STORMSHIELD NETWORK SECURITY

NOTES DE VERSION VERSION

Édition française

28 Septembre 2016

Mise à jour

Version minimale requise : Stormshield Network 1.x et NETASQ 9.1.x

Compatibilité matérielle :

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000 et SN6000

NETASQ U30S, U70S, U150S, U250S, U500S, U800S, NG1000-A et NG5000-A

Stormshield Network et NETASQ Virtual Appliances

NOTE
Avant toute mise à jour, il est fortement recommandé de faire une sauvegarde et de lire attentivement le chapitre des Précisions sur les cas d'utilisation.

Points principaux

Fonctionnalités abordées	Niveau de modification
VPN SSL	→ Majeure
Support IPv6	→ Majeure
Activity Report - Traces	→ Majeure
Interfaces réseaux	→ Majeure
Moteur de prévention d'intrusion	→ Majeure
Cloud backup	→ Mineure
Authentification « Guest »	→ Mineure
Proxy HTTP	→ Mineure

Version

Cette note contient le descriptif des principales modifications apportées aux différentes versions d'une même version majeure. Il est recommandé d'appliquer la dernière version afin de bénéficier des nouveautés et correctifs les plus récents.

1.6.1		Vulnérabilités résolues	
Problèmes identifiés			
1.6.0		Vulnérabilités résolues	Correctifs
1.5.0		Vulnérabilités résolues	Correctifs
1.4.4			Correctifs
1.4.3		Vulnérabilités résolues	
1.4.2		Vulnérabilités résolues	Correctifs
1.4.1	Fonctionnalités		
1.4.0	Fonctionnalités	Vulnérabilités résolues	Correctifs
1.3.4		Vulnérabilités résolues	
1.3.3		Vulnérabilités résolues	Correctifs
1.3.2		Vulnérabilités résolues	Correctifs
1.3.1		Vulnérabilités résolues	Correctifs
1.3.0	Fonctionnalités	Vulnérabilités résolues	Correctifs
1.2.2			Correctifs
1.2.1		Vulnérabilités résolues	Correctifs
1.2.0	Fonctionnalités	Vulnérabilités résolues	Correctifs
1.1.3			Correctifs
1.1.2	Fonctionnalités		
1.1.1			Correctifs
1.1.0	Fonctionnalités	Vulnérabilités résolues	Correctifs
1.0.0	Fonctionnalités		
Précisions sur les cas d'utilisation			

Gestion du cycle de vie des versions

Conformément au document Product Life Cycle Stormshield Network Security, la maintenance des versions de firmware de la branche 1.x est garantie jusqu'au 31/12/2016.

Précautions avant Migration

Le binaire NSRPC (exécutable Windows) permet de se connecter à distance sur des Firewalls et d'exécuter des commandes CLI de manière séquentielle. Depuis la version 1.0, l'authentification des communications s'effectuant via le protocole HMAC-SHA2, il est nécessaire de mettre à jour le client NSRPC. Celui-ci est disponible depuis les espaces clients et partenaires.

Objets dynamiques

Dans une version de firmware NETASQ antérieure à 9.0.6, une configuration pouvait contenir des objets dynamiques ayant une adresse IP égale à 0.0.0.0. Ce type de valeur pouvant entraîner un conflit lors du traitement par le moteur ASQ, il est conseillé de chercher ce type d'objet et de remplacer la valeur 0.0.0.0 par une adresse IP valide, avant la migration.

Entrées ARP

Si la configuration du nombre d'entrées ARP avait été personnalisée (champ MaxEntries du fichier ConfigFiles / arp), celle- ci sera réinitialisée lors d'une opération de migration. Cette personnalisation doit donc être renouvelée à l'issue du changement de version (champs MaxARPEntries et MaxNDPEntries du fichier ConfigFiles / ether).

1.6.1 Vulnérabilités résolues

Faille de sécurité OpenSSL

Une vulnérabilité (CVE-2016-6304 - *OCSP Status Request extension unbounded memory growth*) a été corrigée par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1u. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Problèmes identifiés

Prévention d'intrusion

Référence support 45406

Dans les configurations de règles de filtrage combinant de la translation d'adresse et une inspection en mode « Firewall » ou « IDS », les connexions utilisant un protocole nécessitant la réécriture de paquets (FTP par exemple) peuvent être altérées. En effet, un paquet TCP présentant un numéro de séquence hors de la fenêtre TCP attendue, stoppe l'analyse protocolaire (plugin attaché en raison du type de protocole). Cette dernière réécrivant les paquets, son interruption fausse ainsi le NAT associé.

Référence support 49241

Le plugin de protection SIP ne supporte pas la méthode REFER (RFC 3515) de ce protocole.

Système

Interfaces

L'option de connexion « en cas de trafic (à la demande) » ne permet pas à un modem de fonctionner correctement. C'est pourquoi, lors de la création d'un modem à l'aide de l'assistant, l'option de connexion « permanente » est sélectionnée par défaut.

Sur les modèles U30S et SN200, il est désormais autorisé de créer plusieurs VLAN au sein d'un bridge via l'interface d'administration web. Cependant, cette opération est fortement déconseillée et non supportée car susceptible d'entraîner un défaut de transmission des réponses aux requêtes ARP reçues sur ces VLANs vers les autres interfaces du bridge.

Référence support 52236

Licence

L'interface Web d'administration de certains firewalls peut ne pas être accessible, le firewall présentant alors une page affichant la mention « Echec de déchiffrement ». Il s'agit d'un problème de déchiffrement de la licence ayant été appliquée au firewall. Pour obtenir la procédure permettant de contourner cette anomalie, veuillez consulter la base de connaissances ou vous rapprocher de votre support Stormshield.

1.6.0 Vulnérabilités résolues

Faille de sécurité OpenSSL

Une vulnérabilité (CVE-2016-2107 - Attack against an AES CBC session implemented with AES-NI) a été corrigée par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1t. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Protocole NTP

Un ensemble de vulnérabilités :

- CVE-2015-8158 (*Potential Infinite Loop in ntpq*);
- CVE-2015-8138 (*Zero Origin Timestamp Bypass*);
- CVE-2015-7979 (*Off-path Denial of Service (DoS) attack on authenticated broadcast mode*);
- CVE-2015-7978 (*Stack exhaustion in recursive traversal of restriction list*);
- CVE-2015-7977 (*reslist NULL pointer dereference*);
- CVE-2015-7976 (*ntpq saveconfig command allows dangerous characters in filenames*);
- CVE-2015-7975 (*nextvar() missing length check*);
- CVE-2015-7974 (*Skeleton Key: Missing key check allows impersonation between authenticated peers*);
- CVE-2015-7973 (*Replay attack on authenticated broadcast mod*).

a été corrigé par la mise à jour des librairies de gestion du protocole d'heure réseau (NTP). Le détail de ces vulnérabilités est disponible sur notre site https://advisories.stormshield.eu.

1.6.0 Correctifs

Prévention d'intrusion

Une anomalie dans la prise en compte de règles de filtrage précisant des interfaces inactives (exemple : interfaces modem) pouvait perturber l'application des autres règles de filtrage de la politique. Cette anomalie a été corrigée.

Système

L'envoi répété de commandes de supervision depuis SN Real-Time Monitor pouvait provoquer une consommation mémoire anormale de la part du serveur d'administration du firewall. Ce problème a été corrigé.

1.5.0 Vulnérabilités résolues

Faille de sécurité SNMP

Une vulnérabilité (CVE-2015-5621) pouvant entraîner une attaque de type Déni de Service a été corrigée par la mise à jour de la bibliothèque NetSNMP. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

Faille de sécurité DHCP

Une vulnérabilité (CVE-2015-8605) pouvant entraîner une attaque de type Déni de Service a été corrigée par la mise à jour des composants DHCP. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu.

1.5.0 Correctifs

Système

Haute disponibilité

Référence support 48239 - 50250 - 51660 - 51936

Dans une configuration de firewalls en haute disponibilité, une anomalie dans la gestion de la mémoire virtuelle du firewall pouvait entraîner une erreur de communication entre les membres du cluster (message « Communication impossible entre les membres du groupe de H.A. » affiché dans la section **Matériel** de Stormshield Network Real-Time Monitor ou de l'interface Web d'administration). Ce problème, qui pouvait également empêcher l'affichage des propriétés du cluster dans l'interface Web d'administration (menu **Système** > **Haute Disponibilité**), a été corrigé.

Référence support 52441

Proxy SMTP

Lorsqu'un serveur SMTP répondait à la première requête d'un client en y insérant un nom de domaine DNS, le firewall pouvait considérer cette réponse comme non conforme et bloquer le flux correspondant. Ce problème a été résolu.

Matériel

Référence support 51616

Sur les firewalls modèle SN6000, le mécanisme de supervision des modules d'alimentation électrique pouvait générer une quantité excessive de traces dans les journaux d'audit. Cette anomalie a été corrigée.

Référence support 52264

Sur les firewalls modèle NG1000, suite à l'ajout d'une second disque dur, la construction du RAID pouvait échouer du fait d'une différence de capacité des disques supérieure à 5%. Le problème a été corrigé en supprimant cette limitation.

