GUIDE

STORMSHIELD NETWORK SECURITY

MANUEL D'UTILISATION ET DE CONFIGURATION

Version 4

Date : 18 décembre 2019

Référence : sns-fr-manuel_d'utilisation_et_de_configuration-v4.0.1

Table des matières

BIENVENUE 10

Recommandations sur l'environnement d'utilisation 10
- Présentation 10
- Veille sécurité 11
- Mesures de sécurité physiques 11
- Mesures de sécurité organisationnelles 11
- Agents humains 12
- Environnement de sécurité TI (Technologies de l'Information) 12

Sensibilisation des utilisateurs 14
- Gestion des accès des administrateurs 14
- Gestion des mots de passe de l'utilisateur 15
- Environnement de travail 16
- Gestion des accès d'utilisateurs 17

ACTIVE UPDATE 18

Mises à jour automatiques 18

Configuration avancée 18
- Serveurs de mise à jour de la Base d'URL 18
- Serveurs de mise à jour des signatures de protection contextuelle personnalisées 18
- Serveurs de mise à jour 18

ADMINISTRATEURS 19

Onglet « Administrateurs » 19
- Les interactions 19
- Les manipulations possibles 19
- La grille des droits 21

Onglet « Compte admin » 23
- Authentification 23
- Exports 24

Onglet « Gestion des tickets » 24
- La grille 24
- Les actions possibles 24

AGENT SNMP 26

L'onglet « Général » 26
- Configuration des informations MIB-II ..26
- Envoi des alertes SNMP (traps) 26

L'onglet « SNMPv3 » 27
- Connexion à l'agent SNMP 27
- Authentification 27
- Chiffrement (optionnel) 27
- Envoi des alertes SNMPv3 (traps) 27

L'onglet « SNMPv1 - SNMPv2c » 28
- Connexion à l'agent SNMP 29
- Envoi des alertes SNMPv2c (traps) 29
- Envoi des alertes SNMPv1 (traps) 29

MIBS et Traps SNMP 29
- Format d'alerte et d'évènement SNMP Stormshield Network (TRAPs) 30
- Base d'information consultables (MIBs) 32

ALERTES E-MAILS 46

L'onglet « Configuration » 46
- Activer les notifications par e-mail 46
- Serveur SMTP 46
- Fréquence d'envoi des e-mails (en minutes) 47
- Alarmes de prévention d'intrusion 47
- Evénements système 47

L'onglet « Destinataires » 48
- Créer un groupe 48
- Supprimer un groupe 49
- Vérifier 49

L'onglet « Modèles » 49
- Edition du modèle (HTML) 49
- Management des vulnérabilités 50
- Demande de certificat 50
- Enrôlement d'un utilisateur 50
- Liste des variables 50
- Exemple de rapport reçu par e-mail pour les alarmes 51

ANTISPAM 52

L'onglet «Général » 52
- Paramètres SMTP 52
- Configuration avancée 53

L'onglet « Domaines en liste blanche» 54
- Les interactions 55

L'onglet « Domaines en liste noire » 55
- Les interactions 55

ANTIVIRUS 57

Moteur antiviral 57

Paramètres 57
- L'analyse des fichiers ClamAV 57
- L'analyse des fichiers Kaspersky 57

Analyse sandboxing 58

APPLICATIONS ET PROTECTIONS 59

Vue par profil d'inspection 59
- Sélection du profil de configuration 59
- Les différentes colonnes 61

Vue par contexte 63

AUTHENTIFICATION 64

Onglet « Méthodes disponibles » 64

Les interactions 64
Méthodes d'authentification 65
Onglet « Politique d'authentification » 72
Les actions sur les règles de la politique d'authentification 72
Les interactions 74
Nouvelle règle 74
Onglet « Portail captif » 75
Portail captif 75
Serveur SSL 76
Conditions d'utilisation de l'accès à Internet 76
Configuration avancée 77
Onglet « Profils du portail captif » 77
La barre d'actions 77
Authentification 78
Conditions d'utilisation de l'accès à Internet 78
Durées d'authentification autorisées 78
Configuration avancée 78
Proxy HTTP transparent ou explicite et objets Multi-utilisateur 81
Objets Multi-utilisateur 81
Proxy transparent (implicite) 81
Proxy explicite 82

CERTIFICATS ET PKI 83

Les actions possibles 84
La barre de recherche 84
Le filtre 84
Ajouter 84
Révoquer 84
Actions 85
Télécharger 85
Vérifier l'utilisation 85
Ajouter des autorités et des identités 85
Ajouter une autorité racine 85
Ajouter une sous-autorité 87
Ajouter une identité utilisateur 88
Ajouter une identité Smartcard 90
Ajouter une identité serveur 91
Importer un fichier 93
Révoquer une autorité, une sous-autorité ou un certificat 93
Révoquer une autorité 93
Révoquer une sous-autorité ou un certificat 94
Révoquer un certificat 94
Créer, renouveler ou supprimer une CRL 94
Créer une CRL 95
Renouveler une CRL 95
Supprimer une CRL 95
Supprimer la clé privée d'une identité (et conserver le certificat) 96
Définir une autorité ou une sous-autorité par défaut 96
Télécharger un certificat 96
Télécharger une identité 96
Télécharger une CRL 97

COMPTES TEMPORAIRES 98

Liste des comptes temporaires 98
La grille 98
Les actions possibles 99

CONFIGURATION 101

L'onglet « Configuration générale » 101
Configuration générale 101
Paramètres cryptographiques 101
Politique de mots de passe 102
Paramètres de date et d'heure 103
Configuration avancée 103
Firewalls industriels uniquement (modèles SNi40) 104
L'onglet « Administration du Firewall » 105
Accès à l'interface d'administration du Firewall 105
Accès aux pages d'administration du Firewall 106
Avertissement pour l'accès à l'interface d'administration 106
Accès distant par SSH 107
L'onglet « Paramètres réseaux » 107
Support IPv6 107
Serveur proxy 107
Résolution DNS 108

CONFIGURATION DE LA SUPERVISION 109

Intervalles de rafraîchissement 109
La grille de configuration des interfaces et des files d'attente de QoS à superviser 109
Onglet "Configuration des interfaces" 109
Onglet "Configuration de la QoS" 109

CONFIGURATION DES ANNUAIRES 111

Fenêtre principale 111
Bouton "Ajouter un annuaire" 111
Liste "Action" 111
Création d'un LDAP interne 112
Etape 1 : Choix de l'annuaire 112
Etape 2 : Accès à l'annuaire 112
Ecran de l'annuaire LDAP interne 112
Connexion à un annuaire LDAP externe 113

Etape 1 : Choix de l'annuaire 113
Etape 2 : Accès à l'annuaire 113
Ecran de l'annuaire LDAP externe 114
Connexion à un annuaire LDAP externe de type PosixAccount 117
Etape 1 : Choix de l'annuaire 117
Etape 2 : Accès à l'annuaire 117
Ecran de l'annuaire LDAP externe 118
Connexion à un annuaire Microsoft Active Directory 121
Etape 1 : Choix de l'annuaire 121
Etape 2 : Accès à l'annuaire 121
Ecran de l'annuaire Microsoft Active Directory 122

CONFIGURATION DES RAPPORTS 126
Menu "Général" 126
La grille des rapports et graphiques historiques 126
Onglet "Liste des rapports" 126
Onglet "Liste des graphiques historiques" 127

CONSOLE CLI 128
La liste des commandes 128
La zone de saisie 129

DHCP 130
Général 130
Service « Serveur DHCP » 130
Paramètres par défaut 130
Plage d'adresses 131
Réservation 131
Configuration avancée 132
Service « Relai DHCP » 133
Paramètres 133
Interfaces d'écoute et de sortie du service DHCP Relai 134

DNS DYNAMIQUE 135
Liste des profils de DNS dynamique 135
Configuration d'un profil 135
Résolution DNS 135
Fournisseur du service DNS dynamique 136
Configuration avancée 136

DROITS D'ACCES 137
Onglet « Accès par défaut » 137
VPN SSL Portail 137
IPSEC 137
VPN SSL 138
Parrainage 138
Onglet « Accès détaillé » 138
Les manipulations possibles 138
Les interactions 138
La grille de configuration 138
Onglet « Serveur PPTP » 140
Les interactions 140

ENREGISTREMENT DES COMMANDES DE CONFIGURATION 141
Enregistrer une séquence de commandes de configuration 141

ENRÔLEMENT 142
La grille d'enrôlement 142
Les actions possibles 142
Les demandes d'enrôlement utilisateurs et certificats 142
Propriétés avancées 143

ÉVÉNEMENTS SYSTÈME 144
Les actions possibles 144
Rechercher 144
Restaurer la configuration par défaut 144
La liste des événements 144
Liste des alarmes système 145

FILTRAGE ET NAT 149
Evaluation du filtrage et impact du NAT ... 149
Mode « FastPath » 149
Les politiques 149
Sélection de la politique de filtrage 150
Les actions 151
La sélection multiple 151
Le glisser-déposer (« drag'n'drop ») 151
L'onglet « Filtrage » 152
Les actions sur les règles de la politique de filtrage 152
Les interactions 154
La grille de filtrage 155
L'onglet « NAT » 169
Les actions sur les règles de la politique de NAT 169
Les interactions 172
La grille de NAT 172

FILTRAGE SMTP 178
Les profils 178
Sélection du profil 178
Les boutons 178
Les règles 178
Les manipulations possibles 179

Les interactions 179
La grille 179
Erreurs trouvées dans la politique de filtrage SMTP 180

FILTRAGE SSL 181

Les profils 181
Sélection du profil 181
Les boutons 181
Les règles 182
Les manipulations possibles 182
Les interactions 182
La grille 182
Erreurs trouvées dans la politique de filtrage SSL 183

FILTRAGE URL 184

Les profils 184
Sélection du profil 184
Les boutons 184
Les règles 184
Les manipulations possibles 185
Les interactions 185
La grille 185
Erreurs trouvées dans la politique de filtrage d'URL 186

HAUTE DISPONIBILITE 187

Etape 1 : Créer ou rejoindre un cluster en Haute Disponibilité 187
Etape 2 : Configuration des interfaces réseaux 188
Si vous avez choisi de créer un cluster 188
Si vous avez choisi de rejoindre un cluster 189
Etape 3 : Clé pré partagée du cluster et chiffrement des données 189
En cas de création de cluster 189
En cas de cluster existant 190
Etape 4 : Résumé et finalisation du cluster 190
En cas de création de cluster 190
En cas de cluster existant 190
Ecran de la Haute disponibilité 191
Communication entre les firewalls du groupe de haute disponibilité 191
Configuration avancée 191

INTERFACES 194

Modes de fonctionnement entre interfaces 194
Mode avancé 194
Mode Bridge ou mode transparent 194
Mode hybride 195
Agrégation de liens (LACP) – SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100. 195
Conclusion 195
Présentation de l'écran de configuration 195
L'arborescence des interfaces 196
La barre d'outils 197
Créer un bridge 198
Créer un bridge sans membres 198
Créer un bridge contenant des interfaces pré-sélectionnées 198
Modifier un Bridge 198
Onglet "Configuration Générale" 199
Onglet "Configuration avancée" 199
Supprimer un bridge 201
Modifier une interface Ethernet (en mode Bridge) 201
Onglet « Configuration générale » 201
Onglet « Configuration avancée » 203
Modifier une interface Ethernet (en mode avancé) 204
Créer ou modifier une interface Wi-Fi (WLAN) 204
Onglet « Configuration générale » 204
Créer un VLAN 206
Créer un VLAN sans interface parente 206
Créer un VLAN rattaché à des interfaces présélectionnées 206
Modifier un VLAN 206
Onglet « Configuration Générale » 206
Onglet « Configuration avancée » 207
Supprimer un VLAN 208
Créer un modem PPTP 208
Modifier un modem PPTP 209
Onglet "Configuration générale" 209
Onglet "Configuration avancée" 209
Créer un modem PPPoE 210
Modifier un modem PPPoE 210
Onglet "Configuration générale" 210
Onglet "Configuration avancée" 211
Supprimer un modem 211
Remarques générales sur la configuration d'un modem 211
Créer une interface USB / Ethernet (pour clé USB / Modem) 211
Créer un profil de modem 211
Créer une interface USB / Ethernet 212
Modifier une interface USB / Ethernet 212
Onglet « Configuration générale » 212
Créer une interface GRETAP 213

Créer une interface GRETAP 214
Modifier une interface GRETAP 214
Onglet « Configuration générale » 214
Onglet « Configuration avancée » 215
Convertir une interface en agrégat de liens (LACP) 216
Créer un agrégat sans membre 217
Créer un agrégat contenant des interfaces présélectionnées 217
Modifier un agrégat de liens (LACP) 218
Onglet "Configuration générale" 218
Onglet "Configuration avancée" 219

INTERFACES VIRTUELLES 220

Création ou modification d'une interface IPSec (VTI) 220
Présentation de la barre de boutons 220
Les interactions 220
Présentation de la grille 221
Création ou modification d'une interface GRE 221
Présentation de la barre de boutons 221
Les interactions 222
Présentation de la grille 222
Création ou modification d'une interface Loopback 222
Présentation de la barre de boutons 222
Les interactions 223
Présentation de la grille 223

LOGS - JOURNAUX D'AUDIT 224

Données personnelles 224
Collaborative security 224
Support de stockage : Carte SD 224
Actions 225
Barre d'outils N°1 : période 225
Barre d'outils N°2 : recherche simple ou avancée 225
Barre d'outils n°3 : actions 227
Informations 227
Afficher les détails d'une ligne de log 227
Les interactions 227
Mode Recherche simple 227
Mode Recherche avancée 228
Adresses IP et objets machine 228
URLs 229
Ports 230
Paquets réseau 231
Vue Alarmes 231
Vue Événements système 231
Les Journaux 231

LICENCE 234

L'onglet « Général » 234
Les boutons 234
Les dates 234
Les informations importantes sur la licence 234
Installation à partir d'un fichier 235
Configuration avancée 235
L'onglet « Détails de la licence» 236
Les boutons 236
La grille 236

MANAGEMENT DES VULNERABILITES 240

Configuration générale 240
Liste des éléments réseaux sous surveillance 241
Configuration avancée 242
Liste d'exclusion (éléments non supervisés) 242

MAINTENANCE 243

Onglet « Mise à jour du système » 243
Mises à jour disponibles : 243
Mise à jour du système 243
Configuration avancée 244
Onglet « Sauvegarder » 244
Sauvegarde de configuration 244
Sauvegarde automatique de configuration 245
Onglet « Restaurer » 246
Restauration de configuration 246
Restauration de sauvegarde automatique 247
Onglet « Configuration » 248
Disque système 248
Maintenance 248
Haute disponibilité 248
Rapport système (sysinfo) 248

MESSAGES DE BLOCAGE 249

L'onglet « Antivirus » 249
Protocole POP3 249
Protocole SMTP 249
Protocole FTP 249
L'onglet « Page de blocage HTTP » 249
Onglets des pages de blocage 250
L'édition des pages de blocage 250

OBJETS RÉSEAU 252

La barre d'actions 252
Les interactions 253
Le filtre 253
Les différents types d'objets 254
Machine 254
Réseau 254
Plage d'adresses IP 255

Port – plage de ports ... 255
Protocole ... 256
Groupe ... 256
Groupe de ports ... 256
Routeur ... 257
Groupe de régions ... 259
Nom DNS (FQDN) ... 260
Objet temps ... 260
L'événement ponctuel ... 260
Le jour de l'année ... 260
Les Jour(s) de la semaine ... 260
Les plage(s) horaire(s) ... 260

OBJETS WEB ... 262

Onglet « URL » ... 262
Grille de catégorie d'URL ... 262
Grille d'URL ... 263
Onglet « Nom de certificat (CN) » ... 264
Onglet « Groupes de catégories » ... 264
Grille des groupes ... 264
Onglet « Base d'URL » ... 265

PORTAIL D'IDENTIFICATION ... 266

Connexion ... 266
Présentation de l'écran ... 266
Déconnexion ... 268

PRÉFÉRENCES ... 269

Paramètres de connexion ... 269
Paramètres de l'application ... 269
Paramètres de l'interface de management ... 270
Liens externes ... 270
Paramètres des traces ... 270

PROFILS D'INSPECTION ... 271

Inspection de sécurité ... 271
Configuration commune à chaque profil ... 271
Configurer les profils ... 272

PROTOCOLES ... 273

Recherche ... 273
Liste des protocoles ... 273
Les profils ... 273
Sélection du profil applicatif ... 273
Les boutons ... 274
Configuration globale des protocoles 274
Configuration globale du protocole TCP/UDP ... 275
Configuration globale du protocole SSL ... 275
Configuration globale du protocole ICMP ... 276
ICQ – AOL IM (OSCAR) ... 277
L'écran des profils ... 277
Live Messenger (MSN) ... 277
L'écran des profils ... 277
Yahoo Messenger (YMSG) ... 277
L'écran des profils ... 277
ICMP ... 278
Onglet « IPS » ... 278
IP ... 278
Onglet « IPS » ... 278
SCTP ... 278
Onglet « IPS » ... 279
TCP-UDP ... 279
L'écran des profils ... 279
BACnet/IP ... 281
Gestion des services ... 281
Support ... 281
CIP ... 281
Paramètres ... 281
Gestion des services ... 282
ETHERNET/IP ... 282
Paramètres ... 282
Gestion des commandes ... 282
Support ... 283
IEC 60870-5-104 (IEC 104) ... 283
Paramètres ... 283
Redondance ... 283
Gestion des ASDU ... 283
Support ... 284
MODBUS ... 284
Paramètres généraux ... 284
Paramètres Modbus ... 284
Gestion des codes de fonction Modbus ... 284
Gestion des adresses Modbus ... 285
Support ... 285
Onglet OPC AE (IPS) ... 285
Gestion des services OPC AE ... 285
Onglet OPC DA (IPS) ... 286
Gestion des services OPC DA ... 286
Onglet OPC HDA (IPS) ... 286
Gestion des services OPC HDA ... 286
OPC UA ... 286
Paramètres OPC UA ... 286
Gestion des services OPC UA ... 287
Support ... 287
PROFINET IO ... 287
Paramètres des squelettes de connexion ... 287
Gestion des UUID ... 287
Gestion des numéros d'opérations ... 288
Support ... 288
PROFINET-RT ... 288

Paramètres 288
Support 288
S7 288
Paramètres 288
Gestion des codes de fonction 289
Support 289
UMAS 289
Paramètres UMAS 289
Gestion des codes de fonction UMAS 290
Support 290
Protocole MS-RPC 290
Onglet DCE/RPC (IPS) 290
Onglet NETBIOS EPMAP (IPS) 292
Onglet OPC AE (IPS) 292
Onglet OPC DA (IPS) 293
Onglet OPC HDA (IPS) 293
NetBios CIFS 293
L'écran des profils 293
Onglet NETBIOS EPMAP (IPS) 294
Squelettes 294
NetBios SSN 294
MGCP 295
L'écran des profils 295
RTCP 295
Onglet « IPS » 295
RTP 295
Onglet « IPS » 295
RTSP 296
Commandes RTSP 296
Taille maximale des éléments (en octets) 296
Paramètres de session RTSP 296
Fonctionnalités RTSP 297
Support 297
SIP 297
Commandes SIP 297
Taille maximale des éléments (en octets) 298
Paramètres de session SIP 298
Extension du protocole SIP 298
Support 299
DNS 299
L'écran des profils 299
FTP 300
Onglet « IPS » 300
Onglet « Proxy » 301
Onglet « Commandes FTP » 302
Onglet « Utilisateurs FTP » 306
Onglet « Analyse des fichiers » 306
Onglet « Analyse sandboxing» 307
HTTP 307
Onglet « IPS » 308
Onglet « Proxy » 311
Onglet « ICAP » 312
Onglet « Analyse des fichiers » 313
Onglet « Analyse sandboxing» 314
NTP 315
POP3 318
Onglet « IPS - PROXY » 318
Onglet « Commandes POP3» 318
Onglet « Analyse des fichiers» 319
Onglet « Analyse sandboxing» 320
SMTP 320
Onglet « IPS » 320
Onglet « Proxy » 321
Onglet « Commandes SMTP» 322
Onglet « Analyse des fichiers» 323
Onglet « Analyse sandboxing» 323
SNMP 324
Versions autorisées 324
Champs vides autorisés 324
Gestion des commandes SNMP 324
Communautés 325
Identifiants 325
OID 325
Support 326
SSL 326
Onglet « IPS » 326
Onglet « Proxy » 327
TFTP 330
L'écran des profils 330
Autres 330

PROXY CACHE DNS 331
Activer le cache de requête DNS 331
Liste des clients DNS autorisés à utiliser le cache 331
Configuration avancée 331

QUALITE DE SERVICE (QoS) 333
Trafic réseau 333
Réservation ou limitation de la bande passante (CBQ) 333
Files d'attente 334
File d'attente par classe d'application ou d'affectation (CBQ) 334
Surveillance du trafic (monitoring) 335
File d'attente par priorité 336
Files d'attente disponibles 337
Cas d'application et recommandations d'utilisation 337

RAPPORTS 339
Données personnelles 339

Collaborative security 339
Support de stockage : Carte SD 339
Rapports d'activités 340
Les actions 340
Interactions 341
Les rapports 342
REGLES IMPLICITES 348
Règles de filtrage implicites 348
La grille de règles 348
Configuration avancée 350
RÉPUTATION DES MACHINES 351
Onglet "Configuration" 351
Général 351
Onglet "Machines" 352
Machines supervisées 352
Configuration avancée 352
ROUTAGE 353
L'onglet « Routes statiques » 353
Présentation de la barre de boutons 353
Les interactions 354
Présentation de la grille 354
L'onglet « Routage dynamique » 354
Configuration avancée 355
Envoi de la configuration 355
L'onglet « Routes de retour » 355
Présentation de la barre de boutons 355
Les interactions 355
Présentation de la grille 356
ROUTAGE MULTICAST 357
Les actions sur les règles de la politique de routage multicast IPv4 357
Les interactions 357
Nouvelle règle 357
La grille 358
SERVEUR PPTP 359
Configuration générale 359
Paramètres transmis aux clients PPTP 359
Configuration avancée 359
Chiffrement du trafic 359
STORMSHIELD MANAGEMENT CENTER 360
Rattachement du firewall à SMC 360
Les boutons 360
SUPERVISION 361
Données personnelles 361
La grille 362
Les info-bulles 362
Matériel / Haute Disponibilité 363
L'onglet "Matériel" 363
L'onglet "Détails du cluster" 364
Système 366
L'onglet "Temps réel" 366
L'onglet "Historique" 366
Interfaces 367
L'onglet "Temps réel" 367
L'onglet "Historique" 367
QoS 368
L'onglet "Temps réel" 368
L'onglet "Historique" 369
Machines 370
L'onglet "Temps réel" 370
L'onglet "Historique" 375
Utilisateurs 376
L'onglet "Temps réel" 376
Connexions 381
La grille "Temps réel" 381
Routage 385
L'onglet "Temps réel" 385
DHCP 386
La grille "Temps réel" 386
Tunnels VPN SSL 386
La grille "Temps réel" 386
La grille "Informations" 387
Tunnels VPN IPSec 388
La grille "Politiques" 388
La grille "Tunnels" 389
Liste noire / liste blanche 389
La grille "Temps réel" 389
TABLEAU DE BORD 391
Le menu de configuration des modules 391
Les modules favoris 391
Configuration 391
La zone dynamique : les widgets 392
Réseau 392
Protections 393
Propriétés 393
Indicateurs de santé 394
Services 395
Pay As You Go 395
TRACES - SYSLOG - IPFIX 397
Onglet « Stockage local » 397
Configuration de l'espace réservé pour les traces 398
Onglet « Syslog » 399
Grille de profils syslogs 399

Configuration d'un profil 399
Onglet « IPFIX » 400
Configuration avancée 401

TRUSTED PLATFORM MODULE (TPM) 402

Initialiser le TPM 402

UTILISATEURS 403

Les actions possibles 403
La barre de recherche 403
Le filtre 404
Les interactions 404
Créer un groupe 404
Créer un utilisateur 405
Supprimer 405
Vérifier l'utilisation 405
La liste des utilisateurs (CN) 406
L'onglet « Compte » 406
L'onglet « Certificat » 406
L'onglet « Membres des groupes » 406

VPN IPSEC 408

L'onglet Politique de chiffrement – Tunnels 408
Site à site (Gateway - Gateway) 409
Anonyme – Utilisateurs nomades 412
L'onglet « Correspondants» 415
La liste des correspondants 415
Les informations des correspondants 416
L'onglet « Identification» 422
Autorités de certification acceptées . 422
Tunnels nomades : clés pré partagées 423
Configuration avancée 423
L'onglet « Profils de Chiffrement » 424
Profils de chiffrement par défaut 424
Tableau des profils 424

VPN SSL 428

Paramètres réseaux 428
Paramètres DNS envoyés au client 429
Configuration avancée 429
Certificats utilisés 430
Configuration 430

VPN SSL Portail 431

L'onglet « Général » 431
Configuration avancée 432
L'onglet « Serveurs web » 432
Ajout d'un serveur web 432
Ajout d'un serveur web OWA 434
Ajout d'un serveur web Lotus Domino 435
L'onglet « Serveurs applicatifs » 435
Configuration avec un serveur applicatif 435
Configuration avec un serveur Citrix 436
Suppression d'un serveur 437
L'onglet « Profils utilisateurs » 437
Principe de fonctionnement 437
Configuration d'un profil 437
Services VPN SSL sur le portail Web Stormshield Network 438
Accédez aux sites Web de votre entreprise par un tunnel SSL 438
Accédez aux ressources de votre entreprise par un tunnel SSL 439

WI-FI 440

Configuration générale 440
Configuration des canaux 440

Support IPv6 441

Support IPv6 441
Détail des fonctionnalités supportées 441
Fonctionnalités non supportées 443
Généralités 444
Configuration 444
Onglet Paramètres Réseaux 444
Bridges et interfaces 445
Bridge 445
Interface Ethernet en mode Bridge 447
Interface Ethernet en mode avancé 447
VLAN 448
Interfaces virtuelles 448
Onglet « Interfaces IPSec (VTI) » 448
Onglet « Loopback » 448
Routage 448
L'onglet « Routes statiques IPv6 » 449
L'onglet « Routage dynamique IPv6 » 450
L'onglet « Routes de retour IPv6 » 451
DHCP 451
Général 452
Service « Serveur DHCP » 452
Service « Relai DHCP » 454
Objets Réseau 455
La barre d'actions 456
Les différents types d'objets 456
Filtrage 456
L'onglet « Filtrage » 457

Noms autorisés ou interdits 458

Nom du Firewall 458
Identifiant & Mot de passe 458
Commentaires (caractères interdits) 458
Séparateurs de règles (caractères interdits) 458

Nom d'interfaces 458
Objets 458
Objets de type Nom DNS (FQDN) 459
Certificats 459
Utilisateurs 459
VPN IPSec 459
VPN SSL 459
Alertes e-mails 459

Structure d'une base objets au format CSV 460

Machine 460
Plage d'adresses IP 460
Nom DNS (FQDN) 460
Réseau 461
Port 461
Plage de ports 461
Protocole 462
Groupe de machines, d'adresses IP ou de réseaux 462
Groupe de services 462

BIENVENUE

Bienvenue dans le manuel d'utilisation et de configuration Stormshield Network v4.0.1

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), SN210(W), SN310,

SN510, SN710, SN910,

SN2000, SN2100, SN3000, SN3100, SN6000, SN6100,

SNi40,

EVA1, EVA2, EVA3, EVA4 et EVAU.

Copyright © Stormshield 2020. 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

DEFINITION

Les critères communs évaluent (sur une échelle "EAL" de 1 à 7) les capacités d'un produit à fournir les fonctions de sécurité pour lesquelles il a été conçu, ainsi que la qualité de son cycle de vie (développement, production, livraison, mise en service, mise à jour).

Présentation

L'installation d'un firewall s'inscrit bien souvent 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 seulement d'installer le firewall entre votre réseau et l'Internet. Notamment parce que la plupart des attaques viennent de l'intérieur (accident, personne mécontente de son travail,

personne licenciée ayant gardé un accès interne…). Mais aussi parce que l'on conviendra qu'il ne sert à rien d'installer une porte blindée si les murs sont en papier.

Sous l'impulsion des critères communs, Stormshield Network vous propose donc de prendre en compte les recommandations d'utilisation de la suite d'administration et du produit firewall énoncées ci-dessous. Ces recommandations vous exposent les exigences d'utilisation à respecter pour garantir le fonctionnement de votre firewall dans le cadre de la certification aux critères communs.

Veille sécurité

Consultez régulièrement les bulletins de sécurité des produits Stormshield publiés sur https://advisories.stormshield.eu.

Appliquez systématiquement une mise à jour de votre équipement si elle corrige une faille de sécurité. Ces mises à jour sont disponibles sur https://mystormshield.eu.

Mesures de sécurité physiques

Les boîtiers appliances firewall-VPN Stormshield Network 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

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, ce mot de passe peut être modifié 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*.

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 boîtiers appliances firewall-VPN, et ce uniquement lors de l'installation de l' appliance firewall-VPN 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 appliances firewall-VPN se font sous sa surveillance, que l'accès soit motivé par des interventions sur l'Appliance ou sur d'autres équipements. Toutes les interventions sur les boîtiers appliances firewall-VPN se font sous sa responsabilité.

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/ou de contrôle de ceux-ci.

Exemple

Mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.

Les administrateurs sont sensibilisés à ces bonnes pratiques de part leur fonction et Il est de leur responsabilité de sensibiliser tous les utilisateurs à ces bonnes pratiques (Cf. section suivante : SENSIBILISATION DES UTILISATEURS).

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux dits "Trusted" 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 de l'Appliance par un administrateur compétent.

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. Notamment, leur compétence et leur organisation implique que :

- Différents administrateurs avec les mêmes droits ne mènent des actions d'administration qui se contredisent.
- L'exploitation des journaux et le traitement des alarmes sont effectués dans les délais appropriés.

Exemple

Modifications incohérentes de politique de contrôle des flux d'information.

Environnement de sécurité TI (Technologies de l'Information)

Les boîtiers appliances firewall-VPN Stormshield Network doivent être installés conformément à la politique d'interconnexion des réseaux en vigueur et 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 boîtier appliance firewall-VPN installé dans l'architecture réseau.

A part l'application des fonctions de sécurité, les boîtiers appliances firewall-VPN ne fournissent pas de service réseau autre que le routage et la translation d'adresse

Exemple

Pas de DHCP, DNS, PKI, proxies applicatifs, etc.*

Les boîtiers Stormshield Network ne sont pas configurés pour retransmettre les flux "IPX", "NetBIOS", "Appletalk", "PPPoe" ou "IPv6".

Les boîtiers appliance firewall-VPN ne dépendent pas de services externes « en ligne » ("DNS", "DHCP", "RADIUS", etc.)* pour l'application de la politique de contrôle des flux d'information.

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 appliances firewall-VPN et au stockage des sauvegardes.

Les équipements réseau avec lesquels l'appliance firewall-VPN 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 boîtiers appliances firewall-VPN.

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.

** Ces services sont disponibles sur un firewall mais ne font pas partie du cadre d'évaluation des critères communs.*

Configurations et mode d'utilisation soumis à l'évaluation

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

- Le mode de distribution des certificats et des CRL est manuel (importation).
- Le mode d'utilisation soumis à l'évaluation exclut le fait que la TOE s'appuie sur d'autres services tels que PKI, serveur DNS, DHCP, proxies. Les modules que Stormshield Network fournit en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester. Il s'agit précisément :
    - de l'infrastructure à clés publiques (PKI) interne,
    - du module d'authentification des utilisateurs,
    - du module VPN SSL (Portail et Tunnel),
    - du moteur antivirus (ClamAV ou Kaspersky),
    - du module Active Update,
    - du module de routage dynamique (Service de Routage dynamique BIRD),
    - du cache DNS (Cache DNS/Proxy),
    - des serveurs SSH, DHCP, MPD et SNMPD (Serveur SSH, Serveur DHCP et Agent SNMP),
    - du client DHCP (Serveur DHCP),
    - du démon NTP (Client NTP),
    - du relai DHCP (Relai DHCP),
    - du service « Cloud backup ».
- Bien que supportée, la fonctionnalité IPv6 est désactivée par défaut et doit le rester dans le cadre de l'évaluation.
- Les administrateurs et les utilisateurs IPSec sont gérés par l'annuaire LDAP interne. Le mode d'utilisation soumis à l'évaluation exclut le fait que des clients LDAP externes au boîtier appliance firewall-VPN puissent se connecter à cette base.
- Les journaux d'audit sont, selon les modèles, stockés localement ou émis par Syslog.
- La possibilité offerte par la politique de filtrage d'associer à chaque règle de filtrage une inspection applicative (proxies HTTP, SMTP, POP3, FTP) et une programmation horaire est hors du cadre de cette évaluation et ne devra pas être utilisé.
- L'option proposée par la politique de filtrage d'associer l'action « déchiffrer » (proxy SSL) à une règle de filtrage est hors du cadre de cette évaluation et ne devra pas être employée.

Algorithmes cryptographiques nécessaires pour être conforme au RGS et utilisés pour l'évaluation

Algorithme	Taille des clés
Diffie-Hellman	2048, 3072, 4096

Algorithme	Taille des clés
RSA	2048, 4096

Algorithmes	Taille d'empreintes numériques
HMAC-SHA1	160
HMAC-SHA2	256, 384, 512
SHA2	256, 384, 512

Algorithmes	Taille des clés
AES	128, 192, 256
Triple DES	168
Blowfish	128 à 256
CAST	128

L'option Perfect Forward Secrecy (PFS) effectue un nouvel échange Diffie-Hellman lors de la seconde phase d'IKE. Cela permet d'assurer que si une clé est cassée, on ne pourra en déduire les clés suivantes ou précédentes, et d'empêcher ainsi de déchiffrer tout l'échange IPsec, mais seulement la partie de la communication protégée par la clef corrompue. Il est fortement recommandé de laisser actif le PFS pour être conforme au RGS, ce qui est le cas retenu pour l'évaluation.

La sécurité de la connexion au portail d'authentification et à l'interface d'administration a été renforcée, conformément aux recommandations de l'*Agence Nationale de la Sécurité des Systèmes d'Information* (*ANSSI*). Cet accès se fait en imposant certaines versions du protocole SSL/TLS ; la version SSLv3 est désactivée au profit des versions TLS. L'utilisation de suites de chiffrement AES avec Diffie-Hellman est également imposée. Cette configuration n'étant pas supportée par le navigateur Internet Explorer en version 6, 7 et 8, il conseillé d'utiliser une version supérieure de ce navigateur. Il ne faut pas désactiver cette configuration pour rester dans le cadre de l'évaluation.

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. Ce changement est proposé via l'Assistant de première installation, dans l'écran *Administration de l'équipement*. Dans l'interface d'administration web, ce mot de passe peut être modifié 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. Par 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 (comme beaucoup d'autres systèmes) basé sur un système de login/mot de passe n'implique pas forcément de déloguage à 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 malgré avoir 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).

Dans la documentation, Stormshield Network Security est désigné sous la forme abrégée : SNS et Stormshield Network sous la forme abrégée : SN.

ACTIVE UPDATE

Le module d'**Active Update** se compose d'un seul écran de configuration. Cet écran se divise en 2 parties :

- **Mises à jour automatiques** : permet l'activation d'un module de mise à jour.
- **Configuration avancée - Serveurs de mise à jour**: permet de définir les serveurs de mise à jour.

Mises à jour automatiques

État	Activation ou non par un double clic de la mise à jour via l'Active Update pour le type de mise à jour sélectionné.
Module	Type de mise à jour (la liste des modules varie selon la licence acquise).

Configuration avancée

Serveurs de mise à jour de la Base d'URL

Si la **Base d'URL Stormshield Network** est choisie comme Fournisseur de Base d'URL (menu **Objet** > **Objets Web**, onglet **Base d'URL**), d'autres serveurs que ceux de Stormshield Network peuvent être renseignés. Cela permet ainsi de mettre à jour la Base URL Stormshield Network par des sites miroirs internes ou d'importer votre propre base URL.

URL	Les fichiers de mise à jour sont récupérés sur un des serveurs définis par l'utilisateur. 4 URL sont définies par défaut. Pour ajouter une URL, cliquez sur **Ajouter** ; l'url suivante est ajoutée par défaut : http://update.1.stormshield.eu/1. Remplacez par votre adresse URL puis cliquez sur **Appliquer**. Pour supprimer une URL de la liste, sélectionnez-là puis cliquez sur **Supprimer**.
Fréquence de mise à jour	Indication de la fréquence des mises à jour des listes d'URL dynamiques, des signatures contextuelles ASQ et de la configuration de l'antispam. La fréquence est indiquée à 3 heures, la modification de cette fréquence peut se faire via le mode Console.

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 connaissance 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* : cet onglet 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* : cet onglet permet aux administrateurs gérant les droits d'accès aux données personnelles de créer des tickets temporaires d'accès complet aux logs.

Onglet « Administrateurs »

L'écran de cet onglet est divisé en trois parties :

- Une barre des tâches (en haut) : celle-ci affiche les différentes actions possibles sur un administrateur (**Ajouter un administrateur**, **Supprimer**, **Copier les droits** etc.).
- La liste des utilisateurs et groupes d'utilisateurs répertoriés en tant qu'admin (à gauche).
- La grille des droits des administrateurs (à droite).

