STORMSHIELD

STORMSHIELD NETWORK SECURITY

NOTES DE VERSION

Version 4

Dernière mise à jour du document : 13 octobre 2021

Référence : sns-fr-notes_de_version-v4.2.2

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.

Vulnérabilités résolues de la version 4.2.2

Portail d'authentification

Une vulnérabilité de sévérité moyenne a été corrigée dans l'API de gestion du portail d'authentification.

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

OpenLDAP

Une vulnérabilité de sévérité moyenne a été corrigée par la mise à jour du composant OpenLDAP.

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

OpenSSL

Une vulnérabilité de sévérité moyenne a été corrigée par la mise à jour du composant OpenSSL.

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

Commandes CLI / Serverd

Une vulnérabilité de sévérité forte a été corrigée dans le mécanisme des commandes CLI / Serverd.

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

ClamAV

Des vulnérabilités de sévérité moyenne ont été corrigées dans le moteur antiviral ClamAV.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu,
- https://advisories.stormshield.eu.

FreeBSD

Une vulnérabilité de sévérité moyenne a été corrigée par l'application d'un correctif FreeBSD.

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

Matériel

Une vulnérabilité de sévérité faible a été corrigée par l'application d'un nouveau micro-code pour les processeurs Intel.

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

Correctifs de la version 4.2.2

Système

Certificats et PKI

Référence support 81909

A l'ouverture du module **Certificats et PKI**, le processus de recherche automatique permettant d'afficher la liste des CA, des identités et des certificats échouait lorsque le DN d'un certificat excédait 127 caractères. Le contenu du module **Certificats et PKI** ne pouvait alors pas être affiché. Ce problème a été corrigé.

VPN IPSec

Référence support 82179

Lorsqu'une politique IPSec respectait les deux conditions suivantes :

- La politique débutait par une ou plusieurs règles de *bypass* : règles dont le correspondant est *None*, destinées à créer une exclusion aux règles suivantes de la politique de chiffrement. Le trafic de ces règles est régi par la politique de routage.
- Ces règles étaient suivies de plusieurs règles distinctes de tunnels IPSec mobiles.

Alors le fichier de configuration IPSec généré était erroné et seul le premier tunnel mobile configuré parvenait à s'établir. Ce problème a été corrigé.

VPN IPSec - Tunnels site à site IKEv1

Références support 82199 - 82197

Suite au changement de moteur de gestion des tunnels IPSec IKEv1, un firewall en version 4.2.1 ne pouvait plus négocier de tunnel IPSec IKEv1 avec un firewall SNS en version 4.1.x (ou inférieure) lorsque les deux conditions suivantes étaient réunies :

- Le firewall en version 4.1.x utilisait une politique IPSec exclusivement basée sur des correspondants IKEv1,
- Le firewall en version 4.2.1 était initiateur de la négociation.

Ceci est dû à l'introduction de la fonction ESN, non supportée par les versions 4.1.x (et inférieures), et à un problème lié au nouveau moteur de gestion des tunnels IPSec.
Afin de résoudre ce problème, un firewall en version 4.2.2 (ou supérieure) désactive l'ESN lorsque le correspondant est en IKEv1.

Machines virtuelles

VPN IPSec

Référence support 81914

Lors de l'installation d'une machine virtuelle EVA SNS 4.2.1 au format OVA, le moteur de gestion des tunnels VPN IPSec échouait à démarrer. Aucun tunnel IPSec ne pouvait donc être établi. Ce problème a été corrigé.

Interface Web d'administration

VPN IPSec - Authentification par certificats

Référence support 82185

Lors de la sélection du certificat d'un correspondant IPSec, la liste déroulante pouvait ne laisser apparaître que les certificats créés par défaut (certificats issus des CA proxy SSL et VPN SSL). Cette liste affiche de nouveau correctement tous les autres certificats présents dans la PKI.

Compatibilité

Version minimale requise

Vous devez disposer au minimum d'une version 3.7.18 LTSB, 3.11.6 LTSB, 4.1.1 ou 4.2.1 de Stormshield Network pour faire une mise à jour en 4.2.2.

Compatibilité matérielle

SN160(W), SN210(W), SN310, SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100
SNi20 et SNi40
Stormshield Network Elastic Virtual Appliances : EVA1, EVA2, EVA3, EVA4, EVAU et VPAYG

Hyperviseurs

VMware ESXi	Versions 6.5 et 6.7
Citrix Xen Server	Version 7.6
Linux KVM	Red Hat Enterprise Linux 7.4
Microsoft Hyper-V	Windows Server 2012 R2 et 2019

Authentification - Serveurs Microsoft

Radius Kerberos Microsoft Active Directory - LDAP(S)	Windows Server 2012 R2 et 2019
SPNEGO	Windows Server 2012 R2, 2016 et 2019

Logiciels clients Stormshield Network

SSO Agent Windows	Version 3.0.1
SSO Agent Linux	Version 3.0.1
SSL VPN Client	Version 2.9.1
IPSec VPN Client	Version 6.64.003

SN Real-Time Monitor

SN Real-Time Monitor version 4.0.0 n'est pas compatible avec les firewalls en version 4.2.1 et 4.2.2. Une version spécifique de SN Real-Time Monitor compatible avec les firewalls SNS en version 4.2 sera proposée ultérieurement.

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.

VPN IPSec

La version 4.2 de firmware n'assure plus le support des algorithmes suivants :

- Blowfish,
- DES,
- CAST128,
- MD5,
- HMAC_MD5,
- NON_AUTH,
- NULL_ENC.

Si la politique IPSec d'un firewall devant être mis à jour en version 4.2 utilise l'un ou l'autre de ces algorithmes, il est impératif de remplacer ces algorithmes dans la configuration IPSec du firewall avant de réaliser cette mise à jour.

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 et SN210(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 et SN210(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.

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

VPN IPSec

Interruption de négociation d'une phase 2

Le moteur de gestion IPSec Charon, utilisé dans le cadre de politiques IKEv1, peut interrompre tous les tunnels avec le même correspondant si une seule phase 2 échoue.

Cela est dû à l'absence de notification de la part du correspondant suite à un échec de négociation lié à une différence d'extrémités de trafic.

Comme indiqué plus haut, le comportement du moteur de gestion IPSec Racoon a été modifié en version 4.1.0 afin que cela ne se produise pas dans le cadre d'un tunnel Racoon <=> Charon.

Vous pouvez néanmoins être confronté à ce problème dans le cas où le moteur de gestion IPSec Charon négocie avec un équipement qui n'émet pas de notification d'échec.

Restrictions IPSec

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 peut 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.

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 en envoyant des messages ISAKMP.

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 annoncé 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).

SN Real-Time Monitor

SN Real-Time Monitor version 4.0.0 n'est pas compatible avec les firewalls en version 4.2.1 et 4.2.2. Une version spécifique de SN Real-Time Monitor compatible avec les firewalls SNS en version 4.2 sera proposée ultérieurement.

Réseau

Routage - Réseau directement connecté à une interface du firewall

Référence support 79503

Lorsqu'un réseau est directement connecté à une interface du firewall, le firewall crée une route implicite d'accès à ce réseau. Cette route est appliquée en amont des règles de PBR (Policy Based Routing - Filtrage par politique) : le routage par PBR est donc ignoré pour ces réseaux directement connectés.

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 1.6.8, 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).

Système

Référence support 78677

Cookies générés pour l'authentification multi-utilisateurs

Suite à l'implémentation d'une nouvelle politique de sécurité sur les navigateurs Web du marché, l'authentification multi-utilisateurs SNS n'est plus fonctionnelle dans le cas où un site non sécurisé (via HTTP) est consulté.

Ce comportement aboutit à l'affichage d'un message d'erreur ou d'un avertissement selon le navigateur Web utilisé, et est lié au fait que les cookies d'authentification du proxy ne peuvent pas utiliser l'attribut "Secure" conjointement à l'attribut "SameSite" dans le cadre d'une connexion non sécurisée HTTP.

Pour rétablir la navigation sur ces sites, une opération manuelle doit être effectuée dans la configuration du navigateur Web.

En savoir plus

Préférences de l'interface Web d'administration

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

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.

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.

Antivirus Kaspersky

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

Agrégation de liens (LACP)

Référence support 76432

L'agrégation de liens (LACP) n'est pas compatible avec le module réseau SFP+ 40G LM4 (référence NA-TRANS-QSFP40-SR).

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.

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.

Support IPv6

En version SNS 4, voici les principales fonctionnalités non disponibles pour le trafic IPv6 :

- Le trafic IPv6 au travers de tunnels IPSec basés sur des interfaces IPSec virtuelles (VTI),
- La translation d'adresses IPv6 (NATv6),
- Inspections applicatives (Antivirus, Antispam, Filtrage URL, Filtrage SMTP, Filtrage FTP, Filtrage SSL),
- L'utilisation du proxy explicite,
- Le cache DNS,
- Les tunnels VPN SSL portail,
- Les tunnels VPN SSL,
- L'authentification via 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.

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 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.

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.

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.

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
- CLI Serverd - Commands reference guide
- CLI Console / SSH - Commands reference guide
- Stormshield Network Pay As You Go - Guide de déploiement

Notes techniques

Authentification

- Configuration SSO : Microsoft SPNEGO
- Configurer les méthodes "Guest"
- Stormshield Network SSO Agent pour Windows
- Stormshield Network SSO Agent pour Linux

Configuration

- Adapter la politique de sécurité SES d'un poste selon sa réputation SNS
- Configurations de base en Interface ligne de commande (CLI)
- Configuration initiale par clé USB
- Configurer un modem 3G/4G sur SNS
- Filtrer les connexions HTTPS
- Haute disponibilité sur SNS
- Identifier les commandes de protocoles industriels traversant le firewall
- Mise en œuvre d'une règle de filtrage
- Stacking : répartition de trafics sur plusieurs firewalls
- Sauvegardes automatiques
- Se conformer aux règlements sur les données personnelles
- Signatures de protection contextuelle personnalisées
- Sécurité collaborative

Hardware

- Restauration logicielle par clé USB
- Option Secure Return

- Mise à jour du firmware IPMI
- Échange d'un module d'alimentation

Logs

- Description des journaux d'audit

Routage

- Routage dynamique BIRD

SNS for Cloud

- EVA sur Amazon Web Services
- EVA sur Microsoft Azure
- VMWare NSX - Firewall SNS dans le rôle d'un routeur périphérique

VPN

- Intégration du NAT dans IPSec
- Interfaces virtuelles IPSec
- Tunnels VPN SSL
- VPN IPSec Mobile IKEv1 - Authentification par clé pré-partagée
- VPN IPSec Mobile IKEv2 - Authentification par clé pré-partagée
- 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).

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 4.2.2 de Stormshield Network Security :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

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.

Versions précédentes de Stormshield Network Security 4

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de Stormshield Network Security 4.

4.2.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.1.6	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.1.5			Correctifs
4.1.4			Correctifs
4.1.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.1.2			Correctifs
4.1.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.0.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.0.2	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.0.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs

Nouvelles fonctionnalités de la version 4.2.1

Système

Mode Diffusion Restreinte (DR)

Les firewalls SNS proposent l'implémentation d'un mode IPSec renforcé appelé **Mode Diffusion Restreinte (DR)** et respectant les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

En version SNS 4.2, de nombreuses mesures de renforcement ont été apportées au Mode DR, notamment :

- La négociation des tunnels IPSec est désormais exclusivement réalisée sur le port UDP/4500, rendant la détection du NAT-T (NAT traversal) inutile,
- Les tunnels VPN IPSec peuvent être uniquement basés sur le protocole IKEv2,
- Le support de l'ESN pour l'anti-rejeu ESP est implémenté,
- La création d'une politique VPN IPSec active le jeton de configuration *CRLRequired,*
- Restrictions concernant les algorithmes d'authentification et de chiffrement autorisés,
- Deux profils de chiffrement spécifiques "Mode DR" (un pour IKE, un pour IPSec) ont été ajoutés aux profils existants (StrongEncryption, GoodEncryption et Mobile).

IMPORTANT
Le Mode DR de la version SNS 4.2 n'est pas compatible avec le Mode DR des versions SNS précédentes et la mise à jour d'un firewall avec le Mode DR activé vers la version SNS 4.2.0 (ou supérieure) est refusée par le firewall. Il est nécessaire de désactiver le mode DR pour pouvoir réaliser la mise à jour du firewall.

En savoir plus

Modification des traces activées par défaut

Le stockage sur disque de certaines traces (dont les connexions) est désormais désactivé par défaut sur un firewall en version SNS 4.2 en configuration d'usine. Les seules traces activées et stockées par défaut sont les suivantes :

- Administration (fichier log *l_server*),
- Authentification (fichier log *l_auth*),
- Événements système (fichier *l_system*),
- Alarmes (fichier *l_alarm*),
- Politiques de filtrage (fichier log *l_filter*),
- Négociation IKE/ IPSec (fichier log *l_vpn*),
- VPN IPSec (fichier log *l_vpn*),
- VPN SSL (fichier log *l_xvpn*),
- Statistiques du filtrage et statistiques IPSec (fichier log *l_monitor*),
- Sandboxing (fichier log *l_sandboxing*).

Le stockage sur disque des autres traces peut être activé manuellement dans le module **Traces - Syslog - IPFIX**.

En savoir plus

VPN IPSec IKEv1

Le moteur de gestion des tunnels VPN IPSec IKEv1 est désormais identique à celui gérant les VPN IPSec IKEv2 (Strongswan Charon).

Les configurations listées ci-dessous ne sont plus autorisées en version 4.2 :

- Règles IKEv1 basées sur l'authentification par clé pré-partagée en mode agressif (tunnels nomades et tunnels site à site),
- Règles IKEv1 basées sur l'authentification en mode hybride (tunnels nomades),
- Correspondants de secours IKEv1.

Il est donc nécessaire de mettre en conformité la politique IPSec active (respect des restrictions pour une politique mixte IKEv1 / IKEv2) avant de mettre à jour le firewall en version 4.2.

En savoir plus

VPN IPSec

La répartition des opérations de chiffrement / déchiffrement du module IPSec a été améliorée : ceci induit une amélioration notable des débit IPSec dans le cas d'une configuration comportant un seul tunnel IPSec.

Ce mécanisme d'optimisation peut être activé ou désactivé manuellement à l'aide de la commande CLI / Serverd :

```
CONFIG IPSEC UPDATE slot=<x> CryptoLoadBalance=<0|1>
```

où <x> est le N° de la politique IPSec active.

Le détail de cette commande est disponible dans le Guide de référence des commandes CLI / Serverd.

En savoir plus

Une nouvelle commande CLI / Serverd `PKI CA CHECKOCSP` a été ajoutée afin de pouvoir surcharger l'URL d'un serveur OCSP dans les certificats utilisés pour la négociation de tunnels IPSec.

En savoir plus

Logs - Type de règle VPN IPSec

Un champ précisant le type de règle VPN (tunnel mobile ou tunnel site à site) a été ajouté aux logs VPN IPSec.

En savoir plus

Logs - Nom de règle VPN IPSec

Il est désormais possible, depuis le module de configuration VPN IPSec, de rechercher directement le nom d'une règle dans les logs VPN IPSec afin d'afficher les traces correspondantes.

Agent SNMP

Dans le cas d'une politique IPSec IKEv2 ou IKEv1 + IKEv2, un événement (*trap*) SNMP est désormais émis lorsqu'un correspondant VPN IPSec est injoignable.

Une nouvelle MIB (STORMSHIELD-OVPNTABLE-MIB) permet de superviser via SNMP les utilisateurs connectés au travers du VPN SSL.

La MIB STORMSHIELD-VPNSA-MIB propose des statistiques IPSec complémentaires. Deux nouvelles MIB IPSec lui ont été adjointes :

- STORMSHIELD-VPNIKESA-MIB : cette MIB propose des informations sur les SA IKE négociées,
- STORMSHIELD-VPNSP-MIB : cette MIB présente propose des informations sur les SP (Security Policies).

Toutes les MIB SNS sont téléchargeables depuis la rubrique MIBS du site institutionnel Stormshield.

