# RECOMMANDATIONS POUR UNE CONFIGURATION SÉCURISÉE D'UN PARE-FEU STORMSHIELD NETWORK SECURITY (SNS) EN VERSION 3.7.17

## GUIDE ANSSI

ANSSI-BP-031
02/04/2021

**PUBLIC VISÉ :**

Développeur | **Administrateur** | **RSSI** | DSI | Utilisateur

# Informations

## Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations pour une configuration sécurisée d'un pare-feu Stormshield Network Security (SNS) en version 3.7.17 »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [17].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

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, l'ANSSI ne peut 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 par l'ANSSI 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.

## Évolutions du document :

| VERSION | DATE | NATURE DES MODIFICATIONS |
|---|---|---|
| 1.0 | 27/04/2016 | Version initiale |
| 2.0 | 27/12/2017 | Intégration SNS v2.7.2 |
| 3.0 | 02/04/2021 | Mise à jour des chapitres 7.2 et 8 à 11.<br>Intégration SNS v3.7.17 |

# Table des matières

# 1
# Préambule

Ce document a pour objectif de présenter les bonnes pratiques relatives au déploiement sécurisé des pare-feux Stormshield Network Security (SNS), en version physique ou en version virtuelle [1]. Les recommandations détaillées dans ce document traitent des fonctions

- d'administration ;
- de filtrage ;
- de chiffrement IPsec ;
- de supervision ;
- de sauvegarde ;
- de journalisation.

Ce document vient en complément des publications [6] et [10] de l'ANSSI relatives aux pare-feux ainsi qu'aux bonnes pratiques relatives aux interconnexions.

### 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.

## 1.1 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.
- **ASQ** : *Active Security Qualification*, moteur d'analyse des équipements Stormshield.
- **CRL** : *Certificate Revocation List*, liste de révocation de certificats.
- **CRLDP** : *CRL Distribution Point*, point de distribution de CRL.

1. Les contraintes liées à la virtualisation ainsi que les bonnes pratiques sont expliquées dans le guide [4].

- **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.
- **IKE** : *Internet Key Exchange*, protocole d'échange de clé authentifiant entre correspondants.
- **IP** : *Internet Protocol*, protocole de communication de réseaux informatiques.
- **IPsec** : *Internet Protocol Security*, cadre de standards permettant de sécuriser des communications IP.
- **IPS** : *Intrusion Prevention System*, mécanisme permettant de détecter un trafic malicieux et de le bloquer.
- **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 l'équipement en ligne de commande.
- **OID** : *Object IDentifier*, identifiant de ressource représenté par une suite de nombres entiers.
- **QoS** : *Quality of Service*, qualité de service.
- **SI** : Système d'Information.
- **SIEM** : *Security Information and Event Management*, gestionnaire d'informations de sécurité et d'évènements.
- **SNMP** : *Simple Network Management Protocol*, protocole de gestion et 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.
- **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.
- **TCP** : *Transport Control Protocol*, protocole de transport.
- **TLS** : *Transport Layer Security*, évolution de SSL.
- **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

## 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 (voir le chapitre 10 pour les recommandations liées à la journalisation) afin de s'assurer qu'elles ont été menées par un administrateur légitime et autorisé.

R1

#### 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 ou au serveur d'administration (NSRPC).

Certaines opérations exceptionnelles ne sont pas réalisables depuis un compte nominatif. Ces opérations sont par exemple :

- la modification manuelle de fichiers de configuration ;
- l'usage de `tcpdump` en vue d'une analyse du trafic réseau ;
- la modification des droits accordés aux admininistrateurs.

Un compte administrateur local non nominatif (admin) est présent sur l'équipement et peut réaliser ces actions depuis l'interface web, la console locale ou par SSH.

R2

#### Protéger le compte administrateur local

Le compte administrateur présent sur l'équipement doit disposer d'un mot de passe fort (se référer au guide [3]) 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

#### Limiter l'administration par SSH

Le service SSH étant limité au seul compte administrateur, il ne doit être activé qu'à titre exceptionnel à partir du menu `Système` → `Configuration` → `Administration du Firewall`.

R4

### Utiliser une authentification par mot de passe pour SSH

Lorsque l'accès SSH est activé à titre exceptionnel, il est recommandé d'utiliser une authentification par mot de passe et de modifier ce dernier à chaque utilisation.

## 2.1.2 Authentification locale

Les pare-feux SNS offrent la possibilité de créer un annuaire interne (menu `Utilisateurs` → `Configuration de l'annuaire`) permettant une authentification locale. Cette authentification est utilisée pour la connexion aux serveurs web et NSRPC. Dans ce cas, le pare-feu stocke les éventuels mots de passe ou leurs dérivés. Une compromission de l'équipement compromet alors également ces éléments secrets. 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. Les recommandations associées à l'utilisation de certificats sur des équipements SNS sont présentées dans la section 6. L'accès au serveur NSRPC n'autorise cependant qu'une authentification par mot de passe.

R5

### 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 équipement SNS.

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

R6

### Définir une politique de mots de passe adaptée

Si un accès NSRPC est nécessaire à un administrateur, son mot de passe doit suivre une politique conforme au guide [3] et configurée dans le menu `Système` → `Configuration` → `Configuration générale`.

## 2.1.3 Authentification centralisée

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

La solution SNS permet l'utilisation d'une solution d'authentification centralisée. Sa mise en œuvre implique la gestion des utilisateurs sur un équipement 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 est détaillée à la section 4.4.

R7

### Dédier un annuaire externe aux administrateurs

Conformément au guide relatif à l'administrations sécurisée [8], il est recommandé d'utiliser un annuaire externe et dédié à l'administration pour authentifier les administrateurs.

R8

### Utiliser un compte d'accès restreint et sécurisé

Le compte utilisé par le pare-feu pour accéder à la solution d'authentification centralisée doit être limité à cette fonction, dédié au pare-feu et faire l'object 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 de l'équipement SNS.

## 2.1.4 Droits d'accès

Un pare-feu 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 équipement, il est recommandé, dans l'idéal, de dédier un équipement pour chaque fonction et un compte d'administration afférent. Si la mutualisation d'un équipement est impérative, il convient alors de créer des comptes d'administration pour chaque fonctionnalité comme préconisé dans le guide relatif à l'administration sécurisée [8].

