configuré. Pour configurer l'option de **DPD**, quatre choix sont disponibles : • **Inactif** : les requêtes DPD provenant du correspondant sont ignorées. • **Passif** : les requêtes DPD émises par le correspondant obtiennent une réponse du firewall. Par contre, le firewall n'en envoie pas. • **Bas** : la fréquence d'envoi des paquets DPD est faible, et le nombre d'échecs tolérés est élevé (*delay* 600, *retry* 10, *maxfail* 5). • **Haut** : la fréquence d'envoi des paquets DPD est élevée et le nombre d'échecs est relativement bas (*delay* 30, *retry* 5, *maxfail* 3). La valeur *delay* définit le temps après une réponse avant l'envoi de la prochaine demande. La valeur *retry*, définit le temps d'attente d'une réponse avant la réémission de la demande. La valeur *maxfail*, c'est le nombre de demandes sans réponses avant de considérer le correspondant comme absent.
DSCP	Ce champ permet de préciser la valeur du champ DSCP affecté aux paquets réseau IKE émis à destination de ce correspondant. Sélectionnez l'une des valeurs proposées ou précisez un champ DSCP personnalisé (entier compris entre 0 et 63).

NOTE

Pour chaque champ comportant la mention « Passerelle » et l'icône, vous pourrez ajouter un objet à la base existante en précisant son nom, sa résolution DNS, son adresse IP et en cliquant ensuite sur **Appliquer**.

Les informations des correspondants de type « mobile »

Sélectionnez un correspondant dans la liste pour en afficher les informations.

Commentaire	Description associée au correspondant distant.
Passerelle distante	Ce champ est grisé pour les correspondants mobiles.
Adresse locale	Ce champ permet de sélectionner l'interface externe présentée pour établir le tunnel avec le correspondant affiché.
Profil IKE	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils pré-configurés: **StrongEncryption**, **GoodEncryption**, et **Mobile**. Il est possible de créer ou de modifier d'autres profils au sein de l'onglet *Profils de chiffrement*.
Version d'IKE	Cette option permet de choisir la version du protocole IKE (IKEv1 ou IKEv2) utilisée par le correspondant.

Identification

Méthode d'authentification	Ce champ affichera la méthode d'authentification choisie lors de la création de votre correspondant via l'assistant. Vous pouvez modifier votre choix en sélectionnant une autre méthode d'authentification présente dans la liste déroulante. **NOTE** Pour un correspondant mobile, vous avez le choix entre **Certificat**, **Clé pré-partagée (PSK)**, **EAP-Generic Token Card (GTC)** ou **Certificat et EAP-Generic Token Card (GTC)**.
Certificat	Ce champ n'apparaît que si vous avez choisi la méthode d'authentification par **Certificat**, **EAP-Generic Token Card (GTC)** ou **Certificat et EAP-Generic Token Card (GTC)**. Il affiche le certificat que vous présentez pour établir le tunnel avec ce correspondant, ou vous propose de le sélectionner au sein de la liste déroulante. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module.
Local ID (Optionnel)	Ce champ représente une extrémité du tunnel VPN IPsec, partageant le « secret » ou la PSK avec l' « ID du correspondant», autre extrémité. Le « Local ID » vous représente. Cet identifiant doit avoir la forme d'une adresse IP, d'un nom de domaine (FQDN ou Full Qualified Domain Name) ou d'une adresse e-mail (user@fqdn). **NOTE** Ce champ n'est accessible que si vous avez choisi la méthode d'authentification par **Clé pré-partagée**.

ID du correspondant (optionnel)	Ce champ représente une extrémité du tunnel VPN IPsec, partageant le « secret » ou la PSK avec le « Local ID », autre extrémité. L' « ID du correspondant » représente votre correspondant. Le format est analogue au champ précédent.
Groupes	Cette grille n'apparaît que si vous avez choisi la méthode d'authentification **EAP-Generic Token Card (GTC)** ou **Certificat et EAP-Generic Token Card (GTC).** Elle affiche les groupes d'utilisateurs rattachés à ce profil de correspondant définis lors de sa création. Vous pouvez la modifier pour **Ajouter** ou **Supprimer** des groupes.
Clé pré-partagée (ASCII)	Ce champ n'est affiché que si vus avez choisi la méthode d'authentification par **Clé pré-partagée (PSK)**. Vous pouvez éditer ce champ pour visualiser / modifier votre PSK au format que vous avez choisi lors de la création du correspondant via l'assistant : caractères ASCII ou hexadécimaux (case à cocher au bas du champ si vous souhaitez en changer).
Éditer	Ce bouton permet de modifier directement la clé pré-partagée servant à établir le tunnel IPsec avec ce correspondant.

Clés pré-partagées post-quantiques (PPK)

La puissance de calcul d'un ordinateur quantique pourra très probablement à l'avenir lui permettre de déchiffrer des clés négociées via les méthodes Diffie-Hellman (DH) et Elliptic Curve Diffie-Hellman (ECDH), et mettre en danger la sécurité du protocole IKEv2.

Un utilisateur malveillant pourrait dès à présent réaliser une attaque de type "stocker maintenant, déchiffrer plus tard" : intercepter des communications IPsec et les stocker afin de les déchiffrer ultérieurement à l'aide d'un ordinateur quantique.

Pour les clients qui souhaitent dès à présent se protéger de telles attaques, il est déjà possible d'utiliser des clés pré-partagées post-quantiques (PPK) destinées à protéger les échanges des clés de chiffrement des données.

Pour en savoir plus sur l'utilisation de clés pré-partagées post-quantiques pour le protocole IKEv2, nous vous invitons à consulter la RFC 8784.

Afin de suivre ces recommandations, les version SNS 4.8 et supérieures offrent la possibilité de définir des clés pré-partagées post-quantiques pour les correspondants utilisant le protocole IKEv2 avec authentification par certificats.

NOTE
Pour être efficaces, ces PPK doivent respecter une entropie suffisamment élevée (256 bits minimum selon la RFC 8784).

Identifiant de PPK	Cet identifiant doit avoir la forme d'une adresse IP, d'un nom de domaine (FQDN ou Full Qualified Domain Name) ou d'une adresse e-mail (user@fqdn). Si cet identifiant correspond à celui d'une PPK déjà définie sur le firewall (onglet Identification du module VPN IPsec), cette PPK sera automatiquement utilisée. Il n'est pas nécessaire dans ce cas d'utiliser le champ **Mot de passe de la PPK**. Ce champ doit être obligatoirement renseigné si la case **PPK requise** est cochée.

Mot de passe de la PPK	Si l'Identifiant de PPK précédemment renseigné ne correspond à aucune PPK définie sur le firewall (onglet **Identification** du module VPN IPsec), un clic sur le bouton **Éditer** ouvre la boite de dialogue destinée à renseigner le mot de passe (aussi appelé *secret*) pour cette nouvelle PPK. Ce mot de passe peut être renseigné en caractères ASCII ou en caractères hexadécimaux.
PPK requise	En cochant cette case, vous indiquez qu'il est obligatoire d'utiliser une PPK pour établir un tunnel avec le correspondant.

Configuration avancée

Ne pas initier le tunnel (Responder-only)	Cette case est grisée et validée, car il est impossible d'initier un tunnel vers un client mobile dont l'adresse IP est inconnue. Dans cette configuration, le firewall est donc en mode de réponse uniquement.
DPD	Ce champ permet de configurer la fonctionnalité VPN dite de DPD (*Dead Peer Detection*). Celle-ci permet de vérifier qu'un correspondant est toujours opérationnel. Quand le DPD est activé sur un correspondant, des requêtes de test de disponibilité (*R U there*) sont envoyées à l'autre correspondant. Ce dernier devra acquitter la requête pour valider sa disponibilité (*R U there ACK*). Ces échanges sont sécurisés via les SA (*Security Association*) ISAKMP (Internet Security Association and Key Management Protocol). Si on détecte qu'un correspondant ne répond plus, les SA négociées avec celui-ci sont détruites. **IMPORTANT** Cette fonctionnalité apporte une stabilité au service VPN sur les Firewalls Stormshield Network, à la condition que le DPD soit correctement configuré. Pour configurer l'option de **DPD**, quatre choix sont disponibles : • **Inactif** : les requêtes DPD provenant du correspondant sont ignorées. • **Passif** : les requêtes DPD émises par le correspondant obtiennent une réponse du firewall. Par contre, le firewall n'en n'envoie pas. • **Bas** : la fréquence d'envoi des paquets DPD est faible, et le nombre d'échecs tolérés est élevé (*delay* 600, *retry* 10, *maxfail* 5). • **Haut** : la fréquence d'envoi des paquets DPD est élevée et le nombre d'échecs est relativement bas (*delay* 30, *retry* 5, *maxfail* 3). La valeur *delay* définit le temps après une réponse avant l'envoi de la prochaine demande. La valeur *retry*, définit le temps d'attente d'une réponse avant la réémission de la demande. La valeur *maxfail*, c'est le nombre de demandes sans réponses avant de considérer le correspondant comme absent.
DSCP	Ce champ permet de préciser la valeur du champ DSCP affecté aux paquets réseau IKE émis à destination de ce correspondant. Sélectionnez l'une des valeurs proposées ou précisez un champ DSCP personnalisé (entier compris entre 0 et 63).
Encapsuler le trafic ESP dans UDP	Ce champ n'apparaît que lorsque la **compatibilité avec le mode DR** a été activée. Il permet d'activer / désactiver l'encapsulation du trafic ESP dans le protocole UDP pour chaque correspondant afin de suivre la recommandation de l'ANSSI.

L'onglet Identification

Autorités de certification acceptées

Cette grille permet de lister les autorités pour identifier vos correspondants au sein du module VPN IPsec.