En savoir plus

Calcul d'entropie - TPM (Trusted Platform Module)

Les firewalls équipés d'un module TPM utilisent désormais ce TPM comme source d'entropie dans les fonctions cryptographiques. L'entropie de ces fonctions cryptographiques en est donc améliorée.

Calcul d'entropie - Politique de mots de passe

L'entropie, dont le calcul prend en compte l'imprédictibilité d'un mot de passe et le nombre de caractères le composant, a été intégrée à la définition de la politique de mot de passe pour assurer la robustesse de ces mots de passe.

Il est donc désormais possible d'imposer une valeur minimale d'entropie pour les mots de passe définis sur le firewall (comptes de services, comptes d'administration, mots de passe de sauvegardes automatiques,...).

En savoir plus

Haute disponibilité

Dans une configuration en haute disponibilité, en cas de défaillance d'une interface d'un nœud du cluster, le temps de bascule du nœud passif en état actif a été significativement réduit sur les modèles SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN2100, SN3000, SN3100, SN6000 et SN6100, réduisant ainsi la coupure du trafic réseau.

En savoir plus

Authentification SPNEGO

Référence support 73844

La version 4.2 de firmware introduit le support de Windows Server 2019 pour la méthode d'authentification SPNEGO. La version 1.7 du script *spnego.bat*, disponible dans l'espace client Mystormshield, doit être utilisée sur cette version de Windows Server.
Cette version du script est également compatible avec Windows Server 2016, 2012 et 2012 R2.

Authentification - Annuaire LDAP interne

Pour une sécurité accrue, le hachage des mots de passe contenus dans l'annuaire LDAP interne peut désormais être réalisé à l'aide des algorithmes SHA2 ou PBKDF2.

En savoir plus

Authentification - Portail captif

Sur un firewall configuré en mode HTTPS strict (à l'aide la commande CLI / Serverd `CONFIG AUTH HTTPS sslparanoiac=1`), la configuration du portail captif n'accepte plus la sélection de certificats autres que des certificats serveur comportant l'*ExtendedKeyUsage ServerAuth*.

Avant de mettre à jour un firewall en version 4.2, il est donc nécessaire de sélectionner un certificat de portail captif conforme à cette exigence.

Authentification - Agent SSO

La connexion des agents SSO au service d'authentification du firewall est désormais basée sur le protocole TLS v1.2 en lieu et place de SSLv3. Il est donc nécessaire d'utiliser l'Agent SSO v3.0 (ou supérieur) avec les firewalls SNS en version 4.2

Logs - Emplacement des fichiers *verbose.**

Les fichiers de logs créés lors de l'activation du mode verbeux des services du firewall sont désormais placés dans un répertoire dédié /log/verbose et non plus directement dans le répertoire /log. Les fichiers existants sont automatiquement déplacés vers ce nouveau répertoire lors de la mise à jour du firewall en version 4.2.

Commandes CLI / Serverd

Les commandes CLI / Serverd sont désormais versionnées pour permettre un meilleur suivi des changements. Une section présentant les modifications, ajouts ou suppressions de commandes CLI / Serverd entre la dernière version SNS et la version SNS LTSB précédente a été ajouté en première partie du Guide de référence des commandes CLI / Serverd.

Les commandes CLI / Serverd relatives à la gestion du VPN IPSec (`CONFIG IPSEC PROFILE PHASE1` et `CONFIG IPSEC PROFILE PHASE2`) ont été modifiées afin d'offrir la possibilité de vérifier la configuration avant que celle-ci ne soit appliquée sur le firewall.
Ceci permet ainsi d'éviter les interruptions de service en cas d'anomalie dans la configuration.

En savoir plus

Restauration de configuration

Un mécanisme de contrôle d'intégrité de la configuration réseau permet désormais d'éviter des erreurs de configuration de firewalls lors de déploiements via SMC ou lors de restaurations de sauvegardes de configuration.

La restauration partielle d'une configuration est précédée d'une analyse de cohérence. Lorsque le mécanisme d'analyse détecte une anomalie, celui-ci affiche un message d'avertissement. L'administrateur peut toutefois décider de restaurer cette sauvegarde, mais des modifications de configuration devront être réalisées pour rendre opérationnels les modules concernés par la restauration.

VPN SSL

Dans le cadre du durcissement du système d'exploitation SNS, le fichier de configuration destiné au client VPN SSL Stormshield inclut le paramètre *auth-nocache* pour imposer au client de ne pas conserver le mot de passe utilisateur en mémoire (à l'exception des clients VPN SSL configurés en **Mode manuel**).

Clés SSH du firewall

Dans le cadre du durcissement du système d'exploitation SNS, les clés SSH du firewall (clé du firewall pour les connexions SSH vers le firewall, clés créées pour la haute disponibilité, clé du compte *admin*) sont désormais chiffrées par défaut à l'aide de l'algorithme ECDSA en lieu et place de l'algorithme RSA utilisé avant la version SNS 4.2.

La clé SSH du firewall est désormais générée à l'activation du service SSHD du firewall (et non au démarrage du firewall) afin de présenter une meilleure entropie (robustesse de la clé). Elle peut également être à nouveau générée à l'aide de la commande CLI / Serverd `CONFIG SSH REGENHOSTKEY`.

La clé SSH du compte *admin* est systématiquement générée à chaque changement de mot de passe de ce compte. Il est donc conseillé de modifier ce mot de passe après avoir mis à jour un firewall en version 4.2.

En savoir plus

Protocole TLS v1.3

La version SNS 4.2 introduit le support du protocole TLS v1.3 pour les services du firewall (portail captif, LDAPS, Syslog TLS, Autoupdate ...).

Les versions du protocole TLS utilisables par les clients à destination du firewall sont désormais exclusivement les versions 1.2 et 1.3. La version du protocole TLS utilisable peut être configurée à l'aide de la simple commande CLI Serverd :

```
CONFIG CRYPTO ClientTLSv12=<0|1> ClientTLSv13=<0|1>
```

Pour plus de détails sur cette commande, veuillez vous référer au Guide de référence des commandes CLI / Serverd.

Notez que l'implémentation du protocole LDAPS basé sur TLS1.2 ou TLS 1.3 nécessite que le serveur hébergeant un annuaire LDAP externe supporte et utilise une suite de chiffrement compatible.
La liste de ces suites de chiffrement est détaillée dans le Manuel Utilisateur SNS v4.

NSRPC

L'algorithme SHA256 est désormais utilisé dans la librairie NSRPC pour le calcul des *hash* des mots de passe.

Mise à jour - Logs

Référence support 79529

Des traces concernant les actions exécutées avant le redémarrage du firewall ont été ajoutées dans le fichier *update.log* afin de discerner les causes d'échecs de mise à jour de firmware.

Prévention d'intrusion

Protocole TLS v1.3

Le moteur de prévention d'intrusion détecte et analyse désormais les trames déchiffrées du protocole de sécurisation des communications TLS v1.3. Ceci permet notamment :

- D'autoriser le mode 0-RTT,
- De définir le comportement à adopter vis à vis des valeurs / extensions (extensions GREASE [Generate Random Extensions And Sustain Extensibility], extensions définies dans la RFC TLS v1.3 ou extensions inconnues est paramétrable).
- De définir une liste noire d'extensions TLS.

Notez que les flux liés peuvent désormais être assujettis à des alarmes protocolaires.

En savoir plus

Protocole RDP sur UDP

Le moteur de prévention d'intrusion détecte et analyse désormais le trafic RDP basé sur UDP en plus du trafic RDP basé sur TCP.

Notez que les flux liés peuvent désormais être assujettis à des alarmes protocolaires.

Protocole IPv6

La version 4.2 introduit la détection et le blocage de paquets IPv6 contenant une option RDNSS (*Recursive DNS Server*) non conforme (cf. RFC 8106).

Interface Web d'administration

Supervision VPN IPSec

Le module de supervision VPN IPSec intègre désormais deux tables présentant les caractéristiques des Security Associations (SA) du tunnel VPN IPSec sélectionné :

- Table des SA IKE :
  - Nom de la règle IPSec,
  - Version IKE du tunnel,
  - Passerelle locale,
  - Adresse IP de la passerelle locale,
  - Passerelle distante,
  - Adresse IP de la passerelle distante,
  - État de la SA,
  - Rôle (responder / initiator),
  - Cookie initiator,
  - Cookie responder,
  - Identifiant local,
  - Identifiant du correspondant,
  - Présence de NAT-T ou non,
  - Algorithme d'authentification utilisé,
  - Algorithme de chiffrement utilisé,
  - Algorithme de PseudoRandom Function (PRF) utilisé,
  - Perfect Forward Secrecy (PFS) utilisé,
  - Durée de vie de écoulée.
- Table des SA IPSec :
  - État de la SA,
  - Passerelle locale,
  - Passerelle distante,
  - Octets entrants,
  - Octets sortants,
  - Durée de vie écoulée,
  - Algorithme d'authentification utilisé,
  - Algorithme de chiffrement utilisé,
  - Présence d'ESN,
  - Encapsulation UDP des paquets ESP activée.

Tableau de bord

Le tableau de bord intègre un nouveau widget **Messages** destiné à afficher les notifications et avertissements issus du système. Des messages y sont affichés si :

- IPv6 est activé sur le firewall,
- Le mode DR est activé sur le firewall,
- Le moteur d'authentification utilise les certificats par défaut du firewall.

Supervision des interfaces

Le module de supervision des interfaces peut désormais afficher des courbes (temps réel et historique) de débit et de nombre de paquets échangés pour les VLAN définis sur le firewall.

Les courbes historiques de débit et de nombre de paquets échangés sont désormais également disponibles pour les agrégats d'interfaces.

Protocoles - NTP

Un clic sur le lien associé à la **Protection contre les attaques de type Time Poisoning** (**Configuration** > **Protection applicative** > **Protocoles** > **NTP** > onglet **IPS**) permet désormais d'accéder directement à la configuration de l'horloge du firewall.

En savoir plus

Certificats et PKI

L'interface Web d'administration autorise désormais la création d'un certificat dont le FQDN comporte le caractère spécial "*" (exemple : *.stormshield.eu).

Vulnérabilités résolues de la version 4.2.1

Processeurs Intel

Les microcodes des processeurs Intel utilisés sur les firewalls modèles SN510, SN710, SN910, SN2000, SN3000, SN2100, SN3100 et SN6100 ont été mis à jour afin de corriger les vulnérabilités CVE-2020-0543, CVE-2020-0548 et CVE-2020-0549.

Interface Web d'administration / Pages de blocage

Afin de contrer une possible faille XSS, l'affichage de prévisualisation HTML des pages de blocage HTTP n'est plus disponible. Seul le texte brut du code HTML des pages de blocage est affiché.

Interface Web d'administration / Portail d'authentification

Une protection supplémentaire contre l'injection de code a été ajoutée aux réponses émises par l'interface Web d'administration et le portail d'authentification du firewall.

OpenSSL

Une vulnérabilité d'un score global CVSS de 3.0 a été corrigée par la mise à jour du composant OpenSSL.

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

Requêtes NDP

L'accumulation jusqu'à un certain seuil de requêtes NDP (IPv6) sans réponse déclenchait le mécanisme de protection de la table NDP du firewall. Ceci entraînait la perte des premiers paquets d'une communication vers un hôte inconnu le temps que la résolution des requêtes NDP se réalise.

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

Authentification - Agent SSO

Un firewall SNS refuse désormais toute négociation avec un agent SSO utilisant les suites de chiffrement AES_CBC.
Il est donc nécessaire d'utiliser l'agent SSO v3 avec un firewall SNS 4.2.

ClamAV

Une vulnérabilité d'un score global CVSS de 5.8 a été corrigée dans le moteur antiviral ClamAV.

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

Protocole SNMP

Référence support 80471

Une vulnérabilité d'un score global CVSS de 5.5 dans le mécanisme de protection lié à l'analyse protocolaire SNMP a été corrigée.

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

Correctifs de la version 4.2.1

Système

Sauvegarde de configuration - Trusted Platform Module (TPM)

Référence support 79671

Lors d'une sauvegarde de configuration avec le paramètre *privatekeys* positionné à *none* (paramètre uniquement modifiable à l'aide de la commande CLI / Serverd : `CONFIG BACKUP`), les clés privées stockées en mode *ondisk* sur le TPM ne sont plus déchiffrées à tort.

Référence support 79671

Il n'est plus possible de lancer deux sauvegardes de configuration en même temps ou dans un laps de temps très court. Les clés privées stockées en mode *ondisk* sur le TPM ne sont ainsi plus déchiffrées à tort.

Haute disponibilité

Sur les configurations en haute disponibilité, une optimisation a été apportée à l'option **Redémarrer toutes les interfaces pendant le basculement (à l'exception des interfaces HA)**, destinée à indiquer aux équipements tiers de connexion réseau (commutateurs,...) tout changement de rôle au sein du cluster. Cette option n'est en effet plus activée sur des agrégats de liens lorsque la case **Activer l'agrégation de liens lorsque le firewall est passif** est cochée.

En savoir plus

Les erreurs survenant lors de la mise à jour du membre passif d'un cluster sont désormais correctement affichées dans l'interface Web d'administration du firewall

Haute disponibilité - Clés SSH

Lors du passage à une version SNS antérieure (accompagné d'une remise en configuration d'usine du firewall) d'une configuration en haute disponibilité générée en version 4.2, les clés SSH du cluster sont désormais correctement supprimées.

Haute disponibilité - Annuaire LDAP

Référence support 78461

Une anomalie dans la synchronisation des données LDAP, liée à une mauvaise gestion du caractère spécial "\" potentiellement présent dans le mot de passe d'accès à l'annuaire, rendait cet annuaire LDAP inopérant. Cette anomalie a été corrigée.

Haute disponibilité - Synchronisation des objets

Référence support 77441

Le mécanisme de synchronisation des objets entre les membres du cluster cessait de fonctionner lorsque le serveur DNS utilisé pour résoudre les objets de type FQDN n'acceptait pas les requêtes DNS basées sur TCP. Cette anomalie a été corrigée.

Proxies

Référence support 79204

Des problèmes de fuites mémoire dans les proxies ont été corrigés.

Références support 79957 - 80108 - 79952

Dans une configuration utilisant de l'authentification multi-utilisateurs, le chargement complet d'une page Web intégrant une directive CSP (*content-security-policy*) pouvait dysfonctionner. Cette anomalie a été corrigée.

Référence support 79858

Un problème d'accès concurrentiel lors de l'enregistrement d'une nouvelle connexion par le proxy a été corrigé. Ce problème pouvait entraîner un arrêt inopiné du firewall et un changement de rôle des membres d'une configuration en haute disponibilité.

Proxy SMTP

Référence support 78196

Un redémarrage inopiné du proxy pouvait survenir suite à la mise en file d'attente d'un e-mail et de la réception d'une erreur SMTP 421 émise par le serveur. Cette anomalie a été corrigée.

Référence support 77586

L'activation du proxy SMTP, associée au déchiffrement SSL des flux sortants et à l'analyse antivirale sur le trafic SMTP (avec l'action *Passer sans analyser* pour les options **Lorsque l'antivirus ne peut analyser** et **Lorsque la collecte de données échoue** du paramétrage de l'analyse protocolaire SMTP) ne provoque plus à tort la journalisation multiple des mêmes événements dans le fichier *l_smtp*.

Proxy HTTP

Référence support 79584

Dans une configuration possédant toutes les conditions suivantes :

- Le proxy HTTP est utilisé,
- L'antivirus Kaspersky est activé,
- Le filtrage d'URL est activé.

L'émission par un navigateur Internet de plusieurs requêtes HTTP contenues au sein d'une connexion TCP unique (*pipelining*) n'est plus susceptible de provoquer un redémarrage inopiné du service proxy.

Agent SNMP

Références support 77226 - 78235

L'OID "SNMPv2-MIB::sysObjectID.0", permettant d'identifier la nature de l'équipement interrogé, présentait la valeur par défaut liée à *net-snmp* au lieu de présenter la valeur propre à Stormshield. Cette anomalie a été corrigée.

