STORMSHIELD

STORMSHIELD NETWORK SECURITY

NOTES DE VERSION

Version 4.3 LTSB

Dernière mise à jour du document : 24 septembre 2024

Référence : sns-fr-notes_de_version-v4.3.30-LTSB

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.

Label LTSB (Long-Term Support Branch)

Les versions majeures ou mineures disposant de ce label sont considérées comme des versions stables à long terme. Leur prise en charge est assurée pendant 12 mois minimum. Ces versions sont recommandées pour les clients qui accordent plus d'importance à la stabilité qu'aux nouvelles fonctionnalités et optimisations.

Pour plus d'informations, reportez-vous au document **Cycle de vie produits Network Security & Tools**.

Historique des modifications

Date	Description
24 septembre 2024	Nouveau document

Points d'attention pour une mise à jour depuis une version 3.7 LTSB ou 3.11 LTSB

IMPORTANT
Si vous envisagez de mettre à jour un firewall depuis une version 3.7 LTSB / 3.11 LTSB vers la version 4.3 LTSB, nous vous recommandons de lire attentivement cette section.

NOTE
La liste exhaustive des changements de comportements automatiques liés à la mise à jour de votre firewall SNS en version 4.3 LTSB depuis la dernière version 3.7 LTSB disponible est consultable dans la section Changements de comportement de ces Notes de Versions.

Classification d'URL *Extended Web Control* (EWC)

La classification d'URL *Extended Web Control* utilise désormais la base d'URL du fournisseur *Bitdefender*.

Ce changement de base d'URL impose de remanier la politique initiale de sécurité du firewall (politique de filtrage, politique de filtrage URL et politique de filtrage SSL) après sa mise à jour.

Veuillez consulter la Note Technique Migrer une politique de sécurité vers la nouvelle base d'URL EWC pour connaître les étapes de migration d'une politique de filtrage d'URL / filtrage SSL lors de la mise à jour du firewall en version SNS 4.3.24 LTSB ou supérieure.

Fonctionnalité de Cache HTTP

La fonction Cache HTTP au sein d'une règle de filtrage n'est plus disponible. Avant de mettre à jour votre firewall, il est nécessaire de :

- Supprimer les options "cache HTTP" des règles de filtrage concernées,
- Désactiver le proxy cache.

Dans le cas contraire, le proxy ne sera plus fonctionnel.

Haute disponibilité (HA)

Les ports utilisés pour la communication via les liens de HA ont évolué. La politique de filtrage doit donc être adaptée en conséquence sur les membres du cluster ainsi que sur les éventuels équipements intermédiaires par lesquels les flux de HA transitent avant de réaliser la mise à jour du firewall. Ceci afin d'éviter une perte de connexion entre les membres du cluster.

Les ports utilisés par la HA sont disponibles dans la section Flux réseau liés à la HA de la note technique Haute disponibilité sur SNS.

VPN IPsec

VPN IPsec et HA
Les tunnels IPsec établis ne seront pas synchronisés entre les 2 membres du cluster lors de la mise à jour : ils seront interrompus et renégociés afin de pouvoir faire transiter le trafic chiffré.

Mode DR

Le mode DR défini en version 4.3 LTSB 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 est refusée par le firewall.

Veuillez consulter la note technique VPN IPsec - Mode Diffusion Restreinte pour la configuration du mode DR des versions 4.3 LTSB.

IKEv1

Les configurations listées ci-dessous ne sont plus autorisées en version 4.3 LTSB :

- 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.

Algorithmes non supportés

Les versions de firmware 4.3 LTSB n'assurent plus le support des algorithmes suivants :

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

Si la politique IPsec du firewall à mettre à jour en version 4.3 LTSB 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 la mise à jour.

NAT-T

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.

Qualité de service (QoS)

Les configurations de QoS définies dans une version antérieure à SNS 4.3 LTSB ne sont plus valides et il est impératif de reconfigurer la QoS après mise à jour du firewall.

Veuillez consulter la note technique Configurer la QoS sur les firewalls SNS pour la configuration de la QoS en version 4.3 LTSB.

Filtrage

SNS permet maintenant de définir et d'utiliser dans les politiques de filtrage des objets réseau basés sur les adresses MAC. Lorsqu'une adresse MAC est précisée dans un objet utilisé au sein d'une règle de filtrage, tout trafic provenant de cet objet et correspondant à cette règle de filtrage ne sera pas évalué si l'adresse MAC présentée durant l'échange diffère de celle de l'objet.

Firewalls équipés d'un TPM

Après une mise à jour en version SNS 4.3, les secrets stockés dans le TPM nécessitent d'être scellés avec les nouvelles caractéristiques techniques du système à l'aide de la commande : `tpmctl -svp <TPMpassword>`.

Pour plus d'informations sur ce sujet, consultez la Base de connaissances Stormshield.

VPN SSL

Il est nécessaire d'utiliser la dernière version 3.x du client VPN SSL.

Masque des réseaux assignés aux clients

La taille minimale du masque de l'objet réseau assigné aux clients UDP et TCP dans la configuration VPN SSL est à présent de /28.

Si le masque de cet objet réseau était de /29, il doit être modifié avant la migration du firewall en version 4.3 LTSB.

Authentification

Portail captif

Le portail captif n'accepte plus la sélection de certificats autres que des certificats serveur comportant l'ExtendedKeyUsage ServerAuth.

Agent SSO

Il est nécessaire d'utiliser la dernière version 3.x de l'Agent SSO.

Routage dynamique

Noms internes des interfaces sur les firewalls modèles SN160 et SN210(W)

Le nom interne des interfaces a changé sur les firewalls modèle SN160 et SN210(W).

Afin d'éviter des incohérences dans la configuration, il est fortement recommandé d'utiliser le nom utilisateur des interfaces (exemple : *out*) en lieu et place des noms internes des interfaces (exemple : *eth0*) et ce, quel que soit le modèle de firewall.

Protocole BGP

Dans les configurations utilisant le protocole BGP avec de l'authentification, il est nécessaire d'utiliser la directive "source address <ip>;".

Pour de plus amples informations sur la configuration de Bird, veuillez consulter la note technique Routage dynamique Bird.

Protocoles industriels

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

Système

Durcissement du système d'exploitation

Le durcissement du système d'exploitation impose les contraintes suivantes pour les scripts personnalisés :

- Seuls les scripts *shell* sont autorisés et ils doivent explicitement être appelés par l'interpréteur (par exemple : sh script.sh et non ./script.sh).
- Pour les scripts lancés par le biais du planificateur d'événements (*eventd*), l'interpréteur doit être ajouté pour chaque tâche décrite dans le fichier de configuration du planificateur d'événements.
- Les scripts doivent être exclusivement situés dans la partition root (/) pour pouvoir être exécutés.

Protocole TLS - Suites cryptographiques

Les suites cryptographiques utilisées par le firewall pour initier ses propres connexions TLS (LDAPS, SYSLOG TLS, SMTPS...) ont été mises à jour. Les suites utilisables sont désormais :

- TLS_AES_128_GCM_SHA256,
- TLS_CHACHA20_POLY1305_SHA256,
- TLS_AES_256_GCM_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV.

Cette mise à jour peut rendre le firewall incompatible avec des serveurs utilisant des suites moins robustes. Nous vous invitons donc à vérifier la compatibilité des services TLS en interaction avec le firewall. Dans le cas précis du service LDAPS Microsoft Azure, il est nécessaire de forcer le firewall à initier des connexions utilisant des suites cryptographiques moins robustes (ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384 ou DHE-RSA-AES256-SHA256) à l'aide la commande CLI / Serverd `CONFIG CRYPTO SSLParanoiac=0`.

Un redémarrage du firewall est nécessaire pour la prise en compte de cette modification.

Protocole TLS et services du firewall

Les services du firewall (LDAP, authentification, proxy...) utilisant le protocole TLS imposent désormais l'utilisation de TLS 1.2 ou 1.3. Les tentatives de connexion dans des versions antérieures de ce protocole n'aboutiront plus.

Active Update

Utilisation de miroirs internes

Si vous utilisez un site miroir interne Active Update, il est nécessaire de mettre à jour les paquets hébergés sur votre serveur avec les paquets signés par la nouvelle autorité de certification.

Il est également possible d'héberger le site miroir Active Update sur un serveur Stormshield Management Center (SMC).

En savoir plus sur l'**utilisation de SMC comme point de distribution Active Update**.

Sécurité renforcée pour les mises à jour de 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.

SN Real-Time Monitor (SNRTM)

SN Real-Time Monitor n'est pas compatible avec les versions 4.3 LTSB.
La supervision des firewalls doit désormais être réalisée au travers de l'onglet **Monitoring** de l'interface Web d'administration.

Firewalls virtuels

Pour pouvoir mettre à jour en version 4.3 LTSB un firewall virtuel initialement en version SNS 3.7 ou inférieure, veuillez suivre la **procédure de migration d'un firewall virtuel V / VS-VU vers un modèle EVA**.

Changements notables introduits entre la dernière version 3.7 LTSB et la dernière version 3.11 LTSB

VPN IPsec et CRL

Lorsque le paramètre *CRLRequired* est activé dans la configuration d'une politique VPN, il est désormais nécessaire de disposer de toutes les CRL de la chaîne de certification.

VPN SSL (OpenVPN)

Renforcement du niveau de sécurité

Le niveau de sécurité mis en œuvre lors de la négociation et de l'utilisation de tunnels VPN SSL (OpenVPN) a été accru.

Si vous utilisez le client VPN SSL Stormshield avec le **mode automatique désactivé** ou un autre client OpenVPN, la configuration des clients VPN SSL doit donc être modifiée en conséquence. Pour cela, téléchargez la configuration VPN SSL depuis le portail captif du firewall SNS hébergeant le service VPN SSL et importez la sur les clients. Avec le client VPN SSL Stormshield en mode automatique, le client récupérera automatiquement sa configuration.

Les nouvelles exigences à respecter sont les suivantes :

- L'utilisation d'algorithmes d'authentification et de chiffrement de force supérieure :
  - SHA256,
  - ECDHE-RSA-AES128-SHA256,
  - AES-256-CBC (sauf sur les firewalls modèles SN160(W), SN210(W), SN310 qui conservent l'algorithme AES-128-CBC).
- Une compression des données activable basée sur les algorithmes LZ4,

- La vérification stricte du certificat présenté par le serveur (nom du certificat, et certificat de type "serveur").

Si vous n'utilisez pas le client VPN SSL Stormshield, notez qu'il est impératif de travailler avec une version récente des clients OpenVPN (2.4.x) ou OpenVPN Connect (smartphones et tablettes).

VPN SSL et certificats

Dans les configurations VPN SSL utilisant des certificats qui ne disposent pas du champ *KeyUsage*, les services externes peuvent ne plus parvenir à communiquer avec le firewall.

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

Changements de comportement

Cette section liste les changements de comportements automatiques liés à la mise à jour de votre firewall SNS en version 4.3.30 LTSB depuis la dernière version 3.7 LTSB disponible.

Changements introduits en version 4.3.28 LTSB

- Analyse Sandboxing - Seuls les fichiers classifiés dans l'une des catégories Archive, Document bureautique, Exécutable, PDF et Java sont désormais soumis à l'analyse Sandboxing afin de limiter la charge du service. Les fichiers classifiés dans Autre ou Inconnu ne sont plus envoyés pour analyse.

Changements introduits en version 4.3.26 LTSB

- Module réseau NC-1-8xG-FIB-SFP - Sur les firewalls modèles SN-L-Series et SN-XL-Series, un défaut d'ordonnancement des ports du module 8 ports fibre référence NC-1-8xG-FIB-SFP présent en version SNS 4.3.25 LTSB est corrigé lors de la mise à jour du firewall en version SNS 4.3.26 LTSB.

Ordre des ports du module en version SNS 4.3.25 LTSB :

1	3	5	7
2	4	6	8

Ordre des ports du module en version SNS 4.3.26 LTSB :

1	2	3	4
5	6	7	8

Changements introduits en version 4.3.25 LTSB

- Agent SNMP - La valeur retournée par l'OID *1.3.6.1.2.1.1.7* est désormais 76, ce qui correspond à un équipement offrant des services sur les couches OSI 3, 4 et 7. Auparavant, la valeur retournée était 72.

Changements introduits en version 4.3.24 LTSB

- SN1100 - Le nombre maximal de tunnels IPsec acceptés par un firewall SN1100 était trop élevé. Il a été diminué pour correspondre aux données annoncées.

- Classification d'URL *Extended Web Control* (EWC) - La base d'URL utilisée est désormais celle du fournisseur *Bitdefender*.

  Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est-à-dire de positionner explicitement les catégories d'URL à interdire dans des règles de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Ces règles sont à placer au-dessus de la règle autorisant toutes les autres catégories.

  Dans le cadre de la mise à jour en version SNS 4.3.24 LTSB ou supérieure d'un firewall utilisant une politique de filtrage d'URL / filtrage SSL en mode "liste blanche" (règles de filtrage autorisant explicitement certaines catégories et placées au-dessus de la règle bloquant toutes les autres catégories), il est fortement recommandé d'ajouter une règle autorisant les catégories d'URL *misc* (Divers), *unknown* (Inconnu), *computersandsoftware* (Sites de téléchargement de logiciels) et *hosting* (Hébergement de sites Web) pour éviter un risque de dégradation de l'expérience utilisateur. Cette règle est à placer au-dessus de la règle bloquant toutes les autres catégories.

  Pour plus d'informations sur la migration d'une politique de filtrage d'URL / filtrage SSL lors de la mise à jour du firewall en version SNS 4.3.24 LTSB ou supérieure, veuillez consulter la **Note Technique** Migrer une politique de sécurité vers la nouvelle base d'URL EWC.

  IMPORTANT
  Il est impératif de contrôler minutieusement toute politique de filtrage d'URL / filtrage SSL mise à jour suite au passage du firewall en version SNS 4.3.24 LTSB.

Changements introduits en version 4.3.23 LTSB

En savoir plus

- Routage - Les objets de type *loopback* utilisés en passerelle par défaut sont automatiquement remplacés par l'objet *blackhole* lors de la mise à jour du firewall en version SNS 4.3.23 LTSB ou supérieure.
- Protocoles Oscar et Gnutella - Les protocoles Oscar et Gnutella sont désormais considérés comme obsolètes. L'analyse de ces protocoles est automatiquement désactivée lors de la mise à jour du firewall en version SNS 4.3.23 LTSB.

Changements introduits en version 4.3.22 LTSB

En savoir plus

- Connexions SSH à destination du firewall - Sur un firewall en configuration d'usine et en version SNS 4.3 LTSB (à partir de la version 4.3.22 LTSB), les algorithmes de chiffrement ssh-rsa, hmac-sha2-256 et hmac-sha2-512 ne sont plus autorisés pour les connexions SSH à destination du firewall.

Changements introduits en version 4.3.21 LTSB

En savoir plus

- IPsec DR - Le référentiel IPsec DR de l'ANSSI demande de remplacer l'algorithme utilisé dans la génération des Certificate Request Payload par le SHA2 (anciennement SHA1). Les versions SNS 4.3 LTSB (à partir de la version 4.3.21 LTSB) respectent cette recommandation.
  Si le mode IPsec DR est activé sur un firewall SNS en version 4.3.21 LTSB, la négociation de tunnels VPN est possible uniquement avec des correspondants respectant cette recommandation.
- Client VPN Exclusive (avec mode DR) - Il est nécessaire d'utiliser le client VPN Exclusive 7.4 (ou supérieur) pour établir des tunnels IPsec en mode DR avec des firewalls en version SNS 4.3.21 LTSB et versions 4.3 LTSB supérieures.

Changements introduits en version 4.3.18 LTSB

En savoir plus

- Routage dynamique BIRD - Dans les configurations utilisant le protocole BGP avec de l'authentification, il est nécessaire d'utiliser la directive "source address <ip>;" pour que les sessions BGP continuent de s'établir après la mise à jour du firewall SNS.

Changements introduits en version 4.3.17 LTSB

En savoir plus

- VPN IPsec sur les firewalls modèles SN 160(W), SN210(W) et SN310 - L'option ESN (*Extended Sequence Number*) n'est plus activée automatiquement lorsque l'algorithme de chiffrement sélectionné est compatible avec l'accélération matérielle. Cette activation automatique entraînait en effet une baisse de performances.

Changements introduits en version 4.3.16 LTSB

En savoir plus

- Protocoles basés sur SSL / TLS - Pour des raisons de sécurité, les suites de chiffrement utilisant un échange de clés basées sur les méthodes Diffie-Hellman (suites basées sur DHE) ont été supprimées. Seules les suites basées sur ECDHE sont disponibles sur les firewalls SNS.
  Cette modification peut impacter les connexions émises depuis ou vers le firewall pour les différents protocoles sécurisés par SSL (HTTPS, SSH, LDAPS, SMTPS...) ainsi que les connexions SSL réalisées au travers du proxy du firewall.
  Elle peut potentiellement rendre incompatibles avec les firewalls SNS les anciens logiciels clients et services / machines externes utilisant ces protocoles.

  Les suites de chiffrement basées sur ECDHE et disponibles sur les firewalls SNS sont les suivantes :
  - TLS_AES_128_GCM_SHA256,
  - TLS_CHACHA20_POLY1305_SHA256,
  - TLS_AES_256_GCM_SHA384,
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV.

Changements introduits en version 4.3.15

En savoir plus

- Qualité de service (QoS) - Le champ **Traitement en cas de saturation**, permettant de sélectionner l'algorithme de traitement des congestions de paquets (**TailDrop** ou **BLUE**) dans les files d'attente, a été supprimé du paramétrage de la QoS. L'algorithme utilisé par défaut est désormais **TailDrop** et est exclusivement modifiable à l'aide de la commande CLI / Serverd `CONFIG OBJECT QOS DROP`.
- Protocole TLS 1.3 - Le mécanisme d'analyse des certificats TLS 1.3 des serveurs SSL est désormais automatiquement désactivé lors de la migration d'un firewall depuis une version inférieure à SNS 4.3.x vers une version supérieure ou égale à SNS 4.3.15. Il est également désactivé par défaut dans le profil entrant d'analyse SSL *SSL_00* pour les firewalls en configuration d'usine en version 4.3.15 ou supérieure.

Changements introduits en version 4.3.11

En savoir plus

- Durcissement du système d'exploitation - Les éditeurs de texte *vim* et *joe* ont été supprimés du système au profit de l'éditeur *vi*.
- IPsec / IPv6 - Il n'est plus possible d'activer le mécanisme de *keepalive* pour les tunnels IPsec en IPv6.
- IPsec mode DR - Lors de la première activation du mode DR, le groupe Diffie-Hellman DH28 est désormais proposé comme groupe par défaut pour les profils IKE DR et IPsec DR.

Changements introduits en version 4.3.10

En savoir plus

- Qualité de service (QoS) - La définition de files d'attente en pourcentage de bande passante est obsolète. Après la mise à jour en version 4.3.10 ou supérieure d'un firewall SNS dont la configuration de QoS utilisait une file d'attente définie par un pourcentage de bande passante, ce pourcentage est automatiquement transformé en valeur absolue de bande passante équivalente.

Changements introduits en version 4.3.9

En savoir plus

- VPN IPsec IKEv2 - Lorsqu'un tunnel IPsec IKEv2 établi avec un correspondant nomade en mode CONFIG est interrompu brutalement par le client distant, l'adresse IP qui lui a été attribuée reste verrouillée et indisponible. Le paramètre *unique* (pour *UniqueIDs*) a été ajouté aux commandes CLI / Serverd **`CONFIG IPSEC PEER NEW`** et **`CONFIG IPSEC PEER UPDATE`** afin de pouvoir modifier ce comportement.
  Par exemple, pour permettre à un utilisateur de retrouver sa précédente adresse IP, utilisez le paramètre *unique=no*, puis rechargez la configuration de la politique VPN avec les commandes CLI / Serverd `CONFIG IPSEC ACTIVATE` et `CONFIG IPSEC RELOAD` (interrompt les tunnels en cours).

Changements introduits en version 4.3.7

En savoir plus

- Mode furtif - En configuration d'usine un firewall SNS est désormais en mode furtif par défaut.

Changements introduits en version 4.3.3

En savoir plus

- QoS - Les configurations de QoS définies dans une version antérieure à SNS 4.3 ne sont plus valides et il est impératif de reconfigurer la QoS après mise à jour du firewall.
- Haute disponibilité et agrégats de liens - Sur une configuration disposant d'agrégats de liens, l'initialisation de la haute disponibilité active par défaut l'option **Activer l'agrégation de liens lorsque le firewall est passif**.
- Firewalls équipés d'un TPM (SNi20, SN1100 et SN3100) - Après une mise à jour en version SNS 4.3, les secrets stockés dans le TPM nécessitent d'être scellés avec les nouvelles caractéristiques techniques du système à l'aide de la commande : `tpmctl -svp <TPMpassword>`.
  Pour plus d'informations sur ce sujet, consultez la Base de connaissances Stormshield.
- Protocole TLS 1.3 - Certains flux TLS 1.3 peuvent à présent être bloqués alors qu'ils ne l'étaient pas auparavant en raison d'une nouvelle analyse de certificats serveur.
- Protocole TLS 1.3 - L'analyse par le firewall des certificats TLS 1.3 des serveurs SSL peut nécessiter d'ajouter explicitement dans les équipements périphériques de sécurité l'autorisation d'accès de l'adresse IP (ou des adresses IP) du firewall aux serveurs SSL contactés.
- Protocole TLS 1.3 - Le proxy SSL supporte désormais le protocole TLS 1.3.
- Profils IPsec / Groupes Diffie-Hellman - Lors de la création d'un profil IKE / IPsec, le groupe Diffie-Hellman proposé par défaut est désormais le DH14 (plus sécurisé) et non plus le DH1.
- Protection contre les attaques par force brute - L'accès distant par SSH au firewall est désormais protégé contre les attaques par force brute.
- Authentification RADIUS - Le nombre maximum d'essais et le délai d'inactivité autorisé pour réaliser une connexion à un serveur RADIUS (serveur principal et serveur de secours) peuvent désormais être configurés.
- Authentification RADIUS - Il est désormais possible de joindre des serveurs RADIUS en IPv6.
- VPN SSL- La taille minimale du masque de l'objet réseau assigné aux clients UDP et TCP dans la configuration VPN SSL est à présent de /28. Si le masque de cet objet réseau était de /29, il doit être modifié avant la migration du firewall en version 4.3.3 ou supérieure.

- Enrôlement des certificats - Lors de la réalisation d'une demande d'enrôlement de certificat, les utilisateurs doivent à présent définir eux-mêmes la clé de chiffrement utilisée pour chiffrer leur clé privée.
- Durcissement du système d'exploitation - Il n'est plus possible de préciser un port spécifique local de connexion aux agents / serveurs (principaux et de secours) pour les méthodes d'authentification RADIUS et Agent SSO. Ces options étaient exclusivement configurables par le biais des jetons *AgentBindPort* et *BackupBindPort* présents dans les fichiers de configuration de ces méthodes d'authentification.
- Durcissement du système d'exploitation - Le firewall SNS génère désormais un événement système lorsque le mécanisme de vérification d'intégrité des fichiers exécutables refuse de lancer un binaire.

Changements introduits en version 4.2.7

En savoir plus

- Authentification par certificat (SSL) avec TLS v1.3 - Le support du *Post-Handshake Authentication* sur le firewall nécessite que le navigateur Web utilisé autorise le *Post-Handshake Authentication* pour que la méthode d'authentification par certificat (SSL) avec TLS v1.3 soit fonctionnelle.

Changements introduits en version 4.2.5

En savoir plus

- Authentification SPNEGO - Le script spnego.bat, disponible dans l'espace personnel MyStormshield, prend désormais en charge l'algorithme cryptographique AES256-SHA1, remplaçant l'ancien algorithme cryptographique utilisé RC4-HMAC-NT.

Changements introduits en version 4.2.4

En savoir plus

- Durcissement du système d'exploitation - Seuls les scripts *shell* sont autorisés, mais ils doivent explicitement être appelés par l'interpréteur (par exemple : sh script.sh et non ./script.sh).
- Durcissement du système d'exploitation - Pour les scripts lancés par le biais du planificateur d'événements (*eventd*), l'interpréteur doit être ajouté pour chaque tâche décrite dans le fichier de configuration du planificateur d'événements.
- Durcissement du système d'exploitation - Les scripts doivent être exclusivement situés dans la partition root (/) pour pouvoir être exécutés.
- Mode furtif - En configuration d'usine un firewall SNS n'est désormais plus en mode furtif par défaut.
- Mode IPsec DR - De nouveaux avertissements sont affichés dans le widget **Messages** du tableau de bord lorsque le mode IPsec DR est activé.
- Mode IPsec DR - La correction d'une anomalie dans l'implémentation de l'algorithme ECDSA basé sur les courbes elliptiques Brainpool 256 rend impossible l'établissement de tunnels IPsec en mode DR, basés sur ECDSA et courbes elliptiques Brainpool 256, entre un firewall en version SNS 4.2.1 ou SNS 4.2.2 et un firewall en version SNS 4.2.4 (ou supérieure).

- Active Update - Pour les clients utilisant des sites miroirs internes, il convient de mettre à jour les paquets Active Update hébergés sur leurs propres serveurs afin d'utiliser ceux signés par la nouvelle autorité de certification.
- Agent Stormshield Management Center - Sur un firewall SNS administré via SMC en version 3.0, si la liaison avec le serveur SMC n'a pas pu s'établir dans un délai de 30 secondes après une restauration de configuration, alors la configuration précédente est restaurée.
- Logs - Le stockage sur disque de tous les types de traces (dont les connexions) a été réactivé par défaut sur les firewalls en configuration d'usine.

Changements introduits en version 4.2.2

En savoir plus

- VPN IPsec - Le firewall désactive l'ESN lorsque le correspondant est en IKEv1.

Changements introduits en version 4.2.1

En savoir plus

- VPN IPsec - Le support de l'ESN pour l'anti-rejeu ESP est activé automatiquement.
- VPN IPsec - 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 est refusée par le firewall.
  Veuillez consulter la note technique VPN IPsec - Mode Diffusion Restreinte pour la configuration du mode DR des versions SNS 4.2 et supérieures.
- 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.
- VPN IPsec - La version 4.2 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.
- NAT-T - 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.
- Logs - Un champ précisant le type de règle VPN (tunnel mobile ou tunnel site à site) a été ajouté aux logs VPN IPsec.

- SNMP - Un événement (*trap*) SNMP est désormais émis lorsqu'un correspondant VPN IPsec est injoignable.
- SNMP - Une nouvelle MIB (STORMSHIELD-OVPNTABLE-MIB) est disponible.
- SNMP - La MIB STORMSHIELD-VPNSA-MIB propose des statistiques IPsec complémentaires.
- Authentification - Portail captif - La configuration du portail captif n'accepte plus la sélection de certificats autres que des certificats serveur comportant l'*ExtendedKeyUsage ServerAuth*.
- Authentification - Agent SSO - Il est nécessaire d'utiliser l'Agent SSO v3.0 (ou supérieur) avec les firewalls SNS en version 4.2.
- VPN SSL - Il est nécessaire d'utiliser le client VPN SSL v2.9.1 minimum et il est recommandé d'utiliser la dernière version du client VPN SSL avec les firewalls SNS en version 4.2.
- Logs - 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*.
- VPN SSL - 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).
- Protocole TLS v1.3 - Le protocole TLS v1.3 est utilisé pour les services du firewall (portail captif, LDAPS, Syslog TLS, Autoupdate ...).
- Les suites cryptographiques utilisées par le firewall pour initier ses propres connexions TLS (LDAPS, SYSLOG TLS, SMTPS...) ont été mises à jour. Les suites utilisables sont désormais :
  - ECDHE-ECDSA-AES128-GCM-SHA256,
  - ECDHE-RSA-AES128-GCM-SHA256,
  - DHE-RSA-AES128-GCM-SHA256,
  - ECDHE-ECDSA-CHACHA20-POLY1305,
  - ECDHE-RSA-CHACHA20-POLY1305,
  - ECDHE-ECDSA-AES256-GCM-SHA384,
  - ECDHE-RSA-AES256-GCM-SHA384,
  - DHE-RSA-AES256-GCM-SHA384,
  - TLS_AES_128_GCM_SHA256,
  - TLS_CHACHA20_POLY1305_SHA256,
  - TLS_AES_256_GCM_SHA384.

  Cette mise à jour peut rendre le firewall incompatible avec des serveurs utilisant des suites moins robustes. Nous vous invitons donc à vérifier la compatibilité des services TLS en interaction avec le firewall. Dans le cas précis du service LDAPS Microsoft Azure, il est nécessaire de forcer le firewall à initier des connexions utilisant des suites cryptographiques moins robustes (ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384 ou DHE-RSA-AES256-SHA256) à l'aide la commande CLI / Serverd `CONFIG CRYPTO SSLParanoiac=0`. Un redémarrage du firewall est nécessaire pour la prise en compte de cette modification.

Changements introduits en version 4.1.6

En savoir plus

- Suite à la mise à jour des certificats de signature, il est obligatoire d'utiliser la procédure USB Recovery pour installer une version inférieure à la version 4.1.6 sur un firewall en version 4.1.6 ou supérieure.

Changements introduits en version 4.1.4

En savoir plus

- VPN SSL - Une nouvelle version du composant utilisé par le VPN SSL en mode portail est proposée pour les utilisateurs de ce service.

Changements introduits en version 4.1.3

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.
- VPN SSL - 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).
- Passerelle par défaut - Il est de nouveau possible de définir sur le firewall une passerelle par défaut située dans un réseau IP publique autre que le plan d'adressage public du firewall. Ce comportement est déjà présent en version 3.11.

