GUIDE

STORMSHIELD NETWORK SECURITY

RECOMMENDATIONS FOR THE SECURE CONFIGURATION OF AN SNS FIREWALL

Version 4.3 LTSB

Document last updated: May 21, 2025

Reference: sns-en-anssi_configuration_recommandations_guide-v4.3-LTSB

Table of contents

1. Getting started

Welcome to the guide, in which you will find recommendations for the secure configuration of a Stormshield Network Security (SNS) firewall in version 4.3 LTSB.

Unless otherwise provided by regulation, these recommendations are not prescriptive; they are given as is and adapted to threats as at the time of their publication. Given the diversity of information systems, the ANSSI is not in a position to guarantee that such information can be applied without some form of adaptation to target information systems. In any case, decisions on the suitability of implementing suggested elements must be made beforehand by the system administrator and/or persons in charge of the security of information systems.

1.1 Information

This guide is based on the document that sets out recommendations for the secure configuration of SNS firewalls in version 3.7.17 LTSB. Stormshield has edited its contents to factor in new features found in SNS version 4.3 LTSB.

The original document, Recommendations for the secure configuration of an SNS firewall in version 3.7.17 LTSB, was written by the ANSSI and has been made available at cyber.gouv.fr. With the ANSSI's consent, this document has been published on *Stormshield's Technical Documentation* website.

1.2 Change history

Date	Description
May 21, 2025	- Chapters 1.3, 4.2, 5.2, 5.3, 6.1, 7.1 and 7.3 updated *Original document last updated by ANSSI on: April 3, 2021*
March 4, 2024	- New document *Original document last updated by ANSSI on: April 3, 2021*

1.3 Objective

The aim of this document is to present best practices for the secure deployment of SNS firewalls, in physical or virtual versions (the restrictions relating to virtualization and best practices are explained in the guide Security issues associated with virtualized information systems - in French).

The recommendations given in this document apply to SNS firewalls. Recommendations regarding configurations on the SMC server aim to secure the deployment of SNS firewalls. All recommendations cover the following functions:

- Administration,
- Filtering,
- IPsec encryption,
- Monitoring,
- Backup,
- Logging.

This document is to be read together with the ANSSI's publications (in French) Recommendations for the definition of a firewall's filter policy and Recommendations relating to the interconnection of information systems to the Internet.

INFORMATION
The features presented in this guide are not restricted to those evaluated during the qualification of the product. Features that were not evaluated are specified in the body of this document with the caption *"This feature was not part of the security target during the SNS firewall qualification process"*.
The use of unevaluated features therefore requires additional risk analysis that must be submitted to the IS approval committee. The committee will then decide whether to accept residual risks or implement adapted protection measures.
SMC server features are not part of the security target.

1.4 Reading convention

For certain recommendations, several architecture solutions of varying security levels are proposed. As such, readers can choose a solution that matches their security requirements. Furthermore, in an iterative approach to security, the various levels of security offered can be used to set an architecture target, and to identify the steps required to reach it.
Recommendations are therefore presented in the following manner:

- **Rx** constitutes a state-of-the-art recommendation,
- **Rx+** constitutes an alternative recommendation to Rx, of a higher security level. It is intended for entities with mature information system security,
- **Rx-** constitutes an alternative recommendation to Rx, of a lower security level.

Next to the recommendation number is an indication of whether the recommendation applies to SNS firewalls, the SMC server, or both (e.g., **Rx | SNS-SMC**).

1.5 SNS firewall configuration modes

The configuration recommendations provided in this document can be applied in various ways:

- SNS firewall side:
  - Via the SNS firewall web administration interface,
  - Via the SNS command line interface through SSH.
- SMC server side:
  - Via direct access to the SNS firewalls' web administration interface from the SMC server, without the need to re-authenticate. This access makes it possible to manage the entire configuration of an SNS firewall,
  - Via the SMC server's web administration interface, to configure certain features on several SNS firewalls,
  - Via SNS CLI scripts, to automate tasks on several SNS firewalls.

In this document, configuration recommendations apply to the web administration interface on SNS firewalls, and when possible, to the web administration interface of the SMC server.

For more information on the configuration of SNS firewalls and the SMC server, refer to the SNS Technical documentation and SMC Administration guide.

1.6 Acronyms

The acronyms of the SNS firewall-related terms presented in this section are used throughout this document.

ASQ	Active Security Qualification, engine that analyzes SNS firewalls.
CA	Certification authority.
CRL	Certificate Revocation List.
CRLDP	CRL distribution point.
DNS	Domain Name System, service that translates domain names and associated IP addresses.
DR	*Diffusion Restreinte*, restricted distribution.
DSCP	Differentiated Services Code Point, field in the header of an IP packet that differentiates and prioritizes services during congestion.
FQDN	Fully Qualified Domain Name, domain name that indicates all the domains to pass through before reaching the resource.
FTP	File Transfer Protocol.
HTTP	HyperText Transfer Protocol.
HTTPS	HTTP Secure, secure upgraded version of HTTP that relies on an SSL/TLS channel.
IDS	Intrusion Detection System, mechanism that makes it possible to detect malicious traffic and raise an alarm.
IKE	Internet Key Exchange, protocol in which authentication keys are exchanged between peers.
IP	Internet Protocol, computer network communication protocol.
IPS	Intrusion Prevention System, mechanism that makes it possible to detect malicious traffic and block it.
IPsec	Internet Protocol Security, framework of standards that make it possible to secure IP communications.
IS	Information system.
LDAP	Lightweight Directory Access Protocol.
LDAPS	LDAP Secure, secure upgraded version of LDAP that relies on an SSL/TLS channel.
MIB	Management Information Base, structured set of resources used in monitoring.
NSRPC	NetAsq Secure Remote Protocol Client, Stormshield administration protocol that uses TCP port 1300. It is implemented by a server that allows the SNS firewall to be managed in command line.
OID	Object IDentifier, resource identifier represented by a series of whole numbers.
PKI	Public Key Infrastructure.
QoS	Quality of Service.
RGS	*Référentiel général de sécurité* (General Security Guidelines), regulatory framework that establishes trust in communications within public bodies and with citizens.
SIEM	Security Information and Event Management.

SMC	Stormshield Management Center, server for the virtual administration and centralized monitoring of SNS firewalls.
SNMP	Simple Network Management Protocol, protocol that manages and monitors appliances remotely.
SNS	*Stormshield Network Security*.
SSH	Secure SHell, secure communication protocol.
SSL	Secure Sockets Layer, protocol that secures exchanges.
TCP	Transport Control Protocol.
TLS	Transport Layer Security, upgrade of SSL.
UAC	User Access Control, mechanism that controls user access.
URL	Uniform Resource Locator, string of characters used to locate a resource on a network in the form of an address.
VLAN	Virtual Local Area Network, local switching network.
VPN	Virtual Private Network, system that makes it possible to create a communication tunnel between two appliances.

2. Managing SNS firewalls

2.1 Administrator accounts

2.1.1 Using accounts assigned to users by name

Being able to trace all operations performed on the SNS firewall and on the SMC server is particularly important (see the chapter on Logging for recommendations on logging) to guarantee that they were performed by a legitimate and authorized administrator.

R1 | SNS-SMC | Use accounts assigned to users by name
Regardless of their privileges, administrators are advised to use their personalized accounts when they connect to the web interface, the NSRPC server, or in SSH.

Some exceptional operations can be carried out with a personalized account from the web interface, local console or via SSH, such as the manual editing of configuration files.

A local generic administrator account (admin) exists on the SNS firewall, and can also perform these operations. However, only this account can change the privileges granted to administrators.

On the SMC server, certain advanced or maintenance operations are only available in command line (via SSH or console mode).

R2 | SNS-SMC | Protect the local administrator account
The administrator account found on the SNS firewall must be protected by a strong password (refer to the guide Relating to multifactor authentication and passwords (in French) and must only be used to access personalized accounts. Its password must be kept in a vault, and when it is used, it must be monitored and restricted to a set group of persons.

R3 | SNS | Restrict administration via SSH
The SSH service has to be restricted to only necessary administrator accounts, and must be enabled only for exceptional reasons in **Configuration > System > Configuration > Firewall administration**.

R4 | SNS | Use SSH key authentication
When SSH is enabled for exceptional reasons, we recommend using SSH key authentication, in line with the Recommendations on the secure use of (Open)SSH (in French).

2.1.2 Local authentication

SNS firewalls make it possible to create an internal directory (**Configuration > Users > Directory configuration**) to allow local authentication. Once authenticated, users can then connect to web, NSRPC and SSH servers. In this case, SNS firewalls will store passwords or their derivatives, if any. If the SNS firewall is compromised, so will these secrets. Users can also authenticate with certificates on the web administration interface. When certificates are used, only public data will be stored on the SNS firewall. The recommendations regarding the use of certificates on

SNS firewalls can be found in the chapter Certificates and PKI. However, access to the NSRPC server allows only password authentication.

R5 | SNS | Authenticate locally using certificates
In local authentication, users are advised to use their personalized certificates to authenticate on the web interface of an SNS firewall.

Certification authorities then have to be added in advance in **Configuration > Objects > Certificates and PKI**. The *SSL certificate* authentication method has to be configured in advance in **Configuration > Users > Authentication > Available methods** with the desired authorities.

R6 | SNS | Define an appropriate password policy
If an administrator requires access to the NSRPC server, their password must comply with a policy that meets the criteria in the Recommendations relating to multifactor authentication and passwords (in French). It can be configured in **Configuration > System Configuration > General configuration**.

2.1.3 Centralized authentication

This feature was not part of the security target during the SNS firewall qualification process.

SNS and SMC solutions support the use of a centralized authentication mechanism with which users can be managed via an LDAP directory. Using such a solution aims to restrict the amount of sensitive data stored locally and simplify administration processes. For external directories, the SNS firewall configuration is described in the chapter Using an external directory.

R7 | SNS | Dedicate an external directory to administrators
In line with the Recommendations on the secure administration of information systems (in French), an external directory dedicated to administration is recommended for the authentication of administrators.

R8 | SNS | Use a restricted-access and secure account
The account that the SNS firewall uses to access the centralized authentication solution must be restricted to this function, dedicated to the SNS firewall, and very carefully configured. The account in particular must have only read privileges to prevent any changes to the directory's data from the SNS firewall.

2.1.4 Access privileges

SNS firewalls provide many features – filtering, tunnels, VPN, etc. An administrator dedicated to a specific task must have only one restricted area of responsibility, so that risks can be contained if the account is compromised, and accidental changes to the configuration can be prevented. Ideally, to lower the risk of compromising an administration account or an SNS firewall, each function should be managed by a dedicated SNS firewall and its associated administration account.

If several SNS firewalls must be shared, administration accounts must then be created for each feature in line with the recommendations in the Recommendations on the secure administration of information systems (in French).

R9 | SNS | Adjust administration privileges strictly to what is required
Only the privileges that the various administrators strictly require for their tasks should be granted in **Configuration > System** > **Administrators** > **Administrators**.