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.

Une fois sa tâche terminée, il peut alors relâcher ce droit de visualisation des données personnelles.

Les interactions

Certaines opérations, détaillées dans la section "Les manipulations possibles", peuvent être réalisées en effectuant un clic droit sur la grille des administrateurs :

- Ajouter un administrateur,
- Supprimer (un administrateur),
- Copier les droits,
- Coller les droits,
- Donner tous les droits.

Les manipulations possibles

Vous allez pouvoir constituer votre grille d'administrateurs issus de votre base LDAP ainsi que leurs droits respectifs.

Ajouter un administrateur

Administrateur sans droit	Ce type d'administrateur dispose des droits de base à savoir l"accès au **Dashboard** et aux modules suivants : **Licence, Maintenance, Active Update,** la **Haute disponibilité** et son assistant, la console **CLI, Réseau, Routage, DNS dynamique, DHCP, Proxy cache DNS**, les **Objets**, les **catégories d'URL** et leurs groupes, **Certificats et PKI, l'Authentification** et son assistant, le **Filtrage URL, SSL** et **SMTP, Applications et protections, Profils d'inspection, Antivirus, Antispam, Messages de blocage,** et les 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 les onglets Administrateurs et Compte Admin du module **Administrateurs**. **REMARQUE** 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 **Accès restreint aux logs** afin d'activer le droit **Accès complet aux logs (données personnelles)** sans devoir saisir un code d'accès aux données privées.
Administrateur sans accès aux données personnelles	Ce type d'administrateur peut accéder à l'ensemble des logs ne contenant pas de données personnelles. Pour activer le droit **Accès complet aux logs (données personnelles)**, il doit obligatoirement cliquer sur le lien **Accès restreint aux logs** puis saisir un code d'accès aux données privées qui lui aura été fourni.

Une fois votre administrateur importé, il apparaît dans la liste « **Utilisateur – groupe d'utilisateur** » à gauche de l'écran.

Vous pouvez effectuer diverses actions sur celui-ci.

Supprimer	Sélectionnez l'administrateur à retirer de la liste et cliquez sur **Supprimer**.
Monter	Placer l'administrateur au-dessus du précédent dans la liste.
Descendre	Placer l'administrateur au-dessous du suivant dans la liste.
Copier les droits	Sélectionnez l'administrateur dont vous souhaitez copier les droits et cliquez sur ce bouton.
Coller les droits	Sélectionnez l'administrateur auquel vous souhaitez attribuer les mêmes droits que celui que vous venez de copiez et cliquez sur ce bouton.
Donner tous les droits	Quelques soient les droits attribués à l'administrateur sélectionné, en cliquant sur ce bouton,

La grille des droits

Votre interface est en « **vue simple** » par défaut. La grille affiche 5 colonnes représentant les 5 catégories de droits auquel un administrateur est affilié ou non : **Système, Réseau, Utilisateurs, Firewall** et **Supervision**.

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.

En passant en « **vue avancée** » à l'aide de l'icône ou (en fonction de la longueur de votre écran), la grille affichera le détail des droits par catégorie. Pour connaître précisément les droits correspondant à chaque colonne, une bulle informative est disponible sur l'en-tête de chacune d'entre elles.

Exemple

Si vous vous positionnez en haut de la colonne **Système,** vous verrez apparaître les accès qu'elles incluent, à savoir les droits de « Maintenance, Objets ».

NOTE

Un double clic sur les icônes représentées change l'état des permissions (de « accordé » à « non accordé » par exemple). Un double clic sur cette icône accordera les droits, et celle-ci la remplacera à l'affichage.

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`).

La liste des droits attribuables par la vue simple est la suivante :

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 dans Stormshield Network Real-Time Monitor). Droits de modification de la base objet	modify, base, maintenance, object
Réseau	Droit de modification de la politique de filtrage et du routage (route par défaut, routes statiques and réseaux de confiance)	modify, base, filter, route
Utilisateurs	Droit de modification des utilisateurs et de la PKI	modify, base, user, pki

Firewall	Droit de modification de la configuration VPN, de la prévention d'intrusion (IPS) et du management de vulnérabilités	modify, base, vpn, asq, pvm
Supervision	Droit de modification de la configuration à partir de Stormshield Network Real-Time Monitor et modification des traces	modify, base, log, maintenance
Comptes temporaires	Droit de gestion des comptes temporaires pour la politique d'authentification "Comptes temporaires"	modify,base,voucher

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, log_read, report_read, 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, log_read, modify, privacy, privacy_read, report_read
PKI	Droit de modification de la PKI	modify, base, pki
Monitoring	Droit de modification de la configuration à partir de Stormshield Network Real-Time Monitor	modify, base, mon_write
Filtrage de contenu	Droits pour les politiques de filtrage URL, Mail, SSL et la gestion des antivirus	modify, base, contentfilter
Objets	Droit de modification de la base objet	modify, base, object
Utilisateurs	Droit de modification des utilisateurs	modify, base, user
Réseau	Droit de modification de la configuration réseau (interfaces, bridges, modems, VLANs et configuration du DNS dynamique)	modify, base, network
Routage	Droits de modification du routage (route par défaut, routes statiques and réseaux de confiance)	modify, base, 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 dans Stormshield Network Real-Time Monitor).	modify, base, maintenance
Comptes temporaires	Droit de gestion des comptes temporaires (module **Utilisateurs** > **Comptes temporaires**)	modify, base, voucher
Prévention d'intrusion	Droits de modifier la configuration de la prévention d'intrusion (IPS)	modify, base, asq

Management de vulnérabilités	Droit de modifier la configuration de management de vulnérabilités (Stormshield Network Vulnerability Manager)	modify, base, pvm
Objets (global)	Droits d'accès aux objets globaux	modify, base, globalobject
Filtrage (global)	Droits d'accès à la politique de filtrage globale	modify, base, globalfilter
Rapports (E)	Droits de modifier Stormshield Network Activity Report	base, report_read
Rapports (L)	Droits d'accès à Stormshield Network Activity Report	modify, base, report, 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 (certificats, clés...).	modify, base, tpm

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 va permettre de définir les données d'authentification du compte administrateurs.

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

NOTE

Le mot de passe par défaut de l'utilisateur 'admin' (super administrateur) doit être modifié lors de la première utilisation du produit.

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.

Authentification

Mot de passe	Définition du mot de passe du compte admin. **REMARQUE** Il ne doit pas contenir le caractère ".
Confirmer le mot de passe	Confirmation du mot de passe du compte admin, 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.

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 **Accès restreint aux logs** (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

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 cryptage, 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.

L'option **Activer l'agent** permet l'activation du module. 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 cryptage, 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.
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	**Ne pas envoyer** : en cochant cette option, vous ne recevrez pas les alarmes ASQ. En cochant **Envoyer uniquement les alarmes majeures**, vous pourrez recevoir les alarmes ASQ majeures. En cochant **Envoyer les alarmes majeures et mineures**, les alarmes majeures et mineures ASQ seront émises.
Evénements systèmes	En cochant **Ne pas envoyer**, vous ne recevrez pas les alarmes système. En cochant **Envoyer uniquement les alarmes majeures**, vous pourrez recevoir les alarmes système majeures. En cochant **Envoyer les alarmes majeures et mineures**, les alarmes systèmes majeures et mineures seront émises.

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	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.

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	Les deux types de chiffrement possibles sont DES et AES. Par défaut le chiffrement se fait en DES.

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. **NOTE** 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. **NOTE** 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 clef spécifique.**
Algorithme	Les deux types de chiffrement possibles sont DES et AES-128. Par défaut le chiffrement se fait en AES-128.

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, snmp trap.
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.

MIBS 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 d'administration web de votre Firewall.

Dans ce module, vous pouvez configurer les stations vers lesquelles le firewall doit envoyer les alertes et d'événements SNMP (traps) et d'autre part 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 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 rassembler les données de la Base d'information Stormshield Network (ces MIB sont disponibles sur le site Stormshield Network, à l'adresse indiquée dans la section MIBs Stormshield Network). Les informations MIBs sont des fichiers au format texte qui décrivent une liste d'objets SNMP utilisés par le superviseur. Ces MIBs mettent donc à disposition les informations dont le superviseur a besoin pour interpréter les traps SNMP, les évènements et les messages de requêtes envoyées au Firewall.

Les valeurs de traps des MIBs Stormshield Network sont décrites dans la section suivante.

Format d'alerte et d'évènement SNMP Stormshield Network (TRAPs)

Traps de la MIB SNMPv2-MIB

http://www.net-snmp.org/docs/mibs/snmpMIB.html#notifications

coldStart NOTIFICATION-TYPE

STATUScurrent

DESCRIPTION "A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered."

::= { snmpTraps 1 }

warmStart NOTIFICATION-TYPE

STATUS current

DESCRIPTION"A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered."

::= { snmpTraps 2 }

authenticationFailure NOTIFICATION-TYPE

STATUS current

DESCRIPTION"An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated."

::= { snmpTraps 5 }

Traps gérées par DISMAN-EVENT-MIB

Pour avoir la liste des Traps qui sont émises, il est nécessaire d'utiliser la MIB **DISMAN-EVENT-MIB**

http://www.net-snmp.org/docs/mibs/dismanEventMIB.html

Les tables **mteTriggerTable** et **mteEventNotificationTable** sont les plus utiles.

Exemple d'utilisation d'un outil de consultation MIB SNMP :

snmpwalk -v 2c -c public -M +/usr/local/share/snmp/mibs/ -m ALL 192.168.4.250 mteEventNotificationTable

....

DISMAN-EVENT-MIB::mteEventNotification."_snmpd"."_linkDown' = OID: IF-MIB::linkDown

DISMAN-EVENT-MIB::mteEventNotification."_snmpd"."_linkUp' = OID: IF-MIB::linkUp

....

Pour connaître les conditions de déclenchement, utilisez **mteTriggerTable**

(basé sur IF-MIB::ifOperStatus)

...

Les Traps particulièrement utiles sont les suivantes :

IF-MIB::linkDown

IF-MIB::linkUp

Vous trouverez les descriptions de **IF-MIB::linkDown et IF-MIB::linkUp** à l'adresse : http://www.net-snmp.org/docs/mibs/IF-MIB.txt

linkDown NOTIFICATION-TYPE

OBJECTS{ ifIndex, ifAdminStatus, ifOperStatus }

STATUScurrent

DESCRIPTION "A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 3 }

linkUp NOTIFICATION-TYPE

OBJECTS{ ifIndex, ifAdminStatus, ifOperStatus }

STATUScurrent

DESCRIPTION"A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus."

::= { snmpTraps 4 }

Traps Stormshield Network

.1.3.6.1.4.1.11256.1.5

Les Traps Stormshield Network sont définies dans la **MIB STORMSHIELD-ALARM-MIB.txt**

time	.0.1.1
srcif	.0.1.2
src	.0.1.5
dst	.0.1.6
msg	.0.1.11

time	.1.1.1
srcif	.1.1.2
src	.1.1.4
dst	.1.1.5
msg	.1.1.10

NOTE

La notification "snsAMessage" contient le message de l'alarme ou de l'événement système. La documentation des alarmes est disponible en ligne sur la security KB ; elle est accessible via l'interface d'administration, dans le module Événements systèmes en cliquant sur le lien *Afficher l'aide* de chaque événement.

La description des alarmes systèmes est également disponible dans la section **ÉVÉNEMENTS SYSTÈMES** > **Liste des événements**.

Base d'information consultables (MIBs)

MIBs Stormshield Network

Voici la liste des champs des MIBs Stormshield Network, les commandes CLI correspondantes, ainsi que les commandes console.

Les liens sont téléchargeables à l'adresse : https://www.stormshield.com/products-services/services/mibs/

STORMSHIELD-SMI-MIB: Mib chapeau de l'ensemble

STORMSHIELD-ALARM-MIB: Table des alarmes

.1.3.6.1.4.1.11256.1.5

==> Contenu des logs

Contient 2 tables :

Alarmes

time	.0.X.1
srcif	.0.X.2
dstif	.0.X.3
proto	.0.X.4
src	.0.X.5
dst	.0.X.6
srcport	.0.X.7
dstport	.0.X.8
srcname	.0.X.9
dstname	.0.X.10
msg	.0.X.11

Alarmes ICMP

time	.1.X.1
srcif	.1.X.2
dstif	.1.X.3
src	.1.X.4
dst	.1.X.5
type	.1.X.6
code	.1.X.7
srcname	.1.X.8
dstname	.1.X.9
msg	.1.X.10

STORMSHIELD-HA-MIB: Informations de la haute disponibilité

.1.3.6.1.4.1.11256.1.11

==> (CLI) HA INFO

==> (console) hainfo

Informations générales

NbNode	.1.0
NbDeadNode	.2.0
NbActiveNode	.3.0
NbHALinks	.5.0
NbFaultyHALinks	.6.0
HASyncStatus	.8.0
HAFwAdminRevision	.9.0

Table des membres HA

FwSerial	.7.X.2
Online	.7.X.3
Model	.7.X.4
Version	.7.X.5
HALicence	.7.X.6
HAQuality	.7.X.7
HAPriority	.7.X.8
HAStatusForced	.7.X.9
HAActive	.7.X.10
Uptime	.7.X.11

Table de suivi des modules d'alimentation

NodePowerSupplyPowered	.10.X.2
NodePowerSupplyStatus	.10.X.3

Table de suivi des disques

NodeDiskName	.11.X.2
NodeDiskSmartResult	.11.X.3
NodeDiskIsRaid	.11.X.4
NodeDiskRaidStatus	.11.X.5
NodeDiskPosition	.11.X.6

Table de suivi des processeurs

NodeCpuTemp	.12.X.2

Table de suivi des ventilateurs

NodeFanName	.13.X.2
NodeFanStatus	.13.X.3
NodeFanRpm	.13.X.4

STORMSHIELD-POLICY-MIB: Politique de filtrage

.1.3.6.1.4.1.11256.1.8.1

==> (CLI) MONITOR POLICY

==> (console) slotinfo

Name	.X.2
Slot_Name	.X.3
Active	.X.4
Sync	.X.5

STORMSHIELD-AUTHUSERS-MIB: Table des utilisateurs authentifiés

.1.3.6.1.4.1.11256.1.2.1

==> (CLI) MONITOR USER

==> (console) sfctl -s user

AuthIpAddr	.X.1
AuthTimeout	.X.2
AuthUserName	.X.3
AuthUsersDomain	.X.4

STORMSHIELD-HOSTS-MIB: Tables de machines protégées

.1.3.6.1.4.1.11256.1.3.1

==> (CLI) MONITOR HOST

==> (console) sfctl -s host

HostIpAddr	.X.1
HostName	.X.2
Interface	.X.3
Packet	.X.4
Bytes	.X.5
CurrThroughput	.X.7
MaxThroughput	.X.8
InBytes	.X.9
OutBytes	.X.10
InCurrThroughput	.X.11
OutCurrThroughput	.X.12
InMaxCurrThroughput	.X.13
OutMaxCurrThroughput	.X.14

STORMSHIELD-PROPERTY-MIB: Informations retournées par la commande "SYSTEM PROPERTY"

.1.3.6.1.4.1.11256.1.0

==> (CLI) SYSTEM PROPERTY, SYSTEM IDENT, SYSTEM LANGUAGE

Model	.1.0
Version	.2.0
SerialNumber	.3.0
SystemName	.4.0
SystemLanguage	.5.0
NbEther	.6.0
NbVlan	.7.0
NbDialup	.8.0
NbPPTP	.9.0
NbSerial	.10.0
NbLoopback	.11.0
Watchdog	.12.0
Led	.13.0
Clone	.14.0
HADialup	.15.0

STORMSHIELD-SYSTEM-MONITOR-MIB: Compteurs d'utilisation des ressources ASQ

.1.3.6.1.4.1.11256.1.10

==> (CLI) MONITOR STAT

Informations générales

Date	.1.0
UpTime	.2.0
Mem	.3.0
StatTime	.4.0

Table de suivi des disques

DiskEntryDiskName	.5.X.2
DiskEntrySmartResult	.5.X.3
DiskEntryIsRaid	.5.X.4
DiskEntryRaidStatus	.5.X.5
DiskEntryPosition	.5.X.6

Suivi des modules d'alimentation

PowerSupplyPowered	.6.X.2
PowerSupplyStatus	.6.X.3

Suivi des processeurs

CpuTemp	.7.X.2

Table de suivi du Bypass matériel

BypassI2CAddress	.8.X.2
BypassSystemOff	.8.X.3
BypassJustOn	.8.X.4
BypassRunTime	.8.X.5
BypassWatchdog	.8.X.6

STORMSHIELD-AUTOUPDATE-MIB: État des différents modules mis à jour par Active Update

.1.3.6.1.4.1.11256.1.9.1

==> (CLI) MONITOR AUTOUPDATE

AutoupdateSubsys	.X.2
AutoupdateState	.X.3
AutoupdateLast	.X.4

STORMSHIELD-IF-MIB: État des interfaces vue par l'ASQ

.1.3.6.1.4.1.11256.1.4.1

==> (CLI) MONITOR INTERFACE

ifUserName	.X.2
ifName	.X.3

ifAddr	.X.4
ifMask	.X.5
ifType	.X.6
ifColor	.X.7
ifMacThroughput	.X.8
ifCurThroughput	.X.9
ifMaxThroughput	.X.10
ifPktAccepted	.X.11
ifPktBlocked	.X.12
ifPktFragmented	.X.13
ifPktTcp	.X.14
ifPktUdp	.X.15
ifPktIcmp	.X.16
ifTotalBytes	.X.17
ifTcpBytes	.X.18
ifUdpBytes	.X.19
ifIcmpBytes	.X.20
ifTcpConn	.X.21
ifUdpConn	.X.22
ifTcpConnCount	.X.23
ifUdpConnCount	.X.24
ifInCurThroughput	.X.25
ifOutCurThroughput	.X.26
ifInMaxThroughput	.X.27
ifOutMaxThroughput	.X.28
ifInTotalBytes	.X.29
ifOutTotalBytes	.X.30
ifInTcpBytes	.X.31
ifOutTcpBytes	.X.32
ifInUdpBytes	.X.33
ifOutUdpBytes	.X.34
ifInIcmpBytes	.X.35
ifOutIcmpBytes	.X.36
ifProtected	.X.37
ifDrvName	.X.38

STORMSHIELD-SERVICES-MIB: État des services du firmware

.1.3.6.1.4.1.11256.1.7.1

==> (CLI) MONITOR SERVICE

==> (console) dstat

ServicesName	.X.2
ServicesState	.X.3
ServicesUpTime	.X.4

STORMSHIELD-VPNSA-MIB: Table des SA IPSEC négociées

.1.3.6.1.4.1.11256.1.1.1

==> (CLI) MONITOR GETSA

==> (console) showSAD

VPNSAIndex	.X.1
VPNIPSrc	.X.2
VPNIPDst	.X.3
VPNType	.X.4
VPNMode	.X.5
VPNSpi	.X.6
VPNPeerSpi	.X.7
VPNReqID	.X.8
VPNEnc	.X.9
VPNAuth	.X.10
VPNState	.X.11
VPNLifeTime	.X.12
VPNBytes	.X.13
VPNMaxLifeTime	.X.14
VPNMaxBytes	.X.15

STORMSHIELD-ASQ-STATS-MIB: Table des statistiques ASQ

.1.3.6.1.4.1.11256.1.12

==> pas de commande CLI

==> (console) sfctl –s stat

Statistiques SPD

ASQStatsStatefulPktBlocked	.1.1
ASQStatsStatefulPktBlockedAsync	.1.2
ASQStatsStatefulPktBlockedSynProxy	.1.3
ASQStatsStatefulPktAccepted	.1.4
ASQStatsStatefulLogged	.1.5
ASQStatsStatefulLogOverflow	.1.6
ASQStatsStatefulFilterOverflow	.1.7
ASQStatsStatefulAlarmOverflow	.1.8
ASQStatsStatefulSeismoFacts	.1.9
ASQStatsStatefulSeismoOverflow	.1.10
ASQStatsStatefulMinorAlarm	.1.11
ASQStatsStatefulMajorAlarm	.1.12
ASQStatsStatefulPktFragmented	.1.13
ASQStatsStatefulInBytes	.1.14
ASQStatsStatefulOutBytes	.1.15
ASQStatsStatefulNatFailures	.1.16
ASQStatsStatefulFlowConflicts	.1.17
ASQStatsStatefulFlowFailures	.1.18
ASQStatsStatefulInterfaceMute	.1.19
ASQStatsStatefulTcpPkt	.1.20
ASQStatsStatefulTcpInBytes	.1.21
ASQStatsStatefulTcpOutBytes	.1.22
ASQStatsStatefulTcpConn	.1.23
ASQStatsStatefulTcpNatConnSrc	.1.24
ASQStatsStatefulTcpNatConnDst	.1.25

ASQStatsStatefulTcpNoNatConnSrc	.1.26
ASQStatsStatefulTcpNoNatConnDst	.1.27
ASQStatsStatefulTcpSmallWindowRst	.1.28
ASQStatsStatefulTcpEmptyDupAckBlk	.1.29
ASQStatsStatefulUdpPkt	.1.30
ASQStatsStatefulUdpInBytes	.1.31
ASQStatsStatefulUdpOutBytes	.1.32
ASQStatsStatefulUdpConn	.1.33
ASQStatsStatefulUdpNatConnSrc	.1.34
ASQStatsStatefulUdpNatConnDst	.1.35
ASQStatsStatefulUdpNoNatConnSrc	.1.36
ASQStatsStatefulUdpNoNatConnDst	.1.37
ASQStatsStatefulIcmpPkt	.1.38
ASQStatsStatefulIcmpInBytes	.1.39
ASQStatsStatefulIcmpOutBytes	.1.40
ASQStatsStatefulHttpTimeoutRst	.1.41
ASQStatsStatefulNatUnusable	.1.42
ASQStatsStatefulSctpAssoc	.1.43
ASQStatsStatefulSctpPackets	.1.44
ASQStatsStatefulSctpInBytes	.1.45
ASQStatsStatefulSctpOutBytes	.1.46
ASQStatsStatefulEtherstateConn	.1.47
ASQStatsStatefulEtherstatePackets	.1.48
ASQStatsStatefulEtherstateInBytes	.1.49
ASQStatsStatefulEtherstateOutBytes	.1.50

Statistiques SAD

ASQStatsGlobalTimeSinceReset	.2.1

STORMSHIELD-IPSEC-STATS-MIB: Table des statistiques IPSEC

.1.3.6.1.4.1.11256.1.13

==> pas de commande CLI

==> (console) ipsecinfo

Statistiques SPD

IPSECStatsSPDIn	.1.1
IPSECStatsSPDOut	.1.2

Statistiques SAD

IPSECStatsSADLarval	.2.1
PSECStatsSADMature	.2.2
IPSECStatsSADDying	.2.3
IPSECStatsSADDead	.2.4

STORMSHIELD-ROUTE-MIB: Table des routeurs

.1.3.6.1.4.1.11256.1.14.1

==> (CLI) MONITOR ROUTE

==> (console) sfctl -s route

RouteType	.X.2
RouteIPVersion	.X.3
RouteRouterName	.X.4
RouteGatewayName	.X.5
RouteGatewayAddr	.X.6
RouteGatewayType	.X.7
RouteLastCheck	.X.8
RouteState	.X.9
RouteStateLastChange	.X.10
RouteActive	.X.11
RouteActiveLastChange	.X.12
RouteSysDefaultGateway	.X.13
RouteSysDefaultGatewayLastChange	.X.14
RouteRtid	.X.15
RouteUsagePrct	.X.16

STORMSHIELD-HEALTH-MONITOR-MIB: Table de l'état de santé du firewall

.1.3.6.1.4.1.11256.1.16

==> (CLI) MONITOR HEALTH

GlobalHealth	.1
FirewallIndex	.2.1.1
SerialHealth	.2.1.2
HaModeHealth	.2.1.3
HaLinkHealth	.2.1.4
PowerSupplyHealth	.2.1.5
FanHealth	.2.1.6
CpuHealth	.2.1.7
MemHealth	.2.1.8
DiskHealth	.2.1.9
RaidHealth	.2.1.10

Autres Standards MIBs

Vous trouverez les liens pour accéder au différentes MIBs.

Seuls les champs ou sous-ensembles listés sont supportés par l'agent SNMP.

SNMPv2-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMPv2-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpMIB.html

rfc=http://www.ietf.org/rfc/rfc3418.txt

system.*.0

sysORTable

snmp.*.0

setSerialNo.0

SNMP-FRAMEWORK-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-FRAMEWORK-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpFrameworkMIB.html

rfc=http://www.ietf.org/rfc/rfc3411.txt

snmpEngine.*.0

SNMP-TARGET-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-TARGET-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpTargetMIB.html

rfc=http://www.ietf.org/rfc/rfc3413.txt

snmpTargetSpinLock.0

snmpTargetAddrTable

snmpTargetParamsTable

snmpUnavailableContexts.0

snmpUnknownContexts.0

SNMP-NOTIFICATION-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-NOTIFICATION-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpNotificationMIB.html

rfc=http://www.ietf.org/rfc/rfc3413.txt

snmpNotifyTable

snmpNotifyFilterProfileTable

snmpNotifyFilterTable

nlmConfig.*.0

nlmStats.*.0

NOTIFICATION-LOG-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NOTIFICATION-LOG-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/notificationLogMIB.html

rfc=http://www.ietf.org/rfc/rfc3014.txt

SNMP-USER-BASED-SM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-USER-BASED-SM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpUsmMIB.html

rfc=http://www.ietf.org/rfc/rfc3414.txt

usmStats.*.0

usmUserTable

SNMP-VIEW-BASED-ACM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-VIEW-BASED-ACM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/snmpVacmMIB.html
rfc=http://www.ietf.org/rfc/rfc3415.txt

vacmContextTable
vacmSecurityToGroupTable
vacmAccessContextTable
vacmViewSpinLock.0
vacmViewTreeFamilyTable

SNMP-USM-DH-OBJECTS-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SNMP-USM-DH-OBJECTS-MIB.txt
desc=http://www.net-snmp.org/docs/mibs/snmpUsmDHObjectsMIB.html
rfc=http://www.ietf.org/rfc/rfc2786.txt

usmDHPublicObjects.*.0
usmDHUserKeyTable

IF-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IF-MIB.txt
desc=http://www.net-snmp.org/docs/mibs/ifMIBObjects.html
rfc=http://www.ietf.org/rfc/rfc2863.txt

ifNumber.0
ifTable
ifXTable

RFC1213-MIB

mibfile=http://www.net-snmp.org/docs/mibs/RFC1213-MIB.txt
rfc=http://www.ietf.org/rfc/rfc1213.txt

atTable

IP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IP-MIB.txt
desc=http://www.net-snmp.org/docs/mibs/ip.html
rfc=http://www.ietf.org/rfc/rfc4293.txt

ip.*.0
icmp.*.0

ipAddrTable
ipRouteTable
ipNetToMediaTable

ipNetToPhysicalTable

IPV6-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6MIB.html

rfc=http://www.ietf.org/rfc/rfc2465.txt

ipv6MIBObjects.?.0

ipv6Interfaces

ipv6IfTable

ipv6IfStatsTable

IPV6-TCP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6TcpMIB.html

rfc=http://www.ietf.org/rfc/rfc2452.txt

ipv6TcpConnTable

IPV6-UDP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-UDP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6UdpMIB.html

rfc=http://www.ietf.org/rfc/rfc2465.txt

ipv6UdpTable

IPV6-ICMP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IPV6-ICMP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ipv6IcmpMIB.html

rfc=http://www.ietf.org/rfc/rfc2466.txt

ipv6IfIcmpTable

TCP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/TCP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/tcp.html

rfc=http://www.ietf.org/rfc/rfc4022.txt

tcp.*.0

tcpConnTable

UDP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/UDP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/udp.html

rfc=http://www.ietf.org/rfc/rfc4113.txt

udp.*.0

udpTable

IF-INVERTED-STACK-MIB

mibfile=http://www.net-snmp.org/docs/mibs/IF-INVERTED-STACK-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ifInvertedStackMIB.html

rfc=http://www.ietf.org/rfc/rfc2864.txt

HOST-RESOURCES-MIB

mibfile=http://www.net-snmp.org/docs/mibs/HOST-RESOURCES-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/host.html

rfc=http://www.ietf.org/rfc/rfc2790.txt

hrSystem.*.0

hrMemorySize

hrStorageTable

hrDeviceTable

hrProcessorTable

hrNetworkTable

hrPrinterTable

hrDiskStorageTable

hrPartitionTable

hrFSTable

hrSWRunTable

hrSWRunPerfTable

hrSWInstalled.*.0

hrSWInstalledTable

DISMAN-EVENT-MIB

mibfile=http://www.net-snmp.org/docs/mibs/DISMAN-EVENT-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/dismanEventMIB.html

rfc=http://www.ietf.org/rfc/rfc2981.txt

mteTriggerTable

mteTriggerDeltaTable

mteTriggerExistenceTable

mteTriggerBooleanTable

mteTriggerThresholdTable

mteObjectsTable

mteEventTable

mteEventNotificationTable

DISMAN-SCHEDULE-MIB

mibfile=http://www.net-snmp.org/docs/mibs/DISMAN-SCHEDULE-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/schedMIB.html

rfc=http://www.ietf.org/rfc/rfc3231.txt

schedLocalTime.0

schedTable

AGENTX-MIB

mibfile=http://www.net-snmp.org/docs/mibs/AGENTX-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/agentxMIB.html

rfc=http://www.ietf.org/rfc/rfc2742.txt

NET-SNMP-AGENT-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NET-SNMP-AGENT-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/netSnmpAgentMIB.html

nsModuleTable

nsCacheTable

nsConfigDebug.*.0

nsDebugTokenTable

nsConfigLogging

nsLoggingTable

netSnmpExampleScalars

netSnmpIETFWGTable

netSnmpHostsTable

nstAgentModules

NET-SNMP-VACM-MIB

mibfile=http://www.net-snmp.org/docs/mibs/NET-SNMP-VACM-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/netSnmpVacmMIB.html

nsVacmAccessTable

UCD-DISKIO-MIB

mibfile=http://www.net-snmp.org/docs/mibs/UCD-DISKIO-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/ucdDiskIOMIB.html

UCD-DLMOD-MIB

mibfile=http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html

desc=http://www.net-snmp.org/docs/mibs/ucdDlmodMIB.html

SCTP-MIB

mibfile=http://www.net-snmp.org/docs/mibs/SCTP-MIB.txt

desc=http://www.net-snmp.org/docs/mibs/sctpMIB.html

rfc=http://www.ietf.org/rfc/rfc3873.txt

sctpStats
sctpParameters
sctpAssocTable
sctpAssocLocalAddrTable
sctpAssocRemAddrTable
sctpLookupLocalPortTable
sctpLookupRemPortTable
sctpLookupRemHostNameTable
sctpLookupRemPrimIPAddrTable
sctpLookupRemIPAddrTable

ALERTES E-MAILS

L'écran se décompose en trois parties :

- L'onglet 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.
- L'onglet Destinataires : permet de définir les groupes qui seront utilisés dans les politiques de mailing mais aussi dans d'autres modules de configuration où l'envoi de mails est nécessaire.
- L'onglet Modèles : visualisation et modification des formats de mails, utilisés lors de l'envoi des notifications aux utilisateurs et aux administrateurs.

L'onglet « Configuration »

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

L'écran comporte les éléments suivants :

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.

REMARQUE

La notification des e-mails 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**, une fenêtre vous invite à saisir l'adresse destinataire de l'e-mail de test puis à cliquer sur le bouton 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 du mail s'effectue par tranche horaire et non par alarme déclenchée. La valeur indiquée par défaut est 15.

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.

Le délai d'envoi du rapport des alarmes se modifie dans le champ « Fréquence d'envoi » du menu **Fréquence d'envoi des e-mails (en minutes).**

Exemple

Si vous spécifiez un envoi toutes les 15 minutes dans le champ « Fréquence d'envoi », vous serez averti par e-mail toutes les 15 minutes des alarmes déclenchées durant ce laps de temps sur le firewall.

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 email configurée (module **Applications et Protections** / colonne *Avancé*).
Destinataire du message	Choix du groupe qui recevra les alarmes de prévention d'intrusion majeures.
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 email configurée (module **Applications et Protections** / colonne *Avancé*).
Destinataire du message	Choix du groupe qui recevra les alarmes de prévention d'intrusion majeures et mineures.

Evénements système

Tout comme le champ précédent, un groupe peut également être notifié pour recevoir les événements système.

Le délai d'envoi des évènements système se modifie, de la même façon, dans le champ **Fréquence d'envoi** du menu **Fréquence d'envoi des e-mails (en minutes)**.

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

REMARQUE

L'état des événements système est visible dans un module portant le même nom : Dans le menu, vous pouvez vous rendre dans **Notifications\Evénements système.**

L'onglet « Destinataires »

L'écran se compose de 2 vues:

- Groupes de destinataires
- Sélectionnez un groupe

Un groupe contient un certain nombre d'adresses e-mails.

Il est possible de créer jusqu'à 50 groupes.

Il n'existe aucun groupe préconfiguré. Vous pouvez ajouter de nouveaux groupes, et commentaires, ou encore les supprimer.

Un groupe doit contenir au moins une adresse e-mail. Le nombre d'adresses e-mails dans un groupe est indéfini.

Il sera possible ensuite de choisir un groupe pour l'envoi des rapports de vulnérabilités, détaillés ou simplifiés dans le menu **Protection Applicative => Management de vulnérabilités.**

Créer un groupe

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

1 Cliquez sur le bouton **Nouveau groupe de destinataires.** Une ligne supplémentaire s'affiche dans la liste et vous demande de saisir le nom que vous souhaitez donner à votre groupe.

2 Vous pouvez attribuer un commentaire à ce groupe, en vous positionnant sur « Commentaire » et en remplissant le champ prévu à cet effet.

Pour ajouter un destinataire, positionnez-vous sur le groupe choisi. Son nom s'affiche sur la droite, dans le champ **Destinataire membre du groupe : <nomdugroupe>**. Cliquez ensuite sur le bouton **Ajouter un destinataire au groupe**. Un écran s'affiche permettant d'indiquer soit le mail du

destinataire soit l'utilisateur ou le groupe auquel il appartient si celui-ci se trouve dans la base d'objets. La saisie de l'adresse e-mail est libre mais le format de l'adresse est vérifié.

Supprimer un groupe

1. Sélectionnez la ligne à supprimer.
2. Cliquez sur le bouton Supprimer. Le message suivant « Voulez-vous vraiment supprimer le groupe nommé <nom du groupe> ? » s'affiche. En cliquant sur Oui, le groupe est supprimé de la liste.

> **REMARQUE**
>
> La suppression d'un groupe ne peut être réalisée que si le groupe n'est pas utilisé dans une autre configuration du firewall.

Si l'on veut supprimer un groupe déjà actif dans un module, un pop-up d'avertissement s'affiche et propose de : forcer la suppression, de vérifier l'utilisation du groupe, ou d'annuler l'action.

Vérifier

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

1. Sélectionnez la ligne à vérifier.
2. Cliquez sur le bouton **Vérifier** afin d'effectuer la vérification.

L'onglet « Modèles »

Il permet d'utiliser un courrier type personnalisable, pour l'émission des mails. Six modèles sont disponibles, contenant chacun, un corps qui diffère selon le message que l'on veut envoyer.

Edition du 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 remplaçés ensuite par des valeurs. Par exemple, un mot-clé peut afficher de manière automatique le nom de l'utilisateur.

Pour modifier un contenu, il suffit de cliquer sur le bouton **Modifier**.

L'écran se subdivise en 2 parties :

- En haut : l'aperçu du modèle d'e-mail
- En bas : l'écran de modification

2 boutons vous permettent de modifier le corps du message :

Insérer une variable	Ce bouton vous permet de sélectionner des variables qui seront ensuite remplacées par des valeurs réelles lors de l'envoi du message.
Appliquer le modèle par défaut	Permet de réinitialiser le modèle à sa présentation initiale. Lorsque vous cliquez sur ce bouton, le message suivant s'affiche : "*Voulez-vous vraiment réinitialiser le contenu de ce modèle à sa valeur par défaut ?*"

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.

Demande de certificat

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

Enrôlement d'un utilisateur

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

Liste des variables

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 3 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.

L'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 du serveur SMTP (FQDN)	Cette information facultative permet de définir un domaine dit « de confiance ». Les 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** : les mails ne sont pas bloqués mais sont marqués comme spams. • **Bloquer tous les spams** : le mail est rejeté quel que soit le seuil de confiance. • **Bloquer les spams de niveau 2 ou supérieur** : 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.

REMARQUE

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 boîtier UTM Stormshield Network. 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 boîtier UTM 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 auxquels vous souhaitez que l'Appliance se connecte. Pour ajouter un serveur, cliquez sur le bouton **Ajouter.** Une nouvelle ligne est ajoutée. 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 le bouton **Supprimer**.

NOTE

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

Rappel : seule la liste de ces serveurs est mise à jour par **Active Update**.

Les interactions

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

- Ajouter,
- Supprimer.

Analyse heuristique

L'analyse heuristique est basée sur le moteur antispam Vade Retro. 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.

