STORMSHIELD

STORMSHIELD NETWORK SECURITY

# NOTES DE VERSION

Version 5

Dernière mise à jour du document : 15 octobre 2026

Référence : sns-fr-notes_de_version-v5.1.4-EA

# Table des matières

Historique des modifications ..... 3
Points d'attention pour une mise à jour depuis la dernière version 4.8 LTSB ..... 4
Changements de comportement ..... 6
Vulnérabilités résolues de SNS 5.1.4 EA ..... 12
Compatibilité ..... 13
Problèmes connus ..... 14
Limitations et précisions sur les cas d'utilisation ..... 15
Ressources documentaires ..... 25
Installer cette version ..... 26
Versions précédentes de SNS v5 ..... 29
Contact ..... 85

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 « EA » (Early Adopter)

Les versions mineures ou majeures avec ce label incluent des nouvelles fonctionnalités importantes qui n'ont pas encore été déployées en grand volume en production chez nos clients. Si aucune des nouvelles fonctions n'est nécessaire à votre environnement de production, il est préférable de choisir une version standard ou LTSB pour plus de stabilité.

Le Label EA n'est pas attaché à une version sur le long terme et il disparaît lors de la publication d'une version corrective suivante.

# Historique des modifications

| Date | Description |
|---|---|
| 15 octobre 2026 | Nouveau document |

# Points d'attention pour une mise à jour depuis la dernière version 4.8 LTSB

**IMPORTANT**
Si vous envisagez de mettre à jour un firewall depuis la **dernière version** 4.8 LTSB vers la version 5.1 EA, 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 5.1 EA depuis la **dernière version** 4.8 LTSB disponible est consultable dans la section Changements de comportement de ces Notes de Versions.

### Chemin de mise à jour depuis une version 4.8 LTSB

Il est fortement recommandé de mettre à jour votre firewall depuis la version SNS 4.8 LTSB la plus récente. Vérifiez également avant la mise à jour en version SNS 5.1 qu'aucun élément de configuration ne déclenche un message avertissant qu'une fonction utilisée est obsolète.

## Changements introduits en version 5.1.0

### Prérequis pour la mise à jour

La mise à jour en version 5.1 des configurations suivantes est refusée :

- Configuration utilisant la méthode d'authentification SPNEGO, cette méthode n'étant plus supportée.
- Configuration utilisant le monitoring via SNMP v1, cette version du protocole SNMP n'étant plus supportée.
- Configuration avec un VLAN dont l'interface parente est une interface HA, cette configuration n'étant pas supportée.
- Configuration utilisant des noms personnalisés d'interfaces préfixées par <all_> ou <internals_>.
- Configuration utilisant du routage par interface, cette configuration n'étant plus supportée.

**IMPORTANT**
Si vos firewalls sont administrés par SMC, vous devez commencer par mettre à jour le serveur SMC en version 3.9 puis de mettre à jour ensuite vos firewalls en version 5.1.0. En effet, un serveur en version inférieure à SMC 3.9 sera incapable de déployer une configuration à base de VTI sur des firewalls en version 5.1.0 ou supérieure.

### Fonctionnalités obsolètes en version 5.1

- Définition d'une méthode et d'une action par défaut dans la politique d'authentification.
- Authentification multi-utilisateurs et authentification par cookie. Veuillez la remplacer par la méthode Agent TS.

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

  Plus d'informations sur la **mise à jour de la MIB STORMSHIELD-ROUTE-MIB**.
- Les fonctionnalités de proxy HTTP explicite et de WPAD sont obsolètes et ne doivent plus être utilisées en production.
  Des messages d'avertissement sont affichés lorsque ces fonctionnalités sont utilisées dans une configuration mise à jour en version 5.0.6 (tableau de bord, règles de filtrage, accès au fichier .pac).

### Supervision via SNMP

Veuillez lire attentivement la section **Changements de comportement** de ces Notes de Versions avant de mettre à jour en version SNS 5.1 un firewall faisant l'objet d'une supervision via SNMP.

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

Veuillez lire attentivement la section **Changements de comportement** de ces Notes de Versions avant de mettre à jour en version SNS 5.1 une configuration utilisant des interfaces virtuelles IPsec impliquées dans du routage dynamique OSPF.

### Classification d'URL - Extended Web Control (EWC)

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.

### Sauvegardes automatiques

Lorsque le module des sauvegardes automatiques est configuré pour utiliser un certificat signé avec l'algorithme obsolète SHA1, ce certificat est refusé et la sauvegarde automatique s'interrompt sans transmettre de données pour des raisons de sécurité. Un message d'erreur invite l'administrateur à générer un nouveau certificat personnalisé signé à l'aide d'un algorithme sécurisé.

### Machines virtuelles EVA

Les firewalls virtuels EVA en configuration d'usine disposent désormais d'une partition /data d'une taille de 4 Go contre 2 Go dans les versions précédentes de SNS. Cette modification ne s'applique pas aux EVA installés dans une version antérieure et mis à jour en version 5 de SNS. Il est conseillé de réinstaller ces machines virtuelles directement version 5 de SNS.
Notez que 2 Go de mémoire sont nécessaires pour bénéficier de l'antivirus.

# Changements de comportement

Cette section liste les changements de comportements liés à la mise à jour de votre firewall SNS en version 5.1.4 EA depuis la dernière version 4.8 LTSB disponible.

La version 5 de SNS étant une version majeure, elle introduit des changements de comportement pouvant avoir des impacts importants sur les configurations en production : il est donc fortement recommandé de consulter attentivement cette liste de changements de comportements ainsi que les pré-requis à la mise à jour en version 5.

## Changements introduits en version 5.1.0

### Prérequis pour la mise à jour

La mise à jour en version 5.1 des configurations suivantes est refusée :

- Configuration utilisant la méthode d'authentification SPNEGO, cette méthode n'étant plus supportée.
- Configuration utilisant le monitoring via SNMP v1, cette version du protocole SNMP n'étant plus supportée.
- Configuration avec un VLAN dont l'interface parente est une interface HA, cette configuration n'étant pas supportée.
- Configuration utilisant des noms personnalisés d'interfaces préfixées par <all_> ou <internals_>.

**IMPORTANT**
Si vos firewalls sont administrés par SMC, vous devez commencer par mettre à jour le serveur SMC en version 3.9 puis de mettre à jour ensuite vos firewalls en version 5.1.0. En effet, un serveur en version inférieure à SMC 3.9 sera incapable de déployer une configuration à base de VTI sur des firewalls en version 5.1.0 ou supérieure.

### Fonctionnalités obsolètes en version 5.1

- Définition d'une méthode et d'une action par défaut dans la politique d'authentification.
- Authentification multi-utilisateurs et authentification par cookie. Veuillez la remplacer par la méthode Agent TS.
- Utilisation du proxy HTTP explicite et de WPAD.
- Les anciennes OID au format STRING de la MIB STORMSHIELD-ROUTE-MIB, respectivement snsRouteUsagePrct, snsRoutePacketLossPrct et snsRouteUnreachPrct, sont encore présentes dans cette MIB mais les valeurs qu'elles retournent sont marquées comme obsolètes. La configuration des outils de supervision SNMP doit donc être mise à jour en conséquence.

  Plus d'informations sur la mise à jour de la MIB STORMSHIELD-ROUTE-MIB.
- Un message d'avertissement précise que l'utilisation par le firewall des serveurs DNS racine pour effectuer des requêtes DNS est obsolète et qu'il s'agit d'une mauvaise pratique. Lorsque le firewall doit effectuer des requêtes DNS, il est donc nécessaire de renseigner au moins un serveur DNS dans sa configuration.

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

Les interfaces VTI impliquées dans le routage dynamique BIRD ne sont pas compatibles par défaut avec les interfaces VTI des versions inférieures de SNS. Vous devez ajouter la directive `type nbma;` dans la configuration BIRD, section OSPF puis sous section interface, afin d'être compatibles au travers du protocole OSPF.

Il est fortement recommandé de réaliser cette modification de configuration sur l'ensemble des routeurs avant la mise à jour du firewall en version SNS 5.1.

Il est également fortement recommandé de référencer les interfaces VTI par leur nom, et non celui de leur pilote, dans la configuration BIRD. Le nom du pilote est en effet modifié en version SNS 5.1.

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.

### Routage dynamique BIRD

Lorsque BIRD v1 n'est pas utilisé dans la configuration du firewall, l'onglet correspondant n'est plus affiché dans le module **Réseau** > **Routage dynamique**.

### Authentification - Agent TS

Pour des raisons de sécurité, la liste des suites de chiffrement proposées lors de l'établissement d'une connexion TLS par l'Agent TS a été limitée aux suites basées sur TLS v1.3.

### SNMP - Algorithmes de chiffrement et de hachage obsolètes

Le passage en version 5.1 d'une configuration SNMP utilisant les algorithmes obsolètes de hachage SHA128 et / ou MD5, ou de chiffrement DES, entraînera l'utilisation forcée des algorithmes SHA256 et de AES après mise à jour.

La configuration des outils de supervision SNMP doit donc être mise à jour en conséquence.

### Serveurs DNS par défaut

A compter de la version SNS 5.1, les serveurs DNS Quad9 sont les serveurs DNS utilisés par défaut par les firewalls en configuration d'usine.

### Classification d'URL - Extended Web Control (EWC)

La solution de classification d'URL EWC utilise désormais uniquement le serveur ewc.stormshieldcs.eu comme source de classification.

