STORMSHIELD NETWORK SECURITY

NOTES DE VERSION VERSION 3

Édition française

3 juillet 2017

Table des matières

Dans la documentation, Stormshield Network Security est désigné sous la forme abrégée : SNS et Stormshield Network sous la forme abrégée : SN.

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

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

Nouvelles fonctionnalités de la version 3.2.1

Système

Mises à jour

Lorsqu'une nouvelle version de firmware est disponible, un lien permettant de télécharger les *Notes de Version* de cette mise à jour est affiché dans le module **Système** > **Maintenance** > onglet **Mise à jour du système** et dans le **Tableau de bord** > panneau **Propriétés**.

Vulnérabilités résolues de la version 3.2.1

Faille de sécurité ASN.1

Une vulnérabilité (CVE-2017-9023 - Incorrect Handling of CHOICE types in ASN.1 parser and x509 plugin) a été corrigée par la mise à jour du moteur de gestion des tunnels IPSec IKEv2 en version 5.5.3. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Correctifs de la version 3.2.1

Système

Vérification des CRL

Référence support 64074

Le firewall n'effectuait plus de résolution DNS pour obtenir l'adresse des points de distribution des listes de révocation de certificats (CRL - Certificate Revocation Lists). Ce problème a été corrigé.

Objets réseau

Référence support 64023

La validation d'un nouvel objet réseau par le bouton "Créer et dupliquer", rendait ce bouton et le bouton "Créer" inactifs pour valider l'objet suivant. Cette anomalie a été corrigée.

Filtrage URL

Référence support 64489

Lors de la connexion à l'interface d'administration d'un firewall SNS via Stormshield Management Center, la requête générée par un clic sur le bouton **Ajouter des règles par catégorie** du module **Filtrage URL** n'aboutissait pas. Cette anomalie a été corrigée.

Prévention d'intrusion

Protocole HTTP

Référence support 61269

L'analyse de pages Web utilisant des balises HTML dont la chaîne de caractères définissant certains attributs était conséquente, déclenchait l'alarme bloquante "Dépassement de capacité dans un attribut HTML". Ce comportement, légitime, pouvait également aboutir à un blocage du firewall. Ce problème a été corrigé.

Référence support 64941 - 64920

Lorsque les analyses Web 2.0 étaient activées (cases **Inspecter le code HTML** et **Inspecter le code Javascript** cochées dans le module **Protocoles** > **HTTP** > onglet **IPS**), la consultation de pages incluant du code vbscript commenté pouvait aboutir à un blocage du firewall. Ce problème a été corrigé.

Compatibilité

Version minimale requise : Stormshield Network 2.x

Compatibilité matérielle :

SN150, SN160(W), SN200, SN210(W), SN300, SN310, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000 et SN6000

SNi40

NETASQ U30S, U70S, U150S, U250S, U500S et U800S

Stormshield Network et NETASQ Virtual Appliances

Compatibilité avec les hyperviseurs :

VMWare ESX/ESXi : version 5.5 ou supérieure

Citrix Xen Server : version 6.2 ou supérieure

Microsoft Hyper-V : Windows Server 2012 ou supérieure

Linux KVM : Red Hat Enterprise Linux 7.2 ou supérieure

Versions minimales requises pour les logiciels clients Stormshield Network :

SSO Agent : version 1.4 ou supérieure

SSL VPN Client : version 2.0 ou supérieure

Compatibilité logicielle pour l'installation de la suite d'administration (SN Real-Time Monitor et SN Global Administration) :

Microsoft Windows 7, 8 et 10

Microsoft Windows Serveur 2008 et 2012

NOTE

Pour un fonctionnement optimal de l'interface d'administration des firewalls, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Internet Explorer et Mozilla Firefox (version LTS - Long Term Support). Pour de plus amples renseignements sur ces versions, nous vous invitons à consulter les Cycles de Vie des Produits des éditeurs concernés.

Préconisations

Avant de migrer une configuration existante vers la version 3 de firmware, veuillez :

- lire attentivement la section Problèmes connus,
- lire attentivement la section Précisions sur les cas d'utilisation,
- **réaliser une sauvegarde** de la partition principale vers la partition secondaire ainsi qu'une sauvegarde de configuration.

Extended Web Control

Si le mode synchrone est activé pour la solution de filtrage d'URL Extended Web Control, il est impératif de le désactiver avant de mettre à jour le firewall en v3. Pour ce faire, supprimez la ligne contenant le paramètre *X-CloudURL_Async* (section *[Config]* du fichier de configuration *ConfigFiles/proxy*).

Mise à jour d'un cluster avec plusieurs liens de haute disponibilité

Pour un cluster mettant en œuvre plus d'un lien dédié à la haute disponibilité, il est nécessaire de s'assurer que le lien principal est actif avant de procéder à la mise à jour en version 3.

Méthode d'authentification "Agent SSO"

Dans une configuration utilisant la méthode d'authentification "Agent SSO", il est nécessaire d'effectuer la migration de l'agent SSO en version 1.4 avant de réaliser celle du firewall.

Il est également nécessaire de renseigner le champ "Nom de domaine" dans la configuration de l'agent SSO AVANT MIGRATION DU FIREWALL. Ce nom de domaine doit correspondre au nom réel du domaine (exemple: stormshield.eu) pour permettre le fonctionnement de l'agent SSO.

Routage par politique de filtrage

Si une remise en configuration d'usine du firewall (*defaultconfig*) est réalisée suite à une migration d'une version 1 vers une version 2 puis vers une version 3, 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).

Politique de filtrage et utilisateurs

Dans les versions précédentes de firmware, la politique de filtrage ne distinguait pas les utilisateurs des groupes. En version 3, la gestion des annuaires multiples impose une vérification stricte des utilisateurs. Une migration de configuration vers la version 3 de firmware peut ainsi générer des avertissements invitant l'administrateur à ressaisir les utilisateurs dans sa politique de filtrage pour lever cette ambiguïté.

Problèmes connus

Prévention d'intrusion

Protocole SIP

Les requêtes SIP de type REGISTER contenant un astérisque dans le champ Contact de leur en-tête ne sont pas supportées. Elles génèrent l'alarme bloquante « *The SIP request contains an invalid URI (Contact field)* ».

Protocole SSL/TLS

La version 1.3 du protocole de sécurisation TLS (Transport Layer Security) n'étant pas finalisée, le firewall déclenche une alarme lorsqu'il détecte une tentative de négociation utilisant cette version du protocole TLS.

Système

Journaux d'audit - Rapports

Référence support 58515 58520 58594 58634

La migration vers la version 3 de firmware désactive volontairement le rapport "Top des recherches Web". En effet, ce rapport est susceptible d'entraîner des blocages réguliers du service de journalisation du firewall et cette instabilité provoque de fortes perturbations du trafic réseau (proxy et inspections de sécurité).

Le rapport peut néanmoins être réactivé à l'issue de la migration (module **Notifications** > **Configuration des rapports**).

Routage

Il n'est pas possible d'utiliser les interfaces IPSec pour spécifier le routage au sein de règles de filtrage pour des flux IPv6. Cette restriction concerne les interfaces directement spécifiées ainsi que les objets routeurs contenant des interfaces IPSec.

Filtrage

Le champ correspondant au nom d'une règle de filtrage (*rulename*) n'apparaît pas dans les fichiers de traces des proxies.

Proxies

Référence support 55656

L'accès à des sites utilisant un mécanisme de partage d'origine croisées (CORS : Cross-Origin Resource Sharing) depuis une machine multi-utilisateur ne permet pas d'afficher les ressources externes du site visité.

Machines virtuelles

Plate-forme d'hébergement Microsoft Azure

La plate-fome Azure autorisant l'utilisation des guillemets dans le mot de passe du compte *admin*, et ce caractère étant interdit par le firewall, celui-ci remplace le mot de passe saisi par le mot de passe par défaut ("admin").

Précisions sur les cas d'utilisation

Réseau

Modems 4G

Référence support 57403

La connectivité du firewall à un modem USB 4G nécessite l'utilisation d'un équipement de marque HUAWEI supportant la fonction HiLink (exemple : E8372H-153).

Protocoles Spanning Tree (RSTP / MSTP)

Les Firewalls Stormshield Network ne supportent pas les configurations multi-régions MSTP. Un firewall implémentant une configuration MSTP et positionné en interconnexion de plusieurs régions MSTP pourrait ainsi rencontrer des dysfonctionnements dans la gestion de sa propre région.

Un firewall ayant activé le protocole MSTP, et ne parvenant pas à dialoguer avec un équipement qui ne supporte pas ce protocole, ne bascule pas automatiquement sur le protocole RSTP.

Le fonctionnement des protocoles RSTP et MSTP nécessite que les interfaces sur lesquelles ils sont appliqués disposent d'une couche Ethernet. En conséquence :

- le protocole MSTP ne supporte pas les modems PPTP/PPPoE,
- le protocole RSTP ne supporte ni les Vlans, ni les modems PPTP/PPPoE.

Interfaces

Les interfaces du firewall (VLANs, interfaces PPTP, interfaces agrégées [LACP], etc.) sont désormais rassemblées dans un pool commun à l'ensemble des modules de configuration. Lorsqu'une interface précédemment utilisée dans un module est libérée, elle ne devient réellement réutilisable pour les autres modules qu'après un redémarrage du firewall.

La suppression d'une interface VLAN provoque un ré-ordonnancement de ce type d'interfaces au redémarrage suivant. Si ces interfaces sont référencées dans la configuration du routage dynamique ou supervisées via la MIB-II SNMP, ce comportement induit un décalage et peut potentiellement provoquer un arrêt de service. Il est donc fortement conseillé de désactiver une interface VLAN non utilisée plutôt que de la supprimer.

Les interfaces Wi-Fi ne peuvent pas être incluses dans un bridge.

Sur les modèles SN150 et SN160w, une configuration comportant plusieurs VLANs inclus dans un bridge n'est pas supportée.

Un problème a été identifié sur les modèles U30S et SN200 lors de la création de plusieurs VLANs au sein d'un bridge. Ce problème peut potentiellement entraîner un défaut de transmission des réponses aux requêtes ARP reçues sur ces VLANs vers les autres interfaces du bridge.

Routage dynamique Bird

Le moteur de routage dynamique Bird ayant été mis à jour en version 1.6, il est nécessaire, dans les configurations implémentant le protocole BGP avec de l'authentification, d'utiliser l'option "*setkey no*". Pour de plus amples informations sur la configuration de Bird, veuillez consulter la Note Technique "**Routage dynamique Bird**".

Lorsque le fichier de configuration de Bird est édité depuis l'interface d'administration Web, l'action « Appliquer » envoie effectivement cette configuration au firewall. En cas d'erreur de syntaxe, 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.

