STORMSHIELD

STORMSHIELD NETWORK SECURITY

NOTES DE VERSION

Version 4.8 LTSB

Dernière mise à jour du document : 15 octobre 2026

Référence : sns-fr-notes_de_version-v4.8.20-LTSB

Table des matières

Historique des modifications ... 3
Points d'attention pour une mise à jour depuis une version 4.3 LTSB ... 4
Changements de comportement ... 7
Vulnérabilités résolues de SNS 4.8.20 LTSB ... 16
Compatibilité ... 17
Problèmes connus ... 18
Limitations et précisions sur les cas d'utilisation ... 19
Ressources documentaires ... 31
Installer cette version ... 32
Versions précédentes de SNS v4 ... 34
Contact ... 357

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.

Pour maintenir votre firewall dans des conditions de sécurité et de fonctionnement optimales, il est important d'appliquer la mise à jour de firmware la plus récente ainsi que les recommandations de configuration fournies par Stormshield.

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
15 octobre 2026	Nouveau document

Points d'attention pour une mise à jour depuis une version 4.3 LTSB

IMPORTANT
Si vous envisagez de mettre à jour un firewall depuis une version 4.3 LTSB vers la version 4.8 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 4.8 LTSB depuis la dernière version 4.3 LTSB disponible est consultable dans la section Changements de comportement de ces Notes de Versions.

Chemin de mise à jour depuis une version 4.3 LTSB

Il est fortement recommandé de mettre à jour votre firewall depuis la version SNS 4.3 LTSB la plus récente en passant par la version SNS 4.3.24 LTSB si nécessaire.

La liste exhaustive des changements de comportements intervenus en version SNS 4.8 LTSB est consultable dans la section Changements de comportement de ces Notes de Versions.

Version d'origine	Mises à jour intermédiaires requises
4.3.23 LTSB ou inférieure	Version 4.3.24 LTSB recommandée, car la partition de secours du firewall serait inutilisable après un passage direct vers la nouvelle version
4.3.24 LTSB ou supérieure	Aucune

Routage Dynamique BIRD

La version 1 du moteur de routage dynamique BIRD est à présent considérée comme obsolète et sera supprimée dans une version SNS à venir. La version 2 du moteur de routage dynamique BIRD étant disponible en version SNS 4.8. LTSB, il est fortement conseillé de migrer les configuration BIRD v1 vers BIRD v2.

Lors de la mise à jour d'une configuration utilisant BIRD v1 vers une version SNS 4.8 LTSB, la configuration initiale est conservée et il est nécessaire de réaliser manuellement la migration de configuration de BIRD v1 vers BIRD v2.

Dans le cas où votre parc de firewalls SNS est géré par un serveur SMC, il n'est pas possible de gérer le routage dynamique de vos firewalls en version SNS 4.8 LTSB depuis une version de SMC inférieure à la 3.6.

Firewalls équipés d'un TPM

Après une mise à jour en version SNS 4.8 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, veuillez consulter la section Trusted Platform Module du manuel utilisateur SNS ainsi que la Note Technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.

Pour les firewalls supportant Secure Boot dans l'UEFI (modèles SN-XS-Series-170, SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN3100, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200, SN-XL-Series-6200, SNi10, SNi20, SNxr1200), il est fortement recommandé d'activer Secure Boot avant de procéder à cette opération de rescellement des secrets.

Pour plus d'information sur les impacts de l'activation de Secure Boot, veuillez consulter la Note Technique Gérer Secure Boot dans l'UEFI des firewalls SNS.

Suppression de l'analyse protocolaire OSCAR, MSN, YMSG et eDonkey

Les protocoles OSCAR, MSN, YMSG et eDonkey étant obsolètes, le moteur de prévention d'intrusion ne prend plus en charge leur analyse. Après mise à jour en version SNS 4.8 LTSB d'une configuration présentant une règle de filtrage relative à l'un de ces protocoles, cette règle est ignorée et un message d'avertissement est affiché au sein de la politique de filtrage concernée.

VPN SSL

La version SNS 4.8 LTSB ajoutant l'option *data-cipher* au fichier de configuration des clients VPN SSL, les clients VPN SSL v2 ne sont plus compatibles avec SNS 4.8 LTSB.

La compression est désormais désactivée par défaut. Il est possible de consulter et de changer l'état de la compression (activée ou désactivée) depuis la console CLI. Il est fortement déconseillé de réactiver la compression, car c'est une fonctionnalité qui ne sera plus supportée dans une version ultérieure de SNS.

Catégories de réputation

Les catégories de réputation Exchange Online, Microsoft Authentication, Office 365, Office Online, SharePoint Online et Skype for business, présentes dans les versions antérieures ne sont plus disponibles depuis la version SNS 4.4.1. Après mise à jour en version SNS 4.8 LTSB d'une configuration utilisant l'une de ces catégories, les règles de filtrage faisant appel à ces catégories deviennent inopérantes jusqu'au remplacement de ces catégories par les services Web introduits en version SNS 4.4.1.

Fonctionnalités et algorithmes devenus obsolètes en version SNS 4.8 LTSB

Les fonctionnalités et algorithmes listés ci-après sont devenus obsolètes en version SNS 4.8 LTSB et sont amenés à être supprimés dans une prochaine version de firmware SNS.

Network Vulnerability Manager (SNVM)

Le module **SNVM** est obsolète. Il sera supporté toute la durée de vie de la versions SNS 4.8 LTSB. Pour plus d'informations sur la date de fin de vie du module SNVM, reportez-vous à la section Services du *Cycle de vie produits*.

Filtrage URL / SSL
La base d'URL embarquée est obsolète. Pour continuer d'utiliser du filtrage URL / SSL, vous pouvez souscrire à l'option Extended Web Control.

VPN Serveur PPTP
La fonctionnalité Serveur PPTP est obsolète.

Protocole SCEP (enregistrement de certificats)
Les algorithmes de hachage md2, mdc-2, md4, md5, rmd160, et l'algorithme de chiffrement des-ede3-cbc sont obsolètes.

Agent SNMPv3
L'algorithme d'authentification MD5 et les algorithmes de chiffrement DES et SHA1 utilisés par l'Agent SNMPv3 sont obsolètes.

Annuaire LDAP interne
Les algorithmes de hachage des mots de passe MD5, SMD5, SHA, SSHA, SHA256, SHA384 et SHA512 utilisés par l'annuaire LDAP interne sont obsolètes.

VPN SSL Portail
La fonctionnalité VPN SSL Portail est obsolète.

Changements de comportement

Cette section liste les changements de comportements automatiques liés à la mise à jour de votre firewall SNS en version 4.8.20 LTSB depuis la dernière version 4.3 QS disponible.

Au besoin, nous vous invitons également à consulter les Changements de comportement de la version SNS 4.3 introduits depuis la dernière version 3.7.x LTSB disponible.

Changements introduits en version 4.8.17 LTSB

Routage dynamique BIRD - Protocole OSPF - Interfaces virtuelles IPsec (VTI)

Afin de préparer une mise à jour de configuration en version 5.1 ou supérieure, la directive `"type nbma;"` (nbma : non-broadcast multiple access) doit être ajoutée dans la configuration des interfaces VTI impliquées dans le routage dynamique.

Il est fortement recommandé de réaliser cette modification de configuration sur l'ensemble des routeurs.

Il est également fortement recommandé de référencer les interfaces VTI par leur nom, et non celui de leur pilote, dans la configuration BIRD.

Un message d'avertissement est affiché dans l'interface Web de configuration du routage dynamique lorsque des interfaces VTI pour lesquelles le mode *nbma* n'est pas précisé sont utilisées dans le routage dynamique BIRD.

Changements introduits en version 4.8.16 LTSB

Fonctionnalités obsolètes en version 4.8

L'utilisation de proxy HTTP explicite et de WPAD sont obsolètes.
Des messages d'avertissement sont affichés lorsque ces fonctionnalités sont utilisées dans une configuration mise à jour en version 4.8.16 (tableau de bord, règles de filtrage, accès au fichier .pac).

Remise en configuration d'usine - Interfaces réseau

Suite à une remise en configuration d'usine d'un firewall en version SNS 4.8.16 LTSB ou supérieure, la première interface réseau du firewall est automatiquement positionnée en adressage IP dynamique (DHCP).

Changements introduits en version 4.8.15 LTSB

Authentification multi-utilisateurs obsolète

L'authentification multi-utilisateurs (authentification par cookie) est obsolète et sera supprimée dans une version à venir. Veuillez la remplacer par la méthode Agent TS.

Remplacement du package de rattachement d'un firewall SNS

Depuis SMC, vous pouvez générer à tout moment un nouveau package de rattachement pour un firewall déjà connecté à SMC, mais l'interface Web d'administration du firewall ne permet pas de remplacer le package déjà installé. Une commande CLI est disponible pour effectuer le remplacement. Pour plus d'informations, reportez-vous à la section Installer un nouveau package de rattachement sur un firewall SNS du Manuel utilisateur SNS.

Certificats et PKI
Afin de se conformer aux bonnes pratiques et pour conserver la compatibilité avec les versions à venir de certains navigateurs Web, les certificats serveur ne présentent désormais plus la directive Extended Key Usage (XKU) "clientAuth".

Changements introduits en version 4.8.13 LTSB

- Authentification SPNEGO - L'authentification SPNEGO est obsolète et sera supprimée en version SNS 5.1. Des messages d'avertissement vous informent de cette obsolescence :
  - Lorsque vous souhaitez activer l'authentification SPNEGO dans le module **Configuration > Utilisateurs > Authentification**,
  - Dans l'encart **Messages** du tableau de bord si l'authentification SPNEGO est activée.

  Stormshield recommande fortement d'utiliser d'autres méthodes d'authentification SSO telles que la méthode Agent TS.

Changements introduits en version 4.8.10 LTSB

- SNMPV1 - La version 1 de SNMP est obsolète et sera supprimée en version SNS 5.1. Un message d'avertissement vous informe de cette obsolescence dans l'onglet **SNMPV1 - SNMPV2C** du module **Configuration > Notification > Agent SNMP**.

Changements introduits en version 4.8.9

- Firewall administré par SMC - Dans le cas d'un firewall administré par SMC, la mise à jour vers une version SNS 4.8.9 ou supérieure est bloquée si ces deux conditions sont réunies :
  - La clé privée du certificat utilisé pour les communications avec le serveur SMC est protégée par le TPM,
  - Le firewall est en version SNS 4.8.2 ou inférieure.

  Afin de réaliser la mise à jour, il est également nécessaire de déprotéger le certificat SMC soit par l'interface Web d'administration, soit par la commande CLI / Serverd `CONFIG FWADMIN PROTECT tpm=none tpmpassword=<password`. Pour plus d'informations, reportez-vous à la section Protéger les clés privées de certificats d'un firewall SNS de la note technique *Configurer le module TPM et protéger les clés privées de certificats du firewall SNS*.
- Moteur antiviral ClamAV - Le moteur antiviral ClamAV est obsolète et sera supprimé en version SNS 5. Les mises à jour du moteur s'arrêtent en septembre 2025. Des messages d'avertissement vous informent de cette obsolescence :
  - Dans le module **Protection applicative > Antivirus**,
  - Dans l'encart **Messages** du tableau de bord si le moteur antiviral ClamAV est utilisé.

  De plus, l'icône antivirus de l'encart **Services** du tableau de bord est orange.
  La mise à jour en version SNS 5 sera impossible si le moteur antiviral ClamAV est utilisé.
  Si vous souhaitez continuer à utiliser un moteur antiviral, vous devez souscrire à l'option d'antivirus avancé. Pour plus d'informations, contactez votre revendeur.

Changements introduits en version 4.8.7

- Firewalls équipés d'un TPM - Sur les versions SNS 4.8.7 et supérieures, la protection assurée par le module TPM est incomplète tant que la fonctionnalité Secure Boot n'est pas activée. Il est recommandé de l'activer avant de mettre à jour le firewall SNS en version 4.8.7 si le module TPM est initialisé. Pour plus d'informations, reportez-vous à la note technique Configurer le module TPM et protéger les clés privées de certificats du firewall SNS.
- Firewalls dont les certificats VPN sont protégés par le TPM - Après une mise à jour en version SNS 4.8.7 et si les certificats utilisés pour les services VPN IPsec ou VPN SSL sont protégés par le TPM, il est nécessaire de resceller le module TPM.
- Network Vulnerability Manager (SNVM) - Le module **SNVM** est obsolète et est amené à être supprimé en version SNS 5. Il sera supporté toute la durée de vie de la versions SNS 4.8. Pour plus d'informations sur la date de fin de vie du module SNVM, reportez-vous à la section Services du *Cycle de vie produits*. Des messages d'avertissement vous informe de cette obsolescence :
  - Si le mode DR est activé, dans l'encart **Message** du tableau de bord,
  - Si le mode DR n'est pas activé, dans l'encart **Message** du tableau de bord et dans le module **SNVM**.

    Routage par politique - Le routage par politique étant prioritaire sur le routage statique, il est désormais correctement appliqué lorsque du trafic non-explicitement routé est abandonné (décision d'envoi de ce trafic vers une passerelle de type *blackhole*).

Changements introduits en version 4.8.5

- Annuaire LDAP interne - L'algorithme de hachage des mots de passe CRYPT utilisé par l'annuaire LDAP interne est obsolète. Il n'est plus possible de créer d'annuaire LDAP interne avec cet algorithme. Les annuaires déjà existants utilisant cet algorithme ne sont pas impactés.

Changements introduits en version 4.8.3 EA

En savoir plus

- Firewalls équipés d'un TPM - Après une mise à jour en version SNS 4.8.3, 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.

- Services Web dans le filtrage - L'utilisation dans une règle de filtrage d'un service web personnalisé dont le nom comporte exactement 20 caractères rend cette règle de filtrage inopérante. Cette situation entraîne l'affichage d'un message d'avertissement dans le widget **Messages** du **Tableau de bord**. Ce message précise la politique de filtrage et le numéro de règle concernés.
  Pour corriger la situation, vous devez :
  - Mettre en conformité (moins de 20 caractères) le nom du service Web dans le fichier d'import CSV initialement utilisé,
  - Réimporter ce fichier dans le module **Objets** > **Services Web** > onglet **Import de services personnalisés**,
  - Modifier la règle de filtrage pour utiliser le nouveau nom du service Web.
- La configuration d'usine d'un firewall en version SNS 4.8.3 EA ou supérieure autorise de nouveau par défaut le retour à une version inférieure de firmware.
- Filtrage URL / SSL - La base d'URL embarquée est obsolète, elle n'est plus mise à jour et est amenée à être supprimée dans une prochaine version de firmware SNS.
  Pour continuer de réaliser du filtrage URL / SSL, vous pouvez :
  - Souscrire à l'option Extended Web Control,
  - Continuer d'utiliser le moteur de filtrage d'URL embarqué en l'associant avec une base de filtrage d'URL fournie par un tiers, par exemple :
    - Base de filtrage d'URL française fournie par le Rectorat de Toulouse (Académie de Toulouse), en suivant la méthode décrite dans la Base de connaissances Stormshield (authentification requise),
    - Base de filtrage d'URL polonaise fournie par Dagma, en suivant la méthode suivante : https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku.
- VPN Serveur PPTP - La fonctionnalité Serveur PPTP est obsolète et est amenée à être supprimée dans une prochaine version de firmware SNS.
- Protocole SCEP (enregistrement de certificats) - Les algorithmes de hachage md2, mdc-2, md4, md5, rmd160, et l'algorithme de chiffrement des-ede3-cbc sont obsolètes. Ils sont amenés à être supprimés dans une prochaine version de firmware SNS.

Changements introduits en version 4.8.1 EA

En savoir plus

- Un firewall en version SNS 4.8.1 EA refuse un retour à une version inférieure à SNS 4.7.3 ou SNS 4.3.24 LTSB.
- Firewalls équipés d'un TPM - Après une mise à jour en version SNS 4.8, 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.
- Agent SNMPv3 - L'algorithme d'authentification MD5 et les algorithmes de chiffrement DES et SHA1 utilisés par l'Agent SNMPv3 sont obsolètes et seront supprimés dans une prochaine version de firmware SNS.

- Annuaire LDAP interne - Les algorithmes de hachage des mots de passe MD5, SMD5, SHA, SSHA, SHA256, SHA384 et SHA512 utilisés par l'annuaire LDAP interne sont obsolètes et seront supprimés dans une prochaine version de firmware SNS.
- VPN SSL Portail - La fonctionnalité VPN SSL Portail est obsolète et est amenée à être supprimée dans une prochaine version de firmware SNS.
- Routage Dynamique BIRD
  - La version 1 du moteur de routage dynamique BIRD est à présent considérée comme obsolète. La version 2 du moteur de routage dynamique BIRD est désormais disponible,
  - Dans le cas où votre parc de firewalls SNS est géré par un serveur SMC, il n'est pas possible de gérer le routage dynamique de vos firewalls en versions 4.8.1 EA et supérieures depuis une version de SMC inférieure à la 3.6.
- Agent SNMP - La valeur attribuée au champ *sysname* présenté par l'agent SNMP respecte désormais un nouvel ordre.

Changements introduits en version 4.7.7

- 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 4.7.5

- 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 4.7.3

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

Changements introduits en version 4.7.2 EA

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 4.7.2 EA 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 4.7.2 EA.

Changements introduits en version 4.7.1 EA

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 4.7 et supérieures respectent cette recommandation.
  Si le mode IPsec DR est activé sur un firewall SNS en version 4.7, 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 4.7 et supérieure.
- Firewalls équipés d'un TPM - Après une mise à jour en version SNS 4.7, 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.
- 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 4.7.1 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 4.7 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 4.7.1.

- Remise en configuration d'usine - La remise en configuration d'usine (*defaultconfig*) d'un firewall supprime désormais par défaut tous les fichiers de configuration personnalisée ajoutés par l'administrateur. Si vous ne souhaitez pas les supprimer, utilisez la commande `defaultconfig -T`.
- Synchronisation des adresses MAC (HA) - Pour les machines virtuelles (EVA) déployées en version 4.7 ou supérieure et configurées en haute disponibilité (HA), la synchronisation des adresses MAC lors d'une bascule du cluster est à présent désactivée par défaut.

- Durcissement du système - Le durcissement du système en version SNS 4.7 rend inutilisable la partition de secours du firewall en version SNS 4.3.23 LTSB ou inférieure après un passage direct en version SNS 4.7. Il est recommandé de mettre à jour le firewall en version SNS 4.3.24 LTSB ou supérieure avant de le mettre à jour en version SNS 4.7.

Changements introduits en version 4.6.9

En savoir plus

- Connexions SSH au firewall - Sur un firewall en configuration d'usine et en version SNS 4.6.9 ou supérieure, 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 4.6.8

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 4.6.3

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 4.5.3

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*.
- 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`.
- 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 4.5.2

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 4.5.2 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 4.5.1

En savoir plus

- VPN SSL - La version SNS 4.5 est exclusivement compatible avec le client VPN SSL 3.1 ou le client OpenVPN 2.5 (ou supérieur). Il est nécessaire de mettre à jour le client VPN SSL (ou OpenVPN) sur les postes clients avant de mettre à jour le firewall en version SNS 4.5. Il sera également nécessaire de mettre à jour la configuration (disponible sur le portail captif) des clients OpenVPN suite à la mise à jour du firewall en version 4.5.
- QoS - La définition de files d'attente en pourcentage de bande passante est obsolète. Après la mise à jour en version SNS 4.5 d'un firewall dont la configuration de QoS utilisait une file d'attente définie par un pourcentage de bande passante, un message d'avertissement est affiché dans la grille des files d'attente afin d'inviter l'administrateur à modifier la configuration de cette file.
- Kerberos - L'authentification Kerberos est désormais basée par défaut sur le protocole TCP (objet *kerberos_tcp* - port 88/TCP).

Changements introduits en version 4.4.1

En savoir plus

- Catégories de réputation - Les catégories de réputation Exchange Online, Microsoft Authentication, Office 365, Office Online, SharePoint Online et Skype for business, présentes dans les versions antérieures à SNS 4.4.1, ne sont plus disponibles. Les règles de filtrage les utilisant deviennent inopérantes jusqu'au remplacement de ces catégories par les services Web introduits en version SNS 4.4.1.

- Mode furtif (*stealth* mode) - En configuration d'usine, un firewall SNS est désormais en mode furtif par défaut. Notez que la désactivation du mode furtif (*stealth* mode) impacte les performances de traitement des paquets. En effet, pour être en mesure de répondre à un message d'erreur ICMP, le firewall doit garder une trace de chacun des paquets. Le mode furtif permet donc au firewall de faire l'économie de toutes ces traces de paquets.

Vulnérabilités résolues de SNS 4.8.20 LTSB

Le niveau de sévérité de chaque vulnérabilité est indiqué dans son bulletin de sécurité publié sur le site https://advisories.stormshield.eu/.

Mise à jour de firmware - Installation de licence - Restauration de configuration

Des vulnérabilités ont été corrigées dans les modules de mise à jour de firmware, d'installation de licences et de restauration de configuration. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-031.

Enrôlement des utilisateurs

Une vulnérabilité a été corrigée dans la page d'enrôlement des utilisateurs. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-027.

Une vulnérabilité a été corrigée dans la page d'enrôlement des utilisateurs. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-026.

VPN IPsec

Des vulnérabilités ont été corrigées dans le moteur de gestion du VPN IPsec. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-028.

Logs VPN SSL

Une vulnérabilité a été corrigée dans les logs du VPN SSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-030.

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

Authentification Agent TS

Dans certaines configurations, la méthode d'authentification Agent TS peut ne pas être prise en compte si elle n'est pas située en tête de la liste des méthodes de la politique d'authentification. Ceci aboutit alors à une erreur d'authentification des utilisateurs de la méthode Agent TS.

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 4.8 ou supérieure.

La QoS implémentée 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.

Authentification - TOTP

Référence support 84686

La modification des paramètres avancés de l'authentification TOTP (**Durée de vie**, **Taille du code** et **Algorithme de hachage**) entraîne le dysfonctionnement de cette méthode d'authentification en cas d'utilisation conjointe avec les applications de génération de codes *Google Authenticator* et *Microsoft Authenticator*.
Un message d'avertissement a été ajouté pour inviter l'administrateur à vérifier la compatibilité des paramètres avancés avec l'application de génération de codes utilisée.

Routage multicast dynamique

Le routage multicast dynamique implémenté en version 4.8 présente les limitations suivantes :

- IGMPv1 n'est pas supporté,
- IGMP Snooping n'est pas supporté,
- PIM Dense Mode n'est pas supporté,
- PIM Sparse-Dense Mode n'est pas supporté,
- PIM BiDir n'est pas supporté,
- Multicast BGP Extension n'est pas supporté,
- MSDP (Multicast Source Discovery protocol) n'est pas supporté,
- AnycastRP n'est pas supporté,
- IPV6 et le protocole MLD (Multicast Listener Discovery) ne sont pas supportés,
- Il n'est pas possible d'activer simultanément le routage multicast statique et le routage multicast dynamique,
- Il n'y a pas de synchronisation des tables de routage multicast dynamique au sein de la HA,
- Les bridges et interfaces contenues dans un bridge ne peuvent pas être sélectionnés comme interfaces participant au routage multicast dynamique,
- Le protocole *Cisco AutoRP* n'est pas supporté,
- Un firewall SNS peut être intégré dans une infrastructure *Cisco AutoRP* lorsque les équipements *Cisco* sont configurés pour supporter les standards BSR,
- Dans une configuration HA, les interfaces participant au routage multicast dynamique doivent impérativement porter une adresse IP statique,
- Le moteur de prévention d'intrusion n'analyse pas le protocole PIM,
- Le nombre d'interfaces du firewall participant au routage multicast dynamique est limité à 31.

Services Web

L'utilisation des services Web dans la configuration du firewall nécessite l'activation de l'analyse du protocole DNS.

Support des *jumbo frames* sur les firewalls modèles SN160, SN210 et SN310

Bien qu'il soit possible de configurer la MTU des *jumbo frames* jusqu'à une taille de 9216 octets sur les firewalls SN160, SN210 et SN310, notez que les limitations matérielles de ces modèles impliquent une vérification logicielle des sommes de contrôle des paquets présentant une MTU supérieure à 1600 octets. Ceci peut donc impacter les performances globales de ces modèles de firewalls.

Firewalls équipés d'un TPM

Référence support 83580

Après une mise à jour en version SNS 4.8, les secrets stockés dans le TPM nécessitent d'être scellés. Cette action est réalisée à l'aide d'un assistant dédié dans l'interface graphique. Dans le cas d'un cluster HA, le rescellement du firewall passif se fait depuis l'interface graphique du firewall actif.

