STORMSHIELD

STORMSHIELD MANAGEMENT CENTER

NOTES DE VERSION

Version 3

Dernière mise à jour du document : 12 décembre 2023

Référence : sns-fr-SMC-notes_de_version-v3.5.3

Table des matières

Dans la documentation, Stormshield Management Center est désigné sous la forme abrégée : SMC et Stormshield Network sous la forme abrégée : SNS.

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

Changements de comportement

Changements introduits en version 3.4

Utilisation de la commande RSYNC

La commande système RSYNC a été supprimée dans le cadre d'un nettoyage de packages système que SMC n'utilise pas. Pour copier des fichiers, vous pouvez néanmoins utiliser la commande `cp`.

Interfaces avec adresses de réseau ou broadcast

SMC ne permet plus de créer des interfaces avec des adresses de réseau ou de broadcast afin d'être homogène avec les firewalls SNS.

Pour plus d'informations avant de mettre à jour SMC en version 3.4, reportez-vous à la section Préconisations.

Déploiement de configuration et sauvegarde automatique

SMC génère désormais un avertissement lorsqu'une sauvegarde automatique est programmée pour démarrer alors qu'un déploiement de configuration est en cours. La sauvegarde automatique est alors annulée.

Changement introduit en version 3.2.1

SMC ne permet plus de rattacher et gérer des firewalls SNS en version inférieure à la 3.7.

Si vous possédez des firewalls SNS en version inférieure à la 3.7 rattachés à SMC, ils ne pourront plus se connecter à SMC 3.5.3. Nous vous recommandons de mettre à jour les firewalls SNS dans une version supportée par SMC.

Nouvelles fonctionnalités et améliorations de SMC 3.5.3

Système

Redondance du serveur SMC

IMPORTANT
Cette fonctionnalité est en accès anticipé.
Veuillez impérativement consulter le *Guide d'administration* avant d'activer cette fonctionnalité.

Vous pouvez désormais mettre en place un système de redondance entre deux serveurs SMC, permettant d'assurer la continuité de service. En cas de panne du nœud primaire, les firewalls SNS se connectent automatiquement au nœud secondaire. La configuration des deux nœuds est synchronisée toutes les heures.

En savoir plus

Modification des répertoires système

Les fichiers présents dans le répertoire */var/tmp* ont été déplacés dans le répertoire */data/tmp*.

Le répertoire */var/fwadmin* a été supprimé et les fichiers ont été déplacés vers le répertoire */data/fwadmin*.

Le lien symbolique entre les répertoires */var/tmp* et */data/tmp* a été supprimé. Les fichiers présents dans */var/tmp* ne sont désormais plus conservés d'une mise à jour à la suivante.

Rapport de diagnostic du serveur SMC

Le rapport de diagnostic du serveur contient une nouvelle section qui fournit des statistiques sur la taille de vos configurations dans SMC : nombre de firewalls administrés, nombres de règles, de routes, d'interfaces, etc. Ces statistiques permettent de mieux diagnostiquer d'éventuels problèmes de performance.

Journalisation

Les fichiers de journaux */var/log/fwadmin-server/cfg2ini.log* et */var/log/fwadmin-server/connections.log* ont été supprimés et leur contenu a été déplacé dans le fichier */var/log/fwadmin-server/server.log*.

Mécanismes de type MAC-then-Encrypt

Pour des raisons de sécurité, les mécanismes de type MAC-then-Encrypt ont été supprimés du serveur SMC.

Configuration des firewalls SNS

Avertissement de modification de la configuration des firewalls

IMPORTANT
Cette fonctionnalité est en accès anticipé.

Veuillez impérativement consulter la liste des limitations dans le *Guide d'administration* avant d'activer cette fonctionnalité.

Cette nouvelle fonctionnalité est désactivée par défaut. Si vous l'activez, un avertissement s'affiche désormais au moment du déploiement de configuration sur les firewalls SNS, dans le cas où d'autres administrateurs auraient fait des modifications de configuration depuis le dernier déploiement. L'administrateur peut alors choisir de poursuivre le déploiement ou de l'annuler.

En savoir plus

Configuration du réseau

Mot-clé *blackhole*

A partir des versions des firewalls SNS :

- 4.3.21 LTSB et 4.3 LTSB supérieures,
- 4.7 et supérieures,

vous pouvez désormais sélectionner le mot-clé *blackhole* en tant que passerelle de la route par défaut ou d'une route statique destinée à détruire un trafic identifié.

Ce mécanisme peut notamment être utilisé dans une configuration comportant des tunnels IPsec : en cas d'indisponibilité d'un tunnel, les paquets qui lui étaient destinés sont ainsi détruits au lieu d'être redirigés vers la passerelle par défaut du firewall.

Compatibilité Microsoft Windows

Support de Windows Server 2022

SMC est désormais compatible avec l'hyperviseur Microsoft Hyper-V pour Windows Server 2022 pour l'installation. Il est également compatible avec des serveurs LDAP et Radius sur Windows Server 2022 pour l'authentification des utilisateurs.

Authentification

Protection contre les attaques par force brute

Lorsqu'un administrateur se connecte à l'interface de ligne de commande de SMC via son compte SSH ou le compte "root" SSH, la connexion se bloque désormais pendant 15 minutes après cinq erreurs successives d'authentification.

Paramétrage d'un serveur Radius

Référence support 85187

Vous pouvez maintenant configurer les valeurs des attributs NAS-IP-Address et NAS-IP-Identifier utilisés dans les requêtes Radius, avec les variables d'environnement :

- SMC_RADIUS_NAS_IP_ADDRESS
- SMC_RADIUS_NAS_IDENTIFIER

API publique de SMC

Topologies et tunnels VPN

Trois nouvelles routes API sont disponibles dans l'API publique de SMC pour gérer les topologies et les tunnels VPN :

Route	Permet de
GET /papi/v1/vpn/topologies	Lister toutes les topologies VPN configurées dans SMC, qu'elles soient déployées ou non. La route remonte tous les éléments de configuration tels que le nom de la topologie, la méthode d'authentification, le nom et le contenu du profil de chiffrement, les correspondants, etc. La route permet également de filtrer les topologies via leur nom ou la version IKE utilisée. Le champ "name" autorise la recherche partielle, et la casse est ignorée.
GET /papi/v1/vpn/topologies/{uuid}	Lister tous les éléments de configuration d'une topologie VPN spécifique configurée sur SMC, qu'elle soit déployée ou non.
GET /papi/v1/vpn/tunnels	Lister tous les tunnels VPN déployés depuis SMC. La route remonte tous les éléments de supervision d'un tunnel VPN tels que le nom de la topologie, l'état du tunnel, les extrémités de trafic, etc. La route permet également de filtrer les tunnels via un nom de topologie, le type, la forme ou l'état d'une topologie. Le champ "topologyName" autorise la recherche partielle, et la casse est ignorée.

Déploiement de configuration

Deux nouvelles routes API sont disponibles dans l'API publique de SMC pour gérer les déploiements de configuration :

Route	Permet de
POST /papi/v1/deployment	Déployer la configuration sur les firewalls.
GET /papi/v1/deployment	Connaître le statut du déploiement en cours ou du dernier déploiement.

Règles de filtrage et de translation

Huit nouvelles routes API sont disponibles dans l'API publique de SMC pour gérer les règles de filtrage et de translation spécifiques à un firewall ou partagées entre plusieurs firewalls :

Route	Permet de
GET /papi/v1/folders/{uuidOrName}/filter-policy	Lister les règles de filtrage présentes dans un dossier. Seules les règles contenues dans le dossier sont remontées et non les règles du dossier parent ou des sous-dossiers. Les règles sont triées par priorité haute ou basse.
GET /papi/v1/folders/{uuidOrName}/nat-policy	Lister les règles de translation présentes dans un dossier. Seules les règles contenues dans le dossier sont remontées et non les règles du dossier parent ou des sous-dossiers. Les règles sont triées par priorité haute ou basse.
PUT /papi/v1/folders/{uuidOrName}/filter-policy	Modifier les règles de filtrage d'un dossier.
PUT /papi/v1/folders/{uuidOrName}/nat-policy	Modifier les règles de translation d'un dossier.

PUT /papi/v1/firewalls/{uuidOrName}/filter-policy	Définir des règles de filtrage spécifiques à un firewall.
PUT /papi/v1/firewalls/{uuidOrName}/nat-policy	Définir des règles de translation spécifiques à un firewall.
GET /papi/v1/firewalls/{uuidOrName}/filter-policy	Lister les règles de filtrage spécifiques à un firewall. Seules les règles spécifiques au firewall sont remontées et non les règles présentes dans le dossier auquel le firewall appartient.
GET /papi/v1/firewalls/{uuidOrName}/nat-policy	Lister les règles de translation spécifiques à un firewall. Seules les règles spécifiques au firewall sont remontées et non les règles présentes dans le dossier auquel le firewall appartient.

Dossiers

Une nouvelle route API est disponible dans l'API publique de SMC pour gérer les dossiers :

Route	Permet de
GET /papi/v1/folders	Lister tous les dossiers présents sur SMC et pour chacun des dossiers, leur nom et leur UUID ainsi que les firewalls qu'il contiennent.

Base d'objets

27 nouvelles routes API sont disponibles dans l'API publique de SMC pour gérer la base d'objets :

Route	Permet de
GET /papi/v1/objects	Lister tous les objets présents dans la base d'objets de SMC.
POST /papi/v1/objects/[*type de l'objet*]	Ajouter des objets de type "Machine", "Groupe", "Réseau", "Port", "Nom DNS", "Temps", "Routeur", "SLA", "Protocole IP", "Plage d'adresses", "Groupe de Ports" et "Géolocalisation". Par exemple : POST /papi/v1/objects/hosts
PUT /papi/v1/objects/[*type de l'objet*]/{uuidOrName}	Modifier des objets de type "Machine", "Groupe", "Réseau", "Port", "Nom DNS", "Temps", "Routeur", "SLA", "Protocole IP", "Plage d'adresses", "Groupe de Ports" et "Géolocalisation". Par exemple : PUT /papi/v1/objects/hosts/{uuidOrName}
DELETE /papi/v1/objects/{type}/{name} DELETE /papi/v1/objects/{uuid}	Supprimer des objets de la base d'objets de SMC à partir de leur nom ou de leur UUID.

