Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 21 avril 2016

N° DAT-NT-31/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 36

# Note technique

# Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS) - Version 1.2

**Public visé :**

| | |
|---|---|
| Développeur | |
| Administrateur | ✓ |
| RSSI | ✓ |
| DSI | |
| Utilisateur | |

# Informations

**Avertissement**

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS) - Version 1.2** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations 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.

**Personnes ayant contribué à la rédaction de ce document :**

| Contributeurs | Rédigé par | Approuvé par | Date |
|---|---|---|---|
| BAS, BSS | BSS | SDE | 21 avril 2016 |

**Évolutions du document :**

| Version | Date | Nature des modifications |
|---|---|---|
| 1.0 | 21 avril 2016 | Version initiale |

**Pour toute question :**

| Contact | Adresse | @mél |
|---|---|---|
| Division Assistance Technique de l'ANSSI | 51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP | conseil.technique@ssi.gouv.fr |

# Table des matières

# 1 Préambule

Ce document a pour objectif de présenter les bonnes pratiques relatives à la sécurisation des pare-feux Stormshield Network Security (SNS), en version physique ou en version virtuelle [1]. Les recommandations détaillées dans ce document ne sont pas exhaustives. Elles traitent des fonctions

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

Ce document vient en complément d'autres publications ANSSI relatives aux pare-feux, en particulier :

- la note technique *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu* [2] ;
- le guide intitulé *Definition d'une architecture de passerelle d'interconnexion sécurisée* [3].

Les recommandations mentionnées dans ce document se basent sur la version 1.2.0 de Stormshield Network Security (SNS). Elles sont en majorité applicables aux produits Netasq, quelques adaptations peuvent cependant s'avérer nécessaires.

1. Les contraintes liées à la virtualisation ainsi que les bonnes pratiques sont expliquées dans une note technique sur la virtualisation : http ://www.ssi.gouv.fr/virtualisation.
2. Cf. http ://www.ssi.gouv.fr/politique-filtrage-pare-feu.
3. Cf. http ://www.ssi.gouv.fr/passerelle-interconnexion.

# 2 Administration du pare-feu

## 2.1 Comptes administrateurs

### 2.1.1 Utilisation de comptes nominatifs

Il est recommandé d'utiliser un compte nominatif pour chaque personne autorisée à se connecter à l'équipement, et ce quel que soient ses privilèges. Cette mesure permet d'assurer la traçabilité de l'ensemble des actions réalisées sur le pare-feu (se reporter à la section 10). Seul un compte administrateur non nominatif (admin) reste présent sur l'équipement. Ce compte doit disposer d'un mot de passe fort et ne doit être utilisé qu'afin de rétablir 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.

L'utilisation de comptes nominatifs n'est possible que pour l'accès aux interfaces d'administration propriétaires SNS : l'interface web et le serveur d'administration (port 1300). Seul le compte admin est disponible pour l'accès SSH. L'accès SSH doit être désactivé par défaut, les tâches d'administration courantes doivent être réalisées à partir des interfaces d'administration SNS en utilisant les comptes nominatifs. L'accès SSH pourra être activé à titre exceptionnel pour réaliser des opérations de configuration ou de maintenance qui ne sont réalisables qu'au travers de celui-ci (ex : `tcpdump`), l'accès devra ensuite être désactivé immédiatement après son utilisation.

**R1** - Utiliser des comptes nominatifs

Il est recommandé d'utiliser des comptes nominatifs pour les administrateurs.

**R2** - Limiter l'administration par SSH

Il est recommandé d'administrer l'équipement par l'interface web ou le serveur d'administration. Le service SSH ne doit être activé qu'à titre exceptionnel.

**R3** - Utiliser une authentification par clés pour SSH

Lorsque l'accès SSH est activé à titre exceptionnel, il est recommandé de n'autoriser que l'authentification par clé.

### 2.1.2 Droits d'accès

Chaque administrateur ne doit disposer que des droits strictement nécessaires aux actions dont il a la charge sur l'équipement. Ces droits se positionnent pour l'administrateur lui-même ou pour un groupe d'administrateurs (cas de l'authentification centralisée présentée en 2.1.4). Le menu `Système` → `Administrateur` permet de définir les droits que l'on souhaite affecter.

**R4** - Ajuster les droits d'administration

Il est recommandé de ne positionner que les droits strictement nécessaires aux tâches des différents administrateurs.

### 2.1.3 Authentification locale

Si une authentification locale est utilisée, il est recommandé d'employer des certificats utilisateurs nominatifs pour authentifier les accès des administrateurs à l'interface web d'un équipement SNS. Les recommandations associées à l'utilisation des certificats sur des équipements SNS sont présentées dans la section 6.

**R5** - Authentifier localement avec des certificats

Si l'authentification locale est utilisée, il est recommandé d'utiliser des certificats utilisateurs nominatifs comme moyen d'authentification.

### 2.1.4 Authentification centralisée

La solution SNS permet de configurer une authentification centralisée, la gestion des droits d'accès restant locale à l'équipement. Afin de limiter les modifications sur l'équipement, de simplifier les procédures d'administration et de maintenir le niveau de sécurité, il est recommandé d'utiliser un annuaire LDAP et d'y définir des groupes d'administrateurs.

Chaque groupe doit correspondre à un besoin fonctionnel (administrateur complet, administrateur en lecture seule, superviseur, etc.). Les droits associés sont définis sur l'équipement et leur modification doit rester une opération exceptionnelle. L'attribution des droits aux administrateurs est effectuée de manière centralisée, dans l'annuaire, par l'affectation d'un compte à un groupe et non plus sur chaque équipement.

L'utilisation de groupes reste une fonctionnalité liée à l'utilisation d'un annuaire LDAP, les autres méthodes d'authentification nécessitent l'attribution de droits par administrateur et par équipement.

Les recommandations d'interconnexion avec un annuaire LDAP sont détaillées à la section 4.4.

La mise en place de l'authentification des administrateurs à partir d'un annuaire LDAP externe se réalise en plusieurs étapes :

1. identifier la structure des groupes qui composent l'annuaire LDAP. Les groupes LDAP d'un annuaire peuvent être de deux types différents : `groupOfNames` ou `posixGroup`. Par défaut, un équipement SNS est configuré pour dialoguer avec un annuaire utilisant des groupes de type `groupOfNames`. Si l'annuaire employé utilise des groupes de type `posixGroup`, les deux commandes suivantes doivent être exécutées en CLI pour reconfigurer l'équipement SNS :

   ```
   config ldap update GroupSchema=PosixGroup
   config ldap activate
   ```

2. configurer le filtre de sélection des groupes d'utilisateurs. Sur une configuration simple, on pourra choisir `ObjectClass=groupOfNames` ou `ObjectClass=posixGroup` en fonction de l'annuaire ;
3. activer l'utilisation de l'annuaire (menu `Configuration` → `Utilisateurs` → `Configuration de l'annuaire`, onglet `Annuaire externe`) et 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.

