GUIDE

STORMSHIELD NETWORK SECURITY

RECOMMANDATIONS POUR UNE CONFIGURATION SÉCURISÉE D'UN PARE-FEU SNS

Version 4.3 LTSB

Dernière mise à jour du document : 4 mars 2024

Référence : sns-fr-guide_anssi_recommandations_configuration-v4.3-LTSB

Table des matières

Informations

Ce guide est basé sur le document présentant les recommandations pour une configuration sécurisée d'un pare-feu SNS en version 3.7.17 LTSB. Son contenu a été modifié par Stormshield afin de tenir compte des nouveautés de la version SNS 4.3 LTSB.

Le document d'origine **Recommandations pour une configuration sécurisée d'un pare-feu SNS en version 3.7.17 LTSB** a été rédigé par l'ANSSI et est disponible sur le site **cyber.gouv.fr**. Il a été publié sur le site de *Documentation Technique Stormshield* avec l'accord de l'ANSSI.

Historique des modifications

Date	Description
4 mars 2024	- Nouveau document *Dernière mise à jour du document d'origine de l'ANSSI : 2 avril 2021*

1. Avant de commencer

Bienvenue dans le guide présentant les recommandations pour une configuration sécurisée d'un pare-feu Stormshield Network Security (SNS) en version 4.3 LTSB.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, il n'est pas possible de garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

1.1 Objectif

Ce document a pour objectif de présenter les bonnes pratiques relatives au déploiement sécurisé des pare-feux SNS, en version physique ou en version virtuelle (les contraintes liées à la virtualisation ainsi que les bonnes pratiques sont expliquées dans le guide **Problématiques de sécurité associées à la virtualisation des systèmes d'information**).

Les recommandations détaillées dans ce document s'appliquent aux pare-feux SNS. Celles concernant les configurations sur le serveur SMC ont pour but de sécuriser le déploiement des pare-feux SNS. L'ensemble des recommandations traitent des fonctions :

- D'administration,
- De filtrage,
- De chiffrement IPsec,
- De supervision,
- De sauvegarde,
- De journalisation.

Ce document vient en complément des publications **Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu** et **Recommandations relatives à l'interconnexion d'un système d'information à Internet** de l'ANSSI.

INFORMATION
Les fonctionnalités présentées dans ce guide ne se limitent pas à celles évaluées lors de la qualification du produit. Les fonctionnalités non évaluées sont précisées dans le corps du présent document à l'aide de la formule "*Cette fonctionnalité n'est pas couverte par la cible de sécurité.*".
L'utilisation des fonctionnalités non évaluées nécessite donc une analyse de risque complémentaire qui doit être portée auprès de la commission d'homologation du SI. C'est ensuite à l'autorité d'homologation d'accepter les risques résiduels ou de mettre en place les protections adaptées.
Les fonctionnalités du serveur SMC ne sont pas couvertes par la cible de sécurité.

1.2 Convention de lecture

Pour certaines recommandations, il est proposé plusieurs solutions d'architecture qui se distinguent par leur niveau de sécurité. Le lecteur a ainsi la possibilité de choisir une solution en adéquation avec ses besoins de sécurité. En outre, dans une démarche itérative de

sécurisation, ces différents niveaux de sécurité proposés peuvent permettre de fixer une cible d'architecture et d'identifier les étapes pour l'atteindre. Ainsi, les recommandations sont présentées de la manière suivante :

- **Rx** constitue une recommandation à l'état de l'art,
- **Rx+** constitue une recommandation alternative à Rx, d'un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information,
- **Rx-** constitue une recommandation alternative à Rx, d'un niveau de sécurité moindre.

À côté du numéro de la recommandation, il est également précisé si cette dernière s'applique aux pare-feux SNS, au serveur SMC, ou les deux (par exemple **Rx | SNS-SMC**).

1.3 Modes de configuration des pare-feux SNS

Les recommandations de configuration détaillées dans ce document peuvent être mises en pratique par le biais de différentes manières :

- Côté pare-feu SNS :
  - Via l'interface web d'administration du pare-feu SNS,
  - Via l'interface de ligne de commande SNS par SSH.
- Côté serveur SMC :
  - Via l'accès direct aux pare-feux SNS sans renouveler l'authentification. Cet accès permet de gérer l'ensemble de la configuration d'un pare-feu SNS,
  - Via l'interface web d'administration du serveur SMC, pour configurer certaines fonctionnalités sur plusieurs pare-feux SNS,
  - Via les scripts CLI SNS, pour automatiser des tâches sur plusieurs pare-feux SNS.

Dans ce document, les recommandations de configuration s'appliquent à l'interface web d'administration des pare-feux SNS et quand cela est possible à l'interface web d'administration du serveur SMC.

1.4 Dénominations

Les sigles présentés dans cette section, en rapport avec les pare-feux SNS, sont utilisés tout au long du document.

AC	Autorité de Certification. Équivalent de CA en anglais (*Certificate Authority*).
ASQ	*Active Security Qualification*, moteur d'analyse des pare-feux SNS.
CRL	*Certificate Revocation List*, liste de révocation de certificats.
CRLDP	*CRL Distribution Point*, point de distribution de CRL.
DNS	*Domain Name System*, service effectuant la traduction entre des noms de domaines et les adresses IP associées.
DR	Diffusion Restreinte.
DSCP	*Differentiated Services Code Point*, champ de l'entête d'un paquet IP utilisé pour différencier et prioriser les services lors d'une congestion.
FQDN	*Fully Qualified Domain Name*, nom de domaine renseignant l'ensemble des domaines à traverser pour joindre la ressource.

FTP	*File Transfer Protocol*, protocole de transfert de fichiers.
HTTP	*HyperText Transfer Protocol*, protocole de transfert hypertexte.
HTTPS	*HTTP Secure*, évolution sécurisée du HTTP grâce à la mise en place d'un canal SSL/TLS.
IDS	*Intrusion Detection System*, mécanisme permettant de détecter un trafic malicieux et de lever une alarme.
IGC	Infrastructure de Gestion de Clés. Équivalent de PKI en anglais (*Public Key Infrastructure*).
IKE	*Internet Key Exchange*, protocole d'échange de clé authentifiant entre correspondants.
IP	*Internet Protocol*, protocole de communication de réseaux informatiques.
IPS	*Intrusion Prevention System*, mécanisme permettant de détecter un trafic malicieux et de le bloquer.
IPsec	*Internet Protocol Security*, cadre de standards permettant de sécuriser des communications IP.
LDAP	*Lightweight Directory Access Protocol*, protocole d'accès à des services d'annuaire.
LDAPS	*LDAP Secure*, évolution sécurisée du LDAP grâce à la mise en place d'un canal SSL/TLS.
MIB	*Management Information Base*, ensemble structuré de ressources utilisées en supervision.
NSRPC	*NetAsq Secure Remote Protocol Client*, protocole d'administration Stormshield utilisant le port TCP 1300. Il est implémenté par un serveur permettant d'administrer le pare-feu SNS en ligne de commande.
OID	*Object IDentifier*, identifiant de ressource représenté par une suite de nombres entiers.
PKI	*Public Key Infrastructure*. Équivalent de IGC en français (Infrastructure de Gestion de Clés).
QoS	*Quality of Service*, qualité de service.
RGS	Référentiel général de sécurité, cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.
SI	Système d'Information.
SIEM	*Security Information and Event Management*, gestionnaire d'informations de sécurité et d'évènements.
SMC	*Stormshield Management Center*, serveur virtuel d'administration et de supervision centralisée des pare-feux SNS.
SNMP	*Simple Network Management Protocol*, protocole de gestion et de supervision à distance d'équipements.
SNS	*Stormshield Network Security*.
SSH	*Secure SHell*, protocole de communication sécurisé.
SSL	*Secure Sockets Layer*, protocole de sécurisation d'échanges.
TCP	*Transport Control Protocol*, protocole de transport.
TLS	*Transport Layer Security*, évolution de SSL.
UAC	*User Access Control*, mécanisme de contrôle d'accès par utilisateur.

URL	*Uniform Ressource Locator*, chaîne de caractères utilisée pour adresser une ressource sur un réseau.
VLAN	*Virtual Local Area Network*, réseau de commutation logique.
VPN	*Virtual Private Network*, système permettant de créer un tunnel de communication entre deux équipements.

2. Administration du pare-feu SNS

2.1 Comptes administrateurs

2.1.1 Utilisation de comptes nominatifs

Il est important de pouvoir assurer la traçabilité de l'ensemble des actions réalisées sur le pare-feu SNS et sur le serveur SMC (voir le chapitre Journalisation pour les recommandations liées à la journalisation) afin de s'assurer qu'elles ont été menées par un administrateur légitime et autorisé.

R1 | SNS-SMC | Utiliser des comptes nominatifs
Il est recommandé d'utiliser des comptes nominatifs pour les administrateurs, quels que soient leurs privilèges, lors d'une connexion à l'interface web, au serveur NSRPC ou en SSH.

Certaines opérations exceptionnelles sont réalisables avec un compte nominatif depuis l'interface web, la console locale ou par SSH, comme la modification manuelle de fichiers de configuration.

Un compte administrateur local non nominatif (admin) est présent sur le pare-feu SNS et peut également réaliser ces actions. Toutefois, seul ce compte peut modifier les droits accordés aux administrateurs.

Sur le serveur SMC, certaines opérations avancées ou de maintenance ne sont disponibles qu'en ligne de commande (via SSH ou le mode console).

R2 | SNS-SMC | Protéger le compte administrateur local
Le compte administrateur présent sur le pare-feu SNS doit disposer d'un mot de passe fort (se référer au guide Recommandations relatives à l'authentification multifacteur et aux mots de passe) et ne doit être utilisé qu'afin d'établir l'accès aux comptes nominatifs. Son mot de passe doit être conservé au coffre-fort et son utilisation doit être supervisée et limitée à un ensemble déterminé de personnes.

R3 | SNS | Limiter l'administration par SSH
Le service SSH doit être limité qu'aux seuls comptes administrateurs nécessaires et ne doit être activé qu'à titre exceptionnel à partir du menu **Configuration > Système > Configuration > Administration du Firewall**.

R4 | SNS | Utiliser une authentification par clé SSH
Lorsque l'accès SSH est activé à titre exceptionnel, il est recommandé d'utiliser une authentification par clé SSH conformément au guide Recommandations pour un usage sécurisé d'(Open)SSH.

2.1.2 Authentification locale

Les pare-feux SNS offrent la possibilité de créer un annuaire interne (menu **Configuration > Utilisateurs > Configuration des annuaires**) permettant une authentification locale. Cette authentification est utilisée pour la connexion aux serveurs web, NSRPC et SSH. Dans ce cas, le

pare-feu SNS stocke les éventuels mots de passe ou leurs dérivés. Une compromission du pare-feu SNS compromet alors ces éléments secrets. Par ailleurs, il est également possible de s'authentifier sur l'interface web d'administration à l'aide d'un certificat. Leur utilisation permet de ne stocker que des données publiques au sein du pare-feu SNS. Les recommandations associées à l'utilisation de certificats sur des pare-feux SNS sont présentées dans le chapitre Certificats et PKI. En revanche, l'accès au serveur NSRPC n'autorise qu'une authentification par mot de passe.

R5 | SNS | Authentifier localement par certificat
Si l'authentification locale est utilisée, il est recommandé d'utiliser des certificats utilisateurs nominatifs comme moyen d'authentification à l'interface web d'un pare-feu SNS.

Les autorités de certification doivent alors avoir été ajoutées dans le menu **Configuration > Objets > Certificats et PKI**. La méthode d'authentification *Certificat SSL* doit avoir été configurée dans le menu **Configuration > Utilisateurs > Authentification > Méthodes disponibles** avec les autorités souhaitées.

R6 | SNS | Définir une politique de mots de passe adaptée
Si un accès au serveur NSRPC est nécessaire à un administrateur, son mot de passe doit suivre une politique conforme au guide Recommandations relatives à l'authentification multifacteur et aux mots de passe. La configuration se fait dans le menu **Configuration > Système > Configuration > Configuration générale**.

2.1.3 Authentification centralisée

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Les solutions SNS et SMC supportent l'utilisation d'une solution d'authentification centralisée permettant la gestion des utilisateurs sur un pare-feu SNS distant. L'utilisation d'une telle solution vise à limiter le nombre de données sensibles stockées localement et de simplifier les procédures d'administration. Dans le cas de l'utilisation d'un annuaire externe, la configuration du pare-feu SNS est détaillée dans le chapitre Utilisation d'un annuaire externe.

R7 | SNS | Dédier un annuaire externe aux administrateurs
Conformément au guide Recommandations relatives à l'administration sécurisée des systèmes d'information, il est recommandé d'utiliser un annuaire externe et dédié à l'administration pour authentifier les administrateurs.

R8 | SNS | Utiliser un compte d'accès restreint et sécurisé
Le compte utilisé par le pare-feu SNS pour accéder à la solution d'authentification centralisée doit être limité à cette fonction, dédié au pare-feu SNS et faire l'objet d'attentions particulières en termes de configuration. En particulier, il ne doit avoir que des droits en lecture afin d'éviter toute modification des données de l'annuaire à partir du pare-feu SNS.

2.1.4 Droits d'accès

Un pare-feu SNS offre de nombreuses fonctionnalités : filtrage, tunnels VPN, etc. Un administrateur dédié à une tâche précise ne doit avoir qu'un périmètre d'action limité. Cela permet de cloisonner les risques en cas de compromission de son compte, ainsi que limiter les

modifications involontaires de configuration. Afin de réduire les risques liés à une compromission d'un compte d'administration, voire d'un pare-feu SNS, il est recommandé, dans l'idéal, de dédier un pare-feu SNS pour chaque fonction et un compte d'administration afférent.

Si la mutualisation de plusieurs pare-feux SNS est impérative, il convient alors de créer des comptes d'administration pour chaque fonctionnalité comme préconisé dans le guide Recommandations relatives à l'administration sécurisée des systèmes d'information.

R9 | SNS | Ajuster les droits d'administration au strict nécessaire
Il est recommandé de ne positionner que les droits strictement nécessaires aux tâches des différents administrateurs dans le menu **Configuration > Système > Administrateurs > Administrateurs**.

Il n'est pas possible d'utiliser la valeur d'un attribut de l'annuaire afin de discriminer les différents profils de droits (administrateur complet, administrateur dédié à une fonction, superviseur, etc.). Il est cependant possible de déclarer des groupes d'utilisateurs au sein de l'annuaire et de leur appliquer un profil de droits sur le pare-feu SNS. Chaque groupe doit correspondre à un besoin fonctionnel et bénéficier des droits adaptés sur le pare-feu SNS. L'attribution de droits à un administrateur est alors effectuée par son affectation à un groupe. Cela se réalise dans l'annuaire de manière centralisée.

