STORMSHIELD

GUIDE

STORMSHIELD NETWORK SECURITY

RECOMMENDATIONS FOR THE SECURE CONFIGURATION OF AN SNS FIREWALL

Version 3.7.17 LTSB

Document last updated: April 2, 2021

Reference: sns-en-anssi_recommendations_guide-v3.7.17-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 3.7.17 LTSB.

This document was written by the ANSSI and can be downloaded from www.ssi.gouv.fr. With the ANSSI's consent, this document is also available on Stormshield's Technical Documentation website.

This is an original work by the ANSSI published under the Etalab mission Open Licence v2.0 scheme.
In line with the Open Licence v2.0, this guide may be reused freely with due attribution (source and date of last update). Reuse includes the right to communicate, circulate, redistribute, publish, forward, reproduce, copy, adapt, modify, extract, convert and use, including for commercial purposes.

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 Objective

The aim of this document is to present best practices for the secure deployment of Stormshield Network Security (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 explained in this document 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 with regard to firewalls and best practices for interconnections.

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"*.
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.

1.2 Acronyms

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

CA	Certification authority.
ASQ	Active Security Qualification, engine that analyzes Stormshield appliances.
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.
PKI	Public key infrastructure.
IKE	Internet Key Exchange, protocol in which authentication keys are exchanged between peers.
IP	Internet Protocol, computer network communication protocol.
IPsec	Internet Protocol Security, framework of standards that make it possible to secure IP communications.
IPS	Intrusion Prevention System, mechanism that makes it possible to detect malicious traffic and block it.
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 appliance to be managed in command line.
OID	Object IDentifier, resource identifier represented by a series of whole numbers.
QoS	Quality of Service.
IS	Information system.
SIEM	Security Information and Event Management.
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.
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.
TCP	Transport Control Protocol.
TLS	Transport Layer Security, upgrade of SSL.
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. Firewall administration

2.1 Administrator accounts

2.1.1 Using accounts assigned to users by name

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

R1 | 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 or the administration server (NSRPC).

However, there are exceptional operations that cannot be performed from personalized accounts, such as:

- Manually modifying configuration files,
- Using tcpdump for the purpose of network analysis,
- Changing privileges granted to administrators.

The appliance includes a non-nominative local administrator account (admin) that can perform these actions from the web interface, local console or via SSH.

R2 | Protect the local administrator account
The administrator account found on the appliance 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 | Restrict administration via SSH
As the SSH service is restricted to only the administrator account, it must be enabled for exceptional reasons from **System** > **Configuration** > **Firewall administration**.

R4 | Use password authentication for SSH
When SSH is enabled for exceptional reasons, users are advised to authenticate with a password and to change the password after every use.

2.1.2 Local authentication

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

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

Certification authorities must be added beforehand in **Objects** > **Certificates and PKI** and the *SSL certificate* authentication method configured in **Users** > **Authentication > Available methods** with the desired authorities.

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

2.1.3 Centralized authentication

This feature was not part of the security target.

A centralized authentication solution can be used on SNS. To implement it, users must be managed from a remote appliance. Using such a solution aims to restrict the amount of sensitive data stored locally and simplify administration processes. For external directories, the firewall configuration is described in chapter Using an external directory.

R7 | 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 | Use a restricted-access and secure account
The account that the firewall uses to access the centralized authentication solution must be restricted to this function, dedicated to the 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 appliance.

2.1.4 Access privileges

A firewall provides 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 appliance, each function should be managed by a dedicated appliance and its associated administration account.

If an appliance 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 | Adjust administration privileges
Only the privileges that the various administrators strictly require for their tasks should be granted in **System** > **Administrator**.

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 firewall can be assigned to them. Each group must correspond to a functional requirement and hold the appropriate privileges on the 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 | Use groups to manage privileges
To manage privileges for access to SNS appliances, the use of groups is recommended.

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 chapter **Using accounts assigned to users by name**.

INFORMATION
Although several centralized authentication methods are available, the management of permissions by user group has only been tested on external directories.

2.2 Administration services

2.2.1 Configuring administration IP addresses

Unrestricted access to the 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 | Define administration sub-networks clearly
The IP addresses or administration sub-networks allowed to access an appliance's administration interfaces should be explicitly defined in **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 | Use an administrator object group
The use of object groups is recommended, containing all sub-networks and IP addresses allowed to manage the firewall.

2.2.2 Dedicated administration interface

Sharing an administration interface with the production network increases the number of individuals and appliances with access to the firewall's administration interface, and also increases the volume of traffic that the interface must handle. As a result, this raises the risk of the administration interface being attacked or unreachable. Moreover, using VLANs does not guarantee airtight access between the configured networks.

R13 | Dedicate an Ethernet interface to administration
SNS appliances 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 the web administration interface contributes to the security of the appliance by protecting the confidentiality and integrity of legitimate administration traffic.