1.4.4 Correctifs

Système

Tunnels VPN SSL

Suite à la mise à jour des librairies OpenSSL, le logiciel Stormshield Network VPN SSL client pouvait échouer à s'authentifier auprès du firewall pour établir les tunnels SSL. Ce dysfonctionnement a été corrigé.

Proxies

Dans une configuration utilisant des règles de filtrage d'URL, une anomalie dans la gestion des connexions closes pouvait entraîner une consommation excessive des ressources mémoire du firewall. Cette anomalie a été corrigée.

1.4.3 Vulnérabilités résolues

Failles de sécurité SSL et TLS

Un ensemble de vulnérabilités (CVE-2015-3194 et CVE-2015-3195) a été corrigé par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1q. Le détail de ces vulnérabilités est disponible sur notre site https://advisories.stormshield.eu.

1.4.2 Vulnérabilités résolues

Faille XSS

Une vulnérabilité pouvant potentiellement affecter les pages de blocage présentées par le proxy SSL a été corrigée. Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/.

1.4.2 Correctifs

Système

Référence support 52087

Interfaces

Sur les firewalls modèles NG1000 et NG5000 équipés de cartes réseau 10Gb/s, la mise à jour vers une version de firmware supérieure à 1.4.0 pouvait entraîner un problème d'ordonnancement des interfaces réseau. Ce problème a été corrigé.

Filtrage
Une anomalie dans l'optimisation de l'évaluation du filtrage sur des flux similaires, appliquée à des objets IPv4 et IPv6, a été corrigée.

1.4.1 Fonctionnalités

Matériel

La version de firmware 1.4.1 est désormais compatible avec les modèles de Firewalls Stormshield Network SN510 et SN710.

1.4.0 Fonctionnalités

Matériel

Les modèles de Firewalls Stormshield Network SN910, SN2000 et SN3000 en version de firmware 1.4.0 ou supérieure supportent les cartes fibre 2x10Gb portant la référence NA-EXT-CARD-2x10G-SFP+.

1.4.0 Vulnérabilités résolues

Faille de sécurité FreeBSD

Une vulnérabilité pouvant entraîner une attaque de type Déni De Service a été résolue par la mise à jour du système d'exploitation FreeBSD (Resource exhaustion due to sessions stuck in LAST_ACK state - CVE-2015-5358).

1.4.0 Correctifs

Système

Référence support 50083
La migration d'une configuration depuis une version 9.1.x vers une version 1.x pouvait potentiellement aboutir au blocage du firewall pendant sa phase de redémarrage (étape d'initialisation du moteur de prévention d'intrusion). Ce problème est désormais résolu.

Référence support 48971
Lors du changement de mot de passe du compte « admin » en ligne de commande, et si le système de fichiers était détecté comme potentiellement défectueux, l'utilitaire de réparation de disque était appelé avec une option incorrecte. Il ne parvenait alors pas à reconnaître le système de fichiers et générait un message d'erreur (*Could not determine filesystem type*). Cette anomalie a été corrigée.

Référence support 50816

Suite à la remise en configuration d'usine (defaultconfig) d'un firewall modèle SN2000, SN3000 ou SN6000, les partitions d'échange (swap) et de journaux d'événements (logs) pouvaient ne plus être accessibles après redémarrage. Ce problème a été résolu.

Proxies

Référence support 49427

Lorsqu'un client utilisait un proxy HTTP explicite au travers d'un tunnel IPSec afin d'accéder à Internet, la connexion échouait et le message d'erreur « Error when setting fw IP from interface » était remonté dans le journal de connexions Web (fichier l_web). Ce problème est désormais corrigé.

Référence support 49935

Le proxy SMTP du firewall ne parvenait pas à ajouter d'étiquette de classification de SPAM dans le sujet d'un e-mail ne présentant aucun en-tête. Ce problème a été corrigé.

Référence support 44815

L'utilisation combinée de proxies et de la solution de filtrage d'URL Extended Web Control pouvait entraîner une consommation processeur importante. Ce problème a notamment été résolu par la mise à jour des librairies utilisées par la solution Extended Web Control.

Référence support 49965 - 50421

Des modifications du proxy SSL ont amélioré sa stabilité.

VPN IPSec

Référence support 48888

La connexion puis la déconnexion d'un client PPTP sur un firewall ayant établi un tunnel IPSec site à site pouvait rendre ce tunnel inopérant. Ce problème a été corrigé.

Référence support 49504

Dans le cas de tunnels VPN IPSec en mode nomade, et basés sur une authentification par certificats, le firewall n'envoyait plus de requête de certificat lors de la négociation de phase 1. Cette anomalie pouvait empêcher l'établissement du tunnel en cas d'utilisation d'un client VPN tiers ne présentant pas son certificat de manière automatique (le logiciel Stormshield VPN Client n'était pas impacté). Cette anomalie est désormais corrigée.

Référence support 49120 - 49322

VPN SSL

Lorsqu'un objet dynamique était sélectionné pour tester la disponibilité d'une passerelle du firewall, les tunnels VPN SSL établis sur le firewall se voyaient régulièrement réinitialisés. Ce problème a été résolu et les tunnels VPN SSL ne sont plus réinitialisés lors du rechargement d'un objet dynamique servant aux tests de disponibilité d'une passerelle.

Haute disponibilité

Des modifications ont été apportées afin d'améliorer la stabilité du mécanisme de haute disponibilité lors d'une forte charge prolongée.

Référence support 50081

Evénements sytème

Suite à la migration d'une configuration en version 1.3.x, certaines alarmes système pouvaient ne plus être disponibles. Cette anomalie a été corrigée.

Prévention d'intrusion

Référence support 50617 - 48378

Dans un groupe de firewalls en Haute disponibilité, les connexions traitées par le firewall actif et bénéficiant des améliorations de performances du mode "fastpath" n'étaient pas synchronisées sur le firewall passif. Cette anomalie a été corrigée.

Interface d'administration Web

Référence support 48028

VPN SSL

L'interface d'administration web n'acceptait pas la définition d'un nom de domaine DNS présentant plus de 6 caractères après le point (exemple : company.internal). Cette anomalie est désormais corrigée.

1.3.4 Vulnérabilités résolues

Faille de sécurité SSL et TLS

Une vulnérabilité (*Alternative chains certificate forgery* - CVE-2015-1793) a été résolue par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1p.

1.3.3 Vulnérabilités résolues

Failles de sécurité SSL et TLS

Des vulnérabilités pouvant entraîner des attaques de type Man in the Middle (MITM) ou Déni De Service ont été résolues par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1o. La liste de ces vulnérabilités est consultable sur le site de l'éditeur de cette librairie.

1.3.3 Correctifs

Prévention d'intrusion

Référence support 49013 - 49356 - 49768 - 48082 - 48898 - 48945 - 48611 - 48513 - 48520 - 49408

Dans une configuration combinant l'utilisation d'un proxy http et de règles de filtrage ayant activé le plugin http, la réécriture des paquets réseau par le moteur de prévention d'intrusion pouvait

potentiellement aboutir à un blocage du firewall. Ce problème a été corrigé.

Référence support 50602 - 47612

Dans une configuration combinant l'utilisation de translation des adresses sources (NAT) et de règles de filtrage en mode IDS ou firewall, le filtrage de paquets réseaux fragmentés pouvait aboutir à un blocage ou un redémarrage du firewall. Ce problème est désormais corrigé.

VPN IPSec

Référence support 49504

Dans le cas de tunnels VPN IPSec en mode nomade, et basés sur une authentification par certificats, le firewall n'envoyait plus de requête de certificat lors de la négociation de phase 1. Cette anomalie pouvait empêcher l'établissement du tunnel en cas d'utilisation d'un client VPN tiers ne présentant pas son certificat de manière automatique (le logiciel Stormshield VPN Client n'était pas impacté). Cette anomalie est désormais corrigée.

1.3.2 Vulnérabilités résolues

Faille de sécurité SSL et TLS

Une vulnérabilité (faille Logjam) a été résolue en imposant une taille minimum pour les clés Diffie-Hellman utilisées lors de la négociation de sessions SSL/TLS à destination du firewall (connexion à l'interface Web d'administration et au portail d'authentification).

Cette taille est de 2048 bits pour le mode renforcé (désactivation de la version SSLv3 au profit de la version TLS, utilisation de suites de chiffrement AES avec Diffie-Hellman), utilisé par défaut sur les Firewalls Stormshield Network. Elle est de 1024 bits si ce mode renforcé a été désactivé (opération exclusivement réalisable à l'aide de la commande CLI : `CONFIG AUTH HTTPS sslparanoiac=0 /CONFIG AUTH ACTIVATE`).

Clam AV

Le moteur d'antivirus ClamAV a été mis à jour en version 0.98.7. Le détail des améliorations et correctifs apportés par cette version est disponible sur le site de l'éditeur.

1.3.2 Correctifs

Système

Référence support 49347 - 50360 - 48454

Proxy SSL

Lors de la renégociation d'un ticket de session SSL, un problème dans la gestion du cache des sessions établies pouvait potentiellement entraîner un redémarrage du proxy SSL. Ce problème a été corrigé.