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

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

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.

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 dans l'ordre des interfaces 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.

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.

Interface Ethernet

Dans une configuration en haute disponibilité, si les nœuds du cluster communiquent via une interface Ethernet, celle-ci doit être dédiée à cet usage. L'utiliser comme interface parent d'une interface virtuelle d'un VLAN n'est pas supporté.

Interfaces VLAN

Dans une configuration en haute disponibilité, l'interface de communication entre les nœuds d'un cluster peut être isolée dans un VLAN. Dans ce cas, certaines fonctionnalités avancées liées à la communication des membres du cluster ne seront pas disponibles.

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.

RADIUS

Il n'est pas possible d'utiliser une authentification RADIUS sans mot de passe ("mode Push") avec SN SSL VPN Client version 4.0 et un SNS en version 4.8.4.

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).

Média 1000Base-LX

Lors de l'exécution de la commande `ifconfig`, une anomalie liée au pilote Intel fait apparaître à tort les médias 1000Base-LX comme des médias 1000Base-T. Ils sont cependant correctement pris en compte par le système et leur bon fonctionnement n'est pas affecté.

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 créées par l'équipe du support technique (Technical Assistance Center).

Installer cette version

Pour mettre à jour votre firewall en version SNS 4.8.20 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 Changements de comportement.

Notez que le mécanisme de mise à jour d'un firewall entraîne nécessairement un redémarrage automatique du firewall en fin de procédure.

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
4.3.23 LTSB ou inférieure	Version 4.3.24 LTSB recommandée, car la partition de secours du firewall serait inutilisable après un passage direct vers la nouvelle version
4.3.24 LTSB ou supérieure	Aucune

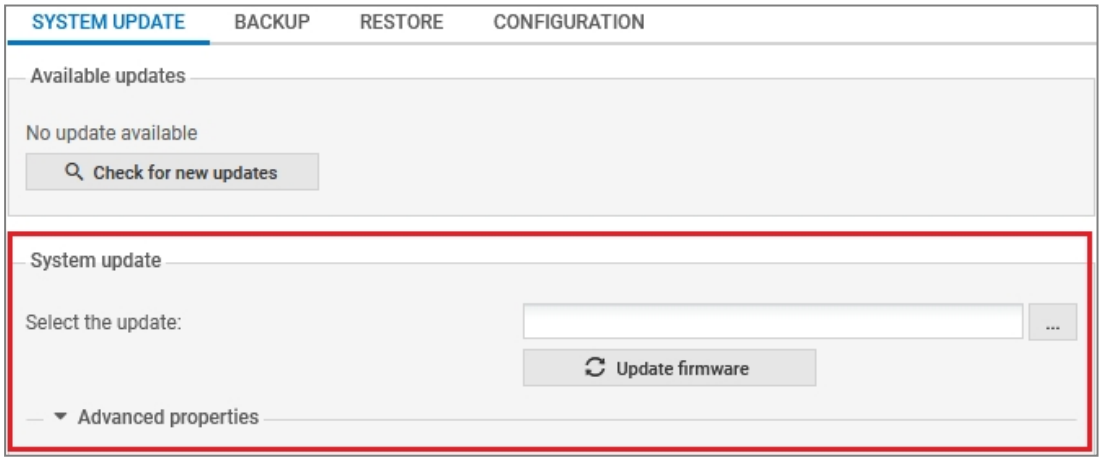
Télécharger la mise à jour

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 de 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, le firewall redémarre.
   Vous êtes déconnecté et invité à vous ré-authentifier une fois le firewall redémarré.
   Si un problème empêche la mise à jour, vous en êtes informé avant le lancement de l'opération.
4. Après le redémarrage du firewall, et pour vérifier que la mise à jour a bien été appliquée, connectez-vous à l'interface Web d'administration et rendez-vous dans l'onglet **Monitoring** > **Tableau de bord**.
   La version SNS installée est indiquée dans le champ **Version**.

Versions précédentes de SNS v4

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SNS v4.8 LTSB.

4.8.19 LTSB	Nouvelles fonctionnalités		Correctifs
4.8.18 LTSB		Vulnérabilités résolues	
4.8.17 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.16 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.15 LTSB	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.14 LTSB	Nouvelles fonctionnalités		Correctifs
4.8.13 LTSB	Nouvelles fonctionnalités		Correctifs
4.8.12 LTSB		Vulnérabilités résolues	Correctifs
4.8.11 LTSB			Correctifs
4.8.10 LTSB	Nouvelles fonctionnalités		Correctifs
4.8.9	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.8			Correctifs
4.8.7	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.6	Nouvelles fonctionnalités		Correctifs
4.8.5	Nouvelles fonctionnalités		Correctifs
4.8.4	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.3 EA	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.8.2 EA			Correctifs
4.8.1 EA	Nouvelles fonctionnalités		Correctifs
4.7.10	Nouvelles fonctionnalités		Correctifs
4.7.9		Vulnérabilités résolues	Correctifs
4.7.8			Correctifs
4.7.7	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.7.6	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.7.5	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.7.4			Correctifs
4.7.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.7.2 EA	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs

4.7.1 EA	Nouvelles fonctionnalités		Correctifs
4.6.11	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.6.10	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.6.9	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.6.8	Nouvelles fonctionnalités		Correctifs
4.6.7	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.6.6		Vulnérabilités résolues	Correctifs
4.6.5	Nouvelles fonctionnalités		Correctifs
4.6.4	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.6.3		Vulnérabilités résolues	Correctifs
4.6.2			Correctifs
4.6.1			Correctifs
4.6.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.5.4	Nouvelles fonctionnalités		Correctifs
4.5.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.5.2	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.5.1	Nouvelles fonctionnalités		Correctifs
4.4.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
4.3.x LTSB		Version 4.3 LTSB	
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

Nouvelles fonctionnalités et améliorations de SNS 4.8.19 LTSB

Amélioration de l'expérience utilisateur

Rapports

De nouveaux rapports sont disponibles dans le module **Monitoring** > **Rapports** :

- Top des connexions à des domaines Web ayant été déchiffrées par le proxy,
- Top des connexions à des domaines Web ayant entraîné une analyse antivirale,
- Top des connexions réalisées par des services Web au travers du proxy,
- Top des volumes de données consommées par les services Web au travers du proxy,
- Top des destinations déchiffrées par le proxy et pour lesquelles un service Web existe,
- Top des volumes de données consommées par ces flux,
- Top des sites Web les plus déchiffrés par le proxy,
- Top des sites Web les plus analysés par l'antivirus.

Shell NSRPC

L'action de décocher la case **Utiliser le shell nsrpc pour les administrateurs autres que le compte admin** entraîne l'affichage du message d'avertissement "L'accès en console des administrateurs leur octroie l'ensemble des droits d'administration et leur permet d'élever leurs privilèges sur le système, s'ils ont connaissance du mot de passe du super-administrateur".

Supervision via SNMP

STORMSHIELD-ASQ-STATS-MIB

Une description a été ajoutée à chaque OID de la MIB STORMSHIELD-ASQ-STATS-MIB pour une meilleure compréhension de son rôle.

STORMSHIELD-ROUTE-MIB

Pour améliorer la supervision SNMP du taux de perte de paquets au sein des objets routeur, trois OID au format INTEGER snsRouteUsagePrctRaw, snsRoutePacketLossPrctRaw et snsRouteUnreachPrctRaw ont été ajoutées à la MIB STORMSHIELD-ROUTE-MIB.

Les anciennes OID au format STRING, respectivement snsRouteUsagePrct, snsRoutePacketLossPrct et snsRouteUnreachPrct, sont toujours présentes dans cette MIB mais les valeurs qu'elles retournent sont marquées comme obsolètes.

Services Web personnalisés

Le mécanisme d'import de services Web prend désormais en charge les fichiers CSV au format UTF8 avec BOM (Byte Order Mark).

Correctifs de SNS 4.8.19 LTSB

Système

Filtrage et NAT

Référence support TAC-1565

Dans certains cas, un accès concurrent au cache pouvait empêcher une règle de filtrage de s'appliquer correctement. Ce problème a été résolu.

Tableau de bord

Référence support TAC-1460

Le lien permettant d'accéder au détail de la licence depuis le tableau de bord est de nouveau fonctionnel.

Tunnels GRE - Valeur de la Maximum Segment Size (MSS)

Référence support TAC-1214

Désormais, le firewall tient bien compte de la valeur de la MSS des paquets TCP traversant un tunnel GRE défini à l'aide de la commande :

```
sysctl -w net.inet.tcp.mssdflt=<valeur>.
```

Stockage

Référence support TAC-1167

La présence d'une carte SD / microSD défectueuse ne bloque plus le démarrage du firewall.

Routage multicast statique

Référence support TAC-1462

Les flux de routage multicast statique émis depuis un bridge sont désormais correctement reçus par les interfaces en dehors du bridge.

Réseau - Interfaces basées sur le pilote igc

Références support TAC-1559 - TAC-817

La connexion d'une interface de firewall basée sur le pilote igc, et forcée à une vitesse autre que 2,5 Gbit/s, sur un équipement compatible avec un débit de 2,5 Gbit/s ne provoque plus à tort la négociation du lien à 2,5 Gbit/s.

Certificats SSL

Référence support TAC-1725

L'authentification auprès d'un firewall SNS via certificat avec TLS 1.2 ne provoque plus d'erreur de protocole SSL avec certains navigateurs Web.

Vulnérabilités résolues de SNS 4.8.18 LTSB

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

VPN SSL

Des vulnérabilités de sévérité forte ont été résolues dans le VPN SSL. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-016.

Commandes CLI / Serverd

Une vulnérabilité de sévérité moyenne a été résolue dans le mécanisme des commandes CLI / Serverd. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-017.

Nouvelles fonctionnalités et améliorations de SNS 4.8.17 LTSB

Nouveau firewall modèle SNi50

La version de firmware 4.8.17 LTSB assure la compatibilité avec les nouveaux firewalls industriels SNi50.

Afin d'assurer une continuité de service dans les milieux industriels, le firewall SNi50 est équipé de deux bypass matériels qui permettent, une fois activés, de laisser passer le trafic réseau en cas de coupure électrique ou de défaillance du firewall.

Classification des URL

Désormais, les URL de catégories inconnues sont classées dans un rapport distinct, afin que les autres rapports de classification d'URL ne contiennent que des URL de catégories connues.

Serveurs DNS

Sur un firewall remis en configuration d'usine (*defaultconfig*), les serveurs DNS racine ne sont plus utilisés par défaut pour les requêtes DNS. Ce comportement peut être activé ou désactivé à l'aide de la commande CLI / Serverd `CONFIG DNS USEROOT state=on|off`.

En savoir plus sur la commande **`CONFIG DNS USEROOT`**.

Possibilité de descendre en version SNS 4.3.30 et supérieure

Il est désormais possible de descendre d'une version 4.8 (à partir de 4.8.17) à une version 4.3 (à partir de 4.3.30) à l'aide d'une configuration par clé USB. Le firewall doit ensuite être remis en configuration d'usine.

En savoir plus sur la Configuration initiale par clé USB.

Routage par politique de filtrage et routage statique

La priorité du routage par politique de filtrage (PBR) sur le routage statique peut être activée ou désactivée à l'aide de la commande CLI / Serverd `CONFIG SECURITYINSPECTION COMMON STATEFUL PBROverrideStatic=0|1`.

En savoir plus sur la commande **`CONFIG SECURITYINSPECTION COMMON STATEFUL`**.

Firewalls virtuels EVA - Support de *cloud-init*

À compter de la version SNS 4.8.17, les firewalls virtuels EVA supportent l'outil de configuration *cloud-init*.

Événements système - Haute disponibilité

Les informations de **Nom du nœud système** ont été ajoutées dans les événements système liés à la HA.

Vulnérabilités résolues de SNS 4.8.17 LTSB

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

Services Web

Une vulnérabilité de sévérité moyenne a été résolue dans la gestion des services Web. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-006.

VPN IPsec

Des vulnérabilités de sévérité moyenne ont été résolues dans le moteur de gestion du VPN IPsec. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-013.

OpenSSL

Des vulnérabilités de sévérité forte ont été résolues dans la bibliothèque OpenSSL. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-014.

Correctifs de SNS 4.8.17 LTSB

Système

VPN SSL - Authentification RADIUS

Référence support TAC-1065

Les groupes d'un utilisateur issu d'un serveur RADIUS sont désormais correctement récupérés lors d'une connexion de cet utilisateur via le VPN SSL.

VPN IPsec

Référence support TAC-1539

Des problèmes de fuite mémoire ont été corrigés dans le moteur VPN IPsec.

Référence support TAC-1464

Dans une configuration IPsec mobile avec authentification par certificat, lorsque le champ DN du certificat utilisateur contient des caractères non ASCII comme des caractères accentués, ces caractères ne sont plus remplacés à tort par des points d'interrogation lorsque les caractéristiques du certificat sont affichées dans les logs ou les retours de commandes en ligne `swanctl`.

Haute disponibilité (HA)

Référence support TAC-1260

Le stockage des clés SSH utilisées par la HA a été modifié afin d'éviter une désynchronisation de ces clés lors d'une restauration de configuration des firewalls.

Haute disponibilité (HA) - VPN IPsec

Référence support TAC-1466

Désormais, si une bascule se produit alors que :

- Des tunnels VPN IPsec sont actifs,
- Il n'y a pas eu de synchronisation,

les phases 2 des tunnels sont supprimées afin que les tunnels soient fermés.

Filtrage et NAT

Référence support TAC-1290

Les messages d'erreur remontés lors de l'échec du chargement d'une politique de filtrage ont été modifiés pour une meilleure compréhension de la cause de cet échec. Exemple : cas d'un groupe comportant un trop grand nombre d'objets.

Logs

Références support TAC-1413

Des fuites mémoire ont été corrigées dans le mécanisme de gestion des logs lors d'une connexion / déconnexion à un serveur Syslog.

Logs - Protocole SNMP

Référence support TAC-1131

Vous pouvez de nouveau activer le mode verbeux du protocole SNMP. Cette régression était apparue en version SNS 4.7.0.

Mécanisme de cache DNS

Référence support TAC-1272

Des améliorations ont été apportées au mécanisme de cache DNS afin de ne plus excéder les limites autorisées pour le firewall et provoquer un arrêt inopiné de l'envoi des requêtes DNS.

Supervision

Référence support TAC-440

La valeur maximale de la température de CPU acceptable est désormais lue une seule fois au démarrage du moteur de supervision.

Démarrage du firewall

Référence support TAC-1469

Les retours d'opérations de mise en place des permissions utilisateurs ne sont désormais plus redirigés vers le fichier `dmesg`, mais vers le fichier `/var/tmp/boot.result`, afin de ne plus ralentir inutilement la phase de démarrage du firewall.

Moteur de prévention d'intrusion

Authentification

Référence support TAC-1491

Des fuites mémoire ont été corrigées dans la gestion des utilisateurs utilisant le proxy explicite.

Interface Web d'administration

Supervision

Référence support TAC-1579

Désormais, dans **Supervision> Système > Historique**, les courbes **Espace utilisateur** et **Utilisations** ne sont plus inversées.

Filtrage URL / SSL

Référence support TAC-1347

Dans l'écran **Filtrage / NAT**, des ralentissements de plusieurs secondes pouvaient se produire lorsque la politique de filtrage affichée contient de nombreuses règles utilisant le filtrage URL / SSL. Ce problème est maintenant corrigé.

Nouvelles fonctionnalités et améliorations de SNS 4.8.16 LTSB

Logs - Authentification

Les logs affichent désormais les événements liés à l'échec d'authentification d'un administrateur lorsque le nombre maximal de sessions d'administration simultanées a été atteint.

Objets routeurs - Supervision des passerelles via ICMP

Référence support TAC-1077

Le nombre de passerelles pouvant être supervisées via ICMP a été doublé.

Vulnérabilités résolues de SNS 4.8.16 LTSB

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

Client NSRPC

Une vulnérabilité de sévérité faible a été résolue dans le client NSRPC. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2025-007.

Interface Web d'administration

Une vulnérabilité de sévérité moyenne a été résolue dans l'interface Web d'administration. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-003.

Authentification à l'interface Web d'administration

Des vulnérabilités de sévérité moyenne ont été résolues dans le module d'authentification à l'interface Web d'administration. Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2025-004,
- https://advisories.stormshield.eu/2025-005.

Authentification par certificat SSL

Une vulnérabilité de sévérité faible a été résolue dans le mécanisme d'authentification par certificat SSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-002.

curl

Une vulnérabilité de sévérité faible a été résolue dans la bibliothèque curl. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-010.

Correctifs de SNS 4.8.16 LTSB

Système

Réseau - Interfaces

Références support TAC-950

Des contrôles additionnels ont été ajoutés lorsqu'une interface utilisée dans la configuration est modifiée pour passer d'une configuration DHCP vers un adressage fixe.

VPN IPsec

Référence support TAC-582

La création via la console CLI d'une interface VTI utilisant le nom système <ipsec0> est désormais interdite afin d'éviter les conflits de nommage.

Haute disponibilité (HA)

Référence support TAC-1463

Les jetons de configuration caractérisant les délais d'attente lors d'un changement d'état d'une interface pour le calcul de qualité HA fonctionnent désormais correctement.

Références support TAC-1448 - TAC-1450

Les jetons de configuration <HAResyncBatchSize> et <HaResyncBatchDelay> peuvent désormais être ajoutés via la commande `setconf` dans la configuration d'une politique globale VPN IPsec (Global/VPN/XX).

Référence support TAC-572

Désormais, lorsque le mot de passe administrateur est modifié après la création du cluster HA, le firewall passif ne remonte plus d'alerte concernant le mot de passe.

Référence support TAC-1099

Les tâches de synchronisation liées à la HA ne sont plus activées à tort lors de la mise à jour de firmware. Cette régression était apparue en version SNS 4.8.0.

Configuration - Renommage d'un objet

Référence support TAC-987

Le renommage d'un objet présent dans des groupes imbriqués ne le supprime plus à tort de ces groupes.

Objets routeur

Référence support TAC-1338

Dans une configuration SD-WAN avec :

- Un objet routeur défini avec une passerelle nominale et une passerelle de secours,
- Les deux interfaces supportant ces passerelles adressées en DHCP.

L'interface supportant la passerelle active est désormais correctement mise à jour lors d'une bascule de passerelle et le moteur de prévention d'intrusion ne redémarre plus en boucle.

Mises à jour automatiques - Active Update

Référence support TAC-1400

La présence d'une exclusion dans la configuration du proxy externe n'empêche plus le fonctionnement du mécanisme de mises à jour automatiques.

Base de données des rapports

Référence support TAC-373 - TAC-1248

Désormais, la commande CLI / Serverd `REPORT RESET report=all` libère correctement l'espace alloué à la base de données.

Classification d'URL - Extended Web Control (EWC)

Référence support TAC-1601

La solution de classification d'URL EWC utilise désormais uniquement le serveur ewc.stormshieldcs.eu comme source de classification. Les requêtes manuelles depuis l'interface Web d'administration sont de nouveau fonctionnelles.

Supervision

Références support TAC-5 - TAC-1185

Un message indiquant qu'un composant physique retrouve un état "opérationnel" (messages du type "CPU health status recovered") n'est désormais généré que si un message de dégradation avait été préalablement envoyé pour ce composant.

Matériel

Firewalls modèle SN910

Référence support TAC-990

La mise à jour de certains firewalls modèle SN910 depuis une version strictement inférieure à SNS 4.7.0 vers une version SNS 4.8.16 ne rend plus ce firewall dysfonctionnel (état *amnesiac*) comme cela était le cas pour les versions SNS intermédiaires.

Moteur de prévention d'intrusion

Protocole TCP

Référence support TAC-1315

Lorsqu'un acquittement TCP contenant des données arrive en retard, il ne provoque plus la levée de l'alarme bloquante "Mauvais numéro de séquence TCP (ACK out of windows 2)" (alarme tcpudp:16) mais celle de l'alarme, non bloquante par défaut, "Numéro de séquence TCP incorrect sur ACK avec données" (alarme tcpudp:785).

Interface Web d'administration

VPN IPsec

Références support TAC-1494

Désormais, le calcul des positions des règles IPsec fonctionne correctement lorsqu'un filtre d'affichage est utilisé. Il n'y a plus de décalage lors de la suppression d'une règle.

Haute disponibilité (HA)

Référence support TAC-1164

Désormais, l'assistant de configuration HA ne propose plus les interfaces parentes de VLAN comme lien principal ou secondaire, car cette configuration n'est pas fonctionnelle.

Nouvelles fonctionnalités et améliorations de SNS 4.8.15 LTSB

Logs

Protocole SCTP

Référence support TAC-1343

Désormais, comme pour TCP et UDP, les logs SCTP comprennent les numéros et noms des ports source et destination.

Rattachement à un serveur Stormshield Management Center (SMC)

La configuration liée au rattachement du firewall à un serveur SMC peut désormais être réinitialisée à l'aide de la suite de commandes CLI / Serverd suivantes :

```
CONFIG FWADMIN DEFAULT
CONFIG FWADMIN ACTIVATE
```

Plus d'informations sur la commande **CONFIG FWADMIN**.

Remise en configuration d'usine - Commande *defaultconfig*

L'option -k de la commande `defaultconfig` supprime désormais les fichiers ne présentant aucun intérêt à être conservés suite à une remise en configuration d'usine du firewall, comme des fichiers d'états de haute disponibilité par exemple.

SNMP - Version du BIOS

La MIB STORMSHIELD-PROPERTY-MIB remonte désormais la version de BIOS.

Vulnérabilités résolues de SNS 4.8.15 LTSB

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

OpenSSL

Des vulnérabilités de sévérité moyenne ont été résolues dans le composant OpenSSL. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2026-001.

Correctifs de SNS 4.8.15 LTSB

Système

Tunnels GRE - Valeur de la Maximum Segment Size (MSS)

Référence support TAC-1214

La valeur de la MSS des paquets TCP traversant un tunnel GRE est désormais correcte.

Sauvegarde de la base de données des rapports

Référence support TAC-1028

La sauvegarde de la base de données des rapports peut être lente lorsque cette base dépasse une taille de l'ordre de 25 Mo, ce qui peut bloquer le processus de mise à jour du firewall. Un délai d'expiration de 60 secondes a été ajouté au mécanisme de sauvegarde afin de ne plus pénaliser la mise à jour du firewall.

Proxy - Antivirus

Référence support TAC-1257

L'analyse antivirale de messages utilisant des en-têtes spécifiques, créées par certains clients de messagerie, comme Fetchmail par exemple, fonctionne désormais correctement.

Classification d'URL

Référence support TAC-1356

L'arrêt du moteur de classification d'URL lorsque des URL sont en attente de classification ne provoque plus une interruption inopinée des connexions établies au travers du proxy.

Logs

Références support TAC-1250 - TAC-1277

Des problèmes de corruption mémoire ont été résolus afin d'éviter des blocages intempestifs du mécanisme de gestion des logs lors de l'envoi de données de télémétrie.

Mises à jour via Active Update

Référence support TAC-1151

La présence d'un objet global dans les serveurs Active Update n'empêche plus le bon fonctionnement de ce mécanisme de mise à jour.

Réseau - Interfaces

Référence support TAC-1320

Une interface configurée en DHCP et désactivée n'est plus présente dans les objets dérivés de l'interface : **Firewall_*nom_interface***, **Firewall_all**.

Supervision - Certificats, CA et CRL déployés via SMC

Référence support TAC-1399

Le module **Supervision** affiche désormais les alertes d'expiration pour les certificats, CA et CRL lorsqu'ils sont déployés via SMC.

Matériel

SNi20 - Stockage Disk-On-Module à interface SATA (SATADOM)

Référence support TAC-1263

Pour éviter d'éventuels dysfonctionnements, une mise à jour de firmware des SATADOM des firewalls modèle SNi20 est automatiquement appliquée lors de la mise à jour en version SNS 4.8.15.

Nouvelles fonctionnalités et améliorations de SNS 4.8.14 LTSB

VPN IPsec

Une colonne indiquant le Traffic Flow Confidentiality (TFC) a été ajoutée dans la grille des politiques IPsec. Cette colonne est masquée par défaut.

SNMP - STORMSHIELD-ALARM-MIB

L'OID (Object Identifier).1.3.6.1.4.1.11256.1.19.1.1.13 dans la MIB STORMSHIELD-ALARM-MIB permet désormais de connaître le niveau d'une alarme protocolaire, ICMP ou système :

- Valeur 1 pour une alarme majeure,
- Valeur 4 pour une alarme mineure.

Base objets

Références support 85742 - 85902

Le temps de synchronisation d'une base objets contenant un nombre important d'objets dynamiques a été réduit.

