GUIDE

STORMSHIELD MANAGEMENT CENTER

GUIDE D'ADMINISTRATION

Version 3.9.4

Dernière mise à jour du document : 30 octobre 2026

Référence : sns-fr-SMC-guide_d_administration-v3.9.4

Table des matières

1. Prendre en main le serveur SMC 9
1.1 Se connecter à l'interface web du serveur SMC 9
1.2 Se connecter à l'interface de ligne de commande 9
1.3 Installer la licence SMC 11
1.3.1 Résoudre les problèmes 11
1.4 Recommandations sur l'environnement d'utilisation 11
1.4.1 Recommandations 12
1.4.2 Configurations et mode d'utilisation des firewalls SNS soumis à l'évaluation 14
1.5 Sensibilisation des utilisateurs 17
1.5.1 Gestion des accès des administrateurs 17
1.5.2 Gestion des mots de passe de l'utilisateur 18
1.5.3 Environnement de travail 19
1.5.4 Gestion des accès d'utilisateurs 19
1.6 Avertissement avant de rattacher des firewalls SNS au serveur SMC 19

2. Rattacher des firewalls SNS au serveur SMC 21
2.1 Rattacher un firewall en configuration d'usine au serveur 21
2.1.1 Déclarer le firewall dans l'interface web du serveur SMC 21
2.1.2 Générer le package de rattachement du firewall 22
2.1.3 Installer le package de rattachement sur le firewall à partir d'une clé USB 23
2.2 Rattacher un firewall déjà en production au serveur 24
2.2.1 Déclarer le firewall dans l'interface web du serveur SMC 24
2.2.2 Générer le package de rattachement du firewall 24
2.2.3 Installer le package de rattachement sur le firewall 26
2.3 Rattacher un cluster haute disponibilité au serveur 27
2.3.1 Déclarer le cluster dans l'interface web du serveur SMC 27
2.3.2 Générer le package de rattachement du cluster 27
2.3.3 Installer le package de rattachement sur le nœud actif du cluster 28
2.4 Consulter les journaux du serveur en cas de problème 29
2.4.1 Génération du package de rattachement d'un firewall 29
2.4.2 Installation du package de rattachement sur le firewall 29
2.5 Importer des firewalls SNS depuis un fichier CSV 29
2.5.1 Créer le fichier CSV 30
2.5.2 Importer des firewalls depuis l'interface web 30
2.5.3 Importer des firewalls en ligne de commande 31
2.6 Installer un nouveau package de rattachement sur un firewall SNS 32

3. Superviser les firewalls SNS 33
3.1 Superviser et classer les firewalls 33
3.1.1 Obtenir des informations sur les firewalls 33
3.1.2 Exporter les données de supervision 34
3.1.3 Classer les firewalls par dossiers 35
3.1.4 Vérifier l'utilisation d'un firewall dans la configuration 36
3.2 Accéder à l'interface de monitoring des firewalls 37
3.3 Accéder au serveur Stormshield Log Supervisor (SLS) 37
3.3.1 Ajouter un menu d'accès au serveur SLS 37
3.3.2 Filtrer la vue SLS sur les journaux d'un firewall 38

4. Configurer les firewalls SNS 39
4.1 Modifier les paramètres des firewalls 39

4.1.1 Ajouter des propriétés personnalisées 40
4.1.2 Modifier la valeur d'une propriété personnalisée de firewall 41
4.1.3 Importer / Exporter des propriétés personnalisées de firewalls 41
4.2 Créer des variables personnalisées 43
4.2.1 Ajouter, modifier ou supprimer une variable personnalisée 44
4.2.2 Définir la valeur d'une variable personnalisée pour un firewall 44
4.3 Vérifier la cohérence de la configuration 44
4.3.1 Désactiver la vérification de la cohérence 45
4.3.2 Désactiver des domaines de vérification ou modifier le niveau de l'anomalie 45
4.3.3 Limiter le nombre d'incohérences remontées 46
4.4 Déployer une configuration sur des firewalls 46
4.4.1 Déployer une configuration sur un firewall depuis l'interface web 47
4.4.2 Déployer une configuration sur un cluster haute disponibilité 48
4.4.3 Déployer une configuration sur un firewall en ligne de commande 49
4.4.4 Activer l'avertissement de modification de la configuration 49
4.4.5 Préserver la connexion lors d'un déploiement 50
4.4.6 Consulter les journaux du serveur en cas de problème 50
4.4.7 Résoudre les problèmes 50
4.5 Compléter la configuration des firewalls par fichier CSV 51
4.5.1 Créer le fichier CSV 51
4.5.2 Importer le fichier CSV dans SMC 51
4.6 Charger et déployer une ancienne configuration 52
4.7 Générer un différentiel de configuration 52
4.8 Détecter des modifications de la configuration locale sur des firewalls 53
4.8.1 Visualiser des modifications locales sur un firewall 53
4.9 Accéder à l'interface web d'administration des firewalls 54
4.10 Utiliser le mode Urgence 54
4.11 Convertir un firewall connecté au serveur SMC en cluster haute disponibilité 55
4.12 Importer ou déclarer un certificat pour un firewall 55
4.12.1 Importer un certificat depuis l'interface web du serveur 55
4.12.2 Importer un certificat depuis l'interface de ligne de commande 56
4.12.3 Importer un certificat sur un cluster haute disponibilité 57
4.12.4 Résoudre les problèmes 57
4.12.5 Déclarer un certificat utilisé par un firewall 58
4.12.6 Modifier le certificat utilisé par défaut dans les topologies VPN 58
4.13 Utiliser SMC en tant que point de distribution Active Update 58
4.13.1 Télécharger les bases de données Active Update 59
4.13.2 Utiliser le serveur Active Update de SMC 60
4.13.3 Personnaliser les paramètres Active Update 62
4.14 Configurer l'avertissement de l'expiration proche des certificats 65
4.15 Configurer l'avertissement de l'expiration proche des options de licence 66
4.16 Désactiver la protection des certificats par TPM (Trusted Platform Module) lors de l'installation sur le firewall 66
4.16.1 Savoir si une clé privée est protégée par TPM 66
4.16.2 Désactiver la protection de la clé privée par TPM 67
4.16.3 Activer la protection par TPM d'une clé privée déjà existante 67
4.17 Choisir le caractère délimiteur dans les fichiers CSV 68

5. Gérer les objets 69
5.1 Déployer les objets sur les firewalls 69
5.2 Créer des objets variables 70
5.3 Vérifier l'utilisation d'un objet dans la configuration 71
5.4 Importer des objets 71

5.4.1 Créer le fichier CSV 72
5.4.2 Importer des objets depuis l'interface web 72
5.4.3 Importer des objets en ligne de commande 73
5.5 Exporter des objets 74
5.6 Utiliser les objets implicites depuis SMC 74
6. Configurer le réseau et le routage 75
6.1 Configurer les interfaces réseau 75
6.1.1 Activer la gestion du réseau d'un firewall SNS par SMC 75
6.1.2 Forcer la récupération des interfaces du firewall 76
6.1.3 Configurer les interfaces 76
6.1.4 Configurer les interfaces IPsec (VTI) 77
6.2 Configurer le routage 79
6.2.1 Configurer les routes depuis SMC 79
6.2.2 Forcer la récupération des routes du firewall 80
6.2.3 Exporter et importer les routes 80
6.2.4 Limitations de la configuration des routes depuis le serveur SMC 81
6.3 Superviser les objets Routeurs 82
6.4 Mettre en œuvre la fonctionnalité SD-WAN 82
6.4.1 Créer un objet SLA 83
6.4.2 Configurer la supervision des liens dans un objet Routeur 83
6.5 Résoudre les problèmes 84
6.5.1 Vous constatez des erreurs de configuration après avoir renommé une interface depuis SMC 84
7. Créer et superviser des tunnels VPN 86
7.1 Créer des topologies VPN par politique 86
7.1.1 Configurer une topologie par politique en maillage 87
7.1.2 Configurer une topologie par politique en étoile 90
7.2 Créer des topologies VPN par route 92
7.2.1 Configurer une topologie par route en maillage 93
7.2.2 Configurer une topologie par route en étoile 95
7.2.3 Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS 98
7.2.4 Définir la politique de routage du trafic 99
7.2.5 Modifier le plan d'adressage VTI 99
7.2.6 Résoudre les problèmes 101
7.3 Gérer les certificats et les autorités de certification 102
7.3.1 Ajouter une autorité de certification ou une chaîne de confiance 102
7.3.2 Mettre à jour une autorité de certification ou une chaîne de confiance 103
7.3.3 Supprimer une autorité de certification ou une chaîne de confiance 103
7.3.4 Importer ou déclarer un certificat pour un firewall 104
7.3.5 Vérifier la validité des certificats 104
7.3.6 Mettre à jour le certificat X509 d'un firewall 105
7.3.7 Renouveler le certificat d'un firewall obtenu par les protocoles SCEP ou EST 105
7.3.8 Comprendre les statuts des certificats 106
7.4 Définir l'adresse de contact des firewalls pour les topologies VPN 106
7.4.1 Définir l'adresse de contact par défaut d'un firewall 107
7.4.2 Définir l'adresse de contact d'un firewall dans une topologie VPN spécifique 107
7.5 Choisir l'interface de sortie des firewalls pour les topologies VPN 107
7.5.1 Créer l'objet Machine correspondant à l'interface 107
7.5.2 Choisir l'interface de sortie d'un firewall sur SMC 107
7.5.3 Configurer une route statique sur le firewall (facultatif) 108
7.6 Modifier, supprimer et vérifier l'utilisation d'une topologie VPN 108

7.7 Gérer la fragmentation des paquets 109
7.8 Désactiver une topologie VPN 109
7.9 Superviser l'état des tunnels VPN 110
7.10 Définir le PRF dans un profil de chiffrement personnalisé 110

8. Définir des règles de filtrage et translation (NAT) 112
8.1 Comprendre l'ordre de lecture des règles 112
8.2 Exemples de cas d'usage 113
8.2.1 Gérer un parc sans partage de règles 113
8.2.2 Gérer un parc avec des règles partagées et des règles spécifiques 113
8.2.3 Gérer un parc multi-sites avec des règles partagées et spécifiques et délégation de filtrage 114
8.2.4 Gérer un parc multi-sites avec des jeux de règles partagés 115
8.3 Créer des règles de filtrage et de translation (NAT) 116
8.4 Créer des jeux de règles 117
8.4.1 Créer un jeu de règles 117
8.4.2 Assigner des jeux de règles à un firewall 117
8.4.3 Modifier des jeux de règles pour un firewall 118
8.4.4 Importer ou exporter des jeux de règles 118
8.4.5 Supprimer un jeu de règles 118
8.5 Identifier les règles 119
8.6 Modifier l'ordre d'exécution des règles 119
8.7 Rechercher une règle dans l'interface web ou dans les journaux SNS 120
8.8 Supprimer des règles 120
8.9 Supprimer des jeux de règles 120
8.10 Importer et exporter des règles de filtrage et de translation 120
8.10.1 Importer des règles depuis un fichier CSV 121
8.10.2 Exporter des règles dans un fichier CSV 123
8.10.3 Importer les règles d'un firewall connecté 124
8.11 Migrer les règles locales existantes d'un firewall pour les gérer dans SMC 124
8.12 Gérer le filtrage d'URL sur les firewalls SNS depuis SMC 125
8.12.1 Créer la politique de filtrage d'URL modèle 125
8.12.2 Sauvegarder la politique de filtrage d'URL du firewall modèle 126
8.12.3 Diffuser la politique de filtrage URL modèle 127
8.13 Gérer les profils d'inspection IPS sur les firewalls SNS depuis SMC 128
8.13.1 Modifier les profils d'inspection IPS modèles 129
8.13.2 Sauvegarder les profils d'inspection IPS du firewall modèle 130
8.13.3 Diffuser les profils d'inspection IPS 131
8.14 Ajouter des services Web 132
8.14.1 Connaître le nom des services Web à utiliser 132
8.14.2 Ajouter les services Web sur le serveur SMC 133

9. Configurer la QoS 135
9.1 Configurer les files d'attente et les Traffic shapers 135
9.1.1 Ajouter des files d'attente et des Traffic shapers 135
9.1.2 Modifier ou supprimer des files d'attente ou des Traffic shapers 137
9.2 Configurer la QoS sur les interfaces des firewalls 137
9.2.1 Prérequis 137
9.2.2 Activer la gestion du réseau d'un firewall SNS par SMC 137
9.2.3 Configurer la QoS sur une interface 138
9.2.4 Forcer la récupération de la configuration QoS sur un firewall 138
9.3 Configurer la QoS dans les règles de filtrage 138

10. Exécuter des commandes CLI SNS sur un parc de firewalls 140
10.1 Créer le script de commandes CLI 140
10.2 Utiliser des variables 141
10.2.1 Utiliser les variables spécifiques aux firewalls 141
10.2.2 Utiliser les variables globales 142
10.2.3 Utiliser un fichier CSV 142
10.3 Exécuter le script CLI SNS depuis l'interface web 142
10.4 Exécuter le script CLI SNS en ligne de commande 143
10.4.1 Afficher la liste des commandes et des options 143
10.4.2 Exécuter un script 144
10.4.3 Ajouter des scripts 144
10.4.4 Supprimer des scripts 145
10.4.5 Afficher la liste des scripts 145
10.4.6 Exemple d'utilisation de script en ligne de commande avec un fichier CSV 145
10.5 Exécuter le script CLI SNS sur un cluster haute disponibilité 146
10.6 Joindre des fichiers à un script et réceptionner des fichiers générés par script 146
10.6.1 Arguments de commande à utiliser dans le script 147
10.6.2 Joindre un fichier à un script 147
10.6.3 Réceptionner un fichier généré par script 148
10.7 Programmer l'exécution d'un script CLI SNS 149
10.7.1 Programmer l'exécution d'un script depuis l'interface web 149
10.7.2 Programmer l'exécution d'un script en ligne de commande 150
10.8 Mettre à jour les firewalls en utilisant les scripts CLI SNS 150
10.9 Résoudre les problèmes 151
10.9.1 Le fichier de script est trop volumineux 151
10.9.2 Certains caractères ne sont pas pris en compte dans le script 152
10.9.3 L'exécution du script échoue sur certains firewalls 152
10.9.4 Il n'est pas possible d'exécuter un script 152

11. Maintenir les firewalls SNS 153
11.1 Sauvegarder la configuration des firewalls 153
11.1.1 Sauvegarder automatiquement la configuration du serveur et des firewalls 153
11.1.2 Sauvegarder manuellement la configuration des firewalls 154
11.1.3 Exclure les clés privées de la sauvegarde automatique des firewalls 154
11.2 Mettre à jour les firewalls 155
11.3 Remplacer un firewall SNS dans le cadre d'un RMA 156

12. Supprimer des firewalls SNS du serveur SMC 158

13. Gérer et maintenir le serveur SMC 159
13.1 Définir les interfaces réseau du serveur SMC 159
13.2 Vérifier la version du serveur SMC en ligne de commande 159
13.3 Modifier le fuseau horaire et la date du serveur SMC 159
13.3.1 Modifier le fuseau horaire 159
13.3.2 Modifier la date manuellement 160
13.3.3 Modifier la date via le protocole NTP 160
13.3.4 Afficher un résumé complet des paramètres date/heure du serveur SMC 160
13.4 Gérer les administrateurs locaux et provenant d'annuaires externes 160
13.4.1 Gérer les droits des administrateurs en tant que super administrateur 162
13.4.2 Gérer les administrateurs locaux 163
13.4.3 Gérer les utilisateurs LDAP 165
13.4.4 Gérer les utilisateurs Radius 169
13.4.5 Restreindre les droits d'accès des administrateurs de dossiers 172

13.4.6 Résoudre les problèmes ... 176
13.5 Consulter les journaux du serveur SMC ... 176
13.6 Envoyer les journaux de SMC vers un serveur distant au format Syslog ... 177
13.6.1 Envoyer les journaux vers un serveur distant sans chiffrement ... 177
13.6.2 Envoyer les journaux vers un serveur distant avec chiffrement ... 177
13.6.3 Désactiver l'envoi des journaux vers un serveur distant ... 177
13.6.4 Résoudre les problèmes ... 178
13.7 Sauvegarder et restaurer la configuration du serveur SMC ... 178
13.7.1 Sauvegarder la configuration du serveur depuis l'interface web ... 179
13.7.2 Sauvegarder la configuration du serveur en ligne de commande ... 179
13.7.3 Restaurer la configuration du serveur depuis l'interface web ... 179
13.7.4 Restaurer la configuration du serveur en ligne de commande ... 180
13.7.5 Restaurer la configuration du serveur depuis l'assistant d'initialisation ... 180
13.8 Générer un rapport de diagnostic du serveur ... 181
13.8.1 Télécharger le rapport depuis l'interface web ... 181
13.8.2 Télécharger le rapport en ligne de commande ... 181
13.9 Mettre à jour le serveur SMC ... 181
13.9.1 Mettre à jour le serveur SMC depuis l'interface web ... 182
13.9.2 Mettre à jour le serveur SMC en ligne de commande ... 182
13.10 Désactiver la synchronisation automatique d'un cluster haute disponibilité ... 182
13.11 Superviser SMC avec le protocole SNMP ... 182
13.11.1 Utiliser le service SNMP ... 183
13.11.2 Utiliser les MIBs ... 183
13.12 Personnaliser le certificat de l'interface web du serveur SMC ... 184
13.12.1 Personnaliser le certificat ... 184
13.12.2 Réinitialiser le certificat ... 184
13.13 Réinitialiser l'autorité de certification interne du serveur SMC ... 184
13.14 Utiliser le mode "Diffusion Restreinte" sur les firewalls SNS ... 185
13.14.1 Activer le contrôle de cohérence du mode "Diffusion Restreinte" ... 185
13.14.2 Activer le mode "Diffusion Restreinte" sur SMC et les firewalls ... 186
13.14.3 Désactiver le mode "Diffusion Restreinte" sur SMC et les firewalls ... 187
13.15 Ajouter un texte de décharge de responsabilité sur la page de connexion (disclaimer) ... 187
13.16 Se connecter à l'interface de ligne de commande via des clés SSH ... 187

14. Activer et gérer l'API publique de SMC ... 189
14.1 Activer l'API publique ... 189
14.2 Autoriser les administrateurs à créer et révoquer des clés API ... 190
14.3 Modifier la politique globale des clés API ... 190
14.4 Créer des clés API ... 191
14.5 Révoquer des clés API ... 192
14.6 Personnaliser le port d'écoute de l'API publique ... 192

15. Pour aller plus loin ... 193

Annexe A. Détails des commandes smc-xxx ... 194

Annexe B. Détails des variables d'environnement SMC_XXX ... 196

Annexe C. Compatibilité SMC/firewalls SNS ... 201

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

1. Prendre en main le serveur SMC

Pour administrer ou maintenir le serveur SMC, vous pouvez vous connecter à l'interface web via un navigateur web ou bien directement en ligne de commande.

SMC dispose également d'une API REST publique. Par défaut, elle n'est pas activée et seul le super administrateur peut l'activer. Pour plus d'informations sur l'API publique de SMC, reportez-vous à la section Activer et gérer l'API publique de SMC.

En cas de perte de mot de passe, reportez-vous à la section Gérer les administrateurs locaux et provenant d'annuaires externes et au *Guide d'installation SMC*.

1.1 Se connecter à l'interface web du serveur SMC

1. Connectez-vous à l'adresse IP du serveur SMC précédée de https:// depuis l'un des navigateurs web suivants :
    - Microsoft Edge, dernière version stable,
    - Google Chrome, dernière version stable,
    - Mozilla Firefox, dernière version stable.
2. Renseignez votre identifiant et mot de passe ou utilisez l'identifiant et mot de passe de l'administrateur par défaut. Les identifiants et mots de passe peuvent provenir de serveurs d'authentification LDAP ou Radius.
   Si vous faites quatre erreurs successives, vous devrez attendre une minute avant de pouvoir vous identifier de nouveau. Si vous tentez de vous identifier une cinquième fois avant que la minute ne s'écoule, le temps d'attente est rallongé d'une minute supplémentaire et peut ainsi augmenter jusqu'à 10 minutes.

Vous pouvez définir plusieurs administrateurs de l'interface web du serveur SMC avec des droits d'accès en lecture/écriture ou en lecture seule. Pour plus d'informations, reportez-vous à la section Gérer les administrateurs locaux et provenant d'annuaires externes.

Le serveur SMC autorise :

- Un nombre illimité de connexions en lecture/écriture sur le serveur SMC,
- Pour chaque firewall, une seule connexion directe via SMC en lecture/écriture,
- Pour chaque firewall, un nombre illimité de connexions directes via SMC en lecture seule.

NOTE
Nous vous recommandons de personnaliser le certificat de l'interface web du serveur SMC. Pour plus d'informations, reportez-vous à la section Personnaliser le certificat de l'interface web du serveur SMC.

1.2 Se connecter à l'interface de ligne de commande

Certaines opérations avancées ou de maintenance sur le serveur ne sont disponibles qu'en ligne de commande. Connectez-vous au serveur SMC en ligne de commande afin de réaliser ces opérations. Vous pouvez vous connecter :

- En console depuis votre hyperviseur,
- En SSH sur le port 22.

Dans les deux cas, connectez-vous :

- avec l'utilisateur "root" et le mot de passe définis lors de l'initialisation du serveur. Pour plus d'informations, reportez-vous au *Guide d'installation Stormshield Management Center*.
- avec vos identifiants d'administrateur si vous possédez les droits d'accès en console et/ou en SSH.

Dans le cas de la connexion en SSH, si vous vous trompez d'identifiants cinq fois successivement, vous devrez attendre 15 minutes avant de pouvoir vous identifier de nouveau.

Pour vous connecter en SSH de façon transparente, vous pouvez également configurer l'authentification via clés SSH. Pour plus d'informations, reportez-vous à la section **Se connecter à l'interface de ligne de commande via des clés SSH**.

Pour le détail des commandes utilisables pour administrer SMC, reportez-vous à la section **Détails des commandes smc-xxx**.

L'utilisateur par défaut "admin" n'a pas accès à SMC en console ou en SSH. Il ne peut accéder à SMC que via l'interface web.

1.3 Installer la licence SMC

Votre licence détermine le nombre maximum de firewalls pouvant se connecter simultanément au serveur SMC.

Un cluster de firewalls SNS Haute Disponibilité ne consomme qu'une seule licence.

Pour installer la licence :

1. Allez dans **Serveur SMC** > **Licence**.
2. Sélectionnez le fichier de licence. Si une licence est déjà installée, ses informations sont affichées.
3. Cliquez sur **Appliquer**.

1.3.1 Résoudre les problèmes

Le serveur SMC refuse toute nouvelle connexion de firewall

- *Situation* : Le serveur SMC refuse toute nouvelle connexion de firewall mais il conserve les connexions en cours.
- *Cause* : Vous ne possédez pas de licence ou celle-ci est expirée ; ou bien vous avez atteint le nombre maximum de firewalls pouvant se connecter au serveur d'après votre licence.
- *Solution* : Consultez les logs du serveur puis contactez votre centre de support Stormshield pour l'obtention d'une licence valide. Une info-bulle vous donne également une indication, ainsi que la colonne **Dernière activité**.

Votre licence n'est plus valide après une restauration de sauvegarde de configuration

- *Situation* : Vous avez effectué une restauration de configuration du serveur SMC et votre licence n'est plus valide.
- *Cause* : Lors d'une restauration de configuration, la licence qui était installée au moment de la sauvegarde est restaurée. Donc, si celle-ci a expiré entre temps, vous ne possédez plus de licence valide.
- *Solution* : Une fois la restauration de configuration effectuée, installez de nouveau votre licence la plus récente.

1.4 Recommandations sur l'environnement d'utilisation

L'installation d'un firewall SNS et d'un serveur SMC s'inscrit dans la mise en place d'une politique de sécurité globale. Pour garantir une protection optimale de vos biens, ressources ou informations, il ne s'agit pas uniquement d'installer le firewall entre votre réseau et l'Internet ou d'installer un serveur SMC pour vous aider à les configurer correctement. En effet, la plupart du temps, les attaques viennent de l'intérieur (accident, personne mécontente de son travail, personne licenciée ayant gardé un accès interne, etc.).

Cette page liste des recommandations de sécurité pour l'utilisation des firewalls SNS et d'un serveur SMC.

IMPORTANT

- Consultez régulièrement les bulletins de sécurité Stormshield sur https://advisories.stormshield.eu et les dernières informations sur la sécurité des produits Stormshield sur https://security.stormshield.eu/.
- Appliquez systématiquement les mises à jour qui corrigent des failles de sécurité sur vos produits Stormshield. Ces mises à jour sont disponibles sur https://mystormshield.eu.

1.4.1 Recommandations

Mesures de sécurité physiques

Les firewalls SNS et le serveur SMC doivent être installés et stockés conformément à l'état de l'art concernant les dispositifs de sécurité sensibles : local à accès protégé, câbles blindés en paire torsadée, étiquetage des câbles, etc.

Mesures de sécurité organisationnelles

Super administrateur

Un rôle administrateur particulier, le super administrateur, présente les caractéristiques suivantes :

- Il est le seul à être habilité à se connecter via la console locale sur les firewalls SNS, et ce uniquement lors de l'installation du firewall SNS ou pour des opérations de maintenance, en dehors de l'exploitation,
- Il est chargé de la définition des profils des autres administrateurs,
- Tous les accès dans les locaux où sont stockés les firewalls SNS et le serveur SMC se font sous sa surveillance, que l'accès soit motivé par des interventions sur le firewall SNS ou sur d'autres équipements. Toutes les interventions se font sous la responsabilité du super administrateur.

IMPORTANT
Le mot de passe par défaut du super administrateur doit être modifié lors de la première utilisation du firewall SNS.

Mot de passe

Les mots de passe des utilisateurs et des administrateurs doivent être choisis de façon à retarder toutes les attaques visant à les casser, via une politique de création et de contrôle de ceux-ci (mélange alphanumérique, longueur minimum, ajout de caractères spéciaux, pas de mots des dictionnaires usuels, etc.).

Les administrateurs peuvent modifier leur mot de passe dans l'interface d'administration web :

- Des firewalls SNS dans **Configuration > Système > Administrateur**, onglet **Compte Admin**,
- Du serveur SMC dans **Maintenance > Serveur SMC > Administrateurs**.

Les administrateurs sont sensibilisés à ces bonnes pratiques de par leur fonction et il est de leur responsabilité de sensibiliser tous les utilisateurs à ces bonnes pratiques (voir la section suivante Sensibilisation des utilisateurs).

Bonne politique de contrôle des flux d'informations

La politique de contrôle des flux d'informations à mettre en œuvre est définie, pour tous les équipements des réseaux dits "de confiance" à protéger, de manière :

- **Complète** : les cas d'utilisation standards des équipements ont tous été envisagés lors de la définition des règles et leurs limites autorisées ont été définies,
- **Stricte** : seuls les cas d'utilisation nécessaires des équipements sont autorisés,
- **Correcte** : les règles ne présentent pas de contradiction,
- **Non-ambigüe** : l'énoncé des règles fournit tous les éléments pertinents pour un paramétrage direct du firewall SNS par un administrateur compétent.

Clés cryptographiques

Les clés cryptographiques générées en dehors du firewall SNS et importées sur ce dernier doivent avoir été générées conformément aux recommandations du référentiel général de sécurité (RGS) de l'*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI).

Agents humains

Les administrateurs sont des personnes non hostiles et compétentes, disposant des moyens nécessaires à l'accomplissement de leurs tâches. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité. Leurs compétences et leur organisation impliquent que :

- Différents administrateurs avec les mêmes droits ne mènent pas des actions d'administration qui se contredisent (modifications incohérentes des politiques de contrôle des flux d'information),
- L'exploitation des journaux et des alarmes dans des délais appropriés.

Environnement de sécurité TI (Technologies de l'Information)

Firewalls SNS

Les firewalls SNS sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle des flux d'information. Ils sont dimensionnés en fonction des capacités des équipements adjacents ou alors ces derniers réalisent des fonctions de limitation du nombre de paquets par seconde, positionnées légèrement en deçà des capacités maximales de traitement de chaque firewall SNS installé dans l'architecture réseau.

À part l'application des fonctions de sécurité, les firewalls SNS ne fournissent pas de service réseau autre que le routage et la translation d'adresse (pas de DHCP, DNS, PKI, proxies applicatifs, etc.). Les firewalls SNS ne sont pas configurés pour retransmettre les flux IPX, Netbios, AppleTalk, PPPoE ou IPv6.

Les firewalls SNS ne dépendent pas de services externes en ligne (comme DNS, DHCP, RADIUS, etc.) pour l'application de la politique de contrôle des flux d'information.

L'environnement de sécurité TI fournit :

- Des horodatages NTP fiables,
- Un état à jour de la révocation d'un certificat X.509 pour les correspondants et les administrateurs,
- Un service d'enrôlement fiable.

Serveur SMC

Une politique de contrôle des flux d'informations doit être appliquée au serveur SMC afin de permettre uniquement à ses administrateurs et aux firewalls SNS administrés de s'y connecter.

La machine virtuelle doit être correctement dimensionnée (RAM, CPU, disque) afin de permettre l'administration des firewalls SNS gérés par le logiciel. Le système d'exploitation du serveur

SMC ne doit en aucun cas être modifié afin de répondre à des besoins en dehors desquels il a été conçu.

La bande passante disponible entre le serveur SMC et les firewalls SNS doit être suffisante et disponible en permanence afin de réaliser toutes les opérations d'administration. L'administrateur devra configurer voire désactiver certaines fonctionnalités afin de répondre à ce besoin, ou bien devra limiter le nombre de paquets par seconde afin de prioriser les flux d'administration.

La production et la distribution des packages de rattachement, permettant aux firewalls SNS d'être administrés par le serveur SMC, doivent être gérées et confiées à des personnes ayant été sensibilisées à la sécurité. Ces packages ne doivent transiter entre le serveur SMC et les firewalls SNS que via des moyens sécurisés (e-mails chiffrés, clés USB sécurisées, etc.).

Interconnectivité

Les stations d'administration à distance sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées. Elles sont installées dans des locaux à accès protégé et sont exclusivement dédiées à l'administration des firewalls SNS, du serveur SMC et au stockage des sauvegardes.

Les équipements réseau avec lesquels le firewall SNS établit des tunnels VPN sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des firewalls SNS.

Les postes sur lesquels s'exécutent les clients VPN des utilisateurs autorisés sont soumis à des contraintes de contrôle d'accès physique, de protection et de maîtrise de leur configuration équivalentes à celles des postes clients des réseaux de confiance. Ils sont sécurisés et maintenus à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications hébergées.

1.4.2 Configurations et mode d'utilisation des firewalls SNS soumis à l'évaluation

Le mode d'utilisation soumis à l'évaluation présente les caractéristiques suivantes :

- Le cadre de l'évaluation comprend la suite logicielle Stormshield UTM / NG-Firewall installée sur l'ensemble des versions de firewalls Stormshield, allant du SN210 au SN6100, ainsi que les modèles industriels SNi20 et SNi40. Certains modèles ne disposent pas d'un support de stockage conséquent pour les logs et doivent émettre les événements par syslog,
- Les firewalls SNS doivent être stockés dans un local à accès sécurisé. Ces mesures, ainsi que les procédures organisationnelles de l'environnement d'exploitation, doivent garantir que les seuls accès physiques aux firewalls SNS se font sous la surveillance du super-administrateur,
- La console locale n'est pas utilisée en exploitation. Seul le super-administrateur peut s'y connecter, et, par hypothèse, ce genre d'intervention ne se fait que lorsqu'une sortie du cadre de l'exploitation – pour procéder à une maintenance ou à une ré-installation – est décidée,
- Les stations sur lesquelles s'exécutent l'interface Web d'administration sont sécurisées, dédiées à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent,
- Le logiciel Stormshield Network IPsec VPN Client est hors du cadre de l'évaluation. L'utilisateur peut utiliser le client VPN IPsec de son choix ; cependant, ces postes clients doivent être sécurisés avec un niveau de rigueur équivalent à celui des stations d'administration à distance,

- Tout service externe utilisé par le firewall SNS sera hors du cadre de l'évaluation. Néanmoins, ces services doivent être dédiés à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent. Sont considérés comme services externes :
  - Les serveurs de temps NTP,
  - Le serveur d'administration LDAP et le serveur d'annuaire des utilisateurs IPsec,
  - Le serveur Syslog,
  - Le serveur CRL ou OCSP,
  - Le serveur SMC,
  - Le serveur d'enrôlement de certificats EST.
- Les paramétrages usine (défaut) doivent être conservés pour ces modules :
  - CRL : celles-ci sont téléchargées périodiquement depuis un serveur CRL,
  - Horloge interne : synchronisée périodiquement avec des serveurs NTP,
  - Services d'administration NSRPC (port TCP 1300) : limités à la loopback,
  - Fonctionnalité de routage IPv6 : bien que supportée, la fonctionnalité IPv6 est désactivée par défaut et doit le rester pour la durée de l'évaluation,
  - Fenêtres d'anti-rejeu ESP, ré-authentification IKE et PFS (Perfect Forward Secrecy) d'IKE : activés,
  - Durées de vie maximales des SA : 24 heures pour les SA d'IKE et 4 heures pour les SA d'IPsec.
- La certification ne concerne que ces fonctionnalités d'analyse applicative :
  - FTP sur TCP,
  - HTTP sur TCP (extensions WebDAV incluses),
  - SIP sur TCP ou UDP,
  - SMTP sur TCP,
  - DNS sur TCP ou UDP.

  Et ces protocoles industriels :
  - OPC UA sur TCP,
  - MODBUS sur TCP.

  D'autres protocoles ne doivent pas être utilisés dans la configuration de production.
- Les paramètres suivants ne doivent pas être utilisés dans une politique de filtrage dans le but d'associer une règle de filtrage avec :
  - Une inspection applicative (proxies HTTP, SMTP, POP3 et FTP),
  - Une programmation horaire (objet temps),
  - L'action "déchiffrer" (proxy SSL),
  - La réputation d'une machine,
  - Un objet FQDN en source ou en destination (services DNS externes requis).

- Les fonctionnalités suivantes peuvent être utilisées, mais ne sont pas considérées comme des fonctions de sécurité :
  - Translation d'adresses (network address translation ou NAT),
  - Qualité de service,
  - Haute disponibilité,
  - Rapports intégrés,
  - Filtrage par géolocalisation et par réputation d'adresse IP,
  - Filtrage par adresse MAC (couche Ethernet),
  - Active Update.
- Le mode d'utilisation soumis à l'évaluation exclut le fait que le firewall SNS s'appuie sur d'autres services que ceux évoqués auparavant. Les modules que Stormshield fournit en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester. Il s'agit précisément :
  - Des modules permettant la prise en charge des serveurs externes (Kerberos, RADIUS, ...),
  - Du module de routage dynamique,
  - Du module de routage statique multicast,
  - De l'infrastructure à clés publiques (PKI) interne,
  - Du module VPN SSL (Portail et Tunnel) ,
  - Du cache DNS,
  - Des moteurs antivirus,
  - Des serveurs SSH, DHCP, MPD et SNMPD,
  - Du client DHCP,
  - Du relai DHCP,
  - De la connexion Wi-Fi pour les périphériques équipés,
  - De la réputation de machine,
  - Sur les modèles SNi40 et SNi20 : des capacités des composants bypass,
  - De toute signature IPS personnalisée,
  - Des objets FQDN (services DNS externes requis),
  - Des messages IPFIX,
  - De la télémétrie,
  - De Breachfighter (Sandboxing),
  - Du Network Vulnerability Manager (SNVM).

  Les outils d'administration et de supervision fournissent un moyen de vérifier, à tout moment lors de l'exploitation, que ces modules sont bien désactivés.

- Les algorithmes cryptographiques d'IKE et d'IPsec mis en œuvre doivent être :

	Standard IPsec	IPsec DR
Identification	Clé pré-partagée ou certificat avec une clé RSA ou ECDSA (1)	Certificat avec une clé ECDSA ou ECSDSA (2) (3)
Authentification/Intégrité	SHA-2 en 256, 384 ou 512 bits	SHA-2 en 256 bits
Négociation de clé	Groupes Diffie-Hellman 14, 15, 16, 17, 18, 19, 20, 21, 28, 29, 30 (4)	Groupe Diffie-Hellman 28
Chiffrement	AES en 128, 192 ou 256 bits en mode CBC, CTR ou GCM	AES en 256 bits en mode GCM ou CTR

(1) : La taille minimale d'une clé RSA doit être de 2048 bits, ou de 3072 bits pour une utilisation au delà de l'année 2030.
(2) : La taille minimale d'une clé doit être de 256 bits.
(3) : Bien que l'usage de RSA soit prohibé dans un environnement DR, un certificat racine RSA peut être utilisé pour signer un certificat intermédiaire, dédié à IPsec par exemple, à partir du moment où l'autorité de certification utilisée comme ancre de confiance sur le firewall est le certificat intermédiaire.
(4) : Pour une utilisation au delà de l'année 2030, le groupe minimal à utiliser doit être le groupe Diffie-Hellman 15.

Ces algorithmes cryptographiques sont nécessaires pour la conformité au Référentiel général de sécurité (RGS) défini par l'ANSSI.

Notez bien que les recommandations sur la mise en œuvre du mode IPsec renforcé, appelé *Diffusion Restreinte (DR)*, en conformité avec le référentiel de l'ANSSI à propos de l'IPsec DR, sont détaillées dans la Note technique SNS "IPsec - mode *Diffusion Restreinte*".

1.5 Sensibilisation des utilisateurs

1.5.1 Gestion des accès des administrateurs

L'administrateur de l'appliance firewall-VPN ou du serveur SMC est responsable de la formation des utilisateurs quant à la sécurité du réseau, des équipements qui le composent et des informations qui y transitent.

En effet, la plupart des utilisateurs d'un réseau sont néophytes en informatique et à fortiori en sécurité des réseaux. Il incombe donc à l'administrateur ou au responsable de la sécurité du réseau de mettre en place des sessions de formation ou tout du moins des campagnes de sensibilisation à la sécurité des réseaux.

Lors de ces sessions, il est important d'insister sur la gestion des mots de passe de l'utilisateur et de son environnement de travail et la gestion de leurs accès aux ressources de l'entreprise, comme indiqué dans la section suivante.

Première connexion au boîtier ou au serveur SMC

La première connexion au boîtier ou au serveur SMC nécessite une procédure de sécurisation si celle-ci s'effectue au travers d'un réseau qui ne soit pas de confiance. Cette opération n'est pas nécessaire si la station d'administration est branchée directement au produit.

L'accès au portail d'administration est sécurisé via le protocole SSL/TLS. Cette protection permet d'authentifier le portail via un certificat, assurant ainsi à l'administrateur qu'il est bien connecté au boîtier désiré ou au serveur SMC désiré. Ce certificat peut être le certificat par défaut du boîtier ou celui renseigné dans sa configuration (*Authentification* > *Portail captif*).

Pour le serveur SMC, reportez-vous à la section Personnaliser le certificat de l'interface web du serveur SMC pour remplacer le certificat par défaut.

1.5.2 Gestion des mots de passe de l'utilisateur

Au cours de l'évolution des technologies de l'information, de nombreux mécanismes d'authentification ont été inventés et mis en place afin de garantir une meilleure sécurité des systèmes d'information des entreprises. Cette multiplication des mécanismes a entraîné une complexité qui contribue aujourd'hui à détériorer la sécurité des réseaux d'entreprises.

Les utilisateurs (néophytes et non formés) choisissent des mots de passe "simplistes", tirés généralement de leur vie courante et la plupart du temps correspondant à un mot contenu dans un dictionnaire. Ces comportements entraînent, bien entendu, une dégradation notable de sécurité du système d'information.

Il faut prendre conscience que l'attaque par dictionnaire est un "outil" plus que performant. Une étude de 1993 montre déjà cet état de fait. La référence de cette étude est la suivante : (http://www.klein.com/dvk/publications/). Ce qui est le plus frappant dans cette étude est sûrement le tableau présenté ci-dessous (basé sur un mot de passe de 8 caractères) :

Type de mot de passe	**Nombre de caractères**	**Nombre de mots de passe**	**Temps de Cracking**
Lexique anglais 8 caract. et +	spécial	250000	< 1 seconde
casse minuscule uniquement	26	208827064576	9 heures
casse minuscule + 1 majuscule	26/spécial	1670616516608	3 jours
minuscules et majuscules	52	53459728531456	96 jours
Lettres + chiffres	62	218340105584896	1 an
Caractères imprimables	95	6634204312890620	30 ans
Jeu de caractères ASCII 7 bits	128	72057594037927900	350 ans

On peut citer aussi un état de fait qui tend à se résorber mais qui est encore d'actualité : les fameux post-its collés à l'arrière des claviers.

L'administrateur doit mettre en place des actions (formation, sensibilisation, ...) dans le but de modifier et de corriger ces "habitudes".

EXEMPLE

- Incitez vos utilisateurs à choisir des mots de passe de longueur supérieure à 7 caractères,
- Demandez-leur d'utiliser des chiffres et des majuscules,
- De changer souvent de mots de passe,
- Et surtout de ne noter en aucun cas le mot de passe qu'ils auront finalement choisi.

L'une des méthodes classiques pour trouver un bon mot de passe est de choisir une phrase que l'on connaît par cœur (vers d'une poésie, parole d'une chanson) et d'en tirer les premières lettres de chaque mot. Cette suite de caractères peut alors être utilisée comme mot de passe.

EXEMPLE
" **S**tormshield **N**etwork, **1**er **c**onstructeur **f**rançais **d**e **b**oîtiers **F**IREWALL **e**t **V**PN…"
Le mot de passe pourrait être le suivant : **SN1cfdbFeV**.

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) propose à ce titre un ensemble de recommandations permettant de définir des mots de passe suffisamment robustes.

1.5.3 Environnement de travail

L'espace de travail est souvent un lieu de passage, un croisement pour de nombreuses personnes internes et extérieures à l'entreprise. Il s'agit donc de sensibiliser les utilisateurs au fait que certaines personnes (fournisseurs, clients, ouvriers, …) peuvent accéder à leur espace de travail et de ce fait recueillir des informations sur l'activité de l'entreprise.

Il est important de faire prendre conscience à l'utilisateur qu'il ne faut pas qu'il divulgue son mot de passe aussi bien par téléphone que par Email (social engineering) et qu'il faut qu'il tape son mot de passe à l'abri des regards indiscrets.

1.5.4 Gestion des accès d'utilisateurs

Pour compléter cette section sur la sensibilisation des utilisateurs à la sécurité des réseaux, l'administrateur doit aborder la gestion des accès utilisateur. En effet le mécanisme d'authentification d'un appliance firewall-VPN Stormshield Network ou d'un serveur SMC (comme beaucoup d'autres systèmes) basé sur un système de login/mot de passe n'implique pas forcément de déloguage à la fermeture de l'application à l'origine de cette authentification (crédit de temps d'authentification). Cet état de fait n'est pas forcément évident pour l'utilisateur néophyte. Ainsi, bien qu'il ait fermé l'application en question, l'utilisateur (qui pense ne plus être connecté) reste authentifié. S'il quitte son poste une personne malintentionnée peut alors usurper son identité et accéder aux informations contenues dans l'application.

Enfin incitez les utilisateurs à verrouiller leurs sessions lorsqu'ils se déplacent et laissent leur poste de travail sans surveillance. Cette tâche qui se révèle parfois fastidieuse peut être facilitée par des mécanismes d'authentification qui automatisent le verrouillage (token USB par exemple).

1.6 Avertissement avant de rattacher des firewalls SNS au serveur SMC

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

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

Ceci comprend :

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

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

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

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

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

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

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

2. Rattacher des firewalls SNS au serveur SMC

Le rattachement du firewall au serveur SMC vous permet d'administrer le firewall depuis l'interface web du serveur SMC. Un package de rattachement généré par le serveur SMC doit être installé sur le firewall.

IMPORTANT
Un package permet de rattacher un seul firewall à SMC, il ne doit pas être réutilisé.

Le serveur SMC 3.9.4 est compatible avec la version 4.3 minimum de Stormshield Network Security. Pour le détail, reportez-vous à la section Compatibilité SMC/firewalls SNS.

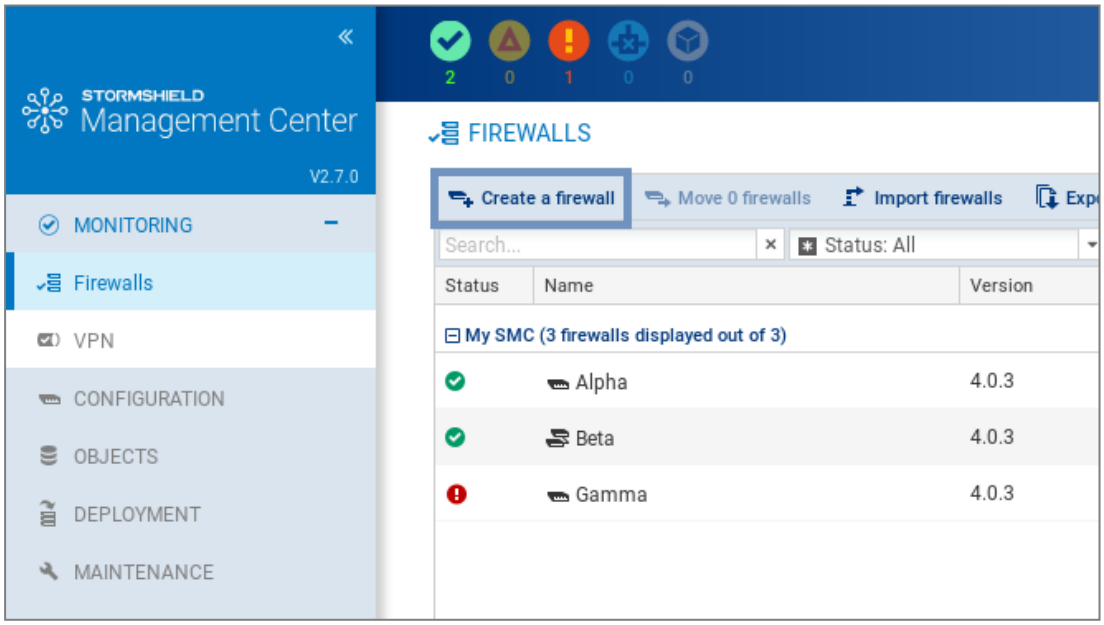
2.1 Rattacher un firewall en configuration d'usine au serveur

Les trois étapes suivantes sont nécessaires pour rattacher un firewall en configuration d'usine au serveur SMC :

1. Déclarer le firewall dans l'interface web du serveur SMC,
2. Générer le package de rattachement du firewall,
3. Installer le package de rattachement sur le firewall.

2.1.1 Déclarer le firewall dans l'interface web du serveur SMC

1. Dans l'interface web du serveur SMC, sélectionnez **Supervision** > **Firewalls** et cliquez sur **Créer un firewall**.



2. Complétez les propriétés du firewall. Les champs **Description** et **Lieu** sont remplis à titre informatif et n'ont aucune incidence sur la configuration.
3. Pour plus d'informations sur l'adresse de contact VPN, reportez-vous à la section Définir l'adresse de contact des firewalls pour les topologies VPN.
4. Pour plus d'informations sur l'interface de sortie VPN, reportez-vous à la section Choisir l'interface de sortie des firewalls pour les topologies VPN.

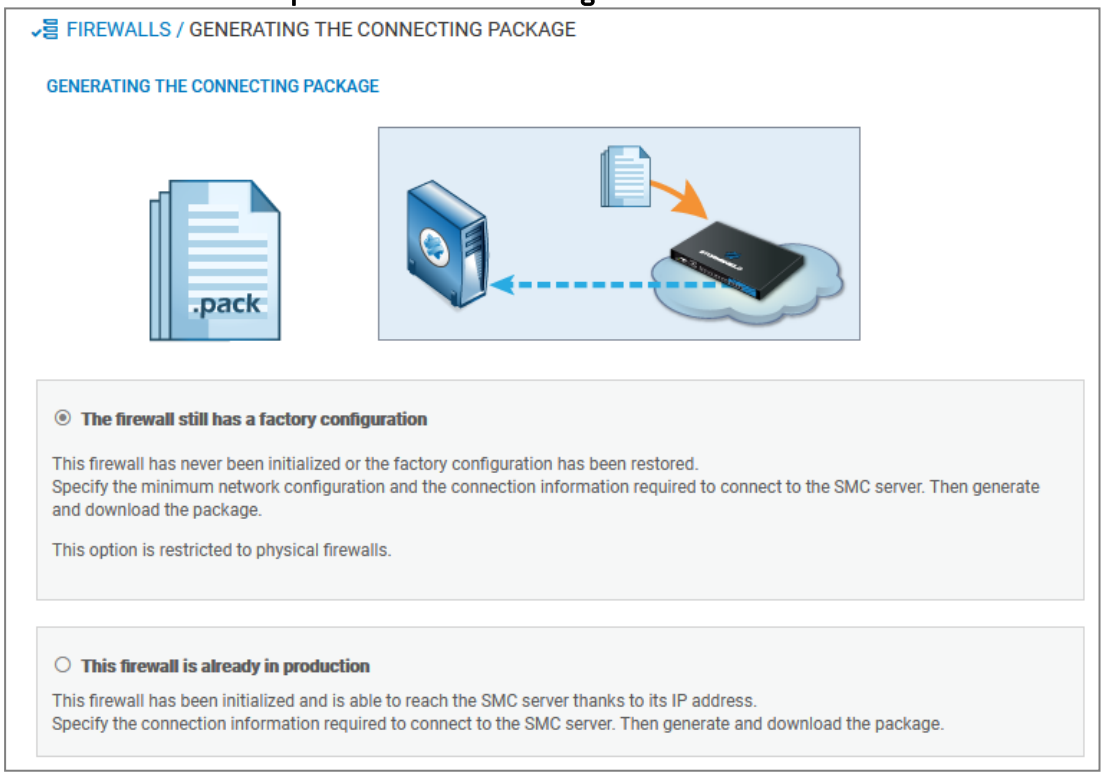
5. Choisissez le dossier dans lequel classer le firewall. Les dossiers sont créés dans le menu de gauche **Configuration** > **Firewalls et dossiers**. Pour plus d'informations, reportez-vous à la section Classer les firewalls par dossiers. Vous devez posséder le droit d'accès en écriture sur le dossier. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

2.1.2 Générer le package de rattachement du firewall

1. Dans la même fenêtre, cochez **Générer le package de rattachement** afin de générer le package de rattachement au serveur simultanément. Ce package de rattachement devra être installé sur le firewall afin de se connecter au serveur SMC.

> **ASTUCE**
> Vous pourrez générer le package plus tard en modifiant le firewall dans le menu **Firewalls**.

2. Cliquez sur **Créer**.
3. Dans le panneau **Génération du package de rattachement**, cliquez sur **Suivant** puis sélectionnez **Ce firewall possède encore sa configuration d'usine**.



4. Sur le panneau suivant, choisissez la version du firewall et renseignez les informations sur la configuration réseau minimale du firewall permettant d'accéder au serveur SMC.

5. Complétez les informations pour la connexion au serveur SMC. Selon la version du firewall, le panneau change. Pour les versions 3.9.0 et supérieures :
   - **Adresse IP ou FQDN** : le firewall se connecte à ces adresses pour contacter le serveur SMC. En fonction de la topologie de réseau, celles-ci peuvent être soit les adresses IP du serveur SMC, soit des adresses IP externes joignables par le firewall et redirigées vers le serveur SMC par le biais d'une translation de destination. Vous pouvez définir jusqu'à dix adresses ou FQDN du serveur SMC à contacter, par ordre de priorité. Le firewall parcourt les adresses de 1 à 10 et se connecte au serveur SMC avec la première adresse accessible. Si l'adresse actuellement utilisée n'est pas la plus prioritaire, le firewall tente régulièrement de joindre une adresse plus prioritaire.
   - **Port** : en fonction de la topologie de réseau, ceux-ci peuvent être soit les ports du serveur SMC (1754 par défaut) soit des ports externes joignables par le firewall et redirigés vers le port du serveur SMC par le biais d'une translation de destination.
   - **Adresse locale** : vous pouvez spécifier une interface de sortie différente pour chaque adresse de contact.
   - Pour les firewalls en version 3.7.X à 3.8.X, vous ne pouvez spécifier qu'une seule interface de sortie, globale à toutes les adresses de contact.
6. Cliquez sur **Générer et télécharger**.

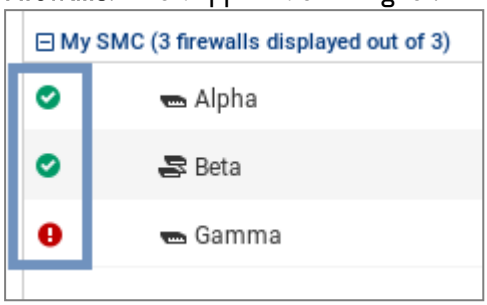
2.1.3 Installer le package de rattachement sur le firewall à partir d'une clé USB

IMPORTANT
Un package permet de rattacher un seul firewall à SMC, il ne doit pas être réutilisé.

IMPORTANT
Le package de rattachement permet l'ouverture d'un flux du firewall vers le serveur SMC. Ne fournissez ce package qu'à des personnes ayant été sensibilisées à la sécurité. Ce package ne doit transiter entre le serveur SMC et le firewall SNS que via des moyens sécurisés (e-mails chiffrés, clés USB sécurisées, etc.).

1. Fournissez le package à l'administrateur responsable du déploiement du nouveau firewall sur le site distant.
2. Assurez-vous que l'administrateur :
   - copie le package de rattachement (*.pack*) et un fichier de mise à jour SNS (*.maj*) sur une clé USB vierge. Le format de la clé doit être FAT32, FAT16 ou UFS. La version 2.3.0 minimum de SNS est requise.
   - branche la clé USB sur le nouveau firewall et connecte l'interface OUT au réseau.
   - démarre le firewall. Le firewall installe d'abord le fichier de mise à jour de SNS et redémarre. Après le démarrage, le firewall installe le package de rattachement : les adresses IP du serveur SMC et de l'interface OUT du firewall sont configurées et le firewall se connecte au serveur SMC.

3. Dans l'interface web du serveur SMC, vérifiez que l'état du firewall change dans le menu **Firewalls**. Il doit apparaître "En ligne".



4. Pour assurer la sécurité de votre équipement, connectez-vous directement à l'interface d'administration du firewall en cliquant sur l'icône et changez le mot de passe d'administration du firewall. Pour plus d'informations sur l'accès direct à l'interface du firewall, reportez-vous à la section Accéder à l'interface web d'administration des firewalls.

ASTUCE
L'administrateur du firewall peut visualiser les paramètres de connexion au serveur SMC sur l'interface web d'administration du firewall : dans le composant de tableau de bord SMC et dans le menu **Configuration** > **Système** > **Management Center**. Il peut également installer un nouveau package de rattachement de l'interface web d'administration.

2.2 Rattacher un firewall déjà en production au serveur

Les trois étapes suivantes sont nécessaires pour rattacher un firewall déjà en production au serveur SMC :

1. Déclarer le firewall dans l'interface web du serveur SMC,
2. Générer le package de rattachement du firewall,
3. Installer le package de rattachement sur le firewall.

2.2.1 Déclarer le firewall dans l'interface web du serveur SMC

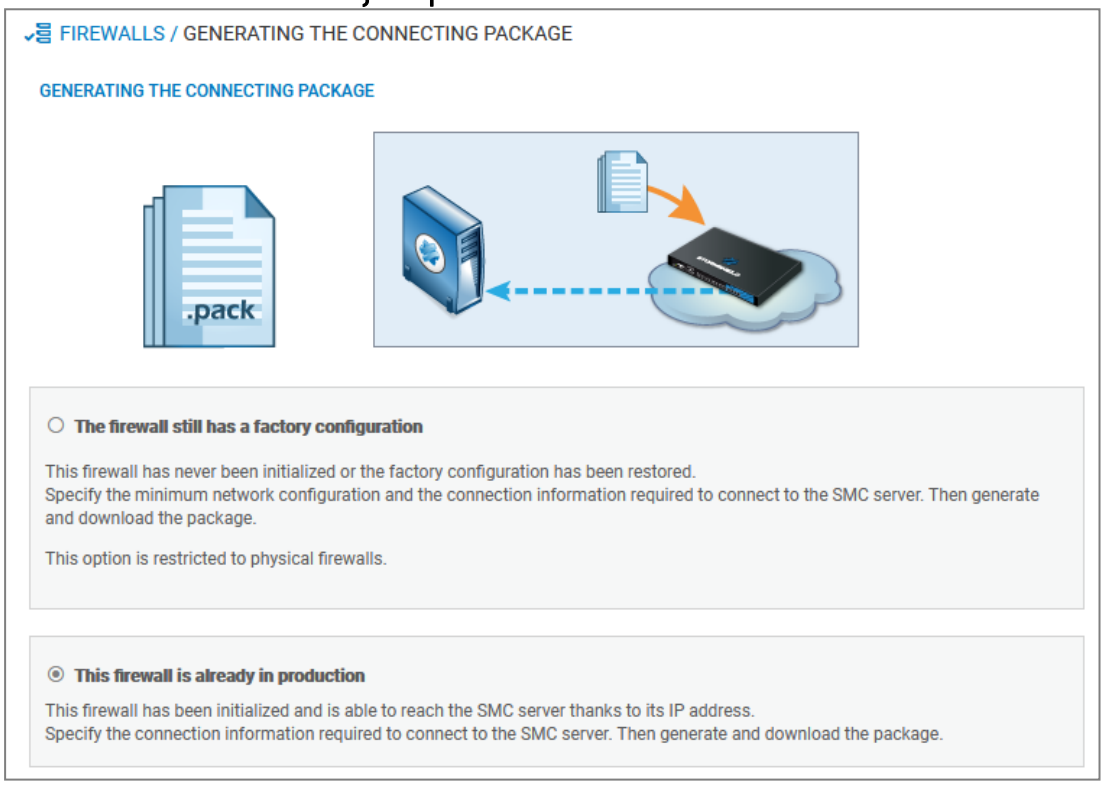
1. Dans l'interface web du serveur SMC, sélectionnez **Supervision** > **Firewalls** et cliquez sur **Créer un firewall**.
2. Complétez les propriétés du firewall. Les champs **Description** et **Lieu** sont remplis à titre informatif et n'ont aucune incidence sur la configuration.
3. Pour plus d'informations sur l'adresse de contact VPN, reportez-vous à la section Définir l'adresse de contact des firewalls pour les topologies VPN.
4. Pour plus d'informations sur l'interface de sortie VPN, reportez-vous à la section Choisir l'interface de sortie des firewalls pour les topologies VPN.
5. Choisissez le dossier dans lequel classer le firewall. Les dossiers sont créés dans le menu de gauche **Configuration** > **Firewalls et dossiers**. Pour plus d'informations, reportez-vous à la section Classer les firewalls par dossiers. Vous devez posséder le droit d'accès en écriture sur le dossier. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

2.2.2 Générer le package de rattachement du firewall

1. Dans la même fenêtre, cochez **Générer le package de rattachement** afin de générer le package de rattachement au serveur simultanément. Ce package de rattachement devra être installé sur le firewall afin de se connecter au serveur SMC.

> **ASTUCE**
> Vous pourrez générer le package plus tard en modifiant le firewall dans le menu **Firewalls**.

2. Cliquez sur **Créer**.
3. Dans le panneau **Génération du package de rattachement**, cliquez sur **Suivant** puis sélectionnez **Ce firewall est déjà en production**.



4. Sur le panneau suivant, choisissez la version du firewall. Vérifiez et modifiez le cas échéant les informations pour la connexion au serveur SMC. Selon la version du firewall, le panneau change. Pour les versions 3.9.0 et supérieures :
   - **Adresse IP ou FQDN** : le firewall se connecte à ces adresses pour contacter le serveur SMC. En fonction de la topologie de réseau, celles-ci peuvent être soit les adresses IP du serveur SMC, soit des adresses IP externes joignables par le firewall et redirigées vers le serveur SMC par le biais d'une translation de destination. Vous pouvez définir jusqu'à dix adresses ou FQDN du serveur SMC à contacter, par ordre de priorité. Le firewall parcourt les adresses de 1 à 10 et se connecte au serveur SMC avec la première adresse accessible. Si l'adresse actuellement utilisée n'est pas la plus prioritaire, le firewall tente régulièrement de joindre une adresse plus prioritaire.
   - **Port** : en fonction de la topologie de réseau, ceux-ci peuvent être soit les ports du serveur SMC (1754 par défaut) soit des ports externes joignables par le firewall et redirigés vers le port du serveur SMC par le biais d'une translation de destination.
   - **Adresse locale** : vous pouvez spécifier une interface de sortie différente pour chaque adresse de contact.
   - Pour les firewalls en version 3.7.X à 3.8.X, vous ne pouvez spécifier qu'une seule interface de sortie, globale à toutes les adresses de contact.
5. Cliquez sur **Générer et télécharger**.

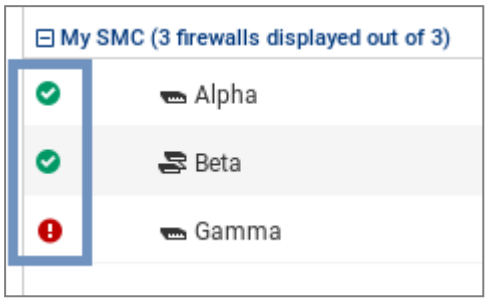
2.2.3 Installer le package de rattachement sur le firewall

IMPORTANT
Un package permet de rattacher un seul firewall à SMC, il ne doit pas être réutilisé.

IMPORTANT
Le package de rattachement permet l'ouverture d'un flux du firewall vers le serveur SMC. Ne fournissez ce package qu'à des personnes ayant été sensibilisées à la sécurité. Ce package ne doit transiter entre le serveur SMC et le firewall SNS que via des moyens sécurisés (e-mails chiffrés, clés USB sécurisées, etc.).

1. Fournissez le package à l'administrateur en charge du firewall sur le site distant.
2. Assurez-vous que l'administrateur se connecte à l'interface web du firewall.
3. Dans le menu **Configuration** > **Système** > **Management Center** de l'interface d'administration du firewall, assurez-vous que l'administrateur sélectionne le package de rattachement. Après l'installation du package, l'administrateur peut visualiser les paramètres de connexion au serveur SMC dans le même menu. Le composant de tableau de bord SMC rappelle également ces informations.

4. Dans l'interface web du serveur SMC, vérifiez que l'état du firewall change dans le menu **Firewalls**. Il doit apparaître "En ligne".



2.3 Rattacher un cluster haute disponibilité au serveur

Les trois étapes suivantes sont nécessaires pour rattacher un cluster haute disponibilité au serveur SMC :

1. Déclarer le cluster dans l'interface web du serveur SMC,
2. Générer le package de rattachement du cluster,
3. Installer le package de rattachement sur le nœud actif du cluster.

2.3.1 Déclarer le cluster dans l'interface web du serveur SMC

1. Dans l'interface web du serveur SMC, sélectionnez **Supervision** > **Firewalls** et cliquez sur **Créer un firewall**. Ce nouveau firewall représente le cluster, il n'est pas nécessaire de déclarer les deux nœuds du cluster.
2. Complétez les propriétés du cluster. Les champs **Nom du firewall**, **Description** et **Lieu** sont remplis à titre informatif et n'ont aucune incidence sur la configuration.
3. Pour plus d'informations sur l'adresse de contact VPN, reportez-vous à la section Définir l'adresse de contact des firewalls pour les topologies VPN.
4. Pour plus d'informations sur l'interface de sortie VPN, reportez-vous à la section Choisir l'interface de sortie des firewalls pour les topologies VPN.
5. Choisissez le dossier dans lequel classer le cluster. Les dossiers sont créés dans le menu de gauche **Configuration** > **Firewalls et dossiers**. Pour plus d'informations, reportez-vous à la section Classer les firewalls par dossiers. Vous devez posséder le droit d'accès en écriture sur le dossier. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

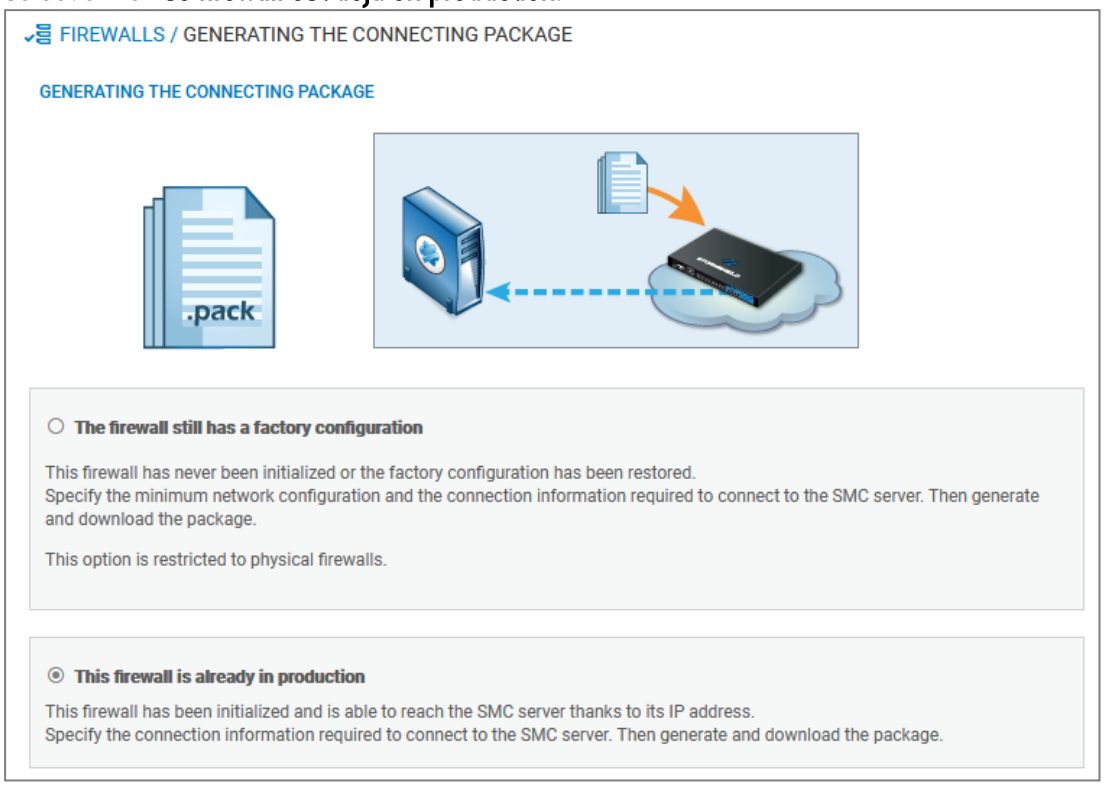
2.3.2 Générer le package de rattachement du cluster

1. Dans la même fenêtre, cochez **Générer le package de rattachement** afin de générer le package de rattachement au serveur simultanément. Ce package de rattachement devra être installé sur le firewall afin de se connecter au serveur SMC.