Correctifs de SMC 3.5.3

Mise à jour de SMC

Référence support 85420

Paramétrage des règles de translation

Lors de l'import de règles de translation à partir d'un fichier CSV, il n'est plus possible d'utiliser la valeur "random" dans le champ "nat_from_port_load_balancing" si le champ "nat_from_port" est vide.

Si vous aviez importé des règles de translation avec cette configuration, la mise à jour en version 3.5.3 permet de corriger cette incohérence de configuration. Si le champ "nat_from_port" n'est pas renseigné, la valeur du champ "nat_from_port_load_balancing" est automatiquement vidée.

Support des caractères spéciaux "<", ">" et "@"

La présence des caractères "<" et ">" dans les descriptions ou commentaires des règles de filtrage et de translation, des séparateurs et des objets ne fait plus échouer la mise à jour de SMC vers la version 3.5.x. Cependant, lors de la mise à jour en version 3.5.3, ces caractères seront supprimés et le reste de la description ou du commentaire sera conservé.

De même, le caractère "@" est de nouveau supporté dans les descriptions des règles et séparateurs de règle.

Serveur Active Update

Référence support 85414

Lorsque la fonctionnalité serveur Active Update était activée sur SMC, les deux problèmes suivants pouvaient se produire et sont désormais résolus :

- SMC pouvait devenir injoignable lorsqu'il ne parvenait pas à se connecter aux serveurs de mise à jour Stormshield pour télécharger les bases de données. Dorénavant, en cas de problème de connexion, SMC reste accessible et une erreur est remontée dans les logs du serveur.
- Lorsque l'on désactivait la fonctionnalité serveur Active Update, la mise à jour automatique des bases de données continuait. Dorénavant, la mise à jour automatique est bien désactivée.

Configuration du réseau

Modification de la configuration du routage dynamique sur le firewall SNS

Référence support 85427

Vous pouvez désormais accéder directement à l'interface d'un firewall SNS depuis SMC et modifier sa configuration de routage dynamique sans que cela rende, dans certains cas, SMC indisponible.

Base d'objets

Export de la base d'objets

Référence support 85367

L'export de la base d'objets via un fichier CSV est de nouveau fonctionnel.

Règles de filtrage et de translation

Import de règles globales d'un firewall SNS

Référence support 85144

Lors de l'import des règles globales d'un firewall dans SMC, si l'une des règles utilise un objet contenant une variable personnalisée, désormais la valeur de la variable propre au firewall n'écrase plus la valeur dans SMC.

Règles s'appliquant à des services Web

Référence support 85251

Lorsque vous importez des règles de filtrage s'appliquant à des services Web via un fichier CSV, si certains services Web ne sont pas connus de SMC, SMC génère dorénavant une erreur par service Web non reconnu.

Synchronisation de la connexion dans un cluster HA

Référence support 84975

Dans une règle de filtrage, menu **Action**, onglet **Configuration avancée**, l'option **Synchroniser cette connexion entre les firewalls (HA)** peut désormais être décochée.

Import des règles d'un firewall dans SMC

Référence support 84919

L'import dans SMC de règles locales d'un firewall SNS échouait lorsqu'un objet de type Machine sur le firewall et un objet de type Nom DNS (FQDN) dans SMC portaient le même nom. L'import est maintenant possible, sans écraser l'objet Nom DNS.

Renommage des protocoles applicatifs dcerpc et steam

Référence support 85307

Les protocoles dcerpc et steam disponibles dans les règles de filtrage et de translation ont été renommés dcerpc_tcp et steam_udp afin d'être compatibles avec le nommage de ces protocoles sur les firewalls SNS.

Taille des champs QoS Queue et QoS ACK Queue

Référence support 84935

La taille maximum des champs QoS Queue et QoS ACK Queue a été augmentée de neuf caractères à 31 caractères.

Attention, ce changement est effectif pour les firewalls à partir de la version SNS 4.3.0. Le déploiement d'une configuration sur un firewall en version inférieure à la version 4.3.0 échouera si la valeur des champs QoS Queue et QoS ACK Queue est supérieure à 9 caractères.

Variables personnalisées dans les règles de filtrage

Référence support 84616

Il n'est plus possible d'utiliser le caractère "%" dans les champs **Nom de groupe** et **Nom de domaine** dans le menu **Source** d'une règle de filtrage. Les variables personnalisées ne sont donc plus supportées pour ces champs.

Configuration des firewalls SNS

Import de firewalls SNS via un fichier CSV

Référence support 85093

Lors de l'import de firewalls via un fichier CSV depuis l'interface web d'administration de SMC, lorsque la case **Générer les packages de rattachement** était cochée, les fichiers nécessaires à la génération des packages pouvaient être corrompus de façon aléatoire au cours de l'import. Les packages de rattachement sont désormais correctement générés lors de l'import de firewalls via un fichier CSV.

Déploiement de topologies VPN

Référence support 85016

Lors du déploiement d'une topologie VPN basée sur une authentification par certificat X.509, si le champ **Adresse IP locale pour vérification de la CRL** est renseigné, cette adresse IP est désormais correctement déployée sur les firewalls SNS appartenant à la topologie.

Accès direct à l'interface d'un firewall

Référence support 83550

Lorsque vous accédez directement à l'interface d'un firewall via SMC, la dernière page visitée s'affiche. Si vous y accédez pour la première fois, la page d'accueil de l'interface d'administration du firewall s'affiche désormais. Auparavant la dernière page visitée sur un autre firewall s'affichait.

Compatibilité

Pour mettre à jour un serveur SMC en version 3.5.3, des mises à jour intermédiaires peuvent être nécessaires selon sa version d'origine :

Depuis une version 2.X	Mettre à jour vers la version 3.1.6

Pour plus d'informations, vous pouvez consulter la base de connaissances Stormshield (authentification nécessaire).

Hyperviseurs

VMware ESXi	6.5, 6.7 et 7.0
Microsoft Hyper-V	Windows Server 2016, 2019 et 2022
KVM	Red Hat 7.9

Serveurs d'authentification

Active Directory	Windows Server 2016, 2019 et 2022
OpenLDAP	2.5
Radius	Windows Server 2016, 2019 et 2022

Navigateurs web

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

Cloud public

Amazon Web Services
3DS Outscale

Compatibilité SMC/firewalls SNS

Le serveur SMC permet d'administrer les firewalls SNS à partir de la version 3.7.

Ce tableau récapitule les versions minimums des firewalls SNS requises pour être compatibles avec les fonctionnalités suivantes de SMC :

Fonctionnalité/Objet	Version de SMC	Version minimum du firewall SNS requise
Scripts CLI SNS	1.1	3.7.0

Règles de filtrage/translation	2.0	3.7.0
Topologies VPN par politique	2.0	3.7.0
Objets Routeur et Temps	2.1.0	3.7.0
Modification de l'interface de sortie des firewalls	2.2.0	3.7.0
Multiples adresses de contact de SMC dans le package de rattachement	2.2.1	3.7.0
SMC en tant que point de distribution de CRL	2.2.1	3.7.0
Indicateurs de santé	2.5	3.7.0
Mode "Responder-only" dans les topologies VPN en étoile	2.5	3.7.0
Algorithme de chiffrement AES GCM 16	2.5	3.7.0
Import de règles de filtrage et de translation depuis l'interface web	2.5	3.7.0
Délai de clôture des SA (VPN Peer Inactivity)	2.6.1	3.7.2
Paramètre CRLRequired	2.6.1	3.8.0
Déclaration d'un serveur SCEP associé à une autorité de certification/renouvellement automatique des certificats SCEP	2.6.1	3.9.0
Interfaces de sortie multiples dans le package de rattachement	2.6.1	3.9.0
Sécurisation des certificats par TPM (Trusted Platform Module)	2.6.1	3.10.1
Paramètre DSCP dans les topologies VPN	2.6.1	3.10.1
Déclaration d'un serveur EST associé à une autorité de certification/renouvellement automatique des certificats EST	2.7	3.10.1 et 4.1.1
Exclusion des clés privées de la sauvegarde automatique de firewalls	2.7	3.10 et 4.1
Topologies VPN par route	2.8	3.7.0
Gestion des interfaces réseau (en lecture seule)	3.0	3.7.0
Gestion des interfaces réseau (en écriture)	3.0.1	4.2.3
Gestion du mode "Diffusion Restreinte (DR)"	3.1	4.3.3
Point de distribution Active Update	3.1	4.3.3
Support de versions différentes de IKE pour un même firewall	3.1.3	3.7.0
Gestion du routage (en lecture seule)	3.2	3.7.0
Gestion du routage (en écriture)	3.2	4.2.3
Support du SD-WAN	3.2	4.3.3
Gestion des interfaces IPsec virtuelles (VTI)	3.4	4.2.3
Filtrage par services Web	3.4	4.4

NOTE

Pour pouvoir superviser l'état des topologies VPN contenant des firewalls SN de la version 4.2. ou supérieure, vous devez utiliser un serveur SMC de la version 2.8.1 ou supérieure.

Préconisations

Informations avant la mise à jour du serveur SMC

Gestion de la configuration des interfaces réseau des firewalls SNS lors d'une mise à jour en version 3.4.x

Après une mise à jour en version 3.4.x, le serveur SMC a besoin de récupérer de nouveau la configuration des interfaces et du routage des firewalls SNS.

Veuillez donc prendre connaissance des points suivants :

1. Avant la mise à jour de SMC, veillez à déployer les modifications de la configuration réseau d'un firewall en cours. Dans le cas contraire, les modifications seraient perdues.
2. La configuration des interfaces et des routes reste en lecture seule sur SMC tant que le firewall SNS ne s'est pas reconnecté à SMC après la mise à jour.

Après la mise à jour en version 3.4, si vous gérez un parc de plus de 200 firewalls, la synchronisation de la configuration réseau des firewalls SNS peut provoquer des ralentissements du système. Dans ce cas, nous vous recommandons de désactiver temporairement le contrôleur de cohérence avant de mettre à jour SMC, puis de le réactiver ensuite. Pour cela :

1. Connectez-vous au serveur SMC 3.3 via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, ajoutez la variable d'environnement : `FWADMIN_ENABLED_CFGCHECK=false` (remplacée par la variable `SMC_CFGCHECK_ENABLED` à partir de la version 3.4).
3. Redémarrez le serveur avec la commande `nrestart fwadmin-server`.
4. Après la mise à jour, lorsque tous les firewalls sont correctement reconnectés, supprimez la ligne du fichier et redémarrez le serveur.

