GUIDE

STORMSHIELD NETWORK SSL VPN CLIENT

SSL VPN ADMINISTRATION GUIDE FOR SNS FIREWALLS AND STORMSHIELD SSL VPN CLIENTS

Document last updated: October 22, 2025

Reference: sns-en-ssl_vpn_administration_guide

Table of contents

Change log

Date	Description
October 22, 2025	New document

Getting started

Welcome to the SSL VPN administration guide for Stormshield SNS firewalls and SSL VPN clients.

In this guide, Stormshield Network Security is referred to as "SNS firewall", and Stormshield Network SSL VPN Client is referred to as "Stormshield SSL VPN client".

SSL VPN allows remote users to securely access an organization's resources - internal or otherwise - via the SNS firewall. An SSL VPN client must be installed on the user's workstation and/or mobile device before they can set up SSL VPN tunnels with the SNS firewall.

Once the SSL VPN tunnel has been set up, communications between the user and the SNS firewall are encapsulated and protected through an encrypted TLS tunnel, referred to in this guide as an "SSL VPN tunnel".

This guide explains:

- The configuration to apply in the **Authentication, Access privileges** and **Filter - NAT** modules on the SNS firewall in order to deploy SSL VPN tunnels,
- How to enable and configure the SSL VPN service on the SNS firewall,
- How to configure the client workstation verification feature when zero trust network access (ZTNA) is used,
- How to track users who are connected to the SNS firewall through an SSL VPN.

Requirements

This section describes the requirements for deploying SSL VPN tunnels with an SNS firewall and compatible SSL VPN clients.

An appropriately scaled SNS firewall

The maximum number of SSL VPN tunnels allowed on SNS firewalls varies according to the model used. You must have a model that fits your requirements.

You can find this information on the Stormshield website, under Product range (SNS), by selecting your model.

A compatible SSL VPN client

Each user must have a compatible SSL VPN client on their workstation and/or mobile device to set up SSL VPN tunnels with the SNS firewall.

Compatible SSL VPN clients:

- The **Stormshield SSL VPN client**. For further information on installing the client, refer to the Stormshield SSL VPN client v5 installation guide. To find out which versions are currently supported, refer to the Network Security & Tools life cycle guide.
- The **OpenVPN Connect** client. This SSL VPN client does not have a mode in which the SNS firewall's SSL VPN configuration can be automatically retrieved, and is not compatible with the SNS firewall's client workstation verification feature.

NOTE
To test the configuration before deployment, install a compatible SSL VPN client on some of your devices now. To deploy the SSL VPN in your organization, you can start by configuring the SNS firewall, then installing all the SSL VPN clients.

Prior connection of the SNS firewall to a directory

The SNS firewall must be connected to a directory. Check this connection in the SNS firewall's web administration interface in **Configuration > Users > Authentication, Available methods** tab. An LDAP line must appear in the grid.

For more information, refer to the section **Directory configuration** in the v4 user guide or v5 user guide, depending on the SNS version used.

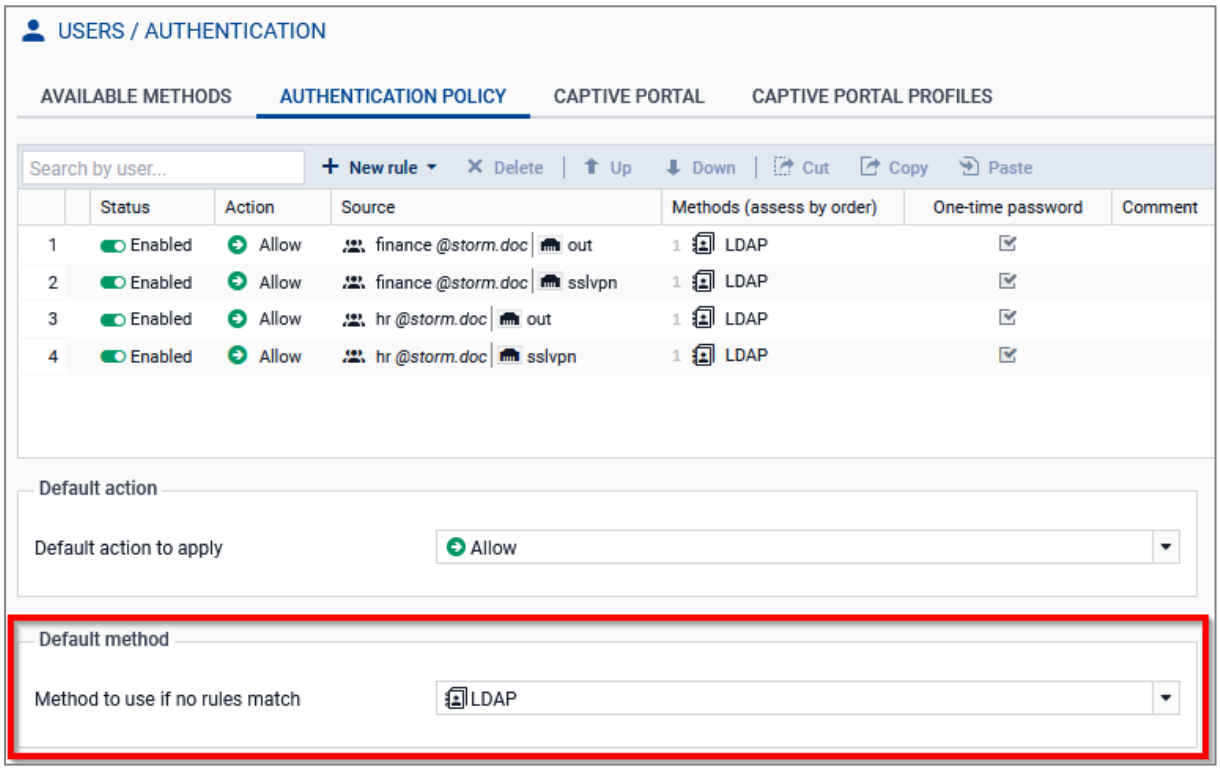
Configuring authentication

This section explains how to configure the Authentication module on the SNS firewall in order to deploy SSL VPN tunnels.

Configuring the authentication policy

This section explains how to configure the authentication policy to be implemented in order to deploy SSL VPN tunnels. You can click on **Apply** at any time to save your changes.

1. Go to **Configuration > Users > Authentication, Authentication policy** tab.
2. Identify the **Method to use if no rules match**.



Proceed accordingly.

Case 1: The "LDAP" method is selected and only this method is used on the SNS firewall

The current configuration of the authentication policy will suffice. Continue to Configuring the captive portal.

Case 2: In all other cases

In all other cases (restricted only to authentication on the SNS firewall, use of multifactor authentication, etc.), you need to add at least two rules to the authentication policy to allow users to authenticate with the Stormshield SSL VPN client and set up SSL VPN tunnels.

For stronger security, we recommend creating these two rules for each user group that is setting up SSL VPN tunnels with the SNS firewall. However, you can also choose to create only two rules for all users, with no particular distinction.

The first rule allows users and Stormshield SSL VPN clients that are configured in Stormshield mode to connect to the SNS firewall's captive portal. Stormshield SSL VPN clients can then automatically retrieve the SSL VPN configuration, and send information that enables the SNS firewall to verify the client workstation's compliance (ZTNA).

1. Click on **New rule > Standard rule**.
2. In the **User** tab, select a user or user group from an SNS firewall directory (such as *finance@domain.tld*). If you wish to do so, select all the users in a directory by setting *Any user@domain.tld*. On SNS in version 5, you can also select all users from all SNS firewall directories by selected **All users (any)**.
3. In the **Source** tab, add the source interface of SSL VPN connections (e.g. *out*).
4. In the **Authentication methods** tab:
   a. Delete the *Default method* row.
   b. Enable the method allowing users and Stormshield SSL VPN clients to connect to the SNS firewall's captive portal, e.g., *LDAP* or *RADIUS*.
   c. If a multifactor authentication method is used (authentication with a one-time password), set the **One-time password** selector to **ON** ON.
5. Click on **OK**.

The second rule allows users to set up SSL VPN tunnels from their SSL VPN clients to the SNS firewall.

1. Click on **New rule > Standard rule**.
2. In the **User** tab, select the same user or user group as the one in the first rule.
3. In the **Source** tab, add the *SSL VPN* interface.
4. In the **Authentication methods** tab:
   a. Delete the *Default method* row.
   b. Enable the method allowing users to set up SSL VPN tunnels from their SSL VPN clients to the SNS firewall, e.g., *LDAP* or *RADIUS*.
   c. If a multifactor authentication method is used (authentication with a one-time password), set the **One-time password** selector to **ON** ON.
5. Click on **OK**.

