TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC VPN: IPSEC VIRTUAL INTERFACES - CONFIGURATION OF ANONYMOUS TUNNELS

Product concerned: SNS 4.3, SNS 4.8 and SNS 5.0

Document last updated: November 4, 2025

Reference: sns-en-IPsec_anonymous_tunnels_VTI_Technical_Note

Table of contents

Change log

Date	Description
November 4, 2025	New document

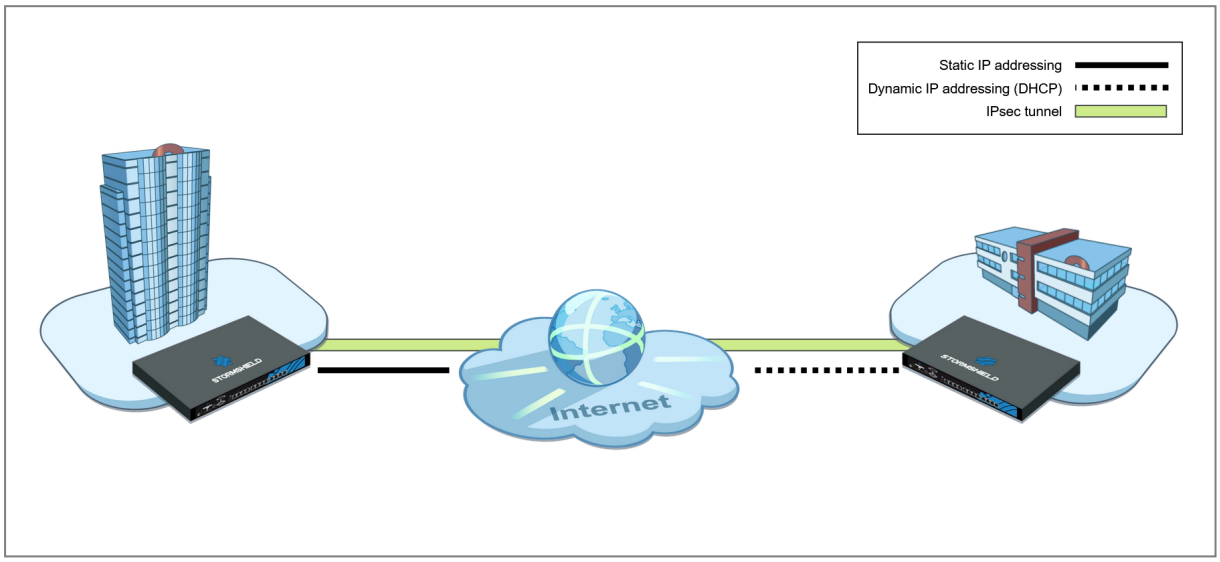
Getting started

On SNS firewalls, IPsec tunnels can be implemented based on various types of routing. Instead of information that has been defined in the Security Policy Database (SPD), routing instructions (static routing, dynamic routing or filter-based routing) now determine whether packets need to pass through these IPsec tunnels.

This technical note explains the use case of a hub and spoke architecture, in which a central site (hub) and a satellite site (spoke) implement virtual IPsec interfaces. The technical note also explains how to set up IPsec tunnels based on routing with a dynamic or anonymous peer. This peer may be a mobile unit, for example, such as an emergency service or a service provider for an event, which would be granted mobile Internet access.

Architecture presented

The main use case in this architecture presents a star topology with a central site (hub) and a satellite site (spoke). This type of architecture is not restricted to a single satellite site.



Each site is able to access the Internet:

- The central site (hub) has Internet access with a static IP address.
- The satellite site (spoke) has Internet access with a dynamic IP address.

The constraint placed by this architecture is the dynamic addressing system on the spoke site, and as such, the need to set up routed IPsec tunnels with an anonymous peer.

Requirements

This section sets out the requirements for configuring each of the firewalls in the architecture presented.

The IP addresses 198.51.100.0/24 and 203.0.113.0/24 used in this technical note to represent the firewall's public IP addresses are reserved for documentation, in line with RFC 5737.

Conditions and limitations

This use case is supported based on the following conditions and limitations:

- You are using one of the firmware versions SNS 4.3, SNS 4.8 or SNS 5
- You are using IKEv2,
- You are using DHCP.

Configuring the network and PKI

You have configured your network in advance, and if necessary your PKI (optional), to allow the various sites to communicate through their physical interfaces.