Interfaces avec adresses de réseau ou broadcast

SMC ne permet plus de créer des interfaces avec des adresses de réseau ou de broadcast afin d'être homogène avec les firewalls SNS

Avant de mettre à jour SMC, vérifiez que vous ne possédez pas ce type d'interface dans votre configuration. Dans le cas contraire, l'interface d'administration de SMC deviendrait inutilisable et il vous faudrait rétablir un snapshot ou un instantané de votre machine virtuelle.

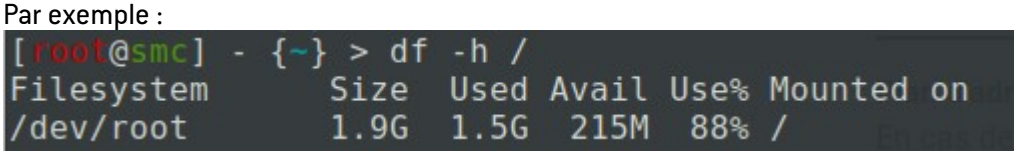
Taille du disque Système

Après plusieurs mises à jour successives du serveur SMC, le disque Système peut manquer d'espace et ne pas permettre l'installation de nouvelles mises à jour :

1. Utilisez la commande suivante pour vérifier l'état de votre disque Système :

   ```
   df -h /
   ```

   Par exemple :

2. Si l'espace sur le disque est presque plein, vous devez déployer une nouvelle machine virtuelle selon la procédure suivante :
   a. Effectuez une sauvegarde de la configuration du serveur SMC 3.x.
   b. Éteignez le serveur SMC.
   c. Déployez un nouveau serveur SMC dans la même version 3.x.
   d. Restaurez la configuration sauvegardée sur la nouvelle machine virtuelle.
3. Mettez à jour votre nouveau serveur SMC dans la nouvelle version 3.y.

EXEMPLE
Pour passer d'une version 3.1.4 à une version 3.1.6 :

a. Effectuez une sauvegarde de la configuration du serveur SMC 3.1.4.
b. Éteignez le serveur.
c. Déployez un nouveau serveur 3.1.4.
d. Restaurez la configuration sauvegardée sur le nouveau serveur 3.1.4.
e. Mettez à jour le nouveau serveur en version 3.1.6.

Pour plus d'informations sur ces procédures ou pour obtenir de l'aide, consultez le *Guide d'administration* de SMC ou contactez le Technical Assistance Center.

Plan d'adressage des micro-services SMC

En cas de conflit entre le plan d'adressage utilisé par vos firewalls SNS et le plan d'adressage utilisé par les micro-services du serveur SMC, vous pouvez modifier l'adresse de l'interface "docker0" (172.17.0.1/16) du serveur SMC. Pour cela, suivez la procédure indiquée dans l'article de la Base de connaissances Stormshield (anglais uniquement).

Accès au serveur SMC pendant une mise à jour

Lorsque vous mettez à jour votre serveur SMC, nous vous recommandons de rendre l'accès à SMC indisponible pour les autres administrateurs le temps de la mise à jour. Dans le cas contraire, s'ils sont en train de travailler sur la configuration, ils ne sont pas prévenus qu'une mise à jour est en cours et pourraient perdre leur travail.

Recommandations matérielles minimum

Afin d'assurer la bonne performance du serveur SMC, nous recommandons de l'installer sur une machine virtuelle disposant d'au moins de 2 vCPU et 4 Go de RAM.

Avertissement avant de rattacher des firewalls SNS au serveur SMC

Veuillez prendre connaissance de ces informations si vous souhaitez rattacher au serveur SMC un parc de firewalls SNS déjà en production et qui contient des éléments de configuration globaux.

Lorsque SMC déploie une configuration sur un firewall, tous les éléments de configuration globaux existant sur ce firewall sont supprimés, et remplacés par les éventuels éléments de configuration définis dans la configuration SMC.

Ceci comprend :

- Les objets globaux définis sur le firewall,
- Les règles de filtrage globales définies sur le firewall,
- Les tunnels VPN globaux définis sur le firewall.

Ces éléments ne sont pas visibles par défaut dans l'interface web de configuration SNS. Pour les afficher, vous devez aller dans les **Préférences** de votre firewall, section **Paramètres de l'application** et activer l'option **Afficher les politiques globales (Filtrage, NAT, IPsec et Objets)**.

En rattachant un firewall SNS à SMC, vous acceptez donc que ces éléments globaux que vous auriez pu mettre en place sur ce firewall soient écrasés dès le premier déploiement de configuration par SMC.

En revanche les objets, règles et tunnels VPN locaux (que vous manipulez par défaut dans l'interface Web d'administration des firewalls) ne seront jamais modifiés ou supprimés par un déploiement de configuration par SMC.

Nous vous préconisons donc de recréer ces éléments globaux sous forme d'éléments locaux sur le firewall ou bien de récrire les règles dans SMC avant de rattacher le firewall à SMC, pour éviter toute perte d'éléments de configuration et ne pas perturber la production.

Dans les cas les plus fréquents, où le firewall à rattacher ne dispose pas d'éléments de configuration globaux, son rattachement à SMC ne nécessite pas de précaution particulière et se fera sans impact sur la production.

Dans tous les cas, nous préconisons de réaliser une sauvegarde de la configuration de votre firewall avant de le rattacher à SMC.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SMC 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.

Précisions sur les cas d'utilisation

Support de versions différentes du protocole IKE pour un même firewall

Dans des topologies VPN, le support de versions différentes du protocole IKE pour un même firewall n'est possible que lorsqu'un seul firewall est commun à plusieurs topologies. Si plusieurs firewalls sont communs à plusieurs topologies paramétrées avec des versions différentes de IKE, c'est la version de la topologie créée en premier dans l'écran de configuration des topologies qui sera déployée.

Utilisation de l'objet All dans les topologies VPN

Au sein d'une topologie VPN par politique, lorsque deux correspondants différents utilisent l'objet *All* pour définir les extrémités de trafic, alors la connexion entre SMC et le firewall SNS peut être interrompue, à moins que des règles de routage par politique soient configurées pour supporter ce cas d'usage. Pour les topologies en étoile, le même problème se produit si l'objet *All* est utilisé à la fois pour le centre de l'étoile et pour un satellite.

Utilisation des objets VTI générés par les topologies VPN par route

Lorsque vous modifiez ou supprimez une topologie VPN par route sur SMC, les objets VTI de type Machine générés automatiquement par cette topologie pour représenter les correspondants distants sont également modifiés ou supprimés. Si vous utilisez ces objets dans la configuration locale de vos firewalls SNS, veillez à d'abord les supprimer avant de modifier ou supprimer une topologie dans SMC.

Déploiement de topologie VPN

Il n'est pas possible de déployer une topologie VPN depuis le serveur SMC si le nom d'un firewall SNS est trop long. Les noms des topologies VPN sur les firewalls ne peuvent pas comporter plus de 127 caractères.

Configuration du routage sur SMC

Plusieurs interfaces pour joindre le serveur SMC sont configurables mais une seule passerelle par défaut sur une seule interface peut être déclarée. Vous devrez configurer manuellement le routage pour les autres interfaces. Un article de la Base de connaissances Stormshield indique la procédure à suivre (anglais uniquement).

Utilisation d'un objet réseau global dans une configuration locale

Sur un firewall SNS, des objets globaux peuvent être utilisés dans une configuration locale. Or lorsque SMC déploie une configuration sur un firewall, les objets globaux existant sur le firewall sont supprimés et remplacés par les objets définis dans la configuration de SMC. Afin que la configuration locale ne cesse pas de fonctionner, vous devez forcer le déploiement des objets globaux nécessaires sur les firewalls concernés.

Pour plus d'informations, reportez-vous à la section Avertissement avant de rattacher des firewalls SNS au serveur SMC.

Migration d'un firewall virtuel modèle V vers un modèle EVA

La mise à jour d'un firewall virtuel V-50, V-100 ou V-200 vers un modèle EVA via la variable %FW_UPD_SUFFIX% dans un script CLI SNS exécuté depuis le serveur SMC n'est pas supportée.

Pour contourner le problème, remplacez la variable %FW_SIZE% par la valeur XL-VM dans le script de mise à jour.

Ressources documentaires

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

Guides

- Guide d'installation Stormshield Management Center
- Guide d'administration Stormshield Management Center
- Documentation de l'API publique de SMC
- Manuel d'utilisation et de configuration des firewalls Stormshield Network Security

Vidéos

- CLI Commands and Scripts, disponible sur Institute.

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 3.5.3 de Stormshield Management Center :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.
4. Téléchargez également les fichiers *build.sha256sum*, *build.sha256sum.sign* et *smc-sign.crt* si vous souhaitez vérifier l'intégrité des binaires.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Management Center, entrez l'une des commandes suivantes :

- Système d'exploitation Linux : `sha256sum -c build.sha256sum`
- Système d'exploitation Windows, dans PowerShell :
  - Entrez `cat build.sha256sum`. La commande retourne les empreintes (hash) et les fichiers associés.
  - Pour comparer l'empreinte d'un fichier, copiez-la et entrez `(Get-FileHash mon-fichier.ext -A SHA256).Hash -eq "empreinte"`.

Vérifier la signature du fichier *build.sha256sum*

Le fichier *build.sha256sum.sign* est la signature du fichier *build.sha256sum*. Sa vérification garantit que le fichier *build.sha256sum* n'a pas été modifié.

OpenSSL est nécessaire pour vérifier la signature du fichier.

1. Si vous avez besoin d'installer OpenSSL sous Microsoft Windows, utilisez l'outil winget et la commande PowerShell suivante :
   ```
   > winget install ShiningLight.OpenSSL
   ```
2. Démarrez ensuite le programme "Win64 OpenSSL Command Prompt".

Pour vérifier la signature sous les systèmes d'exploitation Linux et Windows :

1. Utilisez le certificat *smc-sign.crt* :
   ```
   openssl x509 -in smc-sign.crt -pubkey -noout -out smc-sign.pem
   openssl dgst -sha256 -verify smc-sign.pem -signature
   build.sha256sum.sign build.sha256sum
   ```

Si vous souhaitez vérifier que le certificat est bien issu de l'autorité de certification SMC, utilisez la commande :

```
openssl verify -CAfile Stormshield.Management.Center.2.pem smc-sign.crt
```

Versions précédentes de SMC v3

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SMC v3.

