STORMSHIELD

STORMSHIELD NETWORK SECURITY

NOTES DE VERSION

Version 4

Date : 18 décembre 2019

Référence : sns-fr-notes_de_version-v4.0.1

Table des matières

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

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Nouvelles fonctionnalités de la version 4.0.1

Filtrage

Filtrage des adresses MAC

SNS permet maintenant de définir et d'utiliser dans les politiques de filtrage des objets réseaux basés sur les adresses MAC seules afin de faire du filtrage de niveau 2 à l'image du mode *Stateful*.

Industrie

Support de PROFINET

PROFINET est un ensemble de protocoles utilisés dans les secteurs de la production, de l'agroalimentaire et des transports. PROFINET est composé entre autre de quatre protocoles principaux que sont PROFINET-IO, PROFINET-RT, PROFINET-DCP et PROFINET-PTCP.

SNS permet maintenant le filtrage de ces protocoles pour sécuriser ces environnements.

Licence industrielle

L'option de licence industrielle est maintenant vérifiée et la configuration des protocoles industriels est gelée si cette licence n'est pas présente (ou lorsque la maintenance du firewall est expirée).

Ergonomie

Nouvelle interface graphique

L'interface graphique de SNS version 4.0.1 a été totalement repensée pour améliorer l'ergonomie du produit (navigation entre configuration et monitoring facilitée).

Nouveau Tableau de bord simplifié

Le Tableau de bord a été simplifié pour apporter une meilleure visibilité de l'état du firewall. Un mécanisme d'analyse en profondeur (*drill down*) permet d'accéder aux informations détaillées en cas d'investigation.

Nouveau panneau de configuration du réseau

Le panneau de configuration du réseau a été simplifié afin de faciliter la configuration des interfaces.

Nouveau panneau de gestion des certificats

Le panneau de gestion des certificats a été simplifié pour faciliter la configuration de la PKI.

Nouveau panneau d'affichage des logs

Le panneau d'affichage des logs a été simplifié et propose exclusivement les logs sous formes de vues (regroupements thématiques).

Nouveau design *Responsive* du portail captif

Le portail captif adopte un nouveau design *Responsive* afin d'adapter son affichage à la taille d'écran utilisée et ainsi permettre son utilisation depuis un smartphone ou une tablette.

Suppression de l'assistant d'installation initiale
L'assistant d'installation initiale a été supprimé.

Management

Nouveaux indicateurs de santé
Deux nouveaux indicateurs de santé sont disponibles : le premier relatif à la température du CPU, et le second relatif au mot de passe d'administration si celui-ci est trop ancien ou est encore issu de la configuration par défaut.

Supervision des interfaces Wi-Fi
Il est maintenant possible de visualiser le monitoring des interfaces Wi-Fi.

Support de ARPING
La commande ARPING est maintenant disponible pour faciliter l'analyse.

Exporter une identité (contenant la clé privée) ou un certificat
Il est désormais possible d'exporter une identité (certificat utilisateur, serveur ou smartcard et clé privée associée) ou uniquement un certificat (utilisateur, serveur ou smartcard).

Optimisation de la procédure de mise à jour en mode cluster
La procédure de mise à jour d'un cluster a été optimisée afin d'éviter le double téléchargement du fichier de mise à jour.

Rafraîchissement de la configuration de SSHD
La configuration du service SSHD a été revue pour se conformer aux derniers standards de sécurité.

Télémétrie
Un service de télémétrie est désormais disponible sur SNS afin de maintenir des statistiques anonymes sur le cycle de vie des firewalls SNS. Ces statistiques sont destinées à améliorer la qualité et les performances des produits. Les indicateurs remontés dans cette version sont :

- Le pourcentage d'utilisation de CPU,
- Le pourcentage d'utilisation de mémoire,
- Le volume de logs générés.

Ce service (désactivé par défaut) peut être activé / désactivé au sein du module **Configuration** > onglet **Configuration Générale** > **Configuration avancée**.

Stabilité et performances

Refonte des mécanismes de la HA
Le mécanisme de synchronisation de la Haute Disponibilité a été simplifié pour offrir une meilleure stabilité et des performances accrues.

Refonte des mécanismes de proxy
Les fonctionnalités d'analyse antivirale et d'analyse par détonation (sandboxing - Breach Fighter) ont été extraites du service de proxy et fonctionnent dans un service séparé pour offrir plus de

stabilité.

Amélioration des performances IPS

Le mécanisme de gestion des connexions de l'IPS a été amélioré pour gagner en performances.

Simplification du plugin DCERPC

Le plugin DCERPC a été modifié pour faciliter sa configuration.

Amélioration générale des performances

Le système d'exploitation des firewalls SNS a été mis à jour pour de meilleures performances.

Antivirus ClamAV

Un nouveau paramètre mis à disposition par l'éditeur de l'antivirus ClamAV permet de limiter la durée d'analyse antivirale. Ceci ajoute une protection supplémentaire contre les attaques de type bombes de décompression (*Zip bombs*). Ainsi, si la durée d'une analyse laisse penser qu'un fichier analysé présente un volume de données excessivement important, celle-ci sera interrompue.