R9

### Ajuster les droits d'administration

Il est recommandé de ne positionner que les droits strictement nécessaires aux tâches des différents administrateurs dans le menu `Système` → `Administrateur`.

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. Chaque groupe doit correspondre à un besoin fonctionnel et bénéficier des droits adaptés sur le pare-feu. 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

### Utiliser les groupes pour gérer les droits

Il est recommandé d'utiliser les groupes pour gérer les droits d'accès aux équipements 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 à la section 2.1.1.

### Information

Différentes méthodes d'authentification centralisée sont disponibles, cependant la gestion des autorisations par groupe d'utilisateurs n'a été testée que dans le cadre d'un annuaire externe.

## 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 augmente les risques de tentative d'intrusion et de manipulation par un équipement illégitime qui y aurait accès.

**R11**

#### 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 équipement dans le menu `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 à la section 5.4, l'utilisation de tels groupes d'objets permet une meilleure gestion des autorisations, en cohérence avec les règles de filtrage.

**R12**

#### 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.

### 2.2.2 Interface d'administration dédiée

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

**R13**

#### Dédier une interface Ethernet à l'administration

Il est recommandé d'administrer un équipement SNS sur une interface Ethernet dédiée raccordée à un réseau d'administration, également dédiée à ces opérations. Le filtrage mis en œuvre devra être le plus restrictif possible.

Le guide [8] 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 participe à la sécurité de l'équipement en protégeant en confidentialité et en intégrité les flux légitimes d'administration.

Par défaut, le mode `sslparanoiac` est activé, imposant l'utilisation de TLS 1.2 et de 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-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
```

R14

#### Conserver les suites cryptographiques

Conserver la configuration par défaut des suites cryptographiques permet d'être conforme aux recommandations de l'ANSSI [9] ainsi qu'à l'annexe B1 du RGS [15].

#### Information

L'utilisation de TLS 1.2 et de suites cryptographiques robustes nécessite un navigateur Internet récent.

R14 +

#### Durcir les paramètres TLS de l'interface d'administration

Il est recommandé de conserver uniquement les suites TLS avec `ECDHE` comme préconisé par le guide TLS [9].

La restriction des suites cryptographiques peut s'effectuer à l'aide de la commande NSRPC :

```
config auth https
  cipherlist="ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-SHA256,
ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-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 est un certificat signé par l'AC NetAsq. 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

### 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 maîtrisée [2] afin de renforcer la sécurité de son accès.

La configuration du certificat serveur utilisé par l'interface web d'administration de 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 l'équipement 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 requiert l'accès en lecture à l'empreinte du mot de passe de l'utilisateur [3]. Un détournement de l'accès du pare-feu 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. L'accès à cette console ne nécessite pas d'authentification supplémentaire. L'accès aux empreintes n'est pas nécessaire.

R16

### Utiliser NSRPC depuis l'interface web

Il est recommandé d'utiliser les commandes NSRPC uniquement depuis le menu `Système` → `Console CLI` de l'interface web.

R16 -

### 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 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 l'équipement :

2. Se référer aux recommandations du RGS [12], en particulier les annexes A4 [14] et B1 [15].
3. Cette information est nécessaire au bon fonctionnement du protocole d'authentification utilisé.

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

La langue des traces et des journaux modifie les messages disponibles dans le `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 l'éditeur.

L'ensemble des messages existants est répertorié dans le menu `Notifications` → `Evènements systèmes` et leurs traductions sont disponibles dans le dossier `/usr/Firewall/System/Language/` de l'équipement. 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**

### Unifier la langue des traces et des journaux

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

**R18**

### Utiliser une langue comprise par les exploitants

Il est conseillé de configurer un équipement dans une langue maîtrisée par les exploitants.

### Information

La base de connaissance de l'éditeur Stormshield est composée en grande partie de pages en anglais. Cette base est accessible depuis l'espace personnel Stormshield [1].

## 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 [16]. En particulier, la gestion des primitives cryptographiques matérielles doit être adaptée lorsque que 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 équipés de tels (co)processeurs.

**R19**

### Activer l'option Diffusion Restreinte

Il est nécessaire d'activer le mode `Diffusion Restreinte` dans le menu `Système` → `Configuration` → `Configuration générale` lorsque le pare-feu est positionné

sur un réseau de cette même sensibilité et que ses fonctions cryptographiques sont exploitées.

### Information

Certains modèles de pare-feu SNS utilisent un processeur dont le jeu d'instructions cryptographiques offre des garanties suffisantes pour protéger des données de niveau DR. Il est conseillé de se rapprocher de l'éditeur Stormshield afin de connaître la liste des équipements concernés.

# 3
# Configuration réseau

## 3.1 Désactivation des interfaces non utilisées

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

R20

### Désactiver les interfaces non utilisées

Il est recommandé de désactiver les interfaces réseau non utilisées depuis le menu `Réseau → Interfaces`.

## 3.2 Configuration de l'antispoofing IP

### 3.2.1 Principe de l'antispoofing IP

Le *spoofing* IP 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 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'*antispoofing* 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'*antispoofing* IP est extrêmement efficace pour détecter des erreurs de configuration réseau (mauvaise configuration de règles de routage par exemple).

### 3.2.2 Antispoofing sur les interfaces réseau

Un pare-feu SNS utilise la notion d'interface « interne » pour identifier les interfaces qui alimentent le mécanisme d'*antispoofing*. Le menu `Réseau → Interface → Configuration de l'interface` permet de configurer le type d'interface : un bouclier apparaît lorsqu'une interface est protégée par l'*antispoofing*. 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 refuseront ces mêmes paquets en entrée. Ces règles d'*antispoofing* sont appliquées avant même l'évaluation de la politique de filtrage réseau.

#### Information

Il est possible de compléter la liste des adresses IP autorisées à accéder à une interface « interne » en utilisant l'*antispoofing* par la table de routage décrit à la section 3.2.3.

R21

#### Déclarer les interfaces internes

Afin de profiter des mécanismes d'*antispoofing*, il est recommandé de déclarer une ou plusieurs interfaces « interne ».

#### Attention

Des règles implicites de filtrage autorisent l'administration des équipements à partir des interfaces internes. Ces règles devront êtres désactivées comme expliqué à la section 5.2.