Changements introduits en version 4.1.1

En savoir plus

- Annuaires LDAP - Les connexions sécurisées aux annuaires LDAP internes sont désormais basées sur le protocole standard TLS 1.2.
- Fonctionnalité de Cache HTTP - La fonction Cache HTTP au sein d'une règle de filtrage n'est plus disponible.
  Il est nécessaire de désactiver le proxy cache avant de mettre à jour votre configuration. Dans le cas contraire, le proxy ne sera plus fonctionnel.
- Configuration des annuaires - Le port utilisé par défaut pour accéder au serveur LDAP de secours est désormais identique au port utilisé par le serveur LDAP principal.
- Agent SNMP - L'utilisation de la valeur *snmpEngineBoots* a été modifiée afin de se conformer à la RFC 3414.
- Paramétrage du mode protégé - Un nouveau paramétrage (*stealth mode*) permet d'autoriser la réponse du firewall aux requêtes ICMP. Ce nouveau paramétrage est prioritaire à un appel de type `sysctl net.inet.ip.icmpreply`.

Changements introduits en version 4.0.3

En savoir plus

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

Changements introduits en version 4.0.2

En savoir plus

- 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.

Changements introduits en version 4.0.1

En savoir plus

- 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.
- 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.
- Préférences de l'interface Web d'administration - La mise à jour vers une version SNS 4.0.1 ou supérieure provoque une réinitialisation des préférences de l'interface Web d'administration (exemple : filtres personnalisés).
- 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).
- 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).
- 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).
- Changement d'adresses MAC sur les firewalls SN310 - Le passage en SNS v4 d'un firewall modèle SN310 induit un changement d'adresses MAC pour les interfaces réseau du firewall. Ce changement peut avoir un impact si les anciennes adresses MAC du firewall avaient été renseignées sur des équipements réseau tiers (serveur DHCP, routeur...).
- IPsec et HA - Les tunnels IPsec établis ne seront pas synchronisés entre les 2 membres du cluster lors de la mise à jour : ils seront renégociés afin de pouvoir faire transiter du trafic chiffré.
- Filtrage et adresses MAC - SNS permet maintenant de définir et d'utiliser dans les politiques de filtrage des objets réseau basés sur les adresses MAC. Lorsqu'une adresse MAC est précisée dans un objet utilisé au sein d'une règle de filtrage, tout trafic provenant de cet objet et correspondant à cette règle de filtrage ne sera pas évalué si l'adresse MAC présentée durant l'échange diffère de celle de l'objet.

Changements notables introduits entre la dernière version 3.7 LTSB et la dernière version 3.11 LTSB

VPN IPsec et CRL

Lorsque le paramètre *CRLRequired* est activé dans la configuration d'une politique VPN, il est désormais nécessaire de disposer de toutes les CRL de la chaîne de certification.

VPN SSL (OpenVPN)

Renforcement du niveau de sécurité

Le niveau de sécurité mis en œuvre lors de la négociation et de l'utilisation de tunnels VPN SSL (OpenVPN) a été accru.

Si vous utilisez le client VPN SSL Stormshield avec le **mode automatique désactivé** ou un autre client OpenVPN, la configuration des clients VPN SSL doit donc être modifiée en conséquence. Pour cela, téléchargez la configuration VPN SSL depuis le portail captif du firewall SNS hébergeant le service VPN SSL et importez la sur les clients. Avec le client VPN SSL Stormshield en mode automatique, le client récupérera automatiquement sa configuration.

Les nouvelles exigences à respecter sont les suivantes :

- L'utilisation d'algorithmes d'authentification et de chiffrement de force supérieure :
  - SHA256,
  - ECDHE-RSA-AES128-SHA256,
  - AES-256-CBC (sauf sur les firewalls modèles SN160(W), SN210(W), SN310 qui conservent l'algorithme AES-128-CBC).
- Une compression des données activable basée sur les algorithmes LZ4,
- La vérification stricte du certificat présenté par le serveur (nom du certificat, et certificat de type "serveur").

Si vous n'utilisez pas le client VPN SSL Stormshield, notez qu'il est impératif de travailler avec une version récente des clients OpenVPN (2.4.x) ou OpenVPN Connect (smartphones et tablettes).

VPN SSL et certificats

Dans les configurations VPN SSL utilisant des certificats qui ne disposent pas du champ *KeyUsage*, les services externes peuvent ne plus parvenir à communiquer avec le firewall.

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

Nouvelles fonctionnalités et améliorations de SNS 4.3.30 LTSB

TPM non initialisé

Un firewall dont le TPM n'est volontairement pas initialisé n'affiche plus de manière répétitive un message d'avertissement indiquant qu'il est nécessaire d'initialiser ce TPM.

VPN SSL

Référence support 84357

La compression LZ4 n'est plus activée dans la configuration par défaut du VPN SSL. Ceci n'impacte pas les configurations existantes.

Vulnérabilités résolues de SNS 4.3.30 LTSB

Authentification RADIUS - Portail captif et interface Web d'administration

Une vulnérabilité de sévérité moyenne a été corrigée dans le protocole RADIUS.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-030.

Commandes CLI / Serverd

Des vulnérabilités de sévérité faible ont été résolues dans le mécanisme des commandes CLI / Serverd.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2024-024.

Correctifs de SNS 4.3.30 LTSB

Système

Certificats et PKI - Serveur syslog

Des corrections ont été apportées au mécanisme de vérification des CRL afin de ne plus autoriser la connexion et l'envoi de logs vers un serveur syslog dont le certificat est révoqué.

Qualité de service (QoS)

Référence support 85590

Un problème pouvant entraîner un blocage du firewall lors de la suppression d'une file d'attente de QoS a été résolu.

Sauvegardes automatiques et TPM

Référence support 84907

Suite au durcissement du système d'exploitation, la réalisation d'une sauvegarde automatique sur un firewall équipé d'un TPM initialisé fonctionne de nouveau correctement sans déclencher d'alarme "*TPM operation not permitted*".

Sauvegardes automatiques - Serveur personnalisé

Sur un firewall utilisant les sauvegardes automatiques de configuration vers un serveur personnalisé authentifié à l'aide d'un certificat, un clic sur le bouton **Vérifier l'utilisation** du module **Objets** > **Certificats et PKI** en ayant sélectionné ce certificat indique désormais correctement que ce certificat est utilisé dans la configuration du firewall. De même, il n'est plus possible de supprimer ce certificat sans déclencher d'erreur.

Réputation IP - Périphériques de stockage

Références support 84495 - 84933 - 85038 - 85081 - 85213

Le mécanisme d'ouverture du fichier de métadonnées des réputations IP a été modifié afin de limiter le nombre d'accès au périphérique de stockage. Ces accès disque trop nombreux pouvaient, dans certains cas, entraîner un redémarrage inopiné du firewall.

SD-WAN

Les calculs de priorité ont été revus afin d'éviter des problèmes de bascules de passerelles trop fréquentes : il n'existe plus d'échelle d'état entre passerelles dégradées. Le mécanisme de sélection des passerelles suit désormais les règles suivantes :

- Passerelles actives prioritaires sur les passerelles dégradées,
- Passerelles principales prioritaires sur les passerelles de secours.

Interfaces Intel utilisant le module de noyau *igc*

Référence support 85486

La configuration d'un VLAN sur une interface utilisant le module de noyau *igc* et incluse dans un bridge avec l'option **Préserver le routage initial / Préserver les identifiants de VLAN** activée ne provoque plus à tort le rejet des paquets issus d'autres VLAN traversants.

Ceci concerne les modèles de firewalls et les firewalls équipés des modules réseau suivants :

- Firewalls : SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 et SN-M-Series-920.
- Modules : NA-EX-CARD-8x2_5G-C (8 x 2.5 Gb Ethernet Cuivre) et NC-1-8x2_5G-C (8 x 2.5 Gb Ethernet Cuivre).

Configuration

La mise à jour d'un firewall dont le disque présentait des défauts ne supprime plus le répertoire des fichiers de configuration. Ceci rendait le firewall injoignable.

Firewalls modèles SN160(W) / SN210(W) / SN310

Références support 84495 - 84933 - 85038 - 85081 - 85213

Des modifications ont été apportées au mécanisme de calcul des indicateurs Sécurité et Système afin de réduire le nombre d'accès disques. Ceci pouvait entraîner des redémarrages inopinés des firewalls modèles SN160(W) / SN210(W) / SN310.

Syslog - TLS 1.3

Référence support 85579

L'envoi de logs via Syslog en utilisant le protocole TLS 1.3 n'échoue plus lorsque le certificat utilisé pour l'authentification a été signé par une sous-CA.

Routage multicast statique dans des VLAN

Référence support 85562

Un problème d'interruption aléatoire de flux multicast routé de manière statique dans des VLAN a été corrigé.

Télémétrie

Un problème d'accès concurrentiel pouvant entraîner un arrêt inopiné du moteur de gestion de la télémétrie a été corrigé.

VPN IPsec - Authentification par certificat

Référence support 85607

Une mise à jour du moteur de gestion des tunnels IPsec avait entraîné une mauvaise interprétation par le firewall du SerialNumber comme étant le Surname, ce qui empêchait l'établissement des tunnels IPsec. Ce comportement a été corrigé.

VPN IPsec mode DR - Encapsulation UDP et NAT dynamique

Référence support 85629

Un tunnel configuré en mode DR, avec l'encapsulation UDP activée, et pour lequel l'un des deux correspondants a le port source de son trafic translaté (NAT dynamique) s'établit désormais correctement : le firewall distant détecte bien la nécessité d'encapsuler le trafic dans UDP.

Encapsulation GRE / GRETAP dans un tunnel IPsec

Référence support 85626

L'encapsulation de paquets GRE / GRETAP dans un tunnel IPsec est de nouveau fonctionnelle. Cette régression était apparue en version SNS 4.3.24.

VPN SSL

Référence support 85485

Pour les tunnels VPN SSL basés sur des certificats, la supervision du VPN SSL présente désormais uniquement les connexions établies.

Firewalls virtuels EVA déployés sur l'hyperviseur Linux KVM

Référence support 85722

L'extinction brutale d'une machine virtuelle en cours de configuration sur un hyperviseur KVM ne provoque plus de corruption de certains de ses fichiers de configuration.

Certificats et PKI - Serveur syslog

Des corrections ont été apportées au mécanisme de vérification des CRL afin de ne plus autoriser la connexion et l'envoi de logs vers un serveur syslog dont le certificat était révoqué.

Réseau

Routage dynamique BIRD

Référence support 85322

Des problèmes lors de l'ajout d'une route par défaut sur une interface protégée ou lors du passage d'une interface de publique à protégée avec une route par défaut ajoutée par BIRD ont été corrigés.

Ces problèmes ajoutaient par erreur le réseau *0.0.0.0/0* ou *0.0.0.0/32* dans la table des adresses protégées, ce qui déclenchait à tort l'alarme concernant une tentative d'*IP spoofing* et pouvait amener à perdre du trafic légitime.

Moteur de prévention d'intrusion

Gestion des connexions

Référence support 85370

Un problème dans la gestion des connexions par le moteur de prévention d'intrusion provoquant un redémarrage inopiné du firewall a été corrigé.

Compatibilité

Pour plus d'informations, reportez-vous au Guide de cycle de vie produits.

Problèmes connus

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

Limitations et précisions sur les cas d'utilisation

QoS

IMPORTANT
Cette fonctionnalité est en accès anticipé.
Veuillez impérativement consulter les Problèmes connus avant d'activer cette fonctionnalité ou de mettre à jour une configuration QoS existante vers une version SNS 4.3 ou supérieure.

La QoS implémentée en version SNS 4.3 présente les limitations suivantes :

- Bande passante maximale supportée : 1Gbps,
- Interfaces supportées :
  - Ethernet,
  - IPsec,
  - GRETAP,
  - IPsec virtuelles (VTI),
  - VLAN.
- Les files d'attente de type PRIQ et CBQ ne sont pas compatibles entre elles et ne doivent pas être utilisées sur le même *traffic shaper*,
- Les seuils définis sur les files d'attente doivent être tous en valeur absolue ou tous en pourcentage,
- La somme de la bande passante réservée ne doit pas excéder la bande passante du *traffic shaper*,
- Lorsque la QoS est activée, les flux non soumis à la QoS sont affectés par une baisse globale du débit sur le firewall SNS. Ceci est lié au fait que les flux utilisant des files d'attente de type bypass ne peuvent pas exploiter la totalité de la bande passante disponible à cause d'une gestion non optimale des architectures multi-CPU par le moteur de la QoS.

Gestion des connexions avec NAT lors d'un changement de passerelle au sein d'un objet routeur

Lors d'un changement de passerelle active au sein d'un objet routeur utilisé :

- Soit dans du filtrage basé sur le routage (PBR),
- Soit dans une route statique,
- Soit comme passerelle par défaut.

Si de la translation d'adresse source par connexion (NAT) est appliquée pour les flux empruntant cet objet routeur, les paquets des connexions déjà établies sont alors redirigés vers la passerelle nouvellement active mais en présentant l'adresse IP source correspondant à l'interface de sortie de la passerelle devenue inactive.

Ces connexions s'interrompent mais peuvent néanmoins être toujours considérées comme actives par le moteur de prévention d'intrusion ce qui empêche l'établissement de nouvelles connexions. C'est le cas pour le protocole SIP, par exemple.

Un contournement consiste à purger ces connexions en suivant la procédure décrite dans l'article Established UDP connections fail after routing failover de la Base de connaissances Stormshield (anglais uniquement).

Gestion des connexions lors d'un changement de passerelle au sein d'un objet routeur utilisé dans du filtrage basé sur le routage (PBR)

Lors d'un changement de passerelle active au sein d'un objet routeur utilisé dans du filtrage basé sur le routage, les connexions en cours sont envoyées vers la route par défaut plutôt que vers la passerelle nouvellement active de l'objet routeur.

Un contournement consiste à utiliser une route statique plutôt que du PBR pour ces flux.

Firewalls équipés d'un TPM

Référence support 83580

Après une mise à jour en version 4.3 LTSB, les secrets stockés dans le TPM nécessitent d'être scellés avec les nouvelles caractéristiques techniques du système à l'aide de la commande CLI / Serverd :

```
SYSTEM TPM PCRSEAL tpmpassword=<TPMpassword>
```

Notez que dans le cas d'un cluster, cette action doit être réalisée pour les deux membres du cluster depuis le firewall actif (en ajoutant le paramètre "serial=passive" pour sceller les secrets du firewall passif depuis le firewall actif).

Pour plus d'informations sur le module TPM, reportez-vous à la section Trusted Platform Module du manuel utilisateur SNS 4.3 LTSB.

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 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.

VPN IPsec

Optimisation de la répartition des opérations de chiffrement / déchiffrement

Dans une configuration avec un tunnel IPsec unique au sein duquel transitent plusieurs flux, l'activation du mécanisme d'optimisation des opérations de chiffrement / déchiffrement peut entraîner un déséquencement des paquets et peut provoquer des rejets sur le destinataire des paquets chiffrés suivant la taille de la fenêtre anti-rejeu configurée.

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.

Contraintes IPsec

L'utilisation de correspondants IKEv1 et IKEv2 au sein d'une même politique IPsec nécessite de respecter plusieurs contraintes :

- 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 de CRL peut être rendue obligatoire à l'aide du paramètre "CRLRequired=1" de la commande en ligne (CLI) **CONFIG IPSEC UPDATE**. Lorsque ce paramètre est activé, il est nécessaire de disposer de toutes les CRL de la chaîne de certification.

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.

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.

Correspondants de secours

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

Réseau

Modems 4G

La connectivité du firewall à un modem USB 4G nécessite l'utilisation d'un équipement de marque HUAWEI dans la liste suivante :

- E3372h-153,
- E8372h-153,
- E3372h-320.

D'autres modèles de clés pourraient fonctionner, mais ils n'ont pas été testés.

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.

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 Web d'administration.

Sur les modèles SN160(W), une configuration comportant plusieurs VLAN 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

Dans les configurations utilisant le protocole BGP avec de l'authentification, il est nécessaire d'utiliser la directive "source address <ip>;". 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

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.

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.

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 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.

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).

Messagerie instantanée

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

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).

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.

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`.

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.

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

Annuaires multiples

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).

Ressources documentaires

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

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

Installer cette version

Pour mettre à jour votre firewall en version SNS 4.3.30 LTSB, nous vous recommandons de suivre attentivement la procédure suivante.

Au préalable, il convient d'avoir pris en compte le Guide de cycle de vie produits et la section Points d'attention pour une mise à jour depuis une version 3.7 LTSB ou 3.11 LTSB.

Vérifier la compatibilité des logiciels clients Stormshield Network

Si des logiciels clients Stormshield (SSO Agents, SSL VPN Client et VPN Clients) sont utilisés dans votre architecture, vérifiez leur compatibilité avec la version du firewall SNS que vous souhaitez installer. En cas d'incompatibilité, ces logiciels ne fonctionneront plus correctement.

Pour plus d'informations, reportez-vous au Guide de cycle de vie produits et aux Notes de Version des logiciels clients concernés.

Réaliser une sauvegarde de configuration

Avant de procéder à la mise à jour de votre firewall, nous vous recommandons de sauvegarder sa configuration courante.

Si vous avez activé sur votre firewall la Sauvegarde automatique de configuration, assurez-vous de sa disponibilité sur le serveur de sauvegarde configuré. Si vous n'utilisez pas cette fonctionnalité, nous vous recommandons de l'activer.

Vous pouvez créer des fichiers de sauvegarde de configuration depuis l'interface Web d'administration du firewall dans **Configuration > Système > Maintenance > Sauvegarder**. Pour plus d'informations, reportez-vous à la section Onglet Sauvegarder du manuel utilisateur SNS.

Mettre à jour un cluster de firewalls en haute disponibilité (HA)

La procédure à suivre est spécifique et doit respecter les étapes décrites dans la section Mise à jour logicielle d'un cluster de la note technique *Haute disponibilité sur SNS*.

Mettre à jour le firewall

Chemins de mise à jour

Pour mettre à jour votre firewall, une ou plusieurs mises à jour intermédiaires peuvent être nécessaires selon sa version d'origine :

Version d'origine	Mises à jour intermédiaires requises
2.x	Version 3.7.16 LTSB - puis dernière version 3.7.x LTSB disponible
3.x	Dernière version 3.7.x LTSB ou 3.11.x LTSB disponible
4.0.x à 4.1.5	Version 4.1.6
4.1.6 ou supérieure	Aucune

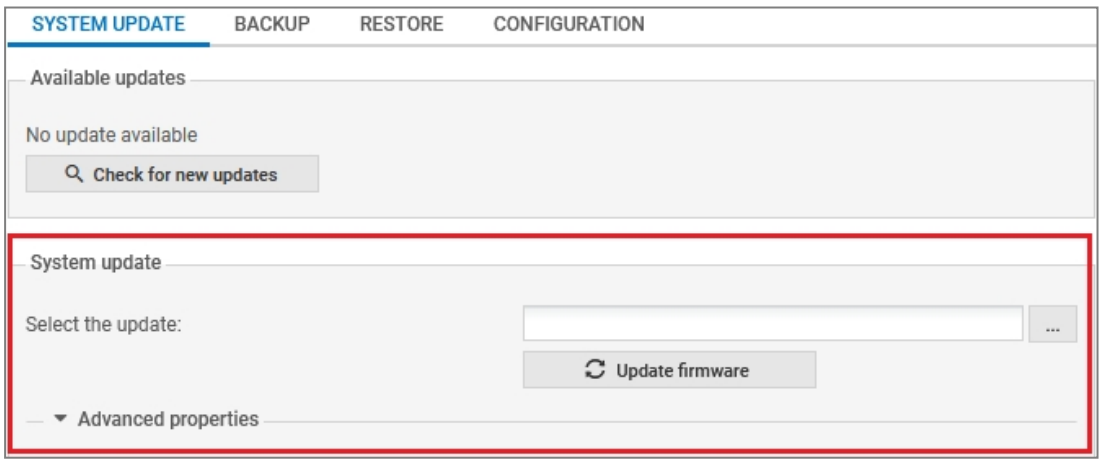
Télécharger la mise à jour

1. Depuis l'interface Web d'administration du firewall, rendez-vous dans **Configuration** > **Système** > **Maintenance**, onglet **Mise à jour du système**.
2. Si une mise à jour de la version LTSB est disponible, elle s'affiche dans la zone **Mises à jour disponibles**. Cliquez sur le lien pour télécharger la mise à jour (fichier *.maj*).
   Dans le cas où l'accès au serveur de mise à jour est impossible ou si vous souhaitez installer une autre version, téléchargez-la depuis votre espace personnel MyStormshield en vous reportant à la procédure Télécharger la dernière version disponible pour un produit.
   Pour plus d'informations sur le label LTSB, reportez-vous au guide Cycle de vie produits.
3. Vérifiez l'intégrité des binaires récupérés grâce à l'une des commandes suivantes :
   - Système d'exploitation Linux :
     ```
     sha256sum <filename>
     sha1sum <filename>
     ```
   - Système d'exploitation Windows :
     ```
     CertUtil -hashfile <filename> SHA256
     CertUtil -hashfile <filename> SHA1
     ```

   Comparez ensuite le résultat obtenu avec l'empreinte SHA1 indiquée sur l'interface Web d'administration du firewall ou avec l'empreinte SHA256 indiquée sur MyStormshield.

Installer la mise à jour

1. Depuis l'interface Web d'administration du firewall, dans **Configuration** > **Système** > **Maintenance**, onglet **Mise à jour du système**, sélectionnez le fichier de mise à jour (*.maj*) téléchargé précédemment.
2. Cliquez sur **Mettre à jour le firewall**.



3. La mise à jour est lancée : **ne débranchez pas le firewall durant cette opération**. Au terme de la mise à jour, vous êtes déconnecté et invité à vous ré-authentifier.
   Si un problème empêche la mise à jour, vous en êtes informé avant le lancement de l'opération.

Versions précédentes de SNS v4.3 LTSB

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SNS v4.3 LTSB.

4.3.29 LTSB			Correctifs
4.3.28 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.27 LTSB			Correctifs
4.3.26 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.25 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.24 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.23 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.22 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.21 LTSB	Nouvelles fonctionnalités		Correctifs
4.3.20 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.19 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.18 LTSB	Nouvelles fonctionnalités		Correctifs
4.3.17 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.16 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.15	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.12.2	Notes de Version 4.3.12.2		
4.3.12	Nouvelles fonctionnalités		Correctifs
4.3.11	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.10	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.9	Nouvelles fonctionnalités		Correctifs
4.3.8	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.7	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.6	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.5			Correctifs
4.3.4	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.2.14		Vulnérabilités résolues	Correctifs
4.2.13			Correctifs

4.2.12			Correctifs
4.2.11	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.2.10		Vulnérabilités résolues	Correctifs
4.2.9		Vulnérabilités résolues	Correctifs
4.2.8		Vulnérabilités résolues	Correctifs
4.2.7		Vulnérabilités résolues	Correctifs
4.2.6			Correctifs
4.2.5	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.2.4	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.2.2		Vulnérabilités résolues	Correctifs
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

Correctifs de SNS 4.3.29 LTSB

Système

Haute disponibilité - Mécanisme de sauvegarde du système sur la partition de secours
Dans une configuration en haute disponibilité (HA), un problème dans le mécanisme de sauvegarde du système sur la partition de secours (*dumproot*) aboutissait à un échec de la mise à jour du firewall passif. Cette régression était apparue en version SNS 4.3.28 LTSB.

Nouvelles fonctionnalités et améliorations de SNS 4.3.28 LTSB

Analyse Sandboxing

Référence support 85532

Seuls les fichiers classifiés dans l'une des catégories Archive, Document bureautique, Exécutable, PDF et Java sont désormais soumis à l'analyse Sandboxing afin de limiter la charge du service. Les fichiers classifiés dans Autre ou Inconnu ne sont plus envoyés pour analyse.

Vulnérabilités résolues de SNS 4.3.28 LTSB

Commandes CLI / Serverd

Des vulnérabilités ont été résolues dans le mécanisme des commandes CLI / Serverd.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2024-024.

Correctifs de SNS 4.3.28 LTSB

Système

Authentification RADIUS

Référence support 85727

Les authentifications RADIUS vers les serveurs FreeRADIUS sont de nouveau fonctionnelles. Cette régression était apparue en version 4.3.26 LTSB.

VPN IPsec

Références support 84983 - 85253 - 85452

En complément du correctif implémenté en version 4.3.20 LTSB concernant le VPN IPsec, des corrections ont été apportées au mécanisme de rechargement des règles de la politique VPN IPsec et le moteur de routage du firewall ne s'arrête plus de manière inopinée lorsque certaines configurations sont inchangées.

Objets dynamiques

Référence support 85397

Des optimisations permettent d'éviter un rechargement du proxy provoquant un ralentissement des connexions lorsqu'un objet dynamique (FQDN ou machine) est utilisé dans un mécanisme de filtrage ou de translation d'adresses du firewall SNS.

Mécanisme de sauvegarde du système sur la partition de secours

Référence support 85390

Des améliorations ont été apportées au mécanisme de sauvegarde du système sur la partition de secours (*dumproot*). Lorsqu'une sauvegarde est brutalement interrompue, la partition principale n'est plus corrompue et le firewall ne redémarre plus indéfiniment. Seule la partition de secours reste endommagée, et une nouvelle sauvegarde doit être réalisée pour rétablir l'état des deux partitions.

Translation d'adresses (NAT)

Référence support 85438

Les règles de la politique de NAT n'étaient pas appliquées dans les cas suivants :

- Lorsque deux paquets appartenant à la même connexion mais dans des directions opposées arrivaient sur des cœurs différents du CPU (par exemple un paquet de A vers B et l'autre de B vers A),
- Lorsqu'au même moment, une connexion était fermée et un nouveau paquet était reçu pour la même connexion.

Ces problèmes ont été corrigés.

Firewalls virtuels EVA déployés sur l'hyperviseur Linux KVM

Référence support 85635

Sur un firewall virtuel EVA déployé sur l'hyperviseur Linux KVM, l'état d'une interface débranchée dans la configuration de l'hyperviseur est désormais correctement pris en compte par le firewall. Ce problème faussait le résultat du calcul du facteur de qualité de la haute disponibilité (HA).

Moteur de prévention d'intrusion

Taille maximale des paquets COTP

Référence support 85353

La valeur maximale des paquets COTP est désormais de 65535 octets. Auparavant, la valeur maximale était de 4096 octets, et pouvait provoquer à tort l'alarme bloquante *Attaque possible des ressources* (ip:91).

Correctifs de SNS 4.3.27 LTSB

Système

VPN SSL et compression LZ4

Référence support 85686

Lorsque la compression LZ4 pour le VPN SSL est activée, la mise à jour en version 4.3.27 LTSB n'empêche plus le démarrage du moteur de gestion du VPN SSL. Cette régression était apparue en version 4.3.26 LTSB suite à la mise à jour du composant OpenVPN.

Nouvelles fonctionnalités et améliorations de SNS 4.3.26 LTSB

Firewalls modèles SN-L-Series-2200 et SN-L-Series-3200

La version SNS 4.3.26 LTSB introduit le support des nouveaux modèles de firewalls SN-L-Series-2200 et SN-L-Series-3200.

Messages d'alarmes matérielles

Les messages d'alarme relatifs à une défaillance matérielle affichent désormais le numéro de série du firewall.

Désactivation du bouton de remise en configuration d'usine (*defaultconfig*)

Référence support 84328

Il est possible de désactiver le bouton de remise en configuration d'usine du firewall. Ceci permet de ne pas réinitialiser la configuration du firewall par un appui malencontreux sur ce bouton.

Cette désactivation ne peut être réalisée qu'en se connectant en console sur le firewall et en appliquant la commande suivante :

```
setconf /usr/Firewall/ConfigFiles/system DefaultConfig EnableButton 0
&& nhup hardwared
```

Vulnérabilités résolues de SNS 4.3.26 LTSB

Réseau Wi-FI

Une vulnérabilité de sévérité forte a été résolue dans le mécanisme de gestion du réseau Wi-Fi.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-018.

OpenVPN

Une vulnérabilité de sévérité moyenne a été corrigée dans OpenVPN.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-005.

Firewalls modèle SN-S-Series-220 / 320

Une vulnérabilité de sévérité faible a été corrigée dans le mécanisme de gestion du port série sur les firewalls modèle SN-S-Series-220 / 320.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-017.

Correctifs de SNS 4.3.26 LTSB

Système

Haute disponibilité - Sauvegardes automatiques

Référence support 84782

Dans une configuration en haute disponibilité avec les sauvegardes automatiques de configuration dans le *Cloud* Stormshield activées : lorsque des changements de rôles réguliers avaient lieu au sein du cluster à une fréquence plus élevée que la fréquence programmée des sauvegardes automatiques (*7* jours par défaut), ces sauvegardes ne se déclenchaient jamais. Ce problème a été corrigé.

Haute disponibilité - Mise à jour du firewall passif pendant une copie de partition de secours

Référence support 85390

Des améliorations ont été apportées au mécanisme de gestion de mise à jour du firewall passif d'un cluster lorsqu'une sauvegarde de partition est en cours sur celui-ci. Ces améliorations sont destinées à ne pas interrompre brutalement la sauvegarde afin de ne pas risquer de corrompre les partitions du firewall passif.

Haute disponibilité - Mise à jour du firewall actif en ligne de commande

Référence support 84997

Dans une configuration en haute disponibilité, la tentative de mise à jour du firewall actif à l'aide la commande `SYSTEM UPDATE UPLOAD fwserial=active` n'échoue plus et ne présente plus l'erreur "Le firewall source et le firewall destination sont les mêmes".

Plus d'informations sur la commande **`SYSTEM UPDATE UPLOAD`**.

Exécution simultanée d'une mise à jour automatique et d'une sauvegarde système sur la partition de secours

Référence support 84744

L'exécution simultanée d'une mise à jour automatique (*autoupdate*) et d'une sauvegarde du système sur la partition de secours (*dumproot*) pouvait aboutir à un échec de cette dernière, notamment lorsque le firewall était administré via SMC.