R10 | SNS-SMC | Utiliser les groupes pour gérer les droits
Il est recommandé d'utiliser les groupes pour gérer les droits d'accès aux pare-feux SNS.

ATTENTION
Seul le compte administrateur non nominatif peut modifier les droits des utilisateurs et groupes d'utilisateurs. Cette action doit donc rester exceptionnelle conformément au chapitre Utilisation de comptes nominatifs.

2.2 Services d'administration

2.2.1 Configuration des adresses IP d'administration

Un accès non restreint aux interfaces d'administration du pare-feu SNS augmente les risques de tentative d'intrusion et de manipulation par un équipement illégitime qui y aurait accès.

R11 | SNS | Définir explicitement les sous-réseaux d'administration
Il est recommandé de définir explicitement les adresses IP ou les sous-réseaux d'administration autorisés à accéder aux interfaces d'administration d'un pare-feu SNS dans le menu **Configuration > Système > Configuration > Administration du Firewall**.

Les adresses IP et les sous-réseaux d'administration doivent être configurés à l'aide d'objets spécifiques, regroupés dans un groupe d'objets. Conformément au chapitre Politique de filtrage, l'utilisation de tels groupes d'objets permet une meilleure gestion des autorisations, en cohérence avec les règles de filtrage.

R12 | SNS | Utiliser un groupe d'objets d'administration
Il est recommandé d'utiliser un groupe d'objets contenant l'ensemble des sous-réseaux et adresses IP autorisés à administrer le pare-feu SNS.

2.2.2 Interface web d'administration dédiée

Une interface web d'administration mutualisée avec le réseau d'opérations augmente le nombre de personnes et d'équipements capables d'accéder à l'interface web d'administration du pare-feu SNS et augmente la charge de trafic que l'interface doit gérer. Le risque de voir l'interface web d'administration attaquée ou injoignable est alors important. De plus, l'utilisation de VLAN ne garantit pas une étanchéité totale entre les réseaux configurés.

R13 | SNS | Dédier une interface Ethernet à l'administration
Il est recommandé d'administrer un pare-feu SNS sur une interface Ethernet dédiée raccordée à un réseau d'administration, également dédié à ces opérations. Le filtrage mis en œuvre devra être le plus restrictif possible.

Le guide Recommandations relatives à l'administration sécurisée des systèmes d'information publié par l'ANSSI détaille les mesures recommandées concernant une administration sécurisée des SI.

2.2.3 Sécurité de l'interface web d'administration

La sécurité de l'interface web d'administration des pare-feux SNS et du serveur SMC participe à leur sécurité en protégeant en confidentialité et en intégrité les flux légitimes d'administration.

Pour le pare-feu SNS, le mode *sslparanoiac* est activé par défaut, imposant l'utilisation de TLS 1.3 ou TLS 1.2 avec des suites cryptographiques robustes. Il est possible de vérifier la configuration du paramétrage TLS de l'interface web d'administration à l'aide de la commande NSRPC `config auth show`. Les suites cryptographiques proposées par défaut sont les suivantes :

```
ECDHE-ECDSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
TLS_AES_128_GCM_SHA256
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_256_GCM_SHA384
```

R14 | SNS | Conserver les suites cryptographiques
Conserver la configuration par défaut des suites cryptographiques permet d'être conforme aux Recommandations de sécurité relatives à TLS de l'ANSSI ainsi qu'à l'annexe B1 du RGS.

R14+ | SNS | Durcir les paramètres TLS de l'interface web d'administration
Il est recommandé de conserver uniquement les suites TLS avec ECDHE comme préconisé par le guide Recommandations de sécurité relatives à TLS.

La restriction des suites cryptographiques peut s'effectuer à l'aide des commandes NSRPC :

```
config auth https cipherlist="ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-
CHACHA20-POLY1305,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-
SHA384"
config auth activate
```

2.2.4 Modification du certificat de l'interface web d'administration

Par défaut, le certificat présenté à l'administrateur lorsqu'il se connecte à l'interface web d'administration d'un pare-feu SNS est un certificat signé par l'AC (Autorité de Certification) Stormshield. Dans le cas du serveur SMC, il s'agit d'un certificat auto-signé. Dans les deux cas, la clé privée utilisée n'est alors pas maîtrisée, ni sur les critères de génération, ni sur l'utilisation qui peut en être faite.

R15 | SNS | Remplacer le certificat de l'interface web
Il est recommandé de remplacer le certificat de l'interface web d'administration par un certificat issu d'une IGC (équivalent de PKI en anglais - *Public Key Infrastructure*) maîtrisée afin de renforcer la sécurité de son accès.
Se référer aux recommandations du RGS, en particulier les annexes **A4** et **B1**.

La configuration du certificat serveur utilisé par l'interface web d'administration du pare-feu SNS se fait à partir du menu **Configuration > Système > Configuration > Administration du Firewall > Configurer le certificat SSL du service**.

INFORMATION
Afin qu'un administrateur puisse authentifier le pare-feu SNS sur lequel il se connecte, la clé publique de l'AC qui a signé le certificat doit être présente dans le magasin de certificats du navigateur utilisé par les administrateurs.

2.2.5 Administration via NSRPC

Dans le cas d'une connexion directe au serveur NSRPC, le pare-feu SNS requiert l'accès en lecture à l'empreinte du mot de passe de l'utilisateur (cette information est nécessaire au bon fonctionnement du protocole d'authentification utilisé). Un détournement de l'accès du pare-feu SNS à l'annuaire peut alors entraîner la compromission de l'ensemble des empreintes des mots de passe stockés. L'empreinte est un élément critique, une attaque par force brute peut compromettre les mots de passe. Il est donc nécessaire de surveiller l'utilisation d'un tel compte dans le système d'information (connexion issue d'un autre équipement, requêtes illégitimes, etc.).

Une console NSRPC est disponible depuis l'interface web d'administration. L'accès à cette console ne nécessite pas d'authentification supplémentaire. L'accès aux empreintes n'est pas nécessaire.

R16 | SNS | Utiliser NSRPC depuis l'interface web d'administration
Il est recommandé d'utiliser les commandes NSRPC uniquement depuis le menu **Configuration > Système > Console CLI** de l'interface web d'administration.

R16 - | SNS | Utiliser des comptes dédiés à la connexion NSRPC directe
Dans le cas d'un accès direct à la console NSRPC, il est recommandé d'utiliser des comptes

dédiés à cet usage, de changer régulièrement leurs mots de passe et d'exposer uniquement les empreintes de ces comptes sur l'annuaire distant.

INFORMATION
Par défaut, les annuaires de type *Active Directory* et *OpenLDAP* n'autorisent pas la lecture des empreintes des mots de passe.

2.2.6 Choix des éléments de localisation

Plusieurs éléments de localisation sont présents sur le pare-feu SNS :

- La langue de l'interface web d'administration, qui peut être choisie sur l'écran de connexion,
- La disposition du clavier de la console, configurable dans le menu **Configuration > Système > Configuration**,
- La langue des traces et des journaux, également configurable dans le menu **Configuration > Système > Configuration**.

La langue des traces et des journaux modifie les messages disponibles dans le menu **Monitoring > Tableau de bord** et dans les fichiers de journalisation locaux et distants. Le choix de cette langue influe sur :

- Leur compréhension par les exploitants,
- Les motifs recherchés par les systèmes de supervision,
- Les recherches effectuées dans la base de connaissance disponible sur le site internet de Stormshield.

L'ensemble des messages existants est répertorié dans le menu **Monitoring > Logs - Journaux d'audit > Évènements système** et leurs traductions sont disponibles sur le pare-feu SNS dans le dossier */usr/Firewall/System/Language/*. Chaque message émissible possède un numéro d'index lié à l'erreur correspondante. Ce numéro est donc identique au sein de l'ensemble des traductions.

R17 | SNS | Unifier la langue des traces et des journaux
Il est recommandé de configurer une langue identique sur l'ensemble des pare-feux SNS pour la langue des traces et journaux. Ceci permet d'en simplifier la lecture et facilite l'intégration dans les outils de supervision.

ATTENTION
Sur le serveur SMC, les journaux ne sont disponibles qu'en anglais. Il est recommandé de configurer les traces et journaux du pare-feu SNS en anglais en cas d'administration via le serveur SMC.

R18 | SNS-SMC | Utiliser une langue comprise par les exploitants
Il est conseillé de configurer un pare-feu SNS dans une langue maîtrisée par les exploitants.

INFORMATION
Le site de Documentation technique de Stormshield est accessible en français et en anglais. La

base de connaissance est accessible depuis l'espace personnel Stormshield uniquement en anglais.

2.3 Option Diffusion Restreinte

En cas d'utilisation d'un pare-feu SNS dans un contexte de sensibilité de niveau "Diffusion Restreinte", des contraintes supplémentaires doivent être appliquées afin de respecter les règles de protection appropriées. Ces contraintes sont détaillées dans la note technique Stormshield VPN IPsec - Mode Diffusion Restreinte.

En particulier, la gestion des primitives cryptographiques matérielles doit être adaptée lorsque le jeu d'instructions du (co)processeur ne fournit pas les garanties suffisantes sur leur utilisation et leur protection (risques d'émission ou de fuite de données). L'utilisation de cette option implique en contrepartie une baisse des performances de chiffrement et de déchiffrement des pare-feux SNS équipés de tels (co)processeurs.

R19 | SNS | Activer l'option Diffusion Restreinte
Il est recommandé d'activer le mode **Diffusion Restreinte** dans le menu **Configuration > Système > Configuration > Configuration générale** lorsque le pare-feu SNS est positionné sur un réseau de cette même sensibilité et que ses fonctions cryptographiques sont exploitées.

R19 | SMC | Activer l'option Diffusion Restreinte
Il est recommandé d'activer le mode **Diffusion Restreinte** sur le serveur SMC dans le menu **Maintenance > Serveur SMC > Paramètres**.

INFORMATION
L'activation du mode **Diffusion Restreinte** sur le serveur SMC entraîne un déploiement automatique destiné à activer le mode **Diffusion Restreinte** sur les pare-feux SNS rattachés au serveur SMC. Une fois activé, il n'est plus possible de rattacher au serveur SMC des pare-feux SNS dont le mode **Diffusion Restreinte** n'a jamais été activé.

3. Configuration réseau

3.1 Désactivation des interfaces non utilisées

La présence d'interfaces réseau inutilisées sur un pare-feu SNS augmente sa surface d'attaque. Une connexion sur une telle interface ne perturbe pas le bon fonctionnement du pare-feu SNS mais pourrait permettre un accès illégitime. De plus, une interface active est utilisable dans les différents menus et augmente le risque d'erreurs de configuration.

R20 | SNS | Désactiver les interfaces non utilisées
Il est recommandé de désactiver les interfaces réseau non utilisées depuis le menu **Configuration > Réseau > Interfaces**.

3.2 Configuration de l'anti-usurpation IP

3.2.1 Principe de l'anti-usurpation IP

L'usurpation IP (*spoofing* en anglais) consiste à usurper une adresse IP légitime dans le but de contourner les règles de filtrage mises en place. Ceci consiste par exemple à envoyer depuis un réseau externe des paquets ayant pour source une adresse IP interne à destination d'une autre adresse IP interne. Sans vérification des interfaces utilisées, le pare-feu SNS interprète la requête comme légitime et provenant du réseau interne vers le réseau interne. Le trafic malicieux est alors routé comme du trafic interne légitime.

Afin de se protéger de ce type d'attaque, les mécanismes d'anti-usurpation IP sont activés par défaut. Ils consistent à vérifier sur chaque interface d'entrée la légitimité de l'adresse IP source des paquets. Cette légitimité repose sur la topologie réseau définie par :

- Les interfaces réseau, pour les réseaux directement connectés,
- La table de routage, pour les réseaux distants.

INFORMATION
En plus d'être un élément indispensable à la sécurité, l'anti-usurpation IP est extrêmement efficace pour détecter des erreurs de configuration réseau (mauvaise configuration de règles de routage par exemple).

3.2.2 Anti-usurpation IP sur les interfaces réseau

Un pare-feu SNS utilise la notion d'interface "interne" pour identifier les interfaces qui alimentent le mécanisme d'anti-usurpation IP. Le menu **Configuration > Réseau > Interfaces** permet de configurer le type d'interface : un bouclier apparaît lorsqu'une interface est protégée par l'anti-usurpation IP. Dès lors, une telle interface n'acceptera que des paquets dont l'adresse IP source provient du réseau de commutation de l'interface. De plus, les autres interfaces du pare-feu SNS refuseront ces mêmes paquets en entrée. Ces règles d'anti-usurpation IP sont appliquées avant même l'évaluation de la politique de filtrage réseau.

INFORMATION
La liste des réseaux protégés est alimentée par la tableau de routage. Il est possible de

compléter la liste des IP autorisées à communiquer vers une interface protégée en configurant celle-ci comme indiqué dans le chapitre Anti-usurpation IP par la table de routage.

R21 | SNS-SMC | Déclarer les interfaces internes
Seules les interfaces donnant accès à un réseau public (Internet) ou non maîtrisé doivent être externes. Il est recommandé de configurer l'ensemble des autres interfaces comme protégées (internes).

ATTENTION
Par défaut, les règles implicites de filtrage autorisent l'administration des pare-feux SNS à partir des interfaces internes. Ces règles devront êtres désactivées comme expliqué dans le chapitre Règles implicites.

3.2.3 Anti-usurpation IP par la table de routage

La définition des routes renseigne le pare-feu SNS sur la topologie réseau et complète implicitement les mécanismes d'anti-usurpation IP. Toute route à destination d'un réseau distant joignable par une interface "interne" est ajoutée aux tables d'anti-usurpation IP. Ainsi, si des paquets dont l'adresse IP source est déclarée joignable par une interface "interne" sont reçus sur une autre interface, ils seront rejetés avant même l'évaluation de la politique de filtrage réseau en place sur le pare-feu SNS. Les routes utilisant des interfaces "externes" ne sont pas protégées car, en général, elles servent à répondre à des équipements dont les adresses IP sources ne sont pas connues à l'avance.

R22 | SNS | Définir des routes statiques pour les réseaux internes
Il est nécessaire de définir des routes statiques pour l'ensemble des réseaux internes connus auxquels les interfaces du pare-feu SNS n'appartiennent pas afin de profiter des mécanismes d'anti-usurpation IP. Ces routes sont reconnaissables dans le menu **Configuration > Réseau > Routage**, onglets **Routes statiques IPv4** et **Routes statiques IPv6** par la présence d'un bouclier.