> **NOTE**
> During an authentication on the SNS firewall, rules in the authentication policy are scanned in order of their appearance in the list.

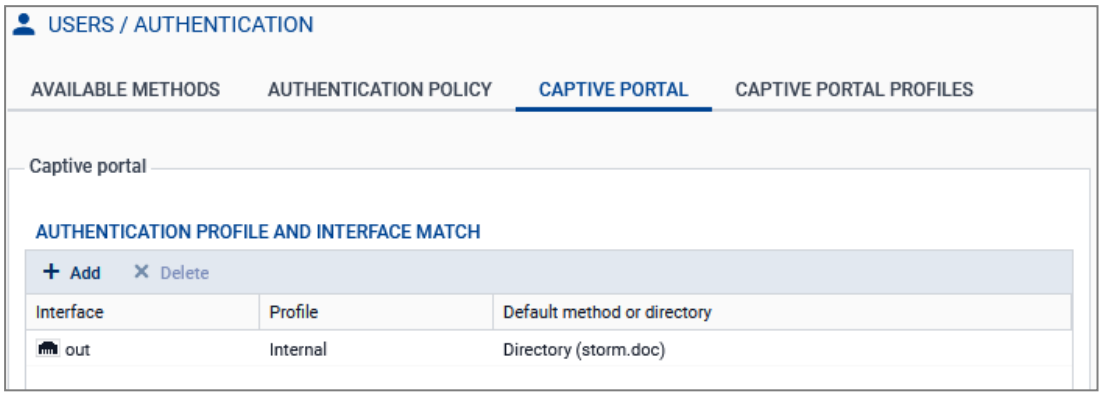
Configuring the captive portal

This section explains how to configure the captive portal in order to deploy SSL VPN tunnels. You can click on **Apply** at any time to save your changes.

Configuring authentication profile and interface match

1. Go to **Configuration > Users > Authentication, Captive portal** tab.
2. In the **Authentication profile and interface match** grid, click on **Add**.
3. In the **Interface** column, select the source interface of SSL VPN connections (e.g., *out*). If you are using a PPPoE or VLAN interface, select it instead of the physical parent interface.

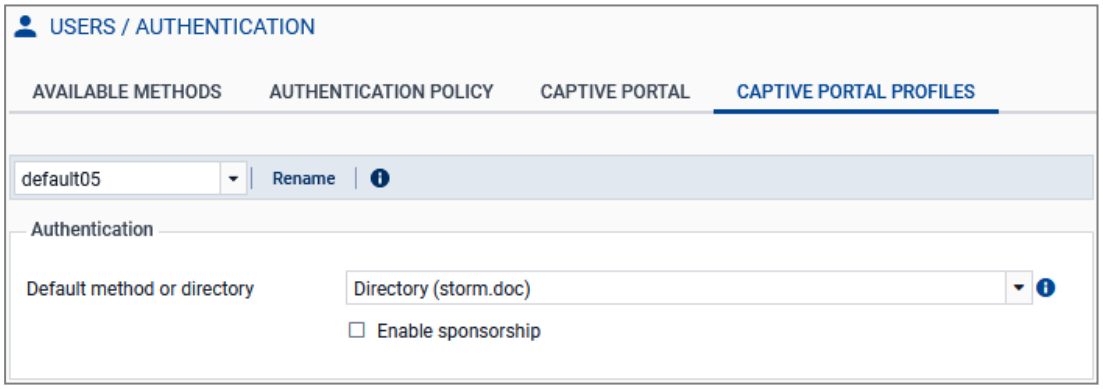
4. In the **Default method or directory** column, if the directory entered matches the directory of the users who are setting up SSL VPN tunnels with the SNS firewall, the value of the **Profile** column does not need to be changed. This configuration allows users to simply enter their ID in their SSL VPN client to set up the SSL VPN tunnel.



Otherwise, users will need to enter their ID with the directory authentication domain (*identifiant@domain.tld*) in their SSL VPN client to set up the SSL VPN tunnel. If you want users to simply enter their ID, adapt the configuration:

a. In the **Profile** column, select another profile (e.g., *default05*).

b. In the **Captive portal profiles** tab, select this other profile and choose the right directory in the **Default method or directory** field.



Checking whether the captive portal is enabled

1. Go to **Configuration > Users > Authentication, Captive portal profiles** tab.
2. Select the profile used for the SSL VPN connections.
3. In the **Advanced properties** section, ensure that the **Enable the captive portal** checkbox has been selected.

Customizing the captive portal's certificate

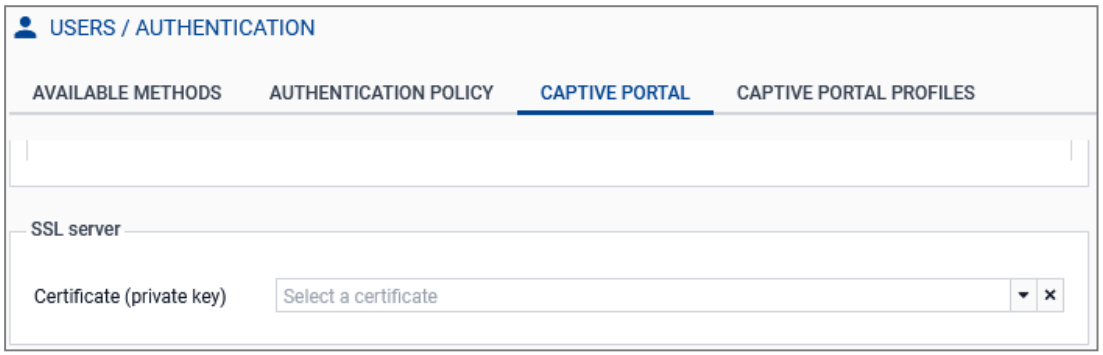
You can customize the certificate presented by the SNS firewall when accessing the captive portal. If this certificate is not customized, the SNS firewall will present a default certificate:

- On SNS in version 4, this will be a certificate corresponding to the SNS firewall serial number,
- On SNS in version 5, this will be a self-generated certificate for this access.

To customize the captive portal's certificate:

1. Go to **Configuration > Users > Authentication, Captive portal** tab.
2. In the **Certificate (private key)** field, select the new certificate. If necessary, you can add a new certificate (server identity) in **Configuration > Objects > Certificates and PKI**.

   On SNS in version 4.8 LTSB and 5, the icon indicates certificates with TPM-protected private key. For more information on this protection, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.



If any of the following criteria applies to the selected certificate:

- The certificate was not signed by a trusted certification authority,
- The certification authority has not been deployed on users' workstations,
- The certificate's **CN** does not match the SNS firewall address that is used for connections to the SSL VPN. This is the case, for example, with the default certificate presented by the SNS firewall.

The certificate cannot be automatically validated by the SSL VPN client or web browser, and a window indicating a probable security risk will appear. Each user must then ensure that the connection is secure by checking the certificate information, and then indicate that they trust the certificate presented by the SNS firewall to set up the SSL VPN tunnel. Although this message does not prevent users from proceeding, we recommend explaining to your users when they should expect to see it.

Multifactor authentication

This section explains some of the multifactor authentication solutions that you can use to set up SSL VPN tunnels with the SNS firewall. If you do not wish to use a multifactor authentication method, proceed to the next section.

General information on multifactor authentication

Multifactor authentication strengthens the authentication of users who set up SSL VPN tunnels with a second authentication factor.

The second factor is generally a one-time password, known as an OTP or TOTP, which the user must enter in addition to their password to set up the SSL VPN tunnel. Stormshield has its own TOTP solution.

An external solution can also be used with a RADIUS server or a third-party application to be installed on a trusted device. For example, the Trustbuilder solution (formerly inWebo) is compatible and allows users to generate OTPs or approve setting up connections (push notifications) in their application.

This document explains some of these solutions. Proceed accordingly.

NOTE
To configure the use of multifactor authentication on the Stormshield SSL VPN client, refer to the Stormshield SSL VPN client v5 user and configuration guide.

Using the Stormshield TOTP solution

Refer to the technical note Configuring and using the Stormshield TOTP solution, which explains how to configure and manage the TOTP solution on the SNS firewall, and presents the enrollment procedure for TOTP solution users.

Ensure that you follow the steps described in this technical note on using the Stormshield TOTP solution to set up SSL VPN tunnels with the SNS firewall.

Using a third-party solution with a RADIUS server

Configuring the third-party multifactor authentication solution

The chosen third-party multifactor authentication solution has to be configured and connected to your RADIUS server. If you need help with this configuration, refer to the documentation for your chosen solution.