By default, *sslparanoiac* mode is enabled, imposing the use of TLS 1.2 and 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-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
```

R14 | 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.

INFORMATION
A recent Internet browser is required for the use of TLS 1.2 and robust cryptographic suites.

R14 + | Harden TLS parameters on the 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 command:

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

2.2.4 Changing the certificate of the web administration interface

By default, the certificate presented to administrators when they connect to the web administration interface is a certificate signed by the Netasq CA. As such, there is no control over the criteria for generating the private key used, or how it can be used.

R15 | Replace the web interface certificate
The certificate of the web administration interface should be replaced with a certificate issued by a controlled PKI 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 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 appliances 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 firewall requires read-only access to the user's password hash (this information is required for the authentication protocol to function properly). If the 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 interface. Access to this console does not require additional authentication. Hashes do not need to be accessed.

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

R16 - | Use accounts dedicated to direct NSRPC connections
During direct access to the NSRPC console, dedicated accounts are recommended for this purpose, and only the hashes of these accounts on the remote directory should be exposed.

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 appliance:

- Web interface language, which can be selected in the connection window,
- Keyboard layout of the console, which can be configured in **System** > **Configuration**,
- Language in which logs are generated, which can be configured in **System > Configuration**.

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

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

All existing messages are listed in **Notifications > System events** and their translations are available on the appliance 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 | Use the same language in logs
The same language should be configured for all logs on all SNS appliances. This will make it easier to read them and integrate them into monitoring tools.

R18 | Use a language that users understand
Appliances must be configured in a language that users understand.

INFORMATION
Most of the pages in Stormshield's knowledge base are written in English. This base can be accessed from Stormshield's personal area.

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. 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 firewalls equipped with such (co)-processors.

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

INFORMATION
Some SNS firewall models use a processor with a set of cryptographic instructions that provides

> sufficient guarantees regarding the protection of DR data. Contact Stormshield for the full list of such models.

3. Network configuration

3.1 Disabling unused interfaces

Having unused network interfaces on an SNS appliance increases its attack surface because connecting to such interfaces does not disrupt the proper operation of the firewall but allows illegal access to it. Moreover, active interfaces can be used from the various menus and increase the risk of configuration errors.

> **R20 | Disable unused interfaces**
> Unused network interfaces should be disabled from **Network** > **Interfaces**.

3.2 Configuring IP anti-spoofing

3.2.1 Concept of IP anti-spoofing

IP 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 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, IP anti-spoofing is extremely effective in detecting network configuration errors, e.g., wrongly configured routing rules.

3.2.2 Anti-spoofing on network interfaces

SNS firewalls use the concept of "internal" interfaces to identify the interfaces that the anti-spoofing mechanism recognizes. In **Network** > **Interface** > **Interface configuration,** 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 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 list of IP addresses allowed to access an internal interface can be added to by using anti-spoofing via the routing table as described in chapter Anti-spoofing via the routing table.

R21 | Declare internal interfaces
To benefit from anti-spoofing mechanisms, one or several internal interfaces should be declared.

WARNING
Implicit filter rules allow appliances to be managed from internal interfaces. These rules must be disabled as explained in chapter Implicit rules.

3.2.3 Anti-spoofing via the routing table

Static routes inform the 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. So 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 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 | Define static routes for internal networks
Static routes must be defined for all known internal networks to which the firewall's interfaces do not belong in order to benefit from anti-spoofing mechanisms. These routes are identified in **Network** > **Routing** > **Static routing** with a shield.

WARNING
Routes for all remote networks reachable via internal interfaces must be declared. Otherwise, the firewall will always reject their packets.

3.2.4 Anti-spoofing on a bridge