Network configuration

Network configuration on the hub:

- WAN interface: 198.51.100.1/24,
- LAN interface: 192.168.1.1/24,
- Default route: GW_default (198.51.100.254).

Network configuration on the spoke:

- WAN interface: 203.0.113.59/24 (DHCP),
- LAN interface: 192.168.2.1/24,
- Default route: Firewall_WAN_router.

PKI configuration (optional)

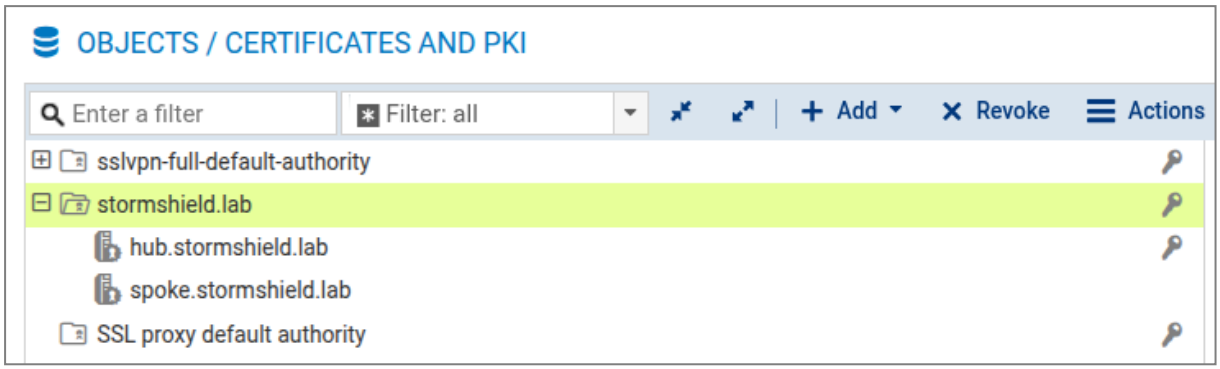
You can choose whether IPsec peers authenticate with certificates or pre-shared keys (PSK).

We recommend certificate authentication.

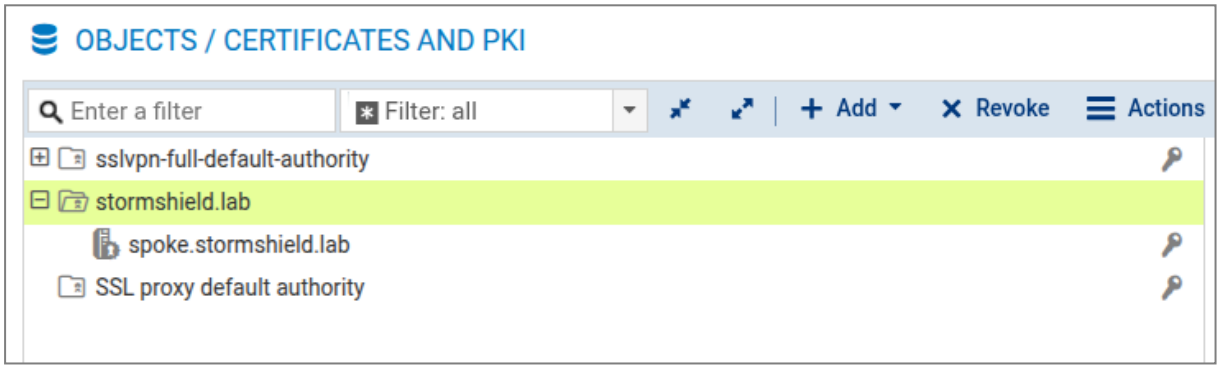
In this case, you will need to set up your PKI in advance:

- The certification authority (CA) and firewall certificates have been created on the hub,
- The CA certificate and identity of the spoke (certificate and private key) have been exported, and imported into the PKI on the spoke,
- The CA has been added to the list of trusted CAs on each of the firewalls to interlink.