Values of directory attributes cannot be used to distinguish different privilege profiles (full administrators, administrators dedicated to a function, supervisors, etc.). However, user groups can be declared in the directory and a set of privileges on the SNS firewall can be assigned to them. Each group must correspond to a functional requirement and hold the appropriate privileges on the SNS firewall. The privileges assigned to administrators therefore depend on the groups to which they belong. Administrators' groups can be defined centrally in the directory.

R10 | SNS-SMC | Use groups to manage privileges
We recommend using groups to manage privileges for access to SNS firewalls.

WARNING
Only the non-nominative administrator account can modify the privileges granted to users and user groups. This must remain an exceptional operation in line with the chapter Using accounts assigned to users by name.

2.2 Administration services

2.2.1 Configuring administration IP addresses

Unrestricted access to the SNS firewall's administration interfaces raises the risk of intrusion attempts, and of the firewall being controlled by other appliances that have obtained illegal access to it.

R11 | SNS | Define administration sub-networks clearly
The IP addresses or administration sub-networks allowed to access an SNS firewall's administration interfaces should be explicitly defined in **Configuration > System > Configuration > Firewall administration.**

These IP addresses and administration sub-networks must be configured using specific objects placed together in an object group. In line with chapter Filter policy, the use of such groups makes it possible to better manage permissions consistently with filter rules.

R12 | SNS | Use an administrator object group
The use of object groups is recommended, containing all sub-networks and IP addresses allowed to manage the SNS firewall.

2.2.2 Dedicated web administration interface

Sharing a web administration interface with the production network increases the number of individuals and appliances with access to the SNS firewall's web administration interface, and also increases the volume of traffic that the interface must handle. As a result, this raises the

risk of the web administration interface being attacked or unreachable. Moreover, using VLANs does not guarantee airtight access between the configured networks.

R13 | SNS | Dedicate an Ethernet interface to administration
SNS firewalls should be managed on a dedicated Ethernet interface connected to an administration network also dedicated to such operations. The filtering applied must be as restrictive as possible.

The ANSSI guide Recommendations on the secure administration of information systems (in French) sets out the recommended measures regarding the secure administration of information systems.

2.2.3 Security on the web administration interface

Security on SNS firewalls' web administration interface, and on the SMC server, contributes to their security by protecting the confidentiality and integrity of legitimate administration traffic.

For SNS firewalls, *sslparanoiac* mode is enabled by default, thereby imposing the use of TLS 1.3 or TLS 1.2 with robust cryptographic suites. The TLS settings of the web administration interface can be checked using the NSRPC command `config auth show`. The cryptographic suites suggested by default are:

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

R14 | SNS | Keep default cryptographic suites
Keeping the default configuration of cryptographic suites facilitates compliance with the ANSSI's Security recommendations relating to TLS (in French) and Appendix B1 of the ANSSI's RGS.

R14+ | SNS | Harden TLS parameters on the web administration interface
Users are advised to keep only TLS suites with ECDHE as recommended in the guide Security recommendations relating to TLS (in French).

Cryptographic suites can be restricted using the NSRPC commands:

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

2.2.4 Changing the certificate of the web administration interface

By default, the certificate presented to administrators when they connect to the web administration interface of an SNS firewall is a certificate signed by the Stormshield CA

(certification authority). For the SMC server, self-signed certificates are used. In both cases, there is no control over the private key used, the criteria for generating it, or how it can be used.

R15 | SNS | Replace the web interface certificate
The certificate of the web administration interface should be replaced with a certificate issued by a PKI (public key infrastructure) to strengthen the security involved in accessing it.
Refer to the ANSSI's General Security Guidelines (in French), in particular **appendices A4** and **B1**.

The server certificate configuration used by the SNS firewall's web administration interface can be configured in **Configuration > System > Configuration > Firewall administration > Configure the SSL certificate of the service**.

INFORMATION
To allow administrators to authenticate the SNS firewall that they are connecting to, the public key of the CA that signed the certificate must be in the certificate store of the browser that administrators use.

2.2.5 Administration via NSRPC

During direct connections to the NSRPC server, the SNS firewall requires read-only access to the user's password hash (this information is required for the authentication protocol to function properly). If the SNS firewall's access to the directory is hijacked, all saved password hashes may then be compromised. The hash is a critical component, as brute force attacks can compromise passwords. The use of such accounts in the information system must therefore be monitored (connections from another appliance, illegal requests, etc.).

An NSRPC console is available from the web administration interface. Access to this console does not require additional authentication. Hashes do not need to be accessed.

R16 | SNS | Use NSRPC from the web administration interface
NSRPC commands should only be used from **Configuration > System > CLI console** in the web administration interface.

R16 - | SNS | Use accounts dedicated to direct NSRPC connections
During direct access to the NSRPC console, dedicated accounts are recommended for this purpose, while regularly changing their passwords and exposing only the hashes of these accounts on the remote directory.

INFORMATION
By default, Active Directory and OpenLDAP directories do not allow password hashes to be read.

2.2.6 Localization features

Several localization features can be found on the SNS firewall:

- Web administration interface language, which can be selected in the connection window,
- Keyboard layout of the console, which can be configured in **Configuration > System > Configuration**,

- Language in which logs are generated, which can also be configured in **Configuration > System > Configuration**.

The language in which logs are generated changes the messages displayed in **Monitoring > Dashboard**, and in local and remote log files. The language chosen affects:

- How users understand log files,
- Patterns that monitoring systems look for,
- The results of searches conducted in the knowledge base on Stormshield's website.

All existing messages are listed in **Monitoring > Logs - Audit logs > System events** and their translations are available on the SNS firewall in the */usr/Firewall/System/Language/* folder. Every generated message bears an index number associated with the corresponding error. This number is the same in all translations.

R17 | SNS | Use the same language in logs
The same language should be configured for all logs on all SNS firewalls. This will make it easier to read them and integrate them into monitoring tools.

WARNING
Logs are available only in English on the SMC server. We recommend configuring the SNS firewall's logs in English if it is managed through the SMC server.

R18 | SNS-SMC | Use a language that users understand
We recommend configuring an SNS firewall in a language that users understand.

INFORMATION
Stormshield's Technical Documentation website is accessible in French and English. The knowledge base can be accessed from your Stormshield personal area, and in English only.

2.3 *Diffusion Restreinte* option

When an SNS firewall is used in a "restricted" context (*Diffusion Restreinte*), additional constraints must be implemented to comply with the appropriate protection rules (in French). These constraints are explained in the the Stormshield technical note IPsec VPN - *Diffusion Restreinte* mode.

The management of the primary cryptographic hardware components in particular must be adapted when the set of instructions from the (co)-processor does not provide sufficient guarantees regarding their use and their protection (risk of data leaks or disclosure). The downside of using this option is that it affects the encryption functions and decryption performance of SNS firewalls equipped with such (co)-processors.

R19 | SNS | Enable the *Diffusion Restreinte* option
Diffusion Restreinte mode must be enabled in **Configuration > System > Configuration > General configuration** when the SNS firewall is located on a network with the same restricted status and its cryptographic functions are used.

R19 | SMC | Enable the *Diffusion Restreinte* option
We recommend enabling ***Diffusion Restreinte*** mode on the SMC server in **Maintenance > SMC server > Parameters**.

INFORMATION
When ***Diffusion Restreinte*** mode is enabled on the SMC server, an automatic deployment enables ***Diffusion Restreinte*** mode on SNS firewalls that are connected to the SMC server. Once this mode is enabled, SNS firewalls on which ***Diffusion Restreinte*** mode has never been enabled will no longer be able to connect to the SMC server.
For more information, refer to the SMC server documentation.

3. Network configuration

3.1 Disabling unused interfaces

The presence of unused network interfaces on an SNS firewall increases its attack surface. While connections on such interfaces do not disrupt the proper operation of the SNS firewall, they may enable illegal access to it. Moreover, active interfaces can be used from the various menus and increase the risk of configuration errors.

R20 | SNS | Disable unused interfaces
Unused network interfaces should be disabled in **Configuration > Network > Interfaces**.

3.2 Configuring IP address spoofing protection

3.2.1 Introduction to IP address spoofing protection

IP address spoofing consists of usurping a legitimate IP address with the purpose of bypassing configured filter rules. This includes, for example, sending from an external network packets that appear to be going from one internal IP address to another. Without proper verification of the interfaces used, the SNS firewall interprets the request as legitimate and originating from the internal network to the internal network. Malicious traffic can therefore be routed as legitimate traffic in this way.

To prevent such attacks, anti-spoofing mechanisms are enabled by default. They verify on each incoming interface whether the source IP address of packets are legitimate. Their legitimacy depends on the network topology defined by:

- Network interfaces, for networks that are directly connected,
- The routing table, for remote networks.

INFORMATION
In addition to being essential for security, anti-spoofing is extremely effective in detecting network configuration errors, e.g., wrongly configured routing rules.

3.2.2 IP address spoofing protection on network interfaces

SNS firewalls use the concept of "internal" interfaces to identify the interfaces that the anti-spoofing mechanism recognizes. In **Configuration > Network > Interfaces,** the type of interface can be configured – a shield appears when anti-spoofing is enabled on an interface. From then on, such interfaces will accept only packets with a source address that is from the interface's switching network. The other interfaces on the SNS firewall will also reject such packets if they are incoming. These anti-spoofing rules are applied even before the network filter policy is evaluated.

INFORMATION
The routing table updates the list of protected networks. The list of IP addresses that are allowed to communicate with a protected interface can be filled in by configuring it as shown in the chapter Anti-spoofing via the routing table.

R21 | SNS-SMC | Declare internal interfaces
Only interfaces that provide access to a public network (Internet) or uncontrolled network have to be external. We recommend configuring all other interfaces as protected (internal) interfaces.

WARNING
By default, implicit filter rules allow SNS firewalls to be managed from internal interfaces. These rules must be disabled as explained in the chapter Implicit rules.

3.2.3 Anti-spoofing via the routing table

Routes inform the SNS firewall about the network topology and implicitly feeds data to anti-spoofing mechanisms. Any route going to a remote network that can be reached via an internal interface is added to anti-spoofing tables. As such, if packets with source IP addresses that were declared reachable are received on another interface, they will be rejected even before the network filter policy on the SNS firewall evaluates them. Routes that use external interfaces are not protected because in general, they are used to respond to appliances with source IP addresses that are not known in advance.

R22 | SNS | Define static routes for internal networks
Static routes must be defined for all known internal networks to which the SNS firewall's interfaces do not belong, in order to benefit from anti-spoofing mechanisms. These routes are identified in **Configuration > Network > Routing, IPv4 static routes** and **IPv6 static routes** tab with a shield.

WARNING
IPv4 and IPv6 routes for all remote networks that can be reached via internal interfaces must be declared. Otherwise, the SNS firewall will always reject their packets.

3.2.4 Anti-spoofing on bridges

A bridge makes it possible to connect several physical interfaces on the same network. However, the SNS firewall applies its anti-spoofing mechanisms independently on each interface on the bridge. Administrators do not need to apply any specific configuration for this anti-spoofing feature when the bridge is enabled.

When appliances are on the same switching network as the SNS firewall, it will keep an updated host table that contains each IP address encountered, and the associated physical interface. If an address is detected on an interface other than the one entered, an alarm will be raised.