Support IPv6

En version 2, voici les principales fonctionnalités non disponibles pour le trafic IPv6 :

- La translation d'adresses IPv6 (NATv6),
- Inspections applicatives (Antivirus, Antispam, cache HTTP, Filtrage URL, Filtrage SMTP, Filtrage FTP, Filtrage SSL),
- L'utilisation du proxy explicite,
- Le cache DNS,
- Les tunnels VPN SSL portail,
- Les tunnels VPN SSL,
- L'authentification via Radius ou Kerberos,
- Le Management de Vulnérabilités,
- Les interfaces modems (en particulier les modems PPPoE).

Haute Disponibilité

Dans le cas où un Firewall est en Haute Disponibilité et a activé la fonctionnalité IPv6, les adresses MAC des interfaces portant de l'IPv6 (autres que celles du lien HA) doivent impérativement être définies en configuration avancée. En effet, les adresses de lien local IPv6 étant dérivées de l'adresse MAC, ces adresses seront différentes, entraînant des problèmes de routage en cas de bascule.

Système

Migration

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

Mises à jour vers une version antérieure

Les firewalls livrés en version 3 de firmware ne sont pas compatibles avec les versions majeures antérieures.

Le retour à une version majeure de firmware antérieure à la version courante du firewall nécessite préalablement une remise en configuration d'usine du firewall (*defaultconfig*). Ainsi par exemple, cette opération est nécessaire pour la migration d'un firewall d'une version 3.0.1 vers une version 2.x.

Filtrage d'URL

Les modèles SN150, SN200, SN300, U30S et U70S ne permettent pas de bénéficier de plus de 10 profils de filtrage d'URL. Sur les autres modèles, l'ajout de profils est exclusivement réalisable en éditant le fichier de configuration du filtrage d'URL (ConfigFiles/URLFiltering/slotinfo) pour y

ajouter des sections supplémentaires puis en créant ou téléchargeant les profils correspondants (11, 12, ...) dans le répertoire ConfigFiles/URLFiltering.

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

Si une sauvegarde de la configuration a été réalisée sur un Firewall dont la version du système est postérieure à la version courante, il ne sera alors pas possible de restaurer cette configuration. Ainsi par exemple, il n'est pas possible de restaurer une configuration sauvegardée en 3.0.0, si la version courante du firewall est la 2.5.1.

Objets dynamiques

Les objets réseau en résolution DNS automatique (dynamic), 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 être utilisés que dans les règles de filtrage.

Lorsqu'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 nécéssiter 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.

Surveillance matérielle (watchdog)

Les modèles SN150 ne disposent pas de la fonction de surveillance matérielle (hardware watchdog).

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.

Qualité de service

Les flux réseaux auxquels sont appliquées des files d'attente de qualité de service (QoS) ne tirent pas entièrement bénéfice des améliorations de performances liées au mode « fastpath ».

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 dépendant du type de trafic qui ne nomme pas forcément de la même façon les objets (*srcname* et *dstname*). Pour éviter de multiples représentations d'un même objet dans les rapports, il est conseillé de donner à l'objet créé dans la base du Firewall, le même nom que celui associé via la résolution DNS.

Prévention d'intrusion

Protocole GRE et tunnels IPSec

Le déchiffrement de flux GRE encapsulés dans un tunnel IPSec génère à tort l'alarme « *Usurpation d'adresse IP sur l'interface IPSec* ». Il est donc nécessaire de configurer l'action à *passer* sur cette alarme pour faire fonctionner ce type de configuration.

Analyse HTML

Le code HTML réécrit n'est pas compatible avec tous les services web (apt-get, Active Update) parce que l'en-tête HTTP « Content-Length » a été supprimé.

Messagerie instantanée

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

Référence support 35960

Préserver le routage initial

L'option permettant de préserver le routage initial sur une interface n'est pas compatible avec les fonctionnalités pour lesquelles le moteur de prévention d'intrusion doit créer des paquets :

- la réinitialisation des connexions lors de la détection d'une alarme bloquante (envoi de paquet RESET),
- la protection SYN Proxy,
- la détection du protocole par les plugins (règles de filtrage sans protocole spécifié),
- la réécriture des données par certains plugins tels que les protections web 2.0, FTP avec NAT, SIP avec NAT et SMTP.

NAT

Référence support 29286

La gestion d'état pour le protocole GRE est basée sur les adresses source et destination. Il n'est donc possible de discerner deux connexions en même temps avec le même serveur, soit du

même client soit partageant une adresse source commune (cas du "map").

Support H323

Le support des opérations de translation d'adresses du protocole H323 est rudimentaire, en particulier : il ne supporte pas les cas de contournement du NAT par les gatekeeper (annonce de l'adresse autre que source ou destination de la connexion).

Proxies

Référence support 35328

Proxy FTP

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

Filtrage

Interface de sortie

Une règle de filtrage précisant une interface de sortie incluse dans un bridge, et qui ne serait pas la première interface de ce bridge, n'est pas exécutée.

Filtrage Multi-utilisateur

Il est possible de permettre l'authentification Multi-utilisateur à un objet réseau (plusieurs utilisateurs authentifiés sur une même adresse IP) en renseignant l'objet dans la liste des Objets Multi-utilisateurs (Authentification > Politique d'authentification).

Les règles de filtrage avec une source de type user@objet (sauf any ou unknow@object), avec un protocole autre qu'HTTP, ne s'appliquent pas à cette catégorie d'objet. Ce comportement est inhérent au mécanisme de traitement des paquets effectué par le moteur de prévention d'intrusion. Le message explicite avertissant l'administrateur de cette limitation est le suivant : « Cette règle ne peut identifier un utilisateur connecté sur un objet multi-utilisateur ».

Géolocalisation et réputation des adresses IP publiques

Lorsqu'une règle de filtrage précise des conditions de géolocalisation et de réputation d'adresses publiques, il est nécessaire que ces deux conditions soient remplies pour que la règle soit appliquée.

Réputation des machines

Si les adresses IP des machines sont distribuées via un serveur DHCP, la réputation d'une machine dont l'adresse aurait été reprise par une autre machine sera également attribuée à celle-ci. Dans ce cas, la réputation de la machine peut-être réinitialisée à l'aide de la commande en ligne `monitor flush hostrep ip = host_ip_address`.

Référence support 31715

Filtrage URL

Le filtrage par utilisateur authentifié n'est pas possible au sein d'une même politique de filtrage URL. Il est toutefois possible d'appliquer des règles de filtrage particulières (Inspection applicative) selon les utilisateurs.

VPN IPsec

Déchiffrement

La répartition du déchiffrement des données est réalisée par correspondant IPSec. Sur les firewalls multi-processeur, ce traitement est donc optimisé lorsque le nombre de correspondants est au moins égal au nombre de processeurs du boitier.

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.

Référence support 37332

DPD (Dead Peer Detection)

La fonctionnalité VPN dite de DPD (Dead Peer Detection) permet de vérifier qu'un correspondant est toujours opérationnel, par des requêtes de test de disponibilité.

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 négocié avant d'avoir identifié le correspondant, et donc avant de connaître si les requêtes DPD peuvent être ignorées pour ce correspondant.

Ce paramètre n'est pas modifié en mode agressif, car dans ce cas le DPD est négocié lorsque le correspondant est déjà identifié, ou dans le cas où le firewall est initiateur de la négociation.

Keepalive IPv6

Pour les tunnels IPSec site à site, l'option supplémentaire keepalive, permettant de maintenir ces tunnels montés de façon artificielle, n'est pas utilisable avec des extrémités de trafic adressées en IPv6. Dans le cas d'extrémités de trafic configurées en double pile (adressage IPv4 et IPv6), seul le trafic IPv4 bénéficiera de cette fonctionnalité.

VPN IPSec IKEv2

Les deux versions du protocole IKE (IKEv1 et IKEv2) ne peuvent actuellement pas être utilisées simultanément au sein d'une même politique IPSec.

Le protocole EAP (Extensible Authentication Protocol) ne peut pas être utilisé pour l'authentification de correspondants IPSec utilisant le protocole IKEv2.

Dans une configuration mettant en œuvre un tunnel IPSec basé sur le protocole IKEv2 et de la translation d'adresse, l'identifiant présenté par la machine source au correspondant distant pour établir le tunnel correspond à son adresse IP réelle et non à son adresse IP translatée. Il est donc conseillé de forcer l'identifiant local à présenter (champ Local ID dans la définition d'un correspondant IPSec IKEv2) en utilisant l'adresse translatée (si celle-ci est statique) ou un FQDN porté par le firewall source.

Il n'est pas possible de définir une configuration de secours pour les correspondants IPSec utilisant le protocole IKEv2. Pour mettre en œuvre une configuration IPSec IKEv2 redondante, il est conseillé d'utiliser des interfaces virtuelles IPSec et des objets routeurs dans les règles de filtrage (PBR).

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.

Les méthodes SPNEGO et Kerberos ne peuvent pas être utilisées sur plusieurs domaines Active Directory.

La phase 1 de négociation IPSec n'est pas compatible avec les annuaires Microsoft Active Directory multiples pour l'authentification des clients mobiles.

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

Annuaires multiples

Les utilisateurs définis comme administrateurs du firewall doivent obligatoirement être issus de l'annuaire par défaut.

Les clients IPSec mobiles ne peuvent s'authentifier que sur l'annuaire par défaut.

Les utilisateurs ne peuvent s'authentifier que sur l'annuaire par défaut via les méthodes certificat SSL et Radius.

Méthode CONNECT

L'authentification multi-utilisateur sur une même machine en mode Cookie, ne supporte la méthode CONNECT (protocole HTTP). Cette méthode est généralement utilisée avec un proxy explicite pour les connexions HTTPS. Pour ce type d'authentification, il est recommandé d'utiliser le mode « transparent ». Pour plus d'informations, consultez l'aide en ligne à l'adresse documentation.stormshield.eu, chapitre Authentification.

Conditions d'utilisation

L'affichage des Conditions d'utilisation d'accès à Internet sur le portail captif peut avoir un rendu incorrect sous Internet Explorer v9 avec le mode compatibilité IE Explorer 7.

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.

Haute Disponibilité

Interaction H.A en mode bridge et switchs

Dans un environnement avec un cluster de Firewall configuré en mode bridge, le temps de bascule du trafic constaté est de l'ordre des 10 secondes. Ce délai est lié au temps de bascule d'1 seconde auquel vient s'ajouter le temps de réapprentissage des adresses MAC par les switches qui sont directement connectés aux Firewalls.

Routage par politique

Une session routée par la politique de filtrage peut être perdue en cas de bascule du cluster.

Modèles

La Haute disponibilité basée sur un groupe (cluster) de Firewalls de modèles différents n'est pas supportée. D'autre part, un groupe avec un Firewall utilisant un firmware en 32 bits et l'autre en 64 bits n'est pas autorisé.

Management des vulnérabilités

Référence support 28665

L'inventaire d'applications réalisé par le Management des vulnérabilités se base sur l'adresse IP de la machine initiant le trafic pour indexer les applications.

Le cas de machines ayant une adresse IP partagée par plusieurs utilisateurs, par exemple un proxy HTTP, un serveur TSE ou encore un routeur réalisant du NAT dynamique de la source, peuvent entraîner une charge important sur le module. Il est donc conseillé de mettre les adresses de ces machines dans la liste d'exclusion (éléments non supervisés).