3.4.3		Vulnérabilités résolues	
3.4.2			Correctifs
3.4.1			Correctifs
3.4	Nouvelles fonctionnalités		Correctifs
3.3.3	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.3.2	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.3.1	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.2.2			Correctifs
3.2.1	Nouvelles fonctionnalités		Correctifs
3.1.6		Vulnérabilités résolues	Correctifs
3.1.5			Correctifs
3.1.4			Correctifs
3.1.3	Nouvelles fonctionnalités		Correctifs
3.1.2			Correctifs
3.1.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.0.1	Nouvelle fonctionnalité	Vulnérabilité résolue	Correctifs
3.0	Nouvelles fonctionnalités		Correctifs

Version 3.5.2 non publiée

La version 3.5.2 n'est pas disponible publiquement.

Version 3.5.1 non publiée

La version 3.5.1 n'est pas disponible publiquement.

Version 3.5.0 non publiée

La version 3.5.0 n'est pas disponible publiquement.

Vulnérabilités résolues de SMC 3.4.3

Authentification

Connexion à SMC

Une vulnérabilité de sévérité forte liée à l'authentification sur le serveur SMC a été corrigée.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2023-030.

Nous vous recommandons de mettre à jour votre version de SMC.

Correctifs de SMC 3.4.2

Configuration du réseau

Mise à jour des interfaces IPsec virtuelles des firewalls SNS

Référence support 85227

Après une mise à jour de SMC, si vous possédez des topologies VPN par route dans votre configuration et que vous gérez la configuration du réseau via SMC, les informations sur les interfaces IPsec virtuelles des firewalls SNS sont désormais correctement récupérées par SMC. Un problème de récupération des informations était apparu en version 3.4.1.

Correctifs de SMC 3.4.1

Configuration du réseau

Ordre des interfaces des firewalls SNS

Références support 85148 et 84475

Dans le cas où la configuration du réseau des firewalls est gérée par SMC, dorénavant le déploiement de configuration depuis SMC ne modifie plus l'ordre des interfaces établi auparavant sur les firewalls, quel que soit le type d'interface.

OpenSSL

Paramètres TLS

Les paramètres TLS ont été mis en conformité avec les recommandations de l'ANSSI.

Nouvelles fonctionnalités et améliorations de SMC 3.4

API publique de SMC

Nouvelle API REST publique

Vos solutions d'orchestration peuvent désormais communiquer avec SMC via une API REST standard. Vous pouvez réaliser les actions suivantes via l'API :

- obtenir les informations de supervision des firewalls SNS rattachés à SMC,
- exécuter des scripts sur les firewalls SNS rattachés à SMC pour effectuer tout type d'opérations.

L'utilisation de l'API publique est sécurisée par des clés API, générées par les administrateurs. Ces clés possèdent des droits en lecture/écriture ou bien lecture seule, ainsi qu'une période de validité paramétrable.

Toutes les actions effectuées via l'API publique sont consignées dans les logs d'audit.

Le super administrateur de SMC peut désactiver à tout moment l'API publique. Son accès est désactivé par défaut.

Pour faciliter l'utilisation de l'API, une documentation OpenAPI est fournie sur le site de la Documentation technique Stormshield et également directement dans SMC.

En savoir plus

Configuration du réseau

Création et gestion des interfaces IPsec virtuelles (VTI)

Vous pouvez désormais créer et gérer des interfaces IPsec virtuelles dans SMC, depuis le nouvel onglet **Interfaces IPsec (VTI)** des paramètres d'un firewall SNS. Le firewall doit être en version 4.2.3 minimum. Ces interfaces peuvent ensuite être utilisées dans la configuration du routage.

En savoir plus

Création automatique des VTI

Lorsque vous créez une topologie VPN par route, les interfaces IPsec virtuelles nécessaires sont dorénavant automatiquement créées dans SMC, pour chaque firewall de la topologie dont SMC gère la configuration du réseau. Elles sont visibles dans l'onglet **Interfaces IPsec (VTI)**. Elles sont classées par topologies VPN auxquelles elles appartiennent.

Pour les firewalls dont SMC ne gère pas la configuration du réseau, vous devez continuer à créer les interfaces manuellement sur le firewall directement.

Utilisation des interfaces des firewalls SNS

Dans les règles de filtrage et de translation, il est maintenant possible de sélectionner les interfaces connues d'un firewall SNS qui s'est déjà connecté à SMC.

Cette action n'est pas possible dans les dossiers et dans les jeux de règles.

Contrôle de la cohérence des routes

Un avertissement était remonté par le contrôleur de cohérence lorsqu'un objet était défini comme passerelle d'une route statique ou d'une route de retour et que cet objet ne faisait pas partie du plan d'adressage de l'interface utilisée dans cette route. Cet avertissement a été supprimé car il pouvait induire en erreur l'utilisateur, dans le cas où SMC ne connaissait pas le plan d'adressage de l'interface utilisée.

Règles de filtrage et de translation

Filtrage par services Web

SMC permet désormais de créer des règles de filtrage par services Web. La liste des services Web est disponible dans l'onglet **Général** des menus **Source** et **Destination** d'une règle de filtrage. Elle a été regroupée avec la liste des Réputations IP.

Le fichier */data/config/smc-ip-reputation.local* est renommé */data/config/smc-webservices.local*. Lors de la mise à jour vers la version 3.4 de SMC, les données présentes dans le fichier sont conservées.

Les Réputations IP suivantes ont toutefois été migrées en services Web :

Réputations IP	Services Web
office365	o365common
skypeforbusiness	o365skype
exchangeonline	o365exchange
sharepointonline	o365sharepoint

Les Réputations IP microsoftauth et officeonline ont été supprimées.

En savoir plus

Topologies VPN

Amélioration du fichier *.csv* de configuration des interfaces IPsec

Le fichier *.csv* de configuration des interfaces IPsec proposé au téléchargement à la fin de la création d'une topologie VPN par route contient de nouvelles informations. Il indique maintenant le nom de l'objet Machine représentant l'interface IPsec virtuelle présente sur le firewall distant ainsi que son adresse IP. Ces informations vous permettent d'automatiser la création de routes de retour via un script CLI SNS.

Système

Maintien de la connexion entre SMC et les firewalls SNS

Le mécanisme de maintien de la connexion entre SMC et les firewalls SNS (délai de *keepalive*) est dorénavant le même pour tous les firewalls. Il peut être configuré côté SMC via la variable d'environnement `SMC_FW_CONNECTION_TIMEOUT_INT`. La valeur par défaut est de 60 secondes. Côté SNS, le token `PingValidity` n'est plus pris en compte par SMC.

Variables d'environnement

Renommage des variables d'environnement FWADMIN_XXX

Les variables d'environnement FWADMIN_XXX utilisées en version 3.3.3 et antérieures pour la configuration du serveur SMC sont remplacées par les variables SMC_XXX. Les anciennes variables sont cependant toujours disponibles et fonctionnelles mais seront retirées dans les futures versions.

Pour connaître la correspondance entre les anciennes et les nouvelles versions des variables, reportez-vous au Guide d'administration.

Les variables d'environnement `FWADMIN_SERVICES_NUM_INSTANCES_CFGCHECK` et `FWADMIN_SERVICES_NUM_INSTANCES_CFG2INI` ne sont plus prises en compte.

Correctifs de SMC 3.4

Gestion des administrateurs

Désactivation de l'authentification locale

Référence support 84575

Le super administrateur peut désormais de nouveau désactiver le mode d'authentification locale pour un administrateur, en décochant l'option **Cet administrateur peut utiliser l'authentification locale** dans les paramètres de l'administrateur.

Règles de translation

Import et export de règles de translation

Référence support 84525

Dans le fichier CSV d'import/export des règles, la colonne *nat_from_port_load_balancing*, correspondant à l'option **Choisir aléatoirement le port source translaté** dans l'onglet **Source translatée**, est désormais correctement prise en compte par SMC. Auparavant, lors de l'import de règles, la colonne était ignorée par SMC, et lors de l'export de règles, la colonne n'était pas présente dans le fichier CSV.

Lors de l'import de règles, la valeur *random* doit être indiquée dans la colonne *nat_from_port_load_balancing* pour être prise en compte par SMC.

Topologies VPN

Modification locale sur le firewall

Référence support 84401

Sur la vue de supervision des firewalls SNS, l'icône d'avertissement signale entre autres qu'une modification locale a été faite directement sur le firewall. Lorsqu'une topologie VPN déployée depuis SMC était désactivée localement sur le firewall, la modification locale était bien signalée par l'icône. Cependant elle persistait lorsque la topologie VPN était réactivée depuis le firewall par la suite. L'icône d'avertissement ne s'affiche désormais plus lorsque la modification locale est annulée.

Mise à jour de SMC

Vérification de la licence

Référence support 84464

Lors de la mise à jour de SMC, la validité de la licence du serveur est dorénavant vérifiée au début du processus de mise à jour. Ceci permet d'afficher immédiatement un message d'erreur en cas de licence manquante ou expirée et d'interrompre le processus sans attendre.

Scripts CLI SNS

Ajout de pièces jointes

Référence support 84372

Dans l'écran d'utilisation des scripts CLI SNS, il n'était pas possible de sélectionner les firewalls sur lesquels exécuter un script lorsqu'un trop grand nombre de pièces jointes étaient ajoutées. Vous pouvez dorénavant ajouter autant de pièces jointes que nécessaire, puis sélectionner les firewalls.

Configuration du routage

Utilisation d'un objet routeur en tant que passerelle d'une route statique

Référence support 84883

Les routes s'affichent désormais correctement dans l'onglet **Routage** en lecture seule d'un firewall lorsque le test de la disponibilité d'une passerelle dans un objet routeur pointe vers une machine différente de la passerelle (colonne **Test de la disponibilité** de l'onglet **Passerelles** dans l'objet routeur).

Affichage des routes utilisant des objets de type Serveur

Référence support 84905

Les routes configurées sur un firewall SNS utilisant des objets de type Serveur s'affichent désormais correctement dans l'onglet **Routage** de SMC.

Système

Suppression d'une erreur en mode console

Référence support 84290

Sur un serveur SMC en mode console, le message d'erreur "Unknown ioctl 1976" s'affichait toutes les minutes dans les journaux du serveur. Cette erreur n'avait pas d'impact sur le fonctionnement de SMC et a été supprimée.

Suppression d'un log dans *connections.log*

Référence support 84697

Le log "Possible EventEmitter memory leak detected" qui s'affichait régulièrement dans le journal *connections.log* a été supprimé. Il n'avait pas d'impact sur le fonctionnement de SMC.