WARNING
The host table will contain entries only when an SNS firewall starts receiving packets. Anti-spoofing on the bridge therefore does not protect contacts that are directly connected but have not yet sent any traffic.

Routing rules are necessary for remote networks, specifying the physical interface used. Anti-spoofing via the routing table, as explained in chapter Anti-spoofing via the routing table, is used.

3.2.5 Additional rules

The SNS firewall's native anti-spoofing mechanisms cannot recognize some configurations. A certain number of address ranges in particular defined in RFC 5735 are pre-configured on the SNS firewall in a specific group. These ranges belong to private networks and should not be used on a public interface.

R23 | SNS | Provide details with IP address spoofing rules
The anti-spoofing rules mentioned earlier should be filled in as much as possible by filter rules deduced from the network topology. For example, address ranges from the RFC 5735 group originating from the Internet should be explicitly prohibited.

4. Configuring services

4.1 Updates

Some features on SNS appliances require regular updates (enabled by default in **Configuration > System > Active Update**). The complete absence of updates would prevent the SNS firewall from obtaining security patches and renewing information databases. These updates can be applied:

- Offline by setting up an internal mirror,
- Online, through a proxy server or directly.

If the update is applied online, there will be as much management traffic as there are SNS firewalls in the IS. This may cause excessive bandwidth consumption. Using an internal mirror will therefore make it possible to restrict the number of SNS firewalls that are allowed to access the Internet.

The SMC server can be used as an internal mirror for SNS firewall updates. This feature can be enabled in **Configuration > Active Update server** on the SMC server.

R24 | SNS | Update from an internal mirror
Services should be updated regularly by enabling automatic updates and using an internal mirror.

For online use, ensure that only the SNS firewall uses the connection to the update server, only to this destination and for this sole purpose. This can be done by configuring a proxy server with authentication. The access account used on the proxy must be a dedicated account, and hold restricted access privileges to features that the SNS firewall must access (URL filtering and IP traffic strictly required for update operations on SNS firewalls, i.e. the URLs *update {1,2,3,4}.stormshield.eu* and *licence{1,2,3,4}.stormshield.eu*).

R24 - | SNS | Update through a proxy
If there is no internal mirror, the SNS firewall must access the mirror online over the Internet through an authentication proxy with a dedicated account and an adapted filter policy.

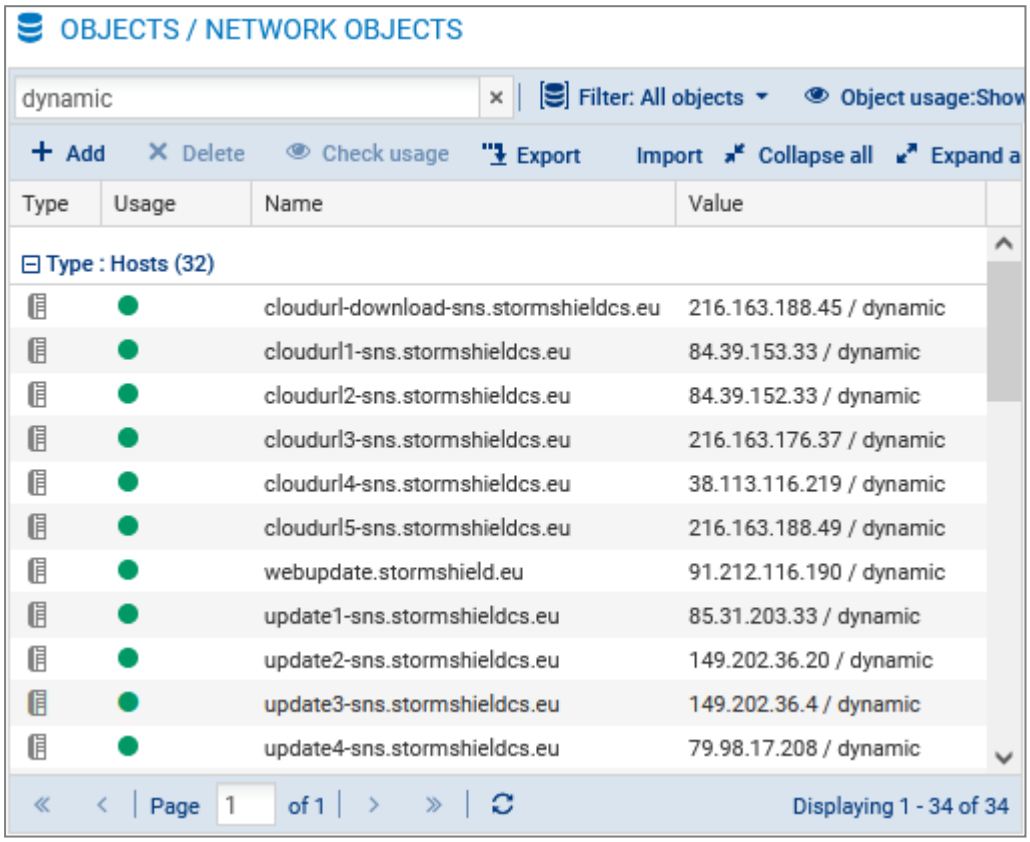
4.2 DNS

Domain name resolution is required when some services are used, e.g. the web proxy. When DNS servers are compromised, attackers can then redirect traffic to fraudulent peers.

R25 | SNS | Choose controlled DNS servers
Controlled DNS resolvers should be configured in **Configuration > System > Configuration > Network settings.**

R25 - | SNS | Change default DNS servers
DNS resolvers configured by default should be replaced with the ISP's if there are no controlled resolvers in the IS.

An SNS firewall's object database makes it possible to create static or dynamic objects. These objects depend on a domain name that the SNS firewall regularly resolves. There are about fifteen such domain names by default, ending in stormshieldcs.eu or stormshield.eu, part of which is represented in the image below (these names may vary depending on updates). By applying recommendation R30, these DNS queries can be blocked by default, which cannot be blocked by filter rules.



Using an internal mirror (recommendation R24) means that an SNS firewall does not have to contact Stormshield's update servers directly. Also, when controlled DNS servers are used (recommendation R25) addresses for Stormshield's other services (license management, etc.) no longer need to be managed.

R26 | SNS | Restrict the use of dynamic objects
Unused dynamic objects should be deleted and objects that remain in static mode should be reconfigured instead in **Configuration** > **Objects** > **Network**.
As dynamic objects are local objects, they cannot be removed from an SMC server.

R26 | SMC | Restrict the use of dynamic objects
Unused dynamic objects (such as FQDNs) should be deleted and objects that remain in static mode should be reconfigured instead in the **Network objects** menu.

4.3 NTP

Some features are closely linked with the system time, such as logging and certificate management. By manually setting the time, the appliance will not be integrated correctly into

the IS. Moreover, simply using the internal clock does not guarantee that there will not be any drift in the long run.

R27 | SNS-SMC | Synchronize system time
NTP synchronization should be enabled on SNS firewalls, and several reliable time servers should be used, in line with the technical note Security recommendations for the implementation of log systems (in French).

4.4 Using an external directory

This feature was not part of the security target during the SNS firewall qualification process.

Various features, including administrator authentication, require a connection to a directory. When this directory is outside the SNS firewall, the security (confidentiality and integrity) of traffic exchanged must be guaranteed and appliances (firewall, administration server and directory server) must be authenticated . Otherwise, attackers would be able to obtain information about the connection.

R28 | SNS-SMC | Configure the LDAP securely
If the LDAP service is configured:

- The LDAPS protocol should be used, with the LDAP server presenting a certificate that has been signed by a controlled PKI,
- The corresponding CA should be imported on the SNS firewall or SMC server,
- The CA imported earlier should be used to validate the connection to the LDAP server.

Authentication from an external directory can be set up in several steps:

- Enable the use of the directory (**Configuration > Users > Directory configuration**), choose its type then configure access:
  - The address of the directory,
  - The base DN,
  - The communication port,
  - The login and password of the SNS firewall's access account on the directory. This account must comply with recommendation R8,
  - Password hashing.
- Specify the structure of the directory (**Structure** tab). The attributes that the SNS firewall manages must be mapped to those in the LDAP directory. The *Stormshield member* attribute in particular, which contains the list of identifiers belonging to a group, must match its equivalent in the LDAP directory,
- Set LDAP as the default authentication method (**Configuration > Users > Authentication**).

5. Filter and NAT policy

5.1 Naming the network filter policy

By default, filter policies found on an SNS firewall do not have explicit names. This does not allow an administrator to easily understand the role of the SNS firewall, or know which policy to apply if there are several. Implementing a naming system makes it possible to:

- Reflect the function of the SNS firewall through the name of the filter policy, e.g., Internet access, isolating traffic for a specific partner, etc.,
- Reduce processing errors, e.g., by enabling the wrong policy,
- Uniformly configure the names of filter policies on all SNS firewalls in the IS.

R29 | SNS-SMC | Rename the production policy
A policy should be implemented setting out filter profile naming criteria, as explained in the guide Recommendations for the definition of a firewall's filter policy] (in French).

5.2 Implicit rules

The SNS firewall is configured by default with implicit filter rules that are evaluated before manually defined filter rules. The purpose of such rules is to simplify the configuration process by allowing particular requests or access privileges. To find out more on available implicit rules, refer to the section on Implicit rules in the *SNS v4.3 LTSB user guide*.

The **Configuration > Security policy > Filter - NAT** menu therefore does not contain all the rules that the SNS firewall applies. As such, a rule created by an administrator may never be evaluated because an opposing rule exists.

R30 | SNS | Disable implicit rules
We recommend disabling all implicit filtering rules, except the rule "Allow mutual access between the members of a firewall cluster (HA cluster)" in a high availability (HA) firewall cluster. Implicit rules can be disabled in **Configuration > Security policy > Implicit rules**.

WARNING
To avoid losing administration powers, new filter rules must be created before disabling the corresponding implicit rules. Depending on requirements, these rules must allow HTTPS, NSRPC or SSH traffic between the SNS firewall and groups defined in the chapter Configuring administration IP addresses on the interfaces defined in the chapter Dedicated web administration interface.
In addition, to avoid downgrading the performance of certain SNS firewall features, new filter rules have to be created before disabling the implicit rules of the options and parameters in use. For example, for ESP traffic, the "Status tracking (stateful)" option is essential in preventing the downgrade of IPsec VPN performance.

INFORMATION
The NSRPC `monitor filter` command makes it possible to display all the filter rules that were

applied. In this case, disabling implicit traffic from hosted services does not block the DNS requests sent by the SNS firewall. Applying recommendation R26 limits such traffic.

5.3 Protocol analysis

Some malicious traffic may share the same network characteristics as authorized traffic. Such traffic cannot be blocked simply with filter rules without impacting legitimate traffic. SNS firewall are equipped with protocol analysis features that enable modular filtering. The way traffic processed by a filter rule is inspected can be configured according to one of three inspection levels: Firewall, IPS or IDS.

Configured with the Firewall inspection level, the SNS firewall only performs superficial compliance checks. It monitors in particular the direction in which connections are set up. It will not check the flags used, sequence numbers or TCP options.