A bridge makes it possible to connect several physical interfaces on the same network. However, the 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 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 appliances start sending packets. Anti-spoofing on the bridge therefore does not protect contacts that are directly connected but have not 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 appliance'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 appliance in a specific group. These ranges belong to private networks and should not be used on a public interface.

> **R23 | Fill in anti-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. Service configuration

4.1 Updates

Some features on SNS appliances require regular updates (enabled by default in **System > Active Update**). The complete absence of updates would prevent the 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 SNS appliances in the IS. This may cause excessive bandwidth consumption. Using an internal mirror will therefore make it possible to restrict the number of appliances allowed to access the Internet.

R24 | 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 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 appliance must access (URL filtering and IP traffic strictly required for update operations on SNS appliances, i.e. the URLs *update {1,2,3,4}.stormshield.eu* and *licence{1,2,3,4}.stormshield.eu*).

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

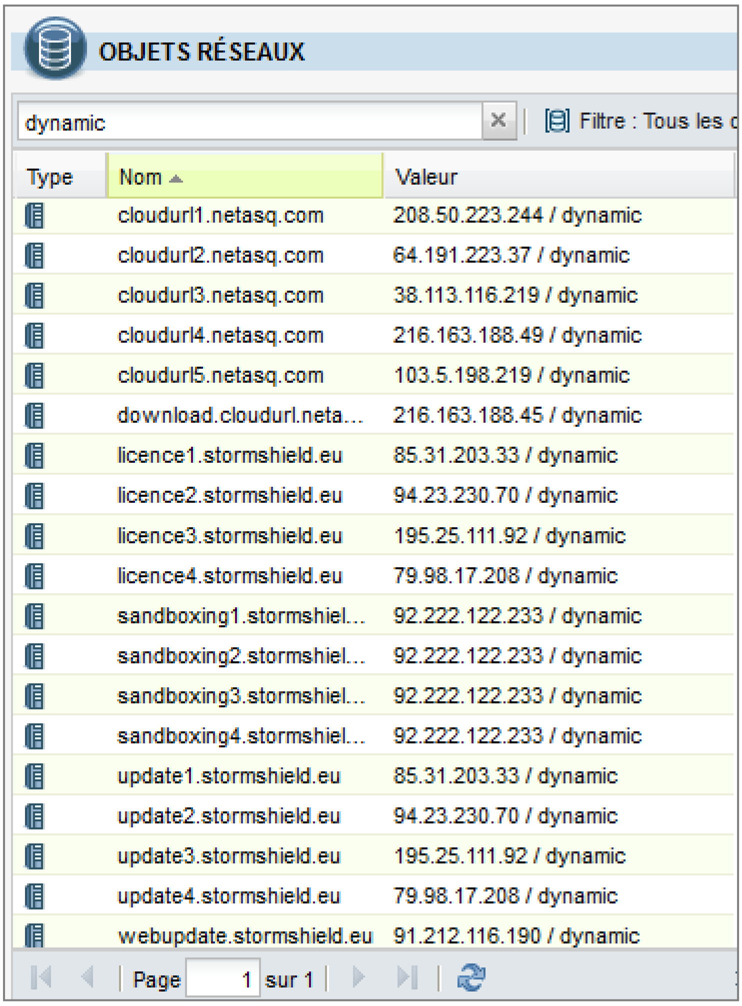
4.2 DNS

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

R25 - | 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 appliance's object database makes it possible to create static or dynamic objects. These objects depend on a domain name that the firewall regularly resolves. There are about fifteen such domain names by default, ending in netasq.com or stormshield.eu, part of which is represented in the image below (these names may vary depending on updates). This generates unnecessary and inconvenient DNS requests that cannot be blocked by filter rules.



dynamic

Type	Nom ▲	Valeur
▤	cloudurl1.netasq.com	208.50.223.244 / dynamic
▤	cloudurl2.netasq.com	64.191.223.37 / dynamic
▤	cloudurl3.netasq.com	38.113.116.219 / dynamic
▤	cloudurl4.netasq.com	216.163.188.49 / dynamic
▤	cloudurl5.netasq.com	103.5.198.219 / dynamic
▤	download.cloudurl.neta...	216.163.188.45 / dynamic
▤	licence1.stormshield.eu	85.31.203.33 / dynamic
▤	licence2.stormshield.eu	94.23.230.70 / dynamic
▤	licence3.stormshield.eu	195.25.111.92 / dynamic
▤	licence4.stormshield.eu	79.98.17.208 / dynamic
▤	sandboxing1.stormshiel...	92.222.122.233 / dynamic
▤	sandboxing2.stormshiel...	92.222.122.233 / dynamic
▤	sandboxing3.stormshiel...	92.222.122.233 / dynamic
▤	sandboxing4.stormshiel...	92.222.122.233 / dynamic
▤	update1.stormshield.eu	85.31.203.33 / dynamic
▤	update2.stormshield.eu	94.23.230.70 / dynamic
▤	update3.stormshield.eu	195.25.111.92 / dynamic
▤	update4.stormshield.eu	79.98.17.208 / dynamic
▤	webupdate.stormshield.eu	91.212.116.190 / dynamic

Page 1 sur 1

Using an internal mirror (recommendation R24) means that an SNS appliance 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 | Restrict the use of dynamic objects
Unused dynamic objects should be deleted and objects that remain in static mode should be reconfigured instead in **Objects** > **Network objects**.

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 | Synchronize system time
NTP synchronization should be enabled on SNS appliances 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.

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

R28 | Configure the LDAP securely

If the LDAP service is configured:

- The LDAPS protocol should be used,
- A certificate originating from a controlled PKI on the LDAP server should be installed,
- The corresponding CA should be imported on the SNS appliance,
- 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 firewall's access account on the directory. This account must comply with **recommendation R8** .
- Specify the structure of the directory (**Structure** tab). The attributes that SNS appliances manage 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 filter policy

The filter policies on SNS appliances do not have any explicit names by default, except two – Pass all and Block all. This does not allow an administrator to easily understand the role of the firewall, or know which policy to apply if there are several. Implementing a naming system makes it possible to:

- Reflect the function of the 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 firewalls in the IS.

R29 | 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 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. The **Security policy > Filter - NAT** menu therefore does not contain all the rules that the firewall applies. As such, a rule created by an administrator may never be evaluated because an opposing rule exists.

R30 | Disable implicit rules
All implicit filter rules should be disabled, including those that apply to outgoing traffic generated from services hosted by the firewall. This operation can be performed in **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 firewall and groups defined in chapter Configuring administration IP addresses on the interfaces defined in chapter Dedicated administration interface.

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 appliance . 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 appliances 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 available levels: Firewall, IPS or IDS.