Références support 77787 - 78693 - 77779 - 78164 - 78967

Des problèmes de consommation mémoire excessive aboutissant à un arrêt inopiné du service Agent SNMP ont été corrigés.

Référence support 78761

Les messages SNMP informRequest sont désormais considérés comme une requête SNMP valide et ne génèrent plus l'alarme bloquante "Protocole SNMP invalide" (snmp:388).

Configuration des annuaires

Références support 70940 - 71329 - 75280 - 77783

La longueur maximale de la chaîne de caractères représentant le sujet du certificat importé pour autoriser la connexion SSL à l'annuaire LDAP interne a été portée de 128 à 256 caractères.

VPN IPSec

Références support 78593 - 73609

Pour les topologies IPSec déployées via SMC, les certificats des correspondants n'étaient pas affichés dans la configuration IPSec du firewall.

Ce problème, qui pouvait inciter un administrateur à sélectionner de nouveau un certificat pour le correspondant, rendant alors la configuration IPSec inopérante, a été corrigé.

VPN IPSec - Règles de filtrage implicite

Référence support 77096

La règle de filtrage implicite "Autoriser ISAKMP (port 500 UDP) et le protocole ESP pour les correspondants VPN IPSec" autorise désormais le trafic IPSec initialisé par des interfaces internes de type *loopback*.

VPN IPSec - Nom de correspondant

Un nom de correspondant de plus de 44 caractères n'empêche plus l'établissement du tunnel IPSec concerné.

Réputation des machines

Référence support 77080

La présence d'un objet invalide dans la liste des machines dont la réputation est supervisée ne provoque plus une erreur système lors d'une tentative de rechargement du proxy.

En savoir plus

Filtrage et NAT

Référence support 78647

L'export au format CSV des règles de filtrage / NAT générait à tort une valeur "Any" pour le champ "#nat_to_target" du fichier d'export, dans le cas où une règle de filtrage n'était associée à aucune règle de NAT. Cette anomalie empêchait alors l'import de ce fichier CSV dans SMC si la règle de filtrage concernée avait pour action "Bloquer".

Référence support 76700

En cas d'erreur de configuration au sein de la politique de filtrage, le firewall ne chargeait aucune règle de filtrage (y compris implicite) lors d'un redémarrage et bloquait donc tous les flux. Ce problème, qui imposait alors d'accéder en console série / VGA au firewall afin d'activer une politique fonctionnelle, a été corrigé.

Référence support 79526

Lorsqu'un groupe contenait 128 objets ou plus dont au moins un avec une adresse MAC forcée, la règle utilisant ce groupe n'était plus jamais appliquée lorsqu'un flux lui correspondait. Cette anomalie a été corrigée.

Références support 79533 - 79636 - 80412 - 80376

Lors de l'activation ou désactivation d'un objet temps, la réévaluation des connexions correspondant à la règle de filtrage contenant cet objet temps ne provoque plus un redémarrage inopiné du firewall.

Référence support 79311

Une règle de translation d'adresse précisant une adresse IP destination et / ou un port destination pour le trafic après translation ne fonctionnait pas au travers d'un tunnel IPSec. Cette anomalie a été corrigée.

VPN SSL

Lors de la tentative d'établissement d'un tunnel VPN SSL avec un firewall dont le mode "furtif" (*stealth mode*) est désactivé, le premier paquet envoyé par le client VPN SSL n'est plus ignoré à tort par le firewall et le tunnel s'établit correctement.

Supervision des tunnels VPN SSL

Référence support 77801

Le nom des utilisateurs connectés via VPN SSL était affiché en clair dans le module de supervision de ces tunnels, même lorsque l'administrateur connecté ne bénéficiait pas de l'accès aux données personnelles. Cette anomalie a été corrigée.

Authentification - Comptes temporaires

Référence support 79296

Lorsque la politique de sécurité définie sur le firewall exige une longueur de mots de passe supérieure à 8 caractères, l'ajout, la modification ou la suppression de la méthode d'authentification de type comptes temporaires ne génère plus une erreur système.

Certificats et PKI

Les Certificate Revocation List (CRL) renseignées dans les certificats sont désormais téléchargées au même titre que celles précisées dans les CA.

Configuration initiale par clé USB

Référence support 75370

Lorsque plusieurs périphériques sont connectés (exemple : clé USB et carte SD), seule la clé USB est désormais prise en compte.

Prévention d'intrusion

Protocole SSL

Référence support 77817

Une erreur dans la déclaration du champ *ExtensionLength* de l'analyse protocolaire SSL provoquait à tort des alarmes bloquantes "Paquet SSL invalide" (alarme ssl:118) pour des paquets SSL *Client Hello* légitimes. Cette anomalie a été corrigée.

Protocole SMB v2

Référence support 78216

Une anomalie dans le moteur d'analyse du protocole SMB pouvait provoquer à tort l'alarme "Protocole NBSS/SMB2 invalide" (alarme nb-cifs:157) et ainsi entraîner le blocage de flux SMBv2 légitimes. Cette anomalie a été corrigée.

Protocole SMB - CIFS

Références support 77484 - 77166

Des anomalies dans l'analyse protocolaire SMB - CIFS pouvaient provoquer à tort l'alarme bloquante "Protocole NBSS/SMB invalide" (alarme nb-cifs:158) lors d'un accès légitime à une ressource disque partagée Microsoft Windows. Ces anomalies ont été corrigées.

Protocole DNS

Référence support 77256

Une anomalie dans l'analyse protocolaire DNS provoquait à tort l'alarme bloquante "Attaque possible DNS rebinding" (alarme dns:154) lors de la réponse d'un serveur DNS présentant une adresse IP externe composée de son adresse IPv6 concaténée avec son adresse IPv4 (*mapping IPv4 - IPv6*). Cette anomalie a été corrigée.

Protocole SMTP

Référence support 77661

Dans une configuration telle que :

- Le moteur de prévention d'intrusion analyse le protocole SMTP,
- L'analyse antivirale est activée pour les flux SMTP,
- Le moteur d'analyse antivirale Kaspersky est utilisé sur le firewall,
- Une Taille max. pour l'analyse antivirale et sandboxing est paramétrée.

L'analyse d'un e-mail contenant une pièce jointe excédant la taille définie ne déclenche plus à tort l'alarme bloquante "Protocole SMTP invalide" (alarme smtp:121).

Mode *Fastpath*

Références support 76810 - 77932

Un problème d'accès concurrentiel lors de l'injection des statistiques de connexions dans le moteur de prévention d'intrusion a été corrigé. Ce problème pouvait provoquer une consommation CPU importante ainsi qu'un rejet inopiné de paquets réseau sur les interfaces IX (modules 2x10Gbps et 4x10Gbps fibre).

Matériel

Configuration par clé USB

Références support 79645 - 79283

Lors de la configuration d'un firewall à l'aide d'une clé USB, un message d'information est désormais affiché en console et un délai d'attente de deux minutes est initié lorsqu'il est nécessaire de retirer la clé USB pour continuer les opérations en cours (mise à jour de firmware, rattachement d'un firewall à un cluster). Le retrait de la clé USB interrompt ce compteur.

Ce mécanisme permet d'éviter les erreurs de déchiffrement de clés sur les firewalls disposant d'un TPM (SN3100, SNi20).

En savoir plus

Machines virtuelles

Numéros de série des firewalls VPAYG

Référence support 76157

Les numéros de série des firewalls VPAYG (numéro de série du firewall auquel est ajoutée une extension de type "-XXXXXXXX") n'étaient pas reconnus par le mécanisme de supervision de la haute disponibilité. Cette anomalie a été corrigée.

Firewalls EVA déployés sur VMWare avec interfaces 10Gb/s

Référence support 76546

Pour les firewalls déployés sur une infrastructure VMWare, le débit maximal affiché pour des interfaces 10Gb/s utilisant le pilote *vmxnet3* n'est plus limité à tort à 10Mb/s.

Interface Web d'administration

Interfaces

Référence support 77682

La suppression d'une interface GRETAP parente d'un VLAN masquait ce VLAN de la liste des interfaces bien qu'il soit toujours défini dans la configuration du firewall. Cette opération laisse désormais bien visible le VLAN à la racine de la liste des interfaces disponibles.

Référence support 77014

L'état de connexion des interfaces USB / Ethernet (4G) est désormais correctement détecté par le système et affiché dans le module **Configuration** > **Réseau** > **Interfaces**.

Interfaces - Profils de configuration des modems

Un compte administrateur en lecture seule ne pouvait pas afficher les profils de configuration des modems. Cette anomalie a été corrigée.

Interfaces - GRETAP

Référence support 78800

Le MTU affecté à une interface GRETAP lors de sa création est de nouveau correct (1462 octets contre 1500 dans les versions 4 précédentes).

Protocoles

Référence support 78157

Après avoir édité et modifié un nom de profil d'analyse protocolaire puis changé de module de configuration, au retour dans le module d'analyse protocolaire modifié, le menu **Éditer** n'est plus vide.

Protocoles - BacNET/IP

Le service avec confirmation *confirmedTextMessage* apparaissait à tort deux fois dans le groupe *Remote Device Management* (identifiants 19 et 20). L'identifiant 20 est désormais correctement affecté au service *reinitializeDevice*.

Sauvegardes automatiques - Serveur personnalisé

Référence support 78018

Le port défini lors de la création d'un serveur de sauvegarde personnalisé est de nouveau correctement présent dans l'URL affichée au sein du module de configuration.

Veuillez noter qu'il ne s'agissait que d'une anomalie d'affichage.

En savoir plus

Authentification - Méthode Radius

Référence support 76824

Lors de l'accès à la configuration du serveur Radius, si le champ clé pré-partagée était accidentellement effacé, une clé pré-partagée vide était enregistrée en lieu et place de la valeur précédente. Ce problème a été corrigé et le firewall refuse toute valeur vide pour ce champ.

Filtrage d'URL - Filtrage SSL

Référence support 77458

Le résultat de la catégorisation d'une URL (modules **Filtrage d'URL** et **Filtrage SSL**) ne reste plus affiché en permanence en bas de l'écran même lors d'un changement de module.

Référence support 79017

La modification simultanée de plusieurs règles de filtrage SSL ou de filtrage d'URL entraînait un nombre anormalement élevé de commandes système. Cette anomalie a été corrigée.

Objets Web - Groupes d'objets

Référence support 76325

Le champ de recherche des groupes de catégories n'est plus sensible à la casse.

Objets Web

Référence support 76327

Un clic sur la colonne de tri du contenu immédiatement après la création d'une nouvelle catégorie d'URL ou de certificats :

- Ne crée plus d'erreur système si aucune autre catégorie n'était sélectionnée lors de l'opération de création,
- N'affiche pas à tort le contenu d'une autre catégorie si celle-ci était sélectionnée lors de l'opération de création.

VPN IPSec

Référence support 74210

L'ajout d'un séparateur de règles IPSec dans une politique comportant plus d'une page de règles ne provoque plus le renvoi systématique à la première page de cette politique IPSec.

Références support 74966 - 75821

Un double-clic sur un séparateur de règles IPSec ouvre correctement celui-ci en édition, et la modification de ce séparateur est de nouveau pleinement fonctionnelle.

Référence support 75810

Lors de la création ou de la modification d'un correspondant, le passage d'une authentification par certificat à une authentification par clé pré-partagée, suivi d'un retour à une authentification par certificat sans avoir rechargé la page de configuration, ne provoque plus d'erreur système liée à la détection du certificat initialement sélectionné.

Références support 77246 - 77264 - 77274

La création ou de la modification d'un correspondant dont la configuration contenait une erreur (signalée par un message dans le champ de **Vérification de la politique**) pouvait néanmoins être validée. Cette anomalie, qui entraînait une erreur de rechargement de la configuration VPN IPSec, a été corrigée.

Référence support 77443

La création, modification ou suppression d'une clé pré-partagée depuis la grille des clés pré-partagées pour les tunnels mobiles (module **Configuration** > **VPN IPSec** > onglet **Identification**) n'est plus susceptible de créer un conflit de clés et d'empêcher l'établissement des tunnels IPSec utilisant ces clés.

VPN IPSec - Correspondants

Des contrôles additionnels ont été ajoutés pour une meilleure gestion de la duplication, du renommage ou de la suppression d'un correspondant en cours de modification (modifications non sauvegardées).

Certificats et PKI

Référence support 78965

Après avoir importé dans la PKI une CA externe (opération uniquement réalisable en ligne de commande), il n'était pas possible de déclarer cette CA comme CA par défaut (pour le proxy SSL par exemple), ou de sélectionner cette CA lors de la création d'une identité (utilisateur, serveur...). Cette anomalie a été corrigée.

Il est désormais possible de renseigner des alias (champ *Subject Alternative Name*) lors de la création d'une identité serveur. Les dernières versions des navigateurs Web exigent parfois ce champ.

Portail captif

Référence support 78805

Lors de la redirection vers la page d'authentification, le champ **Mot de passe** était sélectionné par défaut en lieu et place du champ **Nom d'utilisateur** lorsque celui-ci était vide. Cette anomalie a été corrigée.

Filtrage et NAT - Géolocalisation et Réputation des adresses IP publiques

Référence support 80980

Lorsqu'un groupe géographique ou un groupe de réputation d'adresses IP publiques est utilisé dans une règle de filtrage / NAT, l'info bulle affichée au survol de ce groupe n'indique plus à tort le message "Objet non trouvé".

Version 4.2.0 non publiée

La version 4.2.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités de la version 4.1.6

Système

Agent SNMP

Dans le cas d'une politique IPSec IKEv2 ou IKEv1 + IKEv2, un événement (*trap*) SNMP est désormais émis lorsqu'un correspondant VPN IPSec est injoignable.

Vulnérabilités résolues de la version 4.1.6

OpenSSL

Une vulnérabilité d'un score global CVSS de 3.0 a été corrigée par la mise à jour du composant OpenSSL.

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

ClamAV

Une vulnérabilité d'un score global CVSS de 5.8 a été corrigée dans le moteur antiviral ClamAV.

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

Une vulnérabilité d'un score global CVSS de 5.3 a été corrigée dans le moteur antiviral ClamAV.

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

Portail d'authentification

Une vulnérabilité d'un score global CVSS de 4.3 a été corrigée dans l'API de gestion du portail d'authentification.

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

OpenLDAP

Une vulnérabilité d'un score global CVSS de 4.5 a été corrigée par la mise à jour du composant OpenLDAP.

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

Protocole SNMP

Référence support 80471

Une vulnérabilité d'un score global CVSS de 5.5 dans le mécanisme de protection lié à l'analyse protocolaire SNMP a été corrigée.

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

Correctifs de la version 4.1.6

Système

Sauvegarde de configuration - Trusted Platform Module (TPM)

Référence support 79671

Lors d'une sauvegarde de configuration avec le paramètre *privatekeys* positionné à *none* (paramètre uniquement modifiable à l'aide de la commande CLI / Serverd : `CONFIG BACKUP`), les clés privées stockées en mode *ondisk* sur le TPM ne sont plus déchiffrées à tort.

Référence support 79671

Il n'est plus possible de lancer deux sauvegardes de configuration en même temps ou dans un laps de temps très court. Les clés privées stockées en mode *ondisk* sur le TPM ne sont ainsi plus déchiffrées à tort.

Filtrage et NAT

Référence support 79526

Lorsqu'un groupe contenait 128 objets ou plus dont au moins un avec une adresse MAC forcée, la règle utilisant ce groupe n'était plus jamais appliquée lorsqu'un flux lui correspondait. Ce problème a été corrigé.

Références support 80043 - 79636 - 80412 - 80376 - 79771

Lors de l'activation ou désactivation d'un objet temps, la réévaluation des connexions correspondant à la règle de filtrage contenant cet objet temps ne provoque plus un redémarrage inopiné du firewall.

Proxies

Références support 79957 - 80108

Dans une configuration utilisant de l'authentification multi-utilisateurs, le chargement complet d'une page Web intégrant une directive CSP (*content-security-policy*) pouvait dysfonctionner. Ce problème a été corrigé.