ATTENTION
Il est nécessaire de déclarer des routes IPv4 et IPv6 pour l'intégralité des réseaux distants joignables par les interfaces "internes". Dans le cas contraire, leurs paquets seront systématiquement rejetés par le pare-feu SNS.

3.2.4 Anti-usurpation IP sur un *bridge*

Un *bridge* permet de connecter plusieurs interfaces physiques sur un même réseau. Le pare-feu SNS applique toutefois ses mécanismes d'anti-usurpation IP indépendamment sur chacune des interfaces du *bridge*. Cette fonctionnalité d'anti-usurpation IP ne nécessite pas de paramétrage particulier de la part des administrateurs lorsque le bridge est activé.

Lorsque les équipements sont sur le même réseau de commutation que le pare-feu SNS, celui-ci maintient à jour une table (dite table des hôtes) contenant chaque adresse IP rencontrée et l'interface physique associée. Si une adresse est détectée sur une autre interface que celle renseignée, une alerte est alors levée.

ATTENTION
La table des hôtes n'est renseignée qu'à partir du premier paquet reçu par un pare-feu SNS. L'anti-usurpation IP du *bridge* ne protège donc pas un interlocuteur directement connecté et n'ayant encore émis aucun trafic.

Dans le cas de réseaux distants, des règles de routage sont nécessaires, précisant l'interface physique utilisée. L'anti-usurpation IP par la table de routage détaillé dans le chapitre Anti-usurpation IP par la table de routage est employé.

3.2.5 Règles complémentaires

Certaines configurations ne peuvent pas être prises en compte par les mécanismes d'anti-usurpation IP natifs du pare-feu SNS. En particulier, un certain nombre de plages d'adresses particulières définies dans la RFC 5735 sont pré-configurées dans le pare-feu SNS au sein d'un groupe spécifique. Ces plages concernent des réseaux privés et ne devraient pas être utilisées sur une interface publique.

R23 | SNS | Compléter les règles d'anti-usurpation IP
Il est recommandé de compléter autant que possible les règles d'anti-usurpation IP citées précédemment par des règles de filtrage déduites de la topologie réseau. Par exemple, il est recommandé d'interdire explicitement les plages d'adresses du groupe RFC 5735 en provenance d'Internet.

4. Configuration des services

4.1 Mises à jour

Certaines fonctionnalités d'un pare-feu SNS nécessitent des mises à jour régulières (activées par défaut dans le menu **Configuration > Système > Active Update**). L'absence totale de mises à jour empêcherait le pare-feu SNS d'obtenir des correctifs de sécurité et le renouvellement de bases d'informations. Ces mises à jour peuvent être réalisées :

- Hors ligne par la mise en place d'un miroir interne,
- En ligne, à travers un serveur proxy ou en direct.

Si la mise à jour se fait en ligne, il y aura autant de flux de gestion que de pare-feux SNS dans le SI. Cela peut occasionner une surconsommation de la bande passante. L'utilisation d'un miroir interne permet alors de restreindre le nombre de pare-feux SNS autorisés à accéder à Internet.

Le serveur SMC peut être utilisé en tant que miroir interne pour les mises à jour des pare-feux SNS. Cette fonctionnalité peut être activée depuis le menu **Configuration** > **Serveur Active Update** du serveur SMC.

R24 | SNS | Mettre à jour depuis un miroir interne
Il est recommandé de mettre à jour régulièrement les services par l'activation des mises à jour automatiques et d'utiliser un miroir interne.

Pour une utilisation en ligne, il est recommandé de s'assurer que la connexion vers le serveur de mise à jour est uniquement utilisée par le pare-feu SNS, vers cette seule destination et à cette seule fin. Cela peut se réaliser par la configuration d'un serveur proxy authentifiant. Le compte d'accès utilisé au niveau du proxy doit être un compte dédié et disposer d'accès restreints aux besoins du pare-feu SNS (filtrage d'URL et de flux IP strictement nécessaires aux opérations de mise à jour des pare-feux SNS, à savoir les URL *update{1,2,3,4}-sns.stormshieldcs.eu* et *licence{1,2,3,4}-sns.stormshieldcs.eu*).

R24 - | SNS | Mettre à jour au travers d'un proxy
En l'absence de miroir interne, le pare-feu SNS doit accéder au miroir en ligne sur Internet au travers d'un proxy authentifiant avec un compte dédié et une politique de filtrage adaptée.

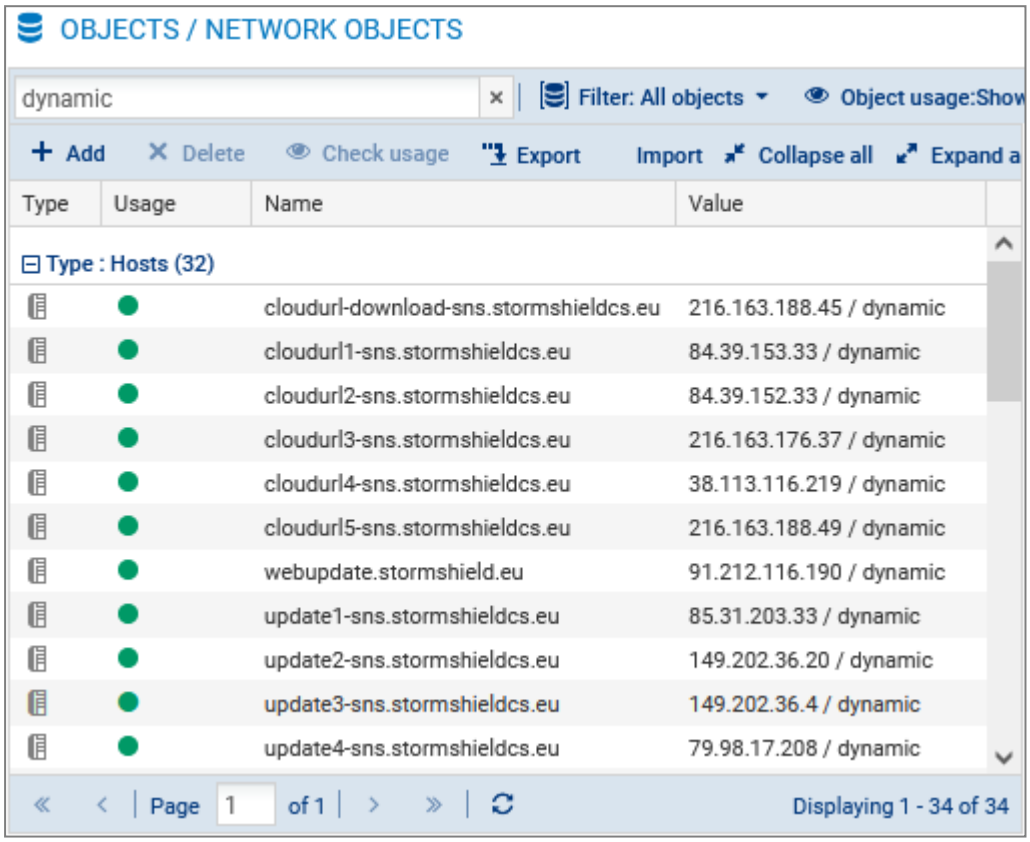
4.2 DNS

L'utilisation de certains services (par exemple *proxy web*) nécessite la résolution de noms de domaine. Dans le cas d'une compromission des serveurs DNS utilisés, un attaquant peut alors rediriger les flux vers des correspondants illégitimes.

R25 | SNS | Choisir des serveurs DNS maîtrisés
Il est recommandé de configurer des résolveurs DNS maîtrisés dans le menu **Configuration > Système > Configuration > Paramètres réseaux**.

R25 - | SNS | Modifier les serveurs DNS par défaut
Il est recommandé de remplacer les résolveurs DNS configurés par défaut par ceux du fournisseur d'accès si aucun n'est maîtrisé dans le SI.

La base d'objets d'un pare-feu SNS permet de créer des objets de type statique ou dynamique. Ces derniers dépendent d'un nom de domaine régulièrement résolu par le pare-feu SNS. Il en existe par défaut une quinzaine qui portent un nom se terminant par stormshieldcs.eu ou stormshield.eu dont une partie est représentée sur l'image ci-dessous (ces noms peuvent évoluer en fonction des mises à jour). L'application de la recommandation R30 permet de bloquer par défaut ces requêtes DNS.



L'utilisation d'un miroir interne (recommandation R24) permet à un pare-feu SNS de ne pas avoir à contacter directement les serveurs de mise à jour de Stormshield. De plus, l'utilisation de serveurs DNS maîtrisés (recommandation R25) permet de déporter la gestion des adresses des autres services de Stormshield (gestion des licences, etc.).

R26 | SNS | Limiter l'usage des objets dynamiques
Il est recommandé de supprimer les objets dynamiques non utilisés et de reconfigurer les objets restants en mode statique dans le menu **Configuration > Objets > Réseau**.
Les objets dynamiques étant des objets locaux, ils ne peuvent pas être supprimés depuis un serveur SMC.

R26 | SMC | Limiter l'usage des objets dynamiques
Il est recommandé de supprimer les objets dynamiques (type FQDN) non utilisés et de reconfigurer les objets restants en mode statique dans le menu **Objets réseau**.

4.3 NTP

Certaines fonctionnalités sont fortement liées à l'heure du système, notamment la journalisation et la gestion des certificats. La configuration manuelle de l'heure ne permet pas

une bonne intégration de l'équipement dans un SI. De plus, la seule utilisation de l'horloge interne ne garantit pas l'absence de dérive sur une longue période.

R27 | SNS-SMC | Synchroniser l'heure du système
Il est recommandé d'activer la synchronisation NTP des pare-feux SNS et d'utiliser plusieurs serveurs de temps fiables, conformément à la note technique Recommandations de sécurité pour la mise en œuvre d'un système de journalisation.

4.4 Utilisation d'un annuaire externe

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Diverses fonctionnalités, dont l'authentification des administrateurs, nécessitent la connexion à un annuaire. Lorsque ce dernier est externe au pare-feu SNS, la sécurité (confidentialité et intégrité) des flux échangés doit être assurée et l'authentification des équipements (pare-feu, serveur d'administration et serveur d'annuaire) doit être réalisée. Dans le cas contraire, un attaquant peut obtenir des informations de connexion.

R28 | SNS-SMC | Configurer LDAP de manière sécurisée
Si le service LDAP est configuré, il est recommandé :

- D'utiliser le protocole LDAPS, le serveur LDAP présentant un certificat signé par une IGC maîtrisée,
- D'importer l'AC correspondante sur le pare-feu SNS ou le serveur SMC,
- D'utiliser l'AC précédemment importée pour valider la connexion au serveur LDAP.

La mise en place d'une authentification à partir d'un annuaire externe se réalise en plusieurs étapes :

- Activer l'utilisation de l'annuaire (menu **Configuration > Utilisateurs > Configuration des annuaires**), choisir son type puis paramétrer l'accès :
  - L'adresse de l'annuaire,
  - La base DN,
  - Le port de communication,
  - L'identifiant et le mot de passe du compte d'accès du pare-feu SNS sur l'annuaire. Ce compte doit respecter la recommandation R8,
  - Le hachage des mots de passe.
- Définir la structure de l'annuaire (onglet **Structure**). La correspondance entre les attributs manipulés par le pare-feu SNS et ceux présents dans l'annuaire LDAP doit être établie. L'attribut *Stormshield member* (qui contient la liste des identifiants appartenant à un groupe) doit en particulier correspondre à son équivalent dans l'annuaire LDAP,
- Définir LDAP comme méthode d'authentification par défaut (menu **Configuration > Utilisateurs > Authentification**).

5. Politique de filtrage réseau et de NAT

5.1 Nommage de la politique de filtrage réseau

Par défaut, les politiques de filtrage présentes sur un pare-feu SNS ne portent pas de nom explicite. Cette pratique ne permet pas à un administrateur de facilement comprendre le rôle du pare-feu SNS, ni de savoir quelle politique appliquer si plusieurs sont configurées. L'application d'une convention de nommage permet de :

- Refléter la fonction du pare-feu SNS dans le nom de la politique de filtrage (accès Internet, isolation d'un partenaire, etc.),
- Minimiser les erreurs de manipulation (activation de la mauvaise politique),
- Disposer d'une configuration homogène au niveau de l'intitulé des politiques de filtrage réseau de l'ensemble des pare-feux SNS présents au sein du SI.

R29 | SNS-SMC | Renommer la politique de production
Il est recommandé d'appliquer une politique de nommage des profils de filtrage réseau comme détaillé dans le guide Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu.

5.2 Règles implicites

Par défaut, le pare-feu SNS est configuré avec des règles implicites de filtrage, évaluées avant les règles de filtrage définies manuellement. Ces règles ont pour but de simplifier la configuration en autorisant des requêtes ou des accès particuliers. Le menu **Configuration > Politique de sécurité > Filtrage et NAT** ne contient alors pas toutes les règles appliquées par le pare-feu SNS. Par conséquent, il est possible qu'une règle créée par un administrateur ne soit jamais évaluée à cause de la présence d'une règle implicite contraire.

R30 | SNS | Désactiver les règles implicites
Il est recommandé de désactiver la totalité des règles de filtrage implicites, sauf la règle "Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster HA)". Cela se réalise dans le menu **Configuration > Politique de sécurité > Règles implicites**.

ATTENTION
Afin d'éviter de perdre les capacités d'administration, il est nécessaire de créer de nouvelles règles de filtrage avant de désactiver les règles implicites correspondantes. Ces règles doivent autoriser, en fonction des besoins, le trafic HTTPS, NSRPC ou SSH entre le pare-feu SNS et les groupes définis dans le chapitre Configuration des adresses IP d'administration sur les interfaces définies dans le chapitre Interface web d'administration dédiée.
De plus, afin d'éviter de dégrader les performances de certaines fonctionnalités du pare-feu SNS, il est nécessaire de créer de nouvelles règles de filtrage avant de désactiver les règles implicites des options et paramètres utilisés. Par exemple pour les flux ESP, l'option "Suivi des états (stateful)" est indispensable pour ne pas dégrader les performances VPN IPsec.

INFORMATION
La commande NSRPC `monitor filter` permet d'afficher l'ensemble des règles de filtrage

appliquées. En l'occurrence, il est possible de constater que la désactivation des flux implicites des services hébergés ne bloque pas les requêtes DNS émises par le pare-feu SNS. L'application de la recommandation R26 limite ces flux.