> **ASTUCE**
> Vous pourrez générer le package plus tard en modifiant le firewall dans le menu **Firewalls**.

2. Cliquez sur **Créer**.

3. Dans le panneau **Génération du package de rattachement**, cliquez sur **Suivant** puis sélectionnez **Ce firewall est déjà en production**.



4. Sur le panneau suivant, choisissez la version du firewall. Vérifiez et modifiez le cas échéant les informations pour la connexion au serveur SMC. Selon la version du firewall, le panneau change. Pour les versions 3.9.0 et supérieures :
   - **Adresse IP ou FQDN** : le firewall se connecte à ces adresses pour contacter le serveur SMC. En fonction de la topologie de réseau, celles-ci peuvent être soit les adresses IP du serveur SMC, soit des adresses IP externes joignables par le firewall et redirigées vers le serveur SMC par le biais d'une translation de destination. Vous pouvez définir jusqu'à dix adresses ou FQDN du serveur SMC à contacter, par ordre de priorité. Le firewall parcourt les adresses de 1 à 10 et se connecte au serveur SMC avec la première adresse accessible. Si l'adresse actuellement utilisée n'est pas la plus prioritaire, le firewall tente régulièrement de joindre une adresse plus prioritaire.
   - **Port** : en fonction de la topologie de réseau, ceux-ci peuvent être soit les ports du serveur SMC (1754 par défaut) soit des ports externes joignables par le firewall et redirigés vers le port du serveur SMC par le biais d'une translation de destination.
   - **Adresse locale** : vous pouvez spécifier une interface de sortie différente pour chaque adresse de contact.
   - Pour les firewalls en version 3.7.X à 3.8.X, vous ne pouvez spécifier qu'une seule interface de sortie, globale à toutes les adresses de contact.
5. Cliquez sur **Générer et télécharger**.

2.3.3 Installer le package de rattachement sur le nœud actif du cluster

> **IMPORTANT**
> Un package permet de rattacher un seul firewall à SMC, il ne doit pas être réutilisé.

IMPORTANT
Le package de rattachement permet l'ouverture d'un flux du firewall vers le serveur SMC. Ne fournissez ce package qu'à des personnes ayant été sensibilisées à la sécurité. Ce package ne doit transiter entre le serveur SMC et le firewall SNS que via des moyens sécurisés (e-mails chiffrés, clés USB sécurisées, etc.).

1. Fournissez le package à l'administrateur en charge du cluster sur le site distant.
2. Assurez-vous que l'administrateur :
   - se connecte à l'interface d'administration du nœud actif du cluster.
   - sélectionne le package de rattachement dans le menu **Configuration** > **Système** > **Management Center** de l'interface d'administration du firewall. Après l'installation du package, l'administrateur peut visualiser les paramètres de connexion au serveur SMC dans le même menu. Le composant de tableau de bord SMC rappelle également ces informations.
   - réalise une synchronisation des deux nœuds depuis l'interface d'administration du nœud actif. Le nœud passif récupère alors la configuration contenue dans le package de rattachement du firewall.
3. Dans l'interface web du serveur SMC, vérifiez que l'état du cluster change dans le menu **Firewalls**. Il doit apparaître "En ligne". L'icône Mode change également : .
   En cas de bascule, le nœud passif devient actif et se connecte automatiquement au serveur SMC.
4. Pour visualiser les différentes informations sur les deux nœuds du cluster, double-cliquez sur la ligne du cluster dans le menu **Firewalls** et ouvrez l'onglet **Haute disponibilité**.

Le serveur SMC opère une synchronisation régulière des deux nœuds des clusters haute disponibilité de firewalls qu'il administre. Pour désactiver cette synchronisation automatique, reportez-vous à la section Désactiver la synchronisation automatique d'un cluster haute disponibilité.

2.4 Consulter les journaux du serveur en cas de problème

Si vous rencontrez des problèmes lors du rattachement d'un firewall au serveur SMC, commencez par consulter les fichiers de journaux suivants.

2.4.1 Génération du package de rattachement d'un firewall

Consultez les journaux sur le serveur SMC, dans */data/log/fwadmin-server/server.log*

2.4.2 Installation du package de rattachement sur le firewall

Consultez les journaux sur le firewall, dans */log/l_system* (et */log/verbose.cad* si le mode verbose est activé).

2.5 Importer des firewalls SNS depuis un fichier CSV

Pour importer rapidement un grand nombre de firewalls dans SMC et générer leur package de rattachement, vous pouvez créer un fichier CSV et l'importer sur le serveur depuis l'interface web ou depuis l'interface de ligne de commande.

Vous devez être administrateur général pour réaliser cette opération, c'est-à-dire posséder le droit d'écriture sur tous les dossiers dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

2.5.1 Créer le fichier CSV

Un exemple de fichier CSV "example-import-firewalls.csv" est disponible sur le serveur, dans le dossier */opt/stormshield/examples/csv/*.

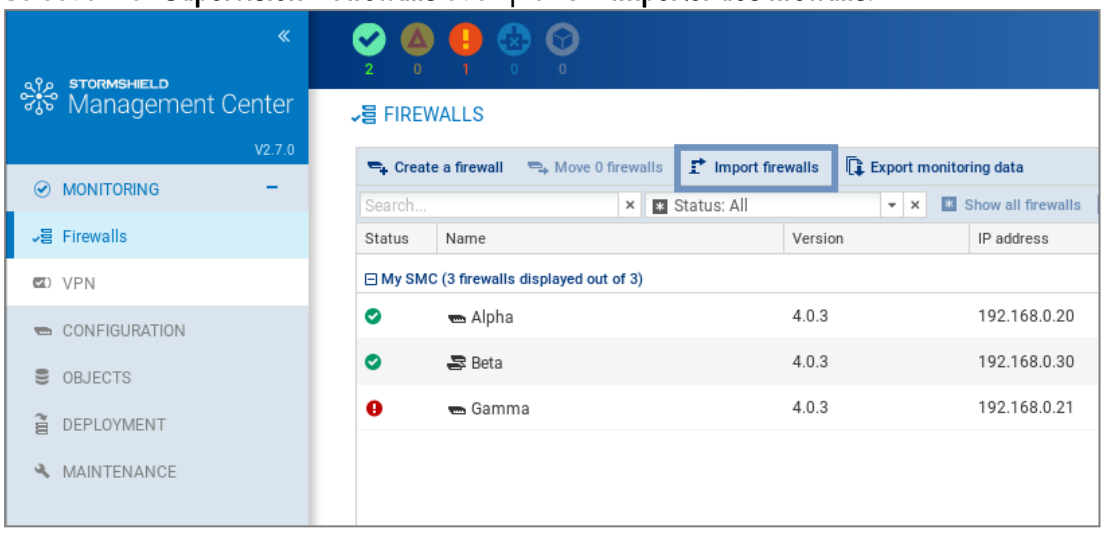
Le fichier peut contenir les paramètres suivants organisés en colonnes, séparés par des virgules. L'ordre des colonnes n'a pas d'importance. Seule la valeur de la première colonne #fwname est obligatoire, les autres colonnes peuvent être vides :

- #fwname : le nom du firewall,
- #fwversion : la version du firewall utilisée pour déterminer la version du package de rattachement généré. Si ce champ n'est pas renseigné, c'est la version 4.0.0 qui est utilisée.
- #fwdesc : la description du firewall,
- #fwplace : le lieu du firewall,
- #folder : le dossier de destination du firewall. Il est possible de spécifier un chemin sous forme <dossier1>/<dossier2>/... pour préciser le dossier de destination au sein de la hiérarchie des dossiers. Si les dossiers spécifiés n'existent pas déjà, le serveur SMC les crée. Si ce champ n'est pas renseigné, le dossier par défaut est le dossier racine.
- #vpn_fw_public_ip_address : l'adresse IP de contact du firewall déterminée manuellement dans ses paramètres et utilisée dans les topologies VPN,
- #vpn_fw_local_address : l'interface de sortie du firewall utilisée comme source dans les tunnels VPN,
- #network_cfg_deploy : définit si les interfaces réseau et le routage sont administrables via le serveur SMC. Si ce champ n'est pas renseigné, l'option est désactivée par défaut.
- #pkg_fw_address : l'adresse de contact du firewall détectée par SMC,
- #pkg_fw_netmask : le masque de sous-réseau,
- #pkg_fw_gateway : la passerelle par défaut du firewall,
- #pkg_smc_addresses (IP1:PORT1:BINDADDR1,IP2:PORT2) : l'adresse IP, le port et l'interface de sortie du serveur SMC. Cette information est nécessaire pour le package de rattachement. Le port et l'interface de sortie sont optionnels. À partir de la version 3.9 des firewalls SNS, vous pouvez spécifier une interface de sortie par adresse IP. Pour les firewalls en versions 3.7.X à 3.8.X, seule la première interface de sortie est prise en compte.
- vpn_fw_subject_dn : dans le cas de certificats obtenus par les protocoles SCEP ou EST, le Distinguished Name du sujet du certificat par défaut du firewall,
- vpn_fw_issuer_dn : dans le cas de certificats obtenus par les protocoles SCEP ou EST, le Distinguished Name de l'émetteur du certificat par défaut du firewall.

IMPORTANT
Vérifiez que le logiciel d'édition du fichier CSV n'a pas modifié le caractère délimiteur ",". L'import sur le serveur SMC risque de ne pas être possible sinon. Pour plus d'informations sur le caractère délimiteur, reportez-vous à la section Choisir le caractère délimiteur dans les fichiers CSV.

2.5.2 Importer des firewalls depuis l'interface web

1. Sélectionnez **Supervision** > **Firewalls** et cliquez sur **Importer des firewalls**.



2. Sélectionnez le fichier CSV.
3. Cochez les options nécessaires.
4. La fenêtre suivante affiche un résumé des opérations et permet de télécharger les packages de rattachement si vous avez coché l'option.

Si parmi les firewalls listés dans le fichier, certains existent déjà sur SMC, leurs propriétés sont mises à jour avec les nouvelles valeurs renseignées dans le fichier. Si une cellule du fichier est vide, la valeur est considérée comme vide et l'ancienne valeur est écrasée.

Si vous souhaitez conserver une valeur existante, supprimez la colonne dans le fichier CSV.

2.5.3 Importer des firewalls en ligne de commande

IMPORTANT
Lorsque plusieurs administrateurs sont connectés simultanément, nous vous recommandons d'importer des firewalls depuis l'interface web plutôt qu'en ligne de commande, pour que les différents administrateurs soient prévenus des modifications.

1. Commencez par copier le fichier CSV sur le serveur SMC à l'aide du protocole SSH, dans le répertoire */data/tmp* par exemple. Cet exemple est repris dans la suite de la procédure.
2. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
3. Tapez la commande :
   `smc-import-firewalls /data/tmp/nomfichier.csv`.

Pour changer la valeur du caractère délimiteur, utilisez la variable d'environnement SMC_CSV_DELIMITER. Pour plus d'informations, reportez-vous à la section Choisir le caractère délimiteur dans les fichiers CSV.

Les packages de rattachement générés sont disponibles dans le répertoire */tmp/import-firewalls-[date de l'import]*.

Un statut d'import s'affiche pour chaque firewall, ainsi qu'un résumé à la fin de l'exécution de l'import.

```
[root@smc] - {~} > smc-import-firewalls /opt/stormshield/examples/csv/example-import-firewalls.csv

S U M M A R Y
Firewalls created successfully : 9
Firewalls updated successfully : 0
Firewalls ignored : 0

Firewalls package created successfully : 9
Firewalls package creation failure : 0

Packages have been generated in : /tmp/import-firewalls-2021-02-26_11-28-17
```

Vous avez également la possibilité :

- D'importer les firewalls sans générer les packages de rattachement, en utilisant l'option `--firewall-only` :

```
smc-import-firewalls /data/tmp/nomfichier.csv --firewall-only
```

- De générer uniquement les packages de rattachement, en utilisant l'option `--package-only` :

```
smc-import-firewalls /data/tmp/nomfichier.csv --package-only
```

Si un firewall importé existait déjà dans SMC, il est automatiquement mis à jour après l'exécution du script.

2.6 Installer un nouveau package de rattachement sur un firewall SNS

Lorsqu'un firewall SNS est déjà rattaché à SMC, si vous souhaitez remplacer le package de rattachement, procédez comme suit. Cette procédure s'applique aux versions de SNS à partir de la 5.0.2.

Assurez-vous auparavant qu'aucun déploiement de configuration, de script CLI SNS ou qu'aucune mise à jour de SMC n'est en cours d'exécution.

1. Depuis SMC, générez un nouveau package de rattachement depuis le menu **Système** > **Configuration** du firewall.
2. Sur le firewall, exécutez la commande CLI `CONFIG RESTORE list=fwadmin < /tmp/mon_fichier.pack` en fournissant le package (*.pack*).

3. Superviser les firewalls SNS

Les différentes informations à propos de chaque firewall affichées dans **Supervision** > **Firewalls** permettent de visualiser et superviser les firewalls. Un accès direct aux journaux et rapports d'activité d'un firewall est également possible ainsi qu'à votre serveur Stormshield Log Supervisor (SLS) si vous en possédez un.

ASTUCE
Cliquez sur le logo Stormshield dans le bandeau supérieur pour revenir sur l'écran de supervision des firewalls.

3.1 Superviser et classer les firewalls

Consultez en temps réel l'état de votre parc et classez vos firewalls selon une hiérarchie de dossiers et sous-dossiers sur lesquels s'appliquent des règles de filtrage et de translation partagées ou spécifiques.

3.1.1 Obtenir des informations sur les firewalls

Depuis le menu **Supervision** > **Firewalls**, visualisez des informations diverses sur chaque firewall telles que l'état de santé, l'adresse IP, le modèle, le numéro de déploiement, la date de fin de maintenance, les options de licence souscrites, etc.

Dans cette vue de supervision, certaines colonnes sont masquées par défaut. Pour afficher une colonne :

1. Survolez n'importe quel titre de colonne avec la souris,
2. Cliquez sur la flèche noire qui s'affiche,
3. Survolez le menu **Colonnes**,
4. Cochez les colonnes qui vous intéressent.

Depuis ce menu, vous pouvez également modifier la configuration, accéder à l'interface web d'administration et aux journaux et rapports d'activité d'un firewall, importer un certificat sur un firewall, vérifier l'utilisation d'un firewall et supprimer un firewall de la liste.

Cinq icônes différentes indiquent l'état de santé des firewalls dans la première colonne de la liste :

- : le firewall est opérationnel,
- : le firewall rencontre un problème non critique,
- : le firewall rencontre un problème critique,
- : le firewall a été déconnecté,
- : le firewall n'a jamais été connecté au serveur SMC.

Passez la souris sur les icônes pour afficher une info-bulle indiquant le détail de l'état de santé de chaque firewall. Pour plus d'informations sur les indicateurs de santé, reportez-vous à la section *Indicateurs de santé* du *Manuel Utilisateur SNS*.

Pour filtrer la liste des firewalls par état de santé :

- Cliquez sur les icônes d'état dans le bandeau supérieur de l'interface.

- ou-

- Utilisez le menu déroulant des états au-dessus de la liste des firewalls. Le filtre **Connecté** affiche les firewalls dont l'état est **Opérationnel**, **Non Critique** et **Critique**.

Pour chaque firewall connecté, l'information sur le processeur, la mémoire utilisée et l'espace disque utilisé sont disponibles. Les valeurs affichées sur le processeur et la mémoire concernent la dernière heure écoulée. Survolez les schémas pour afficher plus de détails.

Les deux indicateurs de santé "Modification locale" et "Validation de configuration" sont remontés par le serveur SMC et sont liés à des problèmes de déploiement. Pour plus d'informations, reportez-vous aux sections Détecter des modifications de la configuration locale sur des firewalls et La validation du déploiement échoue.

Résoudre les problèmes

Un firewall n'affiche pas de date de fin de maintenance valide

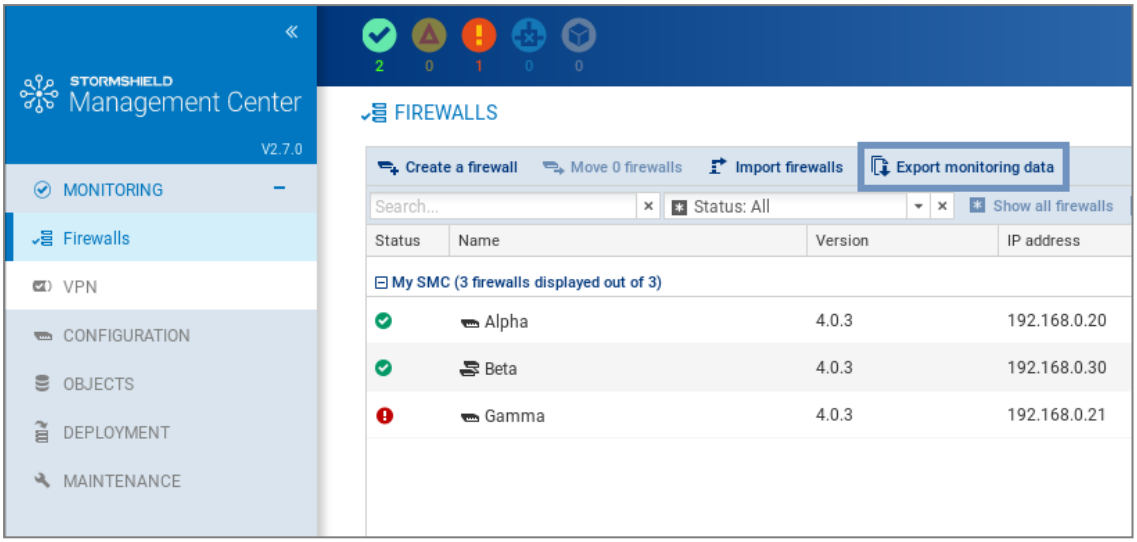
- *Situation* : Dans la vue de supervision, la colonne indiquant la date de fin de maintenance d'un firewall est vide.
- *Cause* : La licence du firewall n'est pas valide.
- *Solution* : Contactez votre centre de support Stormshield pour l'obtention d'une licence valide.

3.1.2 Exporter les données de supervision

Depuis le panneau de supervision des firewalls SNS, vous pouvez exporter et télécharger les données de supervision dans un fichier CSV. Si vous avez filtré les données, seules les lignes visibles dans la grille sont exportées.

L'export des données est possible en lecture/écriture ou en lecture seule.

1. Sélectionnez **Supervision** > **Firewalls**.
2. Si vous souhaitez exporter les données de quelques firewalls uniquement, filtrez les firewalls à l'aide du champ de recherche et du champ **État**.
3. Cliquez sur **Exporter les données de supervision**.



4. Sauvegardez le fichier CSV.

   Par défaut, les données dans le fichier sont séparées par des virgules. Vous pouvez modifier le délimiteur via la variable d'environnement `SMC_CSV_DELIMITER`.

   En cas de problème, consultez le journal *export.log*. Pour plus d'informations, reportez-vous à la section Consulter les journaux du serveur SMC.

3.1.3 Classer les firewalls par dossiers

Pour gérer les firewalls et leur configuration, le serveur SMC se base sur des dossiers organisés hiérarchiquement auxquels sont rattachés les firewalls.

La gestion des dossiers est dynamique, vous pouvez à tout moment créer, déplacer et supprimer des dossiers.

Un dossier contient des firewalls ainsi que des règles de filtrage et de translation globales. Un firewall rattaché à un sous-dossier hérite des règles configurées dans ses dossiers parents. Pour plus d'informations sur les règles de filtrage et de translation, reportez-vous à la section Définir des règles de filtrage et translation (NAT).

Un firewall ne peut appartenir qu'à un seul dossier à la fois.

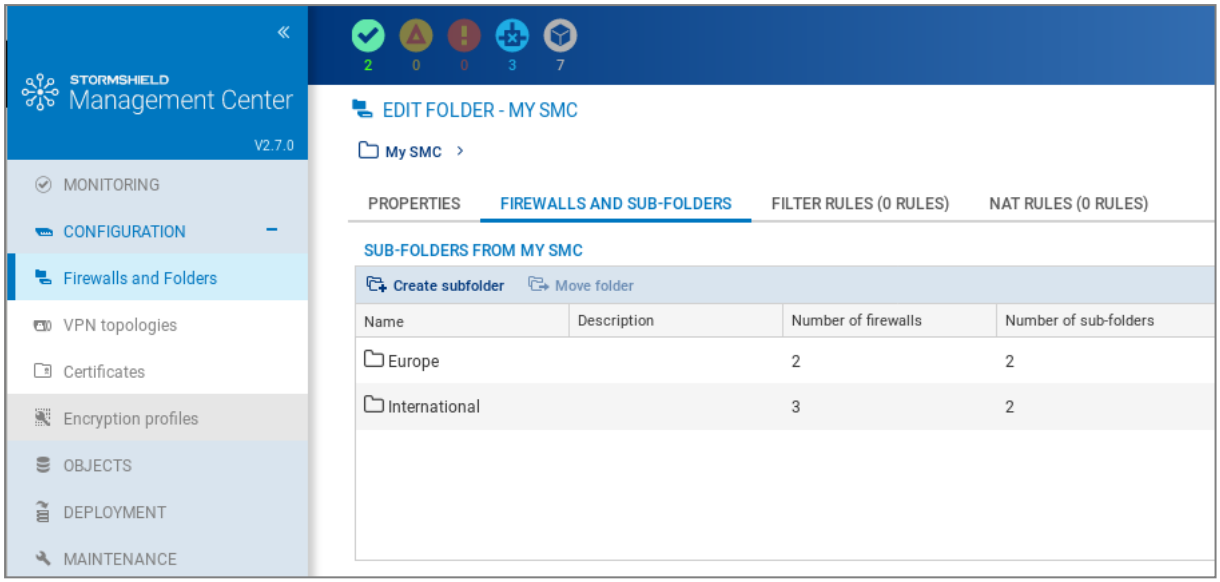
Le dossier racine par défaut **MySMC** ne peut être supprimé. Vous pouvez le renommer à votre convenance. Si vous ne créez pas d'arborescence de dossiers, tous les firewalls sont rattachés à ce dossier racine.

L'arborescence est limitée à quatre niveaux de sous-dossiers.

> **ASTUCE**
> Le champ **Rechercher** dans la liste de firewalls du menu **Supervision**> **Firewalls** prend également en compte les noms de dossier.

Créer les dossiers

1. Rendez-vous dans l'onglet **Firewalls et sous-dossiers** du menu **Configuration** > **Firewalls et dossiers**.
2. Cliquez sur le bouton **Créer un sous-dossier** en vous positionnant au préalable dans le dossier parent souhaité.



Classer les firewalls

Il existe plusieurs possibilités :

- Lorsque vous créez un nouveau firewall depuis les menus **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**, onglet **Firewalls et sous-dossiers**, vous pouvez choisir son emplacement.
- Vous pouvez déplacer un firewall existant depuis ces mêmes panneaux en cliquant sur le bouton **Déplacer 1 firewall**. La sélection multiple est autorisée.

Restreindre le droit d'accès en écriture d'un administrateur à certains dossiers

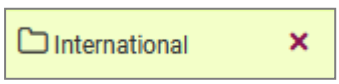
SMC permet de limiter l'accès en écriture des administrateurs à un seul dossier ou à quelques dossiers. Ainsi l'administration d'un groupe de firewalls peut être limitée à un seul administrateur, dit "de dossiers", pour des raisons de sécurité. Celui-ci peut toujours consulter la configuration des autres firewalls rattachés à SMC, mais avec un accès en lecture seule. Le super administrateur et l'administrateur général peuvent toujours accéder en écriture à tous les dossiers.

L'administrateur de dossiers ne peut créer et supprimer des dossiers que dans des dossiers sur lesquels il possède le droit d'accès en écriture.

Pour savoir comment restreindre les accès des administrateurs de dossiers, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Supprimer un dossier

Dans l'onglet **Firewalls et sous-dossiers** du menu **Configuration** > **Firewalls et dossiers**, survolez le nom du dossier et sélectionnez la croix rouge.



Si vous supprimez un dossier, les firewalls et règles dans ce dossier seront déplacés par défaut dans le dossier parent.

3.1.4 Vérifier l'utilisation d'un firewall dans la configuration

Pour vérifier l'utilisation d'un firewall :

1. Allez dans le menu **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**.
2. Survolez le nom du firewall et cliquez sur l'icône . Le panneau de résultats s'ouvre dans le panneau inférieur. Vous pouvez double-cliquer sur un résultat.

3.2 Accéder à l'interface de monitoring des firewalls

A partir du serveur SMC, il est possible d'accéder directement à l'interface de monitoring des firewalls connectés.

Dans **Supervision** > **Firewalls**, déplacez la souris à côté du nom du firewall et cliquez sur l'icône .

L'authentification étant automatique sur le firewall :

- Il n'est pas nécessaire de définir un identifiant sur ce firewall,
- Il n'est pas nécessaire de configurer un poste d'administration autorisé dans l'interface web d'administration du firewall,
- La déconnexion de l'interface web du serveur SMC implique automatiquement la déconnexion de l'interface du firewall.

Pour plus de renseignements sur l'interface de monitoring, consultez le *Manuel Utilisateur SNS*.

3.3 Accéder au serveur Stormshield Log Supervisor (SLS)

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

SLS est la solution de gestion des journaux proposée par Stormshield.

Depuis SMC, vous pouvez accéder à l'interface de votre serveur SLS grâce à un raccourci configurable dans les paramètres de SMC.

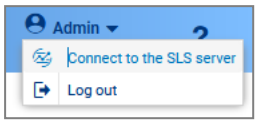
Vous avez également la possibilité d'accéder directement à la vue de SLS filtrée sur les journaux d'un firewall donné.

3.3.1 Ajouter un menu d'accès au serveur SLS

Pour ajouter un menu d'accès à votre serveur SLS depuis le bandeau supérieur de l'interface web de SMC :

1. Rendez-vous dans le menu **Maintenance** > **Serveur SMC** > **Paramètres**.
2. Cochez la case **Raccourci vers le serveur Stormshield Log Supervisor (SLS)**.
3. Indiquez l'adresse IP ou le FQDN du serveur SLS.
4. Cliquez sur **Mettre à jour**.

5. Vérifiez dans le menu déroulant de l'Administrateur dans le bandeau supérieur la présence du menu **Se connecter au serveur SLS** et testez le lien. Vous devez accéder au portail d'authentification de votre serveur SLS.



Une icône SLS est également disponible pour chaque firewall dans le panneau de supervision des firewalls.

3.3.2 Filtrer la vue SLS sur les journaux d'un firewall

Par défaut, lorsque vous cliquez sur l'icône d'un firewall dans la vue de supervision, le lien mène vers la page d'accueil de SLS.

Vous avez la possibilité de configurer un paramètre de l'URL de redirection afin d'accéder directement à la vue filtrée sur les journaux du firewall donné sur votre serveur SLS. Le filtrage s'opère sur l'adresse IP du firewall.

Pour activer cette fonctionnalité :

1. Allez dans le menu **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**.
2. Survolez le nom du firewall et cliquez sur l'icône crayon ou double-cliquez sur la ligne du firewall.
3. Dans l'onglet **Paramètres**, cochez la case **Adresse IP du firewall pour le serveur SLS**.
4. Choisissez d'utiliser l'adresse IP par défaut de SMC ou bien une adresse personnalisée connue du serveur SLS.
5. Cliquez sur **Appliquer**.

Dans la vue de supervision des firewalls, vous pouvez afficher la colonne **Adresse IP pour SLS** et vous servir ainsi de cette adresse pour effectuer une recherche de firewall.

4. Configurer les firewalls SNS

Configurez vos firewalls, objets, règles, routes, interfaces et topologies VPN dans l'interface web du serveur SMC et déployez la configuration sur les firewalls. Un accès direct à l'interface web d'administration d'un firewall est également possible.

Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers concernés dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Certaines opérations de configuration ne sont pas possibles depuis l'interface web du serveur SMC. Vous pourrez les réaliser à partir de commandes CLI SNS. Pour plus d'informations, reportez-vous à la section Exécuter des commandes CLI SNS sur un parc de firewalls.

4.1 Modifier les paramètres des firewalls

Pour modifier les paramètres d'un firewall :

1. Allez dans le menu **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**.
2. Survolez le nom du firewall et cliquez sur l'icône crayon ou double-cliquez sur la ligne du firewall.

La série d'onglets permet entre autres de :

- Modifier l'emplacement du firewall dans l'arborescence des dossiers,
- Activer la configuration des interfaces réseau et du routage depuis le serveur SMC. Par défaut, cette fonctionnalité est désactivée et les onglets **Interfaces** et **Routage** sont en lecture seule.
- Générer un package de rattachement pour le firewall. Pour plus d'informations sur ce package, reportez-vous à Rattacher des firewalls SNS au serveur SMC .
- Définir l'adresse de contact et l'interface de sortie à utiliser par défaut dans les topologies VPN,
- Ajouter un certificat sur le firewall,
- Ajouter des variables personnalisées utilisées dans les scripts CLI SNS ou dans les objets,
- Créer et gérer des règles de filtrage et de translation,
- Gérer les interfaces réseau, reportez-vous à la section Configurer les interfaces réseau.
- Obtenir des informations sur la haute disponibilité dans le cas d'un cluster.

Les champs **Description** et **Lieu** dans l'onglet **Système > Configuration** sont remplis à titre informatif et n'ont aucune incidence sur la configuration.

Si le firewall fait partie d'une topologie VPN par route, modifier son nom peut avoir des conséquences sur la configuration du firewall. Si vous modifiez le nom, les objets correspondant aux interfaces VTI associées sont automatiquement renommés sur SMC, vous devez alors vérifier la configuration locale du firewall. À partir de la version 3.4, si SMC gère la configuration du réseau et du routage du firewall, vous n'avez rien à faire. Pour plus d'informations, reportez-vous à la section Créer des topologies VPN par route.

ASTUCE
Le champ **Rechercher** dans la liste de firewalls prend également en compte les champs **Description** et **Lieu**.

4.1.1 Ajouter des propriétés personnalisées

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Les propriétés personnalisées permettent d'ajouter des critères de description des firewalls. Ceci permet de les identifier et de les filtrer plus efficacement, en utilisant des caractéristiques autres que leur nom, leur version ou les éventuels commentaires.

Ces propriétés personnalisées sont donc particulièrement utiles pour la gestion de parcs de firewalls de grande envergure.

Vous pouvez les créer directement dans SMC ou bien les importer.

NOTE
Les propriétés personnalisées sont destinées uniquement à l'administration via SMC et ne sont donc pas déployées sur les firewalls correspondants.

Le filtrage des firewalls selon les propriétés personnalisées peut être réalisé dans les modules suivants :

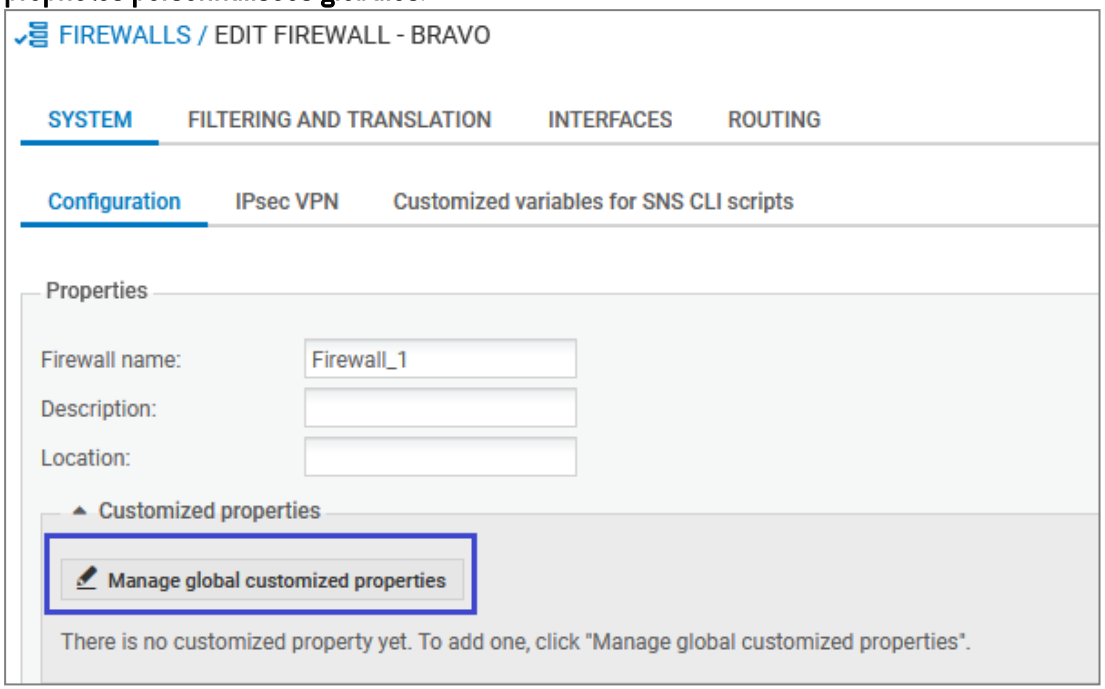
- Supervision des firewalls et dossiers,
- Sélection de correspondants au sein d'une topologie VPN,
- Sélection de firewalls pour un déploiement de configuration,
- Résultats de déploiements de configuration,
- Sélection de firewalls pour un déploiement de scripts CLI,
- Résultats de déploiements de scripts CLI.

Dans les écrans de supervision et de configuration des firewalls, vous pouvez afficher les colonnes représentant ces propriétés personnalisées.

Ajouter une propriété personnalisée à un firewall

Pour ajouter une propriété personnalisée :

1. Dans l'onglet **Système > Configuration** d'un firewall, cliquez sur le bouton **Gérer les propriétés personnalisées globales**.



Une fenêtre s'ouvre et affiche les propriétés disponibles.

2. Cliquez sur **Ajouter**.
3. Saisissez le **Nom** de la propriété.
   Seuls les caractères alphanumériques et les tirets de soulignement sont autorisés.
4. Cliquez sur **Fermer**.
   La fenêtre d'édition des paramètres du firewall affiche un nouveau champ portant le nom de la propriété personnalisée ajoutée.
5. Renseignez la valeur souhaitée (caractères libres) pour cette propriété personnalisée et cliquez sur **Appliquer**. Répétez cette dernière opération pour chaque firewall.

4.1.2 Modifier la valeur d'une propriété personnalisée de firewall

La valeur d'une propriété personnalisée peut être modifiée à tout moment :

1. Éditez les propriétés du firewall concerné.
2. Dans l'onglet **Système > Configuration** > cadre **Propriétés personnalisées**, renseignez la valeur souhaitée (caractères libres) de la propriété personnalisée à modifier.
3. Cliquez sur **Appliquer**.

4.1.3 Importer / Exporter des propriétés personnalisées de firewalls

L'import / export de propriétés personnalisées sont disponibles dans l'onglet **Système > Configuration** de la fenêtre d'édition des paramètres du firewall.

Exporter des propriétés personnalisées

1. Éditez les propriétés d'un firewall.
2. Dans l'onglet **Système > Configuration**, cliquez sur le bouton **Gérer les propriétés personnalisées globales**.
   Une fenêtre additionnelle s'ouvre et affiche les propriétés disponibles.

3. Cliquez sur **Exporter**.
4. Ouvrez ou enregistrez le fichier d'export des propriétés personnalisées.
5. Cliquez sur **Fermer**.

NOTE
Un fichier d'export de propriétés personnalisées présente la structure suivante :

#property,#firewall,#value
Cp1, Fw2, *valeur_cp1*
Cp2, Fw1, *valeur_cp2*
Cp3, Fw1, *valeur_cp3*
...

Importer des propriétés personnalisées

1. Créez un fichier d'import (format CSV) de propriétés personnalisées respectant la structure suivante :
   #property,#firewall,#value
   Cp1, Fw2, *valeur_cp1*
   Cp2, Fw1, *valeur_cp2*
   Cp3, Fw1, *valeur_cp3*
   ...
2. Éditez la configuration d'un firewall.
3. Dans l'onglet **Système > Configuration**, cliquez sur le bouton **Gérer les propriétés personnalisées globales**.
   Une fenêtre additionnelle s'ouvre et affiche les propriétés disponibles.
4. Cliquez sur **Importer**.
5. Sélectionnez le fichier créé à l'étape 1.
6. Cliquez sur **Ouvrir**.

Comportement de SMC lors de l'import

- Lorsqu'un firewall précisé dans le fichier d'import n'est pas rattaché au serveur SMC, l'import complet est annulé.
- Lorsqu'une propriété personnalisée existe déjà pour un firewall rattaché au serveur SMC, la valeur de cette propriété est modifiée pour le firewall considéré.
- Lorsqu'une propriété personnalisée n'existe pas, cette propriété est créée et la valeur correspondante lui est affectée pour chaque firewall précisé dans le fichier d'import.
- Lorsqu'une propriété personnalisée existe déjà sur le serveur SMC et est valorisée pour un firewall donné, sa valeur est remplacée par la valeur attribuée à ce même firewall dans le fichier d'import.

4.2 Créer des variables personnalisées

Vous avez la possibilité de créer des variables personnalisées globales à tous les firewalls SNS rattachés au serveur SMC et de les utiliser dans :

- les objets réseau de type Machine, Réseau et Plage d'adresses IP afin de créer des objets dont l'adresse IP sera déterminée de manière dynamique en fonction du firewall,
- les scripts CLI SNS afin d'exécuter des commandes groupées sur votre parc de firewalls,
- les files d'attente de type CBQ et les Traffic shapers afin de personnaliser les valeurs de bande passante dans le cadre de la QoS.

Pour ajouter des variables personnalisées, vous pouvez vous rendre dans les propriétés de n'importe quel firewall.

Pour définir les valeurs de chaque variable en fonction des firewalls, vous devez vous rendre dans les propriétés des firewalls concernés, à condition de posséder le droit d'accès en écriture sur ces firewalls.

Vous pouvez modifier ou supprimer des variables personnalisées, à condition qu'elles ne soient pas utilisées dans la configuration de firewalls sur lesquels vous ne possédez pas le droit d'accès en écriture. Vous pouvez vérifier leur utilisation comme indiqué ci-dessous. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Vous pouvez créer autant de variables personnalisées que nécessaire.

4.2.1 Ajouter, modifier ou supprimer une variable personnalisée

1. Allez dans le menu **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**,
2. Survolez le nom de n'importe quel firewall et cliquez sur l'icône crayon ou double-cliquez sur la ligne du firewall,
3. Allez dans l'onglet **Système > Variables personnalisées**. Le même tableau **Variables personnalisées** affiché dans l'onglet est accessible depuis tous les firewalls. Il permet de personnaliser les valeurs des variables pour le firewall courant, comme indiqué dans la section suivante.
4. Cliquez sur **Gérer les variables globales**.

Plusieurs actions sont disponibles dans la fenêtre de gestion des variables :

- Lorsque vous cliquez sur **Ajouter** et que vous entrez un nom pour la variable, la syntaxe %CUSTOM_X% est automatiquement appliquée au nom. Les espaces et les tirets ne sont pas supportés dans les noms de variable.
- Vous pouvez supprimer une variable existante, sauf si celle-ci est utilisée dans un objet.
- Le bouton **Copier dans le presse-papier** permet de copier la variable pour l'utiliser dans un objet réseau.
- Le bouton **Vérifier l'utilisation** permet d'afficher les firewalls et les objets qui utilisent la variable. Il est également présent directement dans l'onglet **Variables personnalisées**. Dans le panneau des résultats qui s'ouvre dans la partie inférieure de l'écran, vous avez la possibilité de cliquer sur les éléments pour les afficher et les modifier.
- Vous pouvez exporter et importer les variables au format CSV. Les colonnes du fichier CSV sont : #variable,#comment,#firewall,#value. L'import de variables permet de créer et de modifier des variables. Il ne permet pas de supprimer des variables existantes.
- Vous pouvez commenter la variable. Les commentaires et les variables sont visibles depuis les propriétés de tous les firewalls, mais uniquement modifiables depuis la fenêtre **Gérer les variables globales**.

4.2.2 Définir la valeur d'une variable personnalisée pour un firewall

Il n'est pas obligatoire de définir les valeurs des variables pour tous les firewalls.

Pour définir la valeur d'une variable pour un firewall donné :

1. Allez dans l'onglet **Système > Variables personnalisées** des paramètres du firewall concerné,
2. Double-cliquez dans la colonne **Valeur sur le firewall** pour attribuer une valeur aux variables définies à l'étape précédente.

Les noms des variables et les commentaires sont des champs communs à tous les firewalls. Il faut donc cliquer sur **Gérer les variables globales** pour les modifier.

4.3 Vérifier la cohérence de la configuration

Le contrôleur de cohérence est un outil qui analyse en temps réel la cohérence de votre configuration. Il affiche ainsi dans le panneau inférieur de l'interface web du serveur SMC les avertissements et les erreurs détectés.

Pour afficher le contrôleur de cohérence :

- Sélectionnez le menu **Maintenance** > **Contrôleur de cohérence**.

- ou -

- Ouvrez le panneau inférieur de l'écran en cliquant sur la flèche noire en bas de l'interface .

Le contrôleur affiche les avertissements et erreurs concernant tous les firewalls. Cependant l'analyse des erreurs est prioritaire sur l'analyse des avertissements. Si un firewall remonte au moins une erreur, l'analyse des avertissements sur ce firewall est annulée.

Vous avez la possibilité de filtrer par firewall ou par type d'incohérence ou bien de taper des caractères dans le champ de recherche.

Certains éléments (règles de filtrage ou translation, objets, etc.) sont cliquables et permettent d'ouvrir directement le panneau ou l'élément concerné.

La vérification de la cohérence fonctionne également pendant les déploiements de configuration. Seules les erreurs sont vérifiées, les avertissements sont ignorés. En cas d'erreur détectée, le déploiement échoue.

4.3.1 Désactiver la vérification de la cohérence

La vérification de la cohérence peut altérer les performances du serveur SMC lorsqu'il administre des parcs importants (plus de 500 firewalls SNS).

La variable d'environnement `SMC_CFGCHECK_ENABLED` permet de désactiver cette vérification si nécessaire.

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Modifiez le fichier **/data/config/fwadmin-env.conf.local** en ajoutant la ligne suivante à la fin : `SMC_CFGCHECK_ENABLED=false`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

Dans ce cas, vous avez toujours la possibilité de lancer manuellement la vérification de la cohérence, de façon ponctuelle, en cliquant sur le bouton **Lancer la vérification** dans l'interface du contrôleur de cohérence.

Lorsque vous désactivez la vérification de la cohérence, les vérifications automatiques à chaque déploiement sont cependant effectuées afin de garantir la cohérence de la configuration des firewalls.

La variable d'environnement `SMC_CFGCHECK_BEFORE_DEPLOY_ENABLED` permet de désactiver ces vérifications automatiques en cas de besoin.

4.3.2 Désactiver des domaines de vérification ou modifier le niveau de l'anomalie

ATTENTION
Veuillez suivre les recommandations du Technical Assistance Center de Stormshield pour réaliser ces opérations.

Vous pouvez désactiver spécifiquement certains domaines de vérification ou même certaines vérifications de la cohérence de la configuration. Vous pouvez également modifier le niveau "avertissement" ou "erreur" des vérifications.

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Pour connaître la liste des entrées désactivables, consultez le fichier **/opt/fwadmin-server/config/cfgcheck.ini** (sans le modifier).

3. Dans le fichier **/data/config/cfgcheck.ini** :
   - Ajoutez les clés à désactiver dans la section `DOMAINS` du fichier en indiquant la valeur `false`,
   - Ajoutez les vérifications dans la section `CHECKS` du fichier en indiquant le niveau `error` ou `warning` , ou bien utilisez la valeur `false` pour désactiver une vérification.
4. Redémarrez le serveur avec la commande `nrestart smc`.

EXEMPLE
Fichier **/data/config/cfgcheck.ini** :

```
[DOMAINS]
RULE=false
IPSECDR=false

[CHECKS]
INVALID_INTERFACE_IN_STATIC_ROUTING=error
INVALID_INTERFACE_IN_RETURN_ROUTING=error
IP_COLLISION=warning
OVERLAPPING=warning
RETURN_ROUTE_GATEWAY_WITHOUT_MAC_ADDRESS=false
STATIC_ROUTE_WITHOUT_INTERFACE=false
```

4.3.3 Limiter le nombre d'incohérences remontées

La variable d'environnement `SMC_CFGCHECK_INCOHERENCIES_INT` permet de limiter le nombre d'incohérences remontées par le contrôleur. Par défaut le nombre est de 100. Lorsque la limite est atteinte, SMC annule toutes les analyses en attente.

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez la valeur de la variable d'environnement : `SMC_CFGCHECK_INCOHERENCIES_INT`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

4.4 Déployer une configuration sur des firewalls

A chaque création ou modification de la configuration sur le serveur SMC, vous devez déployer la configuration sur les firewalls.

Tous les déploiements sont enregistrés dans l'historique de déploiement. Reportez-vous à la section Charger et déployer une ancienne configuration.

Lors d'un déploiement, les informations suivantes sont transmises aux firewalls :

- Les objets utilisés dans les règles de filtrage ou de translation liées au firewall ou à ses dossiers parents.
- Les objets pour lesquels vous avez choisi le déploiement sur tous les firewalls ou pour lesquels vous avez sélectionné les firewalls sur lesquels les déployer. Pour plus d'informations, reportez-vous à la section Gérer les objets.

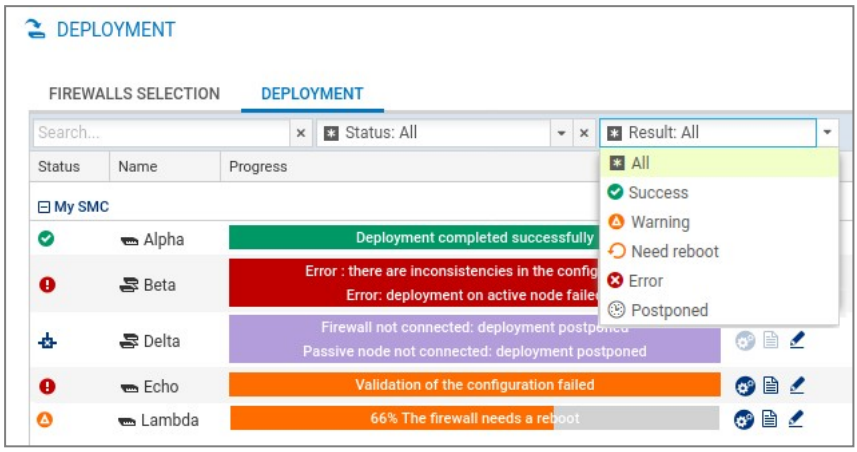
- Si le firewall fait partie d'une topologie VPN : les objets Réseau, Machine et/ou Groupe et l'autorité de certification associés à cette topologie, ainsi que les informations sur le certificat sélectionné pour le firewall dans la topologie (le certificat est déjà installé sur le firewall).

Pour réaliser cette opération, vous devez posséder le droit d'accès en écriture sur les firewalls. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

4.4.1 Déployer une configuration sur un firewall depuis l'interface web

1. Allez dans le menu **Déploiement** > **Déploiement de configuration** ou cliquez sur le bouton dans le bandeau supérieur de l'interface. Ce bouton devient orange lorsque des modifications ont été apportées à la configuration.
2. Choisissez les firewalls dans l'onglet **Sélection des firewalls**.
3. Renseignez un commentaire en bas du panneau si nécessaire. Ce commentaire sera affiché dans l'historique de déploiement.
4. Cliquez sur **Déployer la configuration** à côté du champ de commentaire. L'onglet **Déploiement** s'ouvre automatiquement. Une barre d'état indique l'avancement et le résultat du déploiement pour chaque firewall.
   Lors du déroulement d'un déploiement ou une exécution de script CLI SNS, vous ne pouvez pas lancer un autre déploiement mais il est possible de préparer un déploiement dans l'onglet **Sélection des firewalls**.
5. Pendant ou après le déploiement, vous pouvez cliquer sur la barre d'état d'un firewall pour afficher un résumé du déploiement sur ce firewall. Pour obtenir plus d'informations sur le déploiement, utilisez la commande `clogs` dans l'interface de ligne de commande.
6. Un résumé du déploiement est visible en bas du panneau, affichant les réussites, les avertissements, les erreurs et les déploiements reportés.

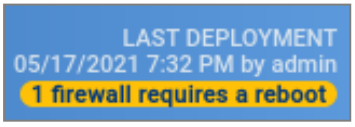
7. Vous pouvez également filtrer la liste des firewalls en sélectionnant un résultat de déploiement dans la liste déroulante tout en haut de la liste.



En cas de déploiement réussi, le numéro de déploiement sera incrémenté dans la colonne **Déploiement**.

> **ASTUCE**
> Si la configuration a été déployée sur des firewalls déconnectés, le déploiement est reporté et les firewalls récupèrent la configuration la prochaine fois qu'ils se connectent.

8. En cas d'erreur, reportez-vous aux journaux du serveur SMC. Vous pouvez également vous connecter aux journaux et rapports d'activité d'un firewall en cliquant sur l'icône dans la colonne **Actions** et consulter les journaux du firewall.
9. Si le firewall doit être redémarré pour terminer le déploiement, ceci est indiqué par l'état de santé "Redémarrage nécessaire". Vous pouvez lancer le redémarrage directement depuis l'écran de déploiement en cliquant sur le bouton **Redémarrer** en bas de l'écran. Vous pouvez également redémarrer le firewall plus tard depuis les écrans de supervision, configuration et déploiement ou en cliquant sur l'information affichée à droite dans le bandeau supérieur de l'interface :



10. Après un premier déploiement, le serveur SMC vérifie régulièrement si la configuration sur le firewall correspond toujours à la configuration sur SMC. Reportez-vous à la section Détecter des modifications de la configuration locale sur des firewalls.

4.4.2 Déployer une configuration sur un cluster haute disponibilité

Les étapes sont identiques à celles de la section précédente.

La configuration est d'abord déployée sur le nœud actif du cluster. Le serveur SMC effectue ensuite une synchronisation des deux nœuds du cluster.

Si le nœud passif n'est pas connecté au nœud actif au moment du déploiement, le serveur SMC effectuera une synchronisation des deux nœuds du cluster lorsque le nœud passif se reconnectera au nœud actif.

4.4.3 Déployer une configuration sur un firewall en ligne de commande

Vous pouvez utiliser la commande `smc-deploy` pour déployer une configuration en ligne de commande.

Faites suivre la commande de la liste des firewalls ciblés par le déploiement avec l'une des deux options :

- --all : déployer sur tous les firewalls,
- --firewall-list <firewallNames> : déployer sur certains firewalls (séparés par des virgules).

Pour voir les autres options de cette commande, tapez `smc-deploy --help`.

Au début du déploiement, le numéro du déploiement s'affiche.

4.4.4 Activer l'avertissement de modification de la configuration

Lorsque vous êtes sur le point de déployer une configuration sur des firewalls, SMC peut afficher un avertissement pour indiquer que d'autres administrateurs ont réalisé des modifications depuis le dernier déploiement.

Vous pouvez alors choisir d'annuler le déploiement ou de le poursuivre. Si vous choisissez de poursuivre le déploiement, les modifications réalisées par les autres administrateurs sont également déployées sur les firewalls sélectionnés.

Par défaut, cette fonctionnalité est désactivée. Pour l'activer :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, ajoutez la variable d'environnement `SMC_WARNING_MODIFICATION_ENABLED=true`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

AVERTISSEMENT
Cette fonctionnalité comporte les limitations suivantes :

- SMC ne prend en compte que les modifications de configuration réalisées dans l'interface web d'administration pour déclencher l'avertissement. Les modifications réalisées via l'interface de ligne de commande ou via l'API publique de SMC ne sont pas prises en compte.
- Toute modification de la configuration d'un firewall déclenche l'avertissement, quels que soient les firewalls sélectionnés pour le déploiement, et même si le firewall en question ne fait pas partie de la sélection ou ne fait pas partie du périmètre d'administration de l'administrateur qui déploie.
- Toute création de ressource, c'est-à-dire objet ou jeu de règles, même si elle est non utilisée ou immédiatement supprimée, déclenche l'avertissement.
- Toute manipulation des séparateurs de règles (déplier/replier) déclenche l'avertissement.
- Lors d'un déploiement, la liste des modifications en attente est vidée, quels que soient les firewalls sélectionnés pour le déploiement. Cela signifie que si vous réalisez une modification sur le firewall A, et qu'un autre administrateur déploie sur le firewall B dans un premier temps, puis sur le firewall A dans un second temps, il ne verra l'avertissement qu'au moment du premier déploiement.

- Si un administrateur restaure une sauvegarde sur SMC, la liste des modifications en attente est vidée. Il n'y aura pas d'avertissement au prochain déploiement.
- Lorsqu'un déploiement de configuration échoue sur un firewall, la liste des modifications en attente est vidée.

4.4.5 Préserver la connexion lors d'un déploiement

Avant qu'une nouvelle configuration déployée par SMC ne soit installée sur un firewall SNS, sa configuration est sauvegardée. Ainsi, si un déploiement altère la connexion entre le serveur SMC et un firewall SNS, la sauvegarde la plus récente est restaurée. Ce mécanisme garantit que le firewall SNS sera toujours joignable par le serveur SMC. Vous pouvez gérer cette fonctionnalité pour chaque firewall à l'aide de trois variables d'environnement :

Variable	Description
SMC_DEPLOYMENT_TIMEOUT_BEFORE_ROLLBACK_INT Par défaut : 30 secondes	Définit le temps d'attente en secondes pendant lequel le firewall essaie de rétablir la connexion. Passé ce délai, la configuration précédente est restaurée.
SMC_SNS_DEPLOYMENT_ROLLBACK_TIMEOUT_INT Par défaut : 180 secondes	Définit le temps d'attente en secondes entre la restauration de la configuration et la reconnexion au serveur SMC. Si la connexion n'est pas rétablie passé ce délai, le déploiement est considéré comme ayant échoué. Nous vous recommandons de ne pas fixer une valeur inférieure à la valeur par défaut.
SMC_FW_DEPLOYMENT_ROLLBACK_ENABLED	Permet de désactiver la fonctionnalité. Par défaut, elle est activée.

4.4.6 Consulter les journaux du serveur en cas de problème

Si vous rencontrez des problèmes lors d'un déploiement de configuration, commencez par consulter les fichiers de journaux suivants.

Côté SMC

/data/log/fwadmin-server/server.log

Côté firewalls

/log/l_system

4.4.7 Résoudre les problèmes

La validation du déploiement échoue

- *Situation* : Après un déploiement de la configuration sur le firewall, l'état du firewall passe en **Critique** et indique "Validation de configuration". La commande `CONFIG STATUS VALIDATE` a donc échoué.

- *Cause* : Le mot de passe utilisé pour valider la configuration sur le firewall SNS a peut-être été modifié et ne correspond plus à celui enregistré sur SMC. Consultez les journaux du serveur pour connaître la cause exacte.
- *Solution* : Connectez-vous sur le firewall pour corriger le problème. Dans le cas d'un mot de passe incorrect, exécutez la commande `CONFIG STATUS REMOVE`.

Il n'est pas possible de déployer une configuration sur certains firewalls

- *Situation* : Certains firewalls ne peuvent pas être sélectionnés pour le déploiement.
- *Cause* : Une exécution de script CLI SNS est en cours ou en état différé sur le firewall et il n'est donc pas possible de déployer une configuration sur ce firewall.
- *Solution* : Attendez la fin de l'exécution du script ou la reconnexion du firewall pour que l'exécution se termine. Vous pouvez aussi annuler l'exécution du script depuis le menu **Scripts CLI SNS**.

4.5 Compléter la configuration des firewalls par fichier CSV

SMC permet d'importer dans les paramètres de chaque firewall un fichier de configuration CSV à prendre en compte lors des déploiements de configuration.

Ce fichier permet de définir des paramètres SNS qui ne sont pas configurables depuis SMC ou de surcharger pour un firewall donné des paramètres communs.

Cette fonctionnalité ne concerne que les paramètres contenus dans des fichiers de configuration générés par SMC. Par exemple, elle ne permet pas d'agir sur les règles de filtrage et de translation locales d'un firewall.

4.5.1 Créer le fichier CSV

1. Créez un fichier CSV selon le modèle suivant :

```
setconf, "file", "section", "field", "value"
setconf, "file", "section", "line"
delconf, "file", "section", "field", "value"
delconf, "file", "section", "line"
```

Les opérations SNS autorisées **setconf** et **delconf** permettent de modifier ou supprimer des paramètres de la configuration.

Par exemple :

```
setconf, network, loopback1, Address, 192.168.1.2
setconf, Global/VPN/01, Global, RemoteFetch, 1
```

Pour plus d'informations sur les fichiers de configuration en général, reportez-vous à la documentation des firewalls SNS.

Si vous souhaitez modifier le caractère délimiteur par défaut dans le fichier, reportez-vous à la section Choisir le caractère délimiteur dans les fichiers CSV.

2. Importez ensuite le fichier dans SMC comme indiqué ci-dessous.

4.5.2 Importer le fichier CSV dans SMC

Pour importer le fichier de configuration dans les paramètres d'un firewall :

1. Allez dans le menu **Supervision** > **Firewalls** ou **Configuration** > **Firewalls et dossiers**.
2. Survolez le nom du firewall et cliquez sur l'icône crayon ou double-cliquez sur la ligne du firewall.
3. Dans l'onglet **Système > Configuration**, dépliez l'encart **Configuration additionnelle du firewall** et cliquez sur **Importer le fichier**.

Une fois le fichier CSV importé dans les paramètres du firewall, il est pris en compte dans les fichiers de configuration de SMC à chaque déploiement de configuration sur le firewall. Vous pouvez le remplacer ou le supprimer.

Pour voir son contenu, exportez le fichier.

4.6 Charger et déployer une ancienne configuration

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Chaque configuration déployée sur les firewalls est enregistrée dans l'historique de déploiement et peut être chargée et déployée à nouveau.

Pour visualiser l'historique de déploiement et redéployer une configuration :

1. Allez dans le menu **Déploiement** > **Historique de déploiement**.
2. Sélectionnez un déploiement et cliquez sur l'icône pour restaurer la configuration. Les modifications en cours sur la configuration actuelle seront perdues.
3. Pour déployer une configuration sur des firewalls, répétez les étapes décrites dans la section Déployer une configuration sur des firewalls.

Si vous chargez une configuration qui n'est pas la plus récente dans l'historique, un message d'avertissement s'affiche en haut de la fenêtre. Ce message reste jusqu'à ce que vous déployiez la configuration sur des firewalls ou chargiez la dernière configuration déployée.

NOTE
L'historique de déploiement est vidé à chaque mise à jour du serveur SMC et contient donc uniquement les révisions d'une version courante. Il n'est pas possible d'utiliser l'historique pour restaurer la configuration d'une ancienne version après la mise à jour.

4.7 Générer un différentiel de configuration

Avant de déployer une nouvelle configuration sur votre parc de firewalls, vous avez la possibilité, pour chaque firewall, d'afficher un différentiel entre la dernière configuration déployée sur le firewall et la configuration préparée depuis le serveur SMC et prête à être déployée sur les firewalls.

1. Allez dans le menu **Déploiement** > **Déploiement de configuration** ou cliquez sur le bouton dans le bandeau supérieur de l'interface. Ce bouton devient orange lorsque des modifications ont été apportées à la configuration.

2. Dans la colonne **Déploiement**, cliquez sur l'icône d'un firewall pour afficher le différentiel de configuration.
   - Le différentiel s'affiche au format brut et ne tient compte que des changements concernant le firewall en question. Dans le cas d'un cluster, seul le nœud actif est pris en compte.

Depuis cette fenêtre de visualisation du différentiel, vous pouvez télécharger le différentiel, le fichier de configuration aux formats *.na* (format exploitable par les firewalls SNS) ou *.tgz* (fichiers de configuration lisibles dans un éditeur de texte), ainsi que déployer la configuration sur le firewall.

Après avoir visualisé le différentiel, une icône d'état est visible dans la colonne **Déploiement** indiquant que :

- : la configuration n'a pas été modifiée, le déploiement n'est pas nécessaire,
- : la configuration a été modifiée et les changements sont détaillés dans la fenêtre de visualisation. Cliquez sur l'icône pour revoir les modifications de configuration.
- : l'état est inconnu ou le dernier différentiel n'est plus valide. Cliquez alors sur l'icône pour actualiser l'état.

Pour visualiser des modifications de la configuration locale sur un firewall après un déploiement, reportez-vous à la section Détecter des modifications de la configuration locale sur des firewalls.

4.8 Détecter des modifications de la configuration locale sur des firewalls

Après un premier déploiement d'une configuration, SMC vérifie régulièrement si la configuration déployée depuis le serveur correspond toujours à celle présente sur le firewall. Le serveur SMC peut donc détecter une modification effectuée directement sur le firewall SNS sans passer par SMC.

Vous pouvez gérer la vérification par une variable d'environnement :

Variable	Description
SMC_CONFIG_STATUS_CHECK_PERIOD_INT Par défaut : 120000 ms	La variable définit à quelle fréquence SMC vérifie la configuration sur les firewalls. La valeur est définie en millisecondes. Définir la variable à 0 désactive la fonctionnalité : la configuration sur les firewalls n'est plus vérifiée.

Si SMC détecte une modification locale de la configuration sur un firewall, l'état du firewall passe en **Critique** et l'indicateur de santé "Modification locale" est affiché.

Le numéro de révision est donc barré en rouge car il ne correspond plus à la configuration sur le firewall.

Lors de la mise à jour d'un firewall, la détection de modification locale est désactivée jusqu'au prochain déploiement de configuration. Après un nouveau déploiement, SMC reprend la surveillance des modifications locales.

4.8.1 Visualiser des modifications locales sur un firewall

Dans le menu **Déploiement**, cliquez sur l'icône à côté du numéro de révision pour visualiser les modifications faites localement sur le firewall. Depuis la fenêtre qui s'ouvre, vous pouvez :

- télécharger le différentiel entre la configuration sur le firewall et la dernière configuration déployée depuis le serveur SMC,
- restaurer la configuration précédant les modifications locales sur le firewall.

4.9 Accéder à l'interface web d'administration des firewalls

L'interface web du serveur SMC ne permet pas la configuration de tous les paramètres d'un firewall. Pour compléter la configuration, il est possible de se connecter directement à l'interface d'administration d'un firewall sans devoir s'authentifier. Le droit d'accéder à l'interface web des firewalls en lecture/écriture est alors requis. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur.

1. Allez dans le menu **Supervision** > **Firewalls**.
2. Survolez le nom d'un firewall. Le firewall doit être en ligne.
3. Cliquez sur l'icône .

L'authentification étant automatique sur le firewall :

- Il n'est pas nécessaire de définir un identifiant sur ce firewall,
- Il n'est pas nécessaire de configurer un poste d'administration autorisé dans l'interface web d'administration du firewall,
- La déconnexion de l'interface web du serveur SMC implique automatiquement la déconnexion de l'interface web d'administration du firewall.

ASTUCE
L'indication "Managed by SMC" s'affiche en haut de l'interface d'administration du firewall.

Pour plus de renseignements sur l'interface web d'administration, consultez le *Manuel Utilisateur SNS*.

Si le firewall n'est pas dans le périmètre d'administration d'un administrateur, l'accès direct à l'interface d'administration du firewall est possible mais en lecture seule. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

4.10 Utiliser le mode Urgence

En cas d'indisponibilité temporaire du serveur SMC, si vous devez modifier la configuration d'un firewall, connectez-vous directement à l'adresse IP de l'interface web d'administration du firewall.

ASTUCE
L'indication "Managed by SMC - Emergency mode" s'affiche en haut de l'interface web d'administration du firewall.

4.11 Convertir un firewall connecté au serveur SMC en cluster haute disponibilité

Un firewall autonome connecté au serveur SMC peut être converti en cluster haute disponibilité :

1. Depuis l'interface web du serveur SMC, connectez-vous à l'interface web d'administration du firewall en cliquant sur l'icône dans la liste des firewalls du menu **Supervision**.
2. Reportez-vous à la section Haute Disponibilité du *Manuel Utilisateur SNS*, pour ajouter un nœud passif. En cas de bascule, le nœud passif devient actif et se connecte automatiquement au serveur SMC

ASTUCE

L'icône dans la colonne **Mode** est mise à jour dans la liste des firewalls sur l'interface web du serveur SMC. Pour visualiser les détails sur les deux nœuds du cluster, double-cliquez sur le nom du cluster dans le menu **Firewalls** et ouvrez l'onglet **Système > Haute disponibilité**.