WARNING
When the SNS firewall that is configured with the Firewall inspection level aborts a session, it sends a reinitialization packet that contains a null sequence number. The peer, not being able to associate this number with any existing connection, will not close any connections.

Configured with the IPS inspection level, the SNS firewall performs additional checks on compliance with protocol standards, as well as analyses that rely on known attack patterns. Inspection modules dedicated to each protocol conduct these analyses. Depending on its settings, the module in question may block traffic that is deemed malicious.

IDS level inspections are the same as those in the IPS inspection level, but will only raise alarms if traffic seems malicious, without blocking it. The IDS inspection level can be used in pre-production to analyze traffic that passes through a system, thereby easing the administrator's task of configuring inspection modules.

There are several operating modes in IDS and IPS inspection levels:

- Inspection modules are automatically loaded by default, depending on the ports used in filter rules and the characteristics of the traffic analyzed by the SNS firewall. This will be referred to as “automatic mode” in the rest of this document,
- The number of modules loaded can also be restricted by specifying only those that need to be used in the filter rule. In this case, the SNS firewall will only conduct the analyses corresponding to the requested protocol. The term “transport mode” will be used in this document when the indicated modules are only transport protocols such as TCP, UDP, etc.
- The modules may also concern a particular application protocol. We will use the concept of “application mode” later on. When loaded modules are evaluated as part of a qualification process, the term "qualified application mode” will be used. This includes the modules relating to the protocols:
  - FTP over TCP,
  - HTTP over TCP (including WebDAV extensions),
  - SIP over TCP or UDP,
  - SMTP over TCP,
  - DNS over TCP or UDP.

  And these Industrial protocols:
  - OPC UA over TCP,
  - MODBUS over TCP.

IPS inspection in automatic mode is selected by default when a filter rule is created. Without an inspection profile, all protocol analysis modules may be loaded during the inspection of traffic that the filter rule analyzes, which can increase the SNS firewall's CPU load. If necessary, limit the loading of these modules by using an inspection profile, as is the case with the IPS inspection level in transport mode. Where possible, protocol analysis functions should be conducted by dedicated appliances such as proxy servers to minimize the risk of compromising the SNS firewall.

R31 | SNS-SMC | Adapt the traffic inspection type to the role of the SNS firewall
IPS inspection levels in application mode, or IPS in transport or Firewall mode are recommended, in line with the role of the SNS firewall in the architecture of the analyzed information system. Particular care is required with regard to its exposure to threats, its role and the criticality of the resources to be protected.

WARNING
IP address spoofing protection is disabled with the Firewall inspection level.

The analysis level and associated mode must be set for each filter rule and vary according to the role of the SNS firewall. For example:

- If it is used only as a VPN gateway at the perimeter of the IS and is itself protected by other firewalls, the Firewall inspection level makes it possible to dedicate resources to cryptographic functions while reducing the attack surface,
- If it is located between a corporate IS and the Internet, the IPS inspection level in transport mode makes it possible to restrict the SNS firewall's attack surface while guaranteeing thorough filtering of connections,
- If it protects application servers that can only be reached from an organization's internal network, the IPS inspection level in qualified application mode can be used.

In the **Security inspection** column in filter rules (**Configuration > Security policy > Filter - NAT > Filtering**), the inspection level can be selected. For IPS and IDS inspection levels, the **Protocol** column allows the analysis level to be restricted. When the **Protocol type** option is set to **IP protocol**, a transport protocol can be chosen in the **IP protocol** menu. If this option is set to **Application protocol**, the menu of the same name will allow users to select the application protocol that the SNS firewall will analyze. Only one protocol (application or transport) can be chosen for each filter rule.

Firewall, IDS and IPS inspection levels rely on the use of inspection profiles, which make it possible to configure the behavior of the SNS firewall according to the type of traffic processed, e.g., types of alarms to raise or traffic to block. Before switching the protocol inspection to a production environment deemed safe (typically, a pre-production environment), it is better to disable alarms that legitimate traffic would generate unnecessarily. This will avoid polluting security monitoring traffic after the inspection goes into production. Using multiple profiles will make it possible to adjust configurations to the use context. More granular and therefore more restrictive inspection profiles are recommended for the most critical applications.

R32 | SNS-SMC | Adapt inspection profiles to the SNS firewall's use context
When protocol analysis is enabled, the policy should be adjusted as closely as possible to the networks that require protection, by relying on the various inspection profiles.

Out of the pre-configured inspection profiles, two are used by default: profile *00* for traffic sent by an external network, and the profile *01* for traffic sent by an internal network. Profiles are

chosen for each filter rule in the **Inspection** tab. These profiles can be configured in **Configuration > Application protection > Inspection profiles**, by selecting **Go to profiles**. Each profile is then based on the policies defined in **Configuration > Application protection > Protocols**. These policies define the general analyses of various protocols, such as default ports, restricted commands, types of analyses, etc. Moreover, **Configuration > Application protection > Applications and protections** defines more specific analyses such as the detection of *buffer overflow* or encoding format, etc. This menu offers views by profile or by context.

5.4 Filter policy

On SNS firewalls, the same objects may need to be used several times if they appear in several filter rules or when these rules are used in addition to a configuration menu. For example, the same sub-network may appear in several filter rules (from a network of workstations to a mail server, or to a web proxy, etc.), or as an administration network (refer to the chapter Configuring administration IP addresses) and in a correlated explicit filter rule (in line with the chapter on Implicit rules).

Every time something is changed (e.g. address range), added (new sub-networks to host new workstations) or deleted (restriction of the number of administration workstations), the configuration must be updated, thereby increasing the risk of error or omission. Using objects and object groups makes it possible to apply a configuration globally and simultaneously when changes are made.

R33 | SNS-SMC | Use object groups
Object groups are recommended when defining filter rules, to remain consistent with the other menus.

When groups are used, it is possible to control for example:

- An administration group containing the IP addresses of administration workstations,
- A user workstation group containing the IP sub-networks used,
- A service group containing the IP addresses of internal servers,
- A BU group containing the ports used by ERPs,
- etc.

After which, items only need to be added to or removed from groups when there is a change of situation.

Furthermore, the best practices with regard to defining a network filter policy are explained in the guide Recommendations for the definition of a firewall's filter policy (in French). The main aim of this document is to set out the practices to adopt to guarantee that the filter policy will be durable and controllable.

6. Certificates and PKI

SNS firewalls and the SMC server need to use certificates in several cases, including:

- The publication of the web administration interface in HTTPS,
- The authentication of administrators via certificate to access the SNS firewall's web administration interface,
- The authentication of users and gateways to set up IPsec VPN tunnels,
- The authentication of users and gateways to set up SSL VPN/TLS services,
- The connection to an external directory in LDAPS,
- The connection of SNS firewalls to the SMC server.

6.1 Using a PKI

When an SNS firewall is involved in an authentication process, the authentication mechanism can rely on certificates issued by a PKI. The level of trust placed in this PKI will determine the trust in the certificate used and therefore the reliability of the authentication. When no external solutions are used to manage certificates, SNS firewalls offer the possibility of generating a certification authority and identities (consisting of a private key, a public key, and the peer certificate) signed by this authority. In this case, private keys are generated by and stored on the SNS firewall. If the SNS firewall is compromised, so will the secrets that are generated by it.

R34 | SNS-SMC | Use a controlled external PKI
We recommend using a controlled PKI that operates separately from the SNS firewall or SMC server to generate the identities used. This PKI and CAs used must comply with the recommendations in Appendix A1 of the RGS (in French).

R34 - | SNS | Use the SNS firewall's PKI
In the absence of an external PKI, the PKI found on the SNS firewall can be used. In this case,

- The generated secrets must be deleted from the SNS firewall after they are exported to recipient SNS firewalls,
- The administrators of the PKI must be dedicated to this role only (see recommendation R9).

R34 - | SMC | Use the SNS firewall's PKI
In the absence of an external PKI, and since the SMC server does not provide a built-in PKI, the PKI found on an SNS firewall can be used.

WARNING
When the SNS firewall's internal PKI is configured, if it is compromised, a hacker will be able to forge an identity that will be considered legitimate on the IS. As such, this function has to be restricted to the SNS firewalls that are the least exposed as possible to uncontrolled networks.

6.2 Managing CRLs in an IPsec VPN tunnel

Certification authorities can revoke certificates before their scheduled expiry. This occurs for example when a private key has been compromised or when an administrator leaves the organization. Accepting such certificates would allow an illegal user or appliance to authenticate on the SNS firewall. When the PKI implements CRLs, affected SNS firewalls can be informed when certificates are revoked. By default, the absence of a CRL does not hinder the setup of an IPsec VPN tunnel, but will simply be reported in the SNS firewall's logs.

R35 | SNS-SMC | Impose CRL verification
CRL verification should be imposed when implementing IPsec VPN tunnels.

This behavior can be changed by modifying the *CRLrequired* parameter and restarting the IPsec service. This can be done using the following NSRPC commands:

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

This parameter is stored in */Firewall/ConfigFiles/VPN/01/*. The IPsec service can be enabled in console mode with the following NSRPC commands:

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

When these commands are used, all VPN tunnels will be closed, and the new VPN policy (01) will be enabled. In both cases, the value of *01* used as an example represents the number of the IPsec policy used.

Retrieved CRLs are stored locally in the folders of their corresponding CAs or delegated CAs and renamed **CA.crl.pem**.

INFORMATION
When the parameter *CRLrequired* is enabled, the user must possess all the CRLs in the certification chain.

6.2.1 Automatically importing CRLs

Even though a CRL has limited validity, it is important to check regularly whether any certificates have been revoked. The frequency with which the CRL is updated must be adapted to the use of authentication via certificate. If updates are too far apart, the SNS firewall may risk authenticating revoked certificates and allowing illegal access. For example, retrieving the CRL every 6 hours would drastically reduce the amount of time in which a revoked certificate can be used.

R36 | SNS | Adapt the automatic refreshment of CRLs
The refreshment time should be adapted to the desired level of responsiveness. If various services require different durations, the shortest must be used.

By default when the URL of a CRL is added and enabled, files are retrieved every 6 hours. Updates can be forced by using the `system checkcrl` NSRPC command. Use `system checkcrl help` for more details regarding the command. The frequency with which CRLs are retrieved via the web administration interface can also be modified.

R37 | SNS-SMC | Configure the CRL retrieval URL and enable automatic retrieval
We recommend configuring the URL for the automatic retrieval of the CRL of each CA, and enabling this feature in **Configuration > System > Configuration** on SNS firewalls, by selecting the **Enable regular retrieval of certificate revocation lists (CRL)** checkbox. On the SMC server, this configuration can be found in **Configuration** > **Certificates** > *CA name* > **CRL distribution points**.

CRL distribution points that are associated with a CA can be set either in the SNS firewall's web administration interface in the menu **Configuration > Objects > Certificates and PKI** > *CA name* > **Certificate profile**, or by using the NSRPC command:

```
pki ca checkcrl add caname=<AC name> uri=<CRL URL>
```

The distribution point URL can be in HTTP, HTTPS, LDAP, LDAPS or FTP.