Publicité

Pour détecter les e-mails publicitaires, activer 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. **AVERTISSEMENT** 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. **AVERTISSEMENT** Les caractères guillemets double ne sont pas autorisés.
Score minimal de définition d'un spam [1-5000]	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 Stormshield Network choisit "200". 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.

L'onglet « Domaines en liste blanche»

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme **légitimes**. Pour ajouter un domaine à autoriser, référez-

vous à la procédure suivante :

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à autoriser. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors dans la liste des domaines en liste blanche. Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur **Supprimer**.

NOTE

L'antispam ne qualifiera JAMAIS comme Spam les messages provenant des domaines cités dans la liste blanche.

Les interactions

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

- Ajouter,
- Supprimer.

L'onglet « Domaines en liste noire »

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

Pour ajouter un domaine à bloquer, référez-vous à la procédure suivante :

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à bloquer. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors 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 respectivement sur **Supprimer**.

REMARQUES GENERALES

L'antispam qualifiera comme Spam tous les messages provenant des domaines cités dans la liste noire.

Les interactions

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

- Ajouter,
- Supprimer.

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.

Pour chacune des listes, il est possible de définir jusqu'à 256 domaines. Il n'est pas possible d'avoir dans une liste deux fois le même domaine. Le domaine peut se trouver, soit en liste blanche, soit en liste noire.

Un nom de domaine peut contenir des caractères alphanumériques, "_", "-" et ".". Les caractères "Wildcard" "*" et "?" sont également autorisés. La longueur du nom de domaine ne peut excéder 128 caractères.

ANTIVIRUS

L'écran de configuration du service Antivirus comporte 3 zones :

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

Moteur antiviral

La liste déroulante permet de migrer entre solutions Antivirus (ClamAV ou Kaspersky). 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 Kaspersky

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.

Activer l'analyse heuristique	L'analyse heuristique est une méthode utilisée pour détecter les nouveaux virus, ainsi que les nouvelles variantes d'un virus déjà connu. Elle est basée sur le comportement supposé d'un programme afin de déterminer si ce dernier est ou non un virus. Cette méthode se différencie de l'analyse statistique qui se base sur la consultation d'un référentiel de virus connus. L'analyse heuristique permet ainsi de détecter des virus non encore référencés chez l'éditeur de moteur antiviral. Cette option n'est pas supportée sur les firewalls modèles SN160(W), SN210(W) et SN310.

Analyse sandboxing

Ce menu n'est disponible (non grisé) que lorsque le moteur antiviral Kaspersky 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.

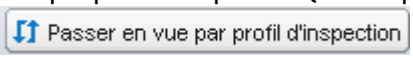
Un **profil d'inspection** (*IPS_00*) est un ensemble de **profils applicatifs** (*default00* – Voir le module **Protocoles**). Un **profil applicatif** contient la configuration des alarmes d'une analyse protocolaire modifiable dans ce module. D'autres éléments de configuration de celle-ci sont accessibles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

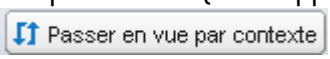
Pour configurer les profils d'inspection selon ces profils applicatifs, rendez-vous dans le module **Profils d'inspection** et cliquez sur le bouton *Accéder aux profils*.

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 Upd**ate).

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 »)
  

Vue par profil d'inspection

Sélection du 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 « Editer » 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 ».

Nouvelles alarmes

Approuver les nouvelles alarmes	En sélectionnant cette option, toutes les nouvelles alarmes matérialisées par l'icône seront acceptées. Cela permet de valider l'action et le niveau de l'alarme fixés par défaut.

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 ASQ : 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.
Email	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	Echange direct de fichiers entre utilisateurs.
Accès à distance	Contrôle d'ordinateur à distance.
Réseaux sociaux	Sites de communautés en ligne.
Web	Autres applications.

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 apparait. 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 paraghraphe 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'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'email. **Mettre la machine en quarantaine** : la machine responsable de l'alarme sera bloquée avec les paramètres suivants. Pour lever la mise en quarantaine, utilisez Stormshield Network Realtime Monitor. • **pour une période de (minutes)** : durée de la mise en quarantaine **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* . **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. 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 « Editer » 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 »**

Vous pouvez supprimer l'état nouveau des alarmes par le bouton **Approuver les nouvelles alarmes** décrit dans la section précédente. Vous pouvez également effectuer une **Recherche** dans les alarmes à l'aide de lettre ou mot saisie dans le champ dédié.

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 4 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 **Ajouter une méthode** ouvre une liste déroulante vous proposant de choisir parmi 8 méthodes d'authentification, que vous pourrez **Supprimer** si besoin. Ces méthodes sont les suivantes :

- LDAP
- Certificat (SSL)
- RADIUS
- Kerberos
- Authentification transparente (SPNEGO)
- Agent SSO
- Invités
- Comptes temporaires
- Parrainage

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 de l'annuaire** 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 multi-annuaires (authentification SSL)	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	Cette liste déroulante permet de sélectionner le champ du certificat dans lequel les chaines de caractères sont recherchées.
Expression régulière	Saisissez l'expression régulière définissant les chaînes à rechercher dans le champ du certificat.
Domaine ou annuaire	Sélectionnez l'annuaire LDAP à parcourir pour authentifier les utilisateurs dont le champ de certificat défini contient une chaine correspondanr 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 Stormshield Network peut se comporter comme un client RADIUS. Il 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, qui présente les éléments suivants :

Accès au serveur

Lorsque la méthode RADIUS est sélectionnée, l'authentification RADIUS est activée. Ce menu vous permet de préciser les informations relatives au serveur RADIUS externe utilisé et d'un éventuel serveur RADIUS de sauvegarde. Pour chacun, la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur RADIUS.
Port	Port utilisé par le serveur RADIUS. Par défaut, le port 1812 / UDP nommé RADIUS est sélectionné.
Clé prépartagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur RADIUS.

Serveur de secours

Serveur	Adresse IP du serveur de secours.
Port	Port utilisé pour le serveur de secours, si le serveur principal n'est plus accessible. Par défaut, le port 1812 / UDP nommé RADIUS est sélectionné.
Clé prépartagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur de secours.

REMARQUE

Le firewall tente de se connecter 2 fois au serveur RADIUS "principal", en cas d'échec il tente de se connecter 2 fois au serveur RADIUS "backup". Si le serveur RADIUS "backup" répond, il bascule en tant que serveur RADIUS "principal". Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur RADIUS "principal" redevient "principal".

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 cryptage 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 (Internet Explorer, 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 depuis votre **Espace privé**, rubrique *Base de Connaissance – en version Anglaise EN* - (article "*Where can I find the last version of the "spnego.bat" script?*").

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/U70XXAZ0000000

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 correspondnat 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 prépartagée.	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 prépartagée	Confirmer la même clé partagée/ mot de passe que dans le champ précédent.
Force de la clé prépartagée	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. **NOTE** Un seul domaine est géré par le firewall, car un unique annuaire peut être configuré.

Configuration Avancée

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.

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.
Accéder à la liste des comptes temporaires	Ce raccourci 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.

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 ; 2 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.
Objets multi-utilisateur	Définissez un ou plusieurs objets réseau autorisés à permettre plusieurs authentifications sur une même adresse IP. Veuillez cliquer sur le bouton « Ajouter un objet » et sélectionner dans le menu déroulant une machine, un réseau, une plage d'adresse IP ou un groupe. **NOTE** La méthode SSO ne permet pas l'authentification « **multi utilisateur** ». Consultez la dernière section **Proxy HTTP transparent ou explicite et objets Multi-utilisateur.**

Les interactions

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 : Authentification d'Utilisateurs

Sélectionnez l'utilisateur ou le groupe concerné ou laissez la valeur par défaut "Tous". Cette étape n'est pas proposée pour les règles associées aux méthodes "**Invités**" ou "**Parrainage**".

Étape 2 : Source d'Authentification

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 3 : Méthodes d'authentification

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

Cliquez sur **Autoriser 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.

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, double cliquez sur l'état « **Désactivé** ».

Méthode 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.

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.

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.

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).

Ces options n'étant pas supportées par le navigateur Internet Explorer en version 6, 7 et 8, il conseillé d'utiliser une version supérieure de ce navigateur. Toutefois, ce mode peut être désactivé par commande CLI (CONFIG AUTH HTTPS sslparanoiac=0 / CONFIG AUTH ACTIVATE).

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 d'authentification (profil du portail captif) préalablement défini 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.

Les interactions

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

- Ajouter,
- Supprimer.

Interface	Sélectionnez l'interface réseau à laquelle un profil de portail captif doit être associé. 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 réseau. Lorsque la case **Activer le portail captif** n'est pas cochée dans le profil sélectionné, le nom du profil est précédé de l'icône
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 un accès au portail en SSL, la CA utilisée par défaut par le module d'authentification du firewall est la CA propre du firewall, le nom associé à cette CA est le numéro de série du produit. Ainsi lorsqu'un utilisateur essaie de contacter 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. En cliquant sur l'icône, l'écran de configuration des CA s'affiche (certificat serveur) et vous pouvez choisir une CA préalablement importée. 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 **Bienvenue** > **Sensibilisation des utilisateurs**, partie *Première connexion au boîtier.*

Conditions d'utilisation de l'accès à Internet

Des *Conditions d'utilisation d'accès à Internet* peuvent être affichées à l'utilisateur. Il devra cocher une case signifiant son accord avant de pouvoir s'authentifier.

Cette option est activable dans les onglets « Méthodes disponibles » (méthode **Invités**) ou « Profils du portail captif » (autres méthodes). Vous pouvez personnaliser ces conditions en renseignant par exemple, le nom de votre entreprise.

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.

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 donne la possibilité de ne pas faire apparaître de bannière (par défaut il s'agit du logo Stormshield) lors de l'authentification de l'utilisateur sur le portail captif, par souci de confidentialité.

Sélectionnez un logo à afficher (800x50 px)	Vous pouvez sélectionner 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.

Le bouton « **Réinitialiser** » vous permet de rétablir les versions d'origine de la *charte graphique* (logo et feuille de style) et des *Conditions d'utilisation d'accès à Internet* par défaut.

Onglet « Profils du portail captif »

Cet écran permet de sélectionner un profil d'authentification prédéfini ou personnalisable, et d'en modifier la configuration.

La barre d'actions

Renommer	Ce bouton permet de renommer le profil sélectionné.
Activer le parrainage	En cochant cette case, vous pouvez activer 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 par défaut.

En survolant l'icône , vous affichez la date et l'heure de la dernière modification apportée au profil de portail captif sélectionné.

Authentification

Méthode ou annuaire par défaut	Ce champ permet de sélectionner la méthode d'authentification ou l'annuaire LDAP (dans le cas d'un firewall ayant défini plusieurs annuaires) affecté par défaut au profil d'authentification en cours de modification. Les méthodes proposées sont celles définies dans l'onglet *Méthodes disponibles*.
Activer le parrainage	En cochant cette case, vous pouvez activer 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 par défaut.

Conditions d'utilisation de l'accès à Internet

Activer l'affichage des conditions d'utilisation d'accès à Internet	Par cette option, des *Conditions d'utilisation d'accès à Internet*, communément appelé *Disclaimer*, peuvent être affichées à l'utilisateur. Une case signifiant son accord est à cocher par l'utilisateur avant de pouvoir s'authentifier. Ces conditions sont personnalisables dans l'onglet « Portail Captif »

NOTE

Cette option d'affichage de Conditions d'utilisation d'accès à Internet n'est pas valide pour la méthode d'authentification transparente Agent SSO, celle-ci ne requérant pas l'activation du portail d'authentification.

Fréquence d'affichage des Conditions	Cette fréquence d'affichage concerne toutes les méthodes d'authentification, sauf la méthode Invité (voir l'onglet *Méthodes disponibles*)

Champs personnalisés du portail captif

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 d'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, positionnable en minutes ou en heures (jusqu'à 24h).
Durée maximale	Durée maximale durant laquelle l'utilisateur peut être authentifié positionnable en minutes ou en heures (jusqu'à 24h).
Pour l'authentification transparente	Pour les méthodes de type SPNEGO et Certificats SSL, il s'agit de définir 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	En cochant cette option, vous activez le module **Authentification** et autorisez l'authentification via un formulaire web depuis les interfaces réseau associées au profil d'authentification.

Activer la page de déconnexion	En cochant cette option, vous activez 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 est affiché. 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	En cochant cette option, vous autorisez 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. En l'activant, ses requêtes multiples seront automatiquement refusées.

Expiration du 'cookie' HTTP

La gestion des cookies pour l'authentification des utilisateurs sur les firewalls permet une sécurisation de l'authentification prévenant par exemple les attaques par rejeu étant donné qu'il est indispensable de posséder le cookie de connexion pour être considéré comme authentifié.

Les cookies sont indispensables pour autoriser plusieurs utilisateurs à être authentifiés depuis une même adresse IP. Ces adresses IP sont à renseigner dans la liste des **objets multi-utilisateur** (onglet *Politique d'authentification*).

NOTE

Cette option concerne toutes les méthodes sauf l'Agent SSO, ne supportant pas l'authentification multi-utilisateur.

Les cookies sont négociés par navigateur Web. Ainsi si une authentification est réalisée avec Internet Explorer, elle ne sera pas effective avec Firefox ou d'autres navigateurs Web.

A la fin de la période d'authentification	Par défaut le cookie HTTP expire **A la fin de la période d'authentification,** ce qui signifie qu'il n'est négocié qu'une seule fois pour toute la durée d'authentification.
A la fin de la session	Le cookie sera négocié à chaque requête vers votre navigateur web.
Ne pas utiliser (déconseillé)	Il est possible de ne pas utiliser de cookie HTTP, mais cette option n'est pas recommandée car elle dégrade la sécurité de l'authentification.

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 sous la forme d'un fichier au format HTML pour pouvoir être chargé sur le firewall.
Réinitialiser la personnaliation 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	En sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur le firewall Stormshield Network.

Les utilisateurs peuvent changer leur mot de passe	En cochant cette case, les utilisateurs peuvent modifier leur mot de passe d'authentification depuis le portail d'authentification, sans contrainte de temps et de validité.
Les utilisateurs doivent changer leur mot de passe	En sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentification à leur première connexion sur le portail d'authentification du firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours sans précision d'heure. Un champ intitulé **Durée de vie (jours)** apparait au-dessous, vous permettant d'indiquer le nombre de jours de validité du mot de passe. **NOTE** Si la durée de validité du mot de passe de l'utilisateur est de 1 jour et que le mot de passe de l'utilisateur est initialisé une première fois le 25 novembre 2010 14:00, ce mot de passe doit être modifié dès le 26 novembre 2010 00:00 et non 24 heures plus tard.

Enrôlement des utilisateurs

Stormshield Network vous 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 (portail d'authentification).

Dans le cas d'une requête de certificat (CSR) par l'utilisateur, celle-ci sera signée par l'autorité de certification (CA) choisie par défaut dans le menu Certificats et PKI.

Ne pas permettre l'enrôlement des utilisateurs	Si cette case est cochée, aucun utilisateur « inconnu » à l'annuaire LDAP ne pourra s'y inscrire ni créer de compte.
Autoriser l'enrôlement web des utilisateurs	La création d'un compte utilisateur doit être effectuée pour que cette option soit fonctionnelle. Si cette case est cochée, tout utilisateur tentant de se connecter et ne figurant pas dans la base des utilisateurs aura la possibilité de demander la création de son compte en remplissant un formulaire web. La demande pourra être validée ou refusée par un administrateur.
Autoriser l'enrôlement web des utilisateurs et créer leur certificat	Si cette option est activée, vous pourrez non seulement demander la création de votre compte si vous ne figurez pas dans la base des utilisateurs, mais aussi demander la création d'un certificat.

Notification d'un nouvel enrôlement

Cette option permet d'avertir les nouveaux enrôlés de la création de leur compte dans la base utilisateurs.

Pas d'email envoyé	Par défaut, la liste déroulante affiche qu'aucun email de sera envoyé à l'administrateur pour le prévenir d'une demande d'enrôlement. Vous pouvez en outre, définir un groupe d'utilisateurs auquel les demandes d'enrôlement seront transmises dans le menu **Notifications\Alertes e-mails** onglet *Destinataires*. Une fois créé, ce groupe sera automatiquement inclus au sein de la liste déroulante et pourra recevoir les requêtes si vous le sélectionnez.

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* ; les informations d'authentification sont enregistrées par le navigateur dans un *Cookie*, lors de la première connexion à chaque nouveau site web interrogé. Ces informations sont retransmises dans les requêtes suivantes pour être interceptées par le Firewall, qui pourra ainsi appliquer sa politique.

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. A l'aide de Stormshield Network Realtime Monitor, inspectez son utilisation dans le module *Utilisateur* et supprimez l'authentification du ou des utilisateurs authentifiés par un clic droit sur ces derniers - action 'Supprimer l'utilisateur de l'ASQ".

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 stocker de manière sécurisée les certificats, les clés, les fichiers de sauvegarde de configuration... et que ce TPM n'a pas été initialisé (que son mot de passe d'administration n'a pas encore été créé), une fenêtre d'initialisation du TPM est affichée à l'ouverture du module **Certificats et PKI**. Pour plus d'informations concernant le module TPM, veuillez consulter la section Trusted Platform Module (TPM).

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, ainsi que les informations concernant la liste de révocation de certificats (CRL - *Certificate Revocation List*) et la configuration de l'autorité ou de la 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 autorités de certifications utilisées dans la configuration. Ces sondes remontent une anomalie dans les cas suivants :

- 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.

Les actions possibles

La barre de recherche

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**.

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 6 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

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 »).

Notez bien que les informations saisies ne seront plus modifiables après la création de l'autorité.

Créer 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 de l'autorité

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

Onglet « Détails »

4 fenêtres présentent les données de l'autorité :

- Sa **Validité** : dates d'émission et d'expiration de l'autorité,
- Son destinataire (**Émis pour**),
- Son **Émetteur** : l'autorité elle-même,
- Ses **Empreintes** : numéro de série de l'autorité, algorithmes de chiffrement et de signature utilisés...

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 (facultatif).

La durée de vie maximum des certificats équivaut à dix ans.

Onglet « Profils de certificats »

Cet onglet présente la **Taille de clé (bits)**, la **Validité (jours)** et **l'Algorithme de chiffrement** 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 l'autorité sélectionnée.

Ajouter une sous-autorité

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.

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 :

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 **Empreintes** : numéro de série de la sous-autorité, algorithmes de chiffrement et de signature utilisés...

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

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 TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour enregistrer cette identité sur 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 :

Onglet « Détails »

6 fenêtres présentent les données de l'identité :

- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**),
- Son **Émetteur** : l'autorité parente,

- Ses **Empreintes** : numéro de série du certificat, algorithmes de chiffrement et de signature utilisés...,
- 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 lidentité 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

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 TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour enregistrer cette identité sur 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 :

Onglet « Détails »

6 fenêtres présentent les données de l'identité :

- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**),
- Son **Émetteur** : l'autorité parente,
- Ses **Empreintes** : numéro de série du certificat, algorithmes de chiffrement et de signature utilisés ...,
- 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.

Notez que ceci n'est cependant possible que si l'autorité utilisée pour générer l'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.
5. Cliquez sur **Publier le certificat**.

Ajouter une identité serveur

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.

Créer 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 TPM et que celui-ci a été initialisé, cochez la case **Protéger cette identité à l'aide du TPM** pour enregistrer cette identité sur 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 :

Onglet « Détails »

6 fenêtres présentent les données de l'identité :

- Sa **Validité** : dates d'émission et d'expiration du certificat,
- Son destinataire (**Émis pour**),
- Son **Émetteur** : l'autorité parente,
- Ses **Empreintes** : numéro de série du certificat, algorithmes de chiffrement et de signature utilisés...,
- 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. 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 est au format PEM (format ASCII - Encodage des données en Base64).

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 **PEM**.
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**. 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 asssocié, 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 – administration se compose de 3 onglets :

- *Configuration générale* : définition des caractéristiques du firewall (nom, langue, clavier) des paramètres de date et d'heure, ainsi que des serveurs NTP.
- *Administration du Firewall* : configuration des accès à l'interface d'administration du firewall (port d'écoute, SSH etc.)
- *Paramètres réseaux* : activation d'Ipv6, configuration du serveur proxy et de la résolution DNS.

L'onglet « Configuration générale »

L'onglet **Configuration générale** permet la modification des paramètres suivants :

Configuration générale

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

Nom du firewall	Ce nom est utilisé dans les mails d'alarmes envoyés à l'administrateur et est affiché sur la fenêtre principale du firewall. 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 ou le CN du certificat comme FQDN » est cochée. La taille maximale du nom du firewall est de 127 caractères.
Langue du Firewall (traces)	Choix de la langue du boitier, limité à **Français** et **Anglais**. Ceci est utilisé pour les traces de types log, syslog et la configuration CLI.
Clavier (console)	Type de clavier supporté par le firewall. 5 langues sont disponibles : **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 régulièrement 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 « Diffusion Restreinte (DR) »	L'option **Activer le mode « Diffusion Restreinte (DR) »** impose au firewall de respecter la doctrine 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 4.0.1 implique les comportements suivants : • IPSec : vérification que le firewall utilise bien la version 2 du protocole IKE. Dans le cas contraire, un avertissement est affiché afin d'inviter l'administrateur à modifier la configuration IPSec. • IPSec : vérification que les algorithmes de chiffrement utilisés appartiennent bien aux groupes DH19 et DH20 (ECP 256 et ECP384). Dans le cas contraire, un avertissement est affiché afin d'inviter l'administrateur à modifier la configuration IPSec. • IPSec : vérification que l'algorithme de chiffrement utilisé est bien AES_GCM_16 (associé par défaut à une authentification SHA256). • Sur les firewalls équipés de processeurs Intel, le mode « Diffusion Restreinte (DR) » force 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. Notez également que l'activation du mode « Diffusion Restreinte (DR) » nécessite un redémarrage du firewall.

Politique de mots de passe

Les paramètres indiqués s'appliqueront à l'ensemble des mots de passe et clés pré-partagées définis dans le firewall (VPN PPTP, VPN IPSec, annuaire LDAP interne, etc.). Ces paramètres sont :

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…)

NOTE

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

Paramètres de date et d'heure

Saisie manuelle	Lorsque vous cochez cette case, 3 champs de saisie sont affichés : • **Date** : Choisissez la date sur le calendrier. • **Heure** : Saisissez l'heure du firewall. • **Fuseau horaire** : Fuseau horaire défini pour le firewall (GMT par défaut). Un changement de fuseau horaire demande un redémarrage du firewall.
Synchroniser avec votre machine	En cliquant sur ce bouton, le firewall se mettra à l'heure de votre machine.
Maintenir le firewall à l'heure (NTP)	Le protocole NTP (Network Time Protocol) permet de synchroniser l'horloge locale de vos machines sur une référence d'heure via votre réseau. En cochant cette option, votre firewall sera automatiquement synchronisé à l'heure locale.
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

Ce tableau n'est accessible que si vous avez coché l'option **Maintenir le firewall à l'heure (NTP)**. Si vous n'avez pas effectué cette manipulation au préalable, la liste des serveurs NTP sera grisée.

Serveurs NTP (machine ou groupe-plages d'adresses) (15 max)	Le serveur NTP représente l'horloge distante sur laquelle on va choisir de synchroniser son firewall. Vous pouvez en **Ajouter** ou en **Supprimer** en cliquant sur les boutons correspondants. Lorsque vous cliquez sur **Ajouter**, une ligne vierge vient s'ajouter à la liste des serveurs NTP. Vous pouvez choisir un objet au sein de la liste déroulante ou en créer un en cliquant sur cette icône . Il sera ainsi possible de créer une machine, une plage d'adresses IP ou un groupe. Cliquez sur **Appliquer** une fois les données du nouvel objet renseignées.
Mot de passe (ASCII)	Bien que cela soit optionnel, vous pouvez renseigner un mot de passe pour votre serveur NTP, avec lequel vous pourrez vous authentifier.

Configuration avancée

Matériel

L'option de surveillance de l'activité matérielle **Watchdog** est disponible sur tous les Firewalls physiques **MODÈLES "S" de la série U**.

Les autres Firewalls de la **série U** peuvent bénéficier de cet outil pouvant améliorer le diagnostic et l'assistance ; par défaut, ce mécanisme est implémenté mais doit s'activer via le système BIOS. Consultez la Base de connaissance du Support technique pour connaître la démarche.

Seuil d'inactivité de la surveillance matérielle (watchdog)	Ce dispositif teste l'activité du système du Firewall. La fréquence de ce test est fixée par ce seuil. En cas d'inactivité, ce « chien de garde » redémarre le Firewall et déclenche un événement système (24). Pour stopper la surveillance, choisissez la valeur **Désactiver**.

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 IP du firewall. • Utiliser le nom du firewall **NOTE** 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 **NOTE** 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 n'est accessible que lorsque la valeur "Préciser un un nom de domaine (FQDN)" a été sélectionnée dans le champ **Redirection vers le portail captif**.

Télémétrie

Autoriser l'envoi à Stormshield de données d'utilisation (anonyme)	Lorsque vous cochez cette case, votre firewall envoie vers le Cloud Stormshield des données d'utilisation à des fins statistiques : consommation CPU, utilisation mémoire, nombre de lignes de log générées, taille des lignes de logs générées. Ces données sont anonymes.

Firewalls industriels uniquement (modèles SNi40)

Afin d'assurer une continuité de service dans les milieux industriels, le firewall SNi40 est équipé d'un bypass matériel qui permet, une fois activé, de faire passer le trafic réseau sans qu'aucune analyse ne soit mise en oeuvre.

NOTE

Ce mécanisme ne peut être activé que sur les deux premières interfaces du firewall.

Deux modes de fonctionnement du firewall sont proposés :

- Le mode **Sécurité** : ce mode privilégie la sécurité et la protection du réseau. Le mécanisme de bypass ne peut pas être activé. C'est le mode de fonctionnement par défaut du firewall.
- Le mode **Sûreté** : ce mode privilégie la continuité de service. Le mécanisme de bypass sera activé en cas de coupure ou de défaillance du boitier.

Lorsque le mode Sûreté est activé, trois types de déclenchements du bypass peuvent être distingués :

- Le bypass de type **SystemOff** : il se déclenche lors d'une défaillance électrique du boitier ou lors d'une coupure de courant.
- Le bypass de type **JustOn** : il se déclenche lors d'un redémarrage du produit et se désactive ensuite.
- Le bypass de type **OnTimer** : lorsque le produit est soumis à une surcharge de connexions, le bypass se déclenche après écoulement du délai précisé dans la configuration du mode Sureté. Une fois le bypass déclenché, le mode Sûreté peut alors être réarmé par l'administrateur du firewall.

IMPORTANT

Une vérification du fonctionnement correct des flux réseau doit être réalisée immédiatement après un réarmement manuel. En effet, les connexions initiées pendant la phase active du bypass ne seront pas reconnues par le firewall et donc systématiquement rejetées.

Lorsque le bypass est déclenché, les deux premières interfaces du firewall sont représentées de la manière suivante :

Activer le mode sûreté	Lorsque vous cochez cette case, vous activez le mécanisme de bypass du firewall. Les trois modes de déclenchement sont automatiquement disponibles.
Seuil d'inactivité du mode sûreté	Sélectionnez le délai au delà duquel le bypass de type OnTimer doit se déclencher. Les valeurs proposées sont : • 1 min • 1 min 30 sec • 2 min • 2 min 30 sec • 3 min • 3 min 30 sec • 4 min
Réarmement du mode sûreté	Lorsque le bypass de type OnTimer s'est déclenché, vous pouvez cliquer sur ce bouton afin de le désactiver pour repasser le firewall en mode sûreté.

L'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. Il est nécessaire de cocher cette case si vous souhaitez conserver ces accès privilégiés. **AVERTISSEMENT** 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 vous pourrez accéder à l'interface d'administration (https, tcp/443 par défaut). **NOTE** Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône . **AVERTISSEMENT** L'objet ne peut être que de type « TCP » (et non « UDP »).
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.
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. En cochant cette case, vous empêcherez cela et dégriserez les deux champs suivants, afin de limiter les tentatives de connexion.
Tentatives d'authentification autorisées	Nombre maximum de tentatives de connexion 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.
Durée de blocage (minutes)	Temps durant lequel vous ne pourrez pas vous connecter au firewall après le nombre d'échecs spécifié ci-dessus. La durée de blocage ne peut excéder 60 minutes.

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

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.
Cochez cette case si vous souhaitez vous connecter à distance en mode console, et ce, de manière totalement sécurisée.

NOTE
En cochant cette option, vous dégriserez les deux champs du dessous.

Autoriser l'utilisation de mot de passe
Le mot de passe en question correspond à celui du compte « admin », étant le seul à pouvoir se connecter en SSH.
L'« admin » devra le présenter pour accéder au firewall via une machine distante.

Vous pouvez aussi utiliser un couple clé privée / clé publique pour vous authentifier.

Port d'écoute
Ce champ représente le port sur lequel vous pourrez accéder à l'interface d'administration (ssh, tcp/22 par défaut).

NOTE
Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône .

AVERTISSEMENT
L'objet ne peut être que de type « TCP » (et non « UDP »).

L'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 la section **Activation d'IPv6** de ce guide.

ATTENTION
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 ActiveUpdate et LicenceUpdate.

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 ce bouton, une ligne vierge vient s'ajouter au tableau et vous permet de sélectionner un serveur DNS au sein de la liste déroulante.
Supprimer	Sélectionnez la ligne à retirer du tableau et cliquez sur **Supprimer**.
Monter	Placer la ligne sélectionnée au-dessus de la ligne précédente.
Descendre	Placer la ligne sélectionnée au-dessous de la ligne suivante.

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 2 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 rafraichissement 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 rafraichissement 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 et des files d'attente de QoS 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 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.

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.

Fenêtre principale

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

Il est divisé en 2 zones distinctes :

- La liste des annuaires et les boutons d'action (colonne de gauche)
- Les onglets présentant la configuration et la structure de l'annuaire sélectionné.

Bouton "Ajouter un annuaire"

Un clic sur ce bouton lance l'assistant de création d'un nouvel annuaire LDAP.

Liste "Action"

En déroulant cette liste, il est possible de **Supprimer** un annuaire, de le **Définir comme défaut**, de **Vérifier la connexion** à un annuaire ou de **Vérifier l'utilisation** d'un annuaire au sein de 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.

Etape 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**.

Etape 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.

NOTE

Seul le mot de passe sera modifiable par la suite, une fois que vous aurez configuré votre LDAP interne.

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

Ecran 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.

Force 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.

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 de DN** 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. **NOTE** 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.

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

Ecran 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)

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 selon une Autorité de certification	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 ci-dessous.
Autorité de certification	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. Vous pouvez cliquer sur l'icône « loupe » ( ) pour effectuer une recherche de la CA correspondante. **NOTE** Cette case sera grisée par défaut si l'option précédente **Vérifier que le nom du serveur correspond au FQDN présenté dans le certificat SSL** n'est pas cochée.

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.
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.

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

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 de type PosixAccount** 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.
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 de DN** 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. **NOTE** L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

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.

Ecran 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)

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 selon une Autorité de certification	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 ci-dessous.
Autorité de certification	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. Vous pouvez cliquer sur l'icône « loupe » ( ) pour effectuer une recherche de la CA correspondante. **NOTE** Cette case sera grisée par défaut si l'option précédente **Vérifier que le nom du serveur correspond au FQDN présenté dans le certificat SSL** n'est pas cochée.

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**.
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.

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 IDAP 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 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'	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*.

Etape 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**.

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.
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 de DN** Le domaine AD est "compagnie.com", le domaine Racine (Base DN) est "dc=compagnie,dc=com".

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=Administrateur,cn=utilisateurs
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. **NOTE** L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

Cliquez sur **Terminer** pour afficher l'écran de l'annuaire Microsoft Active Directory.

Ecran 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** 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)

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 selon une Autorité de certification	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 ci-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. Vous pouvez cliquer sur l'icône « loupe » ( ) pour effectuer une recherche de la CA correspondante. **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.
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.

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

Ces rapports se basent sur les traces enregistrées sur le firewall. Ces traces sont analysées et les valeurs les plus récurrentes sont stockées au sein d'une base de données. Le top 10 et la 11ème valeur correspondant à « Autres » est donc basé donc sur ces valeurs.

L'actualisation des données s'effectue toutes les minutes. L'actualisation comprend un calcul d'un nouveau top 50 des dernières heures et jours afin de mieux représenter les valeurs récurrentes et ne pas surcharger la base.

Les données stockées sur carte SD peuvent être lues par une autre plate-forme équipée du moteur SQLite.

Les rapports se basent sur l'ensemble du trafic traité par le Firewall, c'est-à-dire pour les connexions transitant par toutes les interfaces, qu'elles soient internes ou externes.

AVERTISSEMENT

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 boîtier (*Tableau de Bord* : CPU et mémoire).

Ce module permet également d'activer les graphiques historiques disponibles dans le module **Supervision**.

L'écran se divise en 2 parties :

- En haut : les options permettant d'activer la gestion des rapports et/ou graphiques historiques.
- En bas : un tableau listant au sein de deux onglets, l'ensemble des rapports et graphiques historiques pouvant être sélectionnés.

NOTE

Certains rapports ou graphiques historiques nécessitent d'avoir activé des fonctionnalités comme l'Antivirus, le Management des vulnérabilités ou l'authentification. Reportez-vous au module de supervision concerné pour connaître les fonctionnalités requises et les interactions possibles.

Menu "Général"

Activer les rapports	Cette option permet d'activer les rapports calculés à l'aide des traces stockées sur le disque dur ou sur une carte SD (firewalls Serie "S").
Activer les graphiques historiques	Cette option permet d'activer les graphiques historiques visibles dans le module de **Supervision**.

La grille des rapports et graphiques historiques

Onglet "Liste des rapports"

Le tableau présente les colonnes suivantes :

Etat	Permet d'activer/désactiver le rapport concerné.

Catégorie	Indique à quelle catégorie de données le rapport est rattaché. Le rapport sera consultable dans un menu portant le nom de cette catégorie au sein du module **Rapports**. Les catégories de rapports sont les suivantes : • Réseau • Réseau industriel • Sandboxing • Spam • Sécurité • Virus • Vulnérabilité • Web
Description	Le nom du rapport tel qu'il sera présenté dans le module **Rapports**.
Avertissement	Un message d'avertissement peut s'afficher si, par exemple, une option nécessaire à la construction du rapport n'est pas activée.
Données personnelles	Le symbole est affiché sur la ligne d'un rapport contenant des données personnelles (adresse IP source, nom de machine, nom d'utilisateur...). Ceci indique qu'il est nécessaire d'obtenir le droit **Accès complet aux logs (données personnelles)** pour visualiser le rapport correspondant.

En bas à droite du tableau est indiqué l'espace disque utilisé par la base de données SQLite.

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"

Le tableau présente les colonnes suivantes :

Etat	Permet d'activer/désactiver le rapport concerné.
Description	Précise le type de graphique historique.
Avertissement	Un message d'avertissement peut s'afficher si, par exemple, une option nécessaire à la construction du graphique n'est pas activée.

CONSOLE CLI

Ce module va vous permettre de visualiser les commandes exécutables de la console CLI (Command-Line Interface) de votre boîtier.

Vous pouvez y accéder en vous rendant au sein du menu **Système > Console CLI**.

Celui-ci 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

Pour obtenir l'intégralité des commandes exécutables, consultez le Guide **CLI Serverd Commands reference Guide** disponible depuis sur le site de Documentation Technique Stormshield.

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**.

La liste des commandes

L'écran affiche par défaut, les 16 principales commandes exécutables qui font partie de la catégorie « HELP ».

NOTE

En saisissant la commande « HELP » dans la zone de saisie que nous traiterons ci-après, la liste résumant les commandes principales se réaffichera.

Les commandes visibles sont les suivantes :

AUTH	Utilisée dans le but d'éviter l'usurpation d'identité, cette commande permet à l'utilisateur ou l'administrateur de s'authentifier en toute sécurité.
CHPWD	Permet de redéfinir le mot de passe si nécessaire.
CONFIG	Permet d'accéder aux fonctions de configuration du firewall, regroupant 38 commandes implicites (CONFIG ACTIVATE, CONFIG ANTISPAM etc., cf « La zone de saisie »).
GLOBALADMIN	Permet d'obtenir des informations sur le système et comprend deux commandes implicites : GETINFOS et GETSTATUS.
HA	Permet d'accéder aux fonctions de la Haute Disponibilité, regroupant 8 commandes.
HELP	Cette commande, comme dit précédemment, permet d'afficher la liste des commandes exécutables principales.
LIST	Affiche la liste des utilisateurs connectés, en montrant les droits utilisateurs (par niveau) et les droits pour la session en cours (SessionLevel).
LOG	Permet d'afficher de consulter les journaux d'activités du firewall multifonction Stormshield Network, regroupant 6 commandes.
MODIFY	Cette commande est un droit spécifique permettant à l'utilisateur de modifier la configuration d'un module, en plus de la lecture.
MONITOR	Permet d'accéder aux fonctions relatives au MONITOR, contenant 20 commandes.
NOP	Aucune action ne sera effectuée, tout en évitant la déconnexion du serveur.
PKI	Permet d'afficher ou de télécharger la PKI, regroupant 7 commandes.
QUIT	Permet de se déconnecter.
SYSTEM	Regroupe les 20 commandes relatives au système.
USER	Regroupe les 12 commandes relatives à l'utilisateur.
VERSION	Permet d'afficher la version du serveur.