Référence support 81624

Dans une configuration utilisant de l'authentification multi-utilisateurs, la gestion des directives CSP (content-security-policy) de type "*img-src https://**" provoquait un redémarrage inopiné du service proxy. Ce problème a été corrigé.

Référence support 79858

Un problème d'accès concurrentiel lors de l'enregistrement d'une nouvelle connexion par le proxy a été corrigé. Ce problème pouvait entraîner un arrêt inopiné du firewall et un changement de rôle des membres d'une configuration en haute disponibilité.

Proxy SMTP

Référence support 78196 - 79813 - 81759

Un redémarrage inopiné du proxy pouvait survenir suite à la mise en file d'attente d'un e-mail et de la réception d'une erreur SMTP 421 émise par le serveur. Ce problème a été corrigé.

Proxy HTTP

Référence support 79584

Dans une configuration possédant toutes les conditions suivantes :

- Le proxy HTTP est utilisé,
- L'antivirus Kaspersky est activé,
- Le filtrage d'URL est activé.

L'émission par un navigateur Internet de plusieurs requêtes HTTP contenues au sein d'une connexion TCP unique (*pipelining*) n'est plus susceptible de provoquer un redémarrage inopiné du service proxy.

Proxy SSL

Référence support 77207

Un redémarrage inopiné du proxy SSL pouvait intervenir lorsque toutes les conditions suivantes étaient réunies :

- Une politique de filtrage SSL appliquant une action "Passer sans déchiffrer" lorsqu'un CN n'a pas pu être classifié dans une catégorie,
- Une première connexion correspond à cette règle (action "Passer sans déchiffrer") car la classification du CN échoue,
- Une connexion simultanée au même site voit sa classification aboutir sur une action "Bloquer sans déchiffrer".

Ce problème a été corrigé.

Haute disponibilité

Les erreurs survenant lors de la mise à jour du membre passif d'un cluster sont désormais correctement affichées dans l'interface Web d'administration du firewall.

Événements système

Référence support 80426

L'événement système n°19 : "LDAP inaccessible" se déclenche de nouveau en cas de problème d'accès à un annuaire LDAP défini dans la configuration du firewall.

Agent SNMP

Références support 77226 - 78235

L'OID "SNMPv2-MIB::sysObjectID.0", permettant d'identifier la nature de l'équipement interrogé, présentait la valeur par défaut liée à *net-snmp* au lieu de présenter la valeur propre à Stormshield. Cette anomalie a été corrigée.

Références support 80036 - 77779

Des problèmes de consommation mémoire excessive aboutissant à un arrêt inopiné du service Agent SNMP ont été corrigés.

Récupération régulière des CRL

Référence support 81259

Lorsqu'un proxy explicite avec un port réseau spécifique est défini sur le firewall, le mécanisme de récupération régulière des CRL utilise désormais correctement le port du proxy explicite pour accéder à Internet.

Annuaire LDAP - Serveur de secours

Référence support 80428

Dans une configuration LDAP(S) définie avec un serveur de secours, lorsque :

- Le firewall a basculé sur le serveur LDAP(S) de secours faute de réponse du serveur principal,
- Le serveur de secours ne répond pas à son tour.

Alors le firewall tente de se reconnecter immédiatement au serveur principal sans attendre le délai de 10 minutes défini en configuration d'usine.

Annuaire LDAP externe

Référence support 81531

Après la création d'un annuaire LDAP externe accessible via une connexion sécurisée, l'activation de l'option **Vérifier le certificat selon une Autorité de certification** et la sélection d'une CA de confiance n'aboutissent plus à une erreur interne du firewall.

Service de réputation des IP et de géolocalisation

Référence support 81048

Dans certains cas, le service de réputation des IP et de géolocalisation pouvait s'arrêter de manière inopinée à la suite d'un accès concurrentiel causé par un rechargement de configuration. Même s'il était redémarré automatiquement, une interruption du service pouvait alors survenir. Ce problème a été corrigé.

Référence support 77980

Une anomalie liée au service de réputation des IP et de géolocalisation pouvait provoquer une corruption de mémoire aboutissant à un redémarrage inopiné du firewall. Ce problème a été corrigé.

Réseau

Routage statique et VPN IPSec

Référence support 80862

Dans le cas d'une configuration VPN IPsec par politique (non VTI), lorsque une route statique était créée pour le réseau distant via l'interface IPsec, le trafic censé être chiffré et émis vers ce réseau ne l'était plus. Ce problème a été corrigé.

Bridge - Adresses MAC

Référence support 80652

Dans le cas d'interfaces rattachées à un bridge, lorsqu'un équipement réseau est déplacé et que le trafic réseau qu'il génère n'est plus lié à la même interface physique, le firewall associe automatiquement l'adresse MAC de l'équipement à la nouvelle interface dès réception d'une requête *Gratuitous ARP* issue du nouvel équipement.

Ce basculement n'était pas correctement pris en charge lorsque l'adresse MAC était différente après déplacement. Ce problème a été corrigé.

Prévention d'intrusion

Protocole SMB - CIFS

Références support 77484 - 77166

Des anomalies dans l'analyse protocolaire SMB - CIFS pouvaient provoquer à tort l'alarme bloquante "Protocole NBSS/SMB invalide" (alarme nb-cifs:158) lors d'un accès légitime à une ressource disque partagée Microsoft Windows. Ces anomalies ont été corrigées.

Machines virtuelles

Numéros de série des firewalls VPAYG

Référence support 76157

Les numéros de série des firewalls VPAYG (numéro de série du firewall auquel est ajoutée une extension de type "-XXXXXXXX") n'étaient pas reconnus par le mécanisme de supervision de la haute disponibilité. Ce problème a été corrigé.

Matériel

Configuration par clé USB

Références support 79645 - 79283

Lors de la configuration d'un firewall à l'aide d'une clé USB, un message d'information est désormais affiché en console et un délai d'attente de deux minutes est initié lorsqu'il est nécessaire de retirer la clé USB pour continuer les opérations en cours (mise à jour de firmware, rattachement d'un firewall à un cluster). Le retrait de la clé USB interrompt ce compteur.

Ce mécanisme permet d'éviter les erreurs de déchiffrement de clés sur les firewalls disposant d'un TPM (SN3100, SNi20).

Interface Web d'administration

Filtrage et NAT - Géolocalisation et Réputation des adresses IP publiques

Référence support 80980

Lorsqu'un groupe géographique ou un groupe de réputation d'adresses IP publiques est utilisé dans une règle de filtrage / NAT, l'info bulle affichée au survol de ce groupe n'indique plus à tort le message "Objet non trouvé".

Correctifs de la version 4.1.5

Il est fortement recommandé d'appliquer la mise à jour 4.1.5 sur les firewalls en version majeure 4.x.x.

Dans un but préventif, le certificat servant à signer les nouvelles mises à jour de version a été remplacé dans la version 4.1.5. Ce nouveau certificat, issu de l'autorité de certification de confiance « Stormshield Product and Services Root CA », sera utilisé pour vérifier l'intégrité et la signature de toutes les futures versions SNS.

Les mises à jour signées par l'ancien certificat seront refusées une fois la nouvelle version installée.

IMPORTANT
Pour installer une version précédente signée par l'ancien certificat sur un firewall en version SNS 4.1.5, il est obligatoire d'utiliser la procédure USB Recovery. La manipulation via la procédure classique n'est pas supportée.

Correctifs de la version 4.1.4

Système

VPN SSL en mode portail

Référence support 80332

Suite à une régression de compatibilité avec Java 8 introduite dans la précédente version corrective de SNS, le composant utilisé par le VPN SSL en mode portail a été compilé avec la version 8 du kit de développement Java afin d'assurer la compatibilité avec :

- Java 8 JRE,
  - ou -
- OpenWebStart.

Ceci permet de pallier la suspension prévue des versions publiques de Java JRE 8 dans un avenir proche.

Nouvelles fonctionnalités de la version 4.1.3

Système

Déconnexion en cas d'inactivité

Le super-administrateur peut désormais limiter la durée maximale d'inactivité autorisée des comptes administrateurs sur le firewall. Ces derniers peuvent toujours définir une durée d'inactivité pour leur propre compte, mais elle ne peut excéder celle définie par le super-administrateur.

En savoir plus

VPN IPSec (IKEv1 + IKEv2)

L'avertissement qui était affiché lors de l'utilisation d'une politique IPSec mixte IKEv1 / IKEv2 a été supprimé.
Après une longue période de stabilité, cette fonctionnalité n'est en effet plus considérée comme expérimentale et peut être utilisée dans un environnement de production sans attention particulière.
Nous vous invitons à consulter les précisions sur les cas d'utilisation d'une politique IPSec mixte IKEv1 et IKEv2.

Vulnérabilités résolues de la version 4.1.3

OpenSSL

La vulnérabilité CVE-2020-1968 (*Raccoon attack*) a été corrigée par la mise à jour du composant OpenSSL en version 1.0.2x.

La vulnérabilité CVE-2020-1971 (possibilité de provoquer un déni de service si une CRL de la PKI du firewall était préalablement compromise) a été corrigée par la mise à jour du composant OpenSSL en version 1.0.2x.

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

FreeBSD - ICMPv6

La vulnérabilité CVE-2020-7469, concernant la gestion des messages d'erreur dans la pile réseau ICMPv6 et pouvant déboucher sur une attaque de type *use-after-free*, a été corrigée par l'application d'un correctif de sécurité FreeBSD.

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

Authentification par certificat

Des contrôles additionnels ont été mis en place pour détecter la présence éventuelle du caractère spécial "*" dans le champ adresse e-mail d'un certificat. Ces contrôles permettent de ne plus interpréter ce caractère lors d'une requête à destination de l'annuaire LDAP, ce qui pouvait autoriser une connexion injustifiée au firewall.

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

Correctifs de la version 4.1.3

Système

Proxies

Référence support 75970

Lorsque le proxy doit envoyer une page de blocage, l'absence d'en-tête *Content-Length* dans la réponse (requête de type HTTP HEAD) n'entraîne plus à tort une alarme "Données additionnelles en fin de réponse" (alarme http:150).

Référence support 78432 - 79297

Des problèmes de fuites mémoire dans les proxies, pouvant aboutir à un redémarrage inopiné du service, ont été corrigés.

Références support 78802 - 79204 - 78210 - 77809 - 79584

Un problème lié à l'activation de la protection par force brute et qui pouvait entraîner un blocage du proxy a été corrigé.

Référence support 67947

Dans une configuration avec une politique de filtrage mettant en œuvre :

- Une règle **globale** de déchiffrement,
- Une règle **locale** de filtrage utilisant un proxy **explicite** et dont l'identifiant de règle est égal ou inférieur à celui de la règle globale de déchiffrement.

Une opération de rechargement de la configuration du proxy (changement de politique de filtrage, changement de politique de filtrage SSL/URL, changement du moteur de filtrage SSL/URL, changement du moteur antiviral...) ne provoque plus l'interruption des connexions traitées par le proxy.

Référence support 79584

Un problème lié à la gestion du contexte SSL et qui entraînait un blocage du proxy a été corrigé.

Supervision du matériel

Référence support 77170

Sur les firewalls modèles SN2100, SN3100 et SN6100, des optimisations ont été apportées au mécanisme de supervision de la vitesse de rotation des ventilateurs afin de ne plus remonter à tort d'alarmes mettant en cause le bon fonctionnement de ceux-ci.

Haute disponibilité (HA)

Références support 78758 - 75581

Des problèmes de fuites mémoire notamment dans le mécanisme chargé de la gestion de l'état de la HA ou des changements de rôles au sein d'un cluster ont été corrigés.

Haute disponibilité (HA) et VPN IPSec (IKEV2 ou IKEv1+IKEv2)

Référence support 79874

Un problème d'accès concurrentiels entre le mécanisme de log du VPN IPSec et le cache de la HA, suite à une synchronisation de la configuration IPSec, provoquait une interruption du service VPN IPSec. Ce problème a été corrigé.

Relai DHCP

Référence support 79298

L'option **Relayer les requêtes DHCP pour toutes les interfaces** (module **Configuration** > **Réseau** > **DHCP** > **Relai DHCP**) exclut désormais les interfaces créées lorsque le serveur PPTP est activé (module **Configuration** > **VPN** > **Serveur PPTP**), et qui empêchaient le démarrage du service Relai DHCP.

VPN SSL

Références support 73353 - 77976

Le client VPN SSL applique désormais le délai avant renégociation des clés défini sur le serveur VPN SSL, par défaut de 14400 secondes (4 heures). Les utilisateurs ne bénéficiant pas du client Stormshield Network VPN SSL doivent récupérer un nouveau fichier de configuration sur le portail d'authentification du firewall pour que le nouveau comportement s'applique.

En savoir plus

VPN SSL en mode portail

Référence support 68759

Le VPN SSL en mode portail utilise désormais un composant qui est compatible avec :

- Java 8 JRE,
  - ou -
- OpenWebStart.

Ceci permet de pallier à la suspension prévue des versions publiques de Java JRE 8 dans un avenir proche.

VPN IPSec

Référence support 79553

Lors de la mise à jour en version 4.1 de topologies VPN IPSec x509 (authentification par certificat) déployées à l'aide de SMC (Stormshield Management Center), les tunnels VPN IPSec concernés ne parvenaient plus à s'établir. Ce problème a été corrigé.

VPN IPSec IKEv1 - Authentification par certificat

Référence support 79156

Dans une configuration utilisant exclusivement des tunnels IPSec IKEv1, une anomalie dans le mécanisme de comparaison des *Distinguished Name* (DN) définis dans les certificats présentés par les correspondants locaux et distants empêchait l'établissement de ces tunnels VPN IPSec. Ce problème a été corrigé.

Sandboxing

Référence support 76120

Des alertes "Sandboxing license not available" ne sont plus émises à tort sur les firewalls ne disposant pas de la licence sandboxing (Breach Fighter) et pour lesquels le sandboxing n'est pas activé dans la configuration.

TPM

Sur les firewalls équipés d'un module TPM (Trusted Platform Module), le chiffrement des certificats *ondisk* est à nouveau fonctionnel et le système peut y accéder lorsque la clé symétrique du TPM a été changée.

Certificats et PKI

Référence support 78734

La requête d'affichage des points de distribution des CRL (CRLDP) appliquée à une sous autorité de certification (sous-CA) renvoyait à tort les CRLDP de l'autorité parente de cette sous-CA.
Cette anomalie a été corrigée et la commande appliquée à une sous-CA affiche désormais correctement les CRLDP qui lui sont propres.

Réseau

Passerelle par défaut

Référence support 78996

Il est de nouveau possible de définir sur le firewall une passerelle par défaut située dans un réseau IP public autre que le plan d'adressage public du firewall.

Bridge - Adresses MAC

Référence support 74879

Dans le cas d'interfaces rattachées à un bridge, lorsqu'un équipement réseau est déplacé et que le trafic réseau qu'il génère n'est donc plus lié à la même interface physique, le firewall associe désormais automatiquement l'adresse MAC de cet équipement à la nouvelle interface dès la réception d'une requête *Gratuitous ARP* issue de l'équipement. Ceci permet d'assurer la bonne continuité du filtrage pour l'équipement déplacé.
La bascule de l'équipement ne sera effective que si l'adresse MAC est identique après déplacement.

Supervision des interfaces - Courbes historiques

Références support 78815 - 73024

Le mécanisme de récupération des noms d'interfaces destiné à générer les courbes historiques était sensible à la casse : certaines courbes historiques n'étaient ainsi pas affichées. Cette anomalie a été corrigée.

Prévention d'intrusion

Protocole DCERPC

Référence support 77417

Le moteur d'analyse du protocole DCERPC pouvait créer à tort plusieurs centaines de squelettes de connexions, entraînant alors une consommation CPU excessive du firewall.
Ce problème, qui pouvait notamment empêcher le firewall de répondre aux requêtes de suivi d'état de la HA et provoquer une instabilité du cluster, a été corrigé.

Commande *sfctl*

Référence support 78769

L'utilisation de la commande *sfctl* avec un filtre sur une adresse MAC ne provoque plus un redémarrage inopiné du firewall.