Suite d'administration Stormshield Network

SN Real-Time Monitor

Les commandes de transfert de fichiers (envoi et réception) depuis la console CLI de SN Real-Time Monitor ne fonctionnent plus en versions 2 et supérieures.

Référence support 28665

La commande CLI MONITOR FLUSH SA ALL est initialement dédiée à désactiver les tunnels IPsec en cours, en supprimant leur association de sécurité (SA - security association). Cependant, le routage dynamique Bird utilisant également ce type d'association de sécurité (SA), cette commande dégrade la configuration de Bird, empêchant toute connexion. Ce problème se pose également avec la fonction « Réinitialiser tous les tunnels » proposée dans l'interface de Real Time Monitor.

Pour résoudre ce problème, il est nécessaire de redémarrer le service Bird.

SN Event Reporter

SN Event Reporter n'est plus inclus dans la suite d'administration en version 3 ou supérieure, et les connexions depuis SN Event Reporter sur les firewalls en version 3 ou supérieure ne sont pas supportées

Documentation

Les documentations techniques suivantes sont disponibles au format PDF dans la base documentaire sur l'espace client. Nous vous invitons à vous appuyer sur l'ensemble de ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Stormshield Network Firewall - Manuel d'utilisation et de configuration
- Firewalls Virtuels Stormshield Network - Guide d'installation
- Stormshield Network Global Administration - Manuel d'utilisation et de configuration
- Stormshield Network Real-Time Monitor - Manuel d'utilisation et de configuration
- CLI Serverd - Commands reference guide
- CLI Console / SSH - Commands reference guide

Notes techniques

- Encapsulation niveau 2
- Stacking : répartition de trafics sur plusieurs firewalls
- Agrégation de liens LACP
- Identifier les commandes de protocoles industriels traversant le firewall
- Interfaces virtuelles IPsec
- Tunnels VPN SSL
- Sauvegardes automatiques
- Base de filtrage URL personnalisée
- Description des journaux d'audit
- Mode hybride cloud firewall-appliance
- Routage dynamique bird
- Sécurité collaborative
- Stormshield Network Security for Cloud - Amazon Web Services
- Stormshield Network Security for Cloud - Microsoft Azure
- Adapter la politique de sécurité SES d'un poste selon sa réputation SNS

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

Empreintes

Afin de vérifier l'intégrité des binaires Stormshield Network Security, entrez l'une des commandes suivantes et comparez le résultat avec les empreintes indiquées sur l'espace client MyStormshield, rubrique **Téléchargements** :

- Système d'exploitation Linux : `sha256sum filename`
- Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`

Remplacez `filename` par le nom du fichier à vérifier.

Apport des versions précédentes de Stormshield Network Security 3

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de Stormshield Network Security 3.

3.2.0	Nouvelles fonctionnalités	Correctifs
3.1.2		Correctifs
3.1.1	Nouvelles fonctionnalités	Correctifs
3.1.0	Nouvelles fonctionnalités	Correctifs
3.0.3		Correctifs
3.0.2		Correctifs
3.0.1	Nouvelles fonctionnalités	Correctifs
3.0.0	Nouvelles Fonctionnalités	

Nouvelles fonctionnalités de la version 3.2.0

Système

Active update

Pour les configurations utilisant des signatures de protection contextuelle personnalisées, le module **Active Update** permet de renseigner les URL des machines hébergeant ces signatures, afin de bénéficier de mises à jour automatiques.

Filtrage et NAT

Les règles d'un slot de filtrage et de NAT peuvent être exportées au format CSV (Comma-Separated Values).

Haute disponibilité

Lors d'un problème de communication entre les membres d'un cluster bien que le firewall actif soit joignable, le firewall passif effectue une vérification des priorités réciproques afin de ne pas passer actif en cas de redémarrage.

Un critère de durée minimum pour la sélection des connexions à synchroniser (*ConnOlderThan*) a été ajouté au mécanisme de HA. Il permet, par exemple, de ne synchroniser que les connexions dont la durée excède 10 secondes. Ce paramètre n'est modifiable qu'à l'aide de la commande CLI : `config ha update ConnOlderThan=xx`

Agent SNMP

L'ensemble des MIB NETASQ a été renommé en Stormshield (Exemple : STORMSHIELD-SMI-MIB).

Plusieurs tables ont été ajoutées à STORMSHIELD-SYSTEM-MONITOR-MIB afin de fournir :

- des informations sur le statut du bypass matériel (firewalls industriels SNi40),
- l'état des alimentations électriques,
- la température des processeurs,
- l'état des disques et du RAID éventuel.

Dans le cas d'une configuration en Haute Disponibilité, les informations concernant l'état de synchronisation des membres du cluster, le numéro de révision de déploiement via Stormshield Management Center, l'état des alimentations, la température des processeurs et l'état des disques sont également disponibles pour le firewall actif et le firewall passif en interrogeant STORMSHIELD-HA-MIB

Objets réseau

Lors de la vérification de l'utilisation d'un objets réseau, le nom appliqué à la règle de filtrage ou de NAT concernée est ajouté aux informations affichées.

Droits d'accès

La commande MONITOR USER affiche les droits d'accès des utilisateurs (Accès VPN, Parrainage,...). Un lien dans la fiche d'un utilisateur mène directement dans l'onglet *Accès détaillé* du module **Droits d'accès** en filtrant sur l'utilisateur sélectionné. Ces droits sont également disponibles dans les sauvegardes de configuration.

Notifications
La connexion (Interface Web d'administration / Stormshield Management Center / NSRPC) d'un utilisateur ayant les droits d'administration sur un firewall déclenche une notification de ce firewall à destination des autres administrateurs.

Configuration des annuaires
Un groupe d'utilisateurs peut contenir d'autres groupes. Cette fonctionnalité s'applique à tous les types d'annuaires supportés par les firewalls SNS (Annuaire LDAP interne, Annuaires LDAP externes, Annuaires LDAP externes de type POSIX, Annuaires Microsoft Active Directory).

Proxies
L'analyse Sandboxing a été étendue aux fichiers issus des technologies Java et Flash.

VPN SSL
Le service VPN SSL supporte les connexions basées sur le protocole UDP ou TCP. En cas de défaut de connexion sur UDP, le client bascule alors automatiquement sur le protocole TCP.

Cette fonctionnalité nécessite l'utilisation du logiciel SSL VPN CLient en version 2.4 ou supérieure.

VPN IPsec (IKEv1)
L'authentification d'utilisateurs nomades à l'aide de certificats peut être réalisée au travers d'un annuaire LDAP externe autre que l'annuaire par défaut.

VPN IPsec (IKEv2)
La version 3.2.0 de firmware assure le support du mécanisme de fragmentation pour le protocole IKEv2.

Réseau

Routage dynamique
Une option a été ajoutée afin d'injecter automatiquement, dans la table des réseaux protégés du moteur de prévention d'intrusion, les réseaux propagés par le moteur de routage dynamique (IPv4 / IPv6).

Le nom personnalisé d'une interface réseau est pris en compte par la configuration du moteur de routage dynamique. En cas de restauration de cette configuration sur un équipement ne connaissant pas ce nom personnalisé, c'est le nom système de l'interface qui est automatiquement utilisé.

Réseau Wi-Fi
Une option a été ajoutée afin d'empêcher les connexions directes entre machines connectées au réseau Wi-Fi géré par le firewall (*AP Isolation*). Cette option (module **Réseau** > **Interfaces**) est activée par défaut (configuration type Point d'accès Wi-Fi publique); lorsqu'elle est désactivée, les connexions directes entre équipements connectés au réseau Wi-Fi ne sont plus filtrées.

Prévention d'intrusion

Protocole OPC DA
Le moteur de prévention d'intrusion analyse le protocole industriel OPC DA (OPC Data Access).

Protocole TDS (Microsoft SQL Server)

Le moteur de prévention d'intrusion analyse les paquets de flux de données tabulaires (TDS - Tabular Data Stream) utilisés par l'application Microsoft SQL Server.

Protocole DCE/RPC (Microsoft RPC)

Le module de configuration pour l'analyse de prévention d'intrusion du protocole DCE/RPC a été modifié : il est désormais possible de définir des UUID de services DCE/RPC non prédéfinis dans une liste blanche des services à autoriser.

Interface Web d'administration

Journaux d'audit

Le journal d'événements des alarmes (fichier *l_alarm*) précise le nom des applications détectées par le moteur de prévention d'intrusion et ayant généré une alarme.

Supervision

Les données de supervision peuvent être imprimées sous forme graphique.

Rapports

Le rapport présentant les scores de réputation les plus élevés prend également en compte les machines internes destinataires de flux.

Un rapport présentant les applications ayant généré le plus d'alarmes est disponible dans le module **Rapports** > **Sécurité**.

Correctifs de la version 3.2.0

Système

Certificats et PKI

Référence support 60548

Lors d'une requête SCEP (Simple Certificate Enrollment Protocol) à destination d'une PKI gérée par une plate-forme Microsoft Windows, la phase d'authentification échouait car l'encodage du mot de passe émis était différent de celui attendu (le protocole SCEP ne faisant pas encore l'objet d'une RFC). Cette anomalie a été corrigée.

Agent SNMP

Référence support 49523

L'OID (Object Identifier) correspondant à la quantité totale de mémoire tampon réservée (MIB UCD-SNMP) pouvait retourner à tort une valeur ne correspondant pas au format attendu (32 bits). Ce problème a été corrigé.

Référence support 54961

L'identifiant unique de l'agent SNMP était modifié à chaque redémarrage du service SNMP du firewall, provoquant ainsi potentiellement un défaut de communication avec les solutions de supervision.

Configuration des annuaires

Référence support 58839

La modification du nom d'un annuaire LDAP n'était pas répercutée dans les autres modules référençant cet annuaire (exemple : Filtrage et NAT). Cette anomalie a été corrigée.

Référence support 57419

Dans une configuration LDAP précisant un serveur de secours, et lorsque le serveur principal n'était plus joignable, les requêtes LDAP en mode synchrone (exemple : VPN SSL) n'étaient pas redirigées vers le serveur de secours. Ce problème a été corrigé.

Authentification

Référence support 59422

La première activation d'une méthode d'authentification n'était effective qu'après avoir rempli et validé ses éléments de configuration à deux reprises. Cette anomalie a été corrigée.

Sauvegardes automatiques

Référence support 59229

Des problèmes potentiels de communication entre les firewalls et les serveurs de sauvegardes automatiques ont été résolus en ajoutant l'autorité de certification racine Stormshield dans les autorités de confiance de ces serveurs.

Filtrage et NAT

Référence support 59849

Une règle de filtrage contenant plusieurs milliers d'adresses IP incluses dans des groupes en source ou destination pouvait provoquer un redémarrage en boucle du firewall. Ce problème a été corrigé.