PKI configuration on the hub



PKI configuration on the spoke



NOTE
For security reasons, we recommend that you delete the private key that is generated on the hub as soon as the identity (*spoke.stormshield.lab* in the example) has been exported and imported into the PKI on the spoke,

Configuring the central site (hub)

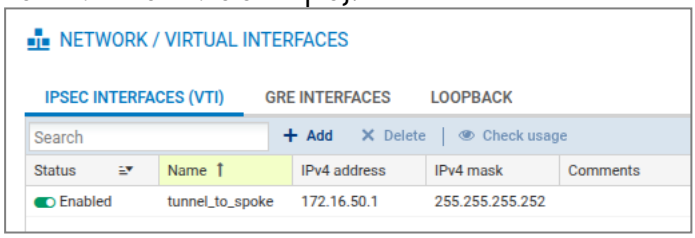
Virtual IPsec interfaces determine the tunnels through which traffic will pass.

You therefore need to create a local virtual IPsec interface that makes it possible to configure the tunnel's local and remote endpoints. In the example, this interface is named **tunnel_to_spoke**. The tunnel endpoints are defined by network objects (**VTI_local_spoke** and **VTI_remote_spoke** in the example).

Creating the local virtual IPsec interface

You will need to create the virtual IPsec interface allowing you to configure the tunnel.

1. Go to **Configuration > Network > Virtual interfaces** and select the **IPsec interfaces (VTI)** tab.
2. Click on **Add**.
3. Fill in the following fields:
   - **Name**: **tunnel_to_spoke** in the example,
   - **IP address: 172.16.50.1** in the example,
   - **Network mask**: the default value is a 255.255.255.252 mask (the mask retains its default value in the example).

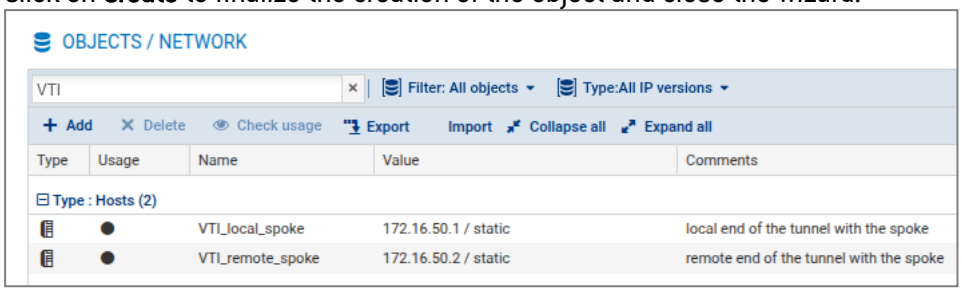


Creating the local and remote tunnel endpoints

The virtual interfaces on the spoke are configured by using network objects. These interfaces are used as gateways in router objects on the hub, and in the configuration of IPsec tunnels. You need to define network objects that correspond to local and remote tunnel endpoints on the spoke.

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add** and select **Host** from the banner on the left.
3. Configure the network object that corresponds to the local tunnel endpoint, by filling in the following fields:
   - **Object name**: **VTI_local_spoke** in the example,
   - **IPv4 address**: **172.16.50.1** in the example,
   - **MAC address**: you can indicate a MAC address,
   - **Comments**: you can enter comments.
4. Click on **Create and duplicate** to finalize the creation of the object and create the next one.
5. Configure the network object that corresponds to the remote tunnel endpoint with the values indicated below.
   - **Object name**: **VTI_remote_spoke** in the example,
   - **IPv4 address**: **172.16.50.2** in the example.

6. Click on **Create** to finalize the creation of the object and close the wizard.



Configure routing

Routing has to be configured on the hub to allow traffic to reach its destination. To do so, you will need to create a network object that corresponds to the local network on the spoke, and configure routing.

Creating network objects

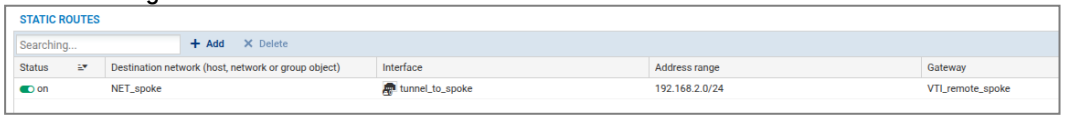
You will need to create a network object that corresponds to the local network on the spoke.

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add** and select **Network** from the banner on the left.
3. Fill in the following fields:
   - **Object name**: **NET_spoke** in the example,
   - **Network IP address**: **192.168.2.0/24** in the example,
   - **Comments**: you can add comments.
4. Click on **Create** to finalize the creation of the object and close the wizard.

Defining routing

You will need to configure the routing of traffic to the local network on the spoke.