Interface Web d'administration

Tableau de bord - Interfaces

Référence support 77313

Suite à la création d'un agrégat de liens, l'ordre d'affichage des interfaces dans le widget **Réseau** du tableau de bord n'est plus modifié à tort.

Portail captif

Référence support 78651

La personnalisation du logo affiché sur le portail captif (module **Configuration** > **Utilisateurs** > **Authentification** > **Portail Captif** > **Configuration avancée**) est désormais correctement prise en compte.

Correctifs de la version 4.1.2

IMPORTANT
Les firewalls participant à une topologie IPSec x509 (authentification par certificats) déployée à l'aide de SMC (Stormshield Management Center) **ne doivent pas** être mis à jour vers une version SNS 4.1.1 ou 4.1.2.
Pour plus d'information sur ce sujet, veuillez consulter l'article de la base de connaissance Stormshield disponible ici.

IMPORTANT

Dans certaines conditions, le proxy peut être impacté par une fuite mémoire, aboutissant à un redémarrage inopiné du service. Si vous pensez être impacté par ce problème, veuillez vous rapprocher du support Stormshield.

Système

Authentification multi-utilisateurs

Référence support 78887

Suite à l'implémentation progressive des directives CSP (content-security-policy) sur certains sites Web et à la vérification de celles-ci par les navigateurs Web du marché, les utilisateurs bénéficiant de l'authentification multi-utilisateurs SNS étaient confrontés à un affichage dégradé de ces sites.

Ce problème a été corrigé par l'ajout du FQDN du firewall à la liste des sites autorisés à servir des ressources externes pour les sites concernés.

Référence support 78677

Suite à la récente implémentation d'une nouvelle politique de sécurité sur les navigateurs Web du marché, l'authentification multi-utilisateurs SNS n'était plus fonctionnelle. Selon le navigateur Web utilisé, ce comportement pouvait aboutir à l'affichage du message d'erreur "Too Many Redirects" ou d'un avertissement dans la console Web du navigateur.

Pour corriger ce problème, les cookies d'authentification générés par le proxy contiennent désormais les attributs "SameSite" et "Secure" lorsque le protocole HTTPS est utilisé.

Dans le cas où un site non sécurisé est consulté, c'est-à-dire utilisant le protocole HTTP, l'attribut "Secure" du cookie ne peut être utilisé. Pour rétablir la navigation sur ces sites, une opération manuelle doit être effectuée dans la configuration du navigateur Web.

En savoir plus

Proxies

Référence support 78190

Des optimisations ont été apportées au mécanisme de génération de notifications d'événements système et d'alertes afin de ne plus provoquer une consommation CPU excessive lorsque le nombre de connexions traversant le firewall s'accroît fortement.

Prévention d'intrusion

Protocoles RDP / COTP

Référence support 78923

Le mécanisme d'évaluation des règles de filtrage pour les connexions concernant les protocoles RDP / COTP prend à nouveau correctement en compte les éventuelles règles de translation d'adresses liées, et ne bloque plus à tort ces flux.

Nouvelles fonctionnalités de la version 4.1.1

Option de désactivation du mode furtif (*stealth mode*)

Des améliorations ont été amenées au mode furtif (*stealth mode*) en permettant sa désactivation, autorisant la réponse aux requêtes ICMP (option **Activer le mode furtif** du module **Protection applicative** > **Protocoles** > **Protocoles IP** > **IP** > onglet **Configuration globale**).

Cette option permet une intégration plus simple du firewall dans les infrastructures existantes en modérant le mode furtif du firewall et permet d'éviter les paquets ignorés silencieusement. Cela autorise par exemple le firewall à se comporter comme un équipement visible du réseau lorsque :

- Un paquet dépasse la MTU et possède un bit DF à 1 (dfbit=1) : le firewall bloque le paquet et émet un paquet ICMP de réponse.
- Un paquet traverse correctement le firewall : le TTL ("Time To Live") est décrémenté par le firewall.

La valeur de cette nouvelle option, inscrite dans la configuration des traitements protocolaires IP du moteur IPS, supplante les anciennes méthodes de paramétrage basées sur les commandes sysctl `net.inet.ip.icmpreply=1` et `net.inet.ip.stealth=0`.

Prévention d'intrusion

Filtrage et analyse des protocoles IEC61850

La version SNS 4.1 assure le support de l'analyse protocolaire IEC61850 (MMS, Goose et SV) et vérifie la conformité des paquets IEC61850 traversant le firewall.

Ces protocoles sont principalement utilisés dans les infrastructures de transport d'électricité pour la commande, la supervision et le monitoring des contrôleurs électriques.

Protocole RDP

Des améliorations ont été apportées à l'analyse protocolaire des flux RDP.

Protocole HTTP

Les protocoles dérivés de HTTP remontent une alarme spécifique (alarme n°732 "HTTP : pile de protocoles upgrade invalide") permettant à l'utilisateur de configurer plus finement les alarmes et le filtrage pour ces protocoles.

Client DHCP

De nouvelles options DHCP (60 [vendor-class-identifier], 77 [user-class] et 90 [authsend]) permettent aux firewalls SNS de s'authentifier sur les réseaux d'opérateurs de télécommunications qui proposent des services de VLAN. Cela permet d'intégrer le firewall SNS dans le réseau opérateur sans nécessité d'utiliser le mode de connexion PPPOE.

Ces options sont paramétrables uniquement à l'aide la commande *CLI / Serverd* :

```
config network interface update ifname=xxx DHCPVendorClassId="aaa"
DHCPUserClass="bbb" DHCPAuthsend="ccc"
config network interface activate
```

Le détail de cette commande est disponible dans le Guide de référence des commandes CLI / Serverd.

Mise à jour

L'algorithme de hachage des fichiers de mise à jour du firmware a été modifié pour être conforme aux meilleurs standards

Nouveaux firewalls modèles SNi20

Compatibilité

La version de firmware 4.1.0 assure la compatibilité avec les nouveaux firewalls industriels SNi20.

Afin d'assurer une continuité de service dans les milieux industriels, le firewall SNi20 est équipé d'un bypass matériel qui permet, une fois activé, de laisser passer le trafic réseau en cas de coupure électrique ou de défaillance du boîtier.

Sécurisation matérielle des secrets des VPNs

Les firewalls SNi20 disposent d'un module matériel TPM (pour Trusted Platform Module) dédié à la sécurisation des secrets de VPN. Celui-ci permet d'ajouter un niveau de sécurité pour les SNi20 dédiés à la concentration de VPNs et dont la sécurité physique n'est pas garantie. Cette version 4.1.0 introduit le support de ce module.

Firewalls modèles SNi20 et SNi40

Agrégation de liens

La version 4.1.0 introduit le support de l'agrégation de liens (LACP) sur les firewalls modèles SNi20 et SNi40.

Protocoles de gestion des boucles réseau

La version 4.1.0 introduit le support des protocoles de gestion des boucles réseau (RSTP et MSTP) sur les firewalls modèles SNi20 et SNi40.

Serverd

Afin de réduire la surface d'attaque sur SNS, le service Serverd peut être paramétré pour écouter uniquement sur l'adresse locale (loopback) du firewall. Ce comportement est activé par défaut sur les firewalls en configuration d'usine.

Il est uniquement modifiable à l'aide de la commande :

```
CONFIG CONSOLE SERVERDLOOPBACK state=0/1
```

Le détail de cette commande est disponible dans le Guide de référence des commandes CLI / Serverd.

Correspondants mobiles VPN IPSec

Il est désormais possible de supporter plus d'une politique mobile simultanément en distinguant les correspondants par leur identifiant (ID). Ces modifications s'effectuent depuis le module **Configuration > VPN > VPN IPsec**, onglet *Correspondants*.

L'utilisation de l'identifiant (ID) permet également de modifier la configuration VPN liée à un correspondant mobile particulier, distingué grâce à son identifiant, sans affecter les tunnels des autres correspondants mobiles.

Compte *admin*

Pour changer le mot de passe du compte *admin* (super administrateur), il est désormais nécessaire de saisir l'ancien mot de passe.

VPN IPSec et groupes LDAP

Lors de la connexion en VPN IPSec via une authentification SSO, le firewall récupère dorénavant les groupes associés à l'utilisateur venant du LDAP pour permettre leur utilisation dans les règles de filtrage.

VPN SSL et certificats

Pour authentifier un correspondant (client ou serveur) en TLS, les firewalls Stormshield acceptent désormais uniquement les certificats disposant du champ *Key Usage* avec l'attribut "ServerAuth", c'est-à-dire les certificats conformes à la norme X509 v3.

Autorités de certification (CA) et certificats globaux

Les certificats et autorités de certification globaux sont désormais affichés et identifiés comme tels lorsque l'option **Afficher les politiques globales (Objets réseau, Certificats, Filtrage, NAT et VPN IPSec)** du module **Préférences** est activée.

Certificats et PKI

Lors de l'import d'un certificat au format p12, le type de certificat (certificat serveur ou certificat utilisateur) est désormais automatiquement détecté.

Enrôlement des certificats

Les firewalls Stormshield supportent désormais le protocole d'enrôlement de certificats EST (Enrollment over Secure Transport) qui se distingue notamment par l'utilisation de requêtes HTTPS, bénéficiant ainsi de toute la sécurité du protocole TLS.

Sa mise en œuvre sur les firewalls Stormshield permet de réaliser les opérations suivantes :

- Distribution de la clé publique de l'autorité de certification (CA) signant les certificats,
- Requêtes de création ou de renouvellement de certificat à l'initiative de l'administrateur de la PKI,
- Requêtes de création ou de renouvellement de certificat à l'initiative du titulaire du certificat (enrôlement).

Les requêtes de renouvellement peuvent être authentifiées directement par le certificat existant et ne nécessitent donc pas de mot de passe si le serveur EST le permet.

Ces opérations sont exclusivement réalisables à l'aide des commandes *CLI / Serverd* débutant par :

```
PKI EST
```

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

Génération des certificats

Il est désormais possible de générer des certificats avec de nouveaux algorithmes plus performants à base de courbes elliptiques. Les commandes *CLI / Serverd* suivantes offrent maintenant le choix de l'algorithme SECP, Brainpool ou RSA :

```
PKI CA CREATE
```

```
PKI CERTIFICATE CREATE
```

```
PKI REQUEST CREATE
```

```
PKI CA CONFIG UPDATE
```

Vous devez positionner aussi le paramètre `size` de ces commandes. Sa valeur doit correspondre à l'algorithme choisi :

Algorithme	Tailles autorisées
RSA	768, 1024, 1536, 2048, ou 4096
SECP	256, 384, ou 521
Brainpool	256, 384, ou 512

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

Haute disponibilité

Agrégation de liens LACP

Sur un firewall contenant des agrégats LACP, vous pouvez désormais attribuer un poids à chaque interface de l'agrégat dans le calcul de la qualité de la haute disponibilité.
Attribuez la valeur *1* au nouveau paramètre *LACPMembersHaveWeight* des commandes *CLI / Serverd* suivantes :

```
CONFIG HA CREATE
```

```
CONFIG HA UPDATE
```

Ceci active l'affichage des interfaces de l'agrégat dans le tableau **Impact de l'indisponibilité d'une interface dans l'indicateur de qualité d'un firewall** du module **Haute disponibilité** de l'interface web d'administration.

Sans ces commandes, le comportement par défaut reste le même : l'agrégat est vu comme une seule interface et le basculement du cluster n'a lieu qu'en cas de perte de toutes les interfaces de l'agrégat.

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

Monitoring de la haute disponibilité via SMC

Des optimisations ont été apportées pour le monitoring via SMC des firewalls configurés en haute disponibilité (récupération de la valeur du champ (**Nom de nœud système**).

Perte d'un module réseau

Le calcul de santé qui détermine le basculement d'un nœud à l'autre du cluster a été amélioré afin de mieux prendre en compte la perte d'un module réseau, même après un redémarrage.

Règle de NAT avec publication ARP

Dans une configuration en haute disponibilité (HA), afin de maintenir le routage du trafic, un firewall peut envoyer un Gratuitous ARP (GARP) pour toutes ses interfaces dans le but de notifier le réseau lorsqu'une adresse MAC change d'emplacement.

Ce fonctionnement a été amélioré afin que toutes les adresses IP virtuelles issues d'une **Publication ARP** d'une règle de NAT envoient une série de Gratuitous ARP (GARP) lors d'une bascule.

Authentification

Nouvel SN SSO Agent pour Linux

Un nouvel SN SSO Agent est disponible sous Linux et supporte les annuaires non Windows (par exemple Samba 4). Sa configuration s'effectue dans le module **Authentification** de l'interface web d'administration et la détection au travers de logs exportés via Syslog. Les logs exportés sont filtrés selon des expressions régulières pré-configurées dans l'interface.

Pour plus d'informations sur la configuration et le fonctionnement de SN SSO Agent pour Linux, veuillez consulter la note technique Agent SSO pour Linux.

Agent SSO - Syslog

Il est désormais possible de configurer un serveur syslog de secours pour la méthode d'authentification Agent SSO.

Comptes temporaires

Le mot de passe généré automatiquement par le firewall à la création d'un compte temporaire (module **Utilisateurs > Comptes temporaires**) respecte dorénavant la longueur minimale des mots de passe définie dans la politique de mots de passe du firewall (module **Système > Configuration** > onglet **Configuration générale**).

LDAP

Il est désormais possible de configurer le serveur LDAP de secours sur un port différent du serveur LDAP principal.

Firewall SN6100 - Performances

La configuration des occupations mémoire a été optimisée sur le moteur IPS du SN6100.
Les performances des firewalls modèles SN6100 peuvent être consultées dans la fiche produit Network Security SN6100.

Synchronisation SNS - SMC

La synchronisation entre SNS et SMC a été améliorée afin de fluidifier les échanges de données entre les deux produits, notamment lors de l'accès direct à l'interface d'administration des firewalls depuis SMC.

Client NTP

Il est désormais possible de configurer l'interface par laquelle les requêtes NTP transitent. Auparavant, le démon en charge de la synchronisation du temps sur un firewall SNS faisait transiter ses requêtes par l'interface par défaut.

Ce nouveau paramètre est uniquement modifiable à l'aide de la commande *CLI / Serverd* :

```
CONFIG NTP SERVER ADD name=<hostname|groupname> bindaddr=<Firewall_obj>
```

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

Objets réseau

Les objets de type **Plage d'adresses** permettent désormais de configurer des plages d'adresses MAC.

Proxy SSL

Les clés générées par le proxy SSL utilisent désormais les mêmes algorithmes de chiffrement que l'autorité de certification du proxy SSL en lieu et place des algorithmes définis par défaut.

Sauvegardes de configuration

L'algorithme de dérivation des mots de passe protégeant les sauvegardes de configuration a été mis à jour pour être conforme aux meilleurs standards.

Système

Le générateur aléatoire du noyau a été modernisé pour se baser sur un algorithme à la fois plus rapide et plus robuste.

Configuration initiale via USB

Routage dynamique (Bird)

Il est désormais possible de définir la configuration du routage dynamique en important des fichiers de configuration *bird.conf* pour l'IPv4 et *bird6.conf* pour l'IPv6. Le format CSV du fichier de commandes a également été enrichi pour l'occasion.

Pour plus d'informations concernant la préparation des fichiers *.bird* et *.bird6*, veuillez vous référer à la note technique Configuration initiale par clé USB.

Opération *setconf*

Dans le cadre de la configuration initiale par clé USB, la commande *setconf* dispose d'une nouvelle fonctionnalité permettant d'écrire des lignes dans des sections en plus d'écrire des

valeurs dans des clés (token). Le format CSV du fichier de commandes a été enrichi pour l'occasion.

Pour plus d'informations concernant la commande *setconf*, veuillez vous référer à la note technique Configuration initiale par clé USB.

Nouvelle opération *sethostname*

Dans le cadre de la configuration initiale par clé USB, une nouvelle opération *sethostname* est disponible permettant de définir notamment le nom d'hôte (hostname) du firewall. Le format CSV du fichier de commandes a été enrichi pour l'occasion.