### Nommage des interfaces

Le nom d'une interface ne peut plus être constitué du nom d'une interface existante suivi par la chaîne <_nombre> afin d'éviter de potentiels conflits de nommage. Exemple : *test_1* n'est plus autorisé.

## Changements introduits en version 5.0.7

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

JIRA SNS-50949

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

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 5.0.6

### Fonctionnalités obsolètes en version 5

Les fonctionnalités de proxy HTTP explicite et de WPAD sont obsolètes et ne doivent plus être utilisées en production.
Des messages d'avertissement sont affichés lorsque ces fonctionnalités sont utilisées dans une configuration mise à jour en version 5.0.6 (tableau de bord, règles de filtrage, accès au fichier .pac).

### 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".

### Classification d'URL - Extended Web Control (EWC)

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.

## Changements introduits en version 5.0.5

### Fonctionnalités obsolètes supprimées en version 5

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.

## Changements introduits en version 5.0.2 EA

### Prérequis pour la mise à jour

- La mise à jour en version 5 d'une configuration VPN SSL utilisant un algorithme différent de AES-128-GCM, AES-192-GCM, AES-256-GCM et ChaCha20-Poly1305) ou avec la compression activée est refusée.

- La mise à jour d'un firewall en version 5 est refusée si le certificat utilisé par le firewall a été signé avec l'algorithme obsolète SHA1.
- La mise à jour d'un firewall en version 5 est refusée si le moteur antiviral ClamAV est utilisé.
- L'algorithme de chiffrement 3DES n'est plus disponible en version 5 de SNS pour les configurations IPsec. La mise à jour en version 5 d'une configuration IPsec utilisant cet algorithme étant refusée, veuillez modifier votre configuration IPsec et remplacer 3DES par un autre l'algorithme avant la mise à jour.
- Le routage par interface n'est plus disponible en version 5 de SNS : la migration d'une configuration v4 utilisant cette fonctionnalité vers une version 5 de SNS est refusée par le système.

### Certificats

Un certificat est généré automatiquement lors du premier démarrage d'un firewall en version 5 de SNS. Ce certificat est utilisé par les services d'authentification du firewall basés sur le protocole TLS (Interface Web d'administration, portail captif) pour les firewalls en configuration d'usine ou lorsque le certificat du portail n'a pas été défini explicitement.

### VPN SSL

- Suite à la mise à jour en version 5 d'un firewall en configuration d'usine, l'option Data Channel Offload (DCO) est activée par défaut lors de l'utilisation du service VPN SSL. Si vous envisagez d'établir des tunnels SSL basés sur le protocole TCP, il est fortement recommandé de désactiver l'option DCO qui est destinée aux tunnels SSL basés sur UDP et n'entraîne aucun gain de performances pour les tunnels SSL basés sur TCP.
- L'activation de l'option Data Channel Offload (DCO) utilisant la suite de chiffrement AES-256-GCM pour le VPN SSL rend les clients VPN TheGreenBow incompatibles avec la fonctionnalité de VPN SSL Stormshield.

### Mots de passe

- La politique de mots de passe définie sur les firewalls en configuration d'usine a été durcie. Elle impose désormais une longueur minimale de 16 caractères (8 auparavant), l'utilisation obligatoire de caractères alphanumériques / majuscules et minuscules / caractères spéciaux et une entropie minimale de 64 (20 auparavant).
- Le jeu de caractères utilisé par le firewall pour encoder les mots de passe est désormais UTF-8 pour les firewalls en configuration d'usine. Ceci évite les soucis de connexion via SSH lorsque le mot de passe contient des caractères non ASCII (exemple : "€", caractères accentués,...).

### Remise en configuration d'usine - Interfaces réseau

Suite à une remise en configuration d'usine d'un firewall en version SNS 5.0.2 EA ou supérieure, la première interface réseau du firewall est automatiquement positionnée en adressage IP dynamique (DHCP).

### Sauvegardes automatiques

Lorsque le module des sauvegardes automatiques est configuré pour utiliser un certificat signé avec l'algorithme obsolète SHA1, ce certificat est refusé et la sauvegarde automatique s'interrompt sans transmettre de données pour des raisons de sécurité. Un message d'erreur invite l'administrateur à générer un nouveau certificat personnalisé signé à l'aide d'un algorithme sécurisé.

### Filtrage URL / SSL

La base d'URL embarquée a été supprimée. 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 :
  1. 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),
  2. 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.

### Agent SNMP

- Les algorithmes obsolètes de chiffrement du mot de passe ne peuvent plus être sélectionnés dans le panneau de configuration de l'agent SNMP v3. Seul l'algorithme AES-SHA2 (SHA256) est disponible par défaut. La mise à jour en version 5 de SNS d'une configuration utilisant un autre algorithme que SHA256 entraîne l'affichage d'une mention qui précise que l'algorithme utilisé est obsolète. Il est possible de le modifier à l'aide de la commande CLI / Serverd `CONFIG SNMP USERV3`.

  Plus d'informations sur la commande **`CONFIG SNMP USERV3`**.
- Les tables SNMP dont l'indice commence à 1 sont désormais utilisées par défaut et les anciennes tables (indice commençant à 0) sont marquées comme obsolètes. Ces dernières sont amenées à disparaître dans une future version SNS.
  Lors de la mise à jour en version 5 ou supérieure d'un firewall SNS utilisant les anciennes tables, un avertissement est affiché pour inviter l'administrateur à activer les nouvelles tables SNMP en suivant la procédure décrite dans le Manuel utilisateur SNS v5.
- Un message indique que la version 1 de SNMP est obsolète. Cette version sera supprimée dans une future version SNS.

### Machines virtuelles EVA

Les firewalls virtuels EVA en configuration d'usine disposent désormais d'une partition /data d'une taille de 4 Go contre 2 Go dans les versions précédentes de SNS. Cette modification ne s'applique pas aux EVA installés dans une version antérieure et mis à jour en version 5 de SNS. Notez que 2 Go de mémoire sont nécessaires pour bénéficier de l'antivirus.

### Proxy HTTP explicite

Le proxy HTTP explicite est obsolète et sera supprimé dans une future version SNS.

### Captures réseau

Pour des raisons de sécurité, le droit nécessaire pour réaliser une capture réseau est désormais le droit "supervision en écriture" (*mon_write*).

### Alarmes

L'alarme "Attaque de type Land" (alarme ip:21) ne se déclenche plus en IPv6 et ne génère plus d'entrée dans les logs. Cette protection est désormais assurée au sein du noyau du système d'exploitation du firewall.

### Objets

Le nombre maximal d'éléments contenus dans un groupe est désormais limité à 3000 objets. La mise à jour en version 5 d'une configuration comprenant un groupe avec plus de 3000 éléments est autorisée, mais il ne sera plus possible d'ajouter d'objets dans ce groupe après la mise à jour.

## Fonctionnalités obsolètes supprimées en version 5

- Fonctions de hachage CRYPT, MD5, SMD5, SHA et SSHA pour l'annuaire LDAP interne,
- Fonctions de hachage MD4, MD5, RIPEMD-160 (rmd160), MD2, MDC-2 et l'algorithme de chiffrement DES-EDE3-CBC pour les protocoles basés sur SSL / TLS,
- SNVM (Stormshield Network Vulnerability Manager),
- VPN PPTP (Point-to-Point Tunneling Protocol),
- Portail VPN SSL applicatif (mode applicatifs Web et applet java),
- Arrêt du support des modems RNIS (modems téléphoniques reliés par câble série).

# Vulnérabilités résolues de SNS 5.1.4 EA

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.

## Connexion à l'interface Web d'administration

Une vulnérabilité a été corrigée dans la page de connexion à l'interface Web d'administration du firewall. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-022.

## 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.

## VPN SSL

Une vulnérabilité a été corrigée dans le VPN SSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-029.

## 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

## Machines virtuelles modèle EVA1

Il est impératif d'affecter 2 Go de RAM à une machine EVA1 utilisant le proxy. Cette quantité de mémoire devient obligatoire en cas d'utilisation de l'antivirus.

## Interface Web d'administration multi-onglets

Lorsque l'onglet Configuration est ouvert avec les droits en écriture, l'ouverture dans un nouvel onglet de la partie Monitoring provoque la perte des droits en écriture sans qu'aucun message n'en informe l'administrateur. Il est alors nécessaire de demander de nouveau les droits en écriture pour pouvoir modifier la configuration du firewall.

## QoS

La QoS implémentée présente les limitations suivantes :

- Bande passante maximale supportée : 1 Gbit/s,
- Interfaces supportées :
  - Ethernet,
  - IPsec,
  - GRETAP,
  - IPsec virtuelles (VTI),
  - VLAN.
- Les files d'attente de type Priority Queuing (PRIQ) et Class-Based Queuing (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.*

## 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 5 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,
- La translation d'adresses sources n'est pas supportée.

## Services Web

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

## Protocole PROFINET-RT

**Référence support 70045**

Une mise à jour du pilote de contrôleur réseau utilisé sur les modèles de firewalls suivants autorise la gestion d'un VLAN ayant un identifiant égal à 0 :

- SN-S-Series-220,
- SN-S-Series-320,
- SN510,
- SN-M-Series-520,
- SN710,
- SN910,
- SN1100,
- SN2100,
- SN3100,
- SN6100,
- SNi40,

- SN-M-Series-720, SN-M-Series-920, SN-L-Series-2200, SN-L-Series-3200, SN-XL-Series-5200 et SN-XL-Series-6200 équipés d'un module réseau additionnel.