Routage dynamique

Commande système *netstat* et protocole de routage dynamique Open Shortest Path First (OSPF)

Références support 85271 - 86200

La commande `netstat -axp ospf` permet désormais d'afficher des informations concernant les statistiques de connexions liées au protocole de routage dynamique OSPF.

Protocole OSPF

Référence support 86200

Il est désormais possible de configurer la taille maximale des tampons (*buffers*) d'émission et de réception des sockets OSPF.

Authentification - RADIUS

Référence support 85699

Le NAS-Identifier est désormais personnalisable. Ceci permet d'utiliser le numéro de série du firewall comme NAS-Identifier par exemple. Pour réaliser cette modification, utilisez la suite de commandes CLI / Serverd :

```
CONFIG AUTH RADIUS CustomNasId=<string>
CONFIG AUTH ACTIVATE
```

Plus d'informations sur la **commande** `CONFIG AUTH RADIUS`.

Correctifs de SNS 4.8.14 LTSB

Système

Maintenance - Active Update

Référence support 85852

Le menu Active Update s'affiche désormais correctement même si tous ses mécanismes de mise à jour automatique sont désactivés.

Agent SNMP

Référence support 86131

L'agent SNMP ne renvoie plus à tort une notification de démarrage complet (*coldStart*) du firewall lors d'un simple redémarrage du démon SNMP du firewall.

Pages d'authentification du firewall

Référence support 85854

La directive CSP 'frame-ancestors' des pages Web d'authentification du firewall était incorrecte et a été corrigée.

Authentification RADIUS

Référence support 84385 - 85474

La tentative d'authentification RADIUS d'un client issu d'un groupe distribué par les Vendor Specific Attribute (VSA) n'échoue plus et ne provoque plus un arrêt inopiné du moteur de gestion de l'authentification du firewall.

Authentification - Annuaire LDAP interne

Référence support 86096

La présence de crochets "[" ou "]" dans la configuration d'un annuaire LDAP interne, par exemple dans un mot de passe, n'empêche plus le chargement de cet annuaire.

Haute disponibilité (HA) - Rapports

Références support 85511 - 85844

La synchronisation HA a été modifiée afin de ne plus déclencher d'erreur lorsque la partition contenant les rapports est remplie à plus de 50%.

Routage multicast dynamique

Référence support 85819

La valeur minimale du paramètre TTL (Time To Live) d'une interface impliquée dans le routage multicast dynamique était erronée et a été corrigée. Cette valeur est désormais égale à 1.

Référence support 86180

Dans une configuration utilisant un agrégat d'interfaces réseau IXL, le redémarrage du firewall ou le passage de l'état inactif à actif de l'agrégat ne bloque plus à tort le passage des paquets multicast au travers de cet agrégat.

Moteur de prévention d'intrusion

Multiple Spanning Tree Protocol (MSTP)

Référence support 86087

Dans une configuration utilisant des agrégats de liens (LACP) et du MSTP, le rechargement du filtrage générait à tort l'événement système "Changement de topologie STP". Ce problème a été corrigé.

Référence support 86087

Auparavant, une modification de la configuration MSTP provoquait une succession d'événements systèmes "Changement de topologie STP" dont la majorité était des faux positifs. Ce problème a été corrigé pour ne plus déclencher que les événements systèmes légitimes.

Interface Web d'administration

Groupes de services Web

Référence support 86248

Un message d'avertissement indique désormais que si les groupes de services Web créés via le module de commandes CLI ne sont pas visibles immédiatement dans l'interface Web d'administration, vous devez vous déconnecter puis vous reconnecter au firewall pour pouvoir les visualiser.

Logs - Journaux d'audit

Référence support 85622

L'action **Accéder à la règle de sécurité correspondante**, accessible via un clic droit sur une ligne de log, fonctionne désormais correctement lorsque le nom de la règle de filtrage est supérieur à 35 caractères.

Filtrage et NAT

Références support 86070 - 86193

Des optimisations ont été apportées au vérificateur de cohérence de la politique de filtrage afin de réduire le temps de rechargement de celle-ci et de son affichage dans l'interface Web d'administration lorsqu'elle contient de nombreux objets réseau. Cela permet également d'éviter des cas de déconnexion inopinée de l'interface d'administration.

Nouvelles fonctionnalités et améliorations de SNS 4.8.13 LTSB

VPN IPsec - Certificats

Référence support 85930

Afin de se conformer à la mention "Other methods of generating unique numbers are also acceptable" de la RFC 5280, les firewalls SNS sont désormais capables de vérifier des CRL récupérées localement pour les certificats générés avec des *SubjectKeyIdentifier* et *AuthorityKeyIdentifier*.

Interfaces virtuelles IPsec (VTI)

Une politique IPsec basée sur des interfaces virtuelles IPsec présentant l'une des configurations listées ci-dessous affiche désormais un message d'avertissement invitant l'administrateur à modifier cette configuration :

- Les sélecteurs de trafic sont des réseaux et non des adresses IP,
- Les sélecteurs de trafic distants et locaux ne sont pas situés dans le même sous-réseau IP,
- Des interfaces virtuelles identiques sont utilisées dans plusieurs règles de la politique.

Analyse sandboxing

Référence support 86046

Afin de ne pas surcharger les files d'attente de traitement, le firewall n'envoie plus vers l'infrastructure d'analyse sandboxing les e-mails sans pièces jointes ni les pièces jointes dont le type n'est pas supporté par le service de sandboxing.

Commande CLI / Serverd - SYSTEM PROPERTY

Désormais, la commande CLI / Serverd `SYSTEM PROPERTY` fournit la version du BIOS grâce au jeton de configuration `BIOSVersion`.

Droits d'accès aux données personnelles

Désormais, lorsque vous vous connectez au firewall avec un compte administrateur :

- Autre que le compte 'admin',
- Disposant du droit d'accès aux données personnelles,

et que vous accédez à un module contenant des données personnelles, une pop-up s'ouvre et vous demande si vous souhaitez prendre les droits d'accès aux données personnelles.

Correctifs de SNS 4.8.13 LTSB

Système

VPN SSL

Référence support 85904

La modification du port d'écoute du service VPN SSL affiche désormais un message indiquant la nécessité de redémarrer le firewall pour une prise en compte correcte du changement.

Mécanisme de bypass - Firewalls industriels SNi20 / SNi40

Le bypass ne se déclenchait plus en cas d'interruption inopinée du mécanisme de gestion matérielle du firewall. Ce problème est maintenant résolu. Cette régression était apparue en version SNS 4.8.7.

Redondance de serveurs SMC

Référence support 86112

En cas de coupure du serveur SMC principal, le firewall SNS se connecte au serveur secondaire. Auparavant, en cas de retour du serveur principal, aucune opération (déploiement, accès firewall, ...) ne pouvait être réalisée depuis ce serveur. Ce problème a été corrigé.

Liste des objets de type groupe

Référence support 86221

Dans la base objets, si le nombre de groupes à afficher est supérieur à 4096 entrées, les commentaires associés à chaque groupe n'étaient pas affichés. Ce comportement a été corrigé, via l'interface web ou lors d'un export de la liste des groupes au format CSV.

Machines virtuelles Pay As You Go (PAYG)

Référence support 86111

L'enrôlement de machines virtuelles PAYG fonctionne de nouveau correctement et n'affiche plus à tort un message indiquant que cet enrôlement était néanmoins réussi.

Mécanisme de récupération des listes de révocation de certificats (CRL)

Référence support 86153

Le mécanisme de récupération des CRL peut de nouveau établir ses connexions avec une IP source identifiée par <Firewall_nom_interface>.

Haute disponibilité

Références support 84970 - 85311 - 85657 - 85802

La synchronisation de certains fichiers au sein du cluster a été améliorée. Ceci évite la génération inappropriée de messages d'erreur dans le fichier de logs système en cas d'absence justifiée de certains de ces fichiers.

Restauration de configuration

Référence support 84995 - 85981 - 86070

Le rechargement de configuration consécutif à un déploiement SMC ou à une restauration de configuration a été optimisé.

Objets

Référence support 86070

Dans une configuration contenant un nombre important d'objets, l'affichage de la liste des objets dans l'interface Web d'administration pouvait prendre un temps significatif. Des optimisations ont été apportées pour diminuer ce temps d'affichage.

Supervision des disques - SNi20

Référence support 86265

Le module de supervision du matériel prend désormais en compte les disques modèle M2 pouvant équiper les firewalls modèles SNi20 et ne génère plus à tort une alerte indiquant qu'un disque est manquant.

Moteur de prévention d'intrusion

Protocole SCTP - Haute disponibilité (HA)

Référence support 85372

A chaque bascule HA, la date d'établissement d'une association SCTP était incrémentée d'une seconde. Ce problème a été résolu.

Interface Web d'administration

VPN SSL portail

Référence support 86186

Les serveurs avec un nom contenant une lettre majuscule ne sont plus affichés à tort comme étant désactivés. Cette régression était apparue en version SNS 4.8.0.

Vulnérabilités résolues de SNS 4.8.12 LTSB

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

CLI / Serverd

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

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2025-003/.

Correctifs de SNS 4.8.12 LTSB

Système

Routage

Référence support 85724

Un message d'avertissement est désormais affiché lors du rechargement de la politique de filtrage pour indiquer qu'une règle de routage par politique ne pourra pas être appliquée faute de route statique ou de route par défaut configurée sur le firewall.

Haute disponibilité (HA)

Référence support 86211

En cas de bascule au sein du cluster, les connexions TCP établies avec un *Window Scale Factor* (facteur d'échelle de fenêtre) important (supérieur à 8) ne sont pas reprises correctement par le nouveau firewall actif : celui-ci n'est pas capable de gérer correctement la quantité de données qu'il reçoit dans ces connexions TCP. En conséquence, des paquets de données sont bloqués par le firewall. Pour contourner ce problème, il est nécessaire de modifier le token *RecoveryToLite* qui a été ajouté à cet effet dans la section *[IPSConnection]* du fichier *ConfigFiles/Protocols/tcpudp/0x* à la valeur 1.

Veuillez noter que ce changement a pour conséquences d'ignorer les numéros de séquence et d'alléger l'analyse des paquets.

Proxy - Antivirus

Références support 85841 - 86055

Un problème pouvant provoquer le blocage du firewall lors de la mise à jour de la base antivirale a été corrigé.

Supervision des modules d'alimentation - Firewalls SN-S-Series-220/320

L'absence de module additionnel d'alimentation dans un firewall modèle SN-S-Series-220/320 ne provoque plus à tort une alerte indiquant qu'un module d'alimentation est défectueux.

Optimisation

Références support 85277

La gestion de la mémoire physique lorsque la Maximum Transmission Unit (MTU) est supérieure à 4000 octets a été optimisée.

Moteur de prévention d'intrusion

Gestion de connexions réparties sur des CPU multiples

Référence support 85947

Une anomalie a été résolue lors de la comparaison sur des intervalles de temps très courts d'ensembles de connexions ou de sessions UDP réparties sur plusieurs CPU. Cette anomalie pouvait entraîner des coupures de ces connexions.

Analyse protocolaire

Références support 85910 - 86013

Des problèmes ont été identifiés et corrigés dans le code du moteur de prévention d'intrusion. Ces problèmes pouvaient engendrer d'éventuels pertes de paquets.

Protocole TCP

Référence support 85929

L'utilisation de l'option **Activer l'ajustement automatique de la mémoire dédiée au suivi de données** associée à des options avancées du type TCP Selective ACKnowledgment (SACK) ne provoque plus à tort un débordement de la file de données, caractérisé par l'alarme bloquante "Débordement de la file de données TCP" (tcpudp:84).

VM PAYG

Référence support 85559

Les objets machines *enroll-sns.stormshieldcs.eu* et *accounting-sns.stormshieldcs.eu* utilisés dans les VM PAYG ont été ajoutés dans la configuration de SNS.

Matériel

Firewalls modèle SN170 - Protocole Profinet

Référence support 86082

Les paquets Profinet, utilisant le VLAN 0, sont désormais correctement pris en charge par un firewall utilisant le driver igc ou doté d'une interface IX,s et ne sont plus bloqués à tort.

Interface Web d'administration

Haute disponibilité - Liens redondants

Référence support 86154

Lors de la création d'un cluster possédant deux liens HA, les adresses IP du lien secondaire sont désormais correctement prises en compte.

Correctifs de SNS 4.8.11 LTSB

Système

Filtrage URL/SSL

Référence support 86204

Suite à la mise à jour en version SNS 4.8.10, si vous utilisiez la base d'URL embarquée dépréciée ou une base tierce (Université de Toulouse par exemple), il était impossible de créer ou de modifier les règles de filtrage URL et SSL. Ce problème a été corrigé. Ce problème n'impactait pas le fonctionnement des règles configurées avant la mise à jour en version SNS 4.8.10.

Nouvelles fonctionnalités et améliorations de SNS 4.8.10 LTSB

Nouveaux serveurs DNS

Les serveurs du fournisseur européen dns0 sont ajoutés aux objets machines des firewall, sous les noms *dns1.dns0.eu* et *dns2.dns0.eu*. Si les paramètres d'usine sont rétablis sur le firewall après la mise à jour en version SNS 4.8.10, les serveurs de dns0 seront utilisés par défaut. Les objets correspondant au service DNS de Google ne sont pas supprimés.

Commande CLI / Serverd - LIST

La commande CLI / Serverd `LIST` fournit désormais l'identifiant de l'utilisateur (UID) complet sous forme nomutilisateur@domaine.

Plus d'informations sur la commande `LIST`.

Script pour les firewalls EVA dans VMWare

Dans un environnement VMWare, il est désormais possible de définir un script "user-data" lors du déploiement d'un modèle OVF d'un firewall EVA dans vSphere Client.

Modification de l'hébergement du service Bitdefender de classification d'URL

Désormais, les requêtes de classification d'URL sont envoyées à un service Bitdefender hébergé par Stormshield et non plus directement sur les infrastructures Bitdefender. Dans une étape de transition jusqu'au 31 décembre 2025, les requêtes basculent sur le service hébergé chez Bitdefender après cinq requêtes infructueuses sur l'infrastructure Stormshield.

Correctifs de SNS 4.8.10 LTSB

Système

VPN IPsec

Référence support 85864

Désormais, dans une configuration avec des clients mobiles IPsec, le client avec la dernière adresse IP du réseau reçoit bien les attributs DNS.

Référence support 85770

Dans une configuration VPN IPsec utilisant des VTI, le rechargement de la configuration avec la commande CLI / SSH `ennetwork -f` pouvait entraîner le blocage du trafic dans les tunnels VPN. Ce problème a été corrigé.

Référence support 85940

Auparavant, il pouvait y avoir une duplication des associations de sécurité IKE si les correspondants essayaient de les renégocier en même temps, ce qui entraînait des problèmes de performance. Le calcul du moment de la renégociation a été modifié afin qu'il n'y ait plus de duplication.

Routage multicast

Référence support 85809

Auparavant, lorsqu'une route par défaut était configurée, l'envoi de trafic multicast dans un bridge provoquait une consommation CPU anormalement élevée. Ce problème a été corrigé.

EWC (Extended Web Control)

Référence support 86059

Auparavant, si l'IP configurée pour l'objet *ewc-sns.stormshieldcs.eu* ne correspondait pas à celle obtenue par résolution DNS, alors le service de filtrage d'URL EWC ne tenait pas automatiquement compte de l'IP obtenue par la résolution DNS. Ce problème a été corrigé.

Référence support 85849

L'adresse IP de l'objet *ewc-sns.stormshieldcs.eu* a été mise à jour dans la configuration du firewall.

Désormais, les licences EWC sont correctement reconnues et toutes les catégories d'URL s'affichent lorsque vous déroulez la liste de la colonne **Catégorie d'URL**.

Serveur LDAPS

Référence support 85766

L'utilisation d'un objet machine global pour configurer un serveur LDAPS telle qu'annoncée en version SNS 4.8.7 est désormais pleinement fonctionnelle.

Interface Web d'administration

Changement d'onglet dans le module Maintenance

Dans le module **Système** > **Maintenance**, une fenêtre pop-up s'affiche désormais si vous changez d'onglet après avoir fait des modifications afin de sauvegarder la nouvelle configuration.

Objets réseau

Référence support 86044

Auparavant, lorsque vous vérifiez l'utilisation d'un objet dans **Configuration** > **Configuration** > **Objets** > **Réseau**, puis cliquiez sur un identifiant de règle de **Filtrage et NAT** dans la panneau latéral, alors dans certains cas, une fenêtre avec un message d'erreur indiquant que la règle n'existait pas s'affichait et le panneau latéral ne fonctionnait plus. Ce problème a été corrigé.

Antivirus

Référence support 86144

Désormais, aucun message d'erreur concernant la licence de l'antivirus ne s'affiche lorsque vous paramétrez une règle avec l'antivirus. Ce message indiquait à tort que vous deviez souscrire une licence d'antivirus, alors que vous en possédiez déjà une et que l'antivirus était fonctionnel.

Droits en écriture

Référence support 86058

Auparavant, lorsqu'un firewall était administré par SMC, si un administrateur autre que le super-administrateur se connectait à l'interface Web d'administration sans passer par le mode proxy de SMC et demandait les droits en écriture, un message d'erreur s'affichait et il ne pouvait pas obtenir ces droits. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de SNS 4.8.9

Mise à jour des objets *updateX-sns.stormshieldcs.eu* et *licenceX-sns.stormshieldcs.eu*

Les adresses IP par défaut des objets dynamiques *updateX-sns.stormshieldcs.eu* et *licenceX-sns.stormshieldcs.eu* ont été mises à jour.

BACnet/IP

Désormais, dans le module **Configuration** > **Protection applicative** > **Protocoles**, vous pouvez mettre des services en liste noire et en liste blanche pour les couches BVLL et NPDU pour le protocole **BACnet/IP**.

Pour plus d'informations, reportez-vous à la section BACnet/IP du *Manuel utilisateur SNS*.

SNMP

Il est désormais possible d'interroger le firewall sur l'OID (Objects Identifiers)1.3.6.1.2.1.1.2 afin d'en connaître le modèle.

Une nouvelle table SNMP *snsMemUsageTable* est disponible avec l'OID 1.3.6.1.4.1.11256.1.10.10. Elle donne des informations sur les consommations de mémoire sous forme de pourcentage.

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

Vulnérabilités résolues de SNS 4.8.9

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

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/2024-029/.

Correctifs de SNS 4.8.9

Système

Proxy

Auparavant, l'analyse sandboxing (Breach Fighter) de fichiers avec un nom long pouvait entraîner des arrêts inopinés du proxy. Ce problème a été corrigé. Cette régression était apparue en version SNS 4.8.3.

Référence support 84388

La gestion des connexions du proxy a été améliorée. Désormais, le proxy utilise le pool de connexions propre au protocole avant d'utiliser le pool de connexions commun, ce qui évite d'avoir des erreurs indiquant qu'il y a trop de connexions alors que le nombre limite de connexions n'est pas atteint.

VPN IPsec

Référence support 85641

Lors de la renégociation d'une association de sécurité IKE, les informations d'authentification sont désormais transférées sur la nouvelle association de sécurité et le moteur de prévention d'intrusion ne coupe plus la connexion.

Référence support 84803

Les tunnels VPN sont de nouveau négociés quand le certificat du correspondant est modifié. Cette régression était apparue en version SNS 4.8.0.

VPN SSL

Référence support 84495 / 84933 / 85038 / 85081 / 85213

Des modifications ont été apportées au chargement de la configuration du VPN SSL afin de réduire le nombre d'accès disque.

Certificats et PKI

Référence support 85968

Auparavant, lorsqu'une sous-autorité de certification et son autorité parente avaient toutes deux des CRLDP, seule la CRL de l'autorité parente était téléchargée. Ce problème est maintenant corrigé et le firewall télécharge bien les deux CRL.

Référence support 85948

La commande CLI / Serverd `PKI SCEP QUERY` prend désormais correctement en compte les arguments *bindaddr* et *bindport* permettant de préciser respectivement une adresse IP locale et un port local spécifiques pour les requêtes SCEP.

Plus d'informations concernant la commande **`PKI SCEP QUERY`**.

Haute Disponibilité

Référence support 85747

Désormais, rattacher un cluster à SMC version 3.2.3 et supérieure ou forcer la récupération des informations d'un firewall du cluster ne provoque plus de logs d'erreur.

MIB STORMSHIELD-HA-MIB

Désormais, vous recevez une réponse lorsque vous interrogez la MIB STORMSHIELD-HA-MIB sur les tables :

- snsNodePowerSupplyTable,
- snsNodeDiskTable,
- snsNodeCpuTable,
- snsNodeFanTable.

TPM

Dans le cas d'un firewall administré par SMC, la mise à jour vers une version SNS 4.8.9 ou supérieure est bloquée si les conditions suivantes sont réunies :

- La clé privée du certificat utilisé pour les communications avec le serveur SMC est protégée par le TPM,
- Le firewall est en version SNS 4.8.2 ou inférieur.

Cela évite de perdre la connexion entre SMC et le firewall.

TPM - VPN IPsec/VPN SSL

Référence support 86126

Il n'est désormais plus nécessaire de resceller le module TPM lorsque les certificats utilisés pour les services VPN IPsec et VPN SSL sont protégés par le TPM. Ce comportement était apparu en version 4.8.7.

Cette situation provoquait à tort l'affichage du message d'erreur "Échec de l'accès à la clef symétrique" dans le tableau de bord.

Serveur LDAP

Référence support 86089

L'utilisation d'un objet machine global pour configurer un serveur LDAP telle qu'annoncée en version SNS 4.8.7 est désormais pleinement fonctionnelle.

Routage multicast

Référence support 85614

Auparavant, si dans une configuration en routage multicast, le câble réseau entre un firewall en position *Last Hop Router* (LHR) et un routeur utilisé en *Rendez-vous Point* (RP) était débranché ou que le routeur redémarrait, le flux était coupé. Ce problème a été résolu.

Extended Web Control (EWC)

Une nouvelle règle implicite a été ajoutée afin de garantir l'accès au serveur Extended Web Control (EWC) lorsque l'on force l'adresse source avec l'argument *bindaddr* d'une commande CLI / Serverd. L'ajout de cette règle implicite empêche désormais le flux de passer par le moteur de prévention d'intrusion. Cette nouvelle règle est visible dans le module **Configuration > Politique de sécurité > Règles implicites**.

Machines virtuelles

Configuration en haute disponibilité (HA) et Pay As You Go (PAYG)

Référence support 85730

Le mécanisme de gestion des licences au sein du cluster a été amélioré afin de permettre au firewall passif de récupérer sa licence par synchronisation avec le firewall actif lors de l'enrôlement Pay As You Go du cluster.

Moteur de prévention d'intrusion

Connexions TCP

Référence support 85712

Dans certaines connexions TCP empruntant le proxy, le moteur de prévention d'intrusion pouvait envoyer en boucle des paquets ACK, quelle que soit la réponse reçue. Désormais, une limite de 10 réémissions permet d'éviter cette boucle.

Protocole OPC UA

Le contrôle de NodeID par le moteur d'analyse protocolaire OPC UA a été modifié afin de se conformer aux spécifications du protocole et ne plus provoquer de blocage injustifié de paquets OPC UA valides.

NAT

Auparavant, lorsque des connexions filles échouaient, le moteur de prévention d'intrusion ne libérait pas correctement les ports utilisés par le NAT. Ce problème est corrigé. Cette régression était apparue en versions SNS 4.8.0.

Gestion des utilisateurs

Référence support 85999

Auparavant, lors du vidage des connexions, une recherche était effectuée afin de relier les IP sources des connexions à des utilisateurs éventuels. La recherche d'utilisateur est désormais effectuée à la création de la connexion afin d'éviter des temps de latence. Cette régression était apparue en version SNS 3.4.0.

BIRD

Référence support 86033

Il est de nouveau possible d'utiliser des CIDR à la place des noms d'interface dans la configuration de BIRD. Cette régression était apparue en 4.8.1

Référence support 84495 / 84933 / 85038 / 85081 / 85213

Le mécanisme de mise à jour des adresses protégées a été optimisé afin de réduire le nombre d'accès disque.

Référence support 86007

Une limite de caractères de la mémoire tampon concernant le nom des interfaces pouvait empêcher de modifier la configuration de BIRD s'il y avait trop d'interfaces. Ce problème a été résolu.

Interface Web d'administration

TPM

Référence support 86093

Désormais, dans le module **Configuration** > **Objets** > **Certificats et PKI**, l'option d'initialisation du TPM ne s'affiche plus lors d'un clic droit sur un certificat si votre firewall ne dispose pas du module TPM.