Enabling the RADIUS method on the SNS firewall

Enable and configure the RADIUS method on the SNS firewall to connect it to your RADIUS server. To do so, go to **Configuration > Users > Authentication, Available methods** tab.

For more information, refer to the section **Authentication > Available methods** tab **> RADIUS** in the v4 user guide or v5 user guide, depending on the SNS version used.

Customizing the idle timeout allowed for the connection to the RADIUS server

The default idle timeout allowed for the connection to a RADIUS server is 3000 milliseconds (3 seconds).

If the chosen multifactor authentication solution involves the use of a third-party application to log in (push mode), the idle timeout has to be customized so that users have enough time to log in. To set a 30-second idle timeout, for example, use the following CLI/serverd commands:

```
CONFIG AUTH RADIUS timeout=30000 btimeout=30000
CONFIG AUTH ACTIVATE
```

Using an authentication method with a user certificate

This section explains how to use an authentication method with a user certificate to set up SSL VPN tunnels with the SNS firewall. If you do not wish to use an authentication method with a user certificate, proceed to the next section.

With this authentication method, users can set up SSL VPN tunnels by authenticating on the SNS firewall with their user certificate.

Requirements

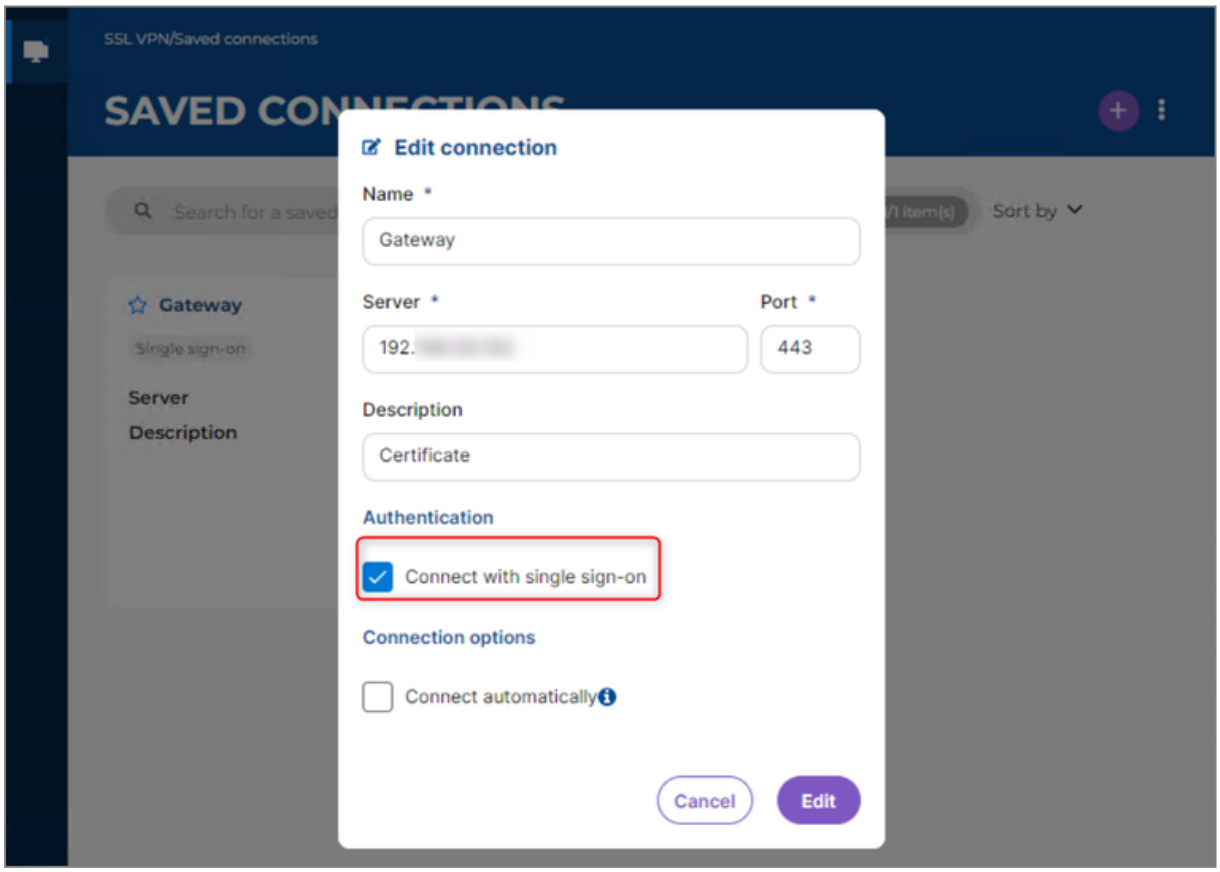
To use the authentication method with a user certificate, you need to meet the following requirements:

- An SNS firewall in version 5.
- Stormshield SSL VPN clients in version 5. Earlier versions of the Stormshield SSL VPN client and third-party SSL VPN clients, such as OpenVPN Connect, are not compatible.
- **SSL certificate** method enabled and configured in **Authentication > Available Methods** on the SNS firewall. For more information, refer to the section **Authentication > Available methods** tab **> Certificate (SSL)** in the v4 user guide or v5 user guide, depending on the SNS version used.
- Rules created, allowing users to authenticate through the **SSL Certificate** method in the **Authentication > Authentication Policy** module on the SNS firewall. Adapt the information in the section Configuring the authentication policy to obtain this configuration.
- SSL VPN service enabled and configured in the **SSL VPN** module on the SNS firewall. This configuration is described in the following sections.
- User certificates installed on the workstations of the users in question. You can download the user identity of the certificate in P12 format in the **Objects > Certificates and PKI** module on the SNS firewall.

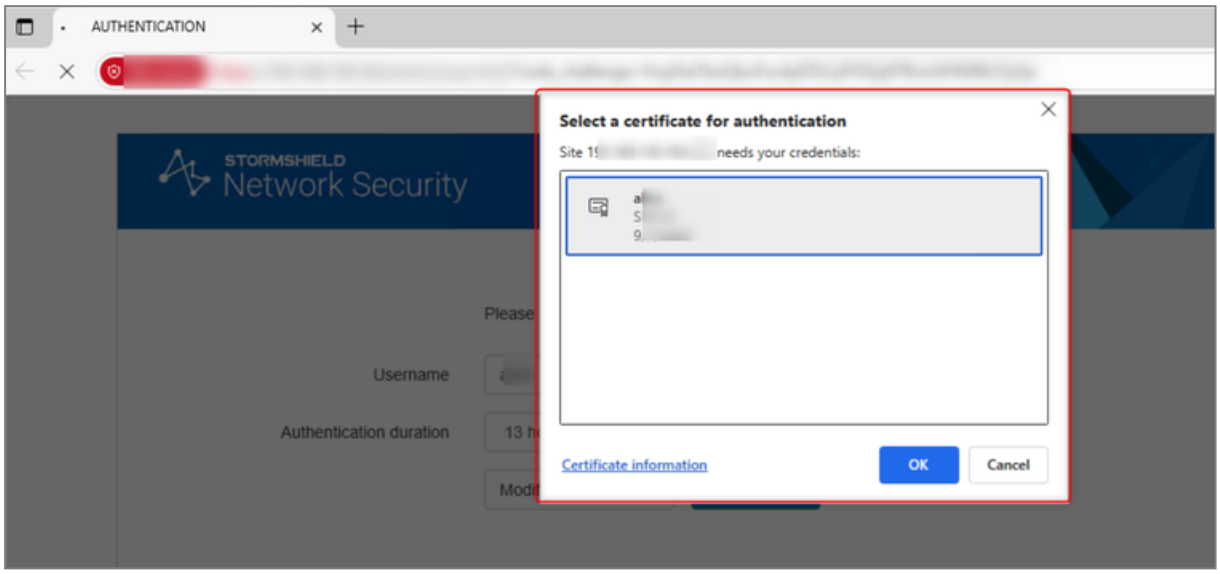
Setting up an SSL VPN tunnel by authenticating with a user certificate

On the Stormshield SSL VPN client, the connection (saved or direct) must be set up with the following parameters:

- **Stormshield mode** has to be selected. OpenVPN connections (imported OVPN file) are not compatible.
- The **Connect with single sign-on** checkbox must be selected.



Once the SSL VPN tunnel has been initiated, the SNS firewall's captive portal opens automatically in the user's web browser. The user then authenticates on the portal by following the instructions.



Once the user is authenticated, the SSL VPN tunnel is set up. The expiry date of the user's authentication session is displayed in the Stormshield SSL VPN client graphical interface. As long as this date has not been reached, and the authentication session is still valid on the SNS firewall, the user does not need to authenticate again to set up the SSL VPN tunnel.

For more information, refer to the section Setting up a secure connection in the *Stormshield SSL VPN client v5 user and configuration guide*.

Known limitations

TLS 1.3 incompatibility

With SNS version 5.0.2, authentication with user certificates is not supported over TLS 1.3. This limitation will be fixed in a future version of SNS.

Workarounds are available, depending on your users' web browser:

- On Firefox, enable the following setting in the Firefox configuration:
  ```
  security.tls.enable_post_handshake_auth
  ```
- For other browsers such as Chrome or Edge, you need to force the SNS firewall's captive portal to use TLS 1.2. To do so, run the following SSH commands on the SNS firewall:
  ```
  setconf /usr/Firewall/ConfigFiles/auth Config TLSv13 0
  ensl
  ```

Entering the user name during authentication

Users currently have to enter their user names on the captive portal before they can select the certificate to be used for authentication. This limitation will be improved in a future version of SNS.

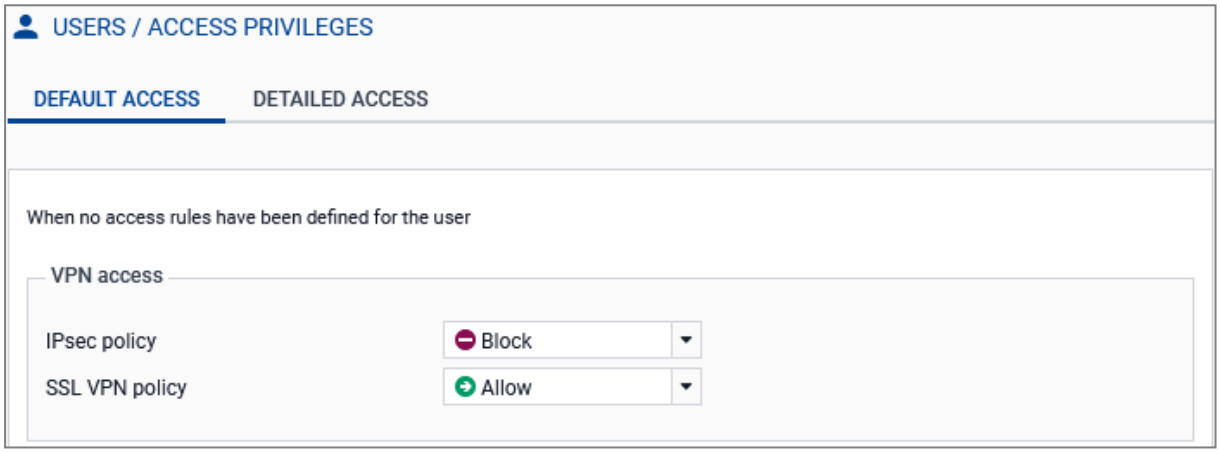
Configuring privileges to access the SSL VPN

This section explains how to grant users the privilege to set up SSL VPN tunnels. This privilege can be assigned to all users, or to certain users and user groups.

Proceed accordingly. You can click on **Apply** at any time to save your changes.

Allowing all users to set up SSL VPN tunnels

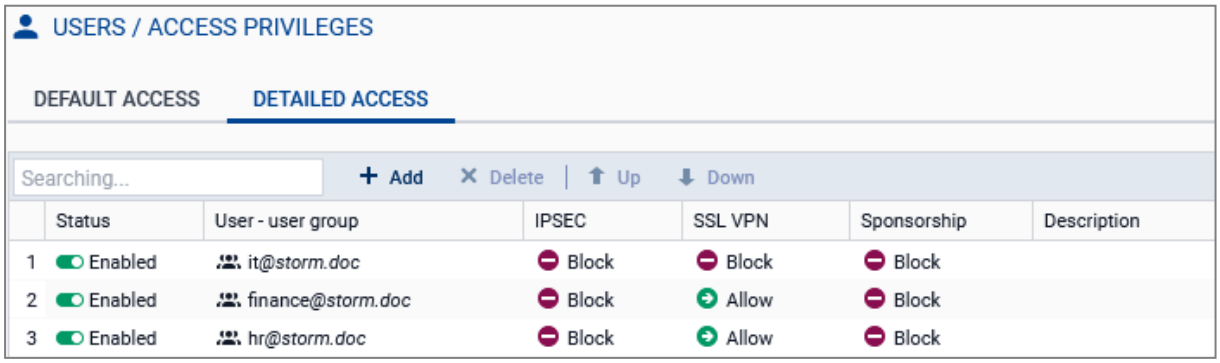
1. Go to **Configuration > Users > Access privileges**, **Default access** tab.
2. In the **SSL VPN policy** field, select **Allow**.



Allowing some users and user groups to set up SSL VPN tunnels

1. Go to **Configuration > Users > Access privileges**, **Default access** tab.
2. In the **SSL VPN policy** field, select **Block**.
3. Go to the **Detailed access** tab.
4. Click on **Add** to create a custom access rule.
5. In the window that appears, select a user or user group from an SNS firewall directory (such as *finance@domain.tld*). If you wish to do so, select all the users in a directory by setting *Any user@domain.tld*. Click on **Apply** or **OK,** depending on the SNS version used.

   A new row will appear in the grid.
6. In the **SSL VPN** column of the new row, select **Allow** as the action.
7. Enable the rule by double-clicking in the **Status** cell of the relevant row.



Configuring the SSL VPN service and client workstation verification (ZTNA)

This section explains how to configure the SNS firewall's SSL VPN service and client workstation verification (ZTNA).

Configure the SSL VPN service

This section explains how to enable and configure the SSL VPN service on the SNS firewall.

Go to **Configuration > VPN** > **SSL VPN**. There are variations between SNS versions. Whenever these variations are relevant, they will be indicated. You can click on **Apply** at any time to save your changes.

Enabling the SSL VPN service

Field	Description
Enable SSL VPN 	Set the selector to **ON** to enable the SSL VPN service.

Configuring the general settings of the SSL VPN service

On SNS in versions SNS 4.8 LTSB and 5, these settings can be configured in the **General settings** tab. On SNS in version 4.3 LTSB version, there is no tab.

NOTE
As of SNS version 4.8.5, a warning will prompt you to disable the LZ4 compression feature if it is enabled. This scenario is described in the section Troubleshooting".

Field	Description
Enable client workstation verification (ZTNA) 	On SNS in version 5, set the selector to **ON** to enable the verification of client workstation compliance. On SNS in version 4.8 LTSB, the feature can be enabled in the **Client workstation verification (ZTNA)** tab. This feature is not available on SNS 4.3 LTSB versions. When client workstation verification is enabled: • SSL VPN clients that are compatible with this feature (see Configuring client workstation verification (ZTNA)) can set up SSL VPN tunnels with the SNS firewall **only if all** the criteria defined in the policy have been met, • SSL VPN clients that are not compatible with this feature cannot set up SSL VPN tunnels with the SNS firewall, **unless** they are explicitly allowed to do so by enabling the **SSL VPN clients incompatible with ZTNA** setting.

Network settings section

Field	Description
Public IP address (or FQDN) of the UTM used	Indicate the IP address that users must use in their SSL VPN client to reach the SNS firewall and set up SSL VPN tunnels. You can specify an FQDN or IP address. • For an FQDN: it must be declared in the DNS servers used by the user's device. If you have a dynamic public IP address, you can use the services of a provider such as *DynDNS* or *No-IP*. Next, configure this FQDN in **Configuration > Network > Dynamic DNS.** • For IP addresses: they must be public, and therefore accessible over the Internet.
Available networks or hosts	Select the object representing the networks or hosts that will be reached through the SSL VPN tunnel. This object makes it possible to automatically set on your organization's devices the routes needed to reach resources that can be accessed through the SSL VPN tunnel. To more granularly allow or prohibit traffic between your users' devices and internal resources, you need to define filter rules (see Configuring the filter and NAT policy). If some of your organization's devices are located between the SNS firewall and accessible internal resources, you can set static routes on these devices for access to the network assigned to SSL VPN clients.
Network assigned to clients (UDP) **Network assigned to clients (TCP)**	Select the object corresponding to the TCP and UDP networks assigned to SSL VPN clients. Select the network or sub-networks according to the following criteria: • The network mask must not be smaller than **/28**. • If you assign two networks, the SSL VPN client will always use the UDP-based SSL VPN tunnel first to ensure better performance. This order is defined in the SSL VPN (OpenVPN) configuration that the SNS firewall provides to SSL VPN clients. • The assigned network must not belong to any existing internal networks, or networks declared by a static route on the SNS firewall. Since the interface used for the SSL VPN is protected, the SNS firewall would then detect an IP spoofing attempt and block the corresponding traffic. • To avoid routing conflicts, select less commonly used sub-networks, such as 10.**60.77**.0/24, as many filtered Internet access networks (public Wi-Fi, hotels,, or private local networks already use the first few reserved address ranges.

Field	Description
Maximum number of simultaneous tunnels allowed	The number appears automatically. This number corresponds to the lowest value, either the number of tunnels allowed on the SNS firewall (see Requirements), or the number of sub-networks available for SSL VPN clients. For sub-networks: • On SNS in version 5: this shows the total number of IP addresses, minus 3. • On SNS in version SNS 4.3 LTSB and 4.8 LTSB: this represents 1/4 of the IP addresses, minus 2. An SSL VPN tunnel takes up 4 IP addresses and the server reserves 2 sub-networks for its own use.

DNS settings sent to client section

Field	Description
Domain name	Enter the domain name assigned to the SSL VPN clients so that they can resolve their host names.
Primary DNS server **Secondary DNS server**	Select the object representing the DNS server to be assigned.

Advanced properties section

Field	Description
Enable DCO kernel acceleration	On SNS in version 5 in factory configuration, the DCO (*Data Channel Offload*) kernel acceleration feature is enabled by default. Select or unselect the checkbox to enable or disable this feature. On SNS in version 4, this feature is not available. This feature improves the performance of **UDP-based SSL VPN tunnels**. It is not compatible with TCP-based SSL VPN tunnels. The SSL VPN client used must be compatible with the DCO feature to benefit from enhancements. As for the Stormshield SSL VPN client: • The Windows version benefits from enhancements. • The Linux version benefits from enhancements **only if** OpenVPN is in version 2.6.0 or higher, and the **openvpn-dco** package has been installed. • The macOS version does not benefit from enhancements. **NOTE** When you enable the DCO feature, a message may appear, prompting you to change the encryption suite if the one you are using is incompatible. Accept the change to enable the feature.
Public IP address of the UTM for the SSL VPN (UDP)	In the following cases, you need to select the object representing the IP address to reach in order to set up UDP SSL VPN tunnels: • The IP address to reach is not the main IP address of the external interface, • The IP address to reach belongs to an external interface that is not linked to the default gateway of the SNS firewall.

Field	Description
Port (UDP) **Port (TCP)**	The listening ports of the SSL VPN service can be changed. Note: • Some ports are reserved for the SNS firewall's internal use only and cannot be selected, • Port 443 is the only port below 1024 that can be used, • If you change any of the default ports, the SSL VPN could become inaccessible from networks (hotels or public WiFi) on which Internet access is filtered.
Interval before key renegotiation (seconds)	You can change the length of time after which the keys used by the encryption algorithms will be renegotiated. By default, it is set to 14400 seconds, or 4 hours. During this operation: • The SSL VPN tunnel will not respond for several seconds. • If multifactor authentication is used, the user will need to enter a new OTP, or approve the new connection on the third-party application, in order to stay connected. In this use case, we advise increasing the interval before key renegotiation so that it aligns with the average length of a workday, such as 28800 seconds, or 8 hours.
Use DNS servers provided by the firewall	You can instruct SSL VPN clients to include the DNS servers retrieved via the SSL VPN in the workstation's (Windows only) network configuration. If DNS servers are already defined on the workstation, they may be queried.
Prohibit use of third-party DNS servers	You can instruct SSL VPN clients to exclude the DNS servers that have already been defined in the workstation's (Windows only) configuration. Only DNS servers sent by the SNS firewall can be queried.

Scripts to run on the client

The Stormshield SSL VPN client In Windows can run *.bat* scripts when an SSL VPN tunnel is opened or closed. In these scripts, you can use:

- Windows environment variables (**%USERDOMAIN%**, **%SystemRoot%**, etc.),
- Variables relating to the Stormshield SSL VPN client: **%NS_USERNAME%** (user name used for authentication) and **%NS_ADDRESS%** (IP address assigned to the SSL VPN client).

Field	Description
Script to run when connecting	Select the script to run when the SSL VPN tunnel is opened. Example of a script that makes it possible to connect the Z: network drive to the shared network: `NET USE Z: \\myserver\myshare`
Script to run when disconnecting	Select the script to run when the SSL VPN tunnel is closed. Example of a script that makes it possible to disconnect the Z: network drive from a shared network: `NET USE Z: /delete`

The Stormshield SSL VPN client in Linux and macOS can also run scripts when an SSL VPN tunnel is opened or closed. These scripts are generally used to accommodate the DNS configuration when OpenVPN does not manage it natively. For further information on the use of these scripts, refer to the Stormshield SSL VPN client v5 installation guide.

Certificates

Select the certificates that the SNS firewall's SSL VPN service and SSL VPN clients must present to set up SSL VPN tunnels. These certificates must be issued from the same certification authority.

By default, a server certificate and a client certificate, issued by the same certification authority dedicated to the SSL VPN, are suggested. These certificates and the certification authority were created when the SNS firewall was initialized.

Field	Description
Server certificate	Select the desired certificate. The icon indicates certificates with a TPM-protected private key. For more information on this protection, refer to the technical note Configuring the TPM and protecting private keys in SNS firewall certificates.
Client certificate	Select the desired certificate. Client certificates with a TPM-protected private key cannot be selected as the private keys of such certificates must be available in plaintext (unencrypted) in the SSL VPN configuration that is distributed to SSL VPN clients.

Configuration

Field	Description
Export the configuration file	Click on this button to export the SSL VPN configuration in OVPN format. You can then import this file into your organization's SSL VPN clients to add a new connection. As for the Stormshield VPN client, this configuration is automatically retrieved for connections that are set up in **Stormshield mode**. For OpenVPN connections (imported OVPN file), the file must be imported to set up or save the connection. For more information, refer to the Stormshield SSL VPN client v5 user and configuration guide.

Configuring client workstation verification (ZTNA)

This section explains how to configure a policy to verify the compliance of client workstations that set up SSL VPN tunnels with the SNS firewall. With this verification, workstations or users that do not comply with the criteria in the policy defined on the SNS firewall will not be able to set up SSL VPN tunnels with the SNS firewall.

You can click on **Apply** at any time to save your changes.

General information on zero trust network access (ZTNA)

ZTNA consists of trusting users and devices only after they have been verified. To do so, ZTNA can rely on the following components:

- Guaranteed compliance of the communication channel through TLS encryption of SSL VPN tunnels.
- User verification, for example through multifactor authentication, such as the Stormshield TOTP solution (see Multifactor authentication).
- A policy verifying the compliance of client workstations and users. This configuration is covered in the section below.
- Granular filtering to restrict users' access to only what is necessary (see Configuring the filter and NAT policy).

Requirements

To use a client workstation compliance verification policy, you must meet the following requirements:

- An SNS firewall in version 4.8 LTSB or 5.
- Compatible SSL VPN clients with the client workstation verification feature:
  - The Stormshield SSL VPN client in version 4.0 and higher is compatible. It must be set to **Stormshield mode** for versions 5 or **Automatic mode** for versions 4.
  - Third-party SSL VPN clients, such as OpenVPN Connect, are not compatible.

Configuring client workstation verification on SNS in version 5

Go to **Configuration** > **VPN** > **SSL VPN**. Settings for this version are configured in the **Client workstation verification (ZTNA)** and **Windows client workstation verification (ZTNA)** tabs.

Client workstation verification (ZTNA) tab

Stormshield SSL VPN client version

Select the checkbox to enable the settings section of the required versions.

Field	Description
Allow a version range (at least v4.0.0)	Select this option to allow multiple versions of the Stormshield SSL VPN client to set up SSL VPN tunnels (when there is a pool of varied Stormshield SSL VPN clients). By selecting this option: • You must enter the **Lowest version** of Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall, • You can enter the **Highest version**, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall.
Allow only one version	Select this option to exclusively allow one Stormshield SSL VPN client version. You must then enter the exact version of the Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall.

Allow tunnels to be set up for the following additional clients

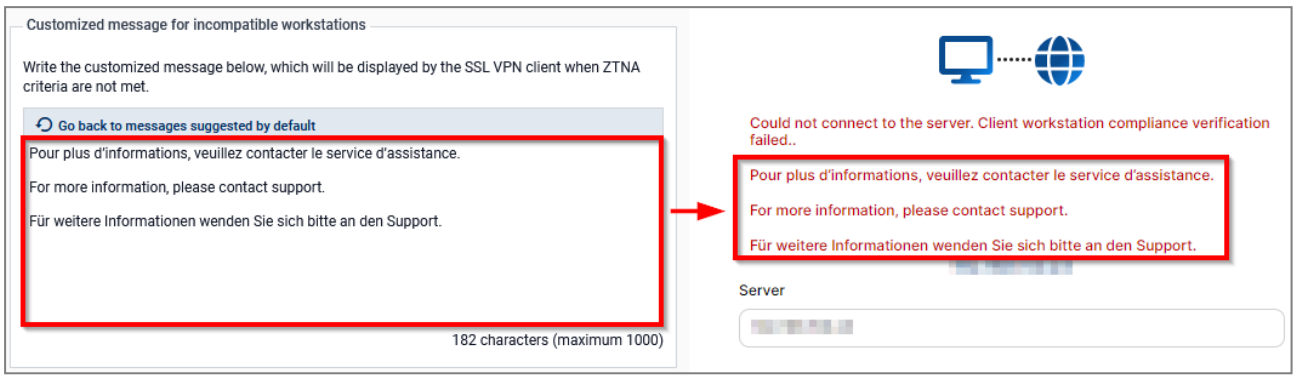
Field	Description
Stormshield SSL VPN clients (Linux or macOS)	Select the checkbox if your organization's pool of Stormshield SSL VPN clients includes Stormshield SSL VPN clients running in Linux and/or macOS. By doing so, specific Windows criteria will not be applied to these workstations.
SSL VPN clients incompatible with ZTNA	Select the checkbox to allow SSL VPN clients that are not compatible with the client workstation verification feature to set up SSL VPN tunnels with the SNS firewall, e.g., for use with mobile devices.

Customized message for incompatible workstations

If an SSL VPN tunnel fails to set up because it does not comply with the policy, the Stormshield SSL VPN Client displays the default message "*For more information, please contact support*" in English, French and German.

In the text entry section, you can change the message, or delete it if you do not wish to display an additional message. Do note that as automatic translation mechanisms have not been set up: you will need to have the message translated with your own means.

You can reset the additional message that you have written by clicking on **Go back to messages suggested by default**.



Windows client workstation verification (ZTNA) tab

IMPORTANT
If you select multiple criteria below, they must all be met to allow the SSL VPN client to set up SSL VPN tunnels with the SNS firewall.

Field	Description
Client workstation antivirus enabled and up to date	When this checkbox is selected, the workstation must be equipped with an active antivirus program **with** the latest antivirus database updates. This information is based on the status of the antivirus recognized by the Windows Security center, which means that third-party antivirus modules can be supported as long as their status is recognized. **NOTE** The Windows service that checks the status of the antivirus takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.
Active firewall on the client workstation	If this checkbox is selected, the workstation's Windows firewall must be running, and the *Domain network*, *Private network* and *Public network* profiles must be enabled. If a profile is inactive, this criterion will be considered non-compliant. **NOTE** The Windows service that checks the status of the Windows firewall takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.
SES installed on the client workstation	If this checkbox is selected, the SES Evolution agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.
Prohibit users holding administration privileges on the client workstation	When this checkbox is selected, users who hold administrator privileges on the workstation cannot set up SSL VPN tunnels with the firewall SNS.

Check the Windows 10/Windows 11 version (build number)

Select the checkbox to enable the settings section of the required Windows 10 and Windows 11 versions. Settings are configured in the tab corresponding to the version in question.

Field	Description
Allow a version range (builds)	Select this option to allow multiple versions of Windows (when there is a pool of varied Windows workstations). By selecting this option: • You must enter the **Lowest version** that the workstation must run, so that it can set up SSL VPN tunnels with the SNS firewall. The default versions are: 10000 for Windows 10 and 20000 for Windows 11. • You can enter the **Highest version**, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall.
Allow only one version	Select this option to exclusively allow one single Windows version. You must then enter the exact Windows version of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall.

Membership in a company domain

Field	Description
Ensure that the host is connected to a company domain	When this option is selected, you have to add to the grid the domains of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall. Do note that this criterion is not related to the configuration of directories on the SNS firewall.
Ensure that the user belongs to a company domain	When this option is selected, you have to add to the grid the domains of users who are allowed to set up SSL VPN tunnels with the SNS firewall. With this criterion, the user's full name, including the domain, will be verified. As such, even if the workstation is connected to a domain, local users on the workstation will not be able to set up SSL VPN tunnels. Do note that this criterion is not related to the configuration of directories on the SNS firewall.

Configuring client workstation verification on SNS in version 4.8 LTSB

Go to **Configuration > VPN > SSL VPN**. Settings are configured in the **Client workstation verification (ZTNA)** tab.

Field	Description
Enable client workstation verification (ZTNA)	Select the checkbox to enable verification of client workstation compliance. When it is enabled: • SSL VPN clients that are compatible with this feature can set up SSL VPN tunnels with the SNS firewall **only if all** the criteria defined in the policy have been met, • SSL VPN clients that are not compatible with this feature cannot set up SSL VPN tunnels with the SNS firewall, **unless** they are explicitly allowed to do so by enabling the **SSL VPN clients incompatible with ZTNA** setting.
Allow tunnels to be set up for Linux or Mac Stormshield SSL VPN clients	Select the checkbox if your organization's pool of Stormshield SSL VPN clients includes Stormshield SSL VPN clients running in Linux and/or macOS. By doing so, specific Windows criteria will not be applied to these workstations.

Field	Description
Allow tunnels to be set up for clients that are not compatible with ZTNA	Select the checkbox to allow SSL VPN clients that are not compatible with the client workstation verification feature to set up SSL VPN tunnels with the SNS firewall, e.g., for use with mobile devices.

Client workstation verification (ZTNA) settings

IMPORTANT
If you select multiple criteria below, they must all be met to allow the SSL VPN client to set up SSL VPN tunnels with the SNS firewall.

Field/Criterion	Description
Client workstation antivirus enabled and up to date	When this checkbox is selected, the workstation must be equipped with an active antivirus program **with** the latest antivirus database updates. This information is based on the status of the antivirus recognized by the Windows Security center, which means that third-party antivirus modules can be supported as long as their status is recognized. **NOTE** The Windows service that checks the status of the antivirus takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.
Active firewall on the client workstation	If this checkbox is selected, the workstation's Windows firewall must be running, and the *Domain network*, *Private network* and *Public network* profiles must be enabled. If a profile is inactive, this criterion will be considered non-compliant. **NOTE** The Windows service that checks the status of the Windows firewall takes several minutes to start up after a session is opened. Users therefore need to wait for a few minutes after opening their Windows session before they can set up an SSL VPN tunnel.
SES installed on the client workstation	If this checkbox is selected, the SES Evolution agent must be installed on the workstation. Do note that the configuration and status of the SES agent are not taken into account.
Prohibit users holding administration privileges on the client workstation	When this checkbox is selected, users who hold administrator privileges on the workstation cannot set up SSL VPN tunnels with the firewall SNS.

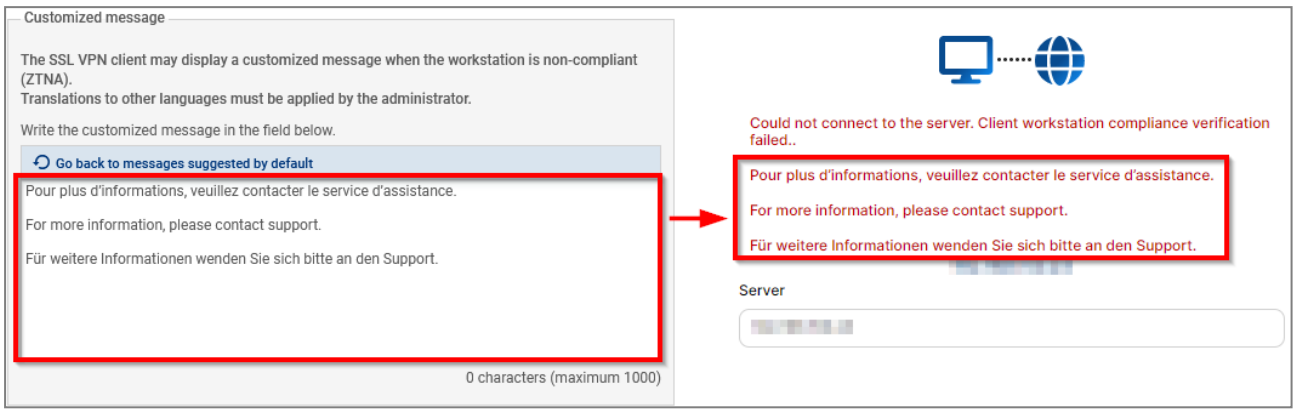
Field/Criterion	Description
Check the Windows 10/Windows 11 versions (build number)	Select the checkbox to enable the settings section of the required Windows 10 and Windows 11 versions. Settings are configured in the tab corresponding to the version in question. • **Allow a version range (builds)**: select this option to authorize several versions of Windows (case of a heterogeneous fleet of Windows workstations). By selecting this option: ◦ You must enter the **Lowest version** that the workstation must run, so that it can set up SSL VPN tunnels with the SNS firewall. The default versions are: 10000 for Windows 10 and 20000 for Windows 11. ◦ You can enter the **Highest version**, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall. • **Allow only one version**: select this option to exclusively allow one single Windows version. You must then enter the exact Windows version of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall.
Host connected to a domain tab	If **Connect the host to a company domain** is selected, in the grid, add the domains of the workstations that are allowed to set up SSL VPN tunnels with the SNS firewall. Do note that this criterion is not related to the configuration of directories on the SNS firewall.
User connected to a domain tab	If **Connect the user to a company domain** is selected, in the grid, add the domains of the users that are allowed to set up SSL VPN tunnels with the SNS firewall. With this criterion, the user's full name, including the domain, will be verified. As such, even if the workstation is connected to a domain, local users on the workstation will not be able to set up SSL VPN tunnels. Do note that this criterion is not related to the configuration of directories on the SNS firewall.
Stormshield SSL VPN client version	Select **Check Stormshield SSL VPN client version** to enable the settings section of the required versions. • **Allow a version range (builds)**: select this option to allow multiple versions of the Stormshield SSL VPN client to set up SSL VPN tunnels (when there is a pool of varied Stormshield SSL VPN clients). By selecting this option: ◦ You must enter the **Lowest version** of Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall. ◦ You can enter the **Highest version**, or leave this field empty to allow all versions equal to or higher than the lowest version to set up SSL VPN tunnels with the SNS firewall. • **Allow only one version**: select this option to exclusively allow one single Stormshield SSL VPN client version. You must then enter the exact version of the Stormshield SSL VPN clients that are allowed to set up SSL VPN tunnels with the SNS firewall.