Des optimisations ont été apportées afin d'éviter cette situation. Désormais :

- Lorsqu'un *dumproot* est en cours, le mécanisme d'*autoupdate* est mis en attente active et démarre une fois le *dumproot* terminé,
- Lorsqu'un mécanisme d'*autoupdate* est en cours, le *dumproot* ne se lance pas et génère un événement système.

Vérification des CRL

Référence support 85402

Le mécanisme de vérification des CRL effectue de nouveau correctement des requêtes DNS lorsque 3 serveurs DNS ou plus sont renseignés sur le firewall.

VPN IPsec

Un mécanisme de vérification et de limitation du nombre de demandes d'établissement de tunnels IPsec a été ajouté afin de ne pas saturer la file d'attente.

Référence support 85603

Lorsqu'une extrémité de trafic porte une adresse IP incluse dans le réseau des machines destination d'un tunnel, la tentative d'établissement de ce tunnel IPsec ne provoque plus un blocage inopiné du firewall. Cette régression était apparue en version SNS 4.3.24 LTSB.

VPN IPsec - Mode Diffusion Restreinte (DR)

Référence support 85507

Pour une configuration en mode DR, la présence de l'option **Ne pas initier le tunnel (*Responder-only*)** chez l'un des correspondants d'un tunnel site à site n'empêche plus ce tunnel de s'établir correctement.

Déploiement par SMC - Accès concurrentiels

Référence support 84003

Des problèmes d'accès concurrentiels ont été corrigés afin de ne plus bloquer inopinément une tentative de déploiement de configuration via SMC.

GRETAP

Référence support 85384

Dans une configuration utilisant le partage de charge CPU pour le chiffrement sur des firewalls modèles SN-M-Series-520 et SN-M-Series-720, un problème de rejet de paquets lors de la phase de renégociation des clés d'un tunnel GRETAP a été résolu.

Trusted Platform Module

Référence support 85378

Sur un firewall dont le TPM est initialisé, une tentative de sauvegarde de configuration du firewall ne provoque plus une erreur système entraînant la déconnexion de l'administrateur.

Interface Web d'administration

Changement du mot de passe du super-administrateur (compte *admin*)

Référence support 85581

Lors de la modification du mot de passe du compte *admin* via l'interface Web d'administration, les guillemets sont de nouveau refusés. Une régression autorisant ces caractères était apparue en version SNS 4.3.22 LTSB.

Nouvelles fonctionnalités et améliorations de SNS 4.3.25 LTSB

Firewalls modèles SN-XL-Series-5200 et SN-XL-Series-6200

La version SNS 4.3.25 introduit le support des nouveaux modèles de firewalls SN-XL-Series-5200 et SN-XL-Series-6200.

Agrégat de liens - Support du mode *broadcast*

La version SNS 4.3.25 introduit le support de l'émission et de la réception de paquets sur l'ensemble des liens inclus dans un agrégat (mode *broadcast*).

Notez que l'équipement qui est connecté aux interfaces agrégées en mode *broadcast* du firewall doit supporter ce type de communication :

- Soit en ayant une interface active et la seconde passive (principal / secours),
- Soit en ignorant les trames provenant d'un des 2 liens.

Cette configuration ne peut être réalisée qu'en modifiant directement dans le fichier de configuration réseau du firewall **ConfigFiles/network** le jeton *Laggmode* à la valeur *broadcast*, puis en validant cette modification à l'aide de la commande *ennetwork*.

Protocole DCERPC

Des UUID ont été ajoutées dans la liste des UUID connues du moteur d'analyse protocolaire DCERPC :

- '0b6edbfa-4a24-4fc6-8a23-942b1eca65d1' : 'IRPCAsyncNotify',
- '1c1c45ee-4395-11d2-b60b-00104b703efd' : 'IwbemFetchSmartEnum',
- '3dde7c30-165d-11d1-ab8f-00805f14db40' : 'BackupKey',
- '423ec01e-2e35-11d2-b604-00104b703efd' : 'IwbemWCOSmartEnum',
- 'ae33069b-a2a8-46ee-a235-ddfd339be281' : 'IRPCRemoteObject',
- 'd4781cd6-e5d3-44df-ad94-930efe48a887' : 'IwbemLoginClientID',
- 'f6beaff7-1e19-4fbb-9f8f-b89e2018337c' : 'Eventlog'.

Protocole TLS

Référence support 85368

Il est désormais possible de désactiver les analyses protocolaires TLS après l'établissement de la connexion, afin d'améliorer les performances en cas de forte charge.

Haute disponibilité - Nom de nœud système

Lorsqu'un nom de nœud système a été défini sur les membres d'un cluster, ce nom est précisé entre parenthèses dans les champs de sélection suivants :

- Module **Configuration** > onglet **Mise à jour du système** > **Mise à jour du système** : champ **Firewall à mettre à jour**,

- Module **Configuration** > onglet **Configuration** > **Maintenance** > champ **Redémarrer / Arrêter le firewall,**
- Module **Configuration** > onglet **Configuration** > **Haute Disponibilité** > **Forcer un firewall à rester actif**.

Vulnérabilités résolues de SNS 4.3.25 LTSB

Notifications par e-mail

Une vulnérabilité de sévérité faible a été résolue dans le module des notifications par e-mail.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-007.

OpenSSL

Une vulnérabilité de sévérité moyenne a été corrigée dans OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-011.

Correctifs de SNS 4.3.25 LTSB

Système

Proxy SSL

Référence support 73331

Le proxy SSL accepte désormais le caractère "_" dans les noms des FQDN pour l'extension SNI (Server Name Indication).

VPN SSL

Référence support 85485

Pour une connexion VPN SSL avec authentification par certificat, la présence de balises HTML ou de caractères de type guillemets (") dans le nom d'utilisateur est désormais correctement traitée.

Référence support 84391

L'option destinée à empêcher un utilisateur de monter plus d'un tunnel SSL (option activable via la commande CLI / Serverd `CONFIG OPENVPN UPDATE ForceOneTunnelPerUser=1`) ne fonctionnait pas lorsque le nom d'utilisateur présenté incluait son nom de domaine (exemple : john.doe@acme.com). Cette anomalie a été corrigée.

Plus d'informations sur la commande **`CONFIG OPENVPN UPDATE`**.

EVA sur Microsoft Azure

Référence support 85325

Le mécanisme de vérification d'intégrité des fichiers a été adapté afin de ne plus déclencher à tort des alertes pour les EVA déployés sur la plate-forme Microsoft Azure. Ces alertes, qui concernaient notamment le chargeur de démarrage de la machine ou des bibliothèques spécifiques à cette plate-forme, perturbaient le bon fonctionnement du pilotage et des sauvegarde des machines virtuelles par Microsoft Azure.

Accès disque

Références support 84495 - 84933 - 85038 - 85081 - 85213 - 84626 - 85197

Des améliorations ont été apportées afin de limiter le nombre d'accès disque. Ces accès disque trop nombreux pouvaient, dans certains cas, entraîner un redémarrage inopiné d'un firewall modèle SN160(W), SN210(W) et SN310.

Haute disponibilité - Associations SCTP

Référence support 82047

Une absence de synchronisation des associations SCTP lors du rechargement de la politique de filtrage sur le firewall actif pouvait aboutir à une incohérence au sein du cluster : une connexion SCTP supprimée sur le firewall actif lors du rechargement du filtrage était toujours considérée comme active sur le firewall passif. Ce problème a été corrigé.

Vérification des certificats

Référence support 85206

Le mécanisme de récupération et de vérification des certificats de serveurs TLS prend désormais en compte les CA de confiance ajoutées par l'administrateur : celles-ci sont en effet stockées dans un répertoire différent de celui utilisé pour le stockage des CA téléchargées.

Filtrage URL / SSL - Extended Web Control (EWC) - Catégorie Divers

Les URL reconnues par le fournisseur de classification d'URL de la solution EWC et qui n'appartiennent à aucune catégorie prédéfinie sont désormais classifiées dans la catégorie **Divers** et non plus dans la catégorie **Inconnu**.

Filtrage URL / SSL - Extended Web Control (EWC) - Messages d'avertissement

Des améliorations ont été apportées dans le cas où une catégorie d'URL inconnue est utilisée dans la configuration du firewall SNS après la migration d'une politique de sécurité vers la nouvelle base d'URL EWC :

- Les messages d'avertissement ne s'affichent plus dans le menu de gauche devant les noms de modules **Filtrage et NAT**, **Filtrage URL** et **Filtrage SSL** lorsque les catégories inconnues se trouvent dans une règle désactivée ou dans une politique inactive,
- Le retour de la commande CLI / Serverd *MONITOR MISC* indique désormais dans les avertissements les catégories inconnues et la politique concernée.

Agent SNMP

Référence support 83679

Une erreur a été corrigée dans la valeur retournée par l'OID *1.3.6.1.2.1.1.7*. Cette valeur est désormais 76, ce qui correspond à un équipement offrant des services sur les couches OSI 3, 4 et 7. Auparavant, la valeur retournée était 72.

GRETAP

Référence support 85417

Une anomalie de formatage des paquets GRETAP sortants (quelques octets excédentaires en début de paquet) a été corrigée. Cette anomalie, apparue en version 4.3.16 LTSB, rendait les captures réseau GRETAP plus difficiles à analyser mais n'impactait aucunement le bon fonctionnement des communications GRETAP.

Authentification - Attaque par force brute

Référence support 81350

Lors du déclenchement du mécanisme de protection contre les attaques par force brute, l'alarme générée ne contient plus une adresse de destination systématiquement égale à 0.0.0.0. Cette régression était apparue en version SNS 4.1.1.

Tableau de bord - Indicateurs de santé

Référence support 85392

L'indicateur de santé des certificats présent sur le module **Tableau de bord** ne remonte plus à tort d'alerte lorsqu'une CA possède une durée de vie supérieure à 68 ans. Ce problème persiste sur les firewalls modèles SN160(W), SN210(W) et SN310.

Moteur de prévention d'intrusion

Connexions TCP - Proxy

Références support 84867 - 85385

A la fin d'un échange de paquets TCP, si le serveur ou le client ignore la fermeture de connexion envoyée par le correspondant, le moteur de prévention d'intrusion du firewall ne continue plus d'envoyer à tort et en boucle des paquets de type ACK ou FIN / ACK.

Protocole SMTP

Référence support 84220

Une connexion SMTP initiée par un client qui envoyait une commande *STARTTLS* avant la commande *EHLO* n'est désormais plus bloquée à tort en générant l'alarme "Protocole SMTP invalide".

Protocole SMTP - Support UTF-8

Référence support 83791

Le moteur d'analyse protocolaire SMTP ne bloque plus à tort les caractères UTF-8 dans le trafic SMTP lorsque le serveur a précisé leur légitimité via l'option SMTPUTF8.

Gestion des vulnérabilités

Référence support 85526

La taille du cache contenant les vulnérabilités détectées sur les machines clientes du firewall a été augmentée afin d'éviter une consommation CPU excessive de la part du moteur de prévention d'intrusion lorsque ce cache était rempli. La taille de ce cache est ainsi passée de 128 à 2048 entrées possibles.

Interface Web d'administration

Filtrage - Règle d'authentification - Objets Web

Référence support 85447

Lorsqu'une règle d'authentification est définie dans la politique de filtrage, il n'est plus possible de créer ou modifier un objet Web directement depuis cette règle. Cette action provoquait une instabilité de l'interface Web d'administration.

Certificats et PKI

Référence support 85388

La vérification de l'utilisation d'une Autorité de Certification (CA) dont le nom contient une apostrophe est désormais fonctionnelle.

VPN IPsec

Référence support 85442

Suite à l'import d'une CA et de plusieurs identités signées par cette CA, seul le certificat de la première identité importée pouvait être utilisé pour la création d'un correspondant IPsec. La sélection d'un autre certificat importé échouait. Ce problème a été corrigé.

Objet machine avec résolution DNS automatique

Référence support 85515

Le caractère "/" n'est plus autorisé à la fin du nom d'un objet machine configuré en résolution DNS automatique.

Objets

Références support 84588 - 84719

Il n'est plus possible de forcer la suppression d'un objet utilisé dans la configuration du firewall, ceci afin de ne plus créer d'incohérences de configuration.

Nouvelles fonctionnalités et améliorations de SNS 4.3.24 LTSB

Classification d'URL *Extended Web Control* (EWC)

La classification d'URL *Extended Web Control* utilise désormais la base d'URL du fournisseur *Bitdefender*.

Pour mettre en place une politique de filtrage d'URL / filtrage SSL, il est recommandé de travailler en mode "liste noire", c'est-à-dire de positionner explicitement les catégories d'URL à interdire dans des règles de filtrage d'URL / filtrage SSL avec l'action *bloquer.* Ces règles sont à placer au-dessus de la règle autorisant toutes les autres catégories.

Dans le cadre de la mise à jour en version SNS 4.3.24 LTSB ou supérieure d'un firewall utilisant une politique de filtrage d'URL / filtrage SSL en mode "liste blanche" (règles de filtrage autorisant explicitement certaines catégories et placées au-dessus de la règle bloquant toutes les autres catégories), il est fortement recommandé d'ajouter une règle autorisant les catégories d'URL *misc (Divers), unknown (Inconnu), computersandsoftware (Sites de téléchargement de logiciels) et hosting (Hébergement de sites Web)* pour éviter un risque de dégradation de l'expérience utilisateur. Cette règle est à placer au-dessus de la règle bloquant toutes les autres catégories.

Pour plus d'informations sur la migration d'une politique de filtrage d'URL / filtrage SSL lors de la mise à jour du firewall en version SNS 4.3.24 LTSB ou supérieure, veuillez consulter la Note Technique **Migrer une politique de sécurité vers la nouvelle base d'URL EWC**.

Supervision

Un message d'information est affiché dans le module **Supervision** et par le biais de la commande CLI/ Serverd `MONITOR MISC` lorsque des paramètres personnalisés ont été mis en place sur le firewall (présence de fichiers de configuration personnalisés dans certains répertoires du firewall).

Plus d'informations sur la **commande CLI / Serverd `MONITOR MISC`**.

Synchronisation de la base de données des objets avec les serveurs DNS

Il est à présent possible d'indiquer l'adresse IP source des requêtes DNS envoyées pour la synchronisation automatique de la base de données des objets. Ainsi, le trafic de ces requêtes peut transiter dans un tunnel VPN. Ce nouveau paramètre est uniquement modifiable à l'aide des commandes CLI / Serverd :

```
CONFIG OBJECT SYNC UPDATE bindaddr=<host>
CONFIG OBJECT SYNC ACTIVATE
```

Pour remettre la configuration par défaut, utilisez les commandes :

```
CONFIG OBJECT SYNC UPDATE bindaddr=
CONFIG OBJECT SYNC ACTIVATE
```

Plus d'informations sur la commande CLI / Serverd **`CONFIG OBJECT SYNC UPDATE`**.

Vulnérabilités résolues de SNS 4.3.24 LTSB

OpenSSH

Une vulnérabilité de sévérité forte a été corrigée dans OpenSSH.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-035.

Firewalls SN-S-Series-220/320 et SN-M-Series-520

Une vulnérabilité de sévérité forte a été corrigée dans le microcode des processeurs des firewalls SN-S-Series-220/320 et SN-M-Series-520.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-004.

Correctifs de SNS 4.3.24 LTSB

Système

Proxies

Références support 85428 - 85495 - 85491

Des problèmes de blocages inopinés des proxies lors d'un rechargement de configuration ont été corrigés.

Captures réseau avec *tcpdump* sur interface *usbus*

Références support 85083- 85313

Le lancement d'une capture réseau avec l'utilitaire *tcpdump* sur une interface de type *usbus* ne provoque plus un redémarrage inopiné du firewall.

Firewalls virtuels EVA

Référence support 85273

Sur un firewall virtuel EVA, la limitation du nombre de CPU associée à l'activation de l'*hyperthreading* ne provoque plus un redémarrage inopiné du firewall.

QoS

Référence support 85019

Un problème dans la gestion de la suppression d'une file d'attente de type CBQ utilisée en tant que File d'attente d'acquittement (ACK) au sein d'une règle de filtrage pouvait aboutir à un redémarrage inopiné du firewall. Ce problème a été corrigé.

Passage en version SNS inférieure

Référence support 85247

Lors du passage d'un firewall dans une version SNS inférieure sans remise en configuration d'usine (*defaultconfig*), une tentative d'affichage de la liste des alarmes disponibles n'entraîne plus des redémarrages inopinés du moteur de prévention d'intrusion et du serveur de configuration par commande (serverd).

NAT

Référence support 84819

Un problème a été corrigé dans le mécanisme de gestion du NAT. Ce problème pouvait remplir à tort la table des ports translatés utilisés pour des flux nécessitant des connexions filles (par exemple : FTP, RTSP...), empêchant alors la création d'une nouvelle connexion fille et provoquant l'interruption du trafic concerné.

Filtrage et NAT

Références support 85357 - 85376

Dans le cas d'une règle de filtrage faisant appel à un ensemble d'objets réseau dont un est lié à une interface configurée en DHCP et désactivée, le redémarrage du firewall ne provoque plus l'activation à tort de la règle de filtrage "(1) *Block all*". Cette régression était apparue en version SNS 4.3.21.

Référence support 85239

Dans une situation telle que :

- Le firewall dispose d'un bridge regroupant plusieurs interfaces. Sur ce bridge :
  - Le trafic depuis une des interfaces du bridge vers une interface externe au bridge est autorisé par une règle de filtrage en mode *Firewall*,
  - Le trafic depuis une autre interface du bridge vers la même interface externe au bridge est bloqué par une autre règle de filtrage.
- Une connexion est établie entre une machine cliente et le serveur via la première règle,
- Une machine infectée ou une sonde d'intrusion située sur la même interface que le serveur envoie un paquet de type *reset* portant les mêmes références que la connexion établie (adresses source / destination et ports source / destination).

Le paquet provenant de la machine infectée ou de la sonde d'intrusion était correctement bloqué, mais l'interface source de la machine cliente était modifiée à tort et sa connexion établie avec le serveur était interrompue. Ce problème a été corrigé.

Connexion à l'interface Web d'administration avec le compte *admin*

Références support 85266 - 85309 - 85349 - 85437 - 85494

Dans certaines circonstances, une tentative de connexion à l'interface Web d'administration avec le compte *admin* pouvait échouer et provoquer un redémarrage inopiné du serveur de configuration par commande (serverd). Ce problème a été corrigé.

Haute disponibilité (HA)

Références support 77890 - 83274

Sur un firewall en haute disponibilité ayant fait l'objet de plusieurs bascules de rôle au sein du cluster, certains paquets empruntaient une route de retour erronée tout en présentant l'adresse IP de la bonne route de retour. Ce problème, qui provoquait l'interruption du flux concerné, a été corrigé.

Haute disponibilité - Synchronisation des listes de certificats révoqués (CRL)

Les CRL récupérées sur le firewall actif sont de nouveau synchronisées avec le firewall passif. Cette régression était apparue en version SNS 4.3.23 LTSB et générait une alarme lorsqu'une CRL du firewall passif était expirée.

Alertes e-mail

Références support 84511 - 82823

Lorsque l'envoi d'un e-mail par le firewall était réalisé au travers d'une connexion chiffrée avec un serveur SMTP à l'aide du protocole TLS, le rechargement de la configuration du service d'envoi d'e-mail provoquait à tort un passage en mode non chiffré pouvant aboutir à un échec de connexion du firewall avec le serveur SMTP. Ce problème a été corrigé.

Fuites mémoire

Référence support 85363

Des problèmes de fuite mémoire ont été corrigés dans les moteurs de configuration du firewall et de gestion de son agent SNMP.

VPN IPsec

Référence support 85439

Des paquets chiffrés dans un premier tunnel IPsec n'étaient plus autorisés à emprunter ensuite un second tunnel établi au travers d'interfaces IPsec virtuelles. Cette régression, apparue en version SNS v4, a été corrigée.

Supervision IPsec

Référence support 85399

La supervision des SA (Security Associations) n'échoue plus lorsque le correspondant contient une plage d'adresses IP.

Annuaire LDAP interne

Référence support 84495

La commande permettant de surveiller les modifications de configuration, utilisée notamment par le serveur SMC, ne déclenche plus de redémarrage du moteur de gestion de l'annuaire LDAP interne.

Interface en DHCP

Référence support 85305

La modification manuelle de la vitesse de média d'une interface configurée en DHCP ne lui fait plus perdre son adresse IP.

Routage dynamique BIRD - BGP et Authentification MD5

Référence support 85373

Dans une configuration de routage dynamique BIRD utilisant le protocole BGP avec de l'authentification MD5, l'absence d'adresse source pour cette configuration BGP provoque désormais l'affichage d'un message d'avertissement invitant l'administrateur à renseigner une adresse source dans la configuration de BIRD. Ceci permet d'éviter un dysfonctionnement de la session BGP concernée. Cette régression était apparue en version SNS 4.3.21 LTSB.

Port d'écoute de l'interface Web d'administration

Référence support 85450

Une tentative de modification du port d'écoute de l'interface Web d'administration (TCP/443 par défaut) ne provoque plus une erreur système dans le moteur de configuration du firewall et est désormais correctement prise en compte.

Gestion des agents SSO

Références support 85430 - 85443

Un problème de fuite mémoire a été corrigé dans le mécanisme de gestion des agents SSO.

Service de gestion des logs - Syslog TCP

Références support 85297 - 85396

Le service de gestion des logs du firewall ne s'arrête plus de fonctionner lorsque sa configuration est modifiée et que la connexion utilisée entre le serveur Syslog TCP et le firewall n'est pas fiable ou instable.

Moteur de prévention d'intrusion

Analyse IPS - Alarmes

Référence support 85210

Des paquets provoquant l'une des alarmes intervenant avant le contrôle du filtrage traversaient néanmoins le firewall malgré la présence d'une règle de filtrage destinée à bloquer le trafic réseau correspondant. Ce problème a été corrigé.

Consultez la liste des alarmes intervenant avant le contrôle du filtrage dans la Base de Connaissances Stormshield (authentification nécessaire).

Protocole LDAP

Référence support 84561

Les paquets d'authentification GSSAPI sont désormais correctement pris en charge par le moteur d'analyse protocolaire LDAP et ne génèrent plus à tort une alarme de type "Mauvais protocole LDAP" (erreur ldap_tcp:427).

Interface Web d'administration

Serveur DHCP et manipulations de la partition de logs

Référence support 84501

L'activation du Serveur DHCP du firewall n'empêche plus les opérations de maintenance sur la partition de logs via l'interface Web d'administration (démontage / montage, formatage...).

Nouvelles fonctionnalités et améliorations de SNS 4.3.23 LTSB

Mécanisme de récupération des certificats de serveurs

Référence support 84671

Le temps d'attente maximal pour la réponse à une requête de récupération de certificat de serveur a été diminué et est désormais configurable pour chacun des profils d'inspection du protocole SSL. Il peut prendre une valeur comprise entre 1 et 10 secondes et est positionné à 2 secondes par défaut.

Notez que cette configuration est exclusivement réalisable et activable à l'aide des commandes CLI / Serverd suivantes :

```
CONFIG PROTOCOL SSL PROFILE IPS CONFIG TLSServerCertTimeout=[1-10] index=
[0-9]
CONFIG PROTOCOL SSL ACTIVATE
```

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

VPN IPsec - Mode Diffusion Restreinte (DR)

Sur un firewall configuré en mode DR, il est désormais possible d'activer / désactiver l'encapsulation du trafic ESP dans le protocole UDP pour chaque correspondant. Pour préserver le fonctionnement d'un firewall en mode DR lors de sa mise à jour en version SNS 4.3.23 LTSB ou supérieure, cette encapsulation est activée par défaut.

Analyse Sandboxing

La classification des fichiers sans extension et sans type MIME spécifique a été modifiée. Désormais, ces fichiers ne sont plus analysés systématiquement afin d'optimiser l'analyse Sandboxing de l'ensemble des autres types de fichiers.

SD-WAN

Pour les configurations SD-WAN utilisant les seuils SLA et dans lesquelles les passerelles principales d'un objet routeur présentent des scores SLA très proches, le délai de changement de passerelle a été raccourci (passage de 25 à 9 secondes maximum).

Vulnérabilités résolues de SNS 4.3.23 LTSB

DHCP

Une vulnérabilité de sévérité moyenne a été résolue dans le service serveur DHCP du firewall.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-023.

VPN IPsec

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur de gestion des tunnels IPsec.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-024.

Service NSRPC

Une vulnérabilité de sévérité moyenne a été corrigée dans le service NSRPC.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-027.

Correctifs de SNS 4.3.23 LTSB

Système

VPN IPsec

Références support 84572 - 84708 - 85270 - 85272

La présence d'un caractère issu d'un encodage autre que l'ASCII dans le sujet du certificat d'une CA de confiance n'empêche plus l'établissement du tunnel IPsec basé sur cette CA.

Authentification SSH multi-utilisateur - Commande SCP

Référence support 84848

Les comptes déclarés administrateurs du firewall avec le droit "Console (SSH)" peuvent de nouveau exécuter la commande SCP en SSH. Le compte "admin" n'était pas concerné par ce problème.

VPN - Vérification de révocation des certificats des correspondants (CRL)

Référence support 82506

Le déploiement d'une topologie VPN depuis un serveur SMC dont le paramètre CRLRequired est activé n'écrase plus sur le firewall SNS la liste de révocation de certificats (CRL) de la CA.

Firewalls modèles SN-S-Series-320 et SN-M-Series-520

Le nombre maximal de connexions HTTP / FTP / SMTP / POP3 autorisées pour les firewalls modèles SN-S-Series-320 et SN-M-Series-520 était erroné et est corrigé lors de la mise à jour du firewall en version 4.3.23 ou supérieure.

Proxies

Références support 85041 - 85048 - 85260 - 85286 - 85314

Un blocage des proxies ne se produit plus lorsqu'une règle de déchiffrement SSL rencontre un certificat présentant les caractéristiques suivantes :

- Certificat avec un champ Sujet vide,
- Certificat signé par une autorité n'étant pas reconnue de confiance par le proxy (exemple : CA auto-signée).

Et que l'action d'analyse du protocole SSL **Certificats inconnus** est positionnée à **Déléguer à l'utilisateur**.

Référence support 85254

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

Supervision des tunnels IPsec

Référence support 85318

Dans la supervision des tunnels IPsec, une anomalie faisant apparaître les tunnels établis avec un correspondant en mode *Responder-only* comme des politiques d'exception (*bypass*) a été corrigée.

VPN SSL

Pour le serveur VPN SSL, il est désormais interdit de sélectionner :

- Un port d'écoute TCP inférieur à 1024,
- Un port d'écoute UDP inférieur à 1024 à l'exception du port UDP/443.

Commandes CLI / SSH

Référence support 85110

L'aide retournée par la commande `sfctl --help -F` précise désormais bien l'existence du jeton *assoc*.

Service client NTP

Le service client NTP ne s'arrête désormais plus de fonctionner sur un firewall disposant de plus de 1024 interfaces.

Routage

Référence support 85320

La mise à jour en version 4.3.23 LTSB d'un firewall pour lequel la route par défaut était définie avec un objet de type *loopback* (exemple : l'objet *localhost* ayant pour adresse IP 127.0.0.1) entraîne le remplacement automatique de cet objet par l'objet *blackhole*. Ceci permet d'assurer la compatibilité du routage préalablement configuré.

Moteur de prévention d'intrusion

Requête ICMP

Références support 84197 - 85387

Dans le cas d'un firewall avec :

- Un serveur derrière une interface protégée,
- Deux accès Internet distincts.

Suite à une requête depuis un réseau non protégé vers le serveur, si le serveur n'écoutait pas sur le port demandé, les paquets ICMP type 3 qu'il renvoyait empruntaient toujours la route par défaut. Les paquets passent à présent par la route de retour configurée.

Protocole NTP

Référence support 85077

Une vérification du champ NTP *reference_timestamp* déclenchait à tort une alarme 451 dans le plugin NTP. Cette vérification étant superflue, elle a été supprimée.

Haute disponibilité

Référence support 84766

Lors d'une bascule au sein du cluster, une anomalie dans le traitement de certaines connexions TCP / UDP déjà établies pouvait entraîner une instabilité du cluster. Cette anomalie a été corrigée.

Interface Web d'administration

VPN IPsec

Référence support 85312

La présence d'un espace dans le nom d'une configuration VPN IPsec nomade empêche le rechargement de la politique IPsec et la rend non fonctionnelle. L'interface Web d'administration du firewall et la commande CLI / Serverd `CONFIG IPSEC POLICY MOBILE UPDATE` interdisent désormais la saisie de ce caractère dans le nom d'une politique IPsec nomade.

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

Référence support 85334

La suppression du nom d'une règle de VPN IPsec est désormais interdite. Une règle avec un nom vide bloque en effet le rechargement de la politique IPSec complète.

Filtrage SMTP

Référence support 85347

L'interface Web d'administration n'interdit plus à tort de définir plusieurs règles référençant le même expéditeur pour des destinataires différents. Cette régression était apparue en version 4.0.

Haute disponibilité - Supervision

Référence support 85398

L'affichage des versions de firmware installées sur les partitions principales et de secours du membre passif du cluster est désormais correct.

Nouvelles fonctionnalités et améliorations de SNS 4.3.22 LTSB

Rapports embarqués

Références support 84495 - 84626 - 84933 - 85038 - 85081 - 85197

Le mécanisme de sauvegarde sur disque de la base de données des rapports embarqués est maintenant exécuté une fois par jour à 00h30 et pendant l'arrêt / redémarrage du produit, afin de limiter les écritures disques qui menaient à des instabilités sur les produits SN160(W), SN210(W) et SN310.

Protocole industriel EMERSON Delta-V

La version 4.3.22 LTSB introduit la détection automatique du protocole industriel EMERSON Delta-V.

Périphériques de stockage

Références support 84901 - 85018 - 85145

Le module **Messages** du **Tableau de bord** peut avertir l'administrateur qu'une mise à jour de firmware du périphérique de stockage système est disponible et doit être réalisée en contact avec le Support Stormshield.
Pour rappel, cette mise à jour permet de corriger d'éventuels problèmes de blocages du firewall.