Prévention d'intrusion

Référence support 50420 - 50532 - 50640

Un problème dans l'analyse de paquets provenant d'outils d'optimisation de réseaux étendus (solutions **Cisco** / **Riverbed Technology**) pouvait entraîner un blocage ou un redémarrage du firewall. Ce problème a été corrigé.

Référence support 50531 - 50627 - 50536

Une anomalie dans la gestion des connexions filles pour les protocoles TCP et UDP pouvait potentiellement aboutir à un blocage du firewall. Ce problème a été corrigé.

1.3.1 Vulnérabilités résolues

Failles de sécurité NTP

Des vulnérabilités pouvant entraîner des attaques de type Man in the Middle (MITM) et Déni de Service (DoS) ont été résolues par la mise à jour du client NTP en version 4.2.8p2. En voici la liste :

- Ntpd accepts unauthenticated packets with symmetric key crypto (CVE-2015-1798).
- Authentication doesn't protect symmetric associations against DoS attacks (CVE-2015-1799).

1.3.1 Correctifs

VPN SSL Portail

Référence support 49950

Malgré la récente signature de l'applet d'accès à un serveur applicatif via le VPN SSL Portail, l'utilisateur se voyait présenter une erreur Java indiquant que cette signature était expirée. La version de l'applet n'ayant pas évolué, le client Java consultait les données contenues dans son cache et considérait ainsi cette signature comme obsolète. Ce problème a été corrigé en modifiant le numéro de version de l'applet Java.

1.3.0 Fonctionnalités

Les firewalls Stormshield Network peuvent désormais télécharger un fichier de mise à jour, une configuration ou une licence depuis une clé USB formatée dans le système de fichiers Microsoft FAT32.

Matériel

Les firewalls haut de gamme SN6000 supportent désormais les modules d'extension 8-ports fibre 1 Gb Ethernet.

1.3.0 Vulnérabilités résolues

Faille de sécurité SSL et TLS

Une vulnérabilité pouvant entraîner une attaque de type Déni de Service (CVE-2015-0286) a été résolue par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1m.

Référence support 49545

Une vulnérabilité dans le protocole IGMP, pouvant entraîner une attaque de type Déni De Service (CVE-2015-1414), a été résolue par l'application d'un ensemble de correctifs FreeBSD.

1.3.0 Correctifs

Réseau

Référence support 47845 - 47855

Dans le cas d'une configuration mettant en œuvre de la répartition de charge sur des interfaces non protégées et une règle de filtrage entre deux interfaces protégées comportant de la translation d'adresses (NAT), le rechargement des règles de filtrage provoquait une coupure des connexions correspondant à cette règle. Ce problème a été corrigé.

Référence support 46512

Dans le cas d'une configuration utilisant le proxy transparent ainsi que des passerelles au sein d'une règle de filtrage (PBR : Policy Based Routing), les flux pouvaient se voir attribuer une interface de destination erronée. Ce problème a été corrigé.

Référence support 47570

La désactivation d'une interface réseau pouvait entraîner la suppression des objets dérivés associés de la base objets (*Firewall_interface_name* et *Network_interface_name*). Ce dysfonctionnement a été corrigé.

Référence support 49490

Dans la table ARP, l'adresse MAC des objets globaux pouvait être remplacée de manière inappropriée par l'adresse MAC du dernier objet local créé.

Agrégation de liens et haute disponibilité

Dans un groupe de Firewalls configurés en Haute Disponibilité et utilisant des liens agrégés (modèles NG, SN2000, SN3000 et SN6000), le firewall passif pouvait parfois émettre du trafic de contrôle LACP. Les flux à destination du cluster se trouvaient alors perturbés, car le firewall passif pouvait dans ce cas être perçu comme étant actif. Ce problème a été résolu.

Système

Référence support 49471 - 49605

Dans le cas d'une migration de configuration vers une version 1.2.x, certains fichiers système pouvaient se voir attribuer un propriétaire incorrect. Ce problème, qui impactait notamment le fonctionnement de la haute disponibilité, a été corrigé.

Référence support 48156 - 47564

Haute disponibilité

Une configuration en haute disponibilité restaurée sur un firewall tiers (remplacement d'un des membres du cluster par exemple) le forçait à activer la haute disponibilité et le plaçait en état « passif ». En effet, les numéros de série des firewalls composant le cluster étant référencés dans la configuration, le nouveau firewall n'était pas reconnu et ne pouvait donc joindre le cluster.

Désormais, dans un contexte similaire, le firewall tiers recevant la configuration n'active plus la Haute Disponibilité.

Référence support 48511

Authentification

La suppression d'une Autorité de certification de confiance déclarée pour la méthode d'authentification SSL n'était pas prise en compte : la connexion d'un utilisateur présentant un certificat signé par cette CA était toujours acceptée. Ce dysfonctionnement est désormais corrigé.

Référence support 48185

SSO Agent

La modification manuelle des paramètres de la section [Agent] du fichier de configuration de l'authentification (port de connexion à SN SSO Agent et adresse IP présentée par le firewall pour réaliser cette connexion) n'était pas prise en compte. Ce dysfonctionnement a été corrigé.

Référence support 49434

Proxies

Dans des configurations utilisant l'antivirus et le proxy http, des en-têtes de requêtes http spécifiques pouvaient provoquer un dysfonctionnement du proxy. Ce problème a été corrigé.

Référence support 48146

Proxy SMTP

Lors d'une analyse antivirale concernant un volume important d'emails et de pièces jointes, les fichiers temporaires nécessaires à cette opération pouvaient ne pas être supprimés en fin de traitement. Ceci pouvait alors potentiellement aboutir à une saturation de la partition dédiée aux fichiers temporaires. Ce comportement a été corrigé et les fichiers temporaires sont correctement supprimés lors du retour à une charge normale d'analyse antivirale.

Référence support 49033

Le choix d'une valeur élevée pour la taille maximale d'un e-mail pouvait se traduire par une interprétation erronée de cette limite, aboutissant à un blocage des e-mails. Ce comportement a été corrigé.

Référence support 48295

L'augmentation du nombre maximal de destinataires d'un e-mail (onglet Proxy du module Protocoles > SMTP) n'était pas prise en compte et restait fixée à sa valeur par défaut (100). Ce comportement a été corrigé, et la hausse de cette limite est désormais respectée.

Référence support 44313

Dans le cas de réponse multiple d'un serveur SMTP à une requête client, le plugin de protection SMTP génère une alarme bloquante. Cependant, si cette alarme était forcée en action « passer », ce type de réponse pouvait potentiellement provoquer un blocage du proxy. Ce risque de blocage a été corrigé.

Référence support 48661

Objets réseau

La résolution DNS dynamique ne fonctionnait pas pour des objets réseau comportant un caractère numérique dans le domaine de premier niveau (exemple : server.mydomain.a2). Il était donc nécessaire de saisir une adresse IP lors de la création de ce type d'objet. Ce problème est désormais corrigé et la résolution DNS dynamique est de nouveau fonctionnelle pour ce type d'objet.

Référence support 48170

Qualité de service

Un changement manuel des champs *PrioritizeLowDelay* ou *PrioritizeAck* dans le fichier de configuration de la QoS était écrasé après modification de la file d'attente correspondante au sein du module Qualité de Service de l'interface d'administration Web. Ce comportement a été modifié.

Référence support 48906

VPN SSL

Lorsque le port utilisé par le serveur VPN SSL avait été modifié dans une configuration en version 1.1, la migration de cette configuration en version 1.2 entraînait la réinitialisation de ce port VPN SSL à sa valeur par défaut (TCP/443). Ce comportement a été corrigé pour conserver la valeur personnalisée du port.

Référence support 48582

Stormshield VPN SSL Client refusait une configuration comportant plus de 100 routes réseau car ce nombre n'était pas explicitement indiqué. Lorsque le nombre de routes dépasse cette valeur, il est désormais précisé dans la configuration envoyée au client (champ **max-routes**) afin que le client VPN SSL prenne en compte l'ensemble des routes et autorise l'établissement du tunnel.

Référence support 48708

Certificats et PKI

Pour les nouvelles installations ou les remises en configuration d'usine (*defaultconfig*), les certificats présentés par le proxy SSL et le serveur OpenVPN référencent désormais le nom Stormshield dans le champ organisation (O).

Référence support 47556

Filtrage et NAT

La modification du nom d'un objet réseau n'était pas répercutée dans la règle de filtrage utilisant cet objet en tant que passerelle (PBR : Policy Based Routing). Cela provoquait ainsi un message d'erreur du type « [Règle X] Nom de routeur incorrect : *nom_passerelle* ». Cette anomalie a été corrigée.

Référence support 47446

Autoupdate

La fonctionnalité de mise à jour automatique pouvait ne pas fonctionner correctement dans des configurations comportant du partage de charge sur les passerelles d'accès à Internet, certains paquets émis ne se présentant pas avec l'adresse IP de leur interface de sortie. Ce dysfonctionnement est désormais corrigé.