La zone de saisie

Lorsque vous accédez au module **Console CLI**, le focus est placé sur la zone de saisie des commandes.

A droite de celle-ci, deux boutons et une case à cocher permettent d'impacter certaines actions :

Exécuter	Ce bouton permet de lancer la commande saisie manuellement. La commande est également lancée lorsque l'utilisateur appuie sur « Entrée ». **NOTE** Au sein de la cellule d'édition de la commande, vous pouvez naviguer à travers les différentes commandes déjà exécutées grâce aux touches fléchées du clavier Haut/Bas. L'historique des commandes est stocké et ré-utilisé à chaque fois que l'application web sera relancée.
Effacer l'affichage	Ce bouton permet d'effacer la liste de commandes affichée au-dessus (cf. « La liste des commandes »). Pour la rendre visible de nouveau, entrez la commande HELP dans la zone de saisie et cliquez sur « Exécuter ».
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 n'est disponible que lorsque vous activez le mode multiligne. En cochant cette case, la séquence de commandes sera interrompue à la première erreur rencontrée.

NOTE

La plupart des commandes affichées dans la liste en haut de page en implique d'autres. Pour visualiser l'ensemble de ces commandes, procédez comme suit :

1. Entrez la commande de votre choix dans la zone de saisie de texte.
2. Cliquez sur « Exécutez ».
3. Selon la commande que vous avez choisie, la liste affichera les commandes supplémentaires inclus dans celle-ci.

Exemple

Si vous saisissez la commande CONFIG, toutes les commandes relatives à celle-ci apparaîtront à l'écran.

Pour utiliser l'une de ces commandes, entrez dans la zone de saisie « CONFIG », suivi d'un espace et de la commande voulue, comme : « CONFIG HA ».

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 :

Etat	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.

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

Résolution DNS

Nom de domaine (obligatoire)	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. Par 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. **NOTE** • 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 de votre fournisseur de service DNS Dynamique.

Fournisseur DNS dynamique (obligatoire)	Fournisseur de services DNS. Actuellement, deux fournisseurs de services DNS sont supportés : **DynDNS et 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. L'objet à spécifier dans ce champ doit obligatoirement se nommer : "members.dyndns.org" ou « members.dyndns.com » pour fonctionner avec Dyn DNS.
Service DNS dynamique (obligatoire)	Cette option vous permet d'indiquer le service que vous avez souscrit auprès de votre fournisseur de services DNS parmi "dynamic DNS", "custom", et "static DNS".

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 et HTTP.
Avertir le fournisseur d'accès	Ce service payant chez **Dyn DNS** 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'ACCES

Ce module se compose de 3 onglets :

- *Accès par défaut* : Cet onglet vous 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 »

VPN SSL Portail

Les profils VPN SSL Portail (voir **menu VPN\module 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.

Profil VPN SSL Portail	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 au sein du menu **VPN\VPN SSL** Portail \onglet **Profils utilisateurs** (voir document VPN SSL Portail). 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 VPN SSL Portail. <Nom du profil utilisateur2> : l'utilisateur aura uniquement accès à cet autre profil VPN SSL Portail.

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

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.

Politique IPSEC	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.

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

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.

Politique VPN SSL	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.

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

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 par défaut	Ce champ permet d'Interdire ou d'Autoriser par défaut les utilisateurs à répondre à des requêtes de parrainage établies depuis le portail captif.

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

Onglet « Accès détaillé »

Les manipulations possibles

- Bouton **Ajouter** : Insérer une ligne à configurer après la ligne sélectionnée.
- Bouton **Supprimer** : Supprimer la ligne sélectionnée.
- Bouton **Monter** : Placer la ligne sélectionnée avant la ligne directement au-dessus.
- Bouton **Descendre** : Placer la ligne sélectionnée après la ligne directement en dessous.

Un champ de recherche par mots/lettres clés permet d'accéder aux utilisateurs souhaités.

Les interactions

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

- Ajouter,
- Supprimer.

La grille de configuration

Elle va vous permettre d'accorder ou non des droits d'accès à vos utilisateurs ou groupes d'utilisateurs, au niveau du **VPN SSL** et de l'**IPSEC**.

La grille présente les colonnes suivantes :

Etat	Etat de la configuration des droits d'accès de l'utilisateur ou du groupe d'utilisateurs : Activé : Double-cliquez un point de la colonne pour activer la règle créée. Désactivé : La règle n'est 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, celles-ci sont d'ailleurs numérotées à gauche de la colonne. 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 sa configuration. **Exemple** : Si vous interdisez l'authentification et/ou l'accès au **VPN SSL** à un groupe en règle 1, et que l'utilisateur en règle 2 peut s'authentifier via le LDAP et à un profil VPN SSL particulier et fait partie du groupe, celui-ci sera bloqué, et n'aura accès ni à l'authentification, ni au VPN SSL.
Utilisateur – groupe d'utilisateurs	Lorsqu'une nouvelle ligne est ajoutée à la grille, vous pouvez sélectionner l'utilisateur ou le groupe d'utilisateur pour lequel vous souhaitez effectuer une configuration. Pour cela, cliquez sur la flèche à droite de la colonne, une liste déroulante s'affiche et vous propose de choisir parmi les CN créés précédemment, au sein du menu **Utilisateurs\module Utilisateurs**. **NOTE** Il est également possible d'ajouter un utilisateur qui ne figure pas dans la base LDAP, par exemple, pour la méthode KERBEROS ou RADIUS.
VPN SSL Portail	Cette colonne vous permet d'attribuer un profil VPN SSL en particulier à un utilisateur ou à un groupe d'utilisateur, préalablement configuré au sein du menu **VPN**\module **VPN SSL**\onglet *Profils utilisateurs*. Vous pouvez également sélectionner l'option Défaut, qui prendra en compte le profil VPN SSL par défaut saisi dans l'onglet précédent (Options par défaut). Si vous choisissez Interdire, l'utilisateur ou groupe d'utilisateur n'aura accès à aucun profil VPN SSL, à l'inverse de l'option Tous les profils qui ouvrira l'accès à tous les serveurs web et applicatifs activés au sein des profils utilisateurs.
IPSEC	Ce champ permet d'**Interdire** ou d'**Autoriser** 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. **REMARQUE** 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	Ce champ permet d'Interdire ou d'Autoriser des utilisateurs à négocier des tunnels VPN SSL. 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.
Description	Commentaire éventuel décrivant l'utilisateur, le groupe d'utilisateurs ou la règle.

REMARQUE

Lorsque vous ajoutez une ligne au tableau et que vous n'avez encore mis en place aucune règle, les colonnes **Authentification**, **VPN SSL** et **IPSEC** sont en « Interdire » par défaut, même si vous les avez configurées différemment au sein de l'onglet Options par défaut.

Il faut donc cliquer sur l'option « Défaut » à l'aide de la flèche de droite dans chaque colonne si vous souhaitez récupérer vos modifications effectuées préalablement.

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 Stormshield Network permet à un utilisateur "inconnu" à la base des utilisateurs de demander la création de son compte d'accès (à Internet, au serveur mail, à tous les services qui nécessitent une authentification) et de son certificat.

Ce module requiert au minimum de l'utilisation d'une base LDAP pour les requêtes utilisateurs et d'une autorité racine (PKI interne) pour les demandes de certificats utilisateur.

L'écran du module **Enrôlement** se compose de 3 zones :

- La grille contenant les demandes d'enrôlement des utilisateurs et des certificats à gauche
- Les informations relatives à l'utilisateur ou au certificat sélectionné à droite
- Les propriétés avancées

La grille d'enrôlement

Les actions possibles

Approuver	Lorsqu'un utilisateur fait une demande d'enrôlement ou de certificat, la requête est entrée dans une grille. Pour valider la demande de l'utilisateur, positionnez-vous sur la ligne correspondante et cliquez sur **Approuvez**. **NOTE** Si un utilisateur fait une demande d'enrôlement avec une demande de certificat, la validation de la requête utilisateur implique celle du certificat (cases cochées simultanément).
Rejeter	Vous pouvez également refuser la demande d'enrôlement ou de certificat d'un utilisateur en sélectionnant la ligne correspondante et en cliquant sur le bouton **Rejeter**.
Ignorer	Ce bouton permet d'annuler l'action approuvée ou rejetée. Cela évite d'utiliser le bouton **Annuler** et d'effacer les opérations en cours.
Actualiser	Ce bouton permet de rafraîchir la liste des demandes d'enrôlement ou de certificats. De cette façon, toute requête récente sera automatiquement ajoutée à la grille, en attente de sa validation ou de son refus.

Les demandes d'enrôlement utilisateurs et certificats

Type	Cette colonne indique le type de requête créée par l'utilisateur : une demande d'enrôlement caractérisée par « **Utilisateur** » ou une demande de « **Certificat** ».
CN utilisateur	Le nom permettant d'identifier l'utilisateur ou le certificat.
E-mail	L'adresse e-mail de l'utilisateur qui permettra de lui envoyer une validation ou un refus de sa demande d'enrôlement ou de certificat.

Le formulaire récapitulatif

Il renseigne les informations de la ligne utilisateur/certificat sélectionnée.

Identifiant	Identifiant de connexion de l'utilisateur
Nom	Nom de l'utilisateur
Prénom	Prénom de l'utilisateur

E-mail	Adresse e-mail de l'utilisateur. Celle-ci sera utile pour lui envoyer une réponse concernant sa demande d'enrôlement ou de certificat.
Description	Description indicative à l'utilisateur
Téléphone	Coordonnées téléphoniques de l'utilisateur
Mot de passe	Mot de passe de l'utilisateur
Requête de certificat	Indique si l'utilisateur a effectué une requête de certificat au cours de sa demande d'enrôlement.

NOTE

Pour le cas des demandes de certificats, seul le détail de l'adresse e-mail s'affiche dans le champ de droite.

Propriétés avancées

Format de l'identifiant utilisateur pour les ID vides

Format de l'identifiant	Définissez une chaîne de caractères par défaut pour les identifiants de connexion. **NOTE** Le format s'écrit sous la forme : **%F.%L** Les variables définissant l'identifiant sont les suivantes : **F** est le prénom, **L** est le nom. La variable **f** transforme la casse de la valeur en minuscule et inversement pour **F** qui la transforme en majuscule, de même pour **l** et **L**. La forme **f1** permet de ne choisir que le premier caractère. **exemple :** pour les valeurs *Firstname* et *Lastname*, **%f1.%l** donne **f.lastname**
Exemple	Exemple illustrant l'identifiant utilisateur. **Exemple :** JEAN.DUPONT

NOTE

Il est possible de définir le nombre de caractère souhaité pour le prénom et/ou le nom en plaçant un chiffre après le F et/ou L

%F1%L

JDUPONT

E-mails

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.

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 certificat.

ÉVÉNEMENTS SYSTÈME

Ce module va vous permettre 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 » apparait. 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'email. **Mettre la machine en quarantaine :** le paquet responsable de l'alarme sera bloqué avec les paramètres suivants. Pour lever la mise en quarantaine, utilisez Stormshield Network Realtime Monitor. • **pour une période de (minutes)** : durée de la mise en quarantaine

NOTE GENERALE

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.

Liste des alarmes système

ID	Dénomination	Description
1	System shutdown	Arrêt du système
2	Authentication failed for	Echec d'authentification pour
3	Connection terminated for	Connexion terminée pour
4	20% left in log file	Il reste 20% d'espace libre pour le fichier de log
5	Connection established for	Connexion établie pour
6	IPsec phase 1 failed	Phase 1 IPSec échouée
7	IPsec phase 2 failed	Phase 2 IPSec échouée
8	IPsec pre-shared key not found	Clé IPsec pré-partagée introuvable
9	Firewall startup	Démarrage du Système
10	HA: Mode change	HA: Changement de mode
11	HA: Peer lost	HA: Perte d'un firewall
12	Invalid CRL	CRL invalide
13	Invalid Certificate	Certificat invalide
14	log partition has changed	La partition log a changé
15	System error	Erreur système

16	User denied in IPSEC negotiation	Utilisateur refusé dans la négociation IPSEC
17	Antivirus: update failed	Antivirus: Mise à jour échouée
18	Antivirus: update successful	Antivirus: Mise à jour réussie
19	LDAP unreachable	LDAP inaccessible
20	DNS error	Erreur DNS
21	Certificate Revocation List is expired	La liste des certificats révoqués a expiré
22	Certificate Revocation List expires in less than 3 days	La liste des certificats révoqués expire dans moins de trois jours
23	RAID alert:	Alerte RAID:
24	Watchdog has rebooted firewall	Le Watchdog a redémarré le firewall
25	System date corrupted at boot	La date système était corrompue au démarrage
26	System updated	Système mis à jour
27	System date has been changed	La date système a été changée
28	Many authentication failures	Nombreux échecs d'authentification
29	Backup dialup(s) activated	Dialup(s) de backup activée(s)
30	Client connection on local PPTP server established for	Connexion cliente sur le serveur PPTP local établie pour
31	Client connection on local PPTP server terminated for	Connexion cliente sur le serveur PPTP local terminée pour
32	Authentication failed on local PPTP server for	Echec d'authentification sur le serveur PPTP local pour
33	No PPPoE peer has answered for	Aucun correspondant PPPoE n'a répondu pour
34	Your release is old, check that you are up to date.	Votre version est ancienne, vérifiez que vous êtes à jour
35	This dynamic DNS client configuration has been tagged invalid:	La Configuration de DNS dynamique suivante a été marquée invalide:
36	This dynamic DNS client configuration has bend successfully updated:	Entrée DNS dynamique mise à jour avec succès
37	Interface up:	Interface activée:
38	Interface down:	Interface désactivée:
39	Server switched:	Commutation de serveur:
40	Custom event:	Evénement personnalisé:
41	Active Update: update successful	Active Update: Mise à jour réussie
42	Active Update: update failed	Active Update: Mise à jour échouée
43	Active Update: your license has expired	Active Update: votre licence est expirée
44	Antivirus failed:	Echec de l'antivirus:
45	Too many Authentication failures:	Seuil d'échecs d'authentification dépassé:
46	DHCP interface got a new IP address:	Une interface DHCP a obtenu une nouvelle adresse IP:
47	DHCP interface has released its IP address:	Une interface DHCP a libéré son adresse IP:
48	Restoring configuration from USB token:	Restauration d'une configuration depuis la clef USB:
49	Installation of the secure configuration:	Prise en charge de la configuration sécurisée:
50	USB error:	Erreur USB:
51	Activation error:	Erreur d'activation:

52	The event returned an unhandled error code:	Un évènement a renvoyé un code d'erreur non géré:
53	The following slot activation did not succeed:	L'activation de la plage horaire a renvoyé une erreur:
54	System was not properly halted	Le système n'a pas été arrêté proprement
55	DNS cache is cycled too quickly	Le cache du DNS est rafraîchi trop rapidement
56	Get CRL failed	La récupération de la CRL a échoué
57	Invalid CRL	CRL invalide
58	Invalid QoS queue in the filtering slot	Queue QoS invalide dans le slot de filtrage
59	Configuration has been modified	La configuration a été modifiée
60	Configuration has been validated	La configuration a été validée
61	L2TP:	L2TP:
62	Error while validating configuration	Erreur durant la validation de la configuration
63	Invalid password for configuration	Le mot de passe de protection de la configuration est invalide
64	HA: PVM database sync failure	HA: Erreur de synchronisation de la base PVM
65	Globalgen : hardware configuration file created	Globalgen : le fichier de configuration hardware a été créé
66	Problem reported on hard disk:	Problème signalé sur le disque dur :
67	Network : Unexpected media type change	Réseau : Changement de type de média inattendu
68	Licence Update: A new licence is available	Licence Update: Une nouvelle licence est disponible
69	Licence Update: Temporary licence, need to register	Licence Update: Licence temporaire, enregistrement nécessaire
70	Licence Update: Download error	Licence Update: Erreur de téléchargement
71	Licence Update: New licence installed	Licence Update: Une nouvelle licence a été installée
72	Licence Update: New licence installed : need reboot	Licence Update: Une nouvelle licence nécessitant un redémarrage a été installée
73	Licence: a feature has expired :	Licence: une fonctionnalité a expiré :
74	Licence: remaining days before expiration of	Licence: jours restants avant expiration de l'option
75	This address is banned from webadmin access : bruteforcing detection	Cette adresse est bannie de l'accès webadmin : tentative de bruteforce détectée
76	IPsec failover: peer is dead, switching to other peer	IPsec failover : le correspondant est injoignable, basculement sur l'autre correspondant
77	LDAP Base backend LDBM not supported. Ldap restore not performed	Base LDAP au format LDBM non supportée. Restauration du LDAP non effectuée
78	The webadmin portal is under brute force attack	L'administration web est sous attaque par bruteforce
79	Configuration Migration:	Migration de la configuration :
80	Patterns database is corrupted, you should try to update it with the force option	La base de signature est corrompue, essayez de la mettre à jour en utilisant l'option force
81	HA: Can't synchronize reports: Some firewalls have a log disk while others don't	HA : impossible de synchroniser les rapports : certains firewalls ont un disque de log tandis que d'autres non
82	Remote host reachable:	Hôte distant joignable:
83	Remote host unreachable:	Hôte distant injoignable:
84	Aggregated link up:	Lien agrégé activé:
85	Aggregated link down:	Lien agrégé désactivé:

86	Backup successful	Sauvegarde réussie
87	Backup failed	Sauvegarde échouée:
88	Power:	Alimentation:
89	Connection error with agentAD:	Erreur de connexion avec l'agentAD
90	Topology change	Changement de topologie
91	Malicious file has been detected, hash:	Un fichier malicieux a été detecté, hash:
92	Remote service is no longer reachable:	Le service distant n'est plus joignable:
93	Remote service is reachable:	Le service distant est joignable:
94	An error occured loading a proxy functionality:	Erreur lors du chargement d'une fonctionnalité du serveur mandataire.

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 préconfigurées, numérotées de 1 à 10 :

« Block all (1) »	Par défaut, cette politique de filtrage est activée en configuration d'usine. Seuls les ports correspondant à l'administration du boitier sont ouverts (1300/TCP et 443/TCP). Le test d'accessibilité PING à destination de toutes les interfaces du boitier est également autorisé. Toutes les autres connexions sont ensuite bloquées. **REMARQUE** 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. **REMARQUE** 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. **REMARQUE** 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. **AVERTISSEMENT** Les règles de Filtrage et de NAT appartenant à la même politique, elles seront activées simultanément.
Editer	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 (*État, 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.

REMARQUE

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

Insérer 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 une appliance 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.
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.

Précision sur les symboles rencontrés lors de configuration d'une règle de filtrage

Comparaison mathématique

Chaque fois que vous rencontrerez une liste déroulante d'objets au sein des colonnes (exceptées « Etat » 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.

Menu Général de la boite d'édition de la règle de filtrage

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 6ème 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 **aucune**, 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.

NOTE
Cette option est indisponible si vous avez préalablement choisi l'action « Tracer » au sein du champ précédent.

Verbeux (journal : filtrage): Si vous choisissez cette option, une trace de chaque connexion correspondant à la règle sera ajoutée dans les logs de filtrage.
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 connaissance - 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 **Qualité de service**, du menu **Politique de Sécurité**.
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. **Equité entre les utilisateurs** : la bande passante sera répartie équitablement entre les différents utilisateurs. **Equité entre les machines** : la bande passante sera répartie équitablement entre les différentes machines. **Equité 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 connexions 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).
URLs 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 web, 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 génèrera 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.

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 adresses IP publiques

Sélectionnez une catégorie de réputation

Ce champ permet d'appliquer la règle de filtrage aux machines dont l'adresse IP publique est classifiée dans l'une des catégories de réputation prédéfinies :

- **anonymiseur** : proxies, convertisseurs IPv4 vers IPv6.
- **botnet** : machines infectées exécutant des programmes malveillants.
- **malware** : machines distribuant des programmes malveillants
- **phishing** : serveurs de messagerie compromis.
- **scanner** : machines exécutant du balayage de ports (port scanning) ou des attaques par force brute.
- **spam** : serveurs de messagerie compromis.
- **noeud de sortie tor** : serveurs d'extrémités du réseau Tor.
- **bad** : regroupe l'ensemble des catégories ci-dessus.

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.

D'autres catégories de machines sont également disponibles afin de faciliter la mise en place de règles de filtrage pour les solutions Microsoft Online :

- **Exchange Online** : serveurs d'hébergement de messagerie d'entreprise.
- **Microsoft Identité et authentification** : serveurs d'authentification utilisés pour l'accès à la solution Microsoft Office 365.
- **Office 365** : serveurs d'hébergement de la solution de stockage et de bureautique Microsoft Office 365.
- **Office Online** : serveurs d'hébergement de la solution de bureautique en ligne gratuite Microsoft Office.
- **Sharepoint Online** : serveurs d'hébergement de la solution collaborative Microsoft Sharepoint en ligne.
- **Skype Entreprise Online** : serveurs d'hébergement de la solution professionnelle de messagerie instantanée Skype.
- **Microsoft** : regroupe l'ensemble des catégories de machines hébergeant les services Microsoft en ligne.

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 redirigé 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 .

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 adresses IP publiques

Sélectionnez une catégorie de réputation	Ce champ permet d'appliquer la règle de filtrage aux machines destination dont l'adresse IP est classifiée dans l'une des catégories de réputation prédéfinies : • **anonymizer** : proxies, convertisseurs IPv4 vers IPv6. • **botnet** : machines infectées exécutant des programmes malveillants. • **malware** : machines distribuant des programmes malveillants • **phishing** : serveurs de messagerie compromis. • **scanner** : machines exécutant du balayage de ports (port scanning) ou des attaques par force brute. • **spam** : serveurs de messagerie compromis. • **tor exit node** : serveurs d'extrémités du réseau Tor. • **Bad** : regroupe l'ensemble des catégories ci-dessus. **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.

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 .

Type de protocole

Selon le type de protocole que vous choisissez ici, le champ qui suivra s'affichera différemment :

Détection automatique du protocole (par défaut)	Si vous cochez cette option, un champ du même nom apparaîtra en dessous avec les données suivantes : Protocole applicatif : Basé sur les ports par défaut ou le contenu Protocole IP : Tous
Protocole applicatif	L'intérêt de ce choix est d'appliquer une analyse applicative sur un port différent du port par défaut. Lorsque vous cochez cette case, le champ suivant portant le même nom vous propose de choisir : Protocole applicatif : Choisissez le protocole souhaité dans la liste déroulante. Protocole IP : Tous
Protocole IP	Si vous cochez cette option, le champ suivant proposera une liste déroulante de différents protocoles IP.

NOTE

Il est possible de suivre l'état des connexions IP pour les protocoles autres que TCP, UDP ou ICMP.

Suivi des états (stateful)	Si vous choisissez le type « Protocole IP », une option « stateful » vous est proposée. Cette option est cochée par défaut pour tout protocole IP autre que TCP, UDP, ICMP et IGMP.

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.

En cas de **translation de la destination choisie**, une option supplémentaire est disponible :

Translation de Port

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

Type d'inspection

Général

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**. **NOTE** 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. **NOTE** 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. **NOTE** L'activation de cette option nécessite l'utilisation de l'antivirus Kaspersky. **NOTE** 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. **NOTE** 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. **NOTE** 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

Insérer 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 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 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.

NOTE

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 filtrage dans le but de la dupliquer.
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 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.
Réinitialiser les statistiques des règles	En cliquant sur ce bouton, vous réinitialisez les compteurs numériques et graphiques d'utilisation des règles de NAT 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 : **Etat**), 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 que le bouton **réinit. colonnes**, vos colonnes réapparaîtront à l'état initial, avant que vous n'ayez coché de case additionnelle. Ainsi, les cases « **Nom** » et « **Port src** » seront de nouveau masquées.

NOTE GENERALE :

Chaque fois que vous rencontrerez une liste déroulante d'objets au sein des colonnes (exceptées « Etat » 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.

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.

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.

Etat

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.

Menu Général de la boite d'édition de la règle de NAT

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**).

Le trafic original (avant translation)

En cliquant dans la colonne « Interface d'entrée » une fenêtre de configuration s'affiche :

Source avant translation (originale)

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 avant translation (originale)

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.

Le trafic après translation

Source après translation

Onglet « 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 après translation

Onglet « 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'équilibrages 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

Type de protocole

Selon le type de protocole que vous choisissez ici, le champ qui suivra s'affichera différemment :

Détection automatique du protocole (par défaut)	Si vous cochez cette option, un champ du même nom apparaîtra en dessous avec les données suivantes : Protocole applicatif : Basé sur les ports par défaut ou le contenu Protocole IP : Tous
Protocole applicatif	L'intérêt de ce choix est d'appliquer une analyse applicative sur un port différent du port par défaut. Lorsque vous cochez cette case, le champ suivant portant le même nom vous propose de choisir : Protocole applicatif : Choisissez le protocole souhaité dans la liste déroulante. Protocole IP : Tous
Protocole IP	Si vous cochez cette option, le champ suivant proposera une liste déroulante de différents protocoles IP.

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 particulariser votre règle de NAT et ses caractéristiques.

FILTRAGE SMTP

Ce module se compose de 2 zones :

- Une zone destinée aux profils,
- Une zone destinée aux 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 « Default », accompagné de sa numérotation.

Exemples :

- Defaut00
- Default01…

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 :

Etat	Action	Expéditeur	Destinataire (to,cc,cci)	Commentaire
Activé	Passer	*@*	*@*	default rule (pass all)

Les boutons

Editer	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. **REMARQUE** 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 emails 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

Le filtrage SSL est désormais intégré à la nouvelle politique de sécurité des firewalls multifonctions Stormshield Network. 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 :

- Une zone destinée aux profils,
- Une zone destinée aux règles de filtrage SSL.

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 « Default », accompagné de sa numérotation.

Exemples :

- Defaut00
- Default01…

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	Passer sans 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 Web** / 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.

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*.

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.
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 2 zones :

- Une zone destinée aux profils,
- Une zone destinée aux règles de filtrage d'URL.

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 « Default », accompagné de sa numérotation.

Exemples :

- Defaut00
- Default01…

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 :

Etat	Action	Catégorie d'URL ou groupe	Commentaire
Activé	Passer	any	default rule (pass all)

Les boutons

Editer	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 Web** / 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.

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 la redirection vers la page de blocage BlockPage_00.

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 catégorie précédemment créé. En cliquant sur le champ, une liste déroulante vous invite à choisir une catégorie d'URL ou un groupe de catégorie, 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.

REMARQUE

Les caractères « [ ] » et « {} » ne sont plus autorisés dans les URL (Internet Explorer 7 et 8).

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:

- Etape 1 : Créer un groupe de firewalls (cluster)/rejoindre un groupe de firewalls (cluster) existant
- Etape 2 : Configuration des interfaces réseaux : le lien principal et le lien secondaire (facultatif)
- Etape 3 : Définition de la clé pré partagée du cluster
- Etape 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**.

Etape 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 reboot sera effectué à la fin de l'assistant. Une fois le reboot 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.

Etape 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 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.

Etape 3 : Clé pré partagée du cluster et chiffrement des données

En cas de création de cluster

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	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.

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.

Etape 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.

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. Etes-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.

Ecran de la Haute disponibilité

Communication entre les firewalls du groupe de haute disponibilité

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 groupe de haute disponibilité

Nouvelle clé pré partagée	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 ce firewall comme actif et le second le relaiera si celui 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 des 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)**. 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.

Configuration 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	En cochant cette case, vous activez l'agrégation de liens sur le firewall même si celui-ci devient passif au sein 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 (switch, 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.

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" qui représentent des éléments physiques ou non de communication entre les différents réseaux qui transitent par le boîtier.

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

Modes de fonctionnement entre interfaces

Vous pouvez configurer le fonctionnement entre interfaces du firewall suivant trois modes différents :

- Mode avancé (Routeur),
- Mode Bridge (ou mode transparent),
- Mode hybride.

Mode avancé

En avancé : avec ce mode de configuration, 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 Bridge ou mode transparent

En transparent (Bridge) : les interfaces font partie du même plan d'adressage déclaré sur le bridge.

Le mode transparent, aussi appelé "Bridge" en anglais, 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 hybride

En 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 transparent.

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.

Agrégation de liens (LACP) – SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100.

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 comme une unique interface logique. Ainsi, en agrégeant *n* liens, on peut établir une liaison de *n* fois 1 Gbps ou 10 Gbps entre deux équipements.

Cette fonctionnalité est uniquement disponible sur les modèles SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100.

NOTE

Assurez-vous que les équipements distants supportent le protocole LACP.

Conclusion

Le choix d'un mode se fait uniquement au niveau de la configuration des interfaces réseau. La configuration du firewall est ensuite la même pour tous les modes.

Au niveau sécurité, tous les modes de fonctionnement sont identiques. On filtre les mêmes choses et la détection d'attaques est identique.

Présentation de l'écran de configuration

L'écran de configuration des interfaces se présente comme suit :

- **L'arborescence des interfaces** (panneau central),
- **La barre d'outils**,
- **Le panneau de configuration** (panneau central) : un double clic sur une interface permet d'afficher son panneau de configuration à côté de l'arborescence des interfaces.

L'arborescence des interfaces

Les interfaces du boîtier sont présentées dans l'ordre suivant : Bridge, Interface, VLAN, Modem.

Un double clic sur une interface permet d'afficher sa configuration. Il est également possible d'utiliser le moteur de recherche pour rechercher une interface spécifique (exemple : en saisissant « br », tous les bridges sont indiqués).
Lorsqu'aucune interface n'est éditée, cette arborescence occupe l'ensemble de la grille centrale et présente 9 colonnes :

Interface	Nom propre donné à l'interface. Exemple : out, dmz1, mybridge, server_vlan... L'icône est affichée à droite du nom de l'interface par laquelle l'administrateur est connecté. L'icône est affichée à droite du nom de l'interface en cours d'édition.
Port	Nom technique de l'interface. Il s'agit d'un nombre entier correspondant au numéro de port physique de l'interface. Dans le cas d'un VLAN ou d'un modem, il s'agit du numéro de port de son interface parente.
Type	Le type de l'interface (Exemple : Bridge, Ethernet, VLAN, PPPoE ...) ainsi que des informations complémentaires : • Protégée ou Non protégée, • Interface Ethernet : taux de transfert (Exemple : 1Gb/s), • VLAN : identifiant de VLAN, taux de transfert de l'interface parente.
État	États particuliers d'une interface : désactivée, non connectée, supervisée... Lorsque l'interface est activée et connectée, cette colonne est vide.
Adresse IPv4	Indique l'adresse IP de l'interface et son masque, ou DHCP lorsque l'interface est en adressage dynamique.
Adresse IPv6	Indique l'adresse IPv6 de l'interface. Cette colonne n'est présente que lorsque IPv6 est activé sur le firewall.
Adresse MAC	Adresse physique (MAC) de l'interface.
Nom système	Il s'agit du nom de l'interface vue par le système d'exploitation du firewall. Exemple : em0, vlan0...
Commentaire	Le commentaire éventuellement ajouté lors de la configuration de l'interface (texte libre).

Glisser-déposer

Un glisser-déposer d'une interface modifie sa configuration (ses relations et son adresse IP). Si le glisser-déposer est autorisé, une coche verte est affichée. Au contraire, si le déplacement est interdit, une icône d'interdiction est affichée.

Lorsqu'une interface est détachée d'un bridge, une fenêtre permettant de renseigner son adresse IP s'affiche.

Les déplacements possibles sont indiqués dans le tableau suivant :

Bridge / Interface	De	Vers
Interface Ethernet	Bridge	Racine
Interface Ethernet	Bridge	Autre bridge
Interface Ethernet	Racine	Bridge
VLAN	Interface Ethernet	Autre interface Ethernet
VLAN	Interface Ethernet	Bridge
VLAN	Bridge	Autre bridge

VLAN	Bridge	Interface Ethernet
Modem (PPPoE)	Interface	Autre interface

Info bulle

Une info bulle est affichée au survol d'une interface. Selon le type d'interface, les informations affichées sont les suivantes :

Bridge	Nom propre, Type, Liste des membres du bridge, Adresse(s) IPv4, Adresse(s) IPv6.
Interface Ethernet	Nom propre, Type, État, Bridge parent éventuel, Port, Adresse MAC, Nom système, VLANs enfants éventuels, Modem rattachés éventuels, Adresse(s) IP.
VLAN	Nom propre, Type, État, Interface parente, Port, Identifiant de VLAN, Adresse MAC, Nom système, Adresse(s) IP.
Agrégat	Nom propre, Type, État, Membres.
Interface GRETAP	Nom propre, Type, État, Adresse locale de tunnel, Adresse distante de tunnel, Adresse (s) IP.
Interface USB / Ethernet	Nom propre, Profil utilisé, Type, État, Adresse(s) IP.
Modem PPPoE	Nom propre, Type, État, Interface parente.
Modem PPTP	Nom propre, Type, État, Adresse IP.

La barre d'outils

La barre d'outils permet :

- De filtrer selon l'interface souhaitée,
- D'étendre ou de réduire l'arborescence des interfaces,
- D'éditer la configuration de l'interface sélectionnée ou des profils de modems,
- D'ajouter ou de supprimer des interfaces (bridge, VLAN, interfaces GRETAP, modem PPPoE ou PPTP, interfaces USB / Ethernet) ou un agrégat de liens,
- De placer sous supervision la ou les interfaces sélectionnées,
- D'accéder directement au module de supervision des interfaces,
- De vérifier l'utilisation d'une interface dans les autres modules de configuration du firewall.

Réduire	Ce bouton permet de regrouper l'arborescence des interfaces.
Déplier	Ce bouton permet d'étendre l'arborescence des interfaces.
Rafraîchir	Ce bouton permet d'actualiser les informations présentées dans le panneau des interfaces.
Éditer	Ce bouton permet d'éditer : • L'interface réseau sélectionnée dans le panneau, • L'un des deux profils de modems USB over Ethernet.
Ajouter	Ce bouton permet d'ouvrir l'assistant de création d'un bridge, d'un vlan, d'une interface GRETAP, d'un modem PPPoE ou d'un modem / clé USB. Il permet également de convertir une interface en agrégat de liens sur les firewalls supportant cette fonctionnalité.
Supprimer	Ce bouton vous permet de supprimer une interface préalablement sélectionnée dans l'arborescence des interfaces. Les interfaces Ethernet ne peuvent être supprimées.
Superviser	Ce bouton permet d'ajouter directement l'interface sélectionnée à la liste des interfaces supervisées. Les graphes correspondants sont automatiquement créés dans le module **Supervision** > **Interfaces**.

Accéder à la supervision	En cliquant sur ce bouton, vous êtes directement redirigé dans le module **Supervision** > **Interfaces**.
Vérifier l'utilisation	Si vous cliquez sur ce bouton après avoir sélectionné une interface, le résultat s'affiche dans l'arborescence des modules. Si vous supprimez une interface, une vérification est faite : si l'interface est utilisée, un message s'affiche : « Attention, *cette interface / bridge est utilisée par un ou plusieurs modules. La supprimer peut rendre le firewall instable* ». Vous pouvez alors forcer la suppression, vérifier l'utilisation ou annuler. Si l'interface n'est pas utilisée, le message : « Voulez-vous réellement supprimer cette interface ? » s'affiche.

NOTE

Un modem 3G externe peut être connecté au port USB.

NOTE

Le renommage d'une interface ne modifie pas les références à celle-ci dans les éléments de configuration utilisant les objets générés tel que "Network_in" par exemple. Un message d'avertissement s'affiche lorsqu'une interface sera renommée.

Créer un bridge

Deux méthodes de création de bridge sont possibles :

- Création d'un bridge sans membres (préparation d'une configuration par exemple),
- Création d'un bridge contenant des interfaces.

Le nombre de bridges pouvant être créés varie selon votre modèle de firewall.

Créer un bridge sans membres

1. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
2. Cliquez sur **Bridge** puis sur **Sans membres**.
   Le nouveau bridge est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Créer un bridge contenant des interfaces pré-sélectionnées

1. Sélectionnez les interfaces réseau à inclure dans le nouveau bridge (*interface_1*, *interface_2* dans cet exemple).
2. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
3. Cliquez sur **Bridge** puis **Avec *interface_1*, *interface_2* ...**
   Le nouveau bridge est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Les champs du panneau de configuration du bridge sont détaillés dans la section Modifier un bridge.

Modifier un Bridge

Faites un double clic sur le bridge à modifier : le panneau de configuration de ce bridge s'affiche.

Onglet "Configuration Générale"

Paramètres généraux

Nom	Nom utilisateur de l'interface (voir l'avertissement en introduction de la section **Interfaces**).
Commentaire	Permet de donner un commentaire pour l'interface.

Plan d'adressage

IP fixe (statique)	En cochant cette option, le bridge a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque de réseau du sous-réseau auquel appartient le bridge.
IP dynamique (obtenue par DHCP)	En cochant cette option, l'adresse IP de interface est définie par DHCP. Vous pouvez dans ce cas indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la requête DHCP (champ **Nom DNS (facultatif)**). 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 à jour automatiquement le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et le temps alloué (obligatoire). Il faut également indiquer une période de conservation de l'adresse IP avant renégociation (champ **Durée de bail demandée (secondes)**). Lorsque l'option **Demander les serveurs DNS au serveur DHCP et créer les objets machine associés** est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP.