Nouvelle carte 8 ports cuivre 2.5 Gb/s

La carte 8 ports cuivre 2.5 Gb/s (référence NA-EX-CARD-8x2.5G-C) est supportée depuis la version SNS 4.3.15 LTSB.
Cette carte est destinée aux firewalls modèles SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN2100 et SN3100.

PKI

L'alarme "La récupération de la CRL a échoué" précise désormais l'URL de la Liste de révocation de certificats (CRL) qui n'a pas pu être jointe.

SD-WAN

Référence support 83962

Dans le fichier de logs des statistiques de routage, la valeur de la dernière mesure de latence jusqu'ici enregistrée a été remplacée par :

- La latence moyenne,
- La latence minimale,
- La latence maximale.

Ces données sont calculées sur la fenêtre glissante d'enregistrement des mesures (15 minutes par défaut).

Plus d'informations sur :

- Les fichiers de logs du firewall,
- Les seuils SLA SD-WAN.

Connexions SSH à destination du firewall

Sur un firewall en configuration d'usine et en version SNS 4.3.22 LTSB (et versions 4.3 LTSB supérieures), les algorithmes de chiffrement ssh-rsa, hmac-sha2-256 et hmac-sha2-512 ne sont plus autorisés pour les connexions SSH à destination du firewall.

Analyse du protocole OSCAR

Un avertissement a été ajouté dans le panneau de configuration de l'analyse du protocole OSCAR afin d'indiquer que ce protocole est considéré comme obsolète à compter de la version SNS 4.3.22 LTSB.

Vulnérabilités résolues de SNS 4.3.22 LTSB

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

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

Protocole ICMP

Référence support 84949

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur d'analyse protocolaire ICMP.

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

Correctifs de SNS 4.3.22 LTSB

Système

Objets routeur

Référence support 84963

La mise à jour en version SNS 4.3.22 LTSB ou supérieure d'un firewall utilisant un objet routeur :

- Créé dans une version antérieure à SNS 4.3,
- Dont le nom comporte l'un des caractères "+" (signe *plus*) ou "^" (accent circonflexe).

Ne rend plus cet objet routeur inopérant dans la configuration du firewall.

Configuration - Objets réseau

Référence support 85274

Le renommage d'un objet appartenant à un groupe auto-généré (exemple de groupe auto-généré : *Network_internals*) est désormais correctement réalisé. Cette opération ne génère plus l'erreur système "L'objet est inclus dans 1 ou plusieurs groupes" et le nouveau nom de l'objet est correctement modifié dans l'ensemble des groupes et modules de configuration l'utilisant. Cette régression était apparue en version SNS 4.3.15 LTSB.

Tunnel GRETAP

La modification de l'adresse IP d'une extrémité de tunnel GRETAP actif est désormais correctement prise en compte.

SD-WAN

Des incohérences dans l'unité de mesure utilisée pour les calculs et pour l'affichage du taux d'indisponibilité des passerelles ont été corrigées.

Référence support 85253

Pour les configurations SD-WAN utilisant les seuils SLA et dans lesquelles les passerelles principales d'un objet routeur présentent des scores SLA très proches, des optimisations permettent désormais d'éviter des changements trop fréquents de priorité entre ces passerelles.

Agent SNMP

Références support 84861 - 85133 - 85213 - 85232

Des problèmes concernant la gestion des tables SNMP, qui pouvaient entraîner un arrêt inopiné de l'agent SNMP, ont été corrigés.

Supervision - Firewalls SN-S-Series et SN-M-Series

Référence support 85261

Un firewall SN-S-Series ou SN-M-Series sorti d'usine, et équipé d'un seul module d'alimentation sur les deux possibles, ne génère plus à tort une alarme majeure indiquant que le deuxième module est absent, débranché ou défectueux.

VPN IPsec

Référence support 84821

Dans une configuration telle que, sur un site A :

- Un premier tunnel IPsec vers un site B est défini dans la politique IPsec,
- Un deuxième tunnel vers un site C est basé sur une interface IPsec virtuelle (VTI),
- Une route statique précise le réseau vers le site C,
- Le réseau défini pour l'extrémité de trafic du site C recouvre le réseau défini pour l'extrémité de trafic du site B.

Alors le trafic réseau destiné au site C (tunnel basé sur VTI) n'est plus dirigé à tort dans le tunnel vers le site B (tunnel défini dans la politique IPsec).

Référence support 85284

Des modifications ont été apportées au mécanisme de chargement du moteur de gestion IPsec afin d'éviter de potentiels accès concurrentiels à son fichier de configuration. Ceci bloquait le chargement de la configuration IPsec au démarrage du firewall.

Référence support 84856

La présence, dans le fichier de configuration IPsec, d'une chaîne (exemple : CN de certificat, nom de certificat...) pouvant faire référence à un algorithme de chiffrement obsolète (exemple : des, blowfish ...) ne bloque plus une mise à jour de firmware du firewall.

Références support 85179 - 84968

Un tunnel VPN IPsec, dont le profil de chiffrement de phase 2 (IPsec) utilise le groupe Diffie-Hellman DH18 MODP (modp8192) comme Perfect Forward Secrecy (PFS), parvient de nouveau à renégocier les clés de ses Associations de Sécurité (SA). Cette régression, qui interrompait le tunnel IPsec, était apparue en version SNS 4.2.

Configuration - IPsec

Référence support 84881

La présence d'un séparateur de règles dans la politique VPN IPsec combinée à l'existence d'un objet de type FQDN dans la base objets ne provoque plus à tort une erreur lors de la requête de résolution de l'objet FQDN.

Authentification - Agent SSO

Référence support 85052

Dans une configuration ayant utilisé simultanément plusieurs Agents SSO mais dont le premier agent de la liste a été supprimé depuis, le moteur d'authentification Agent SSO démarre désormais correctement lors du rechargement de la politique d'authentification.

Machines virtuelles

Répartition de charge IPsec sur les CPU

Référence support 85225

Un problème de répartition de charge du chiffrement IPsec sur les CPU a été corrigé pour les firewalls virtuels EVA déployés sur des hyperviseurs utilisant la spécification SR-IOV (Single

Root I/O Virtualization - Virtualisation d'entrée / sortie à racine unique).

Pour rappel, la répartition de charge de chiffrement IPsec est configurable via la commande CLI / Serverd `CONFIG IPSEC CRYPTOLB UPDATE`.

Moteur de prévention d'intrusion

Protocole TCP

Références support 84807 - 84515

Dans certains cas de figure, la réception d'un paquet RST lors de la fermeture d'une connexion pouvait laisser cette connexion dans un état semi-fermé. Cette situation empêchait les tentatives de connexions vers la même adresse IP et sur le même port et provoquait l'alarme "Paquet TCP invalide par rapport à l'état" (alarme tcpudp:97), jusqu'à ce que le délai d'expiration de la connexion semi-fermée soit atteint. Ce problème a été corrigé.

Protocole OPC-UA

Référence support 85275

Le moteur d'analyse du protocole OPC-UA est désormais basé sur la spécification 1.0.5 de ce protocole. Ceci permet de ne plus bloquer à tort les messages de type *ReverseHello*, comportement qui interrompait la connexion OPC-UA en cours d'établissement.

Interface Web d'administration

Supervision - Logs

Référence support 85279

L'action de rafraîchir l'affichage des logs avec le filtre **Dernière Heure** actif ne provoque plus un décalage croissant de temps entre l'heure des derniers logs affichés et l'heure réelle du firewall.

Tableau de bord - Antivirus avancé

Référence support 85281

Dans une configuration telle que :

- L'antivirus est activé,
- Aucune règle de la politique de filtrage active ne fait appel à l'antivirus.

Le **Tableau de bord** du firewall n'indique plus à tort un état critique de cet antivirus.

Nouvelles fonctionnalités et améliorations de SNS 4.3.21 LTSB

Mise en conformité du mode IPsec DR

Le comportement du moteur de négociation des clés IKE a été modifié afin de le mettre en conformité avec les exigences du référentiel IPsec DR de l'ANSSI. Les modifications apportées ne sont pas perceptibles dans les usages nominaux des produits SNS.

IPsec DR - Génération des Certificate Request Payload

Le référentiel IPsec DR de l'ANSSI demande de remplacer l'algorithme utilisé dans la génération des Certificate Request Payload par le SHA2 (anciennement SHA1).

Les versions SNS 4.3 LTSB (à partir de la version 4.3.21 LTSB) respectent cette recommandation.

Si le mode IPsec DR est activé sur un firewall SNS en version 4.3.21 LTSB, la négociation de tunnels VPN est possible **uniquement** avec des correspondants respectant cette recommandation.

Ainsi, pour que la négociation de tunnels VPN en mode IPsec DR continue de fonctionner après la mise à jour d'un firewall SNS en version 4.3.21 LTSB, vous devrez vous assurer que l'ensemble des correspondants compatibles IPsec DR de votre architecture respectent cette recommandation :

- Pour des firewalls SNS, vous devrez tous les mettre à jour dans une version SNS respectant cette recommandation,
- Pour des firewalls d'un autre fournisseur, rapprochez-vous au préalable de ce dernier pour plus d'informations,
- Pour des clients VPN Exclusive Stormshield, vous devrez vous assurer que chaque client VPN est en version 7.4.018 ou supérieure et y configurer des paramètres supplémentaires. Pour plus d'informations, reportez-vous à la note technique VPN IPsec - Mode Diffusion Restreinte,
- Pour tout autre client VPN, rapprochez-vous au préalable de l'éditeur du logiciel concerné pour plus d'informations.

Routage statique

Le mot-clé *blackhole* peut désormais être sélectionné comme :

- Passerelle dans la définition d'une route statique,
- Passerelle par défaut du firewall.

Plus d'informations sur l'utilisation du mot-clé *blackhole*

Haute disponibilité et TPM

Référence support 85055

Dans une configuration en haute disponibilité telle que :

- Les membres du cluster sont équipés de TPM et ces TPM ont été initialisés,
- L'état de santé des TPM est inclus dans le calcul du facteur de qualité.

Alors, en cas de défaut du TPM du firewall passif (firewall initialement passif ou devenu passif suite à une bascule liée à la dégradation de son indice de qualité), un redémarrage de ce firewall est provoqué afin de retrouver l'état fonctionnel de son TPM.

SD-WAN

Des optimisations ont été apportées au mécanisme de gestion des priorités des passerelles afin d'éviter des rechargements inutiles de la route par défaut lorsque les passerelles présentent des scores de priorité proches.

Le dépassement d'un seuil SLA d'une passerelle génère systématiquement une entrée dans le fichier de logs système.

VPN IPsec

Il est désormais possible de définir un délai d'attente avant qu'une Association de Sécurité (*SA - Security Association*) nouvellement créée ne soit utilisée. Ceci permet d'éviter d'éventuels problèmes d'accès concurrentiels lorsqu'une SA est déjà utilisée pour les mêmes extrémités de trafic IPsec. Cette option *NewSADelay* est exclusivement paramétrable à l'aide de la commande CLI / Serverd `CONFIG.IPSEC.UPDATE NewSADelay=<value>`.

Plus d'informations sur la commande `CONFIG.IPSEC.UPDATE`.

Le mécanisme qui optimise la répartition des opérations de chiffrement et de déchiffrement du service IPsec sur le firewall SNS a été amélioré.

Correctifs de SNS 4.3.21 LTSB

Système

Routage dynamique Bird IPv6

Référence support 84849

L'activation du routage dynamique Bird IPv6 pouvait entraîner une consommation excessive de tampons mémoire lorsque les correspondants OSPFv6 ou BGPv6 étaient injoignables. Ce problème a été corrigé.

Routage statique

Références support 85213 - 85027 - 85218

Une anomalie dans le mécanisme de rechargement de la politique IPsec a été corrigée afin d'éviter un possible échec du chargement des routes statiques.

Périphériques de stockage

Références support 84901 - 85018 - 85145

Des problèmes pouvant aboutir à un blocage inopiné des firewalls SN2100 et SN3100 ont été corrigés par la mise à jour du firmware du périphérique de stockage système.

SD-WAN

Références support 84839 - 85165

Le firewall ne génère plus à tort une entrée de log de type "*Hôte distant joignable*" pour chaque route statique, lors du rechargement de sa configuration réseau, si aucun changement n'est intervenu.

Interfaces - Base Objets

Références support 85267 - 85294

Lorsqu'une interface ne possède pas d'adresse IP (exemple : cas d'une *dialup* pas encore connectée suite au redémarrage du firewall), les objets de type *Firewall_* et *Network_* liés à cette interface sont à nouveau générés automatiquement. Cette régression, apparue en version SNS 4.3.19 LTSB, pouvait empêcher le chargement de la politique de filtrage.

Authentification - SSO Agent

Référence support 85133

Dans une configuration utilisant l'authentification SSO agent basée sur un annuaire LDAP externe principal et un annuaire LDAP externe de secours, la bascule de l'annuaire principal vers l'annuaire de secours pouvait provoquer un arrêt inopiné du moteur d'authentification. Ce problème a été corrigé.

VPN IPsec

Références support 85095 - 85252

Un firewall pour lequel l'option **Ne pas initier le tunnel (Responder-Only)** est activée ne génère plus à tort de requêtes de ré-authentification de phase 1.

Réseau

Il est désormais possible de configurer à un intervalle régulier l'envoi de requêtes ARP vers une passerelle afin que ses entrées ARP sur le firewall SNS n'expirent jamais. Ceci permet d'éviter des pertes de paquets dans certains cas spécifiques.

Moteur de prévention d'intrusion

Protocole SSL

Bien que l'alarme "Paquet SSL invalide" (alarme ssl:118) soit configurée avec l'action *passer* (alarme non bloquante), un paquet levant cette alarme provoquait à tort l'interruption de l'analyse protocolaire SSL. Cette anomalie a été corrigée.

Protocole UDP

Références support 84913 - 85142 - 85157

Un problème a été résolu lors de l'analyse de certains paquets UDP afin de ne plus provoquer de blocage inopiné du firewall.

Protocole LDAP

Référence support 83800

L'alarme "Attaque possible des ressources" (alarme ip:91) n'est plus déclenchée à tort lors du téléchargement d'une CRL de taille supérieure à 128 Ko via une requête LDAP.

Haute disponibilité - Protocole SCTP

Quand les propriétés des machines source ou destination participant à une association SCTP ne sont pas disponibles lors de la synchronisation de cette association entre les membres du cluster, l'association SCTP concernée n'est plus supprimée mais une tentative de synchronisation de cette association est replanifiée.

Interface Web d'administration

Supervision

Référence support 84535

L'action de déplier une catégorie dans la partie **Rapports** de l'onglet **Supervision** ne provoque plus à tort un retour à l'écran précédent.

Certificats et PKI - TPM

Références support 84223 - 84462

Sur un firewall dont le TPM n'était pas initialisé, le statut de santé du TPM indiquait une alerte mineure, et chaque accès au module **Certificats et PKI** entraînait l'affichage d'un message invitant l'administrateur à initialiser le TPM. L'administrateur peut désormais cliquer sur un bouton présent dans ce message afin ne plus le lui rappeler et de faire disparaître l'alerte mineure.

Nouvelles fonctionnalités et améliorations de SNS 4.3.20 LTSB

Supervision SD-WAN

Un onglet "Graphe temps réel" permet d'afficher, pour une passerelle sélectionnée, les deux graphes suivants :

- La latence de la passerelle, mesurée lors des 10 dernières minutes,
- L'état de la passerelle sur la même période.

Vulnérabilités résolues de SNS 4.3.20 LTSB

Portail de connexion

Une vulnérabilité de sévérité faible a été corrigée sur le portail de connexion au firewall.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-020.

Correctifs de SNS 4.3.20 LTSB

Système

VPN IPsec

Références support 84983 - 85133 - 85253

Des optimisations ont été apportées au mécanisme de rechargement des règles de la politique VPN IPsec afin de limiter le risque d'arrêt inopiné du moteur de routage du firewall lorsque certaines configurations sont inchangées.

Références support 82578 - 84680

La gestion des ressources utilisées pour le VPN IPsec a été améliorée afin de réduire les entrées du type "job load of XXX exceeds limit of YY" dans les logs VPN IPsec.

Interfaces réseau

Référence support 85117

Les deux mécanismes alternatifs de renégociation des associations de sécurité IKE (mécanismes *reauthentication* et *rekeying*) ne sont plus lancés à tort l'un après l'autre. Cette régression, qui pouvait entraîner des pertes de paquets dans une configuration en mode Diffusion Restreinte (DR), était apparue en version SNS 4.2.0.

VPN SSL

Référence support 85229

Un utilisateur appartenant à un nombre important de groupes issus de l'annuaire LDAP parvient de nouveau à établir un tunnel VPN SSL. Cette régression était apparue en version SNS 4.3.18.

Référence support 84841

La modification de la configuration VPN SSL sur un firewall avec un tunnel VPN SSL déjà établi pouvait empêcher le moteur de gestion des tunnels de redémarrer. Ce problème, qui empêchait les tunnels VPN SSL de s'établir suite à la modification de la configuration, a été corrigé.

Filtrage et NAT

Référence support 84495

Le mécanisme de rechargement des règles de filtrage et NAT a été optimisé afin d'éviter des accès superflus à la configuration. Cela pouvant entraîner une corruption de la liste des politiques de filtrage et NAT.

Référence support 84734

La présence dans la politique de filtrage de deux règles bloquantes vers et depuis une adresse MAC, positionnées avant la règle autorisant le VPN SSL, n'entraîne plus à tort un blocage du trafic empruntant le tunnel VPN SSL.

Certificats et PKI

Références support 76892 - 85114

Lors de la création d'une demande de signature de certificat (CSR - Certificate Signing Request) à l'aide de la commande CLI / Serverd `PKI REQUEST CREATE`, si des Subject Alternative Name (SAN) ou des User Principal Name (UPN) sont précisés (adresses IP, FQDN...), ils sont désormais correctement pris en compte et apparaissent bien dans la CSR et le certificat signé.

Certificats et PKI - IPsec- Mode Diffusion Restreinte (DR)

Référence support 84942

Dans une configuration avec un chaîne de confiance du type : Autorité de Certification (certificat signé en RSA) -> Sous-Autorité de Certification (certificat signé en ECDSA ou ECSDSA sur courbe ECP 256 ou BP 256) servant d'ancre de confiance (*TrustAnchor*) -> Certificat (signé en ECDSA ou ECSDSA sur courbe ECP 256 ou BP 256), les tunnels IPsec en mode DR refusaient à tort de s'établir. Ce problème a été corrigé pour se conformer aux RFC de référence pour le mode Diffusion Restreinte.

Système - SNi20

Références support 84870 - 85037

Le mécanisme de surveillance de l'activité matérielle du firewall (*watchdog*) se déclenchait à tort avant le mécanisme de surveillance logicielle du système lorsque celui-ci était positionné sur sa valeur par défaut (120 secondes). Ce problème a été corrigé.

Supervision de la mémoire des firewalls SN310

Références support 85022 - 85155

Une anomalie dans la gestion des données de supervision de la mémoire pouvait provoquer à tort une alerte d'utilisation de la mémoire ainsi qu'un changement d'état de l'indicateur de santé correspondant dans le **Tableau de bord** des firewalls SN310. Cette anomalie a été corrigée.

Supervision des tunnels IPsec

Référence support 84776

Le rafraîchissement de l'écran de supervision des tunnels IPsec ne provoque plus l'erreur système *Command processing failed*.

Route par défaut - DHCP - IPv6

Référence support 85124

Dans une configuration telle que :

- La passerelle par défaut du firewall est apprise via DHCP,
- IPv6 est activé sur le firewall.

Toute modification (nom, protégée ou non ...) apportée à une interface ayant un adressage en DHCP n'entraîne plus la suppression de la route par défaut du firewall.

Traces - Syslog - IPFIX

Références support 84493 - 84876

Dans une configuration mettant en œuvre l'envoi de logs par UDP/syslog ou IPFIX sans préciser l'adresse IP du firewall devant être utilisée pour ces opérations, et en cas de forte activité d'envoi de logs, un problème d'accès concurrentiel pouvait entraîner une perte inopinée du réseau du firewall nécessitant un redémarrage de ce dernier. Ce problème a été corrigé.

Mise à jour du firewall via l'interface Web d'administration

Référence support 84962

Un problème lors de la mise à jour du firewall via l'interface Web administration pouvait entraîner un blocage inopiné de l'interface et empêcher la mise à jour du firewall. Ce problème a été corrigé.

Routage dynamique BIRD

Référence support 85249

Dans une configuration utilisant le protocole BGP avec authentification TCP-MD5, le rechargement de la configuration BGP n'empêche plus la renégociation des session BGP. Cette régression était apparue en version SNS 4.3.18.

Référence support 85221

Dans une configuration utilisant le protocole BGP avec authentification TCP-MD5, la directive "setkey no", devenue non fonctionnelle, est automatiquement remplacée par son équivalent "setkey yes" dans le fichier de configuration de bird/bird6 lors de la mise à jour du firewall en version SNS 4.3.20 ou supérieure. La présence de l'ancienne directive empêchait les sessions BGP authentifiées de s'établir après mise à jour du firewall. Cette régression était apparue en versions SNS 4.3.18.

Moteur de prévention d'intrusion

Haute disponibilité - Associations SCTP et connexions TCP/UDP

Référence support 84792

Dans une configuration en haute disponibilité, suite à une double bascule (Actif / Passif / Actif), les dates d'établissement des associations SCTP et des connexions TCP/UDP ne sont plus erronées.

Interface Web d'administration

Filtrage URL / Filtrage SSL / Filtrage SMTP

Référence support 85164

Dans les modules de Filtrage URL, Filtrage SSL ou Filtrage SMTP, la suppression de la première règle de filtrage ne provoque plus une désynchronisation des identifiants des autres règles de la politique.

Interfaces VLAN

Référence support 85226

La tentative de suppression d'un VLAN lorsque le routage dynamique Bird est activé fait de nouveau apparaître la fenêtre indiquant que cette opération n'est pas autorisée et que le routage dynamique doit être désactivé au préalable. Cette régression était apparue en version SNS 4.0.1.

Nouvelles fonctionnalités et améliorations de SNS 4.3.19 LTSB

Protocole HART-IP

La version SNS 4.3.19 introduit le support de l'analyse dynamique du protocole hart-ip. Les objets de type "port" *hart-ip_tcp* (TCP/5094), *hart-ip_udp* (UDP/5094) et *hart-ip* (ANY/5094) ont également été ajoutés à la base objets du firewall.

Vulnérabilités résolues de SNS 4.3.19 LTSB

DHCP

Une vulnérabilité de sévérité forte a été résolue dans le service client DHCP du firewall.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-019.

Correctifs de SNS 4.3.19 LTSB

Système

VPN IPsec

Référence support 84701

Dans une configuration IPsec telle que :

- L'un des réseaux distants recouvrait un réseau local directement connecté ou joignable par une route statique,
- Ce réseau distant n'était pas placé en première position dans la politique IPsec,
- L'option *BypassLocalTraffic* était activée (à l'aide de la commande CLI / Serverd `CONFIG IPSEC UPDATE slot=<1-10> BypassLocalTraffic=1`).

Les phases 2 IPsec correspondantes n'étaient pas enregistrées dans la Security Policy Database et le tunnel ne s'établissait pas. Ce problème a été corrigé.

VPN IPsec - Mode DR

Référence support 85051

Pour un tunnel en mode DR, la requête CREATE_CHILD_SA arrive désormais à son terme et la renégociation des clés de la Child SA en phase 1 n'échoue donc plus.

Proxy

Référence support 84971

Un problème d'accès concurrentiel dans la gestion des ports source de connexion et provoquant des blocages inopinés du proxy a été corrigé.

Authentification par certificat

Référence support 84981

Dans une configuration utilisant l'authentification par certificat et ayant un annuaire LDAP de secours configuré, l'absence de réponse du serveur LDAP principal provoque désormais bien la bascule sur le serveur LDAP de secours.

Moteur de prévention d'intrusion

Haute disponibilité - Protocole SCTP

Référence support 85118

Les associations SCTP sont désormais correctement synchronisées lorsque le flux SCTP correspondant emprunte une règle de filtrage dont la destination est une adresse IP.

Filtrage et NAT

Références support 85004 - 85061 -85072 - 85131 - 85132 - 85133 - 85142 - 85157 - 85173 - 84957 - 84667-84955

Le rechargement de la politique de filtrage suite à la modification d'une de ses règles impliquant de la translation d'adresses ne provoque plus de blocage intempestif du firewall.

Elastic Virtual Appliances (EVA)

Référence support 84714

Le mécanisme d'hyper-threading est de nouveau activé par défaut sur les machines virtuelles EVA qui disposent donc ainsi du nombre attendu de CPU virtuelles. Cette régression était apparue en version SNS 4.2.

Interface Web d'administration

Interfaces VLAN

Référence support 84822

La création d'un VLAN rattaché à une interface dont le nom excédait 10 caractères échouait. En effet, après que l'interface Web d'administration avait imposé de réduire la taille du nom généré pour ce VLAN, celui-ci apparaissait dans la liste des interfaces alors qu'il n'était pas réellement créé. Il n'était par exemple pas possible de lui affecter une adresse IP fixe à l'issue de ces opérations. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de SNS 4.3.18 LTSB

Disponibilité des firewalls SN-S-Series-220 et SN-S-Series-320

Les firewalls SN-S-Series-220 et SN-S-Series-320 sont disponibles. Reportez-vous au guide Cycle de vie produits pour plus d'informations sur la compatibilité de ces modèles avec les versions SNS.

Une présentation de ces firewalls est disponible sur le site de Stormshield, rubrique Nos firewalls Stormshield Network Security.

VPN IPsec - Méthodes Diffie-Hellman obsolètes

Certaines méthodes Diffie-Hellman étant obsolètes (et indiquées comme telles dans l'onglet **Profil de chiffrement** du module **VPN IPsec**), il est conseillé aux administrateurs de modifier leur configuration VPN IPsec si celle-ci les utilise.

Ces méthodes sont les suivantes :

- DH1 MODP Group (768-bits),
- DH2 MODP Group (1024-bits),
- DH5 MODP Group (1536-bits),
- DH25 NIST Elliptic Curve Group (192-bits),
- DH26 NIST Elliptic Curve Group (224-bits),
- DH27 Brainpool Elliptic Curve Group (224-bits).

Correctifs de SNS 4.3.18 LTSB

NOTE
Le correctif ajouté en version 4.3.17 LTSB concernant les fuites mémoire dans le moteur de gestion de la supervision a été supprimé. Il sera revu et réintégré dans une version ultérieure.

Système

VPN IPsec

Référence support 84823 - 84437

Le paramètre *half_open_timeout* peut désormais être personnalisé à l'aide de la commande CLI / Serverd CONFIG IPSEC UPDATE HalfOpenTimeout=<value> (30 secondes par défaut).

Ce paramètre permet de définir le délai à partir duquel une association IKE incomplète est supprimée (authentification du client IPsec en attente par exemple).

VPN IPsec - IKEv1 - Authentication par certificat et XAuth

Référence support 84775

Lors de l'établissement d'un tunnel IPsec IKEv1 avec authentification par certificat et XAuth, les groupes d'utilisateurs sont désormais correctement enregistrés dans les tables du moteur de prévention d'intrusion. L'utilisation de ces groupes au sein des règles de filtrage est donc de nouveau fonctionnelle. Cette régression était apparue en version SNS 4.2.

Certificats et PKI

Référence support 80053

Les attributs personnalisés définis lors de la création d'une sous-autorité de certification (Organisation, Unité d'organisation, État) ou d'une identité serveur (Organisation, Unité d'organisation, Lieu) ne sont plus remplacés à tort par ceux de l'autorité de certification parente lorsqu'ils diffèrent.

Firewalls modèles SN2100 et SN3100 - Mise à jour du firmware des disques SSD

Référence support 84295

Pour éviter d'éventuels dysfonctionnements des disques SSD sur les firewalls modèles SN2100 et SN3100, une mise à jour de firmware de ces disques SSD est automatiquement appliquée lors du passage en version SNS 4.3.18 LTSB ou supérieure. Pour rappel, cette mise à jour était déjà appliquée depuis la version SNS 4.3.15 aux modèles de firewalls dont la liste est disponible dans la section Correctifs de SNS 4.3.15.

Connexion SSH sur le firewall

Référence support 85106

L'ajout d'une bannière SSH provoquait une erreur dans la configuration du serveur SSH du firewall. Cette anomalie a été corrigée.

Filtrage et NAT

L'utilisation de l'opérateur mathématique de comparaison "différent de" (icône  ou "!=") au sein d'une règle de filtrage aboutissait à une génération de plages d'adresses IP erronées pour cette règle.

Commande *sfctl*

Référence support 84362

Le redimensionnement de la fenêtre d'affichage des résultats de la commande *sfctl -T* au moment du rafraîchissement des données ne provoque plus une faute de segmentation entraînant un arrêt inopiné de la commande *sfctl -T*.

Moteur de prévention d'intrusion

Haute disponibilité - Protocole SCTP

Référence support 85130

Un problème a été corrigé dans le mécanisme de synchronisation de masse (*bulk updates*) des associations SCTP établies. Ce problème survenait suite à un redémarrage du firewall passif.

Nouvelles fonctionnalités et améliorations de SNS 4.3.17 LTSB

Disponibilité des firewalls SN-M-Series-520

Les firewalls SN-M-Series-520 sont disponibles. Reportez-vous au guide Cycle de vie produits pour plus d'informations sur la compatibilité de ces modèles avec les versions SNS.

Une présentation de ces firewalls est disponible sur le site de Stormshield, rubrique Nos firewalls Stormshield Network Security.

Vulnérabilités résolues de SNS 4.3.17 LTSB

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-013.

PPTP et L2TP

Une vulnérabilité de sévérité moyenne a été corrigée dans une bibliothèque commune à PPP et L2TP.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-017.

Logs

Une vulnérabilité de sévérité faible a été corrigée dans le module de gestion des logs.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-006.