Pour plus d'informations concernant l'opération *sethostname*, veuillez vous référer à la note technique Configuration initiale par clé USB.

Tableau de bord

Les agents SSO et serveurs syslog sont désormais supervisés et leur état apparaît dans le tableau de bord.

Annuaires LDAP

Les connexions sécurisées aux annuaires LDAP internes sont désormais basées sur le protocole standard TLS 1.2.

Option d'exclusion du proxy pour la sauvegarde automatique

La sauvegarde automatique peut à présent être paramétrée pour ne pas passer à travers le proxy configuré sur le firewall.

Ce nouveau paramètre est uniquement modifiable à l'aide de la commande *CLI / Serverd* :

```
CONFIG AUTOBACKUP SET
```

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

Interface Web d'administration

Nom de nœud système

Il est désormais possible de définir un nom de nœud système pour le firewall (**Configuration** > onglet **Configuration générale** > **Configuration avancée**).

Ce nom est particulièrement utile dans le cadre d'une configuration en haute disponibilité, puisqu'il permet d'identifier aisément le membre du cluster sur lequel vous êtes connecté lorsque vous ouvrez une session en mode console via SSH par exemple.

Lorsqu'il est configuré, ce nom du nœud système apparaît dans le bandeau supérieur de l'interface Web d'administration, entre parenthèses, derrière le nom du firewall.

Filtrage et NAT - Fonctionnalité de Cache HTTP

La possibilité d'utiliser la fonction *Cache HTTP* au sein d'une règle de filtrage n'est plus disponible.

Si un firewall utilisait cette fonction dans une version précédente de firmware, cette fonction est automatiquement désactivée lors de la mise à jour en version 4.1.0 ou supérieure.

Récupération régulière des CRL

Il est désormais possible de préciser l'adresse IP présentée par le firewall pour la **Récupération régulière des listes de révocation de certificats (CRL)**.

Cette adresse est exclusivement configurable à l'aide de la commande CLI / Serverd :

```
PKI CONFIG UPDATE CHECKBINDADDR=ip_address
```

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

Vulnérabilités résolues de la version 4.1.1

FreeBSD

Les vulnérabilités CVE-2019-15879 et CVE-2019-15880 liées au module *cryptodev* ont été corrigées par l'application d'un correctif de sécurité FreeBSD.

JQuery

Référence support 78384

Les vulnérabilités CVE-2020-11022 et CVE-2020-11023 ont été résolues par la mise à jour de la bibliothèque JQuery.

Processeurs Intel

Plusieurs vulnérabilités (CVE-2019-11157, CVE-2019-14607 et CVE-2018-12207) pouvant affecter les processeurs Intel ont été corrigées par l'application d'un correctif FreeBSD et de mises à jour de microcode Intel.

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

Ligne de commande

Le service de ligne de commande de SNS (Serverd) était vulnérable aux attaques par force brute uniquement via les interfaces protégées et seulement si l'accès au serveur d'administration sur le port 1300 était autorisé dans la configuration des règles implicites. Ce défaut a été corrigé.

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

NetBIOS

Une vulnérabilité pouvait permettre par le biais d'une session NetBIOS d'envoyer au travers du firewall des paquets NetBIOS spécialement conçus dans le but de réaliser un déni de service.

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

Authentification par certificat

Des contrôles additionnels ont été mis en place pour détecter la présence éventuelle du caractère spécial "*" dans le champ adresse e-mail d'un certificat. Ces contrôles permettent de ne plus interpréter ce caractère lors d'une requête à destination de l'annuaire LDAP, ce qui pouvait autoriser une connexion injustifiée au firewall.

Certificats et PKI

Des contrôles additionnels ont été mis en place pour les opérations de manipulation telles que le téléchargement d'une identité utilisateur ou la publication d'un certificat dans l'annuaire LDAP. Ces contrôles interdisent l'exécution de code JavaScript qui aurait ainsi pu être placé par un utilisateur malveillant dans le certificat.

Interface Web d'administration / Portail captif / Parrainage

Des contrôles supplémentaires à la connexion (interface Web d'administration / Portail captif / Parrainage) permettent de s'assurer qu'aucune tentative d'exécution de code JavaScript ou de balises HTML additionnelles n'est réalisée au travers de la page optionnelle d'avertissement (*disclaimer*).

Antivirus ClamAV

Les vulnérabilités CVE-2020-3327 et CVE-2020-3341 ont été résolues par la mise à jour du moteur antiviral ClamAV en version 0.102.3.

Correctifs de la version 4.1.1

Système

VPN SSL

Référence support 76762

Le champ **Réseaux ou machines accessibles** était utilisé à tort dans le calcul du nombre de clients VPN SSL possibles, faussant ainsi le calcul. Ce comportement a été corrigé.

VPN SSL Portail

Référence support 77062

Bien que le nombre maximal de serveurs accessibles via SSL VPN Portail soit limité, il était possible de déclarer des machines supplémentaires. Cela entraînait alors des redémarrages en boucle du moteur d'authentification du firewall. Il n'est désormais plus possible de créer de serveurs au delà de cette limite, qui dépend du modèle de firewall.

En savoir plus

Références support 77168 - 77132 - 77388

Le démon SLD pouvait redémarrer et déconnecter tous les utilisateurs lorsque deux d'entre eux étaient connectés en VPN SSL Portail et accédaient à la même ressource.

Bypass matériel - Firewalls modèle SNi40

Référence support 78382

Sur les firewalls industriels SNi40 dont la fonction de bypass matériel était activée (**Configuration** > onglet **Configuration générale**), un problème d'accès concurrentiel au mécanisme de bypass par les processus de supervision du matériel pouvait entraîner une activation inappropriée du bypass ainsi qu'un défaut d'affichage de son état dans l'interface Web d'administration du firewall. Ce problème a été corrigé.

Configuration des annuaires

Référence support 76576

Le port utilisé par défaut pour accéder au serveur LDAP de secours est désormais identique au port utilisé par le serveur LDAP principal.

Supervision des passerelles

Références support 71502 - 74524

Lors du démarrage du mécanisme de supervision des passerelles, si l'une des passerelles utilisées dans les règles de filtrage passait d'un état interne « à priori non joignable » (un test de disponibilité échoué) à l'état interne « joignable », cette passerelle restait néanmoins désactivée pour le filtrage. Cette anomalie a été corrigée.

Un événement est également désormais enregistré dans les logs lors de ce changement d'état de la passerelle.

Référence support 75745

Sur un firewall soumis à une forte charge et utilisant une configuration avec de nombreuses passerelles, le mécanisme de supervision des passerelles pouvait ne pas recevoir les réponses aux tests de disponibilité suffisamment rapidement. Dans ce cas, ce mécanisme réémettait les requêtes de disponibilité de manière continue, puis redémarrait sans émettre de notification (log ou événement système). Ce problème a été corrigé.

Référence support 77579

Des problèmes de redémarrage inopiné du mécanisme de supervision des passerelles ont été résolus.

Référence support 76802

Dans certaines configurations le processus faisant appel au moteur de supervision des passerelles pouvait consommer une quantité excessive de ressources CPU du firewall. Ce problème a été corrigé.

Filtrage d'URL - Extended Web Control

Référence support 78169

La mise à jour d'un firewall vers une version de firmware 4.1.x n'empêche plus la génération des groupes de catégories d'URL utilisés par la solution Extended Web Control.

Proxies

Références support 77514 - 76343 - 78378 - 78438 - 78469 - 78579 - 78582 - 77896

Des problèmes de blocage des proxies lors de l'utilisation conjointe de l'antispam et du moteur antiviral Kaspersky ont été résolus.

Références support 76535 - 75662

Un problème d'accès concurrentiel potentiel entre les files de traitement des proxies SSL et HTTP pouvait entraîner un arrêt inopiné du gestionnaire des proxies. Ce problème a été résolu.

Référence support 71870

Le démon du proxy ne s'arrête plus de manière inopinée lorsque le nombre maximum de connexions simultanées au travers du proxy SSL est atteint.

Références support 70598 - 70926

Le comportement du Proxy HTTP a été modifié afin de ne plus surcharger le démon SLD du firewall, dans le cas où un trop grand nombre de requêtes redirigeaient vers le portail d'authentification. Ce nouveau mécanisme met notamment en œuvre une protection contre les attaques par force brute.

Proxy SSL

Références support 76022 - 76017

La modification de certains paramètres (tampons mémoire, taille de fenêtre TCP) du proxy SSL destinés à optimiser la quantité de données échangées au travers de ce proxy est désormais correctement prise en compte.

Référence support 77207

Une anomalie dans le mécanisme de cache des décisions SSL (déchiffrer, ne pas déchiffrer...) en présence de connexions simultanées avec des adresses IP destination identiques et des

ports différents, pouvait provoquer une corruption de ce cache et aboutir à un blocage du proxy SSL. Cette anomalie a été corrigée.

Référence support 78044

Lorsqu'une tentative de connexion vers un serveur SSL non joignable aboutissait directement à l'émission d'un message d'erreur par le proxy SSL, cette connexion n'était pas correctement clôturée par le firewall. La multiplication de ces connexions considérées à tort comme actives aboutissait alors à un fort ralentissement des flux SSL légitimes. Cette anomalie a été corrigée.

Proxy SMTP

Référence support 77207

Dans une configuration utilisant le proxy SMTP dans une règle de filtrage SMTP :

- En mode d'inspection de sécurité "Firewall",

  ou

- En mode d'inspection de sécurité "IDS" ou "IPS" mais sans analyse protocolaire SMTP (module **Protection applicative** > **Protocoles** > **SMTP** > onglet **IPS** : case **Détecter et inspecter automatiquement le protocole** décochée),

une coupure de connexion à l'initiative du serveur SMTP précédée d'un message serveur SMTP/421 provoquait un blocage du proxy SMTP. Ce problème a été corrigé.

Stockage local

Référence support 75301

Un firewall dont la carte SD (et donc la partition de stockage des logs) était endommagée pouvait redémarrer en boucle. Ce problème a été corrigé.

VPN IPSec IKEv1

Référence support 77679

Dans une configuration IPSec utilisant un correspondant mobile avec authentification par certificat et pour lequel aucun identifiant de correspondant n'est précisé, le message de passage en mode expérimental n'est plus affiché à tort.

Référence support 77358

Lors de l'établissement d'un tunnel VPN IPSec avec un utilisateur distant (appelé également mobile ou nomade), la phase 1 de la négociation IKE pouvait échouer du fait que les paquets fragmentés reçus n'étaient pas reconstruits correctement. Cette anomalie a été corrigée.

Référence support 65964

Le moteur de gestion IPSec (*Racoon*) utilisé pour les politiques IKEv1 n'interrompt plus la négociation d'une phase 2 avec un correspondant lorsque la négociation d'une autre phase 2 avec le même correspondant échoue.

VPN IPSec IKEv2 ou IKEv1 + IKEv2

Référence support 74391

Le rechargement automatique d'une CRL de très grande taille (plusieurs dizaines de milliers de certificats révoqués) n'entraîne plus de redémarrage en boucle du moteur de gestion des tunnels IPSec IKEv2.

Référence support 75303

Un nombre important de redémarrages du moteur de routage dynamique Bird (*bird* pour IPv4 ou *bird6* pour IPv6) provoquait un défaut sur le démon IKE, empêchant alors la négociation des tunnels VPN IPSec. Cette anomalie a été corrigée.

Référence support 75137

La création de plusieurs correspondants nomades utilisant un même certificat n'entraîne plus le chargement de ce certificat à de multiples reprises. Ce comportement provoquait en effet une charge mémoire inutile dans le cas d'un nombre important de correspondants.

Référence support 77722

La présence d'une même Autorité de Certification de confiance avec CRL à la fois dans la politique IPSec locale et la politique IPSec globale ne provoque plus un échec de l'activation de la configuration IPSec du firewall.

Référence support 77097

Des optimisations ont été apportées dans la gestion du processus d'authentification pour l'établissement d'un tunnel VPN IPSec dans une configuration où plusieurs annuaires LDAP sont déclarés et que le temps de réponse d'un ou plusieurs de ces annuaires LDAP est anormalement élevé.

Ces optimisations permettent désormais de ne plus bloquer les tentatives d'établissement d'autres tunnels pendant cette phase d'attente.

VPN IPSec - Interfaces virtuelles

Référence support 77032

Lors du déchiffrement de trafic IPv6 transitant dans des tunnels IPSec IPv4 au travers d'interfaces virtuelles, le firewall ne cherche plus à tort les routes de retour parmi les interfaces virtuelles IPv6. Ces paquets IPv6 sont donc désormais correctement échangés à chaque extrémité du tunnel.

VPN IPSec - Logs

Référence support 77366 - 69858 - 71797

Les chaînes de texte envoyées vers le service de gestion des logs du firewall, et qui dépassent la taille autorisée, sont désormais correctement tronquées et ne contiennent plus de caractères n'appartenant pas au jeu UTF-8. Cette anomalie provoquait un dysfonctionnement de la consultation des logs au travers de l'interface Web d'administration.

De plus :

- La taille maximale d'une ligne de log est désormais de 2048 caractères,
- La taille maximale d'un champ texte contenu dans une ligne de log est désormais de 256 caractères.

Configuration initiale par clé USB

Référence support 77603

Une anomalie dans la gestion des caractères spéciaux (espaces, "&"...) lors de l'import d'un fichier CSV pouvait empêcher la prise en compte de certaines données (exemple : certificats dont le nom contient des espaces). Elle a été corrigée.

Antivirus

Références support 77399 - 77369 - 78378 - 78156 - 78579

Le moteur antiviral ne se bloque plus au démarrage ou lors du rechargement global de sa configuration lorsque la licence sandboxing (Breach Fighter) est absente ou en cas de défaut de configuration du sandboxing.

Objets réseau

Référence support 77385

Lors de la création d'un objet réseau global lié à une interface protégée, cet objet est désormais correctement intégré au groupe *Networks_internals*.

Restauration d'objets réseau

Référence support 76167

Lors de la restauration d'objets réseau (locaux ou globaux) à l'aide d'un fichier de sauvegarde (fichier portant l'extension ".na"), un rechargement des routes réseau du firewall est effectué afin de prendre en compte les modifications qui concerneraient des objets réseau impliqués dans le routage.

TPM

Référence support 76664

Lors de la révocation d'un certificat, le fichier associé portant l'extension .pkey.tpm est désormais correctement supprimé.

Référence support 76665

Lorsqu'un certificat au format PEM et non accompagné de sa clé privée est importé sur le firewall, la commande de diagnostic `tpmctl -a -v` ne retourne plus à tort un message d'erreur de lecture du fichier TPM associé (*tpm file read error*).

Agent SNMP

Références support 65418 - 71393

Les réponses SNMP de type SNMP_NOSUCHOBJECT, SNMP_NOSUCHINSTANCE et SNMP_ENDOFMIBVIEW sont désormais correctement interprétées et ne provoquent plus un arrêt inopiné de l'analyse du protocole SNMP.

Référence support 71584

L'utilisation de la valeur *snmpEngineBoots* a été modifiée afin de se conformer à la RFC 3414.

Références support 74522 - 74521

Des anomalies dans l'indexation des tables reflétant l'état matériel des membres du cluster dans la MIB HA ont été corrigées.

Connexion depuis Stormshield Management Center (SMC)

Lors d'une première connexion depuis SMC à l'interface Web d'administration d'un firewall en version 4.0.1 ou supérieure, la récupération de l'archive contenant l'intégralité des données de l'interface pouvait échouer, empêchant alors toute connexion au firewall depuis SMC. Cette anomalie a été corrigée.

Rapports

Dans certains cas, l'exécution de la commande système *checkdb -C* permettant de vérifier l'intégrité de la base de données des rapports pouvait amener à sa suppression. Le système permettant d'interagir avec cette dernière a ainsi été amélioré afin d'y incorporer plus de rigueur notamment dans la gestion des erreurs.

Pour plus d'informations concernant la syntaxe de cette commande, veuillez vous référer au Guide de référence des commandes CLI / SSH.