Gestion des membres

Sélectionnez les interfaces pour lesquelles vous souhaitez réaliser un bridge.

La liste "Interfaces membres" recense les interfaces Ethernet et les interfaces VLAN déjà présentes dans la configuration du bridge.

Il faut sélectionner au moins deux interfaces qui composeront le bridge :

- Soit par l'intermédiaire des flèches,
- Soit en effectuant un glisser-déposer depuis la liste "Interfaces disponibles" vers la liste "Interfaces membres",
- Soit en double-cliquant sur l'interface.

Cliquez sur **Terminer** pour valider la configuration.

Onglet "Configuration avancée"

Autres paramètres

MTU	Longueur maximale (en octets) de la charge utile d'une trame Ethernet afin que celle-ci soit transmise en une seule fois (sans fragmentation).
Adresse physique (MAC)	Cette option vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall.

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 SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100.

Désactiver les protocoles Spanning Tree	Cette case désactive l'utilisation des protocoles Spanning Tree (RSTP et MSTP) au niveau du bridge. Elle est cochée par défaut.
Activer le protocole Rapid Spanning Tree (RSTP)	Cette case permet d'activer le protocole Rapid Spanning Tree au niveau du bridge.
Activer le protocole Multiple Spanning Tree (MSTP)	Cette case permet d'activer le protocole Multiple Spanning Tree au niveau du bridge.

Lorsque le protocole MSTP est activé, des champs complémentaires sont à renseigner :

Nom de la région (MSTP region)	Nom de la région MSTP dans laquelle se situe le firewall. Le nom de région doit être identique dans la configuration MSTP de tous les équipements réseaux appartenant à cette région.
Sélecteur de format	Ce champ précise quelles sont 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 réseaux 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 réseaux 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 (Grille des instances MSTP).

REMARQUE

Sur un Firewall SNS, une configuration MSTP ne peut définir qu'une seule région.

Grille des instances MSTP

Cette grille permet de définir les différentes instances déclarées dans la configuration du protocole MSTP :

Instance	Cet identifiant unique s'incrémente automatiquement lorsqu'une instance est ajoutée dans la configuration du protocole MSTP.
Identifiant de VLAN	Indiquez les différents identifiants de VLAN (liste d'identifiants séparés par une virgule) inclus dans l'instance sélectionnée.
Priorité	Ce champ permet de fixer 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.

Supprimer un bridge

Pour supprimer un bridge :

1. Sélectionnez le bridge 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.

Si vous confirmez la suppression, une vérification est faite (*check*) pour voir si l'interface est utilisée.

NOTE

La suppression d'un bridge désactive les interfaces qu'il contenait et modifie la configuration de celles-ci en adressage via DHCP.

Modifier une interface Ethernet (en mode Bridge)

Une interface appartenant à un bridge est représentée sous forme de nœud fils par rapport au bridge. Un bridge peut donc contenir plusieurs nœuds fils.

Vous pouvez modifier les paramètres de chaque interface appartenant ou non au bridge. Pour cela, faites un double clic sur une interface située sous un bridge ou en dehors du bridge dans la partie gauche de la fenêtre. Deux onglets s'affichent :

NOTE

Il n'est pas possible d'ajouter ou de supprimer des interfaces Ethernet.

Onglet « Configuration générale »

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver l'interface. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à une interface que l'on a prévu de déployer ultérieurement, mais qui n'est pas encore en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé à l'interface du bridge. (Voir l'avertissement en introduction de la section **Interfaces**)
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être « Interne (protégée) » ou « Externe (publique) ». Si vous sélectionnez « Interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « Externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

Plan d'adressage

Plan d'adressage hérité du Bridge	Si l'interface fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. Lorsque cette case est cochée, un champ **Bridge** permet alors de sélectionner le bridge parent de l'interface.
Dynamique / Statique	Cochez cette case pour préciser lorsque l'adresse IP de l'interface doit être obtenue par DHCP ou fixée (statique). Lorsque cette case est cochée, le champ Adressage IPv4 est affiché et permet de préciser ce choix d'adressage.
IP dynamique (obtenue par DHCP)	Ce champ permet donc de spécifier au firewall que la configuration de l'interface (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « Configuration DHCP avancée » est active.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et son masque de sous-réseau.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour une même interface (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, une interface peut être connectée 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. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Configuration DHCP avancée

Cette zone n'est active que lorsque la case **IP dynamique (obtenue par DHCP)** a été cochée pour l'interface.

Nom DNS (facultatif)	Vous pouvez dans ce cas indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la connexion (champ **Nom DNS (facultatif)**). 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 à jour automatiquement le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et le temps alloué (obligatoire). Il faut également indiquer une période de conservation de l'adresse IP avant renégociation (champ **Durée de bail demandée (secondes)**).
Durée de bail demandée	Période de conservation de l'adresse IP avant renégociation.
Demander les serveurs DNS au serveur DHCP et créer les objets machine associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'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. **NOTE** Cette option est désactivée si l'option **IP dynamique (obtenue par DHCP)** n'est pas activée dans l'onglet *Configuration de l'interface*.

Onglet « Configuration avancée »

Autres paramètres

MTU	Longueur maximale (en octets) de la charge utile d'une trame Ethernet afin que celle-ci soit transmise en une seule fois (sans fragmentation).
Adresse physique (MAC)	Cette option vous 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.

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. Les vitesses proposées sont : "Détection automatique", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gbps Full duplex". **AVERTISSEMENT** 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.

Bridge – Routage sans analyse

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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).

Bridge – Routage par interface

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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".**

Modifier une interface Ethernet (en mode avancé)

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.

Une fois l'interface hors du bridge, vous avez accès aux paramètres de l'interface décrits dans la section Modification d'une interface Ethernet (en mode Bridge).

Créer ou modifier une interface Wi-Fi (WLAN)

Les interfaces correspondant aux points d'accès du firewall (WLAN) sont listées dans la partie gauche de la fenêtre **Interfaces**. Sélectionnez une interface pour en modifier les paramètres. Un onglet s'affiche :

Onglet « Configuration générale »

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver l'interface WLAN. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à une interface que l'on a prévu de déployer ultérieurement mais qui n'est pas encore en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé à l'interface WLAN. (Voir l'avertissement en introduction de la section **Interfaces**)
Commentaire	Permet de donner un commentaire pour l'interface.

Cette interface est	Une interface peut être « interne (protégée) » ou « externe (publique) ». Si vous sélectionnez « interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

Wi-Fi

Nom du réseau	Saisissez le nom attribué au réseau Wi-Fi géré par le firewall (SSID).
Authentification	Sélectionnez l'un des 3 mécanismes d'authentification permettant de se connecter au réseau Wi-Fi géré par le firewall : • Réseau ouvert (aucune authentification). **NOTE** Lorsque vous cochez cette case, le champ **Clé de sécurité** devient inactif (grisé). • WPA (Wi-Fi Protected Access). • WPA 2 (WPA 2 est une évolution de WPA présentant un niveau de sécurité plus élevé).
Clé de sécurité	1. Saisissez la clé de sécurité (mot de passe) nécessaire pour se connecter au réseau Wi-Fi. 2. Confirmez 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 elles sans passer par le firewall. Elle est activée par défaut (configuration type 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	Si l'interface fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. Lorsque cette case est cochée, un champ **Bridge** permet alors de sélectionner le bridge parent de l'interface.
Dynamique / Statique	Cochez cette case pour préciser lorsque l'adresse IP de l'interface doit être obtenue fixée (statique). Lorsque cette case est cochée, le champ Adressage IPv4 est affiché et permet de préciser ce choix d'adressage.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour une même interface (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, une interface peut être connectée 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. Le

rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

NOTE

Il n'est pas possible d'ajouter ou de supprimer des interfaces WLAN.

Créer un VLAN

Deux méthodes de création de VLAN sont possibles :

- Création d'un VLAN sans interface parente,
- Création d'un VLAN rattaché à une ou plusieurs interfaces.

Créer un VLAN sans interface parente

1. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
2. Cliquez sur **VLAN** puis sur **Sans interface parente**.
   Le nouveau VLAN est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Créer un VLAN rattaché à des interfaces présélectionnées

1. Sélectionnez les interfaces réseau auxquelles sera rattaché le nouveau VLAN.
2. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
3. Cliquez sur **VLAN** puis **Pour *interface_1*, *interface_2* ...**
   Le nouveau VLAN est ajouté sous ses interfaces de rattachement et le panneau de configuration de ce VLAN s'affiche.

Les champs du panneau de configuration du VLAN sont détaillés dans la section Modifier un VLAN.

Modifier un VLAN

Faites un double clic sur le VLAN à modifier : le panneau de configuration de ce VLAN s'affiche.

Onglet « Configuration Générale »

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver le VLAN. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à une interface que l'on a prévu de déployer ultérieurement mais qui n'est pas encore en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé au VLAN. (Voir l'avertissement en introduction de la section **Interfaces**)
Commentaire	Permet de donner un commentaire pour le VLAN.
Interface parente	Nom physique de l'interface à laquelle est attaché le VLAN.

Identifiant de VLAN	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) » ou « externe (publique) ». Si vous sélectionnez « interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

Plan d'adressage

Plan d'adressage hérité du Bridge	Si l'interface parente fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. Lorsque cette case est cochée, un champ **Bridge** permet alors de sélectionner le bridge parent de l'interface.
Dynamique / Statique	Cochez cette case pour préciser lorsque l'adresse IP de l'interface VLAN doit être obtenue par DHCP ou fixée (statique). Lorsque cette case est cochée, le champ Adressage IPv4 est affiché et permet de préciser ce choix d'adressage.
IP dynamique (obtenue par DHCP)	Ce champ permet donc de spécifier au firewall que la configuration du VLAN (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « Configuration DHCP avancée » est active.
IP fixe (statique)	En cochant cette option, l'interface VLAN a un adressage statique. Il faut dans ce cas indiquer son adresse IP et son masque de sous-réseau.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour le 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. 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) de la charge utile d'une trame Ethernet afin que celle-ci soit transmise en une seule fois (sans fragmentation).

Routage sans analyse

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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".**

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 du VLAN (*check*) est faite.

Créer un modem PPTP

Les interfaces modem sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur le firewall (port série). Le firewall accepte tout type de modem (ADSL, RNIS, RTC, ...).

Le nombre maximal de modems disponibles sur votre firewall dépend du modèle de firewall.

Pour créer un modem PPTP :

1. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit, puis sélectionnez **Ajouter**.
2. Cliquez sur **Modem** puis sur **PPTP**.
   Le nouveau modem est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Les champs du panneau de configuration du modem sont détaillés dans la section Modifier un modem PPTP.

Modifier un modem PPTP

Faites un double-clic sur le modem PPTP à modifier : le panneau de configuration du modem s'affiche.

Onglet "Configuration générale"

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver le modem. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à un modem que l'on a prévu de déployer ultérieurement mais qui n'est pas encore en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé au modem. (Voir l'avertissement en introduction de la section **Interfaces**)
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	1. Saisissez le mot de passe utilisé pour l'authentification. Si vous cliquez sur l'icône « clé » à droite de ce champ, le mot de passe s'affiche en clair pour une durée de 5 secondes. 2. Confirmez le mot de passe. Une jauge indique la robustesse du mot de passe choisi.

Onglet "Configuration avancée"

Autres paramètres

Connexion	La connexion **A la demande** (en cas de trafic) n'établit la connexion vers Internet 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). La connexion **Permanente** conserve la connexion vers Internet active en permanence.

Créer un modem PPPoE

Les interfaces modem sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur le firewall (port Ethernet). Le firewall accepte tout type de modem (ADSL, RNIS, RTC, ...).

Le nombre maximal de modems disponibles sur votre firewall dépend du modèle de firewall.

Pour créer un modem PPPoE :

1. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis sélectionnez **Ajouter**.
2. Cliquez sur **Modem** puis sur **PPPoE**.
   Le nouveau modem est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Les champs du panneau de configuration du modem sont détaillés dans la section Modifier un modem PPPoE.

Modifier un modem PPPoE

Faites un double-clic sur le modem PPoE à modifier : le panneau de configuration du modem s'affiche.

Onglet "Configuration générale"

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver le modem. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à un modem que l'on a prévu de déployer ultérieurement mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé au modem (Voir l'avertissement en introduction de la section **Interfaces**).
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 est connectée le modem PPPoE.

Authentification

Identifiant	Saisissez l'identifiant utilisé pour l'authentification.
Mot de passe	1. Saisissez le mot de passe utilisé pour l'authentification. Si vous cliquez sur l'icône « clé » à droite de ce champ, le mot de passe s'affiche en clair pour une durée de 5 secondes. 2. Confirmez le mot de passe. Une jauge indique la robustesse du mot de passe choisi.

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.
Connexion	La connexion **A la demande** (en cas de trafic) n'établit la connexion vers Internet 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). La connexion **Permanente** conserve la connexion vers Internet active en permanence.

Supprimer un modem

Pour supprimer un modem :

1. Sélectionnez le modem 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.

Remarques générales sur la configuration d'un modem

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 (problème de ligne), le firewall envoie un message d'alarme.

Créer une interface USB / Ethernet (pour clé USB / Modem)

Les interfaces USB / Ethernet sont créées et utilisées dans le cas de connexions distantes via un modem branché directement sur le firewall (port USB).

Une interface USB / Ethernet est automatiquement créée lorsqu'un modem USB 4G de marque HUAWEI supportant la fonctionnalité HiLink est connecté sur le firewall puis paramétré.

Dans le cas contraire, la création d'une interface USB / Ethernet associée à la clé USB / Modem nécessite la configuration d'un profil de modem. Deux profils de modem peuvent être définis sur le firewall mais une seule interface USB / Ethernet peut être ajoutée au firewall.

Créer un profil de modem

1. Cliquez sur le menu **Éditer**.
2. Cliquez sur **Profils de modem** et sélectionnez l'un des deux profils de modem (nommés Modem 1 et Modem 2 par défaut).
   Le panneau de configuration du profil de modem s'affiche.

Panneau de configuration du profil de modem

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 (chaîne hexadécimale).
Identifiant initial de produit	Identifiant du produit 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. 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.

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	Cette chaîne est optionnelle. Elle permet d'envoyer au modem des commandes de configuration de type "AT" avant son utilisation. Exemple : "ATZ" (commande de réinitialisation du modem), "AT^CURC=0" (commande permettant de désactiver les messages périodiques).
Chaîne d'initialisation N°2	Cette chaîne est optionnelle. Elle permet d'envoyer au modem des commandes de configuration de type "AT" avant son utilisation. Exemple : "ATZ" (commande de réinitialisation du modem), "AT^CURC=0" (commande permettant de désactiver les messages périodiques).
Chaîne d'initialisation N°3	Cette chaîne est optionnelle. Elle permet d'envoyer au modem des commandes de configuration de type "AT" avant son utilisation. Exemple : "ATZ" (commande de réinitialisation du modem), "AT^CURC=0" (commande permettant de désactiver les messages périodiques).

Créer une interface USB / Ethernet

1. Cliquez sur le menu **Ajouter**.
2. Cliquez sur **Interface USB / Ethernet (clé USB / Modem)**.
   Le panneau de configuration de l'interface USB / Ethernet s'affiche.

Les champs du panneau de configuration de l'interface USB / Ethernet sont détaillés dans la section Modifier une interface USB / Ethernet.

Modifier une interface USB / Ethernet

Faites un double clic sur l'interface USB / Ethernet à modifier : le panneau de configuration de cette interface s'affiche.

Onglet « Configuration générale »

Lorsque aucun profil de modem n'est défini ou n'est actif, un message vous invite à configurer un profil de modem :

1. Cliquez sur le bouton **Configurer les profils**.
2. Sélectionnez le profil de modem à activer ou configurer.

Les champs du panneau de configuration d'un profil de modem sont détaillés dans la section Créer une interface USB / Ethernet.

Paramètres généraux

Nom (obligatoire)	Nom de l'interface USB / Ethernet (voir l'avertissement en introduction de la section **Interfaces**).
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être « interne (protégée) » ou « externe (publique) ». Si vous sélectionnez « interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

Plan d'adressage

IP dynamique (obtenue par DHCP)	En cochant cette option, l'adresse IP de interface est définie par DHCP. Vous pouvez dans ce cas indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la connexion (champ **Nom DNS (facultatif)**). 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 à jour automatiquement le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et le temps alloué (obligatoire). Il faut également indiquer une période de conservation de l'adresse IP avant renégociation (champ **Durée de bail demandée (secondes)**). Lorsque l'option **Demander les serveurs DNS au serveur DHCP et créer les objets machine associés** est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et son masque de sous-réseau.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour la même interface (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, une interface USB/Ethernet peut être connectée 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. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Créer une 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.

Créer une interface GRETAP

1. Cliquez sur le bouton **Ajouter.**
2. Cliquez sur **Interface GRETAP**.
   Le panneau de configuration de l'interface s'affiche.

Les champs du panneau de configuration de l'interface GRETAP sont détaillés dans la section Modifier une interface GRETAP.

Modifier une interface GRETAP

Faites un double-clic sur l'interface GRETAP à modifier : le panneau de configuration de l'interface s'affiche.

Onglet « Configuration générale »

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver l'interface concernée. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à une interface que l'on a prévu de déployer ultérieurement mais qui n'est pas en activité. Une interface désactivée, car non utilisée, est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom (obligatoire)	Nom associé à l'interface GRETAP. (Voir l'avertissement en introduction de la section **Interfaces**)
Commentaire	Permet de donner un commentaire pour l'interface.
Cette interface est	Une interface peut être « interne (protégée) » ou « externe (publique) ». Si vous sélectionnez « interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

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	Si l'interface fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. Lorsque cette case est cochée, un champ **Bridge** permet alors de sélectionner le bridge parent de l'interface.

Dynamique / Statique	Cochez cette case pour préciser lorsque l'adresse IP de l'interface doit être obtenue par DHCP ou fixée (statique). Lorsque cette case est cochée, le champ Adressage IPv4 est affiché et permet de préciser ce choix d'adressage.
IP dynamique (obtenue par DHCP)	Ce champ permet donc de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « Configuration DHCP avancée » est active.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et son masque de sous-réseau.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour la même interface (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, une interface peut être connectée 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. Le rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Configuration DHCP avancée

Cette zone n'est active que lorsque la case **IP dynamique (obtenue par DHCP)** a été cochée pour l'interface.

Nom DNS (facultatif)	Vous pouvez dans ce cas indiquer un nom d'hôte DHCP pleinement qualifié (FQDN) pour la connexion (champ **Nom DNS (facultatif)**). 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 à jour automatiquement le serveur DNS avec le nom fourni par le firewall, l'adresse IP qui lui a été fournie et le temps alloué (obligatoire). Il faut également indiquer une période de conservation de l'adresse IP avant renégociation (champ **Durée de bail demandée (secondes)**).
Durée de bail demandée	Période de conservation de l'adresse IP avant renégociation.
Demander les serveurs DNS au serveur DHCP et créer les objets machine associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qui lui a fourni son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'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. **NOTE** Cette option est désactivée si l'option **IP dynamique (obtenue par DHCP)** n'est pas activée dans l'onglet *Configuration de l'interface*.

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 (donc sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.

Adresse physique (MAC)	L'interface GRETAP étant contenue dans un bridge, elle possède donc la même adresse MAC que celui-ci.

Routage sans analyse

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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

NOTE

Ce panneau n'est pas affiché si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans 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**".
Adresse de la passerelle	Ce champ sert au routage par interface. Tous les paquets arrivant sur cette interface seront routés via une passerelle spécifiée.

Convertir une interface en agrégat de liens (LACP)

Cette fonctionnalité est uniquement disponible sur les modèles SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100.

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, on peut établir une liaison de *n* fois 1 Gbps ou 10 Gbps entre deux équipements.

NOTE

Assurez-vous que les équipements distants utilisent le protocole LACP.

NOTE

L'empilage de commutateurs (*stackable switches*) est recommandé car cela permet la redondance des liens entre les deux équipements.

Une interface déjà utilisée dans la configuration ne peut pas être convertie en agrégat.

Une interface convertie en agrégat devient une interface virtuelle, permettant de visualiser et de paramétrer l'agrégation. L'interface physique de cette interface convertie devient alors similaire à toute autre interface ajoutée à l'agrégation. Ces membres de l'agrégation sont appelés « liens agrégés ».

Une interface convertie en agrégat conserve ses paramètres de configuration. L'interface convertie dispose alors d'un onglet supplémentaire appelé « Agrégation de liens (LACP) ». En revanche, une interface devenant un lien agrégé perd ses paramètres de configuration pour hériter de la configuration de l'agrégat (sauf le nom et le réglage Média).

Selon les modules d'extension installés, le maximum d'agrégat possible est le nombre total d'interfaces du modèle divisé par deux. Le nombre maximal d'interfaces pouvant être réunies dans un agrégat est de 8, quel que soit le modèle.

Deux méthodes de création d'agrégat sont possibles :

- Création d'un agrégat sans membres (préparation d'une configuration par exemple),
- Création d'un agrégat à partir d'une sélection d'interfaces.

Créer un agrégat sans membre

1. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
2. Cliquez sur **Agrégat** puis sur **Sans membre**.
   Le nouvel agrégat est ajouté à la liste des interfaces et son panneau de configuration s'affiche.

Créer un agrégat contenant des interfaces présélectionnées

1. Sélectionnez les interfaces réseau à inclure dans le nouveau bridge (*interface_1*, *interface_2* dans cet exemple).
2. Cliquez sur le bouton **Ajouter** de la barre d'outils ou faites un clic droit puis **Ajouter**.
3. Cliquez sur **Agrégat** puis **Avec *interface_1*, *interface_2* ...**
   Le nouvel agrégat est ajouté à la liste des interfaces et son panneau de configuration s'affiche.
   Les interfaces sélectionnées pour être membres de cet agrégat lui sont automatiquement rattachées.

Les champs du panneau de configuration de l'agrégat sont détaillés dans la section Modifier un agrégat de liens.

Modifier un agrégat de liens (LACP)

Faites un double clic sur l'agrégat à modifier : le panneau de configuration de cet agrégat s'affiche.

Onglet "Configuration générale"

État

ON / OFF	Positionnez le sélecteur sur **ON** / **OFF** pour activer / désactiver l'agrégat. En désactivant une interface, on la rend inutilisable. Cela peut correspondre à une interface que l'on a prévu de déployer ultérieurement mais qui n'est pas encore en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.

Paramètres généraux

Nom	Nom utilisateur de l'interface. (Voir l'avertissement en introduction de la section **Interfaces**)
Commentaire	Permet de donner un commentaire pour l'agrégat.
Port physique	Liste des ports Ethernet contenus dans l'agrégation (Exemple : (Port2))
Cette interface est	Une interface peut être « interne (protégée) » ou « externe (publique) ». Si vous sélectionnez « interne (protégée) », vous indiquez le caractère protégé de l'interface. Cette protection comprend une mémorisation des machines connectées sur cette interface, des mécanismes de sécurisation du trafic conventionnel (TCP) et des règles implicites pour les services proposés par le Firewall comme le DHCP (voir la section *Règles Implicites*). Le caractère protégé de l'interface est matérialisé par un bouclier ( ). Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. L'icône du bouclier disparaît lorsque cette option est cochée.

Plan d'adressage

Plan d'adressage hérité du Bridge	Si l'agrégat fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. Lorsque cette case est cochée, un champ **Bridge** permet alors de sélectionner le bridge parent de l'agrégat.
Dynamique / Statique	Cochez cette case pour préciser lorsque l'adresse IP de l'interface doit être obtenue par DHCP ou fixée (statique). Lorsque cette case est cochée, le champ Adressage IPv4 est affiché et permet de préciser ce choix d'adressage.
IP dynamique (obtenue par DHCP)	Ce champ permet donc de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « Configuration DHCP avancée » est active.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et son masque de sous-réseau.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour la même interface (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, une interface peut être connectée 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. Le

rechargement de la configuration réseau appliquera ce masque sur la première adresse, et un masque de /32 sur les suivantes.

Gestion des membres

1. Sélectionnez les interfaces pour lesquelles vous souhaitez réaliser un agrégat.
   La liste "Interfaces membres" recense les interfaces Ethernet déjà présentes dans la configuration de l'agrégat.
   Il faut sélectionner au moins deux interfaces qui composeront l'agrégat :

- Soit par l'intermédiaire des flèches,
- Soit en effectuant un glisser-déposer depuis la liste "Interfaces disponibles" vers la liste "Interfaces membres",
- Soit en double-cliquant sur l'interface.

2. Cliquez sur **Terminer** pour valider la création.

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 (donc sans fragmentation).
Adresse physique (MAC)	Cette option vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall.

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.

Création ou modification d'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 :

Etat	Etat 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.

Création ou modification d'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 :

Etat	Etat 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.

Création ou modification d'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 :

Etat	Etat 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 "Accès complet aux logs (données sensibles)" en cliquant sur **Obtenir le droit d'accès aux données personnelles (logs)** dans le menu déroulant situé sous le nom du compte connecté (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 **Accès complet aux logs (données sensibles)** 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 "Accès complet aux logs (données sensibles)" 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 : Carte SD

La fonctionnalité de **Stockage externe des traces sur carte SD** est disponible pour les firewalls modèles SN160(W), SN210(W) et SN310. Cette fonctionnalité est proposée en souscrivant à l'option « External storage ».

Le type de carte SD doit être au minimum de **Classe 10 (C10) UHS Classe 1 (U1) ou App Performance (A1)** 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.

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 maximum de mémoire supportée est de 2 To.

NOTE

Le stockage sur support externe s'effectue uniquement sur carte SD. 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" / "Rechercheavancée**".

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

ACTION :

- **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.

CONFIGURATION :

- **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

ACTION :

- **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.

CONFIGURATION :

- **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

ACTION :

- **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.

CONFIGURATION :

- **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 d'accès complet aux logs) :

- 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.

URLs

ACTION :

- **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.

CONFIGURATION :

- **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 URLs (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 d'accès complet aux logs) :

- Nom du domaine,
- Adresse IP correspondante.

Ports

CONFIGURATION :

- **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 d'accès complet aux logs) :

- Nom de l'objet port,
- Numéro ou plage de ports correspondants,
- Protocole,
- Commentaire éventuel défini dans l'objet port.

Paquets réseau

ACTION

- **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

CONFIGURATION

- **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

CONFIGURATION

- **Configurer l'événement système** : raccourci pour ouvrir le module **Événements système** avec sélection automatique de l'événement concerné.

Les Journaux

Voici la liste des logs (utilisés dans les vues à but thématique) et le nom du fichier de traces correspondant sur le firewall :

Administration	l_server
Alarmes	l_alarm
Authentification	l_auth

Connexions réseaux	l_connection
Filtrage	l_filter
Proxy FTP	l_ftp
VPN IPSec	l_vpn
Connexions applicatives (plugin)	l_plugin
Proxy POP3	l_pop3
Proxy SMTP	l_smtp
Proxy SSL	l_ssl
Événements systèmes	l_system
Vulnérabilités	l_pvm
Proxy HTTP	l_web
VPN SSL	l_xvpn
Sandboxing	l_sandboxing

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.

- 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.**

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 *Détails de la licence* (ou indication du n° de série type Licence Locale U70XXADA913500 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 par boîtier passif dans le cadre de la Haute Disponibilité.

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 le fichier de licence** valide l'installation du fichier de licence sur le boîtier. Les informations concernant votre 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. Note : 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, syslog, le RealTime Monitor ainsi que les journaux du Stormshield Network Event Analyzer. Afin d'activer l'envoi de ces messages, vous pouvez vous rendre dans le menu **Notifications,** Ecran **Traces-Syslog** ou **Agent SNMP**.

L'onglet « Détails de la licence»

Cet onglet affiche la licence en vigueur du boîtier sur lequel vous êtes connecté.

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 », « Flags », « Global », « Hardware », « Limit », « Network », « Proxy », « Service », « VPN ». Ci-dessous sont détaillées les options liées aux fonctionnalités.
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.

Administration

Manager	Administration possible via l'interface Web. (Valeur par défaut : 1).
Monitor	Monitoring possible via Stormshield Network REALTIME MONITOR (Valeur par défaut : 1).

Date

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 Expresse. 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 Kaspersky	Date limite de mise à jour des bases virales Kaspersky.
Management de vulnérabilités	Date limite de mise à jour des vulnérabilités SEISMO.
Garantie	Date limite pour la garantie.

Options

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)

Global

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.

Matériel

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.

Limites

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)).

Réseau

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. Voir le Menu **: Configuration→ Réseau→ Interfaces/onglet** *Configuration avancée/* **champ Bridge : routage par interface»** (Valeur par défaut : 1).
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).

Proxy

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 Kaspersky	Active ou désactive l'antivirus Kaspersky dans le proxy. (Valeur par défaut : 0).

Services

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*).

Vpn

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)).

Le fonctionnement de cet onglet est identique à celui de la licence locale.

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 préconfigurés 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 notamment depuis le Stormshield Network REALTIME MONITOR. **REMARQUE** 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. **AVERTISSEMENT** 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 de mails 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 de mails 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 connaissance Stormshield Network, qui inclut généralement des indications sur le correctif à appliquer.

REMARQUE

Les groupes de mails 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.

Elément 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. **AVERTISSEMENT** 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. **REMARQUE** 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. **AVERTISSEMENT** 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)

Elément 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'indique les 4 onglets suivants :

- Mise à jour du système
- Sauvegarder
- Restaurer
- Configuration

Onglet « Mise à jour du système »

Une vidéo de la WebTV Stormshield Network sur YouTube vous guide pas à pas pour la Mise à jour d'un groupe de firewalls Stormshield Network (cluster). Cliquez sur ce lien pour accéder à la vidéo : Mise à jour d'un cluster de firewall Stormshield Network.

Mises à jour disponibles :

Rechercher de nouvelles mises à jour	Le firewall va effectuer une recherche des nouvelles mises à jour du système sur les serveurs update (**Objets/Objets réseau**) et les affichera à l'écran.

Mise à jour du système

Sélectionnez la mise à jour :	Choisissez la mise à jour du firewall à installer et insérez-là dans le champ à l'aide du bouton ... . L'empreinte SHA1 du fichier de mise à jour est affichée en cliquant sur le lien du même nom. Lorsqu'une nouvelle version de firmware est disponible, le lien **Release Notes** permet de télécharger les Notes de Version applicables à la version de firmware proposée au téléchargement.
Mettre à jour le firewall	Appliquez la mise à jour sélectionnée sur votre boitier en cliquant sur ce bouton.

NOTE

Dans le cas de Haute Disponibilité, si vous choisissez l'activation sur les 2 firewalls, la mise à jour sera activée uniquement sur le Firewall distant, pour éviter que votre réseau ne devienne inaccessible. Pour activer cette mise à jour sur votre Firewall actif, suivez la procédure suivante :

1. Assurez-vous que la mise à jour du passif soit terminée dans l'écran **Tableau de Bord** (Composant Matériel),
2. Revenez dans le module **Maintenance**, onglet *Mise à jour* du système et sélectionnez "Ce firewall" comme Firewall à mettre à jour
3. En configuration avancée, cochez l'option "Activer le firmware précédemment téléchargé" puis cliquez sur le bouton Mettre à jour le firewall.

Un basculement s'opérera et votre Firewall passif deviendra actif.

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 va permettre d'envoyer le fichier de mise à jour (.maj) et d'activer celui-ci.
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 permettra de l'activer. **NOTE** Si un fichier est présent, 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 »

Lorsque le firewall dispose d'un module TPM (Trusted Platform Module) destiné à stocker de manière sécurisée les certificats, les clés, les fichiers de sauvegarde de configuration... et que ce TPM n'a pas été initialisé (que son mot de passe d'administration n'a pas encore été créé), une fenêtre d'initialisation du TPM est affichée à l'ouverture de l'onglet **Sauvegarder**. Pour plus d'informations concernant le module TPM, veuillez consulter la section Trusted Platform Module.

Sauvegarde de configuration

Via cet écran, vous allez pouvoir effectuer une sauvegarde de la configuration de votre firewall sous forme de fichiers, de manière exhaustive, et en protéger l'accès.

Nom donné à la sauvegarde : Par défaut, le nom de la sauvegarde proposé est « <numéro de série du firewall> jour_mois_année.na ». Ce nom est modifiable.

Télécharger la sauvegarde de configuration	Le fichier sera sauvegardé au format .na (Stormshield Network ARCHIVES). Cliquez sur ce bouton pour l'enregistrer.

Configuration avancée

Il est fortement recommandé de protéger le fichier de sauvegarde par un mot de passe robuste.

Mot de passe	Définissez un mot de passe pour protéger votre sauvegarde.
Confirmer	Confirmez le mot de passe de votre sauvegarde, 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 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 protégeant le TPM pour réaliser une sauvegarde de configuration.

Sauvegarde automatique de configuration

La sauvegarde périodique de votre configuration est maintenant proposée avec le service « Cloud backup ». Ces sauvegardes peuvent être stockées sur un serveur HTTP/HTTPS local ou externalisé, ou encore au sein de l'infrastructure proposée par le service **Stormshield Network Cloud backup.**

La sauvegarde périodique de votre configuration est effectuée de manière sécurisée.

NOTE

Il est recommandé de protéger le fichier de sauvegarde par un mot de passe qui devra être conservé soigneusement. En effet, ce dernier ne pourra être ni récupéré, ni réinitialisé par le support technique.

Les informations concernant la dernière sauvegarde automatique sont également disponibles dans le composant *Propriétés* du **Tableau de Bord.**

NOTE

Pour bénéficier du service, le Firewall doit être sous maintenance.

ON / OFF	Positionnez le sélecteur sur ON pour activer l'envoi périodique d'une sauvegarde de la configuration de votre firewall.

Voici les différents paramètres du service :

Choix du serveur de sauvegarde	**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, selon les critères choisis ci-après.
URL du serveur	Localisation utilisée pour le dépôt des sauvegardes. Cette URL est définie par la résolution du serveur Cloud ou du serveur personnalisé sélectionné ci-dessous combinée au chemin d'accès indiqué ci-après.	
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, qui peut être HTTP ou HTTPS. Le protocole HTTPS nécessite de renseigner un certificat afin que le firewall puisse s'assurer de l'identité du serveur.	

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. L'objectif est que le firewall puisse s'assurer de l'identité du serveur avant de lui transmettre la sauvegarde.
Chemin d'accès	Selon la méthode d'envoi sélectionnée ci-dessous, ce chemin d'accès des données sur serveur 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 (auth)	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.

Selon votre choix de sauvegarde par *Cloud auto-backup* ou sur un serveur personnalisé, vous pouvez sélectionner les paramètres suivants :

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	Si vous le souhaitez, il est possible de chiffrer votre fichier de configuration par un mot de passe. Il est recommandé de mettre un mot de passe complexe. **IMPORTANT** Il est recommandé de conserver ce mot de passe soigneusement, car sans celui-ci, toute restauration du fichier sera impossible. En effet, il n'est pas possible de changer ou réinitialiser ce mot de passe après la sauvegarde.
Mot de passe du fichier de sauvegarde	Ce bouton permet l'affichage d'une fenêtre d'édition d'un nouveau mot de passe. Ce nouveau mot de passe sera valable pour les prochaines sauvegardes uniquement.

Onglet « Restaurer »

Restauration de configuration

Cet écran va permettre de restaurer une sauvegarde précédemment effectuée.

Sauvegarde à restaurer :

Sauvegarde à restaurer	Cliquez sur le bouton à droite du champ (...) afin d'insérer le fichier de sauvegarde au format .na à restaurer.

Restaurer la configuration à partir du fichier de sauvegarde	Cliquez ensuite 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 au sein de l'onglet précédent, Sauvegarder, saisissez-le dans ce champ.

Modules à restaurer : il est possible d'effectuer une restauration totale ou partielle de la configuration de votre firewall.

Restaurer tous les modules du fichier de sauvegarde	Cette case est cochée par défaut, si vous choisissez de la maintenir ainsi, l'intégralité des modules contenus dans le fichier de sauvegarde seront restaurés.

Si vous souhaitez ne restaurer qu'une partie des modules du fichier de sauvegarde, décochez la case du dessus afin de dégriser les champs suivants.

Cochez ceux dont vous souhaitez restaurer la configuration parmi :

- Réseau (Interface, routage et DNS dynamique)
- Filtrage SMTP
- Filtrage URL
- Filtrage SSL
- Objets web
- Modules globaux
- Configuration sécurisée
- Active Update
- Services (SNMP, serveur DHCP)
- Profils d'inspection IPS
- Objets réseau
- Filtrage et NAT
- VPN IPSec
- Annuaire LDAP

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 du fichier de sauvegarde	Cliquez ensuite 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 au sein de l'onglet précédent, Sauvegarder, saisissez-le dans ce champ ; sans celui-ci, toute restauration du fichier sera impossible.

Onglet « Configuration »

Disque système

Il est question du disque système de votre firewall multifonction Stormshield Network.

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 va permettre d'obtenir des informations diverses sur votre firewall, au format « sysinfo ». Par son biais, il est possible de connaître, par exemple, le modèle du firewall, son numéro de série, son état de fonctionnement actuel et l'état sa mémoire.

MESSAGES DE BLOCAGE

L'écran de configuration du module **Messages de blocage** est composé de 2 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 *Page de blocage HTTP* : page affichée lors d'une tentative d'accès à un site non autorisé par les règles de filtrage.