Correctifs de SNS 4.3.17 LTSB

Système

Agent SNMP

Références support 84911- 84990

Un problème de fuite mémoire a été résolu dans l'agent SNMP. Cette régression était apparue en version SNS 4.3.12.

Supervision

Références support 84989 - 85015 - 85043

Des fuites mémoires ont été corrigées dans le mécanisme de supervision des disques.

Haute disponibilité (HA)

Référence support 71538

Une anomalie dans le mécanisme de récupération des informations de HA peut empêcher l'affichage de ces informations dans l'interface Web d'administration du firewall (module **Supervision** > **Système** / **Haute disponibilité**). Des optimisations ont été apportées pour diminuer la fréquence d'apparition de cette anomalie.

Haute disponibilité (HA) - TPM

Références support 85030 - 85031

Le changement de mot de passe du TPM sur le membre actif du cluster est désormais immédiatement répercuté sur le membre passif afin d'éviter qu'une désynchronisation des mots de passe des TPM n'empêche le membre passif d'accéder aux clés des certificats protégés par son TPM.

Haute disponibilité (HA) - Logs

Référence support 84458

Dans le cas où un lien HA subissait beaucoup de pertes de paquets, le message "HA link is down" était indiqué à tort dans les logs bien que le lien soit toujours fonctionnel. Dans ce type de circonstances, le message indiqué dans les logs est désormais "HA link is faulty".

Haute disponibilité (HA) - VLAN

Référence support 84710

Une configuration telle que le seul lien HA actif passe par une interface VLAN entraînait un indisponibilité du cluster. Cette régression, apparue en version SNS 4.3.3, a été corrigée.

VPN IPsec

Référence support 84677

Lors de la création d'un tunnel IPsec, la sélection de l'objet *All* pour les réseaux distants n'inclut plus à tort d'adresses IPv6 lorsque l'option IPv6 n'a pas été activée sur le firewall.

VPN IPsec IKEv2

Référence support 84920

Un certificat utilisateur ne possédant ni l'extension *Extended Key Usage Client Auth*, ni l'extension *Extended Key Usage ServerAuth,* n'était pas évalué par les règles de droits d'accès utilisateurs (module **Configuration** > **Utilisateurs** > **Droits d'accès**) : le tunnel IPsec défini pour ce correspondant s'établissait mais ce correspondant était bloqué par la politique de filtrage car considéré comme non légitime.
Ce problème a été corrigé par l'ajout d'un jeton de configuration *UACForceCert* : en lui affectant la valeur 1, ce jeton impose l'évaluation de ce type de certificat par les règles d'accès utilisateur.
Ce jeton est manipulable à l'aide de la commande CLI / Serverd `CONFIG.IPSEC.UPDATE UACForceCert=<0|1>`

Plus d'informations sur la commande `CONFIG.IPSEC.UPDATE`.

VPN IPsec au travers d'une passerelle par défaut de type *dialup*

Référence support 82369

Lorsque la passerelle par défaut est basée sur un modem PPPoE (connexion de type *dialup*), les tunnels IPsec établis au travers de cette passerelle par défaut remontent désormais correctement après une perte temporaire puis un rétablissement de la connexion *dialup*.

Supervision

Des problèmes de fuites mémoire ont été corrigés dans le moteur de gestion de la supervision.

VPN SSL

Référence support 84564

Lorsqu'un port d'écoute inférieur à 1024 était sélectionné pour le serveur VPN SSL, et notamment le port UDP/443, le serveur VPN SSL ne redémarrait plus et aucun message spécifique dans l'interface Web d'administration n'indiquait que ce port ne pouvait être utilisé.
Il est de nouveau possible de sélectionner le port UDP/443 pour le serveur VPN SSL.

Cette régression était apparue en version SNS 4.3.0.

Résolution DNS des objets dynamiques

Référence support 84889

Dans une configuration avec plusieurs serveurs DNS définis, un problème dans le mécanisme de résolution DNS des objets machine à résolution automatique / dynamique et des objets FQDN a été résolu lorsqu'un des serveurs DNS restait fonctionnel tandis que les autres étaient injoignables.

Réseau

Routage dynamique Bird

Références support 83650

Des optimisations ont été apportées pour améliorer la vitesse de transmission des routes du moteur de routage dynamique Bird au moteur de prévention d'intrusion afin d'éviter des problèmes de latence dans la transmission des paquets réseau.

Bridge avec deux agrégats de liens LACP

Référence support 84552

Lorsqu'un bridge comporte deux agrégats de liens LACP, ces deux agrégats portent désormais la même adresse MAC que le bridge. Ceci permet d'éviter, dans le cadre d'un cluster, que le membre passif du cluster n'envoie des paquets ARP gratuits avec une adresse MAC erronée.

Matériel

SN1100, SN2100, SN3100, SNi20, SNi40 et SNxr1200 - Microcode CPU

Le microcode des processeurs Intel équipant les firewalls modèles SN1100, SN2100, SN3100, SNi20, SNi40 et SNxr1200 a été mis à jour.

Moteur de prévention d'intrusion

Nettoyage des tables du moteur de prévention d'intrusion

Des optimisations ont été réalisées afin de diminuer le temps nécessaire au nettoyage de certaines tables du moteur de prévention d'intrusion et éviter le risque de rejets de paquets durant cette opération. Ce problème était apparu en version SNS 4.3.7.

Interface Web d'administration

Conversion en minuscules

Référence support 84964

Une anomalie dans la fonction de conversion en minuscules de certains champs de configuration pouvait entraîner un blocage de l'interface Web d'administration sur le module considéré. Cette anomalie a été corrigée.

Suppression d'une méthode d'authentification

Référence support 84411

La suppression d'une méthode d'authentification de la liste des méthodes disponibles entraîne désormais l'effacement complet des paramètres de configuration de cette méthode.

Logs

Référence support 84895

Un administrateur dont l'identifiant comporte le caractère "@" peut désormais créer un objet ou ajouter un objet à un groupe depuis la vue Logs - Journaux.

Agent SNMP

Référence support 84952

Les valeurs des champs **Emplacement (sysLocation)** et **Contact (sysContact)** de la **Configuration des informations MIB-II** n'étaient pas encadrées de guillemets lorsqu'elles comportaient un espace. Cette anomalie a été corrigée.

Interfaces VLAN

Référence support 83873

La suite d'actions :

1. Créer et renommer un premier VLAN.
2. Ne pas appliquer la modification de configuration.
3. Créer et renommer un deuxième VLAN rattaché à la même interface physique.

Ne provoque plus à tort une erreur indiquant que les deux VLAN portent le même nom.

Antivirus - Tableau de bord

Suite à la migration en version 4.3.15 (ou supérieure) d'une configuration sans aucune règle de filtrage utilisant l'antivirus, l'icône de supervision de l'antivirus (module **Monitoring** > **Tableau de bord**) ne reste plus à tort affichée en orange avec le message "En cours de téléchargement".

Filtrage et NAT

Référence support 84980

Après avoir réalisé la recherche dans les logs d'une règle de filtrage (clic droit sur une règle et choix de l'action **Chercher dans les logs** dans le menu contextuel), la même opération sur une autre règle de filtrage ne garde plus à tort l'identifiant de la première règle comme critère de recherche.

Nouvelles fonctionnalités et améliorations de SNS 4.3.16 LTSB

Long-Term Support Branch (LTSB)

La version SNS 4.3 dispose du label LTSB permettant de la considérer comme stable à long terme avec une prise en charge assurée pendant 12 mois minimum.

Veuillez-vous reporter à la section **Compatibilité** pour connaître les produits compatibles. Pour plus d'informations sur le label LTSB, reportez-vous au document **Cycle de vie produits Network Security & Tools**.

Vulnérabilités résolues de SNS 4.3.16 LTSB

Service d'authentification interne du firewall (HTTPS)

Une vulnérabilité de sévérité forte a été corrigée dans le service d'authentification interne du firewall (HTTPS).

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-004.

Compression des pages HTTPS

Une vulnérabilité de sévérité forte a été corrigée dans le mécanisme de compression des pages HTTPS.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-003.

Service d'authentification interne du firewall (SSH)

Une vulnérabilité de sévérité forte a été corrigée dans le service d'authentification interne du firewall (SSH).

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-005.

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-027.

OpenSSL

Plusieurs vulnérabilités ont été corrigées dans OpenSSL.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2023-008 (sévérité faible),
- https://advisories.stormshield.eu/2023-009 (sévérité moyenne),
- https://advisories.stormshield.eu/2023-010 (sévérité faible).

Protocole SIP

Une vulnérabilité de sévérité forte a été corrigée dans le moteur d'analyse protocolaire SIP.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2023-007.

Correctifs de SNS 4.3.16 LTSB

Système

Haute disponibilité (HA)

Référence support 84843

Une synchronisation des connexions en HA (*bulk update*) pouvait se répéter indéfiniment lorsqu'elle excédait un délai de 5 secondes. Cette anomalie a été corrigée.

Haute disponibilité (HA) avec lien de secours

Référence support 84458

Dans une configuration HA disposant d'un lien principal et d'un lien de secours, lorsque le lien principal était en défaut puis redevenait opérationnel, le cluster continuait dans certains cas d'utiliser le lien de secours. Cette anomalie a été corrigée.

Supervision du système - Consommation CPU

Référence support 66123

Des anomalies dans le mécanisme de supervision de la consommation CPU ont été corrigées afin d'éviter de remonter des valeurs non réalistes.

Mise à jour du firewall au travers d'une passerelle par défaut de type *dialup*

Références support 80557 - 84626 - 84768

Lors de la tentative de mise à jour d'un firewall connecté à un modem PPPoE (*dialup*), un problème d'ordonnancement de l'arrêt des services au cours de la phase de redémarrage du firewall pouvait empêcher la mise à jour effective du firewall. Ce problème a été corrigé.

Interfaces GRE

Référence support 84625

Dans le cas de configurations utilisant des interfaces GRE en présence de paquets non-IP, des problèmes de fuites mémoire pouvaient entraîner un arrêt inopiné de certains services nécessitant un redémarrage du firewall. Ce problème a été corrigé.

Proxies

Références support 84517 - 84824 - 84826 - 84868 - 84877 - 84879

L'analyse d'un certificat auto-signé et sans champ *Subject* au sein d'un flux empruntant une règle de déchiffrement SSL ne provoque plus le blocage du proxy.

Référence support 84909

La présence de l'option **Cache HTTP** dans une règle de filtrage établie dans une version antérieure à SNS 4.3.0 n'empêche plus le démarrage du proxy après mise à jour du firewall.

Référence support 84991

Dans une configuration combinant l'analyse sandboxing et l'antivirus avancé, une anomalie dans la gestion des fichiers temporaires générés pour les analyses pouvait entraîner un remplissage anormal de la partition concernée ainsi qu'une forte dégradation des performances du proxy (accès Web ralenti). Cette anomalie a été corrigée.

VPN SSL portail

La signature de l'applet Java utilisée pour le VPN SSL portail arrivant à expiration, un message d'avertissement sera présenté aux utilisateurs après expiration de cette signature. La signature de cette applet a été renouvelée et l'applet est automatiquement mise à jour lors de passage du firewall en version SNS 4.3.16.

Moteur de prévention d'intrusion

QoS - Firewalls modèle SN160(W)

Référence support 84937

Une anomalie dans la gestion de la QoS sur les firewalls modèle SN160(W), qui entraînait des blocages du firewall, a été corrigée.

Protocole HTTP

Référence support 82824

Suite à une requête PUT ou POST de la part du client, et lorsque le serveur HTTP renvoie une réponse autre que le message "100 Continue", le moteur d'analyse protocolaire HTTP ne déclenche plus à tort l'alarme bloquante "Données additionnelles en fin de réponse" (alarme http:150).

Tunnels GRE

Référence support 75479

Lors d'un diagnostic avancé, les paquets capturés via *tcpdump* sur les interfaces GRE étaient malformés. Ce problème a été corrigé.

Interface Web d'administration

Interfaces - Haute disponibilité (HA)

Référence support 84863

Il n'est plus possible de modifier les interfaces dédiées à la HA depuis l'interface Web d'administration du firewall. Cette manipulation, autorisée par erreur, rendait la HA non fonctionnelle.

Haute disponibilité (HA) - Initialisation du TPM

Référence support 84530

Dans une configuration en HA, l'initialisation du TPM du firewall actif depuis l'interface Web d'administration déclenche désormais correctement l'initialisation du TPM du firewall passif.

Nouvelles fonctionnalités et améliorations de SNS 4.3.15

Antivirus avancé - Nouveau moteur antiviral

La solution d'antivirus avancé, accessible en option sur les firewalls SNS, repose désormais sur le moteur antiviral *Bitdefender*.

Le téléchargement de la nouvelle base antivirale peut prendre quelques minutes dans les cas suivants :

- Lors de la mise à jour en version SNS 4.3.15 d'un firewall utilisant l'antivirus avancé,
- Lors du passage de l'antivirus *ClamAV* à l'antivirus avancé sur un firewall en version SNS 4.3.15,
- Lors de la bascule d'un firewall passif à l'état actif après la mise à jour logicielle d'un cluster de firewalls utilisant l'antivirus avancé en version SNS 4.3.15.

Durant cet intervalle, l'analyse antivirale échouera, et selon la configuration du firewall SNS, du trafic pourrait être bloqué.

En cas de mise à jour vers une version précédente, le firewall ne disposera plus de moteur antiviral. La manipulation nécessaire pour retrouver l'ancien moteur antiviral existe mais elle n'est pas supportée. Vous pouvez la réaliser en suivant la procédure décrite dans l'article **After a downgrade from a version using Bitdefender, I cannot enable Kaspersky** (authentification nécessaire).

Qualité de service (QoS) - Filtrage

Il est désormais possible de sélectionner la file d'attente de QoS *bypass* dans les règles de filtrage de la politique de sécurité.

Qualité de service (QoS) - *Traffic shapers*

La configuration des Traffic shapers a été améliorée pour l'application de la QoS. Elle permet désormais de définir séparément les débits entrant et sortant de chaque interface. Cette amélioration permet de mettre en place de la réservation de bande passante dans les architectures de type LAN / WAN / DMZ et WAN multiples.

Support des firewalls SN-M-Series-720 et SN-M-Series-920

La version SNS 4.3.15 est la première version SNS 4.3 intégrant le support des firewalls SN-M-Series-720 et SN-M-Series-920.

Plus d'informations sur les firewalls SN-M-Series

Authentification - RADIUS

Référence support 84645

L'argument *BindMethodExternal* a été ajouté à la commande CLI / Serverd **CONFIG AUTH ADVANCED**. Il permet de préciser l'interface du firewall devant être utilisée pour émettre les requêtes RADIUS.
Cette configuration peut être réalisée à l'aide de la séquence de commandes CLI / Serverd :

```
CONFIG AUTH ADVANCED BindMethodExternal=<interface>
CONFIG AUTH ACTIVATE
```

Vulnérabilités résolues de SNS 4.3.15

VPN IPsec

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur de gestion des tunnels IPsec.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-025.

Correctifs de SNS 4.3.15

Système

NAT dynamique et DHCP pour les interfaces de sortie

Référence support 83297

La présence d'une règle de NAT dynamique associée à l'utilisation de DHCP pour définir les adresses des interfaces de sortie pouvait entraîner un blocage du firewall lors du rechargement des règles de filtrage dans le moteur de prévention d'intrusion. Ce problème a été corrigé.

Mise à jour du firmware des disques SSD

Référence support 84295

Pour éviter d'éventuels dysfonctionnements des disques SSD, une mise à jour de firmware de ces disques SSD est automatiquement appliquée lors de la mise à jour en version SNS 4.3.15 des modèles de firewalls suivants :

- SN510, SN710, SN910 équipés d'un SSD Innodisk 3TE7 d'une capacité de 256 Go,
- SN1100 équipés d'un SSD Innodisk 3TE7 d'une capacité de 512 Go,
- SN3000 avec l'option BIG DATA (équipés d'un SSD Innodisk 3TE7 d'une capacité de 1 To).

Mise à jour - Routage statique

Référence support 84716

La mise à jour en version SNS 4.3 d'une configuration comportant une route statique basée sur un routeur inexistant ne provoque plus un arrêt du rechargement des routes après le traitement de cette route incorrecte : les routes suivantes sont de nouveau correctement insérées dans les tables de routage.
Cette régression était apparue en version SNS 4.3.

QoS

La longueur maximale autorisée pour le nom d'une file d'attente de QoS utilisée dans le cas d'une détection par le moteur de prévention d'intrusion est désormais identique à celle des files d'attente de QoS classiques (31 caractères maximum).

Suppression d'une file d'attente de QoS

Des contrôles ont été ajoutés afin d'interdire la suppression d'une file d'attente de QoS lorsque celle-ci est utilisée dans la configuration du firewall.

Gestion du matériel - Firewalls modèles SN160(W), SN210(W) et SN310

Références support 82933 - 84307

Lors de l'extinction d'un firewall modèle SN160(W), SN210(W) ou SN310, une anomalie dans l'ordre d'arrêt des mécanismes de gestion du matériel empêchait le voyant lumineux *Online* de s'éteindre. Cette anomalie, qui pouvait laissait penser que le firewall n'était pas correctement arrêté, a été corrigée.

Interface Ethernet inactive avec adresse MAC forcée et VLAN rattaché

Référence support 80970

Lorsqu'on forçait l'adresse MAC d'une interface Ethernet parente d'un VLAN, ce VLAN n'héritait pas de l'adresse MAC forcée. Cette anomalie a été corrigée.

Interfaces réseau - Routage

Référence support 84706

Le rechargement de la configuration réseau ne provoque plus la disparition pendant plusieurs secondes des routes rattachées aux interfaces configurées en DHCP. Cette régression était apparue en version SNS 4.3.

Haute disponibilité - SNMPv3

Référence support 84500

Les paramètres SNMP (dont *AuthoritativeEngineID* en SNMPv3) sont désormais automatiquement synchronisés dès la création d'un cluster et à chaque bascule de rôle au sein de ce cluster. Ceci afin de ne plus provoquer d'erreurs sur certains outils de supervision SNMP.

Haute disponibilité - Configuration comprenant plusieurs centaines de VLAN

Référence support 84522

Sur des configurations en haute disponibilité comportant plusieurs centaines de VLAN, la requête d'affichage de l'état de la haute disponibilité n'entraîne plus une consommation anormalement élevée de CPU.

Traitement des paquets fragmentés

Référence support 83882

Pour les configurations soumises à un trafic important, un problème dans la gestion des tampons mémoire lors du traitement de paquets fragmentés a été corrigé. Ce problème entraînait des blocages inopinés du firewall.

Renommage de groupes d'objets imbriqués

Référence support 81223

Le renommage d'un groupe inclus dans un groupe, lui même inclus dans un autre groupe, échouait et provoquait l'erreur système "L'objet est inclus dans 1 ou plusieurs groupe(s)". Le renommage n'ayant pas été pris en compte dans la base objets, toute règle de filtrage utilisant le groupe renommé devenait alors invalide. Ce problème a été corrigé.

Rapport système (*sysinfo*)

Références support 84211 - 84210

Des contrôles concernant l'activation / désactivation du mode verbeux pour BIRD, BIRD6 et la politique globale de VPN ont été ajoutés au mécanisme de génération du rapport système (accessible depuis **Configuration** > **Maintenance** > onglet **Configuration**).

Connexion TLS à un serveur Syslog

Référence support 84831

Un délai d'inactivité a été ajouté pour la phase de négociation SSL lors d'une tentative de connexion du firewall à un serveur Syslog en TLS. Cette modification permet de ne plus provoquer de blocage intempestif du mécanisme de gestion des logs du firewall en cas de non-réponse du serveur Syslog lors de la phase de négociation SSL.

Antivirus avancé

L'activation de la nouvelle licence Antivirus avancé sur un firewall ayant toujours utilisé le moteur antiviral ClamAV est désormais fonctionnelle et n'affiche plus à tort le message système "Non disponible avec cette licence".

VPN IPsec

Référence support 84611

Un jeton de configuration *RemoteFetch* a été ajouté à la commande CLI / Serverd `CONFIG IPSEC UPDATE`. Ce jeton, lorsqu'il est positionné à la valeur "0", permet à la fois de :

- Désactiver la récupération des CRL distantes par le moteur de gestion des tunnels IPsec lors de l'établissement d'un tunnel,
- Désactiver le mécanisme OCSP dans le moteur de gestion des tunnels IPsec.

Ceci afin d'éviter une attente inutile de plusieurs secondes pour l'établissement de tunnels IPsec lorsque les points de distribution de CRL (CRLDP) sont absents ou non configurés.

Plus d'informations sur la commande CLI / Serverd `CONFIG IPSEC UPDATE`.

Référence support 82578 - 84680

Des problèmes d'accès concurrentiels provoquant une instabilité des tunnels IPsec ont été résolus. Cela rendait inopérante la supervision des tunnels et générait des entrées du type "job load of XXX exceeds limit of YY" dans les logs VPN IPsec.

Dans une configuration pour laquelle un tunnel IPsec passe par un modem PPPoE (*dialup*), le moteur de gestion des tunnels IPsec ne redémarrait plus après le rechargement de cette *dialup* ou un redémarrage du firewall.
Cette régression, apparue en version SNS 4.3, a été corrigée.

DHCP - Route par défaut

Référence support 84545

Lorsque le firewall obtient pour l'une de ses interfaces une adresse IP via un serveur DHCP utilisant l'option *routers x.x.x.x*, le firewall ne perd plus sa route par défaut si le bail DHCP concerné expire et n'est pas renouvelé (serveur DHCP injoignable par exemple).

Authentification

Référence support 84358

Une erreur de saisie de mot de passe lors d'une tentative de connexion au portail captif ou via SSL VPN Client ne génère plus à tort l'événement système "LDAP unreachable Bind error".

Authentification RADIUS - Configuration avec serveur RADIUS de secours

Référence support 84555

Dans certaines circonstances, une double requête d'authentification RADIUS pouvait être envoyée simultanément vers le serveur RADIUS principal et le serveur RADIUS de secours. Cette anomalie, qui entraînait immédiatement un rejet de la tentative d'authentification, a été corrigée.

Authentification par Certificat SSL

Référence support 80325

L'action d'ajouter la méthode d'authentification par Certificat SSL avec l'option **Activer la recherche dans plusieurs annuaires LDAP** et d'appliquer ce changement, puis de supprimer cette même méthode d'authentification ne bloque plus la connexion à l'interface Web d'administration du firewall ou au portail captif.

Collecteur IPFIX - Numéros des interfaces du firewall

Référence support 78226

Les numéros des interfaces du firewall récupérés par le collecteur IPFIX correspondent désormais aux numéros récupérés dans les tables SNMP.

Moteur de prévention d'intrusion

Nombre maximal de machines protégées

Référence support 84794

Un problème dans l'application de la modification effectuée en version SNS 4.3.10 au sujet du nombre maximal de machines protégées a été corrigé. Ainsi, lors de la mise à jour du firewall en version SNS 4.3.15, un second redémarrage est automatiquement déclenché si la configuration le nécessite.

Protocole SIP et translation d'adresses (NAT)

Référence support 68822

Dans une configuration utilisant du NAT pour les connexions SIP au sein d'une règle en mode Firewall, la réception par le firewall d'une deuxième requête de type *INVITE* pour une connexion déjà établie ne provoque plus un dysfonctionnement du NAT et n'entraîne plus un arrêt inopiné de la connexion SIP établie.

Protocole TLS 1.3

Référence support 84674

Afin de ne pas bloquer à tort certains flux TLS 1.3, le mécanisme d'analyse des certificats TLS 1.3 des serveurs SSL est désormais automatiquement désactivé lors de la migration d'un firewall depuis une version inférieure à SNS 4.3 vers une version supérieure ou égale à SNS 4.3.15. Il est également désactivé par défaut dans le profil entrant d'analyse SSL *SSL_00* pour les firewalls en configuration d'usine en version 4.3.15 ou supérieure.

Ce mécanisme d'analyse des certificats TLS 1.3 des serveurs SSL peut être réactivé, sous réserve d'en évaluer les éventuels impacts, dans **Configuration > Protection applicative > Protocoles > SSL**.

Rechargement de la configuration réseau

Références support 84522 - 84198

Des optimisations ont été apportées au mécanisme de rechargement de la configuration réseau (notamment lorsque aucun changement de configuration n'est intervenu) afin de diminuer le temps de rechargement, de réduire la consommation CPU associée et la durée de non-joignabilité du firewall lié à cette opération.

Interface Web d'administration

Filtrage avec QoS - Balises HTML dans un message d'avertissement

Le message d'avertissement affiché après l'activation ou la désactivation d'une règle de filtrage faisant référence à une file d'attente de QoS supprimée comportait à tort des balises HTML. Cette anomalie a été corrigée.

Version 4.3.14 non publiée

La version 4.3.14 n'est pas disponible publiquement.

Version 4.3.13 non publiée

La version 4.3.13 n'est pas disponible publiquement.

Version 4.3.12.2

Version certifiée ANSSI

La version 4.3.12.2 de SNS dispose de **Notes de Version dédiées**.

La version 4.3.12.2 fait l'objet d'une **certification délivrée par l'ANSSI** (Agence nationale de la sécurité des systèmes d'information), garantissant ainsi la confiance dans la fiabilité et la robustesse des produits de sécurité.

Nouvelles fonctionnalités et améliorations de SNS 4.3.12

SD-WAN - Calcul de la gigue

Dans le but d'obtenir des valeurs de gigue (variation de la latence) plus significatives, la formule de calcul de cet indicateur a été modifiée afin de suivre le modèle basé sur la différence entre deux délais de transmission consécutifs (RFC 4689 et 5481).

Correctifs de SNS 4.3.12

Système

Agent SNMP - MIB et *traps*

Référence support 78102

Afin de suivre au mieux les recommandations de la RFC2578, et pour résoudre un problème de compatibilité avec certains logiciels de supervision, toutes les tables SNMP pour lesquelles le premier indice était positionné à 0 ont été dupliquées en de nouvelles tables dont le premier indice est positionné à 1.

Les anciennes tables SNMP (indice commençant à 0) continuent d'être utilisées par défaut mais sont marquées comme obsolètes et sont amenées à disparaître dans une future version SNS.

Pour activer les nouvelles tables SNMP (indice commençant à 1) sur le firewall, il est nécessaire de :

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

Supervision des tunnels IPsec

La supervision de l'encapsulation UDP des tunnels IPsec a été corrigée et n'indique plus à tort cette encapsulation comme étant systématiquement désactivée.

Routage

Un mauvais ordonnancement des tâches au démarrage du firewall pouvait entraîner des problèmes de chargement de certains services comme IPsec ou Sandboxing. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de SNS 4.3.11

Interface de type *blackhole*

Une interface virtuelle de type *blackhole* peut désormais être sélectionnée lors de la création d'une route statique destinée à détruire un trafic identifié. Ce mécanisme peut notamment être utilisé dans une configuration comportant des tunnels IPsec : en cas d'indisponibilité d'un tunnel, les paquets qui lui étaient destinés sont ainsi détruits au lieu d'être redirigés vers la passerelle par défaut du firewall.

Vulnérabilités résolues de SNS 4.3.11

Éditeur de fichiers *vim*

Une vulnérabilité de sévérité moyenne a été corrigée par la suppression de l'éditeur de fichiers *vim*.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-006.

Correctifs de SNS 4.3.11

Système

Haute disponibilité - VPN IPsec

Références support 84273 - 84460

Un problème de synchronisation des SA (*Security Associations*) lors d'une bascule au sein d'un cluster, et qui pouvait entraîner un dysfonctionnement des tunnels VPN IPsec, a été résolu.

Haute disponibilité (HA) - Synchronisation

Référence support 84340

Le mécanisme de synchronisation de la HA ne provoque plus d'erreur lorsque le fichier relatif au mécanisme de retour arrière pour les déploiements de configuration via SMC est absent.

VPN IPsec

Le mécanisme de *keepalive* pour les tunnels VPN IPsec en IPv6 a été supprimé afin d'améliorer la stabilité des tunnels IPsec.

VPN IPsec au travers d'une passerelle par défaut de type *dialup*

Référence support 84631

Lorsque la passerelle par défaut est basée sur un modem PPPoE (connexion de type *dialup*), les tunnels IPsec établis au travers de cette passerelle par défaut remontent désormais correctement après une perte temporaire puis un rétablissement de la connexion *dialup*.

Mécanisme de gestion des logs

Références support 84605 - 84577

Des problèmes de fuites mémoire dans le mécanisme de gestion des logs, qui pouvaient entraîner un arrêt inopiné de ce mécanisme, ont été corrigés.

DMA remapping (DMAR) sur les firewalls SN1100

Des optimisations ont été apportées au mécanisme DMAR afin de combiner performances et possibilité d'obtenir des fichiers de vidage mémoire (*coredump*) pour analyse en cas de problème sur le firewall.

Routage statique - VPN IPsec

Référence support 84507

Le rechargement des règles de filtrage suite à la modification d'une route statique utilisée par un tunnel IPsec n'aboutit plus à un potentiel arrêt inopiné du moteur de routage statique du firewall.

Routage dynamique Bird

Référence support 84337

Les réseaux déclarés dans le routage dynamique Bird sont de nouveau correctement classifiés comme réseaux protégés dans le moteur de prévention d'intrusion et ne déclenchent plus à tort d'alarme concernant une tentative d'*IP spoofing*. Cette régression était apparue en version SNS 4.3.

Restauration de configuration du firewall SNS ou déploiement de configuration via SMC

Référence support 84630

Un problème empêchant la restauration d'une configuration sur le firewall SNS ou le déploiement d'une nouvelle configuration via le serveur SMC sur le firewall SNS a été corrigé. Ce problème générait l'erreur "*Impossible de déplacer les fichiers restaurés à leur emplacement définitif*" ("*Unable to move restored files to their final location*").