### 3.2.3 Antispoofing par la table de routage

La définition des routes statiques renseigne le pare-feu sur la topologie réseau et complète implicitement les mécanismes d'*antispoofing*. Toute route à destination d'un réseau distant joignable par une interface « interne » est ajoutée aux tables d'*antispoofing*. 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. 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

#### 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 n'appartiennent pas afin de profiter des mécanismes d'*antispoofing*. Ces routes sont reconnaissables dans le menu `Réseau → Routage → Routage statique` par la présence d'un bouclier.

#### Attention

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

### 3.2.4 Antispoofing sur un bridge

Un *bridge* permet de connecter plusieurs interfaces physiques sur un même réseau. Le pare-feu applique toutefois ses mécanismes d'*antispoofing* indépendamment sur chacune des interfaces du *bridge*. Cette fonctionnalité d'*antispoofing* 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, 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 envoyé par un équipement. L'*antispoofing* 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'*antispoofing* par la table de routage détaillé au paragraphe 3.2.3 est employé.

### 3.2.5 Règles complémentaires

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

R23

#### Compléter les règles d'antispoofing

Il est recommandé de compléter autant que possible les règles d'*antispoofing* 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 équipement SNS nécessitent des mises à jour régulières (activées par défaut dans le menu `Système` → `Active Update`). L'absence totale de mises à jour empêcherait le pare-feu 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 d'équipements 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 d'équipements autorisés à accèder à Internet.

**R24**

### 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, 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 de l'équipement (filtrage d'URL et de flux IP strictement nécessaires aux opérations de mise à jour d'équipements SNS [4]).

**R24 -**

### Mettre à jour au travers d'un proxy

En l'absence de miroir interne, l'équipement 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.

4. À savoir les URL update{1,2,3,4}.stormshield.eu et licence{1,2,3,4}.stormshield.eu.

R25

## Choisir des serveurs DNS maîtrisés

Il est recommandé de configurer des résolveurs DNS maîtrisés dans le menu `Système → Configuration → Paramètres réseaux`

R25 -

## 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 équipement 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. Il en existe par défaut une quinzaine qui portent un nom se terminant par netasq.com ou stormshield.eu dont une partie est représentée sur la figure 4.1 [5]. Cela génère des requêtes DNS inutiles et intempestives qui ne peuvent pas être bloquées par des règles de filtrage.

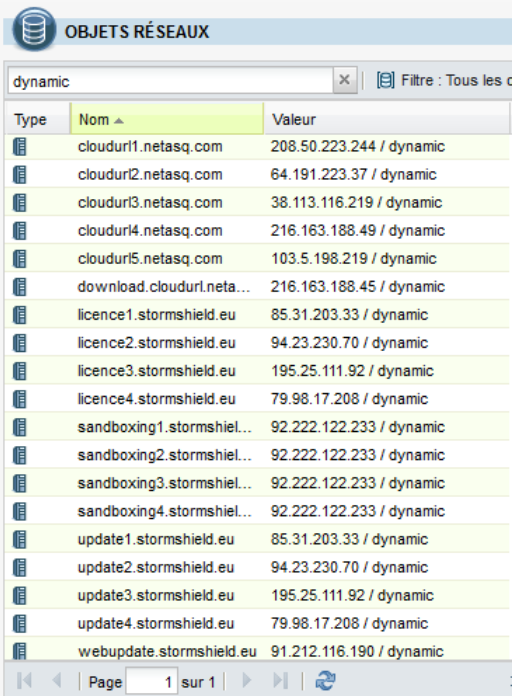


FIGURE 4.1 – Liste des objets dynamiques de type « Machine ».

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

R26

## 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 `Objets → Objets réseaux`.

5. Ces noms peuvent évoluer en fonction des mises à jours de l'éditeur.

## 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**

### Synchroniser l'heure du système

Il est recommandé d'activer la synchronisation NTP des équipements SNS et d'utiliser plusieurs serveurs de temps fiables, conformément à la note technique sur la journalisation [5].

## 4.4 Utilisation d'un annuaire externe

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

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

**R28**

### Configurer LDAP de manière sécurisée

Si le service LDAP est configuré, il est recommandé :

- d'utiliser le protocole LDAPS ;
- d'installer un certificat provenant d'une IGC maîtrisée sur le serveur LDAP ;
- d'importer l'AC correspondante sur l'équipement SNS ;
- 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 de l'annuaire`), 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 sur l'annuaire. Ce compte doit respecter la recommandation R8 ;
- définir la structure de l'annuaire (onglet `Structure`). La correspondance entre les attributs manipulés par l'équipement 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 équipement SNS ne portent pas de nom explicite, à l'exception de deux d'entre-elles (Pass all, Block all). Cette pratique ne permet pas à un administrateur de facilement comprendre le rôle du pare-feu, 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 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 présents au sein du SI.

R29

### Renommer la politique de production

Il est recommandé d'appliquer une politique de nommage des profils de filtrage réseau comme détaillé dans le guide relatif à la définition d'une politique de filtrage [6].

## 5.2 Règles implicites

Par défaut, le pare-feu 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 `Politique de sécurité → Filtrage et NAT` ne contient alors pas toutes les règles appliquées par le pare-feu. 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

### Désactiver les règles implicites

Il est recommandé de désactiver la totalité des règles de filtrage implicites, incluant celles concernant les flux sortants issus des services hébergés par le pare-feu. Cela se réalise dans le menu `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 et les groupes définis à la section 2.2.1 sur les interfaces définies à la section 2.2.2.

### 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 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. L'équipement 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 disponibles : Firewall, IPS ou IDS.

Au niveau Firewall, le pare-feu 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 Firewall, lorsqu'une session est abandonnée par le pare-feu, il 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 IPS, le pare-feu 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 IDS réalise les mêmes inspections que le niveau IPS, mais ne lèvera que des alarmes si du trafic semble malveillant, sans le bloquer. Le niveau 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 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 l'équipement. 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 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 [6], nous utiliserons la dénomination « mode applicatif qualifié ».

Le niveau IPS en mode automatique est sélectionné par défaut à la création d'une règle de filtrage. Cependant, le chargement de modules d'analyses protocolaires augmente la charge processeur du pare-feu ainsi que sa surface d'attaque. 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.

**R31**

### Adapter le type d'inspection de trafic au rôle de l'équipement

Il est recommandé d'utiliser les niveaux Firewall, IPS en mode transport ou IPS en mode applicatif qualifié en cohérence avec le rôle joué par l'équipement 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.