4.12 Importer ou déclarer un certificat pour un firewall

Un certificat au format DER ou PEM est requis pour chaque firewall faisant partie d'une topologie VPN avec authentification .X509.

Une identité au format PKCS#12 peut être installée sur un firewall depuis le serveur SMC, qui récupère le certificat correspondant.

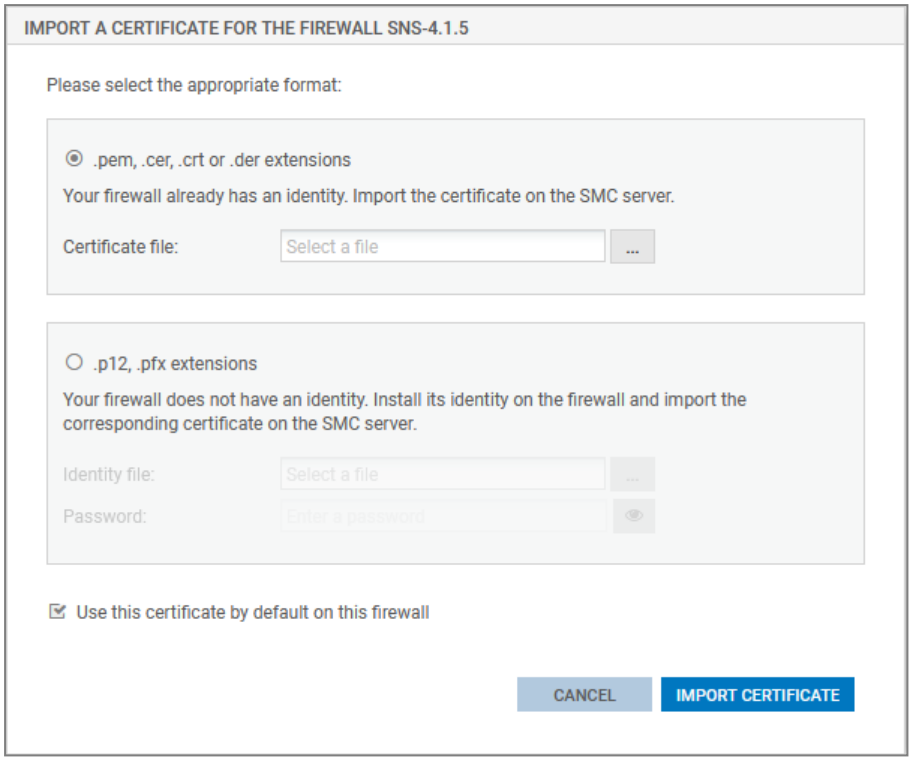
Vous pouvez importer le certificat sur le serveur SMC à partir de l'interface web du serveur ou de l'interface de ligne de commande. Vous pouvez en importer plusieurs pour un même firewall.

Vous pouvez également déclarer sur SMC un certificat utilisé par un firewall SNS sans l'importer sur le serveur (protocoles SCEP ou EST).

Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur le firewall. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

4.12.1 Importer un certificat depuis l'interface web du serveur

La fenêtre d'import de certificat pour un firewall est accessible depuis plusieurs panneaux de l'interface web d'administration.



1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur un firewall connecté.
2. Dans l'onglet **Système > VPN IPsec**, sélectionnez l'option **Par fichier**.
3. Cliquez sur **Importer un nouveau certificat**. Le lien vous amène dans le menu **Configuration** > **Certificats**.
4. Survolez le nom du firewall dans la colonne **Firewall** et cliquez sur l'icône . Pour plus d'informations sur le menu **Certificats**, reportez-vous à la section Gérer les certificats et les autorités de certification.

-ou-

1. Dans le menu **Supervision** > **Firewalls**, survolez le nom d'un firewall connecté et cliquez sur l'icône .

-ou-

1. Dans le menu **Configuration** > **Certificats**, cliquez sur le bouton **Importer un certificat** en haut de la grille . Pour plus d'informations sur le menu **Certificats**, reportez-vous à la section Gérer les certificats et les autorités de certification.

-ou-

1. Pendant la configuration d'une topologie VPN, lors de l'étape du choix des correspondants, cliquez sur l'icône sur la ligne d'un firewall. Pour plus d'informations, reportez-vous à la section Créer des topologies VPN par politique.

L'option **Utiliser ce certificat par défaut pour ce firewall** permet de choisir le certificat utilisé pour les négociations VPN. Il ne peut y avoir qu'un seul certificat par défaut pour un firewall. Pour modifier le certificat utilisé par défaut par la suite, reportez-vous à la section Modifier le certificat utilisé par défaut dans les topologies VPN.

4.12.2 Importer un certificat depuis l'interface de ligne de commande

1. Pour importer un certificat depuis l'interface de ligne de commande, connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande
`smc-install-certificate`

ASTUCE
Affichez l'aide avec l'option --help :

```
[root@smc] - {~} > smc-install-certificate --help
Usage: smc-install-certificate [options]

A tool that imports a certificate file (.p12 or .pfx) on a SNS Firewall.

The certificate's password will be prompted if not provided through the -p option.
It is required for the installation on the Firewall.

Options:
  -V, --version                 output the version number
  -c, --certificate <filepath>  The certificate to import on the firewall
  -f, --firewall <name>         The target firewall name
  -p, --password <password>     The password of the certificate
  -u, --update                  Use this option to update an existing certificate
  -h, --help                    display help for command
```

Parmi ces options, trois sont obligatoires :

- --certificate : chemin du certificat (*.p12* ou *.pfx*) à installer,
- --firewall : nom du firewall pour lequel le certificat doit être installé,
- --password : mot de passe qui protège le certificat dans le cas d'un *.p12*.

L'opération est enregistrée dans le fichier de log */var/log/misc/install-certificate.log*.

4.12.3 Importer un certificat sur un cluster haute disponibilité

Importez le certificat pour le nœud actif du cluster.

Le serveur SMC effectue ensuite une synchronisation des deux nœuds du cluster.

4.12.4 Résoudre les problèmes

Le bouton Importer reste grisé

- *Situation* : Vous avez sélectionné le certificat et rentré le mot de passe et le bouton **Importer** reste grisé.
- *Cause* : Lors du déroulement d'une exécution de script ou d'un déploiement de configuration, vous ne pouvez pas importer un certificat pour un firewall.
- *Solution* : Attendez la fin de l'exécution ou du déploiement en cours.

L'import du certificat sur un firewall provoque une erreur

- *Situation* : Lorsque vous importez un certificat sur un firewall, le serveur SMC retourne l'erreur "Pas assez de privilèges".
- *Cause* : Vous ne pouvez pas importer un certificat sur un firewall sur lequel une session est ouverte en direct ou via SMC.
- *Solution* : Déconnectez-vous du firewall et retentez l'import du certificat.

Autres sources de problèmes possibles

- La taille du fichier dépasse le maximum autorisé qui est de 1 Mo.
- Le format du fichier est autre que *.p12* ou *.pem*. Le serveur SMC ne supporte que les fichiers *.p12* ou *.pem*.
- Vous avez entré un mauvais mot de passe.

4.12.5 Déclarer un certificat utilisé par un firewall

Vous pouvez également déclarer dans SMC un certificat utilisé par un firewall SNS en indiquant son sujet et son émetteur. Vous n'avez alors pas besoin d'importer le certificat sur le serveur.

Ceci peut être utile par exemple lorsque le firewall génère ses propres clés et obtient un certificat automatiquement depuis l'autorité de certification via les protocoles SCEP ou EST.

Il ne peut y avoir qu'un seul certificat obtenu par SCEP ou EST par firewall.

1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur un firewall connecté.
2. Dans l'onglet **Système > VPN IPsec**, sélectionnez **Par noms de sujet et d'émetteur** et entrez les informations correspondantes.

Pour permettre le renouvellement des certificats expirés obtenus par SCEP ou EST, depuis le serveur SMC, vous devez indiquer l'adresse d'un serveur SCEP ou EST dans le panneau des propriétés d'une autorité de certification. Pour plus d'informations, reportez-vous à la section Gérer les certificats et les autorités de certification.

4.12.6 Modifier le certificat utilisé par défaut dans les topologies VPN

Si vous avez importé plusieurs certificats X509 pour un firewall, pour savoir lequel est utilisé par défaut dans les topologies VPN :

1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur la ligne du firewall concerné,
2. Ouvrez l'onglet **Système > VPN IPsec**. Le certificat utilisé par défaut est le certificat sélectionné dans l'encart **Certificat pour l'authentification**.

Pour modifier le certificat utilisé par défaut, sélectionnez un autre certificat dans la liste déroulante ou bien importez un nouveau certificat.

Vous ne pourrez pas modifier le certificat utilisé par défaut s'il est utilisé dans une topologie VPN.

4.13 Utiliser SMC en tant que point de distribution Active Update

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Les firewalls SNS disposent de la fonctionnalité Active Update qui interroge les serveurs de mise à jour Stormshield pour télécharger les dernières bases de données (signatures contextuelles, antivirus, Vulnerability Manager, etc.).

Si vos firewalls SNS ne sont pas connectés à Internet, ils n'ont pas accès aux serveurs de mise à jour Stormshield. Dans ce cas, vous pouvez utiliser SMC comme point de distribution Active Update, et ainsi mettre à disposition sur le réseau interne les bases de données actualisées.

Cette fonctionnalité est compatible avec les firewalls SNS à partir de la version 4.3.

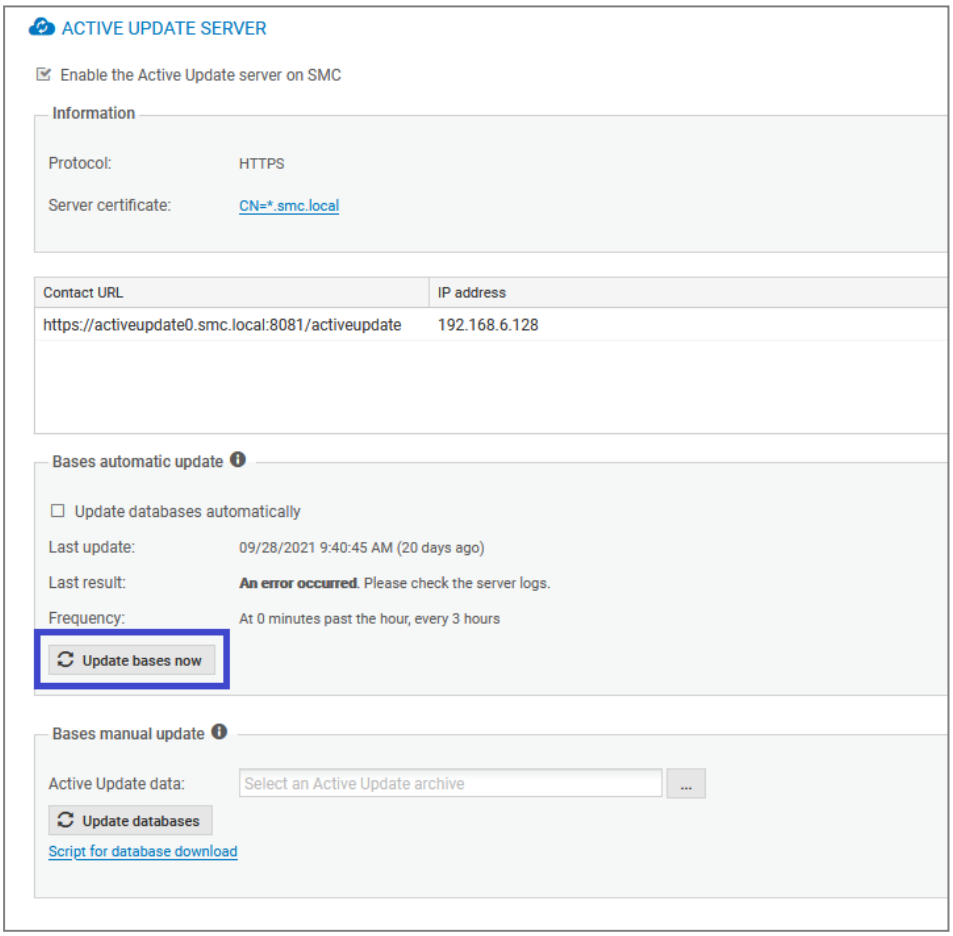
4.13.1 Télécharger les bases de données Active Update

Vous devez télécharger les bases de données Active Update sur le serveur SMC pour pouvoir les distribuer ensuite sur les firewalls SNS. La procédure diffère selon que le serveur SMC est connecté à internet ou non.

Télécharger les bases avec une connexion internet

La résolution DNS doit être activée sur le serveur SMC (menu **Maintenance** > **Serveur SMC** > **Paramètres** > **Serveur de nom de domaine**).

1. Affichez le menu **Configuration** > **Serveur Active Update**.
2. Cochez la case **Activer le serveur Active Update sur SMC**.
3. Cliquez sur **Appliquer** en bas de la fenêtre.
4. Dans la zone **Mise à jour automatique des bases**, cliquez sur **Mettre à jour les bases maintenant**.

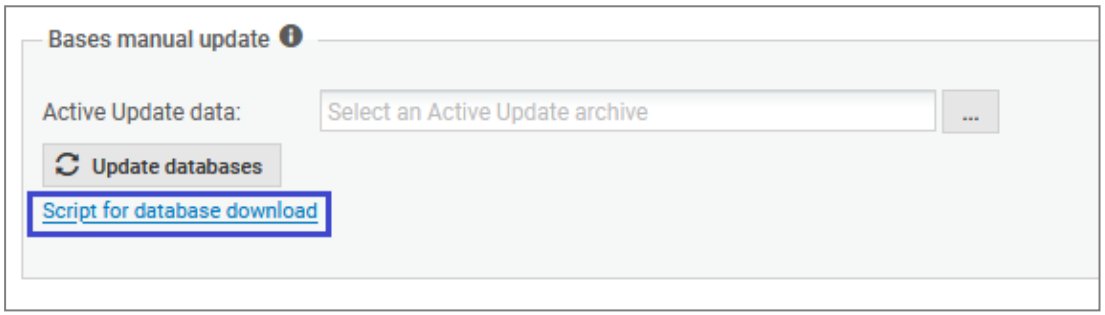


Le serveur SMC se connecte au serveur de mise à jour Stormshield et télécharge les bases de données.

5. Si vous souhaitez que les bases de données se mettent à jour automatiquement toutes les trois heures, cochez la case **Mettre à jour les bases automatiquement**.
   Pour modifier la fréquence de mise à jour ou le nombre de bases de données à mettre à jour, voir Personnaliser les paramètres Active Update.

Télécharger les bases sans connexion internet

1. Affichez le menu **Configuration** > **Serveur Active Update**.
2. Cochez la case **Activer le serveur Active Update sur SMC**.
3. Cliquez sur **Appliquer** en bas de la fenêtre.
4. Dans la zone **Mise à jour manuelle des bases**, cliquez sur le lien **Script de téléchargement des bases**.



5. Copiez et exécutez le script `activeupdate-fetch.sh` sur une machine Linux connectée à internet. La résolution DNS doit être activée sur la machine.
   - Par défaut, le script récupère toutes les bases de données depuis l'URL *https://update1-sns.stormshieldcs.eu/package*. Si vous souhaitez spécifier quelles bases de données récupérer, ou une URL différente, modifiez les paramètres du script avant de l'exécuter.
   - Par défaut, le script utilise le dossier de destination */tmp*. Si l'espace disque est insuffisant dans le dossier */tmp*, le script échoue. Spécifiez alors un dossier de destination différent avec l'option "`-t`" du script.
     Pour plus d'informations, consultez l'aide du script `activeupdate-fetch.sh -h`.
6. Dans le champ **Données Active Update**, sélectionnez l'archive générée par le script.
7. Cliquez sur **Mettre à jour les bases**.
8. Répétez cette procédure régulièrement pour que les bases de données Active Update soient toujours à jour sur le point de distribution SMC.

4.13.2 Utiliser le serveur Active Update de SMC

Une fois les bases de données téléchargées sur le serveur SMC, vous devez configurer les firewalls SNS pour qu'ils utilisent ce dernier en tant que serveur Active Update. Cette configuration peut se faire manuellement si vous avez peu de firewalls SNS, ou automatiquement via un script.

Les fichiers suivants dans le répertoire */etc/certs/activeupdate* sont utilisés pour la négociation TLS :

- *server.crt* : certificat du serveur,
- *server.key* : clé privée du serveur,
- *activeupdate-ca.crt* : autorité de certification générant le certificat du serveur,
- *activeupdate-ca.key* : clé privée de l'autorité de certification.

Ils sont générés au premier lancement de SMC. Le certificat de l'autorité est auto-signé.

En cas de mise à jour de SMC, les fichiers par défaut sont automatiquement mis à jour également.

Le tableau suivant indique les versions minimum de SMC requises si vous utilisez le serveur Active Update de SMC avec les certificats par défaut :

Version SNS	Version SMC minimum
5.1.x et supérieures	3.9.2
4.3.x à partir de 4.3.31 4.8.x à partir de 4.8.7 5.0.x	3.9.1
Toutes les autres versions à partir de 4.3.0	3.1.0

Vous pouvez remplacer les certificats par défaut par votre propre autorité de certification et votre certificat de serveur. Redémarrez alors le serveur SMC avec la commande `nrestart smc` après les avoir remplacés.

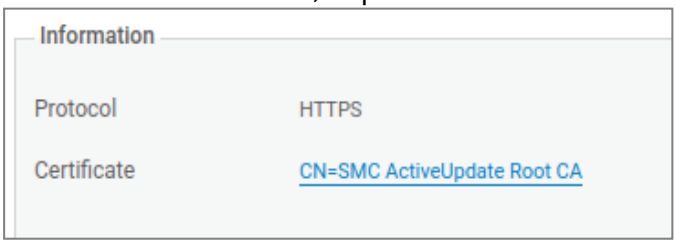
En cas de mise à jour de SMC, vos fichiers personnalisés sont conservés.

Configurer les firewalls SNS manuellement

1. Dans l'interface web du serveur SMC, sélectionnez le menu **Configuration > Serveur Active Update**.
2. Dans la colonne **URL de contact**, cliquez sur l'URL pour la copier.
3. Sur chaque firewall SNS, déclarez le serveur SMC en tant que serveur de mise à jour Active Update en indiquant son URL précédemment copiée. Pour plus de renseignements sur l'Active Update, consultez le *Manuel Utilisateur SNS*.
4. Créez l'objet statique utilisé dans l'URL copiée à l'étape 2 et affectez-lui l'adresse IP utilisée pour contacter le serveur SMC.

Configurer les firewalls SNS automatiquement

1. Importez d'abord le certificat Active Update de SMC sur chaque firewall SNS :
   a. Dans l'interface web du serveur SMC, sélectionnez le menu **Configuration** > **Serveur Active Update**.
   b. Dans la zone **Informations**, cliquez sur **Certificat du serveur** pour télécharger le certificat.



   c. Créez le script de configuration Active Update avec les commandes décrites dans l'exemple suivant en remplaçant si besoin `server.crt` par le nom de fichier de votre certificat :

```
PKI IMPORT format=pem type=ca $FROM_DATA_FILE("activeupdate-ca.crt")
```

   d. Suivez les étapes habituelles d'exécution d'un script comme indiqué dans la section Exécuter le script CLI SNS depuis l'interface web en sélectionnant le fichier du certificat dans le menu **Pièces jointes liées au script**.

2. Créez des objets sur les firewalls SNS, permettant de vérifier le certificat de SMC :
   a. Créez le script de création d'objets avec les commandes décrites dans l'exemple suivant.
   ```
   CONFIG OBJECT HOST NEW name=activeupdate0.smc.local ip=<[private
   or public SMC server IP address]> resolve=static update=1
   CONFIG OBJECT HOST NEW name=activeupdate1.smc.local ip=<[private
   or public SMC server IP address]> resolve=static update=1
   CONFIG OBJECT ACTIVATE
   ```
   La valeur du paramètre `name` est composé d'un nom d'objet de votre choix suivi du nom de domaine. L'adresse IP privée est celle qui est visible dans la colonne **Adresse IP** du panneau **Configuration > Serveur Active Update** de SMC.
   b. Suivez les étapes habituelles d'exécution d'un script comme indiqué dans la section Exécuter le script CLI SNS depuis l'interface web
3. Créez le script de configuration Active Update avec les commandes décrites dans l'exemple suivant.
   ```
   CONFIG AUTOUPDATE SERVER
   url=https://activeupdate0.smc.local:8081/activeupdate
   CA="CN=SMC ActiveUpdate Root CA" state=on
   CONFIG AUTOUPDATE ACTIVATE
   ```
   Vous trouverez la valeur des paramètres `url` et `CA` dans les champs **URL de contact** et **Certificat du serveur** du panneau **Configuration > Serveur Active Update**.
   Vous pouvez ajouter des paramètres personnalisés au script. Pour plus d'informations, reportez-vous au guide *CLI Serverd Commands Reference Guide*.

   ASTUCE
   Pour spécifier plusieurs URL et plusieurs CA, séparez-les par une virgule :
   ```
   url=https://activeupdate0.smc.local:8081/activeupdate,https://ac
   tiveupdate1.smc.local:8081/activeupdate/activeupdate
   CA="CN=*.smc.local,CN=*.smc.local" state=on
   ```
4. Suivez les étapes habituelles d'exécution d'un script comme indiqué dans la section Exécuter le script CLI SNS depuis l'interface web.

4.13.3 Personnaliser les paramètres Active Update

Certains paramètres Active Update, tels que le numéro de port auquel les firewalls SNS doivent se connecter ou la fréquence de mise à jour automatique, ne sont pas configurables par l'interface web SMC. Vous pouvez néanmoins modifier ces paramètres dans un fichier de configuration.

Ce fichier permet également d'indiquer un proxy HTTPS à joindre pour servir de lien entre SMC et le serveur de mise à jour Stormshield, si vous le souhaitez.

ATTENTION
Seuls les proxy HTTPS sont supportés avec cette fonctionnalité. Vous ne pouvez pas utiliser de proxy HTTP.

1. Ouvrez le fichier */data/config/activeupdate/config.ini*.

```
[General]
State=false
Port=8081
Host=0.0.0.0

[Sync]
Source=https://update1-sns.stormshieldcs.eu/package
Categories=ALL
Tries=3
AutoUpdate=false
AutoUpdatePeriod=0 */3 * * *

[Proxy]
Host=
Port=
User=
Password=
CAPath=
```

2. Modifiez les paramètres souhaités :

State	Activation du serveur Active Update sur SMC.
Port	Port du serveur SMC sur lequel les firewalls SNS doivent de connecter.
Host	Noms des interfaces réseau ou adresses IP portées par des interfaces existantes sur le serveur, sur lesquelles le serveur SMC écoute. Remplacez par exemple la valeur 0.0.0.0 par `eth0` ou `192.168.7.54` pour indiquer que seules ces interfaces sont utilisées.
Source	URL du serveur Stormshield à partir duquel sont téléchargées les bases Active Update.
Categories	Liste des bases Active Update que vous souhaitez télécharger sur le serveur SMC. Les valeurs des catégories sont les suivantes. Séparez les valeurs par des virgules.

Catégorie de base de données	Valeur
Toutes les bases de données	ALL
Antispam : listes noires DNS	ANTISPAM
Antispam : moteur heuristique	VADERETRO
Base URL embarquée	URLFILTERING
Antivirus : signatures antivirales Clamav	CLAMAV
Antivirus : signatures antivirales de l'ancien service d'Antivirus Avancé	KASPERSKY
Antivirus : signatures antivirales du nouveau service d'Antivirus Avancé	ADVANCEDAV1
IPS : signatures de protection contextuelles	PATTERNS
Autorités de certification racine	ROOTCERTS
Géolocalisation / Réputation IP publique	IPDATA
Management des vulnérabilités	SEISMO
Icônes des applications et services Web	METADATA

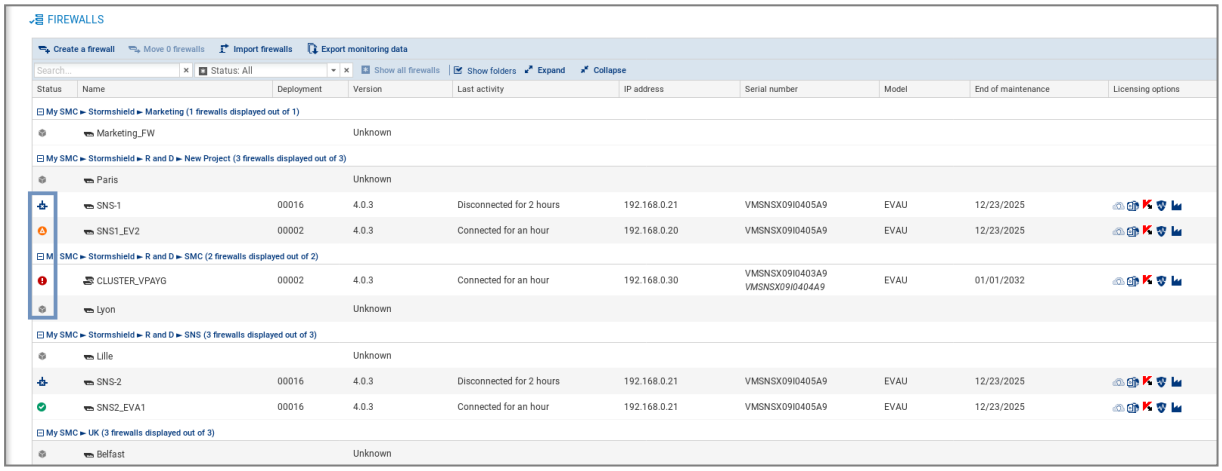
Tries	Nombre de tentatives en cas d'échec de mise à jour des bases.
AutoUpdatePeriod	Fréquence de mise à jour des bases. Les valeurs possibles sont de type CRON. Par défaut, `0 */3 * * *` signifie que les bases sont mises à jour toutes les 3 heures.
Host	Adresse ou nom du serveur proxy HTTPS. Peut être une adresse IP ou un nom FQDN. Seuls les proxy HTTPS sont supportés.
Port	Numéro de port d'écoute du serveur proxy.
User	Nom d'utilisateur pour s'authentifier sur le serveur proxy, s'il requiert une authentification.

Password	Mot de passe pour s'authentifier sur le serveur proxy, s'il requiert une authentification.
CAPath	Chemin vers le certificat de l'autorité de certification (CA) ayant signé le certificat présenté par le serveur proxy.

3. Sauvegardez le fichier. Les modifications sont immédiatement prises en compte.
4. Uniquement si vous avez modifié le paramètre `State`, redémarrez le serveur SMC avec la commande `nrestart smc`.

4.14 Configurer l'avertissement de l'expiration proche des certificats

Lorsque le certificat d'un firewall SNS est proche de l'expiration, l'état de santé affiché par le firewall dans l'écran de supervision des firewalls passe en **Non critique**.



Lorsque le certificat est expiré, le firewall affiche un état de santé **Critique**.

Par défaut, le firewall affiche un état **Non critique** à partir de 30 jours avant l'expiration du certificat.

La variable d'environnement `SMC_SNS_CERTS_PROBE_EXPIRATION_INT` permet de configurer ce délai. La valeur minimale acceptée est un jour.

Pour modifier le délai de 30 jours par défaut :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Modifiez la valeur de la variable d'environnement `SMC_SNS_CERTS_PROBE_EXPIRATION_INT`. Par exemple : `SMC_SNS_CERTS_PROBE_EXPIRATION_INT= 20`
3. Redémarrez le serveur avec la commande `nrestart smc`
4. Redéployez la configuration sur les firewalls.

L'expiration proche des certificats est également signalée dans le panneau **Configuration** > **Certificats**.

Si vous modifiez le délai d'avertissement, tant que la configuration n'est pas redéployée sur les firewalls, il y a un décalage possible entre le statut des certificats indiqués dans le panneau **Certificat** (information fournie par le serveur SMC) et l'état de santé des firewalls indiqué dans le panneau de supervision (information fournie par les firewalls).

Pour plus d'informations sur le panneau **Certificats**, reportez-vous à la section Gérer les certificats et les autorités de certification.

4.15 Configurer l'avertissement de l'expiration proche des options de licence

Les icônes d'état affichées dans le bandeau supérieur de l'interface ainsi que la colonne **Options de licence** dans le panneau de supervision des firewalls peuvent afficher un état **Critique** ou **Non critique** lorsque les options de licence souscrites (Breach Fighter, Extended Web Control, Antivirus Avancé, Stormshield Vulnerability Manager, Industrial Security Pack) sont expirées ou proches de l'être.

Par défaut, cet avertissement est désactivé.

Les variables d'environnement `SMC_FW_LICENSE_WARNING_INT` et `SMC_FW_LICENSE_CRITICAL_INT` permettent d'activer l'avertissement et de configurer les délais.

Pour activer l'avertissement :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Ajoutez les variables d'environnement `SMC_FW_LICENSE_WARNING_INT = 90` et `SMC_FW_LICENSE_CRITICAL_INT = 30`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

Dans cet exemple, un firewall affiche un état **Non critique** à partir de 90 jours avant l'expiration des options de licence et **Critique** à partir de 30 jours avant l'expiration des options de licence.

4.16 Désactiver la protection des certificats par TPM (Trusted Platform Module) lors de l'installation sur le firewall

Les firewalls SNS proposent la protection des certificats par module TPM.

Lorsque vous installez une identité (format *.p12*) sur un firewall SNS depuis le serveur SMC, la protection de la clé privée par module TPM est activée par défaut. La clé privée est protégée par un mot de passe stocké sur le module TPM.

Dans SMC, les clés protégées par TPM ne sont utilisables que dans des topologies VPN IPsec avec des profils de chiffrement de type IKEv2.

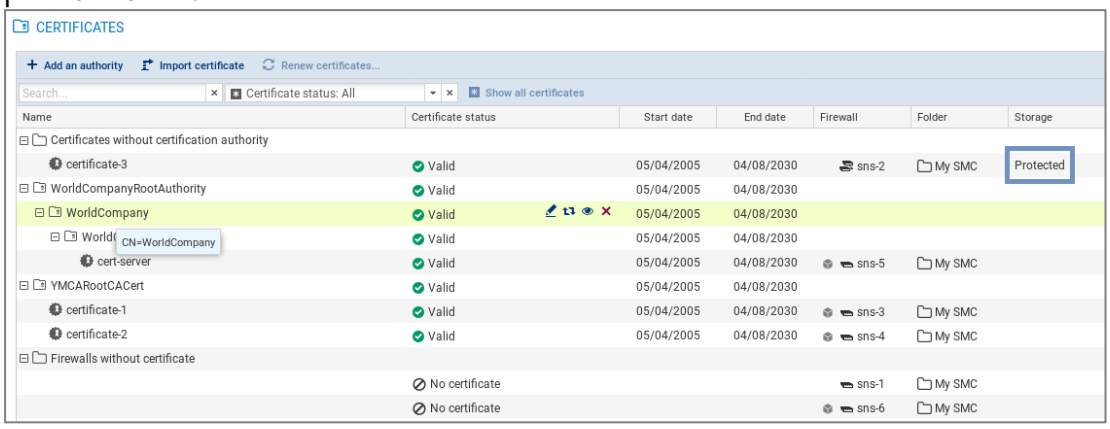
Pour créer des topologies VPN avec des profils de type IKEv1, vous devez désactiver cette protection avec la variable d'environnement `SMC_FW_TPM_ENABLED`.

4.16.1 Savoir si une clé privée est protégée par TPM

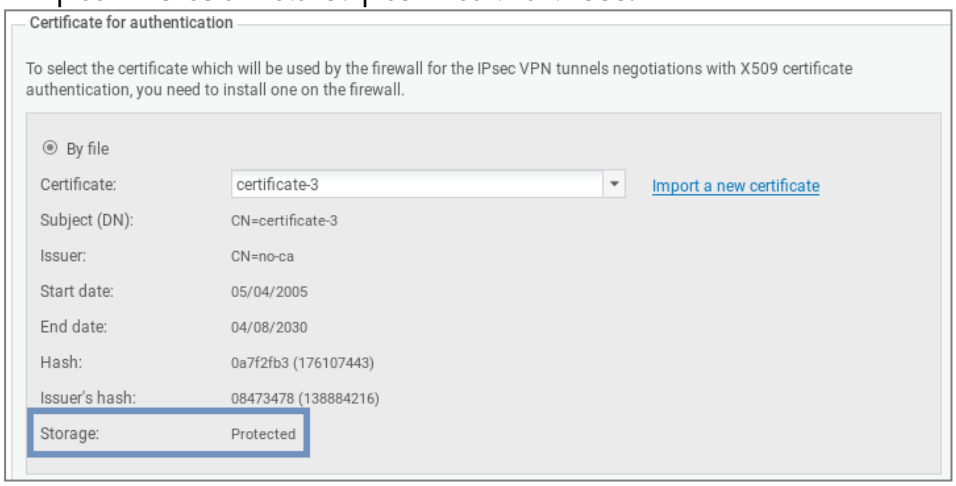
Dès lors que le module TPM est présent et activé sur un modèle de firewall SNS, lorsque vous installez une identité sur un firewall depuis le serveur SMC, la clé privée correspondante est protégée par le module TPM.

Pour savoir si une clé privée est protégée par module TPM, consultez les panneaux suivants dans l'interface web d'administration du serveur SMC :

- Dans le menu **Configuration** > **Certificats**, affichez la colonne **Stockage** (masquée par défaut). La mention **Protégé** est indiquée dans la colonne lorsqu'une clé privée est protégée par module TPM.



- Dans l'onglet **Système > VPN IPsec** des propriétés d'un firewall, la mention **Protégé** est indiquée dans les caractéristiques du certificat X509.



Lorsque vous installez un nouveau certificat sur un firewall, la mention est également indiquée dans la fenêtre de résultat de l'installation du certificat.

4.16.2 Désactiver la protection de la clé privée par TPM

Pour désactiver la protection par TPM lorsque vous installez une identité sur un firewall SNS depuis le serveur SMC, vous devez modifier la variable d'environnement `SMC_FW_TPM_ENABLED` :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez la valeur de la variable d'environnement : `SMC_FW_TPM_ENABLED=false`
3. Redémarrez le serveur avec la commande `nrestart smc`.

4.16.3 Activer la protection par TPM d'une clé privée déjà existante

- Pour activer la protection par TPM d'une clé privée déjà installée sur un firewall, exécutez le script CLI SNS suivant depuis le menu **Scripts/Scripts CLI SNS** :

```
PKI CERTIFICATE PROTECT caname=<CA_name> name=<certificate_CN> tpm=ondisk
```

4.17 Choisir le caractère délimiteur dans les fichiers CSV

Dans SMC, vous pouvez utiliser des fichiers *.csv* pour importer ou exporter des firewalls, des règles de filtrage, des objets par exemple.

La variable d'environnement SMC_CSV_DELIMITER permet de définir le caractère délimiteur utilisé pour tous les exports et imports de fichiers *.csv*.

Le caractère par défaut est la virgule.

Pour le modifier :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez la valeur de la variable d'environnement : `SMC_CSV_DELIMITER=",`".
3. Redémarrez le serveur avec la commande `nrestart smc`.

5. Gérer les objets

Le menu de gauche **Objets** permet de créer, de modifier ou de supprimer un objet de la configuration déployée sur les firewalls.

Tous les objets créés à partir du serveur SMC appartiennent à la politique globale du firewall. Ils sont disponibles dans l'interface web d'administration du firewall.

Pour plus de renseignements sur les objets globaux, consultez le *Manuel Utilisateur SNS*.

Vous pouvez modifier ou supprimer un objet seulement dans les deux cas suivants :

- il n'est utilisé dans aucune configuration de firewall,
- il est utilisé dans la configuration de firewalls sur lesquels vous avez le droit d'accès en écriture.

Pour vérifier l'utilisation d'un objet, reportez-vous à la section Vérifier l'utilisation d'un objet dans la configuration

Si vous avez besoin de modifier un objet existant pour l'utiliser dans la configuration de vos firewalls et qu'il est utilisé dans la configuration d'un firewall sur lequel vous n'avez pas le droit d'accès en écriture, la modification est refusée. Nous vous recommandons de le dupliquer. Pour cela, rendez-vous dans le panneau de modification de l'objet.

Pour plus d'informations sur la restriction des droits d'accès, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

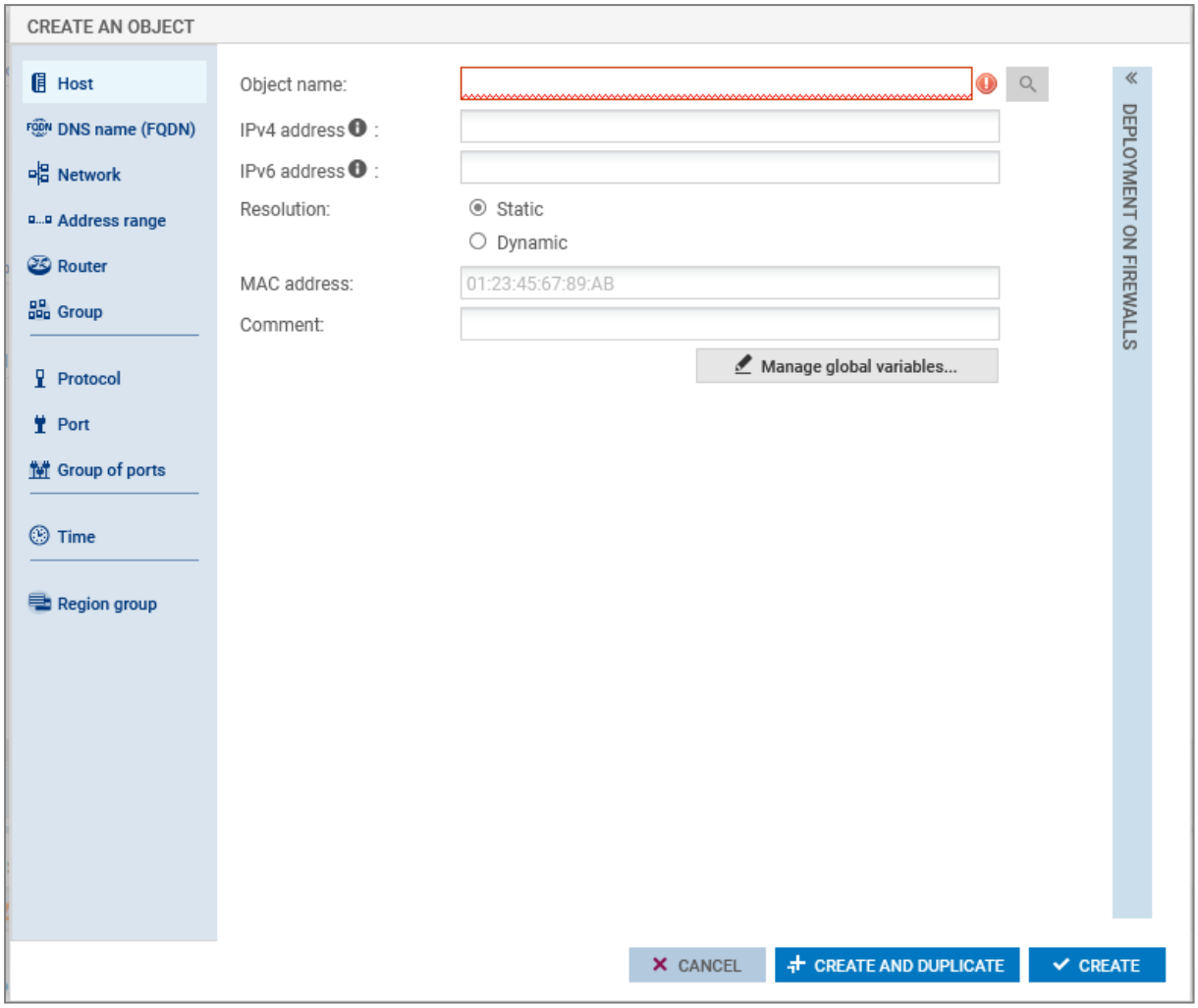
IMPORTANT
Avant de supprimer un objet du serveur SMC, vérifiez l'impact que sa suppression peut avoir sur le fonctionnement de vos firewalls.

5.1 Déployer les objets sur les firewalls

Après avoir créé ou configuré vos objets dans le menu **Objets**, vous pourrez choisir leur mode de déploiement sur les firewalls.

Par défaut, un objet n'est déployé que sur les firewalls qui l'utilisent. Vous pouvez cependant forcer son déploiement sur certains firewalls ou sur tous les firewalls :

1. Dans la fenêtre de création ou modification d'un objet, cliquez sur **Déploiement sur les firewalls** à droite.



2. Choisissez de forcer le déploiement sur une sélection de firewalls ou sur tous les firewalls.
3. Déployez la configuration.

Dans la liste des objets du menu **Objets**, des icônes permettent de distinguer les objets dont le déploiement a été forcé sur une sélection de firewalls ( ) ou sur tous les firewalls ( ).

5.2 Créer des objets variables

Les objets variables sont des objets de type Machine, Réseau et Plage d'adresses IP dont l'adresse IPv4 ou IPv6 prend une valeur différente selon le firewall sur lequel ils sont installés.

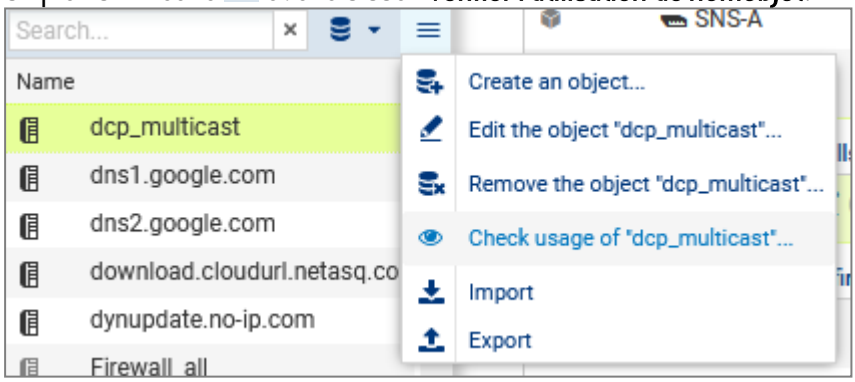
1. Dans le menu **Objets**, créez un objet Machine, Réseau ou Plage d'adresses IP.
2. Remplissez le champ **Adresse IPv4** ou **Adresse IPv6** en utilisant une variable %CUSTOM_X%. La valeur de cette variable personnalisée est définie dans l'onglet **Variables personnalisées** du panneau **Modifier le firewall** accessible en double-cliquant sur la ligne d'un firewall dans la vue de supervision.
   - Vous pouvez consulter la liste des variables disponibles en cliquant sur le bouton **Gérer les variables globales**. Utilisez le bouton **Copier dans le presse-papier** pour les copier ensuite dans le champ souhaité.

   > **EXEMPLE**
   > Entrez l'adresse 10.1.%CUSTOM_IP%.0/24. Si pour un firewall donné, la variable personnalisée vaut "1" dans ses paramètres, l'adresse vaudra 10.1.1.0/24 pour ce firewall dans la règle de filtrage ou dans la topologie VPN.
3. Terminez la création de l'objet.

Pour plus d'informations sur les variables personnalisées, reportez-vous à la section Créer des variables personnalisées.

5.3 Vérifier l'utilisation d'un objet dans la configuration

1. Dans le menu **Objets**, sélectionnez un objet.
2. Cliquez sur l'icône ☰ et choisissez **Vérifier l'utilisation de *nomobjet***.



3. Dans le panneau des résultats qui s'ouvre dans la partie inférieure de l'écran, vous avez la possibilité de cliquer sur les éléments pour les afficher et les modifier.

5.4 Importer des objets

> **ATTENTION**
> Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour importer rapidement un grand nombre d'objets déjà existants sur les firewalls SNS ou pour créer facilement des objets, vous pouvez utiliser un fichier CSV et l'importer sur le serveur SMC depuis l'interface web ou depuis l'interface de ligne de commande.

À l'aide de ce fichier, vous pouvez entre autres spécifier les firewalls sur lesquels déployer chaque objet.

Un exemple de fichier CSV "example-import-objects.csv" est disponible sur le serveur, dans le dossier */opt/stormshield/examples/csv/*.

5.4.1 Créer le fichier CSV

Vous pouvez soit exporter des objets existants depuis un firewall soit créer un nouveau fichier CSV.

Pour exporter le fichier CSV depuis un firewall :

1. Connectez-vous au firewall,
2. Allez dans le menu **Objets** > **Objets**,
3. Cliquez sur le bouton **Exporter**.

Ce fichier contient l'ensemble des objets et groupes réseau de votre firewall.

IMPORTANT
Si vous modifiez un fichier CSV exporté depuis un firewall, vérifiez que le logiciel d'édition n'a pas modifié le contenu du fichier. L'import sur le serveur SMC risque de ne pas être possible sinon.

Pour créer un nouveau fichier CSV, afin de connaître le détail des lignes d'en-têtes et des paramètres à préciser en fonction de la catégorie de l'objet, vous pouvez :

- Vous inspirer d'un export d'objets depuis un firewall,
- Consulter l'exemple disponible directement sur le serveur SMC comme indiqué ci-dessus.

Spécifier les firewalls sur lesquels déployer les objets

Par défaut, un objet n'est déployé que sur les firewalls qui l'utilisent. Vous pouvez cependant indiquer dans le fichier CSV les firewalls sur lesquels forcer son déploiement en utilisant la colonne *#deployment*.

Exemple de création d'objets Machine :

1. Saisissez les paramètres suivants dans les colonnes de l'en-tête du fichier :
```
#type,#name,#ip,#ipv6,#resolve,#mac,#deployment,#comment
```
2. Saisissez les valeurs correspondantes aux paramètres sur les lignes suivant l'en-tête pour chaque objet Machine à importer (exemple) :
```
host,dns1.google.com,8.8.8.8,2001:4860:4860::8888,,,ALL,"Google
Public DNS Server"
```

Les valeurs possibles du paramètre *#resolve* sont "dynamic" ou "static".

Les valeurs possibles du paramètre *#deployment* sont :

- Vide ou DEFAULT : comportement par défaut, l'objet n'est déployé que sur les firewalls qui l'utilisent.
- ALL : l'objet est déployé sur tous les firewalls.
- "Firewall 1,Firewall 2" : liste de noms de firewalls entre guillemets et séparés par une virgule. L'objet est déployé sur ces firewalls et sur les firewalls qui l'utilisent.

5.4.2 Importer des objets depuis l'interface web

Pour importer des objets depuis l'interface web :

1. Dans le menu **Objets**, cliquez sur l'icône ☰.
2. Choisissez **Importer**.
3. Sélectionnez le fichier CSV à importer.
4. Si besoin, cochez l'option permettant de mettre à jour des objets qui existent déjà en les remplaçant par les objets contenus dans le fichier.

En cas d'erreur, consultez le résumé de l'import.

Aucune autre action ne peut être effectuée sur le serveur pendant l'import d'objets.

5.4.3 Importer des objets en ligne de commande

1. Commencez par copier le fichier CSV sur le serveur SMC à l'aide du protocole SSH, dans le répertoire */tmp* par exemple.
2. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
3. Pour importer tous les types d'objets, tapez la commande :
   `smc-import-objects --csv-file /tmp/fichier.csv`.
4. Pour voir les objets importés dans l'interface web de SMC, rafraîchissez la page ou déconnectez-vous et reconnectez-vous.

Un statut d'import s'affiche pour chaque objet ou groupe, ainsi qu'un résumé à la fin de l'exécution de l'import.

Vous avez également la possibilité de choisir les types d'objets à importer.

EXEMPLE
Pour importer seulement les objets de type Machine et Plage d'adresses IP d'un fichier CSV, entrez la commande :
`smc-import-objects --csv-file /tmp/fichier.csv --host --range`

Les commandes à entrer selon le type d'objets sont :

Type de l'objet	Commande
Machine	--host
Nom DNS (FQDN)	--fqdn
Réseau	--network
Plage d'adresses IP	--range
Routeur	--router
SLA	--sla
Groupe [1]	--group
Protocole IP	--protocol
Service (port)	--service
Groupe de ports	--servicegroup
Temps	--time

Les variables personnalisées %CUSTOM_X% peuvent être utilisées à la place des valeurs des adresses IPv4 ou IPv6 dans les objets de type Machine, Réseau et Plage d'adresses IP. Ces variables personnalisées sont définies dans l'onglet **Variables personnalisées** du panneau **Modifier le firewall** accessible en double-cliquant sur la ligne d'un firewall dans la vue de supervision.

Si un objet importé existait déjà dans SMC, une erreur s'affiche. Vous pouvez utiliser l'option `--update` pour écraser l'objet existant par celui indiqué dans le fichier CSV.

[1] Dans le cas de l'import d'un groupe, les objets compris dans le groupe doivent déjà être présents sur le serveur SMC, sinon le groupe ne sera pas créé. Importez-les préalablement via un autre fichier CSV ou créez-les manuellement dans l'interface web.

5.5 Exporter des objets

Le serveur SMC permet d'exporter le contenu complet de votre base d'objets au format CSV.

Un accès en lecture simple suffit pour exporter des objets.

1. Dans le menu **Objets**, cliquez sur l'icône ☰.
2. Choisissez **Exporter**.
3. Sauvegardez le fichier CSV.

5.6 Utiliser les objets implicites depuis SMC

La base d'objets de SMC comprend par défaut des objets Firewall_xx et Network_xx correspondant aux interfaces réseau des firewalls administrés. Par exemple, les objets Firewall_in et Firewall_out.

Ces objets implicites n'ont pas de valeur définie et ne sont pas déployés par SMC sur les firewalls.

Vous pouvez créer d'autres objets implicites manuellement. Ils doivent correspondre à une interface connue lorsqu'ils sont utilisés dans la configuration d'un firewall. Leur valeur est remplacée dans la configuration par l'adresse de l'interface réseau du firewall portant le même nom. Si aucune interface réseau du firewall ne porte le même nom, le déploiement de la configuration échoue.

Si vous renommez l'interface réseau d'un firewall localement ou via SMC lorsqu'il gère la configuration réseau, les objets Firewall_xx et Network_xx correspondants ne sont pas automatiquement renommés sur SMC ni mis à jour dans les règles ou politiques dans lesquelles ils sont utilisés. Nous vous recommandons de réaliser cette opération manuellement pour éviter des erreurs de configuration. Nous vous recommandons de suivre les étapes suivantes lorsque le réseau de votre firewall est géré par SMC:

1. Localement sur le firewall concerné, modifiez le nom de l'interface,
2. Sur SMC, forcez la récupération de la configuration des interfaces et du routage depuis le menu **Système** > **Configuration** des paramètres du firewall,
3. Sur SMC, créez les objets Firewall_xx et/ou Network_xx portant le nouveau nom de l'interface.
4. Si les précédents objets implicites portant l'ancien nom sont utilisés dans la configuration du firewall concerné, remplacez-les par les nouveaux objets.
5. Déployez la configuration.

6. Configurer le réseau et le routage

SMC permet de gérer de façon centralisée les interfaces et routes de vos firewalls SNS. Les interfaces et routes déjà configurées sur les firewalls sont automatiquement récupérées sur SMC. Vous pouvez en créer de nouvelles et les déployer sur les firewalls.

SMC permet également de mettre en œuvre la fonctionnalité SD-WAN sur votre parc. Celle-ci garantit la sélection des meilleurs liens en fonction du type de trafic grâce à des critères d'engagement SLA (*Service Level Agreement*) et à des options de supervision des passerelles définies dans les objets Routeurs. Utilisez ces objets dans des règles de filtrage pour mettre en place du routage par politique (PBR - *Policy Based Routing*).

Le menu **Supervision** > **Routeurs** permet de surveiller en temps réel la qualité des connexions et l'état des passerelles associées aux objets Routeurs et déployées depuis SMC.

La configuration des interfaces et des routes depuis SMC est compatible avec les firewalls SNS à partir de la version 4.2.3 en lecture/écriture et de la version 3.7 en lecture seule. La mise en œuvre du SD-WAN est compatible avec les firewalls SNS à partir de la version 4.3.3.

Pour plus d'informations sur la configuration des interfaces, des routes et de la fonctionnalité SD-WAN, reportez-vous au *Manuel Utilisateur SNS* :

- Interfaces,
- Routage,
- SD-WAN et routage par politique (PBR).

6.1 Configurer les interfaces réseau

Depuis le serveur SMC, configurez les interfaces réseau de vos firewalls.

Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers concernés dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

6.1.1 Activer la gestion du réseau d'un firewall SNS par SMC

Allez dans l'onglet **Système** > **Configuration** du firewall concerné et vérifiez que la case **Configurer le réseau pour ce firewall depuis SMC** est cochée pour indiquer que SMC gère le réseau pour ce firewall.

Rendez-vous ensuite dans les onglets **Interfaces** > **Interfaces** et **Interfaces** > **Interfaces IPsec (VTI)** pour configurer les interfaces.

Si cette option n'est pas cochée, SMC ne gère pas le réseau pour ce firewall et l'onglet **Interfaces** du firewall est en lecture seule.

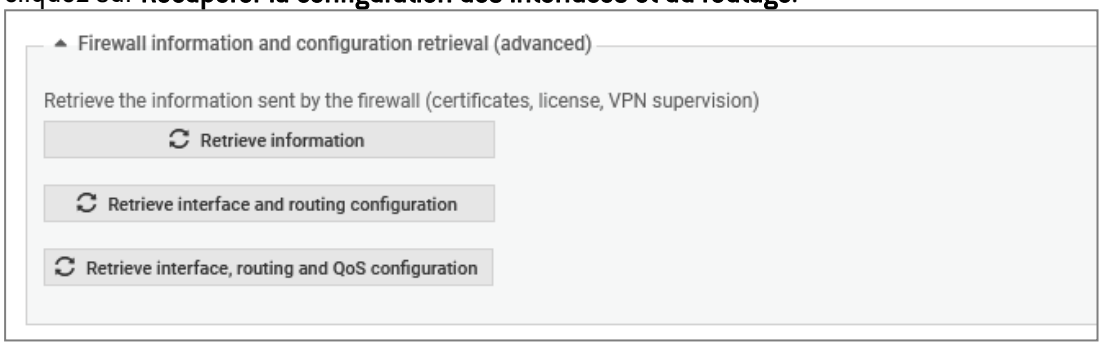
Si vous cochez l'option alors qu'un firewall fait déjà partie d'une topologie VPN par route, les interfaces IPsec (VTI) associées manquantes sont automatiquement créées et affichées dans l'onglet **Interfaces IPsec (VTI)**. Pour plus d'informations, reportez-vous à la section Configurer les interfaces IPsec (VTI).

6.1.2 Forcer la récupération des interfaces du firewall

Lorsque l'onglet **Interfaces** est en lecture seule, les interfaces du firewall sont récupérées par SMC à chaque ouverture de la page de modification des paramètres du firewall. Ce n'est pas le cas lorsque la configuration du réseau et du routage est gérée par SMC.

Vous pouvez alors forcer la récupération de la configuration des interfaces et du routage dans les paramètres du firewall :

1. Rendez-vous dans les paramètres du firewall,
2. Dans l'onglet **Système > Configuration**, cochez la case **Configurer le réseau pour ce firewall depuis SMC** si elle n'est pas déjà cochée,
3. Dépliez l'encart **Récupération des informations et de la configuration du firewall (avancé)** et cliquez sur **Récupérer la configuration des interfaces et du routage**.



Lorsque vous forcez la récupération des interfaces d'un firewall, si le firewall possède des interfaces IPsec virtuelles (VTI), nous vous recommandons de consulter les Journaux du serveur pour vérifier qu'il n'y a pas de conflit de nom d'interface ou d'adresse IP et de masque entre les interfaces IPsec créées sur SMC et les interfaces IPsec créées sur le firewall. Des noms ou adresses identiques pourraient supprimer des interfaces utilisées dans des routes ou règles.

6.1.3 Configurer les interfaces

Le serveur SMC affiche automatiquement les interfaces de votre firewall dans l'onglet **Interfaces > Interfaces** des paramètres du firewall. Vous pouvez ainsi les configurer de manière centralisée. Vous pouvez également en ajouter manuellement. Pour plus d'informations sur la configuration des interfaces, reportez-vous à la section *Interfaces* du *Manuel Utilisateur SNS*.

SMC permet la configuration en IPv4 des interfaces réseau suivantes :

- Interfaces Ethernet
- Bridges
- VLAN
- Agrégats

Trois modes d'agrégat sont possibles :

- LACP, qui est le mode par défaut.
- Failover, uniquement pour les firewalls SNS en versions 4.3 et supérieures.
- Broadcast, uniquement pour les firewalls SNS en versions 4.3.25, 4.7.5, 4.8.1 et supérieures.

Il est également possible de récupérer en lecture seule les interfaces non supportées par SMC (Wi-Fi, dialup, Loopback, GRETUN, GRETAP, USB/Ethernet). Ces interfaces sont affichées en tant que **Autre interface** dans la grille.

Elles ne peuvent pas être modifiées depuis SMC mais vous pouvez les utiliser dans la configuration du routage.

La récupération par SMC des routes affichées dans l'onglet Routage d'un firewall implique la récupération automatique des interfaces. Si des interfaces ont été créées sur SMC mais n'ont pas été déployées, elles seront écrasées par la récupération des routes.

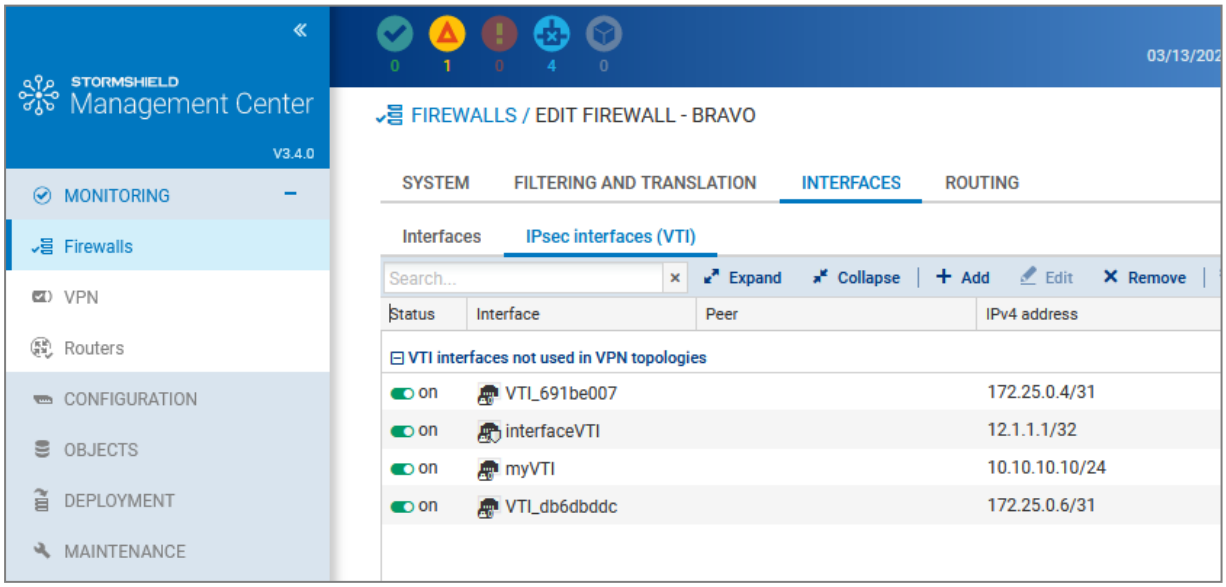
Lors du déploiement de la configuration réseau, les interfaces VLAN, agrégats et bridges présentes sur le firewall ne sont pas conservées. La configuration réseau déployée depuis le serveur SMC est prioritaire et écrase la configuration locale sur le firewall.

Limitations de la configuration des interfaces depuis le serveur SMC

- La configuration en IPv6 n'est actuellement pas supportée.
- Haute disponibilité : Les interfaces réseau utilisées pour les liens de la haute disponibilité sont affichées sur le serveur SMC mais ne sont pas configurables.
- Supervision : La supervision des interfaces depuis le serveur SMC n'est actuellement pas supportée. Pour superviser les interfaces d'un firewall, connectez-vous au firewall en question.
- Configuration des modems : Le mode **Sûreté / Bypass** n'est actuellement pas supporté.
- Pour les interfaces configurées en DHCP, SMC n'affiche pas leurs valeurs détaillées.
- Bridge : Un bridge peut être modifié et supprimé même s'il contient des interfaces qui ne sont pas administrables via le serveur SMC.
- Les interfaces GRE/GRETAP ne sont pas supportées. Les VLAN attachés à un GRETAP ne sont donc pas affichés sur le serveur SMC.

6.1.4 Configurer les interfaces IPsec (VTI)

Le serveur SMC affiche automatiquement les interfaces IPsec de votre firewall dans l'onglet **Interfaces > Interfaces IPsec (VTI)** des paramètres du firewall. Vous pouvez ainsi les configurer de manière centralisée. Le firewall doit être en version 4.2.3 minimum.



Les interfaces IPsec des firewalls peuvent être utilisées dans les topologies VPN par route et dans la configuration de routes et de règles de filtrage PBR (Policy Based Routing).

Pour plus d'informations sur les interfaces IPsec, reportez-vous à la section *Créer ou modifier une interface IPsec (VTI)* du *Manuel Utilisateur SNS* et à la Note technique *Interfaces virtuelles IPsec*.

Les interfaces IPsec affichées dans SMC proviennent de trois sources différentes et les comportements peuvent varier selon que la configuration du réseau du firewall est gérée par SMC ou non :

Le firewall fait partie d'une topologie VPN par route	SMC crée automatiquement les interfaces IPsec associées si la configuration du réseau du firewall est gérée par SMC. Elles sont classées par topologies VPN dans la grille. Vous ne pouvez pas les modifier, ni les supprimer. Le bouton **Voir la configuration VPN** permet de vous rendre sur le panneau de configuration de la topologie VPN concernée.
Les interfaces IPsec ont été créées sur le firewall	SMC les récupère automatiquement lors de la migration de la version 3.3 vers la version 3.4 de SMC, même si la configuration du réseau du firewall n'est pas gérée par SMC. Si la configuration du réseau du firewall est gérée par SMC, vous pouvez forcer la récupération des interfaces à tout moment comme expliqué à la section Configurer les interfaces réseau. Si elles sont utilisées dans une topologie VPN par route créée depuis SMC, elles sont bien associées à la topologie en question dans la grille de l'onglet **Interfaces IPsec (VTI)**. Si la configuration du réseau est gérée par SMC à partir de la version 3.4, nous vous recommandons de ne plus créer directement d'interface IPsec sur les firewalls, elles seraient écrasées au prochain déploiement de configuration.
Les interfaces IPsec ont été créées manuellement depuis SMC	Cela est possible seulement si le réseau du firewall est géré par SMC, à partir de la version 3.4.

Vous pouvez modifier ou supprimer une interface IPsec seulement pour les firewalls dont SMC gère la configuration du réseau, et si elle ne fait pas partie d'une topologie VPN par route.

Concernant les interfaces IPsec utilisées dans des topologies VPN par route, certaines modifications effectuées dans une topologie peuvent avoir un impact sur la configuration des interfaces IPsec. Dans ce cas, l'impact est automatiquement répercuté sur les interfaces IPsec des firewalls dont SMC gère la configuration du réseau.

Dans le cas des firewalls dont SMC ne gère pas la configuration du réseau, les modifications effectuées dans une topologie ont les conséquences suivantes :

- Si vous supprimez une topologie, les interfaces IPsec associées ne sont pas supprimées automatiquement ,
- Si vous modifiez le nom d'une topologie ou d'un correspondant, le commentaire associé à l'interface IPsec et affiché dans l'onglet **Interfaces IPsec (VTI)** n'est pas mis à jour automatiquement,
- Si vous modifiez le plan d'adressage VTI de la topologie, les adresses IP des interfaces IPsec sont modifiées et vous devez répercuter la modification manuellement sur les firewalls SNS.

6.2 Configurer le routage

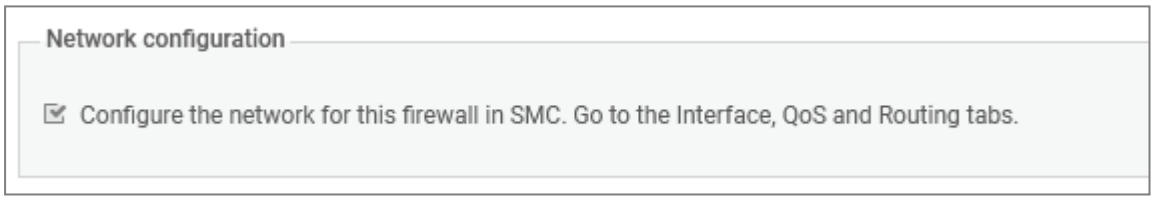
Depuis le serveur SMC, vous pouvez gérer et configurer les routes statiques et dynamiques ainsi que les routes de retour et routes par défaut de vos firewalls à partir de la version 4.2.3.

Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers concernés dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

ATTENTION
À partir de la version 4.8.1 EA de SNS, pour gérer le routage dynamique depuis SMC, la version 3.6 minimum est obligatoire. Déployer des configurations avec du routage dynamique depuis une version de SMC inférieure à la 3.6 sur des firewalls SNS en versions 4.8.1 EA et supérieures n'est pas possible.

6.2.1 Configurer les routes depuis SMC

Rendez-vous dans l'onglet **Système > Configuration** du firewall concerné et vérifiez que la case **Configurer le réseau pour ce firewall depuis SMC** est cochée.