Correctifs de SNS 4.8.8

NOTE
Annoncé dans les Notes de version 4.8.7, le correctif concernant les limites d'hôtes sur le firewall SNS a été supprimé. Il sera revu et réintégré dans une version ultérieure.

Firewalls virtuels EVA

Déploiement

Référence support 86050

Le déploiement d'un EVA sur les hyperviseurs Microsoft Hyper-V et KVM fonctionne désormais correctement. Cette régression était apparue en version SNS 4.8.4.

Nouvelles fonctionnalités et améliorations de SNS 4.8.7

VPN IPsec

Référence support 85633

Vous pouvez désormais forcer un firewall à rester *responder* pendant toute la durée de vie du tunnel VPN IPsec grâce au token `reauth=2` des commandes CLI / Serverd `CONFIG IPSEC PEER NEW` et `CONFIG IPSEC PEER UPDATE`.

Plus d'informations sur les commandes **`CONFIG IPSEC PEER NEW`** et **`CONFIG IPSEC PEER UPDATE`**.

Détection des algorithmes de hachage obsolètes

Désormais, un certificat signé avec un algorithme de hachage obsolète (SHA1 et MD5) ou par une CA signée avec un algorithme de hachage obsolète est signalé :

- Par un message d'avertissement dans le tableau de bord,
- Par une alerte au niveau du certificat dans **Configuration** > **Objets** > **Certificats et PKI**.

Répartition de charge du chiffrement IPsec - Firewalls équipés de cartes réseau 2,5 Gbe

Le mécanisme de répartition de charge du chiffrement IPsec est désormais compatible avec les firewalls équipés de cartes réseau 2,5 Gbe.

Mise à jour de la mémoire non volatile (NVM) des cartes réseau 2,5 Gbe i226

Référence support 85329

La mémoire non volatile (NVM) des cartes réseau 2,5 Gbe i226 a été mise à jour.

Vous pouvez désormais activer l'option d'optimisation énergétique d'Ethernet. Pour ce faire, rendez-vous dans le module **Configuration** > **Réseau** > **Interfaces**, puis dans l'onglet **Configuration avancée** de l'interface que vous souhaitez configurer et cochez la case **Activer la norme IEEE 802.3az (EEE)**.

Cette mise à jour permet également la gestion des interconnexions entre des ports 2,5Gb/s et 100Mb/s.

Trusted Platform Module (TPM)

Le fonctionnement du TPM a été amélioré : la politique de scellement du module TPM ne tient plus compte de l'empreinte du Platform Configuration Register (PCR) liée à la séquence de démarrage du firewall SNS. La procédure d'initialisation du TPM a été revue et s'effectue désormais à l'aide d'un assistant dédié dans l'interface graphique. Dans le cas d'un cluster HA, le rescellement du firewall passif se fait depuis l'interface graphique du firewall actif. Il est recommandé de sceller le TPM pour profiter de la nouvelle politique de scellement.

Pour plus d'informations, reportez-vous à la note technique **Configurer le module TPM et protéger les clés privées de certificats du firewall SNS**.

BACnet/IP

Désormais, dans le module **Configuration** > **Protection applicative** > **Protocoles**, vous pouvez mettre des services en liste noire et en liste blanche pour les couches BVLL et NPDU pour le protocole **BACnet/IP**.

Vulnérabilités résolues de SNS 4.8.7

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

OpenSSL

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

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-035/.

Routage multicast

Une vulnérabilité de sévérité moyenne a été corrigée dans le mécanisme du routage multicast.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2025-002/.

Correctifs de SNS 4.8.7

Système

Proxy

Référence support 85644

Auparavant, un problème pouvait empêcher le nettoyage des connexions proxy et pouvait amener à une saturation de celles-ci. Désormais, lorsqu'une connexion du proxy se termine, elle est purgée automatiquement au bout de 10 secondes.

Proxy TLS

Référence support 85895 / 85961

La mise en cache des sessions dans le proxy TLS provoquait parfois des arrêts inopinés du proxy ou une consommation mémoire excessive. Ce problème a été corrigé.

VPN SSL Portail

Référence support 85899

Il est de nouveau possible d'accéder au portail VPN SSL lorsqu'un seul serveur est configuré. Cette régression était apparue en version SNS 4.8.0.

OpenVPN

Référence support 85690

Auparavant, lorsqu'OpenVPN cherchait un groupe d'autorités de certification (CA), il utilisait un chemin temporaire, ce qui pouvait provoquer une erreur au redémarrage. Il utilise désormais un chemin pérenne.

Référence support 85842

Auparavant, les fichiers temporaires contenus dans le dossier */var/tmp/Openvpn/* n'étaient pas supprimés, ce qui pouvait à terme empêcher d'établir des tunnels VPN, car le nombre maximum de fichiers dans un dossier était atteint. Désormais, les fichiers sont bien supprimés.

VPN IPsec

Référence support 85831

Désormais, la limite du nombre de tâches du moteur de gestion des tunnels VPN IPsec n'est valable que lorsque la protection contre les attaques par déni de service (DoS) est activée. De plus, le moteur n'a plus besoin d'être redémarré lorsque cette limite est atteinte.

Référence support 85717

Lorsque des tunnels VPN IPsec utilisant des interfaces virtuelles (VTI) étaient déployés via SMC, ils étaient négociés avant la fin du déploiement et n'étaient pas fonctionnels. Ce problème a été corrigé.

Certificats et PKI

Le firewall vérifie désormais correctement le contenu de l'extension *basicConstraints* du certificat d'une autorité de certification (CA).

Une option de configuration permet d'autoriser ou non l'import d'une CA pour laquelle cette extension n'a pas de valeur : il s'agit du jeton de configuration `StrictCACheck`, présent dans le fichier **ConfigFiles** > **system**. L'import d'une telle CA est autorisé lorsque la valeur 0 est affectée à ce jeton.

Longueur du complément d'alarme du log *l_alarm*

Référence support 85621

Désormais, le nombre de caractères maximum du complément d'alarme dans les logs *l_alarm* est de 512 caractères. Des points de suspension sont ajoutés à la fin du complément s'il est tronqué.

Serveur LDAPS

Référence support 85766

Vous pouvez désormais utiliser un objet machine global pour configurer un serveur LDAPS.

Port d'accès au serveur d'administration web du firewall

Référence support 85510

Désormais, lorsque vous modifiez le port d'accès au serveur d'administration web du firewall :

- Pour un port inférieur à 1024 alors qu'il était auparavant supérieur à 1024,
- Pour un port supérieur à 1024 alors qu'il était auparavant inférieur à 1024,

Le nouveau port configuré n'est pris en compte qu'après redémarrage du firewall. Un message dans le bandeau supérieur et sous forme de notification vous indique qu'un redémarrage est nécessaire pour appliquer la nouvelle configuration.

Bypass

Référence support 85358

L'interruption de connexion lors de la ré-alimentation d'un firewall avec le mode *bypass* activé dure à présent six secondes ou moins.

Filtrage et NAT

Référence support 85713

Auparavant, certaines politiques de filtrage fonctionnelles en versions SNS 3.11 ne se chargeaient plus en version SNS 4.8, ce qui bloquait les flux transitant par le firewall. Désormais, la politique de filtrage se charge, mais un message d'avertissement s'affiche dans le validateur de configuration du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**.

Référence support 85677

Lorsqu'IPv6 est activé, une erreur dans le mécanisme d'optimisation des règles de filtrage pouvait rendre certaines règles de filtrage inopérantes. Ce problème a été corrigé.

PKI

Référence support 85798

Le DN d'un certificat créé avec la commande `PKI EST QUERY` et le DN d'un certificat créé avec les commandes `PKI CERTIFICATE CREATE`, `PKI REQUEST CREATE` et `PKI CA CREATE` sont désormais encodés avec le même encodage, ce qui améliore la compatibilité avec les caractères spéciaux ou les logiciels PKI tiers.

Serveur de sauvegarde

Référence support 86010

Le nom de l'objet utilisé comme serveur de sauvegarde peut désormais compter jusqu'à 255 caractères.

Haute Disponibilité (HA)

Référence support 85781 / 85949

Désormais, l'utilisation de l'interface d'administration d'un firewall dans un cluster en Haute Disponibilité ne déclenche plus le clignotement intempestif de l'icône de synchronisation de configuration. Cette régression était apparue en version SNS 4.8.1.

Haute disponibilité - Optimisation du basculement

Référence support 85773

Désormais, lorsque la case **Redémarrer toutes les interfaces pendant le basculement (à l'exception des interfaces HA)** est cochée, seules les interfaces contenues dans un bridge redémarrent.

TPM

Référence support 85600

Désormais, un firewall avec le TPM activé et administré par SMC ne perd plus la communication avec SMC lorsqu'un package de rattachement est réimporté.

Indicateur de santé TPM

Référence support 86012

L'indicateur de santé TPM est de nouveau fonctionnel. Cette régression était apparue en version SNS 4.8.5.

Fuite mémoire

Référence support 86009

Pour les firewalls administrés par SMC, un problème de fuite mémoire a été corrigé. Cette régression était apparue en version SNS 4.8.4.

Routage multicast

Référence support 85614

Auparavant, un firewall qui recevait un flux multicast d'un routeur PIM utilisé en RP et qui perdait la connexion avec ce routeur ne transmettait plus le flux après avoir été reconnecté au routeur. Ce problème a été résolu.

Machines virtuelles *Pay As You Go* (PAYG)

Référence support 85987

Depuis la version SNS 4.8.0, une machine virtuelle PAYG dont la licence était expirée ne pouvait plus établir plus de 1000 connexions même après le renouvellement de sa licence. Ce problème a été corrigé.

Moteur de prévention d'intrusion

Liste noire

Référence support 85782

Désormais, le nombre limite d'adresses IP en liste noire est respecté et ne peut plus être dépassé.

Connexions IPS

Référence support 85716 / 85718

En cas d'utilisation d'un ou plusieurs sous-réseaux, le moteur de prévention d'intrusion n'empêche plus les connexions IPS lorsque l'alarme protocolaire "Paquet avec destination sur la même interface" (*ip:95*) est en **Autoriser**.

Protocole DCERPC

Référence support 85661

Auparavant, lorsque des connexions enclenchées avec le protocole DCERPC échouaient, le moteur de prévention d'intrusion ne libérait pas correctement les ports. Ce problème a été corrigé.

Hôtes

Auparavant, la limite des hôtes réservés et des hôtes de manière générale était la même, ce qui pouvait impacter les performances du firewall. Ce problème a été corrigé.

Mode *broadcast*

Référence support 85763

La gestion des paquets fragmentés transmis sur un bridge mode *broadcast* a été améliorée afin qu'il n'y ait plus de blocage.

Interface Web d'administration

Profils d'inspection

Vous pouvez désormais de nouveau renommer, copier et éditer les profils d'inspection dans l'onglet **Configuration générale** du module **Configuration > Protection applicative > Profils d'inspection**.

De plus, un onglet **Profils** permet de visualiser les profils et les protocoles qui leur sont associés.

Protocoles - Filtrage dans l'onglet Analyse Sandboxing

La fonction de filtrage dans l'onglet **Analyse Sandboxing** des protocoles HTTP / SMTP / POP3 et IMAP et dans la grille des autorités de certification du protocole SSL est de nouveau fonctionnelle. Cette régression était apparue en version SNS 4.8.0.

Trafic réseau

Référence support 85937

Il est de nouveau possible de mettre une adresse IP en liste noire en faisant un clic-droit dessus dans le module **Monitoring > Trafic réseau**.

Impression des informations d'un compte temporaire

Référence support 85946 / 85962

Le contenu de la page d'impression des informations d'un compte temporaire est de nouveau lisible. Cette régression était apparue en version SNS 4.8.0.

VPN SSL Portail

Référence support 85920

Désormais, lorsque l'option **Uniquement l'accès aux serveurs applicatifs** du module **Configuration > VPN > VPN SSL Portail** est cochée, le VPN SSL reste activé. Cette régression était apparue en version SNS 4.8.0.

Interface DHCP en statique

Référence support 85534

Il est désormais impossible de passer une interface DHCP en statique alors qu'un objet nom DNS ou Firewall_ifname_router associé est utilisé dans une règle de filtrage ou de NAT, car cela avait pour conséquence d'empêcher le firewall de charger une politique de filtrage ou de NAT.

Nouvelles fonctionnalités et améliorations de SNS 4.8.6

Alimentation

Référence support 85754

Pour les modèles de firewall suivants :

- SN-L-Series-2200 et SN-L-Series-3200,
- SN1100,
- SN2100,
- SN3000,
- SN3100,
- SN6100,

il est désormais possible d'obtenir des informations sur l'alimentation du firewall, même si celle-ci est défaillante. Ces informations sont accessibles avec la commande CLI / Serverd :

```
MONITOR POWER
```

Plus d'informations sur la commande **MONITOR POWER**.

Correctifs de SNS 4.8.6

Système

Limite du nombre d'objets de réputation IP

Référence support 85733

La limite du nombre d'objets de réputation IP, qui inclut les services Web, les services Web personnalisés et les groupes de réputation IP, a été augmentée et adaptée à chaque modèle de firewall.

GRETAP et bridge

Référence support 85957

Le gestionnaire de configuration réseau ne s'arrête plus inopinément lorsqu'il y a une interface GRETAP dans un bridge. Cette régression était apparue en version SNS 4.8.4.

Ventilateurs SN-L-Series-2200 et SN-L-Series-3200

Référence support 85744

Les deux ventilateurs non utilisés des SN-L-Series-2200 et SN-L-Series-3200 ne sont plus pris en compte par la surveillance. Ils ne remontent donc plus d'alertes à tort.

Ordonnancement des modules SN-XL-Series-5200 et SN-XL-Series-6200

Les modules des SN-XL-Series-5200 et SN-XL-Series-6200 sont de nouveau ordonnés correctement (1 à 8 de gauche à droite et de haut en bas). Cette régression était apparue en version SNS 4.8.3.

Authentification par la méthode Agent SSO

Référence support 85959 / 85960

Un problème de récupération de groupes et d'utilisateurs lors de l'utilisation de l'authentification par la méthode Agent SSO a été résolu. Cette régression était apparue en version SNS 4.8.0.

Interface Web d'administration

Certificats et PKI

Référence support 85731

Dans le module **Configuration > Objets > Certificats et PKI**, le type de certificat est désormais pris en compte s'il est indiqué manuellement par l'utilisateur. Cette régression était apparue en version SNS 4.7.0.

Administrateurs - Compte *admin*

La clé privée et la clé publique du compte super-administrateur (compte *admin*) sont désormais exportées dans fichier au format texte (.txt) et non plus au format CSV.

Nouveau groupe ou utilisateur

Référence support 85813

Désormais, dans le module **Configuration** > **Utilisateurs** > **Utilisateurs**, un utilisateur ou un groupe tout juste créé apparaît lors de la configuration d'un utilisateur ou d'un groupe déjà existant.

Nouvelles fonctionnalités et améliorations de SNS 4.8.5

Accès réseau Zero Trust (ZTNA) - Contrôle de conformité des postes clients

Dans **Configuration >VPN > VPN SSL > Vérification des postes clients (ZTNA)**, l'option **Autoriser l'établissement de tunnels pour des clients VPN SSL Stormshield Linux ou Mac** a été ajoutée. Si vous cochez cette case, les critères spécifiques Windows ne sont pas pris en compte pour les postes clients avec un client VPN SSL Stormshield Linux ou Mac (disponibles prochainement).

Certificate Revocation Lists (CRL) expirées

Référence support 85690

Désormais, un message d'avertissement dans le widget Message du tableau de bord vous avertit lorsque la configuration autorise l'établissement d'un tunnel VPN SSL avec une CRL expirée.

Type par défaut de clé NTP

Désormais, lors de l'ajout d'une clé NTP, le type de clé par défaut est SHA256.

VPN IPsec

Référence support 85633

Le jeton de configuration *IkeDeleteDelay* peut désormais être configuré directement avec la commande CLI / serverd :

```
CONFIG IPSEC UPDATE
```

Ce jeton permet de définir un délai en secondes entre la demande d'arrêt d'une association de sécurité IKE et son arrêt effectif lors d'une réauthentification. Le jeton accepte une valeur de 0 à 20.

VPN SSL

Désormais, si la compression est activée sur le firewall, une fenêtre s'affiche lorsque vous accédez au module **VPN SSL** vous informant qu'il est vivement conseillé de désactiver la compression pour des raisons de sécurité.

Il est possible de consulter et de changer l'état de la compression (activée ou désactivée) avec les commandes CLI / serverd :

```
CONFIG OPENVPN SHOW
CONFIG OPENVPN UPDATE compress=<0|1>
```

Plus d'information sur les commandes `CONFIG OPENVPN SHOW` et `CONFIG OPENVPN UPDATE`

Correctifs de SNS 4.8.5

Système

VPN SSL

Il est de nouveau possible pour les utilisateurs d'établir leur tunnel VPN en s'authentifiant avec des services externes (mode Push) lorsque la fonction *HostChecking* est activée. Cette régression était apparue en version SNS 4.8.3.

Haute disponibilité (HA)

Référence support 85551

Le firewall passif ne tente plus de lancer la tâche de récupération des CRL. Celle-ci est en effet réalisée régulièrement par le firewall actif et les CRL ainsi récupérées sont immédiatement synchronisées avec le firewall passif.

Supervision de la date de validité des Certificate Revocation Lists (CRL)

Référence support 85624

Le mécanisme de supervision de la date de validité des CRL n'émet plus d'alertes mineures pour des CRL dont la durée de vie initiale est inférieure à 24 heures. Ces alarmes étaient émises toutes les 3 heures.

Services Web

Référence support 85853

Désormais, dans un groupe de services Web contenant déjà un service Web, l'utilisation de la barre de recherche pour ajouter un nouveau service Web ne supprime plus le service Web déjà présent. Cette régression était apparue en version SNS 4.8.0.

Serveur de configuration par commande (serverd)

Référence support 84546/84672

Lors de la consultation des modules **Logs - Journaux d'audit**, le serveur de configuration par commande (serverd) pouvait s'arrêter inopinément. Ce problème a été résolu.

Alarmes

Référence support 85900

Des alarmes indiquant le retour à la normale de certains indicateurs de santé étaient systématiquement générées au démarrage du firewall même en l'absence d'anomalie. Cette régression, apparue en version SNS 4.8.4, a été corrigée.

Sauvegarde

Dans le cas d'un firewall disposant d'un module TPM, le message d'erreur en cas de mauvais mot de passe TPM lors d'une sauvegarde a été reformulé pour être plus explicite.

Moteur de prévention d'intrusion

Routage dynamique BIRD

Référence support 84579

Désormais, seules les routes que BIRD envoie au noyau sont récupérées dans la table des adresses réseaux protégées.

Interface Web d'administration

VPN IPsec

Dans **Monitoring** > **Supervision** > **Tunnels VPN IPsec**, les valeurs des champs **État** et **Rôle** de la zone **Association de sécurité** sont désormais correctement traduites.

Protocole TCP-UDP

Dans **Configuration** > **Protection applicative** > **Protocoles** > **TCP-UDP**, la zone **Support** est désormais correctement traduite.

Routes de retour

Référence support 858111

Dans **Configuration** > **Réseau** > **Routage** > **Routes de retour IPv4 / IPv6**, il n'est désormais plus possible de choisir une interface USB / Ethernet (modem 4G) dans le champ **Interface** de la route de retour.

Administrateur

Référence support 85474

Il est désormais possible de laisser le champ **Nom de domaine** vide ou d'indiquer *none* lors de la création ou la modification d'un administrateur.

Objet temps

Référence support 85805

Désormais, la création, la modification et l'utilisation d'un objet temps personnalisé ne provoque plus d'erreur. Cette régression était apparue en version SNS 4.8.0.

Nouvelles fonctionnalités et améliorations de SNS 4.8.4

Certificats et PKI

Dans l'écran **Objets** > **Certificats et PKI**, la zone **Empreintes** a été renommée **Détails** et trois nouveaux champs ont été ajoutés : **Type de clé**, **Taille de la clé** et **Extended Key Usage**.

Le firewall vérifie désormais que le certificat associé à une CRL possède effectivement le droit de signer des CRL (présence du *keyUsage* "crlSign").

Filtrage et NAT

Dans l'onglet **Action** de la fenêtre d'édition d'une règle de filtrage du module **Filtrage et NAT**, une icône d'information vous avertit qu'un niveau de trace autre que standard peut provoquer une surcharge de logs.

Analyse Sandboxing

Référence support 85532

Des optimisations ont été apportées pour réduire le nombre de fichiers envoyés en analyse Sandboxing et limiter le risque de saturation de la file d'attente.

Chiffrement

Des améliorations ont été apportées au binaire de vérification des fonctions cryptographiques (*cryptotest*). Lorsque cet utilitaire est lancé en mode verbeux, il inclut désormais une vérification du TPM, si le firewall en est équipé, et affiche dans le fichier *verbose* résultant le nom de l'utilisateur qui l'a déclenché.

De plus, certains messages d'erreur ont été reformulés pour être plus explicites.

Supervision

Une alerte SNMP (*traps*) est désormais générée lors du retour à une situation normale pour chacun des indicateurs de santé suivants :

- État des ventilateurs,
- Température et taux d'utilisation des processeurs,
- Consommation mémoire,
- État des disques,
- État du R.A.I.D,
- Statut des certificats,
- Statut des CRL,
- État du TPM,
- Statut des mots de passe.

Vulnérabilités résolues de SNS 4.8.4

Le niveau de sévérité indiqué est celui en vigueur lors de la première publication du bulletin de sécurité sur le site https://advisories.stormshield.eu/.

Gestion des administrateurs du firewall

Référence support 85555

Une vulnérabilité de sévérité faible a été corrigée dans le mécanisme de gestion des administrateurs du firewall.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-028.

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/2024-034.

Correctifs de SNS 4.8.4

Système

Proxies

Références support 85568 - 85625 - 85701

Des problèmes dans le proxy SSL pouvant entraîner un blocage inopiné des flux empruntant le proxy ont été résolus.

Proxy POP3 - Antispam et/ou antivirus

Référence support 81432

Lors de l'analyse antivirus et/ou antispam, le proxy POP3 pouvait détecter à tort du traitement par lots d'e-mails (*pipelining*) et fractionner un message de manière inappropriée. Ce comportement a été corrigé.

VPN IPsec

Référence support 85786

Lorsque la configuration IPsec d'un firewall en version inférieure à SNS 4.8 utilise un profil de phase 2 avec le champ PFS positionné sur *Aucun*, la mise à jour de ce firewall en version SNS 4.8 ne supprime plus à tort le jeton correspondant dans le fichier de configuration IPsec. Cette anomalie empêchait l'établissement des tunnels IPsec utilisant ce profil de phase 2.

La phase 1 d'un tunnel IPsec est désormais automatiquement supprimée lorsque la phase 2 unique associée est supprimée pour cause d'inactivité.

Référence support 85721

Suite au déploiement via SMC d'une configuration IPsec :

- Qui utilise des interfaces virtuelles (VTI),
- Dont le correspondant est défini en mode **Ne pas initier le tunnel (ResponderOnly).**

La tentative d'établissement du tunnel ne provoque plus un blocage inopiné du firewall.

Référence support 85676

La stabilité des configurations en haute disponibilité soumises à une forte charge a été améliorée. Cela évite les arrêts inopinés du moteur de gestion des tunnels IPsec.

VPN SSL

Il est de nouveau possible pour les utilisateurs d'établir leur tunnel VPN en s'authentifiant avec des services externes (mode Push). Cette régression était apparue en version SNS 4.8.3.

Autorité de certification importée

Référence support 85740

Il est désormais possible de supprimer la CRL d'une autorité de certification importée.

Importation des certificats

Référence support 85731

Les certificats .cert et .crt sont désormais identifiés comme des certificats PEM lors de l'importation. Auparavant, ils étaient considérés comme des certificats P12, ce qui provoquait une erreur.

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

Référence support 84495 - 84933 - 85038 - 85081 - 85213

Des modifications ont été apportées afin de réduire le nombre d'accès disques au fichier de configuration *ConfigFiles/Openvpn/openvpn*. Ceci pouvait entraîner des redémarrages inopinés des firewalls modèles SN160(W) / SN210(W) / SN310.

Haute disponibilité (HA) - CRL

Référence support 85558

Les CRL issues de CA globales sont désormais synchronisées toutes les 60 minutes entre le firewall actif et le firewall passif.

Référence support 85553

Les CRL récupérées par le firewall actif sont désormais immédiatement synchronisées avec le firewall passif. Cette synchronisation n'était réalisée auparavant que toutes les 60 minutes. En cas de bascule au sein du cluster pendant ce laps de temps, le nouveau firewall actif pouvait ainsi ne pas connaître l'ensemble des CRL et empêcher l'établissement de tunnels IPsec par exemple.