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

- si l'équipement 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 Firewall permet de dédier ses ressources aux fonctions cryptographiques tout en réduisant sa surface d'attaque ;
- si le pare-feu est situé entre un SI d'entreprise et le réseau Internet, le niveau IPS en mode transport permet de limiter la surface d'attaque de l'équipement tout en assurant un filtrage fin des connexions ;
- si le pare-feu protège des serveurs applicatifs joignables uniquement depuis le réseau interne d'une entreprise, le niveau IPS en mode applicatif qualifié peut être utilisé.

La colonne `Inspection de sécurité` des règles de filtrage (menu `Filtrage et NAT`) permet de choisir le niveau d'inspection, Firewall, IPS ou IDS. Dans les cas de l'IPS et de l'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 l'équipement agira. Un seul protocole (applicatif ou de transport) peut être choisi par règle de filtrage.

Les niveaux IPS et IDS reposent sur l'utilisation de Profils d'inspection. Ces profils permettent de configurer le comportement du pare-feu en fonction du trafic traité (types d'alarmes à lever,

6. Il s'agit des modules liés aux protocoles suivants : FTP, HTTP (incluant WebDAV), SIP, SMTP, DNS, Modbus, S7 et UMAS.

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**

### Adapter les profils d'inspection en fonction du contexte d'emploi du pare-feu

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` en entrée et le profil `01` en sortie. Le choix du profil se fait à chaque règle de filtrage, à l'onglet `Inspection de sécurité`. La configuration de ces profils se fait dans le menu `Protection applicative` → `Profils d'inspection`, en sélectionnant `Accèder aux profils`. Chaque profil est alors basé sur les politiques définies au menu `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 `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 équipement Stormshield, 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 à la section 2.2.1) et au sein d'une règle de filtrage explicite corrélée (conformément à la section 5.2).

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**

### 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 un guide spécifique [6]. 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 équipements SNS, dont :

- la publication de l'interface d'administration web en HTTPS ;
- l'authentification par certificat des administrateurs pour l'accès à l'interface web d'administration de 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.

## 6.1 Utilisation d'une IGC

Lorsqu'un équipement 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 certificats signés par cette autorité. Dans ce cas, les clés privées sont générées par et stockées sur le pare-feu. La compromission du pare-feu impliquera alors de fait celle des éléments secrets générés par l'équipement.

**R34**

### Utiliser une IGC maîtrisée externe

Il est recommandé d'utiliser une IGC maîtrisée externe à l'équipement SNS pour générer les certificats utilisés par le pare-feu. Cette IGC ainsi que les AC utilisées doivent être conformes aux préconisations du RGS [13].

**R34 -**

### Utiliser l'IGC de l'équipement

En l'absence d'IGC externe, il est possible d'utiliser l'IGC présente dans l'équipement. Dans ce cas

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

### Attention

Lorsque l'IGC interne à l'équipement est configurée, la compromission de l'équipement SNS 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 équipements les moins exposés possible à des réseaux non maîtrisés.

## 6.2 Gestion des CRLs dans le cadre d'un tunnel 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. La mise en place par l'IGC de CRLs permet d'avertir les équipements concernés de la révocation de certificats. Par défaut l'absence de CRL n'est pas bloquante pour établir un VPN IPsec, elle est simplement signalée dans les journaux de l'équipement.

R35

### Imposer la vérification des CRLs

Il est recommandé d'imposer la vérification de CRLs pour la mise en œuvre des tunnels 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 la commande :

```
envpn 00 && envpn 01
```

Dans les deux cas, la valeur `01` utilisée en exemple représente le numéro de la configuration IPsec employée.

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

### 6.2.1 Importation automatique de CRLs

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 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

### Adapter le rafraichissement automatique des CRLs

Il est recommandé d'adapter le temps de rafraichissement 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 ajoutée et activée, 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 console `checkcrl`. Il est également possible de modifier la fréquence de récupération des CRLs via l'interface d'administration.

Par ailleurs, le champ `CRLDP` contenu dans le certificat d'une AC n'est pas exploité par un pare-feu SNS. Il ne permet donc pas de configurer automatiquement ses points de distribution lors de l'importation d'une AC.