Ajouter	Lorsque vous cliquez sur ce bouton, une fenêtre regroupant les CA et sous CA que vous avez créées au préalable apparaît. Sélectionnez les autorités qui permettront de vérifier les identités de vos correspondants, en cliquant sur **Sélectionner**. La CA ou sous CA choisie vient s'ajouter au tableau.
Supprimer	Sélectionnez la CA à retirer de la liste et cliquez sur **Supprimer**.

CA

En dessous de ce champ figurent les autorités de certification ajoutées et acceptées.

Tunnels mobiles : clés pré-partagées (PSK)

Si vous avez préalablement créé un correspondant mobile ayant pour méthode d'authentification la **Clé pré-partagée (PSK)**, cette grille sera déjà pré-remplie.

Vous aviez dû éditer une clé en lui définissant un ID et une valeur (en caractères hexadécimaux ou ASCII).

Rechercher	Bien que la grille affiche toutes vos clés pré-partagées de tunnels mobiles par défaut, vous pouvez effectuer une recherche par occurrence, lettre ou mot, de manière à ce que seules les clés souhaitées s'affichent à l'écran.
Ajouter	En cliquant sur ce bouton, une fenêtre d'édition de clé s'affichera : vous devrez lui fournir un ID, une valeur, et confirmer cette dernière. Vous pourrez choisir d'éditer en caractères hexadécimaux ou ASCII.
Supprimer	Sélectionnez la clé à retirer de la liste et cliquez sur **Supprimer**.

Identité

Cette colonne affiche les ID de vos clés pré-partagées, qui peuvent être représentés par un nom de domaine (FQDN), une adresse e-mail (USER_FQDN) ou une adresse IP.

Clé

Cette colonne affiche les valeurs de vos clés pré-partagées en caractères hexadécimaux.

NOTES

- La création de clés pré-partagées est illimitée.
- La suppression d'une clé pré-partagée appartenant à un tunnel VPN IPsec entraîne le dysfonctionnement de ce tunnel.
- Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur.

Clés pré-partagées post-quantiques (PPK)

La puissance de calcul d'un ordinateur quantique pourra très probablement à l'avenir lui permettre de déchiffrer des clés négociées via les méthodes Diffie-Hellman (DH) et Elliptic Curve Diffie-Hellman (ECDH), et mettre en danger la sécurité du protocole IKEv2.

Un utilisateur malveillant pourrait dès à présent réaliser une attaque de type "stocker maintenant, déchiffrer plus tard" : intercepter des communications IPsec et les stocker afin de les déchiffrer ultérieurement à l'aide d'un ordinateur quantique.

Pour les clients qui souhaitent dès à présent se protéger de telles attaques, il est déjà possible d'utiliser des clés pré-partagées post-quantiques (PPK) destinées à protéger les échanges des clés de chiffrement des données.

Pour en savoir plus sur l'utilisation de clés pré-partagées post-quantiques pour le protocole IKEv2, nous vous invitons à consulter la RFC 8784.

Afin de suivre ces recommandations, les version SNS 4.8 et supérieures offrent la possibilité de définir des clés pré-partagées post-quantiques pour les correspondants utilisant le protocole IKEv2 avec authentification par certificats.

NOTE
Pour être efficaces, ces PPK doivent respecter une entropie suffisamment élevée (256 bits minimum selon la RFC 8784).

IMPORTANT
Si vous avez préalablement créé ou modifié un correspondant mobile pour lui créer une PPK qui n'existait pas, cette PPK ne sera pas ajoutée automatiquement à la grille.

Les actions possibles

Clé recherchée	Vous pouvez effectuer une recherche par occurrence, lettre ou mot, de manière à ce que seules les clés souhaitées s'affichent à l'écran.
Ajouter	En cliquant sur ce bouton, une fenêtre d'édition de clé s'affiche. Vous devez renseigner : • Un ID sous la forme d'un nom de domaine (FQDN), d'une adresse e-mail ou d'une adresse IP, • La valeur de la clé (mot de passe) et la confirmer. Vous pouvez choisir de saisir / éditer la valeur de la clé en caractères hexadécimaux ou ASCII.
Supprimer	Sélectionnez la clé à retirer de la liste et cliquez sur **Supprimer**.
Éditer la sélection	Sélectionnez la clé à éditer et effectuez les modifications souhaitées.
Exporter la liste des PPK	Ce bouton vous permet d'exporter la liste des PPK au format CSV et de la télécharger sur votre poste de travail.

NOTE
Une PPK créée directement au niveau du correspondant n'apparaît pas dans cette grille.

Configuration avancée

Activer la recherche au travers de plusieurs annuaires LDAP (modes clé pré-partagée ou certificats)	Lorsque plusieurs annuaires LDAP sont définis, cocher cette case permet au firewall de parcourir ces annuaires séquentiellement pour authentifier un correspondant mobile. Cette méthode est disponible quel que soit le type d'authentification choisi (clé pré-partagée ou certificat). Si cette case est décochée, le firewall consulte uniquement l'annuaire défini par défaut.

Liste des annuaires

Les différents annuaires listés sont parcourus selon leur ordre dans la grille.

Ajouter	En cliquant sur ce bouton, une ligne est ajoutée à la grille, sous forme de liste déroulante permettant de sélectionner un des annuaires définis sur le firewall. Ce bouton est grisé lorsque tous les annuaires du firewall ont été sélectionnés.
Supprimer	Sélectionnez la clé à retirer de la liste et cliquez sur **Supprimer**.
Monter	Ce bouton permet de monter l'annuaire sélectionné dans la liste afin que le firewall le parcoure de manière plus prioritaire.
Descendre	Ce bouton permet de descendre l'annuaire sélectionné dans la liste afin que le firewall le parcoure de manière moins prioritaire..

L'onglet Profils de Chiffrement

Profils de chiffrement par défaut

Les valeurs définies dans la phase 1 et la phase 2 seront présélectionnées pour chaque nouveau correspondant créé.

IKE

La phase 1 du protocole IKE vise à établir un canal de communication chiffré et authentifié entre les deux correspondants VPN. Ce "canal" est appelé SA ISAKMP (différent de la SA IPsec). Deux modes de négociations sont possibles : le mode principal et le mode agressif.

La liste déroulante permet de choisir le modèle de protection associé à votre politique VPN, parmi les 4 profils pré-configurés : **GoodEncryption**, **Mobile**, **DR** et **StrongEncryption**. Il est également possible d'en créer d'autres à l'aide du bouton **Ajouter**.

IPsec

La phase 2 du protocole IKE négocie de manière sécurisée (au moyen du canal de communication SA ISAKMP négocié dans la première phase) les paramètres des futures SA IPsec (une entrante et une sortante).

La liste déroulante permet de choisir le modèle de protection associé à votre politique VPN, parmi les 4 profils pré-configurés : **GoodEncryption**, **Mobile**, **DR** et **StrongEncryption**. Il est également possible d'en créer d'autres à l'aide du bouton **Ajouter**.

Tableau des profils

Ce tableau propose une série de profils de chiffrement prédéfinis, de phases 1 (IKE) ou 2 (IPsec).

Les actions possibles

Ajouter	En cliquant sur ce bouton, vous pouvez choisir d'ajouter un **Nouveau profil de phase 1** (IKE) ou un **Nouveau profil de phase 2** (IPsec), qui sera affiché dans la colonne lui correspondant. Vous pouvez lui donner le « Nom » que vous souhaitez. Il est également possible de copier un profil et ses caractéristiques : pour cela, sélectionnez le profil voulu et cliquez sur l'option **Copier la sélection**, puis donnez-lui un nom.
Actions	Ce menu déroulant vous offre la possibilité d'appliquer l'une des 4 actions suivantes au profil sélectionné : • **Dupliquer** le profil, • **Définir le profil par défaut**, • **Supprimer** le profil, • **Vérifier l'utilisation** du profil.

Profil IKE

Pour le profil IKE ajouté ou sélectionné, vous verrez apparaître ses caractéristiques à droite de l'écran (champs « **Général** » et « **Propositions** »).

Général

Commentaire	Description associée à votre profil de chiffrement.
Diffie Hellman	Ce champ représente deux types d'échange de clé: si vous avez sélectionné un profil de chiffrement type **IKE**, c'est l'option **Diffie-Hellman** qui apparaîtra. **Diffie-Hellman** permet à 2 correspondants de générer chacun de leur côté un secret commun, sans transmission d'informations sensibles sur le réseau. En complément, si vous optez pour un profil **IPsec**, le **PFS** vous sera proposé. Le **Perfect Forward Secrecy** permet de garantir qu'il n'y a aucun lien entre les différentes clés de chaque session. Les clés sont recalculées par l'algorithme de Diffie-Hellman sélectionné. Plus le nombre indiquant la taille de la clé est élevée, plus la sécurité est importante. Que vous choisissiez l'un ou l'autre, une liste déroulante vous propose de définir un nombre de bits qui permet de renforcer la sécurité lors de la transmission du secret commun ou mot de passe d'un correspondant à l'autre. Des algorithmes de chiffrement basés sur des courbes elliptiques (algorithme ECDSA : Elliptic Curve Digital Signature Algorithm) peuvent également être sélectionnés. **NOTES** • Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur. • Plus la taille du mot de passe (ou « clé ») est grande, plus le niveau de sécurité est élevé, mais consomme aussi davantage de ressources. • La fonction PFS d'IPsec (isakmp) est recommandée.

Durée de vie maximum (en secondes)	Période de temps au bout de laquelle les clés sont renégociées. La durée de vie par défaut pour un profil de type **IKE** est 21600 secondes.

Propositions

Cette grille vous propose de modifier ou d'ajouter des combinaisons d'algorithmes de chiffrement et d'authentification à la liste pré-établie du profil sélectionné.