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 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.

### IKEv1 - 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.

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.

### IKEv1 - 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 CLI / Serverd `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)

En IKEv1 et IKEv2 : la fonctionnalité VPN dite de DPD (Dead Peer Detection) permet de vérifier qu'un correspondant est toujours opérationnel en envoyant des messages ISAKMP.

En IKEv1 uniquement : 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.

## Réseau

### Routage - Réseau directement connecté à une interface du firewall

**Référence support 79503**

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

### 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

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.

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 v2".

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 et la version 5, 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).

### 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 sur certains firewalls SNS. Ils sont cependant correctement pris en compte par le système et leur bon fonctionnement n'est pas affecté.

## Système

**Référence support 78677**

### Cookies générés pour l'authentification multi-utilisateurs

Suite à une modification de la politique de sécurité embarquée dans 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

Notez que depuis la version SNS 5.1, cette fonction est obsolète et doit être remplacée par la méthode d'authentification Agent TS.

**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 5.0.1, si la version courante du firewall est la 4.8.9.

### 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 v4 vers SNS v5 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 5, 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,
- L'authentification via Kerberos,
- 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 *gatekeepers* (annonce de l'adresse autre que source ou destination de la connexion).

## Proxies

**Référence support 35328**

### Proxy FTP

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

**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-utilisateurs

Il est possible de permettre l'authentification Multi-utilisateurs 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@object (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-utilisateurs ».

Notez que depuis la version SNS 5.1, cette fonction est obsolète et doit être remplacée par la méthode d'authentification Agent TS.

### 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

### 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.

La méthode Kerberos ne peut pas être utilisée sur plusieurs domaines Active Directory.

### 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-utilisateurs 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 la section Authentification du Manuel Utilisateur SNS.

Notez que depuis la version SNS 5.1, cette fonction est obsolète et doit être remplacée par la méthode d'authentification Agent TS.

### 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.

# 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 5.1.4 EA, 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.

## Prérequis pour la mise à jour en version 5 de SNS

La mise à jour en version 5.1 des configurations suivantes est refusée :

- Configuration utilisant la méthode d'authentification SPNEGO, cette méthode n'étant plus supportée.
- Configuration utilisant le monitoring via SNMP v1, cette version du protocole SNMP n'étant plus supportée.
- Configuration avec un VLAN dont l'interface parente est une interface HA, cette configuration n'étant pas supportée.
- Configuration utilisant des noms personnalisés d'interfaces préfixées par <all_> ou <internals_>.
- Configuration VPN SSL utilisant un algorithme différent de AES-128-GCM, AES-192-GCM, AES-256-GCM et ChaCha20-Poly1305) ou avec la compression activée.
- Certificat utilisé par le firewall signé avec l'algorithme obsolète SHA1.
- Configuration IPsec utilisant l'algorithme de chiffrement 3DES. Remplacez 3DES par un autre l'algorithme avant la mise à jour.
- Configuration utilisant le routage par interface.

**IMPORTANT**
Si vos firewalls sont administrés par SMC, il est recommandé de commencer par mettre à jour le serveur SMC en version 3.9 puis de mettre à jour ensuite vos firewalls en version 5.1.0. En effet, un serveur en version inférieure à SMC 3.9 sera incapable de déployer une configuration à base de VTI sur des firewalls en version 5.1.0 ou supérieure.

## 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

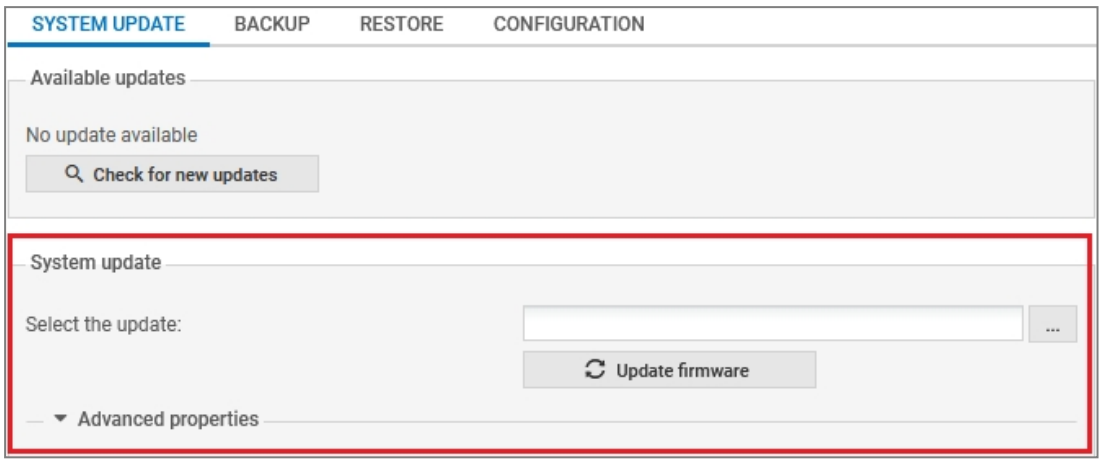
1. Depuis l'interface Web d'administration du firewall, rendez-vous dans **Configuration** > **Système** > **Maintenance**, onglet **Mise à jour du système**.
2. Si une mise à jour de la version est disponible, elle s'affiche dans la zone **Mises à jour disponibles**. Cliquez sur le lien pour télécharger 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.
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 v5

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SNS v5.

| | | | |
|---|---|---|---|
| 5.1.3 EA | Nouvelles fonctionnalités | | Correctifs |
| 5.1.2 EA | | Vulnérabilités résolues | |
| 5.1.1 EA | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |
| 5.0.10 | | Vulnérabilités résolues | |
| 5.0.9 | Nouvelles fonctionnalités | | Correctifs |
| 5.0.8 | | Vulnérabilités résolues | |
| 5.0.7 | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |
| 5.0.6 | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |
| 5.0.5 | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |
| 5.0.4 EA | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |
| 5.0.3 EA | Nouvelles fonctionnalités | | Correctifs |
| 5.0.2 EA | Nouvelles fonctionnalités | Vulnérabilités résolues | Correctifs |

# Nouvelles fonctionnalités et améliorations de SNS 5.1.3 EA

## 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 est défini,
- 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".

# Correctifs de SNS 5.1.3 EA

## 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.

### VPN IPsec - Politique globale avec interfaces virtuelles IPsec (VTI)

La mise à jour en version SNS 5.1 d'une configuration comportant une politique IPsec globale avec des règles utilisant des VTI, issue par exemple d'un déploiement via Stormshield Management Center, ne provoque plus à tort une duplication de ces règles.

# Vulnérabilités résolues de SNS 5.1.2 EA

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 ont été résolues dans le VPN SSL. Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2026-015 : sévérité moyenne,
- https://advisories.stormshield.eu/2026-016 : sévérité forte.

## 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 5.1.1 EA

## VPN IPsec

### Compatibilité des Interfaces IPsec virtuelles (VTI) avec des éditeurs tiers

Les interfaces IPsec virtuelles (VTI) sont désormais compatibles avec les éditeurs tiers Fortinet, Palo Alto Networks, Checkpoint, SonicWall, CISCO, Microsoft Azure VPN Gateway, Amazon Web Services VPN Gateway. Les avantages sont les suivants :

- La compatibilité IPsec avec les autres éditeurs n'est plus limitée aux seuls tunnels par politique.
- Il n'est plus nécessaire de préciser les réseaux distants dans la politique IPsec,
- La politique IPsec est indépendante des adresses IP des extrémités de trafic et des flux pris en charge,
- La sélection des flux à chiffrer dans le tunnel est beaucoup plus souple et précise,
- Un seul tunnel, et donc une seule négociation de phase 2, est nécessaire, quel que soit le nombre de réseaux mis en relation.

En savoir plus sur la configuration des interfaces VTI.

**IMPORTANT**
Si vos firewalls sont administrés par SMC, vous devez commencer par mettre à jour le serveur SMC en version 3.9 puis de mettre à jour ensuite vos firewalls en version 5.1.0. En effet, un serveur en version inférieure à SMC 3.9 sera incapable de déployer une configuration à base de VTI sur des firewalls en version 5.1.0 ou supérieure.

### Tunnels IPsec avec authentification via EAP-TLS

Introduite en version SNS 5.1.0, la méthode EAP-TLS permet de mettre en place de l'authentification multi-facteurs (MFA) sur les clients natifs de différents systèmes d'exploitation (Microsoft Windows, macOS, iOS, Android) pour la création de tunnels IPsec (IKEv2) avec un firewall SNS. L'utilisation d'un client VPN IPsec spécifique sur les postes utilisateurs n'est lus nécessaire pour bénéficier d'une authentification renforcée.

En savoir plus sur la configuration d'un tunnel avec authentification via EAP-TLS.

### Tunnels IPsec avec authentification par certificats multiples

Cette méthode d'authentification, basée sur la RFC 4739, permet de mettre en place de l'authentification multiple en mode Diffusion Restreinte. Le correspondant mobile est alors authentifié par la présentation de deux certificats :

- Celui de son poste de travail, protégé par exemple par le TPM de la machine,
- Son certificat utilisateur, stocké sur une smartcard par exemple.

Notez qu'il est nécessaire de disposer d'un client VPN IPsec supportant également cette méthode.

En savoir plus sur la configuration d'un tunnel avec authentification par certificats multiples.