5.3 Analyse protocolaire

Certains flux malveillants peuvent avoir les mêmes caractéristiques réseau que des flux autorisés. Le blocage de ces flux est impossible par de simples règles de filtrage sans impact sur le trafic légitime. Le pare-feu SNS est doté de capacités d'analyses protocolaires permettant un filtrage fin. L'inspection effectuée sur les flux traités par une règle de filtrage peut être paramétrée suivant un des trois niveaux d'inspection : Firewall, IPS ou IDS.

Au niveau d'inspection Firewall, le pare-feu SNS n'effectue que des vérifications sommaires de conformités. En particulier, il contrôlera le respect du sens d'établissement des connexions. Il ne vérifiera ni les drapeaux utilisés, ni les numéros de séquence, ni les options TCP.

ATTENTION
Au niveau d'inspection Firewall, lorsqu'une session est abandonnée par le pare-feu SNS, celui-ci envoie un paquet de réinitialisation possédant un numéro de séquence nul. Le correspondant, ne pouvant le relier à une connexion existante, n'en clôturera aucune.

Au niveau d'inspection IPS, le pare-feu SNS effectue des vérifications supplémentaires sur le respect des standards des protocoles, ainsi que des analyses reposant sur des signatures d'attaques déjà connues. Ces analyses sont réalisées grâce à des modules d'inspection dédiés à chaque protocole. Suivant le réglage mis en place, le module concerné pourra bloquer les flux identifiés comme malveillants.

Le niveau d'inspection IDS réalise les mêmes inspections que le niveau d'inspection IPS, mais ne lèvera que des alarmes si du trafic semble malveillant, sans le bloquer. Le niveau d'inspection IDS peut être utilisé en pré-production pour analyser les flux qui transitent dans un système et ainsi faciliter l'action de l'administrateur dans sa tâche visant à configurer les modules d'inspection.

Aux niveaux d'inspection IPS et IDS, il existe différents modes de fonctionnement :

- Par défaut, les modules d'inspection sont chargés automatiquement, en fonction des ports utilisés dans les règles de filtrage et des caractéristiques du trafic observé par le pare-feu SNS. Dans la suite, nous parlerons alors de "mode automatique",
- Il est également possible de limiter le chargement de ces modules en indiquant ceux à utiliser dans la règle de filtrage. Dans ce cas, le pare-feu SNS n'effectuera que les analyses correspondant au protocole demandé. Nous utiliserons dans ce document le terme de "mode transport" dès lors que les modules indiqués sont uniquement des protocoles de transport (TCP, UDP, ...),
- Les modules peuvent aussi concerner un protocole applicatif particulier. Nous utiliserons par la suite la notion de "mode applicatif". Dès lors que les modules chargés ont fait l'objet d'une évaluation dans le cadre de la qualification, nous utiliserons la dénomination "mode applicatif qualifié". Il s'agit des modules liés aux protocoles FTP, HTTP (incluant WebDAV), SIP, SMTP, DNS, Modbus, S7 et UMAS.

Le niveau d'inspection IPS en mode automatique est sélectionné par défaut à la création d'une règle de filtrage. Sans profil d'inspection, tous les modules d'analyses protocolaires peuvent être chargés lors de l'inspection des flux traités par la règle de filtrage, ce qui peut augmenter la charge processeur du pare-feu SNS. Si nécessaire, limitez le chargement de ces modules en utilisant un profil d'inspection, comme avec le niveau d'inspection IPS en mode transport. Dans

la mesure du possible, il convient de faire réaliser les fonctions d'analyse protocolaire par des équipements dédiés comme des serveurs proxy afin de limiter le risque de compromission du pare-feu SNS.

R31 | SNS-SMC | Adapter le type d'inspection de trafic au rôle du pare-feu SNS
Il est recommandé d'utiliser les niveaux d'inspection IPS en mode applicatif, IPS en mode transport ou Firewall qualifié en cohérence avec le rôle joué par le pare-feu SNS dans l'architecture du système d'information considéré. En particulier, il convient d'être vigilant quant à son exposition aux menaces, à son rôle et à la criticité des ressources à protéger.

ATTENTION
L'anti-usurpation IP est désactivée avec le niveau d'inspection Firewall.

Le niveau d'analyse et le mode associé sont à définir pour chaque règle de filtrage et varient en fonction du rôle du pare-feu SNS. Par exemple :

- S'il est utilisé exclusivement en tant que passerelle VPN en bordure de SI et qu'il est lui-même protégé par d'autres pare-feux, le niveau d'inspection Firewall permet de dédier ses ressources aux fonctions cryptographiques tout en réduisant sa surface d'attaque,
- S'il est situé entre un SI d'entreprise et le réseau Internet, le niveau d'inspection IPS en mode transport permet de limiter la surface d'attaque du pare-feu SNS tout en assurant un filtrage fin des connexions,
- S'il protège des serveurs applicatifs joignables uniquement depuis le réseau interne d'une entreprise, le niveau d'inspection IPS en mode applicatif qualifié peut être utilisé.

La colonne **Inspection de sécurité** des règles de filtrage (menu **Configuration > Politique de sécurité > Filtrage et NAT > Filtrage**) permet de choisir le niveau d'inspection. Pour les niveaux d'inspection IPS et IDS, la colonne **Protocole** permet de limiter le niveau d'analyse. L'option **Type de protocole** positionnée à **Protocole IP** permet de choisir un protocole de transport dans le menu **Protocole IP**. Si cette option est positionnée à **Protocole applicatif**, le menu du même nom permet de choisir le protocole applicatif sur lequel le pare-feu SNS agira. Un seul protocole (applicatif ou de transport) peut être choisi par règle de filtrage.

Les niveaux d'inspection Firewall, IPS et IDS reposent sur l'utilisation de profils d'inspection. Ces profils permettent de configurer le comportement du pare-feu SNS en fonction du trafic traité (types d'alarmes à lever, blocage du flux). Avant le passage en production de l'inspection protocolaire, dans un environnement réputé sain (typiquement un environnement de pré-production), il est souhaitable de désactiver les alarmes qui seraient inutilement générées par le trafic légitime afin de ne pas polluer la supervision de sécurité après le passage en production. L'utilisation de multiples profils doit permettre d'ajuster les configurations au contexte d'emploi. Il est en particulier recommandé de créer des profils d'inspection plus fins et donc plus restrictifs pour les applications les plus critiques.

R32 | SNS-SMC | Adapter les profils d'inspection en fonction du contexte d'emploi du pare-feu SNS
Lorsque l'analyse protocolaire est active, il est recommandé d'ajuster au mieux la politique aux réseaux à protéger en s'appuyant sur différents profils d'inspection.

Parmi les profils d'inspection pré-configurés, deux sont utilisés par défaut : le profil *00* pour les flux émis par un réseau externe et le profil *01* pour les flux émis par un réseau interne. Le choix du profil se fait à chaque règle de filtrage, dans l'onglet **Inspection**. La configuration de ces profils se fait dans le menu **Configuration > Protection applicative > Profils d'inspection**, en

sélectionnant **Accéder aux profils**. Chaque profil est alors basé sur les politiques définies au menu **Configuration > Protection applicative > Protocoles**. Ces politiques définissent les analyses générales réalisées sur les différents protocoles : les ports par défaut, les commandes à restreindre, le type d'analyse à effectuer, etc. De plus, le menu **Configuration > Protection applicative > Applications et protections** définit les analyses plus spécifiques comme la recherche de *buffer overflow*, de format d'encodage, etc. Ce menu propose une vue par profil ou par contexte.

5.4 Politique de filtrage

Sur un pare-feu SNS, il peut être nécessaire d'utiliser les mêmes objets à plusieurs reprises, s'ils apparaissent dans plusieurs règles de filtrages ou lorsque ces dernières viennent en complément d'un menu de configuration. Par exemple, un même sous-réseau peut apparaître dans plusieurs règles de filtrage (réseau de postes de travail vers un serveur de mail, vers un proxy web, etc.), ou en tant que réseau d'administration (se référer au chapitre Configuration des adresses IP d'administration) et au sein d'une règle de filtrage explicite corrélée (conformément au chapitre Règles implicites).

Lors d'éventuels changements (par exemple de plan d'adressage), ajouts (nouveaux sous-réseaux pour accueillir de nouveaux postes de travail) ou suppressions (restriction du nombre de postes d'administration), les mises à jour doivent être réalisées à chacune des occurrences, ce qui augmente les risques d'erreur de configuration et d'oubli. L'utilisation d'objets et de groupes d'objets permet un traitement global et simultané sur l'ensemble de la configuration lors d'un changement.

R33 | SNS-SMC | Utiliser des groupes d'objets
Il est recommandé d'utiliser des groupes d'objets lors de la définition des règles de filtrage en cohérence avec les autres menus.

Dans ce cas, il est possible de maîtriser par exemple :

- Un groupe d'administration comprenant les adresses IP des postes d'administration,
- Un groupe des postes utilisateur comprenant les sous-réseaux IP utilisés,
- Un groupe de service comprenant les adresses IP des serveurs internes,
- Un groupe métier comprenant les ports utilisés par les applications métier,
- etc.

Il est alors suffisant de retirer ou ajouter un élément à un groupe pour s'adapter à une nouvelle situation.

Par ailleurs, les bonnes pratiques relatives à la définition d'une politique de filtrage réseau sont détaillées dans le guide Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu. Ce document a pour objectif principal de présenter l'organisation à adopter afin de garantir une politique de filtrage pérenne et maîtrisée.

6. Certificats et PKI

Plusieurs cas d'usage impliquent l'utilisation de certificats par des pare-feux SNS et par le serveur SMC, dont :

- La publication de l'interface web d'administration en HTTPS,
- L'authentification par certificat des administrateurs pour l'accès à l'interface web d'administration du pare-feu SNS,
- L'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place de tunnels VPN IPsec,
- L'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place d'un service de VPN SSL/TLS,
- La connexion à un annuaire externe en LDAPS,
- La connexion des pare-feux SNS au serveur SMC.

6.1 Utilisation d'une IGC

Lorsqu'un pare-feu SNS est impliqué dans un mécanisme d'authentification, ce dernier peut reposer sur des certificats issus d'une IGC. La confiance placée dans cette IGC détermine alors la confiance du certificat utilisé et donc la fiabilité de l'authentification. En cas d'absence de solution externe de gestion des certificats, les pare-feux SNS offrent la possibilité de générer une autorité de certification ainsi que des identités (composées d'une clé privée, d'une clé publique et du certificat correspondant) signées par cette autorité. Dans ce cas, les clés privées sont générées par et stockées sur le pare-feu SNS. La compromission du pare-feu SNS impliquera alors de fait celle des éléments secrets générés par l'équipement.

R34 | SNS-SMC | Utiliser une IGC maîtrisée externe
Il est recommandé d'utiliser une IGC maîtrisée externe au pare-feu SNS ou au serveur SMC pour générer les identités utilisées. Cette IGC ainsi que les AC utilisées doivent être conformes aux préconisations de l'annexe A1 du RGS.

R34 - | SNS | Utiliser l'IGC du pare-feu SNS
Il est possible d'utiliser l'IGC présente dans le pare-feu SNS en l'absence d'IGC externe. Dans ce cas,

- Les éléments secrets générés doivent être supprimés du pare-feu SNS après leur export vers les pare-feux SNS destinataires,
- Les administrateurs de l'IGC doivent être uniquement dédiés à ce rôle (voir la recommandation R9).

R34 - | SMC | Utiliser l'IGC du pare-feu SNS
En l'absence d'IGC externe, il est possible d'utiliser l'IGC présente sur un pare-feu SNS.

ATTENTION
Lorsque l'IGC interne au pare-feu SNS est configurée, sa compromission permet à un attaquant de se forger une identité qui sera considérée comme légitime sur le SI. Il est donc important de limiter cette fonction aux pare-feux SNS les moins exposés possible à des réseaux non maîtrisés.

6.2 Gestion des CRL dans le cadre d'un tunnel VPN IPsec

Un certificat peut être révoqué par son AC avant son expiration prévue. Cela arrive par exemple lorsqu'une clé privée est compromise ou qu'un administrateur quitte la société. L'acceptation d'un tel certificat permet alors à un utilisateur ou équipement illégitime de bénéficier d'une authentification sur le pare-feu SNS. La mise en place par l'IGC de CRL permet d'avertir les pare-feux SNS concernés de la révocation de certificats. Par défaut, l'absence de CRL n'est pas bloquante pour établir un tunnel VPN IPsec, elle est simplement signalée dans les journaux du pare-feu SNS.

R35 | SNS-SMC | Imposer la vérification des CRL
Il est recommandé d'imposer la vérification de CRL pour la mise en œuvre des tunnels VPN IPsec.

Le changement de ce comportement est à effectuer en modifiant le paramètre *CRLrequired* puis en relançant le service IPsec. Cela se réalise par les commandes NSRPC suivantes :

```
config ipsec update slot=01 CRLrequired=1
config ipsec activate
```

Ce paramètre est stocké dans le fichier */Firewall/ConfigFiles/VPN/01/*. En mode console, le service IPsec peut être activé via les commandes NSRPC suivantes :

```
config slot activate global=0 slot=00 type=vpn
config slot activate global=0 slot=01 type=vpn
```

À l'utilisation de ces commandes, l'ensemble des tunnels VPN seront fermés, puis la nouvelle politique VPN (01) sera activée. Dans les deux cas, la valeur *01* utilisée en exemple représente le numéro de la politique IPsec employée.

Les CRL récupérées sont stockées localement dans le répertoire de leur AC (ou de leur AC déléguée) correspondante et renommées en **CA.crl.pem**.

INFORMATION
Lorsque le paramètre *CRLrequired* est activé, il est nécessaire de disposer de toutes les CRL de la chaîne de certification.

6.2.1 Import automatique de CRL

Bien qu'une CRL ait une durée de validité, il est important de vérifier fréquemment que de nouveaux certificats n'ont pas été révoqués. Cette fréquence de mise à jour de la CRL doit être adaptée à l'usage de l'authentification par certificat. Si les mises à jour sont trop espacées, le pare-feu SNS peut authentifier des certificats révoqués et créer un accès illégitime. Par exemple, une récupération toutes les 6 heures permet de diminuer fortement le délai pendant lequel un certificat révoqué peut être utilisé.

R36 | SNS | Adapter le rafraîchissement automatique des CRL
Il est recommandé d'adapter le temps de rafraîchissement en fonction de la réactivité recherchée. Si différents services nécessitent des délais différents, le plus court doit être utilisé.