Ajouter	La combinaison proposée par défaut est la suivante : • Algorithme de chiffrement **des** d'une « Force » de 64 bits, • Algorithme d'authentification **sha1** d'une « Force » de 160 bits. Cliquez sur la flèche à droite de leur colonne « Algorithme » respective si vous souhaitez les modifier. Chaque fois que vous ajoutez une ligne au tableau, celle-ci passe en priorité suivante.
Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Monter	Sélectionnez la ligne à déplacer vers le haut de la grille afin d'augmenter la priorité de la combinaison Chiffrement / Authentification correspondante.
Descendre	Sélectionnez la ligne à déplacer vers le bas de la grille afin de diminuer la priorité de la combinaison Chiffrement / Authentification correspondante.

Chiffrement

Algorithme	4 choix vous sont proposés : • 3des (obsolète), • aes, • aes_gcm_16 (recommandé), • aes_ctr. Lorsque vous sélectionnez un profil prédéfini, les choix recommandés sont automatiquement proposés par défaut. L'algorithme aes_gcm-16 présente l'avantage de réaliser à la fois l'authentification et le chiffrement. Il n'est donc pas proposé de choisir un algorithme d'authentification dans ce cas.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Authentification

Algorithme	4 choix vous sont proposés : • **sha1** (obsolète), • **sha2_256,** • **sha2_384,** • **sha2_512**.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Groupe DH

Il est possible d'associer à chaque proposition de Chiffrement / Authentification IKE listée dans cette grille un groupe DH différent du groupe **Diffie-Hellman par défaut** sélectionné dans le cadre **Général**.

Si aucun groupe DH spécifique n'est précisé pour une proposition, c'est le groupe **Diffie-Hellman par défaut** du cadre **Général** qui sera appliqué à cette proposition.

Profil IPsec

Pour chaque profil IPsec ajouté ou sélectionné, vous verrez apparaître ses caractéristiques à droite de l'écran (champs « **Général** », « **Propositions d'authentification** » et « **Propositions de chiffrement** »).

Général

Commentaire	Description associée à votre profil de chiffrement.
Diffie Hellman	Ce champ représente deux types d'échange de clé: si vous avez sélectionné un profil de chiffrement type **IKE**, c'est l'option **Diffie-Hellman** qui apparaîtra. **Diffie-Hellman** permet à 2 correspondants de générer chacun de leur côté un secret commun, sans transmission d'informations sensibles sur le réseau. En complément, si vous optez pour un profil **IPsec**, le **PFS** vous sera proposé. Le **Perfect Forward Secrecy** permet de garantir qu'il n'y a aucun lien entre les différentes clés de chaque session. Les clés sont recalculées par l'algorithme de Diffie-Hellman sélectionné. Plus le nombre indiquant la taille de la clé est élevée, plus la sécurité est importante. Que vous choisissiez l'un ou l'autre, une liste déroulante vous propose de définir un nombre de bits qui permet de renforcer la sécurité lors de la transmission du secret commun ou mot de passe d'un correspondant à l'autre. Des algorithmes de chiffrement basés sur des courbes elliptiques (algorithme ECDSA : Elliptic Curve Digital Signature Algorithm) peuvent également être sélectionnés. **NOTES** • Pour définir une clé pré-partagée au format ASCII suffisamment sécurisée, il est indispensable de suivre les mêmes règles qu'un mot de passe utilisateur décrites dans la section **Bienvenue**, partie Sensibilisation des utilisateurs, paragraphe Gestion des mots de passe de l'utilisateur. • Plus la taille du mot de passe (ou « clé ») est grande, plus le niveau de sécurité est élevé, mais consomme aussi davantage de ressources. • La fonction PFS d'IPsec (isakmp) est recommandée.
Durée de vie (en secondes)	Période de temps au bout de laquelle les clés sont renégociées. La durée de vie par défaut pour un profil de type **IPsec** est de 3600 secondes.

Propositions d'authentification

Cette grille vous propose de modifier ou d'ajouter des algorithmes d'authentification à la liste pré-établie du profil sélectionné.

Ajouter	L'algorithme d'authentification apparaissant par défaut en cliquant sur ce bouton est **hmac_sha256,** d'une « Force » de 256 bits. Cliquez sur la flèche à droite de la colonne « Algorithme » si vous souhaitez le modifier. Chaque fois que vous ajoutez une ligne au tableau, celle-ci passe en priorité suivante.

Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Algorithme	4 choix vous sont proposés : • **hmac_sha1** (obsolète), • **hmac_sha256**, • **hmac_sha384**, • **hmac_sha512**.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Propositions de chiffrement

Cette grille vous propose de modifier ou d'ajouter des algorithmes de chiffrement à la liste pré-établie du profil sélectionné.

Ajouter	L'algorithme de chiffrement apparaissant par défaut en cliquant sur ce bouton est **aes_gcm_16 (recommandé),** d'une « Force » de 256 bits. Cliquez sur la flèche à droite de la colonne « Algorithme » si vous souhaitez le modifier. Chaque fois que vous ajoutez une ligne au tableau, celle-ci passe en priorité suivante.
Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Algorithme	4 choix vous sont proposés : • **3des** (obsolète), • **aes**, • **aes_gcm_16** (recommandé), • **aes_ctr**. L'algorithme aes_gcm-16 présente l'avantage de réaliser à la fois l'authentification et le chiffrement.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Propositions PFS

Ajouter	Vous pouvez ajouter des groupes Diffie-Hellmann à associer aux propositions de chiffrement / authentification IPSec.
Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Groupe DH	Après avoir cliqué sur **Ajouter**, sélectionnez un groupe Diffie-Hellmann à ajouter à la liste des propositions.

Cliquez sur **Appliquer** une fois votre configuration effectuée.

VPN SSL

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée à des ressources, internes à une entreprise ou non, en passant par le firewall SNS. Pour qu'un tunnel VPN SSL puisse s'établir avec le firewall SNS, un client VPN SSL doit être installé sur le poste de travail ou le terminal mobile de l'utilisateur.

Il existe plusieurs clients VPN compatibles avec le service VPN SSL du firewall SNS. Le client VPN SSL de Stormshield (SN SSL VPN Client) dispose d'un mode de connexion lui permettant de récupérer automatiquement et de manière sécurisée sa configuration VPN, à l'inverse d'OpenVPN Connect pour qui la configuration VPN doit être intégrée manuellement.

Activer le service VPN SSL

Activer le VPN SSL

Active ou désactive le service VPN SSL du firewall SNS.

Configurer le service VPN SSL

Deux onglets permettent respectivement de configurer :

- Les paramètres généraux du service VPN SSL,
- La politique de vérification de la conformité des postes clients (ZTNA). Le ZTNA (pour *Zero Trust Network Access*) consiste à ne faire confiance aux utilisateurs et aux appareils qu'après leur vérification.

NOTE

Si la fonctionnalité de compression LZ4 du service VPN SSL est activée, un avertissement s'affiche automatiquement à l'ouverture du module vous invitant à désactiver cette fonctionnalité. Il est fortement conseillé de la désactiver pour des raisons de sécurité. Si vous avez ignoré cet avertissement, un message restera affiché tant qu'elle ne sera pas désactivée. Pour la désactiver, vous devez utiliser les commandes CLI Serverd :
`CONFIG OPENVPN UPDATE compress=0` puis `CONFIG OPENVPN ACTIVATE`.

À noter que la mise en œuvre de tunnels VPN SSL nécessite également de configurer les modules **Authentification**, **Droits d'accès** et **Filtrage et NAT**. Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser le VPN SSL des firewalls SNS.

Onglet Configuration générale

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée	Indiquez l'adresse que les utilisateurs devront utiliser pour joindre le firewall SNS pour établir des tunnels VPN. Vous pouvez indiquer une adresse IP ou un FQDN. • Pour une adresse IP : elle doit être publique, donc accessible sur Internet, • Pour un FQDN : il doit être déclaré dans les serveurs DNS utilisés par le poste de travail lorsque celui-ci est en dehors du réseau de l'entreprise. Si vous disposez d'une adresse IP publique dynamique, vous pouvez recourir aux services d'un fournisseur comme *DynDNS* ou *No-IP*, puis paramétrez ce FQDN dans le module DNS dynamique.
Réseaux ou machines accessibles	Sélectionnez l'objet représentant les réseaux ou machines qui seront joignables au travers du tunnel VPN. Cet objet permet de définir automatiquement sur le poste de travail les routes nécessaires pour joindre les ressources accessibles via le VPN. Des règles de filtrage (dans le module Filtrage et NAT) seront nécessaires pour autoriser ou interdire plus finement les flux entre les postes de travail distants et les ressources internes. Il peut également être nécessaire de définir des routes statiques d'accès au réseau attribué aux clients VPN sur les équipements de l'entreprise situés entre le firewall SNS et les ressources internes mises à disposition.
Réseau assigné aux clients (UDP) **Réseau assigné aux clients (TCP)**	Sélectionnez l'objet correspondant au réseau assigné aux clients VPN en UDP et TCP. La taille minimale du masque réseau est de **/28**. Si vous assignez deux réseaux, le client VPN choisira toujours en premier le réseau UDP pour de meilleures performances. Concernant le choix du réseau ou des sous-réseaux : • Le réseau assigné ne doit pas appartenir aux réseaux internes existants ou déclarés par une route statique sur le firewall SNS. L'interface utilisée pour le VPN SSL étant protégée, le firewall détecterait alors une tentative d'usurpation d'adresse IP (*spoofing*) et bloquerait les flux correspondants. • Pour éviter des conflits de routage, choisissez des sous-réseaux peu communément utilisés (comme 10.**60.77**.0/24) car de nombreux réseaux d'accès à Internet filtrés (Wi-Fi public, hôtels) ou réseaux locaux privés utilisent déjà les premières plages d'adresses réservées.
Maximum de tunnels simultanés autorisés	Le nombre s'affiche automatiquement. Il correspond à la valeur minimale, soit du nombre de tunnels autorisés sur le firewall SNS, soit du nombre de sous-réseaux disponibles pour les clients VPN. Pour ce dernier, cela représente 1/4 des adresses IP, moins 2. Un tunnel VPN SSL consomme 4 IP et le serveur réserve 2 sous-réseaux pour son propre usage.