### Modifications apportées au module VPN IPsec dans l'interface Web d'administration

- L'onglet **Politique de chiffrement - Tunnels** se décompose désormais en trois sous-onglets pour distinguer :
  - Les tunnels basés sur le routage, établis au travers d'interfaces IPsec virtuelles (VTI). Vous pouvez les configurer avec une interface VTI de secours et une passerelle distante de secours afin d'offrir de la redondance.
  - Les tunnels par politique,
  - Les tunnels liés aux clients nomades.
- La définition de ces tunnels est réalisée au travers de trois nouveaux assistants de configuration.
- Les correspondants sont désormais répartis en trois types :
  - Passerelles statiques : passerelles dont l'adresse IP est fixe et connue,
  - Passerelles dynamiques : passerelles dont l'adresse IP peut varier,
  - Clients nomades.
- La supervision des tunnels IPsec distingue également les trois types de tunnels.

## Authentification - Support de fournisseurs d'identités via OpenID Connect (OIDC)

Le support d'OIDC, introduit en version SNS 5.0 pour Microsoft Entra ID, est étendu pour être compatible avec d'autres fournisseurs d'identités : Keycloak, ADFS, Thales Safenet, InWebo Trustbuilder et Wallix Trustelem.

L'intégration de votre firewall SNS avec ces solutions tierces permet une harmonisation de la gestion des identités de vos utilisateurs et de leurs privilèges en créant des politiques par groupe d'utilisateurs. En se reposant sur les mécanismes d'authentification de ces solutions, vous vous assurez de l'identité des utilisateurs ou des administrateurs connectés localement ou au travers d'un VPN.

Notez que l'authentification OIDC nécessite l'utilisation de serveurs NTP pour le maintien à l'heure du firewall. Une alarme est émise lorsque ce n'est pas le cas.

## Portail captif

La page d'authentification du portail captif peut désormais présenter les éléments suivants :

- Le formulaire d'authentification (LDAP),
- Un bouton d'authentification via OpenID Connect (OIDC),
- Un bouton d'authentification par certificat (SSL).

L'affichage de ces éléments est réalisé au travers de la commande CLI / Serverd `CONFIG AUTH INTERFACE ADVANCED`, en utilisant les jetons de configuration `LoginFormEnabled=0|1`, `SSLButtonEnabled=0|1`, `OIDCButtonEnabled=0|1` et conditionné à l'activation des méthodes d'authentification liées. Ainsi :

- Le formulaire d'authentification est affiché sur la page d'authentification dans tous les cas sauf si le jeton `LoginFormEnabled` est positionné à 0,
- Le bouton d'authentification OIDC est affiché si la méthode OIDC est activée sur le firewall et si le jeton `OIDCButtonEnabled` est positionné à 1,
- Le bouton d'authentification SSL est affiché si la méthode SSL est activée sur le firewall et si le jeton `SSLButtonEnabled` est positionné à 1.

## Mise à jour automatique de services Web et catégories d'adresses IP personnalisés

Les services Web et catégories d'adresses IP personnalisés vous permettent d'adapter votre protection en créant des politiques de sécurité en rapport avec votre situation ou votre législation. En plaçant ces services Web dans des règles de blocage, vous créez des listes d'indicateurs de compromission (IOC) personnalisés basés sur des adresses IP ou des noms de domaines.

Ces objets peuvent désormais être mis à jour automatiquement dans le module Active Update. Une nouvelle grille vous permet de définir les points de distributions tiers hébergeant les mises à jour de ces services Web.

En savoir plus sur la **mise à jour automatique des services Web et catégories d'adresses IP personnalisés**.

## 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`**.

## VPN SSL

L'archive *openvpn_client.zip* générée par le firewall à destination des client Stormshield VPN SSL intègre désormais les scripts de connexion / déconnexion pour les clients Linux et macOS.

## Interdire le retour à une version antérieure de SNS

Une option présente dans le module **Maintenance** > **Configuration avancée** permet au super-administrateur (compte *admin*) d'interdire l'installation d'une version antérieure de firmware SNS sur le firewall.

## Firewalls virtuels EVA

### BIOS UEFI

A compter de la version SNS 5.1, les firewalls virtuels EVA utilisent un BIOS UEFI.

### Support de *cloud-init*

A compter de la version SNS 5.1, les firewalls virtuels EVA supportent l'outil de configuration *cloud-init*.

## Sécurité

**Références support TAC-1279 TAC-1566**

Auparavant, l'autorité de certification utilisée par défaut par le proxy SSL contenait le numéro de série du produit à partir duquel elle était générée. Elle contient désormais "SNS-SSLProxy-default-authority". Notez que cette autorité n'est pas régénérée pendant la mise à jour en version 5 de SNS.

## Supervision du routage

Deux commandes CLI / Serverd sont désormais disponibles pour superviser les routes injectées dans le noyau du système :

- `MONITOR ROUTEGET` : affiche la route associée à une destination (objet machine ou adresse IP) passée en paramètre,
- `MONITOR ROUTETABLE` : affiche les tables de routage.

Plus d'informations sur les commandes CLI / Serverd **`MONITOR ROUTEGET`** et **`MONITOR ROUTETABLE`**.

## Routage dynamique BIRD

### Protocole OSPF

**Référence support TAC-1384**

Les tampons mémoire d'émission et de réception de paquets OSPF sont désormais configurables dans les fichiers de configuration de BIRD v1 et BIRD v2.

## Routage statique

La commande `CONFIG NETWORK ROUTE (IPV6) CHECK` permet de vérifier la cohérence du routage statique et d'afficher les éventuels erreurs et avertissements concernant la configuration des routes statiques et route par défaut sur le firewall.

Plus d'information sur les commandes **`CONFIG NETWORK ROUTE CHECK`** et **`CONFIG NETWORK ROUTE IPV6 CHECK`**.

## Restauration de configuration

Toute restauration de sauvegarde de configuration provenant d'une version SNS inférieure fait désormais l'objet d'une vérification et permet d'abandonner la restauration en cas de doute ou d'erreur.

## Filtrage SSL / URL

Vous pouvez désormais configurer 30 profils de filtrage SSL / URL, contre 10 dans les versions inférieures de SNS.

## 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.

### STORMSHIELD-SYSTEM-MONITOR-MIB, STORMSHIELD-SERVICES-MIB et STORMSHIELD-HA-MIB

Pour améliorer la supervision SNMP des firewalls SNS, trois OID au format TimeTicks ont été ajoutées :

- snsSysUptime dans la MIB STORMSHIELD-SYSTEM-MONITOR-MIB,
- snsServicesSysUptime dans la MIB STORMSHIELD-SERVICES-MIB,
- snsHASysUptime dans la MIB STORMSHIELD-HA-MIB.

Les anciennes OID au format STRING, respectivement snsUptime, snsServicesUptime et snsHAUptime, sont toujours présentes mais les valeurs qu'elles retournent sont marquées comme obsolètes.

### STORMSHIELD-ALARM-MIB

Pour permettre l'agrégation de plusieurs occurrences d'une même alarme dans une seule ligne de log, un champ *repeat* indiquant le nombre d'occurrences a été ajouté dans la MIB STORMSHIELD-ALARM-MIB ainsi que dans les *traps* relatifs à cette MIB.

Une OID correspondant à la priorité de l'alarme a également été ajoutée à cette MIB ainsi que dans les *traps* relatifs à cette MIB.

### STORMSHIELD-LICENCE-MIB

La MIB STORMSHIELD-LICENCE-MIB permet désormais de fournir des informations sur les options souscrites et leur date d'expiration.

### STORMSHIELD-IPSEC-STATS-MIB

La MIB STORMSHIELD-IPSEC-STATS-MIB permet désormais d'obtenir les statistiques concernant les paquets IPsec ESP rejoués ou rejetés.

## 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`**.

## Amélioration de l'expérience utilisateur

### Recherche d'objets par leur adresse IP

Dans le module **Objets Réseau**, la saisie d'une adresse IPv4 ou IPv6 dans le champ de recherche permet de rechercher cette adresse parmi les objets de type machine, groupe, réseau et plage d'adresses IP. Vous pouvez alors identifier les modules de configuration utilisant les objets correspondant à l'adresse IP recherchée.

Les objets retournés sont :

- Les objets machine correspondant à l'adresse IP saisie,
- Les objets de type groupe incluant un membre correspondant à cette adresse IP,
- Les objets de type plage d'adresses et réseau qui englobent cette adresse IP.

### Routage

Le module de configuration du routage intègre désormais une console de vérification permettant de détecter et d'afficher les erreurs de configuration.

### Haute disponibilité (HA)

Lorsque le mode verbeux de la HA est activé, une entrée de log est ajoutée pour préciser la raison du passage à 0 de la qualité d'un membre du cluster.

### Événements système - Haute disponibilité

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

### Partition active

Un message d'avertissement est affiché lorsque la partition active du firewall est la partition de secours.

### Commande CLI / Serverd LIST

La commande CLI / Serverd `LIST` retourne désormais le nom complet de l'administrateur sous la forme <utilisateur@domaine> dans la liste des utilisateurs connectés au firewall.

### Services Web

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

### Logs - Authentification

L'authentification d'un utilisateur appartenant à plus de 250 groupes ou pour lequel la longueur de la chaîne des noms de groupes dépasse 4096 caractères déclenche l'écriture d'une ligne dans le journal d'authentification.