Par défaut, lorsque l'URL d'une CRL est ajouté et activé, la récupération du fichier est réalisée toutes les 6 heures. Il est possible de forcer la mise à jour à l'aide de la commande NSRPC `system checkcrl`. Utilisez `system checkcrl help` pour plus de détails au sujet de la commande. Il est également possible de modifier la fréquence de récupération des CRL via l'interface web d'administration.

R37 | SNS-SMC | Configurer l'URL de récupération de la CRL et activer la récupération automatique
Il est recommandé de configurer l'URL de récupération automatique de la CRL de chaque AC et activer cette fonctionnalité dans le menu **Configuration > Système > Configuration** des pare-feux SNS, en cochant la case **Activer la récupération régulière des listes de révocation de certificats (CRL)**. Sur le serveur SMC, cette configuration se réalise dans le menu **Configuration** > **Certificats** > *nom de l'AC* > **Liste des points de distribution de CRL**.

Les points de distribution de CRL associées à une AC peuvent être positionnés soit via l'interface web d'administration du pare-feu SNS dans le menu **Configuration > Objets > Certificats et PKI** > *nom de l'AC* > **Profil de certificats**, soit à l'aide de la commande NSRPC :

```
pki ca checkcrl add caname=<nom de l'AC> uri=<URL de la CRL>
```

L'URL du point de distribution peut être de type HTTP, HTTPS, LDAP, LDAPS et FTP.

INFORMATION
Pour que le pare-feu SNS puisse résoudre le FQDN de l'URL du point de distribution de la CRL, un objet de type **Machine** correspondant au FQDN doit être défini dans sa base d'objets.

6.2.2 Import manuel de CRL

Dans certains cas, il peut être difficile, voire impossible, d'importer automatiquement une CRL. Le cas se présente si un tunnel VPN est nécessaire afin de l'obtenir, et que la précédente n'est plus valide ou n'a jamais été importée. L'import d'une CRL peut alors être réalisé manuellement. Cette opération implique l'intervention d'un administrateur et la manipulation de fichiers. Elle nécessite donc des procédures organisationnelles strictes et devrait rester une opération exceptionnelle.

R37 - | SNS-SMC | Importer manuellement une CRL
Si un import automatique est impossible, il est recommandé d'importer manuellement la CRL.

Sur un pare-feu SNS, l'import manuel d'une CRL s'effectue via l'interface web d'administration, dans le menu **Configuration > Objets > Certificats et PKI > Ajouter > Importer un fichier**. Le fichier de CRL doit être importé au format PEM ou DER et son nom ne doit pas comporter d'extension. À l'import, le fichier de CRL est copié dans le répertoire de l'AC à laquelle il est associé, puis converti au format PEM et renommé en **CA.crl.pem**.

Sur un serveur SMC, l'import manuel d'une CRL s'effectue via l'interface web d'administration, dans le menu **Configuration** > **Certificats** > *nom de l'AC* > **SMC en tant que point de distribution de CRL**.

7. VPN IPsec

Certains échanges de flux doivent parfois être réalisés au travers de réseaux non maîtrisés ou de sensibilité inférieure aux données transmises. Dans de tels cas, les risques et conséquences de fuite ou de modification de données sont accrus. Il est alors nécessaire de s'assurer que les données sont échangées entre entités authentifiées, de manière intègre et confidentielle. Ces besoins peuvent être couverts par la mise en place de tunnels VPN IPsec chiffrés. Cette section décrit la politique de configuration à appliquer sur un pare-feu SNS utilisé comme passerelle chiffrante.

7.1 Profils de chiffrement

La confidentialité et l'intégrité des flux échangés sur un VPN (site-à-site ou client-à-site) reposent sur l'utilisation d'algorithmes cryptographiques robustes négociés entre les deux parties. L'utilisation de profils de chiffrement permet d'expliciter les algorithmes autorisés. Bien que le profil pré-configuré *StrongEncryption* soit compatible avec les exigences de l'annexe B1 du RGS, il est conseillé de redéfinir manuellement des profils de chiffrement IKE et IPsec.

Les tableaux ci-dessous donnent le profil minimum de chiffrement compatible avec les préconisations du RGS. Les cryptopériodes indiquées dans ces tableaux ne sont pas directement issues du RGS mais données à titre indicatif. Elles doivent être définies en fonction de la politique de sécurité de l'organisme.

Profil minimum de chiffrement IKE compatible avec le RGS

Paramètre	Valeur
Algorithme de chiffrement	AES-CBC 128
Fonction de hachage	SHA 256
Groupe Diffie-Hellman	Groupe DH14 (2048 bits)
Cryptopériode	21600s

Profil minimum de chiffrement IPsec compatible avec le RGS

Paramètre	Valeur
Algorithme de chiffrement	AES-GCM 256
Fonction de hachage	SHA 384
Groupe Diffie-Hellman	Groupe 19 (256 bits)
Cryptopériode	3600s

R38 | SNS-SMC | Utiliser des algorithmes robustes pour IKE et IPsec
Il est recommandé d'utiliser au moins les algorithmes AES-GCM 256, SHA 384 et le groupe Diffie-Hellman 19 dans les profils de chiffrement IKE et IPsec.
Les profils de chiffrement se trouvent dans le menu **Configuration > VPN > VPN IPsec > Profils de chiffrement** pour les pare-feux SNS et dans le menu **Configuration > Profils de chiffrement** sur le serveur SMC.

7.2 Échange de clés et authentification

7.2.1 Protocole IKE

Le niveau de protection offert par un tunnel VPN IPsec dépend de la robustesse de la suite cryptographique mise en place ainsi que la fiabilité du mécanisme d'échange des clés : cet échange peut se faire grâce au protocole IKEv2 sur les pare-feux SNS en version 2.0.0 et supérieure. L'utilisation des protocoles récents est conforme aux préconisations du guide Recommandations de sécurité relatives à IPsec.

R39 | SNS-SMC | Utiliser la version 2 du protocole IKE
Si tous les correspondants des tunnels VPN IPsec sont compatibles, il est recommandé d'utiliser le protocole IKE dans sa version 2.

7.2.2 Authentification

Pour éviter toute usurpation d'identité du correspondant, et ce quel que soit le type de tunnel configuré (site-à-site ou client-à-site), il est nécessaire d'authentifier le correspondant distant lors de la création du tunnel. Cette authentification réalisée par le protocole IKE peut se faire à l'aide d'une clé partagée ou de certificats. L'utilisation d'une clé partagée ne permet pas de distinguer chaque correspondant ni de leur appliquer des droits adaptés. De plus, si une clé doit être renouvelée (perte ou vol d'un équipement distant, perte des droits d'un utilisateur), il est nécessaire de renouveler la clé sur tous les pare-feux SNS configurés. Seule l'utilisation d'une IGC permet une identification de chaque correspondant et une gestion aisée des droits et des révocations.

R40 | SNS-SMC | Utiliser l'authentification mutuelle par certificat
Il est recommandé de mettre en œuvre une authentification mutuelle par certificat des correspondants d'un tunnel VPN IPsec en renseignant les autorités de certification acceptées dans le menu **Configuration > VPN > VPN IPsec > Identification** des pare-feux SNS et dans le menu **Configuration** > **Topologies VPN** du serveur SMC.

R40 - | SNS-SMC | Utiliser une clé partagée robuste
Si une authentification par clé partagée est choisie pour un VPN IPsec, il est recommandé de la choisir conforme aux recommandations de l'annexe B3 du RGS et du guide Recommandations relatives à l'authentification multifacteur et aux mots de passe.

ATTENTION
Si une authentification par clé partagée est choisie, il est impératif de respecter les prérequis suivants :

- Le secret doit disposer d'une entropie d'au moins 128 bits (22 caractères aléatoires parmi les minuscules, les majuscules et les chiffres). Se référer à l'annexe B1 du RGS pour plus de précisions,
- Le secret doit respecter les règles relatives à la génération des mots de passe décrites dans le guide Recommandations relatives à l'authentification multifacteur et aux mots de passe,
- Un secret différent doit être utilisé pour chacun des tunnels VPN site-à-site,

- Le secret doit être renouvelé régulièrement, sa cryptopériode (durée maximale durant laquelle perdre la confidentialité et l'intégrité du trafic est accepté si le secret venait à être compromis) doit être définie en fonction de la politique de sécurité de l'organisme.

7.3 Politiques de routage et de filtrage sortant, et configuration d'un VPN IPsec

Lorsque le pare-feu SNS est utilisé en tant que passerelle VPN, la bonne définition des routes et des règles de filtrage est critique pour garantir la confidentialité et l'intégrité des flux. Quatre fonctions sont fortement liées :

- Le routage,
- La politique de filtrage,
- La NAT avant IPsec,
- La politique IPsec.

Dans le cadre de la mise en œuvre de tunnels VPN IPsec, il est nécessaire d'avoir une route permettant de joindre les réseaux distants accessibles au travers des tunnels. Dans le cas contraire, le paquet est supprimé à l'étape de routage et n'atteint pas l'étape de chiffrement IPsec.

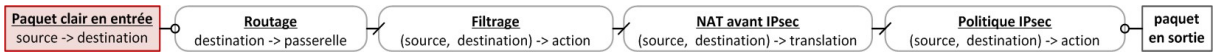
Pour éviter toute fuite de données, il est recommandé de configurer une route avec comme passerelle une IP fictive sur sa boucle locale, par exemple un objet de type machine ayant comme adresse 127.42.42.42. Cette technique est également appelée *blackholing*.

Après l'application de la politique IPsec, la politique de routage sera ré-évaluée en fonction du paquet chiffré. Cependant, en cas d'erreur sur la politique IPsec, les paquets seront détruits au lieu de sortir en clair.

Le séquencement des fonctions de routage, de filtrage, de NAT avant IPsec et de politique IPsec représenté sur l'image ci-dessous a un impact direct sur la confidentialité des flux. Ce séquencement n'est qu'une partie du cheminement complet du paquet dans le pare-feu SNS. En effet, lorsqu'il est chiffré, le paquet est ensuite traité par les fonctions de filtrage, de NAT après IPsec et de routage.

Il est indispensable d'écrire les règles les plus spécifiques pour la politique de filtrage et les règles les moins spécifiques pour la politique IPsec.

Briques fonctionnelles



R41 | SNS-SMC | Configurer les tunnels VPN IPsec de manière sécurisée

Lorsqu'un VPN IPsec est configuré, il est recommandé de :

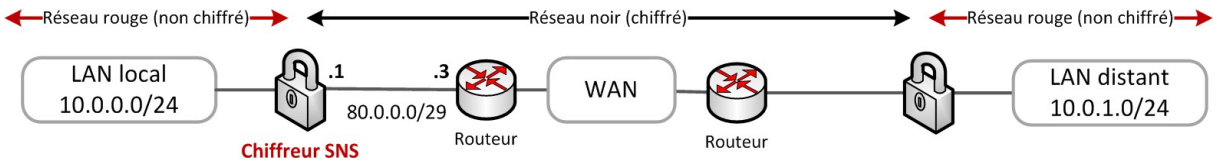
- Configurer une route statique à destination de la boucle locale (*blackholing*) pour joindre les réseaux distants accessibles au travers de tunnels VPN IPsec,
- S'assurer que la politique IPsec n'est jamais désactivée y compris lors de phases transitoires,
- S'assurer que les règles de filtrage sont toujours plus spécifiques que les règles de NAT avant IPsec,

- S'assurer que les flux (adresse IP source et destination) après la translation (NAT) correspondent à la politique IPsec,
- S'assurer qu'en l'absence de règles de NAT, les règles de filtrage sont toujours plus spécifiques que la politique IPsec.

ATTENTION
Idéalement, des pare-feux SNS distincts devraient être mis en œuvre afin de dissocier les fonctions de chiffrement, de filtrage des flux clairs et de filtrage des flux chiffrés.

Les exemples ci-dessous permettent d'illustrer l'intérêt de la recommandation précédente. Ils s'appliquent sur le pare-feu SNS en tant que passerelle VPN pour des flux en sortie du LAN local et à destination d'un LAN distant au travers d'un tunnel VPN IPsec établi avec une passerelle VPN distante. L'architecture est représentée sur l'image ci-dessous.

Schéma d'architecture



Dans chaque exemple sont données les configurations des briques fonctionnelles SNS traversées par un paquet réseau (image Briques fonctionnelles). Le paquet réseau entre avec une source et une destination spécifique. Les fonctions traversées sont, dans l'ordre :

- Le pré-routage,
- Le filtrage,
- La NAT avant IPsec,
- La politique IPsec.

Le résultat obtenu est décrit par le paquet de sortie, à savoir s'il est :

- Chiffré,
- Clair (non chiffré),
- Détruit,
- Filtré.

Un code couleur noir, rouge, vert est appliqué pour représenter respectivement : le cas nominal, le cas d'erreur (clair), le comportement après correction.

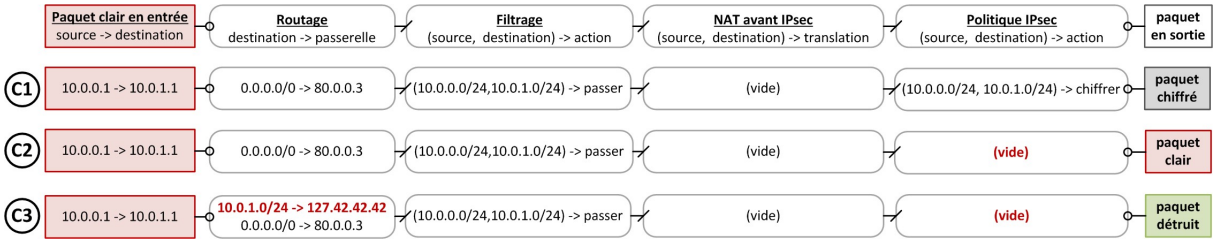
Pour chaque exemple, trois cas (C) sont représentés :

C1	Configuration ne respectant pas la recommandation, les paramètres d'entrée sont nominaux.
C2	Mise en évidence des problèmes liés à la configuration précédente. Une modification des entrées ou de la configuration est réalisée. Cette modification est repérée par l'utilisation d'un texte rouge.
C3	Configuration proposée afin de ne pas tomber dans le problème précédent. Cette modification est repérée par l'utilisation d'un texte rouge.