Réseau

Module 8 ports RJ45

Référence support 82270

Lorsque des blocages inopinés du module réseau 8 ports RJ45 sont détectés, un redémarrage automatique du firewall est déclenché pour permettre la reconnexion de ce module au réseau.

Interface Web d'administration

Balises HTML dans les messages de logs

Référence support 84494

Lorsque l'interface Web d'administration détecte des balises HTML dans les messages d'erreurs associés à certaines entrées de logs, elle n'affiche plus à tort le message d'erreur "XSS protection: HTML tag found in following commands".

Certificats et PKI

Référence support 84470

La tentative de génération de la CRL d'une sous-autorité de certification n'exige plus à tort la clé privée de l'autorité de certification racine et ne provoque plus d'erreur système.

Certificats et PKI - Point de Distribution de CRL (CRLDP)

Référence support 84618

L'ajout d'un CRDLP (module **Objets** > **Certificats et PKI** > onglet **Profils de certificats** de la CA sélectionnée) ne proposait pas la possibilité d'**Activer la récupération régulière des listes de révocation de certificats (CRL)**. Cette anomalie, qui pouvait empêcher l'établissement de tunnels IPsec basés sur des certificats, a été corrigée.

Nouvelles fonctionnalités et améliorations de SNS 4.3.10

Description des interfaces réseau

Référence support 81461

Les descriptions (optionnelles) ajoutées aux interfaces réseau depuis l'interface Web d'administration sont désormais stockées sous un format `clé=valeur` dans le fichier de configuration des interfaces réseau. Ceci permet de récupérer ces descriptions dans le cas d'une opération de restauration logicielle par clé USB.

VPN IPsec

Référence support 84280

Les données remontées par la commande `showSPD` ont été complétées afin de présenter les informations concernant les extrémités de tunnel VPN.

Vulnérabilités résolues de SNS 4.3.10

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-017.

Correctifs de SNS 4.3.10

Système

VPN IPsec - Objets routeur

Référence support 82369

Dans une configuration avec des tunnels VPN IPsec établis au travers d'un objet routeur, une bascule de passerelle au sein de cet objet routeur pouvait empêcher le rétablissement automatique de certains tunnels VPN IPsec. Cette régression, apparue en version SNS 4.2, a été corrigée.

Qualité de service (QoS)

Des problèmes de pertes de paquets au niveau de Traffic Shapers configurés avec une faible bande passante ont été corrigés.

Lorsqu'un flux empruntait une file d'attente par défaut de QoS, les paquets retour n'empruntaient pas la même file d'attente. Ce problème, qui provoquait des pertes de paquets, a été corrigé.

La longueur maximale des noms de files d'attente autorisée par la commande CLI / Serverd `CONFIG OBJECT QOS QID REMOVE` a été portée de 20 à 32 caractères. L'utilisation de cette commande ne provoque donc plus de problème en cas de manipulation d'une chaîne dont le nom comporte plus de 20 caractères.

Le traitement en parallèle des files de type d'attente par priorité (PRIQ) n'entraîne plus de blocage des autres files PRIQ lorsque l'une d'entre elles sature une interface.

La désactivation puis la réactivation de la QoS par le biais de la commande `sfctl` (`sfctl -q 0 && sfctl -q 1`) n'empêche plus le traitement des files d'attente de QoS.

Qualité de service (QoS) - Supervision

Référence support 84509

Dans une configuration possédant plus de 32 interfaces (interfaces physiques, VLAN, ...), la commande utilisée dans le cadre de la supervision de la QoS pouvait provoquer un blocage du firewall SNS. Cette régression, apparue en version SNS 4.3, a été corrigée.

Routage statique et tunnel VPN IPsec

Référence support 84367

Dans une configuration avec une route statique empruntant l'interface IPsec, le rechargement de la politique de filtrage entraînait une coupure des flux traversant le tunnel VPN IPsec. Cette régression, apparue en version SNS 4.3, a été corrigée.

Flux SSL à destination du firewall SNS

Référence support 84264

TLS 1.2 étant la version minimale de protocole à utiliser pour les flux SSL à destination du firewall SNS, les jetons de configuration correspondant aux versions SSL v3, TLS v1.0 et TLS v1.1 ont été supprimés du fichier de configuration du protocole SSL afin de les rendre inutilisables.

Proxy SSL

Référence support 84524

Dans une configuration comportant une règle de déchiffrement SSL et une règle de filtrage SSL avec l'action "Ne pas déchiffrer", le proxy du firewall SNS pouvait exclure à tort l'une des extensions TLS négociées entre le client et le proxy. Ce problème, qui empêchait l'établissement des connexions correspondant à cette extension TLS, a été corrigé.

Mot de passe du compte *admin* contenant des caractères UTF-8

Références support 81324 - 80974 - 82761- 84322 - 84503

Lorsque le mot de passe du compte *admin* contenait des caractères UTF-8 (exemple : le caractère €), ce mot de passe ne pouvait plus être modifié depuis l'interface Web d'administration. Cette régression, apparue en version SNS 4.1, a été corrigée.

Suppression d'un alias d'interface réseau

Référence support 79663

Des contrôles ont été ajoutés afin d'interdire la suppression d'un alias d'interface lorsque celui-ci est utilisé dans la configuration du firewall SNS.

Haute disponibilité (HA) - Synchronisation

Référence support 83721

Des anomalies pouvant entraîner une consommation mémoire excessive ont été corrigées dans le mécanisme de synchronisation de configuration de la HA.

Clé USB / Modem 4G - Huawei E3372h-320

Référence support 84253

Des correctifs ont été intégrés afin de supporter la version 10 de firmware des clés USB / Modem 4G Huawei E3372h-320.

Logs

Référence support 82287

La taille de la file de traitement des logs ainsi que la mémoire allouée à ce traitement ont été augmentées afin de minimiser les risques de perte de logs en cas de forte activité du firewall SNS.

Agent SNMP - Agrégat de liens

Référence support 82991

Lors de la perte d'un lien physique au sein d'un agrégat, les *traps* SNMP "*aggregate link down*" pouvaient être perdus et n'étaient donc pas réémis sur les autres liens physiques de l'agrégat. Ce problème a été corrigé.

Moteur de prévention d'intrusion

Protocole HTTP

Référence support 84292

Un problème dans l'analyse protocolaire HTTP, pouvant entraîner un blocage du firewall SNS, a été corrigé.

Nombre maximal de machines protégées

Référence support 84537

Un problème dans la gestion du nombre maximal de machines protégées, survenant lors de la mise à jour d'un firewall SNS en version 4.3.7 ou supérieure, a été corrigé.

Accès concurrentiel

Référence support 84486

Un problème d'accès concurrentiel entre deux mécanismes du moteur de prévention d'intrusion, qui pouvait entraîner un blocage du firewall SNS et une coupure de ses accès réseau, a été corrigé.

Nouvelles fonctionnalités et améliorations de SNS 4.3.9

Commande tpmctl

Référence support 83999

Des optimisations ont été apportées à la commande `tpmctl`.
Ces optimisations réduisent notamment de manière significative le temps nécessaire pour lister l'état des certificats protégés par le TPM lorsque ce nombre de certificats est important.

VPN IPsec IKEv2 - Correspondants nomades en mode CONFIG

Référence support 84482

Lorsqu'un tunnel IPsec IKEv2 établi avec un correspondant nomade en mode CONFIG est interrompu brutalement par le client distant, l'adresse IP qui lui a été attribuée reste verrouillée et indisponible. Le paramètre *unique* (pour *UniqueIDs*) a été ajouté aux commandes CLI / Serverd **`CONFIG IPSEC PEER NEW`** et **`CONFIG IPSEC PEER UPDATE`** afin de pouvoir modifier ce comportement.

Par exemple, pour permettre à un utilisateur de retrouver sa précédente adresse IP, utilisez le paramètre *unique=no*, puis rechargez la configuration de la politique VPN avec les commandes CLI / Serverd `CONFIG IPSEC ACTIVATE` et `CONFIG IPSEC RELOAD` (interrompt les tunnels en cours).

Correctifs de SNS 4.3.9

Système

Haute disponibilité, agrégat de liens et reprise des requêtes ARP

Des optimisations ont été apportées pour améliorer de manière sensible le délai de reprise des requêtes ARP suite à une bascule forcée au sein d'un cluster utilisant un agrégat de liens.

Enrôlement des utilisateurs

Référence support 84344

Un problème concernant l'enrôlement des utilisateurs via le portail captif sur un firewall ne possédant pas d'Autorité de Certification (CA) par défaut a été corrigé. Cette régression était apparue en version SNS 4.3.0.

Commande CLI / Serverd PKI CA CHECK

Référence support 84347

La commande CLI / Serverd `PKI CA CHECK` prend désormais en compte le fichier de configuration du mécanisme Autoupdate.

Moteur de prévention d'intrusion

Envoi de requêtes ARP pendant le rechargement de la configuration des interfaces dans le moteur de prévention d'intrusion

Référence support 84272

Un problème d'accès concurrentiel lorsque le moteur de prévention d'intrusion rechargeait la configuration des interfaces alors que des requêtes ARP étaient envoyées a été résolu. Ce problème provoquait un blocage du firewall.

Nouvelles fonctionnalités et améliorations de SNS 4.3.8

Tunnels IPsec site à site avec des extrémités de trafic en IPv6

L'option *keepalive* peut désormais être activée pour un tunnel IPsec présentant des extrémités de trafic en IPv6.

Routes statiques utilisant un objet routeur comme passerelle

Référence support 84239

Dans une configuration utilisant un objet routeur comme passerelle pour une route statique sans précision de l'interface réseau utilisée, cette interface est dynamiquement déterminée afin d'être ajoutée aux interfaces réseau protégées.

Vulnérabilités résolues de SNS 4.3.8

Analyse des protocoles SOFBUS et LACBUS

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur d'analyse des protocoles SOFBUS et LACBUS.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-015/.

Correctifs de SNS 4.3.8

Système

VPN SSL

Référence support 83972

L'établissement d'un tunnel VPN SSL n'échoue plus pendant la phase de négociation TLS lorsque l'authentification du client Stormshield VPN SSL nécessitait un laps de temps important (authentification à 2 facteurs par exemple).

Supervision des routeurs et des liens - Logs

Référence support 84125

Une anomalie dans le suivi de changement d'état des routeurs et des liens provoquait chaque minute l'écriture d'une trace du type "Hôte distant joignable" dans le fichier de logs systèmes. Cette anomalie a été corrigée.

Haute disponibilité

Référence support 84100

Dans une configuration en haute disponibilité, en cas de perte d'un lien sur le nœud actif du cluster, le temps de bascule du nœud actif en état passif a été réduit. Ceci permet au nœud passif d'opérer plus rapidement une bascule en état actif et de réduire ainsi la coupure du trafic réseau.

Actualisation des adresses IP des objets de type FQDN

Les adresses IP des objets de type FQDN s'actualisent désormais correctement dans la politique de filtrage. Cette régression était apparue en version SNS 4.3.6.

Visualisation des groupes de filtrage URL et SSL

L'aide de la commande CLI / SSH `tproxyd` ne précise plus à tort la possibilité de visualiser les informations des groupes de filtrage URL et SSL. Ces informations sont retournées par la commande `urlctl -g` depuis la version SNS 4.1.

La commande CLI / SSH `sysinfo` affiche de nouveau les informations des groupes de filtrage URL et SSL du fait qu'elle se réfère désormais à la commande `urlctl -g` pour les récupérer. Cette régression était apparue en version SNS 4.1.

Récupération régulière des CRL

Référence support 84431

Lors de l'utilisation de la commande `PKI CONFIG UPDATE`, il n'est plus possible de renseigner une valeur incorrecte (comme *Any*) à l'argument *checkcrlbindaddr*.

Prévention d'intrusion

Commande d'affichage des règles de QoS en console

Des anomalies ont été corrigées dans la commande système destinée à afficher les règles relatives à la QoS (commande `sfctl -s qos`) :

- Les règles de filtrage concernant le protocole ICMP et utilisant une file d'attente de QoS avec **Seuil de connexion** (onglet **Action** > **Qualité de service**) n'affichent plus à tort le seuil du protocole UDP,
- Les règles de filtrage utilisant une file d'attente de QoS sans **Seuil de connexion** sont désormais affichées.

Nouvelles fonctionnalités et améliorations de SNS 4.3.7

Support du firewall extra-durci SNxr1200

La version SNS 4.3.7 introduit le support du firewall extra-durci SNxr1200.

Plus d'informations sur le firewall SNxr1200.

Limitation de consommation mémoire par les services du firewall

Un mécanisme de limitation de l'utilisation de la mémoire par les services du firewall a été mis en place afin de se prémunir d'une utilisation anormalement élevée de la mémoire par l'un de ces services.

Adresses IP multicast présentées en source

Référence support 84041

Une nouvelle alarme "Paquet src IP multicast" (alarme ip:755) permettant de bloquer par défaut les paquets présentant une adresse IP multicast comme adresse source a été ajoutée dans le moteur de prévention d'intrusion.

Vulnérabilités résolues de SNS 4.3.7

OpenSSL

Une vulnérabilité de sévérité forte a été corrigée dans le moteur OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-008/.

Éditeur de fichiers *vim*

Des vulnérabilités de sévérité moyenne impactant l'éditeur de fichiers *vim* ont été corrigées.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2022-004.

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-005.

Moteur de prévention d'intrusion

Une vulnérabilité de sévérité forte a été corrigée dans le moteur de prévention d'intrusion.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-009.

Correctifs de SNS 4.3.7

Système

Haute disponibilité

Référence support 70868

Lorsque dans un cluster :

- Chaque membre possède un unique agrégat de liens raccordé à un même commutateur réseau,
- Cet agrégat est utilisé comme première interface dans un bridge,
- L'option **Activer l'agrégation de liens lorsque le firewall est passif** est activée,

Alors, en cas de bascule, l'adresse MAC du bridge n'est plus forcée au détriment de l'adresse MAC de l'agrégat sur le nouveau membre actif.

Agrégat de liens sans adresse IP

Référence support 83524

La migration vers une version SNS 4.x d'une configuration réalisée en version SNS 3.x et comportant un agrégat de liens sans adresse IP (agrégat inactif) tentait d'activer à tort cet agrégat et provoquait l'erreur système "Erreur AggX L'interface est activée mais ne possède pas d'adresse IP". Ce problème a été résolu et l'agrégat reste désactivé suite à la migration.

Import d'objets via un fichier CSV

Référence support 84224

Des contrôles additionnels ont été implémentés afin d'empêcher tout import d'objet via un fichier CSV qui comporterait des caractères non conformes au standard UTF-8 (y compris dans les commentaires des objets).

Filtrage et NAT

Référence support 82567

Dans certains cas, le seuil de connexion **TCP (c/s)** défini dans les paramètres de la qualité de service (QoS) d'une règle de filtrage n'était pas appliqué. Ce problème a été corrigé.

Prévention d'intrusion

Protocole ICMP

Les firewalls SNS en configuration d'usine étant en mode furtif (*stealth* mode) par défaut, la désactivation du mode furtif n'entraîne plus à tort la levée de l'alarme "Message ICMP invalide" (alarme icmp:67) en cas de destination injoignable.

Interface Web d'administration

Suppression d'un profil de chiffrement IPsec

Lors de la tentative de suppression d'un profil local de chiffrement IPsec, une fenêtre de confirmation de l'action est affichée : l'appui sur la touche [Échap] ne confirme plus à tort cette action de suppression mais l'annule comme souhaité.

Nouvelles fonctionnalités de SNS 4.3.6

VPN SSL

Des optimisations ont été réalisées dans le moteur VPN SSL (TCP et UDP) afin d'en améliorer les performances.

Vulnérabilités résolues de SNS 4.3.6

VPN SSL

Une vulnérabilité de sévérité forte a été corrigée dans le VPN SSL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-003.

Micro-codes CPU - Firewalls modèles SN1100, SN2100, SN3100 et SN6100.

Des vulnérabilités de sévérité moyenne ont été corrigées dans les micro-codes CPU des firewalls modèles SN1100, SN2100, SN3100 et SN6100.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2021-067.

Correctifs de SNS 4.3.6

Système

Classification d'URL - Extended Web Control (EWC)

Référence support 83619

Une anomalie dans la communication avec les serveurs EWC pouvait intervenir après plusieurs tentatives infructueuses de classification d'une URL. Cette anomalie a été corrigée.

Proxy HTTP

Référence support 83607

Des problèmes d'accès concurrentiels aux compteurs de connexions pouvant entraîner un arrêt inopiné du proxy ont été corrigés.

VPN IPsec - Sélection du protocole

Références support 83711 - 83777

La sélection du seul protocole autorisé à déclencher l'établissement d'un tunnel IPsec (choix de TCP, UDP, ICMP ou GRE dans la colonne **Protocole** de la grille des tunnels) empêchait la supervision des tunnels IPsec au sein de l'interface Web d'administration. Cette régression, apparue en version SNS 4.2, a été corrigée.

Réputation des machines

Référence support 77080

Il était possible de supprimer de la base objets une machine référencée dans la liste de supervision de réputation des machines. Ce comportement inapproprié, qui provoquait une erreur système empêchant le démarrage du proxy, a été corrigé.

Statistiques de trafic - Interfaces virtuelles IPsec

Référence support 82960

Les compteurs de paquets transitant au travers d'interfaces virtuelles IPsec n'étaient plus actualisés (requêtes SNMP ou commande système *netstat*). Cette anomalie apparue en version SNS 4.1 a été corrigée.

Statistiques de trafic sortant - VPN SSL

Référence support 79814

Les compteurs de paquets sortant de l'interface réseau liée au VPN SSL n'étaient plus actualisés. Cette anomalie apparue en version SNS 4.1 a été corrigée.

Connexion locale d'un administrateur bénéficiant du droit Console (SSH)

Référence support 84289

Toute tentative de connexion locale (en mode console ou écran / clavier) de la part d'un administrateur bénéficiant du droit **Console (SSH)** échouait et pouvait entraîner un blocage de la console après deux tentatives. Ce problème a été corrigé.

VPN IPsec avec authentification par certificat - Topologie déployée via SMC

Référence support 84231

Lorsqu'une topologie VPN IPsec avec authentification par certificat était déployée depuis un serveur SMC, toute tentative de modification depuis l'interface Web d'administration du firewall du correspondant défini dans cette topologie provoquait à tort l'affichage d'un message d'erreur système "Un token obligatoire pour cette méthode n'est pas spécifié". Ce problème a été corrigé.

QoS - Modification d'une file d'attente par défaut configurée initialement en pourcentage

Toute tentative de reconfiguration d'une file d'attente par défaut (ou d'une file d'attente de type ACK par défaut) initialement configurée en pourcentage de bande passante provoquait une erreur et entraînait l'affichage du message d'erreur "Référence nécessaire pour le pourcentage". Ce problème a été corrigé.

Machine en résolution dynamique d'adresse IP utilisée dans un sous groupe

Références support 84202 - 81951

Lorsqu'une machine était :

- Définie avec de la résolution dynamique d'adresse IP,
- Placée dans un sous groupe lui-même utilisé dans un module de configuration du firewall (règles de filtrage, droits d'accès à l'interface Web d'administration...).

Alors tout changement d'adresse IP de cette machine était ignoré dans le module de configuration concerné. Ce problème a été corrigé.

Prévention d'intrusion

Protocole SOFBUS - LACBUS

Une anomalie dans le moteur d'analyse du protocole SOFBUS entraînait à tort la levée de l'alarme "SOFBUS : protocole invalide" (modbus:741). Cette anomalie a été corrigée.

Applications *Android WhatsApp* et *Facebook*

Référence support 82865

Des paquets légitimes issus des application *Android WhatsApp* ou *Facebook* déclenchaient à tort l'alarme bloquante "Différence dans la version SSL" (alarme ssl:117). Cette régression, apparue en version SNS 4.2.1, a été corrigée.

Protocole SSL

L'activation de l'option **Autoriser le mécanisme 0-RTT** pouvait entraîner à tort l'alarme "SSL : réponse invalide au regard de l'état de la connexion" (alarme ssl:735). Ce problème a été corrigé.

Correctifs de SNS 4.3.5

Système

Mise à jour du firewall

Référence support 84361

Le firewall pouvait redémarrer en boucle après avoir été mis à jour en version SNS 4.3. Ce problème a été corrigé.

Nouvelles fonctionnalités de SNS 4.3.4

SD-WAN

La commande CLI / Serverd `MONITOR ROUTER name=`*`router_name`* permet d'afficher les valeurs des métriques SD-WAN des différentes passerelles composant le routeur précisé en argument.

Pour plus d'informations, reportez-vous au **Guide de référence des commandes CLI / Serverd (EN)**.

Vulnérabilités résolues de SNS 4.3.4

Micro-code CPU - Firewalls modèle SNi20 et SNxr1200

Des vulnérabilités de sévérité moyenne et forte ont été corrigées dans le micro-code CPU des firewalls modèle SNi20.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-040,
- https://advisories.stormshield.eu/2021-043.

Micro-code CPU - Firewalls modèle SN2100 et SN3100

Des vulnérabilités de sévérité basse et moyenne ont été corrigées dans le micro-code CPU des firewalls modèles SN2100 et SN3100.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-041,
- https://advisories.stormshield.eu/2021-042.

Correctifs de SNS 4.3.4

Système

Authentification - VPN SSL

Références support 78073 - 81741

Dans une configuration utilisant un annuaire LDAP externe principal et un annuaire LDAP externe de secours, la bascule de l'annuaire principal vers l'annuaire de secours pouvait provoquer un arrêt inopiné du moteur d'authentification, empêchant les utilisateurs d'accéder au VPN SSL. Ce problème a été corrigé.

Firewall administré depuis Stormshield Management Center (SMC)

Référence support 81863

Lors de la connexion d'un administrateur à un firewall depuis son serveur de rattachement SMC, l'identifiant de connexion de cet administrateur est désormais correctement affiché dans le bandeau supérieur droit de l'interface Web d'administration du firewall.

Valeurs des paramètres de supervision SD-WAN

Afin de correspondre à la majorité des besoins en termes de SD-WAN, les valeurs par défaut et les valeurs acceptables pour paramètres des tests de disponibilité ont été modifiées :

- Délai d'inactivité : 1s par défaut (contre 2s avant SNS 4.3.4),
- Fréquence : 5 secondes par défaut, avec un minimum de 2 secondes (contre 15s avant SNS 4.3.4),
- Nombre de tentatives : 5 (contre 3 avant SNS 4.3.4).

Logs - Statistiques SD-WAN

Référence support 83961

Les statistiques concernant les métriques SD-WAN (latence, gigue, taux de perte de paquets) sont désormais collectées toutes les 10 minutes (au lieu de 15) pour une meilleure synchronisation avec les statistiques de routage.

Logs VPN

Référence support 83792

Les logs VPN anonymisés (sans droit d'accès spécifique accordé) laissaient apparaître à tort des informations du certificat utilisateur distant (champ *remoteid*). Cette anomalie a été corrigée.

Configuration réseau

Référence support 84225

La présence dans le fichier de configuration du réseau de deux sections portant exactement le même nom provoquait un blocage du mécanisme de rechargement des paramètres réseau. Ce problème a été corrigé.

Routage statique

Une anomalie pouvant empêcher certaines routes d'être correctement prises en compte (cas de passerelles non routables) a été corrigée.

SD-WAN - Logs

Dans une configuration utilisant le SD-WAN, le log système inclut désormais la cause ayant provoqué une bascule de liens.

Supervision matérielle - Disques

Référence support 84083

Le mécanisme d'analyse des résultats des tests SMART a été adapté afin de ne pas provoquer d'alertes inappropriées sur certaines références de SSD.

Agent SNMP

Référence support 81710

Des anomalies pouvant entraîner des fuites mémoire au sein de l'agent SNMP ont été corrigées.

QoS

Après avoir affecté un *Traffic shaper* à une interface, il n'était plus possible de modifier la file d'attente par défaut, ou la file d'attente de type ACK par défaut, de cette interface. Cette anomalie a été corrigée.

La définition d'une file d'attente de QoS de type CBQ, en utilisant à la fois une valeur absolue et un pourcentage pour ses caractéristiques de bande passante min. et max. (ou min. inverse et max. inverse), pouvait entraîner une incohérence de la configuration de la QoS et un blocage des flux correspondants. Ce type de configuration est désormais explicitement refusé.

QoS configurée dans une alarme protocolaire

Référence support 84237

Le renommage d'une file d'attente de QoS utilisée au sein d'une alarme protocolaire provoquait la disparition de cette file d'attente de la configuration de l'alarme et entraînait une erreur système. Ce problème a été corrigé.

Interface Web d'administration

Haute disponibilité

Références support 83724

En cas d'erreur lors de la tentative de rattachement d'un firewall à un cluster, l'interface Web d'administration ne reste plus bloquée sur le message "Configuration de la haute disponibilité en cours".

VPN IPsec - Profils de chiffrement

Références support 84245

Lors de la sélection de l'algorithme AES-GCM_16 en phase 1 (IKE), le champ permettant de préciser un algorithme d'authentification est désormais grisé.

En effet, l'algorithme AES-GCM-16 ne supporte que la méthode d'authentification prfsha256 et celle-ci lui est automatiquement affectée.

Activation du mode Diffusion Restreinte (DR)

Référence support 82914

Lors de l'activation du mode DR sur une configuration IPSec ne respectant pas tous les prérequis nécessaires à ce mode, le message d'avertissement indiquant que la configuration IPsec a été désactivée est désormais accompagné du clignotement du symbole indiquant qu'un redémarrage manuel du firewall est nécessaire pour prendre en compte la modification (partie supérieure droite de l'écran).

Nouvelles fonctionnalités de SNS 4.3.3

SD-WAN et QoS

IMPORTANT

Ces fonctionnalités sont en accès anticipé.

Veuillez impérativement consulter les Problèmes connus et les Limitations et précisions sur les cas d'utilisation avant d'activer ces fonctionnalités ou de mettre à jour une configuration QoS existante vers une version SNS 4.3.

Sélection du meilleur lien

Il est désormais possible de configurer des critères précis afin de définir si un lien WAN respecte le niveau de qualité adapté à son type de trafic (VoIP, vidéo, etc.).

Pour cela, vous pouvez définir pour chaque type de trafic un engagement *SLA* (Service Level Agreement) basé sur un ou plusieurs seuils parmi les critères suivants :

- Latence,
- Gigue,
- Perte de paquets.

Dès qu'au moins un des seuils n'est plus respecté, le firewall sélectionne pour le trafic concerné un autre lien WAN pour lequel le statut SLA est bon.

Cette configuration peut être réalisée sur du trafic standard ou sur des communications chiffrées.

Indépendamment du type de trafic, vous pouvez également mettre en place une configuration plus générale permettant d'assurer que toutes les communications seront automatiquement basculées vers un lien de secours lorsque la qualité du lien principal utilisé est dégradée.

Vous pouvez visualiser la qualité de vos différents liens à tout moment depuis l'interface Web d'administration du firewall.

Pour plus d'informations, reportez-vous aux sections Objets réseau - Routeur, Supervision - SD-WAN et Rapports du Manuel Utilisateur SNS.

Amélioration de la fonctionnalité de Qualité de Service (QoS)

La fonctionnalité de Qualité de Service (QoS) a été améliorée pour répondre aux exigences des infrastructures récentes. Ces modifications permettent d'améliorer significativement la définition de priorités des flux ainsi que la limitation et la réservation de la bande passante.

Pour plus d'informations, reportez-vous à la section Qualité de Service (QoS) du Manuel Utilisateur SNS.

IMPORTANT

Les configurations de QoS définies dans une version antérieure à SNS 4.3 ne sont pas automatiquement valides. Elles nécessitent le paramétrage des *Traffic shapers* pour pouvoir être activées après mise à jour en version SNS 4.3.

Routage statique - Objets routeur

Il est désormais possible de sélectionner un objet routeur en tant que passerelle lors de la création ou la modification d'une route statique. Ceci apporte la possibilité de définir pour chaque route statique une stratégie de sélection de liens.

Vous pouvez toujours décider d'appliquer une politique de sélection de liens différente sur certains flux spécifiques en les configurant directement dans les règles de votre politique de filtrage (Policy Based Routing). Ces configurations sont prioritaires par rapport à celles mises en place dans le routage statique.

Pour plus d'informations, reportez-vous aux sections Routes statiques IPv4 / IPv6, Objets réseau - Routeur et Filtrage du Manuel Utilisateur SNS.

NOTE
Les objets routeur définis avec du partage de charge ne sont pas compatibles avec cette fonctionnalité.

Protocole TLS 1.3

Analyse des certificats serveur

Le moteur de prévention d'intrusion tente désormais de récupérer le certificat serveur pour chaque flux TLS 1.3 traversant le firewall afin d'analyser les éventuelles failles de sécurité liées à ce certificat et rendre opérationnel les signatures d'attaques et d'applications reposant sur l'analyse de ce certificat.

Cette analyse est activée par défaut sur le firewall. Certains flux TLS 1.3 peuvent à présent être bloqués alors qu'ils ne l'étaient pas auparavant en raison de cette nouvelle analyse protocolaire.

En savoir plus

Proxy SSL

Le proxy SSL supporte désormais le protocole TLS 1.3.

Protocoles industriels SOFBUS et LACBUS

Les firewalls SNS peuvent désormais détecter et analyser les protocoles SOFBUS et LACBUS. Cette analyse, désactivée par défaut, permet de détecter les comportements anormaux et de filtrer des commandes spécifiques SOFBUS et LACBUS afin de diminuer la surface d'attaque et le risque de compromission. Ces protocoles sont principalement utilisés dans les infrastructures de gestion des eaux. Ils sont la propriété intellectuelle de LACROIX Sofrel.

En savoir plus

Captures réseau

Un nouvel outil de captures réseau est désormais disponible dans l'interface Web d'administration des firewalls SNS et peut être utilisé à des fins de résolution de problèmes. Les critères de filtres les plus communs (IP, port, interface, etc.) peuvent être renseignés dans un assistant de création de filtre permettant aux utilisateurs n'ayant pas de connaissances sur l'outil *tcpdump* ou sur le format de ses filtres de créer des captures réseau. Le filtre *tcpdump* peut aussi être renseigné manuellement pour une utilisation avancée.