INFORMATION
To allow the SNS firewall to resolve the FQDN of the CRL distribution point's URL, a **Host** object corresponding to the FQDN must be defined in its object database.

6.2.2 Manually importing CRLs

In some cases, automatically importing a CRL may be difficult, or even impossible. This occurs when a VPN tunnel is needed in order to obtain one, and the previous CRL is no longer valid or was never imported. The CRL can then be imported manually. During this operation, the administrator's action is required, and files need to be handled. Strict organizational procedures are therefore necessary and this operation must only be conducted exceptionally.

R37 - | SNS-SMC | Manually import CRLs
If CRLs cannot a imported automatically, they can be imported manually.

They can be imported manually on the SNS firewall via the web administration interface in **Configuration > Objects > Certificates and PKI > Add > Import a file**. The CRL file must be imported in PEM or DER and its name must not contain any extensions. During import, the CRL file will be copied into the folder of the CA with which it is associated, then converted to PEM and renamed **CA.crl.pem**.

On an SMC server, CRLs can be manually imported through the web administration interface, in **Configuration** > **Certificates** > *CA name* > **SMC as CRL distribution point**.

7. IPsec VPN

Traffic must sometimes be exchanged over networks that are not controlled or with less protection of exchanged data. In such cases, there are higher risks of data leaks or tampering, and with more serious consequences. Data must therefore be exchanged between authenticated entities through channels that guarantee integrity and confidentiality. Encrypted IPsec VPN tunnels meet such needs. This section describes the configuration policy to apply to SNS firewalls used as encrypting gateways.

7.1 Encryption profiles

The confidentiality and integrity of data exchanged over a VPN (site to site or client to site) depend on the use of robust cryptographic algorithms negotiated between both parties. By using encryption profiles, allowed algorithms can be specified. Even though the pre-configured *StrongEncryption* profile is compatible with the requirements of Appendix B1 of the RGS (in French), it is advisable to manually reconfigure the IKE and IPsec encryption profiles.

In order of preference, the following algorithms are recommended:

- 256-bit or 128-bit encryption algorithms: AES-GCM, AES-CTR, and AES-CBC;
- If AES-GCM, SHA2-512, SHA2-384 or SHA2-256 are used, embedded GMAC authentication or integrity algorithms;
- Diffie-Hellman (PFS in phase 2) key exchange algorithms of at least 256 bits on elliptical curves. If no elliptical curves are available, use modules that are at least 3072 bits. This translates to DH group numbers in order of strength: 30 or 21, 29 or 20, 28 or 19, 18, 17, 16, or 15.

The tables below provide the lowest encryption profile that is compatible with the recommendations in the RGS. The cryptoperiods indicated in these tables are not taken directly from the RGS but given for information only. They must be set according to the organization's security policy.

ANSSI-recommended IKE encryption profile

Parameter	Lowest value	Recommended value
Encryption algorithm	AES GCM 256	AES GCM 256
Diffie-Hellman group	Group DH15 (3072 bits)	Group DH28 (256 bits)
Cryptoperiod	86400s	21600s

ANSSI-recommended IPsec encryption profile

Parameter	Lowest value	Recommended value
Encryption algorithm	AES CBC 128	AES GCM 256
Hashing/authentication	SHA 256	
Diffie-Hellman group	Group DH14 (2048 bits)	Group DH28 (256 bits)
Cryptoperiod	21600s	3600s

For more information, refer to ANSSI's Guide on selecting cryptographic algorithms (in French).

R38 | SNS-SMC | Use strong algorithms for IKE and IPsec
We recommend using encryption algorithms that are in line with the details given above, and with ANSSI's Guide on selecting cryptographic algorithms (in French).
Encryption profiles can be found in **Configuration > VPN > IPsec VPN > Encryption profiles** for SNS firewalls, and in **Configuration > Encryption profiles** on the SMC server.

7.2 Key exchange and authentication

7.2.1 IKE protocol

The level of protection provided by an IPsec VPN tunnel depends on the robustness of the cryptographic suite implemented, as well as the reliability of the key exchange mechanism: keys can be exchanged via the IKEv2 protocol over SNS firewalls in version 2.0.0 and higher. The use of recent protocols complies with the Security recommendations relating to IPsec (in French).

R39 | SNS-SMC | Use version 2 of the IKE protocol
If all the IPsec VPN tunnel peers are compatible, IKE in version 2 is recommended.

7.2.2 Authentication

To prevent the peer's identity from being spoofed, regardless of the type of tunnel configured (site to site or client to site), the remote peer must authenticate when the tunnel is created. In this step, which goes through IKE, the peer can authenticate using a pre-shared key or certificate. When pre-shared key are used, peers cannot be differentiated and adapted privileges cannot be applied individually to them. Moreover, if a key must be renewed (e.g., when remote appliances have been compromised, or a user loses privileges), the key must be renewed on all configured SNS firewalls. Only when a PKI is used can each peer be identified, and privileges and revocations can be more easily managed.

R40 | SNS-SMC | Use mutual certificate-based authentication
The mutual authentication of IPsec VPN tunnel peers via certificate is recommended, by entering the accepted certification authorities in the **Configuration > VPN > IPsec VPN > Identification** menu on SNS firewalls, and in the **Configuration** > **VPN topologies** menu on the SMC server.

R40 - | SNS-SMC | Use a robust pre-shared key
If pre-shared key authentication is selected for an IPsec VPN, it should be chosen in compliance with the recommendations in Appendix B3 of the RGS (in French) and the Recommendations relating to multifactor authentication and passwords(in French).

WARNING
If pre-shared key authentication is selected, the following requirements must be met:

- The entropy of the secret must be at least 128 bits (22 random characters including uppercase and lowercase characters and numbers). Refer to Appendix B1 of the RGS for further detail,

- The secret must comply with the rules regarding passwords set out Relating to multifactor authentication and passwords(in French),
- A different secret must be used for each site-to-site VPN tunnel,
- The secret must renewed regularly, and its cryptoperiod (maximum amount of time for which the breach of traffic integrity and confidentiality is accepted if the secret is compromised) must be set according to the organization's security policy.

7.3 Routing policies, outgoing filter policies and IPsec VPN configuration

When an SNS firewall is used as a VPN gateway, routing and filter rules must be properly configured to guarantee the confidentiality and integrity of traffic. Four functions are closely linked:

- Routing,
- Filter policy,
- NAT before IPsec,
- IPsec policy.

When IPsec VPN tunnels are implemented, a route must be configured to reach the remote networks that can be accessed through tunnels. Otherwise, the packet will be deleted during routing and will not reach the IPsec encryption stage.

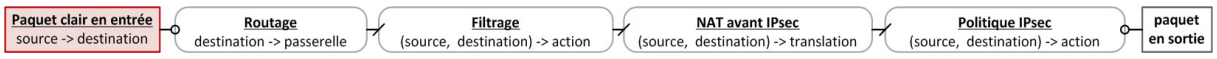
We recommend configuring the special blackhole object as a gateway for its routes. This object creates a route to an IP address in the local loop, and adds a special marker in it, which tells the system that packets passing through it must be destroyed.

After the IPsec policy is applied, the routing policy will be evaluated again based on the encrypted packet. However, if there is an error in the IPsec policy, the packets will be destroyed instead of leaving in plaintext.

The order of the routing, filtering, NAT before IPsec and IPsec policy functions shown on the image below, directly impacts the confidentiality of traffic. This sequence is only part of the packet's full path in the SNS firewall. Indeed, when it is encrypted, the packet will then be processed by filtering, NAT after IPsec, and routing.

The most specific rules must be defined for the filter policy and the least specific for the IPsec policy.

Functional components



R41 | SNS - SMC | Configure IPsec VPN tunnels securely

During the configuration of an IPsec VPN tunnel, the following is recommended:

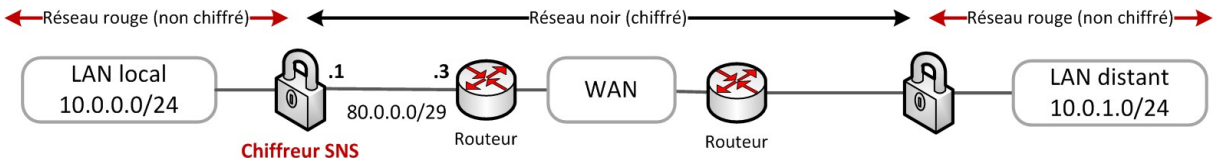
- Configure a static route to the special blackhole object to reach remote networks that can be accessed through IPsec VPN tunnels,
- Ensure that the IPsec policy is never enabled, even during transitional phases,
- Ensure that filter rules are always more specific than NAT before IPsec rules,

- Ensure that traffic (source and destination IP addresses) after translation (NAT) matches the IPsec policy,
- Ensure that in the absence of NAT rules, filter rules are always more specific than the IPsec policy.

WARNING
Ideally, separate SNS firewalls should be implemented to dissociate encryption from the filtering of plaintext traffic, and the filtering of encrypted traffic.

The examples below illustrate the advantage of the previous recommendation. They apply to SNS firewalls that act as a VPN gateway for outgoing traffic on the local LAN, and for traffic going to a remote LAN through an IPsec VPN tunnel set up with a remote VPN gateway. The architecture is represented on the image below.

Architecture



Each example provides the configuration of the SNS functional components that a network packet passes through (Functional components image. The network packet enters with a specific source and destination. Packets pass through these functions in this sequence:

- Pre-routing,
- Filtering,
- NAT before IPsec,
- IPsec policy.

The end result is described by the outgoing packet, whether it is:

- Encrypted,
- Plaintext (not encrypted),
- Destroyed,
- Filtered.

A black, red or green color code is applied to represent respectively: the primary path, error (plaintext), and behavior after correction.

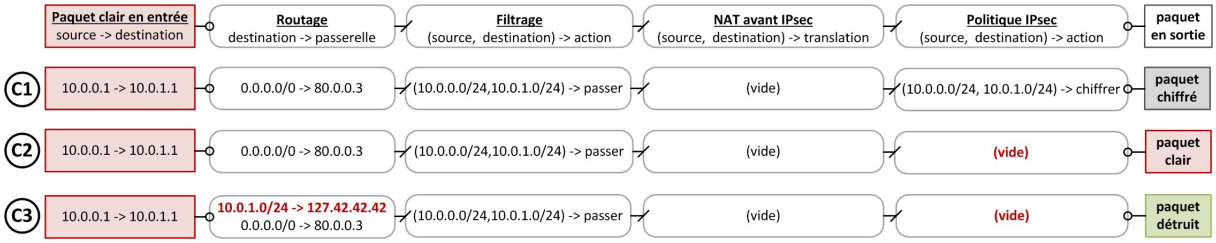
For each example, three cases (C) are represented:

C1	Configuration that does not comply with the recommendation, the input parameters are nominal.
C2	Issues relating to the previous configuration are highlighted. Some entries or the configuration will be modified. Changes are shown in red.
C3	Suggested configuration to avoid reproducing the earlier issue. Changes are shown in red.

7.3.1 Constantly active IPsec policy

The example represented in the image below illustrates the need for remote IPsec networks to use a route to the special blackhole object. In the case of **C1**, packets first go into the routing table, which contains a valid route to the remote LAN (the default route in the example). The packets then go through the filter policy, which accepts the packets, which then move on to the IPsec policy, which encapsulates, encrypts and protects the integrity of the traffic. The source and destination of encrypted packets are different from those of plaintext packets. The destination of the encrypted packet in particular is the remote VPN gateway. Packets go through the routing table again (the route to the remote LAN is not used, only the route towards the remote VPN gateway is used), which contains a valid route to the IPsec gateway (default route). Outgoing packets are encrypted.

Constantly active IPsec policy, route to the special blackhole object



Next, the IPsec policy switches from enabled (**C1**) to disabled (**C2**). It can be disabled permanently or for a transitional period, which occurs when the IPsec policy is disabled then enabled again.

In the case of **C2**, packets first go into the routing table, which contains a valid route to the remote LAN. The packets then go through the filter policy, which accepts the packets. However, since no IPsec policies were defined, the packets are sent in plaintext at the next hop, i.e., the default gateway defined in the routing table. Data is leaked.

The solution presented in **C3** consists of defining a route to the special blackhole object. This creates a route to an IP address in the local loop, and adds a special marker in it, which tells the system that packets passing through it must be destroyed. In the absence of an IPsec policy, the SNS firewall will destroy the packet instead of sending it to the default gateway.

R41+ | SNS-SMC | Do not use the default route
If all the networks used are known, the default route is not recommended. Choose explicit routes instead to reach all remote peers. In this way, only the packets that have an explicitly defined route will be able to leave in plaintext.

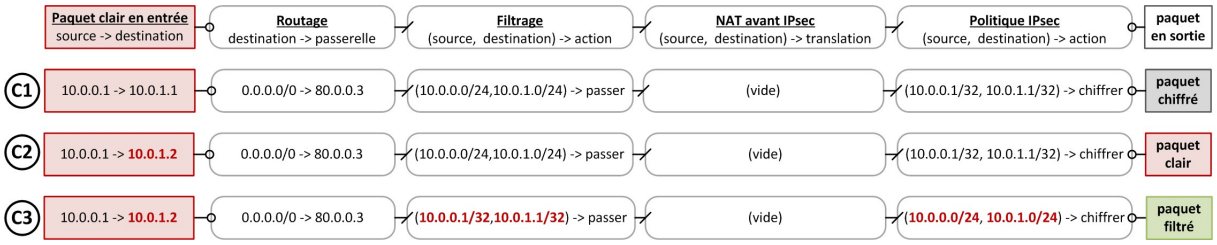
WARNING
Address ranges must be chosen to prevent confusion between red and black networks as described in architecture image, and to facilitate the creation of routes.

7.3.2 Filter rules always more specific than the IPsec policy

The example represented in as in the image below illustrates the need to specify a filter policy that is always more specific than the IPsec policy. In the case of C1, the filter policy is defined in /24 while the IPsec policy is in /32. The administrator wants, for example, to define a

cryptographic context per IP address pair, while keeping a shared filter policy. At the beginning, only two hosts communicate with each other. Packets pass through the filter policy, then the IPsec policy, and are sent encrypted.

Filter rules always more specific than the IPsec policy



In **C2**, an appliance is added to the network, but the SNS firewall configuration does not change. Packets to this new IP address are accepted by the filter policy and not selected by the IPsec policy, so they are sent in plaintext. Data is leaked.

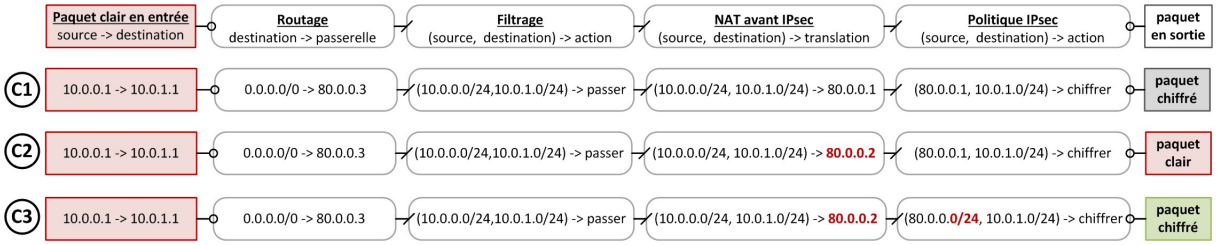
The correction implemented in **C3** consists of setting a filter policy in /32 and an IPsec policy in /24. The filter policy is therefore always more restrictive than the IPsec policy. Packets will either be filtered or Encrypt, but cannot be sent in plaintext.

When an IPsec policy is used to interconnect networks, it must not be modified too often and the networks used can be extended, unlike a filter policy, which can be very specific and modified frequently.

7.3.3 NAT before IPsec rules included in the IPsec policy

The example represented in the image below illustrates the need to specify NAT before IPsec rules included in the IPsec policy. In the case of **C1**, a NAT before IPsec rule is applied. Its result is a selection criterion in the IPsec policy. Modifying this rule will directly affect the confidentiality of data. Packets are accepted by the filter policy then modified by the NAT before IPsec rule and then selected by the IPsec policy. They are encrypted on the way out.

NAT before IPsec rules included in the IPsec policy



In the case of **C2**, a NAT before IPsec rule is modified. Packets are accepted by the filter policy then modified by the NAT before IPsec rule. As the outgoing IP address is modified, the IPsec policy will no longer select it, so packets are sent in plaintext. Data is leaked.

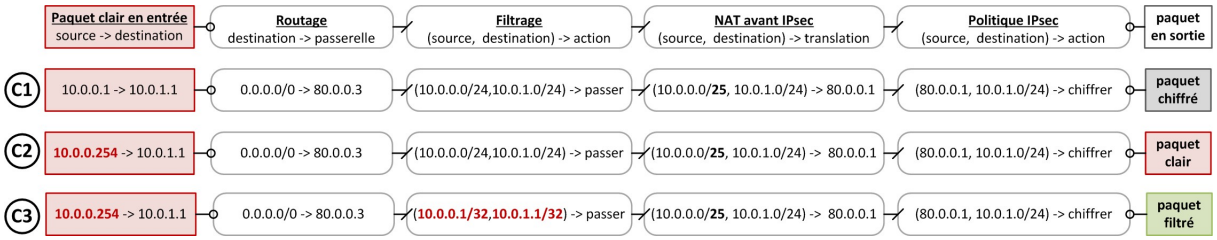
The solution shown in **C3** consists of defining an IPsec policy broader than the NAT rule used. Even if the outgoing IP address is modified, the IPsec policy will still select the packet, which will be encrypted by the SNS firewall.

INFORMATION
The NAT rule must go together with an ARP publication if the address(es) used do(es) not belong to the SNS firewall's interfaces.

7.3.4 Filter rules always more specific than NAT before IPsec rules

The example represented in the image below illustrates the need to specify filter rules that are always more specific than NAT before IPsec rules. In **C1**, the source network of the NAT before IPsec rule is in /25 while the source network in the filter rule is in /24. Packets originate from a source address that is included in both /24 and /25. Packets are accepted by the filter rule, then the NAT before IPsec rule is applied, and finally the IPsec policy. Outgoing packets are encrypted.

Filter rules always more specific than NAT before IPsec rules



In **C2**, the source IP address is included in /24 but not in /25. Packets are accepted by the filter policy and not selected by NAT before IPsec rules. The IPsec policy is not applied, so packets are sent in plaintext. Data is leaked.

The correction implemented in **C3** consists of setting a filter policy in /32. The filter policy is therefore more restrictive than the NAT before IPsec rules. Packets will either be filtered or encrypted.

7.4 Incoming filter policy in IPsec VPN tunnels

A hacker on the network can send traffic to the SNS firewall by spoofing a legitimate peer's red address. These unencapsulated messages must be identified and rejected. Traffic can be blocked with a filter rule that allows plaintext traffic only if it originates from an IPsec VPN tunnel. If the tunnel has not been set up, it will be systematically blocked.

When editing a filter rule, the **IPsec VPN tunnel** value must be entered in the **Source > Advanced properties > Via** field.

On an SNS firewall, this feature can be configured in **Configuration > Security policy > Filter - NAT > Filtering**.

On an SMC server, this feature can be configured in **Configuration** > **Firewalls and folders** > **Filter rules**.

R42 | SNS-SMC | Confirm the source of incoming traffic
Indicate the source of the traffic, which can only be accessed through a VPN tunnel to filter traffic arriving in plaintext with the same source address.

In addition, the security policies of each IPsec VPN tunnel ensure that traffic passes through the tunnel that they deem legitimate.

7.4.1 IP address spoofing protection on IPsec VPN tunnels

SNS firewalls treat IPsec VPN tunnel endpoints as interfaces. As such, the status of an internal interface, explained in the chapter IP address spoofing protection on network interfaces, also applies to them. In **Configuration > Application protection > Inspection profiles**, the option **Treat IPsec interfaces (except virtual IPsec interfaces) as internal interfaces. Applies to all tunnels - remote networks will need to be explicitly legitimized.** This option increases the network's security when it is associated with appropriately defined routes and filter rules.

R43 | SNS-SMC | Declare the internal VPN interface
VPN interfaces that are considered "internal" should be declared to benefit from anti-spoofing mechanisms.

7.5 Mobile access tunnels

In a client-to-site VPN tunnel, a mobile device with an unknown connecting IP address is interconnected with a local network. In such a setup, the mobile device is both the remote peer (which sends and receives unprotected traffic) and endpoint of the IPsec VPN tunnel that protects incoming and outgoing traffic. The IP address that carries unprotected traffic is called a red IP address, as opposed to the black IP address, which represents the tunnel endpoint.

It therefore functions differently from a site-to-site VPN tunnel, which is configured between two VPN gateways that in principle have black IP addresses known in advance; the traffic that requires encryption originates from separate subnetworks.

Mobile tunnels can be configured in **Configuration > VPN > IPsec VPN > Mobile – Mobile users**. The peer can either select its own red IP address, or be provided with one. In the first case, it is difficult to control routes and filter rules, while ensuring that there are no address conflicts between peers. In the second case, config mode allows the SNS firewall to send the red IP address that the client must use, which protects it from the risks mentioned.

R44 | SNS | Configure mobile tunnels in *config* mode
Config mode is recommended in mobile tunnels so that remote red IP addresses can be controlled. This mode can be set when the VPN access policy is created or subsequently in **VPN** > **IPsec VPN** > **Mobile – Mobile users.**

Setting up mobile VPN tunnels makes it possible to interconnect mobile users with local networks. It is therefore important to ensure that only explicitly authorized users can set them up. On SNS firewalls, this authorization is determined by default based on the validity of the shared key or the certificate (it cannot rely on the peer's public IP address, which is not authenticated and not known in advance in mobile VPN tunnels).

In mobile VPN tunnels, a shared key has to be defined for each client. However, this method raises a few security issues:

- In the event of compromise or suspected compromise, this key must be changed on all mobile clients,
- The authentication of mobile clients is not guaranteed,
- The VPN gateway is vulnerable to brute force attacks.