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 HTTP »

Cette fenêtre présente par défaut la page de blocage HTTP qui est affichée lors d'une tentative d'accès à un site bloqué par les règles de filtrage URL. 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. 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 propose leur paramétrage via un menu déroulant **Modifier**. Les entrées sont les suivantes :

Modifier	Permet de personnaliser la page de blocage HTTP en modifiant le code HTML. Ce bouton fait apparaitre **deux onglets dédiés** en dessous de la fenêtre de blocage. Ces onglets proposent l'utilisation **d'un éditeur simplifié ou d'un éditeur HTML,** détaillés dans la section suivante**.**
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 email de notifications 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 dynamique 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**

Editeur simplifié

L'édition simplifiée propose une interface de type WYSIWYG et propose l'import d'une image.

Les actions sur la grille

Ajouter	Crée une nouvelle version de la page HTML. En cliquant sur ce bouton, une nouvelle ligne s'affiche vous permettant d'indiquer la langue et les différentes informations à afficher.
Supprimer	Supprime une version existante. Sélectionnez la ligne à supprimer puis cliquez.
Modifier l'image	Ce bouton permet de personnaliser la page de blocage en important une image. Seuls les formats JPG, GIF et PNG sont acceptés.
Langage par défaut	Ce champ sélectionne la version de la page à afficher, dans le cas où le navigateur n'a pas de langue spécifiée par défaut ou que la langue spécifiée dans le navigateur ne correspond pas à une déclinaison prévue dans la page.

La grille

Chaque ligne correspond à une langue du message de la page HTML et une version de l'éventuel notification email à l'administrateur (demande de déblocage d'accès).

Langage ID	Langage du message à afficher par la page HTML. Ce champ doit être un identifiant à deux caractères de pays valide (ISO 3166-1 alpha-2) pour être détecté par le navigateur.
Titre de la page	Titre affiché dans la fenêtre ou l'onglet du navigateur
Message de blocage	Un simple clic sur la cellule ouvre une fenêtre d'édition : une boite de saisie permet de renseigner la version du message de la page de blocage. Ce champ permet la saisie de balises HTML pour la mise en forme du texte.
E-mail de contact	Un simple clic sur la cellule ouvre une fenêtre d'édition : il est possible de renseigner le libellé du lien email à la fin du message. Si ce champ est vide, aucun email ne figurera sur la page. Le champ prévisualisation permet d'afficher le mail qui sera envoyé à condition qu'un client mail soit installé sur la machine. Les informations à renseigner sont l'email d'un ou deux destinataires, le sujet du mail et le message par une boite de saisie. Un encadré rappelle les variables utilisables.

Editeur HTML

La boite de saisie permet de copier l'intégralité du code HTML de la page de blocage en vue de le modifier. Il est également possible de coller le code d'une page HTML personnalisée.

Une image intégrée dans la page HTML, doit être encodée en base64 et contenue dans la balise image.

Ce code intègre les différentes versions du message de la page et des informations de la notification email.

OBJETS RÉSEAU

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 Noms autorisés.

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) clef(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 IP	Matérialisée par l'icône , cette option permet d'afficher uniquement les plages d'adresses IP.
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

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.

Réseau

Sélectionnez un réseau pour visualiser ou éditer ses propriétés. Ils possèdent chacun un nom, une IP et un masque réseau.

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.
Commentaire	Description associée au réseau sélectionné.

Adresse IP	Adresse IP du réseau sélectionné. L'adresse est suivie du symbole "/" et du masque de réseau associé.

Plage d'adresses IP

Sélectionnez une plage d'adresses IP 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.
Début	Première adresse IP associée à la plage.
Fin	Dernière adresse IP associée à la plage.
Commentaire	Description associée à la plage d'adresses IP sélectionnée.

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).

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.

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.
Editer ce groupe	Ce bouton comporte une boîte de dialogue d'ajout d'objet(s) au sein du groupe. Deux colonnes apparaissent : 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, sélectionnez-le dans la colonne de droite et cliquez sur cette flèche. **NOTE** En cliquant sur le bouton « Editer 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.

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.

Editer ce groupe	Ce bouton comporte une boite de dialogue permettant d'ajouter des port(s) 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 port(s) et en inclure de nouveaux au sein du groupe. Deux colonnes apparaissent : Celle de gauche comporte la liste de tous les ports que vous pouvez ajouter à votre groupe. La colonne de droite comporte les ports qui figurent déjà dans le groupe. Pour ajouter un port 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 port (en tête de la liste). Pour retirer un objet du groupe, sélectionnez-le dans la colonne de droite et cliquez sur cette flèche ←. **NOTE** En cliquant sur le bouton « Editer 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 ports figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

Routeur

Les objets routeurs peuvent être utilisés :

- Comme passerelle par défaut pour le firewall,
- Pour spécifier du routage au sein des règles de filtrage (PBR : Policy Based Filtering).

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.

Sélectionnez un routeur pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom donné à l'objet routeur lors de sa création.
Commentaire	Description associée à l'objet routeur.

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.

Appliquer	Envoie la configuration du routeur.
Copier	Permet de créer par duplication un nouvel objet routeur reprenant les mêmes caractéristiques.
Annuler	Annule la configuration du routeur.

Grilles des passerelles utilisées et des passerelles de secours

Ces deux grilles comportent les colonnes ci-dessous :

Machine (Obligatoire)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine composant le routeur.
Equipement(s) pour tester la disponibilité (Obligatoire)	Machine ou groupe de machines à tester (ping) 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.** **NOTE** Si la valeur **Pas de test de disponibilité** est sélectionnée pour l'ensemble des passerelles, la fonction de bascule vers les passerelles de backup est alors désactivée.
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.
Commentaire (Optionnel)	Texte libre.

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.

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.
Editer 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, sélectionnez-le dans la colonne de droite et cliquez sur cette flèche ←. **NOTE** En cliquant sur le bouton « Editer 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 pays et continents figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

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, il faudra cliquer sur « **Appliquer** » ou « **Sauvegarder** » pour enregistrer le changement.
Adresse IP	Adresse IP de l'objet sélectionné.
Commentaire	Description associée au nom DNS sélectionné.

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. **Exemple** : Pour un événement ponctuel : du <*date*> à <*heure*> au <*date*> à <*heure*>

L'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 ».

Le 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.

Les 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.

Les 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 WEB

Il existe deux types de catégorie d'URL et de certificats : des catégories personnalisées (entrées manuellement par l'administrateur) et des catégories dynamiques. Le fournisseur de Base d'URL mettant à disposition les catégories d'URL dynamiques, est par défaut Stormshield Network.

Ce module propose de créer des catégories d'URL ou de certificats personnalisés, et des groupes pouvant contenir des catégories personnalisée et dynamique. Ce module permet également de renseigner le fournisseur de Base d'URL.

Pour une catégorie donnée - par exemple « banks », dans laquelle seront rassemblées des URL des banques les plus consultées- il sera possible de créer une règle dans le module de **Filtrage URL** (**Politique de Sécurité\Filtrage URL**) pour en interdire l'accès.

Ainsi, lorsque vous tenterez de vous connecter au site web de votre banque, une page de blocage s'affichera, avec un message d'erreur. (Voir le module **Notifications\Messages de blocage**\onglet *Page de blocage HTTP*).

REMARQUE

Dans les politiques de filtrage, il est préférable d'utiliser les catégories dynamiques fournis par les bases d'URL, ceux-ci sont plus riches et plus performantes que les listes d'URL personnalisées.

Ce module se compose de 4 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.
- *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.
- *Groupe de catégories* : Propose de créer des groupes de catégories d'URL ou de certificats, parmi les catégories personnalisées ou dynamiques (Base d'URL).
- *Base d'URL* : Suivant le type d'option souscrite, les listes d'URL disponibles sont mises à jour par des fournisseurs différents (parmi Stormshield Network ou Stormshield Network Extended Web Control). Les listes d'URL Stormshield Network sont proposées par défaut.

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 personnalisées et de leur URL classées.

Grille de catégorie d'URL

L'écran URL se décompose en 2 parties : une première partie pour les Catégories personnalisées d'URL, une seconde partie pour les URL.

Vous pouvez, au niveau de la configuration des catégories, effectuer les actions suivantes :

Ajouter une catégorie personnalisée	Crée une nouvelle catégorie. En cliquant sur ce 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 ligne à supprimer puis cliquez. Un message de confirmation s'affiche et si la catégorie est utilisée, un message d'avertissement vous demande à nouveau ce que vous souhaitez faire.
Vérifier l'utilisation	Permet de vérifier si la catégorie sélectionnée au préalable est utilisée dans une configuration. Lorsque vous cliquez sur ce bouton, un panneau s'affiche au niveau de l'arborescence des modules et indique les modules qui utilisent cette catégorie.
Vérifier la classification d'une URL	Permet de vérifier si une URL appartient à une catégorie. Cette recherche s'effectue dans les catégories personnalisées et dynamiques également. Cela permet de déterminer s'il est nécessaire de l'ajouter à une catégorie. Lorsque vous cliquez sur ce bouton, un panneau apparait en bas de l'onglet et affiche les catégories qui contiennent cette URL.

La grille présente les éléments indiqués ci-dessous :

Groupe d'URL	Nom de la catégorie d'URL.
Commentaire	Description de la catégorie d'URL.

REMARQUE

Le nombre de caractères pour une catégorie d'URL est limité à 255.

Grille d'URL

Format

La liste des **Caractères autorisés** et les indications de syntaxe suivantes sont valables pour les URL uniquement. Les catégories d'URL ne sont pas concernées par ces restrictions de format.

La saisie d'un masque d'URL peut contenir des méta-caractères (wildcard) et comporter la syntaxe suivante:

*	Remplace une séquence de caractères quelconque. **Exemple :** *.compagnie.com/ permet de définir le domaine Internet de la société COMPAGNIE.
?	Remplace un caractère. **Exemple :** ???.compagnie.com est équivalent à www.compagnie.com ou de ftp.compagnie.com mais pas à www1.compagnie.com.

Un masque d'URL peut contenir une URL complète (**exemple** : www.compagnie.com*) ou des mots-clés contenus dans l'URL (**exemple** : *mail*).

Il est aussi possible de filtrer des extensions de fichiers :

Exemple : le masque d'URL '*.exe' peut servir à filtrer les fichiers exécutables.

Grille

Vous pouvez, au niveau de la configuration des URL, effectuer les actions suivantes :

Ajouter une URL	Ajoute une URL à une catégorie. Sélectionnez d'abord la catégorie dans laquelle vous voulez ajouter une URL dans la colonne de gauche, puis cliquez.
Supprimer	Supprime une URL à une catégorie. Sélectionnez d'abord la catégorie dans laquelle vous voulez supprimer une URL dans la colonne de gauche, puis cliquez.

La grille présente les éléments indiqués ci-dessous :

Nom de l'URL	Nom de l'URL. Il peut contenir des méta-caractères (wildcard)
Commentaire	Vous avez la possibilité d'ajouter un commentaire pour décrire chaque URL listée.

Onglet « Nom de certificat (CN) »

Cet écran propose de créer des catégories de nom de certificat, ce qui peut s'avérer utile pour le filtrage SSL (voir le module **Politique de Sécurité\Filtrage SSL).** Il est composé de 2 parties : une pour les catégories, une seconde pour les certificats.

Concernant les boutons, l'écran se présente de manière similaire à celui de l'onglet *URL*. La liste de droite contient ici des noms de certificats (CN) et d'éventuels commentaires associés.

La seule différence concerne les méta-caractères (wildcard) qui ont l'indication de syntaxe supplémentaire suivante :

Les caractères "*" et "?" ne sont autorisés qu'en début et suivi d'un "."
Exemple: *.compagnie.com

NOTE

Le nombre de caractères pour une catégorie de CN est limité à 255.

Onglet « Groupes de catégories »

Grille des groupes

Cet écran propose de créer des groupes de catégories d'URL ou de certificats.

- Un **Groupe de catégories URL** peut contenir des catégories personnalisées d'URL ou des catégories dynamiques (Base d'URL).
- Un **Groupe de catégories Certificats** peut contenir des catégories personnalisées de certificats ou des catégories dynamiques (Base d'URL).

Il est composé de 2 parties : une pour les groupes, une seconde pour le contenu des groupes.

Recherche	Le champ de recherche vous permet de trouver les groupes de catégorie par un mot ou par une lettre clé.
Filtre	Ce bouton permet de choisir le type d'objets à afficher. Un menu déroulant vous propose d'afficher uniquement les Groupes de catégories URL ou les Groupes de catégories Certificats.
Ajouter	Crée un nouveau groupe. En cliquant sur ce bouton, une fenêtre s'affiche. Celle-ci permet de choisir entre la création d'un Groupe de catégories URL ou un Groupe de catégories Certificats. Indiquez le nom du groupe et un éventuel commentaire dans les champs prévus à cet effet. La colonne de gauche liste les catégories personnalisées (d'URL ou de certificats) et les catégories dynamiques (Base d'URL) connues. Sélectionnez les catégories à intégrer au groupe dans la colonne de gauche et copiez-les à l'aide des flèches dans la colonne de droite listant les objets contenus dans le groupe.

Supprimer	Supprime un groupe existant. Sélectionnez la ligne à supprimer puis cliquez. Un message de confirmation s'affiche et si le groupe est utilisé, un message d'avertissement vous demande à nouveau ce que vous souhaitez faire.
Vérifier l'utilisation	Permet de vérifier si le groupe sélectionné au préalable, est utilisé dans une configuration. Lorsque vous cliquez sur ce bouton, un panneau s'affiche au niveau de l'arborescence des modules et indique les modules qui utilisent ce groupe.

Détails

Des champs proposent l'édition du Nom du groupe et de l'éventuel commentaire.

La grille repend l'ensemble des catégories personnalisées ou dynamiques contenues dans le groupe sélectionné dans la colonne de gauche. Le bouton **Editer ce groupe** affiche une fenêtre similaire à l'écran de création, permettant l'ajout ou la suppression de catégories au sein du groupe.

Onglet « Base d'URL »

Cet onglet permet de modifier le fournisseur de catégories d'URL/nom de certificat.

Suivant le type d'option souscrite (**Voir la politique tarifaire Stormshield Network en cours**), les listes d'URL disponibles sont mises à jour dynamiquement par un fournisseur de Base URL. Par défaut lorsqu'un service de maintenance "standard" est souscrit, ce sont les listes d'URL **Stormshield Network** qui sont proposées.

Le nouveau fournisseur **Extended Web Control** propose une base d'URL hébergée « dans le Cloud ». Ce filtrage d'URL a l'avantage d'avoir une qualité supérieure aux solutions embarquées.

Si vous avez souscrit l'option **Stormshield Network EWC**, pour activer la fonctionnalité de filtrage d'URL sur les listes d'URL **Extended Web Control,** sélectionnez l'entrée dans la liste des fournisseurs proposés.

Fournisseur de base d'URL	Par défaut, la base d'URL **Stormshield Network** est sélectionnée.

Le téléchargement des mises à jour des listes d'URL Stormshield Network s'effectue grâce au module **Active Update**. Ce module vous permet de modifier l'adresse des serveurs de mise à jour dans le cas d'utilisation de site miroir.

Un encadré situé sous la liste déroulante affiche des informations concernant les catégories d'URL du fournisseur en cours d'utilisation (noms des Catégories et leurs descriptions).

NOTE

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.

De même, 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 Stormshield Network Extended Web Control.

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).

Ces options n'étant pas supportées par le navigateur Internet Explorer en version 6, 7 et 8, il conseillé d'utiliser une version supérieure de ce navigateur. Toutefois, ce mode peut être désactivé par commande CLI (CONFIG AUTH HTTPS sslparanoiac=0 / CONFIG AUTH ACTIVATE).

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'IHM Web. 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.

REMARQUE

- 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 « Caps lock » 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>.

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

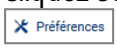
Pour vous déconnecter d'un firewall, suivez la procédure suivante :

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 votre interface web et de gagner en ergonomie et rapidité selon vos choix d'options.

Il est accessible en haut à droite de l'interface Web d'administration, via le menu déroulant portant l'identifiant de l'administrateur connecté.

Cliquez sur le nom de l'administrateur connecté (partie supérieure droite de l'écran) puis sur 

pour ouvrir ce module.

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 Vous pouvez également choisir de « Toujours rester connecté ».

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 (Filtrage, NAT, VPN IPSec et Objets)	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.
Commentaires des règles avec date de création (Filtrage et NAT)	En cochant cette case, les commentaires créés pour les règles de filtrage et de NAT intégreront automatiquement la date et l'heure de création.

Affichage de la politique de sécurité	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 essayera de déduire le nombre de règles par page, en fonction de votre configuration.

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.

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 connaissance Stormshield Network.
URL d'accès à la suite d'administration	Cette URL vous permet de télécharger la suite d'administration Stormshield Network soient : Monitor, Reporter, et GlobalAdmin.

Paramètres des traces

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.

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 commune à chaque profil

Configuration par défaut

Configuration pour le trafic entrant	Définissez le profil à appliquer pour le trafic entrant du réseau via le firewall Stormshield Network. Le trafic entrant représente le trafic d'une interface non protégée (comme Interner) vers une interface protégée (votre réseau local/interne).
Configuration pour le trafic sortant	Définissez le profil à appliquer pour le trafic sortant du réseau via le firewall Stormshield Network. 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\Alarmes**. En la cochant, les nouvelles alarmes se mettront à jour automatiquement et seront livrées avec la signature Stormshield Network. Les trois options suivantes seront grisées car vous aurez fait le choix d'une configuration automatique. Si vous souhaitez les appliquer vous-mêmes, décochez la case et définissez les paramètres des champs suivants.
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\Alarmes**. 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.

Configuration avancée

Appliquer les opérations de translation (NAT) avant le VPN IPSec	Cette option signifie que les adresses IP seront modifiées avant le chiffrement effectué par le VPN IPSec.

Considérer l'(es) interface(s) IPsec comme interne(s) (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.

Configurer les profils

Cet écran se compose de 2 parties :

- Une zone d'édition des différentes configurations de profils possibles
- Une zone d'association des profils protocolaires

Choisissez le profil applicatif associé au protocole en le sélectionnant au sein de la liste déroulante, à l'aide de la flèche à droite du champ.

Pour revenir au menu précédent cliquez sur le bouton « **Accéder à la configuration globale** ».

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

Editer	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. 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 connaitre 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 sécurisé : 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.

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.

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**.

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.

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.

ICQ – AOL IM (OSCAR)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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 OSCAR	Active ou désactive les logs permettant de tracer les requêtes OSCAR.

Live Messenger (MSN)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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.

IP

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 140 et 65535 octets.
Expiration d'une session (en secondes)	Cela doit être compris entre 2 et 30 secondes.

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.

Protection contre le déni de service

Nombre maximal de connections simultanées par machine source (0 désactive cette protection)	Cette option permet de limiter le nombre de connexions simultanées pour une même machine source. Lorsque la valeur choisie vaut 0, aucune restriction n'est appliquée. **AVERTISSEMENT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.
Nombre maximal de nouvelles connections par machine source dans l'intervalle de temps paramétré (0 désactive cette protection)	Cette option permet de limiter le nombre de nouvelles connexions initiées par une machine source dans un intervalle de temps déterminé. Lorsque la valeur choisie vaut 0, aucune restriction n'est appliquée. **AVERTISSEMENT** Le choix d'un nombre trop faible peut empêcher le fonctionnement de certaines applications ou l'affichage de pages Web.
Intervalle de temps pour la limitation des nouvelles connexions	Définissez l'intervalle de temps de référence pour le calcul du nombre de nouvelles connexions autorisées par machine source. Cette valeur doit être comprise entre 1 et 3600 secondes.

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 (valeur par défaut : 1800 secondes).
Connexion 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 3600 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 10 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.

BACnet/IP

Gestion des services

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, Object Access, Remote Device Management, Virtual Terminal et Security.

Les services avec confirmation BACnet/IP prédéfinis sont autorisés par défaut (action *Analyser*) et cette action peut être modifiée pour chacun d'entre eux. Les boutons **Bloquer par jeu de services**, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser* / *Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services BACnet/IP listés dans la grille.

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.

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 *Analyser*) et cette action peut être modifiée pour chacun d'entre eux. Le bouton **Modifier tous les services** permet de modifier l'action (*Analyser* / *Bloquer*) appliquée à l'ensemble des services BACnet/IP listés dans la grille.

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.

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.

CIP

Paramètres

Nombre max. 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 (*Analyser / Bloquer*) appliquée à chaque service peut être modifiée en cliquant dans la colonne **Action**. Le bouton **Modifier tous les services** permet de modifier l'action (*Analyser / Bloquer*) 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 *Analyser*). Ces services sont classifiés par groupe de services : Acknowledge Handler Object, Assembly Object, Connection Configuration Object, Connection Manager Object, Connection 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 et Time Sync Object.

Les boutons **Bloquer par jeu de services**, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) 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

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

Commandes publiques

Cette liste recense les commandes EtherNet/IP publiques autorisées par défaut par le firewall. L'action (*Analyser / Bloquer*) appliquée à chaque commande peut être modifiée en cliquant dans la colonne **Action**. Le bouton **Modifier toutes les commandes** permet de modifier l'action (*Analyser / Bloquer*) qui est appliquée à l'ensemble des commandes.

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 EtherNet/IP	Active ou désactive les logs permettant de tracer les requêtes EtherNet/IP.
Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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*: Informations système, Paramètres et Processus d'information.

Ces identifiants de type publiques sont autorisés par défaut (action *Analyser*). Les boutons **Bloquer par jeu de Type Id**, **Analyser par jeu de Type Id** et **Modifier tous les Type ID** permettent de modifier l'action (*Analyser / Bloquer*) 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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

MODBUS

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 (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 (*Analyser / Bloquer*) 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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

Onglet OPC AE (IPS)

Gestion des services OPC AE

Services prédéfinis

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 *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC AE listés dans la grille.

Onglet OPC DA (IPS)

Gestion des services OPC DA

Services prédéfinis

Cette grille recense les services OPC DA prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Client,
- OPC Group,
- OPC Server,
- OPC Type Library.

Les services OPC DA prédéfinis sont autorisés (analysés) par défaut (action *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC DA listés dans la grille.

Onglet OPC HDA (IPS)

Gestion des services OPC HDA

Services prédéfinis

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 *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) 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 *Analyser*). Les boutons **Bloquer par jeu de services**, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) 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 (*Analyser / Bloquer*) 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 (*Analyser / Bloquer*) 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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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 *Analyser*). Les boutons **Bloquer par jeu d'opérations**, **Analyser par jeu d'opérations** et **Modifier toutes les opérations** permettent de modifier l'action (*Analyser* / *Bloquer*) 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.

UMAS

Le protocole UMAS (Unified Messaging Application Services) est la propriété intellectuelle de la société Schneider Electric.

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 **Bloquer par groupe de fonctions** et **Analyser par groupe de fonctions** permettent de modifier l'action (*Analyser / Bloquer*) 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 MS-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 RPC services.
- Microsoft Scheduler.

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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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)

Gestion des services OPC AE

Services prédéfinis

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 *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser* / *Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC AE listés dans la grille.

Onglet OPC DA (IPS)

Gestion des services OPC DA

Services prédéfinis

Cette grille recense les services OPC DA prédéfinis dans le firewall. Ces services sont classifiés par jeu de service:

- Component Categories,
- OPC Client,
- OPC Group,
- OPC Server,
- OPC Type Library.

Les services OPC DA prédéfinis sont autorisés (analysés) par défaut (action *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC DA listés dans la grille.

Onglet OPC HDA (IPS)

Gestion des services OPC HDA

Services prédéfinis

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 *Analyser*). Les boutons **Bloquer par jeu de service**s, **Analyser par jeu de services** et **Modifier tous les services** permettent de modifier l'action (*Analyser / Bloquer*) appliquée au jeu de services sélectionné ou à l'ensemble des services OPC HDA listés dans la grille.

NetBios CIFS

NetBios est un protocole utilisé pour le partage de fichier/imprimantes, généralement par les systèmes Microsoft.

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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.

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

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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 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.

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.

Commandes RTSP

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**.

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

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 ...).

Détection automatique du protocole	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage.

Commandes SIP

Commandes SIP 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**.

Commandes SIP 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)

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.

DNS

L'écran des profils

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)

Cette liste contient les noms de domaines autorisés (de type <*www.dedomaine.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**.

Types d'enregistrements DNS

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 (*Analyser / Bloquer*) appliquée à un type DNS peut être modifiée en cliquant dans la colonne *Action* correspondant à ce type.

Le bouton **Modifier toutes les opérations** permet de modifier l'action (*Analyser / Bloquer*) appliquée à l'ensemble des types DNS.

Types additionnels à interdire

Cette liste permet de bloquer 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

Onglet « IPS »

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.

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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

Commandes principales

Bouton **Modifier les commandes d'écriture :** Ce bouton permet de passer sans analyser bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur, ceci, pour les commandes d'écriture.

Bouton **Modifier toutes les commandes :** Ce bouton permet de passer sans analyser, bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur, ceci, aussi bien pour les commandes génériques que les commandes de modification.

Commande	Nom de la commande.
Action	3 autorisations possibles entre « Passer sans analyser », « Analyser » et « Bloquer ».
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 laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Autres commandes autorisées

Il est possible d'**Ajouter** des commandes supplémentaires, dans la limite de 21 caractères, et de les **Supprimer** si besoin.

IPS

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.

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

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.

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. La taille positionnée par défaut dépend du modèle de firewall : • Firewalls modèle S (SN160(W), SN210(W) et SN310) : 4000 Ko. • Firewalls modèle M (SN510, SN710 et SNi40) : 4000 Ko. • Firewalls modèle L (SN910) : 8000 Ko. • Firewalls modèle XL (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100) : 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 : « Passer » et « Bloquer ». En sélectionnant « Bloqué », le fichier analysé n'est pas transmis. En sélectionnant « Passer », 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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 de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**

Onglet « Analyse sandboxing»

Sandboxing

Etat	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 quatre types de fichiers: • **Archive** : sont inclus les principaux types d'archives (zip, arj, lha, rar, cab…) • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous windows (fichiers avec extension ".exe",".bat",".cmd",".scr", …). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Flash** (fichiers avec extension ".swf"). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar").
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.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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 **Passer** ou **Bloquer.** 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. • **Bloquer** : le téléchargement partiel est interdit • **Bloquer si l'antivirus est actif** : le téléchargement partiel est autorisé sauf si le flux correspond à un trafic inspecté par une règle avec analyse antivirale. • **Passer** : le téléchargement partiel est autorisé mais il n'y a pas d'analyse antivirale effectuée.
Taille maximale d'un fichier [0-2147483647 (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.
URLs 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)

Etat	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. • **Passer sans analyse des fichiers** : Le fichier peut être téléchargé librement, aucune analyse antivirale n'est effectuée. • **Bloquer** : 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)	Ce champ correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. La taille positionnée par défaut dépend du modèle de firewall : • Firewalls modèle S (SN160(W), SN210(W) et SN310) : 4000 Ko. • Firewalls modèle M (SN510, SN710 et SNi40) : 8000 Ko. • Firewalls modèle L (SN910) : 16000 Ko. • Firewalls modèle XL (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100) : 32000 Ko.

Actions sur les fichiers

Lorsqu'un virus est détecté	Ce champ contient 2 options. En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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 de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**. **Exemple :** Si le disque dur est plein, le téléchargement des informations ne pourra pas être effectué.

Onglet « Analyse sandboxing»

Sandboxing

Etat	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 quatre types de fichiers: • **Archive** : sont inclus les principaux types d'archives (zip, arj, lha, rar, cab…) • **Document bureautique (logiciels Office)** : tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable** : fichiers exécutables sous windows (fichiers avec extension ".exe",".bat",".cmd",".scr", …). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Flash** (fichiers avec extension ".swf"). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar").

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.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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 analysées et 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 (valeur par défaut: 20 minutes), 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) .

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 générale

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.

L'action (*Analyser / Bloquer*) appliquée à chaque mode peut être modifiée à l'aide d'un double-clic dans la colonne action correspondante.

Configuration avancée

Reference Id interdites

Cette liste permet de bloquer des Reference Id NTP additionnelles (LOCL, LCL...) en précisant leur nom. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Onglet « IPS - NTP v2»

Configuration générale

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.

L'action (*Analyser / Bloquer*) appliquée à chaque mode peut être modifiée à l'aide d'un double-clic dans la colonne action correspondante.

Configuration avancée

Reference Id interdites

Cette liste permet de bloquer des Reference Id NTP additionnelles (LOCL, LCL...) en précisant leur nom. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Onglet « IPS - NTP v3»

Configuration générale

Taille maximale des paquets (octets)	Renseignez la taille maximale autorisée pour les paquets NTP v3 (valeur par défaut: 72 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.

L'action (*Analyser / Bloquer*) appliquée à chaque mode peut être modifiée à l'aide d'un double-clic dans la colonne action correspondante.

Configuration avancée

Reference Id interdites

Cette liste permet de bloquer des Reference Id NTP additionnelles (LOCL, LCL...) en précisant leur nom. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Onglet « IPS - NTP v4»

Configuration générale

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.

L'action (*Analyser / Bloquer*) appliquée à chaque mode peut être modifiée à l'aide d'un double-clic dans la colonne action correspondante.

Configuration avancée

Gestion des Reference Id

Cette grille permet de placer en liste noire ou liste blanche des Reference Id NTP additionnelles (LOCL, LCL...).

Cliquez sur le bouton **Block All** pour déplacer toutes les Reference Id NTP prédéfinies de la liste blanche vers la liste noire.

Il est également possible 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 et cliquez sur le bouton **Supprimer**.

Paquets Kiss of death

Cette grille permet de placer en liste noire ou liste blanche des Reference Id NTP additionnelles pouvant être impliquées dans les attaques de type Kiss of Death (DENY, RSTR, RATELCL...).

Cliquez sur le bouton **Block All** pour déplacer toutes les Reference Id NTP prédéfinies de la liste blanche vers la liste noire.

Il est également possible 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 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.

IPS

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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

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 **Modifier toutes les commandes :** Permet d'autoriser, de rejeter ou de vérifier toutes les commandes.

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 : • **Analyser** : 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. • **Passer sans analyser** : la commande est autorisée, sans vérification. • **Bloquer** : la commande est bloquée d'office, une alarme sera remontée pour le stipuler. • **Javascript** (fichiers avec extension ".js")

Autres commandes autorisées

Commande	Ce champ permet d'ajouter des commandes personnelles supplémentaires.

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 positionnée par défaut dépend du modèle de firewall : • Firewalls modèle S (SN160(W), SN210(W) et SN310) : 4000 Ko. • Firewalls modèle M (SN510, SN710 et SNi40) : 4000 Ko. • Firewalls modèle L (SN910) : 8000 Ko. • Firewalls modèle XL (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100) : 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 « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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 de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**.

Onglet « Analyse sandboxing»

Sandboxing

Etat	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 quatre types de fichiers attachés en pièce-jointe: • **Archive** : sont inclus les principaux types d'archives (zip, arj, lha, rar, cab…) • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous windows (fichiers avec extension ".exe",".bat",".cmd",".scr", …). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Flash** (fichiers avec extension ".swf"). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar").
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.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. En sélectionnant **Bloquer**, le fichier analysé n'est pas transmis. En sélectionnant **Passer**, 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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 SEISMO 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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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 de notification de sens de connexion ATRN et ETRN	Permet de filtrer les données contenues dans la demande de notification 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 [64 – 4096]	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.)
Ligne de réponse serveur [64 – 4096]	Nombre maximum de caractères que peut contenir la ligne de réponse du serveur SMTP.
Données Exchange (XEXCH50) [102400 – 1073741824]	Taille maximale des données lors d'un transfert de fichier au format MBDEF (Message Database Encoding Format).
En-tête de l'extension BDAT [102400 – 10485760]	Taille maximale des données transmises via la commande BDAT.
Ligne de commande [64 – 4096]	Taille maximale des données que peut contenir une ligne de commande (en dehors de la commande DATA).

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.
Ligne de message [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 maximum du message [0 – 2147483647 (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.

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

Commandes principales

Bouton **Modifier toutes les commandes** : Permet d'autoriser, de rejeter ou de vérifier toutes les commandes.

Commande	Indication du nom de la commande.
Action	Indication de l'action effectuée.

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

Commandes SMTP autorisées

Liste des commandes SMTP supplémentaires autorisées. Il est possible d'en **Ajouter** ou d'en **Supprimer**.

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)	La taille positionnée par défaut dépend du modèle de firewall : • Firewalls modèle S (SN160(W), SN210(W) et SN310) : 4000 Ko. • Firewalls modèle M (SN510, SN710 et SNi40) : 4000 Ko. • Firewalls modèle L (SN910) : 8000 Ko. • Firewalls modèle XL (EVA1, EVA2, EVA3,EVA4, EVAU, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100) : 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 : « Passer » et « Bloquer ». En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier même s'il est détecté comme infecté.
Lorsque l'antivirus ne peut analyser	L'option **Passer sans analyser** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer 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»

Sandboxing

Etat	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 quatre types de fichiers attachés en pièce-jointe: • **Archive** : sont inclus les principaux types d'archives (zip, arj, lha, rar, cab…) • **Document bureautique (logiciels Office)**: tous les types de documents pouvant être ouverts avec la suite MS Office. • **Exécutable**: fichiers exécutables sous windows (fichiers avec extension ".exe",".bat",".cmd",".scr", …). • **PDF**: fichiers au format *Portable Document Format* (Adobe). • **Flash** (fichiers avec extension ".swf"). • **Java** (fichiers compilé java. Exemple : fichiers avec extension ".jar").
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.

Action sur les fichiers

Lorsqu'un malware connu est identifié	Ce champ contient 2 options. En sélectionnant **Bloquer**, le fichier analysé n'est pas transmis. En sélectionnant **Passer**, 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 **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

SNMP

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 (*Analyser / Bloquer*) 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

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.

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

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.

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

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.

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, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

SSL

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,...).

AVERTISSEMENTS

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.

Le navigateur Internet Explorer en version 7 ou 8 n'active pas, par défaut, le support du protocole TLS 1.0. Pour des raisons de sécurité, il est donc recommandé d'activer le support de TLS 1.0 via un objet Active Directory définissant les configurations machines (group policy object ou GPO).

La validation par un serveur ICAP des requêtes HTTPS déchiffrées par le proxy SSL n'est pas supportée.

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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.

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.

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.
- **Bloquer** : 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.
- **Bloquer** : 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.
- **Bloquer** : 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. • **Bloquer** : 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. • **Bloquer** : 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. • **Bloquer** : 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 **Bloquer le trafic** ou de **Passer sans 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 **Passer sans déchiffrer** ou **Bloquer**. Si un certificat n'est pas répertorié dans une catégorie de certificat, cette action détermine si le trafic est autorisé ou non.

TFTP

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, l'inspection sera automatiquement appliquée à la découverte d'un trafic correspondant, autorisé par le filtrage.

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.
Etat	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)

L'écran de configuration de la qualité de service se compose d'un écran unique.

Trafic réseau

Un élément important dans la "Qualité de Service" est de résoudre le problème du niveau généralement très haut du taux de perte de paquets sur l'Internet. En effet lorsqu'un paquet est perdu avant d'atteindre sa destination, toutes les ressources mises en œuvre lors de son transit sont gâchées. Dans certain cas, cette situation peut même amener une situation de congestion grave qui parfois entraîne la paralysie totale des systèmes.

On est loin de la nécessité de stabilité et de "temps réel" des applications de vidéoconférence d'aujourd'hui. Le contrôle optimisé des situations de congestion et la gestion des queues de données deviennent un enjeu important de la "Qualité de Service".

Les firewalls Stormshield Network disposent de deux algorithmes pour leur traitement des congestions, l'algorithme **TailDrop** et l'algorithme **BLUE.** Stormshield Network recommande toutefois l'utilisation de l'algorithme BLUE comme algorithme de traitement des congestions.

Traitement en cas de saturation	Cette option permet de définir l'algorithme de traitements des congestions. Elle a comme objectif d'éviter les ralentissements.

REMARQUE

Le réglage de la File d'attente par défaut a été retiré de l'interface d'administration web, car cela pouvait activer la QoS sur toutes les interfaces du Firewall. Cette option est conservée en réglage avancé par commande CLI serverd.

Cette option permet de sélectionner, parmi les files d'attente définies, laquelle sera la file d'attente par défaut. Plus exactement, cette option permet de choisir la façon dont le trafic par défaut (qui ne correspond à aucune queue) sera traité par rapport au reste. Par défaut, ce trafic est prioritaire sur le trafic traité par la QoS (« Prioritaire sur tout »), mais il est possible de soumettre le trafic à une certaine queue, en la sélectionnant dans cette liste déroulante.

Réservation ou limitation de la bande passante (CBQ)

Bande passante totale	La valeur de référence en Kbits/s ou en Mbits/s permet d'indiquer une référence sur laquelle seront basées les limitations de bande passante indiquée en pourcentage dans la configuration des files d'attente.

IMPORTANT

Cette valeur limitera l'ensemble des flux soumis à la QoS. La somme de tous les flux passant par la QoS ne pourra pas dépasser cette valeur et les paquets réseau excédentaires seront éliminés. Il est donc important de positionner une valeur de référence en adéquation avec le débit de l'interface réseau concernée.

Les paquets « ACK » et « low delay » DSCP sont traités avec une meilleure priorité par défaut (afin d'accélérer le transfert de données à travers une bande passante limitée).