7.3.1 Politique IPsec toujours active

L'exemple représenté par l'image ci-dessous illustre la nécessité d'utiliser une route à destination de la boucle locale pour les réseaux IPsec distants. Dans le cas **C1**, les paquets passent en premier dans la table de routage. Elle contient une route valide vers le LAN distant (la route par défaut dans l'exemple traité). Ils passent ensuite dans la politique de filtrage qui accepte les paquets puis dans la politique IPsec qui se charge de l'encapsulation, du chiffrement et de la protection en intégrité des flux. La source et la destination des paquets chiffrés sont différentes de celles des paquets clairs. En particulier, la destination du paquet chiffré est la passerelle VPN distante. La table de routage est de nouveau traversée (la route à destination du LAN distant n'est pas utilisée, seule la route à destination de la passerelle VPN distante est utilisée), elle contient une route valide vers la passerelle IPsec (la route par défaut). Les paquets sont émis chiffrés.

Politique IPsec toujours active, route à destination de la boucle locale



La politique IPsec passe ensuite d'un état activé (**C1**) à un état désactivé (**C2**). L'état désactivé peut être permanent ou transitoire, ce dernier cas se produit lors de la désactivation puis de la réactivation de la politique IPsec.

Dans le cas **C2**, les paquets passent en premier dans la table de routage. Elle contient une route valide vers le LAN distant. Ils passent ensuite dans la politique de filtrage qui accepte les paquets. Cependant, aucune politique IPsec n'étant définie, les paquets sont envoyés en clair au prochain saut, c'est-à-dire par la passerelle par défaut définie dans la table de routage. Il y a fuite d'informations.

La solution présentée dans le cas **C3** consiste à définir une route à destination de la boucle locale (prendre une adresse IP particulière facilite la maintenance de la configuration, par exemple 127.42.42.42), également appelée *blackholing*. En l'absence de politique IPsec, le paquet sera détruit par le pare-feu SNS au lieu d'être envoyé à la passerelle par défaut.

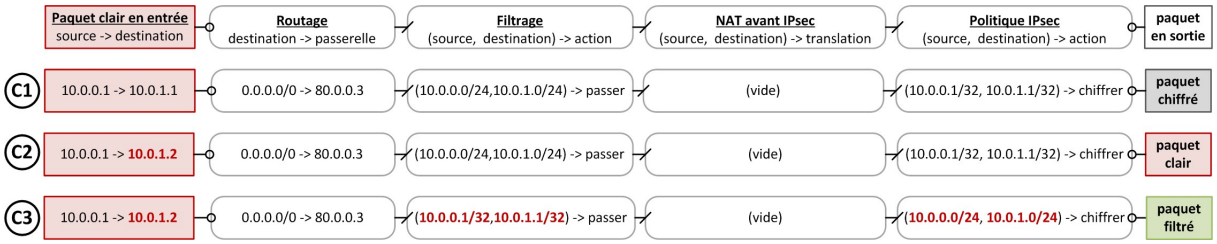
R41+ | SNS-SMC | Ne pas utiliser de route par défaut
Si l'ensemble des réseaux utilisés sont connus, il est recommandé de ne pas utiliser de route par défaut et de privilégier des routes explicites pour joindre l'ensemble des correspondants distants. Ainsi seuls les paquets ayant une route explicitement définie pourront sortir en clair.

ATTENTION
Les plans d'adressage doivent être choisis afin d'éviter toute confusion entre les réseaux rouges et noirs tels que mentionnés dans l'image Schéma d'architecture, et pour faciliter la création des routes.

7.3.2 Règles de filtrage toujours plus spécifiques que la politique IPsec

L'exemple représenté dans l'image ci-dessous illustre la nécessité de définir une politique de filtrage toujours plus spécifique que la politique IPsec. Dans le cas C1, la politique de filtrage est définie en /24 alors que la politique IPsec est en /32. L'administrateur désire, par exemple, définir un contexte cryptographique par couple d'adresses IP, tout en gardant une politique de filtrage commune. Dans un premier temps, seules deux machines communiquent entre elles. Les paquets traversent la politique de filtrage puis la politique IPsec et sont émis chiffrés.

Règles de filtrage toujours plus spécifiques que la politique IPsec



Dans le cas **C2**, un équipement est rajouté sur le réseau, la configuration du pare-feu SNS n'est pas modifiée. Les paquets à destination de cette nouvelle adresse IP sont acceptés par la politique de filtrage et non sélectionnés par la politique IPsec et les paquets sont donc émis en clair. Il y a fuite d'informations.

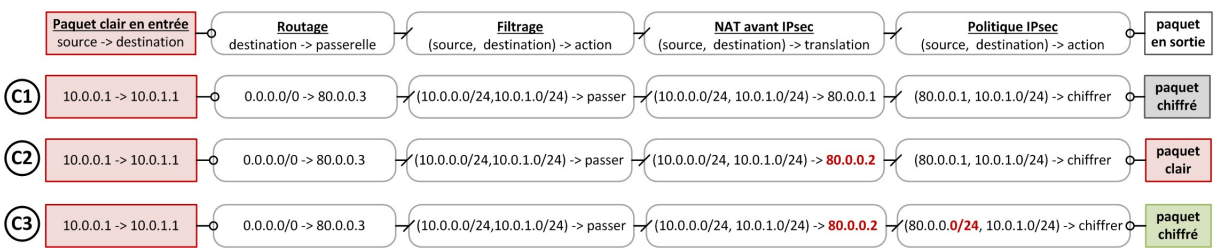
La correction mise en œuvre dans le cas **C3** consiste à positionner une politique de filtrage en /32 et une politique IPsec en /24. La politique de filtrage est ainsi plus restrictive que la politique IPsec. Les paquets seront soit filtrés soit chiffrés mais ils ne pourront pas être émis en clair.

Lorsqu'une politique IPsec est utilisée afin d'interconnecter des réseaux, sa fréquence de modification doit être faible et les réseaux utilisés peuvent être étendus contrairement à une politique de filtrage pouvant être fréquemment modifiée et très spécifique.

7.3.3 Règles de NAT avant IPsec incluses dans la politique IPsec

L'exemple représenté dans l'image ci-dessous illustre la nécessité de définir des règles de NAT avant IPsec incluses dans la politique IPsec. Dans le cas **C1**, une règle de NAT avant IPsec est appliquée. Son résultat est un critère de sélection de la politique IPsec. Toute modification de cette règle a un impact direct sur la confidentialité des données. Les paquets sont acceptés par la politique de filtrage puis modifiés par la règle de NAT avant IPsec et enfin sélectionnés par la politique IPsec. Ils sont émis chiffrés.

Règles de NAT avant IPsec incluses dans la politique IPsec



Dans le cas **C2**, la règle de NAT avant IPsec est modifiée. Les paquets sont acceptés par la politique de filtrage puis modifiés par la règle de NAT avant IPsec. L'adresse IP de sortie est modifiée, elle n'est plus sélectionnée par la politique IPsec et les paquets sont donc émis en clair. Il y a fuite d'informations.

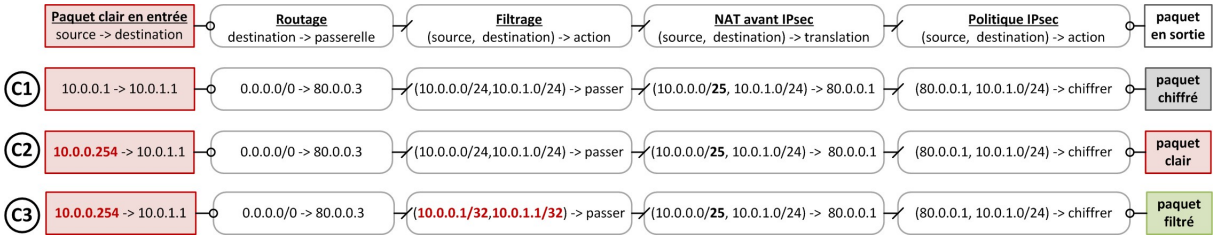
La solution présentée dans le cas **C3** consiste à définir une politique IPsec plus large que la règle de NAT utilisée. Si l'adresse IP de sortie est modifiée, le paquet sera toujours sélectionné par la politique IPsec et sera chiffré par le pare-feu SNS.

INFORMATION
La règle de NAT doit s'accompagner d'une publication ARP si la ou les adresses utilisées n'appartiennent pas aux interfaces du pare-feu SNS.

7.3.4 Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec

L'exemple représenté dans l'image ci-dessous illustre la nécessité de définir des règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec. Dans le cas **C1**, le réseau source de la règle de NAT avant IPsec est en /25 alors que le réseau source dans la règle de filtrage est en /24. Les paquets proviennent d'une adresse source incluse à la fois dans le /24 et dans le /25. Les paquets sont acceptés par la règle de filtrage, puis la règle de NAT avant IPsec est appliquée et enfin la politique IPsec. Les paquets sont émis chiffrés.

Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec



Dans le cas **C2**, l'adresse IP source est incluse dans le /24 mais non incluse dans le /25. Les paquets sont acceptés par la politique de filtrage et non sélectionnés par les règles de NAT avant IPsec. La politique IPsec n'est pas appliquée et les paquets sont donc émis en clair. Il y a fuite d'information.

La correction mis en œuvre dans le cas **C3** consiste à positionner une politique de filtrage en /32. La politique de filtrage est ainsi plus restrictive que les règles de NAT avant IPsec. Les paquets seront soit filtrés, soit chiffrés.

7.4 Politique de filtrage entrant dans le cas d'un VPN IPsec

Un attaquant sur le réseau peut envoyer des flux au pare-feu SNS en usurpant l'adresse rouge d'un correspondant légitime. Ces messages sans encapsulation doivent être identifiés et rejetés. Le blocage peut s'opérer grâce à une règle de filtrage n'autorisant le flux clair que s'il provient d'un tunnel VPN IPsec. Si le tunnel n'est pas monté, il sera systématiquement rejeté.

Dans l'édition d'une règle de filtrage, la valeur **Tunnel VPN IPsec** doit être renseignée dans le champ **Source > Configuration avancée > Via**.

Sur un pare-feu SNS, cette configuration a lieu dans le menu **Configuration > Politique de sécurité > Filtrage et NAT > Filtrage**.

Sur un serveur SMC, cette configuration a lieu dans le menu **Configuration** > **Firewalls et dossiers** > **Règles de filtrage**.

R42 | SNS-SMC | S'assurer de la provenance des flux entrants
Renseigner la provenance des flux dont la source est accessible uniquement au travers d'un tunnel VPN afin de filtrer le trafic arrivant en clair avec la même adresse source.

Par ailleurs, les politiques de sécurité de chaque tunnel VPN IPsec assurent que les flux transitent au travers du tunnel qui leur est légitime.

7.4.1 Anti-usurpation IP sur un tunnel VPN IPsec

Les extrémités de tunnels VPN IPsec sont considérées par un SNS comme une interface. À ce titre, le statut d'interface interne, expliqué dans le chapitre Anti-usurpation IP sur les interfaces réseau, leur est également applicable. Le menu **Configuration > Protection applicative > Profils d'inspection** permet d'activer l'option **Considérer les interfaces IPsec (sauf interfaces IPsec virtuelles) comme internes. S'applique à tous les tunnels : les réseaux distants devront être explicitement légitimés**. Cette option, associée à une définition des routes et des règles de filtrage, augmente la sécurité du réseau.

R43 | SNS-SMC | Déclarer l'interface VPN interne
Il est recommandé de déclarer l'interface VPN "interne" afin de profiter des mécanismes d'anti-usurpation IP.

7.5 Cas des tunnels d'accès nomade

Un tunnel VPN client-à-site est un tunnel interconnectant un équipement nomade, dont l'adresse IP de connexion est inconnue, avec un réseau local. Dans un tel cas d'usage, l'équipement nomade est à la fois le correspondant distant (qui émet et reçoit du trafic non protégé) et l'extrémité du tunnel VPN IPsec qui assure la protection du trafic émis et reçu. L'adresse IP en charge du trafic non protégé est appelée adresse IP rouge, par opposition avec l'adresse IP noire, représentant l'extrémité du tunnel.

Son fonctionnement est donc différent du fonctionnement d'un tunnel VPN site-à-site, configuré entre deux passerelles VPN dont les adresses IP noires sont a priori connues à l'avance et dont les flux à chiffrer proviennent de sous-réseaux distincts.

La configuration des tunnels nomades est réalisable à partir du menu **Configuration > VPN > VPN IPsec > Mobile - Utilisateurs nomades**. Il y est possible de laisser le correspondant choisir son adresse IP rouge, ou de lui en fournir une. Dans le premier cas, il est difficile de maîtriser les routes et les règles de filtrage, et de s'assurer qu'il n'y ait pas de conflit d'adresse entre deux correspondants. Dans le second cas, le mode *Config* permet au pare-feu SNS d'envoyer au client l'adresse IP rouge qu'il doit utiliser, protégeant des risques évoqués.

R44 | SNS | Configurer les tunnels nomades en mode *Config*
Dans le cas de tunnels nomades, il est recommandé d'utiliser le mode *Config* afin de maîtriser les adresses IP rouges distantes. Ce mode peut être défini dès la création de la politique d'accès VPN ou *a posteriori* depuis le menu **VPN > VPN IPsec > Mobile - Utilisateurs nomades**.

La mise en place de tunnels VPN nomades permet d'interconnecter des utilisateurs mobiles avec des réseaux locaux. Il est donc important de s'assurer que seuls les utilisateurs

explicitement autorisés puissent en établir. Par défaut dans un pare-feu SNS, cette autorisation est déterminée uniquement en fonction de la validité de la clé partagée ou du certificat (elle ne peut pas reposer sur l'adresse IP publique du correspondant car cette dernière n'est pas authentifiée et n'est pas connue à l'avance dans le cas d'un VPN nomade).

Dans le cadre de tunnels VPN nomades, une clé partagée doit être définie pour chaque client. Cette méthode présente plusieurs problèmes de sécurité :

- La compromission ou la suspicion de compromission de cette clé demande une modification sur l'ensemble des clients nomades,
- L'authentification des clients nomades n'est pas assurée,
- La passerelle VPN est sujette à des attaques par force brute.

R45 | SNS | Authentifier par certificat les pare-feux SNS et/ou les utilisateurs nomades
L'authentification des pare-feux SNS et/ou des utilisateurs nomades doit être basée sur l'utilisation de certificats afin de se protéger des faiblesses d'une clé partagée et conformément à la recommandation R40.

Lorsqu'une autorité de certification est renseignée comme *acceptée* dans le menu **Configuration > VPN > VPN IPsec > Identification**, l'ensemble des certificats émis par cette autorité sont autorisés à monter un tunnel VPN nomade.

R46 | SNS | Utiliser une autorité de certification intermédiaire dédiée
Afin de gérer les autorisations au service de VPN nomades, il est recommandé de n'accepter qu'une autorité de certification intermédiaire, consacrée à l'émission de certificats dédiés à l'utilisation de ce service.

De plus, l'authentification par certificat permet également d'utiliser le mécanisme d'*UAC* (User Access Control) fourni par le pare-feu SNS lorsqu'un annuaire est également utilisé. Cette fonctionnalité offre la possibilité de gérer finement les autorisations d'accès au service de VPN nomades, ainsi que les règles de filtrage et de NAT.

7.6 Dead-Peer-Detection

Ce mécanisme effectue une vérification périodique de l'état du tunnel IKE grâce à des échanges de messages chiffrés. Sur IKEv1, ce mécanisme est standardisé par la RFC 3706. Sur IKEv2, ce mécanisme a été renommé "*Liveness*" et fait partie intégrante du standard applicatif du protocole. Dans le pare-feu SNS, ce mécanisme s'appelle "*Dead-Peer-Detection*" (ou DPD) aussi bien en IKEv1 qu'en IKEv2.

Les paramètres qui conditionnent les décisions du DPD sont :

- La fréquence du test,
- Le délai d'attente de la réponse,
- Le nombre d'échecs (non-réponse) aux tests.

Si aucune réponse n'est obtenue aux tests de DPD et que donc le seuil du nombre d'échecs maximum est atteint, le tunnel VPN IKE ainsi que les tunnels VPN IPsec liés seront clôturés.

Sur IKEv2, il existe différents modes d'utilisation de ce mécanisme :

- En mode *passif*, le pare-feu SNS ne surveille pas l'état du correspondant et envoie une réponse s'il est sollicité,

- En modes *bas* ou *haut*, le pare-feu SNS surveille l'état du correspondant et envoie une réponse s'il est sollicité. En mode *haut*, les requêtes seront plus fréquentes qu'en mode *bas*.

R47 | SNS-SMC | Activer le mécanisme de Dead-Peer-Detection
Pour un tunnel VPN IPsec, il est recommandé de mettre en œuvre le mécanisme de *Dead-Peer-Detection* en mode *haut* ou *bas*.

R47 - | SNS-SMC | Utiliser le mode DPD passif
Si la mise en œuvre du *Dead-Peer-Detection* sur l'extrémité distante n'est pas connue, il est conseillé d'utiliser le mode passif permettant de répondre si une requête DPD est reçue.

7.7 KeepAlive

Lorsqu'un tunnel VPN IPsec n'est pas utilisé, il peut être clos après une durée prédéfinie afin de libérer les ressources sur les pare-feux SNS. Cependant, si du trafic doit transiter par ce tunnel, il est alors nécessaire de recommencer les négociations. Cela engendre de la latence et une légère perte de paquets. Le mécanisme de *KeepAlive* permet de générer artificiellement du trafic dans un tunnel VPN IPsec afin de maintenir ce dernier actif. Ce flux (protocole *discard*, UDP port 9) n'a pas d'utilité une fois reçu et peut être filtré sans en conserver de traces.

R48 | SNS | Configurer la fonction de KeepAlive
Il est recommandé d'activer la fonction de *KeepAlive* et de filtrer le flux émis par l'équipement distant.

Le paramétrage de cette fonction s'effectue dans le menu **Configuration > VPN > VPN IPsec > Politique de chiffrement - Tunnels** en modifiant l'intervalle de temps entre deux requêtes du mécanisme dans la colonne *KeepAlive*. La valeur *0* indique qu'il n'est pas utilisé.

7.8 Gestion du champ DSCP

Le champ DSCP, présent dans l'entête IP, est utilisé pour la gestion de la congestion. Dans le cas d'une encapsulation IPsec, le comportement par défaut d'un pare-feu SNS est de répliquer la valeur de ce champ de l'en-tête originel dans l'en-tête du paquet chiffré correspondant. La modification de ce champ peut perturber le transit du flux sur un réseau d'opérateur.

R49 | SNS-SMC | Conserver le champ DSCP
En dehors d'un besoin de sécurité renforcée, il est recommandé de conserver le paramétrage par défaut du champ DSCP.

Cependant, en cas de besoin d'un niveau de sécurité élevé, la recopie du champ DSCP peut constituer un canal caché. Il est alors important de maîtriser la valeur de ce champ avant la sortie du pare-feu SNS. Une manière de le maîtriser consiste à utiliser le pare-feu SNS pour en modifier la valeur. Cela est réalisable dans l'onglet **Qualité de service** du menu **Action** d'une règle de filtrage passante. Lorsque l'option **Forcer la valeur** est activée, le menu **Nouvelle valeur DSCP** est disponible. La valeur sélectionnée est utilisée comme valeur du champ DSCP des paquets filtrés. Cette opération est à appliquer sur les règles de filtrage des flux chiffrés sortants.

R49+ | SNS-SMC | Maîtriser le champ DSCP
Dans un contexte nécessitant un niveau de sécurité accru, il est recommandé de modifier le champ DSCP des flux sortants à une valeur arbitraire.

ATTENTION
La modification du champ DSCP d'un paquet chiffré ne peut être effective que si les règles implicites de sortie des services hébergés sont désactivées, comme expliqué dans le chapitre Règles implicites, et qu'une règle de filtrage explicite avec l'option "suivi stateful" est créée.

INFORMATION
L'opérateur de transit peut, dans son réseau, prioriser les paquets en fonction de la valeur du champ DSCP. L'utilisation de la valeur *0* permet de conserver un comportement nominal.

Dans le cas où :

- Plusieurs connexions transitent au sein d'un tunnel,
- L'extrémité distante du tunnel recopie la valeur du champ DSCP des paquets clairs sur les paquets chiffrés,
- Le traitement de la QoS sur le réseau de transit produit un réordonnancement des paquets,
- L'extrémité locale possède une fenêtre anti-rejeu trop faible,

Alors une perte de paquets légitimes peut apparaître.

Ces pertes peuvent être réduites par la modification du paramètre *ReplayWSize*. Cela peut être effectué grâce à la commande NSRPC `config ipsec profile phase2 update replaywsize=XX name=NN` où **XX** est une valeur comprise entre 0 et 33554400 par incrément de 8 et **NN** le nom du profil de chiffrement. Une analyse du réseau et des flux concernés est nécessaire pour définir le paramètre *ReplayWSize* adapté. Il est possible de se rapprocher du centre de support Stormshield pour cette analyse. Cette valeur peut être également ajoutée manuellement au fichier */Firewall/ConfigFiles/VPN/01* où la valeur *01* correspond au numéro de la politique IPsec utilisée.

8. Supervision

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

8.1 Configuration des éléments de base

L'interrogation du pare-feu SNS en SNMP nécessite la configuration d'une règle de filtrage. Seuls les serveurs de supervision doivent être autorisés à interroger le pare-feu SNS en SNMP. Cet accès se fait en lecture seule uniquement.

R50 | SNS-SMC | Filtrer l'interrogation SNMP
Il est recommandé de n'autoriser que les serveurs de supervision à interroger les pare-feux SNS en SNMP grâce à une règle de filtrage adaptée.

Sur un pare-feu SNS, les paramètres *Emplacement(syslocation)* et *Contact(syscontact)* présents dans le menu **Configuration > Notifications > Agent SNMP > Général** désignent respectivement la localisation physique du pare-feu SNS et le contact à utiliser en cas de panne. Leur configuration facilite la cartographie des pare-feux SNS dans les outils de supervision et d'alerte.

R51 | SNS | Utiliser SNMPv3
Il est recommandé d'utiliser la version 3 du protocole SNMP car elle apporte des mécanismes d'authentification et de chiffrement. SNMPv3 peut être activé depuis le menu **Configuration > Notifications > Agent SNMP > Général**.

Sur un pare-feu SNS, la configuration du champ **Connexion à l'agent SNMP** dans l'onglet SNMPv3 permet de définir les algorithmes et mots de passe utilisés pour l'authentification et le chiffrement des échanges.

R52 | SNS | Configurer la connexion à l'agent SNMP
Il est recommandé d'utiliser l'algorithme de chiffrement AES ainsi que la fonction de hachage SHA1 pour apporter aux échanges un niveau de sécurité acceptable mais cependant non conforme au RGS. Les mots de passe utilisés doivent être conformes au guide Recommandations relatives à l'authentification multifacteur et aux mots de passe.

Sur un pare-feu SNS, lorsque des correspondants sont renseignés dans le champ **Liste des serveurs SNMP** de l'onglet SNMPv3**Notifications > Agent SNMP > SNMPv3**, le pare-feu SNS leur enverra des traps SNMP.

ATTENTION
Les traps SNMP émises par le pare-feu SNS passent dans une règle de filtrage implicite. Cette règle est incluse dans la règle des services hébergés, présente dans le menu **Règles Implicites**. Il est recommandé de désactiver cette règle conformément au chapitre Règles implicites et de la remplacer par des règles personnalisées.

8.2 Interrogation du pare-feu SNS en SNMP

Voici un exemple de commande d'interrogation permettant de vérifier le bon fonctionnement de la configuration SNMPv3 d'un pare-feu SNS qui utilise les paramètres de configuration mentionnés précédemment :

```
snmpwalk -v 3 -u <user_snmp > -l authPriv -a SHA -x AES <ip_admin_SNS>
```

Des OID ainsi que leurs valeurs doivent être renvoyés par le pare-feu SNS.

ATTENTION
Il est préférable de positionner les mots de passe dans le fichier de configuration plutôt que dans la ligne de commande, puis de les supprimer.

L'utilitaire *snmpwalk* est disponible sur de nombreuses plateformes, il permet d'interroger le service SNMP d'un pare-feu SNS. Voici en détail les paramètres utilisés dans cet exemple :

-v 3	Correspond à la version du protocole SNMP utilisée.
-u <user_smp>	Correspond au paramètre **Nom d'utilisateur** renseigné sur le pare-feu SNS.
-l authPriv	Indique que la requête SNMP est chiffrée et authentifiée.
-a SHA	Précise le type de fonction de hachage utilisé pour l'authentification. Le mot de passe employé est à positionner dans le fichier de configuration. La variable à renseigner est **defAuthPassphrase**. Le mot de passe doit faire au moins 8 caractères et doit respecter les règles de robustesse présentées dans le guide Recommandations relatives à l'authentification multifacteur et aux mots de passe.
-x AES	Indique l'algorithme utilisé pour le chiffrement. Le mot de passe employé est à positionner dans le fichier de configuration. La variable à renseigner est **defPrivPassphrase**.

8.3 Utilisation d'OID spécifiques

Des indicateurs "classiques" (interface, disque, mémoire) peuvent être obtenus en interrogeant les pare-feux SNS sur des OID appartenant à la MIB standard. Il est également possible d'interroger le pare-feu SNS sur des OID spécifiques à la technologie SNS (politique, haute disponibilité, VPN). La construction de templates de supervision utilisant des indicateurs issus de ces deux MIB est recommandée afin de disposer d'une vision précise de l'état des pare-feux SNS.

Voici par exemple la requête d'interrogation SNMP permettant de récupérer le nom de la politique de filtrage réseau activée sur un pare-feu SNS :

```
snmpwalk -v 3 -u <user_snmp> -l authPriv -a SHA -x AES \ <ip_admin_SNS>
.1.3.6.1.4.1.11256.1.8.1.1.3.1
```

Le pare-feu SNS retournera une réponse de la forme :

```
iso.3.6.1.4.1.11256.1.8.1.1.3.1 = STRING : "POL-PROD-SITE1-FW1"
```

La valeur .1.3.6.1.4.1.11256.1.8.1.1.3.1 représente l'OID par lequel le nom de la politique de sécurité est accessible dans la MIB SNS. La chaîne de caractères "*POL-PROD-SITE1-FW1*" correspond au nom donné à la politique par l'administrateur du pare-feu SNS interrogé.

La liste des OID qui peut être pertinente de superviser sur un pare-feu SNS est donnée dans le tableau ci-dessous.

OID	Description
Informations générales	
.1.3.6.1.4.1.11256.1.0.1.0	Hostname
.1.3.6.1.4.1.11256.1.0.2.0	Version de Stormshield
.1.3.6.1.4.1.11256.1.0.3.0	Numéro de série
.1.3.6.1.4.1.11256.1.10.2.0	Uptime
.1.3.6.1.4.1.11256.1.10.6.1.3	Liste des alimentations et statut
HA	
.1.3.6.1.4.1.11256.1.16.2.1.4.0	État de santé du lien HA
.1.3.6.1.4.1.11256.1.16.2.1.3.0	Mode HA
CPU	
.1.3.6.1.2.1.25.3.3.1.2	Pourcentage d'utilisation du CPU durant la dernière minute
.1.3.6.1.4.1.11256.1.7.1.1.2	Liste des services actifs
Charge	
.1.3.6.1.4.1.2021.10.1.3.1	Charge durant la dernière minute
Mémoire	
.1.3.6.1.4.1.2021.4.5.0	Quantité de mémoire du pare-feu SNS
.1.3.6.1.4.1.2021.4.6.0	Quantité de mémoire actuellement disponible
Espace disque	
.1.3.6.1.2.1.25.2.3.1.5.**31**	Nombre de blocs total de /
.1.3.6.1.2.1.25.2.3.1.6.**31**	Nombre de blocs utilisés sur /
.1.3.6.1.2.1.25.2.3.1.5.**35**	Nombre de blocs total de */log*
.1.3.6.1.2.1.25.2.3.1.6.**35**	Nombre de blocs utilisés sur */log*
Interfaces réseaux	
.1.3.6.1.4.1.11256.1.4.1.1.38	Liste des interfaces
.1.3.6.1.4.1.11256.1.4.1.1.4.**2**	Adresse IP de l'interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.38.**2**	Nom système de l'interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.3.**2**	Nom personnalisé de l'interface **2**
.1.3.6.1.2.1.2.2.1.7.**2**	État administratif de l'interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.28.**2**	Débit Max en sortie sur l'interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.27.**2**	Débit Max en entrée sur l'interface **2**
.1.3.6.1.4.1.11256.1.8.1.1.3.1	Nom de la politique de filtrage active

Tunnels	
.1.3.6.1.4.1.11256.1.8.1.1.3.2	Nom de la politique IPsec active
.1.3.6.1.4.1.11256.1.13.1.1.0	Nombre de SPD entrantes
.1.3.6.1.4.1.11256.1.13.1.2.0	Nombre de SPD sortrantes
.1.3.6.1.4.1.11256.1.13.2.2.0	Nombre de tunnels VPN montés ("état Mature")
.1.3.6.1.4.1.11256.1.13.2.3.0	Nombre de tunnels VPN ("état Dying")
.1.3.6.1.4.1.11256.1.13.2.4.0	Nombre de tunnels VPN ("état Dead")

La liste complète des OID disponibles sur un pare-feu SNS est donnée par la commande suivante :

```
snmpwalk -v 3 -u <user_snmp> -l authPriv -a SHA -x AES <ip_admin_SNS> .1
```

9. Sauvegarde

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

9.1 Configuration des sauvegardes automatiques

En cas d'erreur de configuration, il est nécessaire de pouvoir rétablir rapidement une configuration saine. De plus, en cas de panne, il est nécessaire de pouvoir configurer un pare-feu SNS neuf à l'identique du précédent. Pour cela, il est recommandé de mettre en place un archivage automatique et régulier de la configuration du pare-feu SNS sur un serveur distant.