   Il est recommandé d'utiliser un compte de service LDAP dédié et en lecture seule afin d'éviter toute modification des données de l'annuaire LDAP à partir de l'équipement SNS. La communication entre l'équipement SNS et le serveur LDAP doit être sécurisée à l'aide du protocole TLS. Le serveur LDAP doit donc présenter à l'équipement SNS un certificat serveur

signé par une AC connue de l'équipement SNS pour que celui-ci puisse vérifier la validité du certificat ;

4. 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 ;
5. définir LDAP comme méthode d'authentification par défaut (menu `Configuration` → `Utilisateurs` → `Authentification`) ;
6. sélectionner les groupes autorisés à administrer l'équipement SNS puis paramétrer les droits de chaque groupe sur l'équipement SNS (menu `Configuration` → `Système` → `Administrateurs`).

L'équipement SNS utilise des filtres sur les attributs LDAP pour identifier les utilisateurs et les groupes. Un filtre est disponible pour identifier les utilisateurs et un autre pour les groupes. Les droits d'accès se positionnent sur un utilisateur ou sur un groupe. Il n'est donc pas possible d'utiliser la valeur d'un attribut LDAP pour discriminer les droits d'accès entre utilisateurs.

D'autres méthodes d'authentification centralisées sont disponibles, cependant seule l'utilisation d'un annuaire LDAP permet de gérer également l'autorisation de manière centralisée.

**R6** - Dédier un annuaire LDAP aux administrateurs

Il est recommandé d'utiliser un annuaire LDAP dédié à l'administration pour authentifier les administrateurs sur un équipement SNS.

**R7** - Utiliser les groupes LDAP pour gérer les droits

Il est recommandé d'utiliser les groupes LDAP pour gérer les droits d'accès aux équipements.

## 2.2 Services d'administration

### 2.2.1 Configuration des adressses IP d'administration

Il est recommandé de configurer les adresses IP des postes ou serveurs d'administration autorisés à se connecter au pare-feu, cette liste doit être réduite au strict nécessaire. Afin de faciliter la gestion des machines autorisées, il est conseillé de définir un groupe plutôt que des adresses IP ou des réseaux unitaires.

Le menu `Système` → `Configuration` → `Administration du Firewall` permet la configuration des paramètres associés à cette protection.

**R8** - Définir explicitement les sous-groupes d'administration

Il est recommandé de définir explicitement les adresses IP ou les sous-réseaux d'administration autorisés à accéder aux interfaces d'administration des équipements à l'aide d'un groupe.

### 2.2.2 Interface d'administration dédiée

Idéalement, un équipement SNS doit être raccordé à un réseau d'administration sur une interface Ethernet dédiée. Il ne doit être administrable que depuis ce réseau et cette interface. La politique de filtrage doit être configurée afin de n'autoriser l'accès aux services d'administration de l'équipement (HTTPS et nsrpc) qu'aux adresses IP des postes d'administration déclarées dans le groupe défini pour cet usage. La note technique *Recommandations relatives à l'administration sécurisée des systèmes d'information*[4] détaille ces éléments.

**R9** - 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. Le filtrage mis en œuvre devra être le plus restrictif possible.

### 2.2.3 Renforcement de la sécurité de TLS de l'interface web d'administration

Depuis la version 9.1.0 de NetAsq, la sécurité TLS de l'interface web d'administration a été renforcée avec l'apparition du paramètre `sslparanoiac`. Ce paramètre est activé par défaut sous SNS 1.2. Il impose l'utilisation des versions récentes de TLS et de suites cryptographiques robustes.