1. Go to **Configuration > Network > Routing** and select the **IPv4 static routes** tab.
2. Click on **Add**.
3. Fill in the following fields:
   - **Destination network**: **NET_spoke** in the example,
   - **Address range**: **192.168.2.0/24** in the example,
   - **Gateway**: **VTI_remote_spoke** in the example,
   - **Comments**: you can enter comments.

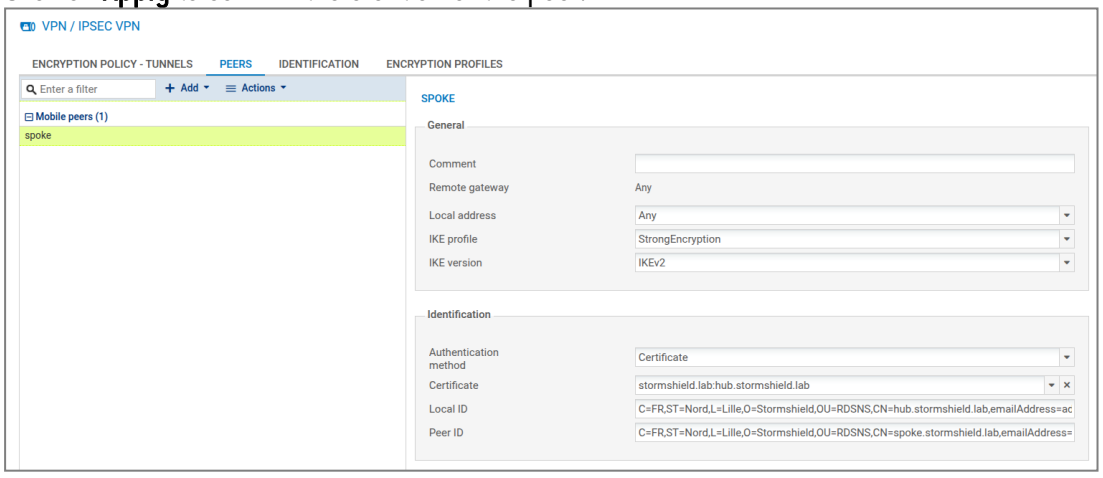


Creating the dynamic (or anonymous) IPsec peer

To allow the hub to accurately identify the spoke, you will need to create the *spoke* peer. You can create it either by using certificate authentication (recommended), or by following the pre-shared key (PSK) authentication method.

Creating the peer with certificate authentication (recommended)

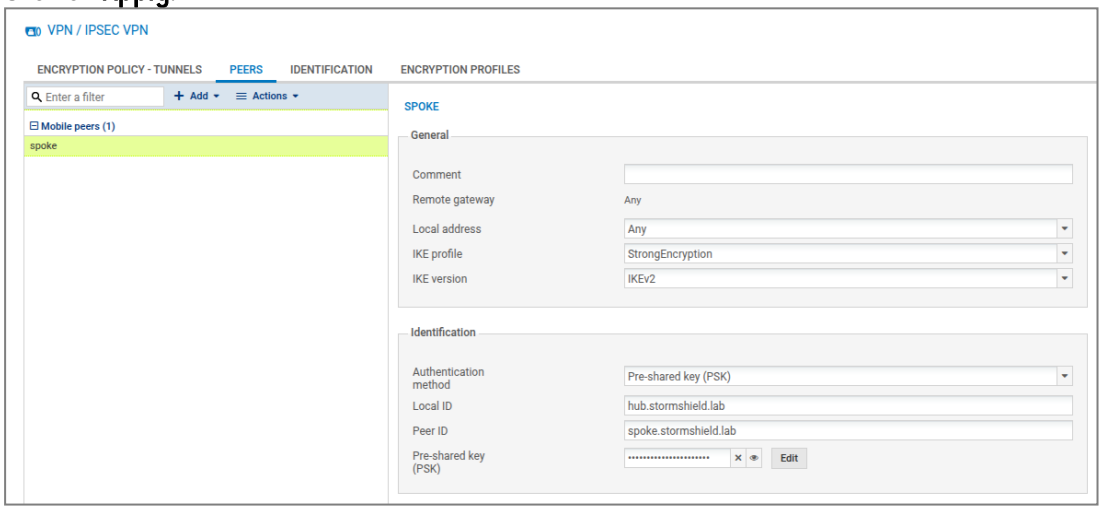
1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**.
3. Select **New mobile peer**. A wizard will appear, prompting you to select the remote gateway.
4. Select **Any**.
5. Enter the name of the peer. By default, its name has "mobile_" as a prefix, but the name can be customized (**spoke** in the example). Confirm.
6. Select **IKEv2** as the IKE version, and click on **Next**.
7. Select **Certificate** authentication.
8. In the **Certificate** drop-down menu, select the certificate that the hub will present to set up the tunnel with its mobile peer, and click on **Next**.
9. In the window that opens, providing a summary of the peer's settings, check the information, then click on **Finish**.
10. In the **Identification** section, fill in the following fields:
    - **Local ID** (optional): this is the local ID that was specified when the peer was created. If you fill in this field, you need to enter the same value in the **Peer ID** field on the spoke.
    - **Peer ID** (optional): this is the ID that was assigned to the peer. We recommend specifying it to formally identify the mobile peer, and to associate the right IPsec policy with it during the tunnel negotiation. If you fill in this field, you need to enter the same value in the **Local ID** field on the spoke.
11. Click on **Apply** to confirm the creation of the peer.