Référence support 48564

Pour un firewall utilisant une règle de filtrage avec analyse antivirale et ne disposant pas d'une base d'antivirus à jour, un redémarrage complet pouvait être fortement ralenti (mise à jour de firmware sur le firewall passif d'un cluster par exemple). Ceci était dû au déclenchement d'une mise à jour de la base antivirale pendant le redémarrage du firewall.

Référence support 49023

Autobackup

Une sauvegarde automatique de configuration basée sur le protocole HTTPS pouvait potentiellement échouer, entraînant un transfert partiel du fichier. Ce dysfonctionnement a été corrigé.

Référence support 48599

Firewalls virtuels

Pour les modèles de firewalls virtuels VS-VU, les fichiers d'installation (OVA) fixent désormais la quantité de mémoire requise à 4Go afin d'éviter d'éventuels problèmes de démarrage des machines de type VU. Ainsi, toute mise à jour en version 1.3 d'un firewall virtuel existant de type VU sera refusée si la mémoire attribuée au firewall virtuel est inférieure à 4Go.

Référence support 48739

La migration d'une machine virtuelle de type VS en version 1.2.x pouvait aboutir à une limitation inappropriée du nombre de règles de filtrage du firewall. Cette anomalie a été corrigée.

Référence support 47318

Les firewalls virtuels utilisant la synchronisation NTP pouvaient voir leur horloge dériver de manière importante, les tentatives d'ajustements progressifs du client NTP se révélant insuffisantes. Ceci pouvait potentiellement générer des problèmes d'authentification dans le cas d'un décalage atteignant plusieurs minutes.

Il est désormais possible de paramétrer le client NTP pour que celui-ci ajuste l'horloge en une seule correction et dès lors que la différence excède le nombre de secondes indiqué. Ces paramètres (*TinkerPanic* et *TinkerStep*) sont exclusivement modifiables en éditant le fichier de configuration du client NTP (ConfigFiles/ntp) et en appliquant la commande enntp afin de prendre en compte cette modification.

Référence support 46981

Extended Web Control

Lorsque le serveur référent était détecté comme indisponible, la connexion à un serveur secondaire pouvait ne pas être immédiate. Cette latence était notamment perceptible lorsque le firewall « passif » d'un cluster devenait « actif ». Ce problème a notamment été résolu par la mise à jour des librairies utilisées par la solution Extended Web Control.

Référence support 48935

Serveur PPTP

Suite à plusieurs connexions et déconnexions rapprochées, un client PPTP pouvait se voir attribuer une adresse IP du type 0.0.0.0. Cette adresse l'empêchait alors d'accéder aux machines du réseau interne. Ce dysfonctionnement a été corrigé.

Prévention d'intrusion

Référence support 49661 - 48322

Lorsqu'elle recevait des paquets de taille importante, la carte réseau du firewall pouvait s'adjuger de manière inappropriée la totalité d'un tampon mémoire, provoquant ainsi une corruption mémoire. Ce problème a été corrigé.

Dans le cas d'un trafic réseau élevé entraînant une consommation mémoire importante du firewall, l'utilisation du plugin CIFS pouvait alors potentiellement provoquer une corruption mémoire. Ce problème a été corrigé.

Au sein d'une connexion TCP, si le serveur renvoyait un acquittement situé en dehors de la fenêtre TCP, le moteur de prévention d'intrusion pouvait ne pas ignorer cet acquittement, provoquant potentiellement un blocage sur un firewall monoprocesseur. Cette anomalie a été corrigée.

Référence support 47976

Analyse DCE/RPC

Les connexions filles générées dans une communication utilisant le protocole DCE/RPC pouvaient potentiellement se voir affecter un profil de prévention d'intrusion erroné, provoquant alors l'affichage du message « DCERPC unknown UUID ». Cette anomalie a été corrigée.

Référence support 48130

Protocole SIP

Certains types de réseaux présentant des phénomènes de latence, les paquets d'une session de voix sur IP pouvaient parfois être réémis. Ces paquets généraient alors une alarme du type « Protocole SIP invalide (no pending request) » qui interrompait la session. Ce comportement a été modifié pour que les paquets générant cette alarme soient bloqués sans interrompre la connexion.

Référence support 48047

Haute disponibilité

Dans le cas de firewalls mettant en œuvre de la Qualité de service (QoS) et utilisant un bridge, les paquets de type multicast pouvaient ne plus être reçus par le firewall lui-même. La gestion de la haute disponibilité étant basée en partie sur des paquets multicast, le fonctionnement de cette dernière pouvait alors être perturbé. Ce problème a été corrigé.

Référence support 49514 - 48929 - 48927

Alarme BYOD

L'alarme relative au blocage des flux pour les terminaux Android, IOS et Windows Phone OS était correctement notifiée mais ne bloquait cependant pas les paquets correspondants. Ce comportement a été corrigé.

VPN SSL Portail

Référence support 49950

Dans une configuration VPN SSL Portail donnant accès à un serveur applicatif, l'utilisateur se voyait présenter une erreur Java indiquant que la signature de l'applet Java était expirée; l'accès au serveur n'était alors possible qu'au moyen d'une exception concernant l'adresse IP du firewall dans la configuration Java du poste. Ce problème a été corrigé et l'accès au serveur applicatif est de nouveau possible sans modification de la configuration Java.

Interface d'administration web

Référence support 48730

VPN SSL Portail

Suite à la migration depuis une version 9.1.x vers une version 1.x d'une configuration comportant un profil utilisateur VPN SSL Portail, les serveurs accessibles pour ce profil se trouvaient alors désactivés. Ce problème est désormais résolu.

Référence support 48731

Suite à la migration d'une configuration 9.1.x vers une version 1.1.x, il n'était plus possible de créer, modifier ou supprimer un profil VPN SSL Portail comportant un caractère « espace ». Ce dysfonctionnement a été corrigé.

Référence support 49250

Tableau de bord

La fenêtre de configuration du tableau de bord laissait apparaître à tort une rubrique Matériel en lieu et place d'une rubrique Haute disponibilité. Cette anomalie a été corrigée.

Référence support 44107

Filtrage et NAT

Dans les règles de Filtrage et NAT, les colonnes de type source, destination ou port acceptent au maximum 5 objets non inclus dans un groupe. En essayant d'ajouter un sixième objet par glisser/déposer, l'icône symbolisant l'ajout d'objet pouvait alors rester fixée au curseur de la souris. Ce dysfonctionnement a été corrigé.

Global administration

Référence support 49054

Le déploiement d'une configuration de filtrage global sur un parc de firewalls en version de firmware 9.1.4.1 pouvait aboutir à un message d'erreur reportant une incompatibilité de versions. Ce problème est désormais corrigé.

Référence support 48656

Le déploiement d'objets par script NSRPC sur un nombre important d'équipements pouvait être fortement ralenti. Ceci s'expliquait par les nombreux contrôles réalisés sur les objets mis à jour et le rechargement des modules utilisant ces objets. Une nouvelle option de déploiement par script (« update=2 »), pour les objets de type machine et plage d'adresses, a été créée afin d'améliorer de manière significative ce temps de déploiement. Cette option ne gérant pas le rechargement des modules, il est donc nécessaire de prévoir ces opérations de rechargement dans le script de déploiement.

Exemple de syntaxe pour le déploiement d'un objet machine:

```
config object host new name=<hostname> [ip=<ipaddress>] [ipv6=<ipv6address>]
[type=router|server|host] [resolve=static|dynamic|manual] [mac=xx:xx:xx:xx:xx:xx]
[color=xxxxxx] [comment=<comment>] [update=<0|1|2>].
```

1.2.2 Correctifs

Réseau

Agrégation de liens et haute disponibilité
Le correctif (v.1.2.1) destiné aux firewalls NG configurés en Haute Disponibilité et utilisant des liens agrégés (LACP) a été supprimé. Il provoquait en effet un dysfonctionnement interne sur les modèles U250S, U500S, U800S, SN700 et SN900 paramétrés en Haute Disponibilité.

1.2.1 Vulnérabilités résolues

OpenVPN

Une vulnérabilité dans le composant Control Channel Packet Handler du serveur OpenVPN, pouvant entraîner une attaque de type Déni De Service (CVE-2014-8104) par un utilisateur authentifié via TLS, a été résolue par la mise à jour du serveur OpenVPN.

ClamAV

Une vulnérabilité dans le composant PE File Handler de l'antivirus ClamAV, pouvant entraîner une attaque de type Déni De Service (CVE-2014-9050), a été résolue par la mise à jour du moteur d'antivirus ClamAV.

1.2.1 Correctifs

Réseau

Agrégation de liens - Modèles NG
Dans un groupe de Firewalls configurés en Haute Disponibilité et utilisant des liens agrégés (LACP), le firewall passif pouvait émettre du trafic de contrôle LACP. Les flux à destination du cluster se trouvaient donc perturbés, car le firewall passif pouvait alors être perçu comme étant actif. Ce problème a été résolu en interdisant au membre passif du cluster d'émettre des contrôles LACP.