Ce paramètre, par défaut à 120 secondes, est uniquement modifiable à l'aide de la commande :

```
CONFIG ANTIVIRUS LIMITS MaxProcTime=<time>
```

Pour plus d'informations concernant la syntaxe de ces commandes, veuillez-vous référer au Guide de référence des commandes CLI / Serverd.

Matériel

Sécurisation matérielle des secrets des VPNs sur les modèles SN3100 compatibles

Depuis la révision A2 des firewalls modèles SN3100, ces derniers implémentent un module matériel (trusted platform module: TPM) dédié à la sécurisation des secrets de VPN. Celui-ci permet d'ajouter un niveau de sécurité additionnel pour les SN3100 dédiés à la concentration de VPNs et dont la sécurité physique n'est pas garantie. Cette version 4.0.1 introduit le support de ce module et permet sa configuration via l'interface et en ligne de commande.

SN6100 - Support des 7e et 8e modules 8x1G

SNS version 4.0.1 introduit le support de huit modules 8x1G sur le SN6100.

Vulnérabilités résolues de la version 4.0.1

Certificats et PKI

Des contrôles supplémentaires ont été implémentés lors de la manipulation des certificats afin d'interdire l'exécution de code JavaScript pouvant être intégré dans un certificat spécialement conçu dans un but malveillant. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

ClamAV

La vulnérabilité **CVE-2019-15961** permettant une attaque par déni de service à l'aide d'un e-mail spécialement conçu à cet effet a été corrigée par la mise à jour du moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

OpenSSL

Les vulnérabilités CVE-2019-1563, CVE-2019-1547 et CVE-2019-1552 ont été corrigées par la mise à jour de la bibliothèque cryptographique OpenSSL.

Le détail de ces vulnérabilités est disponible sur notre site https://advisories.stormshield.eu.

Protocole RTSP

Référence support 70716

Un défaut dans l'analyse IPS du protocole RTSP avec de l'entrelacement, principalement utilisé par les caméras IP, pouvait entraîner un redémarrage inopiné du produit. Ce défaut a été corrigé.

Notez que le support de l'entrelacement n'est pas activé dans la configuration d'usine.

Correctifs de la version 4.0.1

Système

VPN IPSec (IKEV1 + IKEv2)

Référence support 73584

Dans une configuration utilisant à la fois des correspondants IKEv1 et IKEv2, l'utilisation des champs UID (LDAP) et CertNID pour l'authentification est prise en compte et les contrôles de droits des utilisateurs à établir un tunnel IPSec ne sont ainsi plus ignorés.

Référence support 72290

Sur un firewall regroupant des correspondants IKEv1 et IKEv2, les groupes d'un utilisateur établissant un tunnel nomade IKEv1 avec authentification via certificat et XAUTH sont à nouveau pris en compte.

Sauvegardes automatiques - Cloud Backup

Référence support 73218

La restauration d'une sauvegarde de configuration depuis Cloud Backup est à nouveau fonctionnelle.

Système - Fuseau horaire

Référence support 69833

Le fuseau horaire Europe / Moscou du système a été mis à jour afin de corriger un décalage d'une heure.

Firewalls avec carte IXL

Pour les firewalls disposant d'une carte IXL :

- Modules d'extension réseau 4x10Gbps et 2x40Gbps fibre pour SN2100, SN3100 et SN6100,
- Modules 4x10G BASE-T pour SN710, SN910, SN2000, SN2100, SN3000, SN3100, et SN6100,
- Ports onboard 10Gbps fibre du SN6100.

Référence support 73005

Un problème de latence pouvant impacter les firewalls connectés à l'aide d'une carte IXL sur des équipements tiers a été corrigé.

Référence support 72957

Pour éviter certains problèmes de négociation liés à la détection automatique de vitesse du média, les valeurs disponibles pour les cartes réseau IXL peuvent désormais être sélectionnées dans le module **Réseau** > **Interfaces**.

Filtrage et NAT

Les champs **Forcer en IPSec les paquets source**, **Forcer en IPSec les paquets retour** et **Synchroniser cette connexion entre les firewalls (HA)** ont été ajoutés au fichier d'export CSV des règles de filtrage et NAT.

Haute Disponibilité

L'ajout d'un alias sur une interface réseau existante ne provoque plus de bascule HA au sein du cluster.

Haute Disponibilité - VPN IPSec

Référence support 74860

Les compteurs anti-rejeu de la SAD (Security Association Database) sont transmis vers le firewall passif, les numéros de séquence étant incrémentés afin de respecter le fonctionnement du mécanisme de Haute Disponibilité (HA).

Lorsque dans une configuration HA, le firewall passif détectait également du trafic IPSec (exemple : trames de supervision d'interfaces IPSec virtuelles), celui-ci transmettait à son tour au firewall actif des numéros de séquence incrémentés.

Suite à ces incrémentations successives, les numéros de séquence pouvaient alors rapidement atteindre les valeurs limites autorisées et déclencher à tort la protection anti-rejeu IPSec, bloquant ainsi les flux au travers des tunnels. Ce problème a été corrigé.

Haute disponibilité et supervision

Référence support 73615

Un risque de fuite mémoire a été corrigé dans le cas de configurations en Haute Disponibilité avec la supervision activée.

Configuration initiale par clé USB

Référence support 73923

La mise à jour de firmware via clé USB fonctionne de nouveau correctement.