Customized message

If an SSL VPN tunnel fails to set up because it does not comply with the policy, the Stormshield SSL VPN Client displays the default message "*For more information, please contact support*" in English, French and German.

In the text entry section, you can change the message, or delete it if you do not wish to display an additional message. Do note that as automatic translation mechanisms have not been set up: you will need to have the message translated with your own means.

You can reset the additional message that you have written by clicking on **Go back to messages suggested by default**.



Configuring the filter and NAT policy

This section explains how to configure the filter and NAT policy to be implemented in order to deploy SSL VPN tunnels. You can click on **Apply** at any time to save your changes.

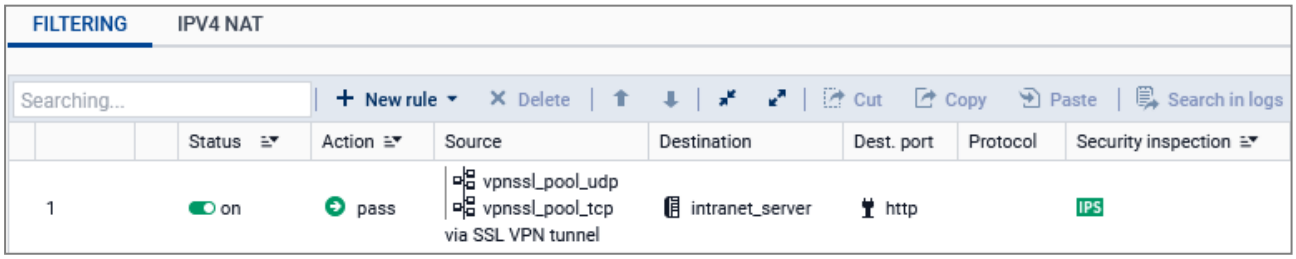
Configuring the filter policy

You need to define rules to grant or deny SSL VPN clients access to your organization's internal resources. In the example below, we are adding a rule to allow all user connections from UDP and TCP SSL VPN clients to an HTTP intranet.

To increase security, you can set up granular filtering to restrict users' access to only what is necessary. To do so, create rules for each user group that is setting up SSL VPN tunnels with the SNS firewall (in the rule editing window: **User** tab on SNS in version 5 or **Source** tab, **User** field on SNS in version 4).

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**, and double-click on the number of the rule to edit it; a new window will open.
3. In the **General** tab, **Status** field, select **On**.
4. In the **Action** tab, **Action** field, select *pass*.
5. In the **Source** tab:
   a. In the **General** tab, **Source hosts** field, select the objects that represent the IP addresses of UDP and TCP SSL VPN clients,
   b. In the **Advanced properties** sub-tab, **Via** field, select *SSL VPN tunnel*.
6. In the **Destination** tab, **Destination hosts** field, select the object that represents the internal server or the intranet.
7. In the **Port - Protocol** tab, **Destination port** field, select *https*.
8. Click on **OK**.

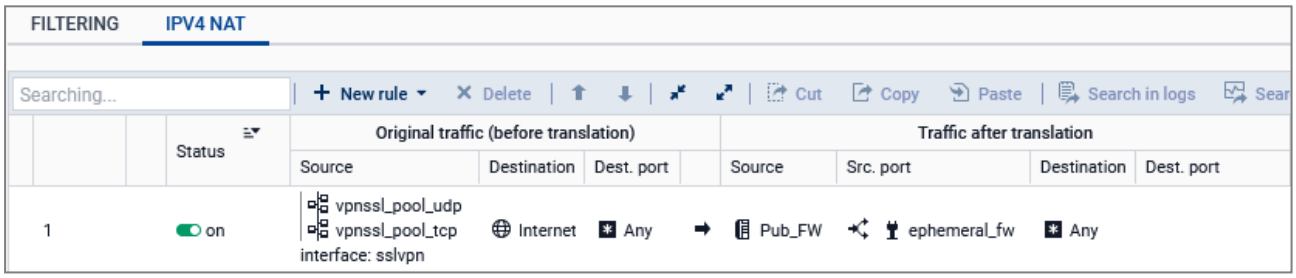
NOTE
Rules will be scanned in the order of their appearance in the list. You can also use advanced filter functions (inspection profiles, application proxies, antivirus scans, etc.).



Configuring the NAT policy

if UDP and TCP SSL VPN clients must access the Internet, you will need to set up a network address translation (NAT) rule.

1. Go to **Configuration > Security policy > Filter - NAT, NAT** tab.
2. Click on **New rule > Source address sharing rule (masquerading)**, and double-click on the number of the rule to edit it; a new window will open.
3. In the **General** tab, **Status** field, select **On**.
4. In the **Original source** tab:
   a. **Source hosts** field, select the objects that represent the IP addresses of UDP and TCP SSL VPN clients,
   b. **Incoming interface** field, select *SSL VPN*.
5. In the **Original destination** tab, **Destination hosts** field, select *Internet*.
6. In the **Translated source** tab, **Translated source host** field, select the object that represents the public IP address.
7. In the **Translated source port** field, select the option **Choose random translated source port**.
8. Click on **OK**.



Tracking connected users

This section explains how to track currently connected users, or those that are connected through the SSL VPN, from the SNS firewall web administration interface.

To improve the readability of images, some columns in tables have been hidden. As such, what you see on your SNS firewall may be slightly different. Not all of the available columns are described in this section. For more information, refer to the in the v4 user guide or v5 user guide, depending on the SNS version used.

Information on access to private data

Some information can be accessed if the user has been granted permissions to look up private data. If you hold this permission or a code to access private data:

- On SNS in version 5: click on the icon representing a user in the upper banner, then click on **Obtain personal data access**. If an access code is required, enter it and click on **Obtain**.
- On SNS in version 4: click on **Logs: restricted access** in the upper banner. If an access code is required, enter it and click on **Obtain**.

For further information, refer to the Technical note Complying with privacy regulations.

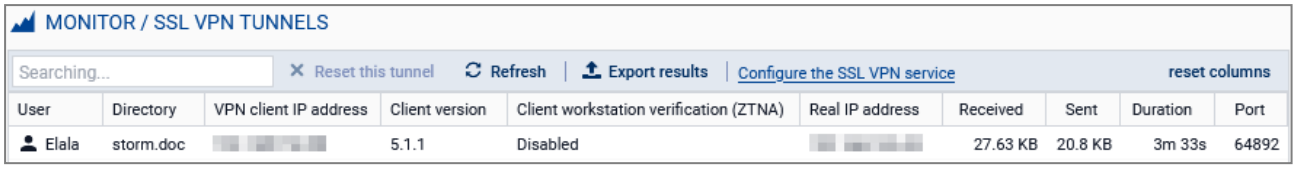
Displaying users currently connected to the SNS firewall through the SSL VPN

In SSL VPN tunnel monitoring

Go to **Monitoring > Monitoring > SSL VPN tunnels.**

This view shows which users are connected to the SNS firewall through the SSL VPN in real time, and includes session details (IP addresses, number of bytes sent and received, etc.).