Logs - Journaux d'audit

Référence support 85563

Un redémarrage du firewall dans les cinq minutes suivant la création d'un filtre dans le module **Logs - Journaux d'audit** > **Tous les journaux** ne supprime plus le filtre.

Routage dynamique Bird

Référence support 85756

À présent, le moteur de routage dynamique BIRD ne redémarre plus en boucle lorsqu'il est en mode verbeux. Cette régression était apparue en version SNS 4.8.0.

Référence support 85271

Lorsque le protocole OSPF est utilisé pour le routage dynamique, la taille du tampon de la *socket* a été augmentée afin qu'il n'y ait plus de perte de paquets.

Référence support 85755

Il n'est désormais plus possible de démarrer BIRD v1 et BIRD v2 en parallèle.

Interface virtuelle

Référence support 85669

Dans le cas d'un tunnel GRE, si la taille d'un paquet dépassait la MTU, le paquet de réponse ICMP n'indiquait pas la bonne valeur de MTU. Ce problème a été corrigé.

Partition de sauvegarde

Référence support 85527

Dans le cas d'un firewall :

- En version SNS 4.8,
- Avec une partition de secours en version SNS 4.3.23 LTSB ou inférieure,

Des dysfonctionnements peuvent se produire en cas d'utilisation de la partition de secours. Il est à présent impossible de faire une mise à jour en version SNS 4.8 si la partition de secours n'est pas en version SNS 4.3.24 LTSB ou supérieure.

Filtrage et NAT

Référence support 68445 - 70036- 85660

La valeur de la colonne *#set_tos* de l'export CSV des règles de filtrage est désormais correcte et de nouvelles colonnes pour la QoS et synproxy on été ajoutées.

Interface Wi-Fi

Référence support 84615

Le gestionnaire de configuration réseau ne s'arrête plus inopinément au démarrage si le code pays de l'interface Wi-Fi est celui de la Jamaïque.

Commandes CLI / Serverd

Référence support 85797

L'utilisation de la commande CLI / serverd `SYSTEM UPDATE UPLOAD` sans argument provoquait un arrêt inopiné de serverd et une déconnexion de la console. Ce problème a été résolu.

Moteur de prévention d'intrusion

Mémoire

Dans certains cas, le firewall rencontrait un blocage inopiné lors du traitement d'erreurs en cas de manque de mémoire. Ce problème a été résolu.

Interface Web d'administration

Applications et protections

Référence support 85779

Désormais, l'index d'un profil de protocole modifié depuis le module *Applications et protections* correspond de nouveau à l'index configuré dans les profils de sécurité. Cette régression était apparue en version SNS 4.8.0.

QoS

Référence support 85458

La liste des caractères interdits dans le nom des files QoS est maintenant conforme à la section **Noms autorisés ou interdits** du *Manuel utilisateur SNS*.

Nouvelles fonctionnalités et améliorations de SNS 4.8.3 EA

VPN IPsec - SN-XL-Series-5200 et SN-XL-Series-6200

Certains paramètres du moteur de gestion des tunnels IPsec ont été modifiés afin d'augmenter sensiblement le nombre de tunnels IPsec pouvant être établis simultanément sur les firewalls modèles SN-XL-Series-5200 et SN-XL-Series-6200.

Des améliorations ont également été apportées à la gestion des paquets afin d'augmenter le débit IPSec.

Haute disponibilité - Rapport système (*sysinfo*)

La commande *sysinfo* lancée sur le firewall actif d'un cluster peut désormais générer et récupérer le rapport système du firewall passif.

Cette opération est réalisable à l'aide de la commande CLI / Serverd `SYSTEM INFORMATION [fwserial=(<serial>|passive|active|local)]` en sélectionnant l'argument *passive*.

Plus d'information sur la commande **`SYSTEM INFORMATION`**

Proxy SSL

Le proxy SSL supporte désormais les deux suites de chiffrement suivantes :

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Changement de mot de passe du compte *admin* via SSH

En console sur le firewall au travers d'une connexion SSH, il est désormais nécessaire de renseigner l'ancien mot de passe du compte *admin* pour pouvoir changer celui-ci.

Vulnérabilités résolues de SNS 4.8.3 EA

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.

Accès SSH - Mode multi-utilisateurs

Une vulnérabilité de sévérité faible a été corrigée dans le mode d'accès SSH multi-utilisateurs.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2024-016.

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 4.8.3 EA

Système

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 4.7.3.

Haute disponibilité et objets dynamiques

Référence support 81176

Lors d'une bascule au sein d'un cluster, la base d'objets dynamiques apparaît désormais immédiatement sur le nouveau firewall actif. Ceci pouvait nécessiter plusieurs minutes auparavant et bloquer le trafic réseau utilisant ces objets pendant ce laps de temps.

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.

Filtrage et NAT - Services Web

Référence support 85539

L'utilisation dans une règle de filtrage d'un service web personnalisé dont le nom comporte exactement 20 caractères rend cette règle de filtrage inopérante.

Cette situation entraîne l'affichage d'un message d'avertissement dans le widget **Messages** du **Tableau de bord**. Ce message précise la politique de filtrage et le numéro de règle concernés.

Pour corriger la situation, vous devez :

1. Mettre en conformité (moins de 20 caractères) le nom du service Web dans le fichier d'import CSV initialement utilisé,
2. Réimporter ce fichier dans le module **Objets** > **Services Web** > onglet **Import de services personnalisés**,
3. Modifier la règle de filtrage pour utiliser le nouveau nom du service Web.

Configuration

Référence support 85434

Le nombre d'adresses IP définies sur une interface ne peut plus dépasser la limite autorisée sur le firewall. Notez que les adresses IP excédentaires n'étaient pas activées mais aucun message d'erreur n'était affiché lors de la validation de la configuration. Cette anomalie a été corrigée.

La commande `system ping host` ne remonte plus à tort l'erreur "Erreur de format" lorsqu'elle est utilisée avec un nom de domaine pleinement qualifié (FQDN) comme argument. Cette régression était apparue en version SNS 4.8.

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.

Référence support 85725

La configuration d'usine d'un firewall en version SNS 4.8.3 EA ou supérieure autorise de nouveau par défaut le retour à une version inférieure de firmware.

Ce comportement est exclusivement modifiable via la commande CLI / Serverd : `SYSTEM UPDATE DOWNGRADE state=off` pour interdire le retour à une version inférieure selon les règles suivantes :

- Firewalls virtuels : retour interdit vers toute version inférieure à la version actuelle.
- Firewalls physiques : retour interdit vers toute version inférieure aux versions de la partition principale et de la participation de secours.

ATTENTION
La commande CLI / Serverd `SYSTEM UPDATE DOWNGRADE state=on` n'est plus acceptée pour autoriser de nouveau le retour à une version inférieure de firmware.

Rapport système (*sysinfo*)

Référence support 85593

Les informations concernant la présence d'un mode *verbose* activé sont désormais correctement remontées dans le rapport système.

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).

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).

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.

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.

Réputation des machines

Référence support 85635

Un problème de droits d'accès qui empêchait le bon fonctionnement du moteur de gestion des réputations de machines a été résolu. Cette régression était apparue en version SNS 4.7.

Télémétrie

Un problème de fuite mémoire a été corrigé dans le moteur de gestion de la télémétrie.

Supervision - Télémétrie

Le service de Télémétrie n'apparaît plus à tort dans le tableau de bord comme étant arrêté.

Authentification - Agent TS

Référence support 85401

L'authentification via la méthode Agent TS échouait logiquement pour un utilisateur dont l'identifiant contenait un espace (caractère interdit) mais aucun message d'erreur n'était affiché pour le signaler. Une alarme est désormais levée dans ce cas. La liste des caractères interdits est également fournie en complément d'information de l'alarme.

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.

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.

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.

Qualité de service (QoS)

Référence support 85590

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

Taille de la partition dédiée aux rapports

Une modification de la taille de partition dédiée au stockage des rapports n'était plus prise en compte. Cette régression, apparue en version SNS 4.8.0, a été corrigée.

Interface Web d'administration

VPN SSL

Référence support 85663

Le changement de certificat présenté par le serveur ou par le client VPN SSL est de nouveau fonctionnel. Cette régression était apparue en version SNS 4.8.1.

Portail captif

Référence support 84750

L'interface *sslvpn_udp* est désormais sélectionnable dans les profils du portail captif. Les utilisateurs se présentant depuis cette interface peuvent donc maintenant accéder au portail captif.

Annuaire LDAP externe Microsoft Active Directory

Référence support 85764

Suite à la création d'un nouvel annuaire LDAP externe de type Microsoft Active Directory, les utilisateurs présents dans cet annuaire sont de nouveau correctement affichés dans le module des utilisateurs. Cette régression était apparue en version SNS 4.8.0.

Correctifs de SNS 4.8.2 EA

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 4.8.1 EA.

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

Nouvelles fonctionnalités et améliorations de SNS 4.8.1 EA

Accès réseau *Zero Trust* (ZTNA) - Contrôle de conformité des postes clients

Afin de mettre en œuvre un accès réseau *Zero Trust* (ZTNA), vous pouvez désormais configurer une politique de vérification de la conformité des postes clients établissant un tunnel VPN SSL avec le firewall SNS. Lorsqu'elle est activée, un poste client ou un utilisateur non conforme aux critères de la politique ne peut pas établir de tunnel VPN SSL avec le firewall SNS.

Seul le client VPN SSL Stormshield en version 4.0 ou supérieure est compatible avec la fonctionnalité de contrôle de conformité des postes clients. Chaque poste de l'entreprise doit donc utiliser le client VPN SSL Stormshield en version 4.0 ou supérieure lorsque cette fonctionnalité est activée.

Toutefois, une option vous permet d'autoriser les clients VPN SSL non compatibles à établir des tunnels VPN SSL. Cette option doit être utilisée de manière temporaire, par exemple pour mettre à jour progressivement un parc de clients VPN SSL vers une version compatible.

Pour plus d'informations sur la mise en œuvre d'un accès réseau *Zero Trust* (ZTNA) et la fonctionnalité de contrôle de conformité des postes clients, reportez-vous à la note technique **Configurer et utiliser le VPN SSL des firewalls SNS**.

Authentification multifacteur en IKEv2 par le biais d'EAP

La version SNS 4.8 introduit le support de l'authentification multifacteur pour les tunnels nomades basés sur IKEv2 par le biais d'EAP (Extensible Authentication Protocol).

Cette authentification multifacteur peut être réalisée grâce aux méthodes suivantes :

- EAP-Generic Token Card : le correspondant mobile doit présenter un couple identifiant / mot de passe,
- Certificat et EAP-Generic Token Card : le correspondant mobile doit présenter un certificat et un couple identifiant / mot de passe,
- Pour une sécurité accrue, il est possible d'utiliser avec les méthodes EAP ci-dessus des codes à usage unique (TOTP) grâce à la solution TOTP Stormshield.

À noter que :

- Les méthodes EAP ne sont pas compatibles avec le mode Diffusion Restreinte (DR) et les tunnels basés sur IKEv1 qui doivent utiliser Xauth pour l'authentification multifacteur,
- Il est nécessaire d'utiliser le client VPN Exclusive Stormshield en version 7.4 ou supérieure pour établir des tunnels nomades basés sur IKEv2 par le biais d'EAP.

Pour plus d'informations, reportez-vous à la note technique **VPN IPSec Mobile IKEv2 - Authentification EAP avec Certificat**.

Protection contre les attaques post-quantiques

La version SNS 4.8 introduit la possibilité de définir des clés pré-partagées post-quantiques (PPK) pour les correspondants utilisant le protocole IKEv2 avec authentification par certificats.

La puissance de calcul d'un ordinateur quantique pourra très probablement à l'avenir lui permettre de déchiffrer des clés négociées via les méthodes Diffie-Hellman (DH) et Elliptic Curve Diffie-Hellman (ECDH), et mettre en danger la sécurité du protocole IKEv2.

Un utilisateur malveillant pourrait dès à présent réaliser une attaque de type "stocker maintenant, déchiffrer plus tard" : intercepter des communications IPsec et les stocker afin de les déchiffrer ultérieurement à l'aide d'un ordinateur quantique.

Pour les clients qui souhaitent dès à présent se protéger de telles attaques, la version SNS 4.8 suit les recommandations de la RFC 8784 et permet donc d'utiliser des PPK destinées à protéger les échanges des clés de chiffrement des données. À noter que pour être efficaces, ces PPK doivent respecter une entropie suffisamment élevée (256 bits minimum selon la RFC).

Pour plus d'informations sur l'utilisation des PPK pour le protocole IKEv2, consultez la RFC 8784.

Pour plus d'informations sur la configuration des PPK, reportez-vous aux sections VPN IPsec Correspondants et Identification du *manuel utilisateur SNS*.

Routage multicast dynamique

Le panneau de configuration du routage multicast a été simplifié et un panneau de supervision a été ajouté.

La fonctionnalité de routage multicast dynamique n'est désormais plus en accès anticipé.

Plus d'informations sur le routage multicast dynamique.

Routage Dynamique BIRD

Ajout de la version 2 et version 1 obsolète

La version 2 du moteur de routage dynamique BIRD est désormais disponible. Dans le panneau de configuration du **Routage dynamique**, vous pouvez :

- Activer une version de **BIRD** en particulier dans un nouvel onglet **Général**,
- Préparer une migration vers la nouvelle version du moteur dans l'onglet **BIRD v2** avant de l'activer. Pendant l'édition de la configuration de BIRD v2, vous pouvez afficher la configuration de BIRD v1 dans un panneau sur la droite.

La version 1 du moteur de routage dynamique BIRD est à présent considérée comme obsolète et un message dans le widget **Messages** vous en informe.

Pour plus d'informations, reportez-vous à la note technique Routage Dynamique BIRD v2.

Cas d'un parc de firewalls SNS géré par un serveur SMC

Dans le cas où votre parc de firewalls SNS est géré par un serveur SMC, il n'est pas possible de gérer le routage dynamique de vos firewalls en versions 4.8.1 EA et supérieures depuis une version de SMC inférieure à la 3.6. Le déploiement de la configuration par le serveur SMC est alors refusée par le firewall SNS et celui-ci remonte une erreur.

Pour plus d'informations sur les versions SMC, reportez-vous à la section Nouvelles fonctionnalités et améliorations de SMC 3.6 des *Notes de version SMC*.

Nouveau module matériel 4 *bypass* (NA-EX-CARD-BP-8xG-C)

La version SNS 4.8 introduit le support du module matériel **NA-EX-CARD-BP-8xG-C** permettant de disposer de 1 à 4 *bypass* pour les modèles de firewalls suivants :

- SN-M-Series-520,
- SN-M-Series-720,
- SN-M-Series-920,
- SN1100 (uniquement dans l'emplacement d'extension de gauche).

Plus d'informations sur le fonctionnement et l'activation des *bypass*.

Support de nouveaux modèles de firewalls

La version SNS 4.8 introduit le support des modèles de firewalls suivants :

- SN-L-Series-2200 et SN-L-Series-3200,
- SN-XL-Series-5200 et SN-XL-Series-6200.

Protection contre les attaques par déni de service (DoS et DDoS)

La protection contre les attaques DoS et DDoS a été renforcée. Ces améliorations concernent les protocoles de transport UDP et TCP et vous pouvez paramétrer de nouveaux seuils de détection dans les profils d'inspection.

Plus d'informations sur la configuration des protections contre les dénis de service des protocoles TCP-UDP.

Sécurité renforcée

Durcissement du système

Le durcissement du système en version SNS 4.8 renforce la sécurité du produit.

Clés NTP - Ajout du choix de l'algorithme

Vous pouvez maintenant sélectionner les algorithmes SHA1, SHA256, SHA384, SHA512 et AES-CBC-128 dans la configuration de la liste des clés NTP.

Plus d'informations sur les paramètres de date et d'heure.

Analyse des mécanismes d'extension pour le DNS (EDNS)

Le moteur de prévention d'intrusion intègre désormais l'analyse des mécanismes d'extension pour le DNS (EDNS) décrite dans la RFC 6891.

Nouvelles restrictions pour les certificats utilisés lors des connexions TLS

Vous ne pouvez plus utiliser les certificats suivants lors des connexions TLS sur le firewall SNS :

- Certificats contenant la contrainte "*CA:TRUE*" (doit être "*CA:FALSE*"),
- Certificats contenant l'XKU "*OCSP Server*".

Agent SNMPv3 - Algorithmes obsolètes

L'algorithme d'authentification MD5 et les algorithmes de chiffrement DES et SHA1 utilisés par l'Agent SNMPv3 sont obsolètes et seront supprimés dans une prochaine version de firmware SNS. Une mention indiquant que ces algorithmes sont obsolètes s'affiche désormais dans le panneau de configuration de l'Agent SNMPv3.

Dorénavant, vous pouvez modifier les algorithmes utilisés par l'Agent SNMPv3 avec les commandes CLI / Serverd suivantes :

```
CONFIG SNMP ACCESS USERV3 username=<username> authtype=SHA256
authpass=<passphrase> privtype=AES privpass=<passphrase>
CONFIG SNMP ACTIVATE
```

Après une mise à jour en version SNS 4.8, l'algorithme de chiffrement *DES* est sélectionné par défaut si aucun algorithme n'était auparavant sélectionné. À noter que le chiffrement du mot de passe reste désactivé tant qu'aucun mot de passe n'est renseigné dans le champ associé à l'algorithme de chiffrement.

Annuaire LDAP interne - Algorithmes obsolètes

Les algorithmes de hachage des mots de passe MD5, SMD5, SHA, SSHA, SHA256, SHA384 et SHA512 utilisés par l'annuaire LDAP interne sont obsolètes et seront supprimés dans une prochaine version de firmware SNS. Une mention indiquant que ces algorithmes sont obsolètes s'affiche désormais dans le panneau de configuration avancée de l'annuaire LDAP interne.

VPN SSL Portail - Fonctionnalité obsolète

La fonctionnalité VPN SSL Portail est obsolète et sera supprimée dans une prochaine version de firmware SNS. Un message indiquant que cette fonctionnalité est obsolète s'affiche désormais dans le panneau de configuration du VPN SSL Portail.

Suppression de l'analyse du protocole OSCAR

Considéré comme obsolète depuis la version SNS 4.6.9, l'analyse du protocole OSCAR a été supprimée du firewall SNS. À noter que l'analyse de ce protocole était automatiquement désactivée lors de la mise à jour du firewall en version SNS 4.7.2 EA.

Taille des clés RSA

La taille des clés RSA générées sur le firewall SNS est à présent de 4096 bits par défaut.

Intégration dans divers environnements

Agrégat de liens - Support du mode *broadcast*

La version SNS 4.8 introduit la possibilité de configurer un agrégat en mode *broadcast* directement depuis l'interface d'administration du firewall dans l'onglet **Configuration avancée** d'un agrégat. Introduite en version SNS 4.7.5, cette configuration ne pouvait être réalisée qu'en modifiant un fichier de configuration du firewall.

Plus d'informations sur la configuration d'un agrégat.

Groupes Diffie-Hellman (DH) multiples

Vous pouvez désormais préciser plusieurs groupes DH dans un même profil de chiffrement IKE et IPsec afin de faciliter la migration des correspondants vers un seul et même groupe.

Plus d'informations sur les profils de chiffrement.

Proxies HTTP et SSL - Support du protocole WebSocket

La version SNS 4.8 introduit le support du protocole WebSocket par les proxies HTTP et SSL. À noter que dans les profils IPS des connexions entrantes (comme *IPS_00*), l'alarme *http:301* bloque par défaut (action *Interdire*) le support du protocole WebSocket.

IPsec DR - OCSP

Dans un contexte IPsec DR, et conformément à la RFC 4806, un correspondant peut désormais valider le certificat de la passerelle distante présenté lors de l'établissement d'un tunnel IKEv2 sans exposer le serveur OCSP.

Cette configuration est possible uniquement avec le jeu de commandes CLI / Serverd :

```
CONFIG IPSEC OCSP
```

Plus d'informations sur les commandes CONFIG IPSEC OCSP.

Authentification asynchrone

Le mécanisme d'authentification du firewall SNS peut désormais gérer les authentifications des utilisateurs de manière asynchrone, ce qui permet d'améliorer l'intégration des solutions tierces d'authentification multifacteur.

SD-WAN

La gestion des routes de la fonctionnalité SD-WAN a été améliorée.

OpenVPN - Adresse source des requêtes TCP

Vous pouvez désormais préciser l'adresse IP source des requêtes TCP envoyées par le moteur OpenVPN. Ce paramètre est uniquement modifiable à l'aide des commandes CLI / Serverd suivantes :

```
CONFIG OPENVPN UPDATE BindAddr=(<firewall_ip_object>|"")
CONFIG OPENVPN ACTIVATE
```

Dans le cas où OpenVPN est le seul moteur du firewall SNS à écouter sur le port TCP, un gain de performance est alors observé.

Plus d'informations sur les commandes CONFIG OPENVPN.

Envoi de données vers les serveurs sekoia.io

Si vous disposez d'un abonnement pour envoyer vos données vers les serveurs sekoia.io, vous pouvez désormais configurer la clé d'authentification que vous a fournie Sekoia (*Intake Key*) dans la configuration des profils Syslog.

Plus d'informations sur la configuration des profils Syslog.

Flux TLS 1.3 - Analyse des certificats serveur

Vous pouvez désormais préciser l'adresse IP source des requêtes envoyées par le moteur de prévention d'intrusion lorsqu'il tente de récupérer le certificat serveur pour chaque flux TLS 1.3 traversant le firewall. Cela permet d'analyser les éventuelles failles de sécurité liées à ce certificat.

Vous pouvez effectuer cette configuration grace à la commande CLI / Serverd suivante :

```
CONFIG PROTOCOL SSL PROFILE IPS CONFIG index=<slot>
TLSServerCertBindAddr=<host>
```

Plus d'informations sur la commande CONFIG PROTOCOL SSL PROFILE IPS CONFIG.

Évolution des performances

TLS 1.3 - Ajout d'un cache lors de l'échec de récupération des certificats

Désormais, lorsqu'une requête ne parvient pas à récupérer un certificat, les requêtes suivantes reçoivent une réponse instantanée grâce à un cache. Ce cache est activé par défaut et est d'une durée de 6 heures.

Vous pouvez personnaliser la durée du cache (en secondes) à l'aide de la commande CLI / Serverd :

```
CONFIG PROTOCOL SSL COMMON IPS CONFIG TLSCertCacheErrorTTL=<60..259200>
```

Plus d'informations sur la commande CONFIG PROTOCOL SSL COMMON IPS CONFIG.

Vous pouvez désactiver ce cache en positionnant la valeur du jeton de configuration *TLSServerCertCacheError* sur *0* dans le fichier *ConfigFiles/Protocols/ssl/* de la politique utilisée.

Amélioration de l'expérience utilisateur

Configuration initiale par clé USB - Nouvelles opérations

Vous pouvez désormais importer un certificat et sa CRL pendant la configuration initiale par clé USB d'un firewall SNS grâce aux opérations *certimport* et *crlimport*.

Pour plus d'informations sur ces opérations, reportez-vous aux sections Opération certimport et Opération crlimport de la note technique *Configuration initiale par clé USB*.

Mode furtif

Lorsque le mode furtif est désactivé, un lien renvoyant vers les paramètres du protocole IP s'affiche désormais dans l'avertissement du widget **Messages** du tableau de bord.

Plus d'informations sur le Mode furtif du protocole IP.

Module Objets URL

Le panneau de configuration des objets URL a été amélioré. La configuration des **Groupes de catégories** s'effectue désormais dans l'onglet **Noms de certificat (CN)**.

Plus d'informations sur la configuration des objets URL.

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

Référence support 84328

Vous pouvez désormais désactiver le bouton de remise en configuration d'usine du firewall. Cela évite de réinitialiser la configuration du firewall par accident.

Cette désactivation ne peut être réalisée qu'à l'aide de la commande CLI / SSH suivante :

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

Profils d'inspection applicative

Seuls les profils d'inspection globaux, nommés par défaut IPS_00, IPS_01..., sont désormais affichés dans le module **Protection applicative** > **Profils d'inspection.**

Amélioration de la visibilité de certaines informations

Messages d'alarme relatifs à la haute disponibilité ou à une défaillance matérielle

Les messages d'alarme relatifs à la haute disponibilité ou à une défaillance matérielle affichent désormais :

- Le numéro de série du firewall SNS,
- Le nom du nœud système, s'il a été défini.

MIB STORMSHIELD-PROPERTY-MIB - Ajout de l'OID snsSystemNodeName

L'OID *snsSystemNodeName* a été ajouté à la MIB **STORMSHIELD-PROPERTY-MIB**. Il retourne comme valeur le nom du nœud système.

Alarmes de restauration de la configuration

Une alarme système est déclenchée sur le tableau de bord quand une restauration de la configuration est réalisée par une commande CLI / Serverd ou via une clé USB. Cette alarme indique :

- S'il s'agit d'une restauration partielle ou complète,
- Le résultat du hachage du contenu du fichier (méthode SHA2),
- Dans le cas d'une commande CLI / Serverd, l'utilisateur qui l'a exécutée.

Commande sfctl - Utilisation du nom d'un objet dans les filtres

Pour faciliter les diagnostics, vous pouvez désormais utiliser un nom d'objet dans les filtres lors de l'utilisation de la commande *sfctl* avec les paramètres *-H type=modifier*.

Plus d'informations sur la commande sfctl.

Ajout de filtres pour les commandes MONITOR GETSA, GETSPD et GETIKESA

Vous pouvez désormais utiliser des filtres dans les commandes CLI / Serverd de supervision VPN IPsec suivantes :

```
MONITOR GETSA Global=<0|1> List=<full|light>
MONITOR GETIKESA Global=<0|1> List=<full|light>
MONITOR GETSPD Global=<0|1> List=<full|light>
```

Pour plus d'informations sur ces commandes, reportez-vous aux sections MONITOR GETSA, MONITOR GETIKESA et MONITOR GETSPD du *guide de référence des commandes CLI / Serverd* (anglais uniquement).

Mécanisme de surveillance de l'activité matérielle du firewall (watchdog)

La gestion du mécanisme de surveillance de l'activité matérielle du firewall (watchdog) a été améliorée. Désormais, les compteurs réels de surveillance sont affichés dans une infobulle et la gestion du mécanisme de surveillance est disponible dans l'interface d'administration des firewalls virtuels.

Agent SNMP

La valeur attribuée au champ *sysname* présenté par l'agent SNMP respecte l'ordre suivant :

1. La valeur éventuellement précisée dans le champ **Nom** de la **Configuration des informations MIB-II** (module **Notifications** > **Agent SNMP**),
2. Sinon, la valeur éventuellement précisée dans le champ **Nom du firewall** (module **Système** > **Configuration** > onglet **Configuration Générale**),
3. Sinon, le numéro de série du firewall.

Télémétrie

État du service de télémétrie

L'état du service de télémétrie s'affiche désormais dans le tableau de bord.

Nouvelles données remontées par le service de télémétrie

Le service de télémétrie de la version SNS 4.8 remonte de nouvelles données :

- Données concernant l'utilisation du module VPN IPsec :
  - Nombre de tunnels site à site ou mobile configurés et activés dans la politique IPsec active,
  - Nombre de tunnels configurés en IKEv1 ou IKEv2 dans la politique IPsec active,
  - Nombre d'utilisations de chaque méthode d'authentification pour les tunnels configurés dans la politique IPsec active,
  - Nombre maximal de tunnels site à site ou mobile connectés,
- Données concernant le cache TLS 1.3 :
  - Nombre total d'entrées dans le cache TLS 1.3,
  - Nombre total de purges du cache en cas de saturation,
  - Nombre de requêtes de certificats en échec.

En transmettant ces données parfaitement anonymes, vous aidez Stormshield à affiner les tailles et limites des futures plate-formes matérielles et versions SNS.

Plus d'informations sur le service de télémétrie.

Correctifs de SNS 4.8.1 EA

Système

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.

VPN SSL

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`**.

Politique d'authentification

Références support 79493 - 84414 - 84713

L'action **Bloquer** a été supprimée du choix de valeurs possibles pour la méthode d'authentification par défaut :

- Le choix de cette valeur bloquait à tort l'authentification des utilisateurs du VPN SSL lorsque l'objet source **Internet** était sélectionné dans la règle d'authentification du VPN SSL,
- Le choix de cette valeur associé à une règle d'authentification précisant d'utiliser la méthode d'authentification par défaut ne bloquait pas les flux d'authentification correspondants,
- Le choix de cette valeur sans aucune règle d'authentification spécifique précisée dans la politique d'authentification autorisait à tort l'authentification sur le firewall via SSH.

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 comportement persiste sur les firewalls modèles SN160(W), SN210(W) et SN310.

Haute disponibilité

Référence support 84512

Sur une configuration en haute disponibilité, lorsque vous consultez les modules de l'interface Web d'administration sans réaliser de modifications, l'icône indiquant la nécessité d'une synchronisation de configuration entre les membres du cluster ne s'affiche plus à tort.

Firewalls SN-S-Series-220/320 et SN-M-Series-520 - Démarrage sur Modem / Clé USB 4G

Lorsque sa configuration réseau ne fait aucune référence à un Modem / clé USB 4G, le démarrage d'un firewall modèle SN-S-Series-220/320 ou SN-M-Series-520 avec un modem / clé USB 4G connecté sur l'un de ses ports USB ne s'interrompt plus lors du choix de la partition de démarrage.

Supervision SD-WAN

Référence support 84874

La supervision d'un objet routeur utilisé dans une route statique est désormais fonctionnelle.

Services Web

Références support 84662 - 84444

L'import de services Web personnalisés depuis un fichier CSV n'autorise plus la présence de guillemets encadrant un commentaire dans le fichier source.

DNS Dynamique

Références support 84480 - 85395

Désormais, la réalisation de la séquence d'actions suivante active correctement le service DNS Dynamique du firewall :

1. Configurer un profil de DNS Dynamique.
2. Appliquer les modifications.
3. Activer ce profil.
4. Appliquer les modifications.

Exécution simultanée d'une commande d'arrêt / redémarrage d'un firewall et d'une sauvegarde système sur la partition de secours

L'exécution simultanée d'une commande d'arrêt (HALT) / redémarrage (REBOOT) du firewall et d'une sauvegarde du système sur la partition de secours (*dumproot*) pouvait aboutir à un échec de cette dernière voire à une corruption de la partition de secours.

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

- Lorsqu'un *dumproot* est en cours, le mécanisme d'arrêt / redémarrage du firewall est mis en attente active et démarre une fois le *dumproot* terminé,
- Lorsqu'une commande d'arrêt / redémarrage du firewall a été lancée, le *dumproot* ne se lance pas et génère un événement système.

Firewalls virtuels - Interdire le retour à une version antérieure de firmware

Sur les firewalls virtuels, le jeton de configuration permettant d'interdire tout retour à une version antérieure de firmware est désormais correctement pris en compte.

Ce comportement peut être exclusivement géré via la commande CLI / Serverd :

```
SYSTEM UPDATE DOWNGRADE state=<on|off>
```

Plus d'informations sur la commande **SYSTEM UPDATE DOWNGRADE**.

Commandes CLI / Serverd - CONFIG LDAP UPDATE HELP

Référence support 85301

La commande CLI / Serverd `CONFIG LDAP UPDATE HELP` ne fait plus référence à tort au paramètre *realbindaddr* au lieu de *bindaddr*.

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

Logs

Référence support 84831

L'indisponibilité du moteur de gestion des logs n'entraîne plus à tort un blocage temporaire du moteur de prévention d'intrusion.

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. Notez que le téléchargement des CRL n'était cependant pas concerné par cette anomalie.

Traps SNMPv3 - securityName

Référence support 85435

La configuration d'un trap SNMPv3 pour l'événement **securityName** contenant des valeurs avec des espaces ne retourne plus l'erreur Serverd *Error in format*.

Collecteur IPFIX - Logs des connexions réseau

Référence support 85054

Les logs des connexions réseau n'étaient pas envoyés au collecteur IPFIX lorsqu'ils étaient issus d'une règle de la politique de filtrage possédant le niveau d'inspection **Firewall**. Ce problème a été corrigé.

Réseau

GRE / GRETAP

Références support 84395 - 76800

Un tunnel GRE / GRETAP basé sur une interface de sortie configurée en DHCP s'établit désormais correctement après le redémarrage du firewall ou lorsque cette interface source change d'adresse IP.

Routage dynamique BIRD version 1

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.

Firewalls virtuels EVA

Hyperviseur basé sur Qemu 8.1 ou supérieur

Référence support 76697

Le déploiement d'un EVA en version SNS 4.7 ou supérieure sur un hyperviseur basé sur Qemu 8.1 ou supérieur fonctionne désormais correctement.

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 4.7.1 EA.

LDAP externe - Affichage de la liste des utilisateurs

Référence support 85287

Lorsqu'un annuaire externe possédait plus de 1000 utilisateurs, la liste des utilisateurs ne s'affichait pas dans le module **Utilisateurs** du firewall SNS. Ce problème a été corrigé et les 500 premiers utilisateurs de l'annuaire s'affichent désormais par défaut dans la liste des utilisateurs.

Filtrage et NAT

Référence support 76697

La modification de l'adresse IP d'une interface est désormais correctement répercutée dans l'infobulle des propriétés de cet objet au sein du module **Filtrage et NAT**.

Supervision VPN IPsec

Référence support 85292

Après avoir réalisé les opérations suivantes :

1. Créer et appliquer un filtre sur les colonnes du module de **Supervision VPN IPsec**.
2. Quitter ce module puis y revenir.

Le filtre est indiqué comme étant actif et est désormais correctement appliqué.

Logs - Journaux d'audit

Référence support 85292

Dans le module **Logs - Journaux d'audit** > **Tous les journaux**, il est désormais possible d'ajouter le type de Logs comme critère de filtrage.

Dans les détails d'un log, le survol du drapeau d'un pays source ou destination affiche désormais correctement l'information "Nom du pays (Code du pays)".

Adresse IPv6 en DHCP

Référence support 85336

Lorsqu'une interface en IPv6 est configurée via DHCP, toutes les infobulles censées préciser cette adresse ne présentent plus à tort l'adresse IPv4 de l'interface.

Adresse IPv6 - Supervision des utilisateurs connectés via la méthode Agent TS

Lorsque l'IPv6 est désactivée sur le firewall SNS, la supervision des utilisateurs connectés via la méthode Agent TS ne présente plus à tort dans la colonne *Adresse IP* l'adresse IPv6 de la machine de l'utilisateur connue par le serveur Windows.

Passerelle dans un objet routeur

Référence support 85211

La modification du nom d'une passerelle membre d'un objet routeur est désormais correctement répercutée dans la liste des passerelles composant l'objet routeur.

Authentification - Radius

Référence support 85128

Dans la configuration de la méthode d'authentification Radius, l'icône présente au bout du champ **Clé pré-partagée** du serveur et de l'éventuel serveur de secours était en partie masquée. Cette anomalie a été corrigée.

Version 4.8.0 non publiée

La version 4.8.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités et améliorations de SNS 4.7.10

Analyse Sandboxing

Référence support 85532

Des optimisations ont été apportées pour réduire le nombre de fichiers envoyés en analyse Sandboxing et limiter le risque de saturation de la file d'attente.

Correctifs de SNS 4.7.10

Système

Proxies

Références support 85568 - 85625 - 85701

Des problèmes dans le proxy SSL pouvant entraîner un blocage inopiné du firewall ont été résolus.

Proxy POP3 - Antispam et/ou antivirus

Référence support 81432

Lors de l'analyse antivirus et/ou antispam, le proxy POP3 pouvait détecter à tort du traitement par lots d'e-mails (*pipelining*) et fractionner un message de manière inappropriée. Ce comportement a été corrigé.

VPN IPsec

Référence support 85676

La stabilité des configurations en haute disponibilité soumises à une forte charge a été améliorée. Cela évite les arrêts inopinés du moteur de gestion des tunnels IPsec.

Référence support 85721

Suite au déploiement via SMC d'une configuration IPsec :

- Qui utilise des interfaces virtuelles (VTI),
- Dont le correspondant est défini en mode **Ne pas initier le tunnel (ResponderOnly).**

La tentative d'établissement du tunnel ne provoque plus un blocage inopiné du firewall.

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

Référence support 84495 - 84933 - 85038 - 85081 - 85213

Des modifications ont été apportées afin de réduire le nombre d'accès disques au fichier de configuration *ConfigFiles/Openvpn/openvpn*. Ceci pouvait entraîner des redémarrages inopinés des firewalls modèles SN160(W) / SN210(W) / SN310.

Haute disponibilité (HA) - CRL

Référence support 85558

Les CRL issues de CA globales sont désormais synchronisées toutes les 60 minutes entre le firewall actif et le firewall passif.

Référence support 85553

Les CRL récupérées par le firewall actif sont désormais immédiatement synchronisées avec le firewall passif. Cette synchronisation n'était réalisée auparavant que toutes les 60 minutes. En cas de bascule au sein du cluster pendant ce laps de temps, le nouveau firewall actif pouvait ainsi ne pas connaître l'ensemble des CRL et empêcher l'établissement de tunnels IPsec par exemple.

Logs - Journaux d'audit

Référence support 85563

Un redémarrage du firewall dans les cinq minutes suivant la création d'un filtre dans le module **Logs - Journaux d'audit** > **Tous les journaux** ne supprime plus le filtre.

Importation des certificats

Référence support 85731

Les certificats .cert et .crt sont désormais identifiés comme des certificats PEM lors de l'importation. Auparavant, ils étaient considérés comme des certificats P12, ce qui provoquait une erreur.

Moteur de prévention d'intrusion

Mémoire

Dans certains cas, le firewall rencontrait un blocage inopiné lors du traitement d'erreurs en cas de manque de mémoire. Ce problème a été résolu.

Interface Web d'administration

QoS

Référence support 85458

La liste des caractères interdits dans le nom des files QoS est maintenant conforme à la section *Noms autorisés ou interdits* du Manuel utilisateur SNS.

Vulnérabilités résolues de SNS 4.7.9

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 4.7.9

Système

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 4.7.3.

Configuration

Référence support 85434

Il n'est plus possible de définir plus d'adresses IP sur une interface que la limite définie sur le firewall ne l'autorise. Notez que les adresses IP excédentaires n'étaient pas activées mais aucun message d'erreur n'était affiché lors de la validation de la configuration. Cette anomalie a été corrigée.

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.

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.

Rapport système (*sysinfo*)

Référence support 85593

Les informations concernant la présence d'un mode *verbose* activé sont désormais correctement remontées dans le rapport système.

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.

Réputation des machines

Référence support 85635

Un problème de droits d'accès qui empêchait le bon fonctionnement du moteur de gestion des réputations de machines a été résolu. Cette régression était apparue en version SNS 4.7.

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).

Télémétrie

Un problème de fuite mémoire a été corrigé dans le moteur de gestion de la télémétrie.

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

Authentification - Agent TS

Référence support 85401

L'authentification via la méthode Agent TS échouait logiquement pour un utilisateur dont l'identifiant contenait un espace (caractère interdit) mais aucun message d'erreur n'était affiché pour le signaler. Une alarme est désormais levée dans ce cas. La liste des caractères interdits est également fournie en complément d'information de l'alarme.

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.

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.

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.

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.

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).

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.

Filtrage et NAT - Services Web

Référence support 85539

L'utilisation dans une règle de filtrage d'un service web personnalisé dont le nom comporte exactement 20 caractères rend cette règle de filtrage inopérante.

Cette situation entraîne l'affichage d'un message d'avertissement dans le widget **Messages** du **Tableau de bord**. Ce message précise la politique de filtrage et le numéro de règle concernés.

Pour corriger la situation, vous devez :

1. Mettre en conformité (moins de 20 caractères) le nom du service Web dans le fichier d'import CSV initialement utilisé,
2. Réimporter ce fichier dans le module **Objets** > **Services Web** > onglet **Import de services personnalisés**,
3. Modifier la règle de filtrage pour utiliser le nouveau nom du service Web.

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.

Interface Web d'administration

Portail captif

Référence support 84750

L'interface *sslvpn_udp* est désormais sélectionnable dans les profils du portail captif. Cette absence empêchait l'accès au portail captif pour les utilisateurs se présentant depuis cette interface.

Correctifs de SNS 4.7.8

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 4.7.7.

Nouvelles fonctionnalités et améliorations de SNS 4.7.7

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 4.7.7

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 4.7.7

Système

VPN IPsec

Références support 84983 - 85253 - 85452

En complément du correctif implémenté en version 4.7.1 EA pour 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.

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.

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).

Interface Web d'administration

Protection applicative - Protocole HTTP

Référence support 85588

L'option **Appliquer la règle de NAT sur le trafic analysé** est de nouveau disponible dans la configuration globale de l'analyse protocolaire HTTP. Cette régression était apparue en version SNS 4.7.1.

Nouvelles fonctionnalités et améliorations de SNS 4.7.6

Messages d'alarmes matérielles

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

Vulnérabilités résolues de SNS 4.7.6

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.

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 4.7.6

NOTE
Annoncé dans les Notes de version 4.6.7, le correctif concernant la longueur du label d'un service Web compatible avec une règle de blocage de flux (référence support 84722) a été supprimé. Il sera revu et réintégré dans une version ultérieure.

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`**.

Haute disponibilité - Authentification TOTP

Référence support 85575

Dans une configuration en haute disponibilité, la synchronisation de la base de données des utilisateurs ayant réalisé leur enrôlement TOTP est de nouveau fonctionnelle. Cette régression était apparue en version SNS 4.7.1 EA.

VLAN dans un agrégat de liens

Le vérificateur de configuration réseau n'est plus sensible à la casse pour les noms de VLAN inclus dans un agrégat. Ce comportement empêchait le rechargement de la configuration réseau.

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.

VPN IPsec

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 4.7.3.

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.

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.

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.

Moteur de prévention d'intrusion

SD-WAN

Référence support 85436

Lorsqu'une route statique utilise un objet routeur dont les passerelles sont toutes rattachées à des interfaces protégées, une bascule de passerelle au sein de cet objet routeur est désormais correctement répercutée dans la table des adresses protégées du moteur de prévention d'intrusion.

Interface Web d'administration

SMC - Suppression de la protection par le TPM

Référence support 85594

La suppression de la protection par le TPM de la clé de communication avec le serveur SMC est désormais fonctionnelle dans l'interface Web d'administration du firewall.

Nouvelles fonctionnalités et améliorations de SNS 4.7.5

Agrégat de liens - Support du mode *broadcast*

La version SNS 4.7.5 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 4.7.5

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 4.7.5

Système

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 85485

La supervision des tunnels VPN SSL n'affiche plus les lignes des utilisateurs "UNDEF" correspondant à des tentatives de connexion. Désormais, seules les connexions établies s'affichent dans la supervision.

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 versions 4.3.16 LTSB et 4.6.1, rendait les captures réseau GRETAP plus difficiles à analyser mais n'impactait aucunement le bon fonctionnement des communications GRETAP.

Certificats et PKI - TPM

Référence support 85431

Lors du renouvellement via EST ou SCEP d'un certificat initialement protégé par le TPM, la protection par le TPM n'était pas conservée. Elle est désormais appliquée automatiquement suite à l'opération de renouvellement.

Authentification - TS Agent

Référence support 85403

Un utilisateur déjà authentifié via la méthode TS Agent ne parvenait pas à se connecter sur l'interface Web d'administration du firewall. Ce problème a été corrigé.

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.

Services Web

Référence support 85539

Lorsqu'un service Web dont le nom dépasse 19 caractères est utilisé dans une règle de filtrage, la politique de filtrage n'est pas appliquée et un avertissement dans le tableau de bord invite l'administrateur à corriger le nom du service concerné.

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.

Authentification - TOTP

Référence support 85473

La modification du **Nombre de codes valides avant et après le code actuel** n'affiche plus à tort la fenêtre indiquant que la base TOTP doit être réinitialisée et que la procédure d'enrôlement TOTP est à recommencer pour tous les utilisateurs.

Correctifs de SNS 4.7.4

Système

VPN SSL et compression LZ4

Référence support 85547

Lorsque la compression LZ4 pour le VPN SSL est activée, la mise à jour en version 4.7.4 n'empêche plus le démarrage du moteur de gestion du VPN SSL. Cette régression était apparue en version 4.7.3 suite à la **mise à jour du composant OpenVPN**.

Nouvelles fonctionnalités et améliorations de SNS 4.7.3

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`.

Certificats et PKI

Référence support 83969

Lorsqu'un certificat provoque une remontée d'alarme (certificat révoqué, certificat expiré ...), un message indiquant la raison de cette alarme est désormais affiché au survol du certificat concerné dans le module **Certificats et PKI**.

Supervision - Tableau de bord - Certificats

Référence support 85412

Lorsqu'un certificat provoque une remontée d'alarme, notamment lorsque le TPM (Trusted Platform Module) a été initialisé et que tous les certificats présents sur le firewall ne sont pas protégés par ce TPM, le survol de l'indicateur de santé **Certificats** du module **Tableau de bord** entraîne l'affichage d'un message indiquant la raison de cette alarme.

Vulnérabilités résolues de SNS 4.7.3

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.

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.

Correctifs de SNS 4.7.3

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 4.7.0.

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).

Même si le paquet de la machine infectée ou de la sonde d'intrusion était correctement bloqué, l'interface source de la machine cliente était cependant 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 4.7.2 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

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 (Associations de Sécurité) n'échoue plus lorsque le correspondant contient une plage d'adresses IP.

Annuaire LDAP interne

Référence support 84495

Des optimisations permettent d'éviter un rechargement systématique du moteur de gestion des annuaires LDAP pour la prise en compte de certaines modifications.

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 dans les versions SNS 4.6.9 et 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.

VPN IPsec - IKEv1 - Authentication par certificat et XAuth

Référence support 85283

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.

Chiffrement / PKI

Référence support 85476

La commande CLI / Serverd `CONFIG FWADMIN PROTECT` permettait à tort de déchiffrer toute clé privée protégée par le TPM sans exiger le mot de passe du TPM. Ce problème a été corrigé.

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...).

VPN IPsec

Référence support 85423

Conformément à ce qui était annoncé dans les Notes de versions SNS 4.7.1, l'assistant de création d'une règle de VPN IPsec mobile en mode *config* permet désormais de sélectionner un groupe de réseaux comme ressources locales.

Assistant de création d'un cluster

Référence support 85405

La présence sur le firewall d'une interface incluse dans un bridge ou d'une interface sans adresse IP n'empêche plus le lancement de l'assistant de création d'un cluster.

Nouvelles fonctionnalités et améliorations de SNS 4.7.2 EA

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
```

Plus d'informations sur la commande `CONFIG PROTOCOL SSL IPS CONFIG`.

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 4.7.2 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

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, le délai de changement de passerelle a été raccourci (passage de 25 à 9 secondes maximum).

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.

Vulnérabilités résolues de SNS 4.7.2 EA

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 4.7.2 EA

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.

VPN IPsec - 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.

Les CRL sont désormais stockées dans le répertoire *~/Data* du firewall SNS. Auparavant, les CRL étaient stockées dans le répertoire *ConfigFiles/Certificates/*.

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.

Classification d'URL Extended Web Control (EWC) et filtrage SSL

Référence support 85374

Après plusieurs accès à une même URL interdite, la page de blocage affichée et le log relatif au protocole SSL indiquaient à tort la catégorie *default* au lieu de la catégorie d'appartenance de l'URL. Cette anomalie a été corrigée.

Firewalls industriels SNi40

Référence support 85078

Sur un firewall SNi40 avec le bypass configuré en mode Sûreté, le mode actif du bypass pouvait être affiché à tort comme étant le mode Sécurité. Ce problème a été corrigé.

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 4.7.2 ou supérieure.

Répartition de charge IPsec sur les CPU - Firewalls modèles SN510, SN2000, SN2100 et SN3100

Un problème d'accès concurrentiels dans le mécanisme de répartition de charge du chiffrement IPsec sur les CPU a été corrigé pour les firewalls modèles SN510, SN2000, SN2100 et SN3100. Pour rappel, la répartition de charge de chiffrement IPsec est configurable via la commande CLI / Serverd `CONFIG IPSEC CRYPTOLB UPDATE`.

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

Référence support 84612

Des contrôles ont été ajoutés afin d'interdire une valeur d'argument *ping* supérieure à la moitié de celle de l'argument *pingrestart* pour la commande CLI / Serverd `CONFIG OPENVPN UPDATE`. Une telle configuration empêchait le client SSL VPN de ré-établir un tunnel suite à une déconnexion et nécessitait un redémarrage du service SSL VPN sur le poste client.

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

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.

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.

Routage

Référence support 85320

La mise à jour en version 4.7.2 EA 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.

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 4.7.1 EA

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 4.7.1 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 4.7 ou supérieure, veuillez consulter la Note Technique Migrer une politique de sécurité vers la nouvelle base d'URL EWC.

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 4.7 et supérieures et 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 4.7, 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 4.7, 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.

Méthode d'authentification Agent TS (authentification Citrix / RDS)

La version SNS 4.7 introduit une méthode d'authentification transparente multi-utilisateurs destinée aux infrastructures de postes virtuels (Virtual Desktop Infrastructure - VDI) : la méthode Agent TS.
Cette méthode repose sur des échanges entre le firewall SNS et un ou plusieurs agents nommés SN TS Agent déployés directement sur les serveurs VDI (Citrix Virtual Apps and Desktops ou Microsoft Remote Desktop Services).

Un firewall SNS peut gérer jusque 100 Agents TS.

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

VPN SSL - Performances accrues

La version SNS 4.7 permet d'établir simultanément un nombre plus important de tunnels VPN SSL sur certains modèles de firewalls. Le débit de données transitant dans chaque tunnel VPN SSL a également été augmenté.

	Nombre de connexions VPN SSL UDP simultanés	
Modèle	**Avant SNS v4.7**	**SNS v4.7**
SN510	100	100
SN710	150	150
SN-M-Series-720	300	300
SN910	150	500
SN-M-Series-920	500	500
SN1100	500	800
SN2100	400	1000
SN3100	500	1000
SN6100	500	1000

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).

Active Update hors ligne

La version SNS 4.7 introduit la possibilité de mettre à jour depuis l'interface Web d'administration les différentes bases de sécurité à l'aide d'un unique pack de mises à jour téléchargé depuis votre espace client MyStormshield.

La date des dernières mises à jour de bases de sécurité réalisées hors ligne ou en ligne via Active Update est désormais affichée dans le widget Active Update du module de Supervision système. Un message d'avertissement vous indique également lorsque la dernière mise à jour d'une base est trop ancienne.

Plus d'informations sur Active Update hors ligne.

Catégorie Web "URL compromises"

Une catégorie "URL compromises" a été ajoutée aux modules **Filtrage URL** et **Filtrage SSL** afin de permettre le blocage d'URL malveillantes lorsque le filtrage d'URL / Filtrage SSL sont utilisés dans les règles de filtrage.
Cette catégorie, mise à jour en permanence par les équipes de sécurité Stormshield afin de vous offrir une sécurité accrue, est récupérable via Active Update (hors ligne / en ligne).

Logs - Informations complémentaires sur les adresses IP ou domaines bloqués

Lorsqu'une communication avec une adresse IP ou un domaine malveillant est bloquée, les logs proposent désormais un lien direct vers des informations complémentaires hébergées sur le portail Stormshield Security.

TPM - Sécurisation possible de toutes les clés privées

A compter de la version SNS 4.7, pour les firewalls disposant d'un TPM, toutes les clés privées de certificats peuvent être sécurisées avec le module TPM. Cette fonctionnalité était jusqu'ici limitée aux certificats utilisés pour l'authentification dans le cadre du VPN IPsec.

Désormais, cette méthode de sécurisation peut également s'appliquer aux certificats utilisés notamment dans les cas suivants :

- Déchiffrement SSL/TLS,
- Communication entre firewalls SNS et serveurs SMC,
- Envois de logs vers un serveur syslog,
- VPN SSL,
- LDAP interne.

Plus d'informations sur la sécurisation des clés privées par le TPM.

NOTE
Après la mise à jour d'un firewall en version SNS 4.7.1, si le TPM était déjà initialisé et des certificats déjà protégés, un message sur le tableau de bord peut indiquer à tort que le TPM n'a pas été initialisé ou que les mises à jour automatiques ne sont pas protégées par mot de passe.

Pour résoudre ce problème, vous devez protéger les certificats utilisés dans la configuration du firewall et qui ne sont pas encore protégés avec le TPM. Pour cela, utilisez la commande CLI / Serverd "`MONITOR CERT`" pour afficher les certificats concernés puis protégez-les dans le module **Configuration** > **Objets** > **Certificats et PKI**.

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*

Sécurité accrue

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.

Intégration

Qualité de service (QoS)

La version SNS 4.7 introduit le support de la QoS sur les interfaces de type PPPoE et PPTP.

Sauvegardes automatiques

Il est désormais possible de sélectionner l'interface réseau utilisée pour se connecter aux serveurs de sauvegardes automatiques (serveurs personnalisés et serveurs Stormshield Cloud backup).

Cloud Amazon Web Services

Depuis la version SNS 4.7, les instances Stormshield Elastic Virtual Appliances (EVA) déployées dans le cloud Amazon Web Services peuvent utiliser les interfaces Elastic Network Adapters (ENA).

Expérience utilisateur

Politique VPN IPsec nomades en mode *config*

Il est désormais possible de sélectionner un groupe de réseaux en tant que réseau local lors de la création ou la modification d'une politique IPsec nomade en mode *config*.
Notez que l'utilisation du client Stormshield IPsec VPN ou du client VPN TheGreenBow impose que ce groupe ne contienne pas plus de 8 réseaux / routes.

Protections applicatives

Il est désormais possible de rechercher les protections IPS à l'aide de leur identifiant.

Indicateur de santé - Serveurs NTP

Un indicateur de santé concernant les serveurs NTP a été ajouté au **Tableau de bord** ainsi qu'au module de **Supervision Système**.

Cet indicateur permet notamment :

- De mettre en avant un défaut ou une anomalie de réponse d'un serveur NTP configuré sur le firewall,
- De signaler l'absence de configuration NTP lorsqu'un service activé sur le firewall nécessite une attention particulière sur la synchronisation de temps pour fonctionner correctement (exemple : authentification TOTP).

Rechargement programmé des règles de filtrage

Référence support 81691

Le rechargement programmé des règles de filtrage (commande *enfilter -u* déclenchée chaque jour à minuit) peut désormais être désactivé en affectant la valeur 0 au jeton de configuration *DailyRefresh* présent dans la section *[Global]* du fichier de configuration *ConfigFiles/Filter/filter*.

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.

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.

Haute disponibilité

Synchronisation *Unicast*

Il est désormais possible de définir une synchronisation *Unicast* entre les membres d'un cluster lors de sa création. Cette option est nécessaire pour déployer la haute disponibilité dans une infrastructure Cloud ne supportant pas le protocole *Multicast*.

Synchronisation des adresses MAC

Il est désormais possible de choisir si la synchronisation des adresses MAC doit être forcée lors d'une bascule du cluster (module **Haute Disponibilité** > **Configuration avancée** > option **Forcer la synchronisation des adresses MAC**).

Pour les machines virtuelles (EVA) déployées en version 4.7 ou supérieure et configurées en haute disponibilité, cette synchronisation est à présent désactivée par défaut. Pour les firewalls physiques en configuration d'usine, cette synchronisation reste activée par défaut.

Il peut être nécessaire de désactiver cette option dans des configurations utilisant les agrégats de liens (LACP) par exemple.

Plus d'information sur la haute disponibilité.

Correctifs de SNS 4.7.1 EA

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.

Commande *sysinfo*

Référence support 84415

La commande de diagnostic système *sysinfo* n'appelle plus à tort certains binaires supprimés dans le cadre du durcissement du système d'exploitation du firewall.

Authentification SSH multi-utilisateur

Références support 84532 - 84847

Lorsque la clé SSH du compte admin était enregistrée sur le firewall, aucun autre administrateur ne pouvait se connecter en SSH au firewall. Cette régression, apparue en version SNS 4.3.3, a été corrigée.

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.

Authentification RADIUS

Référence support 84162

La connexion d'un administrateur via une méthode RADIUS ne générait aucune entrée dans le fichier des logs d'authentification. Cette anomalie a été corrigée.

Références support 84484 - 84497

Le temps de réponse maximal par défaut pour une requête Radius peut désormais être augmenté pour atteindre 600 secondes. Il peut être modifié à l'aide de la commande CLI / Serverd `CONFIG.AUTH.RADIUS`.

Plus d'information sur la commande CLI / Serverd `CONFIG.AUTH.RADIUS`.

Authentification TOTP et accès SSH au firewall

Référence support 84947

L'authentification TOTP n'était pas appliquée pour une connexion console via SSH à destination du firewall lorsque la règle d'authentification TOTP précisait une source d'authentification différente de l'objet *any*.

Services Web personnalisés

L'icône indiquant l'utilisation d'un service Web personnalisé dans la configuration du firewall n'apparaît plus à tort en vert lorsque le service appartient à un groupe mais n'est pas utilisé.

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.

Routage multicast dynamique

Des optimisations ont été apportées au mécanisme d'élection dynamique de Rendez-vous Point (RP) dans le cas d'une architecture où plusieurs firewalls sont candidats à l'élection de RP avec des plages multicast qui se chevauchent.

Haute disponibilité (HA) - SNMPv3

Référence support 81702

Les paramètres SNMPv3 *EngineBoots* et *EngineTime* 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.

Base objets - Import

Référence support 83327

Suite à l'import d'une base au travers d'un fichier CSV, les objets importés n'apparaissaient pas immédiatement dans la base locale du firewall même après avoir rafraîchi l'écran. Une action de déconnexion / reconnexion à l'interface Web d'administration était nécessaire pour faire apparaître ces objets. 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.

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.

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.

Portail captif d'authentification et VPN SSL

Références support 84801

La configuration du portail captif sur le port d'écoute réservé et utilisé par le VPN SSL (port *sslvpn*) déclenche désormais une erreur indiquant que ce port est réservé.

Moteur de prévention d'intrusion

Protocole OPC UA

Un contrôle réalisé sur le jeton d'authentification de la commande OPC UA *CreateSessionRequest* a été supprimé. Ce contrôle pouvait bloquer à tort du trafic OPC UA légitime.

Protocole DCERPC

Des UUID appartenant à la classe "[MS-WMI]: Windows Management Instrumentation Remote Protocol" ont été ajoutées dans la liste des UUID connues du moteur d'analyse protocolaire DCERPC afin de ne plus déclencher à tort l'alarme bloquante "UUID DCERPC inconnue" (alarme nb-cifs:310).

Ces UUID sont les suivantes :

- '027947E1-D731-11CE-A357-000000000001':'IEnumWbemClassObject',
- '9556DC99-828C-11CF-A37E-00AA003240C7':'IWbemServices',
- 'F309AD18-D86A-11D0-A075-00C04FB68820':'IWbemLevel1Login'.

Analyse des options TCP

Référence support 83234

Le déclenchement de l'alarme "Option TCP au mauvais moment" (tcpudp:58), lorsque celle-ci est positionnée sur l'action *passer*, n'interrompt plus à tort l'analyse des options suivantes du paquet TCP et ne provoque plus la levée de l'alarme "Mauvais numéro de séquence TCP" (tcpudp:16).

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 supérieur à 128 Ko via une requête LDAP.

Protocole TLS v1.3

Références support 84244 - 84761 - 84780- 84783 - 84784 - 84785 - 84786 - 84787 - 84788 - 84789 - 84791 - 84796 - 84799 - 84805 - 84806 - 84845

Un problème a été résolu dans le moteur d'analyse du protocole TLS v1.3. Cette régression, qui pouvait entraîner un blocage du firewall, était apparue en version SNS 4.5.3.

Filtrage - Services Web

Référence support 84721

L'utilisation dans deux règles de filtrage distinctes de deux services Web dont le nom différait uniquement par leur dernier caractère entraînait à tort la détection d'un chevauchement de ces règles de filtrage par le vérificateur de cohérence. Cette anomalie a été corrigée.

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.

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.

Réseau

Module 8 ports RJ45

Références support 82270 - 85269

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

Administrateurs avec droits d'accès limités

Des contrôles ont été ajoutés afin qu'un administrateur authentifié avec des droits limités ne puisse pas afficher des modules normalement non autorisés en saisissant directement une URL contenant le nom du module concerné.

Télémétrie

Un administrateur autre que le super administrateur (compte admin) ne peut plus activer ou désactiver la télémétrie.

Configuration du firewall via SSH

Dans le module **Système** > **Configuration** > onglet **Administration du firewall**, les champs liés à l'**Accès distant par SSH (nécessite le compte admin)** sont désormais tous grisés pour un administrateur connecté différent du super-administrateur (compte *admin*).

Politique d'authentification

Il n'était plus possible de réaliser un glisser / déplacer simultané de plusieurs règles dans la grille de la politique d'authentification. Cette régression, apparue en version SNS 4.1, a été corrigée.

Un double clic sur l'une des colonnes **Source** ou **Méthodes (évaluées par ordre)** d'une règle d'authentification pour laquelle la méthode était positionnée sur "Interdire" ne remplace plus à tort cette valeur "Interdire" par "Méthode par défaut".

Relai DHCP - Navigateur Google Chrome

Référence support 84593

Dans le module de configuration d'un relai DHCP (module **DHCP** > **Relai DHCP**), la modification de l'**Adresse IP utilisée pour relayer les requêtes DHCP** par un administrateur connecté à l'interface Web d'administration du firewall au travers du navigateur Google Chrome est désormais bien prise en compte et n'est plus réinitialisée à la valeur "automatique" en changeant de module.

Préférences - Affichage des logs

Référence support 84956

Les valeurs choisies pour les champs **Nombre de lignes affichées par page** et **Nombre de caractère minimum pour lancer la recherche** du module des **Préférences** sont désormais correctement interprétées et n'empêchent plus l'affichage des logs. Cette régression était apparue en version SNS 4.4.

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.

Antivirus

Référence support 85330

Si vous appliquez sur le firewall une licence comportant uniquement le moteur antiviral ClamAV, le module **Antivirus** s'affiche désormais correctement et le message "Aucun accès" n'apparaît plus.

Version 4.7.0 non publiée

La version 4.7.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités et améliorations de SNS 4.6.11

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).

Vulnérabilités résolues de SNS 4.6.11

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.

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.

Correctifs de SNS 4.6.11

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.

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 de 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.

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 4.6.8.

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).

Même si le paquet de la machine infectée ou de la sonde d'intrusion était correctement bloqué, l'interface source de la machine cliente était cependant 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.

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).

Nouvelles fonctionnalités et améliorations de SNS 4.6.10

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 4.6.10 ou supérieure, cette encapsulation est activée par défaut.

VPN IPsec mode Diffusion Restreinte (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 4.6 (à partir de la version 4.6.10), 4.3 LTSB (à partir de la version 4.3.21 LTSB) et les versions SNS 4.7 et supérieures respectent cette recommandation.

Si le mode IPsec DR est activé sur un firewall SNS en version 4.6.10, 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 4.6.10, 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.

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.

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
```

Plus d'informations sur la commande **CONFIG PROTOCOL SSL IPS CONFIG**

Vulnérabilités résolues de SNS 4.6.10

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 4.6.10

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.

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.

Les CRL sont désormais stockées dans le répertoire *~/Data* du firewall SNS. Auparavant, les CRL étaient stockées dans le répertoire *ConfigFiles/Certificates/*.

VPN IPsec - IKEv1 - Authentication par certificat et XAuth

Référence support 85283

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.

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.

Firewalls industriels SNi40

Référence support 85078

Sur un firewall SNi40 avec le bypass configuré en mode Sûreté, le mode actif du bypass pouvait être affiché à tort comme étant le mode Sécurité. Ce problème a été corrigé.

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 4.6.10 ou supérieure.

Répartition de charge IPsec sur les CPU - Firewalls modèles SN510, SN2000, SN2100 et SN3100

Un problème d'accès concurrentiels dans le mécanisme de répartition de charge du chiffrement IPsec sur les CPU a été corrigé pour les firewalls modèles SN510, SN2000, SN2100 et SN3100. Pour rappel, la répartition de charge de chiffrement IPsec est configurable via la commande CLI / Serverd `CONFIG IPSEC CRYPTOLB UPDATE`.

Module 8 ports RJ45

Références support 82270 - 85269

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.

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.

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.

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 4.6.9

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 4.6.9 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 4.6.2.
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.

Connexion SSH au firewall

Sur un firewall en configuration d'usine et en version SNS 4.6.x ou supérieure, 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 4.6.9.

Vulnérabilités résolues de SNS 4.6.9

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 4.6.9

Système

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.

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 d'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.

Objets routeur

Référence support 84963

La mise à jour en version SNS 4.6.9 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 4.6.2.

Tunnel GRETAP

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

Authentification - RADIUS

Références support 84484 - 84497

Le temps de réponse maximal par défaut pour une requête Radius peut désormais être augmenté pour atteindre 600 secondes. Il peut être modifié à l'aide de la commande CLI / Serverd `CONFIG.AUTH.RADIUS`.

Plus d'information sur la commande CLI / Serverd `CONFIG.AUTH.RADIUS`.

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.

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 SSL - TOTP

Références support 84966 - 84992

L'utilisation d'un certificat personnalisé pour le service VPN SSL et de l'authentification via TOTP avec des clients VPN SSL Stormshield n'entraîne plus la nécessité pour le client de saisir un deuxième code TOTP à chaque connexion.

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`.

Plus d'informations sur 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.

Protocole OPC-DA

Référence support 85129

L'entrée *OPC-DA 3.0 Type Lib* n'apparaît plus à tort à plusieurs reprises dans la liste des opérations OPC-DA à analyser.

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 4.6.8

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.

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.

Correctifs de SNS 4.6.8

Système

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.

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.

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 4.6.6, pouvait empêcher le chargement de la politique de filtrage.

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.

Interface Web d'administration

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 4.6.7

Protocole HART-IP

La version SNS 4.6.7 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 4.6.7

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 4.6.7

Système

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 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.

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 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*.

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.

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.

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 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 4.6.7 ou supérieure.

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.

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 4.5.0.

Filtrage et NAT

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

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.

Filtrage et NAT - Services Web

Référence support 84722

L'action *bloquer* fonctionne désormais dans une règle de filtrage utilisant un service Web dont le nom comporte exactement 20 caractères.

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.

Vulnérabilités résolues de SNS 4.6.6

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 4.6.6

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).

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 - 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.

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.

Authentification Kerberos et TOTP

Référence support 84859

Dans une configuration utilisant l'authentification Kerberos et TOTP, le champ Code OTP est désormais correctement affiché sur le portail captif. La connexion d'un utilisateur ne retourne donc plus l'erreur "Code TOTP manquant".

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.

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.

Paquets multicast

Référence support 85180

La ré-écriture des paquets multicast par le moteur de prévention d'intrusion pouvait amener à un double déréférencement provocant un redémarrage inopiné du firewall. Ce problème a été corrigé.

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 4.6.5

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**.

Correctifs de SNS 4.6.5

NOTE
Le correctif ajouté en version 4.6.4 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

SNMPv3 - *Traps*

Référence support 85085
Suite à la mise à jour d'une configuration SNMPv3 existante en version SNS 4.4 ou supérieure, le type d'authentification attribué aux *traps* SNMPv3 était erroné. Cette anomalie a été corrigée.

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 d'un passage en version SNS 4.6.5 ou supérieure. Pour rappel, cette mise à jour était déjà appliquée depuis la version SNS 4.6.2 aux modèles de firewalls dont la liste est disponible dans la section Correctifs de SNS 4.6.2.

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.

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 4.6.4

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 4.6.4

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.

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 4.6.4

Système

Agent SNMP

Références support 84911- 84990

Un problème de fuite mémoire a été résolu dans l'agent SNMP. Cette régression était apparue en versions SNS 4.5.4 et 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) - 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 versions SNS 4.3.3 et 4.4.0, 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 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*.

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`.

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.

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

Protocole ICMPv6

Une anomalie déclenchant à tort l'alarme "Message ICMP invalide" (icmp:67), lorsque cette alarme était associée à l'action *Passer*, a été corrigée dans le moteur d'analyse protocolaire ICMPv6.

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.

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.

Vulnérabilités résolues de SNS 4.6.3

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 4.6.3

Système

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 à tort d'utiliser le lien de secours. Cette anomalie a été corrigée.

Supervision du système - Consommation CPU

Référence support 66123

Le mécanisme de supervision de la consommation CPU pouvait remonter des valeurs non réalistes. Cette anomalie a été corrigée.

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.

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 4.6.3.

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.

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.

Correctifs de SNS 4.6.2

Système

DMA remapping (DMAR) sur les firewalls SN-M-Series-720 et SN-M-Series-920

Référence support 84882

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.

Supervision des modules d'alimentation sur les firewalls SN-M-Series-720 et SN-M-Series-920

Référence support 84880

Un mauvais ordonnancement des tâches au démarrage du firewall pouvait entraîner à tort une alerte concernant le fonctionnement des modules d'alimentation sur les firewalls SN-M-Series-720 et SN-M-Series-920. Ce problème a été corrigé.

Mise à jour du firmware des disques SSD

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 4.6.2 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).

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.

Interfaces réseau - Firewalls modèles SN-M-Series-720 et SN-M-Series-920

La vitesse des interfaces réseau des firewalls modèles SN-M-Series-720 et SN-M-Series-920 peut désormais être forcée à 2.5 Gbit/s.

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.

Mise à jour - Routage statique

Référence support 84716

La mise à jour en version SNS 4.6 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.

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**).

Le contrôle concernant l'activation / désactivation du mode verbeux pour le proxy avait été supprimé à tort et est de nouveau disponible dans le mécanisme de génération du rapport système. Cette régression était apparue en version 4.5.1.

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 4.5.2 au sujet du nombre maximal de machines protégées a été corrigé. Ainsi, lors de la mise à jour du firewall en version SNS 4.6.2, un second redémarrage est automatiquement déclenché si la configuration le nécessite.

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.

Correctifs de SNS 4.6.1

Système

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.

Requêtes ARP vers des interfaces GRE

Référence support 84625

Le firewall n'émet plus inutilement de requêtes ARP vers les interfaces supportant des tunnels GRE. Cette régression était apparue en version SNS 4.4.

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.

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 blocage inopiné du trafic réseau nécessitant un redémarrage du firewall. Ce problème a été corrigé.

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`.

Authentification - TOTP

Référence support 84779

Pour modifier son mot de passe via le portail captif, un utilisateur enrôlé doit désormais renseigner un code TOTP.

Référence support 84808

L'authentification via TOTP n'est désormais plus sensible à la casse pour les noms d'utilisateurs.

SN SSL VPN Client et TOTP

Référence support 84689

Lors de la première connexion à l'aide de SN SSL VPN Client avec l'authentification TOTP activée, il était nécessaire de laisser le champ du codeTOTP vide afin de permettre la récupération automatique du fichier de configuration. Le code TOTP ne devait être renseigné que pour les connexions suivantes. Ce problème a été corrigé.

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".

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).

Nouvelles fonctionnalités et améliorations de SNS 4.6.0

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 d'un firewall utilisant l'antivirus avancé depuis une version SNS 3.x ou 4.x vers SNS 4.6, sauf les versions SNS 4.3 depuis la version 4.3.13 car l'antivirus avancé repose déjà sur *Bitdefender*,
- Lors du passage de l'antivirus *ClamAV* à l'antivirus avancé sur un firewall en version SNS 4.6,
- Lors de la bascule d'un firewall passif à l'état actif après la mise à jour d'un cluster de firewalls utilisant l'antivirus avancé depuis une version SNS 3.x ou 4.x vers SNS 4.6, sauf les versions SNS 4.3 depuis la version 4.3.13 car l'antivirus avancé repose déjà sur *Bitdefender*.

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).

Télémétrie - Antivirus

Une nouvelle sonde de télémétrie permet de remonter le nombre de virus détectés par l'antivirus avancé lorsque celui-ci est activé sur le firewall.

En transmettant ces données anonymes, vous aidez Stormshield à améliorer les futures plate-formes matérielles et versions SNS.

Plus d'information sur le service de télémétrie.

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 4.6.0

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 4.6.0

Système

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.

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.

Firewalls SN160(W) - SN210(W) - SN310

Référence support 84725

Certaines adresses MAC clientes de préfixe 6c:a1:00 ne conduisent plus à des réponses ARP corrompues de la part des firewalls modèles SN160(W), SN210(W) et SN310. Cette régression était apparue en version SNS 4.5.

Authentification

Référence support 84358

Lorsqu'un utilisateur saisit un mot de passe erroné pour une connexion via le client VPN SSL ou sur le portail captif, le firewall ne génère plus à tort l'erreur "LDAP unreachable Bind error" dans le fichier de logs d'alarmes.

Authentification - TOTP

Référence support 84660

La modification du port d'écoute par défaut de l'interface Web d'administration (TCP/443) est désormais correctement répercutée sur le lien hébergé sur la fenêtre de connexion au firewall et pointant vers la page d'enrôlement TOTP.

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.

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.

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.

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

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 4.6.0. Il est également désactivé par défaut dans le profil entrant d'analyse SSL *SSL_00* pour les firewalls en configuration d'usine en version 4.6.0 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**.