La première fois que vous cochez l'option, SMC récupère automatiquement les routes du firewall dans l'onglet **Routage**, s'il est connecté. SMC récupère également les objets contenus dans les routes.

Dans l'onglet **Routage**, vous pouvez configurer de manière centralisée :

- les routes statiques,
- les routes de retour,
- la route par défaut,
- le routage dynamique.

Routes statiques et de retour	Pour créer de nouvelles routes statiques et de retour, cliquez sur **Ajouter** en haut de la grille.
Routage dynamique	Double-cliquez sur la ligne du routage dynamique dans la grille. Sélectionnez la version BIRD à utiliser (v1 ou v2). Vous pouvez modifier la configuration du routage au format de la version BIRD sélectionnée et sélectionner des options avancées. Pour plus d'informations, reportez-vous à la section Routage dynamique du *Manuel Utilisateur SNS*. **NOTE** SMC ne prend pas en charge l'IPv6 pour la configuration BIRD.
Route par défaut	Double-cliquez sur la ligne dans la grille et sélectionnez une passerelle.

Lors du déploiement de configuration, la configuration réseau déployée depuis SMC est prioritaire sur la configuration locale du firewall et écrase celle-ci.

Pour plus d'informations sur la configuration des routes, reportez-vous à la section *Routage* du *Manuel Utilisateur SNS*.

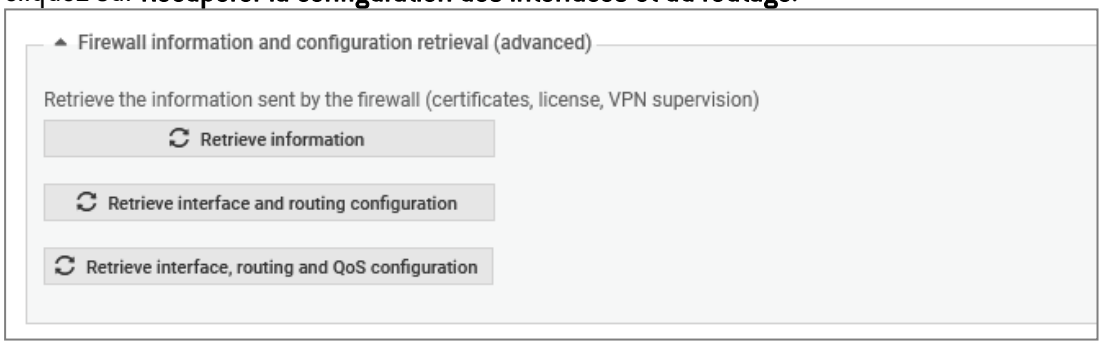
Si la case **Configurer le réseau pour ce firewall depuis SMC** n'est pas cochée, l'onglet **Routage** du firewall est en lecture seule. Les routes du firewall sont alors récupérées par SMC à chaque ouverture de l'onglet. Les objets contenus dans les routes en lecture seule ne sont pas récupérés sur SMC.

6.2.2 Forcer la récupération des routes du firewall

Lorsque l'onglet **Routage** est en lecture seule, les routes du firewall sont récupérées par SMC à chaque ouverture de l'onglet. Ce n'est pas le cas lorsque la configuration du réseau et du routage est gérée par SMC.

Vous pouvez alors forcer la récupération de la configuration des interfaces et du routage dans les paramètres du firewall :

1. Rendez-vous dans les paramètres du firewall,
2. Dans l'onglet **Système > Configuration**, cochez la case **Configurer le réseau pour ce firewall depuis SMC** si elle n'est pas déjà cochée,
3. Dépliez l'encart **Récupération des informations et de la configuration du firewall (avancé)** et cliquez sur **Récupérer la configuration des interfaces et du routage**.



6.2.3 Exporter et importer les routes

Vous pouvez importer manuellement et exporter les routes en ligne de commande.

Exporter les routes

La commande `smc-export-routes` permet de générer un fichier CSV comprenant les routes statiques, de retour et par défaut des firewalls en version 4.2.4 minimum et pour lesquels la gestion de la configuration du réseau depuis SMC est activée.

Par défaut, la commande génère le fichier CSV dans le dossier */tmp*.

Pour exporter les routes d'un firewall :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH,
2. Entrez la commande `smc-export-routes`. Si vous souhaitez modifier le nom par défaut du fichier de sortie (*smc_routes_date.heure.csv*), ajoutez un argument à la commande. Par exemple : `smc-export-routes /data/tmp/mes_routes.csv`.

Importer les routes

La commande `smc-import-routes` permet d'importer sur SMC les routes des firewalls en version 4.2.4 minimum et pour lesquels la gestion de la configuration du réseau depuis SMC est activée, à partir d'un fichier CSV. L'exécution de la commande écrase les routes déjà visibles sur SMC.

EXEMPLE
Un fichier d'import de routes présente la structure suivante :
#firewall,#type,#status,#destination,#gateway,#interface,#comment
SNS1,default,Enabled,any,gateway,auto,
SNS2,reverse,Enabled,,update1-sns.stormshieldcs.eu,out,
...

Pour importer les routes :

1. Pour créer le fichier CSV, vous pouvez exporter les routes comme indiqué ci-dessus et vous inspirer du fichier généré,
2. Copiez le fichier CSV sur le serveur SMC à l'aide du protocole SSH, dans le répertoire */tmp* par exemple,
3. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH,
4. Entrez la commande `smc-import-routes` suivie du chemin vers le fichier CSV en argument.

Si les routes font référence à des éléments de votre configuration SNS qui ne sont pas déjà présents dans la configuration SMC (objets/interfaces), vous devez les importer au préalable sur le serveur.

6.2.4 Limitations de la configuration des routes depuis le serveur SMC

- La configuration en IPv6 n'est actuellement pas supportée.
- SMC peut récupérer les routes d'un firewall SNS et les objets associés via l'activation de la gestion de la configuration du réseau ou bien via la récupération forcée des routes. Si un objet récupéré est déjà présent sur SMC (même type et même nom), les valeurs utilisées dans la configuration sont alors celles de l'objet présent sur SMC.
- Si la passerelle par défaut définie sur un firewall SNS ne correspond pas à un objet présent dans la base d'objets du firewall, la récupération des routes n'est pas supportée. Un log d'erreur est émis dans les logs du serveur expliquant que l'adresse IP doit être représentée par un objet.
- L'utilisation d'objets contenant uniquement des adresses IPv6 ou/et MAC n'est pas supportée.
- L'utilisation d'un objet routeur en tant que passerelle d'une route statique est supportée à partir de la version 4.3.0 des firewalls SNS.
- Routage dynamique - le déploiement de configurations avec du routage dynamique sur des firewalls SNS en versions 4.8.1 et supérieures depuis SMC en versions strictement inférieures à la 3.6 n'est pas supporté.

- Routage dynamique - SMC ne supporte pas les paramètres suivants. En cas de besoin, vous devez les configurer directement depuis le firewall SNS. Ils ne seront pas écrasés par la configuration du routage provenant de SMC :
  - la section "[BGPAuth]",
  - l'exclusion de plages d'adresses IP dans les routes. Pour plus d'informations, reportez-vous à la Base de connaissances Stormshield (anglais uniquement).

6.3 Superviser les objets Routeurs

Le menu **Supervision** > **Routeurs** permet de surveiller la qualité des connexions et l'état des passerelles associées aux objets Routeurs d'un firewall SNS et déployées depuis SMC.

La grille est automatiquement actualisée toutes les 60 secondes.

NOTE
Si vous modifiez un objet Routeur supervisé ou un objet SLA, vous devez redéployer la configuration pour actualiser les données supervisées.

Depuis le panneau de supervision, vous pouvez exporter et télécharger les données de supervision dans un fichier CSV :

1. Cliquez sur **Exporter les données de supervision** en haut du panneau,
2. Sauvegardez le fichier CSV.

Si vous avez filtré les données, seules les lignes visibles dans la grille sont exportées.

Par défaut, les données dans le fichier sont séparées par des virgules. Vous pouvez modifier le délimiteur via la variable d'environnement `SMC_CSV_DELIMITER`.

6.4 Mettre en œuvre la fonctionnalité SD-WAN

Le SD-WAN (*Software Defined Wide Area Network*) est un ensemble de fonctionnalités logicielles facilitant la gestion de réseaux interconnectés et sécurisés ainsi que la gestion de liens WAN multiples.

Une des approches fonctionnelles du SD-WAN consiste à choisir de manière automatique et transparente les liens réseau à emprunter selon l'origine des flux et leurs contraintes de performances associées (latence acceptée, taux de disponibilité...).

SMC permet d'utiliser cette fonctionnalité pour des firewalls SNS à partir de la version 4.3.3.

Pour mettre en œuvre la fonctionnalité SD-WAN sur SMC, créez des objets SLA (*Software Level Agreement*) instaurant des critères d'engagement, puis utilisez-les dans les objets Routeurs. Définissez également des critères de supervision des liens dans les objets Routeurs.

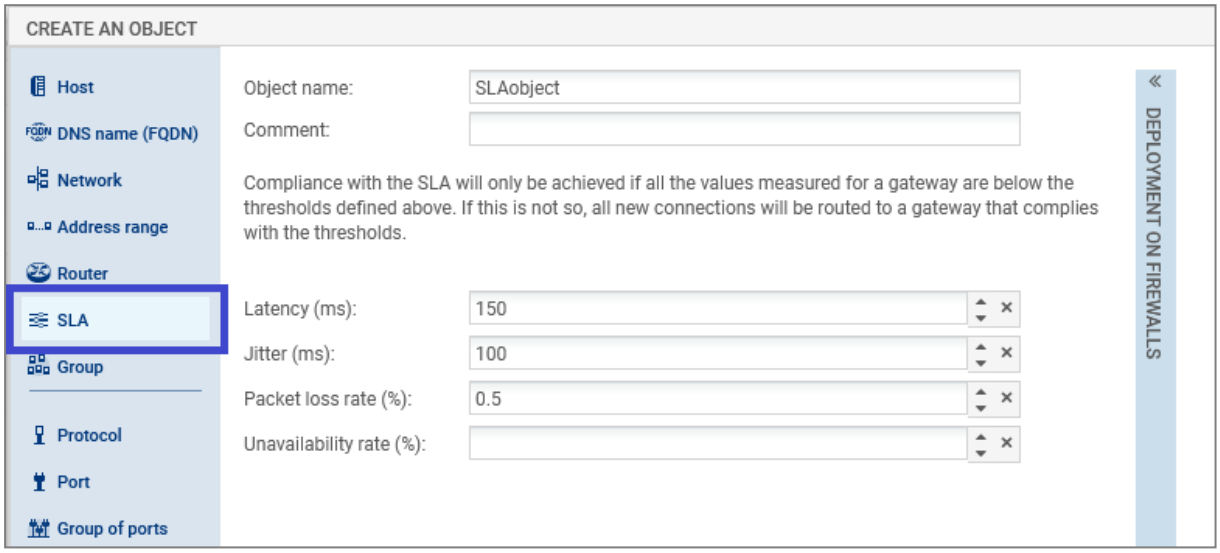
Créez ensuite des règles de filtrage avec ces objets Routeurs pour mettre en place du routage par politique (PBR - *Policy Based Routing*).

EXEMPLE
Créez des règles de filtrage pour optimiser la sélection des liens pour les flux VoIP.

Pour plus d'informations sur la fonctionnalité SD-WAN sur les firewalls SNS, reportez-vous à la Note technique SD-WAN - Sélectionner le meilleur accès réseau.

6.4.1 Créer un objet SLA

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



Pour cela, définissez pour chaque type de trafic un engagement SLA basé sur un ou plusieurs seuils parmi les critères suivants :

- Latence,
- Gigue,
- Taux de perte de paquets,
- Taux d'indisponibilité.

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

Cet engagement SLA est défini au travers d'un objet SLA, que vous pouvez utiliser dans plusieurs objets Routeur.

Pour consulter la définition des quatre critères d'engagement, reportez-vous à la section Routeur du *Manuel Utilisateur SNS*.

Pour créer un objet SLA :

1. Dans le menu **Objets**, créez un objet SLA,
2. Configurez les seuils à ne pas dépasser pour que SMC considère qu'un lien respecte le niveau de qualité attendu et soit emprunté par le trafic. Si ses seuils sont dépassés, le trafic est dirigé vers une autre passerelle qui respecte les critères d'engagement SLA.

Reportez-vous à la section suivante pour utiliser l'objet SLA dans un objet Routeur.

SMC propose deux objets SLA par défaut : Visio et SaaS/Productivity.

NOTE
Les objets SLA ne sont pas visibles sur les firewalls SNS.

6.4.2 Configurer la supervision des liens dans un objet Routeur

Des options de supervision sont disponibles dans les objets Routeurs. Elles permettent de définir la méthode de détection et les paramètres à utiliser pour vérifier la disponibilité des passerelles d'un objet Routeur :

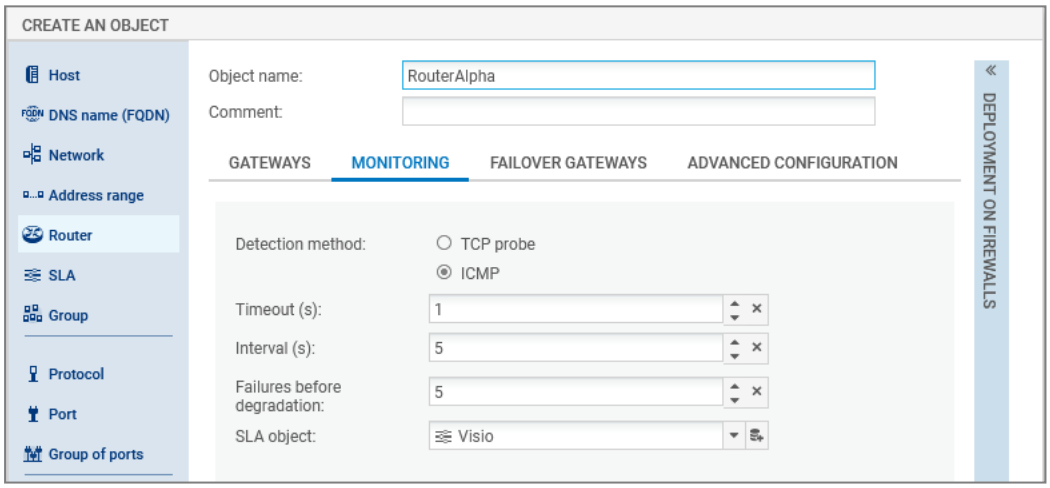
- Méthode de détection,
- Délai d'expiration,
- Intervalle de tests,
- Échecs avant dégradation.

Pour configurer la supervision :

1. Affichez l'onglet **Supervision** d'un objet Routeur,
2. Configurez les paramètres. Pour comprendre les paramètres, reportez-vous à la section Routeur du *Manuel Utilisateur SNS*.

Dans ce même onglet **Supervision**, vous pouvez associer un objet SLA pour définir les seuils à respecter par les passerelles attachées à l'objet Routeur.

Ces paramètres s'appliquent également aux passerelles de secours définies dans l'objet.



Le panneau de supervision des routeurs permet de surveiller l'état des connexions et des passerelles associées à un firewall SNS. Reportez-vous à la section Superviser les objets Routeurs.

NOTE
Si vous modifiez un objet Routeur supervisé ou un objet SLA, vous devez redéployer la configuration pour actualiser les données supervisées.

6.5 Résoudre les problèmes

Consultez cette section pour résoudre les éventuels problèmes rencontrés avec les interfaces et le routage

6.5.1 Vous constatez des erreurs de configuration après avoir renommé une interface depuis SMC

- *Situation* : Vous souhaitez renommer une interface sur un firewall administré par SMC et les objets implicites Firewall_xx et Network_xx découlant de cette interface ne sont pas automatiquement renommés sur SMC. Ceci provoque des erreurs de configuration car les objets ne font plus référence à une interface existante sur le firewall.
- *Cause* : Les objets Firewall_xx et Network_xx sont des objets implicites, pouvant être utilisés dans la configuration de plusieurs firewalls depuis SMC. Ils ne sont pas déployés sur les firewalls. Lorsque vous renommez une interface, ces objets implicites ne sont donc pas automatiquement renommés.
- *Solution* : Pour renommer une interface et contourner le problème, nous vous recommandons de suivre la procédure indiquée dans la section **Utiliser les objets implicites depuis SMC**.

7. Créer et superviser des tunnels VPN

SMC permet de créer et gérer des topologies VPN IPsec site-à-site connectant des réseaux privés via un réseau public de façon sécurisée. Vous pouvez configurer des topologies VPN par politique ou par route :

- Un tunnel VPN par politique relie des réseaux ou sous-réseaux protégés par des firewalls. Il chiffre et encapsule le trafic entre ces réseaux. Ces réseaux sont décrits par une politique. Ce type de topologie correspond à un mode de fonctionnement standard.
- Un tunnel VPN par route utilise des interfaces IPsec virtuelles (VTI - Virtual Tunnel Interface) pour relier des firewalls. Ces interfaces sont vues comme des points d'entrée et de sortie du trafic passant à travers le tunnel et ce trafic est défini par des routes.

Dans les deux cas, les topologies peuvent être en maillage ou en étoile.

SMC version 3.9.4 ne supporte pas les topologies VPN en IPv6. Si une topologie comprend des objets réseau en IPv6, alors ceux-ci sont ignorés au déploiement. Si une topologie s'appuie sur des objets réseau ayant la double configuration IPv4/IPv6, alors seule la configuration en IPv4 est prise en compte et la configuration en IPv6 est ignorée.

Consultez les sections suivantes pour créer des topologies VPN par politique ou par route.

ATTENTION
Pour créer, modifier ou supprimer une topologie VPN, le droit d'accès en écriture sur tous les correspondants est nécessaire. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

7.1 Créer des topologies VPN par politique

SMC permet de créer et gérer des tunnels VPN reliant des réseaux ou sous-réseaux protégés par des firewalls. Ces réseaux sont décrits par une politique.

Ce type de topologie correspond à un mode de fonctionnement standard.

Les firewalls ou passerelles constituent les points d'entrée et de sortie des tunnels et peuvent être :

- Des firewalls SNS en version 3.7 minimum, gérés par le serveur SMC,
- Des correspondants externes, c'est-à-dire des firewalls SNS ou tout autre type de passerelle VPN, non gérés par le serveur SMC.

SMC propose deux formes de topologie VPN : maillage ou étoile.

- Maillage : tous les sites distants sont connectés,
- Étoile : un site central est connecté à plusieurs sites satellites. Les sites satellites ne communiquent pas entre eux. Le site central est obligatoirement un firewall SNS géré par le serveur SMC.

Avant de configurer vos topologies, vous devez :

- Avoir créé vos extrémités de trafic (objets Réseau, Machine ou Groupe) dans le menu **Objets**. Pour plus d'informations, reportez-vous à la section Gérer les objets.
- Avoir créé des objets Machine pour vos correspondants externes si vos topologies en comprennent.

- Dans le cas du choix d'une authentification par certificat X509, avoir importé un certificat pour vos firewalls gérés par SMC compris dans vos topologies et déclaré les autorités de certification. Les procédures correspondantes sont décrites à la section Configurer une topologie par politique en maillage.

Dans cette section, nous décrivons deux cas d'usage, une topologie par politique en maillage et une topologie par politique en étoile. Pour obtenir plus de détails sur chaque menu et option de la configuration des tunnels VPN, consultez le *Manuel Utilisateur SNS*.

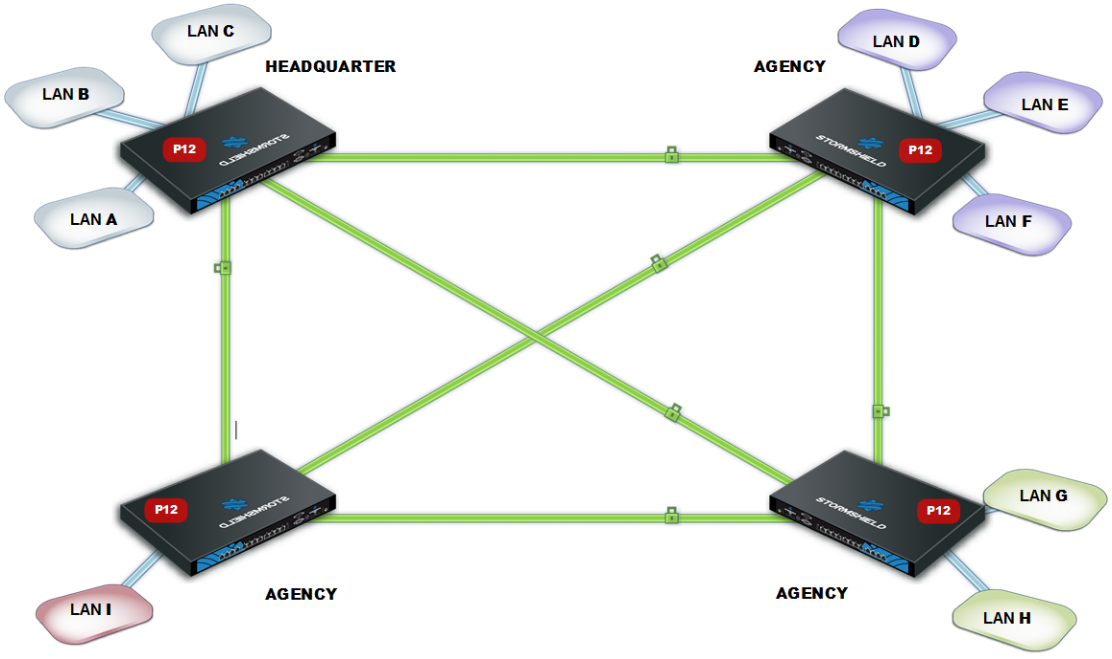
7.1.1 Configurer une topologie par politique en maillage

Exemple de cas d'usage :

Une société possède son siège et deux autres sites en Angleterre, ainsi qu'un site à l'étranger. Chaque site possède son département Recherche et Développement et les quatre sous-réseaux R&D ont besoin de partager des informations. Chaque site est protégé par un firewall géré par le serveur SMC.

Le type d'authentification choisi est l'authentification par certificat X509.

L'autorité de certification qui délivre les certificats peut se trouver sur un des firewalls SNS, celui du siège par exemple, ou bien il peut s'agir d'une autorité externe.



Pour configurer les tunnels VPN entre les quatre sites, suivez les étapes suivantes.

Importer ou déclarer les certificats pour les firewalls SNS

Pour importer ou déclarer un certificat au format PKCS#12 ou PEM depuis l'interface web du serveur SMC, reportez-vous à la section Importer un certificat depuis l'interface web du serveur.

Les certificats peuvent également être importés depuis l'interface de ligne de commande. Reportez-vous à la section Importer un certificat depuis l'interface de ligne de commande.

Déclarer les autorités de certification

Vous devez déclarer sur le serveur SMC les autorités de certification auxquelles les firewalls gérés par SMC font confiance.

Pour que la topologie soit déployée, le serveur SMC doit connaître toute la chaîne de confiance des autorités de certification. Pour plus d'informations et pour savoir comment ajouter une autorité de certification, reportez-vous à la section Gérer les certificats et les autorités de certification.

Indiquer les points de distribution de CRL

Vous devez indiquer au serveur SMC les adresses du ou des points de distribution de la liste de révocation des certificats (CRL) que les firewalls devront utiliser pour chaque autorité déclarée. Ceux-ci peuvent être externes ou bien, vous pouvez définir SMC en tant que point de distribution.

Indiquer les points de distribution externes

1. Dans les propriétés d'une autorité de certification, cliquez sur l'onglet **Liste des points de distribution de CRL**.
2. Ajoutez les adresses du ou des points de distribution externes de la liste de révocation des certificats.

Définir SMC en tant que point de distribution

Le serveur SMC peut faire office de point de distribution de CRL pour des firewalls SNS :

1. Dans les propriétés d'une autorité de certification, cliquez sur l'onglet **SMC en tant que point de distribution de CRL**.
2. Choisissez le fichier de CRL (format *.pem* ou *.der*) à ajouter sur le serveur.
   Le fichier est alors mis à disposition par le serveur SMC pour les firewalls SNS sur l'URI smc://[adresse SMC]:[port SMC]/api/certificates/authorities/[uuid CA].crl.
   La CRL portant une date d'expiration, elle doit être régulièrement importée sur le serveur SMC.
   Le serveur SMC pouvant être contacté sur plusieurs adresses par les firewalls (définies dans le package de rattachement), vous devez indiquer autant d'URI dans cette liste.
   Vous pouvez également importer une CRL sur SMC en ligne de commande, avec la commande `smc-import-crl`.
3. Dans l'onglet **Liste des points de distribution de CRL**, ajoutez cette adresse URI à la liste.
   L'UUID de la CA est indiqué dans l'adresse URL de SMC ainsi que dans l'exemple fourni dans l'onglet.

Créer les objets compris dans la topologie

1. Rendez-vous dans le menu de gauche **Objets**.
2. Créez autant d'objets que d'extrémités de trafic ou de machines qui seront compris dans votre topologie VPN, soit quatre objets dans notre exemple.

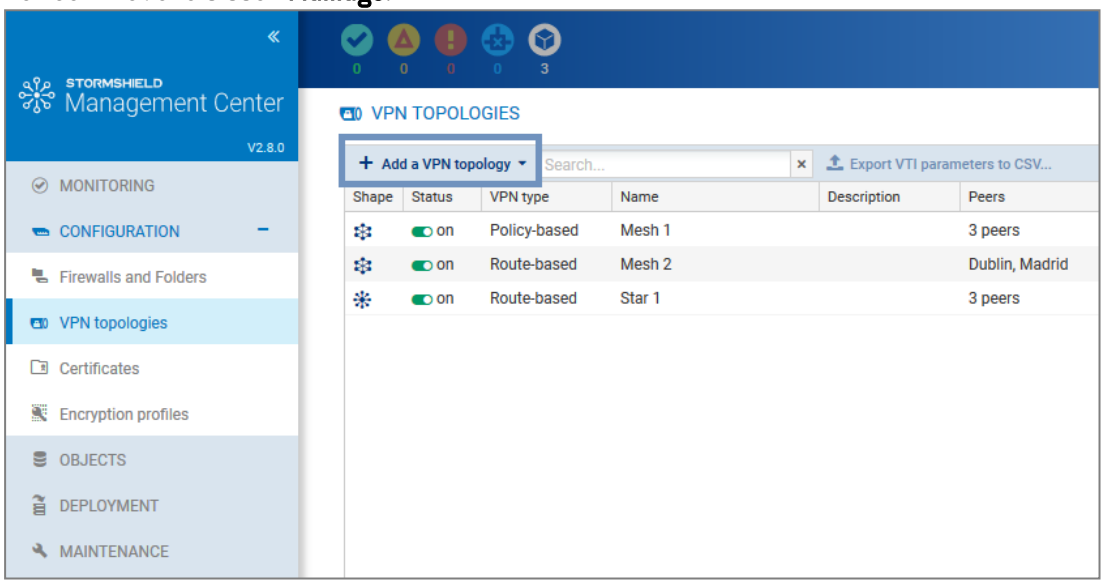
Les objets associés peuvent être de type Réseau, Machine ou Groupe.

IMPORTANT
L'utilisation de groupes contenant des objets variables dans les topologies VPN n'est pas possible. La configuration des tunnels VPN serait invalide.

Créer la topologie VPN

Vous disposez maintenant de tous les éléments nécessaires à la configuration de votre topologie VPN.

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur **Ajouter une topologie VPN** en haut de l'écran et choisissez **Maillage**.



2. Dans la fenêtre qui s'ouvre, choisissez **VPN par politique** et cliquez sur **Créer la topologie**.
3. Entrez un nom. La description est facultative.
4. Choisissez l'authentification par certificat X.509 et sélectionnez les autorités de certification ayant délivré les certificats des firewalls impliqués dans la topologie VPN. Si la CRL d'une autorité a expiré, un avertissement s'affiche dans la liste du menu **Topologies VPN**.
5. Si vous le souhaitez, indiquez un identifiant de clé pré-partagée post-quantique et son mot de passe. Une telle clé permet notamment de se protéger des attaques de type "stocker maintenant, déchiffrer plus tard". Pour plus d'informations, consultez le Manuel Utilisateur SNS. Cette fonctionnalité est disponible uniquement dans le cas de l'authentification par certificat X.509, avec des firewalls en version 4.8.0 minimum et uniquement avec la version IKEv2.
6. Sélectionnez le profil de chiffrement. Le serveur SMC propose des profils pré-configurés. Créez vos profils personnalisés en vous rendant dans le menu **Configuration** > **Profils de chiffrement**. Consultez le *Manuel Utilisateur SNS* pour plus d'informations sur les options des profils de chiffrement.
7. Choisissez les correspondants de votre topologie. Vous pouvez sélectionner des firewalls connectés ou déconnectés. Vous pouvez également sélectionner des firewalls jamais connectés à condition d'avoir défini une adresse IP de contact par défaut personnalisée ou dynamique dans l'onglet **Système** > **VPN IPsec** des paramètres du firewall.
Vous devez posséder le droit d'accès en écriture sur les firewalls que vous souhaitez sélectionner en tant que correspondants. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

8. Choisissez les extrémités de trafic associées à chacun de vos correspondants. Pour plus d'informations sur les paramètres **Adresse de contact** et **Adresse locale**, reportez-vous aux sections Définir l'adresse de contact des firewalls pour les topologies VPN et Choisir l'interface de sortie des firewalls pour les topologies VPN.
9. Cliquez sur **Appliquer**.
10. Déployez la configuration sur les firewalls impliqués dans la topologie. La configuration VPN appartient à la politique globale du firewall.

7.1.2 Configurer une topologie par politique en étoile

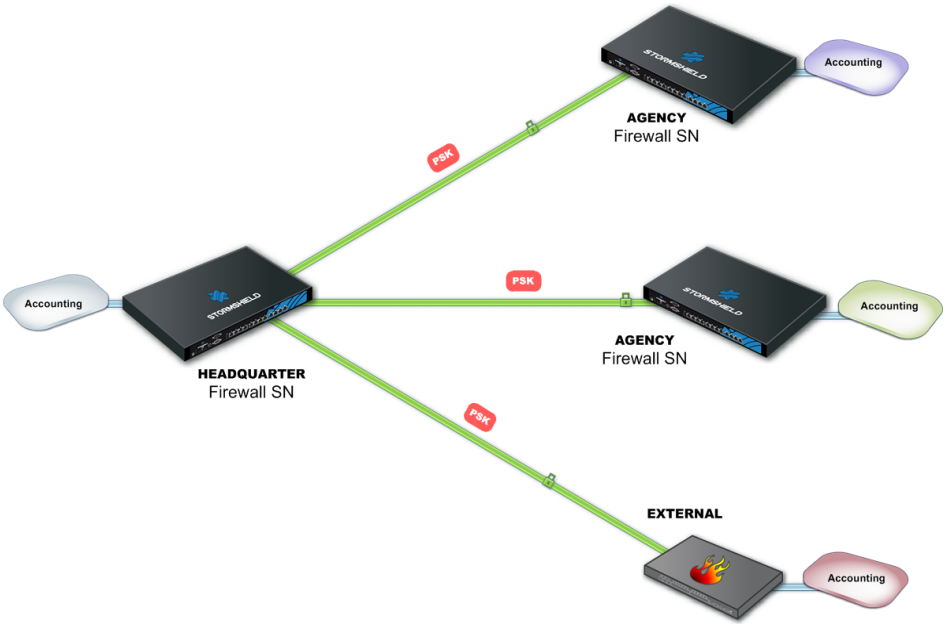
Exemple de cas d'usage :

Une société dont le siège social est à Paris possède deux succursales à Bordeaux et Madrid. Le sous-réseau Comptabilité du siège social doit échanger des informations avec les sous-réseaux Comptabilité des succursales. Les trois sites de la société sont protégés par des firewalls SNS gérés par le serveur SMC.

La société vient d'acquérir une nouvelle entité qui possède également un service Comptabilité et dont le réseau est protégé par un firewall d'un autre fabricant.

L'administrateur doit connaître l'adressage de ce firewall, qui sera déclaré en tant que correspondant externe et l'adressage du sous-réseau.

Le type d'authentification choisi est la clé pré-partagée (PSK - pre-shared key).



Pour configurer les tunnels VPN entre les quatre sites, suivez les étapes suivantes.

Créer les objets compris dans la topologie

1. Rendez-vous dans le menu de gauche **Objets**.
2. Créez autant d'objets que d'extrémités de trafic ou de machines qui seront compris dans votre topologie VPN, soit quatre objets Réseau dans notre exemple.
3. Votre topologie comprend un correspondant externe. Créez un objet Machine pour ce firewall.

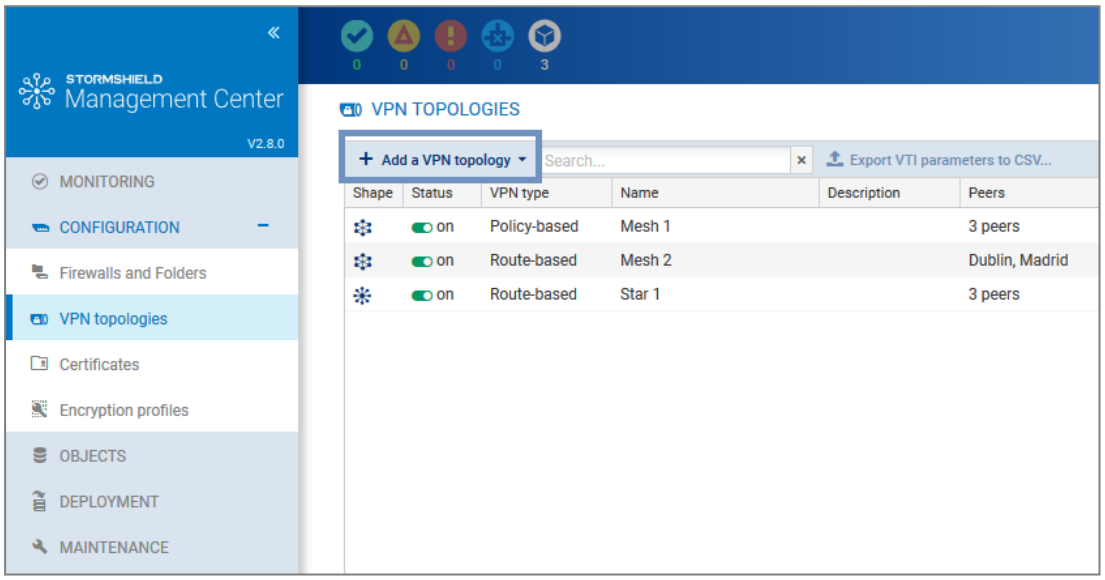
Les objets associés peuvent être de type Réseau, Machine ou Groupe.

IMPORTANT
L'utilisation de groupes contenant des objets variables dans les topologies VPN n'est pas possible. La configuration des tunnels VPN serait invalide.

Créer la topologie VPN

Vous disposez maintenant de tous les éléments nécessaires à la configuration de votre topologie VPN.

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur **Ajouter une topologie VPN** en haut de l'écran et choisissez **Étoile**.



2. Dans la fenêtre qui s'ouvre, choisissez **VPN par politique** et cliquez sur **Créer la topologie**.
3. Entrez un nom. La description est facultative.
4. Choisissez l'authentification par clé pré-partagée.
5. Générez une clé aléatoire.
6. Le profil de chiffrement le plus fort est sélectionné par défaut. Le serveur SMC propose des profils pré-configurés. Créez des profils personnalisés en vous rendant dans le menu **Configuration** > **Profils de chiffrement**. Consultez le *Manuel Utilisateur SNS* pour plus d'informations sur les options des profils de chiffrement.
7. Choisissez le centre de votre topologie. Il présente alors une icône "étoile" dans la liste des firewalls en-dessous, et le firewall s'affiche en gras.
8. Le cas échéant, cochez l'option **Ne pas initier les tunnels (Responder-only)** si l'adresse IP du centre de la topologie est dynamique. Seuls les correspondants pourront alors initier la montée du tunnel VPN.
9. Choisissez les correspondants de votre topologie. Vous pouvez sélectionner des firewalls connectés ou déconnectés. Vous pouvez également sélectionner des firewalls jamais connectés à condition d'avoir défini une adresse IP de contact par défaut personnalisée ou dynamique dans l'onglet **Système** > **VPN IPsec** des paramètres du firewall.
Vous devez posséder le droit d'accès en écriture sur les firewalls que vous souhaitez sélectionner en tant que correspondants. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

10. Choisissez les extrémités de trafic associées à chacun de vos correspondants. Pour plus d'informations sur les paramètres **Adresse de contact** et **Adresse locale**, reportez-vous aux sections Définir l'adresse de contact des firewalls pour les topologies VPN et Choisir l'interface de sortie des firewalls pour les topologies VPN.
11. Cliquez sur **Appliquer**.
12. Déployez la configuration sur les firewalls impliqués dans la topologie. La configuration VPN appartient à la politique globale du firewall.

7.2 Créer des topologies VPN par route

Un tunnel VPN par route est un tunnel dont le trafic est routé via des interfaces IPsec virtuelles (VTI - Virtual Tunnel Interface) pour relier des firewalls SNS gérés par le serveur SMC, et les réseaux et machines protégés par ces firewalls.

Ces interfaces IPsec virtuelles jouent le rôle d'extrémités de trafic des tunnels et tous les paquets routés vers ces interfaces sont alors chiffrés. Ce trafic est décrit par des routes dans une table de routage ou par des règles de filtrage (règles PBR - Policy Based Routing).

Les topologies VPN par route présentent entre autres les avantages suivants :

- Le routage par interfaces IPsec virtuelles est prioritaire sur la correspondance de politique (tunnel IPsec standard).
- Elles nécessitent moins de tunnels qu'une topologie IPsec standard. Un seul tunnel est nécessaire entre deux firewalls, quel que soit le nombre de réseaux protégés par le firewall.

NOTE
Une topologie par route ne peut pas inclure de correspondants externes, c'est-à-dire des firewalls SNS ou tout autre type de passerelle VPN, non gérés par le serveur SMC.

Depuis le serveur SMC, vous pouvez :

- Créer les topologies VPN par route,
- Superviser ces topologies,
- Définir des règles de filtrage. SMC génère automatiquement des objets VTI représentant les correspondants de la topologie, à utiliser dans ces règles,
- Éventuellement configurer les routes statiques et les routes de retour et/ou activer le routage dynamique.

Les interfaces IPsec virtuelles (VTI) sont automatiquement créées sur les firewalls dont SMC gère la configuration du réseau. Elles sont listées dans l'onglet **Interfaces IPsec (VTI)** des paramètres d'un firewall. Pour plus d'informations, reportez-vous à la section Configurer les interfaces IPsec (VTI).

Si la topologie comprend des firewalls dont la configuration du réseau n'est pas gérée par SMC, vous devez créer manuellement les interfaces IPsec virtuelles sur chaque firewall. La colonne **Réseau géré par SMC** dans l'étape de choix des correspondants d'une topologie indique si la configuration du réseau du firewall est gérée par SMC ou non.

Pour plus d'informations, reportez-vous aux sections suivantes.

NOTE
La modification d'une topologie VPN par route peut engendrer des modifications sur les interfaces IPsec virtuelles associées. Pour plus d'informations, reportez-vous à la section Configurer les interfaces IPsec (VTI).

SMC propose deux formes de topologie VPN : maillage ou étoile.

- Maillage : tous les sites distants sont connectés,
- Étoile : un site central est connecté à plusieurs sites satellites. Les sites satellites ne communiquent pas entre eux.

Dans le cas du choix d'une authentification par certificat X509, avant de configurer vos topologies, vous devez avoir importé un certificat pour vos firewalls gérés par SMC compris dans vos topologies et déclaré les autorités de certification. Les procédures correspondantes sont décrites à la section Configurer une topologie par politique en maillage.

Dans cette section, nous décrivons la configuration d'une topologie par route en maillage et la configuration d'une topologie par route en étoile. Pour obtenir plus de détails sur chaque menu et option de la configuration des tunnels VPN, consultez le *Manuel Utilisateur SNS*.

Pour des informations sur la mise en œuvre d'interfaces IPsec virtuelles sur les firewalls, consultez la Note technique dédiée.

NOTE
Les commentaires des interfaces IPsec créées par SMC sont générés à partir des noms de la topologie et des correspondants. S'ils dépassent 127 caractères, ils sont tronqués. Il en est de même avec les commentaires des objets VTI de type Machine, s'ils dépassent 255 caractères.

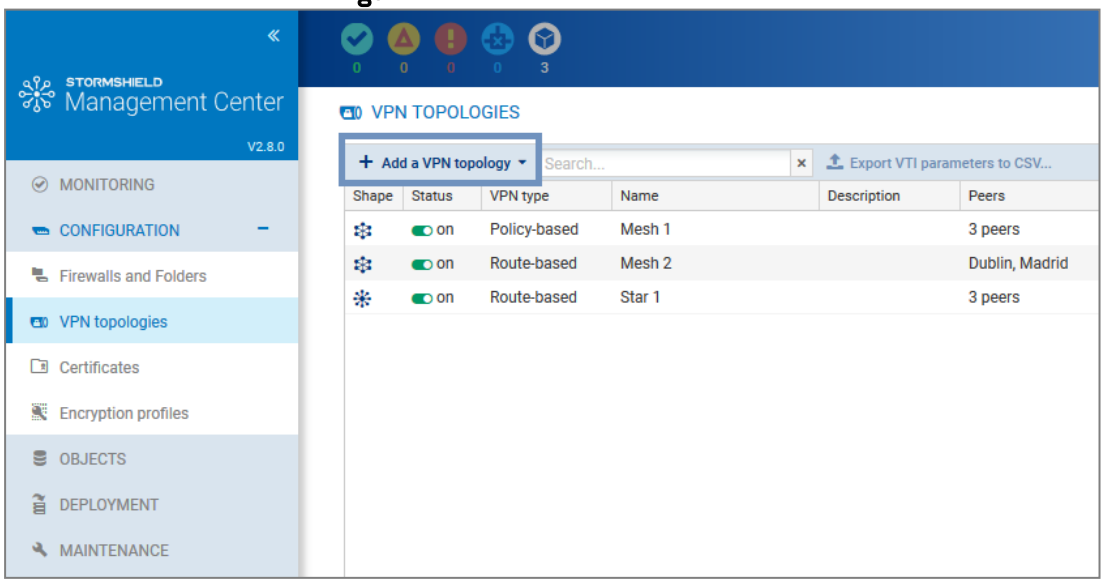
7.2.1 Configurer une topologie par route en maillage

Selon le type d'authentification choisi pour sécuriser votre topologie, des actions préalables peuvent être nécessaires avant de créer la topologie.

- Pour des informations sur l'authentification par certificat X509, reportez-vous à la section Configurer une topologie par politique en maillage.
- Pour des informations sur l'authentification par clé pré-partagée (PSK - pre-shared key), reportez-vous à la section Configurer une topologie par politique en étoile.

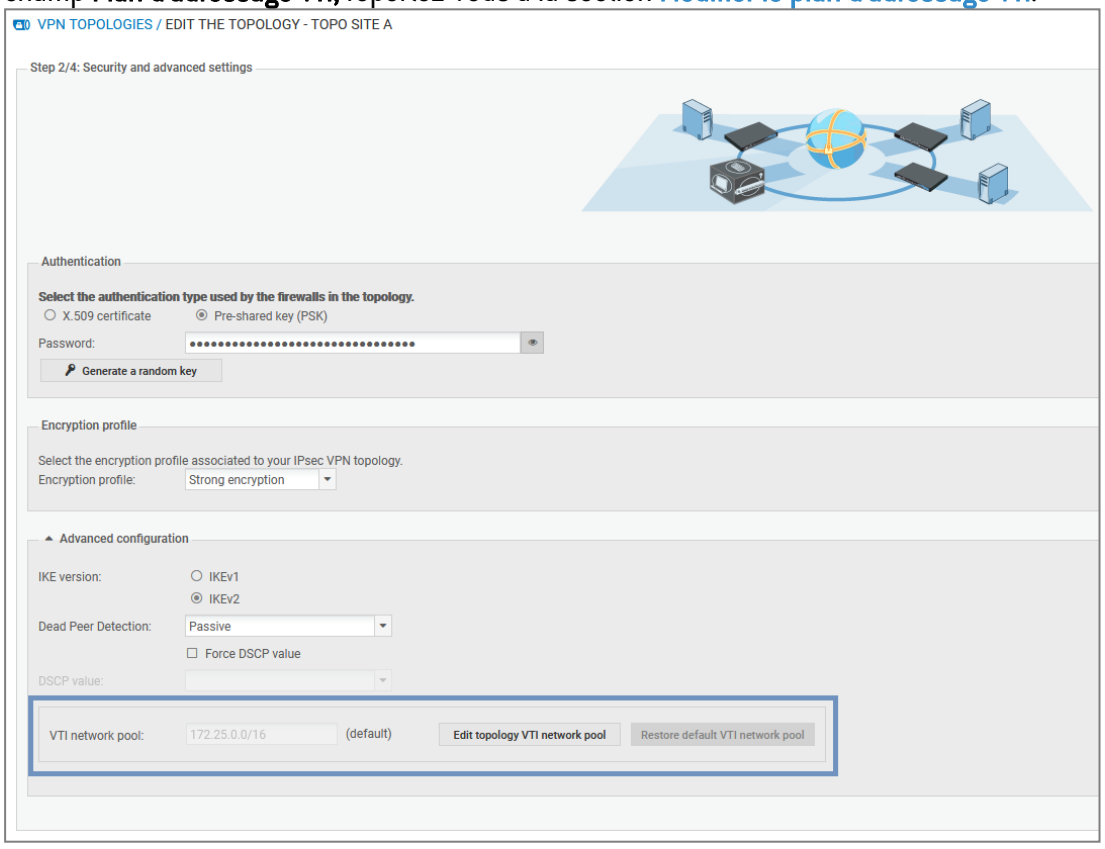
Pour créer la topologie VPN par route , suivez les étapes suivantes :

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur **Ajouter une topologie VPN** en haut de l'écran et choisissez **Maillage**.



2. Dans la fenêtre qui s'ouvre, choisissez **VPN par route** et cliquez sur **Créer la topologie**.

3. Entrez un nom. La description est facultative.
4. A l'étape suivante, choisissez le type d'authentification.
5. Si vous avez choisi l'authentification par certificat X.509, vous pouvez indiquer un identifiant de clé pré-partagée post-quantique et son mot de passe. Une telle clé permet notamment de se protéger des attaques de type "stocker maintenant, déchiffrer plus tard". Pour plus d'informations, consultez le Manuel Utilisateur SNS. Cette fonctionnalité est disponible uniquement dans le cas des firewalls en version 4.8.0 minimum et uniquement avec la version IKEv2.
6. Sélectionnez le profil de chiffrement. Le serveur SMC propose des profils pré-configurés. Créez vos profils personnalisés en vous rendant dans le menu **Configuration** > **Profils de chiffrement**. Consultez le *Manuel Utilisateur SNS* pour plus d'informations sur les options des profils de chiffrement.
7. Si vous avez besoin de modifier le plan d'adressage par défaut des interfaces IPsec virtuelles (VTI), dépliez l'encart **Configuration avancée**. Pour plus d'informations sur le champ **Plan d'adressage VTI,** reportez-vous à la section Modifier le plan d'adressage VTI.



8. A l'étape suivante, choisissez les correspondants de votre topologie. Vous pouvez sélectionner des firewalls connectés ou déconnectés. Vous pouvez également sélectionner des firewalls jamais connectés à condition d'avoir défini une adresse IP de contact par défaut personnalisée ou dynamique dans l'onglet **Système** > **VPN IPsec** des paramètres du firewall.
   Par défaut, pour des performances optimales, vous pouvez sélectionner jusqu'à 50 correspondants. La variable d'environnement `SMC_VPN_MESH_ROUTE_BASED_MAX_PEERS_INT` permet toutefois de configurer cette limitation. Cette limitation n'est valable que pour les topologies VPN par route en maillage.
   Vous devez posséder le droit d'accès en écriture sur les firewalls que vous souhaitez sélectionner en tant que correspondants. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

9. A l'étape suivante, double-cliquez sur la ligne d'un firewall pour ouvrir la fenêtre **Correspondants et VTI** :
   - Pour plus d'informations sur les paramètres **Adresse de contact** et **Adresse locale**, reportez-vous aux sections Définir l'adresse de contact des firewalls pour les topologies VPN et Choisir l'interface de sortie des firewalls pour les topologies VPN.
   - Les adresses des interfaces IPsec virtuelles (VTI) seront générées automatiquement à la fin de la procédure de création de la topologie. Des objets VTI de type Machine représentant les correspondants distants seront également automatiquement générés. Vous pourrez les utiliser dans des routes ou règles de filtrage pour mettre en œuvre du routage. Ils seront visibles dans votre base d'objets, au format "VTI_on_FW1_with_FW2_in_nomtopologie". Ces objets sont automatiquement déployés sur les firewalls. Pour plus d'informations, reportez-vous à la section Définir la politique de routage du trafic.
10. Cliquez sur **Appliquer** pour fermer la fenêtre.
11. Cliquez de nouveau sur **Appliquer** à la fin de l'étape 4/4, pour générer la topologie.
12. Si la topologie comprend des firewalls dont la configuration du réseau n'est pas gérée par SMC, SMC propose de télécharger le fichier *.csv* de configuration des interfaces IPsec. Vous devez créer manuellement les interfaces IPsec sur ces firewalls. Consultez la section Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS pour plus d'informations. Pour les firewalls dont la configuration du réseau est gérée par SMC, les interfaces IPsec sont automatiquement créées par SMC. Consultez la section Configurer les interfaces IPsec (VTI). Le fichier *.csv* indique si les interfaces sont automatiquement créées par SMC dans la colonne "created_by_smc".
13. Déployez la configuration sur les firewalls faisant partie de la topologie. La configuration VPN appartient à la politique globale du firewall.

A ce stade, votre topologie n'est pas encore opérationnelle. Vous devez suivre les étapes suivantes Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS si la topologie comprend des firewalls dont la configuration du réseau n'est pas gérée par SMC et Définir la politique de routage du trafic pour compléter la procédure de mise en œuvre d'une topologie VPN par route.

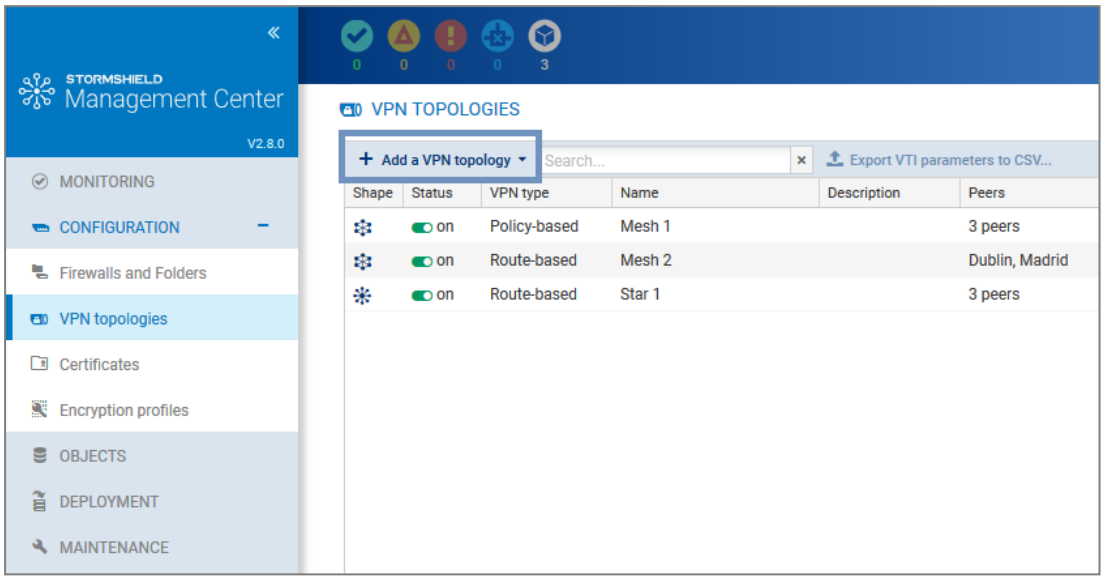
7.2.2 Configurer une topologie par route en étoile

Selon le type d'authentification choisi pour sécuriser votre topologie, des actions préalables peuvent être nécessaires avant de créer la topologie.

- Pour des informations sur l'authentification par certificat X509, reportez-vous à la section Configurer une topologie par politique en maillage.
- Pour des informations sur l'authentification par clé pré-partagée (PSK - pre-shared key), reportez-vous à la section Configurer une topologie par politique en étoile.

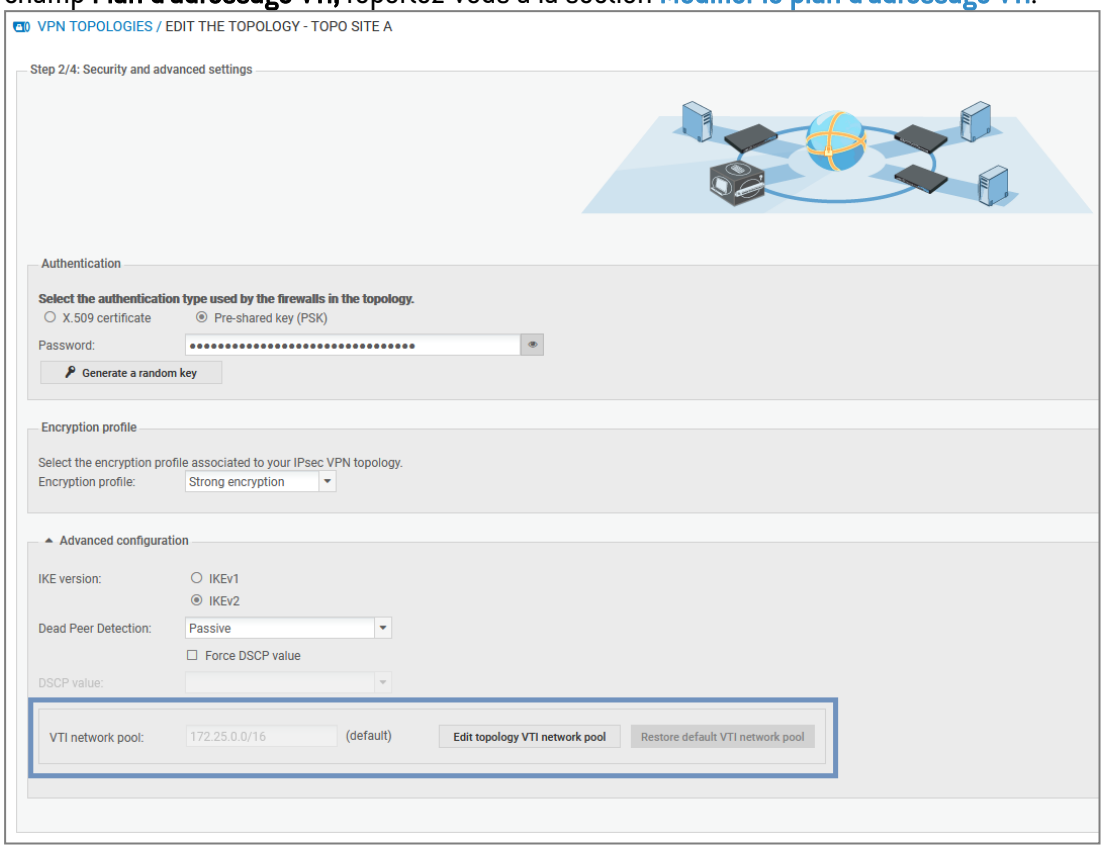
Pour créer la topologie VPN par route, suivez les étapes suivantes :

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur **Ajouter une topologie VPN** en haut de l'écran et choisissez **Étoile**.



2. Dans la fenêtre qui s'ouvre, choisissez **VPN par route** et cliquez sur **Créer la topologie**.
3. Entrez un nom. La description est facultative.
4. A l'étape suivante, choisissez le type d'authentification.
5. Si vous avez choisi l'authentification par certificat X.509, vous pouvez indiquer un identifiant de clé pré-partagée post-quantique et son mot de passe. Une telle clé permet notamment de se protéger des attaques de type "stocker maintenant, déchiffrer plus tard". Pour plus d'informations, consultez le Manuel Utilisateur SNS. Cette fonctionnalité est disponible uniquement dans le cas des firewalls en version 4.8.0 minimum et uniquement avec la version IKEv2.
6. Sélectionnez le profil de chiffrement. Le serveur SMC propose des profils pré-configurés. Créez des profils personnalisés en vous rendant dans le menu **Configuration** > **Profils de chiffrement**. Consultez le *Manuel Utilisateur SNS* pour plus d'informations sur les options des profils de chiffrement.

7. Si vous avez besoin de modifier le plan d'adressage par défaut des interfaces IPsec virtuelles (VTI), dépliez l'encart **Configuration avancée**. Pour plus d'informations sur le champ **Plan d'adressage VTI,** reportez-vous à la section Modifier le plan d'adressage VTI.



8. Choisissez le centre de votre topologie. Il présente alors une icône "étoile" dans la liste des firewalls en-dessous, et le firewall s'affiche en gras.
9. Le cas échéant, cochez l'option **Ne pas initier les tunnels (Responder-only)** si l'adresse IP du centre de la topologie est dynamique. Seuls les correspondants pourront alors initier la montée du tunnel VPN. Cette option est disponible à partir de la version 3.6.0 des firewalls SNS.
10. Choisissez les correspondants de votre topologie. Vous pouvez sélectionner des firewalls connectés ou déconnectés. Vous pouvez également sélectionner des firewalls jamais connectés à condition d'avoir défini une adresse IP de contact par défaut personnalisée ou dynamique dans l'onglet **Système** > **VPN IPsec** des paramètres du firewall.
Vous devez posséder le droit d'accès en écriture sur les firewalls que vous souhaitez sélectionner en tant que correspondants. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

11. A l'étape suivante, double-cliquez sur la ligne d'un firewall pour ouvrir la fenêtre **Correspondants et VTI** :
    - Pour plus d'informations sur les paramètres **Adresse de contact** et **Adresse locale**, reportez-vous aux sections Définir l'adresse de contact des firewalls pour les topologies VPN et Choisir l'interface de sortie des firewalls pour les topologies VPN.
    - Les adresses des interfaces IPsec virtuelles (VTI) seront générées automatiquement à la fin de la procédure de création de la topologie. Des objets VTI de type Machine représentant les correspondants distants seront également automatiquement générés. Vous pourrez les utiliser dans des routes ou des règles de filtrage pour mettre en œuvre du routage. Ils seront visibles dans votre base d'objets, au format "VTI_on_FW1_with_FW2_in_nomtopologie". Ces objets sont automatiquement déployés sur les firewalls. Pour plus d'informations, reportez-vous à la section Définir la politique de routage du trafic.
12. Cliquez sur **Appliquer** pour fermer la fenêtre.
13. Cliquez de nouveau sur **Appliquer** à la fin de l'étape 4/4, pour générer la topologie.
14. Si la topologie comprend des firewalls dont la configuration du réseau n'est pas gérée par SMC, SMC propose de télécharger le fichier *.csv* de configuration des interfaces IPsec. Vous devez créer manuellement les interfaces IPsec sur ces firewalls. Consultez la section Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS pour plus d'informations. Pour les firewalls dont la configuration du réseau est gérée par SMC, les interfaces IPsec sont automatiquement créées par SMC. Consultez la section Configurer les interfaces IPsec (VTI). Le fichier *.csv* indique si les interfaces sont automatiquement créées par SMC dans la colonne "created_by_smc".
15. Déployez la configuration sur les firewalls faisant partie de la topologie. La configuration VPN appartient à la politique globale du firewall.

A ce stade, votre topologie n'est pas encore opérationnelle. Vous devez suivre les étapes suivantes Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS si la topologie comprend des firewalls dont la configuration du réseau n'est pas gérée par SMC et Définir la politique de routage du trafic pour compléter la procédure de mise en œuvre d'une topologie VPN par route.

7.2.3 Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS

Cette étape est nécessaire pour les firewalls dont la configuration du réseau n'est pas gérée par SMC. Pour plus d'informations, reportez-vous à la section Configurer les interfaces réseau.

Connectez-vous sur chacun des firewalls faisant partie de la topologie et créez manuellement les interfaces IPsec virtuelles dans le menu **Réseau** > **Interfaces virtuelles**, à l'aide du fichier *.csv* de configuration téléchargé depuis SMC.

Consultez également le *Manuel Utilisateur SNS* pour plus d'informations sur la création d'interfaces IPsec virtuelles.

Si vous souhaitez automatiser la création des interfaces IPsec, le fichier *.csv* contient toutes les informations nécessaires à l'écriture de commandes Serverd.

Dans ce cas, vous devrez remplir manuellement la colonne *vti_interface_name*. La valeur du nom de l'interface est au format ipsecXX pour les firewalls en versions inférieures à la 5.1.0 et vtiXX pour les versions supérieures ou égales à 5.1.0, où XX correspond à un incrément dépendant du nombre d'interfaces déjà présentes sur le firewall.

Suivez maintenant la dernière étape.

7.2.4 Définir la politique de routage du trafic

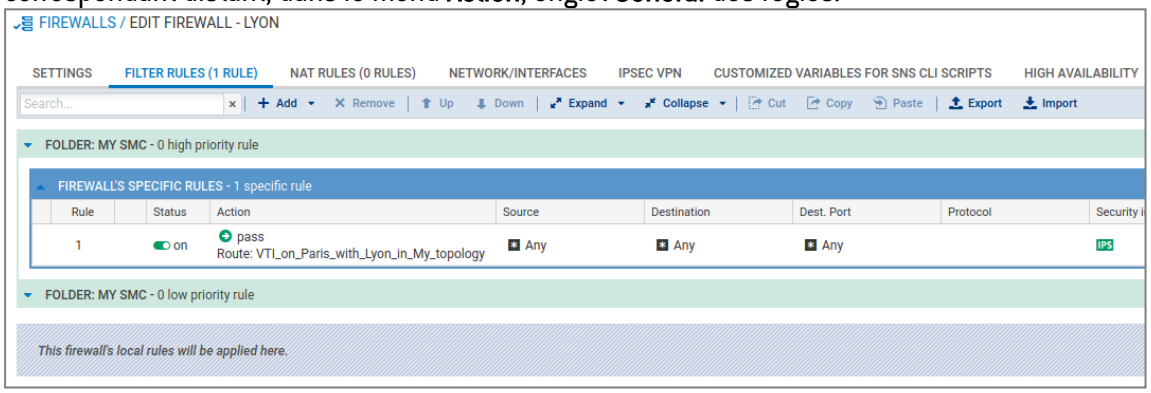
Pour diriger le trafic vers les interfaces IPsec virtuelles (VTI), vous pouvez selon les cas configurer les routes statiques et dynamiques, ainsi que les routes de retour. Vous pouvez également définir des règles de filtrage pour mettre en œuvre du routage.

Vous pouvez réaliser ces actions directement depuis SMC si les firewalls inclus dans la topologie sont en version 4.2.4 minimum et si la gestion de la configuration du réseau est activée sur SMC.

Dans le cas contraire, vous devez configurer les routes directement sur vos firewalls.

Si vous mettez en œuvre du routage par politique (Policy Based Routing) :

1. Créez des règles de filtrage pour chaque firewall afin de permettre le passage du trafic par le tunnel. Vous devez définir en tant que **Passerelle - Routeur** le correspondant distant. Pour cela, sélectionnez l'objet VTI généré automatiquement par SMC et représentant le correspondant distant, dans le menu **Action**, onglet **Général** des règles.



2. Créez les routes de retour dans l'onglet Routage de chaque firewall..

Si vous n'utilisez pas le routage par politique (PBR) :

1. Créez des routes statiques dédiées aux interfaces IPsec virtuelles du correspondant distant pour chaque firewall.
2. Configurez une politique de filtrage pour chaque firewall afin de permettre le passage du trafic par le tunnel.

Pour obtenir de l'aide sur la configuration des routes sur vos firewalls, consultez le *Manuel Utilisateur SNS* et la Note technique dédiée aux interfaces IPsec virtuelles.

Consultez également la section Configurer le réseau et le routage.

7.2.5 Modifier le plan d'adressage VTI

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Lors de la création d'une topologie VPN par route, les adresses IP des interfaces IPsec virtuelles sont choisies par le serveur SMC dans un sous-réseau privé défini par défaut.

Ce sous-réseau constitue une réserve d'adresses disponibles. Il doit être inclus (ou égal) dans un de ces trois sous-réseaux :

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Par défaut le sous-réseau proposé est 172.25.0.0/16.

Ce plan d'adressage par défaut est global à toutes les topologies. Si besoin, vous pouvez modifier le plan global, ou bien le plan spécifique à une topologie.

IMPORTANT
Si vous modifiez le plan d'adressage des interfaces IPsec spécifique à une topologie après la création et le déploiement de la topologie, vous devrez peut-être revoir la configuration des interfaces déjà créées sur vos firewalls, dans le cas où SMC ne gère pas la configuration du réseau.

Modifier le plan d'adressage global par défaut

Le plan d'adressage par défaut est celui utilisé lors de la création d'une nouvelle topologie. Pour le modifier :

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur l'icône ☰ en haut à droite de l'écran et sélectionnez **Modifier le plan d'adressage VTI par défaut**.

2. Indiquez le nouveau plan d'adressage par défaut.

Cette modification n'a pas d'impact sur les topologies existantes, qui gardent le plan défini lors de leur création.