Rapport de diagnostic du serveur

Référence support 85060

Depuis la version 3.3.3, la génération du rapport de diagnostic du serveur SMC ne fonctionnait plus depuis l'interface web et depuis l'interface de ligne de commande. Le problème est résolu.

Nouvelles fonctionnalités et améliorations de SMC 3.3.3

Authentification

Protection contre les attaques par force brute

Lorsqu'un administrateur se connecte à SMC via l'interface web, la connexion se bloque désormais temporairement après plusieurs erreurs successives d'authentification.

En savoir plus

Autorités et certificats

Sécurité des certificats

Pour des raisons de sécurité, les utilisateurs ayant accès à SMC via la console de leur hyperviseur ou en SSH ne peuvent plus lire le certificat utilisé pour signer les packages de rattachement et les fichiers de déploiement.

Seul l'utilisateur "root" peut dorénavant le lire.

Signature des packages de rattachement et fichiers de déploiement

Le certificat utilisé pour signer les packages de rattachement et les fichiers de déploiement de configuration a été mis à jour afin d'utiliser un algorithme plus récent et plus sécurisé.

Sauvegarde de la configuration

Exécution de la sauvegarde

Seul le super administrateur (utilisateur "admin") a dorénavant la possibilité de sauvegarder la configuration du serveur SMC.

Sécurisation des sauvegardes de configuration

Il est désormais possible de chiffrer les sauvegardes de configuration du serveur SMC par un mot de passe. Le mot de passe doit respecter la politique de mots de passe définie pour les administrateurs.

En savoir plus

Système

Support de l'en-tête HSTS

Le serveur SMC supporte désormais l'en-tête de sécurité HSTS.

Vulnérabilités résolues de SMC 3.3.3

Vulnérabilité OpenSSH

Connexion SSH

Une vulnérabilité de sévérité forte a été corrigée par la mise à jour de la configuration du composant OpenSSH.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2023-06.

Vulnérabilités OpenSSL

Une vulnérabilité de sévérité moyenne et une vulnérabilité de sévérité forte ont été corrigées par la mise à jour des composants OpenSSL en version 3.0.8 et Node.js en version 16.19.1.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2023-015
- https://advisories.stormshield.eu/2023-016

Correctifs de SMC 3.3.3

Système

Délai de démarrage de SMC

Référence support 84950

Depuis la version 3.3.0 de SMC, le serveur nécessitait un délai supplémentaire pour démarrer, pouvant aller jusqu'à 130 secondes. Ce problème est résolu.

Nouvelles fonctionnalités et améliorations de SMC 3.3.2

Gestion des administrateurs

Nouvelle politique de mot de passe

La politique de mot de passe appliquée par défaut au premier déploiement de SMC a été modifiée et exige désormais un minimum de 12 caractères, contre 8 auparavant.

Si vous avez mis à jour votre serveur SMC depuis une version antérieure à la version 3.3.2, nous vous recommandons de changer la politique de mot de passe par défaut pour définir un minimum de 12 caractères.

En savoir plus

Configuration du réseau

Interface de type *blackhole*

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

Serveur Active Update

Nouvelle base de données Active Update

SMC supporte dorénavant la base Active Update "AdvancedAV1", qui contient les signatures antivirales du nouveau service d'Antivirus Avancé.

En savoir plus

Vulnérabilités résolues de SMC 3.3.2

Vulnérabilité Node.js

Requête HTTP clandestine

Une vulnérabilité de sévérité forte a été corrigée par la mise à jour du composant Node.js.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-024.

Vulnérabilité OpenSSL

Protection contre les attaques *Buffler overflow*

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

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-026.

Correctifs de SMC 3.3.2

Système

Erreur de Node.js

Référence support 84703

L'environnement Node.js de l'application SMC ne rencontre plus d'erreur soudaine. Cela pouvait être le cas, entre autres, lors de déploiement de configuration ou lors de l'accès direct à un firewall SNS via l'interface d'administration de SMC.

Déploiement de configuration

Amélioration des journaux du serveur pour le déploiement

Référence support 84827

En cas d'échec d'un déploiement de configuration, le contenu des journaux du serveur a été amélioré afin de mieux signaler la cause de l'erreur.

Nouvelles fonctionnalités et améliorations de SMC 3.3.1

Hébergement 3DS Outscale

Le serveur SMC peut désormais être hébergé par 3DS Outscale en mode BYOL (Bring Your Own License).

Vous pouvez choisir entre plusieurs types d'instances afin d'adapter au mieux les ressources du serveur SMC en fonction du nombre de firewalls à administrer.

En savoir plus

Scripts CLI SNS

Exécution de scripts différée

Il est possible de démarrer ou programmer une exécution de script CLI SNS sur des firewalls qui sont déconnectés au moment de l'exécution. Le script sera exécuté automatiquement à la prochaine connexion des firewalls à SMC.

En savoir plus

Supervision des firewalls SNS

Raccourci vers SLS (Stormshield Log Supervisor)

Si vous possédez un serveur SLS pour centraliser la gestion des journaux de vos firewalls SNS, vous pouvez désormais paramétrer des raccourcis depuis SMC vers le serveur SLS. Vous pourrez consulter les journaux du parc entier ou les journaux filtrés sur le firewall de votre choix.

En savoir plus

Topologies VPN

Nouveaux groupes Diffie-Hellman

Dans les profils de chiffrement, vous pouvez maintenant sélectionner les groupes Diffie-Hellman 31 (EC25519) et 32 (EC448).

Règles de filtrage et de translation

File d'attente ACK

Dans le cadre de la gestion de la QoS sur des firewalls en version 4.3.0 minimum, le nouveau champ **File d'attente ACK** dans le menu **Action** > **QoS** d'une règle de filtrage permet de définir une file d'attente spécifique pour les flux TCP de type ACK.

En savoir plus

Ajout du protocole S7+

Le protocole applicatif S7+ est maintenant disponible dans les règles de filtrage et de translation.

Vulnérabilités résolues de SMC 3.3.1

Vulnérabilité Node.js

Requête HTTP clandestine

Une vulnérabilité de niveau fort a été corrigée par la mise à jour du composant Node.js.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-018/.

Librairie Javascript

Une vulnérabilité de niveau faible a été corrigée par la mise à jour de la librairie Javascript "Moment.js".

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-022/.

Correctifs de SMC 3.3.1

Base d'objets

Utilisation d'objets Réseau

Référence support 84405

Il n'est plus possible d'utiliser ni d'importer un objet Réseau possédant un masque de sous-réseau en /32 dans la configuration des firewalls. Le contrôleur de cohérence remonte une alerte si un tel objet existe sur SMC.

Création d'objets Routeur

Référence support 84643

Il est maintenant possible de créer un objet Routeur même si l'objet Port HTTPS n'existe pas dans la base d'objets de SMC.

Supervision de SMC avec le service SNMP

État du service SNMP après mise à jour de SMC

Référence support 84438

Lorsque le service SNMP est activé sur le serveur SMC, il est dorénavant automatiquement redémarré après une mise à jour de SMC. L'activation du service est bien conservée après un redémarrage de SMC.

Système

Utilisation de la commande `service`

Référence support 84381

SMC ne supporte plus la commande `service`. En effet, depuis la version 3.0, l'utilisation de la commande `service --status-all` listant les services du système faisait cesser de fonctionner SMC.

Erreurs provoquant un arrêt de SMC

Certaines erreurs, qui pouvaient se produire pendant un déploiement de configuration par exemple, faisaient cesser de fonctionner le serveur SMC. SMC continue désormais de fonctionner correctement même si ces erreurs se produisent.

Déploiement de configuration

Utilisation du même correspondant dans une topologie VPN

Références support 84584 et 84647

Lorsque le même correspondant est utilisé deux fois dans une topologie VPN, SMC ne redémarre plus pendant le déploiement. Le déploiement échoue et SMC affiche un message d'erreur.

Règles de filtrage

Utilisation du caractère @ dans le commentaire d'une règle

Référence support 84423

Les règles de filtrage locales d'un firewall SNS s'affichent désormais correctement dans SMC lorsque le caractère @ est utilisé dans le commentaire.

Affichage des règles de filtrage locales

Références support 84396, 84440 et 84442

Les règles de filtrage locales d'un firewall SNS s'affichent désormais correctement dans SMC lorsque :

- elles utilisent un groupe de régions, une catégorie de réputation des adresses IP publiques ou des services web inconnus par SMC,
- elles utilisent un objet Routeur,
- elles utilisent un objet qui n'est pas exporté par SNS dans SMC.

Configuration des firewalls SNS

Gestion des interfaces réseau

Référence support 84529

Dorénavant, SMC ne déploie plus la configuration du réseau s'il n'a pas récupéré toutes les interfaces réseau au préalable.

Import de firewalls SNS

Référence support 84644

Lors de l'import de firewalls SNS depuis un fichier CSV, le paramètre #vpn_fw_public_ip_address est de nouveau fonctionnel.

Contrôle de la cohérence sur les interfaces réseau

Référence support 84576

Le contrôle de cohérence n'échoue plus sur l'analyse des interfaces réseau possédant une adresse IP en /32.

Autorités et certificats

Vérification de la liste de révocation

Référence support 84603

SMC force désormais les firewalls SNS à récupérer la liste de révocation des certificats (CRL) après chaque déploiement de configuration. En cas de déploiement de topologie VPN avec l'option de vérification de la CRL activée, les tunnels sont ainsi immédiatement fonctionnels. Il n'est plus nécessaire d'attendre que les firewalls récupèrent la CRL.

Modification de la CRL

Référence support 84646

SMC ignore désormais le fichier de CRL *CA.crl.pem* dans le dossier *ConfigFiles/Global/Certificates/<topo_name>/* des firewalls SNS et ne remonte donc plus d'alerte en cas de modification locale de ce fichier.

Version 3.3.0 non publiée

La version 3.3.0 n'est pas disponible publiquement.

Correctifs de SMC 3.2.2

Autorité de certification SMC

Mise à jour de l'autorité de certification

L'autorité de certification (CA) qui contrôle le certificat de la licence utilisée pour SMC a été renouvelée jusqu'au 9 juin 2026.

Nouvelles fonctionnalités et améliorations de SMC 3.2.1

Configuration du réseau

SD-WAN - Sélection du meilleur lien

SMC permet désormais de définir de façon centralisée des critères précis afin de déterminer si un lien WAN respecte le niveau de qualité adapté à son type de trafic (VoIP, vidéo, etc.).