Référence support 54522

L'option "Protéger des attaques SYN flood" (module **Filtrage et Nat** > **Action** > onglet **Qualité de service** > panneau **Seuil de connexion** > champ **Si le seuil est atteint**) ne fonctionnait pas pour protéger un serveur caché par de la translation d'adresses. Ce problème a été corrigé.

Translation d'adresses

Référence support 58919

Pour translater la source d'un flux émis par le firewall, il était impératif de ne pas spécifier de destination après translation (suppression de la valeur *Any* précisée dans la colonne **Destination** de la section **Trafic après translation**). Cette anomalie a été corrigée.

Commande CLI

Référence support 58853

La commande MONITOR FLUSH STATE *X.Y.Z.A* vidait la table des hôtes et des connexions au lieu de supprimer exclusivement les entrées concernant la machine X.Y.Z.A. Ce problème a été corrigé.

Haute disponibilité

Référence support 53958

L'état des disques des firewalls est pris en compte dans le calcul de qualité des membres d'un cluster.

Référence support 56613

Une instabilité du moteur de synchronisation des données provoquait un redémarrage en boucle du service de gestion de la Haute Disponibilité. Ce dysfonctionnement pouvait entraîner un passage du firewall passif en mode actif, les deux firewalls du cluster devenant alors actifs. Ce problème a été corrigé.

Référence support 56700

Les modifications apportées aux préférences utilisateurs sur le firewall actif n'étaient pas synchronisées avec le firewall passif. Cette anomalie a été corrigée.

Référence support 57317

Lorsque la table des événements à synchroniser était remplie, le moteur de gestion de la haute disponibilité tentait une nouvelle synchronisation complète, au détriment des performances du firewall. Ce comportement a été modifié, et le mécanisme supprime d'abord les plus anciens événements afin de pouvoir ajouter les plus récents dans la file d'attente.

Référence support 58846

Dans une configuration en Haute Disponibilité, les interfaces initialement inactives sur le firewall principal étaient indiquées comme actives après un double changement de rôle de ce firewall au sein du cluster (actif/passif/actif). Cette anomalie a été corrigée.

Référence support 58842

Lors d'un changement de rôle des firewalls au sein d'un cluster, la restauration des connexions actives en mode incrémental ne tenait pas compte de la filiation de ces connexions (flux de connexion / flux de données). Dans ce cas, les flux de données pour des protocoles de type FTP n'étaient ainsi pas transférés. Ce problème a été corrigé.

Proxies

Référence support 60090

Dans une configuration pour laquelle :

- Les analyses Web 2.0 étaient désactivées (case **Inspecter le code HTML** décochée dans l'onglet **IPS** du protocole HTTP),
- L'alarme « http:150 additional data at end of reply » était positionnée à passer.

Des requêtes http de type POST à destination du proxy pouvaient alors entraîner un blocage du firewall. Ce problème a été corrigé.

Référence support 56009

Lorsqu'un client SMTP dépassait la quantité de données autorisées en émission, le proxy envoyait une réponse du type "552 Data size exceeded" puis générait à tort une alarme "Protocole SMTP invalide" provoquant l'interruption de la connexion. Cette anomalie a été corrigée.

Référence support 56619

Le firewall pouvait tenter de réutiliser un certificat venant d'être supprimé. Cette anomalie pouvant provoquer un blocage du proxy a été corrigée.

IPSec (IKEv2)

Référence support 59900

Lors de l'établissement d'un tunnel IPSec IKEv2, les groupes auxquels étaient rattaché un utilisateur n'étaient pas communiqués au moteur de prévention d'intrusion. Cette anomalie a été corrigée.

Référence support 59730

Lors de la négociation d'un tunnel IPSec IKEv2 à l'initiative du firewall, celui-ci envoyait des sélecteurs IP additionnels qui pouvaient ne pas être acceptés par les équipements d'autres constructeurs (CheckPoint), empêchant ainsi l'établissement du tunnel. Ce problème a été corrigé.

VPN SSL

Référence support 48993

Lors d'un rechargement du serveur VPN SSL, la configuration destinée au client pouvait ne pas être complète et empêchait les connexions au service. Ce problème a été corrigé.

Référence support 59518

Le serveur VPN SSL n'acceptait pas les certificats présentant des espaces ou des caractères spéciaux (exemple : apostrophe), et échouait à créer l'archive de configuration destinée à être téléchargée par le client. Ce problème a été corrigé.

Référence support 49110

Les performances du VPN SSL ont été améliorées grâce au support du protocole UDP pour l'établissement des tunnels.

PPTP

Référence support 59237

La tentative d'établissement d'un tunnel PPTP à destination d'un firewall utilisant du routage par interface pouvait entrainer le blocage du moteur de gestion des tunnels PPTP. Ce problème a été corrigé.

Objets réseau - Objets globaux

Référence support 59511

L'export au format CSV des objets globaux ne fonctionnait pas. Ce problème a été corrigé.

Traces - Stockage local

Référence support 59751

Une optimisation dans les paramètres d'accès à la carte SD sur les firewalls modèle U30S, SN200 et SN300 a corrigé des problèmes de redémarrages intempestifs du firewall.

Réseau

LACP

Référence support 59545

La modification de l'adresse MAC d'un agrégat n'était pas répercutée sur la première interface physique appartenant à cet agrégat.

IPv6

Référence support 58635

Les requêtes ICMP, ou de découverte du voisinage réseau, à destination d'une interface paramétrée en IPv6 avec un masque de sous-réseau égal à /64 provoquaient une alarme

bloquante "usurpation d'adresse IP de type 1" (adresse source issue d'une interface non protégée à destination d'une interface protégée). Ce problème a été corrigé.

Objets réseau

Référence support 54843 - 56211

Lors de la manipulation de la base objets, l'ensemble des entrées de la table ARP du firewall était systématiquement effacée. Les solutions de supervision réseau pouvaient alors considérer à tort des machines injoignables pendant la reconstruction de cette table. Ce comportement a été modifié et seules les entrées permanentes de cette table sont supprimées lors de la manipulation de la base objets.

Prévention d'intrusion

Protocole SMB2

Référence support 58662

Une erreur dans la lecture de paquets SMB2 lors d'une tentative d'authentification via la méthode SPNEGO pouvait provoquer à tort l'alarme bloquante "Protocole NBSS/SMB2 invalide". Ce problème a été corrigé.

Protocole Ethernet/IP

Référence support 59987

Le module de prévention d'intrusion dédié à l'analyse du protocole industriel Ethernet/IP pouvait se déclencher à tort sur certains flux UDP, provoquant le blocage de ceux-ci. Cette anomalie a été corrigée.

Management de vulnérabilités

Référence support 55973 58875

Des problèmes de blocage du moteur de prévention d'intrusion ont été résolus par une optimisation du mécanisme de management de vulnérabilités pour les flux provenant ou à destination du firewall.

File d'attente du moteur de prévention d'intrusion

Référence support 59366

Lorsque le nombre de connexions dépassait la file d'attente des événements gérées par le moteur de prévention d'intrusion, le message "HA: Overflow detected while reading ASQ events, resync needed" était généré dans le journaux d'événements, bien que la haute disponibilité ne soit pas activée sur le firewall. Ce message a été modifié en "Overflow detected while reading IPS events, resync needed".

Protocole ICMP

Référence support 59712

Un paramètre fixant le taux global maximum de paquets d'erreurs ICMP autorisés par coeur a été ajouté aux firewalls. Ce paramètre, fixé par défaut à 25000 paquets/s, est modifiable dans la configuration globale du protocole ICMP.

Interface Web d'administration

Filtrage et NAT

Lors de l'édition d'un commentaire, l'utilisation des raccourcis clavier CTRL+C et CTRL+V provoquait un copier / coller d'une nouvelle règle de filtrage plutôt que du commentaire concerné. Cette anomalie a été corrigée.

Référence support 54930

Suite au renommage du protocole *dcerpc* en *dcerpc_tcp*, la sélection de *dcerpc* dans le champ protocole d'une règle de filtrage provoquait une erreur. Ce problème a été corrigé.

Référence support 47826

Le déplacement d'un séparateur de règles replié n'entraînait pas le déplacement des règles de filtrage qui lui étaient rattachées. Cette anomalie a été corrigée.

Traces -Syslog - IPFIX

Référence support 60007

Lorsque le formatage d'une carte SD échouait, l'erreur n'était pas affichée et la fenêtre de formatage restait indéfiniment affichée. Ce problème a été corrigé.

Administrateurs

Référence support 61167

Après validation du changement du mot de passe du compte admin, la page pouvait rester bloquée sur le message "Sauvegarde de la configuration en cours, veuillez patienter...". Cette anomalie a été corrigée.

Configuration des annuaires

Référence support 60079

Lorsque le nom de plusieurs annuaires était dérivé du nom de l'annuaire par défaut (exemple : mycompany.eu [défaut] , mycompany.eu.fr, mycompany.eu.org …), tous ces annuaires étaient représentés comme annuaires par défaut dans le module **Utilisateurs** > **Configuration des annuaires**.

Supervision

Configuration de la supervision

Référence support 59538 - 59590

Les interfaces agrégées ne pouvaient pas être sélectionnées dans la liste des interfaces à superviser. Cette anomalie a été corrigée.

Supervision de la QoS

Référence support 59322

La courbe historique de supervision de la QoS n'affichait pas de données car les identifiants des files d'attente de QoS n'étaient pas pris en compte. Cette anomalie a été corrigée.

Matériel

Horloge du firewall

Référence support 58901

Lorsque la pile gérant l'horloge du firewall tombait en panne, celui-ci adoptait une date aléatoire à chaque démarrage. Si cette date était située avant la date de validité de la licence de l'équipement, le firewall redémarrait sans interruption. Cette anomalie a été corrigée.

Voyants lumineux - SN150

Référence support 58532

Le voyant lumineux *Online* situé en façade du firewall SN150 ne s'allumait pas au démarrage du boîtier. Cette anomalie a été corrigée.

Correctifs de la version 3.1.2

Prévention d'intrusion

Signatures de protection contextuelle personnalisées

Sur les firewalls modèles SN160(W) et SN210(W), la commande de validation du fichier de définition des signatures personnalisées (`enpattern -t`) n'aboutissait pas et générait une consommation CPU excessive. Ce problème a été corrigé.

Nouvelles fonctionnalités de la version 3.1.1

Nouveaux modèles - Réseaux sans fil

La version de firmware 3.1.1 assure la compatibilité avec les nouveaux modèles de firewalls Wi-Fi SN160W et SN210W.

Il est donc nécessaire de mettre à jour ces firewalls après leur réception.

Ces firewalls offrent l'ensemble des fonctionnalités nécessaire à la sécurisation des connexions WI-FI.

La gestion de réseaux sans fil intégrée dans cette version est compatible avec les normes 802.11 a/b/g/n. Deux interfaces wlan, et donc réseaux distincts, peuvent être configurés sur chaque firewall.

Correctifs de la version 3.1.1

Système

Référence support 59936

Sauvegardes automatiques

Lors de l'activation de la fonction de sauvegardes automatiques, le résultat du déroulement de la première sauvegarde n'était pas enregistré. Celle-ci pouvait donc être relancée à tort de manière régulière. Cette anomalie a été corrigée.