VPN SSL Tunnels

Référence support 48588
Le fonctionnement natif du serveur OpenVPN pouvait potentiellement entraîner l'acceptation de connexions VPN SSL Tunnel sans présentation de mot de passe. Ceci pouvait se produire lorsque les conditions suivantes étaient réunies :

- Utilisation d'un client OpenVPN standard (le logiciel Stormshield Network SSL VPN Client est non concerné car exigeant la présentation d'un mot de passe),
- Connexion à un annuaire externe Microsoft Active Directory,
- Firewall utilisant l'authentification LDAP par défaut, avec l'option des requêtes LDAP paramétrées pour s'authentifier avec le compte utilisateur directement sur l'annuaire.

La présentation d'un mot de passe est désormais rendue obligatoire pour établir une connexion depuis un client OpenVPN standard.

Interface d'administration web

Référence support 48720

Routage

Lors de l'ajout d'une route statique, les interfaces de type modem (passerelles de dialup) pouvaient ne pas apparaître dans la liste des interfaces sélectionnables. Ce problème est désormais résolu.

Système

Référence support 48717

Si l'option « passer sans analyser » était sélectionnée lorsque la collecte de données échouait (onglet Analyse des fichiers du module Protocoles > HTTP), le service pouvait s'interrompre. Ce défaut est maintenant corrigé.

1.2.0 Fonctionnalités

Prévention d'intrusion

Référence support 47619

Le moteur de prévention d'intrusion reconnaît et analyse les deux nouvelles suites de chiffrement (ChaCha20 and Poly1305) intégrées dans les serveurs Google (*.google.*) et les versions récentes du navigateur Chrome.

Deux flux Microsoft RPC (DCE/RPC) supplémentaires sont analysés par le moteur de prévention d'intrusion (module **Protocoles**). Il s'agit de Microsoft Exchange EMSMDB interface et de Microsoft Exchange Async EMSMDB interface.

Système

La connexion du firewall à un annuaire LDAP externe utilisant un schéma de groupe de type posixGroup (utilisateurs enregistrés via leur nom d'utilisateur et non via leur nom absolu DN [Distinguished Name]) est désormais possible. Le choix du type d'annuaire LDAP n'est pour le moment accessible qu'au travers des commandes CLI.

Sur les modèles haut de gamme SN6000, l'écran LCD affiche successivement un ensemble d'informations relatives au système ou à certaines fonctionnalités lorsqu'elles sont activées:

numéro de série ou nom du firewall, version de firmware de la partition principale, état de la haute disponibilité (HA), état du RAID, adresse IP de l'interface de gestion intelligente de matériel (IPMI : Intelligent Platform Management Interface).

Interface d'administration web

Afin de renforcer la sécurité des connexions à l'interface d'administration web, les suites de chiffrement basées sur l'algorithme de hachage SHA1 ne sont plus autorisées. Seules les suites basées sur l'algorithme SHA2 peuvent désormais être utilisées. En conséquence, pour certaines versions anciennes de navigateurs web (exemple : Microsoft Internet Explorer v9), il sera nécessaire d'activer le protocole TLS v1.2.

Tableau de bord

L'état des disques, des volumes RAID éventuels (firewalls haut de gamme SN3000 et SN6000) ainsi que des modules d'alimentation (firewalls haut de gamme SN3000 et SN6000) est désormais affiché dans la fenêtre *Matériel* du **Tableau de bord**.

Objets Web

Il est désormais possible d'ajouter un commentaire à chaque élément appartenant à une catégorie personnalisée d'URL, ou à une catégorie personnalisée de noms de certificats.

Protection applicative : FTP

Une option permet désormais de restreindre l'utilisation du protocole FTP à certains comptes utilisateurs, en définissant une liste d'utilisateurs autorisés et/ou une liste d'utilisateurs refusés. Cette option est disponible via l'onglet *Utilisateurs FTP* du module **Protocole FTP**.

VPN SSL Tunnels

Le port d'écoute du serveur VPN SSL Tunnels est désormais configurable (la valeur proposée par défaut reste le port TCP/443). Il est à noter que certains ports réservés (exemple : http_proxy) ne peuvent être utilisés.

Portail d'authentification

Un utilisateur authentifié via le portail du firewall peut désormais se déconnecter de ce portail sans nécessité de ressaisir ses identifiants et mot de passe, grâce à la présence d'un cookie d'authentification.

Firewalls virtuels

Le pilote réseau Ethernet des firewalls virtuels Stormshield Network (vmx) a été mis à jour, leur permettant ainsi de bénéficier de débits pouvant atteindre 10Gb/s.

Stormshield Network Real-Time Monitor

L'état des disques internes, des éventuels volumes RAID (firewalls haut de gamme SN3000 et SN6000) ainsi que des modules d'alimentation (firewalls haut de gamme SN3000 et SN6000) est désormais affiché dans le module Matériel de SN Real-Time Monitor.

1.2.0 Vulnérabilités résolues

Failles de sécurité SSL et TLS
Des vulnérabilités pouvant entraîner une attaque de type Man in the Middle (MITM) ou un Déni De Service ont été résolues par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1j.

En voici la liste :

- SRTP Memory Leak (CVE-2014-3513),
- Session Ticket Memory Leak (CVE-2014-3567),
- SSL 3.0 Fallback,
- Build option no-ssl3 is incomplete (CVE-2014-3568).

Faille de sécurité FreeBSD
Une vulnérabilité concernant le traitement de paquets TCP (FreeBSD-SA-14 :19 – Déni de service dans le traitement de paquets TCP) a été corrigée par l'application d'un correctif de sécurité FreeBSD.

1.2.0 Correctifs

Prévention d'intrusion

Référence support 47370
L'utilisation du protocole SIP, au sein d'une règle de NAT précisant le port de destination, générait une anomalie de translation d'adresses pour le champ *Contact*. Ce dysfonctionnement a été corrigé.

Référence support 47975
Dans le champ *Contact* d'un paquet SIP traversant le firewall, la présence de virgules au sein d'une chaîne de caractères pouvait ne pas être correctement interprétée par le moteur de prévention d'intrusion, empêchant ainsi le téléphone de s'enregistrer auprès d'un serveur SIP. Cette anomalie est désormais corrigée.

Référence support 45544
Le passage de flux provenant d'outils d'optimisation de réseaux étendus (WAN) conçus par **Riverbed Technology**, dans une règle de filtrage définie en mode firewall, pouvait empêcher moteur de prévention d'intrusion de fonctionner correctement du fait de la syntaxe TCP spécifique utilisée par ces équipements. Ce problème est désormais résolu.

Système

Référence support 48124 - 48316
Lorsqu'une connexion à destination d'un firewall était réalisée au travers d'un tunnel PPTP et que ce tunnel était interrompu puis rétabli, certains paquets réseau pouvaient être réémis de manière

continue, entraînant potentiellement un blocage du firewall. Ce problème est désormais corrigé.

Référence support 46864

Lorsque le fichier de configuration *language* comportait un champ **Keyboard** vide ou invalide, le menu **Système** > **Configuration** pouvait ne plus être accessible et engendrer une déconnexion de l'interface d'administration. Ce problème est désormais résolu.

Référence support 48267

Système de fichiers

Le firewall pouvait potentiellement écrire des données sur le secteur disque portant le label d'une partition. Cette partition était alors détectée par le système comme corrompue et irréparable. Ce problème a été résolu par l'adoption du système de partitionnement disque UFS (Unix File System).

Référence support 47595

Interfaces

L'assistant de création de modem sélectionnait par défaut le type de connexion « en cas de trafic (à la demande) », ce qui pouvait entraîner un dysfonctionnement du modem. Ce comportement a été modifié, et le type de connexion « permanente » est désormais le choix prédéfini.

Référence support 47494

DHCP

Sur un firewall disposant déjà d'une plage DHCP associée à une passerelle, il n'était pas possible de créer une seconde plage DHCP routée. Cette anomalie a été corrigée.

Référence support 47030

Dans le cas de configurations comportant sur une même interface protégée une plage d'adresses DHCP ainsi qu'une route statique, le serveur DHCP pouvait potentiellement ne plus respecter le plan d'adressage de cette interface, distribuant ainsi des adresses IP inadaptées. Ce problème est désormais résolu.

Référence support 47396

Dans le cas de configurations comportant un très grand nombre de réservations DHCP, le fichier de configuration généré ne pouvait être lu dans son intégralité par le serveur DHCP et ce dernier pouvait ne pas redémarrer correctement. Cette anomalie est désormais corrigée.

Référence support 46340

Lorsque des clients distants étaient connectés via PPTP, le serveur DHCP ne pouvait être redémarré, car il tentait alors d'écouter les requêtes DHCP sur l'interface virtuelle dédiée à ces tunnels PPTP. Ce problème a été résolu.

Référence support 47667

Authentification

Lorsqu'une règle d'authentification comportait plusieurs méthodes, dont l'authentification via SSO Agent, la méthode listée juste après cette dernière pouvait potentiellement ne pas être appliquée, entraînant ainsi des soucis d'authentification. Ce problème est désormais résolu.