Creating the peer with pre-shared key authentication (PSK)

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**.
3. Select **New mobile peer**. A wizard will appear, prompting you to select the remote gateway.
4. Select **Any**.
5. By default, the name of the peer will be created by adding a prefix “mobile_” to the object name, but this name can be customized (**spoke** in the example). Confirm.
6. Select the **pre-shared key (PSK)** as the authentication method.

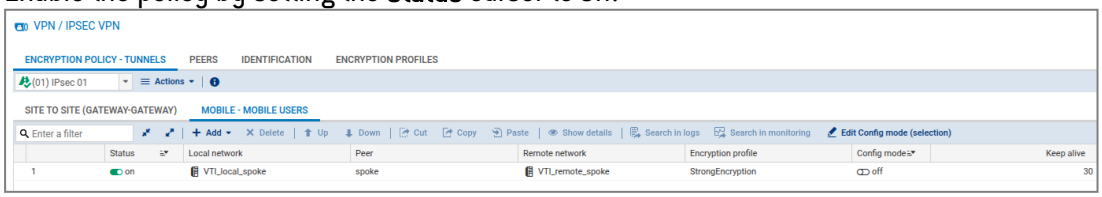
7. In the **Identification** section, fill in the following fields:
   - **Local ID** (optional): this is the local ID that was specified when the peer was created. If you fill in this field, you need to enter the same value in the **Peer ID** field on the spoke.
   - **Peer ID** (optional): this is the ID that was assigned to the peer. We recommend specifying it to formally identify the peer, and to associate the right IPsec policy with it during the tunnel negotiation. If you fill in this field, you need to enter the same value in the **Local ID** field on the spoke.
   - **Pre-shared key**: click on **Edit** and in the fields **Pre-shared key** and **Confirm**, enter a complex key that will be exchanged between the hub and spoke to set up the IPsec tunnel.
     To define a sufficiently secure pre-shared key:
     - Keep to a minimum length of 15 characters,
     - Use uppercase and lowercase letters, numbers and special characters,
     - Do not use a word that can be found in a dictionary.
8. Click on **Apply**.



Configuring the IPsec VPN policy

You will need to define the rules of the encryption policy to be applied to traffic.

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Mobile – Mobile users** tab.
2. Click on **Add**, and then select **New single mobile policy**.
3. Select **spoke** as the **Peer selection**.
4. In the **Local network** field, select the object **VTI_local_spoke**.
5. In the **Remote network** field, select the object **VTI_remote_spoke**.
6. Enable the policy by setting the **Status** cursor to *On*.



You have completed the configuration of the hub, and can now proceed to the configuration of the spoke.

Configuring the satellite site (spoke)

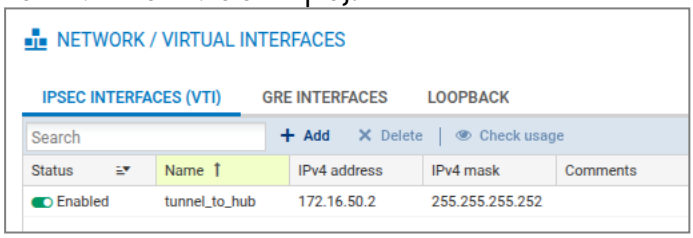
Virtual IPsec interfaces determine the tunnels through which traffic will pass.