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

- Latence,
- Gigue,
- Perte de paquets,
- Indisponibilité.

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

Cet engagement SLA est défini au travers du nouvel objet SLA, que vous pouvez utiliser dans plusieurs objets Routeur.

Les objets Routeur comprennent également désormais des options de supervision, communes à toutes les passerelles spécifiées dans l'objet.

Indépendamment du type de trafic, vous pouvez également mettre en place une configuration plus générale permettant d'assurer que toutes les communications seront automatiquement basculées vers un lien de secours en cas de panne d'une connexion Internet.

Le nouveau panneau de supervision **Routeurs** permet de consulter en temps réel l'état de toutes les passerelles et la qualité des connexions, et ainsi de gagner du temps en cas de panne. En cas de problème de routeur détecté sur un firewall, une sonde avertit l'utilisateur.

Vous pouvez exporter ces données de supervision au format *.csv*.

La gestion du SD-WAN depuis SMC est possible à partir de la version 4.3.3 des firewalls SNS.

En savoir plus

Configuration du routage depuis SMC

La configuration du routage est désormais disponible dans SMC. Elle est accessible en lecture/écriture pour les firewalls SNS en version 4.2.4 minimum, et en lecture seule pour des firewalls à partir de la version 3.7. Seul le protocole IPv4 est supporté.

Depuis SMC, dans le nouvel onglet **Routage** des paramètres de chaque firewall, configurez et déployez :

- des routes statiques,
- des routes de retour,
- une route par défaut,
- les paramètres de routage dynamique.

Les configurations de routage déjà présentes sur les firewalls SNS sont désormais également visibles dans l'onglet **Routage**.

Cette nouvelle fonctionnalité permet ainsi de consulter la configuration du routage et de préparer des modifications même lorsque les firewalls sont déconnectés.

La configuration des routes statiques depuis SMC permet par exemple de créer des routes dédiées aux interfaces IPsec virtuelles (VTI) dans le cadre des topologies VPN par route. Voir ci-dessous la fonctionnalité de visualisation de tous les types d'interfaces dans SMC.

De nouveaux contrôles de cohérence permettent de vérifier la compatibilité de la configuration du routage et de garantir la validité du déploiement.

En savoir plus

Visualisation de tous les types d'interfaces réseau

SMC permettait déjà de visualiser et d'ajouter ou modifier certains types d'interfaces dans l'onglet **Interfaces** des paramètres de chaque firewall. Il est désormais possible de récupérer dans SMC tous les types d'interfaces existants sur un firewall SNS. Les interfaces de type Wi-Fi, dialup, IPsec, Loopback, GRETUN, GRETAP, USB/Ethernet sont affichées en lecture seule en tant que "Autre interface" dans la grille de l'onglet **Interfaces**.

Tous ces types d'interfaces peuvent être utilisés dans la configuration du routage sur SMC.

En savoir plus

Gestion des administrateurs

Mot de passe de l'utilisateur "root"

Vous pouvez désormais définir le mot de passe de l'utilisateur "root", permettant d'accéder au serveur SMC en ligne de commande, durant l'initialisation manuelle du serveur depuis l'environnement virtuel. Auparavant ce mot de passe était défini dans l'assistant d'initialisation de SMC accessible depuis votre navigateur web.

En savoir plus

Personnalisation de l'interrogation des serveurs d'authentification LDAP

Vous pouvez désormais modifier les attributs LDAP utilisés par défaut par SMC pour interroger les serveurs d'authentification grâce à trois nouvelles variables d'environnement.

En savoir plus

Règles de filtrage et de translation

Nommage des règles copiées

Lorsqu'une règle possédant un nom personnalisé est copiée puis collée dans le même contexte (firewall, dossier ou jeu de règles), le suffixe "_copy" est désormais ajouté à la fin du nom. Ceci permet de garder une trace du lien avec la règle d'origine et facilite la création de règles possédant des caractéristiques et noms similaires.

Si elle est collée dans un contexte différent et qu'une règle portant le même nom n'existe pas déjà, le nom reste identique.

Lorsqu'une règle possédant un nom généré par défaut par le système est copiée et collée, un nouveau nom par défaut lui est attribué.

Intégrité des binaires du serveur SMC

Vérification de l'intégrité des binaires

Les binaires SMC sont désormais signés pour garantir une meilleure protection contre leur corruption.

Consultez la section Télécharger cette version pour prendre connaissance de la nouvelle procédure de vérification des binaires.

Correctifs de SMC 3.2.1

Mise à jour de SMC

Processus de mise à jour

Référence support 84277

Pendant le processus de mise à jour de SMC, des erreurs sans gravité et n'affectant pas le bon déroulement de la mise à jour pouvaient s'afficher en mode ligne de commande. Le serveur n'affiche désormais que les erreurs pertinentes.

Gestion des administrateurs

Authentification via OpenLDAP

Référence support 84152

Dans les paramètres de l'authentification LDAP du menu **Administrateurs**, le champ **Identifiant** du compte de connexion a été renommé **DN Administrateur** pour le type de serveur OpenLDAP. Le format d'identifiant attendu dans ce champ est bien un DN (sans la base DN) du type "cn=administrator".

Configuration des firewalls SNS

Nommage d'un firewall

Référence support 84452

Le message d'erreur et le log d'audit émis lors de la création d'un firewall portant le même nom qu'un objet déjà présent en base de données ont été améliorés pour indiquer qu'un firewall ou un objet du même nom existe déjà.

Déploiement de configuration

Synchronisation des nœuds d'un cluster

Référence support 84333

Lorsque la synchronisation automatique d'un cluster HA était désactivée au moyen de la variable d'environnement `FWADMIN_HASYNC_ON_DESYNCHRO`, le déploiement de configuration sur un cluster provoquait automatiquement la désynchronisation des nœuds. Ce problème est résolu.

Topologies VPN

Déploiement d'une topologie IKEv2

Référence support 84230

Lorsqu'une topologie VPN IKEv2 est déployée depuis SMC, modifier les paramètres d'un correspondant directement sur un firewall SNS ne provoque plus d'erreur Serverd.

Échec de la négociation d'un tunnel

Référence support 84490

La négociation d'un tunnel échoue lorsque le certificat d'un correspondant contient l'adresse IP de contact du firewall dans le champ *Subject Alternative Name* du certificat. En effet le firewall utilise alors cette adresse en tant que **Local ID** du correspondant.

Pour empêcher cela, il est possible de forcer l'utilisation de la valeur du champ *Subject* du certificat en tant que **Local ID** du correspondant en définissant la variable FWADMIN_CERT_SUBJECT_AS_PEER_LOCALID sur "True". Par défaut cette variable est définie sur "False".

Consultation des journaux

Journal d'audit

Référence support 84279

Des logs concernant des utilisateurs anonymes remontaient dans le journal d'audit. Ces informations n'ayant pas d'utilité ne sont désormais plus remontées.

Vulnérabilités résolues de SMC 3.1.6

Protection du serveur

Protection contre les attaques par déni de service

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour des composants OpenSSL et NodeJS.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2022-011/.

Correctifs de SMC 3.1.6

Autorités et certificats

Accès à la liste de révocation des certificats

Référence support 84433

Les firewalls SNS ne retournent plus d'erreur lorsqu'un certificat est déployé avec la valeur "any" en tant que **Adresse IP locale pour vérification de la CRL**.

Correctifs de SMC 3.1.5

Mise à jour de SMC

Mise à jour d'une version 2.8.x vers la version 3.1.4

Référence support 84331

En raison d'un problème de migration de la configuration de l'authentification sur le serveur SMC, la mise à jour d'une version 2.8.x vers la version 3.1.4 n'est pas possible. La version 3.1.5 corrige ce problème. Vous pouvez désormais mettre à jour votre serveur SMC 2.8.x en version 3.1.5.

Supervision des firewalls SNS

Statut des options de licence

Référence support 84121

Lorsqu'au moins l'une des options de licence Breach Fighter, Extended Web Control, Kaspersky, Stormshield Vulnerability Manager et Industrial Security Pack était expirée pour un firewall, SMC affichait un état **Critique**, même lorsque l'option n'était plus utilisée.

L'avertissement de l'expiration proche des options de licence est désormais désactivé par défaut.

Le Guide d'administration indique comment l'activer.

Configuration des firewalls SNS

Gestion des interfaces réseau

Référence support 84270

SMC ne pouvait pas afficher les interfaces réseau d'un firewall SNS qui utilisait une interface de type agrégat. Ce problème est résolu et SMC affiche désormais automatiquement tous les types d'interfaces gérés.

Correctif de SMC 3.1.4

Mise à jour de SMC

Mise à jour d'une version 2.8.x vers la version 3.1.3

Références support 189860CW et 189875CW

En raison d'un problème de migration de la configuration de l'authentification sur le serveur SMC, la mise à jour d'une version 2.8.x vers la version 3.1.3 n'est pas possible. La version 3.1.4 corrige ce problème. Vous pouvez désormais mettre à jour votre serveur SMC 2.8.x en version 3.1.4.

Nouvelles fonctionnalités de SMC 3.1.3

Gestion des administrateurs

Gestion de la connexion aux serveurs d'authentification externes

Il est maintenant possible de configurer la connexion aux serveurs d'authentification LDAP, OpenLDAP et Radius directement dans l'interface web du serveur SMC.

Les comptes des administrateurs sont ainsi gérés plus facilement et de façon plus sécurisée.

Le fichier *auth-server.ini* qui permettait de paramétrer ces connexions en ligne de commande n'existe plus. Si vous aviez paramétré des connexions à des serveurs externes via ce fichier, les paramètres sont automatiquement migrés dans la base de données SMC et vous les retrouverez dans l'interface web.

En savoir plus

Topologies VPN

Support de versions différentes du protocole IKE pour un même firewall

À partir de la version 3.7 des firewalls SNS, il est possible d'utiliser un même firewall dans plusieurs topologies paramétrées avec des versions différentes de IKE.

Si un firewall dont la version est inférieure à la 3.7 est utilisé dans plusieurs topologies avec des versions différentes de IKE, le contrôleur de cohérence remontera une erreur empêchant le déploiement.

Le support de versions différentes de IKE pour un même firewall n'est possible que lorsqu'un seul firewall est commun à plusieurs topologies. Si plusieurs firewalls sont communs à plusieurs topologies paramétrées avec des versions différentes de IKE, c'est la version de la topologie créée en premier dans l'écran de configuration des topologies qui sera déployée.

Mise à jour de l'autorité de certification de SMC

Dans les versions précédentes de SMC, l'autorité de certification du composant qui contrôle la signature du fichier de licence expirait le 4 juillet 2022. Dans la version 3.1.2, l'autorité de certification a été mise à jour afin de prolonger sa durée de validité. Vous devez mettre à jour SMC afin de continuer à utiliser votre licence actuelle au-delà du 4 juillet 2022.

Correctifs de SMC 3.1.3

Déploiement de configuration

Déploiement sur des firewalls avec TPM

Référence support 167766PW

Le déploiement de configuration depuis SMC vers un firewall SNS à partir de la version 4.2.4 utilisant un module TPM est maintenant possible. Auparavant le déploiement restait bloqué à 57% d'avancement parce que l'utilisation d'un TPM n'était pas compatible avec la fonctionnalité de sauvegarde de la configuration sur le firewall SNS en cas de problèmes de connexion avec SMC, introduite en version 4.2.4 de SNS.

Cette fonctionnalité de sauvegarde étant activée par défaut, vous pouvez la désactiver si vous utilisez un TPM, avec la variable d'environnement FWADMIN_FW_DEPLOYMENT_DISABLE_ROLLBACK. Pour en savoir plus sur cette fonctionnalité, consultez la section Déployer une configuration sur des firewalls.

Configuration des firewalls SNS

Détection des modifications de la configuration locale sur les firewalls avec TPM

Référence support 168275PW

La fonctionnalité permettant au serveur SMC de détecter les modifications de configuration effectuées localement sur un firewall SNS utilisant un module TPM est maintenant fonctionnelle.

Correctifs de SMC 3.1.2

Mise à jour du serveur SMC

Accès à l'interface web d'administration après mise à jour en version 3.1.0

Après la mise à jour en version 3.1.0, l'accès à l'interface web ne fonctionnait plus lorsque le champ **Interface de sortie** dans les autorités de certification avait été spécifié afin de gérer le renouvellement des certificats.

En version 3.5.3, ce champ est désormais géré de façon individuelle pour chaque firewall, et non plus au niveau des autorités de certification.

L'accès à l'interface est de nouveau fonctionnel.

Gestion des administrateurs

Identifiants contenant le caractère "."

Références support 188742CW et 168382PW

Il est de nouveau possible de se connecter au serveur SMC avec un identifiant contenant le caractère ".", quelle que soit la provenance du compte de l'administrateur (locale, LDAP ou Radius).

Connexion avec un compte LDAPS

Références support 168375PW, 168393PW, 188642CW et 188403CW

Après la mise à jour en version 3.1.2, la connexion au serveur SMC avec un compte LDAPS est de nouveau fonctionnelle.

Mises à jour Active Update

Mise à jour manuelle des bases de données Active Update

Référence support 168411PW

La mise à jour manuelle de toutes les bases de données Active Update à partir du fichier généré par le script de téléchargement des bases est de nouveau fonctionnelle.

Nouvelles fonctionnalités de SMC 3.1.0

Gestion des administrateurs

Accès au serveur SMC en mode console ou en SSH

Tous les administrateurs peuvent désormais se voir accorder le droit d'accès au serveur SMC via la console de l'hyperviseur ou en SSH. Auparavant, seul l'utilisateur "root" était autorisé.

Ceci permet de faciliter l'accès aux fonctions avancées de gestion du serveur SMC et d'identifier dans les journaux du serveur les connexions et actions des administrateurs ainsi que les élévations de privilèges.

Les administrateurs authentifiés via un serveur d'authentification LDAP ou Radius peuvent également accéder à SMC via la console de l'hyperviseur ou en SSH. Le super-administrateur peut leur octroyer les droits via l'interface d'administration.

Gestion des administrateurs provenant de serveurs d'authentification externes

Il est maintenant possible de gérer directement dans l'interface web du serveur SMC les administrateurs et les groupes possédant un compte sur un serveur d'authentification LDAP.

Le fichier *rights.csv* n'est plus utilisé. Et les commandes `smc-auth-check` et `smc-ui-password` ne sont plus disponibles.

De même, il est possible d'ajouter dans l'interface des groupes d'utilisateurs Radius via un attribut VSA, de la même façon que sur les firewalls SNS.

Le serveur d'authentification OpenLDAP 2.5.x est désormais supporté.

Définition d'un serveur d'authentification de secours

Afin de garantir un accès sans interruption des administrateurs au serveur SMC, vous pouvez définir un serveur d'authentification LDAP ou Radius de secours en cas de panne du serveur principal.

En savoir plus

Environnement non connecté

Serveur Active Update

Le serveur SMC peut désormais faire office de serveur Active Update communiquant avec les serveurs de mise à jour Stormshield, pour distribuer les bases de données Active Update aux firewalls SNS, même lorsqu'ils ne sont pas connectés à Internet. Le service télécharge automatiquement les bases de données périodiquement. Les firewalls disposent ainsi toujours des dernières bases de données (signatures contextuelles, antivirus, Vulnerability Manager, etc.).

Dans les cas où le serveur SMC et les firewalls SNS opèrent dans un réseau fermé sans accès à Internet, vous pouvez télécharger manuellement les bases de données Active Update et les distribuer aux firewalls SNS via le serveur Active Update du serveur SMC.

En savoir plus

Renforcement de la sécurité

Conformité avec le mode "Diffusion restreinte"

Le serveur SMC permet désormais de mettre en œuvre le mode "Diffusion restreinte" sur les firewalls SNS. Ce mode respecte les recommandations de l'ANSSI pour la diffusion de certaines communications transitant par VPN IPsec. Un contrôle de cohérence de la configuration du serveur et des firewalls vous aide à déployer ce mode en détectant automatiquement les paramètres nécessitant des modifications.

L'activation du mode DR sur le serveur SMC entraîne un déploiement de configuration sur les firewalls SNS. Un redémarrage manuel des firewalls est nécessaire.

En savoir plus

Configuration des firewalls SNS

Utilisation des propriétés personnalisées des firewalls

Vous pouvez maintenant créer des propriétés personnalisées en plus des propriétés par défaut Nom, Description et Lieu pour les firewalls, et attribuer des valeurs spécifiques à chaque firewall.

Vous pourrez ainsi filtrer la liste des firewalls ou faire des recherches en vous basant sur ces propriétés.

Elles peuvent être importées ou exportées au format CSV et sont également présentes dans l'export des données de supervision.

En savoir plus

Supervision des firewalls SNS

Export des données de supervision des firewalls SNS

L'export des données de supervision comprend désormais uniquement les données des firewalls affichés dans le panneau, dans le cas où la liste est filtrée.

En savoir plus

Statut des options de licence

Les icônes d'état dans le bandeau supérieur de l'interface d'administration ainsi que la colonne **Options de licence** dans le panneau de supervision des firewalls alertent désormais lorsqu'une option de votre licence ou sa maintenance est proche d'expirer ou est expirée.

Des variables d'environnement permettent de configurer les seuils d'alerte.

En savoir plus

Règles de filtrage et de translation

Consultation des règles locales

Les règles locales d'un firewall sont maintenant affichées en lecture seule dans le panneau des règles de filtrage et de translation.

Configuration du serveur SMC

Attribution dynamique d'une adresse via DHCP

Vous pouvez désormais choisir d'attribuer une adresse IP dynamique au serveur SMC via DHCP. Cette option est disponible dans l'assistant d'initialisation du serveur SMC ou dans les paramètres du serveur, dans l'interface d'administration.

Autorités et certificats

Vérification de la liste de révocation des certificats (CRL)

Pour vérifier la validité des certificats, la variable d'environnement FWADMIN_VPN_CRL_REQUIRED n'est plus supportée. La case à cocher **Vérifier la validité des certificats** est désormais disponible dans le panneau **Configuration** > **Certificats**.

Depuis le panneau de gestion des certificats, l'administrateur peut désormais spécifier pour chaque firewall :

- l'adresse IP locale de renouvellement des certificats SCEP/EST des firewalls SNS,
- l'adresse IP locale permettant de vérifier la liste de révocation,
- la fréquence de vérification de la liste de révocation.

La valeur de l'ancienne variable FWADMIN_VPN_CRL_REQUIRED n'est pas conservée lors de la mise à jour du serveur SMC et le champ **Interface de sortie** dans le panneau de renouvellement des certificats a été supprimé.

Adresse IP locale de renouvellement des certificats obtenus par SCEP ou EST

Pour les firewalls SNS possédant des certificats obtenus via les protocoles SCEP ou EST, vous pouvez désormais spécifier une adresse IP locale à utiliser pour le renouvellement des certificats pour chacun d'entre eux. Auparavant, l'adresse de renouvellement était indiquée dans le panneau des paramètres de l'autorité de certification et était donc la même pour tous les certificats issus d'une même autorité.

En savoir plus

Topologies VPN

Configuration du PRF dans les profils de chiffrement

Vous pouvez maintenant choisir un algorithme devant être négocié en tant que PRF (Pseudo-Random Function) dans l'onglet **IKE** des profils de chiffrement utilisés dans les topologies VPN. Cette option est supportée à partir de la version 4.2.3 des firewalls SNS et n'est compatible qu'avec les topologies IKEv2.

En savoir plus

Nouveaux profils de chiffrement

Les trois profils de chiffrement proposés par le serveur SMC par défaut "Strong encryption", "Mobile encryption" et "Good encryption" ont été renommés "Strong encryption legacy", "Mobile encryption legacy" et "Good encryption legacy". Si vous les aviez modifiés, ils retrouvent leur configuration par défaut.

Le profil "Good encryption legacy" utilise désormais l'algorithme AES à la place de l'algorithme Blowfish et le groupe Diffie-Hellman 2 remplace le groupe Diffie-Hellman 14 en phase 2.

Trois nouveaux profils "Strong encryption", "Mobile" et "Good encryption" remplacent les anciens.

Ces six profils sont en lecture seule.

Base d'objets

Import des objets Routeur

La version 4.3.0 des firewalls SNS permet d'exporter des objets Routeur ainsi que les passerelles associées. Le serveur SMC supporte désormais l'import/export des objets Routeur dans le même format que les firewalls SNS.

L'ancien format CSV (avant SMC 3.1) pour les objets Routeur n'est plus supporté. La configuration de passerelle associée à un objet Routeur est incompatible avec les versions de SMC inférieures à 3.1.

Hébergement Amazon Web Services

Le serveur SMC peut désormais être hébergé par Amazon Web Services (AWS) en mode BYOL (Bring Your Own License).

Vous pouvez choisir entre plusieurs types d'instances afin d'adapter au mieux les ressources du serveur SMC en fonction du nombre de firewalls à administrer.

En savoir plus

Vulnérabilités résolues de SMC 3.1.0

Protection du serveur

Protection de la mémoire du serveur

Une vulnérabilité de niveau bas a été corrigée par la mise à jour du composant PostgreSQL.

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

Protection contre les attaques *Buffler overflow*

Une vulnérabilité de niveau moyen a été corrigée par la mise à jour du composant OpenSSL.

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

Correctifs de SMC 3.1.0

Autorités et certificats

Longueur du Sujet dans un certificat

Référence support 184536CW

Auparavant le serveur SMC tronquait le nombre de caractères du champ Sujet (DN) dans les certificats lorsqu'il dépassait 140 caractères et le déploiement des topologies VPN échouait. Le serveur SMC accepte désormais des certificats dont le sujet dépasse 140 caractères.

Mise à jour de certificat en ligne de commande

Référence support 167610PW

Il est désormais possible de mettre à jour un certificat installé sur un firewall via la commande `smc-install-certificate`.

Règles de filtrage et de translation

Filtrage par le nom d'utilisateur

Référence support 167465PW

Dans une règle de filtrage, il est désormais possible de déclarer un flux filtrant sur un nom d'utilisateur contenant une apostrophe.

Avertissement sur l'analyse des flux chiffrés

Référence support 167465PW

Le contrôleur de cohérence ne remonte désormais plus d'avertissement lorsqu'une règle de déchiffrement d'un flux précède une règle d'analyse du même flux déchiffré.

Mise à jour d'un serveur SMC en version inférieure à 2.7.0

Référence support 185398CW

La mise à jour d'un serveur SMC d'une version inférieure à 2.7.0 vers une version 3.0.0 n'était pas possible si une règle de filtrage bloquante réalisant une translation sur la destination avec une valeur égale à "network-any" était présente. Il est désormais possible de mettre à jour un serveur SMC contenant une telle règle vers une version 3.1.0.

Base d'objets

Recherche d'un groupe d'objets

Référence support 167465PW

Dans la fenêtre de création ou de modification d'un groupe d'objets, le champ **Rechercher** fonctionne désormais sur les adresses IP des objets.

Déploiement forcé des objets

Référence support 167698PW

Lors de la mise à jour de votre serveur SMC en version 3.x, les objets pour lesquels vous avez paramétré un déploiement forcé sur les firewalls SNS sont désormais migrés tout en gardant ce paramétrage.

Topologies VPN

Fragmentation IKE

Référence support 167619PW

Il n'était pas possible d'activer la fragmentation IKE depuis le serveur SMC sur des firewalls SNS en version 3.7.x. Il est maintenant possible de l'activer sur des firewalls en version 3.7.22 et de configurer la taille du fragment.

Supervision des firewalls SNS

Erreur d'affichage de l'écran de supervision des firewalls

Références support 186959CW et 186343CW

Dans certains cas d'erreurs sur les firewalls SNS, l'écran de supervision dans la console d'administration ne s'affichait plus. Ce problème est résolu.

Nouvelle fonctionnalité de SMC 3.0.1

Topologies VPN

Extrémités de trafic

Il est désormais possible d'utiliser la valeur *All* pour définir les extrémités de trafic dans une topologie VPN afin de laisser passer tous les flux à travers les tunnels.

Vulnérabilité résolue de SMC 3.0.1

Protection du serveur

Protection contre les attaques par déni de service

Une vulnérabilité de niveau moyen été corrigée par la mise à jour du composant NodeJS.

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

Correctifs de SMC 3.0.1

Règles de filtrage et de translation

Filtrage sur nom de domaine

Références support 82060

Une règle de filtrage utilisant en critère un nom de domaine accepte désormais tout type de format et pas seulement le format URL.

Export dans un fichier CSV

Références support 82236

La valeur du champ **Inspection** d'une règle de filtrage est désormais correctement exportée lorsqu'elle correspond à *firewall*, *IDS* ou *IPS*.

Déploiement de configuration

État du déploiement

Si le firewall SNS effectue une restauration automatique de configuration après un déploiement à partir de SNS, ce déploiement n'est désormais plus considéré comme réussi et son numéro n'est plus incrémenté.

Configuration sur un cluster

Le déploiement d'une configuration comprenant une configuration réseau sur un cluster ne provoque plus le redémarrage du cluster.

Nouvelles fonctionnalités de SMC 3.0

Authentification

Groupes imbriqués

Un administrateur faisant partie d'un groupe LDAP imbriqué dans un autre peut maintenant se connecter au serveur SMC.

Configuration des firewalls SNS

Gestion des interfaces réseau

Vous pouvez désormais gérer les interfaces réseau des firewalls SNS de manière centralisée sur le serveur SMC. Pour les firewalls SNS en version 3.7 minimum, les interfaces réseau sont affichées sur SMC en lecture seule. Pour les firewalls SNS à partir de la version 4.2.3, vous pouvez activer la configuration des interfaces réseau en écriture dans les paramètres SMC.

Les interfaces Ethernet, les bridges, les VLAN et les agrégats en IPv4 des firewalls compatibles seront donc affichés sur le serveur SMC et leur configuration peut être gérée sans avoir à se connecter sur chaque firewall individuellement. Pour les interfaces supportées, SMC vérifie leur configuration et remonte des erreurs grâce au contrôleur de cohérence.

En savoir plus

Maintien de la connexion lors d'un déploiement

Le déploiement d'une configuration erronée par inadvertance peut provoquer la perte de connexion entre le serveur et le firewall. À partir de la version 4.2.3 des firewalls SNS, la configuration précédente sera restaurée si la connexion a été perdue. Ceci permet de garantir que le firewall reste toujours joignable depuis le serveur SMC.

En savoir plus

Redémarrage après un déploiement

Un firewall SNS peut parfois nécessiter un redémarrage après le déploiement d'une configuration réseau pour appliquer les modifications. Dans un tel cas l'information est remontée par SMC grâce au nouvel état de santé "Redémarrage nécessaire", et il est possible de redémarrer les firewalls concernés directement depuis le serveur SMC. Cette fonctionnalité est supportée sur les firewalls seuls en version 4.2.3.

En savoir plus

Détection de modifications locales

Après un premier déploiement sur un firewall SNS rattaché, SMC détecte désormais si la configuration des éléments gérés par SMC a été modifiée localement. Vous pouvez alors décider de déployer la configuration actuellement présente sur le serveur SMC, écrasant ainsi les modifications locales. Vous pouvez aussi restaurer la dernière configuration qui avait été déployée sur le firewall en question.

En savoir plus

Import des firewalls depuis un fichier CSV

La commande permettant d'importer des firewalls SNS depuis un fichier CSV en ligne de commande a été renommée en `smc-import-firewalls`. L'ancienne commande `smc-firewalls-and-packages` n'est plus supportée.

En savoir plus

Règles de filtrage et de translation

Création de jeux de règles

Vous pouvez désormais créer des jeux de règles pour regrouper les règles de filtrage ou de translation que vous souhaitez déployer sur un ou plusieurs firewalls. Cela vous permet de réutiliser un ensemble de règles correspondant à une application particulière dans la configuration de différents firewalls, indépendamment de leur emplacement dans l'arborescence de dossiers.

En savoir plus

Correctifs de SMC 3.0

Configuration des firewalls SNS

Journaux d'audit inaccessibles

Références support 79393 et 80772

En cas de connexion au firewall via le serveur SMC, l'accès aux journaux d'audit pouvait échouer pour certaines versions de firewalls SNS. Ce problème a été corrigé.

Configuration réseau par clé USB impossible

Référence support 79258

En raison d'une section manquante dans le package de rattachement il était impossible d'utiliser une clé USB pour renseigner la configuration réseau pour un firewall en configuration d'usine. La section a été rajoutée et l'utilisation des clés USB est désormais possible.

Initialisation du serveur SMC

Paramètre ambigu

Référence support 82014

Le paramètre `DNS configuration (leave blank if no DNS)` demandé lors de l'initialisation manuelle du serveur SMC a été modifiée en `DNS server IPs (comma separator or leave blank if no DNS)` pour éliminer des ambiguïtés.

Mise à jour

Fuseau horaire non conservé

Référence support : 80779

Le fuseau horaire défini est désormais conservé après une mise à jour de SMC.

Perte de scripts

Référence support : 71885

Les scripts exécutés automatiquement lors de l'activation d'une interface réseau du système hôte de SMC sont désormais conservés après une mise à jour.

Message d'erreur ambigu

Référence support : 0081991

Un message d'erreur ambigu affiché lors d'un problème de restauration du serveur à partir d'une sauvegarde a été modifiée pour indiquer clairement la cause de l'erreur.

Règles de filtrage et de translation

Import de règles

Référence support : 79314

Lors d'un import de règles de filtrage à partir d'un fichier CSV, l'opérateur "!" (différent de) était ignoré. Ce problème a été corrigé et les champs sont désormais importés en tenant compte de cet opérateur.

Références support : 78561 et 79308

Un import de règles contenant la valeur "any" dans un champ `#nat_to_target` du fichier CSV échouait parce que cette valeur est interdite. La valeur pour ce champ est désormais paramétrée automatiquement à "none" et l'import n'échoue plus.

Référence support : 80828

Il est désormais possible d'importer des règles de filtrage et de translation contenant des noms de domaine.

Référence support : 80590

Il est désormais possible d'importer des règles via un fichier CSV contenant certaines catégories IPRep qui manquaient auparavant.

Adaptation du nom de protocole

Référence support 82222

Dans les règles de filtrage le nom du protocole "ldap" a été modifié en "ldap_tcp" afin d'assurer la cohérence entre SNS et SMC.

Erreur de copier-coller

Référence support : 78373

Dans l'écran des règles de filtrage ou de translation, un copier-coller du texte contenu dans le champ de recherche colle uniquement le texte et ne duplique plus la règle en surbrillance.

Système

Erreurs fréquentes

Référence support : 81714

Des erreurs de connexion au port série s'affichaient toutes les cinq minutes. Ce problème a été corrigé.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Rapporter un incident/Suivre un incident**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.