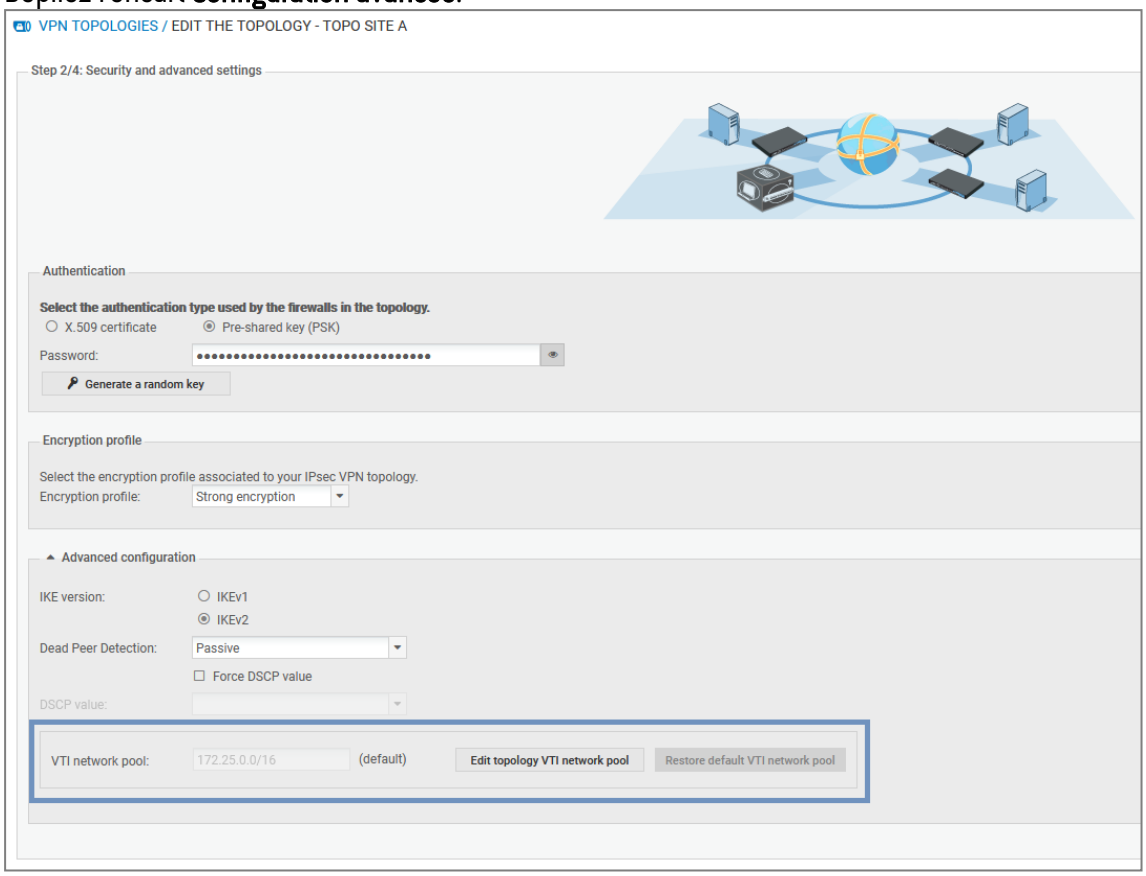
Modifier le plan d'adressage spécifique à une topologie

Vous pouvez modifier le plan d'adressage au moment de la création d'une nouvelle topologie ou après sa création.

Pour le modifier sur une topologie existante :

1. Dans le menu **Configuration** > **Topologies VPN**, cliquez sur l'icône crayon qui s'affiche en survolant la colonne **Plan d'adressage VTI** de la grille.

2. Dépliez l'encart **Configuration avancée**.



3. Cliquez sur **Modifier le plan d'adressage VTI de la topologie**.
4. Cliquez sur **Confirmer la modification** dans la fenêtre d'avertissement. Vous devrez peut-être revoir la configuration des interfaces déjà créées sur vos firewalls.
5. Indiquez un nouveau sous-réseau privé parmi les trois sous-réseaux indiqués au début de la section.
6. Déployez la configuration.

7.2.6 Résoudre les problèmes

Consultez cette section pour résoudre les éventuels problèmes rencontrés lors de la création de topologies VPN par route.

Les tunnels d'une topologie VPN par route ne sont pas opérationnels

- *Situation* : La vue de supervision des topologies indique qu'une topologie n'est pas opérationnelle.
- *Cause* : Si la topologie comprend des firewalls SNS dont la configuration du réseau n'est pas gérée par SMC, toutes les interfaces IPsec virtuelles n'ont peut-être pas été créées manuellement sur les firewalls concernés.
- *Solution* : Vérifiez que toutes les interfaces IPsec virtuelles ont bien été créées sur les firewalls. Pour connaître la liste des firewalls de la topologie dont la configuration du réseau n'est pas gérée par SMC, consultez la colonne **Réseau géré par SMC** dans l'étape de choix des correspondants d'une topologie. Pour accéder à cette étape, depuis le menu **Configuration** > **Topologies VPN**, double-cliquez dans la colonne **Correspondants** de la topologie concernée.

Pour plus d'informations, reportez-vous aux sections Configurer une topologie par route en maillage et Définir les interfaces IPsec virtuelles (VTI) sur les firewalls SNS.

7.3 Gérer les certificats et les autorités de certification

Le menu **Configuration** > **Certificats** permet de consulter et de gérer à la fois les certificats des firewalls et les autorités de certification (CA). Depuis le même panneau, vous pouvez ajouter, mettre à jour ou bien supprimer des certificats et des autorités de certification.

Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers comprenant les firewalls concernés par ces modifications. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

La grille présente les autorités, les sous-autorités et les certificats sous forme d'arborescence. Elle affiche des informations sur les certificats, les firewalls et les topologies concernés.

- Pour sélectionner les colonnes à afficher, survolez le nom d'une colonne et cliquez sur la flèche qui s'affiche.
- Pour afficher les actions possibles sur les autorités et les certificats, survolez la colonne **Statut du certificat**. Des icônes d'action s'affichent.

Les certificats des firewalls peuvent être de type X509 ou émis via les protocoles SCEP ou EST. Les actions possibles sont alors différentes :

	Autorités de certification	Certificats X509	Certificats SCEP/EST
Icônes s'affichant au survol de la ligne			
Actions possibles	• Modifier l'autorité de certification • Mettre à jour l'autorité de certification • Voir les références • Supprimer du serveur SMC	• Mettre à jour le certificat • Voir les références • Supprimer du serveur SMC	• Renouveler le certificat • Voir les références • Supprimer du serveur SMC

ATTENTION
Les caractères suivants ne sont pas supportés dans les noms des certificats :

,	< et >
+	#
=	;
"	double espace

Reportez-vous aux procédures ci-dessous pour plus d'informations sur chacune des actions.

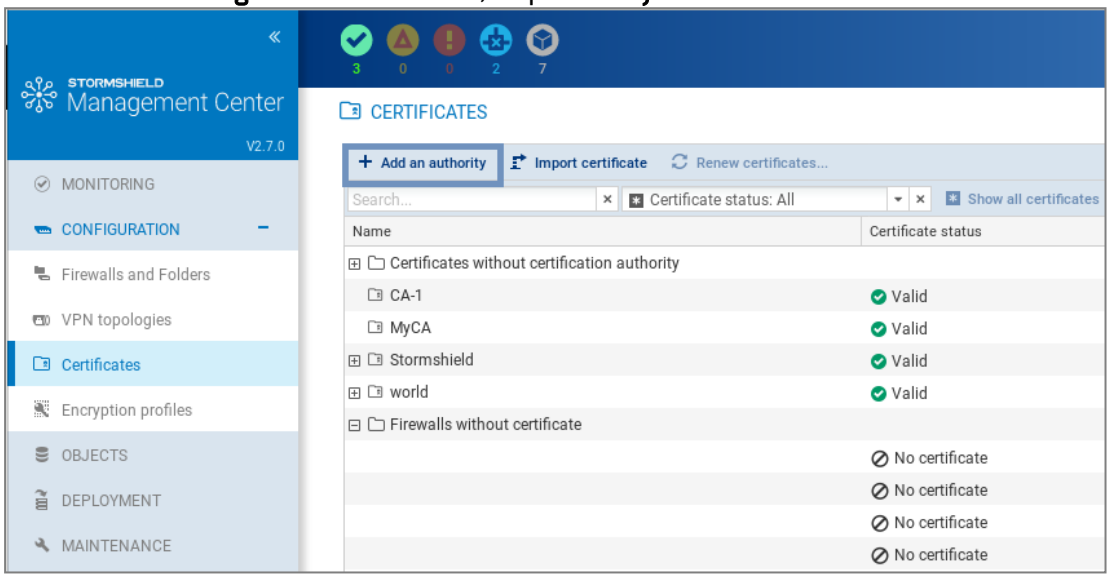
7.3.1 Ajouter une autorité de certification ou une chaîne de confiance

Le serveur SMC ne permet pas l'utilisation d'autorités de certification dont l'émetteur lui est inconnu. Vous devez importer toute la chaîne de confiance d'une autorité.

Pour importer une chaîne de confiance, importez les certificats de l'autorité de certification racine et des différentes sous-autorités un par un en commençant par l'autorité de certification de plus haut niveau. Vous pouvez également tous les importer en une seule fois en fournissant un fichier "bundle".

Lorsque vous ajoutez une autorité de certification, le serveur SMC vérifie sa chaîne de confiance.

1. Dans le menu **Configuration** > **Certificats**, cliquez sur **Ajouter une autorité**.



2. Sélectionnez un fichier aux formats *.pem*, *.cer*, *.crt* ou *.der* et cliquez sur **Ajouter**.
3. Ajoutez les adresses du ou des points de distribution de la liste de révocation des certificats (CRL). Pour plus d'informations, reportez-vous à la section Indiquer les points de distribution de CRL.
4. Si vous utilisez le protocole SCEP ou EST pour renouveler les certificats des firewalls, associez un serveur SCEP ou EST à l'autorité de certification dans l'onglet **Renouvellement de certificats**.
5. Une fois l'autorité déclarée, vous pouvez la modifier ou vérifier son utilisation en survolant le nom de l'autorité dans la grille pour faire apparaître les icônes d'action dans la colonne **Statut du certificat**.

L'ajout d'une nouvelle autorité peut également être réalisé pendant la configuration d'une topologie VPN, à l'étape du choix de l'authentification, en cliquant sur le bouton **Ajouter une autorité**.

7.3.2 Mettre à jour une autorité de certification ou une chaîne de confiance

Lorsque vous mettez à jour une autorité de certification, le nom, le commentaire et l'éventuelle liste des points de distribution de listes de révocation de certificats sont conservés.

La clé publique doit être identique à l'autorité précédente.

- Pour mettre à jour une autorité de certification, survolez le nom de l'autorité de certification et cliquez sur l'icône dans la colonne **Statut du certificat**.

7.3.3 Supprimer une autorité de certification ou une chaîne de confiance

Lorsque vous supprimez une autorité de certification, toutes les autorités qui en dépendent sont également supprimées. Si l'une des autorités intermédiaires est utilisée dans une topologie VPN, vous ne pourrez pas la supprimer.

- Pour supprimer une autorité de certification, survolez le nom de l'autorité de certification et cliquez sur l'icône dans la colonne **Statut du certificat**.

7.3.4 Importer ou déclarer un certificat pour un firewall

La fenêtre d'import des certificats X509 est accessible depuis la colonne **Firewall** de la grille, mais aussi depuis d'autres panneaux de l'interface d'administration.

Pour importer ou déclarer un certificat, reportez-vous à la section Importer ou déclarer un certificat pour un firewall.

Une fois le certificat importé ou déclaré, vous pouvez vérifier son utilisation ou le supprimer en survolant sa ligne dans la grille pour faire apparaître les icônes d'action dans la colonne **Statut du certificat**.

Vous ne pourrez pas le supprimer s'il est utilisé dans une topologie VPN.

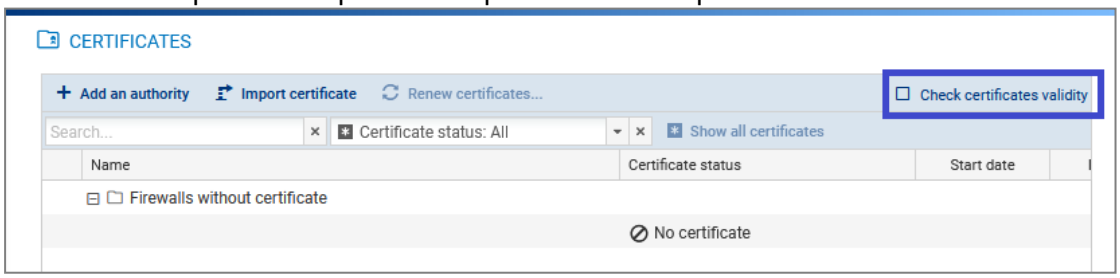
Dans le cas où vous avez importé plusieurs certificats X509 pour un firewall, pour savoir lequel est utilisé par défaut dans les topologies VPN, reportez-vous à la section Modifier le certificat utilisé par défaut dans les topologies VPN.

7.3.5 Vérifier la validité des certificats

Vous pouvez configurer les firewalls SNS afin qu'ils consultent la CRL (liste de révocation des certificats) pour vérifier la validité des certificats utilisés par les correspondants des tunnels VPN.

En mode DR (Diffusion restreinte), cette vérification est obligatoire.

1. Cochez la case **Vérifier la validité des certificats** en haut à droite pour rendre obligatoire la présence d'une CRL valide et détecter ainsi les certificats révoqués. En l'absence de CRL valide ou si le correspondant présente un certificat révoqué, le tunnel VPN ne peut pas s'établir. Cette option est l'équivalent du paramètre CRLRequired sur les firewalls SNS.



2. Si besoin, configurez pour chaque certificat quelle adresse IP locale utiliser pour effectuer la vérification et la fréquence de vérification. Pour cela :
   a. Affichez les colonnes **Adresse IP locale pour vérification de la CRL** et/ou **Fréquence de vérification de la CRL** en survolant le nom d'une colonne et en cliquant sur la flèche, puis sur **Colonnes**.
   b. Sélectionnez un certificat.
   c. Dans la colonne **Adresse IP locale pour vérification de la CRL**, choisissez l'adresse souhaitée. Par défaut, n'importe quelle adresse peut être utilisée (*Any*).
   d. Dans la colonne **Fréquence de vérification de la CRL**, saisissez le nombre de secondes entre chaque vérification. Par défaut la fréquence est de 21600 secondes, soit 6 heures.

7.3.6 Mettre à jour le certificat X509 d'un firewall

- Pour mettre à jour un certificat X509 expiré ou proche de l'expiration, survolez la ligne du certificat dans la grille et cliquez sur l'icône dans la colonne **Statut du certificat**.

Le nouveau certificat doit avoir le même champ "Sujet" que le précédent.

7.3.7 Renouveler le certificat d'un firewall obtenu par les protocoles SCEP ou EST

Pour que le renouvellement des certificats fonctionne, l'adresse du serveur SCEP ou EST doit être indiquée dans l'onglet **Renouvellement de certificats** de l'autorité de certification ayant délivré les certificats, comme indiqué à la section Ajouter une autorité de certification ou une chaîne de confiance.

Si besoin, vous pouvez choisir l'adresse des firewalls SNS qui doit être utilisée pour effectuer le renouvellement du certificat.

Les conditions suivantes s'appliquent pour renouveler les certificats :

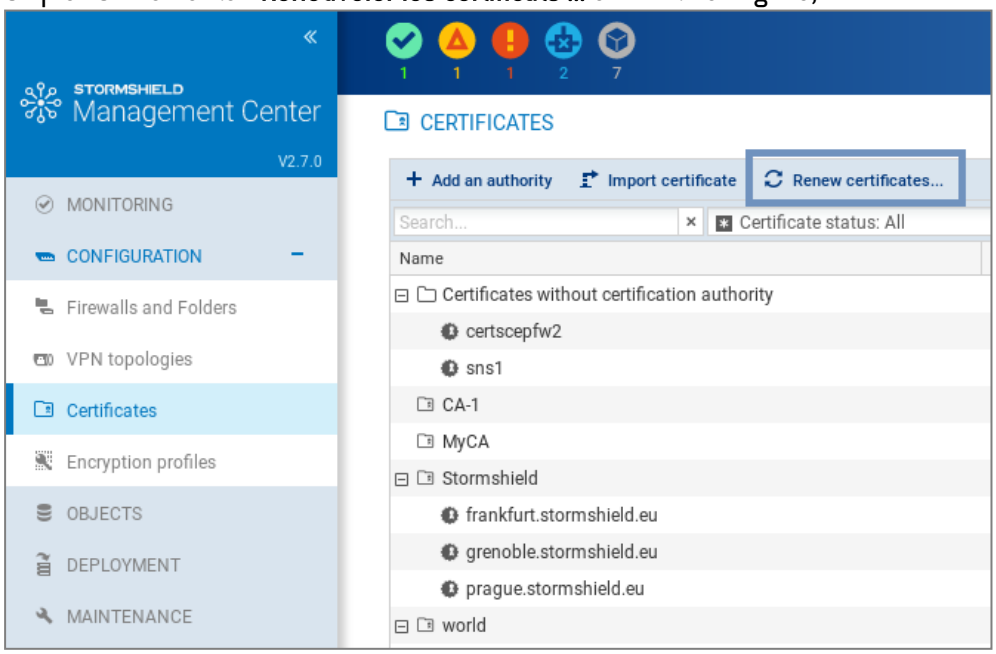
- les firewalls SNS doivent être en version 3.9.0 minimum pour le protocole SCEP et 3.10 ou 4.1 minimum pour le protocole EST,
- les firewalls SNS doivent être connectés.

Pour choisir une adresse spécifique pour le renouvellement d'un certificat :

1. Affichez la colonne **Adresse IP locale pour le renouvellement** en survolant le nom d'une colonne et en cliquant sur la flèche, puis sur **Colonnes**.
2. Cliquez dans la colonne d'un certificat et choisissez l'adresse souhaitée du firewall SNS dans la liste déroulante.

Pour renouveler les certificats :

1. Cliquez sur le bouton **Renouveler les certificats ...** en haut de la grille,



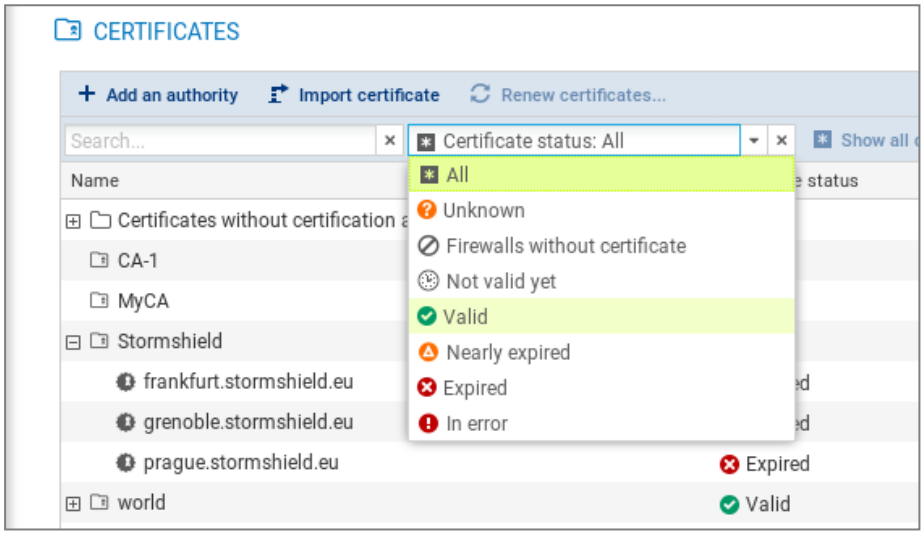
2. Sélectionnez les certificats à renouveler,
3. Confirmez le renouvellement des certificats en bas de la grille. En cas d'erreur, consultez les journaux du serveur pour plus d'informations.

ASTUCE

Pour renouveler un seul certificat, survolez sa ligne dans la grille et cliquez sur l'icône dans la colonne **Statut du certificat**.

7.3.8 Comprendre les statuts des certificats

Au-dessus de la grille, le filtre permet d'afficher les autorités de certification et les certificats en fonction de leur statut.



Pour afficher de nouveau toute l'arborescence, cliquez sur **Afficher tous les certificats**.

Le statut **Inconnu** s'applique aux certificats obtenus par les protocoles SCEP ou EST uniquement. Le certificat SCEP ou EST peut avoir un statut **Inconnu** si le serveur SMC ne connaît pas encore le certificat. Cela peut être le cas parce que le serveur SCEP ou EST ne peut pas être joint ou parce que le firewall ne s'est pas encore connecté depuis la création du certificat.

Le statut **Expiration proche** s'affiche par défaut 30 jours avant l'expiration du certificat. Pour savoir comment configurer l'avertissement de l'expiration proche des certificats, reportez-vous à la section Configurer l'avertissement de l'expiration proche des certificats.

IMPORTANT

La révocation des certificats n'étant pas gérée par le serveur SMC, les certificats révoqués sont affichés comme "valides".

7.4 Définir l'adresse de contact des firewalls pour les topologies VPN

Un firewall d'une topologie VPN peut être contacté par ses correspondants sur une adresse IP fixe. Dans ce cas, deux options sont possibles :

- par défaut, le firewall est contacté sur l'adresse IP qui a été détectée lorsqu'il s'est connecté au serveur SMC pour la dernière fois,
- vous pouvez sinon définir une adresse de contact personnalisée.

Il est également possible d'indiquer qu'un firewall dispose d'une adresse IP dynamique et ne peut donc pas être contacté par ses correspondants : il est toujours à l'initiative de la

négociation du tunnel VPN. Il n'est donc pas possible d'établir un tunnel VPN entre deux correspondants disposant d'une adresse IP dynamique.

Pour un firewall donné, vous pouvez choisir l'adresse sur laquelle il est contacté dans la majorité des topologies VPN. Vous pouvez définir cette adresse de contact par défaut dans les paramètres du firewall. Si vous avez besoin de définir une adresse différente dans certaines topologies, vous pouvez remplacer l'adresse par défaut directement dans ces topologies.

7.4.1 Définir l'adresse de contact par défaut d'un firewall

1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur le firewall.
2. Rendez-vous dans l'onglet **Système > VPN IPsec**, dans **Adresse de contact par défaut**.

Le paramètre choisi ici peut-être remplacé par une adresse de contact différente dans des topologies données, comme indiqué dans la section suivante.

7.4.2 Définir l'adresse de contact d'un firewall dans une topologie VPN spécifique

1. Dans **Configuration** > **Topologies VPN**, rendez-vous à l'étape 4 **Configuration des correspondants et des extrémités** lors de la création ou modification d'une topologie.
2. Double-cliquez dans la colonne **Adresse de contact**.
3. Dans le champ **Adresse IP** , choisissez un objet ou bien **Any** pour indiquer que l'adresse IP est dynamique.

7.5 Choisir l'interface de sortie des firewalls pour les topologies VPN

Vous pouvez choisir l'interface de sortie d'un firewall utilisée comme source dans un tunnel VPN. Deux étapes sont requises :

1. Sur SMC, créer l'objet Machine correspondant à l'interface voulue,
2. Sur SMC, choisir l'interface de sortie,
3. Éventuellement, configurer une route statique sur le firewall.

7.5.1 Créer l'objet Machine correspondant à l'interface

- Dans le menu **Objets**, créez un objet Machine de type Firewall_xx qui correspond à une interface configurée sur le firewall dans le menu **Configuration** > **Réseau** > **Interfaces**. Cet objet ne sera pas déployé sur le firewall. Le firewall utilisera les valeurs indiquées dans son propre objet Firewall_xx.

7.5.2 Choisir l'interface de sortie d'un firewall sur SMC

Sur les firewalls SNS, le même paramètre se trouve dans le menu **Configuration** > **VPN** > **VPN IPsec**> **Correspondants** > **Configuration avancée** > **Adresse locale**.

Pour un firewall donné, vous pouvez choisir l'interface de sortie qu'il utilise dans la majorité des topologies VPN. Vous pouvez définir cette interface de sortie par défaut dans les paramètres du firewall. Si vous avez besoin de définir une interface différente dans certaines topologies, vous pouvez remplacer l'interface par défaut directement dans ces topologies.

Définir l'interface de sortie par défaut d'un firewall

1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur le firewall.
2. Dans l'onglet **Système > VPN IPsec**, sélectionnez la valeur souhaitée pour l'adresse locale dans **Adresse locale par défaut**. La valeur par défaut est **Any**.

Le paramètre choisi ici peut-être remplacé par une interface différente dans des topologies données, comme indiqué dans la section suivante.

Définir l'interface de sortie d'un firewall dans une topologie VPN spécifique

1. Dans **Configuration** > **Topologies VPN**, rendez-vous à l'étape 4 **Configuration des correspondants et des extrémités** lors de la création ou modification d'une topologie.
2. Double-cliquez dans la colonne **Adresse locale**.
3. Dans le champ **Adresse locale VPN**, choisissez une interface.

7.5.3 Configurer une route statique sur le firewall (facultatif)

En fonction de la configuration du routage sur votre firewall, créez si nécessaire une route statique pour chacun des correspondants du tunnel VPN avec les paramètres suivants :

- destination : adresse IP du correspondant
- interface : interface dédiée aux communications VPN (même interface que celle choisie au cours de la procédure ci-dessus)
- passerelle : passerelle de l'interface dédiée aux communications VPN

Pour plus d'informations sur la création de routes sur SMC, reportez-vous à la section Configurer le réseau et le routage.

7.6 Modifier, supprimer et vérifier l'utilisation d'une topologie VPN

Depuis la liste de vos topologies VPN dans le menu **Configuration** > **Topologies VPN**, modifiez ou supprimez une topologie.

Vous pouvez également vérifier l'utilisation d'objets VTI générés dans le cadre d'une topologie par route.

Si les correspondants d'une même topologie sont des firewalls classés dans plusieurs dossiers administrés par des administrateurs de dossiers différents, seul un administrateur général ou un administrateur possédant le droit d'accès en écriture sur tous les dossiers concernés peut la modifier ou la supprimer. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour modifier une topologie :

- Double-cliquez sur la ligne d'une topologie
-ou-
- Survolez une ligne avec la souris pour afficher l'icône crayon . L'icône s'affiche dans chaque colonne et permet d'ouvrir directement le panneau de l'assistant correspondant à la colonne.

Redéployez la configuration après cette action.

Pour supprimer une topologie :

1. Survolez le nom de la topologie dans la liste et cliquez sur la croix rouge .
2. Redéployez la configuration après cette action.

IMPORTANT
Si vous modifiez ou supprimez une topologie VPN par route sur SMC, les objets VTI sont également modifiés ou supprimés. Si vous utilisez ces objets dans la configuration locale de vos firewalls SNS, veillez à d'abord les supprimer avant de modifier ou supprimer une topologie dans SMC.

Pour vérifier l'utilisation d'objets VTI :

Vérifier l'utilisation d'une topologie VPN par route permet de savoir si des objets VTI générés automatiquement par SMC lors de la création de la topologie sont utilisés dans un élément de la configuration (une règle de filtrage par exemple).

Vous ne pourrez pas supprimer une topologie par route ou retirer des correspondants de la topologie si l'un de ces objets est utilisé.

Pour vérifier l'utilisation des objets VTI générés :

- Survolez le nom de la topologie dans la liste et cliquez sur l'icône . Le panneau de résultats s'ouvre dans le panneau inférieur. Vous pouvez double-cliquer sur un résultat.

7.7 Gérer la fragmentation des paquets

Dans les paramètres avancés du menu **Configuration** > **Topologies VPN**, vous pouvez définir la valeur du Path MTU Discovery et la taille des fragments.

Paramètre	Description
Path MTU Discovery	Sélectionnez une valeur de la liste déroulante. • **Désactivé** : Par défaut, l'option est désactivée • **Toujours ajouter le bit DF** : Vous devez désactiver le mode furtif (Stealth mode) sur les firewalls concernés par une commande CLI pour pouvoir sélectionner cette option. • **Conserver le bit DF** : Si le paquet ayant été chiffré avait initialement le bit DF, celui-ci sera conservé.
Taille des fragments	Définissez la taille maximale des fragments IKE en octets. Valeur par défaut : 1280 octets Valeur minimum : 512 octets

Pour plus d'informations sur les commandes Serverd correspondantes qui seront mises à jour sur les firewalls SNS concernés, reportez-vous à la section Config IPsec Update du guide *CLI / SSH Commands Reference Guide*.

7.8 Désactiver une topologie VPN

Si vous souhaitez travailler sur une topologie VPN sans l'inclure dans un déploiement de configuration, vous avez la possibilité de la désactiver.

Ceci signifie que la configuration des tunnels ne sera donc pas déployée sur les firewalls SNS et les tunnels ne s'afficheront pas dans la fenêtre de supervision des topologies VPN.

Par défaut, lorsque vous créez une nouvelle topologie, elle est activée.

Pour réaliser cette opération, vous devez posséder le droit d'accès en écriture sur tous les firewalls compris dans la topologie. Si ce n'est pas le cas, un administrateur général peut la

désactiver. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour désactiver une topologie :

1. Dans le menu **Configuration** > **Topologies VPN**, sur la ligne de la topologie concernée, double-cliquez dans la colonne **État** pour passer de l'état **on** à l'état **off**.
2. Redéployez la configuration pour que la désactivation prenne effet.

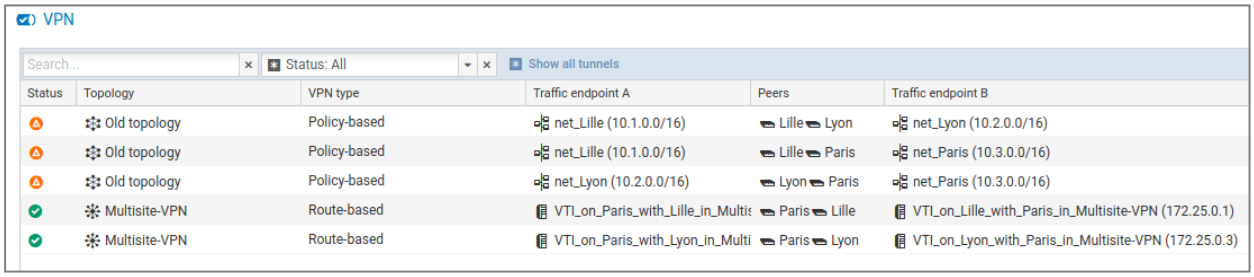
Si une topologie déjà déployée est désactivée dans SMC, et si aucun redéploiement n'est effectué entre temps, ses tunnels seront toujours visibles dans la fenêtre de supervision.

7.9 Superviser l'état des tunnels VPN

Le menu **Supervision** > **VPN** permet de consulter l'état de chaque tunnel configuré dans chaque topologie.

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

Passez votre souris sur l'icône d'état d'un tunnel pour afficher une info-bulle indiquant son état, ainsi que l'état des correspondants.



La colonne **Identifiant de la topologie (rulename)** permet de mener une recherche sur une topologie à partir de l'identifiant "rulename" indiqué dans les journaux d'audit VPN des firewalls SNS.

En cas de mise à jour du serveur SMC, la configuration doit être redéployée sur les firewalls pour que l'identifiant "rulename" soit visible dans les journaux.

7.10 Définir le PRF dans un profil de chiffrement personnalisé

Dans les topologies VPN IKEv2, le PRF (Pseudo-random Function - Fonction pseudo-aléatoire) est un algorithme négocié lors de la phase 1 (phase IKE) du tunnel IPsec.

Il est supporté à partir des versions 4.2.3 des firewalls SNS. Pour les versions inférieures, la valeur du PRF n'est pas déployée.

SMC propose des profils de chiffrement par défaut. Ils ne sont pas modifiables. Vous pouvez créer vos propres profils de chiffrement si vous souhaitez personnaliser les champs.

NOTE
Pour être compatible avec le mode "Diffusion Restreinte (DR)", le PRF d'un profil de chiffrement IKEv2 doit être impérativement positionné sur SHA256. Pour plus d'informations sur le mode DR, reportez-vous à la section Utiliser le mode "Diffusion Restreinte" sur les firewalls SNS.

Pour créer un profil de chiffrement et définir le PRF :

1. Dans le menu **Configuration** > **Profils de chiffrement**, cliquez sur **Créer un profil de chiffrement**.
2. Entrez un nom et une description, si nécessaire.
3. Dans l'onglet **IKE**, indiquez l'algorithme devant être négocié en tant que PRF (champ **Fonction Pseudo-Aléatoire**).
4. Complétez les autres champs. Pour obtenir des informations sur les champs, consultez le *Manuel Utilisateur SNS*.
5. Cliquez sur **Créer**.

8. Définir des règles de filtrage et translation (NAT)

SMC permet de déployer des règles de filtrage et de translation sur votre parc de firewalls. Les règles s'appliquent à des ensembles de firewalls (dossiers et sous-dossiers) ou sont spécifiques à certains firewalls, offrant ainsi la capacité de configurer une seule fois une règle partagée par plusieurs sites tout en gardant la possibilité de déployer des règles spécifiques à un site donné.

Pour classer vos firewalls par dossier, reportez-vous à la section Classer les firewalls par dossiers. Les règles appliquées au dossier racine par défaut **MySMC** s'appliquent à tout le parc de firewalls.

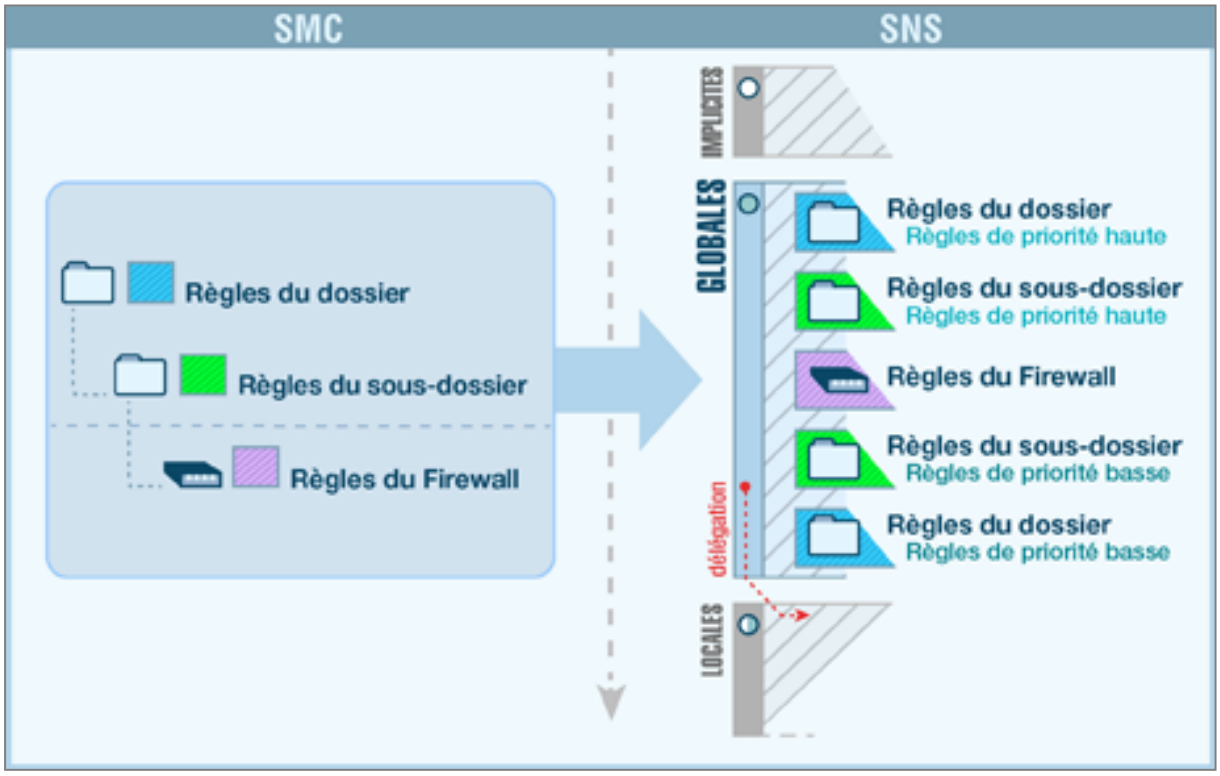
Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers concernés dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour obtenir plus de détails sur chaque menu et option de la configuration des règles, consultez le *Manuel Utilisateur SNS*.

Les règles sont définies dans l'onglet **Filtrage et translation** accessible depuis le menu **Configuration** > **Firewalls et dossiers** ou depuis les paramètres d'un firewall.

8.1 Comprendre l'ordre de lecture des règles

Pour visualiser les règles de filtrage ou de translation (NAT) d'un firewall, dans le menu **Supervision** > **Firewalls**, double-cliquez sur un firewall et sélectionnez l'onglet **Filtrage et translation**. Les règles sont classées par ordre de priorité.



Les règles de filtrage et de translation appliquées à un firewall donné sont la combinaison de deux types de règles créées dans SMC :

- Les règles partagées entre plusieurs firewalls, créées dans les dossiers (dossier auquel appartient le firewall ainsi que ses dossiers parents),
- Les règles spécifiques au firewall, créées dans les paramètres du firewall. Dans la vue de supervision des firewalls, la colonne **Nombre de règles spécifiques** indique combien de règles spécifiques possède chaque firewall.

Ces règles sont déployées dans la politique de sécurité globale du firewall. A la suite de ces règles, s'appliquent les éventuelles règles de la politique de sécurité locale du firewall.

Le firewall hérite des règles du dossier auquel il appartient ainsi que des règles de ses dossiers parents, et celles-ci s'appliquent dans l'ordre suivant :

- Règles de priorité haute configurées dans les dossiers, du général au particulier,
- Règles spécifiques au firewall,
- Règles de priorité basse configurées dans les dossiers, du particulier au général.

EXEMPLE
Une règle de priorité haute dans le dossier **MySMC** ne peut pas être surchargée par une autre règle, elle sera toujours la première règle appliquée. Une règle de priorité basse dans le dossier **MySMC** sera surchargée par toutes les autres règles définies dans les dossiers ou pour un firewall spécifique.

8.2 Exemples de cas d'usage

8.2.1 Gérer un parc sans partage de règles

Prenons l'exemple d'un prestataire qui administre des firewalls SNS pour plusieurs clients :

- Chaque client ne possède qu'un seul firewall,
- Tous les firewalls se trouvent dans le dossier racine **MySMC**, on n'utilise pas les sous-dossiers,
- Les firewalls ne possèdent aucune règle de filtrage ou de translation en commun,
- Le prestataire ne veut pas se connecter sur chaque firewall en direct pour définir des règles.

Le prestataire doit donc :

- Définir des règles spécifiques sur chaque firewall dans SMC, en se rendant dans l'onglet **Filtrage et translation** du firewall.
- Éventuellement, définir une règle dite "Block all" en tant que dernière règle sur chacun des firewalls pour ignorer les règles présentes dans la politique de sécurité locale des firewalls.
- Déployer la configuration sur les firewalls. Ces règles sont déployées dans la politique de sécurité globale des firewalls.

8.2.2 Gérer un parc avec des règles partagées et des règles spécifiques

Prenons l'exemple d'un prestataire qui administre également des firewalls SNS pour plusieurs clients :

- Chaque client ne possède qu'un seul firewall,
- Les firewalls sont classés dans des sous-dossiers aux noms des clients,

- Les firewalls possèdent des règles de filtrage ou de translation en commun et des règles spécifiques.

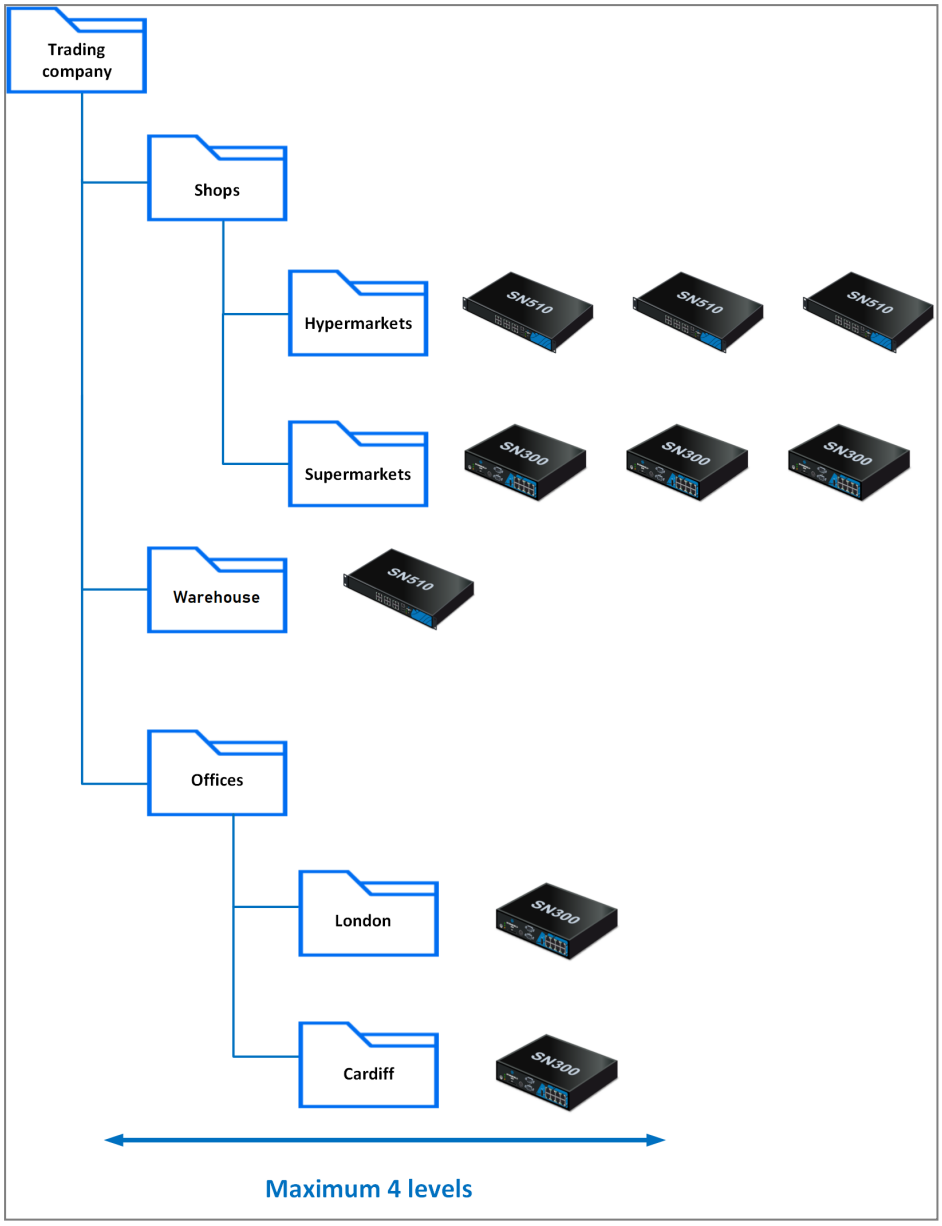
Le prestataire doit donc :

- Définir les règles partagées par tous les firewalls dans le dossier **MySMC**, par exemple pour donner à tous les firewalls l'accès à son datacenter. Il utilise pour cela un objet variable : un objet Machine représentant une interface des firewalls. Ainsi une seule règle et un seul objet suffisent pour tous les firewalls. Pour plus d'informations, reportez-vous à la section Gérer les objets.
- Définir des règles spécifiques sur chaque firewall depuis SMC, en se rendant dans l'onglet **Filtrage et translation** du firewall.
- Éventuellement, définir une règle dite "Block all" en tant que dernière règle de priorité basse dans le dossier **MySMC** pour ignorer les règles présentes dans la politique de sécurité locale des firewalls.
- Déployer la configuration sur les firewalls. Ces règles sont déployées dans la politique de sécurité globale des firewalls.

8.2.3 Gérer un parc multi-sites avec des règles partagées et spécifiques et délégation de filtrage

Prenons l'exemple d'une entreprise de grande distribution possédant un entrepôt, des bureaux et des magasins de type hypermarchés et supermarchés sur plusieurs sites :

- L'administrateur central utilise deux niveaux de sous-dossiers sous le dossier racine pour classer ses firewalls,
- Des règles de filtrage et de translation s'appliquent à tous les firewalls, d'autres sont propres à certains dossiers,
- L'administrateur veut déléguer l'administration de certains flux aux administrateurs locaux afin de leur laisser la possibilité de mettre en place des règles locales sur des services, des protocoles, des utilisateurs ou des réseaux spécifiques. Un magasin pourrait par exemple avoir besoin de communiquer avec un prestataire de vidéo-surveillance.



L'administrateur central doit donc :

- Définir les règles partagées par tous les firewalls dans le dossier **MySMC** en utilisant les objets variables. Pour plus d'informations, reportez-vous à la section Gérer les objets.
- Définir des règles partagées par les entrepôts/bureaux/magasins dans les dossiers et sous-dossiers correspondants.
- Définir éventuellement des règles spécifiques sur certains firewalls depuis SMC, en se rendant dans l'onglet **Filtrage et translation** du firewall.
- Choisir l'action **Déléguer** pour les règles concernées dans le menu **Action** de la règle.
- Définir une règle "Block all" en tant que dernière règle de priorité basse sur le dossier racine **MySMC**.
- Déployer la configuration sur les firewalls. Ces règles sont déployées dans la politique de sécurité globale des firewalls.

8.2.4 Gérer un parc multi-sites avec des jeux de règles partagés

Prenons l'exemple d'une entreprise implantée sur plusieurs sites. Sur chaque site il existe un nombre de services identique dont les réseaux et les firewalls doivent être configurés de manière homogène. Les sites ne sont pas nécessairement configurés dans le même dossier sur SMC.

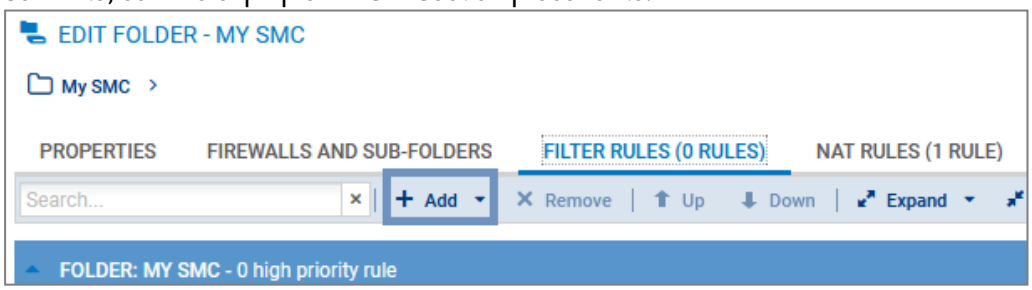
- L'administrateur central veut définir l'ensemble des règles de filtrage et de translation pour un service particulier.
- L'administrateur ne veut pas se connecter sur chaque firewall du service en direct pour définir des règles.

L'administrateur central doit donc :

- Créer un jeu de règles contenant toutes les règles de filtrage et de translation communes à un service dans le menu **Configuration** > **Jeux de règles**.
- Sélectionner les firewalls sur lesquels il veut déployer le jeu de règles.
- Lors du prochain déploiement le jeu de règles sera appliqué à tous les firewalls sélectionnés. Pour plus d'informations, reportez-vous à la section Créer des jeux de règles.

8.3 Créer des règles de filtrage et de translation (NAT)

1. Dans le menu **Configuration** > **Firewalls et dossiers**, naviguez jusqu'au niveau de dossier sur lequel vous souhaitez appliquer une règle ou jusqu'à un firewall spécifique. Dans le cas de règles spécifiques, accédez également directement aux paramètres du firewall depuis la vue de **Supervision**.
2. Ouvrez l'onglet **Filtrage et translation** et choisissez **Règles de filtrage** ou **Règles de translation**.
3. Cliquez sur **Ajouter** et choisissez d'ajouter une règle de priorité haute ou basse (choix de la priorité disponible sur les dossiers uniquement), en tenant compte de l'ordre d'application souhaité, comme expliqué dans la section précédente.



4. Configurez la règle :
   - Lorsque des objets Machine, Réseau ou Plage d'adresses IP sont utilisés dans la règle, vous pouvez utiliser des objets variables, dont l'adresse IP prendra la valeur correspondant au firewall concerné. Pour plus d'informations, reportez-vous à la section Gérer les objets.
   - Vous pouvez faire un glisser-déposer des objets entre règles de filtrage et translation ou depuis le menu **Objets** vers une règle.
   - Vous pouvez créer des séparateurs entre les règles pour les organiser en cliquant sur **Ajouter**. Ces séparateurs n'ont aucun effet sur la politique de sécurité. Cliquez sur le titre du séparateur pour modifier le nom et attribuer une couleur.
   - Les paramètres suivants ne peuvent être complétés par des données remontées par les firewalls et doivent être saisis à la main à travers des champs texte :
     - Menu **Source** > **Général** > **Interface d'entrée**, cliquez sur **Interface personnalisée** (si la règle s'applique à un dossier ou jeu de règles).
     - Menu **Destination** > **Configuration avancée** > **Interface de sortie**, cliquez sur **Interface personnalisée** (si la règle s'applique à un dossier ou jeu de règles).
     - Menu **Action** > **Qualité de service** > **File d'attente**.
     - Menu **Action** > **Qualité de service** > **File d'attente ACK**.
   - Consultez le *Manuel Utilisateur SNS* pour obtenir des détails sur les autres menus et options.
5. Lorsque la configuration des règles est terminée, déployez la configuration sur les firewalls concernés.

En plus des règles du dossier dans lequel vous vous trouvez ou du firewall, les onglets **Règles de filtrage** et **Règles de translation** affichent les règles des dossiers parents ainsi que les règles locales en lecture seule. Ainsi vous visualisez toutes les règles qui s'appliquent à un firewall sur un même écran, dans leur ordre d'application.

8.4 Créer des jeux de règles

Vous pouvez créer des jeux de règles pour regrouper les règles de filtrage ou de translation que vous souhaitez déployer sur un ou plusieurs firewalls. Cette fonctionnalité vous permet de réutiliser facilement des règles sur plusieurs firewalls indépendamment de l'arborescence.

8.4.1 Créer un jeu de règles

1. Dans le menu **Configuration** > **Jeux de règles**, cliquez sur **Créer un jeu de règles de filtrage** ou **Créer un jeu de règles de translation**. Vous ne pouvez pas créer un jeu de règles contenant les deux types de règles ou contenant un autre jeu de règles.
2. Double-cliquez sur le jeu de règles pour modifier son nom et lui affecter une couleur.
3. Dans l'onglet **Règles**, cliquez sur **Ajouter une règle** pour créer les règles qui feront partie de votre jeu de règles de filtrage ou de translation. Pour plus d'informations, reportez-vous à la section Créer des règles de filtrage et de translation (NAT).

Vous pouvez également dupliquer un jeu de règles existant en cliquant sur l'icône .

8.4.2 Assigner des jeux de règles à un firewall

Vous devez posséder le droit d'accès en écriture sur le firewall concerné pour lui assigner des jeux de règles. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Vous avez deux possibilités pour assigner des jeux de règles à un firewall.

- Dans le menu **Configuration** > **Jeux de règles** :

  Sélectionnez les jeux de règles dans la liste à gauche. Allez dans l'onglet **Firewalls**, sélectionnez les firewalls auxquels vous souhaitez assigner les jeux de règles et cliquez sur **Appliquer**. Vous pouvez choisir d'ajouter les jeux de règles en première ou en dernière position aux règles spécifiques des firewalls sélectionnés.

- Dans la politique de sécurité d'un firewall dans les onglets **Règles de filtrage** et **Règles de translation** :

  Cliquez sur **Ajouter** > **Ajouter un jeu de règles**.

Lors du déploiement suivant, les jeux de règles assignés au firewall seront ajoutés aux firewalls sélectionnés. Ils seront affichés dans la politique globale du firewall comme des séparateurs suivis de leur règles.

8.4.3 Modifier des jeux de règles pour un firewall

Pour réaliser les actions suivantes, vous devez posséder le droit d'accès en écriture sur le firewall concerné. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Depuis la politique de sécurité d'un firewall, vous pouvez :

- remplacer un jeu de règles affecté au firewall par un autre,
- modifier les jeux de règles affectés au firewall. Vous serez redirigé vers l'écran **Jeux de règles**.

8.4.4 Importer ou exporter des jeux de règles

Dans le menu **Configuration** > **Jeux de règles**, vous pouvez :

- exporter tous les jeux de règles de filtrage ou de translation dans un fichier CSV. Dans ce fichier ils seront représentés par des séparateurs suivis de leur règles. Pour plus d'informations, reportez-vous à la section Exporter des règles dans un fichier CSV.
- importer tous les jeux de règles de filtrage ou de translation à partir d'un fichier CSV. Les jeux de règles doivent impérativement être créés sur le serveur SMC avant l'import du fichier CSV, sinon l'import échouera. Pour plus d'informations, reportez-vous à la section Importer des règles depuis un fichier CSV.

8.4.5 Supprimer un jeu de règles

Vous pouvez supprimer un jeu de règles uniquement dans un de ces cas :

- il n'est utilisé par aucun firewall.
- il est utilisé par des firewalls sur lesquels vous avez le droit d'accès en écriture.

Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

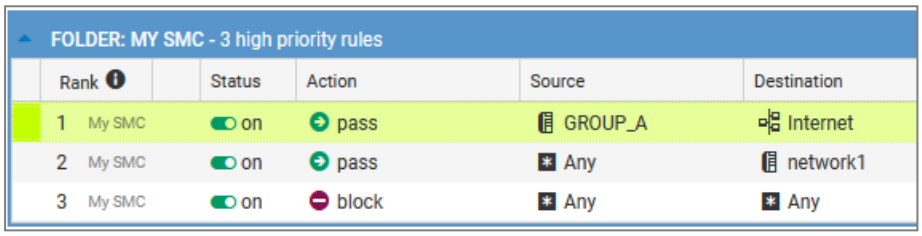
Pour supprimer un jeu de règles :

- Dans le menu **Configuration** > **Jeux de règles**, cliquez sur la croix rouge sur la ligne d'un jeu de règles.

8.5 Identifier les règles

Dans les onglets **Règles de filtrage** et **Règles de translation** d'un firewall, la colonne **Règle** permet d'identifier les règles appliquées à un firewall. Ce numéro est visible dans l'interface d'administration du firewall lui-même et dans les journaux.

Dans la vue des dossiers, la colonne **Règle** est remplacée par la colonne **Rang**. Celle-ci indique la position d'une règle dans le dossier qui la contient.



8.6 Modifier l'ordre d'exécution des règles

Dans les onglets **Règles de filtrage** ou **Règles de translation** d'un dossier ou d'un firewall, vous pouvez modifier l'ordre d'exécution des règles en les déplaçant dans le même dossier ou sur le même firewall, ou bien dans un autre dossier ou firewall.

Vous pouvez sélectionner plusieurs règles à la fois, ou bien un séparateur. Lorsque vous sélectionnez un séparateur replié, vous sélectionnez toutes les règles comprises dans ce séparateur.

Déplacer les règles au sein du même firewall ou dossier

- Sélectionnez la règle, le séparateur ou le jeu de règles et utilisez les boutons **Monter** Up et **Descendre** Down dans la barre d'outils.

-ou-

- Placez le curseur de la souris sur la colonne de gauche d'une règle et faites un glisser-déplacer.

-ou-

- Utilisez les boutons **Couper**/**Copier**/**Coller** ou les raccourcis clavier standards correspondants. Vous pouvez copier des règles ou séparateurs de la grille active ou des dossiers parents.

Déplacer les règles dans un autre dossier ou sur un autre firewall

Pour déplacer la règle, le jeu de règles ou le séparateur dans un autre dossier ou sur un firewall, utilisez les boutons **Couper**/**Copier**/**Coller** dans la barre d'outils ou les raccourcis clavier standards correspondants. Vous pouvez copier des règles de la grille active ou des dossiers parents.

Vous pouvez également créer des jeux de règles pour les réutiliser sur d'autres firewalls, indépendamment de leur dossier. Pour plus d'informations, reportez-vous à la section Créer des jeux de règles.

8.7 Rechercher une règle dans l'interface web ou dans les journaux SNS

Le serveur SMC attribue automatiquement à chaque règle de filtrage et de translation créée un identifiant unique. Cet identifiant ou "nom" de la règle est visible dans l'interface web de SMC, ainsi que dans l'interface web et les journaux du firewall concerné lorsque la règle est déployée. Vous pouvez modifier le nom par défaut dans les propriétés de la règle.

Le nom de la règle facilite l'identification de la règle lors d'une recherche dans les journaux SNS, ou dans le panneau des règles dans l'interface du firewall ou du serveur SMC.

Pour connaître le nom d'une règle dans SMC :

1. Rendez-vous dans le panneau des règles de filtrage ou de translation d'un firewall ou d'un dossier,
2. Survolez n'importe quel titre de colonne avec la souris,
3. Cliquez sur la flèche noire qui s'affiche,
4. Survolez le menu **Colonnes**,
5. Cochez la colonne **Nom**.

- ou-

1. Double-cliquez sur une règle pour afficher ses propriétés,
2. Affichez l'onglet **Général**.
3. Dans l'encart **Configuration avancée**, vous avez la possibilité de copier le nom de la règle pour faire une recherche dans les journaux SNS ou dans l'interface du firewall.

8.8 Supprimer des règles

- Utilisez la touche **Suppr**.

-ou-

- Utilisez le bouton **Supprimer** dans la barre d'outils.

Lorsqu'un dossier est supprimé, ses règles le sont également.

8.9 Supprimer des jeux de règles

Dans le menu **Configuration** > **Jeux de règles**, sélectionnez le jeu de règles que vous souhaitez supprimer et cliquez sur l'icône .

Si le jeu de règles est utilisé sur des firewalls, vous serez averti il vous sera demandé de confirmer sa suppression.

Supprimer un jeu de règles depuis l'écran de modification du firewall ne le supprime pas sur SMC, mais le jeu de règles ne sera plus affecté au firewall en question.

8.10 Importer et exporter des règles de filtrage et de translation

Le serveur SMC permet d'importer des règles depuis l'interface web ou en ligne de commande, ainsi que de les exporter.

L'import et l'export de règles permettent de :

- déployer facilement sur des firewalls des règles déjà existantes sur un autre firewall ou un autre serveur SMC.

- déporter la gestion des règles des firewalls vers le serveur SMC dans le cas d'une migration dans SMC d'un parc de firewalls déjà en production. Si vous êtes dans ce cas, reportez-vous à la section Migrer les règles locales existantes d'un firewall pour les gérer dans SMC.

8.10.1 Importer des règles depuis un fichier CSV

Cette fonctionnalité permet d'effectuer un import de règles depuis un fichier CSV créé manuellement ou exporté depuis un firewall SNS. Le même fichier peut contenir des règles de filtrage et de translation.

Créer le fichier CSV

Un exemple de fichier CSV "example-import-rules.csv" est disponible sur le serveur, dans le dossier */opt/stormshield/examples/csv/*.

Vous pouvez soit exporter des règles existantes depuis un firewall soit créer un nouveau fichier CSV.

Pour exporter le fichier CSV depuis un firewall :

1. Connectez-vous au firewall.
2. Allez dans le menu **Politique de sécurité** > **Filtrage et NAT**.
3. En haut du panneau, choisissez d'afficher la politique globale ou locale que vous souhaitez exporter. Seules les règles du slot actif sont exportées.
4. Cliquez sur le bouton **Exporter**.

IMPORTANT
Vérifiez que le logiciel d'édition du fichier CSV n'a pas modifié le caractère délimiteur ",". L'import sur le serveur SMC risque de ne pas être possible sinon. Pour plus d'informations sur le caractère délimiteur, reportez-vous à la section Choisir le caractère délimiteur dans les fichiers CSV.

Pour créer un nouveau fichier CSV, afin de connaître le détail des lignes d'en-têtes, vous pouvez :

- Vous inspirer d'un export de règles depuis un firewall,
- Consulter l'exemple disponible directement sur le serveur SMC comme indiqué ci-dessus.

Notez que vous devez créer un fichier CSV par dossier de règles ainsi qu'un fichier CSV par firewall pour les règles spécifiques au firewall.

Importer des règles depuis l'interface web

Vous devez posséder un accès en lecture-écriture pour importer des règles.

Si les règles font référence à des objets de votre configuration SNS qui ne sont pas déjà présents dans la configuration SMC, vous devez les importer au préalable sur le serveur. Pour plus d'informations sur l'import d'objets, reportez-vous à la section Importer des objets.

1. Dans le menu **Configuration** > **Firewalls et Dossiers**, naviguez jusqu'au niveau de dossier ou jusqu'au firewall sur lequel vous souhaitez importer les règles.
2. Ouvrez l'onglet **Filtrage et translation** et choisissez **Règles de filtrage** ou **Règles de translation**. Les deux types de règles peuvent être importés depuis l'un ou l'autre des onglets et depuis le même fichier CSV.
3. Cliquez sur le bouton **Importer** dans la barre d'outils.
4. Sélectionnez le fichier CSV à importer.

5. Choisissez d'ajouter les règles aux règles déjà existantes ou de les remplacer par les nouvelles règles importées. Lorsque vous sélectionnez la première option, les nouvelles règles sont ajoutées dans un séparateur indiquant la date de l'import, après les règles existantes.
   Par défaut, les règles sont importées dans les règles de priorité haute d'un dossier. Pour importer des règles dans les règles de priorité basse, spécifiez la valeur "low" dans la colonne *#smc_folder_prio* du fichier CSV (dernière colonne). Si le fichier provient d'un export depuis un firewall, cette colonne n'est pas présente et vous devez l'ajouter manuellement.

NOTE
Si vous souhaitez importer une politique de sécurité contenant des jeux de règles, vous devez d'abord les créer sur le serveur SMC. Pour plus d'informations, reportez-vous à la section Créer des jeux de règles.

En cas d'erreur, consultez le résumé de l'import.

Aucune autre action ne peut être effectuée sur le serveur pendant l'import de règles.

Importer des règles en ligne de commande

La commande d'import des règles est la suivante : `smc-import-rules`

Elle s'accompagne de différentes options selon l'utilisation.

Nous vous recommandons de posséder un accès exclusif en lecture-écriture à la session d'administration au moment de l'import.

Les jeux de règles ne peuvent pas être importés en ligne de commande.

Dans les deux cas suivants, pour chaque règle importée, le statut de l'import est affiché. En cas d'échec d'import d'une règle, la raison est donnée et aucune règle ni objet n'est importé. La totalité du fichier CSV est cependant parcourue afin que le serveur SMC relève toutes les erreurs potentielles. Corrigez ces erreurs avant de retenter un import.

Les règles importées en ligne de commande sont ajoutées après les règles déjà existantes.

Si les règles font référence à des objets de votre configuration SNS qui ne sont pas déjà présents dans la configuration SMC, vous pouvez également les importer sur le serveur, en même temps que les règles.

Vous importez les règles et les objets référencés dans les règles :

1. Exportez la liste des objets au format CSV depuis un firewall SNS en suivant la procédure de la section Créer le fichier CSV.
2. Copiez les deux fichiers CSV (règles et objets) sur le serveur SMC à l'aide du protocole SSH, dans le répertoire */tmp* par exemple.
3. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.

4. Selon la destination des règles, tapez la commande :
   - `smc-import-rules /tmp/fichier-de-regles.csv --objects /tmp/fichier-objets.csv --firewall firewall-de-destination` : la destination des règles est un firewall,
   - `smc-import-rules /tmp/fichier-de-regles.csv --objects /tmp/fichier-objets.csv --folder dossier-de-destination` : la destination des règles est un dossier. Par défaut, les règles sont importées dans les règles de priorité haute d'un dossier. Pour importer des règles dans les règles de priorité basse, ajoutez `--low-priority` à la fin de la commande ou bien spécifiez la valeur "low" dans la colonne *#smc_folder_prio* du fichier CSV (dernière colonne). Si le fichier provient d'un export depuis un firewall, cette colonne n'est pas présente et vous devez l'ajouter manuellement.

Le fichier CSV listant les objets comprend la liste complète des objets présents dans la configuration du firewall SNS, mais à cette étape le serveur SMC n'importe que les objets référencés dans les règles. Si des objets référencés dans les règles sont déjà présents sur le serveur, ils ne sont pas ré-importés.

Cependant, si besoin, vous pouvez forcer la mise à jour de ces objets avec l'option `--update` :

```
smc-import-rules /tmp/fichier-de-regles.csv --update --objects
/tmp/fichier-d-objets.csv --folder dossier-de-destination --low-priority
```

Vous importez les règles seules (sans objet) :

1. Commencez par copier le fichier CSV sur le serveur SMC à l'aide du protocole SSH, dans le répertoire */tmp* par exemple.
2. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
3. Selon la destination des règles, tapez la commande :
   - `smc-import-rules /tmp/fichier-de-regles.csv --firewall firewall-de-destination` : la destination des règles est un firewall,
   - `smc-import-rules /tmp/fichier-de-regles.csv --folder dossier-de-destination` : la destination des règles est un dossier. Par défaut, les règles sont importées dans les règles de priorité haute d'un dossier. Pour importer des règles dans les règles de priorité basse, ajoutez `--low-priority` à la fin de la commande ou bien spécifiez la valeur "low" dans la colonne *#smc_folder_prio* du fichier CSV (dernière colonne). Si le fichier provient d'un export depuis un firewall, cette colonne n'est pas présente et vous devez l'ajouter manuellement.

8.10.2 Exporter des règles dans un fichier CSV

Un accès en lecture simple suffit pour exporter des règles.

1. Dans le menu **Configuration** > **Firewalls et Dossiers**, naviguez jusqu'au niveau de dossier ou jusqu'au firewall dont vous souhaitez exporter les règles.
2. Ouvrez l'onglet **Filtrage et translation** et choisissez **Règles de filtrage** ou **Règles de translation**. Les deux types de règles peuvent être exportés depuis l'un ou l'autre des onglets dans le même fichier CSV. Elles sont différenciées dans le fichier par la colonne *#type_slot*.
3. Cliquez sur le bouton **Exporter** dans la barre d'outils.
4. Sauvegardez le fichier CSV.