La restriction des suites cryptographiques est possible par la commande `config auth cipherlist`. Dans la version SNS 1.2, les suites de chiffrement proposées 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
```

Tous les algorithmes de chiffrement et de hachage utilisés ainsi que les groupes de Diffie-Hellman sur courbes elliptiques (ECDHE) sont conformes au RGS[5]. En revanche, le groupe de Diffie-Hellman qui n'est pas sur courbes elliptiques (DHE) a une taille de 1024 bits, ce qui n'est pas conforme.

Il est possible de vérifier la configuration du paramétrage TLS de l'interface web d'administration à l'aide de la commande `config auth show`.

4. Cf. http ://www.ssi.gouv.fr/securisation-admin-si.
5. Référentiel Général de Sécurité disponible ici : `http://www.ssi.gouv.fr/rgs`.

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

**R10** - Durcir les paramètres TLS de l'interface d'administration

Il est recommandé de ne conserver que les suites TLS avec `ECDHE` pour l'interface d'administration car les autres ne sont pas conformes au RGS.

### 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 auto-signé généré par l'équipement. Afin de renforcer la sécurité de l'accès à l'interface web d'administration, il est recommandé de remplacer le certificat existant par un certificat issu d'une IGC maîtrisée qui respecte les recommandations du RGS (en particulier les annexes A4 et B1). Pour que les administrateurs se connectent sans erreur à l'interface web d'administration, 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.

La configuration du certificat serveur utilisé par l'interface web d'administration de SNS se fait à partir du menu `Configuration` → `Utilisateur` → `Authentification` → `Portail captif`. Bien que cet élément de configuration n'ait pas de lien avec la fonction de portail captif, c'est à partir du même onglet que le certificat est positionné (il n'est pas nécessaire d'activer le portail captif pour pouvoir modifier le certificat utilisé par l'interface web d'administration).

**R11** - 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. L'AC correspondante sera placée dans le magasin de certificat du navigateur des administrateurs afin de permettre la vérification du certificat présenté par le serveur web.

# 3 Configuration réseau

## 3.1 Désactivation des interfaces non utilisées

Les interfaces réseau inutilisées sur un équipement SNS doivent toutes être explicitement désactivées dans l'interface web d'administration. Le menu `Réseau` → `Interface` permet de désactiver les interfaces du pare-feu.

**R12** - Désactiver les interfaces non utilisées

Il est recommandé de désactiver les interfaces réseau non utilisées.

## 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. Le pare-feu interprète la requête comme légitime et provenant du réseau interne vers le réseau interne.

Afin de se protéger de ce type d'attaque, il est indispensable d'activer les mécanismes d'antispoofing. Ils consistent à vérifier sur chaque interface d'entrée la légitimité de l'adresse IP source des paquets. Cette légitimité est définie par la topologie réseau.

Sur SNS, l'antispoofing est activé par défaut. Il est cependant nécessaire de renseigner la topologie réseau. Elle se configure à deux endroits :

- sur les interfaces réseau, pour les réseaux directement connectés ;
- par la table de routage, pour les réseaux distants.

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

### 3.2.2 Antispoofing sur les interfaces réseau

SNS utilise la notion d'interface « interne » (protégée) pour identifier les interfaces qui alimentent le mécanisme d'antispoofing. Seuls les flux provenant des réseaux déclarés sur une interface protégée pourront entrer par cette interface. Les flux provenant des réseaux déclarés sur une interface protégée ne pourront entrer que par cette interface. Les réseaux directement connectés sont automatiquement ajoutés, les réseaux distants sont traités par les routes statiques.

Il est recommandé de déclarer les interfaces internes au SI comme protégées et les interfaces externes comme « publiques ». Ainsi, si des paquets dont l'IP source est normalement associée à une interface « interne » (protégée) se présentent sur une autre interface, ils seront supprimés avant même l'évaluation de la politique de filtrage réseau en place sur le pare-feu. Le menu `Réseau` → `Interface` → `Configuration de l'interface` permet de configurer le type d'interface : un bouclier apparaît lorsqu'une interface est protégée.

Attention cependant, en définissant une interface comme protégée, l'administration devient implicitement possible depuis cette interface. Deux règles implicites autorisent l'administration des

équipements à partir des interfaces internes. Ces règles devront êtres désactivées comme expliqué à la section 5.2.

**R13** - Déclarer les interfaces internes

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

### 3.2.3 Antispoofing par la table de routage

La définition des routes statiques renseigne sur la topologie réseau et complète implicitement les mécanismes d'antispoofing. Toute route définie pour sortir par une interface protégée est ajoutée aux tables d'antispoofing. Ainsi si des paquets dont l'IP source est normalement routée par une interface « interne » (protégée) se présentent sur une autre interface, ils seront rejetés avant même l'évaluation de la politique de filtrage réseau en place sur le pare-feu. Il est donc recommandé de renseigner l'ensemble des réseaux connus sur les interfaces protégées. Les routes externes ne sont pas protégées car, en général, les IP sources ne sont pas connues. Le menu `Réseau` → `Routage` → `Routage statique` permet de configurer les routes statiques. Lorsque l'interface de sortie est une interface protégée, un bouclier apparaît.

**R14** - Définir des routes statiques pour les réseaux internes

Il est recommandé de définir des routes statiques pour l'ensemble des réseaux internes connus afin de profiter des mécanismes d'antispoofing.

### 3.2.4 Antispoofing sur un bridge

Sur un bridge la notion d'antispoofing est plus complexe à mettre en œuvre et ne peut être exhaustive. Les interfaces physiques étant indissociables de l'interface bridge, les propriétés précédentes sont appliquées sur l'interface bridge et non à une interface physique spécifique du bridge. Un réseau distant est interconnecté avec l'ensemble du bridge même si la passerelle d'interconnexion n'est présente que sur une interface physique. Pour les machines directement connectées, SNS propose un mécanisme de détection automatique basé sur la table des hôtes.