Référence support 44621

Filtrage et NAT

Dans certaines configurations de règles de filtrage (routage sur une passerelle autre que la passerelle par défaut, utilisation de la détection automatique de protocole et champ protocole

forcé à TCP), les paquets émis par le firewall pouvaient porter une adresse IP source erronée (adresse de l'interface connectée à la passerelle par défaut). Ce problème a été corrigé.

Policy Based Routing

Certains environnements n'autorisent pas les tests de disponibilité (ping) vers les passerelles d'accès Internet (dialup). Lors de la mise en œuvre de routage vers des passerelles de dialup dans les règles de filtrage (PBR : Policy Based Routing), le mécanisme de contrôle de disponibilité pouvait considérer à tort ces passerelles comme injoignables. Ce mécanisme de détection a été amélioré afin de corriger ce problème.

Référence support 45689 - 47089 - 47940 - 48173

Lorsque des passerelles sont spécifiées dans les règles de filtrage (Policy Based Routing), leur disponibilité est systématiquement testée par un mécanisme de monitoring (message ICMP *echo request*). Dans le cas d'une configuration utilisant deux (ou plus) passerelles de dialup d'un unique Fournisseur d'Accès Internet (FAI), ce dernier présente la même adresse IP distante pour les deux équipements, ce qui n'était pas compatible avec le mécanisme de monitoring des passerelles. Ce problème est désormais résolu.

Référence support 47528

Traces

Suite à la migration de v9.1.x à v1.1.0 d'une configuration ayant activé la rotation des fichiers de traces (menu **Configuration** > **Notifications** > **Traces** - **syslog**), seul le plus ancien fichier de chaque catégorie de traces était supprimé. La taille de ces fichiers pouvant atteindre 20M en version 1.x (contre 5M en version 9.1.x), la partition réservée au stockage de ces fichiers pouvait alors être saturée. La méthode de calcul de l'espace disque nécessaire pour chaque catégorie de traces a été revue pour corriger ce problème.

Proxy SSL

L'utilisation du proxy SSL sur les Firewalls SN150 pouvait potentiellement empêcher ou altérer l'affichage de pages HTTPS. Ce problème est désormais résolu.

Référence support 47636 - 47637

Mises à jour par clé USB

Dans le cadre d'une procédure de mise à jour par clé USB, le firewall effectuait un redémarrage avant d'installer la version de firmware téléchargée depuis la clé, Si la clé USB était toujours présente suite à ce redémarrage, le firewall la détectait de nouveau et tentait de télécharger cette mise à jour une seconde fois. Afin de permettre l'éjection de la clé USB et ainsi éviter de réinstaller une mise à jour identique, ce redémarrage avait été remplacé par un arrêt. En définitive, l'installation est de nouveau précédée d'un simple redémarrage et ce problème est résolu par une détection de la version de la mise à jour présente sur la clé.

Interface d'administration web

Mises à jour

Lorsqu'une mise à jour de firmware était signalée comme disponible dans l'onglet Mise à jour du système du module Maintenance, le lien de téléchargement pouvait ne pas fonctionner. Cette anomalie est désormais corrigée.

Référence support 47384 - 47630

Lors d'une recherche de mise à jour de firmware, un message précisant "Pas d'information disponible sur les versions" pouvait s'afficher de manière inappropriée. Ce problème a été résolu.

Référence support 47344

Routage

Lors de l'ajout d'une route statique utilisant l'interface « VPN IPSec », un message d'erreur précisait que cette interface était introuvable. Cette anomalie est désormais corrigée.

Référence support 45863

Annuaire LDAP

Lorsque le champ Organisation de l'annuaire LDAP comportait des caractères « [ ] » (crochets), les utilisateurs de l'annuaire n'étaient pas visibles dans le menu Utilisateurs du firewall. Ce problème est désormais résolu.

Référence support 46722

Filtrage et NAT

Une règle de filtrage utilisant un proxy (par le biais d'inspection d'URL par exemple), et un port de destination combiné avec un opérateur de comparaison (!=, > ou <), pouvait être indiquée à tort comme invalide. Cette anomalie été corrigée.

Référence support 46523

L'utilisation dans une règle de filtrage de groupes comprenant plus de 256 objets provoquait des messages d'avertissement lors du chargement de la politique de filtrage, et le stockage de ces messages pouvait entraîner le remplissage de la partition dédiée aux traces. Ce comportement a été corrigé.

Référence support 45436

Certificats et PKI

La création de certificat pour un utilisateur ayant une adresse mail identique à celle d'un utilisateur déjà configuré dans le firewall, provoquait un message d'erreur affichant le mot de passe de la CA associée. Cette anomalie a été corrigée.

Référence support 47594 - 47714

Objets

Lorsqu'un groupe vide était créé sur un firewall utilisant exclusivement l'adressage IPv4, ce groupe ne pouvait être affiché (liste des objets réseaux) ou sélectionné au sein de l'interface d'administration (dans une règle de filtrage, par exemple). Cette anomalie a été corrigée.

Référence support 47364

Utilisateurs : Droits d'accès VPN

Suite à la migration de v9.x vers v1.1.0 d'une configuration comprenant des règles de droits d'accès VPN, il n'était plus possible d'apporter une modification à ces droits. Ce problème est désormais résolu.

Référence support 47563

VPN IPSec

L'assistant de création de politique IPSec Nomade - Mode Config ne permettait pas d'utiliser l'objet « all » dans le champ Réseau local. Ce comportement a été modifié.

Référence support 47449

Notifications

Dans le paramétrage du serveur SMTP émettant les notifications par e-mail, le champ Domaine DNS proposait la valeur netasq.com par défaut. Ce champ est désormais vide.

Référence support 47252

Le modèle des e-mails utilisé pour l'envoi de rapports d'alarmes a été modifié.

VPN SSL Tunnel

Référence support 47500

Lors de l'installation du logiciel Stormshield Network SSL VPN Client, le service Windows associé (Stormshield SSL VPN Service) était configuré en mode de démarrage manuel. Ce service est désormais installé en mode de démarrage automatique.

Référence support 47620

Un utilisateur dont le mot de passe comportait le caractère % ne pouvait pas se connecter au travers de Stormshield Network SSL VPN Client. Cette anomalie est désormais corrigée.

Référence support 47479

L'installation de Stormshield Network SSL VPN Client par un utilisateur standard via l'option d'élévation de privilèges (« installer en tant qu'administrateur ») échouait avec le message « le dossier n'existe pas ». Ce problème est désormais résolu.

Référence support 47416

Lorsqu'une erreur se produisait au cours de l'installation de Stormshield VPN SSL Client, la désinstallation de cette application ne pouvait ensuite être réalisée correctement. Ce problème est résolu.

Virtualisation VMWare

Référence support 47281

Le disque virtuel (fichier vmdk) inclus dans les images disques de firewalls (format ova) présentait un souci de compatibilité avec les dernières évolutions du logiciel de virtualisation VMware ESXi (versions 5.0 et 5.1 uniquement). Ce problème a été corrigé et de nouvelles images disques ont été publiées dans votre espace privé.

Stormshield Network SSO Agent

Lors d'un changement rapide du type de connexion d'un utilisateur authentifié (exemple : fin d'une connexion filaire relayée immédiatement par une connexion sans fil), SN SSO Agent pouvait considérer l'utilisateur comme ayant été déconnecté. Ce comportement a été corrigé.

Stormshield Network Real-Time Monitor

Référence support 47504 - 47311

L'ajout d'un firewall dans un carnet d'adresses vide rendait ce carnet inaccessible dans SN Real-Time Monitor, et provoquait l'affichage du message : « Le carnet d'adresses ne peut pas être ouvert. Le fichier n'existe pas ou vous n'avez pas les droits suffisants pour l'ouvrir ». Ce problème a été corrigé.

Stormshield Network Administration Suite

Référence support 47505

L'assistant d'installation de Stormshield Network Administration Suite présentait une URL d'enregistrement des produits erronée. Cette anomalie a été corrigée.

Référence support 47506

L'adresse e-mail de contact et le lien vers le site web Stormshield ont été modifiés dans les écrans d'accueil des applications de SN Administration Suite (SN Real-Time Monitor, SN Unified Manager et SN Event Reporter).

Stormshield Network Unified Manager

Référence support 47508

Dans le menu d'accueil de SN Unified Manager, le texte descriptif de l'option permettant de quitter l'application était tronqué. Ce défaut d'affichage a été corrigé.

Référence support 47511

L'option destinée à importer un carnet d'adresses a été supprimée du menu Fichier de l'application Stormshield Network Unified Manager.

Référence support 46840

Le menu contextuel permettant d'ajouter des outils externes ne fonctionnait pas pour les équipements autres que les firewalls (serveur, poste de travail, etc.). Ce problème est désormais résolu.

1.1.3 Correctifs

Système

Référence support 47633 - 47635

La procédure de mise à jour automatisée d'un Firewall par amorçage sur une clé USB est de nouveau fonctionnelle.

Réseau

Référence support 47548

La mise en œuvre de VLAN sur les modèles haut de gamme des Firewalls Stormshield Network (SN2000, SN3000 et SN6000) ne fonctionnait pas correctement. Ce problème est désormais résolu.