Le menu **Configuration > Système > Maintenance > Sauvegarder** permet de paramétrer l'export de la configuration du pare-feu SNS suivant trois modes :

- Export instantané sur le poste utilisé pour accéder à l'interface web d'administration,
- Export régulier à destination d'un serveur WebDAV hébergé sur internet dans une infrastructure gérée par Stormshield,
- Export régulier à destination d'un serveur WebDAV personnalisé.

Lorsqu'un WebDAV personnalisé est choisi, il est possible d'utiliser une liaison HTTP ou HTTPS. Dans ce dernier cas, il est nécessaire de fournir au pare-feu SNS le certificat utilisé par le serveur.

R53 | SNS-SMC | Mettre en place une sauvegarde automatique sur un serveur maîtrisé
Il est recommandé d'activer la fonction de sauvegarde automatique de la configuration, chiffrée et protégée par un mot de passe. Son export doit être à destination d'un serveur WebDAV personnalisé et maîtrisé via une connexion HTTPS authentifiée ou d'un serveur SMC.

Il est également possible d'activer une sauvegarde automatique locale en ligne de commande. Il n'est cependant pas possible nativement d'exporter automatiquement ces fichiers de sauvegarde sur un serveur distant (SSH par exemple). Le fichier généré localement doit être transféré à l'aide d'un script personnalisé. Par ailleurs, il ne doit pas être récupéré en SSH par une connexion initiée par un serveur distant car cela nécessiterait l'usage d'un compte administrateur du pare-feu SNS, ce qui est fortement déconseillé. Il est recommandé de réaliser un script sur le pare-feu SNS qui se connecte en SSH sur un serveur distant et transfère le fichier de sauvegarde.

R53 - | SNS | Mettre en place une sauvegarde automatique via SSH
Si un serveur WebDAV maîtrisé ou un serveur SMC n'est pas disponible, il est recommandé de configurer une sauvegarde automatique, chiffrée et protégée par un mot de passe. Celle-ci sera exportée par SSH via une connexion initiée par le pare-feu SNS.

La commande `config autobackup` permet de paramétrer et d'activer la sauvegarde locale automatique du pare-feu SNS. Voici un exemple de configuration d'une sauvegarde automatique locale chiffrée déclenchée tous les jours :

```
config autobackup set state=1 distantbackup=0 period=1d
backuppassword=<my_password>
```

Une fois cette sauvegarde paramétrée, il est nécessaire de l'activer :

```
config autobackup activate
```

La mise en place de sauvegardes automatiques à l'aide de ces commandes va générer le fichier **backup.na** dans le répertoire */data/Autobackup/*. Ce fichier est écrasé à chaque nouvelle sauvegarde, il est donc nécessaire de le transférer avant par un canal sécurisé sur un équipement distant.

ATTENTION
Le fichier de sauvegarde porte toujours l'extension **.na** qu'il soit ou non chiffré par un mot de passe. Il est identique au fichier de sauvegarde qui serait généré à partir de l'interface web d'administration (menu **Configuration > Système > Maintenance > Sauvegarder**).

9.2 Ouverture des fichiers de sauvegarde

Les fichiers de sauvegarde Stormshield (extension **.na**) ne peuvent pas être décompressés directement à partir d'un gestionnaire d'archive standard. Ce type de fichier doit être ouvert au préalable à l'aide de l'utilitaire en ligne de commande `decbackup` ; cet outil est présent sur les pare-feux SNS (disponible dans le *PATH* ou dans le dossier */usr/Firewall/sbin*) et sur le serveur SMC dans le dossier */opt/stormshield/security*. Depuis l'espace personnel MyStormshield, il est possible de télécharger des binaires, dont *decbackup*, qui permet d'ouvrir les fichiers de sauvegarde y compris lorsque l'on ne dispose pas d'un pare-feu SNS.

La syntaxe est la suivante :

```
decbackup -i backup.na -o backup.tar.gz [-p <password>]
```

Le fichier de sortie est une archive qui comprend l'ensemble des fichiers de configuration du pare-feu SNS (ceux présents dans */usr/Firewall/ConfigFiles*) ainsi que l'annuaire s'il est interne.

10. Journalisation

10.1 Politique de journalisation

Avant de configurer les journaux sur un pare-feu SNS, il est nécessaire de définir une politique de journalisation. Celle-ci devra notamment spécifier les types d'événements qui sont pertinents de journaliser ainsi que leur lieu de centralisation.

Sur un pare-feu SNS, il est possible de définir de façon indépendante :

- Les types d'événements enregistrés sur le support de stockage local lorsqu'il existe (menu **Configuration > Notifications > Traces - Syslog - IPFIX > Stockage local**). Dans ce cas, ces événements seront directement consultables à partir de l'interface web d'administration du pare-feu SNS dans l'onglet **MonitoringTraces et rapports d'activité**,
- Les types d'événements envoyés sur un (ou plusieurs) serveur(s) syslog (menu **Configuration > Notifications > Traces - Syslog - IPFIX > Syslog**). Ces événements ne sont pas directement consultables à partir de l'interface web d'administration du pare-feu SNS, ils sont destinés à être injectés dans un SIEM ou à être archivés.

R54 | SNS | Définir une politique de journalisation
Il est recommandé de définir une politique de journalisation locale et une politique de journalisation centralisée conformément au guide Recommandations de sécurité pour la mise en œuvre d'un système de journalisation.

L'espace de stockage étant limité sur le disque dur ou la carte SD du pare-feu SNS, une rotation des traces est utilisée.

Il est nécessaire de mettre en place le protocole TLS garantissant la confidentialité et surtout l'intégrité des flux de transfert des journaux, en particulier lorsque les données transitent sur des réseaux non maîtrisés.

R55 | SNS | Sécuriser le transfert des journaux avec le protocole TLS
Il est recommandé d'utiliser des protocoles de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes (conformément au guide Recommandations de sécurité relatives à TLS) en particulier lorsque les données transitent sur des réseaux non maîtrisés (conformément au guide Recommandations de sécurité pour la mise en œuvre d'un système de journalisation).

Le choix du protocole de transfert des journaux s'effectue dans **Configuration > Notifications > Traces - Syslog - IPFIX > Syslog**.

10.2 Déterminer les événements à collecter

Collecter des traces inutiles ajoute des informations à traiter lors de l'analyse des journaux, la complexifiant. Ne pas collecter des traces utiles prive au contraire d'une source d'informations capitale pour la détection d'incidents et la recherche de compromissions.

R56 | SNS | Définir les événements à collecter
Voici une liste non exhaustive des événements qu'il est recommandé de collecter par syslog parmi ceux proposé par le pare-feu SNS sur son interface web d'administration. Le cas d'usage supposé est un équipement utilisé en tant que pare-feu/VPN IPsec, l'IDS et l'IPS n'étant pas

activés :

- Les événements relatifs à la politique de filtrage (paquets rejetés, etc.),
- Les connexions réseaux,
- Les éléments relatifs aux tunnels VPN IPsec (mise en place et destruction de tunnel, etc.),
- Les événements d'authentification (tentatives avortées, réussites, échecs, etc.),
- Les événements d'administration générés par le démon serverd (connexion d'administrateurs, modification de configuration),
- Les statistiques,
- Les événements système,
- Les alarmes.

INFORMATION
Le niveau de trace avancé (journal de connexions et journal de filtrage) n'est pas adapté pour les flux TCP, UDP ou SCTP car les connexions (établies pour TCP) sur ces protocoles seront déjà tracées par défaut dans le journal des connexions.

11. Gestion du parc

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Pour l'administration de plusieurs pare-feux SNS, il est recommandé de mettre en place un SI d'administration conforme aux préconisations du guide relatif à l'administration sécurisée des SI (conformément au guide Recommandations relatives à l'administration sécurisée des systèmes d'information). Ce SI d'administration devrait notamment être utilisé pour :

- Fournir l'authentification centralisée des administrateurs telle que décrite dans le chapitre Authentification centralisée ainsi que l'IGC externe conformément au chapitre Utilisation d'une IGC,
- Accéder à distance aux services d'administration du pare-feu SNS (HTTPS, NSRPC - les outils appropriés utilisent le port TCP 1300) à partir des postes d'administration, conformément au chapitre Services d'administration,
- Transférer les journaux générés par le pare-feu SNS à destination du serveur central de journalisation, conformément au chapitre Journalisation et au guide Recommandations de sécurité pour la mise en œuvre d'un système de journalisation,
- Faire transiter les flux de supervision décrits dans le chapitre Supervision, échangés entre le pare-feu SNS et le serveur central de supervision,
- Transférer les fichiers de sauvegarde du pare-feu SNS en direction du serveur central de sauvegarde conformément au chapitre Sauvegarde.

Le serveur SMC proposé par Stormshield, entre autres, permet de mettre en œuvre ces fonctionnalités. De plus, il permet de gérer simplement un parc de pare-feux SNS important grâce à l'utilisation de fonctionnalités spécifiques telles que :

- La gestion des pare-feux SNS par dossiers,
- L'utilisation de jeux de règles de filtrage et de translation,
- La configuration de pare-feux SNS hors connexion,
- Le report des déploiements de configuration,
- La programmation de l'exécution de scripts CLI SNS sur un parc,
- etc.

12. Liste des recommandations

R1	SNS-SMC	Utiliser des comptes nominatifs
R2	SNS-SMC	Protéger le compte administrateur local
R3	SNS	Limiter l'administration par SSH
R4	SNS	Utiliser une authentification par clé SSH
R5	SNS	Authentifier localement par certificat
R6	SNS	Définir une politique de mots de passe adaptée
R7	SNS	Dédier un annuaire externe aux administrateurs
R8	SNS	Utiliser un compte d'accès restreint et sécurisé
R9	SNS	Ajuster les droits d'administration au strict nécessaire
R10	SNS-SMC	Utiliser les groupes pour gérer les droits
R11	SNS	Définir explicitement les sous-réseaux d'administration
R12	SNS	Utiliser un groupe d'objets d'administration
R13	SNS	Dédier une interface Ethernet à l'administration
R14	SNS	Conserver les suites cryptographiques
R14+	SNS	Durcir les paramètres TLS de l'interface web d'administration
R15	SNS	Remplacer le certificat de l'interface web d'administration
R16	SNS	Utiliser NSRPC depuis l'interface web
R16-	SNS	Utiliser des comptes dédiés à la connexion NSRPC directe
R17	SNS	Unifier la langue des traces et des journaux
R18	SNS-SMC	Utiliser une langue comprise par les exploitants
R19	SNS	Activer l'option Diffusion Restreinte
R19	SMC	Activer l'option Diffusion Restreinte
R20	SNS	Désactiver les interfaces non utilisées
R21	SNS-SMC	Déclarer les interfaces internes
R22	SNS	Définir des routes statiques pour les réseaux internes
R23	SNS	Compléter les règles d'anti-usurpation IP
R24	SNS	Mettre à jour depuis un miroir interne
R24-	SNS	Mettre à jour au travers d'un proxy
R25	SNS	Choisir des serveurs DNS maîtrisés
R25-	SNS	Modifier les serveurs DNS par défaut
R26	SNS	Limiter l'usage des objets dynamiques

R26	SMC	Limiter l'usage des objets dynamiques
R27	SNS-SMC	Synchroniser l'heure du système
R28	SNS-SMC	Configurer LDAP de manière sécurisée
R29	SNS-SMC	Renommer la politique de production
R30	SNS	Désactiver les règles implicites
R31	SNS-SMC	Adapter le type d'inspection de trafic au rôle du pare-feu SNS
R32	SNS-SMC	Adapter les profils d'inspection en fonction du contexte d'emploi du pare-feu SNS
R33	SNS-SMC	Utiliser des groupes d'objets
R34	SNS-SMC	Utiliser une IGC maîtrisée externe
R34-	SNS	Utiliser l'IGC du pare-feu SNS
R34-	SMC	Utiliser l'IGC du pare-feu SNS
R35	SNS-SMC	Imposer la vérification des CRL
R36	SNS	Adapter le rafraîchissement automatique des CRL
R37	SNS-SMC	Configurer l'URL de récupération de la CRL et activer la récupération automatique
R37-	SNS-SMC	Importer manuellement une CRL
R38	SNS-SMC	Utiliser des algorithmes robustes pour IKE et IPsec
R39	SNS-SMC	Utiliser la version 2 du protocole IKE
R40	SNS-SMC	Utiliser l'authentification mutuelle par certificat
R40-	SNS-SMC	Utiliser une clé partagée robuste
R41	SNS-SMC	Configurer les tunnels VPN IPsec de manière sécurisée
R41+	SNS-SMC	Ne pas utiliser de route par défaut
R42	SNS-SMC	S'assurer de la provenance des flux entrants
R43	SNS-SMC	Déclarer l'interface VPN IPsec interne
R44	SNS	Configurer les tunnels nomades en mode Config
R45	SNS	Authentifier par certificat les équipements et/ou les utilisateurs nomades
R46	SNS	Utiliser une autorité de certification intermédiaire dédiée
R47	SNS-SMC	Activer le mécanisme de Dead-Peer-Detection
R47-	SNS-SMC	Utiliser le mode DPD passif
R48	SNS	Configurer la fonction de KeepAlive
R49	SNS-SMC	Conserver le champ DSCP
R49+	SNS-SMC	Maîtriser le champ DSCP
R50	SNS-SMC	Filtrer l'interrogation SNMP

R51	SNS	Utiliser SNMPv3
R52	SNS	Configurer l'accès à l'agent SNMP
R53	SNS-SMC	Mettre en place une sauvegarde automatique sur un serveur maîtrisé
R53-	SNS	Mettre en place une sauvegarde automatique via SSH
R54	SNS	Définir une politique de journalisation
R55	SNS	Sécuriser le transfert des journaux avec le protocole TLS
R56	SNS	Définir les événements à collecter

documentation@stormshield.eu