Depuis un dossier, l'action d'exporter n'exporte que les règles propres au dossier et pas les règles des dossiers parents. La colonne *#smc_folder_prio* du fichier indique la priorité haute ou basse de la règle.

Depuis un firewall (dans SMC), l'action d'exporter exporte toute la politique : les règles du firewall et les règles de ses dossiers parents. La colonne *#folder* du fichier permet alors de retrouver le nom du dossier contenant chaque règle. Les colonnes *#ruleid* et *#rankid* indiquent le numéro de la règle l'identifiant dans la politique et la position de la règle dans un dossier. Pour plus d'informations, reportez-vous à la section Identifier les règles.

Si votre politique de sécurité contient des jeux de règles, ceux-ci seront transformés en séparateurs suivis par leurs règles dans le fichier CSV d'export.

8.10.3 Importer les règles d'un firewall connecté

Pour pouvoir importer les règles d'un firewall connecté au serveur SMC, celui-ci doit être en version 3.3 minimum.

Cette fonctionnalité permet d'importer les règles du slot global ou local du firewall. Dans les deux cas, les règles du slot actif uniquement sont importées.

Si les règles font référence à des objets de votre configuration SNS qui ne sont pas déjà présents dans la configuration SMC, ils sont également importés sur le serveur.

1. Dans le menu **Supervision** > **Firewalls**, double-cliquez sur le firewall.
2. Ouvrez l'onglet **Filtrage et translation** et choisissez **Règles de filtrage** ou **Règles de translation**. Dans les deux cas, les deux types de règle sont importés.
3. Cliquez sur la flèche à droite du bouton **Ajouter**.
4. Cliquez sur **Importer les règles de filtrage et de translation locales** ou **Importer les règles de filtrage et de translation globales**.
5. Suivez les étapes.

À la fin de l'opération, les règles importées sont placées dans un séparateur et sont sélectionnées.

Si l'import échoue via l'interface web, vous pouvez importer les règles en ligne de commande comme indiqué dans la section Importer des règles en ligne de commande. En cas d'erreurs, vous obtiendrez plus de détails.

8.11 Migrer les règles locales existantes d'un firewall pour les gérer dans SMC

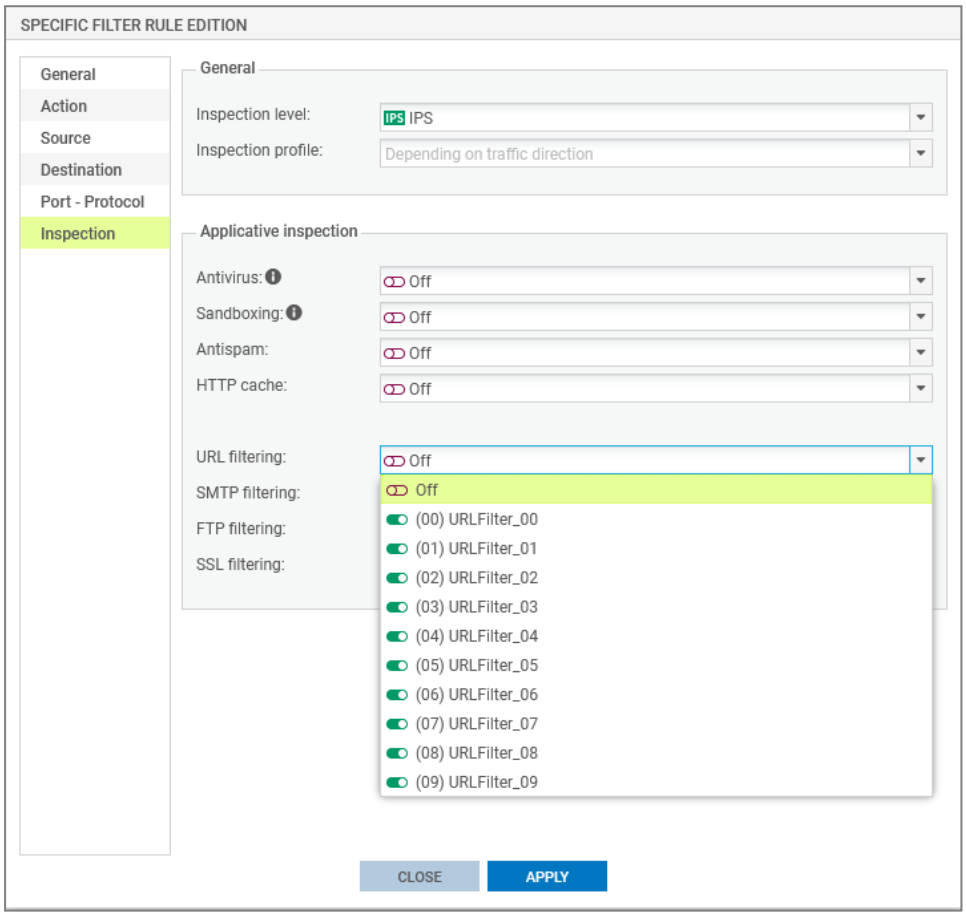
Pour gérer dans SMC des règles déjà existantes sur un firewall dans le cas d'un rattachement à SMC d'un parc de firewalls déjà en production, procédez comme suit :

1. Importez les règles d'un firewall donné sur le serveur SMC en suivant la procédure décrite à la section Importer les règles d'un firewall connecté.
2. Inspirez-vous des Exemples de cas d'usage pour choisir comment organiser les règles nouvellement importées.
3. Depuis SMC, déployez les règles sur le firewall en question. Elles apparaîtront dans la politique globale du firewall et seront appliquées en priorité.
4. Assurez-vous du bon fonctionnement de cette nouvelle organisation.
5. Éventuellement, définissez une règle dite "Block all" en tant que dernière règle de priorité basse dans le dossier **MySMC** pour ignorer les règles présentes dans la politique de sécurité locale des firewalls.
6. À terme, supprimez les règles qui ont été migrées des politiques locales du firewall vers SMC.

Si vous ne créez pas de règle "Block all" en tant que dernière règle dans SMC, les règles de filtrage et de translation locales, c'est-à-dire créées directement sur un firewall, seront lues après les règles dites globales (provenant de SMC).

8.12 Gérer le filtrage d'URL sur les firewalls SNS depuis SMC

Dans SMC, il est possible de créer des règles de filtrage faisant référence à des profils de filtrage d'URL définis localement sur les firewalls, en sélectionnant leur identifiant (00 à 09).



Vous ne pouvez cependant pas paramétrer ces profils directement dans SMC et ceux-ci peuvent être différents sur chaque firewall bien que portant le même identifiant.

Cette section explique comment diffuser une politique de filtrage d'URL commune sur tout ou partie d'un parc de firewalls à l'aide de SMC, à partir de la politique de filtrage d'URL définie sur un firewall "modèle".

Cette pratique nécessite deux scripts : un premier script permettant de récupérer la politique de filtrage d'URL du firewall modèle et un deuxième script permettant de diffuser cette politique sur les firewalls choisis.

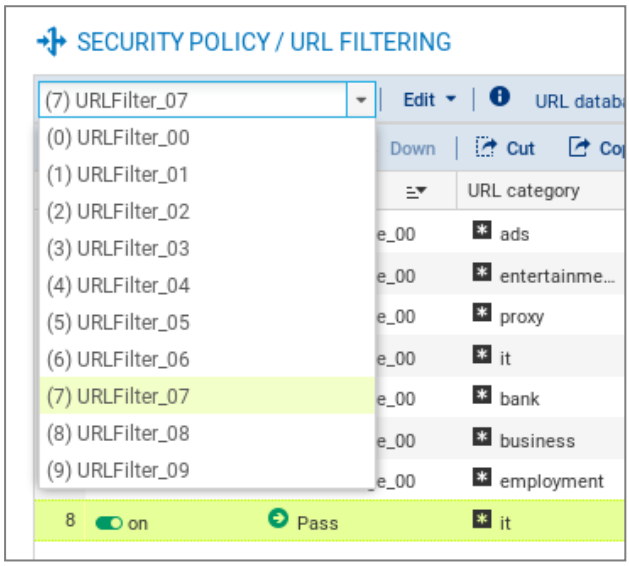
IMPORTANT
Le firewall modèle et les firewalls cibles doivent être dans la même version.

Pour appliquer cette procédure, suivez les trois étapes suivantes dans l'ordre indiqué.

8.12.1 Créer la politique de filtrage d'URL modèle

La première étape consiste à créer ou modifier un ou plusieurs profils de filtrage d'URL sur un firewall (10 profils disponibles). Ce firewall représente la configuration URL modèle à diffuser sur les autres firewalls.

1. Connectez-vous à l'interface web d'administration du firewall "modèle" par son adresse IP ou directement via SMC.
2. Ouvrez le menu **Politique de sécurité** > **Filtrage URL**.
3. Créez ou modifiez les profils de filtrage d'URL nécessaires.



8.12.2 Sauvegarder la politique de filtrage d'URL du firewall modèle

Le script suivant permet de récupérer la politique de filtrage d'URL du firewall modèle (profils de filtrage d'URL et Objets Web).

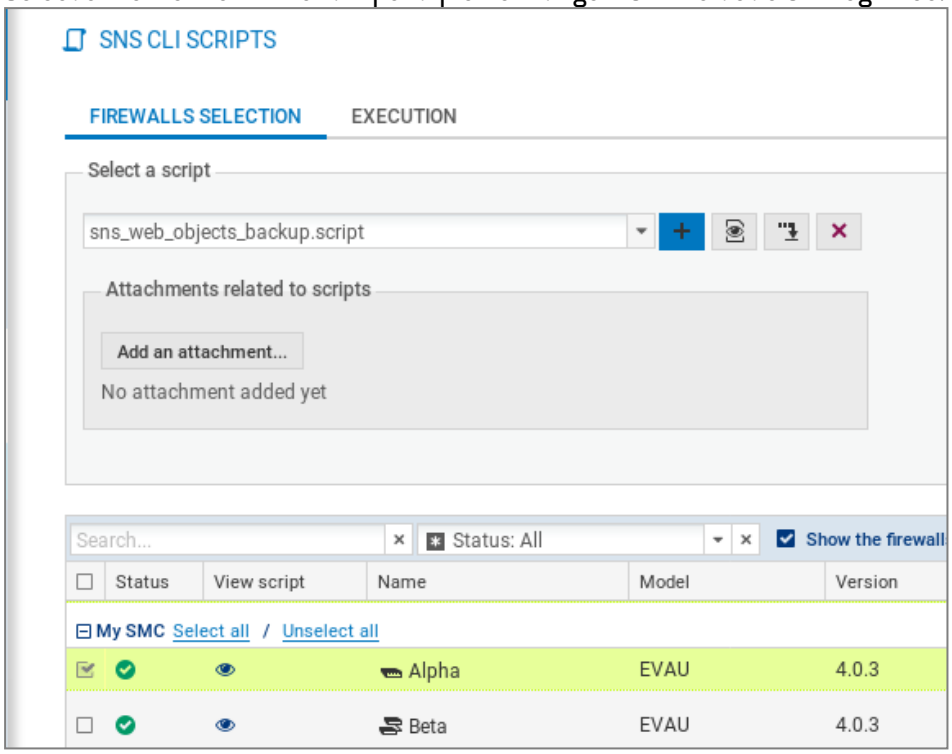
```
#########################################################################
# Save URLs, Certificate names, URL and CN groups and the               #
# URL base of a SNS #firewall                                           #
#                                                                       #
# The $SAVE_TO_DATA_FILE argument indicates the name of the file in     #
# which the result of the execution will be saved                       #
#########################################################################

CONFIG BACKUP list=urlfiltering $SAVE_TO_DATA_FILE("backup-URL.na")
```

Pour utiliser le script :

1. Copiez-le dans un éditeur de texte et sauvegardez-le avec l'extension *.script*.
2. Dans SMC, ouvrez le menu **Déploiement** > **Scripts CLI SNS**.
3. Sélectionnez le script que vous avez sauvegardé.

4. Sélectionnez le firewall dont la politique de filtrage d'URL doit être sauvegardée.



5. Exécutez le script.
6. Téléchargez l'archive générée par le script. L'archive contient la sauvegarde *backup-URL.na*.

Pour plus d'informations sur l'exécution de scripts CLI SNS, reportez-vous à la section Exécuter des commandes CLI SNS sur un parc de firewalls.

8.12.3 Diffuser la politique de filtrage URL modèle

Les scripts suivants permettent de diffuser la politique de filtrage d'URL sauvegardée précédemment sur les autres firewalls.

- Script pour une utilisation du filtrage avec base URL Stormshield embarquée :

```
#####################################################################
# Restore URLs, Certificate names, URL and CN groups and the URL#
# base of a SNS firewall                                            #
#####################################################################

# use the embedded categories
CONFIG OBJECT URLGROUP SETBASE base=NETASQ


# Restore the configuration
CONFIG RESTORE list=urlfiltering fwserial=local $FROM_DATA_FILE("backup-
URL.na")
```

- Script pour une utilisation du filtrage avec base URL Stormshield avancée (avec l'option Extended Web Control) :

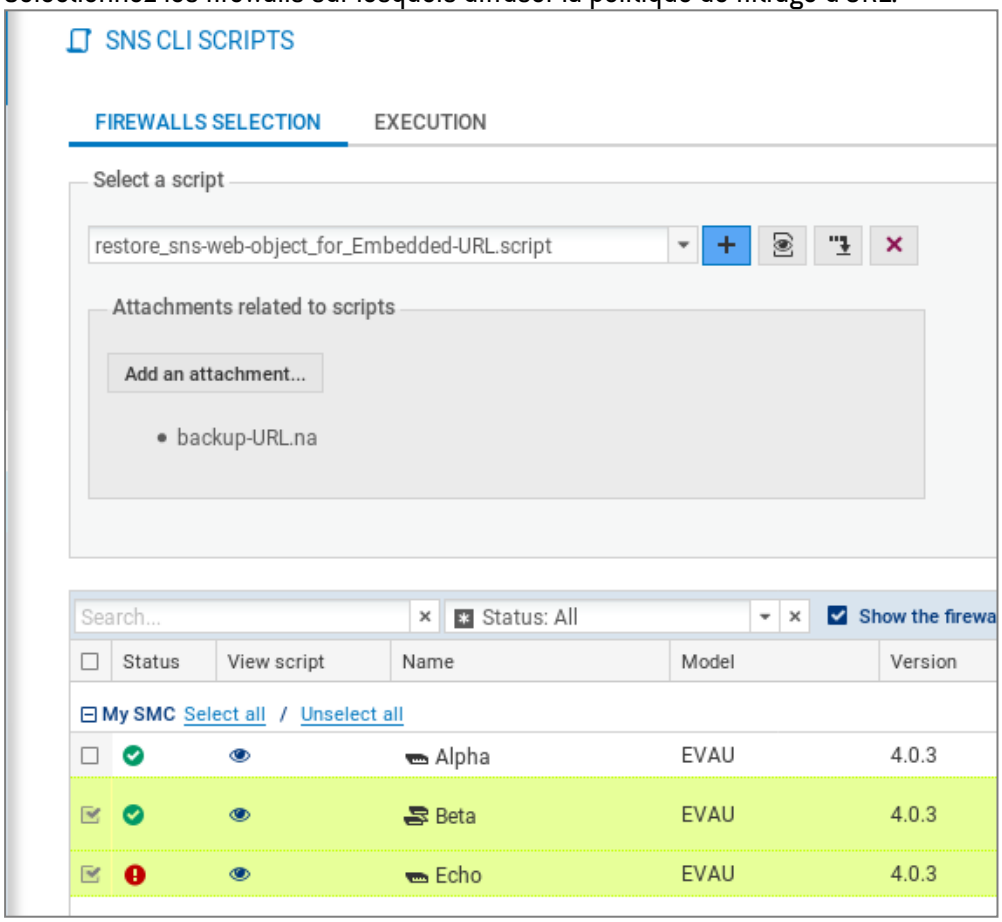
```
#####################################################################
# Restore URLs, Certificate names, URL and CN groups and the URL#
# base of a SNS firewall                                            #
#####################################################################
```

```
CONFIG OBJECT URLGROUP SETBASE base=CLOUDURL


# Restore the configuration
CONFIG RESTORE list=urlfiltering fwserial=local $FROM_DATA_FILE("backup-
URL.na")
```

Pour utiliser les scripts :

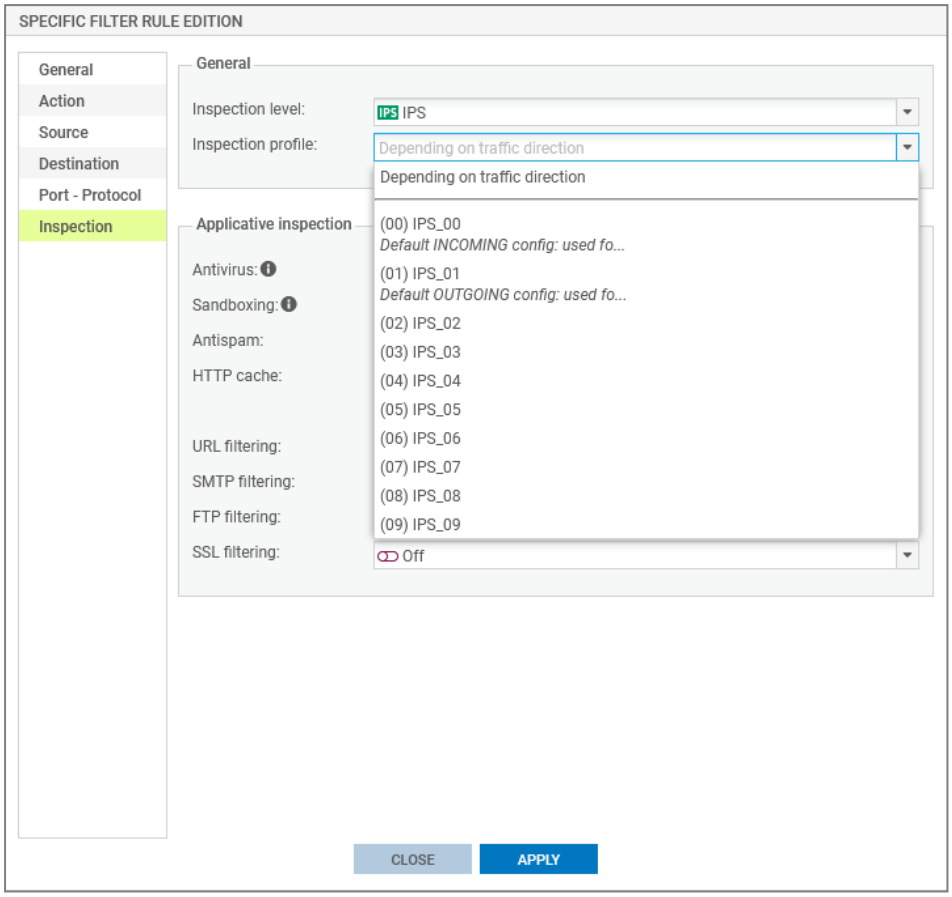
1. Copiez le script de diffusion adapté à la base URL que vous utilisez dans un éditeur de texte et sauvegardez-le avec l'extension *.script*.
2. Dans SMC, ouvrez le menu **Déploiement** > **Scripts CLI SNS**.
3. Sélectionnez le script que vous avez sauvegardé.
4. Sélectionnez en tant que pièce jointe le fichier de sauvegarde *.na* précédemment créé.
5. Sélectionnez les firewalls sur lesquels diffuser la politique de filtrage d'URL.



6. Exécutez le script.
7. Vous pouvez vous connecter sur un firewall via SMC pour constater que la politique de filtrage d'URL a bien été prise en compte.

8.13 Gérer les profils d'inspection IPS sur les firewalls SNS depuis SMC

Dans SMC, il est possible de créer des règles de filtrage faisant référence à des profils d'inspection IPS définis localement sur les firewalls, en sélectionnant leur identifiant (00 à 09).



Vous ne pouvez cependant pas paramétrer ces profils directement dans SMC et ceux-ci peuvent être différents sur chaque firewall bien que portant le même identifiant.

Cette section explique comment diffuser des profils d'inspection IPS communs sur tout ou partie d'un parc de firewalls à l'aide de SMC, à partir des profils définis sur un firewall "modèle".

Cette pratique nécessite deux scripts : un premier script permettant de récupérer les profils du firewall modèle et un deuxième script permettant de diffuser ces profils sur les firewalls choisis.

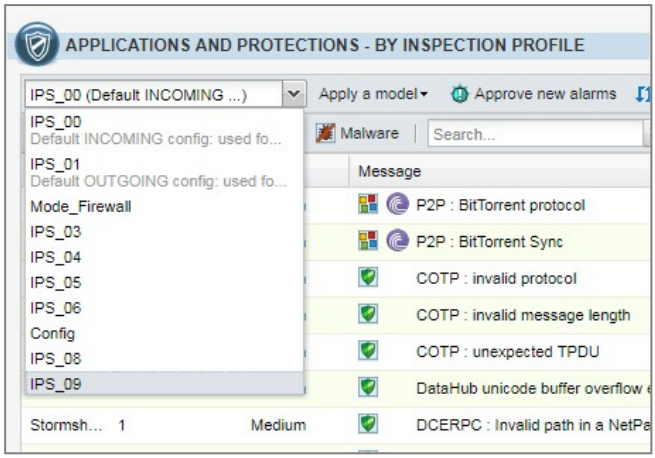
IMPORTANT
Le firewall modèle et les firewalls cibles doivent être dans la même version.

Pour appliquer cette procédure, suivez les trois étapes suivantes dans l'ordre indiqué.

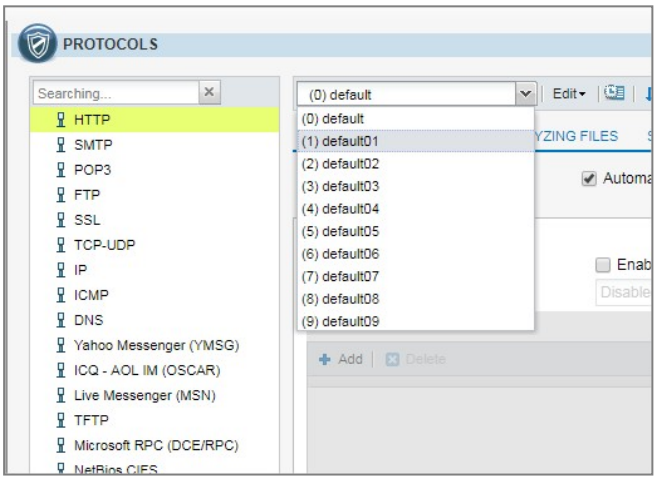
8.13.1 Modifier les profils d'inspection IPS modèles

La première étape consiste à modifier un ou plusieurs profils IPS parmi les 10 profils disponibles sur un firewall. Ce firewall représente la configuration IPS modèle à diffuser sur les autres firewalls.

1. Connectez-vous à l'interface web d'administration du firewall "modèle" par son adresse IP ou directement via SMC.
2. Ouvrez le menu **Protection applicative** > **Applications et protections**.
3. Modifiez les paramètres pour les applications et protections souhaitées.



4. Ouvrez le menu **Protection applicative** > **Protocoles**.
5. Modifiez les paramètres pour les protocoles souhaités.



8.13.2 Sauvegarder les profils d'inspection IPS du firewall modèle

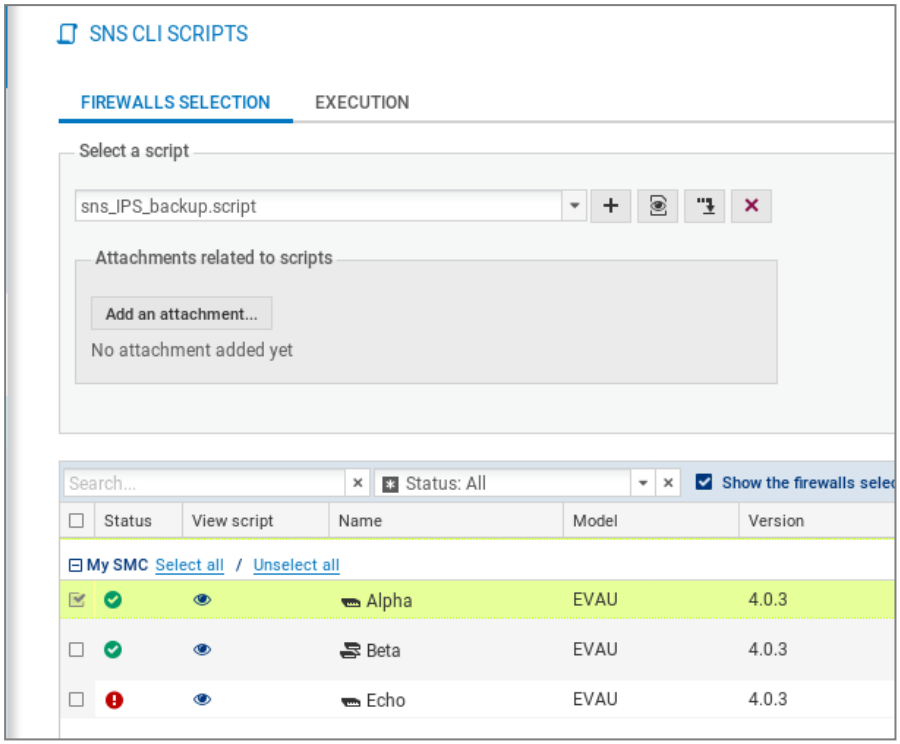
Le script suivant permet de récupérer les profils d'inspection IPS du firewall modèle.

```
#########################################################################
# Save the IPS configuration for a given SNS firewall
#
# The $SAVE_TO_DATA_FILE argument indicates the name of the file in
# which the result of the execution will be saved
#########################################################################


CONFIG BACKUP list=securityinspection $SAVE_TO_DATA_FILE("backup-IPS-
Conf.na")
```

Pour sauvegarder les profils :

1. Copiez le script dans un éditeur de texte et sauvegardez-le avec l'extension *.script*.
2. Dans SMC, ouvrez le menu **Déploiement** > **Scripts CLI SNS**.
3. Sélectionnez le script que vous avez sauvegardé.
4. Sélectionnez le firewall dont les profils d'inspection IPS doivent être sauvegardés.



5. Exécutez le script.
6. Téléchargez l'archive générée par le script. L'archive contient la sauvegarde *backup-IPS-Conf.na*.

Pour plus d'informations sur l'exécution de scripts CLI SNS, reportez-vous à la section Exécuter des commandes CLI SNS sur un parc de firewalls.

8.13.3 Diffuser les profils d'inspection IPS

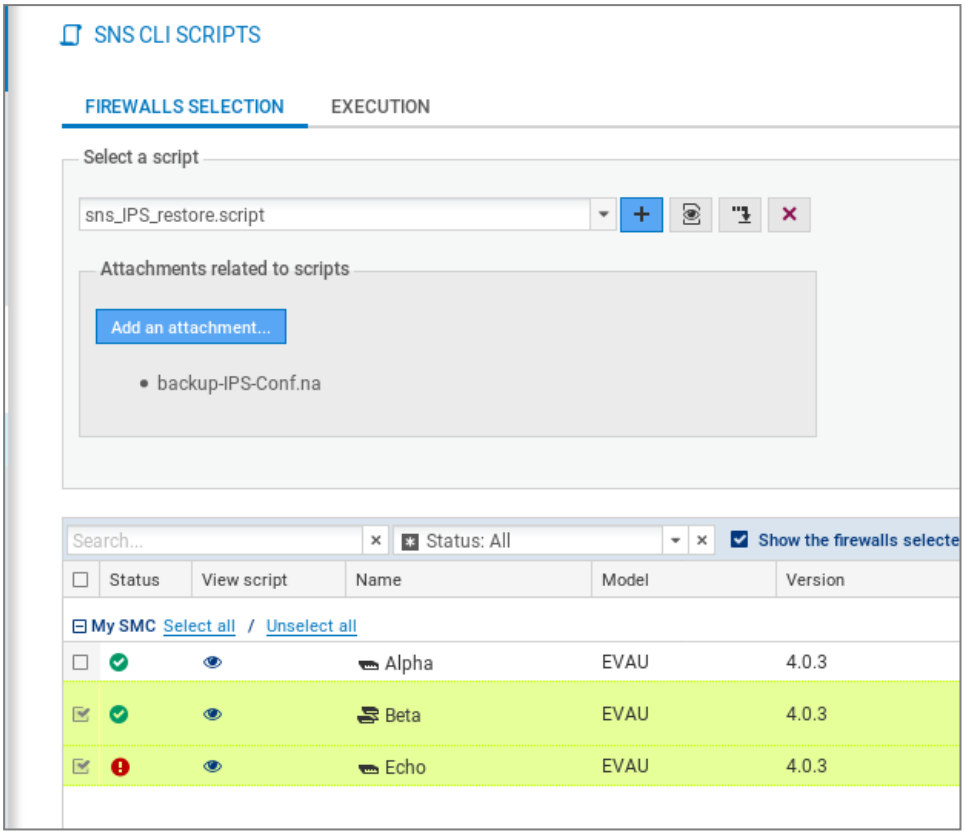
Le script suivant permet de diffuser sur les autres firewalls les profils d'inspection IPS sauvegardés précédemment.

```
#############################################################
# Restore the IPS configuration for one or several SNS firewall(s)
#
# The $FROM_DATA_FILE argument indicates the name of the file that will
# be uploaded to the firewall(s)
#############################################################


# Restore the IPS configuration
CONFIG RESTORE list=securityinspection $FROM_DATA_FILE("backup-IPS-
Conf.na")
```

Pour diffuser les profils :

1. Copiez le script dans un éditeur de texte et sauvegardez-le avec l'extension *.script*.
2. Dans SMC, ouvrez le menu **Déploiement** > **Scripts CLI SNS**.
3. Sélectionnez le script que vous avez sauvegardé.
4. Sélectionnez en tant que pièce jointe le fichier de sauvegarde *.na* précédemment créé.
5. Sélectionnez les firewalls sur lesquels diffuser les profils d'inspection IPS.



6. Exécutez le script.
7. Vous pouvez vous connecter sur un firewall via SMC pour constater que les profils ont bien été pris en compte.

8.14 Ajouter des services Web

Les règles de filtrage peuvent s'appliquer à des machines dont l'adresse IP publique est classifiée dans l'un des services Web (précédemment appelés "groupes de réputation") définis sur les firewalls SNS.

Afin de bénéficier des mises à jour de services Web sur les firewalls SNS, sans avoir à mettre à jour votre version du serveur SMC, vous avez la possibilité d'ajouter manuellement de nouveaux services Web.

Pour ajouter de nouveaux services Web, vous devez connaître le nom des services utilisés sur les firewalls SNS puis les ajouter dans le fichier */data/config/smc-webservices.local*, comme indiqué ci-dessous.

8.14.1 Connaître le nom des services Web à utiliser

Pour connaître le nom des services Web, vous pouvez récupérer la liste soit depuis le Portail de sécurité Stormshield, soit depuis un firewall SNS.

Depuis le Portail de sécurité Stormshield:

1. Accédez à la liste des services Web disponible sur le Portail de sécurité Stormshield.
2. Récupérez la liste au format *.txt* en cliquant sur le bouton en bas de la page.
3. Copiez la liste et ajoutez-la sur le serveur SMC comme indiqué dans la procédure suivante.

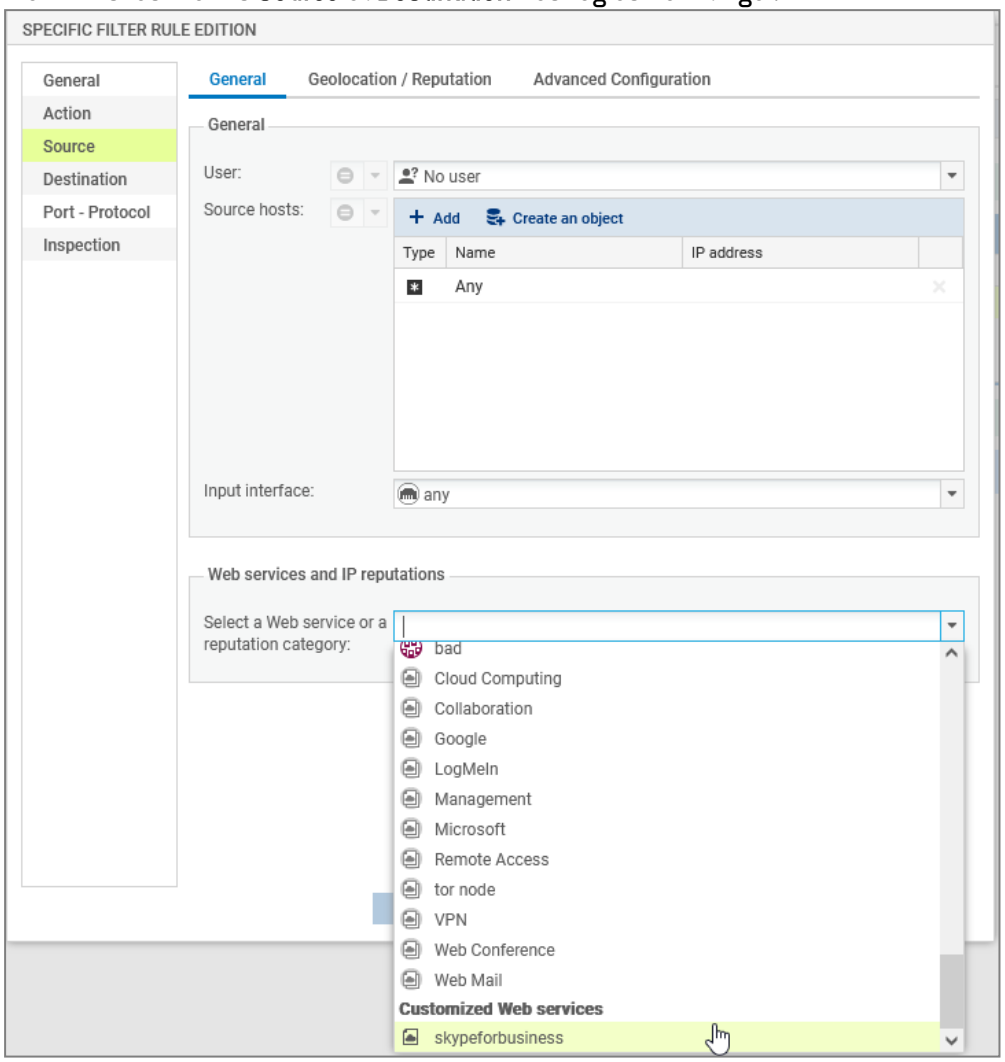
Depuis un firewall SNS:

1. Sur un firewall SNS à jour, exécutez la commande `config object list type=iprep`.
2. Le nom de service Web à utiliser pour l'ajouter sur le serveur SMC est la valeur du champ "name", par exemple "skypeforbusiness" dans l'image ci-dessous.

8.14.2 Ajouter les services Web sur le serveur SMC

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Ajoutez les nouveaux noms de services Web dans le fichier */data/config/smc-webservices.local* en suivant la syntaxe suivante :
   webservice1
   webservice2
   webservice3

3. Dans l'interface web du serveur, rafraîchissez l'affichage pour voir les nouveaux services Web dans les menus **Source** et **Destination** des règles de filtrage :



9. Configurer la QoS

La QoS, ou qualité de service, désigne toute technologie capable de gérer la transmission des données, tout en réduisant la perte de paquets, la latence et la gigue pour les flux prioritaires du réseau. Ce concept a pour but de contrôler et de gérer les ressources réseau, en hiérarchisant certains types de données et flux réseau.

Depuis SMC, vous pouvez configurer la QoS sur les firewalls SNS à partir de la version 4.3.15 LTSB ou 4.5.3.

Pour configurer la QoS dans SMC, procédez comme suit :

1. Ajoutez des files d'attente et des Traffic shapers dans le menu **Configuration**.
2. Associez ces files d'attente et Traffic shapers aux interfaces dans les paramètres des firewalls. Ces files d'attente constituent les files d'attente par défaut.
3. Configurez la QoS dans les règles de filtrage dans les paramètres des firewalls, afin de définir des files d'attente spécifiques en fonction des flux réseau.

NOTE
Vous ne pouvez pas superviser la QoS depuis SMC. Pour superviser la QoS d'un firewall, connectez-vous directement à l'interface web d'administration du firewall.

Pour plus d'informations sur la QoS et pour les détails de sa configuration sur les firewalls, reportez-vous à la Note technique Configurer la QoS sur les firewalls SNS.

9.1 Configurer les files d'attente et les Traffic shapers

Avant de pouvoir appliquer de la QoS sur les interfaces réseau des firewalls et dans les règles de filtrage, vous devez d'abord ajouter et configurer des files d'attente et des Traffic shapers.

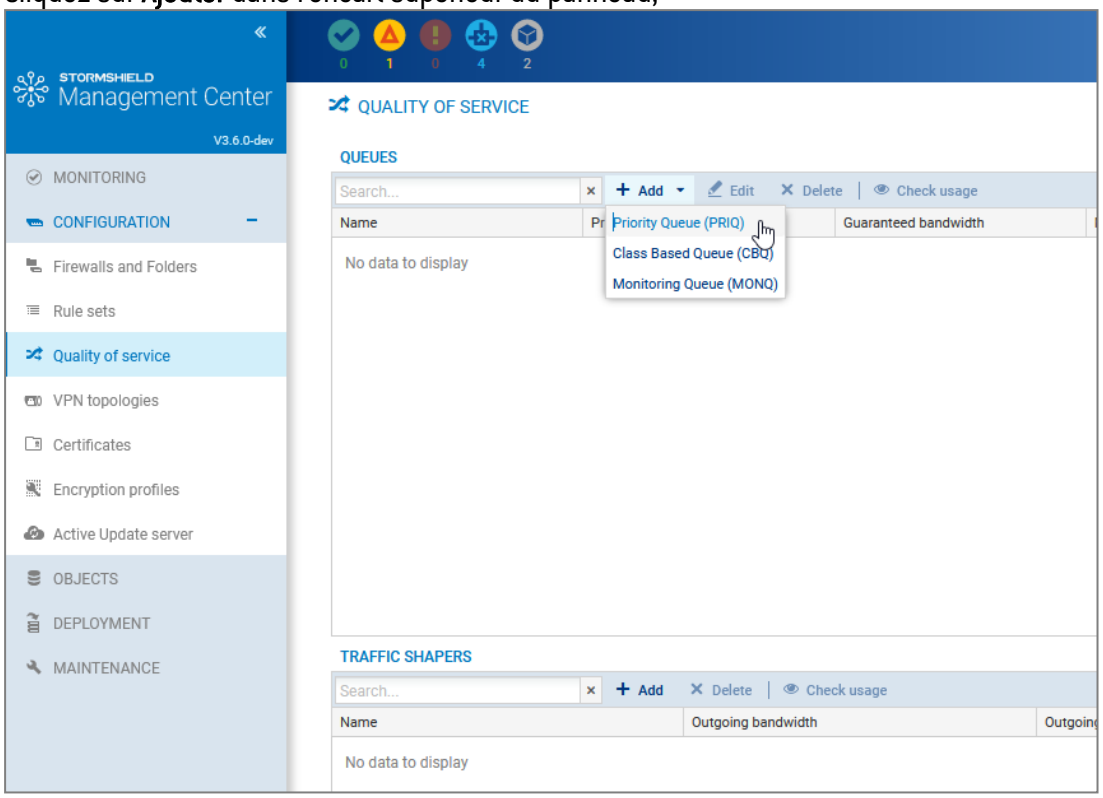
- Les files d'attente permettent de réserver de la bande passante à un type de flux ou de la limiter, en indiquant les bandes passantes garanties ou maximales à appliquer. Vous pouvez également définir des files d'attente par priorité afin de prioriser les paquets selon leur provenance. Vous devez définir des files d'attente par défaut et des files d'acquittement à associer aux interfaces réseau, puis d'autres files d'attente à utiliser dans les règles de filtrage.
- Les Traffic shapers sont des régulateurs de flux, ils permettent de définir la bande passante maximale utilisable sur chaque interface réseau soumise à la QoS.

9.1.1 Ajouter des files d'attente et des Traffic shapers

Pour ajouter des Traffic shapers et des files d'attente, rendez-vous dans le menu **Configuration** > **Qualité de service**.

Pour une file d'attente :

1. Cliquez sur **Ajouter** dans l'encart supérieur du panneau,



2. Sélectionnez le type de file d'attente :

Traitement par priorité (PRIQ)	Elle permet de prioriser les paquets avec un classement de la priorité 0 (flux les plus prioritaires) à la priorité 7 (flux les moins prioritaires). Les paquets associés à une règle de filtrage utilisant une file PRIQ sont traités avant les paquets qui ne sont pas affectés à une file PRIQ ou qui sont attachés à une file PRIQ moins prioritaire.
Réservation ou limitation de bande passante (CBQ)	Elle est utilisée pour la réservation ou la limitation de bande passante, en indiquant les bandes passantes garanties ou maximales à appliquer pour les flux sortants et pour le trafic de retour des connexions. Au moins une valeur doit être différente de 0.
Surveillance du trafic (MONQ)	Elle n'influe pas sur le trafic réseau mais permet d'enregistrer les informations de bande passante utilisée par les flux surveillés.

3. Dans la fenêtre qui s'ouvre, nommez la file d'attente et remplissez les champs obligatoires selon le type choisi. Pour les files de type CBQ, vous pouvez utiliser les variables personnalisées pour indiquer les valeurs de bande passante. Dans ce cas, copiez-collez le nom de la variable souhaitée (par exemple %CUSTOM_VAR1%). L'unité utilisée est le kbit/s.
4. Ajoutez la file d'attente.

Pour un Traffic shaper :

1. Cliquez sur **Ajouter** dans l'encart inférieur du panneau,
2. Nommez le Traffic shaper,
3. Dans la colonne **Bande passante sortante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface,
4. Dans la colonne **Unité**, indiquez l'unité de bande passante,

5. Dans la colonne **Bande passante entrante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface,
6. Dans la colonne **Unité**, indiquez l'unité de bande passante,
7. Validez en cliquant sur **Appliquer**.

Vous pouvez utiliser les variables personnalisées pour indiquer les valeurs de bande passante. Dans ce cas, copiez-collez le nom de la variable souhaitée (par exemple %CUSTOM_VAR2%). L'unité utilisée est le kbit/s.

Pour des conseils détaillés sur le paramétrage des files d'attente et des Traffic shapers, reportez-vous à la Note technique Configurer la QoS sur les firewalls SNS.

9.1.2 Modifier ou supprimer des files d'attente ou des Traffic shapers

Vous pouvez modifier ou supprimer des files d'attente ou des Traffic shapers, à condition qu'ils ne soient pas utilisés par des firewalls sur lesquels vous ne possédez pas le droit d'accès en écriture. Vous pouvez vérifier leur utilisation en cliquant sur le bouton **Vérifier l'utilisation** de chaque grille.

Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

9.2 Configurer la QoS sur les interfaces des firewalls

Pour mettre en œuvre la QoS sur votre réseau, vous devez associer des files d'attente et des Traffic shapers aux interfaces de vos firewalls.

Pour chaque interface concernée par la QoS, vous associez :

- Un Traffic shaper.
- Une file d'attente par défaut : cette file d'attente sera empruntée par tout flux pour lequel aucune file d'attente de QoS n'est précisée dans la règle de filtrage du flux considéré.
- Une file d'attente d'acquittement par défaut.

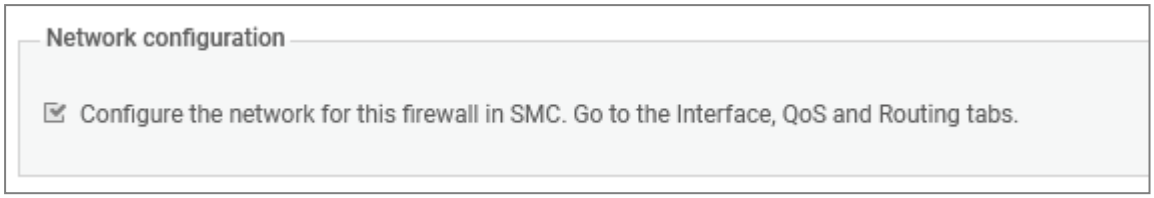
Pour réaliser ces opérations, vous devez posséder le droit d'accès en écriture sur les dossiers concernés dans l'interface web de SMC. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

9.2.1 Prérequis

- La mise en œuvre de la QoS depuis SMC est compatible avec les firewalls SNS à partir de la version 4.3.15 LTSB ou 4.5.3.
- Vous devez avoir configuré des files d'attente et des Traffic shapers sur SMC auparavant. Pour les configurer, reportez-vous à la section Configurer les files d'attente et les Traffic shapers.
- La gestion du réseau depuis SMC doit être activée sur chaque firewall concerné.

9.2.2 Activer la gestion du réseau d'un firewall SNS par SMC

Rendez-vous dans l'onglet **Système > Configuration** du firewall concerné et vérifiez que la case **Configurer le réseau pour ce firewall depuis SMC** est cochée pour indiquer que SMC gère le réseau pour ce firewall.



Si cette option n'est pas cochée, SMC ne gère pas le réseau pour ce firewall et l'onglet **QoS** du firewall est en lecture seule.

9.2.3 Configurer la QoS sur une interface

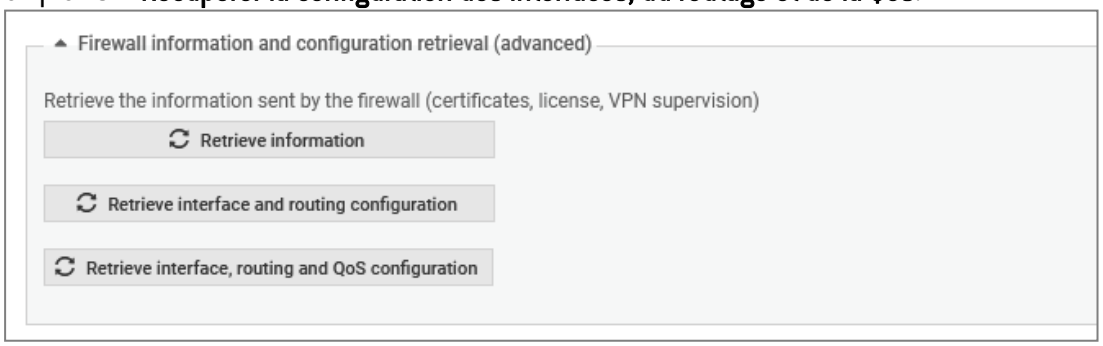
1. Rendez-vous dans l'onglet **QoS** du firewall,
2. Cliquez sur **Ajouter**,
3. Sélectionnez l'interface,
4. Sélectionnez un Traffic shaper,
5. Sélectionnez une file d'attente par défaut,
6. Sélectionnez une file d'acquittement par défaut.

Vous ne pouvez pas configurer la QoS sur une interface de type GRETAP depuis SMC. Dans ce cas, connectez-vous directement au firewall.

9.2.4 Forcer la récupération de la configuration QoS sur un firewall

Si la QoS est déjà configurée localement sur le firewall, vous pouvez récupérer sa configuration dans SMC. La gestion du réseau depuis SMC doit être activée sur le firewall.

1. Rendez-vous dans les paramètres du firewall,
2. Dans l'onglet **Système > Configuration**, cochez la case **Configurer le réseau pour ce firewall depuis SMC** si elle n'est pas déjà cochée,
3. Dépliez l'encart **Récupération des informations et de la configuration du firewall (avancé)** et cliquez sur **Récupérer la configuration des interfaces, du routage et de la QoS**.



9.3 Configurer la QoS dans les règles de filtrage

Par défaut, les flux réseau utilisent les files d'attente associées aux interfaces par lesquelles ils entrent et sortent. Pour définir des files d'attente spécifiques par type de flux, vous devez créer des règles de filtrage. Vous pouvez ainsi prioriser les types de flux selon leur provenance.

1. Créez une règle de filtrage depuis un jeu de règles, les paramètres d'un dossier ou les paramètres d'un firewall.

2. Configurez la règle comme indiqué à la section Créer des règles de filtrage et de translation (NAT).
3. Dans le menu **Action**, onglet **Général**, assurez-vous que l'action sélectionnée est **Passer**. Sinon, il n'est pas possible de configurer la QoS dans la règle.
4. Dans l'onglet **Qualité de service**, sélectionnez la file d'attente et si nécessaire la file d'acquittement (**File d'attente ACK**).
5. Pour des informations sur le champ **Répartition**, reportez-vous au Manuel Utilisateur SNS.

10. Exécuter des commandes CLI SNS sur un parc de firewalls

SMC permet l'exécution de scripts CLI SNS sur des firewalls. Ce mode permet la configuration de toutes les fonctionnalités des firewalls. Ainsi les scripts offrent une solution de déploiement d'une configuration d'un parc de firewalls pour des fonctionnalités non disponibles dans les menus du serveur SMC.

L'exécution des scripts CLI SNS est possible depuis l'interface web du serveur SMC et depuis l'interface de ligne de commande.

Vous devez posséder le droit d'accès en écriture sur les firewalls pour exécuter des scripts CLI SNS. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour consulter un exemple d'utilisation de scripts, reportez-vous à la section Mettre à jour les firewalls en utilisant les scripts CLI SNS .

10.1 Créer le script de commandes CLI

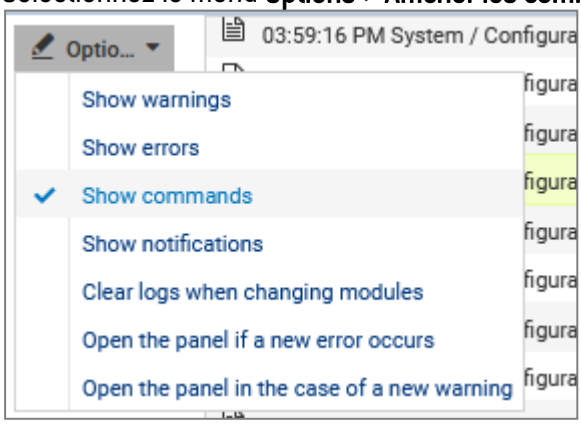
Créez un fichier texte de 5 Mo maximum, encodé en UTF-8 et portant l'extension *.script* qui contient les commandes à exécuter sur votre parc de firewalls.

Les commandes exécutables disponibles de la console CLI sont référencées :

- Dans l'interface web d'administration des firewalls, menu **Configuration** > **Système** > **Console CLI**. Consultez le *Manuel Utilisateur SNS* pour savoir comment utiliser l'interface.
- Dans le guide *CLI Serverd Commands Reference Guide*.

Pour vous aider, vous pouvez également afficher les commandes CLI dans l'interface web d'administration d'un firewall afin de copier les commandes utilisées pour réaliser une action que vous voulez reproduire dans votre script :

1. Cliquez sur la flèche noire en bas de l'interface d'administration d'un firewall pour déplier le panneau d'événements.
2. Sélectionnez le menu **Options** > **Afficher les commandes**.



3. Effectuez une action (créer un objet par exemple) que vous souhaitez répéter dans le script.
4. Copiez les commandes qui ont été exécutées pour produire l'action.
5. Collez-les dans votre script.

Pour adapter les commandes à chaque firewall, utilisez des variables entourées du signe %. Pour connaître les variables à utiliser, référez-vous à la section Utiliser des variables .

POUR ALLER PLUS LOIN
Le dépôt public stormshield/sns-scripting sur GitHub propose des exemples de scripts CLI SNS prêts à l'emploi et conçus pour être exécutés depuis SMC afin de configurer et maintenir votre parc de firewalls. Ce dépôt regroupe également des scripts Python s'appuyant sur l'API SNS, ainsi que des rôles Ansible, si vous souhaitez automatiser davantage les déploiements au-delà des scripts CLI SNS natifs.

10.2 Utiliser des variables

Les propriétés des firewalls indiquées dans la liste des firewalls ou dans les paramètres de chaque firewall (menu **Supervision** > **Firewalls**) constituent des variables qui peuvent être utilisées dans les scripts.

Vous pouvez utiliser encore plus de variables à l'aide d'un fichier CSV. Reportez-vous à la section Utiliser des variables .

Les variables sont sensibles à la casse.

10.2.1 Utiliser les variables spécifiques aux firewalls

Insérez les variables entourées du signe % dans les commandes CLI de votre script.

Ces variables prennent une valeur différente suivant le firewall sur lequel le script est exécuté :

- FW_ADDRESS : champ Adresse IP du firewall connectée au serveur SMC,
- FW_DESCRIPTION : champ Description du firewall,
- FW_LOCATION : champ Lieu du firewall,
- FW_MODEL : modèle du firewall,
- FW_NAME : nom du firewall,
- FW_SERIAL : numéro de série du firewall,
- FW_VERSION : numéro de la version du firewall,
- FW_ARCHITECTURE : architecture du processeur du firewall,
- FW_SIZE : gamme du firewall,
- FW_VM : firewall virtuel,
- FW_UPD_SUFFIX : variable utilisée pour la mise à jour de firewall SNS, prenant la valeur SNS-%FW_ARCHITECTURE%-%FW_SIZE%.maj (par exemple *SNS-amd64-M.maj*). Pour plus d'informations, reportez-vous à la section Mettre à jour les firewalls en utilisant les scripts CLI SNS .
- HA_PEER_SERIAL: numéro de série du firewall passif (sans Haute Disponibilité, la valeur sera vide),
- HA_PEER_FIRMWARE: numéro de la version du firewall passif (sans Haute Disponibilité, la valeur sera vide),
- CUSTOM_X : champs personnalisés

Les variables %CUSTOM_X% sont des variables personnalisables à votre convenance. Double-cliquez sur un firewall dans la liste du menu **Supervision** > **Firewalls** et ouvrez l'onglet **Variables**

personnalisées. Pour plus d'informations, reportez-vous à la section Créer des variables personnalisées.

10.2.2 Utiliser les variables globales

Ces variables ont la même valeur pour tous les firewalls et font référence à la date et heure du serveur :

- NOW : date complète au format local (exemple : "%NOW%" => "20151222-104727"),
- NOW_AS_DATE : date au format local (exemple : "%NOW_AS_DATE%" => "20151222"),
- NOW_AS_TIME : heure au format local (exemple : "%NOW_AS_TIME%" => "104727").

10.2.3 Utiliser un fichier CSV

Afin de réaliser des opérations sur un grand nombre de firewalls ou bien de réaliser une opération complexe sur un firewall, nous recommandons l'utilisation d'un fichier CSV.

Le fichier CSV n'est utilisable que depuis l'interface de ligne de commande. Les variables associées aux firewalls sont alors lues depuis ce fichier et le script est dupliqué autant de fois qu'il y a de lignes dans le fichier CSV pour un firewall donné.

Un exemple de fichier CSV "example-sns-cli-script.csv" est disponible sur le serveur, dans le dossier */opt/stormshield/examples/csv/*.

Pour savoir comment utiliser le fichier CSV depuis l'interface de ligne de commande, reportez-vous à la section Exemple d'utilisation de script en ligne de commande avec un fichier CSV.

10.3 Exécuter le script CLI SNS depuis l'interface web

1. Dans l'interface web du serveur SMC, sélectionnez **Déploiement** > **Scripts CLI SNS**.
2. Dans l'onglet **Sélection des firewalls**, sélectionnez le script à exécuter.
   - Vous pouvez stocker une liste de scripts sur le serveur SMC,
   - Le bouton permet de visualiser le contenu brut du script, tel qu'il se trouve sur votre poste de travail.
3. Dans le menu **Pièces jointes liées au script**, ajoutez le cas échéant un ou plusieurs fichiers à joindre au script. Ces fichiers sont supprimés du serveur SMC après une exécution réussie du script. Pour plus d'informations, reportez-vous à la section Joindre des fichiers à un script et réceptionner des fichiers générés par script.
4. Dans la deuxième partie de l'onglet **Sélection des firewalls**, sélectionnez les firewalls sur lesquels exécuter le script. Pour chaque firewall :
   - L'icône indique le cas échéant que le firewall ne peut pas être sélectionné pour l'exécution du script. Dans ce cas, la ligne est grisée. Survolez l'icône avec la souris pour afficher la raison.
   - L'icône permet de visualiser le contenu du script incluant les variables remplacées par les valeurs associées au firewall en question. L'icône prend la forme en cas d'erreur dans l'analyse du script (fichier joint manquant, variable inconnue). Visualisez le contenu du script pour consulter la ligne qui pose problème.
5. Cliquez sur **Exécuter le script** en bas de l'onglet. L'onglet **Exécution** s'ouvre automatiquement.

6. Suivez la progression et le résultat de l'exécution des scripts sur chacun des firewalls sélectionnés.
   Lors du déroulement d'une exécution de script ou d'un déploiement de configuration, vous ne pouvez pas lancer une autre exécution de script mais il est possible de la préparer dans l'onglet **Sélection des firewalls**.

   > **IMPORTANT**
   > L'exécution d'un script prend automatiquement les droits de lecture/écriture sur les éventuelles sessions d'administration déjà établies sur les firewalls concernés.

7. Un résumé de l'exécution est visible en bas du panneau, affichant les réussites, erreurs et les firewalls sur lesquels le script n'a pas pu être déployé.
8. Vous pouvez également filtrer la liste des firewalls en sélectionnant un état dans la liste déroulante en haut de la liste.

   > **ASTUCE**
   > Si le script a été exécuté sur des firewalls déconnectés, l'exécution est reportée et sera effective la prochaine fois que les firewalls se connecteront.

9. En cas d'erreur, reportez-vous aux journaux du serveur SMC. Vous pouvez également vous connecter aux journaux et rapports d'activité d'un firewall en cliquant sur l'icône dans la colonne **Actions**.

10.4 Exécuter le script CLI SNS en ligne de commande

Depuis l'interface de ligne de commande, vous pouvez :

- ajouter un script dans le répertoire de scripts sur le serveur SMC et l'exécuter immédiatement,
- exécuter un script déjà stocké sur le serveur SMC,
- ajouter un script dans le répertoire de scripts sur le serveur SMC,
- supprimer un script du répertoire de scripts du serveur SMC,
- afficher la liste des scripts stockés sur le serveur SMC.

La commande principale `smc-sns-cli-script` doit être suivie d'une des cinq commandes correspondant à ces actions.

Le répertoire de stockage des scripts s'appelle *nsrpc-scripts* et est accessible dans */data/users/*.

10.4.1 Afficher la liste des commandes et des options

- Pour afficher la liste des commandes, tapez --help :

```
smc-sns-cli-script <command>

Commands:
  smc-sns-cli-script add <file-path>       Add a SNS CLI script to the SMC scrip
                                           ts repository
  smc-sns-cli-script delete <script-name>  Delete a SNS CLI script from the SMC
                                           scripts repository
  smc-sns-cli-script exec <file-path>      Add a specific SNS CLI script and run
                                            it immediately
  smc-sns-cli-script list                  List all the installed SNS CLI script
                                           s in the SMC scripts repository
  smc-sns-cli-script run <script-name>     Run a specific SNS CLI script

Options:
  -h, --help  Show help
```

- Chacune de ces commandes possède des options spécifiques. Pour les afficher, tapez la commande `smc-sns-cli-script <nom_action> -h`.

10.4.2 Exécuter un script

- Pour ajouter le script sur le serveur SMC et l'exécuter immédiatement, utilisez la commande :
  `smc-sns-cli-script exec <chemin_fichier>`
- Pour exécuter un script déjà stocké sur le serveur SMC, utilisez la commande :
  `smc-sns-cli-script run <nom_script>`

Parmi les options de ces commandes, choisissez obligatoirement entre :

- --firewall-list : à faire suivre d'une liste de noms de firewalls séparés par des virgules,
- --all : indique qu'on exécute le script sur tous les firewalls,
- --csv-file : à faire suivre d'un chemin vers un fichier CSV comprenant la liste des firewalls et les variables associées. La commande reprend alors les firewalls spécifiés dans ce fichier. Pour plus d'informations, reportez-vous à la section Utiliser un fichier CSV.

L'option --csv-file peut être utilisée conjointement avec les options --firewall-list et --all. Dans ce cas, ces deux dernières options précisent la liste des firewalls sur lesquels exécuter le script.

Les options facultatives sont les suivantes :

- --dry-run : permet d'afficher le contenu du script incluant les variables associées à chaque firewall, uniquement à des fins de consultation,
- --raw-output : permet d'afficher le déroulement de l'exécution du script en texte brut,
- --update : permet de forcer l'ajout du script sur le serveur si un script portant le même nom est déjà présent. Cette option n'est disponible que pour la commande `exec`.

Lorsqu'un déploiement de configuration est en cours ou qu'un autre script est en cours d'exécution, il est impossible d'exécuter un nouveau script en ligne de commande. Un message d'erreur s'affiche si le déploiement n'est pas totalement terminé sur tous les firewalls connectés ou si le script n'a pas fini de s'exécuter. Les firewalls pour lesquels le déploiement de configuration a été différé n'empêchent pas l'exécution de scripts.

Pour envoyer ou réceptionner des fichiers joints à un script, reportez-vous à la section Joindre des fichiers à un script et réceptionner des fichiers générés par script.

10.4.3 Ajouter des scripts

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour ajouter un script dans le répertoire de scripts du serveur SMC, utilisez la commande `smc-sns-cli-script add <chemin_fichier>`.

L'option --update : permet de forcer l'ajout du script sur le serveur si un script portant le même nom est déjà présent.

10.4.4 Supprimer des scripts

Pour supprimer un script du serveur SMC, utilisez la commande `smc-sns-cli-script delete <nom_script>`.

10.4.5 Afficher la liste des scripts

Pour afficher la liste des scripts présents dans le répertoire de scripts du serveur SMC, utilisez la commande `smc-sns-cli-script list`.

10.4.6 Exemple d'utilisation de script en ligne de commande avec un fichier CSV

Voici un exemple d'utilisation d'un fichier CSV avec un script. Pour tous les firewalls d'un parc (deux dans cet exemple), on souhaite créer un objet qui représente le serveur Active Directory principal et un objet qui représente le serveur AD secondaire, en tenant compte des assertions suivantes :

- Le serveur AD principal doit être un objet avec résolution d'adresse IP statique,
- Le serveur AD secondaire doit être un objet avec résolution d'adresse IP dynamique,
- Le nom de chaque objet doit indiquer s'il s'agit du serveur principal ou secondaire,
- Le commentaire de chaque objet doit indiquer le nom du firewall sur lequel il sera créé,
- L'adresse IP de chaque serveur AD est différente pour chaque firewall.

1. Créez le script */data/tmp/ad.script* :

```
# Create a new host

CONFIG OBJECT HOST NEW name=name=%type%AD.%FW_NAME%".com
comment="%type% AD server for FW %FW_NAME%" ip="%ip_addr%"
resolve=%mode%
CONFIG OBJECT ACTIVATE
```

2. Créez le fichier CSV */data/tmp/ad.csv* pour le parc de deux firewalls :

```
firewall;type;ip_addr;mode
paris;Main;1.1.1.1;static
paris;Backup;1.1.2.2;dynamic
lyon;Main;4.4.4.4;static
lyon;Backup;4.4.5.5;dynamic
```

3. Entrez la commande suivante dans l'interface de ligne de commande :

```
smc-sns-cli-script exec /data/tmp/ad.script --csv-file
/data/tmp/ad.csv
```

Voici le résultat attendu pour chacun des deux firewalls paris et lyon :

```
CONFIG OBJECT HOST NEW name=MainAD.paris.com comment="Main AD server for
FW paris" ip="1.1.1.1" resolve=static
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
CONFIG OBJECT HOST NEW name=BackupAD.paris.com comment="Backup AD server
for FW paris" ip="1.1.2.2" resolve=dynamic
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
```

```
CONFIG OBJECT HOST NEW name=MainAD.lyon.com comment="Main AD server for FW
lyon" ip="4.4.4.4" resolve=static
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
CONFIG OBJECT HOST NEW name=BackupAD.lyon.com comment="Backup AD server
for FW lyon" ip="4.4.5.5" resolve=dynamic
100 code=00e01700 msg="Object successfully added"
CONFIG OBJECT ACTIVATE
100 code=00a00100 msg="Ok"
```

Dans un fichier CSV, les champs sont séparés par un délimiteur, souvent la virgule ou le point virgule. Par défaut la commande `smc-sns-cli-script` attend le caractère point virgule (;) en tant que délimiteur. Suivant le fichier CSV, le délimiteur peut être différent. Pour changer le délimiteur attendu par la commande, vous devez modifier la valeur de la variable `SMC_SNS_CLI_CSV_DELIMITER` :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez la valeur de la variable d'environnement : `SMC_SNS_CLI_CSV_DELIMITER=,`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

10.5 Exécuter le script CLI SNS sur un cluster haute disponibilité

Les étapes sont identiques à celles des deux sections précédentes.

Le script est d'abord exécuté sur le nœud actif du cluster. Le serveur SMC effectue ensuite une synchronisation des deux nœuds du cluster.

Si le nœud passif n'est pas connecté au nœud actif au moment de l'exécution, le serveur SMC effectuera une synchronisation des deux nœuds du cluster lorsque le nœud passif se reconnectera au nœud actif.

10.6 Joindre des fichiers à un script et réceptionner des fichiers générés par script

L'exécution de certaines commandes de scripts nécessite l'envoi ou la réception de fichiers vers ou depuis les firewalls. Par exemple :

- La mise à jour des firewalls,
- L'installation de licence,
- La génération de sauvegarde de configuration de firewalls.

Il est possible d'envoyer et de réceptionner des fichiers depuis l'interface web du serveur SMC et depuis l'interface de ligne de commande.