In firewall inspection, the 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
In firewall inspection, when the firewall 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.

In IPS inspection, the 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 IPS, but will only raise alarms if traffic seems malicious without blocking it. The IDS 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 modules are automatically loaded by default, depending on the ports used in filter rules and the characteristics of the analyzed traffic. 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 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, (modules relating to the following protocols: FTP, HTTP (including WebDAV), SIP, SMTP, DNS, Modbus, S7 and UMAS), the term “qualified application mode” will be used.

IPS inspection in automatic mode is selected by default when a filter rule is created. However, loading protocol analysis modules will increase the firewall’s processor load and its attack surface. Where possible, protocol analysis functions should be conducted by dedicated appliances such as proxy servers to minimize the risk of compromising the firewall.

R31 | Adapt inspection type to the role of the appliance
Firewall inspection, IPS in transport mode or IPS in qualified application mode is recommended, in line with the role of the appliance 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.

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

- If the appliance 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 the firewall is located between a corporate IS and the Internet, IPS in transport mode makes it possible to restrict the appliance's attack surface while guaranteeing thorough filtering of connections,
- If the firewall protects application servers that can only be reached from an organization's internal network, IPS in qualified application mode can be used.

The Security inspection column in the filter rules (Filter - NAT menu) makes it possible to choose Firewall, IPS or IDS inspection. For IPS and IDS, 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 appliance will analyze. Only one protocol (application or transport) can be chosen for each filter rule.

IPS and IDS rely on the use of inspection profiles, which make it possible to configure the behavior of the 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 | Adapt inspection profiles to the 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 incoming traffic and profile *01* for outgoing traffic. Profiles are chosen for each filter rule in the **Security inspection** tab. These profiles can be configured in **Application protection > Inspection profiles**, by selecting **Go to profiles**. Each profile is then based on the policies defined in **Application protection > Protocols**. These policies define the general analyses of various protocols, such as default ports, restricted commands, types of analyses, etc. Moreover, **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 Stormshield appliances, 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 chapter Configuring administration IP addresses) and in a correlated explicit filter rule (in line with chapter 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 | 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

In some cases, SNS appliances need to use certificates for several purposes, including:

- The publication of the web administration interface in HTTPS,
- The authentication of administrators via certificate to access the SNS 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.

6.1 Using a PKI

When an appliance 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 certificates signed by this authority. In this case, private keys are generated by and stored on the firewall. If the firewall is compromised, the secrets generated by it will be as well.

R34 | Use a controlled external PKI
A controlled PKI running outside the SNS appliance should be used to generate the certificates that the firewall uses. This PKI and CAs used must comply with the recommendations in Appendix A1 of the RGS (in French).

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

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

WARNING
When the appliance's internal PKI is configured, compromising the SNS appliance would allow an attacker to forge an identity that will be considered legitimate on the IS. It is therefore important that this function be restricted to appliances that are the least exposed to uncontrolled networks.

6.2 Managing CRLs in an IPsec 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 firewall. When the PKI implements CRLs, affected appliances can be informed when certificates are revoked. The absence of a CRL does not hinder the setup of an IPsec VPN, but will simply be reported in the appliance's logs.

R35 | Impose CRL verification
CRL verification should be imposed when implementing IPsec 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 command:

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

In both cases, the value of *01* used as an example represents the number of the IPsec configuration used.

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

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 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 | 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 `checkcrl` console command. The frequency with which CRLs are retrieved via the administration interface can also be modified.

Furthermore, since SNS firewalls do not use the *CRLDP* field found in the certificate of a CA, its distribution points cannot be configured automatically when importing a CA.