Comportement en cas de saturation du service de gestion des logs

Références support 73078 - 76030

Dans le cas où le service de gestion des logs du firewall est saturé, il est désormais possible de définir la manière dont le firewall gère les paquets générant une alarme et ceux traversant une règle de filtrage configurée pour tracer un événement :

- Bloquer les paquets concernés puisque le firewall n'est plus en mesure de tracer ces événements,
- Ne pas bloquer les paquets concernés et appliquer la configuration de la politique de sécurité même si le firewall n'est plus en mesure de tracer ces événements.

Ce comportement du moteur de prévention d'intrusion peut être configuré depuis l'interface d'administration du firewall dans le module **Configuration** > **Protection applicative** > **Profils d'inspection**.

Il est également possible de définir un seuil en pourcentage à partir duquel le firewall considère que son service de gestion des logs est saturé. Une fois atteint, le firewall applique le comportement défini concernant les paquets dont un log devait être conservé.

Le seuil peut être modifié uniquement à l'aide des commandes *CLI / Serverd* suivantes :

```
CONFIG SECURITYINSPECTION COMMON LOGALARM BlockOverflow=<0|1>
BlockDrop=<0-100>
```

```
CONFIG SECURITYINSPECTION COMMON LOGFILTER BlockOverflow=<0|1>
BlockDrop=<0-100>
```

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

Haute disponibilité

Référence support 70003

La validité de licence de l'option **Management de vulnérabilités** est désormais vérifiée avant d'exécuter une synchronisation de configuration afin de ne plus générer inutilement dans les logs des messages d'erreur du type "Target: all From: SNXXXXXXXXXXXXX Command: SYNC FILES failed: Command failed : Command has failed : code 1".

Référence support 56682

Le processus de test permettant aux nœuds d'un même cluster de s'assurer de la disponibilité de l'un et de l'autre a été amélioré afin d'éviter de déclencher à tort la bascule du nœud passif en état actif et de se retrouver dans une configuration avec deux nœuds actifs.

Haute disponibilité - VPN IPSec (politique IKEv2 ou politique IKEv1 + IKEv2)

Dans les configurations en haute disponibilité appliquant une politique IPSec IKEv2 ou IKEv1+IKEv2, une anomalie pouvait entraîner une détection inappropriée de rejeu des numéros

de séquence ESP ainsi que des pertes de paquets après deux bascules au sein du cluster. Cette anomalie a été corrigée.

Haute disponibilité - Agrégat de liens

Référence support 76748

Dans une configuration en haute disponibilité, le basculement d'un nœud actif en état passif ne désactive plus à tort une interface VLAN lorsque celle-ci est contenue dans un agrégat de liens (LACP).

Maintenance - Haute disponibilité

Référence support 75986

Dans une configuration en haute disponibilité, l'option permettant de copier la partition active vers la partition de secours depuis l'autre membre du cluster est de nouveau disponible (module **Système** > **Maintenance** > onglet **Configuration**).

Filtrage et NAT - Adresses MAC

Référence support 76399

Une règle ayant pour destination un objet machine avec une adresse MAC forcée (machine faisant l'objet d'une réservation DHCP par exemple) filtre désormais correctement le trafic qui lui correspond.

Haute disponibilité - Filtrage et NAT - Objets temps

Référence support 76822 - 73023 - 76199

Afin de ne plus provoquer d'instabilités réseau dans le cadre de clusters en haute disponibilité, des optimisations ont été apportées dans la réévaluation des règles de filtrage lors du changement d'état d'un objet temps utilisé dans l'une ou plusieurs de ces règles.

Référence support 76822

Des optimisations ont également été apportées dans la réévaluation des règles de filtrage lors du changement d'état d'un objet temps utilisé dans plusieurs règles de la politique de filtrage.

Routeurs

Références support 75745 - 74524

Lorsqu'un firewall a redémarré, le service de supervision des routeurs tient désormais correctement compte du dernier état connu de ces routeurs.

Certificats et PKI

La tentative d'import d'un certificat déjà présent dans la PKI du firewall alors que la case Écraser le contenu existant dans la PKI était décochée, n'entraîne plus une duplication de ce certificat sur le firewall.

Lors d'une connexion à un firewall depuis un serveur SMC, le firewall contrôle désormais que le certificat de ce serveur SMC comporte bien un champ *ExtendedKeyUsage* disposant de l'attribut *ServerAuth*.

Supervision des certificats et des CRL

Référence support 76169

Dans le cas d'un cluster HA, le mécanisme de supervision de la date de validité des certificats et des CRL sur le firewall passif n'entraîne plus à tort l'émission toutes les 10 secondes d'événements système de type Validité de certificat passif (événement 133) ou Validité de CRL passive (événement 135).

De plus, le mécanisme de supervision de la date de validité des CRL ne génère désormais une alerte que lorsqu'une CRL a dépassé la moitié de sa durée de validité et qu'elle expire dans un délai inférieur à 5 jours.

Mise à jour de firmware

Le certificat utilisé pour la signature des mises à jour de firmware comporte désormais une OID spécifique, contrôlée par le mécanisme de vérification des fichiers de mises à jour du firewall.

Authentification Radius

Référence support 74824

Dans une configuration d'authentification par serveur Radius avec clé pré-partagée, la sélection d'un autre objet machine dans le champ Serveur puis la sauvegarde de cette seule modification n'entraînent plus la suppression de la clé pré-partagée initialement renseignée.

Sauvegardes automatiques

Référence support 75051

Le mécanisme de vérification des certificats des serveurs de sauvegardes automatiques a été modifié suite à l'expiration du certificat précédent.

Référence support 77432

L'absence du répertoire "/log" n'empêche plus le fonctionnement correct des sauvegardes automatiques.

Interfaces réseau

Référence support 76645

Lors de la suppression d'un bridge, toutes les occurrences de ce bridge sont désormais correctement enlevées des fichiers de configuration, n'empêchant ainsi plus l'affichage des nouvelles interfaces lors de l'ajout d'un nouveau module réseau.

Relai DHCP

Référence support 75491

Lorsque des interfaces GRE sont définies sur le firewall, l'action de cocher la case Relayer les requêtes DHCP pour toutes les interfaces ne provoque plus un redémarrage en boucle du service Relai DHCP.

Réseau

Routage dynamique bird

Référence support 77707

La directive *check link* utilisée dans la section *protocol direct* du fichier de configuration du routage dynamique bird est désormais correctement prise en compte pour les interfaces réseau de type 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) et IGB (SNi20, SNi40, SN2000, SN3000, SN6000, SN510, SN710, SN910, SN2100, SN3100, SN6100).

Interfaces

Références support 73236 - 73504

Sur les modèles de firewalls SN2100, SN3100, SN6100 et SNi40, un risque de perte de paquets pouvait survenir lorsqu'un câble était relié sur :

- L'un des ports de management (MGMT) des firewalls modèles SN2100, SN3100, SN6100, ou
- L'une des interfaces d'un firewall modèle SNi40.

Ce problème a été corrigé par la mise à jour du pilote de ces interfaces.

Wi-Fi

Référence support 75238

La modification du mot de passe d'accès à un réseau Wi-Fi hébergé par le firewall est désormais correctement prise en compte lors de l'enregistrement de ce changement de configuration.

Supervision du matériel

Les événements système (identifiants 88 et 111) sont désormais générés lorsqu'un module d'alimentation défectueux revient à l'état optimal (module remplacé ou rebranché).

Prévention d'intrusion

Protocole TNS - Oracle

Références support 77721 - 71272

L'analyse d'une communication client-serveur TNS - Oracle soumise à de la fragmentation de paquets et à de la translation d'adresse (NAT) engendrait une désynchronisation du flux du fait de la réécriture des paquets. Ce problème a été corrigé.

Protocole TCP

Référence support 76621

Lorsqu'un seuil était défini pour le **Nombre maximal de connexions simultanées par machine source** dans la configuration du protocole TCP, et qu'une règle de filtrage basée sur le protocole

TCP était sujette à une tentative de déni de service de type Syn Flood, les paquets incriminés étaient correctement bloqués mais aucune alarme n'était remontée dans le fichier de logs correspondant (*l_alarm*). Cette anomalie a été corrigée.

Protocole RTSP

Référence support 73084

Lorsqu'une requête RTSP utilisant un mode de transport RTP/AVP/UDP traverse le firewall, le moteur d'analyse RTSP ne supprime plus le champ *Transport* et les canaux de diffusion s'établissent correctement.

Routage par politique (PBR)

Référence support 77489

Lors de la création d'une connexion initiée par le firewall, la recherche au sein du moteur de prévention d'intrusion d'un éventuel besoin de routage par politique de filtrage pouvait aboutir à un problème d'accès concurrentiel et entraîner un blocage du firewall. Ce problème a été corrigé.

Protocole HTTP

L'analyse du protocole HTTP ne génère plus d'alarme et n'entraîne plus de blocage de flux lorsqu'un champ de l'entête HTTP est vide, notamment dans le cas où un message SOAP est encapsulé dans une requête HTTP.

Références support 74300 - 76147

Lorsque une valeur est renseignée dans le champ **Longueur max. d'un attribut HTML (octets)** (module **Protection applicative** > **Protocoles** > **HTTP** > **onglet IPS** > **Analyses HTML/Javascript**), et qu'un paquet présente un attribut excédant cette valeur, le firewall ne renvoie plus à tort l'erreur "Attaque possible des ressources (parser data handler (not chunked))" mais bien l'erreur "Dépassement de capacité dans un attribut HTML".

Protocole NTP

Référence support 74654

Afin d'améliorer la compatibilité avec certains éditeurs, la taille maximale des paquets NTP v3 considérés comme valides est désormais fixée à 120 octets par défaut.

Compteur de connexions

Référence support 74110

Des optimisations ont été apportées au mécanisme de comptage des connexions simultanées afin de ne plus déclencher à tort l'alarme "Nombre de connexions par machine source autorisées atteint" (alarme tcpudp:364).

Protocole DNS

Référence support 71552

La gestion des requêtes de mise à jour d'enregistrements DNS a été améliorée pour se conformer à la RFC 2136 et pour ne plus déclencher à tort l'alarme bloquante "Protocole DNS invalide" (alarme dns:88).

Mise en quarantaine sur alarme du nombre de connexions

Référence support 75097

Lorsque l'action de mise en quarantaine est paramétrée pour l'alarme "Nombre de connexions par machine source autorisées atteint" (alarme tcpudp:364), la machine déclenchant cette alarme est désormais correctement ajoutée à la liste noire pour la durée de mise en quarantaine paramétrée.

Filtrage - Protocole SIP

Référence support 76009

Un message d'erreur est désormais affiché lors de la tentative d'activation d'une règle de filtrage telle que :

- L'option **Redirection d'appels SIP (UDP) entrants** est activée (**Action** > **Configuration avancée** > **Redirection**),
- Deux ports destination ou plus sont définis, l'un reposant sur le protocole ANY, et au moins un autre étant basé sur le protocole UDP ou TCP.

Routage par politique

Référence support 76999

Lors du changement d'un routeur directement au sein d'une règle de filtrage (PBR), les tables de connexions IPState (protocoles GRE, SCTP...) tiennent désormais compte du nouvel identifiant de routeur.

Matériel

Firewalls modèle SN6000

Références support 75577 - 75579

Dans des cas rares, un message indiquant que des modules d'alimentation sont manquants peut être envoyé à tort sur un firewall modèle SN6000 équipé d'un module IPMI en version 3.54. Afin de pallier ce problème, un mécanisme de redémarrage du module IPMI a été mis en place.

Désactivé par défaut, ce mécanisme n'affecte pas le trafic traversant le firewall mais rend temporairement indisponible le rafraîchissement des informations des composants. Ce mécanisme nécessite un délai d'environ cinq minutes pour arriver à son terme, comprenant le temps de redémarrage du module IPMI ainsi que le temps nécessaire pour rafraîchir les informations des composants.

Ce nouveau paramètre est uniquement modifiable à l'aide de la commande *CLI / SSH* :

```
setconf /usr/Firewall/ConfigFiles/system Monitord EnableRestartIPMI <0|1>
```

Pour plus d'informations concernant la syntaxe de cette commande, veuillez vous référer au Guide de référence des commandes CLI / SSH.

Machines virtuelles

EVA sur Microsoft Azure

Référence support 76339

Le fichier de traces du service Microsoft Azure Linux Guest Agent (fichier waagent.log) a été déplacé dans le répertoire "/log" du firewall afin de ne plus risquer de saturer le système de fichiers "/var" du firewall.

Interface Web d'administration

Utilisateurs et groupes

Référence support 78413

Dans le cas d'un annuaire possédant plusieurs milliers d'enregistrements (notamment dans des groupes imbriqués), la requête d'affichage des utilisateurs et groupes pour une sélection (exemple : module **Filtrage et NA**T) pouvait être extrêmement longue et aboutir au blocage de l'affichage du module utilisé. Ce problème a été corrigé.

Rapports

Référence support 73376

Le rapport "Top des sessions administrateurs" affiche désormais toutes les sessions des administrateurs du firewall, c'est-à-dire celles du compte *admin* (super administrateur) ainsi que toutes celles des utilisateurs et groupes d'utilisateurs ajoutés en tant qu'administrateurs. Auparavant, il n'incluait que les sessions du compte *admin* (super administrateur).

Modules réseau 40 Gb/s

Le débit maximum indiqué dans le panneau de configuration des interfaces est désormais bien de 40 Gb/s pour les modules réseau concernés.

Protocoles

Référence support 75435

Le filtre de recherche appliqué à l'arbre des protocoles (Protection applicative > Protocoles) ne reste désormais plus appliqué après un rechargement du module.

Supervision des interfaces

Référence support 76162

Le débit théorique des interfaces Wi-Fi tient désormais compte de la norme utilisée (A/B/G/N) et n'indique plus systématiquement 10 Mb/s.

Supervision Matériel / Haute Disponibilité

Le N° de série des deux membres du cluster est désormais affiché dans la liste des indicateurs.

Annuaires LDAP

Référence support 69589

L'accès à un annuaire LDAP externe hébergé sur un autre firewall Stormshield par le biais d'une connexion sécurisée (SSL) et en ayant coché la case Vérifier le certificat selon une Autorité de certification fonctionne désormais correctement.

Filtrage et NAT

Référence support 76698

Les objets réseau définis uniquement par une adresse MAC sont désormais correctement listés parmi les objets réseau disponibles lors de la création d'une règle de filtrage.

Routage statique - Routes de retour

Références support 77012 - 77013

Il est désormais possible de sélectionner une interface USB / Ethernet (modem 4G) comme interface de routage lors de l'ajout d'une route statique ou d'une route de retour.

Filtrage - Règles implicites

Référence support 77095

Lorsque l'administrateur demande à désactiver toutes les règles implicites, la commande système de désactivation est désormais correctement appliquée.

VPN SSL

Référence support 76588

A l'ouverture du module de paramétrage du VPN SSL, la fenêtre indiquant que le portail captif n'est pas activé sur les interfaces externes ne s'affiche plus à tort lorsque cette activation a bien été réalisée.

Objets routeurs globaux

Référence support 76552

Un double clic sur un objet routeur global propose désormais correctement la fenêtre d'édition de routeurs et non plus la fenêtre d'édition de machines.

Protocoles - DNS

Référence support 72583

Après avoir modifié l'action appliquée à un type d'enregistrement DNS, l'affichage successif d'autres profils DNS n'entraîne plus un défaut de rafraîchissement de la grille des types d'enregistrements DNS et des actions appliquées.

Noms d'utilisateurs

Référence support 74102

L'enregistrement d'un nom d'utilisateur dans les tables du moteur de prévention d'intrusion n'est désormais plus sensible à la casse. Ceci permet d'assurer la correspondance des noms

avec les règles de filtrage basées sur des noms d'utilisateurs authentifiés.

Méthodes d'authentification

Référence support 76608

Lors du premier accès au module **Utilisateurs** > **Authentification**, après avoir navigué sans réaliser aucune modification, puis en quittant le module, le message proposant de sauvegarder les modifications n'est plus affiché à tort.