Authentification par certificat

Un contrôle a été ajouté sur le contenu de certains paramètres utilisés lors de la création du cookie.

Rapports

Référence support 74730

Lors du redémarrage du firewall, une anomalie survenant au moment de l'activation de la base de données des rapports pouvait entraîner l'affichage de plusieurs messages d'erreur en console :

```
checkdb[181]: Missing database file: /var/db/reports/reports.db
enreport: checkdb: Unable to restore the reports database
enreport: Unable to mount the reports database.
```

Cette anomalie a été corrigée.

Port série - Éditeurs de fichiers

Référence support 72653

Une anomalie d'affichage lors de l'utilisation des éditeurs de fichiers Joe / Jmacs via le lien série a été corrigée.

Prévention d'intrusion

Référence support 73591

L'activation du mode verbeux du moteur de prévention d'intrusion associée à l'analyse de certains protocoles (DCE RPC, Oracle...) n'entraîne plus de potentiels redémarrages inopinés du firewall.

Interface Web d'administration

Routage statique

Références support 73316 - 73201

Dans le module **Réseau** > **Routage**, il est à nouveau possible de sélectionner l'interface IPSec lors de la définition d'une route statique.

Objets réseau

Référence support 73404

La présence de caractères accentués dans les commentaires d'objets réseau n'empêche plus le chargement correct des pages de l'interface Web d'administration.

DHCP - Serveur

Référence support 73071

Un message d'avertissement indique désormais qu'il n'est pas possible d'ajouter une réservation d'adresse IP lorsqu'un filtre d'affichage est actif.

DHCP - Relais

Référence support 72951

L'interface réseau éventuellement précisée pour relayer les requêtes DHCP était remplacée par la valeur par défaut (*automatique*) après avoir quitté et affiché de nouveau le module DHCP. Cette anomalie a été corrigée.

Caractères spéciaux

Références support 68883 - 72034 - 72125 - 73404

Une anomalie dans la conversion en UTF-8 de caractères spéciaux (caractères asiatiques ou accentués par exemple) pouvait générer des erreurs XML et empêcher l'affichage des modules impactés (Filtrage, NAT, Utilisateurs,...). Cette anomalie a été corrigée.

Certificats et PKI

Référence support 74111

L'affichage du contenu d'une CRL comportant plusieurs milliers de certificats révoqués pouvait ne pas aboutir selon le modèle de firewall. Ce problème a été corrigé et seuls les 1000 premiers éléments sont affichés.

Agent SNMP

Référence support 74337

Lors de la définition d'un serveur SNMPv3, les deux boutons de sélection d'algorithmes de chiffrement restaient systématiquement actifs après avoir été sélectionnés. Cette anomalie a été corrigée.

Protocole Modbus

Référence support 71166

Le firewall ne tenait pas comptes des informations saisies dans la grille UNIT ID autorisés (**Protection Applicative** > **Protocoles** > **Protocoles industriels** > **Modbus** > **Paramètres généraux**). Ces informations n'étaient également plus présentes dans la grille après avoir quitté le module.

Compatibilité

Version minimale requise

Vous devez disposer au minimum d'une version 3.x de Stormshield Network pour faire une mise à jour en 4.0.1.

Compatibilité matérielle

SN160(W), SN210(W), SN310, SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100
SNi40
Stormshield Network Elastic Virtual Appliances : EVA1, EVA2, EVA3, EVA4 et EVAU

Hyperviseurs

VMware ESXi	Versions 6.0, 6.5 et 6.7
Citrix Xen Server	Version 7.6 ou supérieure
Linux KVM	Red Hat Enterprise Linux 7.4 ou supérieure
Microsoft Hyper-V	Windows Server 2012 R2 ou supérieure

Logiciels clients Stormshield Network

SSO Agent	Version 1.9 ou supérieure
SSL VPN Client	Version 2.8 ou supérieure
IPSec VPN Client	Version 6.63.005 ou supérieure

Systèmes d'exploitation pour SN Real-Time Monitor

Microsoft Windows	Version 10
Microsoft Windows Serveur	Version 2012

Navigateurs web

Pour un fonctionnement optimal de l'interface d'administration des firewalls, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Edge, Google Chrome et Mozilla Firefox (version ESR - Extended Support Release). Pour de plus amples renseignements sur ces versions, nous vous invitons à consulter le cycle de vie des produits des éditeurs concernés.

Préconisations

Avant de migrer une configuration existante vers la version 4 de firmware, veuillez :

- Lire attentivement la section **Problèmes connus** de la Base de connaissance Stormshield (anglais uniquement - identifiants identiques à ceux de votre espace client MyStormshield),
- Lire attentivement la section Précisions sur les cas d'utilisation,
- **Réaliser une sauvegarde** de la partition principale vers la partition secondaire ainsi qu'une sauvegarde de configuration.

Migration

La mise à jour vers une version majeure de firmware provoque une réinitialisation des préférences de l'interface Web d'administration (exemple : filtres personnalisés).

Haute disponibilité - Migration

Lors de la mise à jour de SNS v3 vers SNS v4 du membre passif d'un cluster, les tunnels IPSec déjà établis sont renégociés. Ceci est un comportement normal.

Protocole PROFINET-RT

Référence support 70045

Une mise à jour du pilote de contrôleur réseau utilisé sur les firewalls modèles SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100 et SN6100 autorise désormais la gestion d'un VLAN ayant un identifiant égal à 0. Ceci est nécessaire pour le fonctionnement du protocole Industriel PROFINET-RT.

En revanche, les modules réseau IX (modules 2x10Gbps et 4x10Gbps fibre équipés du micro-composant INTEL 82599) et IXL (voir la liste des modules concernés) ne bénéficient pas de cette mise à jour et ne peuvent donc pas gérer le protocole PROFINET-RT.

Firewalls modèles SN160, SN210(W), SN310(W) - Routage dynamique Bird

Depuis la version 4.0.1 de firmware basée sur une nouvelle version de FreeBSD, le nom interne des interfaces a changé pour les firewalls modèles SN160, SN210(W) et SN310(W). Pour les configurations basées sur ces modèles de firewall et utilisant le routage dynamique Bird, il est nécessaire de modifier manuellement la configuration du routage dynamique pour indiquer les nouveaux noms des interfaces réseau.

Machines Virtuelles EVA

Il est recommandé de positionner la mémoire d'une machine EVA à 2 Go en cas d'utilisation intensive de l'antivirus et du sandboxing.

Microsoft Internet Explorer

L'utilisation du navigateur Microsoft Internet Explorer, y compris dans sa version 11, peut entraîner une importante dégradation de l'expérience utilisateur. Il est donc fortement recommandé d'utiliser l'un des navigateurs listés dans la section Compatibilité.

Mise à jour d'un cluster avec plusieurs liens de haute disponibilité

Pour un cluster mettant en œuvre plus d'un lien dédié à la haute disponibilité, il est nécessaire de s'assurer que le lien principal est actif avant de procéder à la mise à jour en version 4.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SNS est consultable sur la Base de connaissance Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissance, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Précisions sur les cas d'utilisation

Réseau

Modems 4G

Référence support 57403

La connectivité du firewall à un modem USB 4G nécessite l'utilisation d'un équipement de marque HUAWEI supportant la fonction HiLink (exemple : E8372H-153).

Protocoles Spanning Tree (RSTP / MSTP)

Les firewalls Stormshield Network ne supportent pas les configurations multi-régions MSTP. Un firewall implémentant une configuration MSTP et positionné en interconnexion de plusieurs régions MSTP pourrait ainsi rencontrer des dysfonctionnements dans la gestion de sa propre région.

Un firewall ayant activé le protocole MSTP, et ne parvenant pas à dialoguer avec un équipement qui ne supporte pas ce protocole, ne bascule pas automatiquement sur le protocole RSTP.

De par leur fonctionnement, les protocoles RSTP et MSTP ne peuvent pas être activés sur les interfaces de type VLAN et modems PPTP/PPPoE.

Interfaces

Sur les firewalls modèle SN160(W) et SN210(W), la présence d'un switch interne non administrable entraîne l'affichage permanent des interfaces réseau du firewall en état « up », même lorsque celles-ci ne sont pas connectées physiquement au réseau.

Les interfaces du firewall (VLAN, interfaces PPTP, interfaces agrégées [LACP], etc.) sont rassemblées dans un pool commun à l'ensemble des modules de configuration. Lorsqu'une interface précédemment utilisée dans un module est libérée, elle ne devient réellement réutilisable pour les autres modules qu'après un redémarrage du firewall.

La suppression d'une interface VLAN provoque un ré-ordonnancement de ce type d'interfaces au redémarrage suivant. Si ces interfaces sont référencées dans la configuration du routage dynamique ou supervisées via la MIB-II SNMP, ce comportement induit un décalage et peut potentiellement provoquer un arrêt de service. Il est donc fortement conseillé de désactiver une interface VLAN non utilisée plutôt que de la supprimer.

L'ajout d'interfaces Wi-Fi dans un bridge est en mode expérimental et ne peut pas s'effectuer via l'interface graphique.

Sur les modèles SN160(W), une configuration comportant plusieurs VLANs inclus dans un bridge n'est pas supportée.

Une configuration avec un bridge incluant plusieurs interfaces non protégées et une route statique sortant de l'une de ces interfaces (autre que la première) n'est pas supportée.

Routage dynamique Bird

Avec le moteur de routage dynamique Bird en version 1.6.7, il est nécessaire, dans les configurations utilisant le protocole BGP avec de l'authentification, d'utiliser l'option "*setkey no*". Pour de plus amples informations sur la configuration de Bird, veuillez consulter la Note Technique "**Routage dynamique Bird**".

Lorsque le fichier de configuration de Bird est édité depuis l'interface d'administration Web, l'action **Appliquer** envoie effectivement cette configuration au firewall. En cas d'erreur de syntaxe, la configuration n'est pas prise en compte et un message d'avertissement indiquant le numéro de ligne en erreur informe de la nécessité de corriger la configuration. En revanche, une configuration erronée envoyée au firewall sera prise en compte au prochain redémarrage du service Bird ou du firewall, empêchant alors le chargement correct du service Bird.

Routage par politique de filtrage

Si une remise en configuration d'usine du firewall (*defaultconfig*) est réalisée suite à une migration de la version 2 vers la version 3 puis vers la version 4, l'ordre d'évaluation du routage est modifié et le routage par politique de filtrage [PBR] devient prioritaire (routage par politique de filtrage > routage statique > routage dynamique > ... > routage par défaut). En revanche, en l'absence de remise en configuration d'usine du firewall, l'ordre d'évaluation reste inchangé par rapport à la version 1 (routage statique > routage dynamique > routage par politique de filtrage [PBR] > routage par interface > routage par répartition de charge > routage par défaut).

VPN IPSec

IPSec - Politique mixte IKEv1 / IKEv2

L'utilisation de correspondants IKEv1 et IKEv2 au sein d'une même politique IPSec entraîne plusieurs restrictions ou obligations :

- Le mode de négociation "agressif" n'est pas autorisé pour un correspondant IKEv1 avec authentification par clé pré-partagée. Un message d'erreur est affiché lors de la tentative d'activation de la politique IPSec.
- La méthode d'authentification "Hybride" ne fonctionne pas pour un correspondant nomade IKEv1.
- Les correspondants de secours sont ignorés. Un message d'avertissement est affiché lors de l'activation de la politique IPSec.
- L'algorithme d'authentification "*non_auth*" n'est pas supporté pour un correspondant IKEv1. Dans un tel cas, la politique IPSec ne peux pas être activée.
- Dans une configuration mettant en œuvre du NAT-T (NAT-Traversal - Passage du protocole IPSec au travers d'un réseau réalisant de la translation d'adresses dynamique), il est **impératif** de définir l'adresse IP translatée comme identifiant d'un correspondant utilisant l'authentification par clé pré-partagée et pour lequel un ID local sous la forme d'une adresse IP aurait été forcé.

Déchiffrement

La répartition du déchiffrement des données est réalisée par correspondant IPSec. Sur les firewalls multi-processeur, ce traitement est donc optimisé lorsque le nombre de correspondants est au moins égal au nombre de processeurs du firewall.

PKI

La présence d'une liste des certificats révoqués (CRL) n'est pas requise. Si aucune CRL n'est trouvée pour l'autorité de certification (CA), la négociation sera autorisée.

La présence d'une CRL peut être rendue obligatoire à l'aide du paramètre "CRLRequired=1" de la commande en ligne (CLI) CONFIG IPSEC UPDATE.

Référence support 37332

DPD (Dead Peer Detection)

La fonctionnalité VPN dite de DPD (Dead Peer Detection) permet de vérifier qu'un correspondant est toujours opérationnel, par des requêtes de test de disponibilité.

Si un firewall est répondeur d'une négociation IPSEC en mode principal, et a configuré le DPD en « Inactif », ce paramètre sera forcé en « passif » pour répondre aux sollicitations DPD du correspondant. En effet, pendant cette négociation IPSEC, le DPD est négocié avant d'avoir identifié le correspondant, et donc avant de connaître si les requêtes DPD peuvent être ignorées pour ce correspondant.

Ce paramètre n'est pas modifié en mode agressif, car dans ce cas le DPD est négocié lorsque le correspondant est déjà identifié, ou dans le cas où le firewall est initiateur de la négociation.

Keepalive IPv6

Pour les tunnels IPSec site à site, l'option supplémentaire keepalive, permettant de maintenir ces tunnels montés de façon artificielle, n'est pas utilisable avec des extrémités de trafic adressées en IPv6. Dans le cas d'extrémités de trafic configurées en double pile (adressage IPv4 et IPv6), seul le trafic IPv4 bénéficiera de cette fonctionnalité.

VPN IPSec IKEv2

Le protocole EAP (Extensible Authentication Protocol) ne peut pas être utilisé pour l'authentification de correspondants IPSec utilisant le protocole IKEv2.

Dans une configuration mettant en œuvre un tunnel IPSec basé sur le protocole IKEv2 et de la translation d'adresse, l'identifiant présenté par la machine source au correspondant distant pour établir le tunnel correspond à son adresse IP réelle et non à son adresse IP translatée. Il est donc conseillé de forcer l'identifiant local à présenter (champ **Local ID** dans la définition d'un correspondant IPSec IKEv2) en utilisant l'adresse translatée (si celle-ci est statique) ou un FQDN porté par le firewall source.

Il n'est pas possible de définir une configuration de secours pour les correspondants IPSec utilisant le protocole IKEv2. Pour mettre en œuvre une configuration IPSec IKEv2 redondante, il est conseillé d'utiliser des interfaces virtuelles IPSec et des objets routeurs dans les règles de filtrage (PBR).

Support IPv6

En version 4, 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,
- Les interfaces modems (en particulier les modems PPPoE).

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, entraînant des problèmes de routage en cas de bascule.

Système

Référence support 51251

Serveur DHCP

Lors de la réception d'une requête DHCP de type INFORM émise par un client Microsoft, le firewall envoie au client son propre serveur DNS primaire accompagné du serveur DNS secondaire paramétré dans le service DHCP. Il est conseillé de désactiver le protocole Web Proxy Auto-Discovery Protocol (WPAD) sur les clients Microsoft afin d'éviter ce type de requêtes.