10.6.1 Arguments de commande à utiliser dans le script

Pour une commande requérant un fichier en entrée, utilisez les arguments de commande suivants pour spécifier le nom du fichier à envoyer :

- `$FROM_DATA_FILE("nomDeMonFichier.extension")` pour joindre un fichier sans traitement Unicode,
- `$FROM_TEXT_FILE("nomDeMonFichier.extension")` pour joindre un fichier avec traitement Unicode.

Pour une commande générant un fichier en sortie, utilisez les arguments de commande suivants pour spécifier le nom du fichier à réceptionner :

- `$SAVE_TO_DATA_FILE("nomDuFichier.extension")` pour sauvegarder un fichier sans traitement Unicode,
- `$SAVE_TO_TEXT_FILE("nomDuFichier.extension")` pour sauvegarder un fichier avec traitement Unicode.

Pour connaître les emplacements de ces fichiers, reportez-vous aux sections ci-dessous Joindre un fichier à un script CLI SNS et Réceptionner un fichier généré par script CLI SNS.

Le script ne s'exécutera pas si :

- Aucun fichier n'est spécifié en argument d'une commande qui nécessite un fichier en entrée ou génère un fichier en sortie,
- Un fichier est spécifié en entrée ou en sortie en argument d'une commande qui n'en requiert pas.

Exemple

La commande suivante permet de générer sur le serveur SMC le fichier de sauvegarde d'un firewall nommé *backup-22-09-16.na* :

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-22-09-2016.na")
```

ASTUCE
Vous pouvez utiliser des variables dans la syntaxe d'envoi ou de réception de fichiers. Par exemple, pour créer des sauvegardes de configuration de plusieurs firewalls, écrivez la commande suivante :

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-%FW_NAME%.na")
```

10.6.2 Joindre un fichier à un script

Dans les deux cas suivants, les fichiers joints sont supprimés du serveur SMC après une exécution réussie du script.

Via l'interface web

1. Dans l'interface web du serveur SMC, sélectionnez **Déploiement** > **Scripts CLI SNS**.
2. Dans l'onglet **Sélection des firewalls**, après avoir sélectionné un script, sélectionnez une ou plusieurs pièces jointes dans le sous-menu **Pièces jointes liées au script**.

Via l'interface de ligne de commande

Copiez les pièces jointes à la racine du dossier */data/tmp/sns-cli/input* du serveur SMC à l'aide du protocole SSH.

Le moteur d'exécution du script récupère les fichiers nécessaires à cet emplacement afin de les transmettre aux firewalls.

> **ASTUCE**
> Vous pouvez changer de dossier par défaut dans la variable d'environnement `SMC_SNS_CLI_ATTACHMENTS_DIR` située dans le fichier **/data/config/fwadmin-env.conf.local**. Vous devrez ensuite redémarrer le serveur : `nrestart smc`.

10.6.3 Réceptionner un fichier généré par script

Via l'interface web

Dans l'onglet **Exécution** du menu **Scripts CLI SNS**, récupérez l'ensemble des fichiers et des journaux générés pour chaque firewall par la dernière exécution de script réalisée.

Pour récupérer les fichiers et journaux générés par des exécutions antérieures, reportez-vous à la section suivante Via l'interface de ligne de commande.

Réceptionner les fichiers et journaux

Cliquez sur le bouton **Télécharger tous les fichiers générés** en bas de l'onglet **Exécution** pour télécharger une archive comprenant l'ensemble des fichiers générés et des journaux d'exécution pour tous les firewalls à la fois. L'archive contient un dossier par firewall.

Pour récupérer les fichiers et journaux générés par l'exécution d'un script sur un seul firewall, cliquez sur l'icône dans la colonne **Fichiers générés**.

Consulter les journaux d'exécution

Pour simplement consulter les journaux d'exécution pour un firewall donné, cliquez sur l'icône dans la colonne **Fichiers générés**.

Via l'interface de ligne de commande

L'ensemble des fichiers et des journaux générés pour chaque firewall après l'exécution d'un script est placé par défaut dans le dossier */data/tmp/sns-cli/output* du serveur SMC. L'arborescence créée comprend un dossier pour chaque exécution de script.

> **ASTUCE**
> Vous pouvez changer de dossier par défaut dans la variable d'environnement `SMC_SNS_CLI_OUTPUT_DIR` située dans le fichier */data/config/fwadmin-env.conf.local*. Vous devrez ensuite redémarrer le serveur : `nrestart smc`.

Exemple

Lorsqu'on exécute la commande

```
CONFIG BACKUP list=all $SAVE_TO_DATA_FILE("backup-%FW_NAME%.na")
```

on obtient l'arborescence suivante :

```
/data/tmp/sns-cli/output/latest -> 00001_20160219-171926
/data/tmp/sns-cli/output/00001_20160219-171926
/data/tmp/sns-cli/output/00001_20160219-171926/sns-2
/data/tmp/sns-cli/output/00001_20160219-171926/sns-1/backup-sns-2.na
/data/tmp/sns-cli/output/00001_20160219-171926/sns-2/output.log
/data/tmp/sns-cli/output/00001_20160219-171926/sns-1
/data/tmp/sns-cli/output/00001_20160219-171926/sns-1/backup-sns-1.na
/data/tmp/sns-cli/output/00001_20160219-171926/sns-1/output.log
```

Le dossier *latest* pointe toujours vers la dernière exécution.

10.7 Programmer l'exécution d'un script CLI SNS

Une exécution de script peut être programmée à une date et heure données depuis l'interface web ou en ligne de commande. Vous pouvez par exemple programmer une mise à jour de vos firewalls SNS. Consultez la section Mettre à jour les firewalls en utilisant les scripts CLI SNS .

10.7.1 Programmer l'exécution d'un script depuis l'interface web

1. Dans l'interface web du serveur SMC, sélectionnez **Déploiement** > **Scripts CLI SNS**.
2. Dans l'onglet **Sélection des firewalls**, sélectionnez le script à exécuter.
3. Dans le menu **Optionnel : pièces jointes liées au script**, sélectionnez le cas échéant un ou plusieurs fichiers à joindre au script. Pour plus d'informations, reportez-vous à la section Joindre des fichiers à un script et réceptionner des fichiers générés par script.
4. Dans la deuxième partie de l'onglet **Sélection des firewalls**, sélectionnez les firewalls sur lesquels exécuter le script. Pour chaque firewall, dans la colonne **Visualiser le script** :
   - L'icône indique le cas échéant que le firewall ne peut pas être sélectionné pour l'exécution du script. Dans ce cas, la ligne est grisée. Survolez l'icône avec la souris pour afficher la raison.
   - L'icône permet de visualiser le contenu du script incluant les variables remplacées par les valeurs associées au firewall en question. L'icône prend la forme en cas d'erreur dans l'analyse du script (fichier joint manquant, variable inconnue). Visualisez le contenu du script pour consulter la ligne qui pose problème.
5. Cliquez sur **Programmer le script** en bas de l'onglet.
6. Indiquez la date et l'heure d'exécution du script. L'heure choisie ici correspond à l'heure du serveur SMC.
7. Cliquez sur **Appliquer**.
   - Une indication en haut de l'onglet rappelle la programmation du script. Les seules actions possibles sont visualiser le script, télécharger le script ou annuler la programmation.
8. Consultez le résultat de l'exécution du script dans l'onglet **Exécution** lorsque celle-ci est terminée.

Une seule exécution à la fois peut être programmée.

Lorsqu'un script est programmé et en attente d'être exécuté, vous ne pouvez pas exécuter un autre script.

IMPORTANT
L'exécution d'un script prend automatiquement les droits de lecture/écriture sur les éventuelles sessions d'administration déjà établies sur les firewalls concernés.

10.7.2 Programmer l'exécution d'un script en ligne de commande

La commande shell `at` permet de programmer l'exécution de tâches. Elle permet donc entre autres de programmer l'exécution de la commande `smc-sns-cli-script`.

Plusieurs tâches peuvent être programmées, elles s'exécutent alors de façon séquentielle.

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande `at` suivie de l'heure et la date souhaitées en respectant le format : `at hh:mm MM/DD/YYYY`
3. Tapez la commande `smc-sns-cli-script` suivie dans l'ordre :
   - d'une des sous-commandes décrites à la section Exécuter le script CLI SNS en ligne de commande,
   - du nom du script,
   - du nom des firewalls concernés ou de l'option --all pour désigner tous les firewalls,
   - ```
     [root@smc] - {~} > at 16:00 10/15/2019
     warning: commands will be executed using /bin/sh
     at> smc-sns-cli-script run monitor_qos.script --all
     at> smc-sns-cli-script run monitor_stat.script --all
     ```
4. Tapez Ctrl + D pour valider.
   ```
   at> < EOT >
   job 15 at Tue Oct 15 16:00:00 2019
   ```
5. Après l'heure et la date d'exécution, vous pouvez vérifier le résultat dans le répertoire */data/tmp/sns-cli/output/*. Ce répertoire contient un ensemble de sous-répertoires dont le nom correspond à la date d'exécution des scripts. Pour consulter le résultat d'exécution d'un script sur un firewall donné, consultez le fichier *output.log* dans l'un de ces sous-répertoires.

Si vous devez joindre des fichiers au script, reportez-vous à la section Joindre des fichiers à un script et réceptionner des fichiers générés par script.

Pour vois la liste des tâches programmées, utilisez la commande `atq`.

Pour supprimer une tâche programmée, utilisez la commande `atrm`.

10.8 Mettre à jour les firewalls en utilisant les scripts CLI SNS

ATTENTION
Si vous ne souhaitez pas utiliser de scripts CLI SNS pour mettre à jour votre parc de firewalls, reportez-vous à la section Mettre à jour les firewalls pour utiliser la fonctionnalité prévue à cet effet.
   ```

Pour mettre à jour des firewalls en utilisant des scripts CLI SNS, vous devez télécharger au préalable les fichiers de mise à jour adéquats depuis votre espace personnel MyStormshield (*.maj*).

Si vous possédez des firewalls seuls et des clusters haute disponibilité, nous vous recommandons de créer un script pour chaque cas (firewalls seuls, nœuds actifs, nœuds passifs, les deux nœuds en même temps).

Nous vous recommandons de sauvegarder la configuration des firewalls avant de les mettre à jour.

Suivez les étapes suivantes :

1. Créez le script de mise à jour avec les commandes décrites dans les exemples suivants, en remplaçant 3.7.1 par la version souhaitée (pour plus d'informations sur la variable %FW_UPD_SUFFIX%, reportez-vous à la section Utiliser des variables) :
    - Pour des firewalls seuls :
      ```
      SYSTEM UPDATE UPLOAD $FROM_DATA_FILE("fwupd-3.7.1-%FW_UPD_
      SUFFIX%")
      SYSTEM UPDATE ACTIVATE
      ```
    - Pour des clusters :
        - Nœuds passifs :
          ```
          SYSTEM UPDATE UPLOAD fwserial=passive $FROM_DATA_FILE
          ("fwupd-3.7.1-%FW_UPD_SUFFIX%")
          SYSTEM UPDATE ACTIVATE fwserial=passive
          ```
        - Nœuds actifs :
          ```
          SYSTEM UPDATE ACTIVATE fwserial=active
          ```
2. Dans l'interface web du serveur SMC, sélectionnez **Déploiement** > **Scripts CLI SNS**.
3. Dans l'onglet **Sélection des firewalls**, sélectionnez le script à exécuter.
4. Dans le menu **Optionnel : pièces jointes liées au script**, sélectionnez le fichier ou les fichiers de mise à jour correspondants à vos modèles et versions de firewalls. Par exemple pour mettre à jour des firewalls SN510 et SN6000 en version 3.7.1, les pièces jointes à fournir sont *fwupd-3.7.1-SNS-amd64-M.maj* et *fwupd-3.7.1-SNS-amd64-XL.maj*.
5. Suivez ensuite les étapes habituelles d'exécution d'un script comme indiqué dans la section Exécuter le script CLI SNS depuis l'interface web, à partir de l'étape 4.

> **NOTE**
> Après l'exécution d'un script de mise à jour sur un cluster, la synchronisation automatique entre les deux nœuds opérée par le serveur SMC échoue dans tous les cas car l'un des nœuds est rendu indisponible par la mise à jour. Cette erreur, visible dans l'onglet **Exécution**, n'empêche pas le bon déroulement de la mise à jour.

6. Après quelques minutes, vérifiez dans le panneau **Supervision** > **Firewalls** que le numéro de version a bien changé dans la colonne **Version**.

10.9 Résoudre les problèmes

Consultez cette section pour résoudre les éventuels problèmes rencontrés lors de l'utilisation de scripts CLI SNS.

10.9.1 Le fichier de script est trop volumineux

- *Situation* : Lors de la sélection du fichier de script, un message d'erreur indique que le script est trop volumineux.
- *Cause* : La taille du fichier ne doit pas dépasser 5 Mo par défaut.
- *Solution* : Si besoin, augmentez la limite en ajoutant la ligne ci-dessous dans le fichier `/data/config/fwadmin-env.conf.local`. Par exemple, fixez la limite à 10 Mo : `SMC_SNS_CLI_SCRIPT_MAX_UPLOAD_SIZE_INT=$((10*1024*1024))`

10.9.2 Certains caractères ne sont pas pris en compte dans le script

- *Situation* : Certains caractères accentués ou spéciaux ne s'affichent pas correctement dans le script. L'exécution du script échoue.
- *Cause* : Le fichier *.script* n'est pas encodé en UTF-8.
- *Solution* : Modifiez l'encodage du script en UTF-8.

10.9.3 L'exécution du script échoue sur certains firewalls

- *Situation* : L'onglet **Exécution** du menu **Scripts CLI SNS** indique des erreurs.
- *Cause* : Le script fait appel à des variables personnalisées et/ou à des pièces jointes et celles-ci sont manquantes. L'encodage du script n'est pas correct. D'autres problèmes peuvent être à l'origine de l'échec de l'exécution.
- *Solutions* :
  - Consultez la cause de l'erreur qui s'affiche dans la barre de progression de l'exécution du script pour un firewall donné.
  - Consultez les journaux du serveur dans */data/log/fwadmin-server/server.log* pour plus de détails.
  - Avant d'exécuter le script, dans l'onglet **Sélection des firewalls**, vous pouvez visualiser celui-ci pour un firewall donné. Certaines erreurs peuvent être précisées.

10.9.4 Il n'est pas possible d'exécuter un script

- *Situation* : Des firewalls sont sélectionnés pour l'exécution d'un script et le bouton d'exécution reste grisé ou bien certains firewalls ne peuvent pas être sélectionnés.
- *Cause* : Une exécution de script ou un déploiement de configuration est en cours ou en état différé sur un firewall. Il n'est donc pas possible d'exécuter un script sur ce firewall.
- *Solution* : Attendez la fin de l'exécution de script. Ou bien attendez la fin du déploiement ou la reconnexion du firewall pour que le déploiement se termine.

11. Maintenir les firewalls SNS

Le serveur SMC permet de sauvegarder la configuration des firewalls SNS et de mettre à jour votre parc.

11.1 Sauvegarder la configuration des firewalls

SMC offre la possibilité de mettre en place des sauvegardes automatiques de la configuration des firewalls ainsi que de la configuration du serveur SMC. Vous pouvez également à tout moment réaliser manuellement une sauvegarde intégrale de votre parc de firewalls.

11.1.1 Sauvegarder automatiquement la configuration du serveur et des firewalls

SMC peut sauvegarder automatiquement de manière récurrente la configuration des firewalls et du serveur lui-même afin de pouvoir restaurer la totalité du parc en cas de besoin.

Par défaut, la sauvegarde automatique est désactivée.

Seul le super administrateur (utilisateur "admin") est autorisé à activer ou désactiver la sauvegarde automatique, et à télécharger les sauvegardes de configuration du serveur SMC. Tous les administrateurs peuvent télécharger les sauvegardes de configuration des firewalls SNS.

ATTENTION
Dans le cas des firewalls équipés d'un module TPM (Trusted Platform Module) initialisé, les clés privées sont exclues de la sauvegarde automatique par défaut.

Activer la sauvegarde automatique

- Cochez **Activer la sauvegarde automatique**.

Afficher la liste des sauvegardes

- Rendez-vous dans le menu de gauche **Maintenance** > **Sauvegarde**.

La liste affiche toutes les sauvegardes conservées. Elles sont conservées pendant sept jours. Au-delà de sept jours, seule une sauvegarde par jour est conservée. Au-delà de un mois, seule une sauvegarde par semaine est conservée. Au-delà de 12 mois, les sauvegardes sont supprimées.

Une icône dans la colonne **État** indique que les configurations de tous les firewalls ont bien été sauvegardées ou au contraire que certains firewalls posent problème. Survolez les icônes avec la souris pour afficher une info-bulle.

Récupérer une sauvegarde

- Cliquez sur dans la colonne **Actions**.
  L'archive contient un fichier de métadonnées, la sauvegarde de la configuration du serveur SMC et les sauvegardes de configuration de chaque firewall au format *.na*.

Restaurer une sauvegarde

Pour savoir comment restaurer une sauvegarde de configuration du serveur SMC, reportez-vous à la section Sauvegarder et restaurer la configuration du serveur SMC.

Pour savoir comment restaurer une sauvegarde de configuration d'un firewall, consultez le *Manuel Utilisateur SNS*.

Afficher plus de détails sur une sauvegarde

- Double-cliquez sur une ligne ou cliquez sur dans la colonne **Actions**.

11.1.2 Sauvegarder manuellement la configuration des firewalls

Vous pouvez également sauvegarder de manière ponctuelle la configuration de tout ou partie de votre parc de firewalls.

1. Rendez-vous dans le menu de gauche **Maintenance** > **Sauvegarde**.
2. Dans l'onglet **Manuelle**, entrez un mot de passe si vous souhaitez chiffrer les sauvegardes. Les caractères #, % et " sont interdits et le mot de passe ne peut dépasser 255 caractères. Il doit également respecter la politique de mot de passe des firewalls concernés.
3. Cliquez sur **Utiliser le script de sauvegarde des firewalls**.
4. Le panneau des scripts CLI SNS s'affiche. Le script de sauvegarde manuelle de la configuration des firewalls est préchargé.
5. Sélectionnez les firewalls dont vous voulez sauvegarder la configuration puis exécutez le script.

Pour plus d'informations sur les scripts, reportez-vous à la section Exécuter le script CLI SNS depuis l'interface web.

Cette sauvegarde manuelle n'inclut pas la configuration du serveur SMC. Pour sauvegarder la configuration du serveur, reportez-vous à la section Sauvegarder et restaurer la configuration du serveur SMC ou activez les sauvegardes automatiques.

ATTENTION
Dans le cas des firewalls équipés d'un module TPM (Trusted Platform Module) initialisé, les clés privées sont exclues de la sauvegarde automatique par défaut.

11.1.3 Exclure les clés privées de la sauvegarde automatique des firewalls

La sauvegarde automatique de la configuration des firewalls contient par défaut l'identité complète d'un firewall, c'est-à-dire ses certificats ainsi que ses clés privées.

Si vous souhaitez exclure de la sauvegarde automatique les clés privées, pour des raisons de confidentialité par exemple, vous pouvez modifier la variable d'environnement `SMC_AUTOBACKUP_EXCLUDE_PRIVATE_KEY_ENABLED:`

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez la valeur de la variable d'environnement : `SMC_AUTOBACKUP_EXCLUDE_PRIVATE_KEY_ENABLED=true`
3. Redémarrez le serveur avec la commande `nrestart smc`

Dans le cas des firewalls équipés d'un module TPM (Trusted Platform Module) initialisé, les clés sont exclues de la sauvegarde automatique par défaut. Vous n'avez pas besoin de modifier la variable d'environnement.

Pour plus d'informations sur la protection des certificats par TPM, reportez-vous à la section Désactiver la protection des certificats par TPM (Trusted Platform Module) lors de l'installation sur le firewall.

11.2 Mettre à jour les firewalls

SMC permet de mettre à jour votre parc de firewalls.

ATTENTION
Nous vous recommandons de mettre à jour un maximum de 10 firewalls simultanément.

Vous devez posséder le droit d'accès en écriture sur les firewalls pour les mettre à jour. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour les firewalls dont le module TPM est initialisé, la mise à jour est possible depuis SMC à partir de la version 4.8.9 de SNS.

1. Téléchargez au préalable les fichiers de mise à jour adéquats depuis votre espace personnel MyStormshield (*.maj*).
2. Dans l'interface web du serveur SMC, sélectionnez **Déploiement** > **Mise à jour des firewalls**.
3. Dans la première partie de l'onglet **Sélection des firewalls**, importez un ou plusieurs fichiers de mise à jour au format *.maj* en cliquant sur :
   - Les fichiers importés sont stockés sur le serveur SMC. Par défaut, ils sont conservés 14 jours. La variable d'environnement SMC_SNS_UPDATE_MAX_KEEP_DAYS_INT permet de modifier la durée de stockage des fichiers de mise à jour.

     ATTENTION
     Assurez-vous de disposer d'assez d'espace pour stocker les fichiers. La saturation de l'espace pourrait entraîner des dysfonctionnements.

   - Le bouton permet d'indiquer l'URL d'un serveur HTTPS depuis lequel SMC peut importer un fichier de mise à jour.
   - Le bouton permet de visualiser l'en-tête du fichier de mise à jour et de vous assurer que le fichier est compatible avec la version des firewalls à mettre à jour.
   - La case **Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le firewall** permet de sauvegarder la partition active du système sur la partition de secours, afin d'en conserver une trace. En fonction de la taille de la partition, de la configuration et du modèle du firewall, l'opération peut prendre du temps. La variable d'environnement SMC_SNS_UPDATE_SYSTEM_CLONE_TIMEOUT_INT permet de configurer le temps maximum autorisé pour la sauvegarde.
     Dans le cas des firewalls EVA qui ne disposent pas de partition de sauvegarde, l'activation de cette case n'empêche pas la mise à jour du firewall mais elle s'exécute sans sauvegarder la partition active. Nous vous recommandons de sauvegarder un instantané de la machine avant la mise à jour.
4. Sélectionnez le fichier de mise à jour à appliquer.

5. Dans la deuxième partie de l'onglet **Sélection des firewalls**, sélectionnez les firewalls à mettre à jour.
   - L'icône indique le cas échéant que le firewall ne peut pas être sélectionné pour l'exécution de la mise à jour. Dans ce cas, la ligne est grisée. Survolez l'icône avec la souris pour afficher la raison.
   - Il est possible de sélectionner des firewalls déconnectés. La mise à jour est différée et sera exécutée lors de leur reconnexion. À la reconnexion d'un firewall, si des exécutions de script CLI SNS ou des déploiements de configuration sont déjà en attente, la mise à jour sera exécutée en priorité et sera suivie de l'exécution de script ou du déploiement de configuration.
   - Dans le cas d'un cluster haute disponibilité, le firewall passif est mis à jour en premier. À son redémarrage, il prend la place du firewall actif pendant la mise à jour de l'autre firewall. Ainsi, le service n'est pas interrompu.
6. Cliquez sur **Mettre à jour les firewalls** en bas de l'onglet. L'onglet **Exécution** s'ouvre automatiquement.
7. Suivez la progression et le résultat de la mise à jour sur chacun des firewalls sélectionnés. Lorsqu'une mise à jour est en cours sur un firewall, vous ne pouvez pas exécuter un script CLI SNS ou déployer une configuration sur ce firewall, et inversement. Vous pouvez exécuter des mises à jour sur d'autres firewalls.

   IMPORTANT
   L'exécution d'une mise à jour prend automatiquement les droits de lecture/écriture sur les éventuelles sessions d'administration déjà établies sur les firewalls concernés.
8. Si besoin, filtrez la liste des firewalls en sélectionnant un état dans la liste déroulante en haut de la liste.
9. En cas d'erreur, reportez-vous aux journaux du serveur SMC. Vous pouvez également vous connecter aux journaux et rapports d'activité d'un firewall en cliquant sur l'icône dans la colonne **Actions**.
10. Après quelques minutes, vérifiez dans le panneau **Supervision** > **Firewalls** que le numéro de version a bien changé dans la colonne **Version**.

La mise à jour des firewalls depuis SMC est également possible via l'utilisation de scripts CLI SNS. Pour réaliser cette opération, reportez-vous à la section Mettre à jour les firewalls en utilisant les scripts CLI SNS .

11.3 Remplacer un firewall SNS dans le cadre d'un RMA

Si vous devez remplacer un firewall géré par SMC, suivez la procédure habituelle de remplacement d'un boîtier dans le cadre d'un RMA (Return Material Authorization).

Une fois le nouveau boîtier prêt :

1. Sur SMC, dans l'onglet **Système** > **Configuration** des propriétés du firewall, cochez la case **Autoriser le rattachement d'un autre firewall avec le même package dans le cadre d'un remplacement de matériel défectueux (RMA)** pour autoriser le nouveau boîtier présentant un numéro de série différent à se connecter à SMC à la place de l'ancien boîtier.
2. Restaurez la configuration du firewall sur le nouveau boîtier grâce à un fichier de sauvegarde *.na*.
   Le firewall se reconnecte automatiquement à SMC.

Aucune action supplémentaire n'est nécessaire, vous n'avez pas besoin de générer un nouveau package de rattachement.

12. Supprimer des firewalls SNS du serveur SMC

Pour réaliser cette opération, vous devez posséder le droit d'accès en écriture sur les dossiers dans lesquels sont classés les firewalls à supprimer. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

Pour ne plus administrer un firewall à partir du serveur SMC et le supprimer de la liste de firewalls dans l'interface web :

- Survolez le nom du firewall dans le menu **Supervision** > **Firewalls** et cliquez sur la croix rouge.

La suppression du firewall de SMC entraîne automatiquement la suppression de la configuration du rattachement à SMC sur le firewall, à condition qu'il soit connecté à SMC au moment de la suppression. Les fichiers **.tpm* et **.pem* sont supprimés du répertoire /usr/Firewalls/ConfigFiles/Cad sur le firewall. Le firewall ne pourra ainsi plus se connecter au serveur SMC.

Supprimer manuellement la configuration du rattachement à SMC sur le firewall

En cas de besoin, la procédure ci-dessous permet de supprimer manuellement la configuration du rattachement à SMC sur le firewall :

1. Connectez-vous au firewall en SSH ou via la console de votre hyperviseur,
2. Entrez les lignes de commande suivantes :

```
nstop cad
setconf /usr/Firewall/ConfigFiles/Cad/cad Server State 0
rm /usr/Firewall/ConfigFiles/Cad/*.pem
rm /usr/Firewall/ConfigFiles/Cad/*.tpm
rm /usr/Firewall/ConfigFiles/nsconf_int
encad
```

Dans le cas d'un cluster en Haute Disponibilité, entrez ces commandes sur le nœud actif du cluster et synchronisez les deux nœuds.

13. Gérer et maintenir le serveur SMC

Les opérations de gestion et de maintenance s'effectuent soit à partir de l'interface web soit à partir de l'interface de ligne de commande, ou les deux pour certaines.

13.1 Définir les interfaces réseau du serveur SMC

Depuis votre hyperviseur, vous pouvez définir plusieurs interfaces sur des réseaux différents pour le serveur SMC. Les adresses IPv6 ne sont pas supportées.

Ces interfaces sont visibles dans le panneau **Maintenance** > **Serveur SMC** > **Paramètres** de l'interface web d'administration du serveur et sont modifiables.

Par défaut les autres interfaces que eth0 sont désactivées. Vous devez les activer dans la colonne **Plan d'adressage** de ce panneau, et les configurer.

L'interface eth0 ne peut être désactivée.

Vous ne pouvez définir qu'une seule passerelle pour l'ensemble des interfaces. C'est la passerelle par défaut . Celle-ci doit se trouver dans le même sous-réseau que l'interface correspondante.

Le fichier */etc/network/interfaces* accessible en ligne de commande contient les informations liées aux interfaces du serveur SMC.

Pour les topologies réseau pour lesquelles vous devez configurer des routes statiques en plus de la passerelle par défaut, suivez la procédure indiquée sur la Base de connaissances Stormshield.

13.2 Vérifier la version du serveur SMC en ligne de commande

Pour vérifier la version du serveur SMC :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande `smc-version`.
3. L'information suivante s'affiche :
   - SMC_DISTRIB_VERSION : indique la version sous la forme 1.2.3,
   - SMC_DISTRIB_BUILD_NUMBER : indique la date du build du serveur ainsi que les empreintes Stormshield qui pourront être fournies au support Stormshield Network Security en cas d'incident.

13.3 Modifier le fuseau horaire et la date du serveur SMC

Le fuseau horaire du serveur SMC est en GMT+1 (heure de l'Europe Centrale) par défaut.

13.3.1 Modifier le fuseau horaire

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande `smc-date-time --timezone "timezone"` pour modifier le fuseau. Remplacez `timezone` par le bon fuseau horaire.
   - Pour visualiser les fuseaux horaires disponibles, tapez la commande `ls -l /usr/share/zoneinfo/`,
   - Pour trouver la ville dans la zone de votre choix (zone Asia par exemple), tapez la commande `ls /usr/share/zoneinfo/Asia`.
3. Redémarrez le serveur avec la commande `reboot`. Cette étape est nécessaire pour que tous les services prennent en compte le nouveau fuseau horaire.
4. Tapez la commande `smc-date-time` pour vérifier que la modification a bien été prise en compte.

13.3.2 Modifier la date manuellement

1. Tapez la commande `smc-date-time --date-time "YYYY-MM-DD hh:mm:ss"` pour modifier la date.
2. Tapez la commande `smc-date-time` pour vérifier que la modification a bien été prise en compte.

13.3.3 Modifier la date via le protocole NTP

Pour activer le protocole NTP sur le serveur SMC :

1. Tapez la commande `smc-date-time --ntp-servers ntp1.org,ntp2.com,adresseIP` en séparant les serveurs NTP par une virgule s'il y en a plusieurs. Les serveurs NTP peuvent être désignés par leur adresse IP ou leur nom DNS.
2. Tapez la commande `date` pour vérifier que la modification a bien été prise en compte.

Pour désactiver le protocole NTP, vous devez repasser en mode de date manuelle.

La fréquence d'interrogation d'un serveur NTP est la fréquence par défaut du démon NTP.

13.3.4 Afficher un résumé complet des paramètres date/heure du serveur SMC

- Tapez la commande `smc-date-time` pour afficher tous les paramètres date/heure du serveur :

```
smc-date-time
TIMEZONE=Asia/Dubai
NTPSERVERS=none
LOCALDATE=2016-05-18 09:05:19
```

13.4 Gérer les administrateurs locaux et provenant d'annuaires externes

Pour gérer l'authentification des administrateurs sur le serveur SMC, il existe trois possibilités :

- Créer des comptes localement sur le serveur SMC,
- Paramétrer une connexion à un serveur LDAP depuis le serveur SMC,
- Paramétrer une connexion à un serveur RADIUS depuis le serveur SMC.

Le menu **Maintenance** > **Serveur SMC** > **Administrateurs** de l'interface web d'administration permet de gérer les administrateurs disposant de comptes locaux sur le serveur SMC ou de comptes provenant de serveurs d'authentification Radius ou LDAP.

Il existe quatre profils d'administrateur : super administrateur (utilisateur "admin"), administrateur général, administrateur de dossiers, administrateur en lecture seule.

L'affichage du panneau diffère selon que vous êtes connecté au serveur en tant que super administrateur (utilisateur "admin") ou en tant qu'autre administrateur.

Les trois profils d'administrateurs en écriture possèdent les droits suivants :

	Super administrateur	Administrateur général	Administrateur de dossiers
Administrateurs	Ajout/Suppression/Modification	Modification de son propre mot de passe	Modification de son propre mot de passe
Configuration des firewalls SNS	• Ajout/Suppression/Modification • Déploiement • Sauvegarde automatique et manuelle	• Ajout/Suppression/Modification • Déploiement • Sauvegarde manuelle	Uniquement dans les dossiers sur lesquels il a le droit d'accès en écriture : • Ajout/Suppression/Modification • Déploiement • Sauvegarde manuelle
Maintenance de SMC	• Installation et mise à jour de la licence • Mise à jour du serveur • Sauvegarde et restauration de la configuration du serveur • Définition des interfaces réseau du serveur • Génération d'un rapport de diagnostic • Activation du mode DR • Gestion de l'accès au serveur SLS	• Génération d'un rapport de diagnostic • Activation du contrôle de cohérence pour le mode DR • Gestion de l'accès au serveur SLS	Génération d'un rapport de diagnostic
Gestion des clés API	• Activation de l'API publique • Révocation des clés API	Création/révocation des clés API si droits activés	Création/révocation de clés API en lecture seule si droits activés

Pour plus d'informations sur l'administrateur de dossiers, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

L'administrateur en lecture seule peut accéder à tous les panneaux de l'interface web d'administration mais ne peut rien modifier, à part son propre mot de passe.

Lorsque le super administrateur tente de se connecter, le serveur SMC recherche l'identifiant et le mot de passe dans sa base locale d'utilisateurs.

Lorsqu'un administrateur général ou de dossiers tente de se connecter, le serveur SMC recherche d'abord l'identifiant et le mot de passe sur le serveur Radius s'il est configuré, puis sur le serveur LDAP s'il est configuré et que l'option de bascule automatique vers le serveur LDAP est activée, puis dans sa base locale si elle est configurée.

Plusieurs administrateurs peuvent se connecter simultanément à l'interface web avec les accès en lecture/écriture et à l'interface de ligne de commande. Dans ce cas, les changements

effectués par un administrateur sont instantanément répercutés sur les écrans des autres administrateurs, y compris les imports d'éléments par fichier CSV. Consultez les journaux d'audit pour voir la liste des changements effectués.

Lorsqu'un administrateur déploie une configuration sur les firewalls, les autres administrateurs voient qu'un déploiement est en cours et qui l'a lancé.

NOTE
L'utilisateur "root" ne figure pas dans la liste des administrateurs mais il possède bien les droits d'accès au serveur en SSH ou via la console d'un hyperviseur. En revanche, le super administrateur ne peut pas accéder au serveur en SSH ou via une console.

Pour gérer les administrateurs en tant que super administrateur, allez dans le menu **Administrateurs** :

- Pour ajouter un administrateur, cliquez sur **Ajouter un administrateur**.
- Pour modifier le profil d'un administrateur, double-cliquez sur la ligne de l'administrateur ou survolez le nom de l'administrateur et sélectionnez l'icône crayon . Il n'est pas possible de retirer le droit **Lecture/Écriture SMC** d'un administrateur si celui-ci possède des clés API actives et avec le droit **Lecture/Écriture**. Pour plus d'informations, reportez-vous à la section Activer et gérer l'API publique de SMC.
- Pour supprimer un administrateur, survolez le nom de l'administrateur et sélectionnez la croix rouge . Il n'est pas possible de supprimer un administrateur s'il possède des clés API actives. Pour plus d'informations, reportez-vous à la section Activer et gérer l'API publique de SMC.

L'utilisateur "admin" ne peut pas être supprimé.

NOTE
Seul le super administrateur a le droit de mettre à jour le serveur SMC, de sauvegarder et restaurer la configuration de SMC et d'activer ou désactiver la sauvegarde automatique depuis l'interface web d'administration.

13.4.1 Gérer les droits des administrateurs en tant que super administrateur

Le super administrateur a tous les droits et décide d'octroyer l'accès aux autres administrateurs :

- à l'interface web de SMC en lecture/écriture ou limité en lecture,
- à l'interface web des firewalls en lecture/écriture ou limité en lecture,
- à l'interface de ligne de commande en SSH,
- à l'interface de ligne de commande via la console d'un hyperviseur.

Le super administrateur peut également restreindre le droit d'accès en écriture d'un administrateur à certains dossiers seulement et par conséquent à certains firewalls. Pour en savoir plus, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers. Cette restriction ne s'applique pas aux accès en SSH et en console.

Les administrateurs ayant le droit d'accéder à l'interface de ligne de commande en SSH ou via la console d'un hyperviseur doivent demander une élévation de privilèges avec la commande "sudo" pour exécuter certaines commandes concernant le système (réseau, comptes utilisateurs, fichiers système, etc.) :

```
[admin-a@smc] - {~} > tcpdump
tcpdump: eth0: You don't have permission to capture on that device
(socket: Operation not permitted)
[admin-a@smc] - {~} > sudo tcpdump
Password:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

C'est également le super administrateur qui attribue aux autres administrateurs le droit de créer et révoquer des clés API permettant d'utiliser les routes de l'API publique de SMC.

Pour que cette action soit disponible, l'API publique doit être activée depuis l'interface web de SMC. Pour plus d'informations sur l'API publique de SMC, reportez-vous à la section Activer et gérer l'API publique de SMC .

13.4.2 Gérer les administrateurs locaux

Les comptes des administrateurs locaux sont créés localement sur le serveur SMC.

Ajouter un administrateur local

Pour ajouter un administrateur local :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Ajouter un administrateur**.
2. Remplissez les champs obligatoires suivants :

Champ	Description
Identifiant	Identifiant de l'administrateur local.
Nom	Nom de l'administrateur local qui est affiché sur SMC.

3. Sélectionnez les droits d'accès. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur et à la section Restreindre les droits d'accès des administrateurs de dossiers.
4. Définissez un mot de passe pour l'administrateur en respectant la politique de mots de passe décrite à la section suivante.

Les termes suivants sont réservés par SMC et donc inutilisables en tant qu'identifiant : root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

Définir une politique de mots de passe pour les comptes locaux

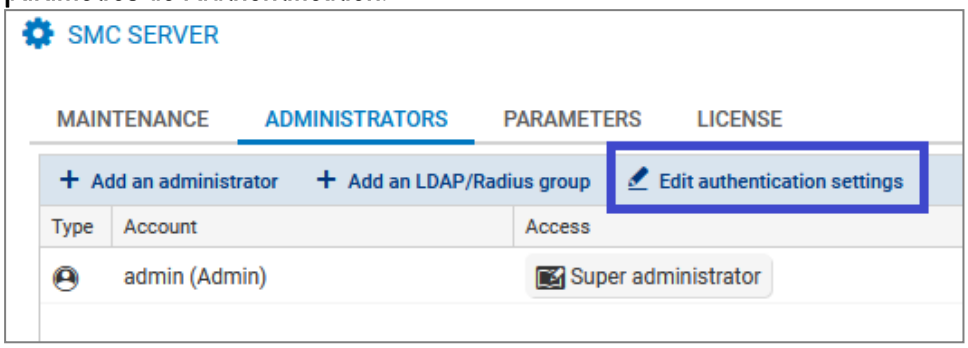
Seul le super administrateur peut définir la politique de mots de passe pour les administrateurs disposant d'un compte local. Il peut choisir :

- La longueur minimale du mot de passe : le mot de passe peut contenir entre un et 128 caractères. Par défaut, il doit contenir au moins 16 caractères.
- Le type de caractères obligatoires : alphanumériques, alphabétiques et spéciaux et alphanumériques et spéciaux ou aucun.
- L'entropie minimale : elle tient compte de la longueur du mot de passe et de la taille du jeu de caractères utilisé. Par défaut, elle est de 64 bits.

Lors du déploiement d'un nouveau serveur SMC, le mot de passe du super administrateur dans l'assistant d'initialisation du serveur doit également comporter 16 caractères au minimum.

Pour définir une politique de mots de passe :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Modifier les paramètres de l'authentification**.



2. Dans l'onglet **Locale**, activez l'authentification locale si besoin.
3. Sélectionnez la longueur minimale.
4. Sélectionnez le type de caractères obligatoires.
5. Sélectionnez l'entropie minimale.

La politique de mots de passe s'applique à tous les administrateurs qui disposent d'un compte local.

Elle s'applique également aux mots de passe de chiffrement des sauvegardes. Pour plus d'informations, reportez-vous à la section Sauvegarder et restaurer la configuration du serveur SMC.

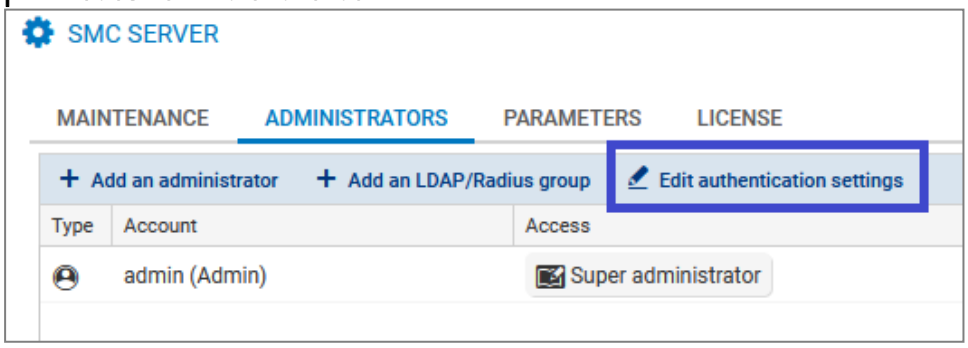
Les mots de passe qui ont été définis avant l'application de cette politique sont toujours valides mais nous vous recommandons de les modifier en accord avec la politique définie.

La limite de 128 caractères au maximum s'applique également à l'identifiant et au nom des administrateurs.

Désactiver l'authentification locale

Le super administrateur peut désactiver l'authentification locale et ainsi ne permettre l'authentification des administrateurs que via un serveur d'authentification Radius ou LDAP.

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Modifier les paramètres de l'authentification**.



2. Dans l'onglet **Locale**, décochez la case **Authentification locale activée**.
3. Cliquez sur **Appliquer**.

Le super administrateur conserve toujours le droit de s'authentifier avec son mot de passe local. Il s'agit du seul mode d'authentification possible pour lui.

13.4.3 Gérer les utilisateurs LDAP

Le serveur SMC peut être lié à un serveur LDAP pour autoriser des utilisateurs de l'entreprise à administrer un parc de firewalls.

Ce type d'authentification est prévu pour fonctionner avec un serveur LDAP de type Active Directory sur Microsoft Windows Server 2016, 2019 et 2022 ou OpenLDAP version 2.5 minimum.

La configuration de l'authentification via serveur LDAP s'effectue dans l'interface web d'administration de SMC.

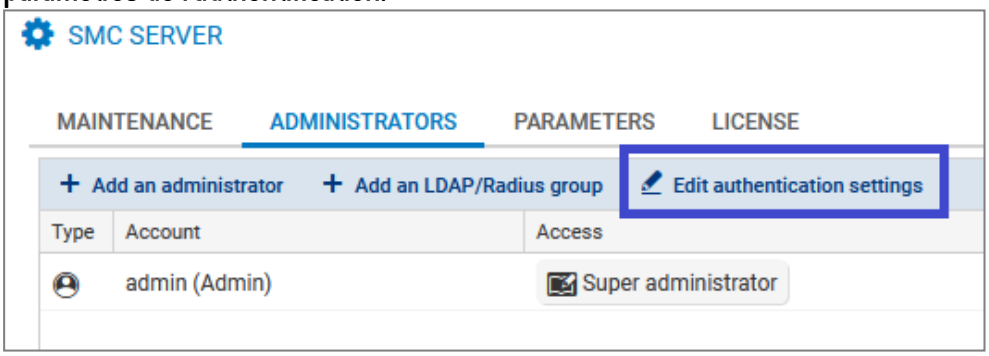
Pour autoriser des administrateurs à se connecter au serveur SMC via un serveur LDAP, suivez les trois étapes suivantes expliquées plus en détails ci-dessous :

1. Configurer la connexion au serveur LDAP,
2. Tester la connexion au serveur,
3. Autoriser des utilisateurs et définir leurs droits d'accès.

Configurer la connexion au serveur LDAP

Pour configurer et activer la connexion à un serveur LDAP :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Modifier les paramètres de l'authentification.**



2. Dans l'onglet **LDAP**, cochez **Authentification LDAP activée**.
3. Remplissez les champs suivants :

Champ	Description
Type de serveur	Serveur de type Active Directory ou OpenLDAP
Hôte	Adresse IP ou FQDN du serveur LDAP principal. S'il s'agit du FQDN du serveur, le service DNS doit être configuré au préalable. Dans le cas où vous utilisez le protocole SSL avec vérification de l'identité de l'autorité de certification pour sécuriser la connexion au serveur LDAP, le nom de l'Hôte doit être identique au nom commun (CN) du certificat du serveur LDAP.
Hôte de secours	Optionnel - Adresse IP ou FQDN du serveur LDAP de secours. S'il s'agit du FQDN du serveur, le service DNS doit être configuré au préalable. Seul ce paramètre est nécessaire pour le serveur LDAP de secours, les autres paramètres sont ceux du serveur principal.
Port	Numéro de port pour accéder au serveur LDAP : par défaut port 636 si le SSL est activé, port 389 sinon
Base DN	Base DN permettant d'accéder au serveur LDAP, répondant au format suivant : dc=sub,dc=domain,dc=com. Avec un serveur OpenLDAP, la Base DN peut également porter sur un emplacement plus précis, par exemple une unité d'organisation : ou=unit,dc=domain,dc=com
Identifiant	Ce champ s'affiche si le type de serveur est Active Directory. Identifiant de l'administrateur permettant de faire une requête au serveur LDAP Active Directory. Par exemple : Administrateur.
DN Administrateur	Ce champ s'affiche si le type de serveur est OpenLDAP. DN de l'administrateur (sans la base DN) permettant de faire une requête au serveur LDAP OpenLDAP. Par exemple : cn=admin.
Mot de passe	Mot de passe permettant de se connecter au serveur LDAP
Sécuriser avec SSL	Si l'option est activée, la connexion au serveur LDAP est sécurisée via les protocoles SSL/TLS. Lorsque le SSL est activé, le port par défaut est modifié en conséquence. Si le SSL est activé, le serveur SMC ne vérifie pas par défaut l'autorité de certification ayant signé le certificat du serveur LDAP.
Vérifier l'identité de la CA du serveur LDAP	Cette option permet de vérifier l'autorité de certification ayant signé le certificat du serveur LDAP, lorsque le SSL est activé. Fournissez le certificat de l'autorité de certification dans le champ ci-dessous.
Certificat	Ce champ permet de transférer sur le serveur SMC le certificat de l'autorité de certification ayant signé le certificat utilisé par le serveur LDAP pour la connexion sécurisée via SSL.

NOTE
Tous les champs sont sensibles à la casse. Nous vous recommandons de bien vérifier la configuration de votre annuaire LDAP.

Tester la connexion au serveur LDAP

Pour tester la connexion au serveur LDAP, utilisez l'outil *ldapsearch* disponible en ligne de commande sur le serveur SMC.

Utilisez les paramètres suivants avec la commande `ldapsearch` afin de tester la connexion à un serveur LDAP et effectuer une recherche dans l'annuaire :

Paramètre	Description
-H	Adresse IP ou FQDN du serveur LDAP, précédée de ldap:// suivi du numéro de port (par défaut le port 389 est utilisé).
-D	Nom distinctif utilisé pour s'authentifier sur le serveur. Ce nom doit correspondre à une entrée spécifique de l'annuaire et doit être autorisé à faire des recherches dans l'annuaire. Il peut être aussi bien un administrateur qu'un utilisateur. Par défaut le format attendu est le suivant : CN=Administrator,DC=mydomain,DC=com Pour interroger un annuaire de type Active Directory, le format peut également être : Administrator@mydomain.com.
-W	Si renseigné, un mot de passe pour l'authentification sera demandé avant de lancer la recherche
-b	Branche de l'arbre LDAP à partir de laquelle vous souhaitez lancer la recherche. Pour rechercher dans l'annuaire entier, indiquez la base DN. Par exemple : DC=mydomain,DC=com.

EXEMPLES

Pour Active Directory :

```
ldapsearch -H ldap://1.2.3.4:536 -D "Administrator@mydomain.com" -W -b
"DC=mydomain,DC=com"
```

Pour OpenLDAP :

```
ldapsearch -H ldap://1.2.3.4:536 -D
"cn=Administrator,dc=mydomain,dc=com" -W -b "dc=mydomain,dc=com"
```

Vous pouvez filtrer la recherche en ajoutant des attributs à la suite de la commande. Ajoutez par exemple l'attribut "member" pour afficher les membres des groupes.

EXEMPLE

```
ldapsearch -H ldap://1.2.3.4:536 -D "Administrator@mydomain.com" -W -b
"CN=Users,DC=mydomain,DC=com" member
```

Autoriser un utilisateur LDAP

Pour autoriser un utilisateur LDAP à s'authentifier sur le serveur SMC, le super administrateur doit l'ajouter dans la liste des administrateurs dans l'interface web d'administration.

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Ajouter un administrateur**.
2. Remplissez les champs obligatoires suivants :

Champ	Description
Identifiant	Identifiant de l'utilisateur LDAP. Ce champ correspond à l'attribut `sAMAccountName` si le serveur LDAP est un ActiveDirectory et à l'attribut `uid` si le serveur LDAP est un OpenLDAP. Il est optionnel si le champ **DN LDAP** est rempli.

DN LDAP	DN de l'utilisateur LDAP. Ce champ correspond aux attributs `DistinguishedName` et `dn`, quel que soit le serveur LDAP configuré. Il est optionnel si le champ **Identifiant** est rempli.
Nom	Nom de l'utilisateur LDAP qui est affiché sur SMC.

3. Sélectionnez les droits d'accès. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur et à la section Restreindre les droits d'accès des administrateurs de dossiers.
4. Décochez la case **Cet administrateur peut utiliser l'authentification locale** si vous ne souhaitez pas définir d'authentification locale pour l'utilisateur LDAP.

Les termes suivants sont réservés par SMC et donc inutilisables en tant qu'identifiant : root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

NOTE
Les identifiants des utilisateurs authentifiés via l'annuaire LDAP ne doivent pas contenir d'espace pour se connecter au serveur SMC.

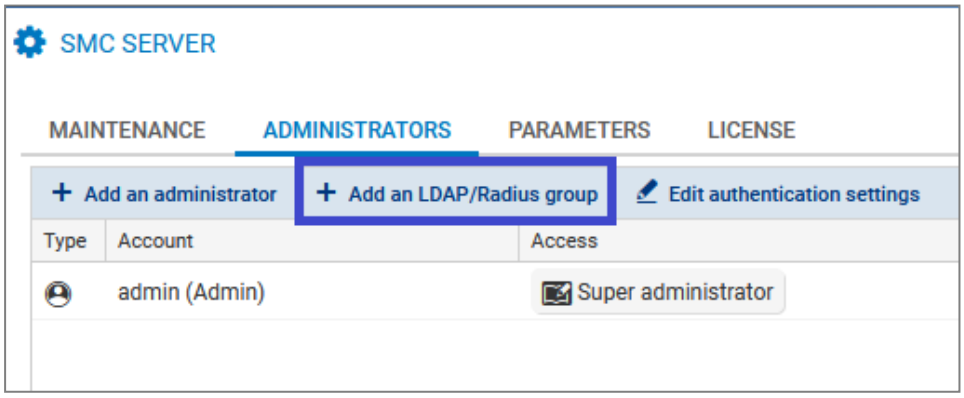
Ajouter un groupe LDAP

Les utilisateurs peuvent faire partie de groupes LDAP.

Par défaut SMC recherche des utilisateurs appartenant à un groupe à l'aide de l'attribut `memberOf`. Cet attribut est utilisé sur les annuaires de type Active Directory. Sur certains annuaires OpenLDAP, vous devez configurer cet attribut.
Vous pouvez utiliser un autre attribut pour rechercher des utilisateurs dans un groupe. Pour plus d'informations, reportez-vous à la section Modifier les attributs LDAP utilisés par défaut par SMC.

Pour ajouter un groupe d'utilisateurs LDAP :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Ajouter un groupe LDAP/Radius**.



2. Remplissez les champs obligatoires suivants :

Champ	Description
DN LDAP	DN du groupe LDAP auquel appartiennent les utilisateurs LDAP. Ce champ correspond aux attributs `DistinguishedName` et `dn`, quel que soit le serveur LDAP configuré.
Nom	Nom du groupe LDAP qui est affiché sur SMC.

3. Sélectionnez les droits d'accès. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur.

Si un administrateur possède un compte nominatif et est en même temps membre d'un ou plusieurs groupes, les droits qui s'appliquent sont ceux de son compte nominatif.

> **NOTE**
> Les identifiants des utilisateurs authentifiés via l'annuaire LDAP ne doivent pas contenir d'espace pour se connecter au serveur SMC.

Modifier les attributs LDAP utilisés par défaut par SMC

Dans la fenêtre **Serveur SMC** > **Administrateurs** > **Ajouter un administrateur**, les champs **Identifiant** et **DN LDAP** correspondent par défaut aux attributs LDAP suivants :

Identifiant	• `sAMAccountName` si le serveur est un Active Directory • `uid` si le serveur est un OpenLDAP
DN LDAP	• `distinguishedName` et `dn` quel que soit le serveur LDAP configuré

SMC s'appuie également sur l'attribut `memberOf` pour rechercher les groupes auxquels appartient un utilisateur. Il peut être nécessaire de le configurer manuellement sur certains serveurs LDAP.

Les variables d'environnement suivantes permettent de modifier ces trois attributs :

- `SMC_LDAP_FIELD_NAME_LOGIN`
- `SMC_LDAP_FIELD_NAME_DN`
- `SMC_LDAP_FIELD_NAME_MEMBEROF`

Pour modifier leur valeur :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, modifiez les valeurs de ces variables d'environnement.
3. Redémarrez le serveur avec la commande `nrestart smc`.

13.4.4 Gérer les utilisateurs Radius

Le serveur SMC peut être lié à un serveur Radius pour autoriser des utilisateurs de l'entreprise à administrer un parc de firewalls.

Ce type d'authentification est prévu pour fonctionner avec un serveur Radius ou FreeRADIUS sur Microsoft Windows Server 2016, 2019 et 2022.

La configuration de l'authentification via serveur Radius s'effectue dans l'interface web d'administration de SMC.

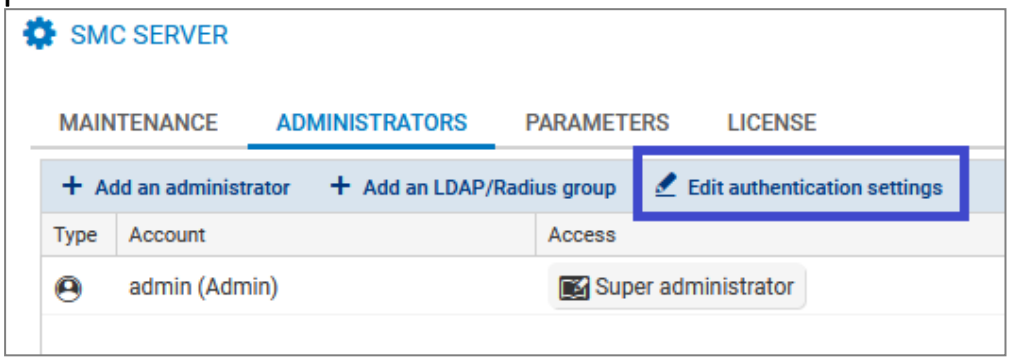
Pour autoriser des administrateurs à se connecter au serveur SMC via un serveur Radius, suivez les trois étapes suivantes expliquées plus en détails ci-dessous :

1. Configurer la connexion au serveur Radius,
2. Tester la connexion au serveur,
3. Autoriser des utilisateurs et définir leurs droits d'accès.

Configurer la connexion au serveur Radius

Pour configurer et activer la connexion à un serveur Radius :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Modifier les paramètres de l'authentification.**



2. Dans l'onglet **Radius**, cochez **Authentification Radius activée**.
3. Par défaut, l'option **Activer la bascule automatique entre serveurs Radius et LDAP en cas d'indisponibilité du serveur Radius** est désactivée. Activez l'option si vous souhaitez envoyer les requêtes d'authentification au serveur LDAP en cas d'indisponibilité du serveur Radius.

> **ATTENTION**
> L'activation de cette option signifie qu'en cas de bascule, le niveau de sécurité de votre authentification correspondra à celui que vous avez défini dans votre configuration LDAP.

4. Remplissez les champs suivants :

Champ	Description
Serveur principal	
Hôte	Adresse IP ou FQDN du serveur Radius principal. S'il s'agit du FQDN du serveur, le service DNS doit être configuré au préalable.
Port	Numéro de port pour accéder au serveur Radius : par défaut port 1812
Clé pré-partagée	Clé secrète partagée afin de s'authentifier sur le serveur
Serveur de secours - Optionnel	
Hôte	Adresse IP ou FQDN du serveur Radius de secours. S'il s'agit du FQDN du serveur, le service DNS doit être configuré au préalable.
Port	Numéro de port pour accéder au serveur Radius : par défaut port 1812
Clé pré-partagée	Clé secrète partagée afin de s'authentifier sur le serveur

Tester la connexion au serveur Radius

Pour tester la connexion au serveur Radius, utilisez l'outil *radtest* disponible en ligne de commande sur le serveur SMC :

EXEMPLE

```
radtest <user-id> <user-password> <radius-server-ip>:<radius-server-port> <NAS-server-port> <pre-shared-key>
```