R37

### 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 `Système` → `Configuration`.

Les points de distribution de CRLs associées à une AC peuvent être positionnés soit via l'interface web d'administration de SNS en éditant l'onglet `CRL` de l'AC concernée, soit en ligne de commande grâce à la commande :

```
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 l'équipement puisse résoudre le FQDN de l'URL du point de distribution de la CRL, un objet de type `host` correspondant au FQDN doit être défini dans la base d'objets de l'équipement.

## 6.2.2 Importation manuelle de CRL

Dans certians 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'importation d'une CRL peut alors être réalisée 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 -

### Importer manuellement une CRL

Si une importation automatique est impossible, il est recommandé d'importer manuellement la CRL.

L'importation manuelle d'une CRL s'effectue via l'interface web d'administration, dans le menu `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'importation, 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`.

# 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 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 (menu `VPN` → `VPN IPsec` → `Profils de chiffrement`) permet d'expliciter les algorithmes autorisées. Bien que le profil pré-configuré *StrongEncryption* soit compatible avec les exigences du RGS [15], il est conseillé de redéfinir manuellement des profils de chiffrement IKE et IPsec.

Les tableaux 7.1 et 7.2 donnent des exemples de profil de chiffrement compatibles 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.

| Paramètre | Valeur |
|---|---|
| Algorithme de chiffrement | AES-GCM 256 |
| Fonction de hachage | SHA 384 |
| Groupe Diffie-Hellman | Groupe 19 (256 bits) |
| Cryptopériode | 21600s |

TABLE 7.1 – Exemple de profil de chiffrement IKE 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 |

TABLE 7.2 – Exemple de profil de chiffrement IPsec compatible avec le RGS

R38

### 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.

## 7.2 Échange de clés et authentification

### 7.2.1 Protocole IKE

Le niveau de protection offert par un tunnel IPsec dépend de la robutesse de la suite cryptographique mise en place ansi 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 IPsec [7].

R39

### Utiliser la version 2 du protocole IKE

Si tous les correspondants des tunnels IPsec sont compatibles, il est recommandé d'utiliser le protocole IKE dans sa version 2.

### 7.2.2 Négociation en IKEv1

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

Dans le cas d'utilisation de la version 1 du protocole IKE, deux modes de négociation sont proposés par l'équipement SNS :

- le mode « principal » disponible lors d'une authentification par certificats ou par clé partagée ;
- le mode « aggressif » disponible lors d'une authentification par clé partagée lorsque les identités des deux extrémités (*local ID*, *remote ID*) sont renseignées.

La méthode « aggressive » est plus rapide. Cependant, les identités des extrémités sont transmises en clair. L'anonymat des correspondants n'est donc pas assuré.

R39 -

### Utiliser le mode de négociation « principal » en cas d'utilisation d'IKEv1

L'utilisation du mode agressif est vulnérable. Il est donc recommandé d'utiliser le mode de négociation dit « principal » lors de l'utilisation de l'IKEv1.

Ce choix n'existe pas en cas d'utilisation d'IKEv2.

### 7.2.3 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 clef 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 équipements configurés. Seule l'utilisation d'une IGC permet une identification de chaque correspondant et une gestion aisée des droits et des révocations.

R40

### 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 `VPN` → `VPN IPsec` → `Identification`.

R40 -

### 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 du RGS [11] et du guide relatif aux mot de passe [3].

### 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 [7] (22 caractères aléatoires parmi les minuscules, les majuscules et les chiffres) ;
- le secret doit respecter les règles relatives à la génération des mots de passe décrites dans le guide de l'ANSSI [3] ;
- un secret différent doit être utilisé pour chacun des tunnels site-à-site ;
- le secret doit être renouvelé régulièrement, sa cryptopériode [8] 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 l'équipement SNS est utilisé en tant que passerelle VPN, la bonne définition des règles de routage et 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.

7. Se référer à l'annexe B1 du RGS pour plus de précisions [15].
8. Durée maximale durant laquelle perdre la confidentialité et l'intégrité du trafic est accepté si le secret venait à être compromis.

Dans le cadre de la mise en œuvre de tunnels 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 [9] (par exemple, un objet de type machine ayant comme adresse 127.42.42.42). Après l'application de la politique de IPsec, la politique de routage sera réévaluée 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 la figure 7.1 a un impact direct sur la confidentialité des flux [10]. 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.


FIGURE 7.1 – Briques fonctionnelles

R41

## Configurer les tunnels 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 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 règles de NAT avant IPsec sont toujours incluses dans 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 équipements 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 IPsec établi avec une passerelle VPN distante. L'architecture est représentée sur la figure 7.2.

9. Cette technique est également appelée *blackholing*.
10. Ce séquencement n'est qu'une partie du cheminement complet du paquet dans l'équipement. En effet, lorsqu'il est chiffré, le paquet est ensuite traité par les fonctions de routage, de filtrage, de NAT après IPsec.

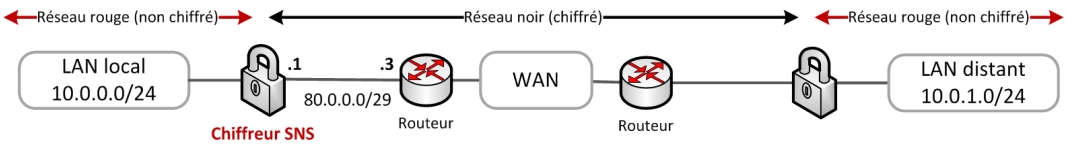


FIGURE 7.2 – Schéma d'architecture

Dans chaque exemple sont données les configurations des briques fonctionnelles SNS traversées par un paquet réseau (Figure 7.1). Le paquet réseau rentre avec une source et une destination spécifiques . Les fonctions traversées sont, dans l'ordre :

- le 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 figure 7.3 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 [11], elle contient une route valide vers la passerelle IPsec (la route par défaut). Les paquets sont émis chiffrés.

11. La route à destination du LAN distant n'est pas utilisée. Seule la route à destination de la passerelle VPN distante est utilisée.

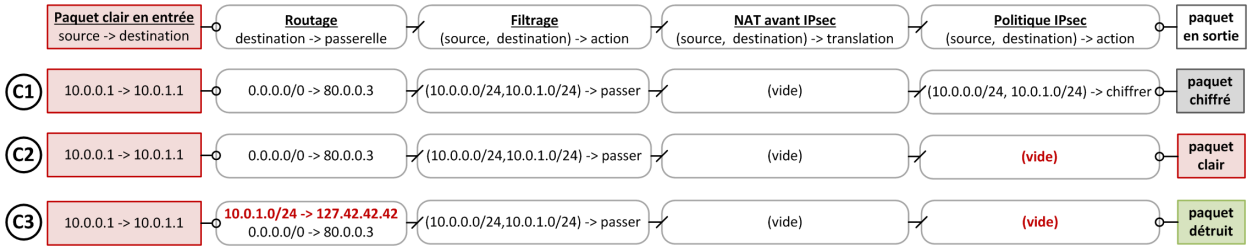


FIGURE 7.3 – Politique IPsec toujours active, route à destination de la boucle locale

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 [12], également appelée *blackholing*. En l'absence de politique IPsec, le paquet sera détruit par l'équipement au lieu d'être envoyé à la passerelle par défaut.

R41 +

### 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 la figure 7.2, et pour faciliter la création des routes.

### Attention

Un avertissement "la passerelle n'est pas routable" est généré lorsque une route à destination de la boucle locale en 127.0.0.0/8 est définie.

## 7.3.2 Règles de filtrage toujours plus spécifiques que la politique IPsec

L'exemple représenté figure 7.4 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

12. Prendre une adresse IP particulière facilite la maintenance de la configuration (par exemple, 127.42.42.42).

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.

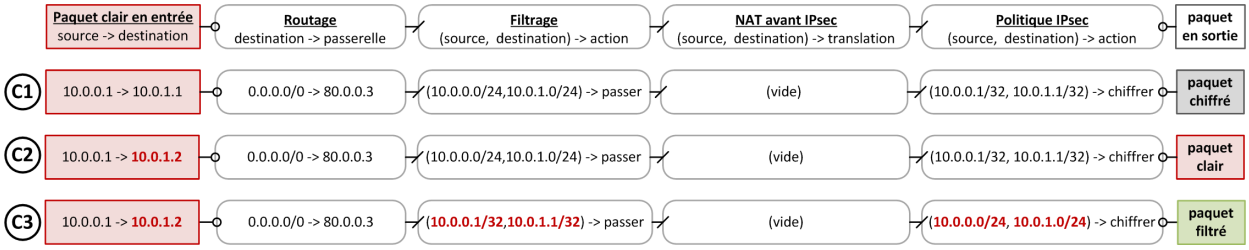


FIGURE 7.4 – Règles de filtrage toujours plus spécifiques que la politique IPsec

Dans le cas **C2**, un équipement est rajouté sur le réseau, la configuration du pare-feu 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 figure 7.5 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.

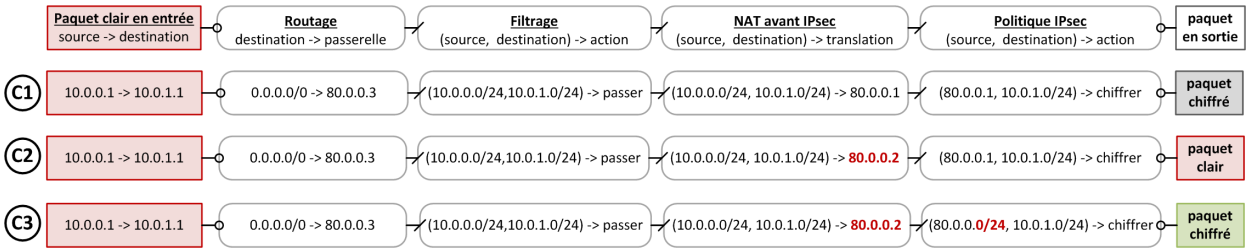


FIGURE 7.5 – Règles de NAT avant IPsec incluses dans la politique IPsec

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 l'équipement.