You therefore need to create a local virtual IPsec interface that makes it possible to configure the tunnel's local and remote endpoints. In the example, this interface is named **tunnel_to_hub**. The tunnel endpoints are defined by network objects (**VTI_local_hub** and **VTI_remote_hub** in the example).

Creating the local virtual IPsec interface

You will need to create the virtual IPsec interface allowing you to configure the tunnel.

1. Go to **Configuration > Network > Virtual interfaces** and select the **IPsec interfaces (VTI)** tab.
2. Click on **Add**.
3. Fill in the following fields:
   - **Name**: **tunnel_to_hub** in the example,
   - **IP address: 172.16.50.2** in the example,
   - **Network mask**: the default value is a 255.255.255.252 mask (the mask retains its default value in the example).

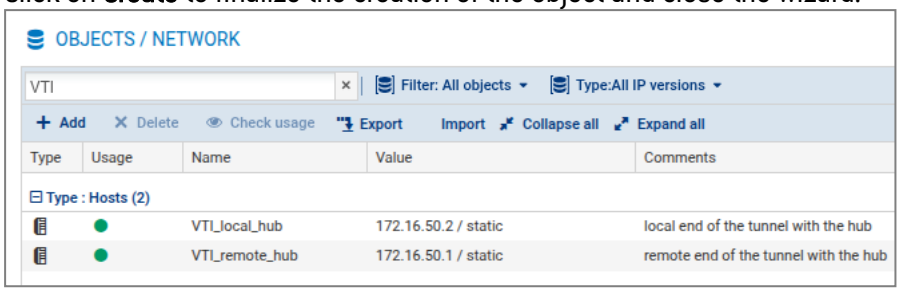


Creating the local and remote tunnel endpoints

The virtual interfaces on the hub are configured by using network objects. These interfaces are used as gateways in router objects on the spoke, and in the configuration of IPsec tunnels. You need to define network objects that correspond to local and remote tunnel endpoints on the hub.

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add** and select **Host** from the banner on the left.
3. Configure the network object that corresponds to the local tunnel endpoint, by filling in the following fields:
   - **Object name**: **VTI_local_hub** in the example,
   - **IPv4 address**: **172.16.50.2** in the example,
   - **MAC address**: you can indicate a MAC address,
   - **Comments**: you can enter comments.
4. Click on **Create and duplicate** to finalize the creation of the object and create the next one.
5. Configure the network object that corresponds to the remote tunnel endpoint with the values indicated below.
   - **Object name**: **VTI_remote_hub** in the example,
   - **IPv4 address**: **172.16.50.1** in the example.

6. Click on **Create** to finalize the creation of the object and close the wizard.



Configure routing

Routing has to be configured on the spoke to allow traffic to reach its destination. To do so, you will need to create a network object that corresponds to the local network on the hub, and configure routing.

Creating network objects

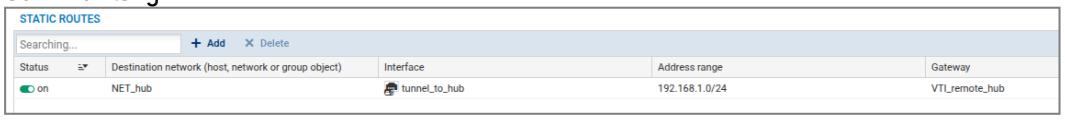
You will need to create a network object that corresponds to the local network on the hub.

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add** and select **Network** from the banner on the left.
3. Fill in the following fields:
   - **Object name**: **NET_hub** in the example,
   - **Network IP address**: **192.168.1.0/24** in the example,
   - **Comments**: you can add comments.
4. Click on **Create** to finalize the creation of the object and close the wizard.

Defining routing

You will need to configure the routing of traffic to the local network on the hub.

1. Go to **Configuration > Network > Routing** and select the **IPv4 static routes** tab.
2. Click on **Add**.
3. Fill in the following fields:
   - **Destination network**: **NET_hub** in the example,
   - **Address range**: **192.168.1.0/24** in the example,
   - **Gateway**: **VTI_remote_hub** in the example,
   - **Comments**: you can enter comments.