Ce nouvel outil permet de lancer jusqu'à 5 captures simultanément. Pour y accéder, le firewall doit posséder un support de stockage sur lequel enregistrer les captures (stockage interne ou carte SD par exemple).

En savoir plus

Accès distant par SSH au firewall

Ouverture de l'accès aux comptes administrateurs du firewall

Les administrateurs déclarés sur le firewall peuvent désormais se voir attribuer un droit d'accès en SSH au firewall. Cet accès est par défaut limité à l'interpréteur *shell nsrpc* (utilisation de commandes CLI / Serverd) et peut être étendu à l'interpréteur *shell* du système d'exploitation par le *super-administrateur* (compte *admin*).

En savoir plus

Protection contre les attaques par force brute

L'accès distant par SSH au firewall est désormais protégé contre les attaques par force brute. Si cette protection est déjà activée sur le firewall, son périmètre est automatiquement étendu.

En savoir plus

Authentification RADIUS

Tableau de bord

Les serveurs RADIUS sont désormais supervisés et leur état apparaît dans le widget **Services** du **Tableau de bord**.

Délai d'inactivité et nombre maximum d'essais de connexion

Le nombre maximum d'essais et le délai d'inactivité autorisé pour réaliser une connexion à un serveur RADIUS (serveur principal et serveur de secours) peuvent désormais être configurés. Ceci entraîne la modification de la commande CLI / Serverd `CONFIG AUTH RADIUS` avec l'ajout des arguments *timeout*, *retry*, *btimeout* et *bretry*.

En savoir plus

Support des *VSA* RADIUS

Il est désormais possible d'associer des utilisateurs authentifiés via RADIUS à des groupes dans le firewall grâce à l'ajout du support des *VSA* RADIUS. Ceci ouvre notamment la possibilité d'ajouter au firewall des administrateurs dont les utilisateurs ou les groupes proviennent d'autres domaines. Pour fonctionner, le serveur RADIUS doit également être configuré pour utiliser des VSA.

Activée par défaut, la prise en charge des *VSA* sur le firewall peut être désactivée en utilisant la commande CLI / Serverd `CONFIG AUTH RADIUS` avec l'argument *[VSAusergroup=<0|1>]*.

En savoir plus

Support de l'IPv6

Il est désormais possible de joindre des serveurs RADIUS en IPv6. Ceci apporte la possibilité de configurer dans le firewall des serveurs RADIUS avec des objets utilisant des adresses IPv6.

Support de l'attribut *domain*

Le nom de domaine d'un utilisateur peut désormais être reporté dans le champ de la requête RADIUS permettant à l'authentification RADIUS de s'intégrer dans une fédération comprenant plusieurs domaines.

Adresse IP source des requêtes RADIUS

L'adresse IP source des requêtes RADIUS peut désormais être configurée.

En savoir plus

Traitement des requêtes RADIUS

Les requêtes RADIUS sont maintenant traitées de manière asynchrone afin de faciliter l'intégration avec les plateformes OTP.

Serveur LDAP

Le serveur LDAP interne du firewall utilise maintenant une configuration TLS en accord avec les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

En savoir plus

VPN

VPN IPsec IKEv2 - Support de MOBIKE

Il est désormais possible d'utiliser MOBIKE avec des correspondants de type nomade (mobile). MOBIKE permet à un utilisateur nomade de ne pas avoir à renégocier un tunnel lorsqu'il change d'adresse IP.

L'activation de MOBIKE se réalise exclusivement à l'aide des commandes CLI / Serverd `CONFIG IPSEC PEER NEW` et `CONFIG IPSEC PEER UPDATE` avec l'argument *[mobike=<0|1>]* selon si vous ajoutez ou mettez à jour un correspondant.

Un paramètre supplémentaire permet de définir dans une politique IPsec les interfaces sur lesquelles le moteur IPsec construit sa liste d'adresses IP qu'il diffuse via MOBIKE. Ceci permet de limiter les adresses IP diffusées dans le cadre de l'utilisation de MOBIKE au strict minimum. La liste des interfaces concernées est modifiable exclusivement à l'aide de la commande CLI / Serverd `CONFIG IPSEC UPDATE` avec l'argument *[UsedInterface=<itf1,itf2,...>]*.

NOTE

MOBIKE n'est pas compatible avec le mode **Diffusion Restreinte (DR)** respectant les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

VPN SSL

La rapidité d'établissement des connexions et le support du protocole TLS 1.3 du VPN SSL ont été améliorés. Pour en bénéficier, vous devez utiliser un client VPN SSL compatible avec le protocole TLS 1.3. À noter que Stormshield Network SSL VPN Client en version 2.9 n'est pas compatible avec ce protocole.

Ces améliorations nécessitent désormais que la taille minimale du masque de l'objet réseau assigné aux clients UDP et TCP dans la configuration VPN SSL soit de /28.

Haute disponibilité et agrégats de liens

Dans une configuration disposant d'agrégats de liens réseau, l'initialisation de la haute disponibilité active par défaut l'option **Activer l'agrégation de liens lorsque le firewall est passif** permettant de bénéficier de temps de bascule optimisés.

Haute disponibilité - Liens directs entre membres du cluster

Dans une configuration en haute disponibilité avec des liens HA directs entre les deux membres du cluster (sans commutateur réseau intermédiaire), la perte complète des liens HA suite à une défaillance du firewall principal déclenche immédiatement la bascule sur l'autre membre du cluster.

Agrégat de liens - Redondance

Il est désormais possible de créer un agrégat de liens de type **Redondance**. La fonction de redondance permet de disposer d'un lien de secours au cas où le lien principal (identifié comme *Maître* dans l'agrégat) ne répond plus. Un agrégat de type **Redondance** doit contenir deux liens.

Cette nouvelle fonctionnalité est uniquement disponible sur les modèles SN510, SN710, SN910, SN1100, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNi20 et SNi40. Les firewalls SNS supportent cette fonctionnalité avec des commutateurs de marque Cisco uniquement.

En savoir plus

Service de télémétrie

Une fenêtre invite les administrateurs de firewalls SNS lorsqu'ils se connectent à l'interface Web d'administration à activer le service de télémétrie si celui-ci est désactivé.

En savoir plus

Certificats et PKI

Enrôlement Web - Enrôlement des certificats

Le service d'enrôlement Web a été amélioré afin de permettre aux utilisateurs d'effectuer des demandes de certificat depuis les dernières versions des navigateurs Web du marché. Lors de la réalisation d'une demande, les utilisateurs doivent à présent définir eux-mêmes la clé de chiffrement utilisée pour chiffrer leur clé privée.

En savoir plus

Rafraîchissement de la CRL d'une CA

Une nouvelle commande CLI / Serverd `SYSTEM CHECKCRL` est disponible permettant de forcer le rafraîchissement de la liste de révocation de certificats (*CRL*) d'une autorité de certification (*CA*).

En savoir plus

Durcissement du système d'exploitation

Mécanisme de vérification d'intégrité des fichiers exécutables

Le firewall SNS génère désormais un événement système lorsque le mécanisme de vérification d'intégrité des fichiers exécutables refuse de lancer un binaire.

Secure Boot

Il est désormais possible d'activer la fonctionnalité **Secure Boot** dans l'UEFI des firewalls SNi20, SN1100 et SN3100. L'activation de cette fonctionnalité permet de renforcer la sécurité du système avec notamment la vérification de signature du système chargé au démarrage du firewall.

Vulnérabilités résolues de SNS 4.3.3

Cartes réseau IXL

Des vulnérabilités de sévérité moyenne ont été corrigées dans les pilotes des cartes réseau IXL et les utilitaires NVM.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2020-029/,
- https://advisories.stormshield.eu/2020-031/,
- https://advisories.stormshield.eu/2020-032/,
- https://advisories.stormshield.eu/2020-033/,
- https://advisories.stormshield.eu/2020-036/,
- https://advisories.stormshield.eu/2020-040/,
- https://advisories.stormshield.eu/2021-066/.

Correctifs de SNS 4.3.3

Système

VPN IPsec

Référence support 78214

Un tunnel IPsec site à site avec l'objet *all* comme origine de trafic ne déclenche plus à tort l'envoi de paquets *keepalive* avec pour adresse source l'adresse de *broadcast* (255.255.255.255) qui étaient alors bloqués du fait de l'émission de l'alarme "Utilisation de l'adresse *broadcast* en source" (ip:89).
Notez que cette anomalie ne perturbait pas le trafic légitime au sein du tunnel IPsec.

Référence support 82729

Lorsqu'un certificat était caractérisé par un nom (DN - Distinguished Name) long de plus de 128 caractères, seuls les 128 premiers caractères étaient conservés par le firewall. Le déploiement via SMC d'une configuration IPsec avec un tel certificat échouait donc car les DN de certificats ne concordaient pas.
Cette taille maximale a été portée à 240 caractères (limite technique).

Référence support 81471

Dans une configuration utilisant un tunnel VPN IPsec soumis à une forte charge réseau, l'expiration d'une entrée ARP ne provoque plus de perte de paquets réseau.

Référence support 81691

Une anomalie dans l'ordonnanceur de processus / threads en cas de changement de priorité dynamique pouvait provoquer des pertes de paquets sur un firewall soumis à une forte activité. Cette anomalie a été résolue.

Référence support 83059

Un tunnel IPsec avec un correspondant dont le nom contient un caractère accentué parvient de nouveau à s'établir correctement. Cette régression était apparue en version SNS 4.2.

VPN IPsec IKEv2

Référence support 79713

L'opération de réauthentification en phase 1 d'un tunnel IPsec IKEv2 pouvait se terminer trop rapidement entraînant ainsi le rejet à tort de paquets légitimes. Pour éviter ce phénomène, un nouveau paramètre peut être utilisé afin de retarder la suppression de l'ancienne IKE SA.

VPN IPsec - Certificats

Références support 78593 - 78611 - 73609

Dans le cas de correspondants IPsec déployés via SMC (politique IPsec globale) et utilisant des certificats définis localement sur le firewall, les certificats utilisés n'étaient pas affichés dans le détail des correspondants. Ce problème a été corrigé.

VPN SSL

Référence support 81349

Le démon OpenVPN pouvait s'arrêter inopinément, entraînant la déconnexion de tous les utilisateurs connectés en VPN SSL. Ce problème a été corrigé.

Proxies

Référence support 79295

Les proxies et les modules basés sur les proxies (classification d'URL,...) gèrent désormais correctement les certificats présentant à la fois un champ *Subject* vide et un champ *Subjectaltname* renseigné.

Création d'interfaces

Référence support 75064

Une configuration comportant plusieurs centaines d'interfaces (interfaces virtuelles, VLAN, ...) entraînait une consommation CPU excessive suite au rechargement répété du fichier de configuration des interfaces réseau.

Réputation des machines

Référence support 78563

Les données liées à la fonction de réputation des machines ne consomment plus une quantité excessive d'espace disque. Ce problème empêchait l'affichage des rapports.

NOTE
Il est nécessaire de réinitialiser la base de données de réputation des machines pour que ce correctif soit pris en compte (module Protection applicative > Réputation des machines > bouton **Réinitialiser le score de toutes les machines dans la base de données**).

Authentification Kerberos UDP

Référence support 78725

La méthode d'authentification Kerberos basée sur UDP ne fonctionnait plus depuis la version SNS 4.0.3 suite à l'introduction du support de pré-authentification FAST dans cette méthode (RFC6113). Ce problème a été corrigé.

Authentification à un serveur LDAPS

Le firewall ne parvenait pas à authentifier un serveur LDAPS présentant un certificat signé par une CA avec CRL. Ce problème a été corrigé.

Configuration initiale par clé USB

Référence support 81713

Lors d'une configuration de firewall via clé USB, une modification de fuseau horaire de référence précisée dans le fichier de configuration additionnelle (format CSV) est désormais correctement prise en compte.

Objets réseau - Import via CSV

Référence support 78683

Les objets réseau importés via un fichier CSV sont désormais immédiatement pris en compte dans la configuration du firewall.

Mise à jour automatiques

Référence support 72728

Un problème de prise en compte de la planification des mises à jour automatiques, lorsque l'intervalle de mise à jour d'un sous-système (définitions antivirales, ...) était modifié, a été corrigé.

Lorsqu'un port spécifique est précisé dans une URL personnalisée de serveur *Active Update*, ce port est désormais correctement pris en compte.

Planificateur d'événements

Référence support 77428

La macro %STATE% utilisable dans le planificateur d'événements est désormais fonctionnelle et retourne les valeurs attendues.

Supervision des disques

Références support 75125 - 75126

Un problème de remontée à tort d'alarmes concernant l'état des disques des firewalls a été corrigé.

Supervision des interfaces - VLAN et agrégats

Référence support 80066

Dans le cas de VLAN rattachés à des interfaces incluses dans des agrégats, le débit affiché dans le module de supervision des interfaces est désormais correct et ne reste plus bloqué à tort à 10Mb/s.

ICMP - IPv6

Référence support 82547

Dans une configuration utilisant IPv6, un problème d'accès concurrentiel pouvait entraîner un blocage du firewall lors de la réception de paquets ICMP de type "destination injoignable". Ce problème a été corrigé.

Serveur PPTP

Le serveur PPTP permettant d'établir des tunnels entre un client PPTP et le firewall est de nouveau opérationnel. Cette régression était apparue en version SNS 4.2.

Accès console via port série

Références support 82054 - 81429

Sur les firewalls autres que les modèles SN210(W) et SN310, l'accès console via le port série ne permettait plus d'interrompre la séquence de démarrage afin de changer le mot de passe du

compte admin en mode *single user*. Ce problème a été corrigé.

Agent SNMP

Des problèmes d'accès concurrentiels qui pouvaient entraîner un arrêt du service ont été corrigés dans le mécanisme de vérification du nombre de notifications SNMP reçues.

Référence support 78695

Une anomalie dans la bande passante des agrégats de liens et des VLAN sur les agrégats de liens remontée par les OID ifSpeed et ifHighSpeed de la MIB IF-MIB a été corrigée.

Connexion à l'interface Web d'Administration avec authentification par certificats

Référence support 79815

Sur un firewall avec une configuration comportant plusieurs annuaires LDAP, l'authentification par certificat d'un administrateur dont le compte était issu de l'un des annuaires secondaires ne fonctionnait pas. Ce problème a été corrigé.

Connexion SSH - Mot de passe contenant le caractère *$*

Référence support 82949

L'enregistrement d'un mot de passe contenant le caractère *$* (exemple : pas$$word) fonctionne désormais correctement. Un utilisateur se connectant en SSH n'est donc plus obligé d'ajouter un caractère d'échappement \ avant chaque caractère *$* lors de la saisie de son mot de passe.

Haute disponibilité

Référence support 82211

Le mécanisme de nettoyage ARP (option de la haute disponibilité) a été amélioré afin d'éliminer les entrées au moment opportun. Avant ce correctif, ces entrées pouvaient être supprimées trop tôt, ce qui pouvait entraîner un délai dans la reprise de certains trafics réseau.

Haute disponibilité - Mode Diffusion Restreinte

L'activation depuis Stormshield Management Center du mode Diffusion Restreinte sur une configuration en haute disponibilité (activation directe ou par restauration de configuration) déclenche correctement le redémarrage du membre passif du cluster.

Haute disponibilité (HA) et agrégats de liens

Références support 82211 - 82855

Dans une configuration en haute disponibilité :

- Utilisant des agrégats de liens reliés à un commutateur réseau,
- Avec l'option **Activer l'agrégation de liens lorsque le firewall est passif**,
- Et pour laquelle chaque membre des agrégats impacte le calcul de l'indice de qualité (paramètre *LACPMembersHaveWeight* positionné à 1 à l'aide des commande CLI / SERVERD `CONFIG HA CREATE` ou `CONFIG HA UPDATE`),

alors la perte puis le retour du commutateur pouvaient entraîner des bascules aléatoires au sein du cluster. Ce problème a été corrigé.

Filtrage et NAT

Références support 81369 - 83651

Un mécanisme d'optimisation permettant d'éviter une perte de paquets réseau au rechargement d'une politique de NAT possédant un grand nombre de règles peut être activé à l'aide la commande CLI / Serverd `CONFIG PROTOCOL IP COMMON IPS CONFIG` en ajoutant le paramètre *natdiff* aux paramètres existants de l'option *OptimizeRuleMatch*.

A partir d'une configuration par défaut, utilisez les paramètres suivants : *OptimizeRuleMatch=equal,diff,cache,natdiff*.
Toute modification doit ensuite être validée par la commande `CONFIG PROTOCOL IP ACTIVATE`.

Notez que ce mécanisme est désactivé par défaut.

NAT - VLAN

Référence support 79759

Dans une configuration supportant plusieurs VLAN sur une même interface physique et mettant en œuvre de la translation d'adresses avec publication ARP sur ces mêmes VLAN, les paquets GARP (*Gratuitous ARP*) étaient envoyés à tort sur un seul de ces VLAN. Ce problème a été corrigé.

Firewalls équipés d'un TPM

Référence support 83580

Suite à une mise à jour de firmware, les registres *PCR* (*Platform Configuration Registers*) connus du TPM pouvaient être modifiés, rendant alors la politique d'accès aux secrets stockés dans le TPM non fonctionnelle.
La commande CLI / Serverd `SYSTEM TPM PCRSEAL tpmpassword=<password> [serial=(<serial>|passive|active|local)]` a été créée afin de pouvoir mettre à jour cette politique d'accès en inscrivant dans le TPM les nouvelles valeurs de *PCRs* acceptables, et ce depuis l'interface Web d'administration via le module **Console CLI**.
Dans le cas d'une configuration en haute disponibilité, cette commande permet également de sélectionner le membre du cluster sur lequel cette opération doit être réalisée.

Prévention d'intrusion

Performances du moteur de prévention d'intrusion

Références support 76810 - 77932

Des modifications ont été apportées au mécanisme d'allocation de mémoire dédiée aux connexions pour le moteur de prévention d'intrusion afin d'en accroître les performances.

Statistiques du moteur de prévention d'intrusion

Références support 79713 - 82437 - 81466

Des optimisations ont été apportées au mécanisme de gestion des statistiques du moteur de prévention d'intrusion. Elles permettent d'éviter de potentielles pertes de paquets lors du traitement récurrent de ces statistiques sur un firewall soumis à une charge réseau importante.

Protocole IP

Référence support 79787

Lorsque des paquets IP reçus par le firewall étaient fragmentés, une anomalie lors de la réécriture des paquets pendant l'analyse protocolaire provoquait la non réception du premier fragment par la machine destinataire lorsque le paquet réémis était plus petit que le paquet original. Ce problème a été corrigé.

Protocole DNS

Référence support 82274

Des alarmes "Attaque possible DNS rebinding" (dns:154) étaient déclenchées à tort lors de l'analyse protocolaire de flux DNS issus de machines Microsoft. Ce problème a été corrigé.

Références support 79494 - 80912

Le moteur d'analyse protocolaire des flux DNS était sensible à la casse utilisée dans les réponses des serveurs DNS et déclenchait l'alarme "Champ query DNS contradictoire" (dns:151) lorsque cette casse était différente de celle utilisée dans la requête. Ce comportement a été corrigé afin d'être compatible avec les RFC 1035, 8490 et 4343.

Protocole RDP dans COTP

Référence support 81814

L'analyse de paquets RDP dans COTP, à destination de serveurs Microsoft Windows et passant au travers d'un *Connection Broker* , ne provoque plus à tort d'alarmes bloquantes "COTP : taille de message invalide" (cotp:385) ou "COTP protocole invalide" (cotp:379).

Protocole SIP

Référence support 82964

Une anomalie dans le moteur d'analyse protocolaire SIP, qui pouvait entraîner un blocage du firewall, a été corrigée.

Administration du firewall

Référence support 78531

Une anomalie dans l'initialisation de la bibliothèque de supervision pouvait entraîner un redémarrage inopiné du service d'administration du firewall. Ceci se traduisait par une augmentation du temps de réponse pour les sessions d'administration via l'Interface Web d'administration ou la console SSH. Cette anomalie a été corrigée et des informations complémentaires ont été ajoutées dans les logs avancés (mode *verbose*).

Moteur de prévention d'intrusion

Référence support 81690

La réception de certains signaux d'interruption par le moteur de prévention d'intrusion ne provoquait pas l'écriture de traces complémentaires (fichier *core*) permettant d'identifier la cause du redémarrage du moteur. Ce problème a été corrigé.

Files d'attente d'informations sur la réputation / géolocalisation

Lorsqu'une requête de réputation de machine est effectuée et que la file d'attente des informations de réputation / géolocalisation est pleine, l'alarme remontée est désormais correcte ("Attaque possible des ressources"). Les statistiques indiquant que la file d'attente était pleine sont également correctement mises à jour.

Protocole SMB / CIFS

Référence support 83660

Une anomalie a été corrigée dans la prise en compte par le moteur d'analyse protocolaire SMB / CIFS des octets de remplissage de fin des paquets SMB.

Interface Web d'administration

Qualité de service (QoS)

Lors de la vérification d'utilisation d'une file d'attente de QoS, et lorsque aucun objet valide n'était trouvé, les messages d'information résultants présentaient des problèmes d'affichage de caractères spéciaux (apostrophes, supérieur, inférieur...). Ce problème a été corrigé.

Filtrage SSL - Filtrage d'URL

Références support 80809 - 80813

Une anomalie dans la commande système utilisée lors du survol des groupes de catégories d'URL ou des groupes de catégories de certificats provoquait à tort l'affichage du message "Cet objet n'existe pas". Cette anomalie a été corrigée.

Configuration

Référence support 82560

Un administrateur doté de tous les droits (autre que le compte super-administrateur admin) ne pouvait plus accéder au panneau **Configuration** de l'interface Web d'administration. Cette régression, apparue en version SNS 4.2.1, a été corrigée.

Configuration - Serveurs NTP

Référence support 81719

L'édition des clés d'authentification associées aux serveurs NTP est de nouveau fonctionnelle. Cette régression était apparue en version SNS 4.2.1.

VPN IPsec - Politiques locales et globales

Référence support 82376

Il n'était plus possible de renommer un objet de la politique IPsec locale, puis de passer sur la politique IPsec globale et d'y renommer un objet (ainsi que la manipulation inverse). Cette régression, apparue en version SNS 4.2.1, a été corrigée.

VPN IPsec - Groupes Diffie-Hellman

Lors de la création d'un profil IKE / IPsec, le groupe Diffie-Hellman proposé par défaut est désormais le DH14 (plus sécurisé) et non plus le DH1.

VPN IPsec - Vérifier l'utilisation d'un correspondant

Dans le module **Configuration > VPN > VPN IPsec**, onglet **Correspondants**, l'action permettant de vérifier l'utilisation d'un correspondant dans la configuration du firewall (disponible par un clic droit sur ce correspondant) prend désormais en compte davantage d'éléments dans sa vérification.

VPN IPsec - Authentification par certificat

Référence support 83287

Lors de l'affichage des caractéristiques d'un correspondant IPsec utilisant l'authentification par certificat, la CA ayant émis le certificat sélectionné n'était pas affichée. Cette anomalie a été corrigée et le champ Certificat se présente sous la forme : <CA>:<Certificat>.

Objets réseau

Référence support 79812

Au cours de la création d'un objet plage de ports, le fait de modifier le type d'objet à créer en objet port aboutissait néanmoins au final en la création d'un objet plage de ports. Ce problème a été corrigé.

Référence support 80539

Une fenêtre indiquant qu'un objet réseau avait été modifié pouvait s'afficher à tort lors de l'utilisation du module **Objets réseau**. Ce problème a été corrigé.

Administration du firewall

Référence support 78529

Dans l'onglet **Administration** du module **Configuration**, la création directe d'une machine autorisée à accéder aux pages d'administration du firewall ajoutait correctement la machine à la base objets mais ne l'affichait pas automatiquement dans la liste des machines autorisées. Ce problème a été corrigé.

Supervision - Tunnels VPN IPsec

Dans le module **Supervision > Tunnels VPN IPsec**, le lien permettant d'accéder à la configuration de la politique liée à un tunnel IPsec (disponible par un clic droit sur ce tunnel) tient désormais compte du fait que la politique liée soit globale ou locale et renvoie vers la politique correspondante.

Interfaces réseau

Référence support 83039

Les modifications manuelles de l'adresse MAC d'une interface réseau sont désormais bien conservées dans l'affichage du module Interfaces.

Certificats et PKI

Référence support 83828

Dans l'affichage du détail d'un certificat, le champ "sujet" avait été renommé à tort en "émetteur" depuis la version 4.0.1. Cette anomalie a été corrigée.

Référence support 83709

Pour un certificat ou une sous-CA importés sur le firewall, toute tentative de téléchargement de ce certificat ou de la CRL issue de la sous-CA se soldait par un échec et un message d'erreur système "L'autorité de certification n'a pas été trouvée". Ce problème a été corrigé.

Référence support 83570

Pour un certificat importé sur le firewall, toute tentative de vérification de l'utilisation de ce certificat se soldait par un échec et un message d'erreur système "Pas de certificat valide trouvé". Ce problème a été corrigé.

Référence support 82474

Lorsque plusieurs identités issues d'une même CA externe étaient importées sur le firewall, l'arborescence liée à cette CA était mal créée et les modules permettant de manipuler des certificats (Certificats et PKI, VPN IPSec ...) affichaient cette CA autant de fois que le nombre d'identités importées. Cette régression, apparue en version SNS 4.1, a été corrigée.

Firewalls avec TPM (SNi20, SN3100) - Activation IPv6

Référence support 83578

Sur un firewall modèle SNi20 ou SN3100 dont le TPM est initialisé, l'activation du support IPv6 demande désormais bien le mot de passe de ce TPM afin de réaliser correctement la sauvegarde de configuration sans provoquer l'affichage du message d'erreur système "Erreur de l'opération TPM : non autorisé".

Proxies

Référence support 84079

Il n'était pas possible de choisir une nouvelle CA de signature des certificats du proxy lorsque le mot de passe de cette nouvelle CA était identique à celui de l'ancienne CA. Cette régression, apparue en version SNS 4.2, a été corrigée.

Version 4.3.2 non publiée

La version 4.3.2 n'est pas disponible publiquement.

Version 4.3.1 non publiée

La version 4.3.1 n'est pas disponible publiquement.

Version 4.3.0 non publiée

La version 4.3.0 n'est pas disponible publiquement.

Vulnérabilités résolues de SNS 4.2.14

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-017.

Correctifs de SNS 4.2.14

Système

Haute disponibilité (HA) - Synchronisation

Référence support 83721

Des anomalies pouvant entraîner une consommation mémoire excessive ont été corrigées dans le mécanisme de synchronisation de configuration de la haute disponibilité.

Flux SSL à destination du firewall SNS

Référence support 84264

TLS 1.2 étant la version minimale de protocole à utiliser pour les flux SSL à destination du firewall SNS, les jetons de configuration correspondant aux versions SSL v3, TLS v1.0 et TLS v1.1 ont été supprimés du fichier de configuration du protocole SSL afin de les rendre inutilisables.

VPN IPsec - Objets routeur

Référence support 82369

Dans une configuration avec des tunnels VPN IPsec établis au travers d'un objet routeur, une bascule de passerelle au sein de cet objet routeur pouvait empêcher le rétablissement automatique de certains tunnels VPN IPsec. Cette régression, apparue en version SNS 4.2, a été corrigée.

Moteur de prévention d'intrusion

Nombre de machines protégées

Référence support 84537

Un problème dans la gestion du nombre maximal de machines protégées, survenant lors de la mise à jour d'un firewall SNS en version 4.2.11 ou supérieure, a été corrigé.

Correctifs de SNS 4.2.13

Moteur de prévention d'intrusion

Envoi de requêtes ARP pendant le rechargement de la configuration des interfaces dans le moteur de prévention d'intrusion

Référence support 84272

Un problème d'accès concurrentiel lorsque le moteur de prévention d'intrusion rechargeait la configuration des interfaces alors que des requêtes ARP étaient envoyées a été résolu. Ce problème provoquait un blocage du firewall.

Correctifs de SNS 4.2.12

Système

Création d'interfaces

Référence support 75064

Une configuration comportant plusieurs centaines d'interfaces (interfaces virtuelles, VLAN, ...) n'entraîne plus une consommation CPU excessive suite au rechargement répété du fichier de configuration des interfaces réseau.

Haute disponibilité

Référence support 84100

Dans une configuration en haute disponibilité, en cas de perte d'un lien sur le nœud actif du cluster, le temps de bascule du nœud actif en état passif a été réduit. Ceci permet au nœud passif d'opérer plus rapidement une bascule en état actif et de réduire ainsi la coupure du trafic réseau.

Statistiques de trafic sortant - VPN SSL

Référence support 79814

Les compteurs de paquets sortant de l'interface réseau liée au VPN SSL n'étaient plus actualisés. Cette anomalie apparue en version SNS 4.1 a été corrigée.

Récupération régulière des CRL

Référence support 84431

Lors de l'utilisation de la commande `PKI CONFIG UPDATE`, il n'est plus possible de renseigner une valeur incorrecte (comme *Any*) à l'argument *checkcrlbindaddr*.

Nouvelles fonctionnalités et améliorations de SNS 4.2.11

Prévention d'intrusion

Adresses IP multicast présentées en source

Référence support 84041

Une nouvelle alarme "Paquet src IP multicast" (alarme ip:755) permettant de bloquer par défaut les paquets présentant une adresse IP multicast comme adresse source a été ajoutée dans le moteur de prévention d'intrusion.

Vulnérabilités résolues de SNS 4.2.11

OpenSSL

Une vulnérabilité de sévérité forte a été corrigée dans le moteur OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-008/.

Éditeur de fichiers *vim*

Des vulnérabilités de sévérité moyenne impactant l'éditeur de fichiers *vim* ont été corrigées.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2022-004.