R37 | Configure the CRL retrieval URL and enable automatic retrieval
The URL for the automatic retrieval of each CA's CRL should be configured, and this feature enabled in **System** > **Configuration**.

The CRL distribution points associated with a CA can be set either via the SNS web administration interface, by editing the **CRL** of the CA in question, or in command line using the command:

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

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

INFORMATION
To allow the appliance to resolve the FQDN of the CRL distribution point’s URL, a host object corresponding to the FQDN must be defined in the appliance’s 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 - | Manually import CRLs
If CRLs cannot be imported automatically, they can be imported manually.

They can be imported manually via the web administration interface in **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**.

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 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 (**VPN > IPsec > VPN encryption profiles**), acceptable 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.

The tables below provide examples of encryption profiles that are 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.

Example of an RGS-compatible IKE encryption profile

Parameter	Value
Encryption algorithm	AES-GCM 256
Hash function	SHA 384
Diffie-Hellman group	Group 19 (256 bits)
Cryptoperiod	21600s

Example of an RGS-compatible IPsec encryption profile

Parameter	Value
Encryption algorithm	AES-GCM 256
Hash function	SHA 384
Diffie-Hellman group	Group 19 (256 bits)
Cryptoperiod	3600s

R38 | Use strong algorithms for IKE and IPsec

The algorithms used in IKE and IPsec encryption profiles should be at least AES-GCM 256, SHA 384 and Diffie-Hellman group 19.

7.2 Key exchange and authentication

7.2.1 IKE protocol

The level of protection that an IPsec tunnel provides 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 | Use version 2 of the IKE protocol**
> If all the IPsec tunnel peers are compatible, IKE in version 2 is recommended.

7.2.2 IKEv1 negotiation

This feature was not part of the security target.

When version 1 of the IKE protocol is used, the SNS appliance offers two negotiation modes:

- Main mode, available for authentication via certificate or pre-shared key,
- Aggressive mode, available for authentication via pre-shared key when the identities of both endpoints (*local ID* and *remote ID*) are entered.

While aggressive mode is faster, endpoint identities are communicated in plaintext, so the anonymity of peers is not guaranteed.

> **R39 - | Use main mode when IKEv1 is used**
> As the use of aggressive mode is vulnerable, main mode is recommended when IKEv1 is used.

This option does not exist when IKEv2 is used.

7.2.3 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 keys 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 appliances. Only when a PKI is used can each peer be identified, and privileges and revocations can be more easily managed.

> **R40 | Use mutual certificate-based authentication**
> The mutual authentication of IPsec VPN tunnel peers via certificate is recommended, by entering the accepted certification authorities in **VPN > IPsec VPN > Identification**.

> **R40 - | 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 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 appliance 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 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.

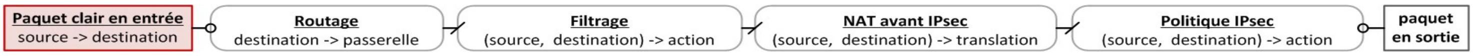
To prevent data leaks, it is advisable to configure a route with a fictitious IP as the gateway on its local loopback, e.g. a host object with 127.42.42.42 as its address. This technique is also called blackhole filtering.

After the IPsec VPN policy is applied, the routing policy will be evaluated again based on the encrypted packet. However, if there is an error on 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 appliance. Indeed, when it is encrypted, the packet will then be processed by the routing, filtering and NAT after IPsec functions.

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

Functional components


Paquet clair en entrée
source -> destination
Routage
destination -> passerelle
Filtrage
(source, destination) -> action
NAT avant IPsec
(source, destination) -> translation
Politique IPsec
(source, destination) -> action
paquet en sortie

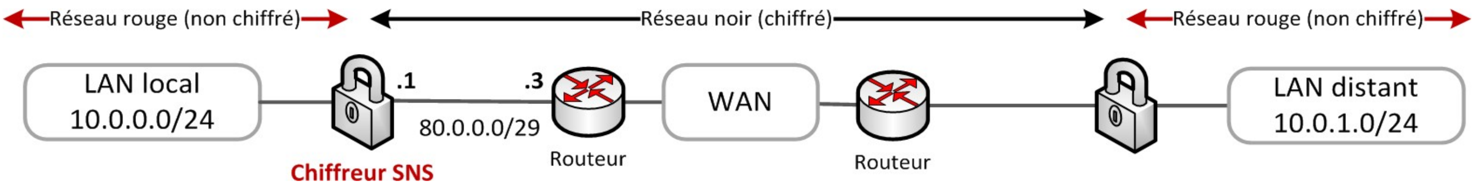
R41 | Configure IPsec tunnels securely
During the configuration of an IPsec VPN, the following is recommended:

- Configure a static route to the local loopback (*black hole*) to reach remote networks accessible via IPsec 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 NAT before IPsec rules are always included in the IPsec policy,
- Ensure that in the absence of NAT rules, filter rules are always more specific than the IPsec policy.

WARNING
Ideally, separate appliances should be implemented to dissociate encryption functions from the filtering of traffic in plaintext and encrypted traffic.

The examples below illustrate the advantage of the previous recommendation. They apply to the SNS firewall as a VPN gateway for outgoing traffic on the local LAN and to a remote LAN through an IPsec 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:

- 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.

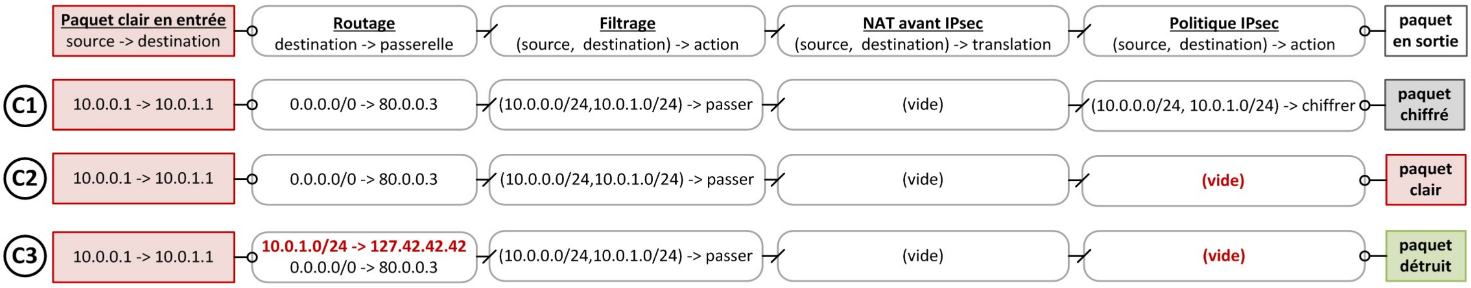
For each example, three cases (**C**) are represented:

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 local loopback. 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 local loopback



	Paquet clair en entrée source -> destination	**Routage** destination -> passerelle	**Filtrage** (source, destination) -> action	**NAT avant IPsec** (source, destination) -> translation	**Politique IPsec** (source, destination) -> action	**paquet en sortie**
C1	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(vide)	(10.0.0.0/24, 10.0.1.0/24) -> chiffrer	**paquet chiffré**
C2	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(vide)	**(vide)**	**paquet clair**
C3	10.0.0.1 -> 10.0.1.1	**10.0.1.0/24 -> 127.42.42.42** 0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(vide)	**(vide)**	**paquet détruit**

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 policy was 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 shown in **C3** consists of defining a route to the local loopback (taking a particular IP address makes it easier to keep the configuration, e.g., 127.42.42.42), also known as black hole filtering. In the absence of an IPsec policy, the firewall will destroy the packet instead of sending it to the default gateway.

R41 + | 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.

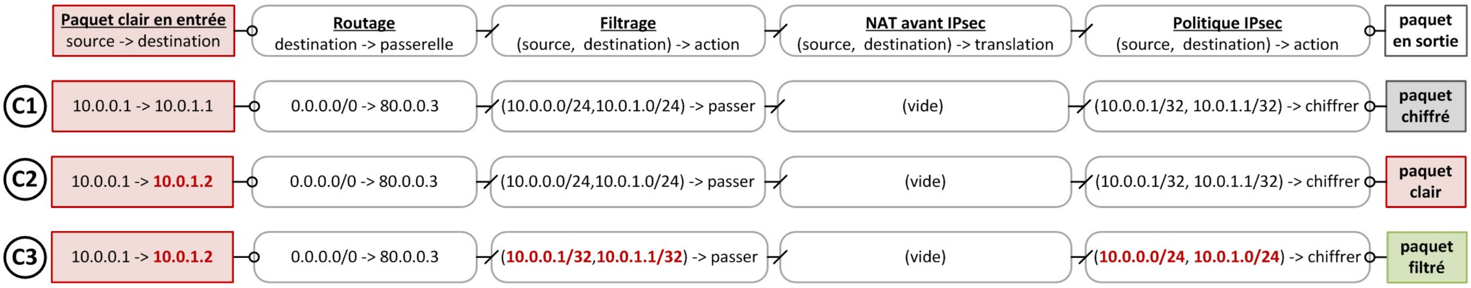
WARNING
Address ranges must be chosen to prevent confusion between red and black networks as described in architecture image, and to facilitate the creation of routes.

WARNING
A warning "the gateway is not routable" is generated when a route to the local loopback is defined in 127.0.0.0/8.

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



	Paquet clair en entrée source -> destination	Routage destination -> passerelle	Filtrage (source, destination) -> action	NAT avant IPsec (source, destination) -> translation	Politique IPsec (source, destination) -> action	paquet en sortie
C1	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(vide)	(10.0.0.1/32, 10.0.1.1/32) -> chiffrer	paquet chiffré
C2	10.0.0.1 -> **10.0.1.2**	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(vide)	(10.0.0.1/32, 10.0.1.1/32) -> chiffrer	paquet clair
C3	10.0.0.1 -> **10.0.1.2**	0.0.0.0/0 -> 80.0.0.3	(**10.0.0.1/32**,**10.0.1.1/32**) -> passer	(vide)	(**10.0.0.0/24**, **10.0.1.0/24**) -> chiffrer	paquet filtré

In the case of **C2**, an appliance is added to the network, but the 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.

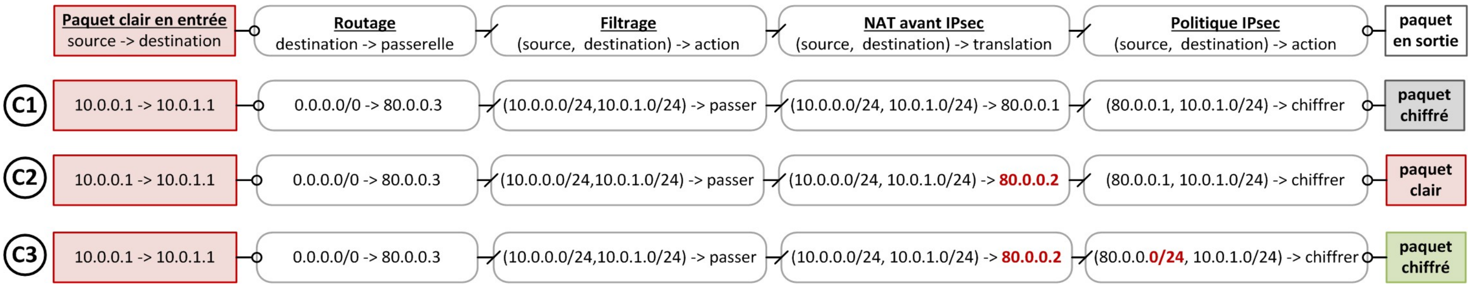
The correction implemented in **C3** consists of setting a filter policy in /32 and an IPsec policy in /24. The filter policy is therefore always more restrictive than the IPsec policy. Packets will either be filtered or Encrypt, but cannot be sent in plaintext.

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



	Paquet clair en entrée source -> destination	Routage destination -> passerelle	Filtrage (source, destination) -> action	NAT avant IPsec (source, destination) -> translation	Politique IPsec (source, destination) -> action	paquet en sortie
C1	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(10.0.0.0/24, 10.0.1.0/24) -> 80.0.0.1	(80.0.0.1, 10.0.1.0/24) -> chiffrer	paquet chiffré
C2	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(10.0.0.0/24, 10.0.1.0/24) -> **80.0.0.2**	(80.0.0.1, 10.0.1.0/24) -> chiffrer	paquet clair
C3	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(10.0.0.0/24, 10.0.1.0/24) -> **80.0.0.2**	(80.0.0.**0/24**, 10.0.1.0/24) -> chiffrer	paquet chiffré

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.

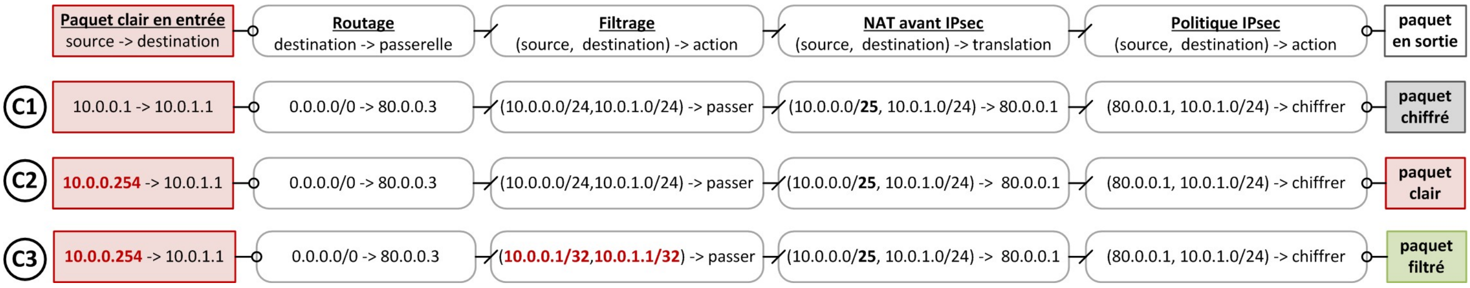
The solution shown in **C3** consists of defining an IPsec policy broader than the NAT rule used. Even if the outgoing IP address is modified, the IPsec policy will still select the packet, which will be encrypted by the appliance.

> **INFORMATION**
> The NAT rule must go together with an ARP publication if the address(es) used do(es) not belong to the 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



	Paquet clair en entrée source -> destination	Routage destination -> passerelle	Filtrage (source, destination) -> action	NAT avant IPsec (source, destination) -> translation	Politique IPsec (source, destination) -> action	paquet en sortie
C1	10.0.0.1 -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(10.0.0.0/**25**, 10.0.1.0/24) -> 80.0.0.1	(80.0.0.1, 10.0.1.0/24) -> chiffrer	paquet chiffré
C2	**10.0.0.254** -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(10.0.0.0/24,10.0.1.0/24) -> passer	(10.0.0.0/**25**, 10.0.1.0/24) -> 80.0.0.1	(80.0.0.1, 10.0.1.0/24) -> chiffrer	paquet clair
C3	**10.0.0.254** -> 10.0.1.1	0.0.0.0/0 -> 80.0.0.3	(**10.0.0.1/32**,**10.0.1.1/32**) -> passer	(10.0.0.0/**25**, 10.0.1.0/24) -> 80.0.0.1	(80.0.0.1, 10.0.1.0/24) -> chiffrer	paquet filtré

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 an IPsec VPN

A network attacker can send traffic to the 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. This rule can be configured in **Security policy** > **Filter - NAT** > **Filtering**: when editing a filter rule, the **IPsec VPN tunnel** value must be entered in the **Source** > **Advanced properties** > **Via** field.

R42 | 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 tunnel ensure that traffic passes through the tunnel that they deem legitimate.

7.4.1 Anti-spoofing on an IPsec tunnel

An SNS firewall treats IPsec VPN tunnel endpoints as interfaces. As such, the status of an internal interface, explained in chapter Antispoofing on network interfaces, also applies to them. This option, which can be enabled in **Application protection > Inspection profiles,** increases the network's security when it is associated with appropriately defined routes and filter rules.

R43 | Declare internal VPN interfaces
VPN interfaces considered "internal" should be declared to benefit from anti-spoofing mechanisms.

7.5 Mobile access tunnels

In a client-to-site 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 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 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 **VPN > IPsec VPN > Anonymous – 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 | 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** > **Anonymous – 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 appliances, 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 single shared key can be defined for all clients. 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 | Authenticate mobile devices and/or users with certificates
Mobile devices 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 **VPN > IPsec VPN > Identification**, all certificates issued by this authority are allowed to set up mobile VPN tunnels.

R46 | 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 mechanism that the appliance 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. If a peer does not respond to requests sent by its counterpart, it will be considered unreachable, and the sender will then shut down the IKE as well as related IPsec tunnels on its side. There are several ways to use this mechanism:

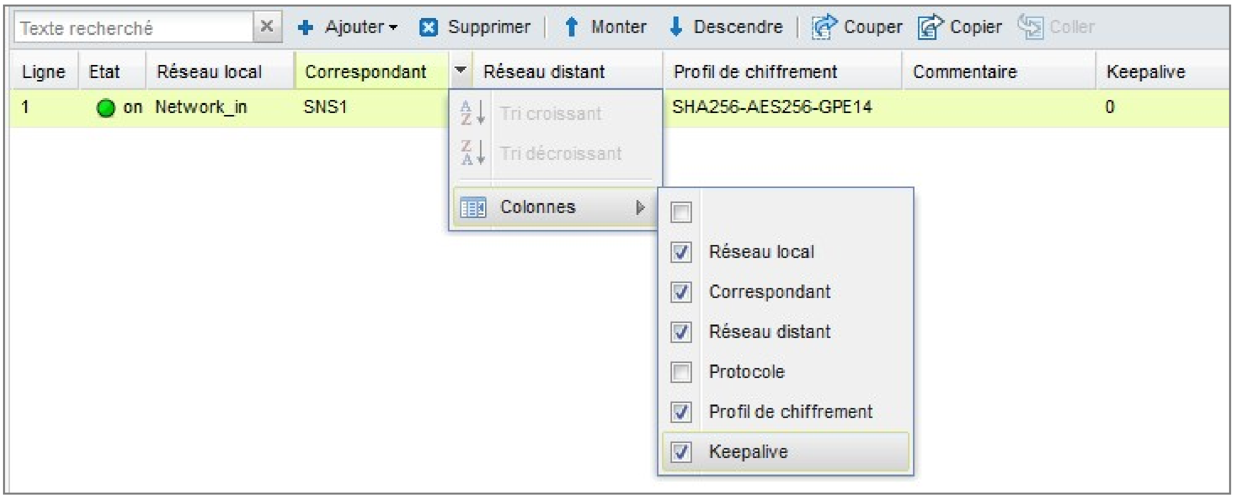
- In *inactive* mode, the firewall does not monitor the status of the peer and does not reply if it is contacted,
- In *passive* mode, the firewall does not monitor the status of the peer but replies if it is contacted,
- In *high* and *low* modes, the firewall monitors the status of the peer and replies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

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

R47 - | 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 tunnel is not in use, it can be shut down after a set period to release resources on appliances. 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 tunnel to keep it running. This type of traffic is of no use when it is received and can be filtered without being logged.



Ligne	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Commentaire	Keepalive
1	● on	Network_in	SNS1		SHA256-AES256-GPE14		0

□
☑ Réseau local
☑ Correspondant
☑ Réseau distant
□ Protocole
☑ Profil de chiffrement
☑ Keepalive

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

This feature can be configured in **VPN > IPsec VPN > Encryption > policy – Tunnels** as shown in the image above. Scrolling over the header of any column in the table will display an arrow. Click on it then go to the **Columns** menu to choose whether to display the Keepalive column. The interval between two requests can then be modified. A value of zero 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 | 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 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 + | 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 Chapter Implicit rules, and an explicit filter rule 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 by using the NSRPC command `config ipsec profile phase2 update replaywsize=XX` where XX is a value between 0 and 33554400 inclusive in increments of 8. 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 configuration used.

8. Monitoring

This feature was not part of the security target.

8.1 Configuring basic components

To query the appliance in SNMP, a filter rule must be configured in **Security policy > Filtering - NAT > Filtering**. Only monitoring servers must be allowed to query the appliance in SNMP, and only in read-only mode.

> **R50 | Filter SNMP queries**
> It is advisable to allow only monitoring servers to query appliances in SNMP, by using an adapted filter rule.

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

> **R51 | Use SNMPv3**
> SNMP version 3 is recommended as it provides authentication and encryption mechanisms.

By configuring the **Connection to the SNMP agent** field in **Notifications > SNMP agent > SNMPv3,** the algorithms and passwords used for authentication and encryption can be set.

> **R52 | Configure access 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).

When peers are entered in the **List of SNMP servers** in **Notifications > SNMP agent > SNMPv3**, the firewall will send SNMP traps to them.

> **WARNING**
> SNMP traps that the appliance sends are part of an implicit filter rule. This rule is included in the hosted services rule found in the **Implicit rules** menu. It is advisable to disable this rule in compliance with chapter Implicit rules and to replace it with custom rules.

8.2 Querying the appliance 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 appliance that uses the configuration parameters mentioned earlier:

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

The appliance 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 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 appliance.
-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 appliances on OIDs that belong to the standard MIB; the appliance can also be queried on SNS-specific OIDs (e.g., policy, high availability, VPN). Documentation on the SNS MIB can be found on Stormshield's Technical Documentation website. 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 firewalls.

The following is for example the SNMP query request making it possible to retrieve the name of the network filter policy enabled on an SNS appliance:

```
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 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 firewall gave to the policy.

The list of OIDs worth monitoring on an SNS appliance 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 appliance
.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 a Stormshield appliance 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. Backup

This feature was not 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. Also, when there is a failure, it must be possible to reproduce the previous configuration on a new appliance. To do so, automatic and regular archiving of the SNS configuration on a remote server should be implemented.

The configuration of the appliance can be exported in **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 firewall.

R53 | Set up automatic backup on a controlled server
It is advisable to enable the automatic configuration backup function and the export of the backup to a controlled custom WebDAV server via an authenticated HTTPS connection.

WARNING
If a custom WebDAV server is used with an HTTPS link, the firewall will verify the identity of the destination server by comparing the certificate entered in the **Server certificate** line with the one provided by the server. However, it will not verify the validity of the certificate, for example, its expiry date or whether its use is authorized.

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 the appliance's admin account, which is not recommended. The creation of a script is recommended on the SNS appliance that connects to a remote server in SSH and transfers the backup files.

R53 - | Set up automatic backup via SSH
If no controlled WebDAV 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 appliance initiated.

With the `config autobackup` command, the appliance'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.enc** 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 **.enc** 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 (**System** > **Maintenance** > **Backup** menu).

9.2 Opening backup files

Stormshield backup files (**.na** or **.na.enc** extension) cannot be unzipped directly from a standard archive manager. Such files must be opened beforehand with a `decbackup` utility in command line, which can be found on every appliance (available in *PATH* or in the folder */usr/Firewall/sbin*). This tool is also available in Linux, making it possible to open backup files, even when the user does not have an SNS appliance.

The syntax is the following:

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

The output file is an archive that includes all of the appliance's configuration files 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 appliance, 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 appliances, the following can be defined separately:

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

> **R54 | 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 is limited on the appliance's hard disk or SD card, the firewall makes it possible to pause logging or automatically erase older logs when the storage medium is full. When logging is paused, older logs can be kept, but any new events will not be logged in the event of a recent attack.

> **R55 | Enable log rotation**
> Automatic log rotation is recommended.

The type of log processing can be defined in **Notifications** > **Logs - syslog** > **Local storage**.

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.

> **R56 | Secure log transfers with the TLS protocol**
> The use of log transfer protocols is recommended (in line with the guide **Security recommendations relating to TLS** - in French), especially those based on robust cryptographic mechanisms, in particular 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 **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.

> **R57 | Events to log**
> Below is a non-exhaustive list of recommended events to collect via syslog among all the events

that the appliance offers in its 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 VPNs, 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.

11. Managing the firewall pool

This feature was not part of the security target.

To manage several SNS appliances, setting up an administration IS is recommended, 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 chapter **Centralized authentication** and the external PKI in compliance with chapter **Using a PKI**,
- Access the appliance's administration services remotely (HTTPS and NSRPC - the relevant tools use TCP port 1300) from administration workstations, in line with chapter **Administration services**.
- Forward logs generated by the SNS appliance to the central log server, in line with chapter **Logging** and the **Security recommendations for the implementation of log systems** (in French),
- Allow the passage of monitoring traffic described in chapter **Monitoring**, exchanged between the SNS appliance and the central monitoring server,
- Forward the SNS appliance's backup files to the central backup server, in line with chapter **Backup**.

12. List of recommendations

R1	Use accounts assigned to users by name
R2	Protect the local administrator account
R3	Restrict administration via SSH
R4	Use password authentication for SSH
R5	Authenticate locally using certificates
R6	Define an appropriate password policy
R7	Dedicate an external directory to administrators
R8	Use a restricted-access and secure account
R9	Adjust administration privileges
R10	Use groups to manage privileges
R11	Define administration sub-networks clearly
R12	Use an administrator object group
R13	Dedicate an Ethernet interface to administration
R14	Keep default cryptographic suites
R14 +	Harden TLS parameters on the administration interface
R15	Replace the web interface certificate
R16	Use NSRPC from the web interface
R16 -	Use accounts dedicated to direct NSRPC connections
R17	Use the same language in logs
R18	Use a language that users understand
R19	Enable the "*Diffusion Restreinte*" option
R20	Disable unused interfaces
R21	Declare internal interfaces
R22	Define static routes for internal networks
R23	Fill in anti-spoofing rules
R24	Update from an internal mirror
R24 -	Update through a proxy
R25	Choose controlled DNS servers
R25 -	Change default DNS servers
R26	Restrict the use of dynamic objects
R27	Synchronize system time

R28	Configure the LDAP securely
R29	Rename the production policy
R30	Disable implicit rules
R31	Adapt inspection type to the role of the device
R32	Adapt inspection profiles to the firewall’s use context
R33	Use object groups
R34	Use a controlled external PKI
R34 -	Use the appliance’s PKI
R35	Impose CRL verification
R36	Adapt the automatic refreshment of CRLs
R37	Configure the CRL retrieval URL and enable automatic retrieval
R37 -	Manually import CRLs
R38	Use strong algorithms for IKE and IPsec
R39	Use version 2 of the IKE protocol
R39 -	Use “main” mode when IKEv1 is used
R40	Use mutual certificate-based authentication
R40 -	Use a robust pre-shared key
R41	Configure IPsec tunnels securely
R41 +	Do not use the default route
R42	Confirm the source of incoming traffic
R43	Declare internal VPN interfaces
R44	Configure mobile tunnels in config mode
R45	Authenticate mobile devices and/or users with certificates
R46	Use a dedicated intermediate certification authority
R47	Enable Dead Peer Detection
R47 -	Use passive DPD mode
R48	Configure Keepalive
R49	Keep the DSCP field
R49 +	Control the DSCP field
R50	Filter SNMP queries
R51	Use SNMPv3
R52	Configure access to the SNMP agent

R53	Set up automatic backup on a controlled server
R53 -	Set up automatic backup via SSH
R54	Define a log policy
R55	Enable log rotation
R56	Secure log transfers with the TLS protocol
R57	Events to log

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.