Référence support 59296

Authentification

Un utilisateur connecté via la méthode SSO Agent ne pouvait pas accepter une demande de parrainage, bien que ce droit lui ait été attribué. Ce problème a été corrigé.

Proxies

Dans une configuration sans analyse Web 2.0 (case **Inspecter le code HTML** décochée dans l'onglet **IPS** du protocole HTTP), une requête HTTP de type POST, contenant des données, et redirigée vers une règle d'authentification, pouvait provoquer un blocage du firewall.

Interface Web d'administration

Référence support 59717 60282

Microsoft Internet Explorer 11 - Mozilla Firefox 51.0.1 ou supérieur

Un problème de lenteur d'affichage de certaines pages de l'interface d'administration (Exemple : **Objets réseau**) a été résolu.

Nouvelles fonctionnalités de la version 3.1.0

Système

Objets réseau

De nouveaux objets correspondant aux services et groupes de services utilisés par la solution Stormshield Endpoint Security ont été intégrés dans la base objets des Firewalls SNS.

VPN IPSec (IKEv2)

Les groupes Diffie-Hellman DH19 NIST Elliptic Curve Group (256-bits) et DH20 NIST Elliptic Curve Group (384-bits) ont été ajoutés aux profils de chiffrement disponibles pour les tunnels IPSec IKEv2.

VPN IPSec

Un bouton permettant de renommer les correspondants IPSec a été ajouté dans l'onglet **Correspondants** du module **VPN IPSec**.

Référence support 56589

Notifications

Les noms des objets associés aux adresses IP source et destination ont été ajoutés dans les rapports de notifications envoyés par e-mail.

Certificats et PKI

La période de vérification des CRL (Certificates Revocation List) était fixée à 24h. Elle peut désormais être paramétrée entre 3600 secondes (1 heure) et 604800 secondes (1 semaine). La valeur par défaut est de 21600 secondes (6 heures).

Ce paramétrage est réalisable uniquement via la commande CLI : `PKI CONFIG UPDATE checkcrlperiod= xxxxx`.

Page de blocage HTTP

Le code de retour associé à la page de blocage HTTP (valeur par défaut : *202 - Accepté*) peut être modifié à l'aide de la ligne de commande : `config protocol http profile proxy urlfilteringindex=X HTTPCodeOnFail=Y`.

Haute disponibilité

Lors d'un changement de qualité du firewall passif (exemple : perte d'un lien, déconnexion d'un module d'alimentation…), une alerte SNMP (TRAP) est émise par le cluster afin d'avertir l'administrateur. Le firewall ajoute également un message du type « La qualité de l'un des nœuds du cluster a été modifiée : SN910XXXXXXXXX 12 -> 11 » dans le journal des événements système (fichier *l_system*).

Sur une configuration en Haute Disponibilité, dont le facteur de qualité est inférieur à 100%, un message d'avertissement indiquant le risque de changement de rôle des membres du cluster est affiché dans différents cas, notamment :

- lors de la création, ajout ou suppression d'une interface dans un agrégat,
- en cas de désactivation d'une interface connectée,
- en cas d'activation d'une interface déconnectée.

VPN SSL

Les options **Utiliser les serveurs DNS fournis par le firewall** (*register-dns*) et **Interdire l'utilisation de serveurs DNS tiers** (*block-outside-dns*) indiquant respectivement au client VPN SSL d'écrire dans sa configuration le(s) serveur(s) DNS précisé(s) par le firewall Stormshield Network et de ne pas utiliser de serveur DNS tiers sont paramétrables depuis le module **Configuration** > **VPN SSL**. Cette fonctionnalité réduit le délai nécessaire pour la réception des réponses aux requêtes DNS du client, notamment pour les machines fonctionnant sous Microsoft Windows 10.

VPN SSL Portail

La connexion au VPN SSL Portail utilise l'application Java Webstart en remplacement de l'application Java standard.

Objets globaux

Les firewalls SNS supportent désormais les objets temps et objets routeurs globaux. Ceux-ci peuvent donc être gérés et déployés à l'aide de la solution Stormshield Management Center.

Vérification des CRL et support du BindAddr dans les requêtes LDAP du firewall

Dans la configuration LDAP du firewall, le paramètre BindAddr suivi de l'adresse IP privée du firewall impose à celui-ci de présenter cette adresse IP lors des requêtes LDAP à destination d'un

annuaire externe : les flux LDAP peuvent ainsi être encapsulés dans un tunnel IPSec afin de chiffrer les requêtes vers l'annuaire.

Ce paramètre n'est modifiable qu'en ligne de commande : `setconf ConfigFiles/ldap LDAP_Name BindAddr FW_Private_IP`.

Supervision - Rapports - Journaux d'audit

Supervision

Chaque ligne présentant une vulnérabilité détectée sur une machine inclut désormais un lien vers la page détaillant cette vulnérabilité.

De nouveaux menu contextuels sont accessibles en effectuant un clic droit sur une ligne de données :

- **Supervision des machines** : rechercher la machine dans les traces, afficher les détails de la machine, réinitialiser le score de réputation, ajouter la machine à la base Objets et/ou l'ajouter dans un groupe...
- **Supervision des utilisateurs** : rechercher la valeur dans les traces, afficher les détails de la machine sur laquelle est connectée un utilisateur, désauthentifier l'utilisateur...
- **Supervision des connexions** : afficher la ligne complète, ajouter l'objet source ou destination à la base Objets, afficher les détails de la machine, effectuer un ping vers la source ou la destination...

Prévention d'intrusion

Protocole IEC 60870-5-104

Le moteur de prévention d'intrusion analyse le protocole industriel IEC 60870-5-104 (IEC 104).

Protocole HTTP

Un contexte de signature *vbscript* a été ajouté à l'inspection de sécurité du protocole HTTP.

Référence support 54140

Le moteur de prévention d'intrusion détecte les tentatives d'altération de cache (*cache poisoning*) pour les proxies Web de type *Squid* et déclenche l'alarme bloquante Possible HTTP proxy poisoning.

Proxy SSL

Les algorithmes de chiffrement RC4 et MD5, considérés comme faibles, ont été supprimés de la liste des algorithmes disponibles pour le proxy SSL.

Protocole Modbus

Une alarme est générée lorsque le nombre maximum de serveurs Modbus bénéficiant d'une réservation UMAS est atteint.

Protocoles IP (sauf TCP, UDP et ICMP)

Les connexions correspondant aux protocoles IP autres que TCP, UDP, ICMP (exemple : GRE) sont référencées dans le journal des statistiques de connexions (champs IPStateMem , -IPStateConn, -IPStatePacket, -IPStateByte du fichier */filterstat*).

Firewalls industriels SNi40

Bypass matériel

Lors du déclenchement du bypass matériel, les connexions en cours sur les interfaces incluses dans le bypass n'étaient pas modifiées et finissaient par être clôturées faute de réception d'un trafic réseau correspondant. Ce comportement a été modifié, et ces connexions sont désormais maintenues actives jusqu'au retour à une configuration réseau standard (réarmement du bypass).

Matériel

Haute disponibilité

Dans le cadre d'une remise en configuration d'usine du firewall (*defaultconfig*), le délai de déclenchement de la fonction de surveillance matérielle (*hardware watchdog*) est ramené à 120 secondes contre 300 auparavant.

Correctifs de la version 3.1.0

Système

Authentification

Référence support 52192

Une tentative de connexion à l'interface Web d'administration via le navigateur Google Chrome et la méthode SSL (certificat) ou la méthode SPNEGO n'aboutissait pas et provoquait une alarme d'attaque par force brute. Ce problème a été corrigé.

Référence support 56711

Lors de la configuration de la méthode "Parrainage", le champ Expiration du 'cookie' HTTP n'était pas automatiquement positionné à *Ne pas utiliser*, ce qui entraînait un dysfonctionnement de cette méthode d'authentification. Cette anomalie a été corrigée.

Référence support 56595

La tentative de création d'un nouvel objet au sein de l'assistant de politique d'authentification échouait et affichait un "?" en lieu et place du nom de l'objet. Ce problème a été corrigé.

Référence support 59731

Une anomalie dans l'encodage de l'e-mail de parrainage rendait le lien de validation inclus dans cet e-mail invalide. Cette anomalie a été corrigée.

Objets

Référence support 58476 - 58944

Les objets routeurs et objets temps n'étaient pas pris en charge lors d'une restauration partielle de configuration. Cette anomalie a été corrigée.

Référence support 56113

Les objets globaux intégrés dans un objet routeur n'étaient pas pris en compte. Cette anomalie a été corrigée.

Référence support 53218

Lorsqu'une dialup (modem PPoE, PPTP, PPP ou L2TP) active et fonctionnelle était intégrée dans un objet routeur, celui-ci ne récupérait pas son état et la considérait donc comme injoignable. Ce problème a été corrigé.

Référence support 59083

Certificats et PKI

Dans le cadre d'un renouvellement de certificat via le protocole Simple Certificate Enrollment Protocol (SCEP), à l'aide de la commande en ligne `SCEP RENEW`, et lorsque le Distinguished Name (DN) de ce certificat contenait plus d'un attribut du même type (OU, CN, O,...), seule la première occurrence de cet attribut était conservée après l'opération. Cette anomalie a été corrigée.

Référence support 51618

VPN SSL Portail

Les connexions vers des serveurs applicatifs au travers de l'application VPN SSL Portail ne fonctionnaient plus en version 3. Ce problème a été corrigé.

VPN SSL

Référence support 58856

Le nombre maximal de tunnels VPN SSL autorisé physiquement sur les firewalls Netasq modèle U série S était inférieur au nombre de tunnels prévus. Cette anomalie a été corrigée.

Référence support 52972 - 53289

Un problème pouvant empêcher l'établissement de nouveaux tunnels VPN SSL (connexion bloquée à l'étape "GET CONF") a été corrigé.

Proxies

Référence support 52034

Lorsqu'une règle de filtrage faisait appel au proxy explicite, le changement du port d'écoute de ce proxy (TCP/8080 par défaut) n'était pas pris en compte par les règles d'authentification contenues dans la politique de filtrage. Cette anomalie a été corrigée.

Référence support 55700

Une anomalie dans la gestion des tailles maximales du nom d'utilisateur et de domaine composant une adresse e-mail a été corrigée.

Référence support 54003

Le proxy HTTP pouvait considérer à tort des téléchargements comme partiels. Cette anomalie a été corrigée.

Référence support 56464

Une anomalie dans la lecture des informations situées derrière le nom de domaine précisé dans la commande *EHLO* bloquait à tort le flux SMTP correspondant.

Référence support 52848

Après analyse Sandboxing d'un e-mail, le nom de la pièce attachée référencée dans les journaux de traces était erroné. Ce problème a été corrigé.