Nouvelles fonctionnalités et améliorations de SNS 4.5.4

Authentification TOTP

L'interface de configuration de la méthode d'authentification TOTP a évolué afin de fluidifier l'expérience utilisateur.

Correctifs de SNS 4.5.4

NOTE
Le correctif ajouté en version 4.5.3 concernant la vérification des certificats serveurs TLS (Référence support 84244) a été supprimé. Il sera revu et réintégré dans une version ultérieure.

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 en tant que super-administrateur (compte *admin*),
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.

Moteur de prévention d'intrusion

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.

Nouvelles fonctionnalités et améliorations de SNS 4.5.3

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

Les versions SNS 4.5.3 et supérieures supportent les firewalls SN-M-Series-720 et SN-M-Series-920.

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

Vulnérabilités résolues de SNS 4.5.3

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 4.5.3

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.

Authentification - TOTP

L'action de décocher la case d'authentification via TOTP sur le portail captif (menu **Utilisateurs** > **Authentification**) désactivait à tort la page d'enrôlement TOTP sur le portail captif, cette page étant nécessaire pour les autres modules utilisant potentiellement la méthode TOTP (VPN SSL, Interface Web d'administration, SSH / Console, IPsec / Xauth). Cette anomalie a été corrigée.

VPN IPsec

Référence support 84568

Un paramètre manquait à l'option *keepalive* lors de l'appel de la commande de rechargement d'une politique IPsec. Cette anomalie entraînait l'événement système 52 "Une événement a renvoyé un code d'erreur non géré : IPSEC_KEEPALIVE_30->4" mais n'empêchait cependant pas le rétablissement des tunnels VPN IPsec.
Cette régression, apparue en version SNS 4.3.8, a été corrigée.

Référence support 84569

L'envoi réussi d'un paquet *keepalive* ne provoque plus à tort l'émission de l'événement système 52 "Un événement a renvoyé un code d'erreur non géré : IPSEC_KEEPALIVE_30->4".
Cette régression était apparue en version SNS 4.3.8.

Références 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.

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*.

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.

Services Web personnalisés

Référence support 84496

Dans certaines conditions, les services Web personnalisés comportant un caractère joker ("*") dans leur FQDN pouvaient ne pas être correctement pris en compte dans des règles de filtrage bloquantes. Cette anomalie a été corrigée.

Dans le cas d'une base de services Web personnalisés de grande taille, l'import de services Web personnalisés s'interrompt et un message d'avertissement est affiché lorsque la partition destinée à recevoir la base de services personnalisée atteint 95% de remplissage.

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.

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.

VPN SSL

Référence support 84610

La fonction *inactive=<seconds>* du VPN SSL peut désormais être correctement appliquée via la commande CLI / Serverd `CONFIG OPENVPN UPDATE`.

Moteur de prévention d'intrusion

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.

Protocole IEC61850 MMS - Mode IDS

Le niveau d'inspection IDS appliqué à une règle de filtrage portant sur des flux IEC61850 MMS ne se comporte plus à tort comme le niveau d'inspection IPS et ne bloque plus les paquets incriminés au lieu de déclencher uniquement les alarmes correspondantes.

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).

Protocole TLS - Vérification des certificats serveurs

Référence support 84244

Des optimisations ont été apportées au mécanisme de vérification des certificats serveurs : lorsque plusieurs demandes concernant la vérification d'un même certificat serveur sont reçues de manière quasi-simultanée, une seule requête interne est émise afin de ne pas saturer la file d'attente du mécanisme de vérification et de ne plus risquer de provoquer un blocage de celui-ci pendant plusieurs dizaines de secondes.

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".

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.

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 4.5.2

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 4.5.2

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 4.5.2

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.

Sauvegardes de configuration

La base de données TOTP est désormais incluse dans les éléments sauvegardés.

Authentification TOTP

Dans le cas d'un nom de domaine LDAP d'une longueur supérieure à 30 caractères, le code QR d'enrôlement et les informations TOTP s'affichent désormais correctement sur le portail d'authentification.

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.

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.

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 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.

Nouvelles fonctionnalités et améliorations de SNS 4.5.1

IMPORTANT
La version SNS 4.5 est exclusivement compatible avec le client VPN SSL 3.1 ou le client OpenVPN 2.5 (ou supérieur).
Il est nécessaire de mettre à jour le client VPN SSL (ou OpenVPN) sur les postes clients avant de mettre à jour le firewall en version SNS 4.5.

Authentification à 2 Facteurs (2FA - *2 Factors Authentication*)

La version SNS 4.5 permet d'accroître la sécurité des authentifications gérées par le firewall grâce à une nouvelle méthode d'authentification 2FA permettant d'utiliser des mots de passe à usage unique basés sur le temps (TOTP - *Time-based One-time Password*).
Cette sécurisation supplémentaire des accès est embarquée sur le firewall et ne nécessite pas la mise en place d'une solution TOTP tierce. Les utilisateurs soumis à l'authentification TOTP SNS n'ont besoin que d'une application sur leur smartphone ou dans leur navigateur Internet pour générer les codes d'authentification TOTP.

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

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

Plus d'information sur l'authentification TOTP.

Routage multicast dynamique

IMPORTANT
Cette fonctionnalité est en accès anticipé et n'est pas destinée à des firewalls en production. Veuillez impérativement consulter les Limitations et précisions sur les cas d'utilisation avant d'activer cette fonctionnalité.

La versions SNS 4.5 supporte le routage multicast dynamique basé sur les protocoles IGMPv2 et v3 et PIMv2.
Le paramétrage du routage multicast dynamique est réalisé au sein du module **Configuration** > **Réseau** > **Routage multicast** ou à l'aide des commandes CLI / Serverd `CONFIG MULTICASTROUTING`.

NOTE
Il n'est pas possible d'activer simultanément le routage multicast dynamique et le routage multicast statique.

Plus d'information sur le routage multicast dynamique.

Protocole S7 Plus

La version SNS 4.5 permet désormais l'analyse du protocole industriel de communication S7 Plus (propriété intellectuelle de Siemens).

Plus d'information sur l'analyse protocolaire S7 Plus.

Protocole OPC-DA

Le moteur d'analyse protocolaire permet désormais de distinguer les opérations de lecture et d'écriture pour le protocole OPC-DA. Ceci garantit un contrôle plus fin des flux OPC-DA traversant le firewall.

Plus d'information sur l'analyse protocolaire OPC-DA.

Protocole IEC 60870-5-104

Référence support 82460

Une nouvelle alarme "IEC 60870-5-104 : Message de TESTFR act invalide au regard du contexte de la connexion" (iec104:756) a été créée afin de pouvoir laisser passer les paquets IEC 60870-5-104 *TESTFR act* (contrôle d'état *stateful* des paquets) tout en laissant active l'analyse protocolaire IEC 60870-5-104.

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.

Déconnexion automatique des sessions VPN SSL expirées

Il est désormais possible de configurer un délai maximal d'inactivité sur le service VPN SSL après lequel les sessions VPN SSL inactives sont automatiquement déconnectées.

La configuration de cette option est exclusivement réalisable à l'aide de la commande CLI / Serverd :

```
CONFIG OPENVPN UPDATE Inactive=x (seconds)
```

Pages de blocage HTTPS

Les pages permettant de bloquer les flux HTTPS non autorisés par le filtrage SSL ont été modifiées. Leur modèle est entièrement personnalisable.

Télémétrie

De nouvelles données sont remontées par le service de télémétrie de la version SNS 4.5 :

- Nombre d'objets par type,
- Nombre de règles de filtrage et de NAT,

- Nombre d'alertes IPS,
- Nombre de signatures IPS utilisées.

En transmettant ces données parfaitement anonymes, vous aidez Stormshield à affiner les tailles et limites des futures plate-formes matérielles et versions SNS.

Plus d'information sur le service de télémétrie.

Profils de chiffrement IPsec

Les groupes Diffie-Hellman DH31 et DH32 sont désormais disponibles dans les profils de chiffrement IPsec. Notez que ces profils ne peuvent pas être sélectionnés si le firewall est en mode Diffusion Restreinte.

Plus d'information sur les profils de chiffrement IPsec.

Logs VPN IPsec

Référence support 82931

La ligne de logs "Installing IPSEC SA failed" a été complétée avec les valeurs des *SPI in* et *SPI out* afin de faciliter l'analyse du problème rencontré.

Alerte en cas de mise à jour des utilitaires NVM pour cartes réseau Intel

L'événement 152 "Logiciel de carte réseau" permet d'informer l'administrateur d'une mise à jour automatique ou d'un échec de mise à jour automatique des utilitaires NVM de gestion de versions des firmware de cartes réseau Intel.

Correctifs de SNS 4.5.1

Système

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.

Temps nécessaire pour lister les certificats protégés par TPM

Référence support 83999

Le temps nécessaire pour lister tous les certificats protégés par un TPM a été fortement diminué grâce à la réduction du nombre d'accès au TPM lors de la réalisation de cette opération.

Affichage des commentaires affectés aux membres d'un groupe

Référence support 82069

Les commentaires affectés aux membres d'un groupe sont désormais affichés lors du listage du contenu de ce groupe (survol du groupe avec le curseur ou utilisation de la commande `CONFIG OBJECT GROUP SHOW`).

Authentification par Certificat SSL

Référence support 80325

La suppression de la méthode d'authentification par Certificat SSL ne bloque plus à tort la connexion à l'interface Web d'administration du firewall ou au portail captif d'authentification.

Proxy SSL

Référence support 84316

Une anomalie dans la vérification de la chaîne de confiance par le proxy SSL a été corrigée : l'accès aux serveurs Cisco Webex n'est plus bloqué à tort.

Supervision

Référence support 84203

Lorsque le fichier de données de supervision est corrompu, les services de supervision ne se bloquent plus et un nouveau fichier de données de supervision est généré.

Désactivation de l'interface parente d'un VLAN

Référence support 81749

Lorsque l'interface parente d'un VLAN était désactivé, le firewall envoyait à tort un paquet GARP (*Gratuitous ARP*) portant l'adresse IP de l'interface désactivée, en plus du paquet GARP légitime portant l'adresse IP du VLAN. Cette anomalie a été corrigée.

Manipulation via les commandes CLI / Serverd de clés pré-partagées (PSK - *Preshared keys*) trop longues

Référence support 83626

Les messages d'erreur renvoyés lors de la manipulation (création ou modification via les commandes CLI / Serverd) de PSK trop longues ont été simplifiés. Il n'existe désormais plus qu'un seul message : "PSK too long".

Stockage des logs sur carte SD - Firewalls SN160(W), SN210(W) et SN310

Le formatage du support de stockage des logs ne peut plus être lancé lorsque les logs sont encore actifs.

Réseau

Routage multicast

Référence support 84250

Des paquets multicast fragmentés entrant sur le firewall sont désormais correctement transmis sur l'ensemble des interfaces réseau participant au routage multicast.

Version 4.5.0 non publiée

La version 4.5.0 n'est pas disponible publiquement.

Nouvelles fonctionnalités et améliorations de SNS 4.4.1

Granularité de QoS et de routage par application pour les services Web en fonction du SLA (SD-WAN)

La version SNS 4.4 permet d'identifier à quels services sont associés certains flux Web reconnus du marché, et de distinguer ainsi les flux Salesforce des flux YouTube, Microsoft 365 ou Zoom, par exemple. Des services Web personnalisés peuvent également être créés selon les besoins.
Il devient ainsi possible de définir des politiques fines de SLA, de QoS et de routage par application pour chaque service Web utilisé dans l'entreprise, permettant ainsi d'assurer une connectivité optimale pour les flux Web prioritaires.

Plus d'informations sur les services Web.

Politique de sécurité adaptée aux applications temps réel SaaS

Cette identification des services Web permet également d'adapter la politique de sécurité aux différents flux identifiés en désactivant certaines analyses de sécurité inutiles pour ces flux. Cela permet, par exemple, de ne pas forcer le passage par le proxy de ces flux applicatifs identifiés, accélérant ainsi le passage de ces flux spécifiques tout en déchargeant le proxy au profit des autres flux Web.

Ces objets de type services Web et services Web personnalisés permettent également de lever certaines limitations liées aux objets de type FQDN.

Protocole IEC61850 MMS

Le moteur de prévention d'intrusion assure l'analyse du protocole IEC61850 MMS en complément de l'analyse du protocole MMS.

Support des jumbo frames sur les firewalls modèles SN160(W), SN210(W) et SN310

La version SNS 4.4 introduit le support des *jumbo frames* sur les firewalls modèles SN160(W), SN210(W) et SN310. Ceci permet notamment de configurer correctement ces firewalls dans le cas d'un fournisseur d'accès utilisant une Maximum Transmision Unit (MTU) légèrement supérieure à 1500 octets.

Bien qu'il soit possible de configurer cette MTU jusqu'à une taille de 9198 octets pour les firewalls SN160(W) et SN210(W) et une taille de 8996 octets pour les firewalls SN310, notez que les limitations matérielles de ces modèles impliquent une vérification logicielle des sommes de contrôle des paquets présentant une MTU supérieure à 1600 octets. Ceci peut donc impacter les performances globales de ces modèles de firewalls.

VPN SSL - Lien de secours

Sur un firewall disposant de deux liens Internet distincts, il est désormais possible de définir une adresse IP de secours pour le serveur VPN SSL (réseau différent du réseau incluant l'adresse primaire). Ceci permet de pallier tout problème réseau sur l'interface définie initialement et permet aux clients de continuer d'utiliser le service VPN SSL. Cette information de connexion de secours est automatiquement ajoutée dans le fichier de configuration du client VPN SSL.
La configuration de cette adresse IP de secours est exclusivement réalisable à l'aide des commandes CLI / Serverd :

```
CONFIG OPENVPN UPDATE serverPublicAddrSecondary=w.x.y.z
CONFIG OPENVPN ACTIVATE
```

Il est également possible de configurer le service VPN SSL pour que toutes les sessions VPN SSL ayant atteint la durée maximale d'inactivité configurée soient automatiquement déconnectées.

Performances IPsec

Référence support 81691

Le mécanisme qui optimise la répartition des opérations de chiffrement et de déchiffrement du service IPsec a été modifié. Ceci améliore ses performances dans le cas où le chiffrement est réalisé avec une interface d'entrée dont le trafic est en clair et une interface de sortie dont le trafic est chiffré.

Il est désormais possible de répartir de manière statique les CPU qui traiteront les paquets du service IPsec sur le firewall. Cette configuration s'effectue uniquement à l'aide de la commande CLI / Serverd suivante :

```
CONFIG IPSEC CRYPTOLB UPDATE ifincoming=<interface> ifoutgoing=<interface>
state=<0|1>
```

SNMPv3 - Communications sécurisées

La version SNS 4.4 ajoute l'algorithme SHA2 à la liste des algorithmes (SHA1, MD5) pouvant être utilisés pour sécuriser les communications basées sur le protocole SNMPv3.

Agent SNMP - Adresse IP d'écoute du service

Il est désormais possible de préciser l'interface du firewall par laquelle transitent les requêtes SNMP. Ceci est réalisable au travers de l'argument *bindaddr* de la commande CLI / Serverd :

```
CONFIG SNMP SYSTEM BindAddr=<host>
```

En savoir plus

Interdire le retour à une version antérieure de firmware

Sur un firewall en version 4.4, il est possible d'interdire tout retour à une version antérieure de firmware. Ceci permet d'éviter, par exemple, la réintroduction d'une vulnérabilité corrigée depuis.

Ce comportement peut être exclusivement activé via la commande CLI / Serverd :

```
SYSTEM UPDATE DOWNGRADE off
```

Notez que le retour à une version antérieure de firmware est autorisé par défaut.

En savoir plus

Télémétrie

La télémétrie d'un firewall en version SNS 4.4 ajoute aux indicateurs déjà existants (pourcentage d'utilisation de CPU, pourcentage d'utilisation de mémoire et volume de logs générés) des données concernant l'utilisation du proxy : nombre de connexions par protocole et nombre de connexions simultanées au travers du proxy.

En transmettant ces données parfaitement anonymes, vous aidez Stormshield à affiner les paramètres de performances du proxy pour les futures versions SNS.

Vulnérabilités résolues de SNS 4.4.1

Cartes réseau IXL

Une vulnérabilité de sévérité moyenne a été corrigée dans le firmware des cartes réseau IXL.

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2021-049.

Cartes réseau avec contrôleur i210

Des vulnérabilités de sévérité moyenne ont été corrigées dans le firmware des cartes réseau avec contrôleur Intel i210 (firewalls modèles SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SNi20 et SNi40).

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2020-038,
- https://advisories.stormshield.eu/2020-039,
- https://advisories.stormshield.eu/2020-043.

Une vulnérabilité de sévérité faible a été corrigée dans le firmware des cartes réseau avec contrôleur Intel i210 (firewalls modèles SN510, SN710, SN910, SN2000, SN2100, SN3000, SN3100, SNi20 et SNi40).

Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2020-046.

Correctifs de SNS 4.4.1

Système

Connexion SSH sur un cluster

Un administrateur connecté en SSH sur le membre actif d'un cluster avec son propre compte (autre que le compte *admin*) était obligé de saisir le mot de passe du compte *admin* s'il souhaitait également se connecter en SSH au membre passif du cluster. Cette anomalie a été corrigée.

Requêtes HTTP

Référence support 83085

Suite à un changement de composant dans la version SNS 4.1.1, les en-têtes *User-Agent* et *Connection: close* n'étaient plus présentes dans les requêtes HTTP, ce qui pouvait notamment bloquer la récupération automatique des CRL. Ce problème a été corrigé.

Proxy SSL

Référence support 73331

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

Commandes CLI / Serverd

L'aide retournée par la commande `CONFIG IPSEC PEER NEW HELP` indique désormais une plage de valeurs correcte pour le jeton *ikedscp* (<0-63> au lieu de la valeur erronée précédente <0-56>).

L'aide retournée par la commande `CONFIG COMMUNICATION SYSLOG PROFILE UPDATE HELP` précise désormais bien l'existence du jeton *LogRouterStat*.

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.

Filtrage et NAT

Référence support 82534

Une anomalie dans l'export CSV des règles de NAT a été corrigée : cet export prend désormais en compte le contenu de la colonne **Protocole**.

Référence support 79079

Une interface VPN SSL (TCP / UDP) est désormais directement sélectionnable comme interface source au sein d'une règle de filtrage.

VPN IPsec et GRE

Référence support 82051

La double encapsulation ESP -> GRE -> ESP (encapsulation d'un tunnel IPsec dans un tunnel GRE, lui même encapsulé dans un tunnel IPsec) fonctionne de nouveau. Cette régression était apparue en version SNS 4.1.

Limiter la durée des sessions distantes d'administration

La fonction permettant au super-administrateur de limiter la durée maximale d'inactivité autorisée des comptes administrateurs sur le firewall fonctionne à nouveau (régression apparue en version SNS 4.2).

Proxy HTTP

Référence support 80100

La modification de la configuration ICAP (en particulier la désactivation de cette configuration) d'un profil d'analyse protocolaire HTTP alors qu'une connexion impliquant ICAP est en cours ne provoque plus un blocage inopiné du proxy.

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.

Mode console et port série activé

Référence support 82054

Sur un firewall avec la configuration d'affichage mode console et port série activée, il était anormalement obligatoire de connecter un clavier et un écran physique pour pouvoir effectuer un redémarrage en mode *single user* (pour un changement de mot de passe du compte *admin* par exemple). Ce problème a été corrigé.

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.

Prévention d'intrusion

Protocole MMS - Mode IDS

Le mode IDS appliqué à une règle de filtrage portant sur des flux MMS se comportait à tort comme le mode IPS et bloquait les paquets incriminés plutôt que de déclencher uniquement les alarmes correspondantes.

Protocole NTP

L'alarme "NTP : KoD refusé" (alarme ntp:456) n'est plus remontée à tort pour du trafic NTP légitime lorsqu'un paquet KoD (Kiss'o'Death) NTP n'est pas présent dans la liste blanche et est réglé sur l'adresse sur l'adresse IP du serveur NTP.

Protocole SIP

Dans le cas d'une règle de filtrage de flux SIP entrants, avec l'option **Redirection d'appels SIP (UDP) entrants** activée (serveur SIP interne), les requêtes OPTIONS destinées à demander la capacité du serveur SIP ne sont désormais plus bloquées à tort. Cette régression était apparue en version SNS 4.0.3.

Protocoles Ethernet

Le profil d'analyse "(0)" était systématiquement appliqué pour l'analyse des protocoles Ethernet (Profinet IO, Profinet RT, IEC 61850...) et les autres profils étaient ignorés. Ce problème a été corrigé.

Protocole TCP-UDP

Une anomalie dans la gestion du compteur de connexions du moteur d'analyse protocolaire TCP-UDP a été corrigée.

Requêtes ARP pendant un rechargement de configuration du moteur de prévention d'intrusion

Référence support 84272

Un problème d'accès concurrentiel lié à des requêtes ARP effectuées pendant un rechargement de configuration du moteur de prévention d'intrusion pouvait aboutir à un blocage inopiné du firewall. Ce problème a été corrigé.

Interface Web d'administration

Configuration des annuaires

Référence support 82849

Le choix *None* dans le champ de sélection d'un serveur LDAP de secours ne provoque plus à tort une erreur système "Hôte de backup invalide".

VPN IPsec

Référence support 83017

Il n'est désormais plus possible d'affecter la valeur *Inactif* au mode DPD (Dead Peer Detection) lors de la création ou la modification d'un correspondant IPsec. Cette valeur n'était en effet plus supportée et provoquait une erreur système "Erreur d'arguments Commande : CONFIG IPSEC PEER UPDATE dpd_mode=off".

Filtrage URL / SSL / SMTP

Référence support 83587

La modification d'une règle de filtrage URL / SSL /SMTP par une action de glisser / coller n'entraînait pas l'activation du bouton **Appliquer**, bien que la modification ait été prise en compte. Cette anomalie a été corrigée.

Interfaces VLAN

Référence support 83873

L'action de créer un VLAN, de le renommer sans avoir préalablement enregistré la modification de configuration, de créer un autre VLAN sur la même interface physique et de renommer ce deuxième VLAN provoquait une erreur indiquant que les deux VLAN portaient le même nom. Cette anomalie a été corrigée.

Authentification - Annuaire Microsoft Active Directory

Référence support 52539

Lorsque la requête d'affichage des utilisateurs d'un annuaire externe Microsoft Active Directory dépasse le paramètre *MaxSizeLimit* paramétré sur le serveur Microsoft Active Directory, le message d'erreur système *No user found* n'est plus affiché à tort : le firewall affiche désormais le nombre maximal d'utilisateurs pouvant être récupérés et présente un message indiquant que la limite du nombre d'utilisateurs récupérables a été atteinte.

Recherches dans les logs

Référence support 77587

Des optimisations ont été mises en œuvre afin de réduire les temps de recherche dans les logs.

Nom de domaine VPN SSL

Référence support 74996

Le champ **Nom de domaine** DNS destiné aux clients du service VPN SSL refusait à tort le caractère "_". Cette anomalie a été corrigée.

Filtrage

Référence support 80794

Lorsqu'une règle utilisant le protocole ICMP comme critère de filtrage était clonée, que sa copie était modifiée en remplaçant ICMP par un autre protocole, puis que cette copie était à son tour clonée en une troisième règle, alors cette troisième règle comportait à tort les références au protocole ICMP de la règle d'origine. Ce comportement inapproprié, qui empêchait l'activation de la politique de filtrage et provoquait une erreur "Cette règle comporte un filtre sur des messages ICMP alors que le protocole défini n'est pas ICMP", a été corrigé.

Objets réseau - Plage d'adresses MAC

Référence support 77968

Lors de la création d'un objet réseau de type plage d'adresses MAC, l'utilisation de la notation condensée (sans séparateur de type ":" ou "-". Exemple : 01af3b54c89c) est acceptée et ne provoque plus à tort le message d'erreur "Adresse MAC invalide".

Supervision système

Référence support 81041

Le mécanisme de supervision système envoyait à tort et de manière systématique la commande de vérification de la synchronisation du cluster, même lorsque la HA n'était pas activée sur le firewall. Cette anomalie, qui entraînait l'affichage toutes les minutes d'un message d'erreur "200 HA non initialisée" dans le panneau d'affichage des messages situé en bas de chaque module de configuration, a été corrigée.

Version 4.4.0 non publiée

La version 4.4.0 n'est pas disponible publiquement.

Version 4.3 LTSB

Long-Term Support Branch

La version 4.3 LTSB (pour Long-Term Support Branch) de SNS dispose de **Notes de Version dédiées**.

Les versions majeures ou mineures disposant du label LTSB 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**.

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 UPDATE 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 SSO Agent pour Linux

Un nouvel 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 NAT**) 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.

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

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.