Prévention d'intrusion

Un problème de calcul de numéro de séquence TCP lors de la réécriture de données pouvait potentiellement provoquer un blocage du firewall. Cette anomalie a été corrigée.

1.1.2 Fonctionnalités

Support des modèles haut de gamme

La version 1.1.2 est désormais compatible avec l'ensemble de la gamme des Firewalls Stormshield Network, et notamment le modèle haut de gamme SN6000.

1.1.1 Correctifs

Système

Si l'option *Activer le stockage des traces* était désactivée, il n'était ensuite plus possible de la réactiver. Ce problème était dû à une erreur de détection de la partition hébergeant les traces. Cette anomalie est maintenant résolue.

Réseau

La création ou la modification d'un VLAN attaché à une seule interface (extrémité de VLAN) n'était plus possible à partir de l'interface d'administration Web depuis la version1. En effet, la sélection d'une interface était impossible, empêchant la modification de ce paramètre pour un VLAN existant ou de valider la création d'un VLAN via l'assistant. Ce problème a été corrigé.

1.1.0 Fonctionnalités

Support des modèles haut de gamme

La version 1.1.0 assure désormais le support des modèles haut de gamme des Firewalls Stormshield Network SN2000 et SN3000.

Global Administration

Déploiement

Pour les firewalls qui ont activé la Haute Disponibilité, les assistants de déploiement d'objets et de politique de filtrage proposent désormais une option permettant la synchronisation des membres du cluster à la fin du déploiement.

1.1.0 Vulnérabilités résolues

Faille de sécurité SSL et TLS

Une vulnérabilité pouvant entrainer une attaque de type Man-in-the-middle (MITM) a été résolue par la mise à jour de la bibliothèque cryptographique OpenSSL en version 1.0.1h. Cela protège d'une attaque potentielle complexe lors de la négociation TLS (CVE-2014-0224).

1.1.0 Correctifs

Interface d'administration web

Référence support 43992

Tableau de bord

Dans le cas d'un firewall disposant de disques redondants, l'état du volume RAID n'était pas correctement affiché dans la fenêtre Matériel du module **Tableau de bord** (message « Pas de RAID disponible »). Cette anomalie est désormais corrigée, et les propriétés de chaque disque appartenant à une grappe RAID sont affichées (identification du disque, appartenance au volume RAID et état du disque).

1.0.0 Fonctionnalités

VPN SSL

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée aux ressources internes de l'entreprise : partages réseaux, bases de données, applications, intranet, etc. Toutes les communications entre l'utilisateur distant et le site central sont alors encapsulées et protégés via un tunnel chiffré en SSL. Cette solution garantit donc authentification, confidentialité, intégrité et non-répudiation.

Du point de vue client, le fonctionnement du VPN SSL est similaire à celui d'un client VPN IPSec avec le mode XAUTH, mais présente l'avantage d'une configuration simplifiée. D'autre part, il utilise uniquement le port TCP 443, et offre ainsi un accès aisé depuis les réseaux avec filtrage d'accès à Internet (hôtels, wifi public, connexion 3G, etc.).

Ce mode de fonctionnement basé sur la technologie libre **Open VPN** (OpenVPN est sous licence GPL version 2), le rend accessible sur tout type de terminal (Windows, IOS, Android, etc.) via le

Client VPN SSL ou un client OpenVPN, ce qui est devenu une nécessité dans les environnements BYOD (Bring Your Own Device).

Le trafic réseau empruntant un tunnel VPN SSL bénéficie en outre des fonctionnalités avancées des Firewalls telles que l'authentification, le filtrage URL et la prévention d'intrusion.

Support IPv6

Le support d'IPv6, proposé dans cette nouvelle version, permet aux Firewalls d'être intégrés dans des infrastructures IPv4 et/ou IPv6. Les fonctions de Réseau (interfaces et routage), Filtrage, VPN et Administration sont compatibles IPv6. Ce support est optionnel et activable dans le module **Configuration**.

L'interface d'administration web est alors accessible indifféremment en IPv6 ou IPv4 car les interfaces réseau du Firewall peuvent disposer uniquement d'une adresse IPv6 fixe ou en complément d'une adresse IPv4 (*double pile*). De plus, les routes statiques et passerelles peuvent désormais être renseignées en IPv6.

Le mécanisme SLAAC (StateLess Address AutoConfiguration) est implémenté sur le Firewall afin de générer des Annonces Routeur (RA - Router Advertisements). Celles-ci permettent l'auto-configuration des machines du réseau par la distribution des préfixes IPv6 à utiliser. Ces annonces permettent également de communiquer des paramètres DNS (Support du RDNSS - RFC 6106) et de définir le Firewall comme passerelle par défaut. Ce mécanisme peut être complété par le service de serveur ou relai DCHPv6 du Firewall, pour bénéficier par exemple de la réservation d'adresses en IPv6.

Les objets réseaux (machines, réseaux et plages d'adresses IP) peuvent être adressés en IPv6, ou de manière hybride. Les politiques de filtrage sont ainsi applicables aux objets IPv6 et peuvent faire appel à l'inspection de sécurité (profils d'inspection personnalisables). En revanche, les fonctions d'inspections applicatives (Antivirus, Antispam et filtrages URL, SMTP, FTP et SSL) ne sont pas disponibles dans cette version. De même, il n'est pas possible de réaliser de la translation d'adresses (NAT) sur des objets IPv6.

NOTE

Les interfaces adressées en IPv6 et appartenant à un bridge doivent, en *Configuration avancée*, décocher l'option de routage sans analyse du protocole IPv6, afin d'autoriser le filtrage sur le trafic.

Les tunnels IPSec sont également compatibles IPv6 ; il est ainsi possible d'établir des tunnels entre deux extrémités IPv6 et d'y faire transiter indifféremment des flux IPv4 ou IPv6. Inversement, les flux IPv6 peuvent emprunter des tunnels IPSec IPv4.

Le routage dynamique Bird embarqué sur les Firewalls est également compatible IPv6.

Rapports d'activité

Traces

Les rapports d'activités vous permettent maintenant de superviser et d'exploiter les traces générées par les équipements et stockées localement. Leur consultation est facilitée par des vues de type alarmes, connexions, traces WEB, etc. Les critères de filtrage proposés en recherche avancée, permettent une analyse détaillée des traces.

Rapports d'activité

Dans la catégorie **Vulnérabilités**, 3 nouveaux rapports de type "Top 10" permettent de visualiser les vulnérabilités ayant une cible *Client* ou *Serveur*, ainsi qu'un rapport des applications les plus vulnérables.

Collaborative security

Pour une sécurité plus collaborative, à partir des rapports de vulnérabilités remontés par Vulnerability Manager, il est maintenant possible d'augmenter le niveau de protection d'une machine identifiée comme vulnérable en un clic. Ainsi, en cas de détection de vulnérabilités critiques, une nouvelle interaction vous permet d'ajouter les machines concernées à un groupe préalablement établi, et se voir attribuer un profil de protection renforcée ou des règles de filtrage spécifiques (zones de mise en quarantaine, accès limité, etc.).

Réseau

Agrégation de liens - Modèles NG

Pour des besoins de performance et de disponibilité des liens physiques, la nouvelle version introduit la fonction d'agrégation de liens LACP (Link Aggregation Control Protocol). Ainsi, plusieurs ports physiques des appliances peuvent être regroupés pour être considérés comme une unique interface en vue d'augmenter le débit par la répartition de charge ou pour servir de relais en cas de panne (redondance). Cette fonctionnalité est uniquement disponible sur les modèles SN2000, SN3000, SN6000, NG1000 et NG5000.

DHCP à travers VPN IPsec

Les utilisateurs locaux peuvent désormais bénéficier de la configuration automatique des paramètres IP d'un serveur DHCP distant au travers d'un tunnel IPsec. Pour cela, il est nécessaire de renseigner le paramètre « *Adresse IP utilisée pour relayer les requêtes DHCP* » dans les options du relai DHCP et de sélectionner l'interface IPsec dans les interfaces d'écoute.

Support TCP-MD5 pour BIRD

Support de l'authentification TCP-MD5 pour le routage dynamique BIRD permettant la protection des sessions BGP par authentification des trames dans l'entête TCP (RFC2385).

Prévention d'intrusion

Mode « FastPath »

Pour les règles avec une inspection en mode « Firewall », le trafic a été optimisé et les débits multipliés. Cette amélioration est appliquée aux flux IPv4, sans NAT et sans analyse ouvrant des connexions dynamiques (ex : FTP).

Ce mode est conseillé dans les cas de flux dédiés à la sauvegarde ou à la réplication de données, ou encore aux accès de sites VPN satellites à un Firewall principal si celui-ci analyse déjà le trafic.

Signatures multi-contexte

Cette version apporte une amélioration significative du moteur de prévention d'intrusion. Pour contrer les attaques complexes, le moteur IPS est dorénavant capable de réaliser des corrélations de signatures dans des contextes différents. Les mécanismes de protection anti-évasion ont ainsi été renforcés.