```
[root@smc] - {~} > radtest user-radius password 1.2.3.5:1812 1812 P@s5w0rD
Sent Access-Request Id 4 from 0.0.0.0:46901 to 1.2.3.5:1812 length 87
        User-Name = "user-radius"
        User-Password = "password"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Framed-Protocol = PPP
        Cleartext-Password = "password"
Received Access-Accept Id 4 from 1.2.3.5:1812 to [redacted]:46901 length 20
```

Autoriser un utilisateur Radius

Pour autoriser un utilisateur Radius à s'authentifier sur le serveur SMC, le super administrateur doit l'ajouter dans la liste des administrateurs dans l'interface web d'administration.

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Ajouter un administrateur**.
2. Remplissez les champs obligatoires suivants :

Champ	Description
Identifiant	Identifiant de l'utilisateur Radius
Nom	Nom de l'utilisateur Radius qui est affiché sur SMC

3. Sélectionnez les droits d'accès. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur et à la section Restreindre les droits d'accès des administrateurs de dossiers.
4. Décochez la case **Cet administrateur peut utiliser l'authentification locale** si vous ne souhaitez pas définir d'authentification locale pour l'utilisateur Radius.

Les termes suivants sont réservés par SMC et donc inutilisables en tant qu'identifiant : root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, sshd, dhcpcd, messagebus, fwadmin-server, nobody.

NOTE

Les identifiants des utilisateurs authentifiés via l'annuaire Radius ne doivent pas contenir d'espace pour se connecter au serveur SMC.

Ajouter un groupe Radius

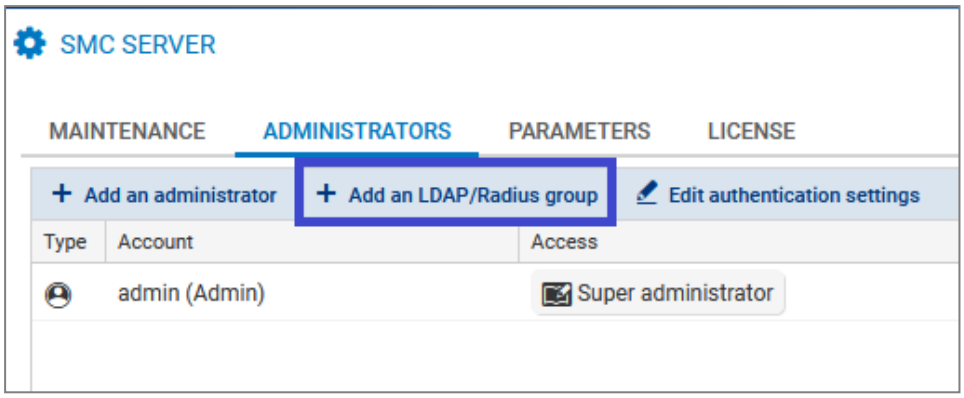
Les utilisateurs peuvent faire partie de groupes Radius.

Au préalable, vous devez configurer le Vendor Specific Attribute (VSA) sur le serveur Radius de la manière suivante, afin que les groupes soient visibles par SMC :

- Vendor code = 11256
- Vendor-assigned attribute number = 1
- Attribute format = string
- Attribute value = group1, group2... (nom des groupes)

Pour ajouter un groupe d'utilisateurs Radius :

1. Dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**, cliquez sur **Ajouter un groupe LDAP/Radius**.



2. Remplissez les champs obligatoires suivants :

Champ	Description
Identifiant Radius	Identifiant du groupe Radius
Nom	Nom du groupe Radius

3. Sélectionnez les droits d'accès. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur.

Si un administrateur possède un compte nominatif et est en même temps membre d'un ou plusieurs groupes, les droits qui s'appliquent sont ceux de son compte nominatif.

NOTE
Les identifiants des utilisateurs authentifiés via l'annuaire Radius ne doivent pas contenir d'espace pour se connecter au serveur SMC.

13.4.5 Restreindre les droits d'accès des administrateurs de dossiers

SMC permet de segmenter l'administration de votre parc de firewalls en assignant des administrateurs différents à des groupes de firewalls. Pour ce faire, vous pouvez restreindre l'accès en écriture d'un administrateur à un groupe de firewalls, en vous appuyant sur l'arborescence de dossiers disponible dans SMC. Cette segmentation permet de définir un périmètre d'administration pour chaque administrateur et ainsi de renforcer la sécurité sur votre parc de firewalls.

Pour plus d'informations sur la gestion des dossiers, reportez-vous à la section Classer les firewalls par dossiers.

EXEMPLE
Si votre parc de firewalls s'étend sur plusieurs pays ou continents, vous pouvez choisir de définir un administrateur différent par pays ou continent. Chaque administrateur peut alors administrer les firewalls du dossier de sa zone uniquement. Il peut également consulter en lecture seule la configuration des autres firewalls et du serveur SMC.

Seul le super administrateur peut limiter le droit d'accès en écriture des autres administrateurs à certains dossiers.

Il peut alors définir deux profils d'administrateur possédant le droit d'accès en écriture :

Administrateur général	• Il possède le droit d'accès en écriture au dossier racine de SMC, c'est-à-dire à tous les sous-dossiers et donc tous les firewalls SNS. • Il peut modifier la configuration de tous les firewalls SNS rattachés à SMC. • Il peut créer et modifier tous les éléments de configuration présents dans SMC (objets, règles, topologies VPN, QoS, certificats, profils de chiffrement, etc.). • Il peut réaliser certaines opérations de maintenance du serveur SMC.
Administrateur de dossiers	• Son droit d'accès en écriture est restreint à un ou plusieurs dossiers et aux firewalls qu'ils contiennent. • Il peut modifier uniquement la configuration des firewalls qu'il administre. • Il peut créer des éléments de configuration et les utiliser pour les firewalls qu'il administre. • Il peut créer des topologies VPN uniquement avec les firewalls qu'il administre. • Il peut accéder en lecture/écriture directement à l'interface des firewalls qu'il administre via SMC. • Il peut accéder en lecture seule à la configuration des firewalls hors de son périmètre d'administration, à tous les éléments de configuration présents dans SMC, à la configuration du serveur SMC. • Il peut accéder directement à l'interface des firewalls hors de son périmètre d'administration via SMC, mais en lecture seule uniquement.

Pour plus de détails sur les profils d'administrateurs, les implications et limitations de la restriction des droits d'accès à des dossiers, reportez-vous à la section Gérer les administrateurs locaux et provenant d'annuaires externes et aux sections ci-dessous.

Restreindre le droit d'écriture d'un administrateur de dossiers

Le super administrateur choisit le ou les dossiers sur lesquels un administrateur de dossiers possède le droit d'écriture. Cela signifie qu'il donne à l'administrateur un accès en écriture complet sur ces dossiers, leurs éventuels sous-dossiers et les firewalls qu'ils contiennent, ainsi que sur les futurs sous-dossiers ou firewalls.

L'administrateur de dossiers peut toujours consulter en lecture seule la configuration des firewalls qui ne font pas partie de son périmètre d'administration.

Pour restreindre les droits d'un administrateur :

1. Rendez-vous dans le menu **Maintenance** > **Serveur SMC** > **Administrateurs**.
2. Double-cliquez sur la ligne de l'administrateur.
3. Dans la liste déroulante **Dossiers**, sélectionnez le ou les dossiers que l'administrateur doit pouvoir administrer.
4. Appliquez la modification.

Dans la vue de supervision des firewalls, par défaut l'administrateur de dossiers ne voit que les firewalls dans son périmètre d'administration, c'est-à-dire appartenant aux dossiers sur lesquels il possède le droit d'accès en écriture.

Pour afficher tous les firewalls, cliquez sur **Voir les dossiers en lecture seule**.

Comprendre les implications de la restriction des droits d'écriture

Un administrateur de dossiers peut créer des éléments de configuration (objets, règles, files d'attente QoS, etc.) et les utiliser dans la configuration des firewalls qu'il administre. Il peut également utiliser tous les éléments de configuration disponibles dans SMC et qui ont été ajoutés par d'autres administrateurs.

Cependant, il ne peut pas modifier ou supprimer ces éléments s'ils sont utilisés dans la configuration de firewalls qui ne sont pas dans son périmètre d'administration.

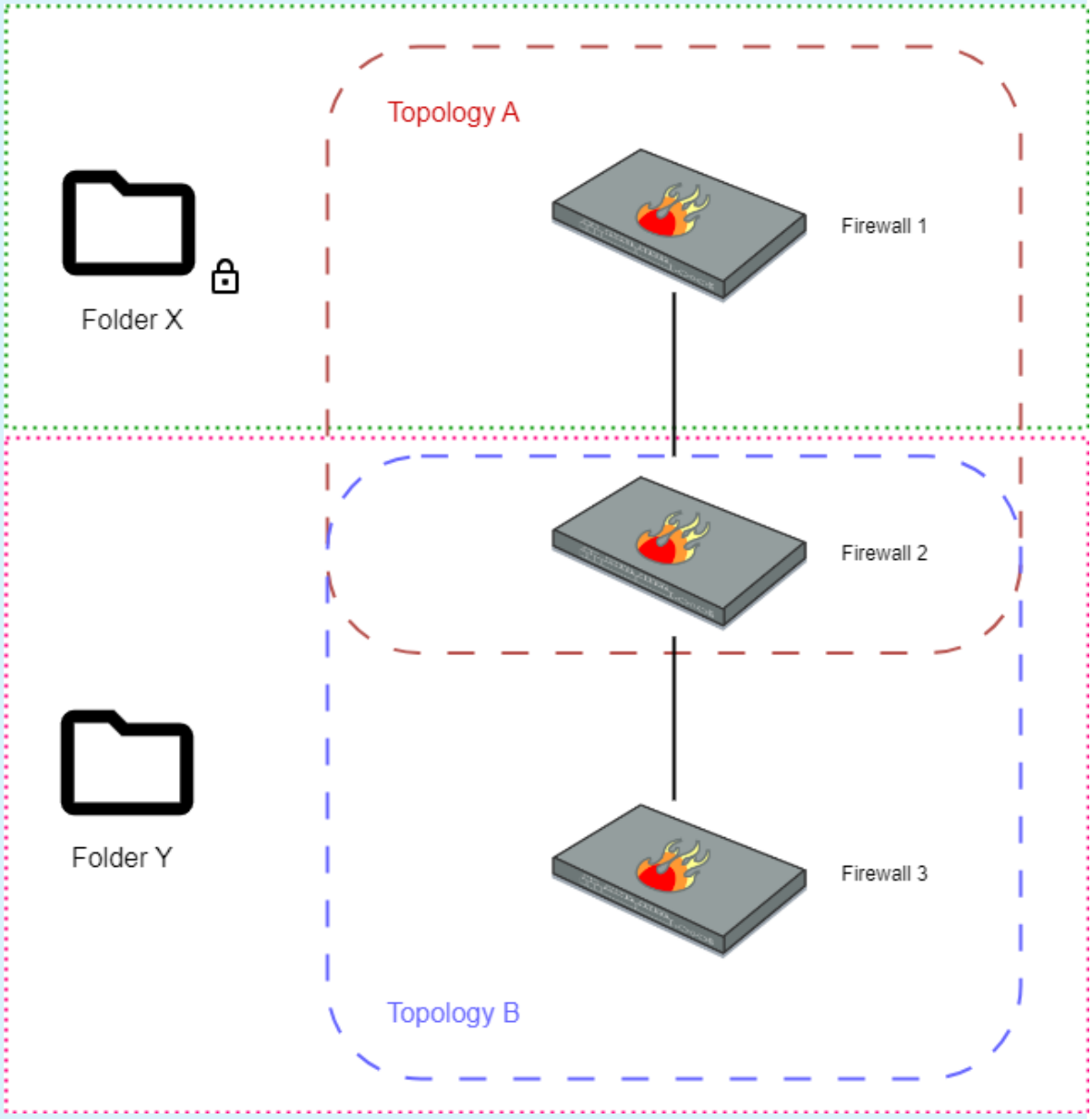
Gérer les topologies VPN avec un accès aux dossiers restreint

Pour pouvoir créer, modifier ou supprimer une topologie VPN, l'administrateur de dossiers doit posséder le droit d'accès en écriture sur tous les firewalls compris dans la topologie.

Si ce n'est pas le cas, c'est-à-dire si les correspondants d'une même topologie sont des firewalls classés dans plusieurs dossiers administrés par des administrateurs de dossiers différents, seul un administrateur général peut la créer, la modifier ou la supprimer.

Le droit d'accès en écriture au dossier prime sur le droit d'accès en écriture à une topologie. Ainsi, un administrateur de dossiers conserve le droit de configurer un firewall sur lequel il a le droit d'écriture, même si celui-ci fait partie d'une topologie sur laquelle il n'a pas l'accès complet.

EXEMPLE



Dans cet exemple, le Firewall 1 est classé dans le dossier X et les Firewalls 2 et 3 sont classés

dans le dossier Y. L'administrateur du dossier Y ne peut pas modifier la topologie A car elle comprend le firewall 1 sur lequel il n'a pas le droit d'accès en écriture. Néanmoins, il conserve le droit d'accès en écriture sur le firewall 2, même s'il fait partie de la topologie A.

Connaître les limitations des actions sur la configuration générale de SMC

Un administrateur de dossiers ne peut pas réaliser les actions suivantes sur la configuration générale de SMC :

- ajouter ou modifier les propriétés personnalisées globales des firewalls,
- importer des objets via un fichier CSV,
- modifier le plan d'adressage VTI par défaut dans les topologies VPN,
- charger et déployer une ancienne configuration,
- activer ou modifier le contrôle de cohérence pour le mode "Diffusion restreinte (DR)",
- saisir ou modifier un raccourci vers le serveur Stormshield Log Supervisor (SLS),
- ajouter un script CLI SNS ou une pièce jointe à un script,
- modifier les paramètres du serveur Active Update,
- créer des clés API avec une utilisation "écriture" pour accéder à l'API publique de SMC.

13.4.6 Résoudre les problèmes

Consultez cette section pour résoudre les éventuels problèmes rencontrés avec la gestion des administrateurs.

Un administrateur possédant un caractère accentué dans son identifiant ne peut pas se connecter à SMC

- *Situation* : La connexion à SMC est refusée à un administrateur provenant d'un serveur d'authentification LDAP et possédant un caractère accentué dans son identifiant.
- *Cause* : Lorsque vous ajoutez un administrateur provenant d'un serveur LDAP dans SMC, si son nom comprend un caractère accentué (champ **DN LDAP**), l'accent n'est pas pris en compte dans l'identifiant SMC.
- *Solution* : Pour se connecter, l'administrateur doit entrer son identifiant sans accent.

13.5 Consulter les journaux du serveur SMC

Le serveur SMC fournit deux types de journaux :

- *server.log* : recense toutes les actions enregistrées sur le serveur SMC. Ce fichier peut être consulté depuis l'interface web du serveur et depuis l'interface de ligne de commande via la commande `nlogs`.
- *audit.log* : recense toutes les actions effectuées par un administrateur sur le serveur. Ce fichier peut être consulté depuis l'interface web du serveur et depuis l'interface de ligne de commande via la commande `alogs`.

Pour consulter les Journaux du serveur depuis l'interface web :

1. Affichez le menu **Maintenance** > **Journaux du serveur** ou bien affichez et masquez à tout moment les journaux en cliquant sur la flèche noire en bas de l'interface .
2. Déplacez le curseur pour sélectionner les journaux minimum à afficher, des moins au plus critiques : information, avertissement ou erreur.
   1000 lignes maximum peuvent être affichées. Lorsque la limite est atteinte, les journaux les plus anciens sont écrasés par les plus récents dans l'interface.
3. Pour visualiser l'intégralité du contenu du fichier, connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH et tapez la commande `nlogs`.

Pour consulter les Journaux d'audit depuis l'interface web :

1. Affichez le menu **Maintenance** > **Journaux d'audit** ou bien affichez et masquez à tout moment les journaux en cliquant sur la flèche noire en bas de l'interface .
2. Vous pouvez afficher la colonne **Détails**, masquée par défaut.

> **NOTE**
> Le serveur SMC conserve les journaux des 12 dernières semaines dans la limite de 100 Mo par fichier. Pour assurer l'archivage légal d'un an, envoyez les journaux à un serveur Syslog distant.

Pour savoir comment envoyer les journaux vers un serveur Syslog distant, consultez la section Envoyer les journaux de SMC vers un serveur distant au format Syslog.

13.6 Envoyer les journaux de SMC vers un serveur distant au format Syslog

SMC supporte le protocole Syslog afin de collecter tous les journaux du système et de SMC et de les envoyer sur un serveur Syslog distant, avec ou sans chiffrement.

Pour utiliser le service Syslog sur SMC :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Entrez la commande `smc-syslog-ng`. La configuration courante du service s'affiche.

13.6.1 Envoyer les journaux vers un serveur distant sans chiffrement

1. Entrez la commande `smc-syslog-ng --wizard` pour choisir le mode de fonctionnement.
2. Choisissez l'option **Store logs locally and send logs to a syslog-ng server through TCP**.
3. Entrez l'adresse IP ou le nom FQDN du serveur distant ainsi que le numéro de port.

13.6.2 Envoyer les journaux vers un serveur distant avec chiffrement

Pour chiffrer la communication lors du transfert des journaux vers le serveur distant, vous avez besoin de trois fichiers issus de votre PKI (Public Key Infrastructure) :

- Le certificat client au format PEM qui permet à SMC d'être identifiée par le serveur distant,
- La clé privée du client au format PEM qui permet à SMC de chiffrer les données de manière à ce que seul le serveur distant puisse les déchiffrer,
- Le certificat de l'autorité de certification au format PEM qui permet à SMC de faire confiance au serveur distant.

1. Avant de configurer le service Syslog, copiez ces trois fichiers sur SMC, dans `/tmp` par exemple.
2. Entrez la commande `smc-syslog-ng --wizard` pour choisir le mode de fonctionnement.
3. Choisissez l'option **Store logs locally and send logs to a syslog-ng server through TCP with TLS**.
4. Entrez l'adresse IP ou le nom FQDN du serveur distant ainsi que le numéro de port.
5. Indiquez l'emplacement des certificats. L'assistant Syslog les copie dans le dossier `/data/certs/syslog-ng/`.

13.6.3 Désactiver l'envoi des journaux vers un serveur distant

1. Entrez la commande `smc-syslog-ng --wizard` pour choisir le mode de fonctionnement.
2. Choisissez l'option **Store logs locally in /var/log/messages (default)**.

13.6.4 Résoudre les problèmes

Le serveur Syslog distant est injoignable

- *Situation* : Vous avez spécifié le nom du serveur Syslog distant par son nom FQDN et le serveur reste injoignable.
- *Cause* : Le service DNS n'est peut-être pas correctement configuré ou ne peut pas résoudre le nom FQDN.
- *Solution* : Vérifiez la résolution du serveur DNS en entrant la commande `nslookup server-syslog.domaine.com` dans l'interface de ligne de commande de SMC.

En cas de transfert des journaux avec chiffrement, le serveur distant ne reçoit pas les journaux de SMC

- *Situation* : Vous avez configuré l'envoi des journaux vers un serveur Syslog distant avec chiffrement. Vous avez fourni les certificats nécessaires, et la communication chiffrée n'est pas acceptée par le serveur Syslog.
- *Cause* : Les certificats ne sont peut-être pas acceptés par le serveur Syslog distant (révoqués, périmés).
- *Solution* : Vérifiez l'erreur renvoyée par le serveur Syslog distant en entrant les commandes suivantes dans l'interface de ligne de commande de SMC :

```
MY_SERVER_ADDR=xxx.xxx.xxx.xxx
MY_SERVER_PORT=xxxx
openssl s_client -connect ${MY_SERVER_ADDR}:${MY_SERVER_PORT} -cert
/data/certs/syslog-ng/xxxx.pem -key /data/certs/syslog-ng/xxxx.pem -CAfile
/data/certs/syslog-ng/xxxx.pem
```

13.7 Sauvegarder et restaurer la configuration du serveur SMC

Seul le super administrateur est autorisé à sauvegarder ou restaurer la configuration du serveur SMC.

La sauvegarde et la restauration de la configuration sont possibles à partir de l'interface web du serveur (utilisateur "admin") ou de l'interface de ligne de commande (utilisateur "root").

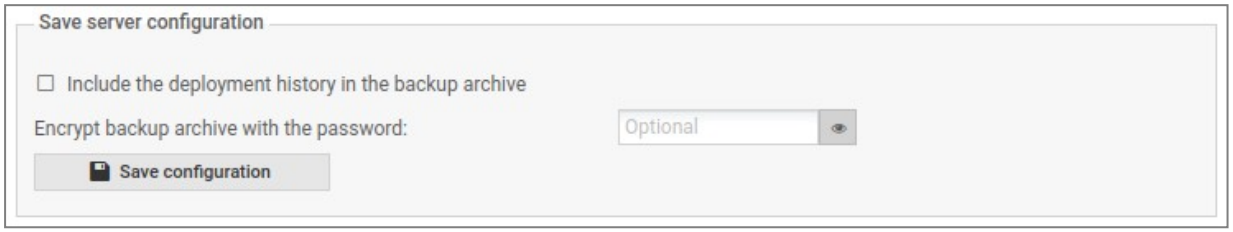
> **ASTUCE**
> La restriction suivante s'applique à la restauration d'une configuration du serveur : la version du serveur SMC doit être la même que celle du serveur à partir duquel le fichier de sauvegarde a été généré.

Les journaux du serveur ne sont pas contenus dans le fichier de sauvegarde.

Vous pouvez également mettre en place une sauvegarde automatique de la configuration des firewalls ainsi que de la configuration du serveur SMC. Pour plus d'informations, reportez-vous à la section Sauvegarder la configuration des firewalls .

13.7.1 Sauvegarder la configuration du serveur depuis l'interface web

En tant qu'utilisateur "admin", dans le menu **Maintenance** > **Serveur SMC** > **Maintenance**, cliquez sur **Sauvegarder la configuration** dans le volet **Sauvegarder la configuration du serveur**.



SMC permet de chiffrer la sauvegarde en définissant un mot de passe. Le mot de passe doit respecter la politique de mots de passe définie pour les administrateurs possédant des comptes locaux.

Le fichier de sauvegarde de la configuration peut être restauré à partir de :

- L'interface web du serveur SMC,
- L'interface de ligne de commande,
- L'assistant d'initialisation du serveur SMC.

Pour plus d'informations, reportez-vous aux sections Restaurer la configuration du serveur depuis l'interface web, Restaurer la configuration du serveur en ligne de commande et Restaurer la configuration du serveur depuis l'assistant d'initialisation .

13.7.2 Sauvegarder la configuration du serveur en ligne de commande

1. Pour sauvegarder la configuration du serveur depuis l'interface de ligne de commande en tant qu'utilisateur "root", connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande
   `smc-config-backup`
   Le nom de l'archive s'affiche.
3. Pour sauvegarder la configuration sans l'historique de déploiement, tapez la commande `smc-config-backup --no-history`.
4. Si vous souhaitez chiffrer la sauvegarde, tapez la commande `smc-config-backup --password <my_password>`. Remplacez `my_password` par le mot de passe de chiffrement de la sauvegarde. Le mot de passe doit respecter la politique de mots de passe définie pour les administrateurs possédant des comptes locaux.

Le fichier de sauvegarde de la configuration peut être restauré à partir de :

- L'interface web du serveur SMC,
- L'interface de ligne de commande,
- L'assistant d'initialisation du serveur SMC.

Pour plus d'informations, reportez-vous aux sections Restaurer la configuration du serveur depuis l'interface web, Restaurer la configuration du serveur en ligne de commande et Restaurer la configuration du serveur depuis l'assistant d'initialisation .

13.7.3 Restaurer la configuration du serveur depuis l'interface web

En tant qu'utilisateur "admin", dans le menu **Maintenance** > **Serveur SMC** > **Maintenance**, sélectionnez un fichier de sauvegarde à restaurer dans le volet **Restaurer la configuration du**

serveur.

Si le fichier de sauvegarde a été chiffré par un mot de passe, une fenêtre vous demande de le saisir.

Pour savoir comment créer une sauvegarde de serveur, reportez-vous aux sections Sauvegarder la configuration du serveur depuis l'interface web et Sauvegarder la configuration du serveur en ligne de commande.

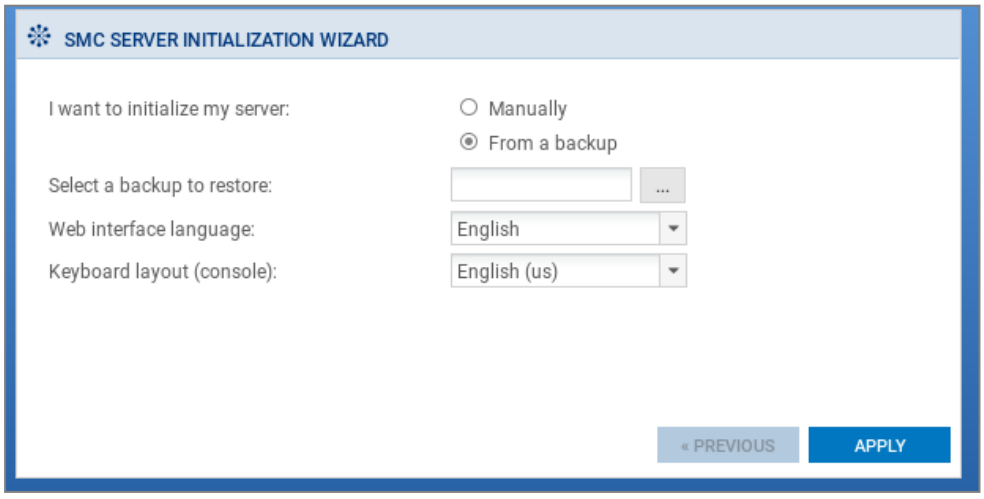
13.7.4 Restaurer la configuration du serveur en ligne de commande

1. Pour restaurer une configuration de serveur en ligne de commande en tant qu'utilisateur "root", copiez le fichier de sauvegarde dans */data/tmp* sur le serveur SMC à l'aide du protocole SSH.
2. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
3. Tapez la commande `smc-config-restore --backup-file /path/to/backup`. Remplacez `/path/to/backup` par le chemin et le nom du fichier.
4. Si le fichier de sauvegarde a été chiffré par un mot de passe, tapez la commande `smc-config-restore --backup-file /path/to/backup --password <my_password>`. Remplacez `/path/to/backup` par le chemin du fichier et `my_password` par le mot de passe de chiffrement de la sauvegarde.
5. Redémarrez.

Pour savoir comment créer une sauvegarde de serveur, reportez-vous aux sections Sauvegarder la configuration du serveur depuis l'interface web et Sauvegarder la configuration du serveur en ligne de commande.

13.7.5 Restaurer la configuration du serveur depuis l'assistant d'initialisation

Lors de l'initialisation d'un nouveau serveur SMC après le déploiement d'une nouvelle machine virtuelle, sélectionnez une sauvegarde à restaurer lors de la première étape de l'assistant d'initialisation du serveur. Si besoin, saisissez le mot de passe de chiffrement de la sauvegarde.



Pour savoir comment créer une sauvegarde de serveur, reportez-vous aux sections Sauvegarder la configuration du serveur depuis l'interface web et Sauvegarder la configuration du serveur en ligne de commande.

L'intégrité du fichier de sauvegarde est vérifiée avant sa restauration, et une nouvelle connexion est requise.

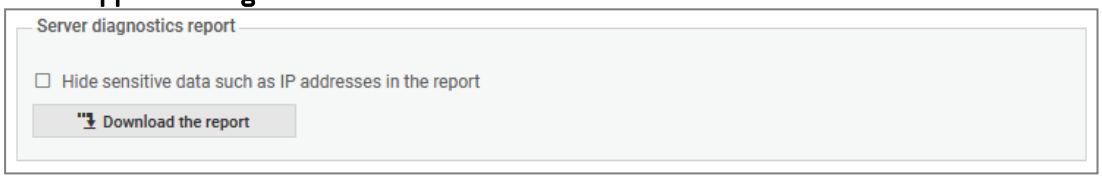
13.8 Générer un rapport de diagnostic du serveur

Vous pouvez télécharger un rapport de diagnostic sur l'état de santé du serveur SMC.

Ce rapport peut fournir des informations en cas de problèmes sur le serveur.

13.8.1 Télécharger le rapport depuis l'interface web

1. Dans **Maintenance** > **Serveur SMC** > **Maintenance**, cliquez sur **Télécharger le rapport** dans le volet **Rapport de diagnostic serveur**.



   Le rapport se présente comme une archive *tar.gz* dont le nom contient la date et l'heure de création.
2. Double-cliquez sur le fichier *index.html* pour ouvrir le rapport au format HTML.

13.8.2 Télécharger le rapport en ligne de commande

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Entrez la commande `smc-diag` ou `smc-diag --help` pour obtenir des détails sur les options possibles.
   Le rapport se présente comme une archive *tar.gz* dont le nom contient la date et l'heure de création. Par défaut, le rapport est généré dans le dossier */tmp*.
3. Double-cliquez sur le fichier *index.html* pour ouvrir le rapport au format HTML.

L'option --confidential permet de masquer les adresses IP et MAC.

13.9 Mettre à jour le serveur SMC

Les Notes de version SMC contiennent des informations importantes. Veuillez les consulter avant de mettre à jour le serveur SMC.

Une archive de mise à jour (*.upd*) est requise afin de mettre à jour le serveur SMC. L'archive implique la mise à jour de l'interface web et du système d'exploitation.

Avant de faire une mise à jour, nous vous recommandons fortement de faire un snapshot ou un instantané de votre machine virtuelle.

Pendant le processus de mise à jour, les firewalls fonctionnent toujours. Les firewalls n'ont pas besoin d'être mis à jour.

À chaque mise à jour, la configuration de SMC est migrée du fichier de configuration vers la base de données. Le fichier de configuration unifié est supprimé. Une sauvegarde de ce fichier est automatiquement faite sur l'ancien système avant la migration.

ASTUCE
En fonction de la configuration de votre hyperviseur, la mise à jour peut prendre du temps. Pour suivre l'avancement de la mise à jour, consultez le fichier /var/log/update.log.

13.9.1 Mettre à jour le serveur SMC depuis l'interface web

Pour mettre à jour le serveur SMC depuis l'interface web, vous devez être super administrateur.

1. Téléchargez l'archive de mise à jour sur votre poste de travail, depuis votre espace personnel MyStormshield.
2. Dans le menu **Maintenance** > **Serveur SMC** > **Maintenance**, sélectionnez le fichier de mise à jour dans le volet **Mettre à jour SMC**.
3. Cliquez sur le bouton **Mettre à jour SMC**.
4. Lorsque la mise à jour est terminée, reconnectez-vous au serveur SMC.

Pendant la mise à jour, le serveur SMC est indisponible. Aucun administrateur ne peut s'y connecter.

13.9.2 Mettre à jour le serveur SMC en ligne de commande

1. Téléchargez l'archive de mise à jour sur votre poste de travail, depuis votre espace personnel MyStormshield.
2. Copiez l'archive dans */data/tmp* sur le serveur SMC à l'aide du protocole SSH.
3. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
4. Tapez la commande `smc-update -u /data/tmp/archivename`. Remplacez `archivename` par le nom de votre archive.
   Pour les versions antérieures à la version 2.6 de SMC, la commande à entrer est `fwadmin-update -u /data/tmp/archivename`.
5. Attendez la fin de la mise à jour. Pendant le processus, le serveur reste disponible dans la version actuelle.
6. Tapez la commande `reboot`. Le système mis à jour redémarre.

13.10 Désactiver la synchronisation automatique d'un cluster haute disponibilité

Le serveur SMC opère une synchronisation régulière des deux nœuds des clusters haute disponibilité de firewalls qu'il administre.

Si besoin, vous pouvez désactiver cette synchronisation automatique :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Modifiez le fichier **/data/config/fwadmin-env.conf.local** en ajoutant la ligne suivante à la fin : `SMC_HASYNC_ON_DESYNCHRO_ENABLED=false`
3. Redémarrez le serveur avec la commande : `nrestart smc`

13.11 Superviser SMC avec le protocole SNMP

SNMP (Simple Network Management Protocol) est un protocole de communication qui permet aux administrateurs réseau de superviser des équipements et de diagnostiquer des problèmes réseau et matériel à distance.

Par défaut ce service n'est pas activé sur le serveur SMC. Si vous l'activez, il n'est pas nécessaire de l'activer à nouveau après un redémarrage du serveur. L'activation est conservée.

Le serveur SMC utilise par défaut la version 2c du protocole SNMP. Vous pouvez choisir une autre version (version 1 ou v3 USM) dans le fichier de configuration qui se trouve dans */etc/snmp/snmpd.conf*.

Pour choisir la v3 dans le fichier de configuration, veuillez suive la procédure indiquée sur la Base de connaissances Stormshield (anglais uniquement).

NOTE
Si vous choisissez d'utiliser la version 3 de SNMP, les protocoles d'authentification et de chiffrement associés et supportés par SMC sont SHA256 et AES-128.

13.11.1 Utiliser le service SNMP

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Entrez l'une des commandes suivantes :

Action	Commande
Activer le service	`/etc/init.d/snmpd restart ; update-rc.d -f snmpd remove ; update-rc.d snmpd defaults 98`
Consulter le statut du service	`/etc/init.d/snmpd status`
Redémarrer le service	`/etc/init.d/snmpd restart`
Désactiver le service	`nstop snmpd ; update-rc.d -f snmpd remove`

13.11.2 Utiliser les MIBs

SMC supporte les MIBs suivantes pour la supervision de SMC :

Catégorie	RFC	MIB
system	RFC 1213	.1.3.6.1.2.1.1
ifaces	RFC 1213 RFC 2863	.1.3.6.1.2.1.2 .1.3.6.1.2.1.31
ips	RFC 1213	.1.3.6.1.2.1.4
tcp	RFC 1213	.1.3.6.1.2.1.6
udp	RFC 1213	.1.3.6.1.2.1.7
snmp	RFC 1213	.1.3.6.1.2.1.11
mem	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4
disk	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9
load	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10

cpu	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
sysstats	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11
perf	RFC 1514	.1.3.6.1.2.1.25.4 .1.3.6.1.2.1.25.5

13.12 Personnaliser le certificat de l'interface web du serveur SMC

13.12.1 Personnaliser le certificat

Vous pouvez personnaliser le certificat présenté par l'interface web d'administration du serveur SMC de deux façons différentes :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Remplacez par vos propres certificat et clé privée les fichiers *server.crt* et *server.key* qui se trouvent dans le dossier `/etc/certs/uiserver`. Les droits des fichiers doivent rester les mêmes.
3. Redémarrez le serveur avec la commande `nrestart smc`.

- ou-

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Surchargez la variable d'environnement `SMC_UI_SERVER_CERT_PATH` dans le fichier **/data/config/fwadmin-env.conf.local** avec le chemin du dossier qui contient vos propres certificat et clé privée.
3. Redémarrez le serveur avec la commande `nrestart smc`.

13.12.2 Réinitialiser le certificat

Pour revenir à la configuration d'usine :

1. Utilisez la commande `smc-gen-autosigned-cert` en indiquant le dossier de destination ainsi que le sujet du certificat. Cette commande permet de générer à nouveau le certificat SSL présenté au navigateur web. Ce certificat est auto-signé.
   ```
   smc-gen-autosigned-cert /etc/certs/uiserver/ <sujet du certificat>
   ```
2. Redémarrez le serveur avec la commande `nrestart smc`.

13.13 Réinitialiser l'autorité de certification interne du serveur SMC

L'autorité de certification interne du serveur SMC émet et gère les certificats joints aux packages de rattachement et qui permettent la connexion, l'authentification et l'identification des firewalls SNS qui se connectent au serveur.

Lorsqu'un nouveau package de rattachement est généré pour un firewall déjà connu du serveur SMC, les certificats qui avaient été joints à des packages antérieurs sont alors révoqués par l'autorité de certification dès la connexion du firewall avec le nouveau package. De même, lorsqu'un firewall est supprimé du serveur SMC, tous les certificats joints aux différents packages de rattachement générés pour ce firewall sont révoqués.

En cas de besoin, il est possible de réinitialiser cette autorité de certification interne.

EXEMPLE
Cela peut être le cas si vous souhaitez passer d'un environnement de pré-production à un environnement de production et que vous devez réinitialiser l'autorité de certification car les contraintes de sécurité sont différentes entre les deux environnements.

Pour réinitialiser l'autorité de certification interne :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Tapez la commande `smc-reset-ca`.
3. Après l'exécution du script, les firewalls SNS qui étaient connectés au serveur SMC sont déconnectés. Vous devez générer des nouveaux packages de rattachement pour chacun d'eux et les installer.

13.14 Utiliser le mode "Diffusion Restreinte" sur les firewalls SNS

SMC permet d'activer sur les firewalls SNS un ensemble de paramètres de sécurité répondant au mode "Diffusion restreinte" (DR). Ceci garantit ainsi un niveau de confidentialité très élevé pour les communications transitant via VPN IPsec.

Afin d'activer le mode DR depuis SMC, vous devez au préalable vérifier la compatibilité de la configuration des firewalls rattachés avec les exigences du mode DR et, le cas échéant, corriger les anomalies de configuration incompatibles.

Pour plus d'informations sur le mode DR des firewalls SNS, reportez-vous au *Manuel Utilisateur SNS* et à la Note technique IPsec - Mode Diffusion Restreinte.

Cette fonctionnalité est disponible pour des firewalls SNS en version 4.3 minimum.

Il est possible de rattacher des firewalls en mode DR à un serveur SMC dont le mode DR n'est pas activé.

13.14.1 Activer le contrôle de cohérence du mode "Diffusion Restreinte"

ATTENTION
Un administrateur de dossiers dont l'accès en écriture est limité à certains dossiers sur SMC ne peut pas effectuer cette opération. Pour plus d'informations, reportez-vous à la section Restreindre les droits d'accès des administrateurs de dossiers.

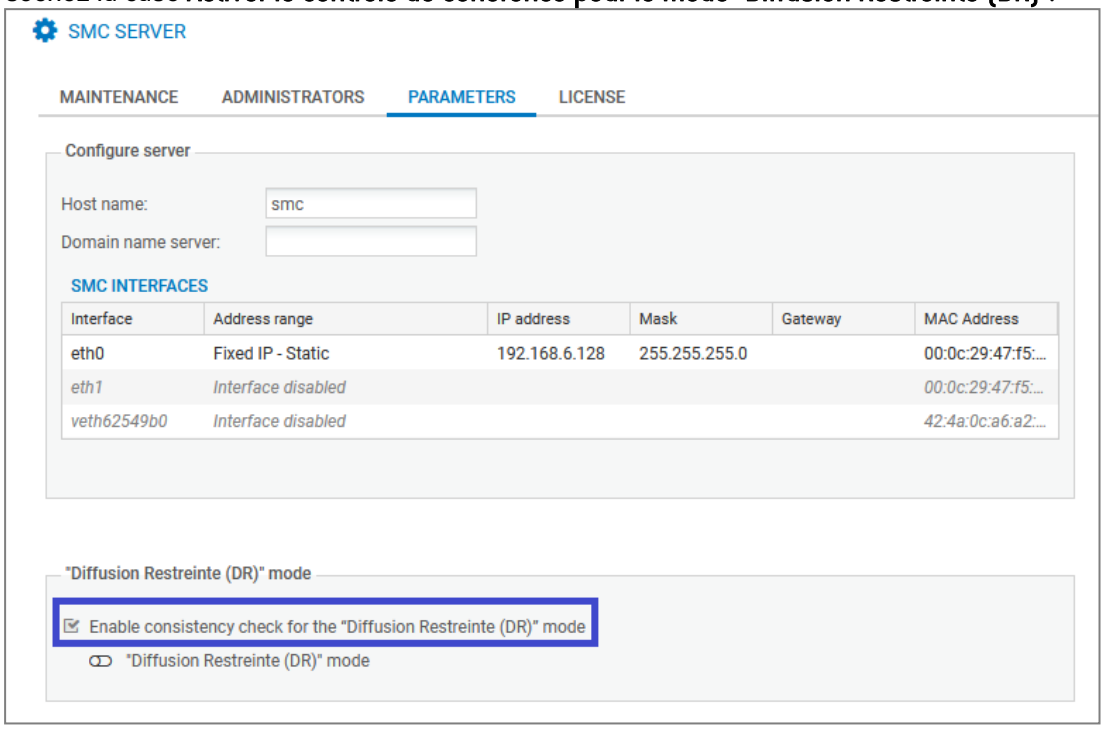
SMC permet de vérifier la compatibilité de la configuration des firewalls rattachés avec les exigences du mode DR grâce à un contrôle de cohérence :

- Algorithmes de signature et tailles de clés des certificats des firewalls et des certificats d'autorités,
- Profils de chiffrement, méthode d'authentification et version IKE des topologies VPN. Nous vous recommandons d'utiliser le profil de chiffrement DR par défaut fourni par SMC. Pour consulter ce profil, allez dans le menu **Configuration** > **Profils de chiffrement**. Pour plus d'informations sur la sélection des profils de chiffrement dans les topologies, reportez-vous à la section Créer et superviser des tunnels VPN.
- Versions des firewalls rattachés à SMC.

Ce contrôle de cohérence préalable à l'activation du mode DR est obligatoire.

Pour activer le contrôle de cohérence du mode DR :

1. Placez-vous dans le menu **Maintenance** > **Serveur SMC** > onglet **Paramètres** > panneau **Mode "Diffusion Restreinte (DR)"**.
2. Cochez la case **Activer le contrôle de cohérence pour le mode "Diffusion Restreinte (DR)"**.



3. Cliquez sur le bouton **Appliquer**.

Les éventuels messages indiquant des incompatibilités de configuration sont alors affichés dans le contrôleur de cohérence situé en bas de l'écran. Vous pouvez cocher la case **N'afficher que les incohérences Mode Diffusion Restreinte** afin de limiter l'affichage des messages au contrôle de cohérence du mode DR.

13.14.2 Activer le mode "Diffusion Restreinte" sur SMC et les firewalls

Le super administrateur (compte *admin*) peut activer le mode DR sur le serveur SMC et les firewalls SNS rattachés.

Dans le cas d'un cluster, vous n'activez le mode DR que sur le nœud actif. Il est automatiquement activé sur le nœud passif.

Les firewalls doivent tous être connectés au serveur SMC pour activer le mode DR.

Pour activer le mode DR :

1. Activez le contrôle de cohérence comme décrit dans la section précédente.
2. Activez la case **Mode "Diffusion Restreinte (DR)"**.
3. Acceptez les conditions et cliquez sur **Activer le mode DR**.
   L'activation du mode DR sur le serveur SMC entraîne un déploiement automatique destiné à activer le mode DR sur les firewalls rattachés au serveur.
4. Redémarrez aussitôt manuellement les firewalls.

Les conséquences de l'activation du mode DR sur le serveur SMC sont les suivantes :

- Les anomalies liées au contrôle de cohérence du mode DR remontent sous forme d'erreurs et non plus d'avertissements,

- La création d'un package de rattachement SMC n'est possible que pour les firewalls en version SNS 4.3 ou supérieure,
- Il n'est plus possible de rattacher à SMC des firewalls dont le mode DR n'a jamais été activé.

13.14.3 Désactiver le mode "Diffusion Restreinte" sur SMC et les firewalls

Le super administrateur (compte *admin*) peut désactiver le mode DR sur le serveur SMC. La désactivation depuis SMC ne désactive pas le mode DR sur les firewalls.

Pour désactiver le mode DR :

1. Placez-vous dans le menu **Maintenance** > **Serveur SMC** > onglet **Paramètres** > panneau **Mode "Diffusion Restreinte (DR)"**.
2. Désactivez la case **Mode "Diffusion Restreinte (DR)"**.
   Le mode DR du serveur SMC est désactivé et l'action n'entraîne aucune modification sur les firewalls, qui peuvent continuer à se connecter au serveur SMC.

13.15 Ajouter un texte de décharge de responsabilité sur la page de connexion (disclaimer)

Vous avez la possibilité d'ajouter un texte d'avertissement à l'attention des administrateurs, sur la page de connexion à l'interface web d'administration du serveur SMC. Vous pouvez ainsi les avertir, avant que ceux-ci ne se connectent, de certaines contraintes ou précautions qu'ils devront respecter lors de l'utilisation du serveur SMC.

Le texte est alors affiché dans un cadre **Décharge de responsabilité**.

Pour ajouter un fichier de décharge de responsabilité :

1. Créez un fichier texte nommé *login_disclaimer* contenant le texte souhaité. Pour une mise en forme enrichie, le texte peut-être au format HTML mais sans utilisation de Javascript. L'encodage UTF-8 est supporté.
2. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
3. Ajoutez le fichier *login_disclaimer* (sans extension) dans le répertoire *data/config*.

Ce fichier est conservé dans la sauvegarde de configuration du serveur.

13.16 Se connecter à l'interface de ligne de commande via des clés SSH

Pour vous connecter à l'interface de ligne de commande de SMC en SSH de façon transparente, vous pouvez configurer l'utilisation de clés SSH.

Au préalable, vous devez avoir généré une paire de clés SSH sur votre poste de travail.

Les clés SSH des administrateurs sont stockées dans le dossier `/data/ssh` de SMC.

Pour ajouter une clé SSH vous permettant de vous connecter à SMC :

1. Assurez-vous que vous possédez le droit d'accès à SMC en SSH dans votre profil. Pour plus d'informations, reportez-vous à la section Gérer les droits des administrateurs en tant que super administrateur.
2. Sur votre poste, copiez votre clé SSH publique.
3. Connectez-vous en SSH à SMC avec votre mot de passe.
4. Créez le fichier `/data/ssh/authorized_key.<user-name-smc>`. Remplacez <user-

name-smc> par votre identifiant tel que défini dans votre profil SMC.

5. Collez votre clé publique dans le fichier que vous venez de créer.

Vous pouvez maintenant vous connecter à SMC via SSH.

Si le serveur SMC est hébergé dans le cloud d'Amazon Web Services, veuillez suivre la procédure Créer une paire de clés dans la console de gestion AWS pour l'accès SSH dans le *Guide d'installation* pour la génération de la paire de clés.

14. Activer et gérer l'API publique de SMC

SMC dispose d'une API REST standard permettant d'utiliser et d'interroger vos serveurs SMC via vos propres outils d'orchestration.

Toutes les fonctionnalités de SMC ne sont pas encore disponibles dans l'API publique. Celle-ci est enrichie au fur et à mesure des versions.

Par défaut, l'API publique n'est pas activée. Seul le super administrateur de SMC peut l'activer.

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

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

Pour faciliter l'utilisation de l'API, une documentation OpenAPI est accessible sur le serveur SMC via l'adresse *https://<@IP de SMC>/docs/papi* ou via le lien affiché dans l'interface web de SMC.

Vous pouvez réaliser des appels API directement depuis la documentation. Cependant certaines actions ne sont pas recommandées en raison de limitations de performance (par exemple récupérer plusieurs milliers de règles via la route "GET /papi/v1/firewalls/{uuidd0rName}/filter-policy"). Pour ce type d'action, nous vous recommandons d'utiliser votre propre outil d'orchestration.

La documentation est également disponible en version "lecture seule" sur le site de la Documentation technique Stormshield.

NOTE
En cas d'utilisation intensive de l'API, c'est-à-dire plusieurs requêtes en écriture dans un délai de quelques secondes, alors que d'autres utilisateurs utilisent l'interface web d'administration en même temps, les performances de SMC peuvent être impactées. Certaines requêtes pourraient ne pas aboutir.
De même, si vous planifiez une utilisation intensive régulière, nous vous recommandons de désactiver la vérification de la cohérence de la configuration pour ne pas impacter les performances de SMC. Pour plus d'informations, reportez-vous à la section Vérifier la cohérence de la configuration.

14.1 Activer l'API publique

L'API publique de SMC est désactivée par défaut.

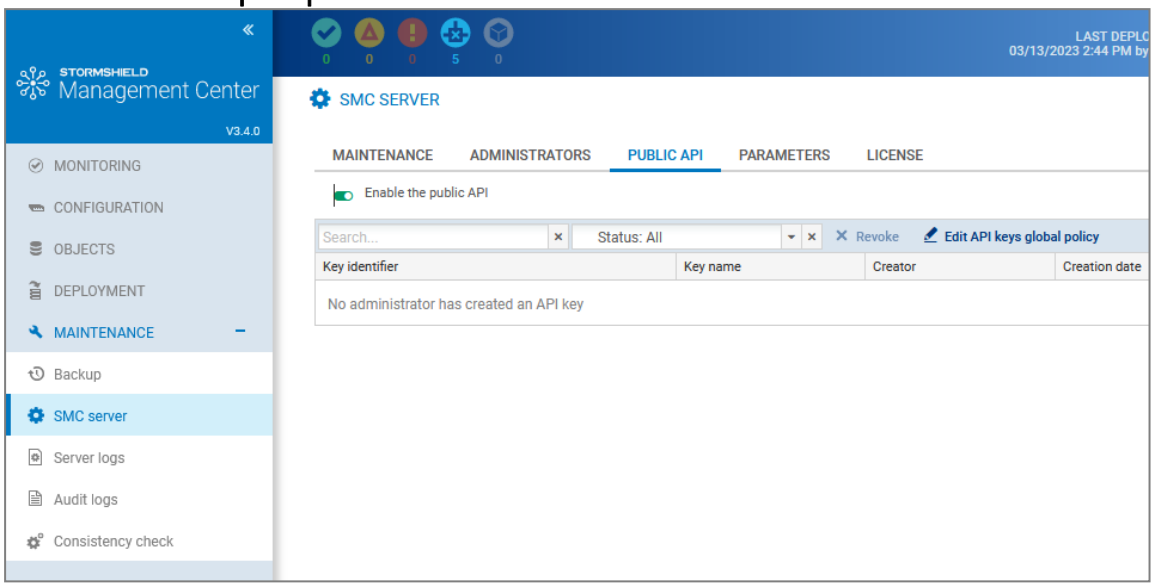
Seul le super administrateur a le droit de l'activer et de la désactiver depuis l'interface web d'administration de SMC.

Lorsque l'API publique est activée :

- l'accès aux routes de l'API est autorisé,
- l'accès à la documentation de l'API est autorisé,
- le super administrateur peut accorder le droit de créer et révoquer des clés API aux autres administrateurs,
- les administrateurs possédant le droit peuvent créer et révoquer des clés API.

Pour activer l'API publique :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **API publique**,
2. Cochez **Activer l'API publique**.



L'onglet **API publique** affiche les clés API créées par les autres administrateurs. Le super administrateur ne peut pas créer de clé API, mais il peut les révoquer. Pour plus d'informations sur la révocation des clés, reportez-vous à la section Révoquer des clés API.

14.2 Autoriser les administrateurs à créer et révoquer des clés API

Une clé API est nécessaire pour être authentifié sur l'API publique. Les administrateurs créent les clés API dans l'interface web d'administration de SMC. Ils choisissent une utilisation lecture/écriture ou lecture seule pour les clés, ainsi qu'une date d'expiration. Pour en savoir plus sur la création des clés, reportez-vous à la section Créer des clés API.

Les clés API créées doivent être ajoutées dans l'en-tête *Authorization* de chaque requête API.

EXEMPLE DE REQUÊTE API
En ligne de commande : `curl -H "Authorization: Bearer <API_KEY>" https://<IP_SMC>/api/v1/firewalls`

Le droit de créer et révoquer des clés API est accordé par le super administrateur, dans le profil des administrateurs.

NOTE
Le super administrateur ne peut pas créer de clé API.

Pour accorder à un administrateur le droit de créer et révoquer des clés API :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **Administrateurs**,
2. Double-cliquez sur le profil d'un administrateur,
3. Cochez **Création/Révocation de clés API** dans la section **Droits d'accès**.

Cette option est grisée si l'API publique est désactivée.

14.3 Modifier la politique globale des clés API

Le super administrateur a la possibilité de définir une période de validité par défaut pour les clés API. Lorsqu'un autre administrateur crée une clé, la période de validité définie par le super administrateur est donc proposée par défaut dans le champ **Date d'expiration**, et l'administrateur peut modifier cette date.

Pour modifier la politique globale des clés API :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **API publique**,
2. Cliquez sur **Modifier la politique globale des clés API**.
3. Définissez la période de validité proposée par défaut aux administrateurs lorsqu'ils créent une clé et appliquez. Celle-ci ne peut excéder 25 ans.

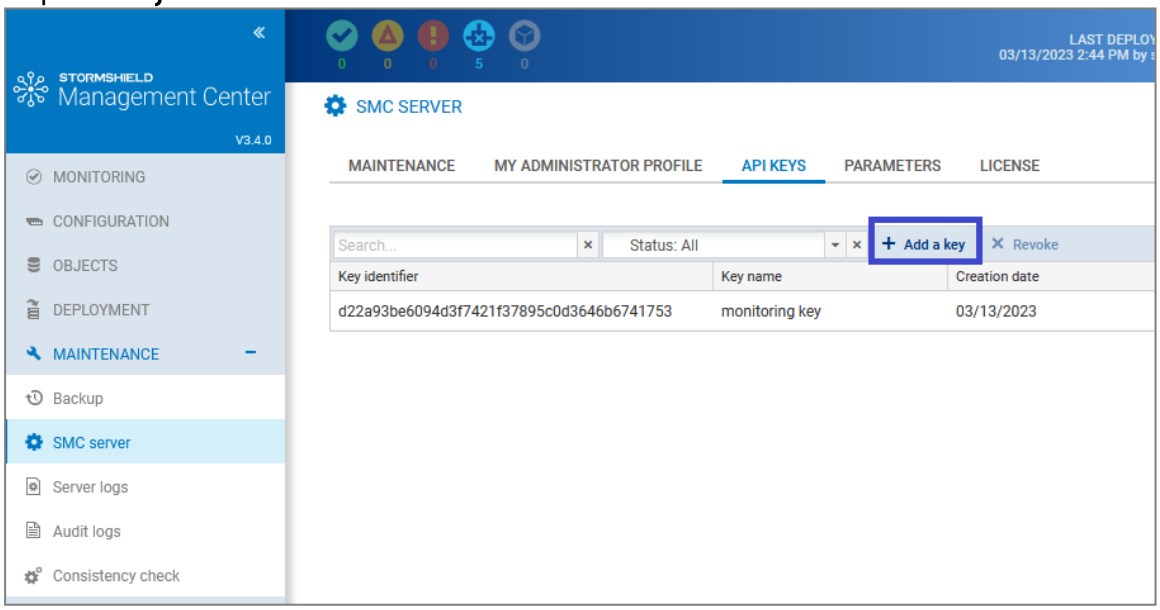
14.4 Créer des clés API

Les administrateurs possédant le droit **Création/Révocation de clés API** peuvent créer des clés API à utiliser pour l'authentification sur l'API publique. Pour en savoir plus sur ce droit, reportez-vous à la section Autoriser les administrateurs à créer et révoquer des clés API.

Ces clés possèdent un identifiant, un nom, une date d'expiration et une utilisation lecture/écriture ou lecture seule. Elles sont nécessaires pour chaque requête de l'API publique.

Pour créer une clé :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **Clés API**. Il liste les clés déjà créées et leurs informations.
2. Cliquez sur **Ajouter une clé**.



3. Entrez un nom et une date d'expiration. La période de validité par défaut est définie par le super administrateur. Pour plus d'informations, reportez-vous à la section Modifier la politique globale des clés API.
4. Dans le champ **Utilisation**, sélectionnez l'option souhaitée. Vous ne pouvez pas sélectionner l'utilisation **Écriture** si vous-même ne possédez pas ce droit sur SMC en tant qu'administrateur.
5. Lorsque vous cliquez sur **Appliquer**, la clé n'est pas enregistrée en base de données. Vous devez la copier et la stocker en sécurité car elle ne sera plus disponible par la suite.

Une clé API peut être utilisée dans la documentation de l'API pour tester les requêtes :

1. Cliquez sur le lien **Voir la documentation API** dans l'onglet **Clés API** depuis la vue Administrateur ou dans l'onglet **API publique** depuis la vue Super administrateur.
2. Cliquez sur le bouton

.
3. Entrez la clé API dans le champ **Value**.
4. Cliquez sur **Authorize** puis sur **Close**.

Lorsque le profil d'un administrateur de SMC est supprimé, les clés API qui lui sont associées sont automatiquement supprimées, si elles ont été révoquées auparavant. Pour plus d'informations sur la révocation, reportez-vous à la section suivante.

14.5 Révoquer des clés API

Le super administrateur peut révoquer toutes les clés API et les administrateurs peuvent révoquer les clés API qu'ils ont créées eux-mêmes. Lorsque les clés API sont révoquées, vous ne pouvez plus les utiliser pour faire des requêtes sur l'API.

En tant que super administrateur :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **API publique**,
2. Sélectionnez la clé à révoquer dans la grille,
3. Cliquez sur **Révoquer**.

Si en tant que super administrateur, vous souhaitez supprimer le profil d'un administrateur, vous devez révoquer les clés API qui lui sont associées auparavant. Il n'est pas possible de supprimer un profil si l'administrateur possède des clés actives.

De même, vous ne pouvez pas retirer le droit **Lecture/Écriture SMC** d'un administrateur si celui-ci possède des clés API actives et avec l'utilisation **Lecture/Écriture**. Vous devez auparavant révoquer les clés concernées.

En tant qu'administrateur :

1. Dans le menu **Maintenance** > **Serveur SMC**, affichez l'onglet **Clés API**,
2. Sélectionnez la clé à révoquer dans la grille,
3. Cliquez sur **Révoquer**.

14.6 Personnaliser le port d'écoute de l'API publique

Par défaut, l'API publique et sa documentation utilisent le port 443.

Vous pouvez modifier le port par défaut à l'aide de la variable d'environnement SMC_PUBLIC_API_PORT_INT :

1. Connectez-vous au serveur SMC via la console de votre hyperviseur ou en SSH.
2. Dans le fichier **/data/config/fwadmin-env.conf.local**, ajoutez la variable d'environnement `SMC_PUBLIC_API_PORT_INT="portNumber"`.
3. Redémarrez le serveur avec la commande `nrestart smc`.

15. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

Annexe A. Détails des commandes smc-xxx

Cette section présente la liste des commandes propres à SMC utilisables dans l'interface de ligne de commande pour administrer le serveur. Pour savoir comment se connecter à l'interface de ligne de commande, reportez-vous à la section Se connecter à l'interface de ligne de commande.

D'autres commandes smc-xxx existent et ne sont pas mentionnées dans cette liste car elles sont destinées au fonctionnement interne du serveur uniquement.

Les commandes smc-xxx remplacent les commandes fwadmin-xxx utilisées en versions 2.5 et antérieures. Celles-ci sont toujours disponibles et fonctionnelles mais seront retirées dans les versions futures.

Commande	Action
`smc-config-backup`	Sauvegarder la configuration du serveur SMC. Voir section Sauvegarder la configuration du serveur en ligne de commande.
`smc-config-restore`	Restaurer la configuration du serveur SMC. Voir section Restaurer la configuration du serveur en ligne de commande.
`smc-date-time`	Afficher et configurer les date et heure du système ainsi que le fuseau horaire. Voir section Modifier le fuseau horaire et la date du serveur SMC.
`smc-deploy`	Déployer la configuration sur les firewalls SNS. Voir section Déployer une configuration sur des firewalls.
`smc-diag`	Télécharger un rapport de diagnostic du serveur SMC. Voir section Générer un rapport de diagnostic du serveur
`smc-export-routes`	Exporter dans un fichier CSV les routes statiques, de retour et par défaut des firewalls en version 4.2.4 minimum, et pour lesquels la gestion de la configuration du réseau est activée dans SMC. Voir section Configurer le routage.
`smc-import-firewalls`	Créer des firewalls dans SMC ainsi que leur package de rattachement. Voir section Importer des firewalls SNS depuis un fichier CSV.
`smc-import-routes`	Importer les routes pour les firewalls en version 4.2.4 minimum, et pour lesquels la gestion de la configuration du réseau est activée dans SMC. Voir section Configurer le routage.
`smc-gen-autosigned-cert`	Réinitialiser le certificat présenté par l'interface web d'administration du serveur SMC. Voir section Personnaliser le certificat de l'interface web du serveur SMC.
`smc-import-crl`	Importer une liste de révocation de certificats (CRL). La CRL est automatiquement associée à l'autorité de certification l'ayant signée.
`smc-import-objects`	Importer des objets provenant d'un export de firewall au format CSV. Voir section Importer des objets.
`smc-import-rules`	Importer les règles de filtrage et de translation, et les objets qui dépendent de ces règles, à partir de l'export des règles d'un firewall SNS au format CSV. Voir section Importer les règles d'un firewall connecté.
`smc-install-certificate`	Installer un certificat P12 sur un firewall donné. Voir section Importer ou déclarer un certificat pour un firewall.
`smc-keyboard`	Modifier la langue du clavier dans l'interface de ligne de commande.
`smc-log-debug`	Activer le mode verbose du serveur SMC.
`smc-logs`	Afficher les journaux de toutes les actions enregistrées sur le serveur SMC. Équivalente à la commande `nlogs`.
`smc-redundancy --secondary <IP_NOEUD_SECONDAIRE>`	Activer la redondance entre deux serveurs SMC. Voir section Mettre en place la redondance de serveurs SMC du *Guide d'installation*.
`smc-reset-ca`	Réinitialise l'autorité de certification interne du serveur SMC. Voir section Réinitialiser l'autorité de certification interne du serveur SMC.
`smc-sns-cli-script`	Exécuter un script CLI SNS sur un ensemble de firewalls. Voir section Exécuter des commandes CLI SNS sur un parc de firewalls.

`smc-syslog-ng`	Configurer le service de journalisation au format Syslog. Voir section Envoyer les journaux de SMC vers un serveur distant au format Syslog.
`smc-update`	Mettre à jour le serveur SMC. Voir section Mettre à jour le serveur SMC .
`smc-version`	Afficher la version du serveur SMC. Voir section Vérifier la version du serveur SMC en ligne de commande.

Annexe B. Détails des variables d'environnement SMC_XXX

Cette section présente la liste des variables d'environnement utilisables sur SMC.

Elles sont paramétrées dans le fichier **/data/config/fwadmin-env.conf.local**. Pour connaître leur rôle, reportez-vous aux sections du *Guide d'administration SMC* ou à la Base de connaissances Stormshield.

D'autres variables existent et ne sont pas mentionnées dans cette liste car elles sont destinées au fonctionnement interne du serveur uniquement.

- Les variables dont le nom se termine par "_ENABLED" doivent contenir des valeurs booléennes "true" ou "false".
- Les variables dont le nom se termine par "_INT" doivent contenir des nombres. Vérifiez que la valeur est cohérente avec l'unité correspondante, le cas échéant.
- Dans tous les autres cas, les valeurs des variables sont considérées comme des chaînes de caractères.
- Si la variable n'est pas définie, la valeur par défaut est la valeur choisie par SMC.

Nom de la variable	Unité	Valeur par défaut	Description
SMC_AUTOBACKUP_EXCLUDE_PRIVATE_KEY_ENABLED		false	Inclut ou exclut les clés privées de la sauvegarde automatique des firewalls. Plus d'informations.
SMC_BULK_RULES_OPERATIONS_TIMEOUT_INT	sec	600 (minimum 30)	Permet de paramétrer le temps d'expiration après un copier/couper/coller des règles de filtrage et de translation.
SMC_CERT_SUBJECT_AS_PEER_LOCALID_ENABLED		false	Active ou désactive le sujet du certificat comme "Local ID" du correspondant.
SMC_CFGCHECK_BEFORE_DEPLOY_ENABLED		true	Active ou désactive la vérification de la cohérence de la configuration au déploiement. Ignorée si la variable SMC_CFGCHECK_ENABLED est activée. Plus d'informations.
SMC_CFGCHECK_ENABLED		true	Active ou désactive la vérification de la cohérence de la configuration. Plus d'informations.
SMC_CFGCHECK_INCOHERENCIES_INT		100	Limite le nombre d'incohérences remontées par le contrôleur de cohérence. Plus d'informations.
SMC_CONFIG_STATUS_CHECK_PERIOD_INT	msec	120000 (minimum 1 - maximum 2147483647)	Définit la fréquence à laquelle SMC vérifie l'état de la configuration sur les firewalls. Plus d'informations.
SMC_CSV_DELIMITER		,	Définit le caractère délimiteur utilisé pour tous les exports et imports de fichiers *.csv*. Plus d'informations.

SMC_DECBACKUP_DIR		/opt/stormshield/security	Spécifie le chemin du fichier binaire *decbackup*.
SMC_DEPLOYMENT_ROLLBACK_CHECK_DONE_TIMEOUT_INT	msec	900000	Définit le temps d'attente de réception d'une réponse du firewall dans le cas où SMC a déployé une configuration qui a déconnecté le firewall et où celui-ci doit restaurer sa précédente configuration.
SMC_DEPLOYMENT_TIMEOUT_BEFORE_ROLLBACK_INT	sec	30 (minimum 3600 - maximum 2147483647)	Définit le délai pendant lequel le firewall essaie de rétablir la connexion avec SMC après un déploiement de configuration. Passé ce délai, la configuration précédente du firewall est restaurée. Plus d'informations.
SMC_FW_CONNECTION_TIMEOUT_INT	sec	60	Dans le cadre de connexions VPN IPsec, permet de définir le délai maximum de maintien de la connexion des tunnels entre SMC et les firewalls (délai de *KeepAlive*). Plus d'informations.
SMC_FW_DEPLOYMENT_ROLLBACK_ENABLED		true	Active ou désactive la fonctionnalité de préservation de la connexion lors d'un déploiement de configuration. Plus d'informations.
SMC_FW_DEPLOYMENT_TIMEOUT_INT	sec	300	Définit le temps d'attente maximal pour la collecte des informations de déploiement.
SMC_FW_DEPLOYMENT_VPN_PEER_INACTIVITY_INT	sec	0	Permet de détecter l'inactivité d'un tunnel VPN dans le sens entrant et dans le sens sortant.
SMC_FW_LICENSE_CRITICAL_INT	days	0	Définit le délai d'avertissement de l'expiration prochaine des options de licence. Affiche l'état **Critique**. Plus d'informations.
SMC_FW_LICENSE_WARNING_INT	days	0	Définit le délai d'avertissement de l'expiration prochaine des options de licence. Affiche l'état **Non critique**. Plus d'informations.
SMC_FW_TPM_ENABLED		true	Active ou désactive la protection des certificats par TPM.
SMC_GETSA_POLLING_PERIOD_INT	msec	30000	Définit la fréquence d'exécution de la commande MONITOR GETSA.
SMC_GETSPD_POLLING_PERIOD_INT	msec	30000	Définit la fréquence d'exécution de la commande MONITOR GETSPD.
SMC_HAINFO_POLLING_PERIOD_INT	msec	30000 (minimum 1)	Définit la fréquence d'exécution de la commande HA INFO.

SMC_HASYNC_ON_DESYNCHRO_ENABLED		true	Active ou désactive la synchronisation automatique d'un cluster en Haute Disponibilité. Plus d'informations.
SMC_IMPORT_RULES_FROM_SNS_TIMEOUT_INT	sec	600 (minimum 30)	Définit le temps d'attente maximal pour la récupération des règles locales et globales d'un firewall connecté à SMC.
SMC_LDAP_FIELD_NAME_DN			Dans le cas où des utilisateurs proviennent d'un serveur LDAP, permet de choisir les attributs LDAP correspondant au champ **DN LDAP** de la fenêtre d'ajout d'un administrateur. Par défaut le champ correspond aux attributs *distinguishedName,dn,entryDN*. Plus d'informations.
SMC_LDAP_FIELD_NAME_LOGIN			Dans le cas où des utilisateurs proviennent d'un serveur LDAP, permet de choisir l'attribut LDAP correspondant au champ **Identifiant** de la fenêtre d'ajout d'un administrateur. Par défaut le champ correspond à l'attribut *sAMAccountName* ou *uid*. Plus d'informations.
SMC_LDAP_FIELD_NAME_MEMBEROF			Dans le cas où des utilisateurs proviennent d'un serveur LDAP, permet de choisir l'attribut LDAP correspondant aux groupes d'utilisateurs. Par défaut le champ correspond à l'attribut *memberOf*. Plus d'informations.
SMC_LOCK_SERIAL_NUMBER_ENABLED		true	Active ou désactive la vérification du numéro de série du firewall lors de sa connexion à SMC. Plus d'informations.
SMC_MESSAGING_RESPONSE_DEFAULT_TIMEOUT_INT	sec	120	Définit le temps d'attente d'une réponse du firewall à un message websocket envoyé par SMC. Cette variable est surchargée par la variable SMC_PROXY_RESPONSE_TIMEOUT_INT pour les commandes Serverd.
SMC_MONITOR_ROUTE_POLLING_PERIOD_INT	msec	60000 (minimum 60000)	Définit la fréquence de surveillance des routes.
SMC_MONITOR_STAT_POLLING_PERIOD_INT	msec	60000 (minimum 1 - maximum 2147483647)	Définit la fréquence de surveillance de l'utilisation du processeur, de la mémoire, de l'espace disque et d'autres informations du firewall.
SMC_PROXY_RESPONSE_TIMEOUT_INT	sec	300	Définit le temps d'attente maximal d'une réponse d'un firewall pour des commandes Serverd exécutées par SMC. Plus d'informations.
SMC_RADIUS_NAS_IDENTIFIER			Permet de définir l'attribut Radius NAS-ID.

SMC_RADIUS_NAS_IP_ADDRESS			Permet de définir l'attribut Radius NAS-IP-Address.
SMC_SNS_CERTS_PROBE_EXPIRATION_INT	days	30 (minimum 1)	Permet de définir le délai d'avertissement de l'expiration prochaine du certificat d'un firewall. Plus d'informations.
SMC_SNS_CLI_ATTACHMENTS_DIR		/data/tmp/sns-cli/input	Permet de modifier le dossier par défaut de stockage des pièces jointes à un script CLI SNS. Plus d'informations.
SMC_SNS_CLI_CSV_DELIMITER		;	Permet de définir le caractère délimiteur utilisé dans les fichiers *.csv* attachés aux scripts CLI SNS exécutés en ligne de commande. Plus d'informations.
SMC_SNS_CLI_OUTPUT_DIR		/data/tmp/sns-cli/output	Permet de modifier le dossier par défaut de réception des fichiers générés par des scripts CLI SNS. Plus d'informations.
SMC_SNS_CLI_SCRIPT_MAX_UPLOAD_SIZE_INT	bytes	2097152 (minimum 1)	Permet de paramétrer une limite de taille des fichiers de scripts CLI SNS. Plus d'informations.
SMC_SNS_CLI_STEP_TIMEOUT_INT	sec	120	Permet de définir le temps d'attente maximal pour la synchronisation du nœud secondaire après l'exécution d'un script CLI SNS.
SMC_SNS_DEPLOYMENT_ROLLBACK_TIMEOUT_INT	sec	180 (maximum 2147483647)	Permet de définir le temps d'attente maximal entre la restauration de la configuration et la reconnexion au serveur SMC en cas de problème lors d'un déploiement de configuration. Plus d'informations.
SMC_SNS_UPDATE_HA_LINK_TIMEOUT_INT	sec	1800	Permet de définir le temps d'attente maximal pour rétablir le lien HA lorsque le nœud secondaire redémarre après la mise à jour du firmware. La fréquence de vérification est définie par la variable SMC_HAINFO_POLLING_PERIOD_INT.
SMC_SNS_UPDATE_MAX_KEEP_DAYS_INT	days	14	Permet de modifier la durée de stockage des fichiers de mise à jour des firewalls sur SMC. Plus d'informations.
SMC_SNS_UPDATE_SYSTEM_CLONE_TIMEOUT_INT	sec	1800	Lors de la mise à jour des firewalls, permet de configurer la durée maximum pour réaliser une sauvegarde de partition active du système du firewall. Plus d'informations.
SMC_SYSTEM_PROP_POLLING_PERIOD_INT	msec	3600000 (minimum 1 - maximum 2147483647)	Permet de définir la fréquence de récupération des informations du firewall. Par exemple, le numéro de série ou le modèle de firewall.
SMC_UI_PORT_INT		443	Permet de personnaliser le port de l'interface web d'administration de SMC.

SMC_UI_SERVER_CERT_PATH		/etc/certs/uiserver	Permet de personnaliser le certificat de l'interface web d'administration de SMC. Plus d'informations.
SMC_PUBLIC_API_PORT_INT		443	Permet de personnaliser le port d'écoute de l'API publique de SMC. Plus d'informations.
SMC_VPN_MESH_ROUTE_BASED_MAX_PEERS_INT		50	Permet de définir le nombre maximal de correspondants dans une topologie VPN par route en maillage. Plus d'informations.
SMC_WARNING_MODIFICATION_ENABLED		false	Permet d'activer l'avertissement de modification de la configuration par un autre administrateur. Plus d'informations.

Annexe C. Compatibilité SMC/firewalls SNS

Le serveur SMC permet d'administrer les firewalls SNS à partir de la version 4.3.

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

Fonctionnalité/Objet	Version de SMC	Version minimum du firewall SNS requise
Gestion des interfaces réseau (en lecture seule)	3.0	3.7.0 [1]
Gestion des interfaces réseau (en écriture)	3.0.1	4.2.3
Gestion du mode "Diffusion Restreinte (DR)"	3.1	4.3.21 LTSB ou 4.7
Point de distribution Active Update	3.1	4.3.3
Support de versions différentes de IKE pour un même firewall	3.1.3	3.7.0
Gestion du routage (en lecture seule)	3.2	3.7.0
Gestion du routage (en écriture)	3.2	4.2.3
Support du SD-WAN	3.2	4.3.3
Gestion des interfaces IPsec virtuelles (VTI) et des topologies VPN par route	3.4	4.2.3
Champ **Adresse IPv4 de destination** des VTI	3.9	5.1.0
Filtrage par services Web	3.4	4.4
Configuration de la QoS	3.6	4.3.15 LTSB ou 4.5.3
Gestion du routage dynamique avec BIRD v2	3.6	4.8.1

NOTE
Pour pouvoir déployer des topologies VPN par route ou des interfaces IPsec virtuelles (VTI) sur des firewalls SNS en version 5.1.0 ou supérieures, vous devez utiliser un serveur SMC de la version 3.9 ou supérieure. Avant toute mise à jour, veuillez consulter la section Préconisations des *Notes de version*.

[1] À partir de SMC version 3.6, la compatibilité avec les versions 3.x de SNS n'est plus testée.

documentation@stormshield.eu

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

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.