Référence support 49996

Une anomalie dans la gestion des réponses du protocole Internet Content Adaptation Protocol (*ICAP*) en mode *Request Modification* (*reqmod*) pouvait entraîner une surconsommation de ressources mémoire ou un blocage du proxy HTTP.

Référence support 57326

Lorsqu'un e-mail contenait une commande de fin de ligne erronée dans ses données, la connexion était réinitialisée uniquement entre le client et le firewall, le serveur restant en attente jusqu'à l'expiration de la connexion. Cette anomalie a été corrigée.

Référence support 58824

Lorsqu'un client envoyait une commande RESET à destination du serveur de messagerie, la connexion était réinitialisée uniquement entre le client et le firewall, le serveur restant en attente jusqu'à l'expiration de la connexion. Cette anomalie a été corrigée.

Référence support 56475

Lorsqu'un e-mail contenait une adresse émettrice ou destinataire excédant la taille définie par la RFC (partie locale ou nom de domaine), le proxy ne clôturait pas la connexion après l'envoi du message d'erreur ("553 Localpart too long" ou "553 Domain name too long"). Ce problème a été corrigé.

Référence support 59420

Le proxy pouvait refuser de se lancer sur un firewall utilisant une règle de filtrage avec au moins une case de destination des traces décochée (onglet **Configuration Avancée** du module **Action** dans la boîte d'édition d'une règle de filtrage). Ce problème a été corrigé.

Référence support 58567

Remise en configuration d'usine

L'aide du script de remise en configuration d'usine (*defaultconfig*) présentait une explication erronée pour l'option « –D » (*Only Restore the data partition on G2 hardware*). Cette anomalie a été corrigée (*Only Restore the data partition*).

Référence support 56394

Proxies – Firewalls modèle SN 910

Les limites en nombre de connexions autorisées pour les proxies (HTTP, SSL, SMTP, POP3 et FTP) des Firewalls modèle SN910 étaient incorrectes. Elles ont été augmentées pour correspondre aux véritables performances autorisées par ce modèle.

Référence support 57286

IPSec

Dans une configuration présentant un tunnel IPSec site à site et une politique IPSec Anonyme (utilisateurs nomades), la désactivation du tunnel site à site (état du tunnel à *off*) ne supprimait pas le correspondant du fichier de configuration IPSec. Cette anomalie, qui provoquait le dysfonctionnement des connexions nomades, a été corrigée.

IPSec (IKEv2)

Référence support 54831

Lors de la renégociation d'une phase 1 de tunnel IPSec en IKEv2, le moteur IPSec détruisait la SA existante (Security Association – Association de Sécurité) ainsi que les SA filles avant de négocier la nouvelle SA.

Ce comportement, qui pouvait provoquer des pertes de paquets importantes, a été modifié afin de procéder en premier lieu à la négociation de la nouvelle SA avant de détruire les anciennes.

Référence support 59152

Un problème pouvant empêcher l'établissement de tunnels IPSec IKEv2 à destination des firewalls modèle SN150 a été corrigé.

Référence support 59280

Le nombre de SA IKE pour un même tunnel IPSec IKEv2 pouvait augmenter au fil du temps sans que les SA inutilisées ne disparaissent. Cette anomalie a été corrigée.

Haute Disponibilité

Référence support 56268

L'ajout ou la suppression d'une interface dans un agrégat (LACP) n'était pas répercutée sur l'indicateur de qualité du mécanisme de Haute Disponibilité. Cette anomalie a été corrigée.

Référence support 57056

Une optimisation dans les paramètres de détection de perte du firewall actif sur problème électrique (paramètre *ConsensusTimeout*) a permis de réduire de manière importante le délai de bascule du cluster.

Référence support 56613

Après plusieurs redémarrages accidentels du moteur de gestion de la Haute Disponibilité, les jetons associés n'étaient pas supprimés. La table des jetons pouvait ainsi être saturée et empêchait alors le démarrage d'autres services du firewall. Ce problème a été corrigé.

Référence support 56478

Une instabilité du moteur de synchronisation des données provoquait un redémarrage en boucle du service de gestion de la Haute Disponibilité. Ce dysfonctionnement pouvait entraîner un passage du firewall passif en mode actif, les deux firewalls du cluster devenant alors actifs. Ce problème a été corrigé.

Référence support 50048

Un changement de rôle suite au redémarrage du membre actif du cluster pouvait entraîner une désynchronisation concernant les tunnels IPSec négociés par les deux membres du cluster.

Référence support 54289 - 58842

Lors d'un changement de rôle des firewalls au sein d'un cluster, la restauration des connexions actives ne tenait pas compte de la filiation de ces connexions (flux de connexion / flux de données). Les flux de données pour des protocoles de type FTP n'étaient ainsi pas transférés. Ce problème a été corrigé.

Référence support 55076

Protection applicative

Dans une configuration utilisant le moteur antiviral Karspersky, l'analyse d'un fichier de type bombe de décompression (*zip bomb*) pouvait provoquer une saturation de la partition temporaire, induire une charge CPU importante et aboutir à une erreur d'analyse. Ce problème a été corrigé.

Filtrage et NAT

Référence support 56570

Lorsque le nom saisi pour une règle de filtrage excédait la taille maximale autorisée, celle-ci n'était pas précisée dans le message d'erreur. Cette anomalie a été corrigée et il est désormais indiqué que ce nom ne doit pas excéder 255 caractères.

Référence support 56672

Lors du survol d'un groupe de services utilisé dans une règle de filtrage, l'infobulle détaillant l'ensemble des services inclus dans le groupe n'était pas affichée. Cette anomalie a été corrigée.

Référence support 58535

Lors du survol d'un service utilisé dans une règle de filtrage, les informations présentes dans l'infobulle étaient incomplètes. Cette anomalie a été corrigée.

Référence support 59297

Lors du survol d'un objet réseau de type *Plage d'adresses IP* utilisé dans une règle de filtrage, l'infobulle affichait par erreur le message "Objet non trouvé". Cette anomalie a été corrigée.

Référence support 55190

Routage par politique (PBR)

Dans une configuration telle que :

- Une route statique est appliquée à un réseau,
- Une règle de filtrage met en oeuvre du routage par politique (PBR) à ce même réseau pour un port particulier,
- De la translation d'adresses est réalisée en sortie de firewall,

le rechargement des règles de filtrage empêchait les connexions correspondant à la règle de PBR de s'établir.

Référence support 50977

DNS dynamique

Les modifications d'adresse IP du firewall n'étaient plus répercutée chez le fournisseur de DNS Dynamique lorsque le protocole SSL était utilisé. En effet, la vérification du certificat de ce fournisseur échouait. Ce problème a été corrigé.

Référence support 55728

Configuration

La modification du nom du firewall (module **Système** > **Configuration**) n'était répercutée ni dans le nom d'émetteur des alertes par e-mail, ni dans le tableau de bord de SN Real-Time Monitor. Cette anomalie a été corrigée.

Référence support 56734

Événements système

Le rapport généré lors d'un blocage d'attaque par force brute ne contenait pas l'adresse IP source bannie. Cette anomalie a été corrigée.

Réseau

Référence support 57328

VLAN

Le dernier fragment d'un paquet UDP destiné à emprunter un VLAN n'était pas correctement transmis par le firewall à l'interface parente du VLAN. Ce problème a été corrigé.

Interfaces virtuelles

Référence support 53881

Lorsqu'une interface virtuelle GRE créée initialement comme inactive se voyait attribuer une adresse IP, son changement d'état n'était pas immédiatement répercuté dans l'interface Web

d'administration. Il était ainsi nécessaire de changer de module puis de revenir dans le module interfaces virtuelles pour visualiser ce changement. Cette anomalie a été corrigée.

Référence support 58685

Les statistiques de débit sortant des interfaces virtuelles IPSec affichaient toujours une valeur nulle. Cette anomalie a été corrigée.

Prévention d'intrusion

Référence support 57396

Lorsque des flux utilisant systématiquement le même port source traversaient une règle en mode Firewall ou IDS, la réinitialisation de la première connexion empêchait l'établissement des connexions immédiatement suivantes. En effet, celles-ci étaient alors considérées comme également réinitialisées. Ce problème a été corrigé en autorisant la réutilisation immédiate d'un même port source dans les modes Firewall et IDS (*TCP Closed FastReuse*).

Référence support 53011 - 58465

Application TeamViewer

Suite à une évolution de l'application TeamViewer, l'analyse IPS des flux relatifs à cette application déclenchait à tort l'alarme bloquante « Paquet SSL invalide ». Ce problème a été corrigé.

Référence support 53094

Protocole RTSP (Real-Time Streaming Protocol)

Le moteur de prévention d'intrusion bloquait à tort l'en-tête *Scale* de la méthode *Play*. Cette anomalie a été corrigée.

Référence support 51867

Protocole HTTP

Dans une configuration utilisant le routage par politique (PBR) pour les flux HTTP, l'activation de l'option **Appliquer la règle de NAT sur le trafic analysé** (**Configuration globale** du protocole HTTP dans le module **Protection applicative** > **Protocoles**) provoquait un routage incorrect des paquets issus du proxy

Référence support 53640

Le mécanisme de filtrage *YouTube for Education* n'étant plus actif, il a été remplacé par le mécanisme *Restrictions Youtube*. Celui-ci peut être activé et paramétré (limitation stricte ou modérée) dans l'onglet **IPS** du protocole HTTP (module **Protection applicative** > **Protocoles**).

Référence support 58409

Protocole SIP

Le nombre maximum de connexions filles autorisées pour le protocole SIP a été augmenté afin de permettre :

- 127 appels simultanés sur les modèles U30S, U70S, SN150, SN160W, SN200, SN210W et SN300,
- 127 appels simultanés sur les modèles U30S, U70S, SN150, SN160(W), SN200, SN210(W), SN300 et SN310,
- 1023 appels simultanés pour les autres modèles,

contre 16 auparavant pour l'ensemble des modèles.

Référence support 53886

Protocole ICMP

Lors de la réception ou de la transmission de plusieurs requêtes ICMP présentant un même identifiant, une même séquence et des données différentes, le firewall ne prenait pas en compte les paquets de réponse de la première requête et bloquait les suivantes (alarme "Modification des données ICMP ECHO"). Cette anomalie a été corrigée.

Interface Web d'administration

Référence support 54459

Protocole SSL

Lorsqu'une case était cochée dans la section **Négociation SSL** d'un profil déterminé, et que cette modification était appliquée, la même case se retrouvait cochée à tort dans l'ensemble des profils. Ce problème a été corrigé.

Supervision - rapports - Journaux d'audit

Référence support 56766

Rapports

Sur les modèles de firewalls ne possédant pas de partition de traces (modèles sans disque dur), une anomalie dans la gestion de la case à cocher d'activation des rapports (onglet **Stockage local** du module **Notifications** > **Traces - Syslog - IPFIX**) a été corrigée.

Référence support 57247

Supervision

Lorsque les rapports étaient désactivés et que les graphiques historiques étaient désactivés (module **Notifications** > **Configuration des rapports**), les graphiques historiques couvrant les 30 derniers jours ne pouvaient pas être affichés. Ce problème a été résolu.