Antivirus ClamAV

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur antiviral ClamAV.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-005.

Moteur de prévention d'intrusion

Une vulnérabilité de sévérité forte a été corrigée dans le moteur de prévention d'intrusion.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-009.

Correctifs de SNS 4.2.11

Système

Filtrage et NAT

Référence support 82567

Dans certains cas, le seuil de connexion **TCP (c/s)** défini dans les paramètres de la qualité de service (QoS) d'une règle de filtrage n'était pas appliqué. Ce problème a été corrigé.

Vulnérabilités résolues de SNS 4.2.10

VPN SSL

Une vulnérabilité de sévérité forte a été corrigée dans le VPN SSL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2022-003.

Micro-codes CPU - Firewalls modèles SN1100, SN2100, SN3100 et SN6100.

Des vulnérabilités de sévérité moyenne ont été corrigées dans les micro-codes CPU des firewalls modèles SN1100, SN2100, SN3100 et SN6100.

Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2021-067.

Correctifs de SNS 4.2.10

Système

VPN IPsec avec NAT-T et *Path MTU Discovery* (PMTUD) activés

Référence support 83292

L'activation de l'option de PMTUD (commande CLI / Serverd `CONFIG IPSEC UPDATE slot=<1-10> PMTUD=<0|1>`) pour un tunnel IPsec soumis au NAT-T et utilisant l'association d'algorithmes AES-CBC 256 et SHA2_256 pouvait générer des paquets possédant une MTU trop importante. Ces paquets se retrouvaient alors bloqués par les équipements réseau empruntés.

Proxies

Référence support 79295

Les certificats présentant à la fois un champ Subject vide et un champ Subjectaltname renseigné sont désormais correctement traités par le Proxy SSL.

Proxy HTTP

Référence support 83607

Des problèmes d'accès concurrentiels aux compteurs de connexions pouvant entraîner un arrêt inopiné du proxy ont été corrigés.

Classification d'URLs - Extended Web Control (EWC)

Référence support 83619

Une anomalie dans la communication avec les serveurs EWC pouvait intervenir après plusieurs tentatives infructueuses de classification d'une URL. Cette anomalie a été corrigée.

Utilisation d'un proxy explicite et de la base de classification d'URLs Extended Web Control (EWC)

Référence support 82913

L'utilisation conjointe d'un proxy explicite et de la base de classification d'URLs EWC provoquait l'arrêt inopiné du moteur de classification d'URLs. Ce problème a été corrigé.

NAT - VLAN

Référence support 79759

Dans une configuration supportant plusieurs VLAN sur une même interface physique et mettant en œuvre de la translation d'adresses avec publication ARP sur ces mêmes VLAN, les paquets GARP (*Gratuitous ARP*) étaient envoyés à tort sur un seul de ces VLAN. Ce problème a été corrigé.

Prévention d'intrusion

Applications *Android WhatsApp* et *Facebook*

Référence support 82865

Des paquets légitimes issus des application *Android WhatsApp* ou *Facebook* déclenchaient à tort l'alarme bloquante "Différence dans la version SSL" (alarme ssl:117). Cette régression, apparue en version SNS 4.2.1, a été corrigée.

Interface Web d'administration

Tableau de bord - Machines virtuelles *Pay As You Go* (PAYG)

Référence support 83326

Le widget PAYG présent sur les machines virtuelles en mode *Pay As You Go* ne laisse plus apparaître à tort des balises HTML.

Vulnérabilités résolues de SNS 4.2.9

Micro-code CPU - Firewalls modèle SNi20

Des vulnérabilités de sévérité moyenne et forte ont été corrigées dans le micro-code CPU des firewalls modèle SNi20.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-040,
- https://advisories.stormshield.eu/2021-043.

Micro-code CPU - Firewalls modèle SN2100 et SN3100

Des vulnérabilités de sévérité basse et moyenne ont été corrigées dans le micro-code CPU des firewalls modèles SN2100 et SN3100.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-041,
- https://advisories.stormshield.eu/2021-042.

Correctifs de SNS 4.2.9

Système

Authentification - VPN SSL

Références support 78073 - 81741

Dans une configuration utilisant un annuaire LDAP externe principal et un annuaire LDAP externe de secours, la bascule de l'annuaire principal vers l'annuaire de secours pouvait provoquer un arrêt inopiné du moteur d'authentification, empêchant les utilisateurs d'accéder au VPN SSL. Ce problème a été corrigé.

Authentification à un serveur LDAPS

Référence support 84199

Le firewall ne parvenait pas à authentifier un serveur LDAPS présentant un certificat signé par une CA avec CRL. Ce problème a été corrigé.

Supervision matérielle - Disques

Référence support 84083

Le mécanisme d'analyse des résultats des tests SMART a été adapté afin de ne pas provoquer d'alertes inappropriées sur certaines références de SSD.

Agent SNMP

Référence support 81710

Des anomalies pouvant entraîner des fuites mémoire au sein de l'agent SNMP ont été corrigées.

Interface Web d'administration

Haute disponibilité

Référence support 83724

En cas d'erreur lors de la tentative de rattachement d'un firewall à un cluster, l'interface Web d'administration ne reste plus bloquée sur le message "Configuration de la haute disponibilité en cours".

Vulnérabilités résolues de SNS 4.2.8

Connexion en console ou via SSH

Une vulnérabilité de sévérité forte a été corrigée pour les connexions en console ou via SSH.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2021-069/.

Moteur de prévention d'intrusion

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur de prévention d'intrusion.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2021-050/.

Correctifs de SNS 4.2.8

Système

VPN IPsec

Références support 83903 - 84062

Monter un tunnel VPN IPsec avec authentification par certificat pouvait échouer lorsque la clé privée était protégée par le TPM. Une erreur "No private key found for <CN>" était alors enregistrée dans les logs. Ce problème a été corrigé.

Haute disponibilité (HA) - Mise à jour des firewalls

Lorsque le firewall passif d'un cluster HA était mis à jour en version SNS 4.2.3 ou supérieure puis basculé en état actif, la mise à jour du nouveau firewall passif en version SNS 4.2.3 ou supérieure échouait. Ce problème a été corrigé.

Authentification

Référence support 83411

Lorsqu'une redirection vers le portail captif (portail d'authentification) était réalisée par une règle de filtrage de type **Règle d'authentification**, il n'était plus possible de sélectionner la méthode d'authentification de type **Parrainage** depuis la page de ce portail captif. Cette anomalie, apparue en version SNS 4, a été corrigée.

Réseau

Références support 82366 - 83624 - 84201

Moteur de routage dynamique Bird

Les routes statiques déclarées dans la configuration de Bird et les routes dynamiques apprises par Bird ne déclenchaient pas l'ajout automatique des réseaux correspondants dans la table des adresses protégées. Ce problème a été corrigé.

Prévention d'intrusion

Analyse antivirale

Référence support 80792

Le trafic de l'application Zoom étant incompatible avec l'analyse antivirale, ces CN ont été ajoutés au groupe de CN *proxyssl_bypass*.

Protocole SMB / CIFS

Référence support 83660

Un problème provoquant le blocage de paquets SMB a été corrigé dans la prise en compte par le moteur d'analyse protocolaire SMB / CIFS des octets de remplissage de fin des paquets SMB.

Protocole NTP

L'alarme "NTP : KoD refusé" (ntp:456) n'est plus remontée à tort et en boucle lorsque le KoD (Kiss-of-Death) est associé à l'adresse IP du serveur NTP.

Protocole HTTP

Référence support 83553

Des optimisations ont été apportées à l'analyse protocolaire HTTP permettant d'éviter une consommation mémoire excessive et une surcharge inappropriée du firewall.

Vulnérabilités résolues de SNS 4.2.7

Éditeur de fichiers vim

Des vulnérabilités de sévérité moyenne impactant l'éditeur de fichiers vim ont été corrigées.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-061/,
- https://advisories.stormshield.eu/2021-062/,
- https://advisories.stormshield.eu/2021-063/,
- https://advisories.stormshield.eu/2021-064/.

VPN IPsec

Une vulnérabilité de sévérité moyenne a été corrigée dans le moteur de gestion des tunnels VPN IPsec.

Le détail de ces vulnérabilités est disponible sur notre site https://advisories.stormshield.eu/2021-065/.

Correctifs de SNS 4.2.7

Système

VPN IPsec

Référence support 82645

Dans une configuration IPsec utilisant un groupe contenant des plages d'adresses, les tunnels montés pouvaient être interrompus lorsque le groupe contenant les plages d'adresses était modifié, générant ainsi des erreurs *TS_UNACCEPTABLE*. Ce problème a été corrigé.

Référence support 83354

Lorsqu'une politique IPsec contenait une ou plusieurs règles de *bypass* (règles dont le correspondant est *None* et destinées à créer une exclusion aux règles suivantes de la politique de chiffrement), les réseaux définis par des routes statiques n'étaient pas pris en compte par ces règles de *bypass*.
Ce problème a été résolu en ajoutant une option *bypass* IPsec lors de la définition d'une route statique.

Clé USB 4G

Référence support 82757

Le modèle de clé USB 4G Huawei E3372h-320 est désormais supporté. Il ne provoque donc plus de redémarrages inopinés du firewall hôte.

Authentification par certificat (SSL) avec TLS v1.3

Référence support 82759

La méthode d'authentification par certificat (SSL) n'était pas fonctionnelle lorsque le firewall utilisait le protocole TLS v1.3. Ce problème a été corrigé sur le firewall grâce à l'ajout du support du *Post-Handshake Authentication*. À noter que le navigateur Web utilisé doit également autoriser le *Post-Handshake Authentication* pour que la méthode soit fonctionnelle.

Portail captif - Annuaire LDAP externe

Référence support 82686

La connexion au portail captif d'un utilisateur référencé dans un annuaire LDAP externe ne provoque plus à tort l'événement système "LDAP inaccessible" (événement 19). Cette régression était apparue en version SNS 4.1.4.

Firewalls avec TPM (SNi20, SN3100) rattachés à un serveur SMC

Références support 83380 - 83579

Un déploiement de configuration depuis SMC vers un firewall modèle SNi20 ou SN3100 dont le TPM était initialisé n'aboutissait pas et restait bloqué sur la création de la sauvegarde de configuration. Ce problème a été corrigé.

Correctifs de SNS 4.2.6

Système

VPN IPsec - Routage

Référence support 80662

La prise en compte d'un changement d'état d'une route réseau associée à une Security Policy IPsec n'entraîne plus un arrêt inopiné du service et un blocage du firewall.

Authentification interface Web d'administration - Portail captif

Référence support 83011

Des problèmes pouvant empêcher l'envoi des e-mails de parrainage ou déconnecter les utilisateurs de l'interface Web d'administration de manière intempestive avec le message "Session invalide" ont été corrigés.

Agent SNMP

Référence support 82661

La valeur retournée dans l'OID *UCD-SNMP-MIB::memCached.0* est désormais correcte.

Prévention d'intrusion

Protocole SIP

Références support 79839 - 79344

Des anomalies dans le moteur d'analyse du protocole SIP, qui pouvaient entraîner un blocage du firewall, ont été corrigées.

Mode FastPath

Référence support 83291

Un problème d'accès concurrentiel dans le moteur de prévention d'intrusion, pouvant entraîner un blocage du firewall, a été corrigé.

Protocole COTP

Références support 82784 - 83342

Un problème dans l'analyse du protocole COTP, pouvant entraîner un blocage du firewall, a été corrigé.

Nouvelles fonctionnalités de SNS 4.2.5

Authentification SPNEGO

Le script spnego.bat, disponible dans l'espace personnel MyStormshield, prend désormais en charge l'algorithme cryptographique AES256-SHA1, remplaçant l'ancien algorithme cryptographique utilisé RC4-HMAC-NT.

En utilisant cette nouvelle version du script lors de vos déploiements de l'authentification SPNEGO, il est impératif d'activer la **prise en charge du chiffrement AES 256 bits via Kerberos** dans les propriétés du compte du firewall sur l'Active Directory, onglet **Compte**, zone **Options de compte**.

Vulnérabilités résolues de SNS 4.2.5

Bibliothèque *Curl*

Une vulnérabilité de sévérité moyenne a été corrigée dans la bibliothèque *Curl*.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-048/.

OpenSSL

Des vulnérabilités de sévérité moyenne ont été corrigées par la mise à jour du composant OpenSSL.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2021-054/,
- https://advisories.stormshield.eu/2021-055/.

Bibliothèque *c-ares*

Une vulnérabilité de sévérité moyenne a été corrigée dans la bibliothèque *c-ares*.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-057/.

Correctifs de SNS 4.2.5

Système

VPN IPsec

Références support 82714 - 82784

Des problèmes d'interruption de négociation de tunnels IPsec ou d'arrêt inopiné du moteur de gestion de tunnels IPsec ont été résolus par la mise à jour de ce dernier et la mise en place d'un délai d'inactivité de ce moteur. Ces problèmes généraient également des entrées du type "*ignoring IKE SA setup: job load of XXX exceeds limit of YY*" dans les logs VPN IPsec.

Vérification des CRL

Référence support 82370

Lorsqu'une CRL contient un objet caractérisé par un nom de domaine qualifié (FQDN), la résolution DNS de ce FQDN fonctionne de nouveau correctement lorsque le firewall vérifie la CRL. Cette régression était apparue en version SNS 4.2.1.

Agent SNMP

Référence support 81710

Des améliorations ont été apportées au mécanisme de gestion de la table des alarmes SNMP. Elles permettent d'éviter un phénomène de duplication des OID qui empêchait l'émission de certaines alarmes.

Référence support 81710

Un problème de fuite mémoire lié à l'agent SNMP a été corrigé.

Agrégats de liens réseau

Référence support 82211

La perte d'un lien au sein d'un agrégat réseau ne permettait pas la bascule vers un autre lien avant un délai d'attente de 3 secondes, provoquant donc une interruption des flux durant ces 3 secondes. Ce problème a été corrigé.

Supervision des alimentations - Firewalls modèle SN1100

La supervision des alimentations fonctionne désormais sur les firewalls modèle SN1100.

Réseau

Renouvellement d'un bail DHCP

Références support 82238 - 82359

Lorsqu'un paquet UNICAST en provenance du port 67 et à destination du port 68 tentait de traverser le firewall (notamment dans le cas d'un renouvellement d'un bail DHCP), ce dernier pouvait être bloqué et ne jamais aboutir si l'interface de provenance et de sortie du paquet ne faisait pas partie d'un bridge.

Désormais, il est possible de corriger ce comportement en modifiant la valeur du paramètre **UseAutoFastRoute** à **Off** grâce à la commande CLI / Serverd suivante :

```
CONFIG PROTOCOL TCPUDP COMMON IPS CONNECTION UseAutoFastRoute=<On|Off>
```

En savoir plus

Nouvelles fonctionnalités de SNS 4.2.4

Système

Durcissement du système d'exploitation

La vérification d'intégrité des fichiers exécutables s'étend désormais à la partie *userland* du système.

Seuls les scripts *shell* sont encore autorisés, mais ils doivent explicitement être appelés par l'interpréteur (par exemple : sh script.sh et non ./script.sh). Si ces scripts sont lancés par le biais du planificateur d'événements (*eventd*), l'interpréteur doit être ajouté pour chaque tâche décrite dans le fichier de configuration du planificateur d'événements.

D'autre part, ces scripts doivent être exclusivement situés dans la partition root (/) pour pouvoir être exécutés. Toute mise à jour de firmware effaçant le contenu du répertoire "/", il est donc nécessaire de repositionner ces scripts dans le répertoire "/" après une mise à jour de firmware.

Notez que les outils de mesures de performances système autorisés par ce mécanisme de vérification d'intégrité des fichiers peuvent afficher des valeurs de mémoire consommée légèrement supérieures à celles affichées dans les versions précédentes de SNS. L'utilisation de l'outil *nmemstat* n'est plus autorisée.

Mode furtif (*stealth* mode)

En configuration d'usine, un firewall SNS n'est désormais plus en mode furtif par défaut afin de faciliter l'intégration du firewall dans les infrastructures existantes.

Ce mode furtif peut toutefois être activé manuellement par le biais de l'argument *Stealth* de la commande CLI / Serverd `CONFIG PROTOCOL IP COMMON IPS CONFIG:`

```
CONFIG PROTOCOL IP COMMON IPS CONFIG Stealth=<On|Off>
CONFIG PROTOCOL IP ACTIVATE
```

En savoir plus

Path MTU Discovery (PMTUD)

Pour des cas impliquant du VPN IPsec, les réponses ICMP 3/4 sont désormais pleinement prises en charge au travers de ces tunnels grâce à l'ajout du support du Path MTU Discovery.

Désactivé par défaut, il peut être géré à l'aide de la commande CLI / Serverd :

```
CONFIG IPSEC UPDATE slot=<1-10> PMTUD=<0|1|2>
CONFIG IPSEC ACTIVATE
CONFIG IPSEC RELOAD
```

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

NOTE

Le mode furtif (*stealth* mode) doit être désactivé pour permettre le fonctionnement du PMTUD au travers d'IPsec.

En savoir plus

VPN IPsec - Mode DR

Des avertissements sont affichés dans le widget **Messages** du tableau de bord lorsque le mode IPsec DR est activé et que l'une des conditions suivantes est remplie :

- Une règle de filtrage implique l'utilisation du proxy,
- Le service NSRPC est ouvert vers l'extérieur,
- Le service VPN SSL est actif,
- Le service de cache DNS est actif,
- Le service DHCP est actif.

VPN IPsec - IKEv2

Il est désormais possible de sélectionner les *PseudoRandom Functions* (PRFs) parmi les valeurs suivantes :

- PRF_HMAC_SHA2_256 [RFC4868],
- PRF_HMAC_SHA2_384 [RFC4868],
- PRF_HMAC_SHA2_512 [RFC4868].

Cette configuration est réalisable uniquement en ligne de commande au travers de l'argument *prf* ajouté à la commande CLI / Serverd : `CONFIG IPSEC PROFILE PHASE1 PROPOSALS UPDATE` (toute modification doit ensuite être validée par la commande `CONFIG IPSEC ACTIVATE`).

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

> **NOTE**
> Le mode IPsec DR impose l'usage de PRF_HMAC_SHA2_256.

Active Update

Les paquets du module Active Update sont désormais signés par une nouvelle autorité de certification Stormshield, remplaçant l'ancienne autorité de certification Netasq.

Pour les clients utilisant des sites miroirs internes, il convient de mettre à jour les paquets hébergés sur vos propres serveurs afin d'utiliser ceux signés par la nouvelle autorité de certification. Cette manipulation est indispensable pour que le module Active Update continue de mettre à jours ses bases.

Pour les environnements Linux, une nouvelle version du script *Active Update mirroring (updater.sh)* est disponible sur Mystormshield (section **Téléchargements** > **Stormshield Network Security** > **Tools**). Cette version permet de récupérer l'intégralité des paquets signés par la nouvelle autorité de certification.

En savoir plus

Il est désormais possible de préciser l'interface du firewall par laquelle sortent les requêtes destinées aux serveurs de mises à jour automatiques. Ceci est réalisable au travers de l'argument *bindaddr* ajouté à la commandes CLI / Serverd `CONFIG AUTOUPDATE SERVER`. La modification de ce paramètre doit ensuite être activée à l'aide de la commande `CONFIG AUTOUPDATE ACTIVATE`.

En savoir plus

Vérification automatique des mises à jour de firmware

La vérification automatique de présence d'une mise à jour de firmware peut être activée ou désactivée à l'aide la commande CLI / Serverd `SYSTEM CHECKVERSION state=0|1`.
Ce mécanisme est activé par défaut.

Gestion du réseau

La gestion du réseau d'un firewall SNS a été optimisée afin de ne plus redémarrer systématiquement le firewall dès qu'une configuration réseau est envoyée par SMC.

Dorénavant, le firewall signale à SMC qu'un redémarrage doit être effectué uniquement lorsque cela est nécessaire.

Agent Stormshield Management Center (SMC)

Sur un firewall SNS administré via SMC en version 3.0, si la liaison avec le serveur SMC n'a pas pu s'établir dans un délai de 30 secondes après un déploiement (délai modifiable dans la console d'administration du serveur SMC), alors la configuration précédente est restaurée.

Pour les firewalls en haute disponibilité, il est désormais possible de préciser qu'une modification de configuration réseau appliquée sur le firewall actif doit être appliquée sur le firewall passif sans provoquer de redémarrage de ce dernier.

Ceci est exclusivement réalisable à l'aide de la commande CLI / Serverd `HA SYNC` :

`HA SYNC Ennetwork=0|1` : 0 pour désactiver le redémarrage du passif (comportement par défaut), 1 pour l'activer.

En savoir plus

Synchronisation de la base de données des objets avec les serveurs DNS

La synchronisation automatique de la base de données des objets avec les serveurs DNS configurés sur le firewall peut désormais être activée / désactivée ou modifiée (intervalle de synchronisation).

Ces opérations sont exclusivement réalisables à l'aide de la commande CLI / Serverd `CONFIG OBJECT SYNC` :

- `CONFIG OBJECT SYNC STATE=<0|1>` pour la désactivation / activation de la synchronisation,
- `CONFIG OBJECT SYNC UPDATE period=<period>` pour un intervalle de lancement compris entre 1 min et 1 une journée (exemple : *period=6h5m4s*).

Ces modifications doivent être validées par la commande `CONFIG OBJECT SYNC ACTIVATE`.

En savoir plus

Modification des traces activées par défaut

Contrairement à ce qui a été annoncé dans les Notes de version 4.2.1, le stockage sur disque de tous les types de traces a été réactivé par défaut.

Matériel

La version 4.2.4 introduit le support du firewall modèle SN1100.

Interface Web d'administration

Création d'un correspondant IPsec

Lors de la création d'un nouveau correspondant IPsec, l'assistant de création propose désormais par défaut la version 2 du protocole IKE pour ce correspondant.

Vulnérabilités résolues de SNS 4.2.4

Analyse des protocoles RTSP, SIP, H323 et MGCP

Une vulnérabilité de sévérité forte a été corrigée dans le moteur d'analyse des protocoles RTSP, SIP, H323 et MGCP.

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

Proxies

Une vulnérabilité de sévérité moyenne a été corrigée dans le proxy explicite HTTP et le proxy SMTP.

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

Service DHCP

Une vulnérabilité de sévérité moyenne a été corrigée dans le service DHCP.

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

Bibliothèque *Curl*

Une vulnérabilité de sévérité moyenne a été corrigée dans la bibliothèque *Curl*.

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

Correctifs de SNS 4.2.4

Système

VPN SSL

Référence support 78163

Le lien de téléchargement du client Stormshield VPN SSL présenté par le portail captif du firewall hébergeant ce service tient désormais compte de la langue du navigateur.

Référence support 79149

Des contrôles additionnels ont été implémentés afin d'afficher une erreur lorsque le champ **Réseaux accessibles** est défini par un groupe contenant une plage d'adresses IP. Une telle configuration empêchait le service VPN SSL de fonctionner.

Référence support 73463

Le moteur de gestion du VPN SSL fonctionne désormais correctement avec les suites de chiffrement AES-GCM (taille de clés de 128, 192 ou 256 bits) recommandées par l'ANSSI.

Proxies

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.

Références support 79257 - 79144

Dans une configuration utilisant le proxy explicite HTTP ou le proxy SMTP sans analyse protocolaire, et lorsqu'une connexion cliente se caractérisait par l'envoi du drapeau FIN immédiatement après l'envoi du drapeau CONNECT, le proxy conservait à tort en mémoire la trace de cette connexion fermée. L'accumulation de ces traces de connexions pouvait alors entraîner une consommation excessive de la mémoire du firewall. Ce problème a été corrigé.

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.

Événements système

Référence support 80426

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

Vérification automatique des CRL

Référence support 82035

Une anomalie dans la vérification automatique des points de distributions de CRL (CRLDP) référencés dans une sous-autorité a été corrigée. Cette anomalie générait à tort l'alarme "La CRL publiée sur le point de distribution est invalide".

Vérification automatique des CRL et proxy externe

Référence support 81259

L'utilisation de la vérification des CRL au travers d'un proxy externe ne fonctionnait pas car le port pour joindre le proxy n'était pas correctement pris en compte. Ce problème a été corrigé.

Récupération des mises à jour de firmware et proxy externe

Références support 79538 - 81331

La récupération automatique de firmware au travers d'un proxy externe ne fonctionnait pas car le proxy n'était pas pris en compte. Ce problème a été corrigé.

VPN IPsec

Référence support 77960

Dans le cadre d'une utilisation conjointe de VPN IPsec et de *Path MTU Discovery* (PMTUd), le bit *Don't Fragment* (DF) n'était pas intégré aux paquets ESP et ne permettait donc pas d'utiliser le PMTUd. Cette configuration est désormais supportée.

En savoir plus

Références support 81013 - 81002

Lorsque la durée de vie de phase 1 d'un tunnel est écoulée, l'utilisateur n'est plus supprimé à tort des tables d'authentification du firewall si d'autres tunnels le concernant sont toujours actifs.

Référence support 77477

Une configuration IPsec associée à une règle de NAT concernant les paquets destinés au tunnel et une règle de QoS pour les flux transitant par ce tunnel provoquait la saturation de la mémoire du firewall et entraînait l'instabilité du cluster en cas de configuration en haute disponibilité. Ce problème a été corrigé.

VPN IPsec - Mode Diffusion Restreinte (mode DR)

Sur un firewall configuré en mode Diffusion Restreinte (mode DR), les profils de chiffrement DR n'autorisent désormais plus qu'une taille (force) de 256 bits pour les clés des algorithmes AES-GCM et AES-CTR.

Une erreur dans l'implémentation de l'algorithme ECDSA basé sur les courbes elliptiques Brainpool 256 ne permettait pas l'établissement de tunnels IPsec en mode DR avec le client VPN IPsec TheGreenBow implémentant le mode DR. Cette erreur a été corrigée.

ATTENTION
La correction de cette erreur rend de fait impossible l'établissement de tunnels IPsec en mode DR, basés sur ECDSA et courbes elliptiques Brainpool 256, entre un firewall en version SNS 4.2.1 ou SNS 4.2.2 et un firewall en version SNS 4.2.4 (ou supérieure).

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.

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.

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.

Références support 77326 - 77980 - 79673 - 74614 - 80572 - 80624 - 79664 - 79589

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.

Configuration initiale par clé USB

Référence support 80866

Dans le cadre de la configuration initiale par clé USB, lorsqu'un fichier de configuration additionnelle .CSV était importé dans la séquence d'installation, la commande renseignée à la dernière ligne du fichier n'était pas exécutée. Ce problème a été corrigé.

Portail captif

Référence support 79386

La fermeture de la page de déconnexion du portail captif provoque à nouveau la déconnexion de l'utilisateur, quel que soit le navigateur Internet utilisé.

Service d'authentification

Référence support 81423

Un souci lors de la communication avec un serveur LDAP externe configuré sur le firewall (problème réseau, réponse partielle du serveur...) provoquait un blocage du service d'authentification du firewall, déconnectant les utilisateurs et les empêchant de s'authentifier à nouveau. Ce problème a été corrigé.

Agent SNMP

Référence support 81710

Un problème de fuite mémoire dans la gestion de la file d'attente de l'agent SNMP a été corrigé.

Référence support 81573 - 81588 - 81529

Lorsque le firewall reçoit une requête SNMP, l'adresse de réponse utilisée par l'agent SNMP est de nouveau correcte et correspond bien à l'adresse IP du firewall interrogée lors de cette requête SNMP.

Références support 82734 - 82735

Des erreurs de syntaxe ont été corrigées dans les MIB STORMSHIELD-VPNSP-MIB, STORMSHIELD-VPNSA-MIB, STORMSHIELD-VPNIKESA-MIB et STORMSHIELD-ALARM-MIB.

Certificats

Référence support 82110

Une anomalie dans la gestion d'un champ OCSP vide pouvait engendrer à tort un message d'erreur "XSS Protection" lors de l'affichage des propriétés du certificat concerné. Cette anomalie a été corrigée.

Bypass matériel - Firewalls modèle SNi20

Référence support 82241

Le mécanisme de bypass matériel pouvait ne pas fonctionner sur certains firewalls modèle SNi20. 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), lorsqu'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.

Routage multicast - Translation d'adresse

Référence support 80359

Les paquets d'un trafic réseau multicast ne sont plus dupliqués si le routage multicast est appliqué après une règle de NAT destination appliquée à ce trafic.

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. Cette anomalie a été corrigée.

Prévention d'intrusion

Mécanisme de *FastPath*

Référence support 82078

La combinaison de translation d'adresses (NAT) et d'insertion de routes inappropriées dans les tables du moteur de prévention d'intrusion pouvait entraîner une utilisation inadéquate du mécanisme de *FastPath* et provoquer un blocage du firewall. Ce problème a été corrigé.

Matériel

Les cartes réseau Intel additionnelles installées sur les firewalls SN6100 pouvaient ne pas être reconnues par l'utilitaire Intel de mise à jour du microcode de ces cartes. Cette anomalie a été corrigée.

Supervision

Tunnels IPsec

Référence support 82043

Les tunnels IPsec mobiles établis et définis en *mode Config* apparaissent désormais dans le module de supervision des tunnels IPsec.

Interface Web d'administration

Haute disponibilité

Référence support 80888

La modification de la durée minimale des connexions devant être synchronisées est désormais correctement prise en compte (Haute disponibilité > Configuration avancée).

Version 4.2.3 non publiée

La version 4.2.3 n'est pas disponible publiquement.

Vulnérabilités résolues de SNS 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 SNS 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.

Nouvelles fonctionnalités de SNS 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).

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 SNS 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 SNS 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 SNS 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 SNS 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.

Des vulnérabilités d'un score global CVSS de 5.3 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.

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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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.

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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 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 SNS 4.0.1

Filtrage

Filtrage des adresses MAC

SNS permet maintenant de définir et d'utiliser dans les politiques de filtrage des objets réseau 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 SNS 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 SNS 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 > Gestion des tickets**.

- +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.