### 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.

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

L'exemple représenté figure 7.6, 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.

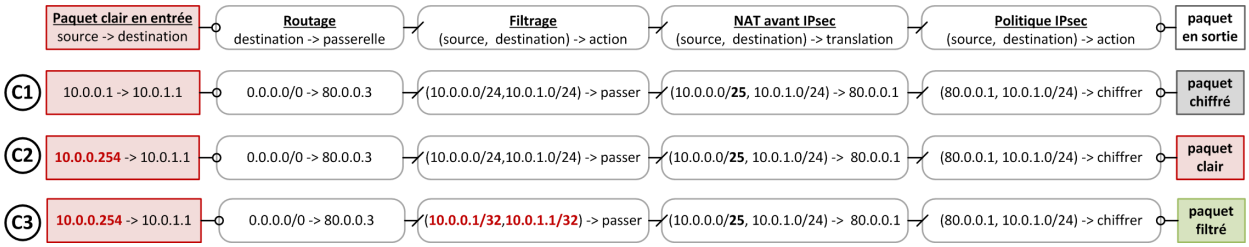


FIGURE 7.6 – Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec

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 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. Cette configuration a lieu dans le menu `Politique de sécurité` → `Filtrage et NAT` → `Filtrage` : dans l'édition

d'une règle de filtrage, la valeur `Tunnel VPN IPsec` doit être renseignée dans le champ `Source` → `Configuration avancée` → `Via`.

**R42**

### 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 IPsec assurent que les flux transitent au travers du tunnel qui leur est légitime.

## 7.4.1 Antispoofing sur un tunnel IPsec

Les extrémités de tunnels VPN IPsec sont considérées par un SNS comme des interfaces. À ce titre, le statut d'interface interne, expliqué à la section 3.2.2, leur est également applicable. Le menu `Protection applicative` → `Profils d'inspection` permet d'activer cette option, qui, associée à une définition des routes et des règles de filtrage, augmente la sécurité du réseau.

**R43**

### Déclarer les interfaces VPN internes

Il est recommandé de déclarer les interfaces VPN « internes » afin de profiter des mécanismes d'*antispoofing*.

# 7.5 Cas des tunnels d'accès nomade

Un tunnel 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 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 site-à-site, configuré entre deux passerelles VPN dons 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 `VPN` → `VPN IPsec` → `Anonyme - 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**

### 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 → Anonyme - 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 équipement SNS, cette autorisation est déterminée uniquement en fonction de la validité de la clé partagée ou du certificat [13].

Dans le cadre de tunnels VPN nomades, une seule clé partagée peut être définie pour l'ensemble des clients. 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**

### Authentifier par certificat les équipements et/ou les utilisateurs nomades

L'authentification des équipements 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 `VPN → VPN IPsec → Identification`, l'ensemble des certificats émis par cette autorité sont autorisés à monter un tunnel VPN nomade.

**R46**

### 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* fourni par l'équipement 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. Si un correspondant ne répond pas aux requêtes envoyées par son pair, il sera alors considéré comme injoignable et l'émetteur clora le tunnel IKE de son côté ainsi que les tunnels IPsec liés. Il existe différents modes d'utilisation de ce mécanisme :

13. Elle ne peut pas reposer sur l'adresse IP publique du correspond car cette dernière n'est pas authentifiée et n'est pas connue à l'avance dans le cas d'un VPN nomade.

- en mode *inactif*, le pare-feu ne surveille pas l'état du correspondant et n'envoie pas de réponse s'il est sollicité ;
- en mode *passif*, le pare-feu ne surveille pas l'état du correspondant et envoie une réponse s'il est sollicité ;
- en modes *bas* ou *haut*, le pare-feu 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

### Activer le mécanisme de Dead-Peer-Detection

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

R47 -

### 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 IPsec n'est pas utilisé, il peut être clos après une durée prédéfinie afin de libérer les ressources sur les équipements. 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 IPsec afin de maintenir ce dernier actif. Ce flux n'a pas d'utilité une fois reçu et peut être filtré sans en conserver de traces.

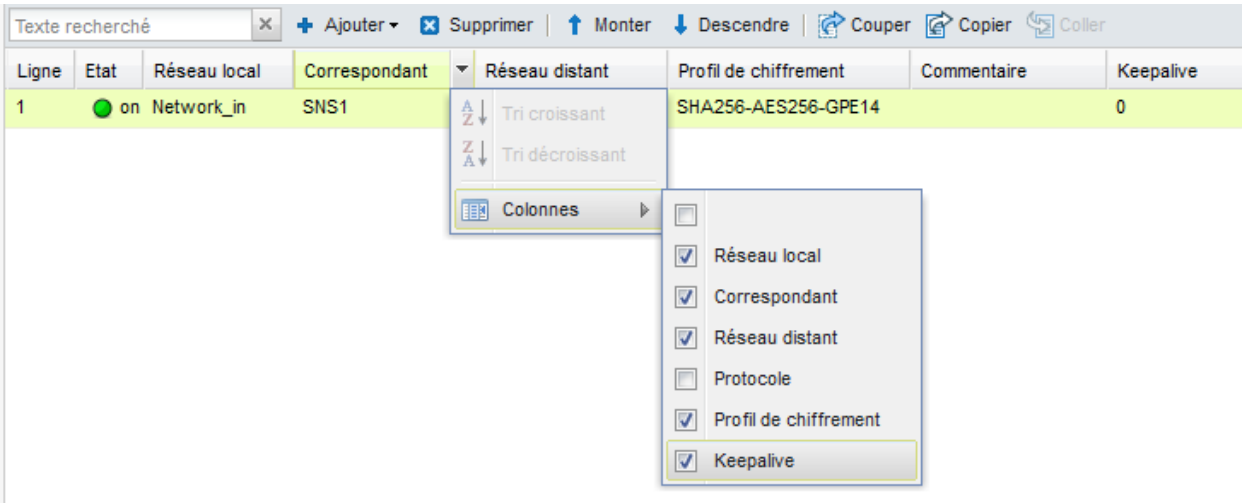


FIGURE 7.7 – Affichage du champ *KeepAlive*

R48

### 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 paramètrage de cette fonction s'effectue dans le menu `VPN` → `VPN IPsec` → `Politique de chiffrement - Tunnels` tel que représenté sur la figure 7.7. En survolant l'entête d'une colonne quelconque du tableau, une flèche apparaît. Cliquer dessus puis aller dans le menu `Colonnes` permet de choisir d'afficher la colonne *KeepAlive*. Il est alors possible de modifier l'intervalle de temps entre deux requêtes du mécanisme. La valeur zéro 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

### Conserver le champ DSCP

En dehors d'un besoin de sécurité renforcée, il est recommandé de conserver le paramètrage 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. Une manière de le maîtriser consiste à utiliser l'équipement 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 +

### 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 à la section 5.2, et qu'une règle de filtrage explicite 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` où XX est une valeur comprise entre 0 et 33554400 par incrément de 8. Cette valeur peut être également ajouté manuellement au fichier `/Firewall/ConfigFiles/VPN/01` où la valeur 01 correspond au numéro de la configuration IPsec utilisée.

# 8
# Supervision

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

## 8.1 Configuration des éléments de base

L'interrogation de l'équipement en SNMP nécessite la configuration d'une règle de filtrage dans le menu `Politique de sécurité` → `Filtrage et NAT` → `Filtrage`. Seuls les serveurs de supervision doivent être autorisés à interroger l'équipement en SNMP. Cet accès se fait en lecture seule uniquement.

**R50**

### Filtrer l'interrogation SNMP

Il est recommandé de n'autoriser que les serveurs de supervision à interroger les équipements en SNMP grâce à une règle de filtrage adaptée.

Les paramètres `Emplacement(syslocation)` et `Contact(syscontact)` présents dans le menu `Notifications` → `Agent SNMP` → `Général` désignent respectivement la localisation physique de l'équipement et le contact à utiliser en cas de panne. Leur configuration facilite la cartographie des équipements dans les outils de supervision et d'alerte.

**R51**

### Utiliser SNMPv3

Il est recommandé d'utiliser la version 3 du protocole SNMP car elle apporte des mécanismes d'authentification et de chiffrement.

La configuration du champ `Connexion à l'agent SNMP` du menu `Notifications` → `Agent SNMP` → `SNMPv3`. permet de définir les algorithmes et mots de passe utilisés pour l'authentification et le chiffrement des échanges.

**R52**

### Configurer l'accès 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 relatif à leur sécurité [3].

Lorsque des correspondants sont renseignés dans le champ `liste des serveurs SNMP` du menu `Notifications` → `Agent SNMP` → `SNMPv3`, le pare-feu leur enverra des traps SNMP.

### Attention

Les traps SNMP émises par l'équipement 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 à la section 5.2 et de la remplacer par des règles personnalisées.

## 8.2 Interrogation de l'équipement en SNMP

Voici un exemple de commande d'interrogation permettant de vérifier le bon fonctionnement de la configuration SNMPv3 d'un équipement 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 l'équipement.

### 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 équipement, 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 l'équipement ;

`-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` [14] ;

`-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 équipements SNS sur des OID appartenant à la MIB standard ; il est également possible d'interroger l'équipement sur des OID spécifiques [15] à la technologie SNS (politique, haute disponibilité, VPN) [2]. 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.

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

14. Le mot de passe doit faire au moins 8 caractères et doit respecter les règles de robustesse présentées dans la note technique relative à la sécurité des mots de passe [3].

15. La documentation de la MIB SNS est disponible à l'adresse `https://www.stormshield.com/products-services/services/mibs/`.