Référence support 53352

Journaux

Les commandes de supervision de services inactifs du firewall (*MONITOR POWER*, *MONITOR FWADMIN*,...) étaient tracées à tort dans le fichier de journaux *l_server*. Cette anomalie a été corrigée.

Référence support 54926

Routage multicast

Un compte utilisateur ayant tous les droits d'administration ne pouvait pas appliquer une modification de configuration réalisée dans le module **Réseau** > **Routage multicast** (message d'erreur "Il n'y a rien à sauvegarder"). Cette anomalie été corrigée.

Stormshield Network Real-Time Monitor

Référence support 58502 - 57414

Utilisateurs

La commande de suppression des utilisateurs, disponible via le menu contextuel (clic droit) du module **Utilisateurs**, ne fonctionnait plus. Ce problème a été corrigé.

Nouvelles fonctionnalités de la version 3.0.3

Système

Protocole SNMP

Une nouvelle OID (Object Identifier) ntqifDrvName correspondant au nom système des interfaces réseau a été ajoutée dans la MIB (Management Information Base) NETASQ-IF-MIB.

Configuration des annuaires

Le champ définissant le nom d'un annuaire LDAP a été renommé en « Nom de domaine ».

Correctifs de la version 3.0.3

Système

Authentification

Référence support 58610

La migration d'une configuration utilisant la méthode d'authentification « Invités » avec le champ personnalisé « e-mail » provoquait une erreur de configuration du portail captif car ce champ était mal converti. Cette anomalie a été corrigée.

Référence support 58816

La mise à jour vers une version 3 de firmware d'une configuration avec un nom de firewall personnalisé (module **Configuration**) et la case **Utiliser le nom du firewall ou le CN du certificat comme FQDN** cochée (onglet **Portail captif** – **Configuration avancée** du module **Users** > **Authentification** en version 2) rendait la méthode d'authentification SPNEGO inopérante.

Configuration des annuaires

Référence support 58512

Lors de la migration en version 3 d'une configuration référençant un annuaire LDAP externe, cet annuaire pouvait prendre le nom d'objet du serveur LDAP en lieu et place du nom de domaine. Cette anomalie, qui rendait la méthode d'authentification SSO Agent inopérante, a été corrigée et le nom de l'annuaire est désormais construit à partir du domaine racine (base DN) déclaré lors de sa création.

Référence support 58883

La migration en version 3 d'une configuration référençant un annuaire LDAP externe dont le domaine racine (DN) contenait une ou plusieurs lettres majuscules rendait cet annuaire invalide. Ce problème a été corrigé.

Référence support 58825

Filtrage et NAT

L'affichage n'était pas rafraîchi en basculant d'une politique de filtrage locale à une politique de filtrage globale portant le même index.

Référence support 58475

Portail VPN SSL

Les dernières versions de l'application clientes java pouvaient empêcher la connexion aux serveurs joignables via le portail SSL VPN, car elles refusaient les autorités de certification signées avec l'algorithme MD5. Ce problème a été corrigé.

Référence support 58746

Droits d'accès

La sélection d'un utilisateur dans l'onglet **Accès détaillé** du module **Droits d'accès** aboutissait au remplacement de son identifiant par ses prénom et nom. Ce problème, qui provoquait un dysfonctionnement de l'authentification, a été corrigé.

Prévention d'intrusion

Référence support 58572 58589 58742 58553

Protocole HTTP

Une anomalie dans l'inspection de sécurité du protocole http pouvait entraîner une consommation CPU excessive du proxy et un blocage du firewall. Cette anomalie a été corrigée.

Interface Web d'administration

Configuration des annuaires

Référence support 58871

Un serveur de secours ajouté dans la configuration avancée d'un annuaire externe (Microsoft Active Directory, LDAP externe, LDAP de type PosixAccount) n'apparaissait plus après navigation au sein d'autres modules de l'interface Web d'administration. Cette anomalie a été corrigée.

Référence support 58734 58704 58900

La modification du Filtre de sélection des groupes d'utilisateurs d'un annuaire externe (onglet **Structure** de l'annuaire) n'était pas prise en compte par l'interface Web d'administration. cette anomalie a été corrigée.

Supervision - Rapports - Journaux d'audit

Référence support 58921

Supervision des utilisateurs

Lorsque plusieurs utilisateurs étaient authentifiés et connectés, le rafraîchissement du module de supervision des utilisateurs par le bouton Actualiser pouvait entraîner un blocage du firewall. Ce problème a été corrigé.

Rapports

Sur les modèles de firewalls ne possédant pas de partition de traces (modèles sans disque dur), l'activation des 5 rapports autorisés ne déclenchait pas l'affichage des données correspondantes.

Correctifs de la version 3.0.2

Prévention d'intrusion

Référence support 57337

Protocole SSL

Un problème d'accès aux sites utilisant des suites de chiffrement des familles CHACHA20 et Poly1305 a été corrigé par la mise à jour de ces suites.

Système

Référence support 57350 57356

VPN SSL - VPN IPsec

Après migration vers SNS v3, les connexions via SSL VPN Client ou VPN IPSec client pouvaient ne plus fonctionner car les interface *sslvpn* et *ipsec* se trouvaient liées au profil *Invité*. Ce problème a été corrigé et ces interfaces ne sont désormais plus associées à un profil après migration.

Référence support 58536

Authentification

La migration vers SNS v3 pouvait entraîner l'association du profil de portail captif *Internal* avec une interface inconnue (interface « 0 »).
Cette anomalie, qui empêchait alors toute modification de ces associations (onglet *Portail captif* du module **Configuration > Utilisateurs > Authentification**), a été corrigée.

Référence support 58433

Proxies

L'activation du cache DNS avant celle d'un proxy pouvait entraîner un blocage de ce proxy lors du redémarrage du firewall.

Référence support 56184

Filtrage

Il était impossible d'ajouter des URL accessibles sans authentification dans une règle de filtrage précisant une redirection vers le portail d'authentification. Ce problème a été corrigé.

Haute disponibilité

Référence support 58530

Dans une configuration en Haute Disponibilité, le mécanisme de synchronisation pouvait tenter d'activer à tort le système de *bypass* matériel réservé aux firewalls industriels (modèle SNi40). Cette anomalie, qui générait une erreur de synchronisation, a été corrigée.

Référence support 58367

La mise à jour en version 3 d'un cluster de firewalls pouvait échouer lors de la synchronisation du fichier de licence avec l'équipement passif. Ce problème a été corrigé.

Référence support 58113

Extended Web Control

Si le mode synchrone de la solution de filtrage d'URL Extended Web Control avait été activé sur un firewall en version SNS v2, ce mode est automatiquement désactivé au profit du mode asynchrone lors d'une migration en v3.0.2 de firmware.

Référence support 58496

Sauvegardes automatiques

L'activation des sauvegardes automatiques dans une configuration utilisant plusieurs annuaires LDAP pouvait échouer et rendre le module LDAP inactif. Ce problème a été corrigé.

Tableau de bord

Référence support 56635

Configuration LDAP

Le tableau de bord d'un firewall ne possédant aucun annuaire LDAP configuré affichait un message erroné ("Configuration LDAP : Non activé. La configuration de l'annuaire est faite mais le module n'est pas activé"). Cette anomalie a été corrigée et le message "Aucun annuaire par défaut n'a été configuré ou activé" est désormais affiché.

Nouvelles fonctionnalités de la version 3.0.1

Firewalls modèle SN150

La version de firmware 3.0.1 assure la compatibilité avec les firewalls SN150.

Correctifs de la version 3.0.1

Prévention d'intrusion

Référence support 56973 57355

Modes IDS / Firewall

Dans une configuration mettant en oeuvre des règles de filtrage en mode IDS ou Firewall et de l'authentification, le déclenchement d'une alarme non bloquante (action *Passer*) par des flux ICMP invalides entraînait un blocage du firewall. Ce problème a été corrigé.

Référence support 56740

Ressources mémoire

Dans le cas d'un nombre très élevé de connexions, une anomalie dans la gestion des ressources mémoires pouvait entraîner un blocage puis un redémarrage du firewall. Cette anomalie a été corrigée.

Système

Référence support 56964

Tunnels IPSec (IKEv2)

Lorsqu'une CA utilisée pour signer des certificats serveurs avait son champ E-mail renseigné, le firewall refusait d'établir les tunnels IPSec IKEv2 dont l'authentification était basée sur ces certificats. Cette anomalie a été corrigée.

Référence support 57359

Filtrage

La politique de filtrage globale du firewall n'était pas activée après le déploiement de règles globales via Stormshield Management Center. Cette anomalie a été corrigée.

Rapports

Rapport "Réputation des machines"

Une erreur dans la prise en compte de la réputation des machines destination pour les connexions SSL a été corrigée.

Nouvelles fonctionnalités de la version 3.0.0

Interface Web unifiée

L'interface Web unifiée couvre dorénavant l'administration, la supervision et le reporting des firewalls Stormshield Network.

Un nouvel écran de supervision propose des graphiques (temps-réel et sous forme d'historique) sur les ressources systèmes utilisées (mémoire et CPU), les débits par interfaces, les utilisateurs connectés ainsi que des informations détaillées sur les machines (connexions en cours, applications utilisées, vulnérabilités détectées, etc.).

De nombreuses interactions facilitent la recherche d'incidents et l'administration des firewalls Stormshield Network.

Gestion des utilisateurs temporaires

Pour faciliter l'accès à Internet aux personnes externes à l'entreprise ou sur des lieux publics, les produits Stormshield Network offrent des fonctionnalités avancées de gestion des utilisateurs temporaires.

En plus du mode invité déjà disponible, la version 3 intègre un nouveau portail de création de « comptes temporaires » et un mode « parrainage ».

Le portail « invité » actuel peut être enrichi de nouveaux champs (prénom, nom, adresse mail, etc.) que l'utilisateur devra renseigner avant d'accepter la charte d'accès à Internet.

La création des comptes temporaires peut facilement être réalisée grâce à un écran simplifié, accessible uniquement par les personnes habilitées à la création de ces comptes.

Le mode « parrainage » offre la possibilité de déléguer, à une personne habilitée, le droit d'accepter ou non la demande d'accès à Internet d'une personne externe à l'entreprise.

De nombreuses améliorations permettent de personnaliser les différents portails d'accès des utilisateurs.

Intégration dans un environnement multidomaine

L'authentification des utilisateurs peut désormais être réalisée sur plusieurs domaines Active Directory. Il est donc possible d'authentifier des utilisateurs provenant de différents domaines et de leur appliquer des politiques de sécurité distinctes.

Les annuaires multiples offrent également la possibilité d'enregistrer les administrateurs du firewall dans un annuaire interne, et de gérer les utilisateurs sans privilèges dans un annuaire externe.

Géolocalisation IP - Filtrage par pays

Grâce à la fonctionnalité de géolocalisation, l'administrateur bénéficie d'une meilleure visibilité sur la provenance ou la destination de son trafic réseau. Il est alors possible d'adapter la politique de sécurité et de filtrer les flux selon un nouveau critère représenté par des objet géographiques de type « Pays » ou « Continent ».