R45 | SNS | Authenticate mobile SNS firewalls and/or users with certificates
Mobile SNS firewalls and/or users must be authenticated using certificates, to guarantee protection from the inherent weakness of pre-shared keys and to comply with recommendation R40.

When a certification authority is entered as *accepted* in **Configuration > VPN > IPsec VPN > Identification**, all certificates issued by this authority are allowed to set up mobile VPN tunnels.

R46 | SNS | Use a dedicated intermediate certification authority
To facilitate the management of permissions granted to mobile VPN tunnels, it is advisable to accept only intermediate certification authorities that serve to issue certificates dedicated to the use of this service.

Furthermore, certificate-based authentication makes it possible to use the UAC (User Access Control) mechanism that the SNS firewall provides when a directory is also used. With this feature, permissions to access mobile VPNs, filter rules and NAT rules can be managed granularly.

7.6 Dead Peer Detection

This mechanism periodically checks the status of IKE tunnels by exchanging encrypted messages. In IKEv1, this mechanism is standardized in RFC 3706. In IKEv2, this mechanism has been renamed "*Liveness*" and is an integral part of the protocol's application standard. On the SNS firewall, this mechanism is known as "*Dead Peer Detection*" (or DPD) in both IKEv1 and IKEv2.

The parameters that determine DPD decisions are:

- Testing frequency,
- Waiting time for response,
- The number of failures (no response) to tests.

If no responses to DPD tests are received, and the maximum number of failures is reached, the IKE VPN tunnel and related IPsec VPN tunnels will be closed.

There are several ways to use this mechanism in IKEv2:

- In *passive* mode, the SNS firewall does not monitor the status of the peer but replies if it is contacted,
- In *high* and *low* modes, the SNS firewall monitors the status of the peer and replies if it is contacted. In *high* mode, requests will be sent more frequently than in *low* mode.

R47 | SNS-SMC | Enable Dead Peer Detection
In an IPsec VPN tunnel, Dead Peer Detection should be implemented in *high* or *low* mode.

R47 - | SNS-SMC | Use passive DPD mode
If it is not known whether Dead Peer Detection is implemented on the remote endpoint, passive mode is recommended, making it possible to reply if a DPD request is received.

7.7 KeepAlive

When an IPsec VPN tunnel is not in use, it can be shut down after a set period to release resources on SNS firewalls. However, if traffic must pass through this tunnel, negotiations must be started all over again. This will generate latency and cause minor packet loss. With the KeepAlive mechanism, traffic can be generated artificially in an IPsec VPN tunnel to keep it running. This type of traffic (*discard* protocol, UDP port 9) is of no use when it is received and can be filtered without being logged.

R48 | SNS | Configure KeepAlive
The KeepAlive function should be enabled, and traffic sent from the remote appliance should be filtered.

This feature can be configured in **Configuration > VPN > IPsec VPN > Encryption policy - Tunnels** by changing the interval between two requests in the KeepAlive column. A value of *0* means that it is not in use.

7.8 Managing the DSCP field

The DSCP field, found in the IP header, is used to manage congestion. In IPsec encapsulation, the default behavior of an SNS firewall is to replicate this field's value in the original header in the header of the corresponding encrypted packet. Changing this field may disrupt the flow of traffic on an operator network.

R49 | SNS-SMC | Keep the DSCP field
Apart from the need for stronger security, it is advisable to keep the default configuration of the DSCP field.

However, when high security is required, making a copy of the DSCP field can create a hidden channel. The value of this field must therefore be controlled before it leaves the SNS firewall. One way to do so is to use the SNS firewall to change its value. This can be done in the **Quality of service** tab in the **Action** menu of a Pass filter rule. When the **Impose value** option is enabled, the **New DSCP value** menu will become available. The selected value is used as the DSCP field value of filtered packets. Apply this operation to filter rules for outgoing encrypted traffic.

R49+ | SNS-SMC | Control the DSCP field
When a higher level of security is required, the DSCP field of outgoing traffic should be changed to an arbitrary value.

WARNING
The DSCP field of an encrypted packet can only be changed if outgoing implicit rules for hosted services have been disabled, as explained in the chapter on Implicit rules, and an explicit filter rule with stateful inspection has been created.

INFORMATION
The network operator can prioritize packets in its network based on the value of the DSCP field. Using a value of *0* makes it possible to keep the primary path.

Where:

- Several connections pass through a tunnel,
- The remote endpoint copies the value of the DSCP field from plaintext packets to encrypted packets,
- QoS processing on the transit network rearranges the sequence of packets,
- The local endpoint has an anti-replay window that is too small,

Legitimate packets may get lost.

The number of lost packets can be minimized by changing the *ReplayWSize* parameter. This can be done using the NSRPC command `config ipsec profile phase2 update replaywsize=XX name=NN`, where **XX** is a value between 0 and 33554400 inclusive in increments of 8, and **NN** is the name of the encryption profile. The network and relevant traffic have to be analyzed in order to define the adapted *ReplayWSize* parameter. You can get in touch with the Stormshield support center to conduct this analysis. This value can also be manually added to the file */Firewall/ConfigFiles/VPN/01* where the value *01* corresponds to the number of the IPsec policy used.

8. Monitoring

This feature was not part of the security target during the SNS firewall qualification process.

8.1 Configuring basic components

In order to query SNS firewalls in SNMP, a filter rule must be configured. Only monitoring servers must be allowed to query SNS firewalls in SNMP, and only in read-only mode.

R50 | SNS-SMC | Filter SNMP queries
We recommend allowing only monitoring servers to query SNSfirewalls in SNMP, by using an adapted filter rule.

On SNS firewalls, the parameters *Location(syslocation)* and *Contact(syscontact)* found in **Configuration > Notifications > SNMP agent > General** refer respectively to the physical location of the SNS firewall, and the contact details to use when a failure occurs. By configuring these parameters, it becomes easier to map SNS firewalls in monitoring and alarm tools.

R51 | SNS | Use SNMPv3
SNMP version 3 is recommended as it provides authentication and encryption mechanisms. SNMPv3 can be enabled in **Configuration > Notifications > SNMP agent > General**.

By configuring the **Connection to the SNMP agent** field on SNS firewalls in the **SNMPv3** tab, the algorithms and passwords used for authentication and encryption can be set.

R52 | SNS | Configure the connection to the SNMP agent
AES is recommended as the encryption algorithm, and SHA1 for hashing. This gives data exchanges an acceptable level of security that does not, however, comply with the RGS. Passwords must comply with the guide Recommendations relating to multifactor authentication and passwords (in French).

On SNS firewalls, when peers are entered in the **List of SNMP servers** field of the SNMPv3 tab in **Notifications > SNMP agent > SNMPv3**, the SNS firewall will send SNMP traps to them.

WARNING
SNMP traps that the SNS firewall sends are part of an implicit filter rule. This rule is included in the hosted services rule found in the **Implicit rules** menu. We recommend disabling this rule in compliance with the chapter on Implicit rules, and replacing it with custom rules.

8.2 Querying SNS firewalls in SNMP

The following is an example of a query command that makes it possible to test the function of the SNMPv3 configuration on an SNS firewall that uses the configuration parameters mentioned earlier:

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

The SNS firewall must send back OIDs and their values.

WARNING
Passwords should preferably be put in the configuration file instead of the command line, then deleted.

The *snmpwalk* utility is available on many platforms, and makes it possible to query an SNS appliance's SNMP service. Details of the parameters used in this example:

-v 3	Corresponds to the version of the SNMP protocol used.
-u <user_smp>	Corresponds to the **User name** parameter entered on the SNS firewall.
-l authPriv	Indicates that the SNMP query is encrypted and authenticated
-a SHA	Specifies the type of hash function used for authentication. The password used must be placed in the configuration file. The variable to add is **def- AuthPassphrase**. The password must be at least 8 characters long and comply with the rules regarding robustness set out in the Recommendations relating to multifactor authentication and passwords (in French).
-x AES	Indicates the algorithm used for encryption. The password used must be placed in the configuration file. The variable to add is **defPrivPassphrase**.

8.3 Using specific OIDs

"Standard" indicators (e.g., interface, disk, memory) can be obtained by querying SNS firewalls on OIDs that belong to the standard MIB; SNS firewalls can also be queried on SNS-specific OIDs (e.g., policy, high availability, VPN). It is advisable to build monitoring templates that use indicators from both of these MIBs in order to get an accurate view of the status of the SNS firewalls.

The following is the SNMP query request that makes it possible to retrieve the name of the network filter policy enabled on an SNS firewall:

```
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
```

The SNS firewall will return a response in the following form:

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

The value .1.3.6.1.4.1.11256.1.8.1.1.3.1 represents the OID through which the name of the security policy can be accessed in the SNS MIB. The character string *"POL-PROD-SITE1-FW1"* corresponds to the name that the administrator of the queried SNS firewall gave to the policy.

The list of OIDs worth monitoring on an SNS firewall is provided in table below.

OID	Description
General information	
.1.3.6.1.4.1.11256.1.0.1.0	Hostname
.1.3.6.1.4.1.11256.1.0.2.0	Stormshield version
.1.3.6.1.4.1.11256.1.0.3.0	Serial number
.1.3.6.1.4.1.11256.1.10.2.0	Uptime
.1.3.6.1.4.1.11256.1.10.6.1.3	List of power supply modules and status
HA	
.1.3.6.1.4.1.11256.1.16.2.1.4.0	Health status of the HA link
.1.3.6.1.4.1.11256.1.16.2.1.3.0	HA mode
CPU	
.1.3.6.1.2.1.25.3.3.1.2	Percentage of CPU used over the last minute
.1.3.6.1.4.1.11256.1.7.1.1.2	List of active services
Load	
.1.3.6.1.4.1.2021.10.1.3.1	Load over the last minute
Memory	
.1.3.6.1.4.1.2021.4.5.0	Amount of memory on the SNS firewall
.1.3.6.1.4.1.2021.4.6.0	Amount of memory currently available
Hard disk space	
.1.3.6.1.2.1.25.2.3.1.5.**31**	Total number of / blocks
.1.3.6.1.2.1.25.2.3.1.6.**31**	Number of blocks used on /
.1.3.6.1.2.1.25.2.3.1.5.**35**	Total number of */log* blocks
.1.3.6.1.2.1.25.2.3.1.6.**35**	Number of blocks used on */log*
Network interfaces	
.1.3.6.1.4.1.11256.1.4.1.1.38	List of interfaces
.1.3.6.1.4.1.11256.1.4.1.1.4.**2**	IP address of interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.38.**2**	System name of interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.3.**2**	Custom name of interface **2**
.1.3.6.1.2.1.2.2.1.7.**2**	Administration status of interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.28.**2**	Max outgoing throughput on interface **2**
.1.3.6.1.4.1.11256.1.4.1.1.27.**2**	Max incoming throughput on interface **2**
.1.3.6.1.4.1.11256.1.8.1.1.3.1	Name of the activated filter policy

Tunnels	
.1.3.6.1.4.1.11256.1.8.1.1.3.2	Name of the active IPsec policy
.1.3.6.1.4.1.11256.1.13.1.1.0	Number of incoming SPDs
.1.3.6.1.4.1.11256.1.13.1.2.0	Number of outgoing SPDs
.1.3.6.1.4.1.11256.1.13.2.2.0	Number of mounted VPN tunnels ("Mature" state)
.1.3.6.1.4.1.11256.1.13.2.3.0	Number of VPN tunnels ("Dying" state)
.1.3.6.1.4.1.11256.1.13.2.4.0	Number of VPN tunnels ("Dead" state)

The full list of OIDs available on an SNS firewall can be obtained by using the following command:

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

9. Backups

Automatic backups were not part of the security target during the SNS firewall qualification process. As for manual SNS firewall backups, and the backup of the SNS firewall configuration via the SMC server, they were part of the security target.