### Logs - Administration

Un module de logs **Administration** a été ajouté : il regroupe tous les logs d'administration du firewall.

### Protocole OSPF

La commande système `netstat -axp ospf` affiche désormais des informations complémentaires concernant le protocole de routage dynamique OSPF :

- R-BATC (Buffer All Time Counter) : nombre maximal de tampons mémoire utilisés par la file d'attente de réception,
- S-BATC (Buffer All Time Counter) : nombre maximal de tampons mémoire utilisés par la file d'attente d'émission,
- R-BATB (Buffer All Time Bytes) : taille maximale, en octets, des tampons mémoire utilisés par la file d'attente de réception,
- S-BATB (Buffer All Time Bytes) : taille maximale, en octets, des tampons mémoire utilisés par la file d'attente d'émission.

# Vulnérabilités résolues de SNS 5.1.1 EA

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/.

## Authentification

Des vulnérabilités de sévérité moyenne ont été résolues dans le moteur d'authentification du firewall. Le détail de ces vulnérabilités est disponible sur notre site : https://advisories.stormshield.eu/2025-004.

## 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.

## VPN IPsec

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

## Portail captif

Une vulnérabilité de sévérité moyenne a été résolue dans le portail captif. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-XXX.

# Correctifs de SNS 5.1.1 EA

## Système

### Authentification - Portail captif

Lors de l'utilisation d'une règle d'authentification référençant plusieurs méthodes, le mot de passe saisi dans le portail captif n'est plus affiché dans l'URL construite par le portail captif.

### Filtrage et NAT

**Référence support TAC-1004**

La création d'une règle de filtrage utilisant une valeur de réputation de machine inférieure à zéro est désormais refusée.

### Supervision via SNMP - VPN SSL

Les MIB SNMP indiquent désormais uniquement les tunnels VPN SSL établis.

### 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.

**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.

### VLAN et Haute disponibilité (HA)

**Référence support TAC-1164**

Il n'est désormais plus possible de créer un VLAN sur une interface dédiée à la HA, ou d'utiliser une interface portant un VLAN comme interface pour la HA lors de la création d'un cluster. Ces configurations empêchaient le bon fonctionnement du protocole ICMP au travers du firewall.

### Déploiement de configuration depuis Stormshield Management Center (SMC)

**Référence support TAC-1217**

Des optimisations ont été apportées afin de réduire le temps de déploiement et de validation par le firewall SNS d'une configuration issue d'un serveur SMC.

### Restauration de configuration

**Référence support TAC-1363**

La restauration d'une configuration comportant d'avantage d'interfaces que la configuration à remplacer ne provoque plus d'alertes à tort dans les tests de compatibilité.

### Proxies

Lors d'un téléchargement complet pour lequel le serveur envoie un nombre d'octets supérieur à celui indiqué dans le champ *Content-Length*, en ajoutant par exemple des caractères "\r\n" en fin de requête, le firewall ne génère plus à tort de logs additionnels en considérant qu'il s'agit d'une nouvelle requête.

### Filtrage et NAT

**Référence support TAC-1290**

Les messages d'erreur remontés lors de l'échec du rechargement 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.

### Stockage

**Référence support TAC-1167**

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

### VPN IPsec

La mise à jour de la politique IPsec ne supprime plus à tort la valeur affectée au paramètre *Traffic Flow Confidentiality* (TFC) si celui-ci était présent avant la mise à jour.

**Référence support TAC-1197**

Le compteur de paquets ESP corrompus a été corrigé et affiche désormais une valeur correcte.

AES-GCM remplace désormais AES-256-CBC comme suite de chiffrement utilisée par défaut dans le profil IPsec PQCTransition.

**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`.

### Réseau - Interfaces

**Références support TAC-380**

Lorsqu'une interface du firewall est inopérante, elle reste joignable via une passerelle si son adresse IP est présente dans la table de routage. Ce comportement peut désormais être paramétré en utilisant le jeton *KeepDownIFAddresses* dans la section [Config] du fichier de configuration ConfigFiles/network. Spécifiez la valeur 1 pour conserver ce comportement ou 0 pour que l'interface inopérante ne réponde plus.

**Références support TAC-950**

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

## 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.

## 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.

## 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.

## VPN SSL - Authentification RADIUS

L'authentification d'un client VPN SSL en mode RADIUS et TOTP autorise de nouveau un mot de passe vide. Cette régression était apparue en version SNS 5.0.0.

**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.

## Supervision

**Référence support TAC-1051**

Le paramètre *content* de la commande CLI / Serverd `REPORT GET LASTHOUR | DAY | LAST7DAYS | LAST30DAYS` est de nouveau correctement pris en compte. Cette régression était apparue en versions SNS 4.3.0.

**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. Cette valeur étant fixe, sa lecture réalisée à fréquence régulière était inadaptée et pouvait entraîner des redémarrages inopinés du firewall.

## Routage dynamique BIRD

**Référence support TAC-1394**

L'activation des traces du routage dynamique est désormais conservée lors de la migration de BIRD v1 vers BIRD v2.

### 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.

### 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.

### 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 de ne plus provoquer un arrêt inopiné de l'envoi des requêtes DNS.

## 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 5.1.0 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).

Le nombre d'acquittements émis par le firewall lors de certaines connexions TCP a été limité afin d'empêcher de potentielles boucles d'échanges de paquets.

### Interrogation de la table des hôtes

**Référence support TAC-1141**

Des améliorations ont été apportées au mécanisme d'interrogation des informations des machines présentes dans la table des hôtes, afin d'éviter des pertes de paquets sur un firewall fortement sollicité. La commande `sfctl -s host -vv` remplace désormais la commande `sfctl -s host -v`.

### Protocole HTTP

**Référence support TAC-887**

Les 3 cas déclenchant l'alarme "Débordement dans le protocole HTTP" (alarme http:55) engendrent désormais 3 compléments d'information distincts afin de faciliter le diagnostic. Ces 3 cas sont les suivants :

- Un débordement dans le corps du message qui conserve le même complément,
- Un débordement dans le champ « info body », qui a été remplacé par le champ complémentaire « reply info body »,
- Un débordement dans n'importe quel autre champ qui a été remplacé par le complément « other field ».

### Authentification

**Référence support TAC-1491**

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

## Interface Web d'administration

### Règles implicites

La sauvegarde de configuration suite au changement d'état d'une règle implicite ne provoque plus à tort l'affichage du message d'avertissement : "En l'absence de règles de filtrage explicites, votre firewall sera inaccessible pour les outils d'administration qui utilisent le port 1300. Voulez-vous réellement enregistrer ?".

### Protocoles

**Références support TAC-1184 - TAC-1361**

La suppression accidentelle de certains jetons dans le fichier de configuration d'un protocole n'empêche plus le chargement de la page de configuration de ce protocole dans l'interface Web d'administration.

### Objets

**Référence support TAC-1136**

Le tri des objets sur les colonnes **Type** et **Valeur** n'étant pas fonctionnel, l'icône de tri a été supprimée des colonnes correspondantes.

### TPM

**Référence support TAC-1352**

Suite à l'initialisation du TPM, l'option **Protéger avec le TPM** est directement visible dans le module **Certificats et PKI** sans nécessité de devoir changer de module de configuration pour la faire apparaître.

### Utilisateurs

**Référence support TAC-1438**

Les détails d'un utilisateur issu d'un annuaire LDAP externe de type Microsoft Active Directory s'affichent de nouveau correctement. Cette régression était apparue en version SNS 5.0.2.

### Logs - Journaux d'audit

**Référence support TAC-973**

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 ou égal à 36 caractères.

### 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.

### 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 contenait de nombreuses règles utilisant le filtrage URL / SSL. Ce problème est maintenant corrigé.

# Vulnérabilités résolues de SNS 5.0.10

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.

## Connexion à l'interface Web d'administration

Une vulnérabilité a été corrigée dans la page de connexion à l'interface Web d'administration du firewall. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-022.

## 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.

## VPN SSL

Une vulnérabilité a été corrigée dans le VPN SSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-029.

## 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.

# Nouvelles fonctionnalités et améliorations de SNS 5.0.9

## 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 5.0.9

## 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.

### Stockage

**Référence support TAC-1167**

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

# Vulnérabilités résolues de SNS 5.0.8

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 ont été résolues dans le VPN SSL. Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2026-015 : sévérité moyenne,
- https://advisories.stormshield.eu/2026-016 : sévérité forte.

## 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 5.0.7

## Routage par politique de filtrage et routage statique

La priorité du routage par politique de filtrage (PBR) sur le routage statique est obsolète et sera supprimée d'une version SNS à venir. Ce comportement peut être activé ou désactivé 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`**.

## 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`**.

## Alarmes - Haute disponibilité (HA)

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

# Vulnérabilités résolues de SNS 5.0.7

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/.

## 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.

## 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 des tunnels 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 5.0.7

## 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.

### 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.

### 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.

### VPN IPsec

AES-GCM remplace désormais AES-256-CBC comme suite de chiffrement utilisée par défaut dans le profil IPsec PQCTransition.

**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`.

### 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.

### 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. Cette valeur étant fixe, sa lecture réalisée à fréquence régulière était inadaptée et pouvait entraîner des redémarrages inopinés du firewall.

### 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 de ne plus provoquer un arrêt inopiné de l'envoi des requêtes DNS.