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, cliquez sur le bouton **Ajouter une file d'attente**, puis sélectionnez **Réservation ou limitation de bande passante (CBQ).** Une ligne est ajoutée à la grille dans laquelle vous pouvez effectuer vos modifications.

Modification d'une file d'attente par classe d'application ou d'affectation

Nom	Nom de la file d'attente à configurer.
Type	Type de file d'attente parmi surveillance (MONQ), priorité (PRIQ), réservation/limitation (CBQ)
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 faible) à 1 (priorité la plus haute).
Bp min	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 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 **Min inv**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Min inv**. En modifiant la valeur de **Min inv**, 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, en Mbits/s, en 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 **Max inv**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Max inv**. En modifiant la valeur de **Max inv**, les valeurs sont différentes et donc désynchronisées.
Min inv.	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 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 **Max inv.**, 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 ».
Max inv.	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, en Mbits/s, en 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.
Couleur	Couleur de différentiation de la file d'attente.
Commentaire	Commentaire associé.

REMARQUE

Lorsque vous sélectionnez 0 dans la colonne « Bpmin » 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 par une file de surveillance.

La grille du menu File d'attente par classe d'application ou d'affectation affiche les différentes files d'attente qui ont été configurées. Un clic sur le bouton **Vérifier l'utilisation** permet d'afficher (dans la barre de navigation à gauche, 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, cliquez sur le bouton **Ajouter** une file d'attente puis sélectionnez **Surveillance du trafic (MONQ).**

Modification d'une surveillance du trafic

Nom	Nom de la file d'attente à configurer.
Type	Type de file d'attente parmi **CBQ**, **PRIQ** ou **MONQ**.
Couleur	Couleur de différenciation de la file d'attente.
Commentaire	Commentaire associé.

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 1 et 7. La priorité 1 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, cliquez sur le bouton **Ajouter une file d'attente**, puis sélectionnez **Traitement par priorité (PRIQ).**

Une ligne est ajoutée à la grille dans laquelle vous pouvez effectuer vos modifications.

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	Type de file d'attente parmi **CBQ**, **PRIQ** ou **MONQ**.
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 faible) à 1 (priorité la plus haute).
Couleur	Couleur de différenciation de la file d'attente.
Commentaire	Commentaire associé.

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	SN510, SN710, SN910	SN2000, SN2100, SN3000, SN3100, SN6000, SN6100
20	100	255

Cas d'application et recommandations d'utilisation

Exemple 1 : Priorisation des flux DNS

Basées sur UDP, les requêtes DNS subissent de nombreuses pertes de paquets du fait de la définition même du protocole UDP. Celui-ci ne prévoit pas de mécanismes de gestion des erreurs de transmission et l'écrasante présence des trafics TCP noient les trafics UDP dans la masse des paquets TCP.

Pour préserver ces trafics, et en particulier les flux DNS, il est recommandé de prévoir une règle de QoS de type "priorité" (PRIQ). Elle permettra de diminuer les trop fréquentes pertes de paquets et la latence qu'il pourrait y avoir sur ce type de trafic qui demande une réactivité importante (c'est d'ailleurs pour cette raison que les requêtes DNS sont réalisées sur UDP).

Définition de la règle de QoS pour le DNS

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par priorité (1 Item)								
QoS_DNS		1						Priorisation flux DNS

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la QoS dans l'onglet *Filtrage*, du module Filtrage et NAT, double-cliquez dans la colonne Action une fois votre règle de filtrage établie (voir document Filtrage et NAT ou menu Politique de Sécurité\module Filtrage et NAT\colonne Action).

Effets sur le trafic

- Baisse voire absence de paquets perdus si la règle est en priorité 1 (et qu'elle est la seul dans ce cas).
- Diminution de la latence.

Exemple 2 : Limitation du trafic HTTP

Parmi les trafics internet, les flux HTTP sont les plus gros consommateurs de la bande passante du lien Internet et du réseau local. Une utilisation importante de l'internet peut entraîner des problèmes de congestions du trafic réseau, les performances globales sont dégradées et l'utilisation du réseau devient fastidieuse.

Pour remédier à cet état de fait, il est recommandé de **limiter le trafic HTTP au moyen d'une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit maximum autorisé**. Elle permettra de préserver la bande passante du réseau et réduire l'impact de l'utilisation de l'internet sur les performances globales du réseau.

Définition de la règle de QoS pour le HTTP

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par classe d'application ou d'affectation (1 Item)								
QoS_HTTP			0kb	512kb	0kb	512kb		Limitation trafic HTTP

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la **QoS** dans l'onglet *Filtrage*, du module **Filtrage et NAT**, double-cliquez dans la colonne **Action** une fois votre règle de filtrage établie (voir document *Filtrage et NAT* ou menu **Politique de Sécurité**\module **Filtrage et NAT**\colonne Action).

Effets sur le trafic

- Diminution du risque de congestion du réseau.
- Réduction de l'impact du trafic sur les performances générales du réseau.

Exemple 3 : Garantie d'un niveau de service minimum

Certaines applications (VoIP par exemple) nécessitent un niveau de services avec la garantie que ce niveau de services sera respecté sous peine de disfonctionnement du service (impossibilité de suivre une conversation VoIP par exemple). Les autres applications et leur impact sur les performances générales du réseau peuvent perturber l'obtention du niveau de services requis.

Pour s'assurer que le niveau de services requis sera maintenu il est recommandé de créer une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit minimum garanti. Elle permettra de garantir un niveau de service pour un trafic donné indépendamment de l'impact des autres trafics sur les performances globales du réseau et sans définir de limitation de bande passante pour ces autres trafics.

Définition de la règle de QoS pour la VoIP

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par classe d'application ou d'affectation (1 Item)								
QoS_VoIP			1kb	0kb	100kb	0kb		Garantie service minimum

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la **QoS** dans l'onglet *Filtrage*, du module **Filtrage et NAT**, double-cliquez dans la colonne **Action** une fois votre règle de filtrage établie (voir document *Filtrage et NAT* ou menu **Politique de Sécurité**\module **Filtrage et NAT**\colonne Action).

Effets sur le trafic

- Garantie d'une bande passante pour un trafic donné.
- Introduction d'un temps de réponse maximal pour le transfert des données du service.

RAPPORTS

Ce menu n'est affiché que lorsque les rapports sont activés sur le firewall (module **Configuration des rapports**).

Le module Rapports présente des rapports de type "Top 10" dans les catégories **Web, Sécurité, Virus, Vulnérabilité et Spam**. Vous pouvez ainsi visualiser l'utilisation de l'accès Internet, les différentes attaques bloquées par votre Firewall et les machines vulnérables de votre société. De nombreuses interactions vous permettent d'agir directement sur la configuration de votre 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 "Accès complet aux logs (données sensibles)" en cliquant sur **Obtenir le droit d'accès aux données personnelles (logs)** dans le menu déroulant situé sous le nom du compte connecté (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 **Accès complet aux logs (données sensibles)** 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 "Accès complet aux logs (données sensibles)" génère une entrée dans les logs.

Collaborative security

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**.

Support de stockage : Carte SD

La fonctionnalité de **Stockage externe des traces sur carte SD** est disponible pour les firewalls modèles SN160(W), SN210(W) et SN310. Cette fonctionnalité est proposée en souscrivant à l'option « External storage ».

Le type de carte SD doit être au minimum de **Classe 10 (C10) UHS Classe 1 (U1) ou App Performance (A1)** 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.

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 maximum de mémoire supportée est de 2 To.

NOTE

Le stockage sur support externe s'effectue uniquement sur carte SD. 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 les Guides **PRÉSENTATION ET INSTALLATION DES PRODUITS NETASQ SÉRIE U - Modèles S** ou **PRÉSENTATION ET INSTALLATION DES PRODUITS STORMSHIELD NETWORK Gamme SN** disponibles sur le site de Documentation Technique Stormshield.

Rapports d'activités

Les rapports sont présentés sous forme d'Histogrammes ou de Camembert et 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.

Les actions

Echelle 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.

Le bouton permet d'accéder à 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.

Le 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.*

	Affichage des données sous forme d'histogramme horizontal
	Affichage des données sous forme d'histogramme vertical
	Affichage des données sous forme de diagramme circulaire

La période analysée est ensuite affichée.

La légende

Un tableau composé de 6 colonnes reprend la description des données affichées. Les informations sont les suivantes :

- Une numérotation précise le classement selon la valeur,
- Une lettre et une couleur permettent de référencer la valeur lorsque les textes sont trop longs pour être affichés (graphique en barres verticales et en camembert),
- Le nom complet de la donnée est affiché,
- La colonne affiche le pourcentage que la donnée représente pour ce top,
- La colonne affiche la valeur de quantité,
- Cette colonne permet un bouton d'état qui affiche ou masque les données. La catégorie « Autres » - représentant les données autres que celles du Top10 - est masquée par défaut. L'état Masqué/Affiché est conservé dans les préférences de l'application.

Selon les rapports, des colonnes supplémentaires peuvent être ajoutées au tableau de légende proposant certaines informations ou interactions en rapport avec les valeurs affichées (exemple : action d'une alarme).

Interactions

Un clic gauche sur une valeur présentée dans un rapport affiche un menu déroulant proposant certaines 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 la partie des Traces.

Tous les éléments d'un diagramme propose l'actions de **Rechercher cette valeur dans les traces :** cette recherche est effectuée dans la partie **Traces**, sur la totalité des traces, en conservant la période consultée et avec comme critère de recherche la valeur de l'élément sélectionné dans le rapport. Cette action est proposée pour l'ensemble des valeurs à l'exception de certaines recherches spécifiques, citées ci-après.

S'il s'agit d'une **adresse IP**, les actions possibles seront :

- Ajouter la machine à la base objet: via une fenêtre de dialogue, la machine peut être ajoutée à la base Objet et ajoutée à un groupe préalablement établi. Cela dans le but d'appliquer à l'objet, une politique de filtrage particulière (zone de mise en quarantaine*)

* Consultez la Technical Note « Sécurité collaborative » pour construire une politique avec zone de remédiation.

Un **nom de domaine** propose les actions supplémentaires suivantes :

- Accéder à l'URL : cette action affiche l'URL dans un nouvel onglet.
- Afficher la Catégorie d'URLs : cette action affiche dans une fenêtre, la catégorie à laquelle le domaine appartient.
- Ajouter l'URL à un groupe : cette action affiche une fenêtre permettant d'ajouter directement l'URL à un groupe d'URL existant.

Voici ci-dessous les interactions particulières selon les rapports :

WEB : Rapport Top des Recherches Web

Effectuer cette recherche via Google : cette action lance dans un nouvel onglet, la recherche des mots-clé dans le moteur de recherche Google.

SECURITE : Rapport Top des alarmes les plus fréquentes

- **Définir l'action de (Autoriser/ Interdire)** : cette modification est effectuée sur le profil concerné par le flux ayant généré l'alarme.
- **Définir le niveau à (Majeur/ Mineur / Autoriser)** : cette modification est effectuée sur le profil concerné par le flu x ayant généré l'alarme.
- **Afficher l'aide** : ce lien renvoie vers la page d'aide de l'alarme levée ou de la vulnérabilité détectée.
- **Rechercher cette valeur dans les traces** : cette recherche est effectuée dans la partie Traces, sur la totalité des traces et en conservant la période consultée.

VULNÉRABILITÉS

Rapport Top des machines les plus vulnérables

- Cliquez pour afficher les vulnérabilités subsistantes pour cette machine : les vulnérabilités subsistantes pour cette machine à cet instant précis sont affichées. En effet, une vulnérabilité remontée à un instant donné peut avoir été résolue au moment de la consultation des rapports. Vous pouvez également vérifier l'état actuel des vulnérabilités via Realtime Monitor.
- Rechercher cette machine dans le journal des Vulnérabilités : cette recherche est effectuée dans la partie Traces, dans la vue Vulnérabilités et en conservant la période consultée.

Rapport Top des vulnérabilités Client et Top des vulnérabilités Serveur

- Afficher les machines présentant cette vulnérabilité : les machines concernées à cet instant précis et leur version de l'application ou du service vulnérable sont affichées. En effet, une vulnérabilité remontée à un instant donné peut avoir été résolue au moment de la consultation des rapports. Vous pouvez également vérifier l'état actuel des vulnérabilités via Realtime Monitor.
- Afficher l'aide : ce lien renvoie vers la page d'aide de l'alarme levée ou de la vulnérabilité détectée.
- Rechercher cette valeur dans les traces : cette recherche est effectuée dans la partie Traces, dans la vue Vulnérabilités et en conservant la période consultée.

Les 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.

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.

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.

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*).

Top des sites Web par volume échangé

Ce rapport se base sur les volumes de données échangées, en émission comme en réception.

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.

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.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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*).

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.

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*).

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

SECURITE

Les rapports *Alarmes* se basent sur les alarmes **Applications et protections** (menu *Protection applicative*) et les **Evénements système** (menu *Notifications*).

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.

Top des alarmes les plus fréquentes

Ce rapport affiche les alarmes les plus fréquentes levées lors de l'analyse du trafic par le Firewall.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

Top des sessions Administrateurs

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.

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.

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 **Accès complet aux logs (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.

VIRUS

L'inspection **Antivirus** est requise pour ces analyses.

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 (http://www.securelist.com).

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 (http://www.securelist.com).

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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 (voir le Module **Management des vulnérabilités** de l'interface d'administration). L'analyse porte

donc sur les machines appartenant aux réseaux internes, identifiées par le nom DNS (fqdn) ou à défaut l'adresse IP.

Pour plus de détails sur les profils et les familles de vulnérabilités, consultez la section **Management des vulnérabilités** de ce guide.

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.

Il contient des données personnelles et nécessite donc l'obtention du droit **Accès complet aux logs (données personnelles)** pour être visualisé.

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*.

Top des vulnérabilités Serveur

Ce rapport remonte toutes les vulnérabilités détectées avec une cible *Serveur,* qui ont un degré de sévérité « 2 » (Moyen), « 3 » (Elevé) ou « 4 » (Critique). Celles-ci incluent les vulnérabilités qui qui ont à la fois des cibles *Client* et *Serveur*.

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.

RESEAU

L'activité analysée dans la catégorie RESEAU 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.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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.

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.

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.

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.

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.

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.

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.

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.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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.

Réseau industriel

L'activité analysée dans la catégorie RESEAU 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.

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.

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.

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.

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.

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.

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.

Top des fichiers malveillants détectés suite à l'analyse sandboxing

Ce rapport présente les fichiers malveillants les plus souvent détectés par l'analyse sandboxing.

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.

Top des types de fichiers les plus fréquemment analysés

Ce rapport présente les types de fichiers les plus souvent envoyés pour une 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 **Accès complet aux logs (données personnelles)** pour être visualisé.

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.

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 **Accès complet aux logs (données personnelles)** pour être visualisé.

REGLES 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	État de la règle : **Activé**/ **Désactivé** : Cliquez dans la case pour activer / désactiver la création d'une ou plusieurs règles implicites. La règle **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces externes (non protégées (Auth_ext)** est désactivée par défaut.
Nom	Nom de la règle implicite : celui-ci n'est pas modifiable.

Les règles suivantes figurent dans la colonne « **Nom** » :

- **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.
- **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 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.
- **Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster H.A)** : cela permet aux différents membres du cluster HA de communiquer entre eux.
- **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 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 le Stormshield Network Real-Time Monitor.
- **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 ISAKMP (port 500 UDP) et le protocole ESP pour les correspondants VPN IPSec**: 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 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 l'écran **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 le port HTTPS :** les connexions relatives à l'établissement de tunnel VPN SSL sont autorisées sur le port HTTPS.
- **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.

AVERTISSEMENTS

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 utilisant le port 1300, à savoir Stormshield Network RealTime Monitor, GlobalAdmin, Stormshield Network Centralized Management et Stormshield Network Event Analyzer.
- **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

Majeures [0-20]	Réglez le curseur afin de définir le poids des alarmes majeures émises par une machine dans le calcul de sa réputation.
Mineures [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

Malicieux [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 trois parties :

- Routage statique : 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 Bird : 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: 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.

L'onglet « Routes statiques »

Cet onglet correspond à la liste des routes statiques dont le nombre maximum varie selon le modèle :

SN160(W)	SN210(W)	SN310	SN510	SN710	SN910	SN2000 SN2100	SN3000 SN3100	SN6000 SN6100
512	512	512	2048	2048	5120	10240	10240	10240

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 Stormshield Network 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 Stormshield Network ne sait pas laisser passer les paquets possédant une adresse de destination différente de celles directement reliées au firewall. Vous pourrez communiquer entre les machines sur les réseaux internes, externes ou DMZ, mais aucun autre réseau (dont Internet). Il est désormais possible de choisir un objet routeur comme passerelle par défaut. 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.

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). Utilisez 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 :

- 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 encore un groupe.
Plan d'adressage	Adresse IP ou groupe d'adresses liés aux éléments de la colonne « Réseau source (objet machine, réseau ou groupe) ».
Interface(Obligatoire)	Une liste déroulante permet de sélectionner une interface parmi Ethernet, Vlan, dialup et IPSec.
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(Optionnel)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine (routeur).
Couleur(Optionnel)	Une fenêtre s'affiche permettant de sélectionner une couleur d'interface (utilisée dans Stormshield Network REALTIME MONITOR).
Commentaire (Optionnel)	Texte libre.

L'onglet « Routage dynamique »

Bird prend en charge les versions suivantes de protocoles de routage dynamique:

- Ripv2
- OSPFv2 pour IPv4 et OSPFv3 pour IPv6
- BGPv4 pour IPv4 et IPv6

Cet onglet permet d'activer et de configurer le moteur de routage dynamique Bird.

ON/OFF	Ce bouton permet d'activer l'utilisation du moteur de routage dynamique Bird.

La fenêtre située sous la case d'activation de Bird permet de saisir directement la configuration du moteur de routage dynamique Bird.

NOTE

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

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.
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.

Envoi de la configuration

Les modifications effectuées sur cet écran sont validées à l'aide du bouton Appliquer.

AVERTISSEMENT

Lorsque la configuration est envoyée au firewall, et en cas d'erreur de syntaxe, un message indiquant le numéro de ligne en erreur informe de la nécessité de corriger la configuration.

L'onglet « Routes de retour »

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 :

- 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 l'interface de sortie pour la route de retour.
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.

ROUTAGE MULTICAST

Le routage multicast permet de diffuser un flux réseau depuis une source vers plusieurs destinations. Source et destinations sont alors réunies dans un "groupe multicast".

Ce type de routage est utilisé pour des applications du type télé-séminaires (pas d'interaction des destinataires), téléconférences (chaque membre du groupe peut être source du flux), diffusion de tables de routage pour le protocole RIPv2, amorçage réseau à distance (protocole BOOTP), ...

IMPORTANT

Le routage multicast statique est prioritaire sur tous les autres types de routage (routage statique, routage dynamique, routage au sein d'un bridge, routage par politique, ...).

Ce bouton permet d'activer ou de désactiver le routage statique multicast.

Les actions sur les règles de la politique de routage multicast IPv4

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	Etat de la route statique multicast: Activé : Double-cliquez pour activer la route créée. Désactivé : La route n'est pas opérationnelle.
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.

SERVEUR PPTP

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.

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 oeuvre de SMC, consultez le Guide d'installation SMC et le Guide d'administration SMC.

Rattachement du firewall à 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.

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.

SUPERVISION

Le module **Supervision** propose des graphiques et données en temps réel (auxquels peuvent s'ajouter des graphiques 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,
- les routes et passerelles réseau définies sur le firewall,
- le service DHCP,
- les tunnels VPN SSL établis,
- les tunnels VPN IPSec établis,
- les listes blanches / noires du 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 "Accès complet aux logs (données sensibles)" en cliquant sur **Obtenir le droit d'accès aux données personnelles (logs)** dans le menu déroulant situé sous le nom du compte connecté (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 **Accès complet aux logs (données sensibles)** 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 "Accès complet aux logs (données sensibles)" génère une entrée dans les logs.

NOTE

Pour les modèles SN160(W), SN210(W) et SN310, vous pouvez bénéficier de l'ensemble de la fonctionnalité en utilisant un support de stockage externe de type carte SD et en souscrivant à l'option « External storage » (consultez le module **Traces –Syslog**). Seul le

format SD est compatible : les cartes Micro SD ou Nano SD équipées d'un adaptateur ne sont pas supportées.

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

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,
- Utilisation mémoire,
- Consommation CPU de chacun des services activés sur le firewall,
- Date et heure du système,
- Durée de fonctionnement depuis le dernier redémarrage (*uptime*).

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.
Enlever une colonne	Ce bouton permet de réduire le nombre de colonnes d'affichage des courbes et informations.
Accéder à la configuration de la supervision	Ce lien permet de se rendre directement dans 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.

L'onglet "Historique"

Cet onglet présente un graphique historique de la consommation CPU du firewall.

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 chacune des interfaces réseau sélectionnées 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 VLANs).

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 . Exemple : 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 filtreest 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.

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)
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.
	• 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 filtreest 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.

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.
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 IP source (multi-homing)	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 IP destination (multi-homing)	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 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 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 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.
	  • 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.

Routage

L'onglet "Temps réel"

Cette vue 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. Les données disponibles pour la vue « **Connexions** » sont les suivantes :

Type	Indique dans quel type de route la passerelle est utilisée (exemple : PBR, DefaultRoute, ...)
Nom	Nom du routeur ou des passerelles composant un objet routeur.
Etat	Indique l'état de chaque passerelle. Trois valeurs sont possibles : • **Actif** : cas d'une passerelle utilisée, • **En veille** : cas d'une passerelle de secours, • **Non joignable** : la passerelle ne répond pas aux tests de disponibilité (Ping).
Version IP	Version d'IP utilisé sur la passerelle (4 ou 6).
Adresse IP	Adresse IP de la passerelle.
Principal / secours	Indique si la passerelle est utilisée (principale) ou est une passerelle de secours.
Dernière vérification	Date et heure du dernier test de disponibilité de la passerelle.
Dernier changement d'état	Date et heure du dernier changement d'état de la passerelle (principal/secours).
Disponible	Indique si la passerelle est disponible à l'utilisation.
Disponible depuis	Délai écoulé depuis le dernier changement de disponibilité de la passerelle.
Passerelle par défaut	Indique si le routeur est utilisé comme passerelle par défaut pour le firewall.
Dernier changement de passerelle par défaut	Date et heure du dernier changement de passerelle par défaut.
Id. de routeur	Identifiant unique du routeur
Répartition	Indique le pourcentage d'utilisation de la passerelle au sein de l'objet routeur.

La barre d'actions

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.

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)**.
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 établis 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 disponibles dans la grille « Politique » sont les suivantes :

Filtrer	Le champ rechercher permet de filtrer les données selon des caractères alphanumériques appartenant à n'importe quelle colonne de la grille.
Cacher les tunnels établis pour n'afficher que les politiques présentant des problèmes	Ce bouton permet de masquer les tunnels IPSec correctement établis. Seuls les tunnels ne parvenant pas à s'établir restent affichés.
ID	Cet identifiant système permet de faire le lien les politiques de sécurité (SP) et les associations de sécurité (SA).
Réseau local	Réseau des machines locales dialoguant au travers du tunnel sélectionné(extrémité de trafic).
Nom du réseau local	Nom de l'objet correspondant au réseau local.
Passerelle locale	Adresse IP présentée par le firewall local pour établir le tunnel (extrémité de tunnel).
Nom de la passerelle locale	Nom de l'objet correspondant à la passerelle locale.
Sens	Sens du trafic réseau au sein du tunnel.
Passerelle distante	Adresse IP présentée par le firewall distant pour établir un ou des tunnels avec le firewall local (extrémité de tunnel).
Nom de la passerelle distante	Nom de l'objet correspondant à la passerelle distante.
Réseau distant	Réseau des machines distantes dialoguant au travers du tunnel sélectionné(extrémité de trafic).
Nom du réseau distant	Nom de l'objet correspondant au réseau local.
Durée de vie	Durée de vie de la politique VPN configurée.
État	Un voyant vert ou rouge indique la présence ou non d'un tunnel établi.

Menu contextuel

Un clic droit sur l'adresse ou le nom d'un réseau (local ou distant) donne accès aux menus contextuels suivants :

- Rechercher cette valeur dans la vue "Tous les journaux",
- Afficher les détails de la machine.

Un clic droit sur l'adresse ou le nom d'une passerelle (locale ou distante) donne accès au menu contextuel suivant :

- Rechercher cette valeur dans la vue "Tous les journaux".

La grille "Tunnels"

Les données disponibles dans la grille « Tunnels » sont les suivantes :

N'afficher que les tunnels correspondant à la politique sélectionnée	En cochant cette case, seuls les tunnels correspondant à la politique sélectionnée dans la grille "Politiques" sont affichés.
Passerelle locale	Adresse IP présentée par le firewall local pour établir le tunnel sélectionné (extrémité de tunnel).
Nom de la passerelle locale	Nom de l'objet correspondant à la passerelle locale.
Passerelle distante	Adresse IP présentée par le firewall distant pour établir le tunnel sélectionné (extrémité de tunnel).
Nom de la passerelle distante	Nom de l'objet correspondant à la passerelle distante.
Durée de vie	Durée de vie de la SA (Security Association) pour le tunnel concerné.
Octets	Nombres d'octets échangés dans le tunnel sélectionné.
État	Indication de l'état du tunnel. (Exemple : Mature).
Chiffrement	Nom de l'algorithme de chiffrement.
Authentification	Nom de l'algorithme d'authentification.

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,
- SN Real-Time Monitor.

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.

TABLEAU DE BORD

Le tableau de bord, représenté par cette icône , forme l'écran d'accueil par défaut. Il présente une vue d'ensemble des informations concernant votre firewall.

Tout au long de la configuration du firewall, il est accessible en cliquant sur l'onglet supérieur **Monitoring**.

Le tableau de bord, est divisé en 2 parties :

- Le menu des modules de monitoring à gauche, contenant 3 onglets dépliables :
  - Logs - Journaux d'audit,
  - Rapports,
  - Supervision.

    Une barre de recherche est disponible pour ces 3 modules.
- Une zone dynamique au centre, contenant 5 modules ou widgets :
  - Réseau,
  - Protections,
  - Propriétés,
  - Services,
  - Indicateurs de santé.

Le menu de configuration des modules

Il est accessible en cliquant sur l'onglet supérieur **Configuration**.

Le menu de configuration se présente sous forme d'une colonne rétractable (bouton), et propose 3 rubriques déroulantes (**Configuration**, **Objets**, **Utilisateurs**) 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 de configuration à la liste des favoris, cliquez sur l'icône située à droite de l'intitulé de ce module.

Configuration

Cette rubrique consiste en une arborescence de menus et de leurs modules. Elle intègre également une barre de recherche par mots clés.

Huit menus sont disponibles (cliquez sur les menus pour afficher leur liste déroulante de modules) :

- **Système**, incluant huit modules : Configuration, Administrateurs, Licence, Maintenance, Active Update, Haute disponibilité, Management Center, Console CLI.
- **Réseau**, incluant sept modules : Interfaces, Interfaces virtuelles, Routage, Routage multicast, DNS Dynamique, DHCP, Proxy cache DNS.

- **Objets**, incluant trois modules : Objets réseau, Objets Web, Certificats et PKI.
- **Utilisateurs**, incluant six modules : Utilisateurs, Comptes temporaires, Droits d'accès, Authentification, Enrôlement, Configuration des annuaires.
- **Politique de sécurité**, incluant six modules : Filtrage et NAT, Filtrage URL, Filtrage SSL, Filtrage SMTP, Qualité de service, Règles implicites.
- **Protection applicative**, incluant sept modules : Applications et Protections, Protocoles, Profils d'inspection, Management de vulnérabilités, Réputation des machines, Antivirus, Antispam.
- **VPN**, incluant quatre modules : VPN IPSec, VPN SSL Portail, VPN SSL, Serveur PPTP.
- **Notifications**, incluant sept modules : Traces - Syslog - IPFIX, Agent SNMP, Alertes e-mail, Événements système, Messages de blocage, Configuration des rapports, Configuration de la supervision.

NOTE

Si vous rencontrez des modules grisés, cela signifie qu'ils nécessitent une licence à laquelle vous n'avez pas souscrit, et donc, que vous n'y avez pas accès.

Cela peut également signifier que l'utilisateur avec lequel vous vous êtes connecté n'a pas les privilèges nécessaires à l'accès de ces menus

La zone dynamique : les widgets

Cet espace vous permet de visualiser certaines mises à jour de votre firewall comme les dernières alarmes remontées ou différents indicateurs de santé.

Réseau

Cette fenêtre affiche le nombre d'interfaces disponibles sur le firewall (32 maximum).

La ou les interfaces utilisées apparaissent en vert. Lorsque le mécanisme de bypass a été activé (firewalls industriels uniquement) et est déclenché, les deux premières interfaces sont représentées comme suit :

Une info bulle contenant les informations de chacune des interfaces est disponible.

Ces informations sont les suivantes :

Nom	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.
Bloqué	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 industriels et n'est affichée que lorsque le bypass a été activé et que le mode de fonctionnement « Sûreté » a été choisi. Les valeurs possibles sont « Mode Sûreté activé » (bypass non déclenché) ou « Mode Bypass activé » (bypass déclenché).

Protections

Cette fenêtre contient la liste des dernières alarmes (ou événements systèmes) levées par le firewall.

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
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 "Accès complet aux logs (données personnelles)" en cliquant sur le lien **Accès restreint aux logs** 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 *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.
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** > 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.

Indicateurs de santé

Cette fenêtre présente l'état des ressources matérielles du firewall. Un code couleur indique d emanière visuelle cet état :

- Gris : ce module n'est pas disponible, installé ou activé sur votre firewall,
- Vert : les indicateurs de santé du module sont optimum,
- 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.

Services

Cette fenêtre présente l'état de certains services du firewall. 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 :

Active update	Date de mise à jour du module Active Update.
Management Center	État de la connexion entre le firewall et le serveur Stormshield Management Center.
Sandboxing	État de la connexion aux serveurs Sandboxing.
Cloud Backup	État de la connexion à infrastructure Cloud Backup lorsque les sauvegardes automatiques sont activées.
Antivirus	Date de mise à jour des définitions virales.
Rapports	Activation des rapports Activation des graphiques historiques

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.

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 type de traces du firewall. Ce menu permet également la modification du comportement du firewall lors de l'enregistrement de ces traces.

Cet écran se divise en 2 parties :

- En haut : un menu présentant différentes options
- En bas : un tableau

NOTE

Cet onglet est grisé si le firewall est un modèle sans disque dur. Dans ce cas, lors de l'ouverture du module, l'onglet *Syslog* s'affiche directement.

Ce bouton permet d'activer ou de désactiver le stockage des traces sur le disque dur ou sur une carte SD (firewalls Serie "S").

Support de stockage

Vous avez le choix d'utiliser comme support de stockage :

- Le disque dur interne de votre firewall – option **Support interne (HDD)**
- Une **carte SD** pour les Firewalls de la série "S" et en souscrivant à l'option "external storage".

NOTE

Pour plus d'informations, consultez les Guides **PRÉSENTATION ET INSTALLATION DES PRODUITS NETASQ SÉRIE U - Modèles S** ou **PRÉSENTATION ET INSTALLATION DES PRODUITS STORMSHIELD NETWORK Gamme SN,** disponibles sur le site de Documentation Technique Stormshield.

En cas de saturation du support de stockage, les traces les plus récentes effacent les traces les plus anciennes.

Actualiser Actualise la liste des supports de stockage

Formater Formate le support de stockage dans un format

NOTE

Lorsque le firewall est en Haute disponibilité, 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, il faut basculer le firewall distant en actif par le module **Maintenance**, puis revenir dans le menu **Traces –SySlog** pour pouvoir manipuler la carte SD.

Configuration de l'espace réservé pour les traces

Le firewall gère un certain nombre de fichiers de traces destinés à recueillir les événements détectés par les fonctions de journalisation. Les fichiers concernés par les événements de sécurité sont :

- **Alarmes** : événements liés à l'application des fonctions de prévention des intrusions (l_alarm),
- **Authentification** : événements liés à l'authentification des utilisateurs (l_auth),
- **Connexions réseaux :** événements liés aux connexions à travers et à destination du firewall (l_connection),
- **Politique de filtrage** : événements liés à l'application des fonctions de filtrage (l_filter),
- **Proxy FTP** : événements liés au trafic FTP (l_ftp),
- **Statistiques :** événements liés au monitoring temps réel (l_monitor),
- **Connexions applicatives (plugin)** : événements liés au traitement des plugins de l'ASQ (l_plugin),
- **Proxy POP3 :** événements liés à l'envoi des messages (l_pop3),
- **Management des vulnérabilités :** événements liés à l'application de consultation des vulnérabilités sur le réseau Stormshield Network Vulnerability Manager (l_pvm),
- **Sandboxing** : événements liés à l'analyse sandboxing des fichiers lorsque cette option a été souscrite et activée (l_sandboxing),
- **Administration (Serverd) :** événements liés au serveur d'administration des firewalls : "serverd" (l_server),
- **Proxy SMTP :** événements liés au trafic SMTP (l_smtp),
- **Evénements systèmes** : c'est dans ce journal que sont enregistrés les événements liés directement au système : arrêt/démarrage du firewall, erreur système, etc. L'arrêt et démarrage des fonctions de journalisation correspondent à l'arrêt et au démarrage des « démons » qui génèrent les traces (l_system),
- **VPN IPSec** : événements liés à l'établissement des SA (l_vpn),
- **Proxy HTTP** : événements liés au trafic HTTP (l_web),
- **VPN SSL :** événements liés à l'établissement du VPN SSL (l_xvpn),
- **Proxy SSL** : événements liés au trafic SSL (l_ssl).

Les fichiers partagent un espace global de stockage avec d'autres fichiers de traces.

Pour chaque menu de traces (Alarmes, Authentification, Connexions réseaux, Politique de filtrage, Proxy FTP, Statistiques, Connexions applicatives (plugin), Proxy POP3, Applications et vulnérabilités (Seismo), Serveur, Proxy SMTP, Evénements systèmes, VPN IPSec, Proxy HTTP, VPN SSL), vous pouvez limiter la taille du fichier de traces en sélectionnant la taille du fichier en pourcentage de l'espace réservé pour les fichiers de logs.

Le tableau présente les colonnes suivantes :

Activé	Permet d'activer/désactiver le fichier de traces. Si vous décochez la ligne, le pourcentage est à 0. Dans ce cas, le type de log ne sera pas stocké sur le disque. En recochant la ligne, le pourcentage indiqué est à 1% par défaut.
Famille	Nom du fichier de traces.
Pourcentage	Taux d'occupation actuel en pourcentage. En cliquant dans une case, il est possible de modifier le pourcentage.
Quota d'espace disque	Proportion d'espace disque qu'occupe chaque fichier sur le disque qui varie selon le pourcentage spécifié.

En bas à droite du tableau est indiqué le total des pourcentages. Si le total est supérieur à 100%, dans ce cas, une ligne d'avertissement au bas de la grille est indiquée en rouge. (*Exemple : « Attention, répartition incorrecte : 113% de l'espace disponible est réservé)*. Les modifications sont toutefois autorisées.

En cliquant sur **Appliquer**, le message suivant s'affiche : « L'espace disque total réservé pour les traces dépasse la capacité pour ce modèle. Voulez-vous vraiment appliquer cette configuration ? ». Vous avez le choix entre forcer l'enregistrement ou annuler.

NOTE

Ces fichiers peuvent être copiés sur la solution Stormshield Network EVENT ANALYZER afin de construire des rapports ou d'effectuer leur archivage.

Onglet « Syslog »

L'onglet *Syslog* permet de configurer jusqu'à 4 profils d'envoi de traces vers des serveurs Syslog.

Vous pouvez notamment envoyer les traces au serveur Stormshield Visibility Center (SVC), la solution de supervision de Stormshield, au format Syslog. Reportez-vous au *Guide d'administration SVC* disponible sur le site de Documentation Technique Stormshield.

Les syslogs 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).

Grille de profils syslogs

Le tableau présentant les profils se compose de 2 colonnes :

État	Permet, par un double-clic d'activer ou de désactiver le profil.
Profil	Affiche le nom du profil Syslog

Configuration d'un profil

Détails

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).
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.
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.
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

Traces activées

Cette grille permet de sélectionner le type de traces devant être envoyées au serveur Syslog.

État	Permet d'activer l'envoi du fichier de traces sélectionné.
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. Quatre patrons sont définis par défaut : • connexions IPv4 sans translation d'adresses (NAT), • connexions IPv4 avec NAT, • connexions IPv6, • alarmes. Ces patrons définissent l'envoi des informations contenues dans les fichiers de traces des alarmes (l_alarm), des connexions (l_connexion), des plugins de prévention d'intrusion (l_plugin), et du filtrage de paquets (l_filter).
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)

Certains modèles de firewalls sont équipés d'un module physique de stockage sécurisé nommé TPM (Trusted Platform Module), destiné à protéger les certificats, clés privées, fichiers de sauvegarde de configuration...

Pour pouvoir utiliser le TPM, celui-ci doit être initialisé, c'est à dire qu'un mot de passe d'administration du TPM doit être créé.