```
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 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 chaine de caractères `"POL-PROD-SITE1-FW1"` correspond au nom donné à la politique par l'administrateur du pare-feu interrogé.

La liste des OID qui peut être pertinente de superviser sur un équipement SNS est donnée dans le tableau 8.1.

| 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 de l'équipement |
| .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”) |

TABLE 8.1 – Liste des OID Stormshield

La liste complète des OID disponibles sur un équipement Stormshield 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 équipement neuf à l'identique du précédent. Pour cela, il est recommandé de mettre en place un archivage automatique et régulier de la configuration du SNS sur un serveur distant.

Le menu `Système` → `Maintenance` → `Sauvegarde` permet de paramétrer l'export de la configuration de l'équipement 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 le certificat utilisé par le serveur.

R53

### Mettre en place une sauvegarde automatique sur un serveur maîtrisé

Il est recommandé d'activer la fonction de sauvegarde automatique de la configuration et son export vers un serveur WebDAV personnalisé et maîtrisé via une connexion HTTPS authentifiée.

### Attention

Dans le cas où un serveur WebDAV personnalisé est utilisé avec une liaison HTTPS, le pare-feu vérifie l'identité du serveur de destination en comparant le certificat renseigné à la ligne `Certificat du serveur` avec celui fournit par le serveur. Il ne vérifie cependant pas la validité du certificat (validité temporelle ou si cela correspond à un usage autorisé par exemple).