Paramètres DNS envoyés au client

Nom de domaine	Indiquez le nom de domaine attribué aux clients VPN SSL pour leur permettre d'effectuer leurs résolutions de noms d'hôtes.
Serveur DNS primaire	Sélectionnez l'objet représentant le serveur DNS à attribuer.
Serveur DNS secondaire	

Configuration avancée

Adresse IP publique de l'UTM pour le VPN SSL (UDP)	Dans l'un des cas suivants, vous devez sélectionner l'objet représentant l'adresse IP à utiliser pour établir les tunnels VPN SSL en UDP : • L'adresse IP utilisée pour établir les tunnels VPN SSL (UDP) n'est pas l'adresse IP principale de l'interface externe, • L'adresse IP utilisée pour établir les tunnels VPN SSL (UDP) est portée par une interface externe qui n'est pas en lien avec la passerelle par défaut du firewall.
Port (UDP) **Port (TCP)**	Vous pouvez modifier les ports d'écoute du service VPN SSL. À noter que : • Certains ports sont réservés à un usage interne du firewall SNS et ne peuvent pas être sélectionnés, • Le port 443 est le seul port inférieur à 1024 qui peut être utilisé, • Si vous modifiez les ports par défaut, le VPN SSL pourrait ne plus être accessible depuis un réseau avec filtrage d'accès à Internet (hôtels, Wi-Fi public).
Délai avant renégociation des clés (en secondes)	Vous pouvez modifier le délai (par défaut 14400 secondes, soit 4 heures) au terme duquel les clés utilisées par les algorithmes de chiffrement sont renégociées. Pendant cette opération : • Le tunnel VPN SSL ne répondra pas pendant quelques secondes, • Si une authentification multifacteur est utilisée, l'utilisateur devra renseigner un nouveau code OTP ou approuver la nouvelle connexion sur son application tierce (Mode Push) afin de rester connecté. Il peut être intéressant d'augmenter le délai pour l'aligner sur la durée moyenne d'une journée travaillée, par exemple à 28800 secondes (8 heures).
Utiliser les serveurs DNS fournis par le firewall	Vous pouvez indiquer aux clients VPN d'inscrire dans la configuration réseau du poste de travail (Windows uniquement) les serveurs DNS récupérés via le VPN SSL. Ceux déjà définis sur le poste de travail pourront être interrogés.
Interdire l'utilisation de serveurs DNS tiers	Vous pouvez indiquer aux clients VPN d'exclure les serveurs DNS déjà définis dans la configuration du poste de travail (Windows uniquement). Seuls ceux envoyés par le firewall SNS pourront être interrogés.

Scripts à exécuter sur le client

Sous Windows, le client VPN SSL Stormshield peut exécuter des scripts *.bat* à l'ouverture et à la fermeture d'un tunnel VPN SSL. Vous pouvez utiliser dans ces scripts :

- Les variables d'environnement Windows (**%USERDOMAIN%**, **%SystemRoot%**, ...),
- Les variables liées au client VPN SSL Stormshield : **%NS_USERNAME%** (nom d'utilisateur servant à l'authentification) et **%NS_ADDRESS%** (adresse IP attribuée au client VPN SSL).

Script à exécuter lors de la connexion	Sélectionnez le script à exécuter à l'ouverture du tunnel VPN. Exemple de script permettant de connecter le lecteur réseau Z: à un partage : `NET USE Z: \\myserver\myshare`
Script à exécuter lors de la déconnexion	Sélectionnez le script à exécuter à la fermeture du tunnel VPN. Exemple de script permettant de déconnecter le lecteur réseau Z: d'un partage : `NET USE Z: /delete`

Certificats

Sélectionnez les certificats que le service VPN SSL du firewall SNS et le client VPN SSL Stormshield doivent présenter pour établir un tunnel. Ils doivent être issus de la même autorité de certification. Par défaut, l'autorité de certification dédiée au VPN SSL ainsi qu'un certificat serveur et un certificat client créés à l'initialisation du firewall sont proposés.

Certificat serveur	Sélectionnez le certificat souhaité. L'icône indique les certificats dont la clé privée est protégée par le TPM. Pour plus d'informations sur le TPM, reportez-vous à la section Trusted Platform Module.
Certificat client	Sélectionnez le certificat souhaité. Vous ne pouvez pas choisir un certificat dont la clé privée est protégée par le TPM car la clé privée de ce certificat doit être disponible en clair (non chiffrée) dans la configuration VPN distribuée aux clients VPN.

Configuration

Exporter le fichier de configuration	Cliquez sur ce bouton pour exporter la configuration VPN SSL au format *.ovpn*.

Onglet Vérification des postes clients (ZTNA)

Depuis la version SNS 4.8.1, il est possible de mettre en place une politique de vérification de la conformité des postes clients (ZTNA) établissant un tunnel VPN SSL à l'aide d'un client Stormshield VPN SSL en version 4.0.0 ou supérieure.

Lorsque cette vérification est activée, un poste de travail ou un utilisateur non conforme aux critères de la politique ne peut pas établir de tunnel VPN SSL avec le firewall SNS.

Activer la vérification des postes clients (ZTNA)	Cochez la case pour activer la fonctionnalité de vérification de la conformité des postes clients et des utilisateurs. Lorsqu'elle est activée : • Un client VPN SSL compatible peut établir un tunnel VPN SSL avec le firewall **uniquement si tous** les critères définis dans la politique sont respectés, • Un client VPN SSL non compatible ne peut pas établir de tunnel VPN SSL avec le firewall, **sauf si** le mode permissif est activé (voir ci-dessous).
Autoriser l'établissement de tunnels pour des clients VPN SSL Stormshield Linux ou Mac	Cochez cette case si vous avez des postes clients avec un client VPN SSL Stormshield Linux ou Mac. Ainsi, les critères spécifiques Windows ne sont pas pris en compte pour ces postes et vous n'avez pas besoin d'adapter vos critères à ces postes.
Autoriser l'établissement de tunnels pour des clients non compatibles avec ZTNA	Cochez la case pour activer le mode permissif autorisant les clients VPN SSL non compatibles avec la fonctionnalité de vérification des postes clients à établir des tunnels VPN SSL avec le firewall SNS. Ce mode permissif permet : • De mettre à jour progressivement un parc de clients VPN SSL Stormshield vers une version compatible, • De continuer à utiliser d'autres clients VPN SSL sur les systèmes d'exploitation non compatibles avec le client VPN SSL Stormshield.

Paramètres de vérification des postes clients (ZTNA)

Définissez les critères de la politique de conformité des postes clients et des utilisateurs à vérifier. Vous devez cocher au moins un critère.

Antivirus du poste client actif et à jour	Le poste de travail doit disposer d'un logiciel antiviral actif **avec** les dernières mises à jour de base de données antivirale. Cette information se base sur l'état de l'antivirus reconnu par le centre de Sécurité Windows. Les antivirus tiers sont donc pris en charge tant que le centre de Sécurité Windows reconnait leur état.
Firewall actif sur le poste client	Le Pare-feu Windows doit être en cours d'exécution sur le poste de travail et les profils *Réseau avec domaine*, *Réseau privé* et *Réseau public* doivent être activés. Si un profil est inactif, le critère sera considéré comme non conforme.
SES installé sur le poste client	Dans les infrastructures ayant déployé la solution SES Evolution, l'agent SES doit être installée sur le poste de travail. À noter que la configuration et l'état de l'agent SES ne sont pas pris en compte.
Interdire les utilisateurs possédant les droits d'administration du poste client	Un utilisateur disposant de droits d'administration sur le poste de travail ne peut pas établir de tunnels VPN SSL avec le firewall.
Vérifier les versions (numéro de build) de Windows 10 / Windows 11	Le poste de travail sous Windows 10 ou Windows 11 doit disposer des versions de Windows spécifiées (numéros de *builds*) pour établir un tunnel VPN SSL avec le firewall. En cochant cette case, vous activez la zone de paramétrage des versions exigibles. **Onglets Windows 10 et Windows 11** • **Autoriser une plage de versions** : si vous choisissez cette option : ◦ Vous devez préciser la **Version minimale** que doit posséder le poste de travail (par défaut 10000 pour Windows 10 et 20000 pour Windows 11), ◦ Vous pouvez préciser la **Version maximale** que doit posséder le poste de travail. Laissez ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale précisée. • **N'autoriser qu'une seule version** : si vous choisissez cette option, vous devez préciser la version exacte de Windows que le poste de travail doit posséder.
Onglet Machine rattachée à un domaine	Si vous cochez la case **La machine doit être rattachée à un domaine d'entreprise**, vous devez ajouter dans la grille **Liste des domaines Active Directory** les domaines d'appartenance des postes de travail autorisés à établir un tunnel VPN SSL avec le firewall. À noter que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall.
Onglet Utilisateur rattaché à un domaine	Si vous cochez la case **L'utilisateur doit être rattaché à un domaine d'entreprise**, vous devez ajouter dans la grille **Liste des domaines Active Directory** les domaines d'appartenance des utilisateurs autorisés à établir un tunnel VPN SSL avec le firewall. Avec ce critère, le nom complet de l'utilisateur composé du domaine est vérifié. Ainsi, même si le poste de travail est rattaché à un domaine, un utilisateur local du poste de travail ne pourra pas établir de tunnel VPN SSL avec le firewall. À noter que ce critère n'est pas lié à la configuration d'un annuaire sur le firewall.

Version de Stormshield VPN SSL Client	Le poste de travail doit disposer des versions du Client VPN SSL Stormshield spécifiées pour établir un tunnel VPN SSL avec le firewall. En cochant la case **Vérifier la version du client VPN SSL Stormshield**, vous activez la zone de paramétrage des versions exigibles. • **Autoriser une plage de versions** : si vous choisissez cette option : ◦ Vous devez préciser la **Version minimale** du client VPN SSL Stormshield autorisée (la version minimale autorisée est 4.0.0), ◦ Vous pouvez préciser la **Version maximale** du client VPN SSL Stormshield autorisée. Laissez ce champ vide pour autoriser toutes les versions égales ou supérieures à la version minimale précisée. • **N'autoriser qu'une seule version** : si vous choisissez cette option, vous devez préciser la version exacte du client VPN SSL Stormshield autorisée (la version minimale autorisée est 4.0.0).

Message personnalisé

En cas d'échec d'établissement d'un tunnel VPN SSL du fait d'une non-conformité du poste de travail ou de l'utilisateur, le client VPN SSL Stormshield affiche le message "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" suivi d'un message additionnel en français, anglais et allemand.

Dans la zone de saisie, vous pouvez :

- Modifier le message additionnel pour le personnaliser. Aucun mécanisme de traduction automatique n'est mis en place, vous devez donc prendre en charge sa traduction,
- Supprimer le contenu si vous ne souhaitez pas afficher un message additionnel.

Vous pouvez réinitialiser le message additionnel en cliquant sur **Revenir aux messages proposés par défaut**.

VPN SSL Portail

IMPORTANT
Le VPN SSL portail est obsolète et est amené à être supprimé dans une prochaine version de firmware SNS.

Le VPN SSL Portail Stormshield Network permet à vos utilisateurs nomades ou non de se connecter sur les ressources de votre société de façon sécurisée.

Le VPN SSL Portail Stormshield Network n'impose pas d'installation de clients sur les postes de vos utilisateurs, et supporte nativement les OS disposant de Java 8 ou d'OpenWebStart (Windows, Linux, macOS).

L'écran de configuration du VPN SSL se compose de 4 onglets :

- **Général** : Permet l'activation du module, le choix du type d'accès ainsi que la configuration avancée.
- **Serveurs web** : Le VPN SSL Stormshield Network permet de sécuriser les accès à vos serveurs HTTP (Intranet, webmail,…) tout en évitant de devoir gérer de multiples serveurs https. De plus, pour l'accès aux utilisateurs nomades, il permet de masquer les informations sur votre réseau interne, la seule adresse IP visible étant celle de votre firewall.
  Le VPN SSL Stormshield Network réécrit de façon automatique les liens HTTP trouvés dans les pages Web consultées par vos utilisateurs. Cela permet de naviguer entre vos différents serveurs, si ces derniers sont configurés, ou d'interdire l'accès à certains serveurs.
  Lorsqu'un lien web dans une page pointe sur un serveur non configuré, le lien est redirigé vers la page de démarrage du VPN SSL Stormshield Network.
- **Serveurs applicatifs** : Cette section rassemble les serveurs configurés pour les accès aux ressources autres que le type Web (telnet, mail) ...
  Le VPN SSL Stormshield Network permet de sécuriser tout protocole basé sur une connexion TCP unique (POP3, SMTP, telnet, accès distant, ...). Dans le cadre de protocoles autres que l'HTTP, le client permettant la connexion sécurisée est une applet JAVA. Cette dernière ouvre un tunnel chiffré. Tous les paquets échangés entre le poste client et le firewall sont chiffrés.
  Le VPN SSL Stormshield Network n'impose pas d'installation de clients sur les postes de vos utilisateurs, et supporte nativement les OS disposant de Java 8 ou d'OpenWebStart (Windows, Linux, macOS).
  Il vous suffit de configurer les serveurs auxquels vous désirez donner l'accès à vos utilisateurs. Ces serveurs seront dynamiquement ajoutés à la liste des serveurs autorisés lors du prochain chargement de l'applet JAVA effectué par vos utilisateurs.
  L'applet JAVA ouvre des ports en écoute sur le poste client. C'est sur ces derniers que devront se connecter les outils clients afin de passer par le tunnel sécurisé établi entre l'applet et le firewall. Il est nécessaire de s'assurer que le port choisi est accessible à l'utilisateur (problème de droit) et qu'il ne peut pas entrer en conflit avec un port utilisé par un autre programme. Ces serveurs seront dynamiquement ajoutés. Cela peut être utilisé afin d'effectuer des contrôles et/ou authentifications transparentes sur la provenance des requêtes.
- **Profils utilisateurs** : Si vous souhaitez restreindre l'accès aux serveurs définis dans la configuration du VPN SSL, vous devez définir des profils contenant la liste des serveurs autorisés, puis de les attribuer aux utilisateurs.

L'onglet Général

Activer le VPN SSL : Permet d'activer le VPN SSL et de choisir entre les trois options proposées dans le tableau ci-dessous.

Uniquement l'accès aux serveurs web	Utilisation du module de VPN SSL pour l'accès aux ressources de type Web. Active l'onglet *Serveurs web*.
Uniquement l'accès aux serveurs applicatifs	Utilisation du module de VPN SSL pour l'accès aux ressources sur une connexion de type TCP. Active l'onglet *Serveurs applicatifs*.
L'accès aux serveurs web et applicatifs	Utilisation du module VPN SSL pour l'accès aux ressources de type Web et de type TCP. Active les deux onglets *Serveurs web* et *Serveurs applicatifs*.

Configuration avancée

Accès aux serveurs via le VPN SSL

Préfixe du répertoire racine de l'URL	La technologie VPN SSL Stormshield Network permet de masquer l'adresse réelle des serveurs vers lesquels les utilisateurs sont redirigés en réécrivant l'ensemble des URL contenues dans les pages HTTP rencontrées. Ces URL sont remplacées par un préfixe suivi de 4 chiffres. Ce champ permet de définir le préfixe qui sera utilisé.
En-tête HTTP pour l'identifiant utilisateur	La valeur de ce champ sera envoyée, accompagnée de l'identifiant de l'utilisateur, au serveur Web dans l'entête HTTP des requêtes émises. Cette valeur peut être utilisée afin d'effectuer des contrôles et/ou authentification transparentes sur la provenance des requêtes. Dans le cas où le serveur vers lequel les flux HTTP sont redirigés demande une authentification, il est possible de spécifier un login dans l'entête du paquet HTTP. Ce login pourrait servir par exemple à indiquer que ces flux arrivant au serveur proviennent du firewall et peuvent être acceptés par le serveur sans authentification.

Configuration du poste client

Commande exécutée au démarrage	Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est lancée, les flux SMTP ou POP sont automatiquement redirigés, sans intervention de l'utilisateur.
Commande exécutée à l'arrêt	Exécutée à la fermeture de l'applet, cette commande permet à l'administrateur de définir des actions préalables à la fermeture de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est fermée, les flux SMTP ou POP ne sont plus automatiquement redirigés et encore une fois sans intervention de l'utilisateur.

L'onglet Serveurs web

Cette section rassemble les serveurs configurés pour les accès aux ressources de type Web.

Ajout d'un serveur web

Pour ajouter un serveur d'accès Web, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter**.
2. **Nom du serveur Web** : indiquez un nom pour ce serveur (le nom ne peut pas être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.).
3. **Serveur de destination** : sélectionnez ou créez l'objet représentant le serveur.
La configuration de ce serveur apparaît. Les explications des différents paramètres sont données ci-dessous.

Serveur de destination	Ce champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder. **AVERTISSEMENT** Veillez à utiliser un objet dont le nom est identique au nom **FQDN** du serveur auquel il fait référence. Si cela n'est pas le cas (nom de l'objet : webmail, nom FQDN : www.webmail.com par exemple), il est possible que les requêtes du firewall auprès de ce serveur soient refusées.
Port	Champ permettant de spécifier le port du serveur auquel l'utilisateur veut accéder. Le port défini est 80 pour http.
URL : chemin d'accès	Cette URL permet d'arriver directement sur la page spécifiée.
URL utilisée par le VPN SSL	Lien calculé selon les 3 champs **Serveur de destination**, **Port** et **URL : chemin d'accès**. (Exemple : http://serveur de destination/URL : chemin d'accès).
Nom du lien sur le portail utilisateur	Le lien défini apparaît sur le portail Web Stormshield Network. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le serveur correspondant.

Configuration avancée

Ne pas réécrire les URL du groupe	En sélectionnant un groupe de machines, vous activez la liste blanche d'URL pour ce groupe. Seuls les liens réécrits par le module VPN SSL sont accessibles au travers du VPN SSL. S'il existe sur un site autorisé un lien vers un site Web extérieur (dont le serveur n'est pas défini dans la configuration VPN SSL), celui-ci sera inaccessible par le VPN SSL. Lorsque la liste blanche est activée, elle permet l'accès à des URL qui ne seraient pas réécrites. Par exemple, pour un accès VPN SSL webmail, si l'on souhaite autoriser les utilisateurs à quitter le vpnssl en cliquant sur les liens contenus dans leurs mails, dans ce cas il faut ajouter une liste blanche contenant « * ». **AVERTISSEMENT** Lorsqu'un lien de cette liste blanche est cliqué par un utilisateur, celui-ci n'est plus protégé par le module de VPN SSL Stormshield Network.

Ne jamais afficher ce serveur sur le portail utilisateur (accès via un autre serveur uniquement)	Tous les serveurs configurés dans la configuration du VPN SSL sont par défaut indiqués sur le portail d'authentification Stormshield Network. Toutefois il pourrait être nécessaire qu'un de ces serveurs ne soit accessible que par l'intermédiaire d'un autre serveur, alors, dans ce cas, il faudrait cocher l'option « Ne pas afficher ce serveur sur le portail ». En effet lorsque cette option est cochée dans la configuration d'un serveur, ce serveur est accessible par le VPN SSL mais n'est pas présent dans la liste d'accès direct. Il faut un lien sur un serveur vers ce serveur pour y accéder. Une application peut utiliser plusieurs serveurs mais n'avoir qu'un seul point d'entrée, donc un seul lien dans le menu du portail.
Désactiver la méthode d'authentification NTLM	Certains serveurs Web peuvent demander une authentification préalable au transfert de flux entre le serveur et l'utilisateur. Ne supportant pas cette méthode d'authentification pour les trafics traversant le firewall, celle-ci peut être désactivée.
Réécrire le champ « User-Agent » (force le mode compatibilité d'OWA)	Le champ "User-Agent" de l'entête d'une requête HTTP contient l'identifiant de navigateur Web utilisé par l'utilisateur. Pour Internet Explorer par exemple : Mozilla/4.0 (compatible; MSIE 6.0 ...). La réécriture du "User-Agent" permet donc de modifier la requête HTTP de telle façon que l'on pense qu'elle provient d'un autre type de navigateur qu'en réalité. Cette option est notamment utile dans une utilisation dégradée d'Outlook **Web Access** (OWA). En effet, **Outlook Web Access** (OWA) en mode premium, mode très évolué d'Outlook **Web Access** fait appel au Webdav, une extension du protocole HTTP. Ces extensions n'étant pas supportées par tous les équipements réseau (le mode premium d'OWA est supporté par le module VPN SSL des Firewalls Stormshield Network), le transit de ces trafics pourrait poser des problèmes de compatibilité en particulier sur Internet. Plutôt que de devoir dégrader l'utilisation d'OWA pour tous les utilisateurs (interne et externe), l'option **Réécriture du User-Agent** permet une utilisation "premium" de OWA en interne (compatibilité avec le mode premium facile à obtenir) et une utilisation "dégradée" en passant par le VPN SSL (utilisé par les utilisateurs nomades, via Internet). En effet les "vieux" navigateurs Web ne supportent pas ces extensions, OWA fonctionne donc automatiquement en mode dégradé lorsqu'il rencontre le "User-Agent" de ces navigateurs.
Réécrire le code spécifique au mode Premium d'OWA	En cochant cette option, vous activez les règles spécifiques de réécriture permettant de supporter Outlook Web Access en mode premium.

Lotus Domino Web Access version 7.0.4 fonctionne à travers les tunnels VPN SSL. Il n'est donc pas nécessaire d'activer les règles spécifiques de réécriture permettant de supporter les applications Web de Lotus domino.

URL alternatives pour ce serveur (alias)

Alias du serveur	Les alias permettent d'indiquer au module VPN SSL que le serveur possède plusieurs noms et/ou adresses IP. Si un serveur de mails est défini comme l'objet « webmail.intranet.com » auquel on assigne l'alias "192.168.1.1", lorsque le lien visité sera « http://webmail.intranet.com » ou "http://192.168.1.1" l'utilisateur sera redirigé vers le serveur de mails. En cliquant sur le bouton **Ajouter**, une ligne s'affiche vous permettant d'ajouter un nouvel alias.

Ajout d'un serveur web OWA

Le module **VPN SSL** des Firewalls Stormshield Network supporte les serveurs OWA ("Outlook Web Access") : Exchange 2003, 2007, 2010.

Le mode « Premium » est basé sur les technologies web comme html, css, javascript mais également sur des technologies propriétaires Microsoft comme htc, xml, activeX.

En Exchange 2003, les liens sont des liens absolus que ce soit dans les pages HTML, les scripts javascripts, dans les données XML, dans les feuilles XSL. C'est-à-dire de type http://www.compagnie.com/index.htm.

Il est donc possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec OWA.

Pour ajouter un serveur HTTP-OWA, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter**.
2. Sélectionnez **Serveur web OWA 2003 (mode Premium)** ou **Serveur web OWA 2007 – 2010 (mode premium)**.
3. Indiquez un nom pour ce serveur (le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.).

Les options pré-remplies pour un serveur OWA 2003 premium sont :

- Le port « http »,
- Le champ **URL : chemin d'accès** avec l'indication "exchange",
- Le champ **Activer la liste blanche d'URL** coché,
- Le champ **Ne pas réécrire les URL de la catégorie** avec l'indication « vpnssl_owa »,
- Le champ **Désactiver la méthode d'authentification NTLM** ,
- Le champ **Réécrire le code spécifique au mode Premium d'OWA**.

Pour un serveur OWA 2007-2010, les champs préremplis sont :

- Le port http,
- Le champ **URL : chemin d'accès** avec l'indication "owa",
- Le champ **Activer la liste blanche d'URL** avec l'indication de la catégorie d'URL « vpnssl_owa »,
- Le champ **Réécrire le code spécifique au mode Premium d'OWA**.

Les autres options non remplies doivent être configurées de la même manière que pour un serveur d'accès Web "normal".

Ajout d'un serveur web Lotus Domino

Le module **VPN SSL** des Firewalls Stormshield Network supporte les serveurs Lotus domino.

Il est possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec LOTUS DOMINO.

Pour ajouter un serveur HTTP-Lotus domino, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter**.
2. Sélectionnez **Serveur web Lotus Domino**.
3. Indiquez un nom pour ce serveur (le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.).

L'option pré-remplie pour un serveur Lotus domino est le champ : Port « http ».

L'onglet Serveurs applicatifs

Ajouter un serveur applicatif

Pour ajouter un serveur d'accès aux ressources autres que le type Web, cliquez sur le bouton **Ajouter** et remplissez les champs suivants :

Configuration du serveur

Nom du serveur applicatif	Indiquez un nom pour ce serveur (le nom ne peut pas être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.).
Serveur de destination	Sélectionnez ou créez l'objet représentant le serveur auquel l'utilisateur pourra accéder.
Port	Sélectionnez ou créez l'objet correspondant au port sur lequel l'utilisateur pourra accéder au serveur.

Paramètres du poste utilisateur

Adresse IP d'écoute (locale)	Choix de l'adresse locale du client.
Port	Ce port situé sur la station distante est utilisé par l'applet JAVA pour la redirection des flux chiffrés à destination du Firewall Stormshield Network. Notez que l'utilisateur doit posséder certains droits sur ce port (pour l'ouverture par exemple), veillez donc à modifier les droits locaux d'administration de la machine en conséquence. De plus, le port spécifié doit être libre d'utilisation sur toutes les machines désirant se connecter au serveur associé via le portail.

Configuration avancée

Activer la compatibilité Citrix	Permet d'activer la compatibilité avec le portail Web d'authentification et l'accès via navigateur Web. Cette option est inutile si le client lourd Citrix est utilisé.
Commande exécutée au démarrage	Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage du serveur. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui vérifierait l'activité de l'antivirus présent sur la machine de l'utilisateur avant de lui donner accès au serveur.

Configuration avec un serveur Citrix

Créer un objet pour le serveur Citrix

1. Accédez à la base d'objets afin de créer une machine
2. Sélectionnez une machine.

Configurer un serveur applicatif

Depuis le module **VPN SSL** :

1. Sélectionnez l'onglet **Serveurs applicatifs**.
2. Cliquez sur le bouton **Ajouter**
3. Sélectionnez **Serveur Citrix**.

4. Donnez un nom à votre serveur.
   L'écran de configuration du serveur Citrix s'affiche.
5. Sélectionnez le serveur Citrix créé précédemment dans la base d'objets (Cf. Etape1)

Configurer un Serveur web

1. Sélectionnez l'onglet **Serveurs web.**
2. Cliquez sur le bouton **Ajouter**
3. Sélectionnez **Serveur web**.
4. Donnez un nom à votre serveur.
   L'écran de configuration du serveur Web s'affiche.
5. Au niveau de l'URL : chemin d'accès, indiquez CitrixAccess/auth/login.aspx (s'il s'agit de la version Presentation Server 4.0).

Envoyer la configuration

Cliquez sur le bouton **Appliquer**.

Autoriser l'accès au portail Web

1. Ouvrez un navigateur Web
2. Identifiez –vous (https://adresse IP de votre firewall ou son nom).
3. Allez dans **Accès sécurisé**
4. Sélectionnez dans la liste déroulante Ouvrir l'accès sécurisé dans un pop-up.

> **AVERTISSEMENT**
> Il est important que l'applet VPN SSL Stormshield Network fonctionne en tâche de fond.

5. Sélectionnez ensuite **Accès portail\Portail** puis saisissez votre nom d'utilisateur, votre mot de passe et le domaine.

Suppression d'un serveur

Pour supprimer un serveur, suivez la procédure suivante :

1. Sélectionnez le serveur à supprimer.
2. Cliquez sur le bouton **Supprimer**.

> **AVERTISSEMENT**
> Lorsqu'un serveur est retiré de la liste des serveurs VPN SSL configurés, il est automatiquement retiré des profils dont il faisait partie.

L'onglet Profils utilisateurs

Principe de fonctionnement

Par défaut tous les serveurs configurés dans le module VPN SSL portail sont affichés sur le portail d'authentification. Ainsi tous les utilisateurs ayant droit aux fonctionnalités de VPN SSL portail offertes au firewall ont accès à tous les serveurs configurés par l'administrateur. La notion de profil permet de déterminer quels utilisateurs auront accès à quels serveurs

configurés dans le VPN SSL portail.

Configuration d'un profil

Ajouter un profil

Pour ajouter un profil dans la liste des profils VPN SSL disponibles, référez-vous à la procédure suivante :

1. Cliquez sur le bouton **Ajouter**.
2. Spécifiez le **Nom du profil**.
3. Cliquez sur **Appliquer**.
   La configuration du profil s'affiche dans la partie droite de l'écran.
4. Activez dans les listes : « Serveurs web accessibles » et « Serveurs applicatifs accessibles » les serveurs qui seront accessibles aux utilisateurs appartenant à ce profil.
5. Cliquez sur **Appliquer** pour activer la configuration.

AVERTISSEMENT
Il est impossible de créer un profil s'il n'existe pas au minimum un serveur VPN SSL configuré.

Supprimer un profil

Pour supprimer un profil, référez-vous à la procédure suivante :

1. Sélectionnez le profil à supprimer.
2. Cliquez sur le bouton **Supprimer**.

Utiliser un profil

Un profil peut être utilisé de 2 manières différentes :

- Soit il est utilisé comme profil par défaut dans la configuration du VPN SSL portail,
- Soit il est assigné à un ou plusieurs utilisateurs comme profil spécifique de ces utilisateurs.

Utiliser un profil comme profil par défaut

Pour utiliser un profil comme profil par défaut de la configuration VPN SSL portail (tous les utilisateurs n'utilisant pas de profil spécifique seront affectés par ce profil par défaut), référez-vous à la procédure suivante :

1. Créez un profil dans le module **VPN SSL portail** > onglet **Profils utilisateurs.**
2. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration **Utilisateurs** > **Droits d'accès VPN** > **Accès par défaut** > **VPN SSL portail**.

Utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs.

Pour utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs (quelle que soit la liste des serveurs définis par le profil par défaut, ces utilisateurs posséderont une liste de serveurs spécifiques), référez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil spécifique (nom du profil et serveurs associés) dans **Profils utilisateurs** du module **VPN SSL Portail**.
2. Appliquez les modifications en cliquant sur **Appliquer.**
3. Dans le module **Utilisateurs** > **Droits d'accès** > **Accès détaillé**, choisissez l'utilisateur.

4. Dans la colonne « VPN SSL », choisissez le profil défini au préalable.
5. Cliquez sur le bouton **Appliquer**.

Services VPN SSL sur le portail Web Stormshield Network

Lorsque l'authentification sur le firewall est activée (module **Utilisateurs\ Authentification** onglet *Général*, et coche « Activer le portail captif »), vous pouvez accéder aux fonctionnalités du VPN SSL Stormshield Network.

Pour accéder aux fonctionnalités du **VPN SSL**, suivez la procédure suivante :

1. Ouvrez un navigateur Web.
2. Indiquez dans la barre d'adresse, l'URL : https://Adresse_Firewall.
   La page d'authentification sur le firewall apparaît.
3. Connectez-vous.
4. Si vous possédez des droits sur l'utilisation des fonctionnalités VPN le menu Accès sécurisé apparaît. Il permet d'accéder aux fonctionnalités VPN SSL.

Lorsque la durée d'authentification est expirée ou que l'accès au VPN SSL est refusé, l'utilisateur sera redirigé vers la page d'authentification transparente (SSO) si cette méthode est disponible.

Accédez aux sites Web de votre entreprise par un tunnel SSL

Ce menu présente les sites Web configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

Les autres accès sécurisés permettent d'accéder au menu des autres sites sécurisés configurés par l'administrateur.

Accédez aux ressources de votre entreprise par un tunnel SSL

Ce menu présente les autres serveurs configurés par l'administrateur et auxquels les utilisateurs peuvent accéder.

AVERTISSEMENT
Sur cette page aucun lien n'est disponible. Il est pourtant indispensable que cette fenêtre reste ouverte pendant toute la durée de la connexion (elle peut être minimisée). La fermeture de la fenêtre entraîne la coupure de la connexion.

Pour accéder aux ressources configurées par l'administrateur, il s'agit d'indiquer au logiciel client, un client de messagerie par exemple, que le serveur auquel il doit se connecter pour récupérer les mails n'est plus le serveur mail habituel mais il faut lui indiquer une adresse du type "127.0.0.1:Port_Ecoute" où "Port_Ecoute" est le port spécifié dans la configuration du serveur.

Le port d'écoute pour chacun des serveurs configurés est rappelé dans la page du portail Web Stormshield Network.

WI-FI

Le module Réseau WI-Fi permet l'activation du réseau Wi-Fi. Il présente également certains paramètres physiques de ce réseau.

> **NOTE**
> Les paramètres présentés dans cet écran sont communs aux deux points d'accès disponibles sur le firewall.

Activer le Wi-Fi : permet d'activer ou de désactiver l'utilisation du réseau Wi-Fi sur le firewall.

Configuration générale

Planification	Sélectionnez un objet temps définissant la période de disponibilité du réseau Wi-Fi.
Mode	Sélectionnez la norme de réseau Wi-Fi devant être gérée par le firewall : • 802.11a (fréquence 5 Ghz - portée inférieure), • 802.11b (fréquence 2.4 Ghz - portée supérieure), • 802.11g (fréquence 2.4 Ghz - version améliorée de la norme b - portée supérieure), • 802.11a/n (haut débit [agrégation de canaux] basé sur la norme a - fréquence 5 Ghz), • 802.11g/n. (haut débit [agrégation de canaux] basé sur la norme g - fréquence 2.4 Ghz).

Configuration des canaux

Pays	Sélectionnez le pays dans lequel le firewall est installé. Ce choix influe sur les canaux de communication disponibles ainsi que sur la puissance du signal pour ces canaux, selon la réglementation locale du pays.
Canal	Sélectionnez le canal utilisé par le réseau Wi-Fi du firewall. Le choix des canaux proposés dépend du pays sélectionné dans le champ précédent.
Puissance du signal	Ce champ permet de régler la puissance d'émission du réseau Wi-Fi pour le canal choisi. Selon le choix du pays et les réglementations locales associées, les puissances proposées peuvent différer.

Configuration des points d'accès : un clic sur ce lien vous dirige vers le modules **Interfaces** afin de paramétrer la (les) interface(s) wlan (nom de réseau, type d'authentification,...) nécessaires.

Caractères autorisés ou interdits

Cette section précise les caractères autorisés ou interdits pour les différents éléments présents dans la configuration de votre firewall.

Nom du firewall

- Le nom du firewall est limité à 127 caractères (caractères **autorisés**) :

```
<alphanum> - _ .
```

Identifiant

- Identifiant (caractères **interdits**) :

```
" <tab> & ~ | = * < > ! ( ) [ ] / \ $ % ? ' ` <space> : ; @ + ,
```

Mot de passe administrateur

- Le mot de passe est limité à 127 caractères (caractères **interdits**) :

```
" <tab>
```

Mot de passe administrateur d'un firewall virtuel sur Microsoft Azure

- Mot de passe (caractères **interdits**) :

```
" ' ` \ $ ( ) &
```

Bases LDAP

- Nom d'un utilisateur dans la base LDAP (caractères **interdits**) :

```
" <tab> , ; & ~ | = * < > ! ( ) \
```

- Identifiant d'un utilisateur (caractères **interdits**) :

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

ATTENTION
Dans le cas d'un annuaire externe de type Microsoft Active Directory, l'identifiant utilisateur **doit à la fois** respecter les critères énoncés ci-dessus **et** les critères imposés par Microsoft.

- Le mot de passe est limité à 127 caractères (caractères **interdits**) :

```
" <tab>
```

- Nom d'un groupe dans la base LDAP, le nom du DN entier est limité à 1023 caractères (caractères **interdits**) :

```
" <tab> & ~ | = * < > ! ( ) \ $ ' ` + , ; @ <space>
```

- Chemin des bases LDAP : DN, CA Dn et consort (caractères **interdits**) :

```
" & ~ | * < > ! ( )
```

PPTP

- Identifiant d'un utilisateur PPTP (caractères **autorisés**) :

```
<alphanum> - _ .
```

- Mot de passe (caractères **interdits**) :

```
" <tab>
```

Alertes e-mail

- Adresse e-mail - partie boite mail (caractères **autorisés**) :

```
<alphanum> ! # $ % & \ * + - / = ? _ ` { } | ~ .
```

- Nom de l'identifiant utilisé pour l'authentification au serveur (caractères **interdits**) :

```
< >
```

- Nom des groupes de destinataires (caractères **interdits**) :

```
<tab> <space> ! " # , = @ [ \ | ]
```

Objets de type Nom DNS (FQDN)

- Le nom est limité à 255 caractères (caractères **autorisés**) :

```
<alphanum> . -
```

Certificats et PKI

- Nom d'une autorité de certification (caractères **interdits**) :

```
/ <tab> " ` % :
```

- Nom court d'un certificat ou d'une autorité de certification (caractères **interdits**) :

```
/ <tab> " ` % : \
```

Objets réseau

- Le nom d'un objet réseau est limité à 255 caractères (caractères **interdits**) :

```
<tab> <space> ! " # , = @ [ \ | ] /
```

- Ce nom ne doit pas contenir l'un des préfixes **interdits** suivants :

```
Firewall_
Network_
ephemeral_
Global_
```

- Les noms suivants sont **interdits** :

```
any
any_v4
any_v6
internet
internet_v4
internet_v6
none
anonymous
broadcast
all
original
blackhole
```

NOTE
Les noms d'objets sont insensibles à la casse.