Analyse MS-RPC

Afin de sécuriser le trafic Microsoft RPC, basé sur le standard DCE/RPC, ce dernier est complétement analysé. Une nouvelle entrée du module Protocole propose d'autoriser ou non chaque flux utilisant ce protocole, détaillé par Service Microsoft (Microsoft Exchange, par exemple). Une info-bulle affiche l'UUID (Universal Unique Identifier) de chaque service au survol de celui-ci. Une liste noire permet le blocage d'un service non répertorié en renseignant son UUID.

Analyse EPMAP et inspections NetBios CIFS et NetBios SSN

Le protocole DCE/RPC pouvant être intégré aux protocoles NetBios CIFS et NetBios SSN, une nouvelle option propose son inspection. Les options du protocole EPMAP, servant à relayer les accès aux services, permet de restreindre les relais. Les ouvertures de connexions dynamiques sur EPMAP (portmapper) sont également supportées.

Adresses MAC

Les adresses MAC sources sont maintenant notifiées dans l'ensemble des traces de connexions pour les machines appartenant à un même réseau.

Services et comptes Google autorisés

Une option permet de restreindre l'accès aux services et comptes proposés par Google. En renseignant les domaines avec lesquels votre entreprise est inscrite à Google Apps, ainsi que les éventuels domaines secondaires, l'accès aux services Google sera limité à ces domaines autorisés. Cette option est disponible via le module **Protocole HTTP**.

Cloud backup

L'option « Cloud backup » est une offre de service permettant de réaliser des sauvegardes régulières de la configuration de votre Firewall de manière sécurisée. Ces sauvegardes peuvent être stockées sur un serveur local, sur un serveur hébergé par un partenaire ou au sein de l'infrastructure de services **Cloud backup Service**.

Authentification

Méthode Guest

Ce mode permet une identification sans authentification, pour l'accès à un réseau WiFi public, par exemple. Cette méthode déclenche par défaut l'affichage de conditions d'utilisation d'accès à Internet, personnalisable dans l'onglet *Portail captif*. La connexion de ces utilisateurs « invités » est notifiée dans les traces par l'ajout des adresses MAC source.

Proxy HTTP

Protocole HTTP

Une option permet d'autoriser ou non, l'usage d'adresse IP comme URL, c'est à dire l'accès à un site par son adresse IP et non par son nom de domaine. En effet, cet usage peut être un contournement du filtrage URL. Ce blocage s'appliquant après l'évaluation du filtrage, un serveur interne peut rester joignable par son adresse IP, si son accès est explicitement autorisé dans la politique de filtrage.

Proxy cache HTTP

Grâce à la mise en mémoire de ressources par le proxy-cache HTTP, les performances de navigation WEB peuvent être améliorées en cas de liaison internet à faible bande passante ou pour l'accès à un nombre de sites WEB limité. Les utilisateurs bénéficient alors de temps de réponse optimisés lors des consultations de sites WEB, permettant également un gain de bande passante.

NOTE

Cette fonctionnalité est disponible uniquement pour les modèles équipés d'un disque dur.

Elle s'applique sur les flux HTTP(S) dans la politique de Filtrage, en option de l'inspection de sécurité. Le suivi des ressources mises en mémoire et la gestion du cache peuvent être visualisés via Realtime Monitor (Tableau de Bord).

Proxy HTTP explicite

Afin de permettre une politique similaire sur un Firewall hébergé dans le Cloud et une appliance physique, le port d'écoute d'un proxy explicite HTTP peut désormais être configuré dans la politique de filtrage (*Port de destination*) ; celui-ci peut ainsi être différent du port par défaut (8080/TCP).

Pour l'élaboration d'une politique dans ce mode, consultez la Note technique « **Mode hybride Cloud Firewall - Appliance** ».

Interface d'administration web

Filtrage et NAT

Fenêtre unique d'édition de règle

Afin de faciliter la saisie des différents paramètres d'une règle de filtrage ou de NAT, une fenêtre unique s'affiche au double-clic sur la règle. Cette fenêtre permet ensuite par un menu, d'éditer les différents paramètres proposés par chaque colonne.

Statistiques d'usage des règles

Dans la politique active, chaque règle de filtrage et de NAT activée affiche un compteur d'utilisation. Au survol de l'icône, une info-bulle indique le nombre exact d'exécutions de la règle. Les 4 niveaux d'utilisations correspondent à la valeur 0, puis aux valeurs situées entre 0, 2, 20 et 100% de l'utilisation totale de la règle la plus utilisée. Pour obtenir un nouvel indicateur, un bouton « Réinitialiser les statistiques des règles » recommence une nouvelle collecte.

Commentaire

Le commentaire des nouvelles règles indique la date de création et l'utilisateur l'ayant créée si ce dernier n'est pas le compte « admin ».

Tableau de Bord : Propriétés

Une entrée vous informe de toute nouvelle mise à jour du firmware disponible. Le numéro de la version affiché comporte un lien permettant de télécharger le fichier de mise à jour. Pour l'installer, rendez-vous dans le module **Maintenance**, onglet *Mise à jour du système*.

Real Time Monitor

VPN SSL

Le module Tunnels VPN différencie maintenant par deux onglets, les tunnels montés via VPN IPsec et via VPN SSL. Le nouvel onglet *Tunnels VPN SSL* trace les communications entre l'utilisateur distant et le site central au travers de tunnels VPN SSL. Les informations disponibles sont le nom de l'utilisateur, ses adresses IP VPN et IP d'origine, la durée, les nombres de données envoyées et reçues et le port utilisé.

Proxy cache HTTP

La mise en mémoire de ressources par le proxy-cache HTTP peuvent améliorer les performances de navigation WEB en cas de liaison internet à faible bande passante ou pour l'accès à un nombre limité de sites WEB.

Le suivi des ressources mises en mémoire et leur gestion est présenté dans le **Tableau de Bord**, sous forme de 3 diagrammes. Deux indiquent le pourcentage des données mises en mémoire selon le nombre total de requêtes et leur poids total, et le troisième présente l'utilisation de la mémoire.

Collaborative security

Dans les modules **Evènements**, **Machines** et **Management des vulnérabilités**, il est maintenant possible depuis une machine affichée dans la grille, de l'enregistrer dans la base Objet réseaux, et également de l'ajouter à un groupe. Ainsi, en cas de détection de vulnérabilités critiques, cette interaction vous permet d'attribuer à ces machines, un profil de protection renforcée ou des règles de filtrage spécifiques (zones de mise en quarantaine, accès limité, etc.).

Diagrammes

L'ensemble des diagrammes intégrés aux différents modules de l'interface présentent un nouveau rendu graphique.

Précisions sur les cas d'utilisation

Support IPv6

En version 1.x, 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, entrainant des problèmes de routage en cas de bascule.

Migration

Interfaces

Lorsqu'une configuration d'origine ne contient pas toutes les interfaces Ethernet attendues, en raison d'une suppression manuelle dans le fichier de configuration réseau, ces interfaces sont recréées dans la configuration cible lors de la migration. Au cours de cette opération, le nom des interfaces recréées est celui d'origine (exemple : Ethernet2), mais ce nom n'est pas reconnu comme valide par l'interface d'administration. Ce problème peut être résolu en éditant et modifiant le nom de l'interface concernée (exemple : dmz1 en lieu et place de Ethernet2).

Système

Mises à jour

Suite à l'adoption du système de partitionnement UFS (Unix File System) depuis la version 1.2.0, le retour à une version de firmware 1.1.x ou antérieure sur un firewall en version 1.2.0 n'est pas autorisé par l'outil de mise à jour de l'interface d'administration. Pour réaliser cette opération, seule une restauration du firewall par clé USB est possible. Cette procédure est décrite dans la Note Technique « Restauration logicielle par clé USB » disponible dans votre espace sécurisé.

De plus, 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 1.x vers une version 9.1.x.

Référence support 31201

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 1.2.0, si la version courante du firewall est la 1.1.3.

Objets dynamiques

Les objets réseaux en résolution DNS automatique (dynamic), pour lesquels le serveur DNS propose un type de répartition de charge round-robin, provoque le rechargement de la configuration des modules uniquement si l'adresse actuelle n'est plus présente dans les réponses.

Surveillance matérielle (watchdog)

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

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

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 ASQ 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 basé 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 31308

Proxy SSL

Le protocole SSL (Secure Sockets Layer), devenu Transport Layer Security (TLS) en 2001, est supporté en version 3 (1996). Les sites utilisant une version antérieure (présentant des défauts de sécurité) ou ne supportant pas un début de négociation en TLS seront bloqués.

Le navigateur Internet Explorer en version 7 ou 8 n'active pas, par défaut, le support du protocole TLS 1.0. Pour des raisons de sécurité, il est donc recommandé d'activer le support de TLS 1.0 via un objet Active Directory définissant les configurations machines (group policy object ou GPO).

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 ».

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.

Réseau

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

VPN IPsec

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.

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.

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 création de plusieurs utilisateurs avec le même identifiant (« login ») est autorisée, mais n'est pas compatible avec l'authentification des utilisateurs.

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

L'identifiant de routeur des connexions n'est pas transféré au Firewall passif. En conséquence 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).

Real Time Monitor

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.

STORMSHIELD