9.1 Configuring automatic backups

When a configuration error occurs, there must be a way to quickly recover a sound configuration. Moreover, when there is a failure, it must be possible to reproduce the previous configuration on a new SNS firewall. To do so, automatic and regular archiving of the SNS firewall configuration on a remote server should be implemented.

The configuration of the SNS firewall can be exported in **Configuration > System > Maintenance > Backup** in three different modes:

- Instant export to the workstation that was used to access the web administration interface,
- Regular export to a WebDAV server hosted on the Internet in an infrastructure managed by Stormshield,
- Regular export to a custom WebDAV server.

When a custom WebDAV server is selected, a HTTP or HTTPS link can be used. For HTTPS, the certificate used by the server must be submitted to the SNS firewall.

R53 | SNS-SMC | Set up automatic backup on a controlled server
We recommend enabling the password-protected, encrypted automatic configuration backup function. The configuration has to be exported to a customized and controlled WebDAV server via an authenticated HTTPS connection, or to an SMC server.

Local automatic backups can also be enabled in command line. However, in native mode, such backup files cannot be exported automatically to a remote server, e.g. via SSH. Files generated locally must be transferred using a custom script, but must not be retrieved via SSH in a connection initiated by a remote server as this would require the use of an SNS firewall administrator account, which is not recommended. The creation of a script is recommended on the SNS firewall that connects to a remote server in SSH and transfers the backup files.

R53 - | SNS | Set up automatic backup via SSH
If no controlled WebDAV servers or SMC servers are available, the configuration of an encrypt, password-protected automatic backup is recommended. This backup will be exported via SSH through a connection that the SNS firewall initiated.

With the `config autobackup` command, the SNS firewall's local automatic backup can be configured and enabled. The following is a sample configuration of a local encrypted automatic backup that is launched every day:

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

Once it has been configured, it must be enabled:

```
config autobackup activate
```

Implementing automatic backups through such commands will generate the **backup.na** file in the folder */data/Autobackup/*. Every new backup overwrites this file, so it must be transferred over a secure channel to a remote appliance beforehand.

WARNING
The extension of the backup file will always be **.na** regardless of whether it is encrypted with a password. It is the same as the backup file that is generated from the web administration interface (**Configuration > System > Maintenance > Backup** menu).

9.2 Opening backup files

Stormshield backup files (**.na** extension) cannot be unzipped directly from a standard archive manager. Such files must be opened in advance with a `decbackup` utility in command line, which can be found on SNS firewalls (available in *PATH* or in the folder */usr/Firewall/sbin*), and on the SMC server in the folder */opt/stormshield/security*. Binary files can be downloaded from the MyStormshield personal area, including *decbackup*, with which backup files can be opened, even when the user does not have an SNS firewall.

The syntax is as follows:

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

The output file is an archive that includes all of the SNS firewall's configuration files (those found in */usr/Firewall/ConfigFiles*), as well as the directory if it is internal.

10. Logging

10.1 Log policy

Before logs are configured on an SNS firewall, a log policy must first be defined. In particular, this policy must specify the types of events worth logging, and where they will be saved.

On SNS firewalls, the following can be defined separately:

- The types of events saved on the local storage medium when there is one (**Configuration > Notifications > Logs - Syslog - IPFIX > Local storage**). In this case, such events can be viewed directly from the SNS firewall's web administration interface in the **Monitoring** tab in the **Logs and activity reports** page,
- The types of events that are sent to one or several syslog servers (**Configuration > Notifications > Logs - Syslog - IPFIX > Syslog)**. These events cannot be viewed directly from the SNS firewall's web administration interface, as they will be injected into an SIEM system or archived.

R54 | SNS | Define a log policy
The definition of a local log policy and centralized log policy is recommended in line with the guide Security recommendations the implementation of log systems (in French).

As storage space on the SNS firewall's disk or SD card is limited, logs are rotated.

The TLS protocol must be set up to guarantee the confidentiality and integrity of log transfer traffic in particular when data passes through uncontrolled networks.

R55 | SNS | Secure log transfers with the TLS protocol
We recommend the use of log transfer protocols based on robust cryptographic mechanisms (in line with the guide Security recommendations relating to TLS - in French), particularly when data passes through uncontrolled networks (in line with the guide Security recommendations for the implementation of log systems- in French).

The log transfer protocol can be selected in **Configuration > Notifications > Logs - Syslog - IPFIX > Syslog.**

10.2 Determining the events to log

Gathering unnecessary logs creates more information to process when logs are analyzed, thereby complicating the analysis. On the other hand, not collecting any logs means missing out on a crucial source of information that would help to detect incidents and search for compromised areas.

R56 | SNS | Set events to be logged
Below is a non-exhaustive list of recommended events to collect via syslog among all events that the SNS firewall offers in its web administration interface. The assumed use case is an appliance used as a firewall/IPsec VPN with IDS and IPS disabled:

- Events relating to the filter policy, such as rejected packets, etc.,
- Network connections,

- Events relating to IPsec VPN tunnels, such as the setup and destruction of tunnels, etc.,
- Authentication events, e.g., aborted, successful or failed attempts,
- Administration events that the serverd daemon generated, e.g., administrator connections, changes to the configuration,
- Statistics;
- System events,
- Alarms.

INFORMATION
The advanced (connection log and filtering log) log level is not suitable for TCP, UDP and SCTP traffic, as the connections (set up for TCP) on these protocols will already have been logged by default in connection logs.

11. Managing the firewall pool

This feature was not part of the security target during the SNS firewall qualification process.

To manage several SNS firewalls, we recommend setting up an administration IS, as this complies with the recommendations in the guide relating to the secure administration of information systems (in line with the Recommendations on the secure administration of information systems - in French). This administration IS should be used in particular to:

- Provide centralized authentication of administrators as described in the chapter Centralized authentication, and the external PKI in compliance with the chapter Using a PKI,
- Access the SNS firewall's administration services remotely (HTTPS and NSRPC - the relevant tools use TCP port 1300) from administration workstations, in line with the chapter Administration services.
- Forward logs generated by the SNS firewall to the central log server, in line with the chapter Logging and the Security recommendations for the implementation of log systems (in French),
- Allow the passage of monitoring traffic described in the chapter Monitoring, which is exchanged between the SNS firewall and the central monitoring server,
- Forward the SNS firewall's backup files to the central backup server, in line with the chapter Backup.

The SMC server provided by Stormshield, among others, makes it possible to implement these features. Furthermore, a large pool of SNS firewalls can be easily managed, through the use of specific features such as:

- Folder-based SNS firewall management,
- Use of of filter and translation rule sets,
- Offline SNS firewall configuration,
- Postponement of configuration deployments,
- Scheduling the execution of SNS CLI scripts on a pool,
- etc.

12. List of recommendations

R1	SNS-SMC	Use accounts assigned to users by name
R2	SNS-SMC	Protect the local administrator account
R3	SNS	Restrict administration via SSH
R4	SNS	Use SSH key authentication
R5	SNS	Authenticate locally using certificates
R6	SNS	Define an appropriate password policy
R7	SNS	Dedicate an external directory to administrators
R8	SNS	Use a restricted-access and secure account
R9	SNS	Adjust administration privileges strictly to what is required
R10	SNS-SMC	Use groups to manage privileges
R11	SNS	Define administration sub-networks clearly
R12	SNS	Use an administrator object group
R13	SNS	Dedicate an Ethernet interface to administration
R14	SNS	Keep default cryptographic suites
R14+	SNS	Harden TLS parameters on the web administration interface
R15	SNS	Replace the certificate on the web administration interface
R16	SNS	Use NSRPC from the web interface
R16-	SNS	Use accounts dedicated to direct NSRPC connections
R17	SNS	Use the same language in logs
R18	SNS-SMC	Use a language that users understand
R19	SNS	Enable the "*Diffusion Restreinte*" option
R19	SMC	Enable the "*Diffusion Restreinte*" option
R20	SNS	Disable unused interfaces
R21	SNS-SMC	Declare internal interfaces
R22	SNS	Define static routes for internal networks
R23	SNS	Provide details with IP address spoofing rules
R24	SNS	Update from an internal mirror
R24-	SNS	Update through a proxy
R25	SNS	Choose controlled DNS servers
R25-	SNS	Change default DNS servers
R26	SNS	Restrict the use of dynamic objects

R26	SMC	Restrict the use of dynamic objects
R27	SNS-SMC	Synchronize system time
R28	SNS-SMC	Configure the LDAP securely
R29	SNS-SMC	Rename the production policy
R30	SNS	Disable implicit rules
R31	SNS-SMC	Adapt the traffic inspection type to the role of the SNS firewall
R32	SNS-SMC	Adapt inspection profiles to the SNS firewall's use context
R33	SNS-SMC	Use object groups
R34	SNS-SMC	Use a controlled external PKI
R34-	SNS	Use the SNS firewall's PKI
R34-	SMC	Use the SNS firewall's PKI
R35	SNS-SMC	Impose CRL verification
R36	SNS	Adapt automatic CRL refreshment
R37	SNS-SMC	Configure the CRL retrieval URL and enable automatic retrieval
R37-	SNS-SMC	Manually import CRLs
R38	SNS-SMC	Use strong algorithms for IKE and IPsec
R39	SNS-SMC	Use version 2 of the IKE protocol
R40	SNS-SMC	Use mutual certificate-based authentication
R40-	SNS-SMC	Use a robust pre-shared key
R41	SNS-SMC	Configure IPsec VPN tunnels securely
R41+	SNS-SMC	Do not use the default route
R42	SNS-SMC	Confirm the source of incoming traffic
R43	SNS-SMC	Declare the IPsec VPN interface as an internal interface
R44	SNS	Configure mobile tunnels in config mode
R45	SNS	Authenticate mobile devices and/or users with certificates
R46	SNS	Use a dedicated intermediate certification authority
R47	SNS-SMC	Enable Dead Peer Detection
R47-	SNS-SMC	Use passive DPD mode
R48	SNS	Configure Keepalive
R49	SNS-SMC	Keep the DSCP field
R49+	SNS-SMC	Control the DSCP field
R50	SNS-SMC	Filter SNMP queries

R51	SNS	Use SNMPv3
R52	SNS	Configure access to the SNMP agent
R53	SNS-SMC	Set up automatic backup on a controlled server
R53-	SNS	Set up automatic backup via SSH
R54	SNS	Define a log policy
R55	SNS	Secure log transfers with the TLS protocol
R56	SNS	Set events to be logged

documentation@stormshield.eu