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 du compte admin de l'équipement, ce qui

est fortement déconseillé. Il est recommandé de réaliser un script sur l'équipement SNS qui se connecte en SSH sur un serveur distant et transfère le fichier de sauvegarde.

R53 -

### Mettre en place une sauvegarde automatique via SSH

Si un serveur WebDAV maîtrisé 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 l'équipement.

La commande `config autobackup` permet de paramétrer et d'activer la sauvegarde locale automatique de l'équipement. 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.enc 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 `.enc` 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 `Système` → `Maintenance` → `Sauvegarder`).

## 9.2 Ouverture des fichiers de sauvegarde

Les fichiers de sauvegarde Stormshield (extension `.na` ou `.na.enc`) 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 équipements (disponible dans le `PATH` ou dans le dossier `/usr/Firewall/sbin`). Il est également disponible sous Linux [16], ce qui permet d'ouvrir les fichiers de sauvegarde y compris lorsque l'on ne dispose pas d'un équipement SNS.

La syntaxe est la suivante :

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

Le fichier de sortie est une archive qui comprend l'ensemble des fichiers de configuration de l'équipement (ceux présents dans `/usr/Firewall/ConfigFiles`) ainsi que l'annuaire s'il est interne.

16. Il faut en faire la demande à l'éditeur.

# 10 Journalisation

## 10.1 Politique de journalisation

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

Sur un équipement SNS, il est possible de définir de façon indépendante :

- les types d'évènements enregistrés sur le support de stockage local lorsqu'il existe (onglet `Stockage local` du menu `Notifications → Traces - syslog`). Dans ce cas, ces évènements seront directement consultables à partir de l'interface web d'administration de l'équipement SNS à la page `Traces et rapports d'activité`;
- les types d'évènements envoyés sur un (ou plusieurs) serveur(s) syslog (onglet `Syslog` du menu `Traces - syslog`). Ces évènements ne sont pas directement consultables à partir de l'interface web d'administration de l'équipement SNS, ils sont destinés à être injectés dans un SIEM ou à être archivés.

**R54**

### Définir une politique de journalisation

Il est recommandé de définir une politique de journalisation locale et une politique de journalisation centralisée conformément au guide relatif à la mise en œuvre d'un système de journalisation[5].

L'espace de stockage est limité sur le disque dur ou la carte SD de l'équipement. Le pare-feu propose donc un arrêt de l'écriture des traces ou l'effacement automatique des traces les plus anciennes en cas de saturation du support de stockage. L'arrêt de l'écriture permet de conserver les traces anciennes mais d'éventuelles nouvelles traces ne sont pas disponibles en cas d'attaque récente.

**R55**

### Activer la rotation des traces

Il est recommandé de mettre en place une rotation automatique des traces.

Le choix du comportement se fait sur la page `Notifications → Traces - syslog → Stockage local`.

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 maitrîsés.

R56

### Sécuriser le transfert des journaux avec le protocole TLS

Il est recommandé d'utiliser des protocoles[9] de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes en particulier lorsque les données transitent sur des réseaux non maîtrisés[5].

Le choix du protocole de transfert des journaux s'effectue dans `Notifications` → `Traces - Syslog - IPFIX` → `Syslog`.

## 10.2 Déterminer les évènements 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.

R57

### Évènements à collecter

Voici une liste non exhaustive des types d'évènements qu'il est recommandé de collecter par syslog parmi ceux proposé par l'équipement sur son interface 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 évènements relatifs à la politique de filtrage (paquets rejetés, etc.) ;
- les connexions réseaux ;
- les éléments relatifs aux VPN IPsec (mise en place et destruction de tunnel, etc.) ;
- les évènements d'authentification (tentatives avortées, réussites, échecs, etc.) ;
- les évènements d'administration générés par le démon `serverd` (connexion d'administrateurs, modification de configuration) ;
- les statistiques ;
- les évènements système ;
- les alarmes.

# 11
# Gestion du parc

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

Pour l'administration de plusieurs équipements SNS, il est recommandé de mettre en place un SI d'administration conforme aux préconisations du guide relatif à l'administration sécurisée des SI [8]. Ce SI d'administration devrait notamment être utilisé pour :

- fournir l'authentification centralisée des administrateurs telle que décrite à la section 2.1.3 ainsi que l'IGC externe conformément à la section 6.1 ;
- accéder à distance aux services d'administration de l'équipement (HTTPS, NSRPC [17]) à partir des postes d'administration, conformément à la section 2.2 ;
- transférer les journaux générés par l'équipement SNS à destination du serveur central de journalisation, conformément à la section 10 et au guide sur la mise en œuvre d'un système de journalisation[5] ;
- faire circuler les flux de supervision décrits à la section 8, échangés entre l'équipement SNS et le serveur central de supervision ;
- transférer les fichiers de sauvegarde de l'équipement SNS en direction du serveur central de sauvegarde conformément à la section 9.

17. Les outils appropriés utilisent le port TCP 1300.

# Liste des recommandations

# Bibliographie


[1] *Espace personnel Stormshield*.
Page web, Stormshield, novembre 2017.
https://www.mystormshield.eu/.

[2] *MIBS et Traps SNMP*.
Page web, Stormshield, novembre 2018.
https://documentation.stormshield.eu/SNS/v3/fr/Content/User_Configuration_Manual_SNS_v3/SNMP_Agent/MIBS_and_traps_SNMP.htm.

[3] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[4] *Problématiques de sécurité associées à la virtualisation des systèmes d'information*.
Note technique DAT-NT-011/ANSSI/SDE/NP v1.1, ANSSI, septembre 2013.
https://www.ssi.gouv.fr/virtualisation.

[5] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[6] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

[7] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[8] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[9] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[10] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
https://www.ssi.gouv.fr/passerelle-interconnexion.

[11] *RGS Annexe B3 : Règles et recommandations concernant les mécanismes d'authentification*.
Référentiel Version 1.0, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/rgs.

[12] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[13] *RGS Annexe A1 : Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques*.
Référentiel Version 3.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[14] *RGS Annexe A4 : Profils de certificats/LCR/OCSP et algorithmes cryptographiques*.
Référentiel Version 3.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[15] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[16] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[17] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-BP-031
Version 3.0 - 02/04/2021


**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN