# BETA SNS 5.0
# Release Notes

11/06/2025

# Table of contents

# New firewall behavior

This section lists the automatic behavioral changes related to the update of your SNS firewall to version 5.0.1 BETA from the previous version 4.8 available.

If necessary, we also invite you to consult the **New firewall behavior** of version SNS 4.8 introduced since the last version 4.3 LTSB available.

**Changes introduced in version 5.0.1 BETA**

- VPN SSL - Updating a VPN SSL configuration using an algorithm other than AES-128-GCM, AES-192-GCM, AES-256-GCM, and ChaCha20-Poly1305, or with compression enabled, is refused.
- Updating a firewall to version 5 is refused if the certificate used by the firewall was signed with the obsolete SHA1 algorithm.
- A certificate is automatically generated during the first start-up of a firewall in version 5 of SNS. It is used by default by the firewall's authentication services based on the TLS protocol (Web administration interface, captive portal).
- Automatic Backups - When the automatic backup module is configured to use a certificate signed with the obsolete SHA1 algorithm, this certificate is refused and the automatic backup is interrupted without transmitting data for security reasons. An error message prompts the administrator to generate a new custom certificate signed with a secure algorithm.
- Password Policy - The password policy defined on firewalls in factory configuration has been hardened. It now requires a minimum length of 16 characters (8 previously), the mandatory use of alphanumeric characters / uppercase and lowercase letters / special characters, and a minimum entropy of 64 (20 previously).
- Password Encoding - The character set used by the firewall to encode passwords is now UTF-8 for firewalls in factory configuration. This avoids connection issues via SSH when the password contains non-ASCII characters (example: "€", accented characters, ...).
- Several obsolete features have been removed from version 5 of SNS:
    - SNVM (Stormshield Network Vulnerability Manager),
    - VPN PPTP (Point-to-Point Tunneling Protocol)
    - VPN SSL portal (application mode and Java applet).
    - URL/SSL Filtering - The embedded URL database has been removed. To continue using URL/SSL filtering, you can:

- Subscribe to the Extended Web Control option,
- Continue using the embedded URL filtering engine by associating it with a URL filtering database provided by a third party, for example:
    - French URL filtering database provided by the Rectorate of Toulouse (Academy of Toulouse), following the method described in the Stormshield Knowledge Base (authentication required),
    - Polish URL filtering database provided by Dagma, following the method: https://stormshield.pl/pomoc/baza-wiedzy/item/zmiana-klasyfikacji-url-na-rozszerzona-klasyfikacje-dedykowana-dla-polskiego-rynku.

- SNMP Agent - Obsolete password encryption algorithms can no longer be selected in the SNMP v3 agent configuration panel. Only the AES-SHA2 (SHA256) algorithm is available by default. Migrating to SNS version 5 from a configuration using an algorithm other than SHA256 results in a message indicating that the used algorithm is obsolete. It is possible to modify using the CLI / Serverd CONFIG SNMP USERV3 command.
- SNMP Agent - SNMP tables with an index starting at 1 are now used by default and the old tables (index starting at 0) are marked as obsolete. The latter are expected to disappear in a future SNS version. When updating to SNS version 5 or higher of a firewall using the old tables, a warning is displayed to invite the administrator to activate the new SNMP tables by following the procedure described in the SNS User Manual.
- SNMP Agent - A message indicates that SNMP version 1 is obsolete. This version will be removed in a future SNS version.
- EVA - Virtual firewalls EVA in factory configuration now have a /data partition of 4 GB, compared to 2 GB in previous SNS versions. This change does not apply to EVA installed in a previous version and updated to SNS version 5.
- Explicit HTTP Proxy - The explicit HTTP proxy is obsolete and will be removed in a future SNS version.
- SSL/TLS-based protocols - The MD4, MD5, RIPEMD-160 (rmd160), MD2, MDC-2 hash functions and the DES-EDE3-CBC encryption algorithm have been removed as they are obsolete.
- IPSec - The 3DES encryption algorithm is no longer available in SNS version 5. Updating to version 5 of an IPsec configuration using this algorithm is refused, please modify your IPsec configuration and replace 3DES with another algorithm before updating your firewall to SNS version 5.
- Internal LDAP Directory - The CRYPT, MD5, SMD5, SHA and SSHA hash functions have been removed as they are obsolete.
- Network Captures - For security reasons, the right required to perform a network capture has been set to a more restrictive value.

- IPv6 - The "Land-type attack" alarm (alarm ip:21) no longer triggers in IPv6 and no longer generates an entry in the logs. This protection is now ensured within the firewall's operating system kernel.
- SSL VPN - Enabling the Data Channel Offload (DCO) option using the AES-256-GCM encryption suite for SSL VPN makes TheGreenBow VPN clients incompatible with the Stormshield VPN SSL feature.
- SSL VPN - Following the update to version 5 of a firewall in factory configuration, the Data Channel Offload (DCO) option is enabled by default when using the SSL VPN service. If you plan to establish SSL tunnels based on the TCP protocol, it is strongly recommended to disable the DCO option, which is intended for SSL tunnels based on UDP and causes significant performance degradation for SSL tunnels based on TCP.
- Object Groups - The maximum number of elements contained in a group is now limited to 3000 objects. Updating to version 5 of a configuration containing a group with more than 3000 elements is allowed, but it will no longer be possible to add objects to this group after the update.
- Routing by Interface - Routing by interface is no longer available in SNS version 5. Migration of a v4 configuration using this feature to an SNS version 5 is refused by the system.
- Modems - RNIS modems (telephone modems connected by serial cable) are no longer supported on firewalls in SNS version 5.

# New features and enhancements of SNS 5.0.1 BETA

## VPN IPsec - Hybrid Cryptography for Post-Quantum Encryption

From version 5.0 of SNS, hybrid cryptography can be used to protect against quantum attacks using hybrid algorithms standardized by NIST in the Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). You can use a post-quantum resistant algorithm in addition to the traditional algorithm to protect key exchange from quantum attacks. Note that symmetric cryptography is not vulnerable to this type of attack.

The supported algorithms in version 5.0 of SNS are the following:

- ML-KEM-512,
- ML-KEM-768,
- ML-KEM-1024.

Two encryption profiles using these hybrid algorithms are now proposed in the VPN IPsec

Encryption Profiles tab:

- PQCEncryption: intended for configurations with correspondents using exclusively post-quantum encryption standards,
- PQCTransition: intended for configurations in transition to post-quantum encryption standards.

## VPN SSL - Performance

The VPN SSL service now integrates the Data Channel Offload (DCO) module: when DCO is enabled, encryption/decryption operations of data packets passing through VPN SSL tunnels are processed in the operating system kernel and no longer by the VPN SSL service of the firewall.

This offers increased performance and allows the VPN SSL service to handle the establishment of a larger number of VPN SSL tunnels.

Note that DCO:

- Is only compatible with UDP-based VPN SSL tunnels,

- Is not enabled by default during the migration of an existing configuration,
- Requires the selection of the AES-GCM encryption suite.

## VPN IPsec - DR Transition Mode

The Diffusion Restreinte (DR) mode introduced in version SNS 4.2 does not allow cohabitation of policies that comply with the IPsec DR specifications defined by ANSSI and policies that comply with the standard IPsec standard (RFC 7292 IKEv2bis).

Version 5.0 of SNS allows configuring IPsec VPN tunnels that behave like DR mode tunnels, while maintaining the ability to establish VPN IPsec tunnels that comply with the standard. This feature, called "DR Transition Mode", applies to complex architectures whose DR compliance process must go through a transition phase during which IPsec DR and standard (non-DR) policies will coexist.

For more information on DR transition mode, see the Technical Note DR Transition Mode: making an IPsec architecture compatible with DR mode in a progressive manner.

## Enhanced Security

### System Hardening

As part of the hardening of the SNS operating system, privilege management has been strengthened during maintenance operations, firewall updates, or the use of certain services (SNMP agent, email sending...).

### Certificates signed with the SHA1 algorithm

As of version 5.0 of SNS, certificates signed with the SHA1 algorithm are no longer supported and can no longer be used in the various modules offering certificate use (SSL VPN, Telemetry, Automatic Backups...).

### Secure Boot activation check

The web administration interface displays a warning message when Secure Boot is not enabled on the firewall. Note that enabling Secure Boot imposes constraints: to evaluate these constraints and follow the Secure Boot activation procedure, please refer to the Technical Note **Managing Secure Boot in the UEFI of firewalls.**

### Password Policy

The password policy now allows the use of a combination of alphanumeric characters, uppercase and lowercase letters, and special characters. It is selected by default on firewalls in factory configuration.

## Integration into various environments

### SD-WAN

SD-WAN gateway availability control management has been improved to better take into account specific cases of network outages in environments with multiple WAN accesses.

For more information on SD-WAN configuration, see the Technical Note **SD-WAN - Selecting the best network link**.

## Performance Evolution

### General Performance

Version 5 of SNS improves the general performance of Stormshield firewalls.

For more information on firewall performance, please refer to the product sheets available on Stormshield's institutional website.

### Proxy

Proxy performance has been improved and allows for up to 25% additional throughput.

### Asynchronous Rule Reload

The filtering policy reload can now be performed asynchronously to minimize the impact on network traffic: filtering rules are not re-evaluated immediately, but at the time of their use.

This mechanism is particularly interesting for configurations with a large number of rules and concurrent connections.

It is not active by default and must be activated using the following CLI / Serverd command sequence:

```
CONFIG SECURITYINSPECTION COMMON STATEFUL AsyncReload=1
CONFIG SECURITYINSPECTION ACTIVATE
```

For more information on asynchronous rule reload, see the Technical Note **Asynchronous Rule Reload**.

## Improved User Experience

### Web Administration Interface

The firewall's web administration interface now allows you to open a configuration tab and a monitoring tab simultaneously in the same browser. This makes it easier to visualize the correct application of the configuration.

This can be done by clicking on the icon in the title of the Configuration and Monitoring tabs.

The SNS theme and user interface have been revised for greater navigation fluidity.

### TPM

The TPM processing flow has been improved by eliminating the need to seal stored secrets in the TPM with the new technical characteristics of the system when modifying the firewall's UEFI.

### IPsec Tunnel Monitoring

A search bar is now available in the IPsec VPN monitoring module.

### Real-time Logs

The Real-time Logs module allows you to view the latest logs stored in memory on firewalls without an SD card.

### HTTP Protocol

It is now possible to configure the value of the two configuration tokens *AuthorizationBearerBuffer* and *AuthorizationNegotiateBuffer* in the HTTP protocol analysis configuration module.

### Email Sending

The email sending engine has been hardened for increased security and message templates are now customizable in the web administration interface using variables for each of them.

## Telemetry

### New data reported by the telemetry service

The telemetry service of SNS version 5.0 reports new data:

- Data concerning the SSD status:
  - Number of blocks removed from SSD usage due to programming or erasure failure,
  - Number of hours the SSD has been powered on,
  - Average number of block erasures (number of times the SSD has been completely written),
  - Remaining lifespan percentage,
  - SSD wear indicator (0 - 100%),
  - Total number of 512-byte sectors written during the SSD's lifetime,
  - Total number of 512-byte sectors read during the SSD's lifetime.
- Data concerning filtering policy:
  - Number of filtering policy reloads since firewall startup,
  - Status of asynchronous filtering rule reload mode activation.
- Data concerning IPsec tunnels:
  - Number of mobile tunnels configured with a Key-Encapsulation Mechanism (KEM) using apost-quantum resistant algorithm,
  - Number of mobile tunnels established with a KEM using a post-quantum resistant algorithm,
  - Number of site-to-site tunnels configured with a KEM using a post-quantum resistant algorithm,
  - Number of site-to-site tunnels established with a KEM using a post-quantum resistant algorithm.

By transmitting this completely anonymous data, you help Stormshield refine the sizes and limits of future hardware platforms and SNS versions.

## Miscellaneous

- Operating System: SNS version 5 is based on FreeBSD 14.
- Intrusion Prevention: NPDU and BVLL services are now supported by the BacNet/IP protocol analysis engine.
- The Energy Efficient Ethernet (EEE) feature associated with 2.5 Gbit/s Ethernet network cards is now supported.
- The OID sysObjectID (1.3.6.1.2.1.1.2) now allows the firewall model to be retrieved via an SNMP query.

# SNS 5.0.1 BETA bug fixes

## System

### Syslog - SD-WAN

A parameter managing the delay for resending logs has been added to each syslog profile defined on the firewall.

In a configuration using SD-WAN and router objects, following a network failure and a switch to a backup gateway, this parameter allows, for each profile, to adjust the delay after which the firewall attempts to send logs to the syslog server again and limit the risk of log loss.

This delay, previously fixed at 60 seconds, can be adjusted between 5 and 600 seconds.

### Reports

*Support references 85380 - 82777*

Improvements have been made to limit the size of the reports database and prevent it from filling up its partition unnecessarily.

*Support reference 84256*

In a configuration managing machine reputation, the CLI / Serverd command REPORT RESET report=all now allows to completely clear the reports database as expected.

### IPsec VPN

*Support reference 85641*
*Support reference 84803*

VPN tunnels are now renegotiated when the peer's certificate is modified. This regression appeared in version SNS 4.8.0.

### Virtual IPsec interfaces (VTI)

*Support reference 85770*

Running the command *ennetwork -f* on a configuration with a tunnel based on virtual IPsec interfaces no longer causes an IPsec tunnel interruption.

## Certificates and PKI

*Support reference 85948*

## Network card drivers

The default values of certain queues defined for each network card driver have been increased. This prevents low packet loss even when the firewall's CPU load is not high.

## Filtering and NAT

*References support 80798 - 85537*

You must now double-click on the comment of an unselected NAT or filtering rule to modify the comment. In previous SNS versions, clicking on the comment of an unselected NAT or filtering rule would open and then immediately close the comment editing.

## Configuration - Check usage

When a user/group of users is present in multiple referenced LDAP directories on the firewall, the "Check usage" function now only returns results related to the relevant directory.

## Configuration - SSH access

*Reference support 85101*

The use of characters "<" and ">" in quotes in Serverd CLI commands executed on the firewall via an SSH connection is now correctly interpreted and no longer causes the "Error in format" error message.

## Automatic backups

When the automatic backup module is configured to use a certificate signed with the SHA1 algorithm, this certificate is rejected and a warning message prompts the administrator to generate a new custom certificate signed with secure algorithms.

### High availability - Failover optimization

*Reference support 85773*

Now, when the "Restart all interfaces included in a bridge" checkbox is checked, only the interfaces contained in a bridge restart.

### LDAPS server

*Reference support 85766*

It is now possible to use a global machine object to configure an LDAPS server.

### URL filtering - Extended Web Control (EWC)

*References support 85849 - 86059*

The EWC URL filtering service is functional again after updating the IP address of the ewc-sns.stormshieldcs.eu server

## CLI / Serverd commands

### Filtering and NAT

*Reference support 85566*

The documentation and integrated help of the CLI / Serverd command CONFIG FILTER RULE UPDATE have been corrected: the srcport parameter can only represent a single port or a single range of ports and not a list of ports as previously incorrectly indicated.

## Virtual Machines

### High Availability (HA) and Pay As You Go (PAYG) configuration

*Support reference 85730*

The license management mechanism within the cluster has been improved to allow the passive firewall to retrieve its license by synchronizing with the active firewall during Pay As You Go cluster enrollment.

## Intrusion Prevention Engine

### Dynamic Routing BIRD

*Support reference 84579*

Only the routes that BIRD sends to the kernel are now retrieved in the protected network address table.

### OPC UA Protocol

The NodeID control by the OPC UA protocol analysis engine has been modified to conform to the protocol specifications and no longer cause unjustified blocking of valid OPC UA packets.

### SIP Protocol

The default value of the Action / Level parameters associated with the "Anonymous address in SDP connection" sensitive alarm (alarm sip:465) is now Block / Major. This value was previously incorrectly set to Pass / Minor.

### Stealth mode disabled - IPv6 analysis

*Support reference 85327*

A firewall with stealth mode disabled no longer freezes unexpectedly when analyzing IPv6 packets.

### System commands sfctl

*Support reference 85757*

The analysis of arguments passed to system commands sfctl no longer stops incorrectly after the first alphabetic character. This behavior could cause the triggering of a command that does not match the requested command but is similar to it up to the first alphabetic character.

## Equipment

### Energy Efficient Ethernet (EEE)

Enabling EEE on compatible network cards is now functional. These cards have the checkbox **Enable IEEE 802.3az standard (EEE)** in their advanced configuration.

## Web Administration Interface

### Administrators - Admin Account

The result of exporting the private key or public key of the super-administrator account (admin account) is now a text file. It was previously in csv format.

## Protocols - Filtering in the Sandboxing Analysis Tab

The filtering function in the Sandboxing Analysis tab of the HTTP / SMTP / POP3 and IMAP protocols and in the SSL protocol certification authorities grid is functional again. This regression appeared in version SNS 4.8.0.

## Interfaces - Media Type

The value 5 Gbit/s has been added to the list of media that can be selected for a network interface.

# Thank you

www.stormshield.com