Mises à jour vers une version antérieure

Les firewalls préinstallés avec un firmware en version 4 ne sont pas compatibles avec les versions majeures antérieures.

Le retour à une version majeure de firmware antérieure à la version courante du firewall nécessite préalablement une remise en configuration d'usine du firewall (*defaultconfig*). Ainsi par exemple, cette opération est nécessaire pour la migration d'un firewall d'une version 4.0.1 vers une version 3.x.

Référence support 3120

Configuration

Le client NTP des firewalls ne supporte la synchronisation qu'avec les serveurs utilisant la version 4 du protocole.

Restauration de sauvegarde

Il n'est pas possible de restaurer une sauvegarde de configuration réalisée sur un firewall dont la version du système était postérieure à la version courante. Ainsi, par exemple, il n'est pas possible de restaurer une configuration sauvegardée en 4.0.1, si la version courante du firewall est la 3.9.2.

Objets dynamiques

Les objets réseau en résolution DNS automatique (objets dynamiques), pour lesquels le serveur DNS propose un type de répartition de charge round-robin, provoquent le rechargement de la configuration des modules uniquement si l'adresse actuelle n'est plus présente dans les réponses.

Objets de type Nom DNS (FQDN)

Les objets de type Nom DNS ne peuvent pas être membres d'un groupe d'objets.

Une règle de filtrage ne peut s'appliquer qu'à un unique objet de type Nom DNS. Il n'est donc pas possible d'y ajouter un second objet de type FQDN ou un autre type d'objet réseau.

Les objets de type Nom DNS ne peuvent pas être utilisés dans une règle de NAT. Notez qu'aucun avertissement n'est affiché lorsqu'une telle configuration est réalisée.

Lorsque aucun serveur DNS n'est disponible, l'objet de type Nom DNS ne contiendra que l'adresse IPv4 et/ou IPv6 renseignée lors de sa création.

Si un nombre important de serveurs DNS est renseigné dans le firewall, ou si de nouvelles adresses IP concernant un objet de type Nom DNS sont ajoutées au(x) serveur(s) DNS, l'apprentissage de l'ensemble des adresses IP de l'objet peut nécessiter plusieurs requêtes DNS de la part du firewall (requêtes espacées de 5 minutes).

Si les serveurs DNS renseignés sur les postes clients et sur le firewall diffèrent, les adresses IP reçues pour un objet de type Nom DNS peuvent ne pas être identiques. Ceci peut, par exemple, engendrer des anomalies de filtrage si l'objet de type DNS est utilisé dans la politique de filtrage.

Journaux de filtrage

Lorsqu'une règle de filtrage fait appel au partage de charge (utilisation d'un objet routeur), l'interface de destination référencée dans les journaux de filtrage n'est pas forcément correcte. En effet, les traces de filtrage étant écrites dès qu'un paquet réseau correspond aux critères de cette règle, l'interface de sortie n'est alors pas encore connue. C'est donc la passerelle principale qui est systématiquement reportée dans les journaux de filtrage.

Qualité de service

Les flux réseaux auxquels sont appliquées des files d'attente de qualité de service (QoS) ne tirent pas entièrement bénéfice des améliorations de performances liées au mode « fastpath ».

Antivirus Kaspersky

L'option **Activer l'analyse heuristique** n'est pas supportée sur les modèles SN160(W), SN210(W) et SN310.

Notifications

IPFIX

Les événements envoyés via le protocole IPFIX n'incluent ni les connexions du proxy, ni les flux émis par le firewall lui-même (exemple : flux ESP pour le fonctionnement des tunnels IPSec).

Rapports d'activités

La génération des rapports se base sur les traces (logs) enregistrées par le firewall et celles-ci sont générées à la clôture des connexions. En conséquence, les connexions toujours actives (exemple : tunnel IPSec avec translation) ne seront pas affichées dans les statistiques affichées par les rapports d'activités.

Les traces générées par le firewall dépendent du type de trafic qui ne nomme pas forcément de la même façon les objets (*srcname* et *dstname*). Pour éviter de multiples représentations d'un même objet dans les rapports, il est conseillé de donner à l'objet créé dans la base du firewall, le même nom que celui associé via la résolution DNS.

Prévention d'intrusion

Protocole SSL

Depuis la version 3.7.0 de firmware, les suites de chiffrement présentant un niveau de sécurité faible (suites basées sur MD5, SHA1 et DES) ne sont plus disponibles pour le protocole SSL utilisé par les différents composants du firewall (VPN SSL, Proxy SSL,...).

Pour les configurations qui utilisent ces suites de chiffrement, il est nécessaire de choisir des algorithmes de niveau de sécurité supérieur avant d'effectuer la migration du firewall en version

SNS 3.7.0 ou supérieure. Dans le cas contraire, les services concernés ne fonctionneront pas ou refuseront de démarrer.

Protocole GRE et tunnels IPSec

Le déchiffrement de flux GRE encapsulés dans un tunnel IPSec génère à tort l'alarme « *Usurpation d'adresse IP sur l'interface IPSec* ». Il est donc nécessaire de configurer l'action à *passer* sur cette alarme pour faire fonctionner ce type de configuration.

Analyse HTML

Le code HTML réécrit n'est pas compatible avec tous les services web (apt-get, Active Update) parce que l'en-tête HTTP « Content-Length » a été supprimé.

Messagerie instantanée

Le NAT sur les protocoles de messagerie instantanée n'est pas supporté.

Référence support 35960

Préserver le routage initial

L'option permettant de préserver le routage initial sur une interface n'est pas compatible avec les fonctionnalités pour lesquelles le moteur de prévention d'intrusion doit créer des paquets :

- la réinitialisation des connexions lors de la détection d'une alarme bloquante (envoi de paquet RESET),
- la protection SYN Proxy,
- la détection du protocole par les plugins (règles de filtrage sans protocole spécifié),
- la réécriture des données par certains plugins tels que les protections web 2.0, FTP avec NAT, SIP avec NAT et SMTP.

NAT

Support H323

Le support des opérations de translation d'adresses du protocole H323 est rudimentaire, en particulier : il ne supporte pas les cas de contournement du NAT par les gatekeeper (annonce de l'adresse autre que source ou destination de la connexion).

Proxies

Référence support 35328

Proxy FTP

Si l'option « conserver l'adresse IP source originale » est activée sur le proxy FTP, le rechargement de la politique de filtrage entraîne l'interruption des transferts FTP en cours (en upload ou download).

Filtrage

Interface de sortie

Une règle de filtrage précisant une interface de sortie incluse dans un bridge, et qui ne serait pas la première interface de ce bridge, n'est pas exécutée.

Filtrage Multi-utilisateur

Il est possible de permettre l'authentification Multi-utilisateur à un objet réseau (plusieurs utilisateurs authentifiés sur une même adresse IP) en renseignant l'objet dans la liste des Objets Multi-utilisateurs (Authentification > Politique d'authentification).

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 à cette catégorie d'objet. Ce comportement est inhérent au mécanisme de traitement des paquets effectué par le moteur de prévention d'intrusion. Le message explicite avertissant l'administrateur de cette limitation est le suivant : « Cette règle ne peut identifier un utilisateur connecté sur un objet multi-utilisateur ».

Géolocalisation et réputation des adresses IP publiques

Lorsqu'une règle de filtrage précise des conditions de géolocalisation et de réputation d'adresses publiques, il est nécessaire que ces deux conditions soient remplies pour que la règle soit appliquée.

Réputation des machines

Si les adresses IP des machines sont distribuées via un serveur DHCP, la réputation d'une machine dont l'adresse aurait été reprise par une autre machine sera également attribuée à celle-ci. Dans ce cas, la réputation de la machine peut être réinitialisée à l'aide de la commande CLI `monitor flush hostrep ip = host_ip_address`.

Référence support 31715

Filtrage URL

Le filtrage différencié par utilisateur n'est pas possible au sein d'une politique de filtrage URL. Il est toutefois possible d'appliquer des règles de filtrage particulières (inspection applicative) et d'associer à chacune un profil de filtrage URL différent.

Authentification

Portail captif - Page de déconnexion

La page de déconnexion du portail captif ne fonctionne que pour les méthodes d'authentification basées sur des mots de passe.

SSO Agent

La méthode d'authentification Agent SSO se base sur les évènements d'authentification collectés par les contrôleurs de domaine Windows. Ceux-ci n'indiquant pas l'origine du trafic, la politique d'authentification ne peut être spécifiée avec des interfaces.

Référence support 47378

Les noms d'utilisateurs contenant les caractères spéciaux suivants : " <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` @ <espace> ne sont pas pris en charge par l'Agent SSO. Le firewall ne recevra donc pas les notifications de connexions et déconnexions relatives à ces utilisateurs.

Domaines Microsoft Active Directory multiples

Dans le cadre de domaines Microsoft Active Directory multiples liés par une relation d'approbation, il est nécessaire de définir dans la configuration du firewall un annuaire Active Directory et un agent SSO pour chacun de ces domaines.

Les méthodes SPNEGO et Kerberos ne peuvent pas être utilisées sur plusieurs domaines Active Directory.

La phase 1 de négociation IPSec n'est pas compatible avec les annuaires Microsoft Active Directory multiples pour l'authentification des clients mobiles.

Le protocole IKEv1 nécessite l'emploi de l'authentification étendue (*XAUTH*).

Annuaires multiples

Les utilisateurs définis comme administrateurs du firewall doivent obligatoirement être issus de l'annuaire par défaut.

Les utilisateurs ne peuvent s'authentifier que sur l'annuaire par défaut via les méthodes certificat SSL et Radius.

Méthode CONNECT

L'authentification multi-utilisateur sur une même machine en mode Cookie, ne supporte pas la méthode CONNECT (protocole HTTP). Cette méthode est généralement utilisée avec un proxy explicite pour les connexions HTTPS. Pour ce type d'authentification, il est recommandé d'utiliser le mode « transparent ». Pour plus d'informations, consultez l'aide en ligne à l'adresse documentation.stormshield.eu, section Authentification.

Conditions d'utilisation

L'affichage des Conditions d'utilisation d'accès à Internet sur le portail captif peut avoir un rendu incorrect sous Internet Explorer v9 avec le mode compatibilité IE Explorer 7.

Utilisateurs

La gestion d'annuaires LDAP multiples impose une authentification précisant le domaine d'authentification : user@domain.