### 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.

# Nouvelles fonctionnalités et améliorations de SNS 5.0.6

## Firewalls virtuels EVA - VPN SSL

**VPN SSL**

Suite à l'introduction du mécanisme DCO en version 5, le nombre maximal de tunnels VPN SSL autorisés sur les firewalls virtuels EVA en version 5 a été augmenté comme suit :

| Modèle | Ancienne valeur | Nouvelle valeur |
|---|---|---|
| EVA1 | 100 | 200 |
| EVA2 | 150 | 500 |
| EVA3 | 200 | 750 |
| EVA4 | 250 | 1500 |
| EVAU | 500 | 3000 |

Pour plus d'informations sur la fonctionnalité DCO, reportez-vous à la section Configurer le service VPN SSL du **Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield**.

## Objets routeur - Supervision des passerelles via ICMP

**Référence support TAC-1077**

Le nombre de passerelles pouvant être supervisées via ICMP a été multiplié par deux.

## 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.

## Firewalls virtuels - Définition du mot de passe du super-administrateur

**Référence support TAC-1367**

Lors de la définition du mot de passe du super-administrateur au premier démarrage d'un EVA en version 5 de SNS, les raisons du refus du mot de passe sont désormais affichées si celui-ci ne respecte pas les prérequis de la politique de mot de passe, qui sont par défaut de 16 caractères minimum et d'une entropie égale à 64.

# Vulnérabilités résolues de SNS 5.0.6

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/.

## 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.

## 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.

## 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.

## 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.

## OpenSSL

Une vulnérabilité de sévérité moyenne a été résolue dans la bibliothèque OpenSSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2026-011.

# Correctifs de SNS 5.0.6

## Système

### Haute disponibilité (HA)

**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 d'un firewall. Cette régression était apparue en version SNS 4.8.0.

**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-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.

### 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.

### 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.

### 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.

## 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 5.1.0 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 génère plus 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 - Onglet correspondants

**Référence support TAC-1471**

Le changement de politique globale / locale par le biais du sélecteur présent dans l'onglet **Correspondants** du module VPN IPsec affiche désormais correctement les correspondants associés à la politique sélectionnée.

**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 5.0.5

## 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**.

# Vulnérabilités résolues de SNS 5.0.5

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

Une vulnérabilité de sévérité moyenne a été résolue dans le VPN SSL. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2025-011.

## 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 5.0.5

## Système

### 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.

### VPN IPsec

**Référence support TAC-1197**

Le compteur de paquets ESP corrompus a été corrigé et affiche désormais une valeur correcte.

**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.

**Référence support TAC-1495**

Un espace n'est plus ajouté à tort à la fin de l'adresse e-mail associée au certificat d'un utilisateur VPN issu d'un annuaire LDAP externe. Cette régression, apparue en version SNS 5.0.3, empêchait l'établissement du tunnel IPSec.

Dans une politique IPsec mêlant des correspondants compatibles avec le mode DR et des clients non compatibles, la configuration IPsec non compatible DR n'était pas évaluée et empêchait l'établissement d'un tunnel IPsec avec authentification par certificat depuis un client non compatible avec le mode DR. Ce problème a été corrigé

### 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-1256 - 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**.

### VPN SSL - Authentification RADIUS

L'authentification d'un client VPN SSL en mode RADIUS et TOTP autorise de nouveau un mot de passe vide. Cette régression était apparue en version SNS 5.0.0.

### Supervision

**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.

**Référence support TAC-1501**

La supervision du second module d'alimentation des firewalls SN-M-Series est de nouveau fonctionnelle. Cette régression était apparue en version 5.0.1 de SNS.

# Nouvelles fonctionnalités et améliorations de SNS 5.0.4 EA

## 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.

## 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.

## 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.

## 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 CLI / Serverd **CONFIG AUTH RADIUS**.

## Support de nouveaux modules matériels

La version SNS 5.0.4 EA introduit le support des modules matériels **NC-1-8x10G-FIB-SFP+**, **NC-1-4x25G-FIB-SFP28** et **NC-1-2x100G-QSFP28** pour les modèles de firewalls suivants :

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

# Vulnérabilités résolues de SNS 5.0.4 EA

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/.

## Bibliothèque de compression xz

Une vulnérabilité de sévérité faible a été corrigée dans la bibliothèque de compression xz. Le détail de cette vulnérabilité est disponible sur notre site : https://advisories.stormshield.eu/2025-010.

# Correctifs de SNS 5.0.4 EA

## Système

### Maintenance - Active Update

**Référence support 85852**

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

### Authentification - OpenID Connect

**Référence support 86255**

L'affichage des URL de redirection dans la configuration OIDC / EntraID du firewall est désormais correct lorsqu'un caractère spécial '*' est présent dans le certificat du firewall.

### 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.

### SMC - VPN IPsec

**Référence support 86261**

La migration en version 5.0 de SNS d'une configuration gérée par un serveur SMC définit désormais correctement les profils de phase 1 et de phase 2 compatibles avec le mode DR.

### VPN SSL avec Data Channel Offload (DCO) - VPN IPsec

**Référence support 86282**

Dans une configuration avec le DCO activé pour le VPN SSL et un tunnel IPsec actif, les paquets liés au VPN SSL ne sont plus rejetés à tort par le firewall.

## 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

## Utilisateurs

**Référence support 86270**

Les détails d'un utilisateur issu d'un annuaire LDAP externe de type Microsoft Active Directory s'affichent de nouveau correctement. Cette régression était apparue en version SNS 5.0.2.

## 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.

## TPM

**Référence support 86151**

Suite à l'initialisation du TPM, l'option **Protéger avec le TPM** est directement visible dans le module **Certificats et PKI** sans nécessité de devoir changer de module de configuration pour la faire apparaître.

## 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 5.0.3 EA

## Interfaces virtuelles IPsec (VTI)

Une politique IPsec basée sur des interfaces virtuelles IPsec présentant l'une des configurations incorrectes 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.

## Supervision

**Références support 85911 - 85935**

Les messages indiquant qu'un composant physique retrouve un état "opérationnel" (messages du type "CPU health status recovered") ne sont plus générés à tort lorsque l'état précédent du composant était "mineur" et non "critique".

## 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*.

# Correctifs de SNS 5.0.3 EA

## Système

### 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.

### 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.

### 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 (HA)

**Référence support 85802**

L'ensemble des tâches de synchronisation liées à la HA n'est plus activé de manière systématique lors de la mise à jour d'un firewall. Cette régression, apparue en version 4.8.6, créait de nombreuses entrées inutiles dans les logs d'un firewall non configuré en HA.

**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.

### 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.

### 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'IHM lorsqu'elle contient de nombreux objets réseau. Cela permet également d'éviter des cas de déconnexion inopinée de l'interface d'administration.

## 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.

# Nouvelles fonctionnalités et améliorations de SNS 5.0.2 EA

## Portail captif, VPN SSL et gestion des autorisations grâce à l'authentification Microsoft Entra ID

La version 5.0 de SNS introduit le support du protocole d'autorisation OpenID Connect (OIDC) afin d'être compatible avec l'authentification SSO Microsoft Entra ID.

Ceci permet aux utilisateurs de s'authentifier avec leur compte Microsoft Entra ID et d'être autorisés, selon les droits définis, à accéder au portail captif du firewall, à l'interface Web d'administration du firewall, à établir un tunnel via Stormshield SSL VPN ou d'être reconnus dans les règles de filtrage nécessitant une authentification.

## VPN IPsec - Cryptographie hybride pour le chiffrement post-quantique

À partir de la version 5.0 de SNS, la cryptographie hybride peut être utilisée pour se protéger contre les attaques quantiques à l'aide d'algorithmes hybrides normalisés par le NIST dans le Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).

Vous pouvez utiliser un algorithme résistant aux attaques post-quantiques en plus de l'algorithme traditionnel pour protéger l'échange de clés des attaques quantiques. Notez que la cryptographie symétrique n'est pas vulnérable à ce type d'attaque.

Les algorithmes supportés en version 5.0 de SNS sont les suivants :

- ML-KEM-512,
- ML-KEM-768,
- ML-KEM-1024.

Deux profils de chiffrement utilisant ces algorithmes en mode hybride sont désormais proposés dans l'onglet **Profils de chiffrement** du module VPN IPsec :

- PQCEncryption : destiné aux configurations avec des correspondants utilisant exclusivement ce nouveau chiffrement post-quantique hybride,
- PQCTransition : destiné aux configurations en cours de transition vers ce nouveau chiffrement post-quantique hybride.

## VPN SSL - Performances

Le service VPN SSL intègre désormais le module Data Channel Offload (DCO) : lorsque DCO est activé, les opérations de chiffrement / déchiffrement des paquets de données transitant dans les tunnels VPN SSL sont traitées dans le noyau du système d'exploitation et non plus par le service VPN SSL du firewall. Ceci offre des performances accrues et permet au service VPN SSL de traiter l'établissement d'un nombre plus important de tunnels VPN SSL.

Notez que DCO :

- N'est compatible qu'avec les tunnels VPN SSL basés sur UDP,
- N'est pas activé par défaut lors de la migration d'une configuration existante,
- Nécessite la sélection de la suite de chiffrement AES-GCM.

## VPN IPsec - Mode transition DR

Le mode Diffusion Restreinte (DR) introduit en version SNS 4.2 ne permet pas de faire cohabiter des politiques respectant les spécifications IPsec DR définies par l'ANSSI et des politiques respectant la norme IPsec standard (RFC 7292 IKEv2bis).