Cette initialisation peut être réalisée lors du premier accès à certains modules de configuration :

- **Objets > Certificats et PKI,**
- **Maintenance > onglet Sauvegardes,**
- **Maintenance > onglet Restauration.**

Initialiser le TPM

Pour pouvoir initialiser puis utiliser le TPM, le compte administrateur connecté doit posséder le droit d'**Accès au TPM (E)**. Pour attribuer ce droit aux administrateurs, rendez-vous dans le module Administrateurs > onglet Administrateurs > Passer en vue avancée.

A l'ouverture de l'un des modules précités, la fenêtre d'initialisation du TPM s'affiche :

1. Saisissez le mot de passe d'administration du TPM (8 caractères minimum),
2. **Confirmez** ce mot de passe
   Une jauge indique la robustesse du mot de passe choisi.
3. Si le firewall est membre d'un cluster (Haute Disponibilité activée), cochez la case **Dériver la clé depuis le mot de passe du TPM** afin que les deux firewalls disposent d'une clé identique et ne rencontrent pas de problèmes d'accès au TPM en cas de bascule HA.
4. Cliquez sur **Appliquer**.

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 document *Configuration de l'annuaire* ou module **Utilisateurs\Configuration de l'annuaire**).

Les comptes contiennent l'ensemble des informations relatives à ces utilisateurs :

Identifiant de connexion

- Nom
- Prénom
- Mail (optionnel)
- Téléphone (optionnel)
- Description (optionnel)

L'écran des **Utilisateurs** se décompose en 2 parties :

- Un bandeau affichant les différentes options
- La liste des **CN** (ou utilisateurs) dans la colonne de gauche, accompagnés de leurs informations dans la colonne de droite.

Voici les tableaux indiquant le nombre maximum d'utilisateurs pouvant être authentifiés simultanément selon votre modèle de firewall :

Modèle - Gamme SN	SN160(W)	SN210(W)	SN310	SN510	SN710
NB. Max. utilisateurs	15	30	50	100	200

Modèle - Gamme SN	SN910	SN2000	SN2100	SN3000	SN3100	SN6000	SN6100
NB. Max. utilisateurs	500	1000	2000	2500	4000	15 000	15000

Modèle - Gamme EVA	EVA1	EVA2	EVA3	EVA4	EVAU
NB. Max. utilisateurs					

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 le login correspondent aux mots clefs 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.

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).

Créer 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. **REMARQUE** 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**.

Créer 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.

Id	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.

REMARQUE

Les champs « Id », « 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.
Force du mot de passe	Une jauge indiquant la force du mot de passe choisi est affichée.

Cliquez sur le bouton **Appliquer** de cette fenêtre pour valider la création du mot de passe.

REMARQUE

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.

Supprimer

Ce bouton permet de supprimer un utilisateur ou un groupe :

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. Cliquez sur **Oui**.

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.

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.

L'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 menu **Utilisateurs**\module **Authentification**\onglet(s) *Interfaces internes* (ou **externes**)*Mot de passe des utilisateurs* et cocher l'option **Les utilisateurs peuvent changer leur mot de passe**.
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.
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.

L'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 menu **Objets**\module **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.

L'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. 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**.

Une personne, par exemple 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 nomades sur lesquels seraient installés des clients VPN.

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.

NOTE

Il n'existe pas de droit spécifique au "vpn_global".

L'écran du module VPN IPSec est composé de 4 onglets :

- *Politique de chiffrement – Tunnels* **:** cet onglet permet de créer vos tunnels IPSec entre deux firewalls (**Site à site – Gateway- Gateway**) ou entre un firewall multifonctions Stormshield Network et un utilisateur nomade (**Anonyme – Utilisateurs nomades**). 10 profils de chiffrement vierges peuvent être configurés, activés et édités. La politique anonyme 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 nomade "classique": une adresse IP non prévisible.
- *Correspondants* : vous pourrez ici créer de nouveaux correspondants (site distant ou correspondant anonyme nomade) en renseignant notamment leur **profil IKE**, leur méthode de négociation, ainsi que les paramètres spécifiques à chaque méthode de négociation.
- *Identification* : cet onglet permet de lister vos autorités de certification acceptées dans les tunnels utilisant les méthodes PKI, ainsi que les clés pré-partagées (PSK) de vos tunnels nomades dans deux tableaux.
- *Profils de chiffrement* : définissez ici 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.

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 v3***). Cette fonctionnalité n'ayant pas pu être testée dans des environnements complexes et hétérogènes, il est donc fortement conseillé de l'éprouver sur une configuration de tests.

La barre des profils	Le menu déroulant propose 10 profils IPSec numérotés de (1) 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 ce slot écrasent les paramètres en vigueur.

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 « 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 va permettre 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.

Le bouton "Ajouter" est détaillé dans la section suivante.

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 copié.

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

Vous allez ici définir chacune des extrémités de votre tunnel ainsi que le correspondant.

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 :

IKEv1

1 Sélection de la passerelle :

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 .

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.

Cliquez sur **Suivant**.

2 Identification du correspondant :

2 choix sont possibles, l'identification par **Certificat** ou par **Clé pré partagée (PSK** – Pre-Shared Key**)**. Cochez l'option voulue.

1. 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.
2. 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.

Cliquez sur **Suivant.**

3 Terminer la création du correspondant :

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.

Cliquez sur **Terminer**.

Créer un correspondant IKEv2	Les étapes sont identiques à celles suivies pour la création d'un correspondant IKEv1.
Réseau local	Machine, groupe de machines, réseau ou groupe de réseaux qui vont être accessibles via le tunnel VPN IPSec.
Réseau distant	Machine, groupe de machines, réseau ou groupe de réseaux accessibles via le tunnel IPsec avec le correspondant.

Configuration en étoile

Ce procédé consiste à diriger plusieurs tunnels VPN vers un même point. Il permet, par exemple, de relier des agences à un site central.

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.
Sites distants	Définissez les paramètres de vos sites distants : choisissez votre correspondant parmi la liste de ceux déjà créés ou cliquez sur l'icône » pour en créer un nouveau, et sélectionnez les réseaux distants parmi les objets de la liste déroulante. Vous pouvez en **Ajouter** ou en **Supprimer** en cliquant sur les boutons prévus à cet effet.
Considérer l'(es) interface(s) IPSec comme interne(s) (s'applique à tous les tunnels)	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 précisées. 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. Si cette option a été activée par erreur dans l'assistant d'installation de tunnels VPN IPsec, elle peut être désactivée en décochant la case **Considérer l'(es) interface(s) IPSec comme interne(s) (s'applique à tous les tunnels - les réseaux distants devront être explicitement légitimés)** présente dans le panneau *Configuration avancée* du module **Protection applicative** > **Profils d'inspection**.
Créer les politiques sans chiffrement (none) pour les réseaux internes	Cette case permet de générer automatiquement des politiques sans chiffrement (none) dédiées aux réseaux internes (*Network_internals* vers *Network_internals*). Si la politique existe déjà, un message avertit que ces politiques ont déjà été créées.

Cliquez sur **Terminer**.

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 en créez un, celui-ci s'active par défaut. Cliquez deux fois dessus pour le désactiver.
	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 : • Extrémités du tunnel : objet local / objet distant • Extrémités du trafic : objet local / objet de destination • Authentification : Mode / Type / Certificat / Clé pré-partagée • Profils de chiffrement (phase 1 & 2) : algorithmes, groupe Diffie Helman, durée de vie Ces informations sont sélectionnables, ce qui permet leur copie.

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.
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*.
Commentaire	Description associée à la politique VPN.

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.

Cette option n'est valide que pour les **tunnels site à site**. Elle est disponible en cochant la valeur *Keepalive* dans le menu *Colonnes*, apparaissant au survol de l'intitulé des colonnes de la grille.

Keepalive	Pour activer cette option, affectez une valeur différente de 0, correspondant à l'intervalle en seconde, entre chaque envoi de paquet UDP.

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.

Anonyme – Utilisateurs nomades

Le VPN IPSec comporte deux extrémités : l'extrémité de tunnel, et l'extrémité de trafic. Pour les anonymes ou utilisateurs nomades, 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 »).

Notez que depuis la version 3.8.0, il est possible de construire une politique IPSec nomade 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 nomade par l'assistant, reportez-vous à la section **« Création de correspondant nomade »** ci-dessous.

Pour les utilisateurs nomades, il est possible de définir des paramètres clients VPN (Mode Config) par l'assistant de création de *politique Mode Config*.

Nouvelle politique

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 nomade 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 nomade".

Une fois créée, la cellule correspondant à la colonne Mode Config propose un bouton **Modifier**, 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 nomade

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 nomade** » via l'assistant de politique VPN IPSec nomade.
2. Donnez un nom à votre configuration nomade, et cliquez sur **Suivant**.
3. 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 créé 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.
Hybride	Si vous optez pour la méthode hybride, vous devrez également fournir un « **Certificat** » (serveur) à présenter au correspondant et éventuellement, sa CA. L'authentification du serveur est faite par certificat durant la phase 1, et celle du client le sera par XAuth juste après cette phase 1.
Certificat et XAuth (iPhone)	Cette option permet aux utilisateurs mobiles (roadwarriors) de se connecter sur la passerelle VPN de votre entreprise via leur téléphone portable, à l'aide d'un certificat durant la phase 1. Le serveur est également authentifié par certificat pendant cette phase 1. Une authentification supplémentaire du client est effectuée par XAuth après la phase 1. **NOTE** C'est le seul mode compatible avec l'iPhone.
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.

4. Cliquez sur **Suivant**.
5. Vérifiez l'écran de résumé de votre configuration nomade et cliquez sur **Terminer**.

6. Renseignez ensuite la ressource locale, ou « **réseau local** » auquel l'utilisateur nomade 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.

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 en créez un, celui-ci s'active par défaut. Cliquez deux fois dessus pour le désactiver.
	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 : • Extrémités du tunnel : objet local / objet distant • Extrémités du trafic : objet local / objet de destination • Authentification : Mode / Type / Certificat / Clé pré-partagée • Profils de chiffrement (phase 1 & 2) : algorithmes, groupe Diffie Helman, durée de vie Ces informations sont sélectionnables, ce qui permet leur copie.
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 nomade	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 nomade 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.
Domaine (Annuaire)	Cette option permet de préciser le domaine (annuaire) sur lequel le correspondant nomade 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 **Domaine (Annuaire)**.
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. Celui-ci 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 **Modifier** permet de renseigner les paramètres du Mode config IPsec, qui sont les suivants :

Serveur DNS	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.
Liste des 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	Pour activer cette option, affectez une valeur différente de 0, correspondant à l'intervalle en seconde, entre chaque envoi de paquet UDP.

REMARQUE

Vous ne pourrez utiliser et créer qu'une seule configuration nomade (« 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 nomade.

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 :

- A gauche : la liste des correspondants VPN IPSec et VPN IPSec nomades.
- A droite : Les informations du correspondant sélectionné.

La liste des correspondants

Chercher dans les correspondants	Ce champ permet d'effectuer une recherche sur le nom de l'objet et ses différentes propriétés, par occurrence, lettre ou mot.

Filtrer	3 choix sont possibles : Vous pouvez afficher dans la liste « **Tous les correspondants** », passerelles et nomades confondus. Vous pouvez également ne laisser apparaître que les « **Passerelles** » ou uniquement les « **Correspondants mobiles** » (nomades).
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 : un « **Nouveau site distant** », un « **Nouveau site distant IKEv2** », un « **Nouveau correspondant anonyme (nomade)** » ou un « **Nouveau correspondant anonyme (nomade) IKEv2** ». Vous pouvez aussi « **Copier depuis la sélection** » un correspondant, celui-ci sera dupliqué. Pour cela, positionnez-vous sur le correspondant à copier et entrez son nouveau nom dans la fenêtre affichée.
Supprimer	Sélectionnez le correspondant à retirer de la liste et cliquez sur **Supprimer**.
Renommer	Sélectionnez le correspondant dans la liste puis cliquez sur Renommer.
Nom	Nom donné au correspondant lors de sa création.

Les informations des correspondants

Correspondant (de type « passerelle »)

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.
Configuration de secours	Ce champ précise si vous avez défini une configuration de secours lors de la création du correspondant, il affichera « None » par défaut si vous n'en avez créé aucune. Vous pouvez toutefois en définir une en la sélectionnant dans la liste déroulante contenant vos autres correspondants distants.
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 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 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 affichera votre certificat. Si vous avez opté pour la clé pré partagée, ce champ sera grisé.
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).
Confirmer	Confirmation de votre clé pré partagée (PSK).

Configuration avancée

Mode de négociation	En IPSec, 2 modes de négociation sont possibles : le mode principal (ou « main » mode) et le mode agressif. Ils influent notamment sur la « phase 1 » du protocole IKE (phase « d'authentification »). Ce mode est automatiquement déterminé en fonction des paramètres de configuration ; le mode agressif n'est utilisé qu'en cas de configuration anonyme par clé pré-partagées. Ce mode est néanmoins modifiable via une commande CLI. **Mode principal**: Dans ce mode, la phase 1 se déroule en 6 échanges. La machine distante ne peut être identifiée que par son adresse IP avec une authentification en clés pré-partagée. En mode PKI, l'identifiant est dans le certificat. Le mode principal assure l'anonymat. **Mode agressif** : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et la machine distante. Les identités des correspondants peuvent être une adresse IP, un FQDN ou une adresse mail mais pas un certificat. L'authentification est faite par clé pré-partagée. Le mode agressif n'assure pas l'anonymat. **AVERTISSEMENT** L'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécurisé que les autres modes du protocole IPsec. Ainsi Stormshield Network recommande l'utilisation du mode principal et en particulier du mode principal + certificats pour les tunnels à destination de nomades. En effet la PKI interne du firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation. **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.

Mode de secours	Le mode de secours est le mode de bascule pour le failover IPSec, si un serveur n'est plus accessible, un autre prend le relai, de manière transparente. Quand le tunnel est basculé sur le correspondant de secours, deux choix sont possibles : Le mode « **temporaire** » : une fois le correspondant principal de nouveau joignable, le tunnel rebascule sur celui-ci. Le mode « **permanent** » : le tunnel reste sur le correspondant de secours tant qu'il est fonctionnel, même si le correspondant principal est de nouveau joignable. **NOTE** Ce champ n'est éditable qu'en mode expert (CLI). Reportez-vous à la Base de connaissances (version anglaise) du support technique pour davantage d'informations (How can I modify the backup mode for a specific IPSec peer ?).
Adresse locale	Objet sélectionné comme étant l'adresse IP locale utilisée pour les négociations IPSec avec ce correspondant. Ce champ est en « Any » par défaut, ce qui correspond au choix automatique de l'interface, basé sur la table de routage.
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.

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. **AVERTISSEMENT** 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**.

Le mode de négociation (principal ou agressif), lorsqu'il a été forcé, est conservé quand on modifie la configuration d'un correspondant IPSec.

Correspondant (de type nomade / « correspondant mobile »)

Commentaire	Description associée au correspondant distant.
Passerelle distante	Ce champ est grisé pour les correspondants de type nomade.
Configuration de secours	Ce champ est grisé pour les correspondants de type nomade.

Profil IKE	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés: **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 de type « nomade », vous avez le choix entre **Certificat**, **Clé pré partagée (PSK)**, **Hybride**, **Certificat et Xauth (iPhone).**
Certificat	Si vous avez choisi la méthode d'authentification par **Certificat**, **Hybride** ou **Certificat** et **XAuth**, ce champ affichera votre certificat ou vous proposera de le sélectionner au sein de la liste déroulante. Si vous avez opté pour la clé pré partagée, ce champ sera grisé.
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). **NOTE** Ce champ n'est accessible que si vous avez choisi la méthode d'authentification par **Clé pré partagée**.
Cliquer ici pour éditer la liste des PSK	En cliquant sur ce lien, vous basculerez dans l'onglet *Identification* du module VPN IPSec. Vous pourrez y ajouter vos **Autorités de certification acceptées** ainsi que vos **Tunnels nomades : clés pré partagées**.

Configuration avancée

Mode de négociation

En IPSec, 2 modes de négociation sont possibles : le mode principal (ou « main » mode) et le mode agressif. Ils influent notamment sur la « phase 1 » du protocole IKE (phase « d'authentification »).

Mode principal : Dans ce mode, la phase 1 se déroule en 6 échanges. La machine distante ne peut être identifiée que par son adresse IP avec une authentification en clé pré-partagée.
En mode PKI, l'identifiant est dans le certificat. Le mode principal assure l'anonymat.

Mode agressif : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et la machine distante. La machine distante peut être identifiée avec une adresse IP, FQDN ou une adresse mail mais pas avec un certificat par clé pré-partagée. Le mode agressif n'assure pas l'anonymat.

NOTE
Le firewall paramètre automatiquement l'utilisation des méthodes d'authentification par certificat, hybride ou XAuth en mode principal.
Si le client veut utiliser la PSK, il doit se positionner en mode agressif.

AVERTISSEMENT
L'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécurisé que les autres modes du protocole IPSec. Ainsi Stormshield Network recommande pour les correspondants mobiles, l'utilisation du mode principal, soit avec une authentification par certificats, soit en utilisant la méthode hybride.
Dans le cas d'une authentification par certificats, la PKI interne du firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation.

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.

Mode de secours

Le mode de secours est le mode de bascule pour le failover IPSec, si un serveur n'est plus accessible, un autre prend le relai, de manière transparente.

Néanmoins, ici, le champ est grisé car la configuration de secours n'est pas applicable pour une configuration nomade.

NOTE
Ce champ n'est éditable qu'en mode expert (CLI). Reportez-vous à la Base de connaissances (version anglaise) du support technique pour davantage d'informations (*How can I modify the backup mode for a specific IPSec peer ?*).

Adresse locale

Objet sélectionné comme étant l'adresse IP locale utilisée pour les négociations IPSec avec ce correspondant.
Ce champ est en « Any » par défaut.

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. **AVERTISSEMENT** 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).

L'onglet « Identification»

Autorités de certification acceptées

Ce tableau va permettre 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 créé au préalable apparaît. Sélectionnez les autorités qui permettront de vérifier les identités de vos correspondants, en cliquant sur Selectionner. 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 nomades : clés pré partagées

Si vous avez préalablement créé un correspondant nomade ayant pour méthode d'authentification la **Clé pré partagée (PSK)**, ce tableau sera déjà pré-rempli.

Vous aviez dû éditer une clé en lui définissant un ID et une valeur (en caractères hexadécimaux ou ASCII).

Rechercher	Bien que le tableau affiche toutes vos clés pré partagées de tunnels nomades 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.

REMARQUES

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.

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.

Configuration avancée

Activer la recherche au travers de plusieurs annuaires LDAP (modes clé prépartagée 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.

Profil de chiffrement IKE (phase 1)

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 3 profils pré-configurés : **StrongEncryption, GoodEncryption,** et **Mobile**. Il est également possible d'en créer d'autres.

Profil de chiffrement IPSec (phase 2)

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 3 profils pré-configurés : **StrongEncryption, GoodEncryption,** et **Mobile**. Il est également possible d'en créer d'autres.

Tableau des profils

Ce tableau propose une série de profils de chiffrement prédéfinis, de phases 1 ou 2.

Ajouter	En cliquant sur ce bouton, vous pouvez choisir d'ajouter un **Profil de phase 1** (IKE) ou **Profil de phase 2 (IPSec)**, qui sera affiché dans la colonne « Type ». 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.
Supprimer	Sélectionnez le profil de chiffrement à retirer de la liste et cliquez sur **Supprimer**.

Profil de type IKE

Pour chaque 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. **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. **REMARQUE** Plus la taille du mot de passe (ou « clé ») est grande, plus le niveau de sécurité est élevé, mais consomme aussi davantage de ressources. **NOTE** 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, et 3600 secondes pour un profil de type **IPSec**.

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	6 choix vous sont proposés : **des**, **3des**, **blowfish, cast128**, **aes** et **aes_gcm_16**. 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	5 choix vous sont proposés : **sha1, md5, sha2_256, sha2_384, sha2_512**.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Profil de type 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. **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. **REMARQUE** Plus la taille du mot de passe (ou « clé ») est grande, plus le niveau de sécurité est élevé, mais consomme aussi davantage de ressources. **NOTE** 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 **IKE** est 21600 secondes, et 3600 secondes pour un profil de type **IPSec**.

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_sha1,** d'une « Force » de 160 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	6 choix vous sont proposés : **hmac_sha1, hmac_md5, hmac_sha256, hmac_sha384, hmac_sha512** ou **non_auth**.
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 **des,** d'une « Force » de 64 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	6 choix vous sont proposés : **des**, **3des**, **blowfish, cast128**, **aes**, **aes_gcm_16** ou **null_enc**. 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.

Cliquez sur **Appliquer** une fois votre configuration effectuée.

VPN SSL

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée aux ressources internes de l'entreprise par des communications chiffrées en SSL. Son utilisation requiert l'installation d'un client VPN SSL installé sur le poste de travail ou sur tout type de terminal mobile (Windows, IOS, Android, etc.).

Les tunnels VPN SSL peuvent être basés sur les protocoles UDP ou TCP. Lorsqu'un tunnel basé sur UDP échoue, la connexion bascule sur le protocole TCP.

Dans le cas de l'utilisation du Client VPN mis à disposition, la connexion nécessite uniquement de renseigner l'adresse IP du firewall et les informations d'authentification (identifiant / mot de passe). Dans le cas de l'utilisation d'un client OpenVPN, le client doit récupérer les informations de configuration sur le portail d'authentification (menu 'Données personnelles') puis les intégrer au client.

En plus du paramétrage de ce module, l'**Authentification** doit définir la méthode et autoriser l'utilisateur dans sa politique. Enfin, une règle de filtrage doit spécifier en source (configuration avancée) l'entrée 'Via Tunnel VPN SSL' pour autoriser le trafic.

Pour plus d'informations, reportez-vous à la Note technique **Tunnels VPN SSL** disponible depuis votre espace sécurisé.

Ce module se compose d'un unique écran de configuration divisé en 4 zones :

- Activer le service
- **Paramètres réseaux :** cette zone comporte des éléments de configuration du serveur VPN SSL, des réseaux ou machines joignables, et du réseau affecté aux clients.
- **Paramètres DNS envoyés au client :** cette zone comporte des éléments de configuration DNS envoyés au client.
- **Configuration avancée** : une zone pour personnaliser la durée de vie avant renégociation SSL, définir d'éventuels scripts à exécuter lors de la connexion/déconnexion du client et sélectionner les certificats client et serveur pour l'établissement du tunnel SSL.

Ce bouton permet d'activer ou de désactiver le serveur VPN SSL du firewall.

Paramètres réseaux

Adresse IP (ou FQDN) de l'UTM utilisée	Indiquez l'adresse IP publique de l'IPS-Firewall (ou un FQDN associé à cette adresse. Exemple : sslserver.compagnie.com) par laquelle les clients pourront joindre le serveur VPN SSL.
Réseaux ou machines accessibles	Indiquez quels seront les réseaux et hôtes visibles pour les clients. Tous les paquets issus du client et destinés à ces réseaux passeront par le tunnel SSL. Cet objet peut être du type « réseau », « machine » ou « groupe » (contenant des réseaux et/ou des machines). Il peut être créé directement dans cette fenêtre en cliquant sur Par défaut, ce champ a pour valeur « Network_internals », offrant une connectivité avec l'ensemble des réseaux protégés par le Firewall. **REMARQUE** Il s'agit uniquement d'une notion de routage réseau. Il est nécessaire de créer des règles de filtrage pour autoriser ou interdire les flux entre le réseau des clients distants et les ressources internes.

Réseau assigné aux clients (UDP)	Sélectionnez un objet de type « réseau » (les objets de type « plage d'adresses IP » ou « Groupe » ne sont pas acceptés). Chaque client établissant un tunnel basé sur le protocole UDP se verra attribuer une adresse IP appartenant à ce réseau. Ce réseau doit être différent de celui attribué aux clients de tunnels basés sur TCP. L'objet peut être créé directement dans cette fenêtre en cliquant sur l'icône **IMPORTANT** Afin d'éviter des conflits de routage sur les postes clients lors de la connexion au VPN SSL, choisissez plutôt, pour vos clients, des sous-réseaux peu communément utilisés (exemple : 10.60.77.0/24, 192.168.38.0/24, etc.). En effet, de nombreux réseaux d'accès internet filtrés (wifi public, hôtels…) ou réseaux locaux privés utilisent les premières plages d'adresses réservées à ces usages (exemple : 10.0.0.0/24, 192.168.0.0/24).
Réseau assigné aux clients (TCP)	Sélectionnez un objet de type « réseau » (les objets de type « plage d'adresses IP » ou « Groupe » ne sont pas acceptés). Chaque client établissant un tunnel basé sur le protocole TCP se verra attribuer une adresse IP appartenant à ce réseau. Ce réseau doit être différent de celui attribué aux clients de tunnels basés sur UDP. L'objet peut être créé directement dans cette fenêtre en cliquant sur l'icône **IMPORTANT** Afin d'éviter des conflits de routage sur les postes clients lors de la connexion au VPN SSL, choisissez plutôt, pour vos clients, des sous-réseaux peu communément utilisés (exemple : 10.60.77.0/24, 172.168.38.0/24, etc.). En effet, de nombreux réseaux d'accès internet filtrés (wifi public, hôtels…) ou réseaux locaux privés utilisent les premières plages d'adresses réservées à ces usages (exemple : 10.0.0.0/24, 192.168.0.0/24).
Maximum de tunnels simultanés autorisés	En fonction de la taille du réseau choisi pour les clients et du modèle de Firewall, le nombre de tunnels pouvant être établis simultanément est indiqué. Ce nombre correspond au minimum des deux valeurs suivantes : • Le quart du nombre d'adresses IP incluses dans le réseau client choisi (exemple : 63 pour un réseau de classe C). En effet, chaque tunnel SSL consomme 4 adresses IP. • Le nombre maximal de tunnels autorisés sur le modèle d'IPS-Firewall utilisé.

Paramètres DNS envoyés au client

Nom de domaine	Nom de domaine attribué au client pour lui permettre d'effectuer ses résolutions DNS.
Serveur DNS primaire	Serveur DNS primaire affecté au client.
Serveur DNS secondaire	Serveur DNS secondaire affecté au client.

Configuration avancée

Adresse IP de l'UTM pour le VPN SSL (UDP)	Indiquez l'adresse IP publique de l'IPS-Firewall par laquelle les clients pourront joindre le serveur VPN SSL sur UDP.
Port (UDP)	Sélectionnez ou créez l'objet correspondant au port UDP à utiliser pour établir les tunnels.
Port (TCP)	Sélectionnez ou créez l'objet correspondant au port TCP à utiliser pour établir les tunnels. Ce port est également utilisé comme mécanisme de secours lorsque les tunnels ne peuvent pas être établis à l'aide du protocole UDP.

Délai avant renégociation des clés (en secondes)	Période de temps au bout de laquelle les clés sont renégociées. La valeur par défaut est de 14400 secondes, soit 4 heures.
Utiliser les serveurs DNS fournis par le firewall	En cochant cette case, le client VPN SSL inscrit dans la configuration réseau du poste les serveurs DNS récupérés via le VPN SSL. Les serveurs DNS éventuellement déjà définis sur le poste de travail pourront néanmoins être interrogés.
Interdire l'utilisation de serveurs DNS tiers	En cochant cette case, les serveurs DNS déjà définis dans la configuration du poste de travail sont exclus par le client VPN SSL. Seuls les serveurs DNS envoyés par le firewall pourront être interrogés. Ces serveurs DNS doivent être joignables au travers du tunnel VPN SSL.
Script à exécuter lors de la connexion	Sélectionnez un script que le client exécutera localement lors de sa connexion au tunnel SSL (exemple : connexion d'un disque à un partage réseau distant).
Script à exécuter lors de la déconnexion	Sélectionnez un script que le client exécutera localement lors de sa déconnexion du tunnel SSL (exemple : déconnexion d'un disque à un partage réseau distant).

NOTE

Seules les machines clientes fonctionnant sous Windows et avec le client Stormshield Network peuvent bénéficier du service des scripts exécutables. Le format des fichiers est obligatoirement du type « .bat ».

NOTE

Toutes les variables d'environnement Windows peuvent être utilisées au sein des scripts de connexion/déconnexion (exemple : %USERDOMAIN%, %SystemRoot%, etc.).

Deux variables d'environnement liées au tunnel VPN SSL sont également utilisables :

- %NS_USERNAME% : le nom d'utilisateur servant à l'authentification,
- %NS_ADDRESS% : l'adresse IP attribuée au client.

Certificats utilisés

Certificat serveur	Sélectionnez le certificat présenté par le serveur pour l'établissement d'un tunnel SSL. Par défaut, le certificat serveur proposé est celui créé à l'initialisation de l'IPS-Firewall. Il est issu de la CA dédiée au VPN SSL par défaut.
Certificat client	Sélectionnez le certificat présenté par le client pour l'établissement d'un tunnel SSL. Le certificat client proposé par défaut est celui créé à l'initialisation de l'IPS-Firewall. Il est issu de la CA dédiée au VPN SSL par défaut. Ce certificat est commun à l'ensemble des clients. Leur authentification est réalisée une fois la connexion SSL établie.

IMPORTANT

Si vous choisissez de créer votre propre CA, vous devez utiliser deux certificats signés par celle-ci. S'il ne s'agit pas d'une autorité racine, les deux certificats doivent être issus de la même sous-autorité.

Configuration

Télécharger le fichier de configuration	Cliquez sur ce bouton pour obtenir une archive contenant le fichier de configuration du serveur VPN SSL.

VPN SSL Portail

Le VPN SSL Stormshield Network permet à vos utilisateurs nomades ou non de se connecter sur les ressources de votre société de façon sécurisée.

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 (Windows, Linux, MAC OS-X,…).
  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.

Le nombre de serveurs Web configurables varie selon les modèles de boîtiers :

Modèle	Nbre max. serveurs HTTP	Nbre max. serveurs Autres
SN160(W), SN210(W), SN310	64	64
SN510, SN710	128	128
SN910	256	256
SN2000, SN2100, SN3000, SN3100, SN6000, SN6100	512	512

Ajout d'un serveur web

Pour ajouter un serveur d'accès Web, suivez la procédure suivante :

1 Cliquez sur le bouton **Ajouter** puis sélectionnez l'un des serveurs proposés. Un écran contenant des noms de serveurs s'affiche.

2 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.)

3 La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données ci-dessous.

Serveur de destination	Le 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

Activer la liste blanche d'URLs	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 via le champ **Ne pas réécrire les URLs de la catégorie.** Par exemple, pour un accès vpnssl 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.

URLs 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 utilisable sous Windows avec Internet Explorer 5 ou + uniquement. Il 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** puis sélectionnez Serveur web OWA 2003 (mode Premium) ou Serveur web OWA 2007 – 2010 (mode premium). L'écran suivant s'affiche :

2 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.)

3 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'URLs** coché, le champ **Ne pas réécrire les URLs de la catégorie** avec l'indication « vpnssl_owa », le champ **Désactiver la méthode d'authentification NTLM** et 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'URLs** avec l'indication de la catégorie d'URL « vpnssl_owa », et 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** puis sélectionnez **Serveur web Lotus Domino**.

2 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 »

Configuration avec un serveur applicatif

Pour ajouter un serveur d'accès aux ressources autres que le type Web, suivez la procédure suivante :

1 Cliquez sur le bouton **Ajouter** puis sélectionnez **Serveur applicatif.**

2 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.)

3 La configuration de ce serveur apparaît alors, 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.
Port	Ce champ permet de spécifier le port sur le serveur auquel l'utilisateur pourra accéder.

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

1 Etape 1 : Création d'un objet pour le serveur Citrix

Accédez à la base d'objets afin de créer une machine puis sélectionnez une machine.

2 Etape 2 : Configuration d'un serveur applicatif

Depuis le module VPN SSL, sélectionnez l'onglet *Serveurs applicatifs*. Cliquez sur le bouton Ajouter puis sélectionnez Serveur Citrix. Donnez un nom à votre serveur. L'écran de configuration du serveur Citrix s'affiche.

Sélectionnez le serveur Citrix créé précédemment dans la base d'objets (Cf. Etape1)

3 Etape 3 : Configuration d'un Serveur web

Sélectionnez l'onglet *Serveurs web*.

Cliquez sur le bouton Ajouter puis sélectionnez "Serveur web". Donnez un nom à votre serveur. L'écran de configuration du serveur Web s'affiche.

Au niveau de l'URL : chemin d'accès, indiquez CitrixAccess/auth/login.aspx (s'il s'agit de la version Presentation Server 4.0).

4 Envoi de la configuration

Cliquez sur le bouton Appliquer.

5 Accès au portail Web

Ouvrez un navigateur Web puis identifiez –vous (https://adresse IP de votre firewall ou son nom).

Allez dans "Accès sécurisé" puis 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.

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 desquels il faisait partie.

L'onglet « Profils utilisateurs »

Principe de fonctionnement

Par défaut tous les serveurs configurés dans le module VPN SSL sont affichés sur le portail d'authentification. Ainsi tous les utilisateurs ayant droit aux fonctionnalités de VPN SSL 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.

Configuration d'un profil

Ajout d'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** puis spécifiez le nom du profil.
2. Sélectionnez dans les listes : « Serveurs web accessibles » et « Serveurs applicatifs accessibles » les serveurs qui seront accessibles aux utilisateurs appartenant à ce profil.
3. 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.

Suppression d'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, 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 (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 VPN SSL\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.

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 puis appliquez les modifications en cliquant sur **Appliquer.**
2. Dans le module Utilisateurs \Droits d'accès VPN \Accès VPN, choisissez l'utilisateur puis dans la colonne « VPN SSL », choisir le profil défini au préalable et 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. Ouvrir un navigateur Web.
2. Indiquer dans la barre d'adresse, l'URL : https://Adresse_Firewall.
3. La page d'authentification sur le firewall apparaît, vous devez vous connecter.
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.

Support IPv6

Le support d'IPv6, proposé dans cette nouvelle 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. Ils sont également consultables depuis l'application SN Real-Time Monitor.

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 1.0, voici les principales fonctionnalités non disponibles pour le trafic IPv6 :

- La translation d'adresses IPv6 (NATv6),
- Inspections applicatives (Antivirus, Antispam, cache HTTP, 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 Radius ou Kerberos,
- Le Management de Vulnérabilités.

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 : Routage dynamique

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 :

Etat	Etat 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).
Couleur(Optionnel)	Une fenêtre s'affiche permettant de sélectionner une couleur d'interface (utilisée dans Stormshield Network REALTIME MONITOR).
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 :

Etat	Etat 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.

AVERTISSEMENTS

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. **Exemple** : 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).

En version Stormshield Network 1.0, 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, cache HTTP, filtrage URL, filtrage SMTP, filtrage FTP ou filtrage SSL)	[Règle X] Les inspections applicatives s'appliqueront uniquement sur le trafic IPv4.

Noms autorisés ou interdits

Voici les caractères autorisés ou interdits des éléments enregistrés sur votre firewall :

Nom du Firewall

Le nom du firewall ne peut contenir qu'au maximum 127 caractères. Les caractères autorisés sont :

```
<alphanum> - _ .
```

Identifiant & Mot de passe

- Identifiant (caractères interdits) :

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

- Identifiant PPTP (caractères autorisés) :

```
<alphanum> - _ .
```

- Mot de passe (caractères interdits) :

```
" <tab> <space>
```

Commentaires (caractères interdits)

```
" # @ < >
```

Séparateurs de règles (caractères interdits)

```
>
```

Nom d'interfaces

- Les noms des interfaces ne peuvent contenir les appellations suivantes si elles sont suivies immédiatement par des chiffres (ex : ethernet0, dialup123) :

```
loopback ethernet wifi dialup vlan bridge agg ipsec sslvpn gretun gretap
```

- Les noms ne doivent pas commencer par les préfixes suivants :

```
firewall network serial loopback
```

- Les noms ne doivent pas être un mot réservé :

```
Ipsec dynamic sslvpn any protected notprotected
```

- Les noms ne doivent pas comporter les caractères suivants :

```
@ " # <tab> <space>
```

Objets

- Caractères interdits :

```
<tab> <space> | ! " # , = @ [ \ ]
```

- Préfixes interdits :

```
Firewall_ Network_ ephemeral_ Global_
```

- Noms interdits :

```
any internet none anonymous broadcast all
```

Objets de type Nom DNS (FQDN)

Caractères interdits :

```
*
```

Certificats

Nom d'autorité de certification (caractères interdits) :

```
` " : _ [ / ]
```

Utilisateurs

- Nom d'utilisateur de la base (caractères interdits) :

```
<tab> " , ; & ~ | = * < > ! ( ) \
```

- Nom de groupe de la base Utilisateur (caractères interdits) :

```
<tab> <space> & ~ | = * < > ! ( ) \ $ % ! ' " `
```

- Chemin des Bases LDAP : DN, CA Dn et consort (caractères interdits) :

```
" & ~ | * < > ! ( )
```

VPN IPSec

Nom de correspondant IPSec (caractères interdits) :

```
# = @ [ \ ]
```

VPN SSL

- Identifiant du serveur web (caractères autorisés) :

```
<alphanum> - _ . :
```

- Préfixe du répertoire racine de l'URL (caractères autorisés) :

```
<alphanum> - _
```

Alertes e-mails

Nom des groupes d'e-mails (caractères interdits) :

```
<tab> <space> | ! " # , = @ [ \ ]
```

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.

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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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 Noms autorisés),
- 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"

STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2020. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.