- Un commentaire ne doit pas contenir les caractères suivants (caractères **interdits**) :

```
" <tab> < >
```

Nom d'interfaces réseau

- Un nom d'interface est limité à 15 caractères. Il ne peut pas contenir les appellations suivantes si elles sont suivies immédiatement et exclusivement par des chiffres (ex : ethernet0, dialup123) :

```
ethernet
switch
usbethernet
wifi
vlan
bridge
dialup
pptp
loopback
agg
ipsec
sslvpn
gretun
gretap
usb
```

- Un nom d'interface ne doit pas commencer par l'un des préfixes suivants :

```
firewall
network
serial
loopback
```

- Un nom d'interface ne doit pas être l'un des mots réservés suivants :

```
ipsec
sslvpn
dynamic
any
protected
notprotected
blackhole
```

- Un nom d'interface ne doit pas comporter les caractères suivants (caractères **interdits**) :

```
@ " # <tab> <space> [ ] < >
```

VPN SSL Portail

- Nom de serveur et alias (caractères **autorisés**) :

```
<alphanum> - _ . :
```

- Préfixe du répertoire racine de l'URL (caractères **autorisés**) :

```
<alphanum> - _
```

Filtrage et NAT

- Commentaire et séparateur de règle (caractères **interdits**) :

```
< > "
```

VPN IPsec

- Nom d'un correspondant IPsec (caractères **interdits**) :

```
" <tab> < > # @ [ \ ]
```

- Nom d'une règle IPsec (caractères **interdits**) :

```
. , : { } [ ] = " # \n <tab> <space>
```

Qualité de service (QoS)

Files d'attente de QoS

- Le nom est limité à 31 caractères (caractères **interdits**) :

```
< > @ [ ] # ! \ " | = <space> <tab>
```

ATTENTION
Les restrictions pour les noms d'interface réseau s'appliquent également pour les noms des files d'attente de QoS.

Traffic shapers

- Le nom est limité à 15 caractères (caractères **interdits**) :

```
< > @ [ ] # ! \ " | = <space> <tab>
```

Géolocalisation

- Le nom d'une catégorie de géolocalisation comprend au maximum 5 caractères et doit respecter le format suivant : "nom court du continent" ou "nom court du continent:nom court du pays". Exemples : "EU", "EU:FR". Caractères **autorisés** :

```
<alphanum> : : (":" autorisés sauf en début et fin de nom)
```

Services Web - Réputation

- Le nom d'un service Web ou d'une catégorie de réputation ne doit pas dépasser 40 caractères (caractères **autorisés**) :

```
<alphanum> : : (":" autorisés sauf en début et fin de nom)
```

Mot de passe du TPM

- Le mot de passe est limité à 240 caractères (caractères **interdits**) :

```
" <tab>
```

Structure d'une base objets au format CSV

Cette section définit, pour chaque type d'objet pouvant être importé ou exporté, la structure d'une ligne constituant la base objets au format CSV.

Vous pouvez réaliser ces opérations d'import / export dans le module **Objets** > OBJETS RÉSEAU / TEMPS.

Sur chaque ligne du fichier, tous les champs sont séparés par des virgules. Les champs optionnels vides sont inclus entre deux virgules.

Machine

- Type d'objet (obligatoire) : **host**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Adresse IPv4 (obligatoire),
- Adresse IPv6 (optionnel),
- Résolution DNS : **static** ou **dynamic**,
- Adresse MAC (optionnel),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLES
host,dns1.google.com,8.8.8.8,2001:4860:4860::8888,,,"Google Public DNS Server"
host,AD_Server,192.168.65.12,,static,,""

Plage d'adresses IP

- Type d'objet (obligatoire) : **range**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Première adresse IPv4 de la plage (obligatoire),
- Dernière adresse IPv4 de la plage (obligatoire),
- Première adresse IPv6 de la plage (optionnel),
- Dernière adresse IPv6 de la plage (optionnel),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
range,dhcp_range,10.0.0.10,10.0.0.100,,,""

Nom DNS (FQDN)

- Type d'objet (obligatoire) : **fqdn**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Adresse IPv4 (obligatoire),

- Adresse IPv6 (optionnel),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
fqdn,www.free.fr,212.27.48.10,,""

Réseau

- Type d'objet (obligatoire) : **network**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Adresse IPv4 (obligatoire),
- Masque réseau (obligatoire),
- Adresse IPv6 (optionnel),
- Longueur du préfixe IPv6 (optionnel) : indiqué en nombre de bits,
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLES
network,IANA_v6_doc,,,,2001:db8::,32,""
network,rfc5735_private_2,172.16.0.0,255.240.0.0,12,,,""

Port

- Type d'objet (obligatoire) : **service**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Protocole (obligatoire) : TCP, UDP ou Any,
- Port (obligatoire) : numéro de port utilisé par le service,
- Premier port de la plage : champ vide,
- Derrnier port de la plage : champ vide,
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
service,bgp,tcp,179,,"Border Gateway Protocol"

Plage de ports

- Type d'objet (obligatoire) : **service**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Protocole (obligatoire) : TCP, UDP ou Any,
- Port : champ vide,
- Premier port de la plage (obligatoire) : numéro du premier port utilisé par la plage de ports,

- Derrnier port de la plage (obligatoire) : numéro du dernier port utilisé par la plage de ports,
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
service,MyPortRange,tcp,2000,2032,""

Protocole

- Type d'objet (obligatoire) : **protocol**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Numéro de protocole (obligatoire) : numéro normalisé disponible auprès de l'IANA (Internet Assigned Numbers Authority),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
protocol,ospf,89,"Open Shortest Path First"

Groupe de machines, d'adresses IP ou de réseaux

- Type d'objet (obligatoire) : **group**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Eléments composant le groupe (obligatoire) : liste des éléments inclus dans le groupe (liste encadrée par des guillemets - éléments séparés par des virgules),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
group,IANA_v6_reserved,"IANA_v6_6to4,IANA_v6_doc,IANA_v6_linklocal_unicast,IANA_v6_teredo,IANA_v6_multicast,IANA_v6_uniquelocal",""

Groupe de services

- Type d'objet (obligatoire) : **servicegroup**,
- Nom (obligatoire) : chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits),
- Eléments composant le groupe (obligatoire) : liste des éléments inclus dans le groupe (liste encadrée par des guillemets - éléments séparés par des virgules),
- Commentaire (optionnel) : chaîne de texte encadrée par des guillemets.

EXEMPLE
servicegroup,ssl_srv,"https,pop3s,imaps,ftps,smtps,jabbers,ldaps","SSL Services"

Structure du fichier d'import de services Web personnalisés (format CSV)

Cette section définit, pour chaque service Web personnalisé pouvant être importé ou exporté, la structure d'une ligne constituant le fichier au format CSV.

Importer / exporter des services Web personnalisés

Vous pouvez réaliser ces opérations d'import / export dans le module **Objets** > SERVICES WEB :

- Onglet **Import de services personnalisés** pour l'import,
- Onglet **Liste des services Web** pour l'export (menu **Exporter la base personnalisée**).

Fichier d'import CSV : structure et limitations

- Chaque ligne du fichier est constituée de plusieurs champs, tous séparés par des virgules,
- Les champs optionnels vides sont inclus entre deux virgules,
- Le fichier doit comporter une ligne vide après le dernier enregistrement.

```
#name,#ip/fqdn,#date,#revision,#comment
```

Champ	Description
Nom du service (obligatoire)	Chaîne de texte respectant les critères suivants : • Maximum 20 caractères alphanumériques, • Chaîne de texte respectant les caractères acceptés (voir section Caractères autorisés ou interdits), • Non sensible à la casse, le nom est toujours considéré en minuscule. Les majuscules ne sont pas conservées sur le firewall SNS lors de l'import.
Adresse IP ou FQDN (obligatoire)	Adresse IPv4 / IPv6 publique ou un FQDN. Un FQDN ne peut contenir qu'**un seul** méta-caractère (*wildcard*) ***** en début ou au milieu de son nom. Si un service Web repose sur plusieurs adresses IP ou FQDN, la ligne le décrivant doit être dupliquée autant de fois que le service Web comporte d'adresses IP ou de FQDN. Seules les informations optionnelles de la première ligne seront conservées.
Date de révision (optionnel)	Date et heure de révision au format **YYYY/MM/DD** ou **YYYY/MM/DD hh:mm** (exemple : *2022/10/15 10:30*).
Numéro de révision (optionnel)	Numéro de révision pouvant contenir jusqu'à 3 chiffres : **major.minor.patch** (exemple : *10.2*).
Commentaire (optionnel)	Chaîne de texte libre pouvant être encadrée de guillemets si elle contient une virgule.

```
name1,1.1.1.1,2021/09/21 11:00,1.1.1,Simple case
name2,2.2.2.2,2021/12/31,2,"Comment, with comma"
name2,domain.tld,2022/01/01,3,"Date, revision and comment are discarded"
name3,*.newdomain.tld,,,No date and revision
```

Une limitation sur le nombre de lignes autorisées dans le fichier d'import existe :

Firewalls physiques SNS	Firewalls virtuels EVA

SN160(W)	5 000
SN210(W), SN310	10 000
SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN510, SN710, SNi10, SNi20, SNi40	100 000
SN-M-Series-520, SN-M-Series-720, SN910, SN-M-Series-920, SN1100, SN2000, SN2100, SN-L-Series-2200, SN3000, SN3100, SN-L-Series-3200, SN-XL-Series-5200, SN6000, SN6100, SN-XL-Series-6200	1 000 000

EVA avec 1 Go de RAM	10 000
EVA avec 2 Go à 6 Go de RAM	100 000
EVA avec 8 Go à 64 Go de RAM	1 000 000

Une limitation sur le nombre de lignes possédant un FQDN avec un méta-caractère ***** au milieu existe : 10 % du nombre de lignes autorisées dans le fichier d'import.

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.