**R15** - Utiliser les bridges pour des réseaux de même confiance

Il est recommandé d'utiliser les interfaces bridge uniquement pour joindre des réseaux de même confiance. Plus généralement, une DMZ ne devrait jamais être interconnectée au travers d'une interface bridge.

### 3.2.5 Antispoofing, règles complémentaires

Certaines configurations ne peuvent pas être prises en compte par les mécanismes d'antispoofing natifs de l'équipement. Il est cependant tout a fait possible de compléter ces mécanismes par des règles de filtrage adaptées.

**R16** - Compléter les règles d'anti-spoofing

Il est recommandé de compléter autant que possible les règles d'antispoofing citées précédemment par des règles déduites de la topologie réseau.

En particulier, un certain nombre de plages d'adresses particulières définies dans la RFC 5735 sont pré configurées dans l'équipement. Ces plages peuvent faire l'objet d'une règle de filtrage interdisant les paquets correspondants à entrer par l'interface Internet. Un groupe spécifique contenant l'ensemble des plages d'adresses concernées est préconfiguré sur les équipements SNS.

**R17** - Interdire les IP RFC5735 depuis Internet

Il est recommandé d'interdire explicitement les places d'adresses du groupe RFC5735 provenant d'Internet.

# 4 Configuration des services

## 4.1 Accès Internet

Certaines fonctionnalités d'un équipement SNS nécessitent des mises à jour régulières (Menu `Système` → `Active Update`). 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.

Pour une utilisation en ligne, il est recommandé de configurer un serveur proxy authentifiant pour permettre cet accès. 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/IP flux strictement nécessaires aux opérations de mise à jour de SNS [6]).

**R18** - 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.

**R18**- - Mettre à jour au travers d'un proxy

> Il est recommandé de mettre à jour régulièrement les services par l'activation des mises à jour automatiques. En l'absence de miroir interne, le 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. Lorsque ces services sont activés, il est recommandé de configurer des résolveurs internes, à défaut les résolveurs du fournisseur d'accès. Dans tous les cas, les serveurs DNS configurés par défaut doivent être supprimés.

La base d'objets SNS permet de créer des objets de type dynamique. Ces objets dépendent d'un nom de domaine régulièrement résolu par la solution. Ces requêtes DNS ne peuvent pas être bloquées par des règles de filtrage. Afin d'éviter les requêtes DNS inutiles et intempestives, il est nécessaire de modifier l'ensemble des objets dynamiques présents dans la base d'objets. En version 1.2.0, il en existe par défaut une quinzaine qui portent un nom se terminant par netasq.com dont une partie est représentée sur la figure 1. Il est nécessaire de supprimer les objets dynamiques inutiles et reconfigurer les objets restants en mode statique afin d'éviter toute résolution DNS.

**R19** - Limiter l'usage des objets dynamiques

> Il est recommandé de configurer des résolveurs DNS internes, de supprimer les objets dynamiques non utilisés et de reconfigurer les objets restants en mode statique.

6. À savoir les adresses update{1,2,3,4}.netasq.com et licence{1,2,3,4}.netasq.com.

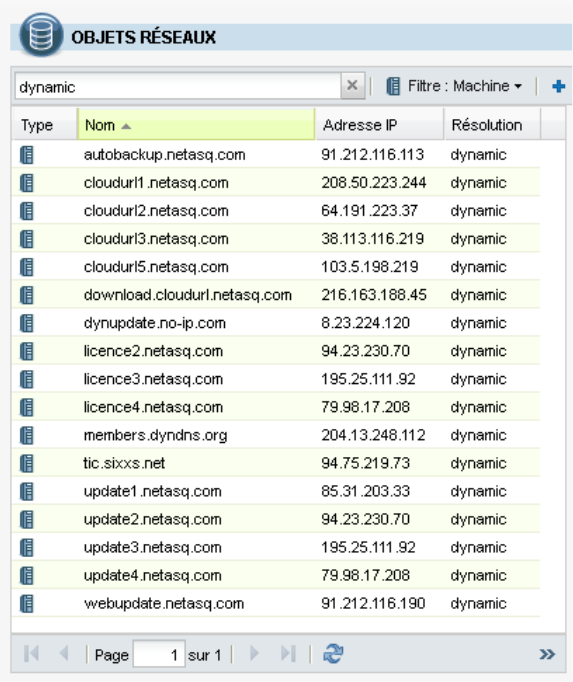



FIGURE 1 – Liste des objets dynamiques de type « Machine ».

## 4.3 NTP

La mise à l'heure d'un pare-feu ainsi que l'activation de la synchronisation NTP doivent faire partie des premières actions d'initialisation d'un équipement SNS. En effet, certaines fonctionnalités sont fortement liées à l'heure du système, notamment la journalisation et la gestion des certificats. Il est donc très important de disposer d'une heure juste et synchronisée sur une source de temps fiable. Il est recommandé d'activer la synchronisation NTP en utilisant plusieurs serveurs de temps internes au système d'information. Ces serveurs doivent être synchronisés sur des sources de temps fiables.

**R20** - Activer NTP

Il est recommandé d'activer la synchronisation NTP en se basant sur plusieurs serveurs de temps internes.

## 4.4 LDAP

Si le pare-feu nécessite la connexion à un serveur LDAP pour pouvoir authentifier les utilisateurs ou les administrateurs, il est recommandé d'activer le protocole LDAPS et d'installer sur le serveur LDAP un certificat qui a été généré à l'aide d'une autorité de certification connue du pare-feu pour qu'il puisse vérifier la signature du certificat présenté (importation de la clé publique de l'AC).

Si le pare-feu ne propose aucun service utilisant l'authentification des utilisateurs, il est recommandé de désactiver l'ensemble des options de configuration associées, en particulier les méthodes autorisées. Bien qu'aucun serveur LDAP ne soit activé par défaut sur les équipements Stormshield, la méthode d'authentification des utilisateurs est « activée » ; il est recommandé de supprimer cette

méthode via le menu `Utilisateurs` → `Authentification` → `Méthodes disponibles`.

**R21** - 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.

Si le service LDAP n'est pas utilisé il est recommandé de supprimer le service LDAP des méthodes d'authentification.

La solution SNS ne permet de configurer qu'un seul annuaire LDAP. Il n'est donc pas possible d'utiliser LDAP pour authentifier des administrateurs et des utilisateurs en respectant les règles de séparation des annuaires comme préconisé dans la note technique sur les architectures sécurisées de l'ANSSI [7]. Si seuls des administrateurs s'authentifient via l'annuaire LDAP, cet annuaire doit par contre leur être dédié.

7. Cf. http://www.ssi.gouv.fr/securisation-admin-si.

# 5 Politique de filtrage réseau et de NAT

## 5.1 Nommage de la politique de filtrage réseau

Les politiques de filtrage présentes par défaut sur SNS ne portent pas des noms explicites (Low, Medium, High, Block all). C'est la raison pour laquelle il est recommandé de renommer les politiques activées en production, d'une part pour minimiser les erreurs de manipulation (activation de la mauvaise politique) et d'autre part, pour que le nom reflète la fonction du pare-feu (accès Internet, isolation d'un partenaire, etc.). La définition d'une convention de nommage [8] est recommandée pour que l'ensemble des pare-feux présents au sein du SI disposent d'une configuration homogène au niveau de l'intitulé de leur politique de filtrage réseau. Les politiques non utilisées devront être supprimées.

**R22** - Renommer la politique de production

Il est recommandé de renommer la politique de filtrage de production et de supprimer les politiques non utilisées afin de limiter les erreurs de manipulation.

## 5.2 Flux implicites

Il est recommandé de désactiver l'ensemble des flux implicites activés sur le pare-feu, il est en effet préférable de redéfinir manuellement l'ensemble des règles de filtrage qui composent la politique de sécurité appliquée par le pare-feu ; cela permet de conserver une meilleure maîtrise des flux réseaux ouverts et de pouvoir visualiser la politique de filtrage de façon exhaustive. La désactivation de ces flux se fait via le menu `Politique de sécurité` → `Flux implicites`.

**R23** - Désactiver les règles implicites

Il est recommandé de désactiver la totalité des règles de flux implicites.

Afin d'éviter de perdre les capacités d'administration, il est nécessaire de créer de nouvelles règles d'administration (HTTPS, SSH) avant de désactiver les règles implicites correspondantes.

## 5.3 Comportement de l'IDS/IPS

L'équipement SNS est équipé d'une fonction IDS [9]/IPS [10]. Lors de la création d'une règle de filtrage, la fonction IDS est activée par défaut. L'ajustement de cette fonction est souvent nécessaire pour prendre en compte différents cas d'usage.

En particulier, il convient de rappeler que cette fonction augmente sensiblement la surface d'attaque de l'équipement et elle doit donc être utilisée avec précaution. Ainsi, il convient de la désactiver si l'équipement remplit une fonction critique comme :

- le filtrage en périphérie d'un SI ;
- le rôle de passerelle de chiffrement.

8. Il est possible d'utiliser la convention proposée dans la note technique ANSSI intitulée *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*. Cette note est disponible à l'adresse : http://www.ssi.gouv.fr/politique-filtrage-pare-feu.
9. Intrusion Detection System : mécanisme de détection, ne bloque pas.
10. Intrusion Prevention System : mécanisme de protection, bloque.

Dans la mesure du possible, il convient de faire réaliser les fonctions d'analyse protocolaire par des équipements dédiés comme des serveurs proxy.

Il est ainsi possible de désactiver la fonction IDS/IPS de manière à ce que la solution se comporte uniquement comme un pare-feu à états (stateful). Cette fonction est désactivable par règle de filtrage. La colonne `Inspection de sécurité` présente sur chacune des règles de flux de la politique permet de déterminer le comportement de l'inspection applicative. L'option `Niveau d'inspection` de cette colonne doit être positionnée à `Firewall` pour que l'IDS/IPS n'agisse pas sur la règle.

**R24** - Désactiver la fonction IDS/IPS sur les équipements critiques

La fonction IPS/IDS augmentant sensiblement la surface d'attaque et la charge de l'équipement, il est recommandé de la désactiver lorsque celui-ci est en forte charge ou assure une fonction de sécurité critique.

Deux profils sont utilisés par défaut, un profil en entrée et un profil en sortie (`Profils d'inspection`). Ces profils sont directement modifiables. Il est également possible d'en créer de nouveaux, de les dupliquer ou d'utiliser des modèles prédéfinis dans la limite de dix profils.

Chaque profil est configurable via les menus `protocoles` et `applications et protections`. Le menu `protocoles` définit l'analyse générale réalisée sur les protocoles : les ports par défaut, les commandes à restreindre, le type d'analyse à effectuer, etc. Le menu `applications et protections` définit l'analyse plus spécifique, la recherche de buffer overflow, de format d'encodage, etc. Ce menu propose une vue par profil ou par contexte.

Lors d'un déploiement par défaut dans un contexte maîtrisé, aucun faux positif ne doit remonter d'alarme afin de ne pas polluer la supervision. L'utilisation des multiples profils doit permettre d'ajuster les configurations au contexte d'emploi. Outre les deux profils utilisés par défaut, chaque règle de flux (menu `Filtrage et NAT`) permet de forcer le comportement attendu : IDS ou IPS (colonne `Inspection de sécurité` option `Niveau d'Inspection`) , ainsi que le profil à utiliser (option `Profil d'inspection`). La granularité est fortement liée au contexte. Un pare-feu isolant un petit nombre d'applications critiques pourra probablement utiliser des profils très restrictifs.

**R25** - Adapter l'emploi des profils IDS/IPS en fonction du contexte

Lorsque la fonction IDS/IPS est active, il est recommandé d'ajuster au mieux la politique aux réseaux à protéger en s'appuyant sur différents profils.

## 5.4 Politique de filtrage

Les bonnes pratiques relatives à la définition d'une politique de filtrage réseau sont détaillées dans la note technique intitulée *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*[11]. Ce document a pour objectif principal de présenter l'organisation à adopter afin de garantir une politique de filtrage pérenne.

## 5.5 Politique de filtrage et configuration d'un VPN IPsec

Lorsque l'équipement SNS est utilisé en tant que chiffreur IPsec, la bonne définition des règles de routage et de filtrage est critique pour garantir la confidentialité et l'intégrité des flux.

11. Cf. http://www.ssi.gouv.fr/politique-filtrage-pare-feu.

Quatre fonctions sont fortement liées :
– le routage ;
– la politique de filtrage ;
– la NAT avant IPsec ;
– la politique IPsec.

Dans le cadre de la mise en œuvre de tunnels 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 [12] (par exemple, 127.42.42.42). Elle sera surchargée par la politique de IPsec. Cependant, en cas d'erreur sur cette dernière, 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 2 a un impact direct sur la confidentialité des flux [13]. 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 2 – Briques fonctionnelles

**R26** - Configurer les tunnels IPsec de manière sécurisée

Lorsqu'un VPN IPsec est configuré, il est recommandé de :
– ne pas utiliser de route par défaut et de privilégier une route explicite pour joindre les passerelles IPsec distantes ;
– configurer une route 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 que les règles de filtrage sont toujours plus spécifiques que la politique IPsec.

Les exemples ci-dessous permettent d'illustrer l'intérêt des recommandations précédentes. Ils s'appliquent sur le chiffreur SNS 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 IPsec distante. L'architecture est représentée sur la figure 3.

12. Cette technique est également appelée *blackholing*.
13. 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.

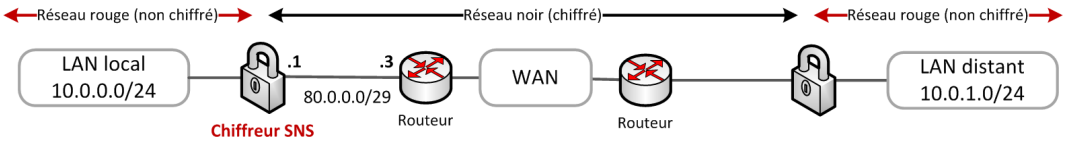



FIGURE 3 – Schéma d'architecture

Dans chaque exemple sont données les configurations des briques fonctionnelles SNS traversées par un paquet réseau (Figure 2). Le paquet réseau rentre avec une source et une destination spécifique. 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.

### Politique IPsec toujours active

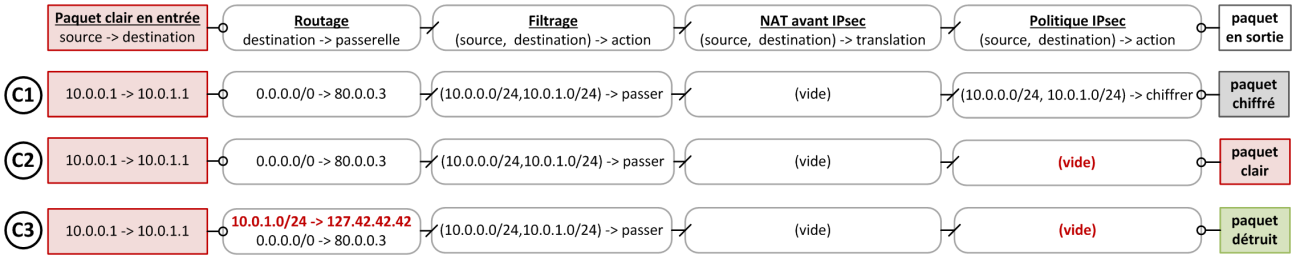



FIGURE 4 – Politique IPsec toujours active, route à destination de la boucle locale

L'exemple représenté figure 4 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). 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 IPsec distante.

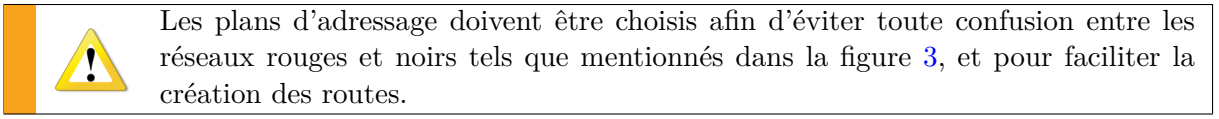
La table de routage est de nouveau traversée [14], elle contient une route valide vers la passerelle IPsec (la route par défaut). Les paquets sont émis chiffrés.

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 [15], 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.

Dans l'idéal, et si le contexte le permet, la route par défaut devrait être supprimée. Ainsi seuls les paquets ayant une route explicitement définie pourront sortir en clair.



Les plans d'adressage doivent être choisis afin d'éviter toute confusion entre les réseaux rouges et noirs tels que mentionnés dans la figure 3, et pour faciliter la création des routes.

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

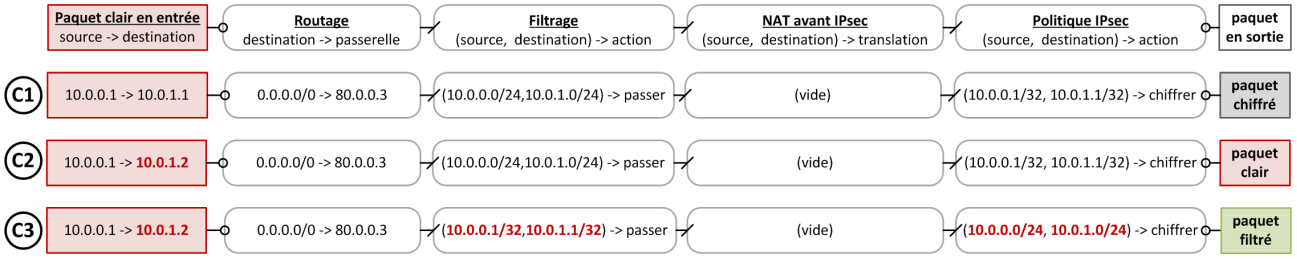



FIGURE 5 – Règles de filtrage toujours plus spécifiques que la Politique IPsec

L'exemple représenté figure 5 illustre la nécessité de définir une politique de filtrage toujours plus spécifique que la politique IPsec.

Dans le cas C1, la politique de filtrage est définie en /24 alors que la politique IPsec est en /32. L'administrateur désire, par exemple, définir un contexte cryptographique par couple d'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.

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.

14. La route à destination du LAN distant n'est pas utilisée. Seule la route à destination de la passerelle IPsec distante est utilisée.
15. Prendre une adresse IP particulière facilite la maintenance de la configuration (par exemple, 127.42.42.42).

Les paquets seront soit filtrés soit chiffrés mais ils ne pourront pas être émis en clair.

Lorsque 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.

> ⚠ Idéalement, un pare-feu dédié devrait être mis en œuvre afin de dissocier la fonction de filtrage de la fonction de chiffrement de flux.

### Règles de NAT avant IPsec incluses dans le politique IPsec

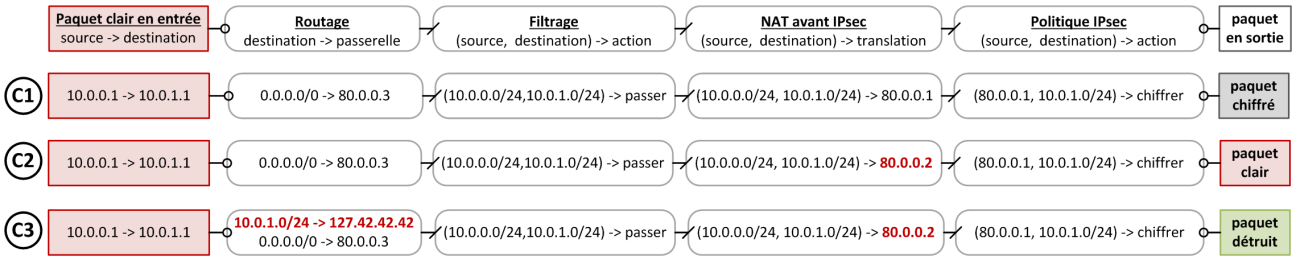



FIGURE 6 – Règles de NAT avant IPsec incluses dans le politique IPsec

L'exemple représenté figure 6 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.

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'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 route à destination de la boucle locale. Si le paquet n'est pas sélectionné par la politique IPsec, il sera détruit par l'équipement au lieu d'être envoyé à la passerelle par défaut.

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

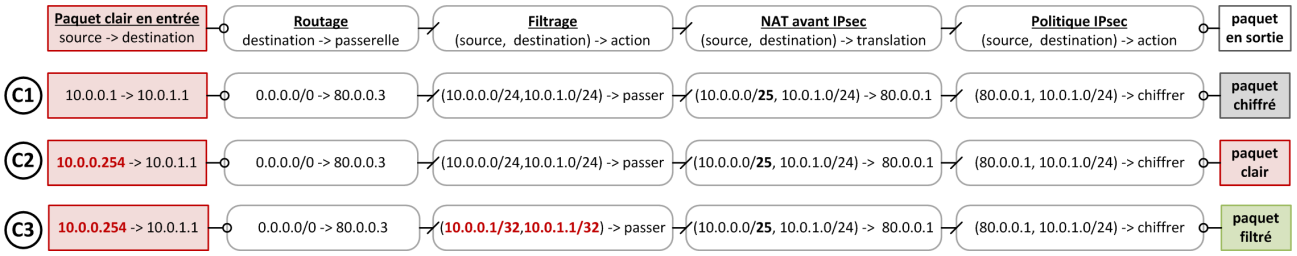



FIGURE 7 – Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec

L'exemple représenté figure 7, 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 inclue 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.

Dans le cas C2, l'IP source est inclue dans le /24 mais non inclue 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.

Plusieurs cas d'usage des certificats sont possibles sur 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 LDAP externe à l'équipement SNS.

## 6.1 Utilisation d'une AC externe

Quel que soit le cas d'usage, il est recommandé d'utiliser une IGC maîtrisée externe à l'équipement SNS pour générer les certificats utilisés par le pare-feu (cela permet de disposer d'un véritable écosystème de gestion de certificats).

**R27** - Utiliser une IGC externe pour IPsec

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

## 6.2 Utilisation d'une AC interne (non recommandé)

Si les mécanismes de génération internes à SNS sont utilisés, il est recommandé d'être extrêmement vigilant concernant la configuration de l'AC en charge de la génération des différents types de certificats.

Ainsi, il est nécessaire de modifier la fonction de hachage utilisée par l'AC pour que celle-ci soit compatible avec les recommandations cryptographiques énnoncées dans le RGS. En effet, par défaut la fonction de hachage utilisée par SNS est SHA1 qu'il faut remplacer par SHA256. Il n'est pas possible de modifier cette fonction via l'interface web d'administration de Stormshield, il est donc nécessaire de réaliser l'ajustement directement dans plusieurs fichiers de configuration.

La modification doit être réalisée à deux endroits :

1. Il est nécessaire de modifier le fichier qui définit les paramètres des AC internes. Ce fichier se nomme `pki.conf`. Il se trouve dans le répertoire `/data/Main/ConfigFiles/Certificates/`.
2. Une fois une AC générée, il est nécessaire de modifier le fichier de configuration de celle-ci pour que les certificats générés utilisent la bonne fonction de hachage. Ce fichier se nomme `pki.conf`. Il se trouve dans le répertoire `/data/Main/ConfigFiles/Certificates/MYCA/` si l'autorité de certification générée se nomme MYCA. Il est donc nécessaire de faire cette opération pour toutes les autorités de certification internes utilisées.

Dans les deux cas, pour modifier la fonction de hachage, il est nécessaire de remplacer toute les occurences de `sha1` par `sha256` dans les deux fichiers `pki.conf`. La prise en compte de la modification est immédiate, il suffit de se déconnecter de l'interface web d'administration puis de s'authentifier à

nouveau.

**R28** - Utiliser SHA256 pour une AC interne

Si une autorité de certification interne est utilisée, il est recommandé d'utiliser la fonction de hashage SHA256.

## 6.3 Gestion des CRL IPsec

La configuration initiale des CRL est manuelle sur les équipements SNS. Le champ CRLDP présent dans le certificat n'est pas pris en compte. Une URL de téléchargement peut être renseignée pour chaque AC, la mise à jour étant ainsi automatisée. Le fichier de CRL peut également être fourni via l'interface graphique, l'opération étant dans ce cas à renouveler régulièrement.

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. Il est donc recommandé de rendre obligatoire la vérification de la CRL avant la montée d'un tunnel IPsec. Cela est possible à l'aide du paramètre `CRLrequired` qui est disponible uniquement en ligne de commande :

```
config ipsec udpdate slot=01 CRLrequired=1
```

La valeur 01 représente le numéro de la configuration IPsec employée. Il est ensuite nécessaire de réactiver la configuration IPsec par la commande :

```
config ipsec activate
```

**R29** - Imposer la vérification des CRL

Il est recommandé d'imposer la vérification de CRL pour la mise en œuvre des tunnels IPsec avec le paramètre `CRLrequired`.

### 6.3.1 Importation automatique de CRL

Les équipements SNS peuvent récupérer une CRL hébergée sur un serveur distant. Les points de distribution de CRL associés à une AC peuvent être positionnés soit via l'interface web d'administration de SNS, soit en ligne de commande. L'ajout d'un point de distribution de CRL via l'interface web se fait en éditant l'onglet `CRL` de l'AC concernée.

La ligne de commande ne permet pas de configurer les points de distribution associés à une AC déléguée. Il faut utiliser l'interface web ou éditer le paramètre `[crldp]` dans le fichier de configuration de l'AC.

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.

La taille maximale d'une URL est 127 octets par défaut. Cette limite peut être levée en saisissant directement les URL dans le fichier configuration :

```
~/ConfigFiles/Certificates/$CA-Name/CA.db

[crldp]
enabled.1="http://myhost/my_very_long_url/file.crl"
```

L'URL du point de distribution peut être de type HTTP, HTTPS, LDAP, LDAPS et FTP. Dans tous les cas, ces accès doivent être **non authentifiés** du côté client.

Par défaut, lorsqu'une URL de CRL est ajoutée et activée, la récupération du fichier de CRL est réalisée une fois par jour. Il est possible de forcer la mise à jour à l'aide de la commande `checkcrl`, par exemple lors d'une révocation. Il est également possible de modifier la fréquence de récupération des CRL en ajoutant une entrée dans le fichier `/ConfigFiles/Event/rules` faisant appel à la commande `checkcrl`. Par exemple, une récupération toutes les 6 heures permet de diminuer fortement le temps de réaction. La CRL ainsi récupérée est stockée localement dans le répertoire de l'AC (ou de l'AC déléguée) correspondante et renommée en CA.crl.pem.

**R30** - Configurer l'URL de récupération de la CRL

Il est recommandé de configurer l'URL de récupération de la CRL de chaque AC pour permettre leur téléchargement automatique.

**R31** - Adapter le rafraichissement des CRL

Il est recommandé d'adapter le temps de rafraichissement en fonction de la réactivité recherchée.

### 6.3.2 Importation manuelle de CRL

L'importation d'une CRL locale peut se faire manuellement 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 DER et ne doit pas avoir 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`.

Il est également possible de copier directement un fichier de CRL au format PEM dans le répertoire de l'AC, en le nommant `CA.crl.pem`.

# 7 VPN IPsec

La mise en place de VPN IPsec (site à site ou client à site) nécessite l'utilisation de mécanismes cryptographiques. Les profils de chiffrement proposés par défaut par les équipements SNS (StrongEncryption, GoodEncryption, FastEncryption) ne proposent pas des suites cryptographiques pleinement compatibles avec les exigences du RGS, il est donc nécessaire de redéfinir manuellement des profils de chiffrement IKE et IPsec.

Les tableaux 1 et 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 128 |
| Fonction de hachage | SHA 256 |
| Groupe Diffie-Hellman | Groupe 14 (2048 bits) |
| Cryptopériode | 21600s |

TABLE 1 – Exemple de profil de chiffrement IKE compatible avec le RGS

| Paramètre | Valeur |
|---|---|
| Algorithme de chiffrement | AES 128 |
| Fonction de hachage | SHA 256 |
| Groupe Diffie-Hellman | Groupe 14 (2048 bits) |
| Cryptopériode | 3600s |

TABLE 2 – Exemple de profil de chiffrement IPsec compatible avec le RGS

**R32** - Utiliser des algorithmes robustes pour IKE et IPsec

Il est recommandé d'utiliser a minima les algorithmes AES 128, SHA 256 et le Groupe 14 dans les profils de chiffrement IKE et IPsec.

## 7.1 Authentification

Quel que soit le type de VPN IPsec configuré (site à site ou client à site), il est fortement recommandé de mettre en œuvre une authentification mutuelle par certificat plutôt que par clé partagée (PSK).

**R33** - Utiliser l'authentification mutuelle par certificats d'IKE

Pour un VPN IPsec, il est recommandé de mettre en œuvre une authentification mutuelle par certificat.

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 [16] (22 caractères aléatoires en utilisant comme source les miniscules, 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 [17] ;
- un secret différent doit être utilisé pour chacun des tunnels ;
- le secret doit être renouvellé régulièrement, sa cryptopériode [18] doit être définie en fonction de la politique de sécurité de l'organisme ;
- dans le cas d'un VPN IPsec client à site, les identités des deux extrémités ne doivent pas être renseignées (local ID, remote ID) car elles obligent la méthode de négociation dite « agressive » qui ne protège pas ces informations. Le problème ne se pose pas dans le cas des VPN site à site car SNS utilise toujours la méthode de négociation dite « principale ».

**R33**- - Utiliser une clé partagée robuste

Si une authentification par clé partagée est choisie pour un VPN IPsec, il est recommandé de mettre en œuvre une clé robuste d'entropie supérieure ou égale à 128 bits.

## 7.2 Routage

Afin d'établir un tunnel IPsec, il est nécessaire de configurer une route vers les réseaux distants. La section 5.5 précise les bonnes pratiques de mise en œuvre.

16. Se référer à l'annexe B1 du RGS pour plus de précisions.
17. Cf. http://www.ssi.gouv.fr/mots-de-passe.
18. Durée maximale durant laquelle on accepte de perdre la confidentialité et l'intégrité du trafic si le secret venait à être compromis.

# 8 Supervision

## 8.1 Configuration des éléments de base

Il est recommandé de configurer correctement les paramètres SNMP `Emplacement(syslocation)` et `Contact(syscontact)` présents au niveau du menu `Notifications` → `Agent SNMP` → `Général`, cela facilite la cartographie des équipements dans les outils de supervision et d'alerte.

## 8.2 Configuration de SNMPv3

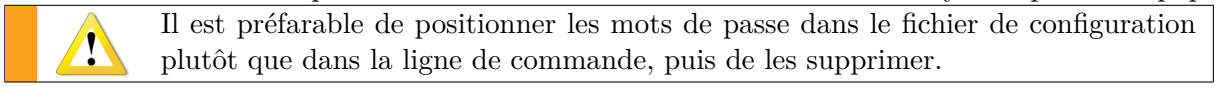
**R34** - Utiliser SNMPv3

Il est recommandé d'utiliser la version 3 du protocole SNMP car elle apporte des mécanismes d'authentification et de chiffrement. L'algorithme de chiffrement AES ainsi que la fonction de hachage SHA1 doivent être utilisés pour apporter aux échanges un niveau de sécurité acceptable mais cependant non conforme au RGS.

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
```

Les OID ainsi que leurs valeurs doivent être renvoyés par l'équipement.



Il est préfarable 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` [19] ;

`-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`.

19. 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 disponible à l'adresse http://ssi.gouv.fr/mots-de-passe.

Les traps SNMP émises par l'équipement passent dans une règle de flux implicite. Cette règle de flux n'est pas présente dans le menu `Règles Implicites` et elle n'est pas désactivable.
L'interrogation de l'équipement en SNMP nécessite la configuration d'une règle de flux. Seuls les serveurs de supervision doivent être autorisés à interroger l'équipement en SNMP.
Par ailleurs, l'accès SNMP se fait en lecture seule uniquement.

**R35** - Filtrer l'interrogation SNMP

Il est recommandé de n'autoriser que les serveurs de supervision à interroger les équipements en SNMP.

## 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 [20] à la technologie SNS (politique, haute disponibilité, VPN). La construction de templates de supervision utilisant des indicateurs issus de ces deux MIB est recommandée afin de disposer d'une vision précise de l'état des pare-feux.

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

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

Le pare-feu 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 qu'il peut être pertinent de superviser sur un équipement SNS est donnée dans le tableau 3.

20. La documentation de la MIB SNS est disponible à l'adresse http://www.netasq.com/netasq-mibs/.

| OID | Description |
|---|---|
| Informations générales | |
| .1.3.6.1.4.1.11256.1.0.1.0 | Hostame |
| .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 |
| .1.3.6.1.2.1.1.3.0 | Uptime |
| CPU | |
| .1.3.6.1.2.1.25.3.3.1.2 | Pourcentage d'utilisation du CPU durant la dernière minute |
| 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 |
| .1.3.6.1.4.1.2021.4.11.0 | Quantité de mémoire libre |
| .1.3.6.1.4.1.2021.4.6.0 | Quantité de mémoire utilisée |
| 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 | |
| .1.3.6.1.2.1.25.3.2.1.3.**262145** | Nom de l'interface em0 (id **262145**) |
| .1.3.6.1.2.1.25.3.2.1.5.**262145** | Etat de l'interface em0 au niveau Stormshield (2=activée, 5=désactivée) |
| .1.3.6.1.2.1.2.2.1.8.**1** | Etat du lien connecté à l'interface em0/id=1 (1=lien ok, 2=lien nok) |
| Tunnels VPN | |
| .1.3.6.1.4.1.11256.1.13.2.2 | Nombre de tunnels VPN montés (état « mature ») |

Table 3 – OID Stormshield

# 9 Sauvegarde

## 9.1 Configuration des sauvegardes automatiques

### 9.1.1 Configuration via CLI

Il est recommandé de mettre en place un mécanisme de sauvegarde automatique qui exporte sur un serveur distant la configuration de l'équipement SNS. L'interface web d'administration permet l'exportation à destination d'un server WebDAV.

Il est également possible d'activer une sauvegarde automatique locale en ligne de commande. Il n'est cependant pas possible d'exporter automatiquement les fichiers de sauvegarde générés sur un serveur distant (SSH par exemple), le fichier généré localement doit être transféré à l'aide d'un script personnalisé. Le fichier de sauvegarde 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.

**R36** - Mettre en place une sauvegarde automatique

Il est recommandé de mettre en place une sauvegarde automatique de la configuration. Cette sauvegarde devrait être exportée en SSH de l'équipement avec une connexion initiée par celui-ci.

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.

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[21], 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`).

21. 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 qu'il est pertinent de journaliser ainsi que leur lieu d'archivage.

Sur un équipement SNS, il est possible de définir de façon indépendante :
- les types d'évènements journalisés sur le support de stockage local lorsqu'il existe (onglet `Stockage local` du menu `Traces - syslog`). Dans ce cas, ces évènements seront directement consultables à partir de l'interface web d'administration de l'équipement SNS. Il est recommandé de mettre en place un écrasement automatique de ces évènements ;
- les types d'évènements envoyés sur un (ou plusieurs) serveur 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.

## 10.2 Journaux à collecter

Voici une liste non exhaustive des types de journaux qu'il est recommandé de collecter par syslog. Le cas d'usage supposé est un 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 (démon `served`) (connexion d'administrateurs, modification de configuration) ;
- les statistiques ;
- les évènements systèmes ;
- les alarmes.

**R37** - Définir une politique de journalisation

Il est recommandé de définir une politique de journalisation locale et une politique de journalisation centralisée [22].

22. Une note technique sur la journalisatation est disponible sur http ://www.ssi.gouv.fr/journalisation.

# 11 Gestion du parc

Pour l'administration de plusieurs équipements SNS, il est recommandé de mettre en place un SI d'administration conforme aux préconisations de la note technique de l'ANSSI correspondante [23]. Ce SI d'administration devrait notamment être utilisé pour :

- accéder à distance aux services d'administration de l'équipement (HTTPS, TCP 1300 [24]) à partir des postes d'administration ;
- transférer les journaux générés par l'équipement SNS à destination du serveur central de journalisation ;
- faire circuler les flux de supervision 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.

23. Cf. http://www.ssi.gouv.fr/securisation-admin-si.
24. Port correspondant au service NSRPC.

# Liste des recommandations