La version 5.0 de SNS permet de configurer des tunnels VPN IPsec se comportant comme des tunnels en mode DR, tout en conservant la possibilité d'établir des tunnels VPN IPsec respectant la norme standard. Cette fonctionnalité, nommée "Mode Transition DR", s'applique aux architectures complexes dont le processus de mise en conformité avec le mode DR doit passer par une phase de transition pendant laquelle des politiques IPsec DR et standard (non-DR) seront amenées à coexister.

Pour plus d'informations sur le mode Transition DR, consultez la Note Technique **Utiliser le mode Transition DR pour rendre une architecture IPSec compatible avec le mode DR**.

## API REST de configuration

La version 5.0 de SNS fournit un premier socle d'API REST pour interagir avec vos firewalls à l'aide d'outils d'orchestration.

Cette première version permet de manipuler les listes noires de machines mises en quarantaine par l'administrateur.

Cette API sera enrichie au fur et à mesure des versions SNS à venir.

Pour plus d'informations sur l'activation de l'API REST et la manipulation des clés API, consultez le **manuel utilisateur SNS v5** ainsi que la **documentation de l'API REST SNS**.

## Qualité de service (QoS)

La fonctionnalité de QoS n'est désormais plus en accès anticipé.

Pour plus d'informations sur la QoS consultez la Note Technique **Configurer la QoS sur les firewalls SNS**.

## Sécurité renforcée

### Durcissement du système

Dans le cadre du durcissement du système d'exploitation SNS, la gestion des privilèges a été renforcée lors d'opérations de maintenance, de mise à jour du firewall ou de l'utilisation de certains services (agent SNMP, envoi d'e-mails...).

### Certificats signé avec l'algorithme SHA1

À compter de la version 5.0 de SNS, les certificats signés avec l'algorithme SHA1 ne sont plus supportés et ne peuvent plus être utilisés dans les différents modules proposant l'utilisation de certificats (VPN SSL, Télémétrie, Sauvegardes automatiques...).

### Vérification de l'activation de Secure Boot

L'interface Web d'administration affiche un message d'avertissement lorsque Secure Boot n'est pas activé sur le firewall. Notez que l'activation de Secure Boot impose des contraintes : pour évaluer ces contraintes et suivre la procédure d'activation de Secure Boot, veuillez consulter la Note Technique **Gérer Secure Boot dans l'UEFI des firewalls**.

### Politique de mots de passe

La politique de mots de passe autorise désormais l'utilisation d'une combinaison de caractères alphanumériques majuscules / minuscules et de caractères spéciaux. Elle est sélectionnée par défaut sur les firewalls en configuration d'usine.

### Configuration d'usine - Modification des serveurs DNS utilisés par le firewall

En configuration d'usine, les firewalls SNS utilisent désormais les serveurs DNS proposés par le service européen dns0.eu.

## Intégration dans divers environnements

### SD-WAN

La gestion du contrôle de disponibilité des passerelles SD-WAN a été améliorée afin de mieux prendre en compte certains cas spécifiques de coupures réseau dans les environnements disposant de plusieurs accès WAN.

Pour plus d'informations concernant la configuration du SD-WAN, consultez la Note Technique SD-WAN - Sélectionner le meilleur lien réseau.

### 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.

## Évolution des performances

### Performances générales

La version 5 de SNS améliore les performances générales des firewalls Stormshield.

Pour plus d'informations concernant les performances des firewalls, veuilles consulter les fiches produits disponibles sur le site institutionnel de Stormshield.

### Proxy

Les performances du proxy ont été améliorées et autorisent jusqu'à 25% de débit supplémentaire.

### Rechargement asynchrone des règles de filtrage

Le rechargement de la politique de filtrage peut désormais être réalisé de manière asynchrone afin de minimiser l'impact sur le trafic réseau : les règles de filtrage ne sont pas réévaluées immédiatement, mais au moment de leur utilisation.

Ce mécanisme est particulièrement intéressant pour les configurations regroupant un nombre élevé de règles et de connexions concurrentes.

Il n'est pas actif par défaut et doit être activé à l'aide de la séquence de commandes CLI / Serverd suivante :

```
CONFIG SECURITYINSPECTION COMMON STATEFUL AsyncReload=1
CONFIG SECURITYINSPECTION ACTIVATE
```

Pour plus d'informations sur le rechargement asynchrone des règles de filtrage, consultez la Note Technique Mettre en œuvre le rechargement asynchrone des règles de filtrage.

## Amélioration de l'expérience utilisateur

### Interface Web d'administration

L'interface Web d'administration du firewall permet désormais d'ouvrir simultanément un onglet de configuration et un onglet de supervision dans un même navigateur. Ceci permet de visualiser plus facilement la bonne application de la configuration.

Cette manipulation est réalisable en cliquant sur l'icône  présente dans l'intitulé des onglets **Configuration** et **Monitoring**.

Le thème SNS et l'interface utilisateur ont été revus pour une plus grande fluidité de navigation.

### TPM

Le flux de traitement lié au TPM a été amélioré en supprimant la nécessité de sceller avec les nouvelles caractéristiques techniques du système les secrets stockés dans le TPM lors d'une modification impactant l'UEFI du firewall.

### Supervision des tunnels IPsec

Une barre de recherche est désormais disponible dans le module de supervision du VPN IPsec.

### Logs en temps réel

Le module **Logs en temps réel** permet de visualiser les derniers logs stockés en mémoire sur les firewalls ne disposant pas d'une carte SD.

### Protocole HTTP

Il est désormais possible de configurer la valeur des deux jetons de configuration *AuthorizationBearerBuffer* et *AuthorizationNegotiateBuffer* dans le module de configuration de l'analyse protocolaire HTTP.

### Envoi d'e-mails

Le moteur d'envoi d'e-mails a été durci pour une sécurité accrue et les modèles de messages sont désormais personnalisables dans l'interface Web d'administration grâce à l'utilisation de variables pour chacun d'entre eux.

### Version du BIOS - Commande CLI / Serverd

La commande CLI / Serverd `SYSTEM PROPERTY` remonte désormais les informations concernant le BIOS du firewall, notamment la version de BIOS.

### SNMP - Nouvelle table snsMemUsageTable

Une nouvelle table snsMemUsageTable a été ajoutée dans la MIB STORMSHIELD-SYSTEM-MONITOR-MIB.txt afin de présenter de manière plus exploitable les différentes mesures de consommation mémoire.

## Télémétrie

### Nouvelles données remontées par le service de télémétrie

Le service de télémétrie de la version 5.0 de SNS remonte de nouvelles données :

- Données concernant l'état du SSD :
  - Nombre de blocs retirés de l'utilisation du SSD en raison d'un échec de programmation ou d'effacement,
  - Nombre d'heures de mise sous tension du SSD,
  - Nombre moyen d'effacements des blocs (nombre de fois où le SSD a été complètement écrit),
  - Pourcentage de durée de vie restante,
  - Indicateur d'usure du SSD (0 - 100%),
  - Nombre total de secteurs de 512 octets écrits pendant toute la durée de vie du SSD,
  - Nombre total de secteurs de 512 octets lus pendant toute la durée de vie du SSD.
- Données concernant la politique de filtrage :
  - Nombre de rechargements de la politique de filtrage depuis le démarrage du firewall,
  - État d'activation du mode de rechargement asynchrone des règles de filtrage.
- Données concernant les tunnels IPsec :
  - Nombre de tunnels mobiles configurés avec un mécanisme Key-Encapsulation Mechanism (KEM) utilisant un algorithme résistant aux attaques post-quantiques,
  - Nombre de tunnels mobiles établis avec un mécanisme KEM utilisant un algorithme résistant aux attaques post-quantiques,
  - Nombre de tunnels site-à-site configurés avec un mécanisme KEM utilisant un algorithme résistant aux attaques post-quantiques,
  - Nombre de tunnels site-à-site établis avec un mécanisme KEM utilisant un algorithme résistant aux attaques post-quantiques.

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**.

## Divers

- Système d'exploitation : la version 5 de SNS est basée sur FreeBSD 14.
- Prévention d'intrusion : les services NPDU et BVLL sont désormais pris en charge par le moteur d'analyse protocolaire BacNet/IP.
- La fonctionnalité Energy Efficient Ethernet (EEE) associée aux cartes réseau Ethernet 2.5 Gbit/s est désormais prise en charge.
- L'OID sysObjectID (1.3.6.1.2.1.1.2) permet désormais de récupérer le modèle du firewall via une requête SNMP.

# Vulnérabilités résolues de SNS 5.0.2 EA

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/.

## Serveur de configuration par commande CLI (*Serverd*)

Une vulnérabilité de sévérité faible a été corrigée dans le serveur de configuration par commande CLI.

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

## 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.

# Correctifs de SNS 5.0.2 EA

## Système

### Syslog - SD-WAN

Un paramètre gérant le délai de reprise d'envoi des logs a été ajouté dans chaque profil syslog défini sur le firewall.

Dans une configuration utilisant le SD-WAN et les objets routeurs, suite à une coupure réseau et une bascule sur une passerelle de secours, ce paramètre permet, pour chacun des profils, de régler le délai après lequel le firewall tente de nouveau d'émettre des logs vers le serveur syslog et de limiter le risque de pertes de logs.

Ce délai, jusque ici fixé à 60 secondes, peut être ajusté entre 5 et 600 secondes.

### Rapports

**Références support 85380 - 82777**

Des améliorations ont été apportées afin de limiter la taille de la base de données des rapports et éviter que celle-ci ne remplisse à tort sa partition.

**Référence support 84256**

Dans une configuration gérant la réputation des machines, la commande CLI / Serverd `REPORT RESET report=all` permet désormais de vider entièrement la base de données des rapports comme attendu.

Plus d'informations concernant la commande **`REPORT RESET`**.

### VPN IPsec

**Référence support 85641**

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

**Référence support 84803**

Désormais, les tunnels VPN sont de nouveau renégociés quand le certificat du correspondant est modifié. Cette régression était apparue en version SNS 4.8.0.

**Référence support 85940**

Des optimisations ont été apportées aux calculs de durée de vie des associations de sécurité afin de limiter les risques de conflits dans le cas d'une mauvaise configuration IPsec.

### Interfaces IPsec virtuelles (VTI)

**Référence support 85770**

L'exécution de la commande `ennetwork -f` sur une configuration comportant un tunnel basé sur des interfaces IPsec virtuelles ne provoque plus à tort une interruption du tunnel IPsec.

## Certificats et PKI

**Référence support 85948**

La commande CLI / Serverd `PKI SCEP QUERY` prend désormais correctement en compte les arguments *bindaddr* et *bindport* permettant de préciser une adresse IP ou un port spécifique pour la requête.

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

## Pilotes de cartes réseau

Les valeurs par défaut de certaines files d'attente définies pour chaque pilote de carte réseau ont été augmentées. Cela permet d'éviter de faibles pertes de paquets bien que la charge CPU du firewall ne soit pas importante.

## Filtrage et NAT

**Références support 80798 - 85537**

Vous devez désormais effectuer un double clic sur le commentaire d'une règle de NAT ou de filtrage non sélectionnée pour modifier ce commentaire. Dans les versions SNS antérieures, un clic sur le commentaire d'une règle de NAT ou de filtrage non sélectionnée provoquait en effet l'ouverture puis la fermeture quasi immédiate de l'édition du commentaire.

## Configuration - Vérifier l'utilisation

Lorsqu'un utilisateur / groupe d'utilisateurs est présent dans plusieurs Annuaires LDAP référencés sur le firewall, l'utilisation de la fonction **Vérifier l'utilisation** ne retourne désormais que les résultats relatifs à l'annuaire concerné.

## Configuration - Accès via SSH

**Référence support 85101**

L'utilisation des caractères "<" et ">" entre guillemets dans les commandes CLI Serverd exécutées en console sur le firewall par le biais d'une connexion SSH est désormais correctement interprétée et ne provoque plus le message d'erreur "Error in format".

## Sauvegardes automatiques

Lorsque le module des sauvegardes automatiques est configuré pour utiliser un certificat signé avec l'algorithme SHA1, ce certificat est refusé et un message d'avertissement invite l'administrateur à générer un nouveau certificat personnalisé signé par des algorithmes sécurisés.

## Haute disponibilité - Optimisation du basculement

**Référence support 85773**

Désormais, lorsque la case **Redémarrer toutes les interfaces incluses dans un bridge** est cochée, seules les interfaces contenues dans un bridge redémarrent.

### Haute disponibilité - Restauration de sauvegarde

**Référence support 86025**

La restauration d'une sauvegarde de configuration ne dissocie plus les clés SSH utilisées pour la synchronisation au sein du cluster. Ce problème rendait toute synchronisation HA impossible.

### Haute disponibilité - 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%.

### Serveur LDAPS

**Référence support 85766**

Il est désormais possible d'utiliser un objet machine global pour configurer un serveur LDAPS.

### Filtrage d'URL - Extended Web Control (EWC)

**Références support 85849 - 86059**

Le service de filtrage d'URL EWC est de nouveau fonctionnel suite à la mise à jour de l'adresse IP du serveur ewc-sns.stormshieldcs.eu dans la configuration du service.

### Proxy - Statistiques

**Référence support 86067**

Le proxy peut désormais écrire ses statistiques dans le répertoire /log/verbose. Cette régression était apparue en version SNS 5.0.0.

### Proxy - Antivirus

**Références support 85841 - 86055**

Un problème pouvant provoquer des arrêts inopinés du proxy lors de la mise à jour de la base antivirale a été corrigé.

Sur un firewall SNS utilisant le contrôle antiviral, la mise à jour depuis la version 4 vers la version 5 provoque le téléchargement automatique de la nouvelle base de données antivirale.

La mise à jour en version 5 d'une configuration utilisant des mises à jour manuelles pour l'antivirus avancé (fichiers portant l'extension ".ssp" et téléchargeables dans l'espace client MyStormshield) n'entraîne plus à tort le téléchargement automatique et régulier de la base de données antivirale.

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

Le fait de ne brancher qu'une seule alimentation sur un firewall modèle SN-S-Series-220/320 ne provoque plus à tort une alerte indiquant qu'un module d'alimentation est défectueux.

### Sauvegarde de la base de données des rapports

**Référence support 85700**

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, notamment dans le cas d'une configuration en haute disponibilité. 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.

### 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.

### Optimisation

**Références support 84995 - 85981 - 86070**

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

### Authentification

L'utilisation de caractères accentués dans un identifiant (connexion à l'interface Web d'administration, VPN ...) ne rend plus à tort cet identifiant sensible à la casse.

### 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 correct de cet annuaire.

### Pages d'authentification du firewall

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

### 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.

### 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.

# Commandes CLI / Serverd

### Filtrage et NAT

**Référence support 85566**

La documentation et l'aide intégrée de la commande CLI / Serverd `CONFIG FILTER RULE UPDATE` ont été corrigées : le paramètre *srcport* ne peut représenter qu'un unique port ou une unique plage de ports et non une liste de ports comme indiqué à tort précédemment.

Plus d'informations concernant la commande **`CONFIG FILTER RULE UPDATE`**.

### Sauvegarde et restauration

La documentation et l'aide intégrée des commandes CLI / Serverd `CONFIG BACKUP` et `CONFIG RESTORE` ont été complétées pour l'argument `list`.

# 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.

### Firewalls virtuels EVA déployés sur l'hyperviseur Microsoft Hyper-V

**Référence support 85840**

Sur un firewall virtuel EVA déployé sur l'hyperviseur Microsoft Hyper-V, 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).

### Firewalls virtuels EVA - Labels de partitions

La partition d'échange (Swap) est de nouveau montée automatiquement au démarrage de la machine virtuelle. La présence de cette partition permet d'absorber une partie de la charge mémoire.

### Machines virtuelles *Pay As You Go* (PAYG)

**Référence support 85559**

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

### Machine virtuelle PAYG sur Microsoft Azure

A la fin du déploiement d'un firewall PAYG sur la plate-forme Microsoft Azure, les accès au firewall en SSH et à l'interface Web administration en HTTPS sont de nouveau opérationnels.

# Moteur de prévention d'intrusion

## Analyse protocolaire

**Références support 85910 - 86013**

Des problèmes ont été identifiés et corrigés dans le code du moteur de prévention d'intrusion. Ces problème pouvaient engendrer un blocage du firewall.

## 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).

## Routage dynamique BIRD

**Référence support 84579**

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

## Protocole SIP

La valeur par défaut des paramètres **Action** / **Niveau** associés à l'alarme sensible "Adresse anonyme dans la connexion SDP" (alarme sip:465) est désormais **Bloquer** / **Majeur**. Cette valeur était auparavant positionnée à tort sur **Passer** / **Mineur**.

## Mode furtif désactivé - Analyse IPv6

**Référence support 85327**

Un firewall dont le mode furtif a été désactivé ne se bloque plus de manière inopinée lors de l'analyse de paquets IPv6.

## Commandes système sfctl

**Référence support 85757**

L'analyse des arguments passés aux commandes système sfctl ne s'arrête plus à tort après le premier caractère alphabétique. Ce comportement pouvait entraîner le déclenchement d'une commande ne correspondant pas à la commande demandée mais similaire à celle-ci jusqu'au premier caractère alphabétique.

## 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.

### Gestion des utilisateurs dans le moteur de prévention d'intrusion

**Référence support 85999**

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

## Matériel

### Energy Efficient Ethernet (EEE)

L'activation de EEE sur les cartes réseau compatibles est désormais fonctionnelle. Ces cartes présentent la case à cocher **Activer la norme IEEE 802.3az (EEE)** dans leur configuration avancée.

### Bus de communication LPC

**Référence support 84328**

Un problème d'accès concurrentiels sur le bus de communication LPC, pouvant entraîner des remises en configuration d'usine inopinées ou des lectures erronées de données de supervision matérielle, a été résolu.

### 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, et ne sont plus bloqués à tort.

## Interface Web d'administration

### Administrateurs - Compte *admin*

Le résultat de l'export de la clé privée ou de la clé publique du compte super-administrateur (compte *admin*) est désormais un fichier au format texte. Il était précédemment au format csv.

### 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.

### Interfaces - Type de média

La valeur 5 Gbit/s a été ajoutée à la liste de médias pouvant être sélectionnés pour une interface réseau.

### Restauration d'une configuration SNS v4.3.3x LTSB

La restauration d'une configuration SNS v4.3.3x LTSB sur un firewall en version 5.0 ne bloque plus l'accès à l'interface Web d'administration du firewall.

### 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.

### Routage dynamique BIRD

Lors d'une erreur de configuration du routage dynamique BIRD, la console de vérification affiche désormais l'ensemble des détails de l'erreur rencontrée. Cette information était auparavant tronquée.

# 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.*