L'ensemble des fichiers de traces et des rapports est désormais enrichi d'un nouvel élément correspondant au pays.

IP Reputation – Réputation des machines externes

Cette fonctionnalité, qui peut être combinée à la géolocalisation, permet de limiter le risque d'attaques subies par une entreprise.

Les IP publiques, dont la réputation est mauvaise (exemple : noeuds de sortie du réseau Tor), sont classifiées dans une des sept catégories : Spam, Phishing, Anonymizer, Botnet, Malware, Tor et Scanneur. Ces catégories sont mises à jour très fréquemment grâce au mécanisme Active Update.

Via sa politique de sécurité, l'administrateur peut ainsi bloquer les tentatives d'accès à l'entreprise des machines externes ayant une mauvaise réputation, mais aussi interdire les connexions des postes internes vers des machines réputées à risques.

Dynamic Host Reputation – Réputation des machines internes

Il est désormais possible d'affecter une politique de sécurité basée sur la réputation des machines internes.

Cette réputation, qui se caractérise par un score, est calculée dynamiquement grâce aux différentes remontées faites par les moteurs d'inspection intégrés aux firewalls Stormshield. Un virus détecté, une alarme majeure ou un malware identifié par notre solution de sandboxing provoque une augmentation automatique du score de la machine.

L'administrateur peut visualiser l'historique du score de réputation d'une machine dans le nouveau module « supervision ». D'autres indicateurs comme le score moyen de son réseau et le score maximum, sont autant d'informations disponibles pour l'aider à définir sa politique de sécurité et intervenir sur les machines concernées.

Cette fonctionnalité nécessite la présence d'une carte SD pour les firewalls ne disposant pas d'un disque dur.

Objets « Noms DNS (FQDN) »

Afin d'affiner une politique de sécurité, il est désormais possible d'utiliser des objets réseau uniquement définis par leur FQDN (adresse(s) IP récupérée(s) automatiquement à l'aide de résolutions DNS) comme « google.com » ou « office365.com ».

Envoi sécurisé des flux Syslog au travers du protocole TLS

L'envoi de traces vers un ou plusieurs serveurs Syslog (4 maximum) via TCP, peut désormais être sécurisé au travers du protocole TLS avec une authentification par certificats client et serveur.

Cet envoi sécurisé de flux Syslog est compatible avec la solution Stormshield Visibility Center.

Les Firewalls Stormshield Network supportent plusieurs formats normalisés de messages Syslog (RFC3164, RFC5424, RFC5425 et RFC6587).

Possibilité de configurer l'algorithme de hachage dans la PKI interne et le proxy SSL

Le module Certificats et PKI offre la possibilité de sélectionner l'algorithme de hachage (notamment l'algorithme SHA256) utilisé pour les certificats du proxy SSL et de la PKI interne du firewall.

Support IPFIX/Netflow

La compatibilité avec les collecteurs Netflow/IPfix permet à un administrateur d'identifier facilement d'éventuels problèmes réseaux.

Signatures personnalisées du moteur de prévention d'intrusion (IPS)

Les administrateurs peuvent désormais créer leurs propres signatures contextuelles afin de détecter des applications internes à l'entreprise.

SNi40 - Bypass matériel

Afin d'assurer une continuité de service dans les milieux industriels, le firewall SNi40 est équipé d'un bypass matériel qui permet, une fois activé, de laisser passer le trafic réseau en cas de coupure électrique ou de défaillance du boîtier.

Import et export du contenu de la base des objets réseau

L'export au format CSV de la base objets permet ainsi de sauvegarder la base et de la réimporter directement dans la solution d'administration centralisée Stormshield Management Center.

La structure des lignes constituant la base objets au format CSV est disponible en **Annexe B** du **Manuel de Configuration et d'Administration Stormshield Network**.

Support officiel des plate-formes de virtualisation KVM et Hyper-V

Le firewalls virtuels Stormhield Network sont disponibles pour les plate-formes Microsoft Hyper-V (format VHD) et KVM (Kernel-based Virtual Machine - format QCOW2). Les version d'hyperviseurs supportées sont disponibles dans le chapitre **Compatibilité** de ce document.

Analyse IPS des flux HTTP avec décompression à la volée

Le moteur de prévention d'intrusion est désormais capable de décompresser les données HTTP à la volée afin de réaliser les analyses IPS de ce protocole. Le firewall ne doit donc plus modifier

l'en-tête des paquets HTTP envoyés par le client afin de masquer le support de la compression (*accept-encoding*). Ce mécanisme réduit ainsi la latence et la quantité de données nécessaires au transfert des paquets HTTP, mais sollicite les ressources du firewall de manière plus importante.

Cette fonctionnalité est activée par défaut et peut être suspendue dans le module de configuration du protocole HTTP.

Possibilité d'ajouter une contrainte sur le *Domain name* du certificat présenté par un correspondant IPSec.

Lorsqu'une autorité de certification (CA) est spécifiée dans les autorités de confiance pour l'établissement de tunnels IPSec, il est possible d'ajouter une contrainte sur le Domain Name (DN) du certificat présenté par le correspondant afin de renforcer la sécurité.

Analyse IPS du protocole industriel Ethernet/IP

Le moteur de prévention d'intrusion offre désormais la possibilité de filtrer (*Analyser / Bloquer*) les jeux de commandes publiques de ce protocole. Il est également possible de spécifier une liste personnalisée de commandes Ethernet/IP devant être autorisés.

Analyse IPS du protocole SNMP

SNMP (Simple Network Management Protocol) est un protocole de supervision d'équipements réseaux. L'analyse IPS de ce protocole a été notablement enrichie. Il est ainsi possible d'autoriser ou de bloquer les paquets SNMP selon la version du protocole (SNMPv1, v2c ou v3), de créer des listes noires/blanches de communautés (SNMPv1 et v2c), d'identifiants (SNMPv3) ou d'OID (*Object Identifier*).

Support du NAT pour le DNS Dynamique

Le module émettant l'adresse IP publique à destination du fournisseur de service d'enregistrement DNS dynamique, différencie désormais l'adresse IP publique réelle, portée par un routeur effectuant du NAT, de l'adresse locale. Cette fonctionnalité s'active en cochant la case Supporter la translation d'adresses (NAT) dans la configuration avancée du module DNS dynamique.

Proxy SSL - Support de nouveaux algorithmes de chiffrement

Le proxy SSL supporte de nouveaux algorithmes de chiffrement basés sur des courbes elliptiques (algorithme ECDSA : Elliptic Curve Digital Signature Algorithm).

Vérification systématique des objets non utilisés

Le module **Objets réseau** affiche la liste des objets présents dans la base du firewall; les objets sont classés par catégorie (machines, réseaux, Nom de domaine DNS [FQDN],...).

Chaque objet est précédé d'un symbole de couleur indiquant dynamiquement si l'objet est utilisé dans la configuration du firewall (puce verte) ou non (puce grise). Un clic sur l'icône « œil » située à droite d'une puce verte liste l'ensemble des modules utilisant l'objet considéré.

Noms des règles dans les traces IPS et le journal des connexions actives

Le module Filtrage et Nat permet d'affecter un nom à chacune des règles créées. Notez que la colonne « Nom » est masquée par défaut.

Ce nom de règle (*rulename*) est référencé dans les journaux de traces IPS et le journal des connexions. Il présente l'avantage de ne pas évoluer en fonction des critères de la règle (« via », « interface », ...) mais aussi de la position de celle-ci dans la politique de filtrage, contrairement à l'identifiant de règle (*ruleid*). Il est ainsi possible de manipuler ou de filtrer aisément les règles de filtrage ou de NAT en fonction de leur nom.

Export des données de supervision et des journaux d'audit

A l'image des données des rapports, les informations affichées dans les journaux d'audit et les données présentées dans les grilles du module de supervision peuvent elles-aussi être exportées dans un fichier au format CSV.

Sandboxing – Formulaire de signalement de faux positifs

Les interactions proposées sur les journaux d'audit permettent d'avertir Stormshield d'une catégorisation erronée issue de l'analyse Sandboxing. Cette fonctionnalité permet ainsi de faire débloquer une pièce-jointe considérée à tort comme malveillante.

Authentification

La longueur maximale d'un identifiant a été portée à 255 caractères. De plus, un utilisateur peut désormais être inclus dans 250 groupes (cette limite était de 50 dans les versions antérieures).

VPN SSL

Le fichier de configuration de SSL VPN Client inclut désormais les options register-dns et block-outside-dns lui indiquant respectivement d'écrire dans sa configuration le(s) serveur(s) DNS précisé(s) par le firewall Stormshield Network et de ne pas utiliser de serveur DNS tiers. Cette fonctionnalité réduit ainsi le délai nécessaire pour la réception des réponses aux requêtes DNS du client, notamment pour les machines fonctionnant sous Microsoft Windows 10.

Connexions filles (FTP actif) au travers d'interfaces IPSec virtuelles

Les flux engendrant des connexions filles (exemple : FTP actif) sont désormais compatibles avec l'utilisation d'interfaces IPSec virtuelles (VTI).

Requêtes DNS basées sur le protocole TCP

Les firewalls Stormshield Network basculent automatiquement leurs requêtes DNS sur le protocole TCP lorsqu'ils reçoivent une réponse excédant 512 octets (réponse avec beaucoup d'entrées comme pour les objets dynamiques et les objets de type Nom DNS [FQDN]).

Ajout de traces pour les pseudo-connexions stateful

Les pseudo- connexions stateful (protocoles GRE, ESP, ...) génèrent désormais des enregistrements dans les fichiers de traces des connexions (*l_connection*) et des statistiques de filtrage (*l_filterstat*).

Support des modem génériques 3G/4G

Pour les modems génériques 3G/4G dont les caractéristiques ne sont pas reconnues automatiquement, il est possible de définir jusqu'à deux profils regroupant les informations de configuration (modèle, identifiant constructeur, ...) renseignées manuellement. Les différents champs à paramétrer sont présentés dans le chapitre **Création d'un modem** du **Manuel de Configuration et d'Administration Stormshield Network**.

Renforcement de l'analyse IPS du protocole TCP

L'analyse IPS du protocole TCP a été renforcée, afin de détecter la présence de données dans un paquet de RESET et de déclencher l'alarme spécifique "TCP RST with data". Elle peut désormais également prendre en charge un nombre de données non acquittées plus conséquent, sans déclencher l'alarme n°84 "TCP data queue overflow".

Autres fonctionnalités

- Amélioration de l'analyse IPS du protocole SSL au sujet des en-têtes fragmentées
- Support des caractères internationaux Unicode dans les certificats
- Présence des noms d'objets sources et destinations dans les e-mails d'alarmes
- Ajout du nom système du firewall dans les invites de commande Shell

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 privé https://mystormshield.eu, menu **Support technique** > **Rapporter un incident / Suivre un incident**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais du site web https://mystormshield.eu.