Le caractère spécial « espace » dans les identifiants (« login ») des utilisateurs n'est pas supporté.

Déconnexion

La déconnexion d'une authentification ne peut se faire que par la méthode utilisée lors de l'authentification. Par exemple, un utilisateur authentifié avec la méthode Agent SSO ne pourra pas se déconnecter via le portail d'authentification, car l'utilisateur doit fournir pour la déconnexion, un cookie n'existant pas dans ce cas.

Comptes temporaires

Lors de la création d'un compte temporaire, le firewall génère automatiquement un mot de passe d'une longueur de 8 caractères. Dans le cas d'une politique globale de mots de passe imposant une longueur supérieure à 8 caractères, la création d'un compte temporaire génère alors une erreur et le compte ne peut pas être utilisé pour s'authentifier.

L'utilisation des comptes temporaires nécessite donc une politique de mots de passe limités à 8 caractères maximum.

Haute Disponibilité

Interaction HA en mode bridge et switches

Dans un environnement avec un cluster de firewalls configurés en mode bridge, le temps de bascule du trafic constaté est de l'ordre de 10 secondes. Ce délai est lié au temps de bascule d'1 seconde auquel vient s'ajouter le temps de réapprentissage des adresses MAC par les switches qui sont directement connectés aux firewalls.

Routage par politique

Une session routée par la politique de filtrage peut être perdue en cas de bascule du cluster.

Modèles

La Haute Disponibilité basée sur un groupe (cluster) de firewalls de modèles différents n'est pas supportée. D'autre part, un groupe avec un firewall utilisant un firmware en 32 bits et l'autre en 64 bits n'est pas autorisé.

VLAN dans un agrégat d'interfaces et lien HA

Référence support 59620

Le choix d'un VLAN appartenant à un agrégat d'interfaces (LACP) comme lien de haute disponibilité n'est pas autorisé. En effet, cette configuration rend le mécanisme de haute disponibilité inopérant sur ce lien: l'adresse MAC attribuée à ce VLAN sur chacun des firewalls est alors 00:00:00:00:00:00.

Management des vulnérabilités

Référence support 28665

L'inventaire d'applications réalisé par le Management des vulnérabilités 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 importante sur le module. Il est donc conseillé de mettre les adresses de ces machines dans la liste d'exclusion (éléments non supervisés).

Suite d'administration Stormshield Network

Référence support 28665

La commande CLI MONITOR FLUSH SA ALL est initialement dédiée à désactiver les tunnels IPsec en cours, en supprimant leur association de sécurité (SA - security association). Cependant, le routage dynamique Bird utilisant également ce type d'association de sécurité (SA), cette commande dégrade la configuration de Bird, empêchant toute connexion. Ce problème se pose également avec la fonction « Réinitialiser tous les tunnels » proposée dans l'interface de Real Time Monitor.

Pour résoudre ce problème, il est nécessaire de redémarrer le service Bird.

Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de Documentation Technique Stormshield ou sur le site Institute de Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Stormshield Network Firewall - Manuel d'utilisation et de configuration
- Elastic Virtual Appliances - Guide d'installation
- Stormshield Network Real-Time Monitor - Manuel d'utilisation et de configuration
- CLI Serverd - Commands reference guide
- CLI Console / SSH - Commands reference guide
- Stormshield Network Pay As You Go - Guide de déploiement

Notes techniques

- Configuration SSO : Microsoft SPNEGO
- Configurer les méthodes "Guest"
- Adapter la politique de sécurité SES d'un poste selon sa réputation SNS
- Configurations de base en Interface ligne de commande (CLI)
- Configurer un modem 3G/4G sur SNS
- Filtrer les connexions HTTPS
- Identifier les commandes de protocoles industriels traversant le firewall
- Configuration initiale par clé USB
- Stacking : répartition de trafics sur plusieurs firewalls
- Sauvegardes automatiques
- Se conformer aux règlements sur les données personnelles
- Signatures de protection contextuelle personnalisées
- Sécurité collaborative
- Mise en œuvre d'une règle de filtrage
- Restauration logicielle par clé USB
- Option Secure Return
- Mise à jour du firmware IPMI
- Échange d'un module d'alimentation
- Description des journaux d'audit
- Routage dynamique BIRD
- EVA sur Amazon Web Services
- EVA sur Microsoft Azure
- VMWare NSX - Firewall SNS dans le rôle d'un routeur périphérique
- Interfaces virtuelles IPSec
- Intégration du NAT dans IPSec

- Tunnels VPN SSL
- VPN IPSec : Authentification par clé pré-partagée
- VPN IPSec : Authentification par certificats
- VPN IPSec : Configuration Hub and Spoke

Vidéos

- Commandes et scripts CLI, disponible sur Institute.

Merci de consulter la Base de connaissance Stormshield pour obtenir des informations techniques spécifiques et pour accéder aux vidéos créées par l'équipe du support technique (Technical Assistance Center).

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Network Security :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur l'espace client MyStormshield, rubrique Téléchargements.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/

La soumission d'une requête auprès du support technique doit se faire par le biais du gestionnaire d'incidents présent dans l'espace client MyStormshield, menu **Support technique** > **Rapporter un incident / Suivre un incident**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace client MyStormshield.

STORMSHIELD