Column	Description
User	Indicates the name of the user currently connected to the SNS firewall through the SSL VPN.
Client version	Indicates the version of the Stormshield SSL VPN client that was used to connect. For SSL VPN clients that are not compatible with the client workstation verification feature, the value "*N/A*" is shown. This column is available only on SNS versions 4.8 LTSB and 5.
Client workstation verification (ZTNA)	Indicates the client workstation's compliance status. There are several possible values: • **Disabled**: the client workstation verification feature has been not enabled. • **Not verified**: the SSL VPN client that was used to set up the SSL VPN tunnel is not compatible with the client workstation verification feature, but SSL VPN tunnels can be set up for incompatible clients. • **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy. This column is available only on SNS versions 4.8 LTSB and 5.

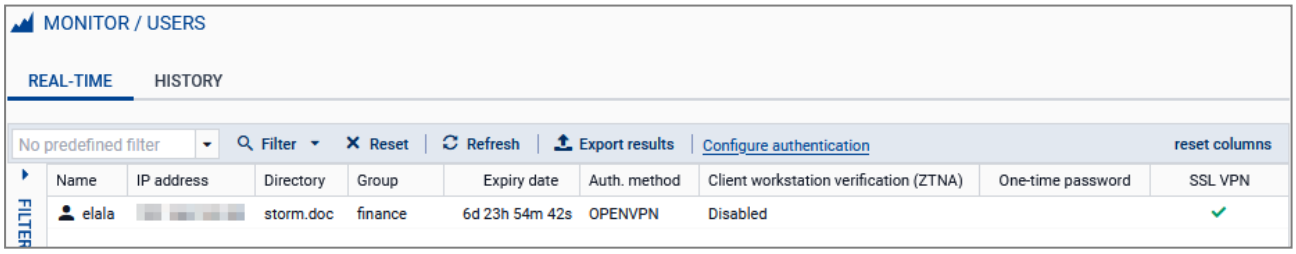


In user monitoring

Go to **Monitoring > Monitoring > Users.**

This view provides a real-time view of the users connected on the SNS firewall.

Column	Description
User	Indicates the name of the user currently connected on the SNS firewall. To find out whether the user is connected to the SNS firewall through the SSL VPN, check the "**SSL VPN**" column.
Client workstation verification (ZTNA)	Indicates the client workstation's compliance status. There are several possible values: • **Disabled**: the client workstation verification feature has been not enabled. • **Not verified**: the SSL VPN client that was used to set up the SSL VPN tunnel is not compatible with the client workstation verification feature, but SSL VPN tunnels can be set up for incompatible clients. • **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy. This column is available only on SNS versions 4.8 LTSB and 5.
One-time password	Indicates whether a user has logged in using a TOTP from the Stormshield TOTP solution. This column is available only on SNS versions 4.8 LTSB and 5.
SSL VPN	Identifies users connected on the SNS firewall through the SSL VPN.



Viewing logs on VPN tunnel events

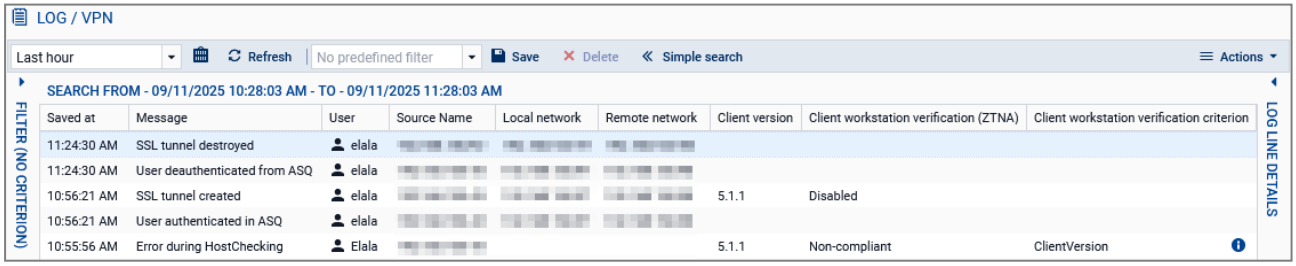
Go to **Monitoring > Logs - Audit logs > VPN.**

This log shows events relating to SSL VPN and IPsec VPN tunnels.

By default, events from the last hour are displayed. You can change the time range by selecting another value in the toolbar above the grid.

Column	Description
Saved at	Indicates the date and time of the event.

Column	Description
Message	Indicates the nature of the event: VPN tunnel connected or disconnected, user authentication in the firewall authentication engine, etc. On SNS versions 4.8 LTSB and 5, messages relating to the client workstation verification feature (*HostChecking* in the logs) may appear: • **Error during authentication: HostChecking failed** with a value of "*Unverified*" in the "**Client workstation verification (ZTNA)**" column: the connection was not set up because the SSL VPN client used is not compatible with the client workstation verification feature, and the policy does not allow SSL VPN tunnels to be set up for incompatible clients. • "*Error during HostChecking*" with a value of "*Non-compliant*" in the "**Client workstation verification (ZTNA)**" column: the connection was not set up because the client workstation does not comply with the criteria defined in the client workstation verification policy.
User	Indicates the user that is associated with the event.
Client workstation verification (ZTNA)	Indicates the client workstation's compliance status. There are several possible values: • **Disabled**: the client workstation verification feature has been not enabled. • **Not verified**: the workstation's compliance status has not been verified as the SSL VPN client used is not compatible with the client workstation verification feature. To find out whether the SSL VPN tunnel has been set up, refer to the "**Message**" column. • **Non-compliant**: the client workstation does not comply with the criteria defined in the client workstation verification policy. • **Compliant**: the client workstation complies with the criteria defined in the client workstation verification policy. This column is available only on SNS versions 4.8 LTSB and 5.
Client workstation verification criterion	Shows non-compliant criteria when an SSL VPN tunnel fails to set up due to the non-compliance of the client workstation or user. This column is available only on SNS versions 4.8 LTSB and 5.



Troubleshooting

This section lists several issues that are frequently encountered when the SSL VPN is used. If the issue you encounter cannot be found in this chapter, we recommend that you refer to the Stormshield knowledge base (authentication required).

A user is unable to log in and the message "*Client workstation compliance verification failed*" appears

- *Situation*: When a user attempts to connect, the SSL VPN tunnel fails to set up and the message "*Client workstation compliance verification failed*" appears on the user's Stormshield SSL VPN client.
- *Cause*: The client workstation that was used does not comply with all the criteria defined in the client workstation verification policy (ZTNA).
- *Solutions*:
  - Check for non-compliant criteria by referring to Viewing logs on VPN tunnel events, then rectify the compliance of the client workstation.
  - Check the configuration of the client workstation verification policy by referring to the section Configuring client workstation verification (ZTNA).

An internal resource cannot be accessed over the SSL VPN tunnel

- *Situation*: The SSL VPN tunnel has been set up, but an internal resource cannot be accessed.
- *Cause*: Either the firewall's filter policy is blocking access to this resource or the resource is no longer accessible. There may also be other causes for this situation.
- *Solutions*:
  - On the SNS firewall, temporarily enable **Advanced** logging in the rule regarding the traffic in question to collect logs (in **Configuration > Security policy > Filter - NAT > Filtering**), then in the logs, check whether the rule applies to the traffic (in **Monitoring > Logs - Audit logs > Filtering**).
  - Ensure that the requested resource is in fact physically available.
  - Clear the workstation's ARP cache by running the command `arp -d *` in a console.

A warning message indicates that LZ4 compression is obsolete

- *Situation*: In the web administration interface of an SNS firewall in version 4.8.5 or higher, if the LZ4 compression feature is enabled, a warning message automatically appears in the SSL VPN module.
- *Cause*: The LZ4 compression feature is obsolete, and we recommend disabling it
- *Solution*: In the warning window, accept the suggestion to disable the feature. If you have ignored this warning, a message will continue to be displayed until this feature is disabled. To disable it, use the following CLI serverd commands:

```
CONFIG OPENVPN UPDATE compress=0
CONFIG OPENVPN ACTIVATE
```

Further reading

For further information on installing, updating and uninstalling the Stormshield SSL VPN client, refer to the **Stormshield SSL VPN client v5 installation guide**.

To configure and use the Stormshield SSL VPN client, refer to the **Stormshield SSL VPN client v5 user and configuration guide**.

Additional information and responses to questions you may have about the Stormshield SSL VPN client are available in the **Stormshield knowledge base** (authentication required).

documentation@stormshield.eu