Version 4.1.0 non publiée

La version 4.1.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités de la version 4.0.3

IMPORTANT

La mise à jour d'un firewall depuis une version SNS 3.10.x ou supérieure vers une version SNS 4.0.x ne doit pas être réalisée et n'est pas supportée.

Veuillez-vous reporter à la section Préconisations pour plus d'informations.

Système

Signature des fichiers du WebGUI

Une signature des fichiers du WebGUI de SNS a été ajoutée pour renforcer les mécanismes de communication avec SMC.

Fonctionnalités et algorithmes obsolètes

Filtrage et NAT - Fonctionnalité de Cache HTTP

La possibilité d'utiliser la fonction *Cache HTTP* au sein d'une règle de filtrage étant amenée à disparaître dans une future version de SNS, un message d'avertissement est maintenant affiché pour encourager les administrateurs à modifier leur configuration.

Ce message s'affiche sous la grille de filtrage dans le champ **Vérification de la politique**.

VPN IPSec - Algorithmes d'authentification et de chiffrement obsolètes

Certains algorithmes étant obsolètes et amenés à disparaître dans une future version de SNS, un message d'avertissement est maintenant affiché pour encourager les administrateurs à modifier leur configuration. Les algorithmes concernés sont les suivants :

- Algorithmes d'authentification : *md5*, *hmac_md5*, *non_auth*,
- Algorithmes de chiffrement : *blowfish*, *des*, *cast128*, *null_enc*.

Ce message s'affiche lorsque ces algorithmes sont utilisés dans le profil d'un correspondant IPSec.

VPN IPSec - Correspondants de secours

L'utilisation de correspondants de secours (désigné en tant que "Configuration de secours") étant obsolète et amenée à disparaître dans une future version de SNS, un message d'avertissement est maintenant affiché pour prévenir les administrateurs afin de les encourager à modifier leur configuration. Ce message s'affiche sous la grille des politiques IPSec dans le champ **Vérification de la politique**.

Pour ce cas d'usage, privilégiez l'utilisation d'interfaces IPSec virtuelles avec des objets routeurs ou du routage dynamique.

Vulnérabilités résolues de la version 4.0.3

Protocole S7

Le firewall redémarrait de manière inopinée dans le cas où :

- Un flux S7 contenait un échange avec un paquet requête invalide suivi d'un paquet réponse invalide,
  et
- L'alarme "S7 : protocole invalide" (alarme s7:380) était configurée en "Autoriser",
  et
- L'option "Tracer chaque requête S7" était activée dans la configuration du protocole S7.

Ce défaut a été corrigé.

Protocole SIP sur TCP

Une anomalie pouvant aboutir à un double verrou sur une session SIP et provoquer l'arrêt inopiné de l'analyse du protocole SIP sur TCP a été corrigée.

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

Protocole SNMP

Référence support 76629

L'exécution d'une opération SNMP lorsqu'un OID incorrect (qui ne commence pas par un ".") était renseigné en liste noire dans la configuration du protocole SNMP ne provoque plus un redémarrage en boucle du firewall.

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

FreeBSD

La mauvaise initialisation d'un champ d'en-tête IPv6 pouvait aboutir à une fuite mémoire non exploitable par un attaquant.

Cette vulnérabilité (CVE-2020-7451) a été corrigée par l'application d'un correctif de sécurité dans la pile réseau TCP de FreeBSD.

NetBIOS

Une vulnérabilité pouvait permettre par le biais d'une session NetBIOS d'envoyer au travers du firewall des paquets NetBIOS spécialement conçus dans le but de réaliser un déni de service.

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

Correctifs de la version 4.0.3

Système

VPN IPsec (IKEv1)

Référence support 75824

Lors du basculement d'un correspondant distant vers son correspondant de secours (désigné en tant que "Configuration de secours"), un redémarrage inopiné du démon IKE pouvait survenir entraînant ainsi la fermeture des tunnels IPsec ouverts. Cette anomalie a été corrigée.

GRETAP et IPSec

Référence support 76066

Dans une configuration comportant une interface GRETAP dialoguant au travers d'un tunnel IPSec, la commande système *ennetwork -f* ne provoque plus un redémarrage en boucle du firewall.

VPN SSL

Un nouveau certificat permettant de signer les fichiers compilés Java (.jar) a été installé, remplaçant l'ancien certificat qui allait expirer prochainement (24/05/2020).

Firewalls modèle SN910

Référence support 76528

À la suite d'une mise à jour d'un firewall depuis une version SNS 3.9.x vers une version SNS 4.0.x, l'ordonnancement des ports des interfaces IX n'était plus correct sur les firewalls modèle SN910 équipés d'une carte IX.

Un mécanisme automatique permettant de rétablir l'ordonnancement des ports a été mis en place.

Temps d'arrêt (shutdown) d'un démon

Référence support 74990

Dans des cas rares, un démon pouvait être arrêté (shutdown) après un certain temps, bloquant alors le processus de mise à jour du firewall. Ce temps a été réduit pour permettre la bonne exécution de la mise à jour du firewall.

Réseau

Réseau Wi-Fi

Références support 73816 - 75634 - 75958

Les équipements disposant d'une carte Wi-Fi "*Intel Wireless-N 7260*" ou "*Qualcomm Atheros AR6004 802.11a/b/g/n*" pouvaient rencontrer des problèmes de connectivité au Wi-Fi du firewall. Cette anomalie a été corrigée.

Prévention d'intrusion

Protocole TDS
L'analyse du champ *Status* dans les paquets de flux de données tabulaires (TDS - Tabular Data Stream) ne remonte plus à tort l'alarme "TDS : protocole invalide" (alarme tds:423).

Protocole NB-CIFS
L'analyse de flux NB-CIFS issus de machines Microsoft Windows ne remonte plus à tort l'alarme "Protocole NBSS / SMB2 invalide" (alarme nb-cifs:157).

Protocole LDAP
L'authentification via SASL (Simple Authentication and Security Layer) supporte dorénavant le protocole NTLMSSP, ce qui ne génère plus d'erreurs lorsqu'un flux LDAP utilisant ce protocole est analysé.

Protocole NTP
Les paquets NTP présentant un complément *origin timestamp* égal à zéro ne déclenchent plus à tort l'alarme "NTP : valeur invalide" (alarme ntp:451).

Protocole DNS

Références support 72754 - 74272

L'analyse du protocole DNS a été modifiée afin de réduire le taux de faux positifs de l'alarme "DNS id spoofing" (alarme dns:38).

Interface Web d'administration

Accès aux données personnelles (logs)
La manipulation pour obtenir un accès complet aux données personnelles (logs) s'effectue de nouveau en cliquant directement sur le message "Logs : Accès restreint" dans le bandeau supérieur.

Configuration des annuaires

Référence support 76069

Lorsqu'un annuaire LDAP externe est défini comme annuaire par défaut, une modification des paramètres de cet annuaire ne remplace plus à tort le nom de l'annuaire par la mention *NaN*.

Interfaces

Référence support 76497

L'affichage des adresses IP des interfaces 11 et supérieures était répliqué sur la seconde interface du firewall, affichant ainsi une information erronée. Cette anomalie a été corrigée.

Authentification
Les champs "Clé prépartagée" lors de la configuration d'une méthode d'authentification "RADIUS" n'étaient pas pris en compte. Cette anomalie a été corrigée.

Nouvelles fonctionnalités de la version 4.0.2

IMPORTANT

La mise à jour d'un firewall depuis une version SNS 3.10.x ou supérieure vers une version SNS 4.0.x ne doit pas être réalisée et n'est pas supportée.

Veuillez-vous reporter à la section Préconisations pour plus d'informations détaillées.

Stabilité et performances

La synchronisation entre SNS et SMC a été améliorée afin de fluidifier les échanges de données entre les deux produits, notamment lors de l'accès direct à l'interface d'administration des firewalls depuis SMC.

Sécurité renforcée lors de la mise à jour du firmware

Le niveau de sécurité des mises à jour de firmware a été renforcé : en plus de protéger par signature l'intégrité des packages de mise à jour, Stormshield sécurise désormais les communications avec les serveurs de mise à jour utilisés. Ces communications s'établissent désormais via le protocole HTTPS et le port 443.

Matériel

Commandes SSH

Une nouvelle commande *CLI / SSH* permet de manipuler le TPM. Elle débute par :

```
tpmctl
```

Elle intègre notamment une commande permettant d'approuver les nouveaux registres *PCRs* (ou *Platform Configuration Registers*) à la suite d'une mise à jour du BIOS ou de modules matériels.

Pour plus d'informations concernant la syntaxe de cette commande, veuillez vous référer au Guide de référence des commandes CLI / SSH.

Vulnérabilités résolues de la version 4.0.2

Portail d'authentification (portail captif)

Des contrôles ont été ajoutés dans la vérification des paramètres utilisés dans l'adresse URL du portail d'authentification (portail captif) du firewall.

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

Commandes CLI / Serverd

Des améliorations ont été apportées à la commande CLI/Serverd CONFIG AUTOUPDATE SERVER afin de mieux contrôler l'usage du paramètre "url".

Bibliothèque *libfetch*

La vulnérabilité **CVE-2020-7450** a été corrigée par l'application d'un correctif de sécurité sur la bibliothèque *libfetch* de FreeBSD.

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

Interface Web d'administration

Des contrôles additionnels ont été implémentés dans la vérification des paramètres utilisés dans l'adresse URL de l'interface Web d'administration du firewall.

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

Correctifs de la version 4.0.2

Système

Proxy SSL

Référence support 74927

Afin d'éviter des problèmes de compatibilité avec certains logiciels embarqués ou certains navigateurs (sous iOS 13 et MacOS 10.15) lors des connexions SSL, la taille des clés de certificats générés par le proxy SSL a été augmentée à 2048 bits.

Référence support 74427

En cas d'expiration de l'autorité de certification du proxy SSL, le firewall ne tente plus de générer inutilement de nouvelles clés lors de certains événements (rechargement de la politique de filtrage, rechargement de configuration réseau, changement de date du firewall...), ce qui entraînait une consommation CPU excessive.

Proxies

Références support 66508 - 71870

Sous forte charge, le proxy pouvait s'arrêter à l'échec d'une analyse d'entête HTTP. Ce problème a été corrigé.

Référence support 71870

Le proxy ne s'arrête plus de manière inopinée lorsque le proxy SSL est utilisé et que le nombre de connexions simultanées maximum est atteint sur le firewall.

Références support 70721 - 74552 - 75874

La consommation de la mémoire en cas d'utilisation du proxy a été optimisée.

Proxy - Filtrage d'URL

Référence support 73516

Le proxy HTTP/HTTPS pouvait perdre la connexion avec le moteur de filtrage d'URL de la solution Extended Web Control, provoquant l'affichage de la page d'information *URL filtering is pending* aux clients dont les connexions utilisaient le proxy. Ce problème a été corrigé.

Filtrage et NAT

Références support 76343 - 76231

La présence de plusieurs règles successives utilisant un objet commun n'empêche plus le rechargement de la politique de filtrage.

VPN IPSec

Références support 74551 - 74456

Une anomalie dans le fonctionnement de la fonction key_dup_keymsg() d'IPSec provoquant l'erreur *Cannot access memory at address* et entraînant un arrêt inopiné du firewall a été corrigée.

Référence support 74425

Un paramètre pouvait empêcher le mode *ResponderOnly* de fonctionner correctement lorsque le mécanisme de *Dead-Peer-Detection* (DPD) s'activait. Cette anomalie a été corrigée.

VPN IPSec (IKEv2 / IKEv1+IKEv2)

Référence support 68796

Dans une configuration utilisant une politique IPSec IKEv2 ou mixant IKEv1 et IKEv2, le firewall n'envoyait pas de masque réseau au client VPN IPSec Stormshield lors de l'établissement d'un tunnel mobile (nomade) en mode config. Le masque réseau choisi arbitrairement par le client IPSec pouvait alors entrer en conflit avec la configuration de réseau local du poste client.

Le firewall envoie désormais systématiquement le masque réseau /32 (255.255.255.255) au client VPN IPSec pour un tunnel mobile (nomade) en mode config.

Objets machine globaux inclus dans un objet routeur

Référence support 71974

Le renommage d'un objet machine global inclus dans un objet routeur est désormais correctement pris en compte au sein de cet objet routeur.

Certificats et PKI

Référence support 76048

Les espaces présents dans le chemin d'import d'une Autorité de Certification sont désormais correctement interprétés et ne bloquent plus cet import.

Mode ANSSI "Diffusion Restreinte"

Lors de l'activation du mode ANSSI "Diffusion Restreinte" (module **Système** > **Configuration** > onglet **Configuration générale**), un mécanisme vérifie la compatibilité des groupes Diffie-Hellmann (DH) utilisés dans la configuration des correspondants IPSec avec ce mode. Cette liste de groupes DH autorisés a été mise à jour et seuls les groupes DH 19 et 28 doivent être utilisés.

Consommation mémoire excessive du démon Serverd

Références support 76158 - 75155

La consommation mémoire du démon Serverd augmentait de façon excessive avec le nombre de connexions distantes établies via SMC. Ce phénomène, pouvant déboucher sur l'impossibilité d'établir une connexion à l'interface Web d'administration du firewall, a été corrigé.

Analyse Sandboxing

Référence support 76121

En l'absence d'une licence d'analyses Sandboxing (option Stormshield Breach Fighter) ou lorsque cette licence est expirée, une tentative de rechargement de sa configuration par le moteur de gestion des analyses Sandboxing (démon AVD) ne provoque plus l'arrêt inopiné de ce dernier.

Réseau

Routage statique

Référence support 72938

L'usage de directives de routage par politique (PBR) est désormais prioritaire par rapport au choix de préserver le routage initial sur l'interface d'entrée d'un bridge. Cette nouvelle priorité ne s'applique pas aux réponses DHCP lorsque l'IPS ajoute automatiquement de préserver le routage initial.

Référence support 72508

Un objet routeur avec répartition de charge configuré en tant que passerelle par défaut sur le firewall pouvait outrepasser une route statique. Ce phénomène initiait depuis le firewall des connexions avec une adresse IP source incorrecte. Cette anomalie a été corrigée.

Trusted Platform Module (TPM)

Référence support 76181

La récupération d'une clé de chiffrement stockée sur le TPM par le moteur de gestion des tunnels IPSec IKE2 / IKEv1+IKEv2 ne provoque plus de fuite mémoire.

Prévention d'intrusion

Protocole SIP

Référence support 75997

Lorsqu'un paquet SIP émis ainsi que sa réponse contenaient un champ avec une adresse IP anonyme et que l'alarme 465 "SIP : Adresse anonyme dans la connexion SDP" était configurée en "Autoriser", le firewall redémarrait de manière inopinée. Cette anomalie a été corrigée.

Protocole SNMPv3

Référence support 72984

L'analyse protocolaire SNMP ne déclenche plus à tort l'alarme "nom d'utilisateur SNMP interdit" (snmp:393) pour les identifiants spécifiés dans la liste blanche du protocole SNMPv3.

Trusted Platform Module (TPM)

Référence support 76181

Dans certains cas, une anomalie dans une fonction pouvait amener à une pénurie de handle (ou identifiant d'objet) utilisé notamment pour s'authentifier sur le TPM, empêchant alors de communiquer avec ce dernier. Cette anomalie a été corrigée.

Firewalls virtuels EVA

Commandes CLI / Serverd

La commande CLI / Serverd MONITOR HEALTH exécutée sur un firewall virtuel EVA retourne désormais la valeur *N/A* pour les modules physiques absents (Ventilateur, Disque...), au lieu de

la valeur *Unknown* qui provoquait une anomalie sur les consoles d'administration SMC.

Interface Web d'administration

Portail d'authentification (portail captif)

Référence support 76398

Le focus n'est plus positionné par défaut sur la valeur *Annuler* de l'écran de connexion du portail captif. Un appui sur la touche [Entrée] du clavier après la saisie de l'identifiant et du mot de passe associé ne provoque donc plus une déconnexion inappropriée de l'utilisateur.

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.

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.

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2021. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.