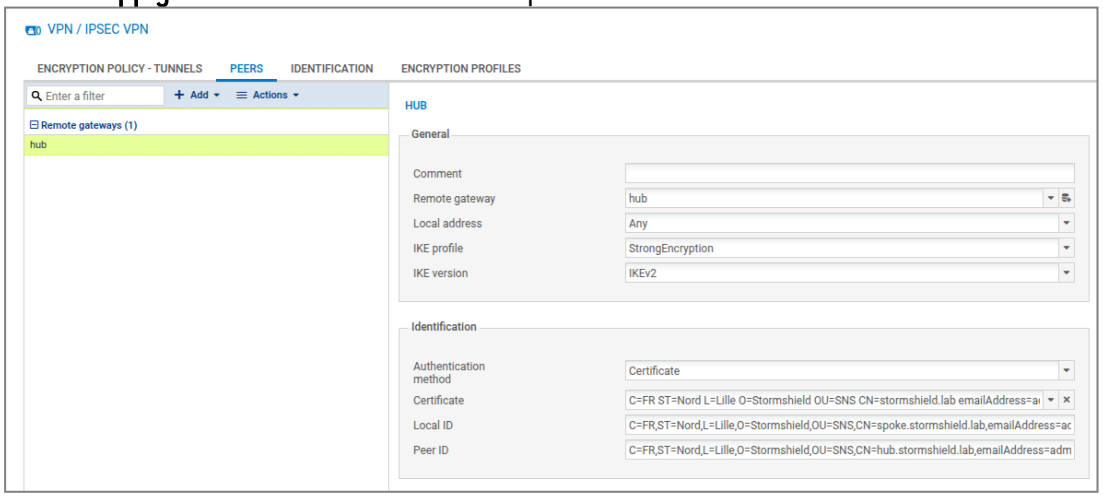
Creating the IPsec peer

To allow the spoke to accurately identify the hub, you will need to create the *hub* peer. You can create it either by using certificate authentication (recommended), or by following the pre-shared key (PSK) authentication method.

NOTE
The local address used has to be "any" so that the IKE service can adapt whenever the network configuration is reloaded (change in routing, renewal of the DHCP lease, etc.).

Creating the peer with certificate authentication (recommended)

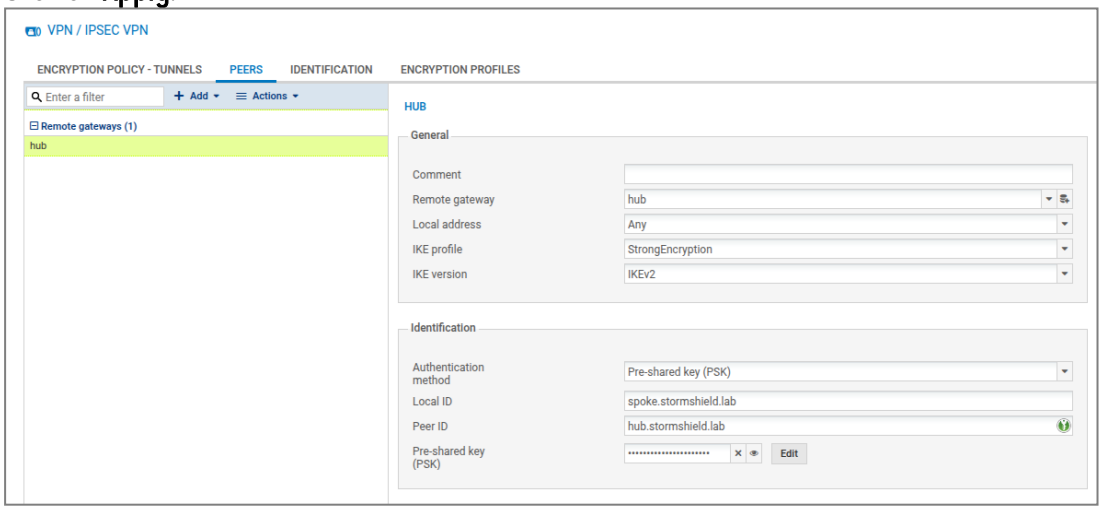
1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**.
3. Select **New remote gateway**. A wizard will appear, prompting you to select the remote gateway.
4. Select **hub**.
5. Enter the name of the peer. By default, its name has "Site_" as a prefix, but the name can be customized (**hub** in the example). Confirm.
6. Select **IKEv2** as the IKE version, and click on **Next**.
7. Select **Certificate** authentication.
8. In the **Certificate** drop-down menu, select the certificate that the spoke will present to set up the tunnel with its peer, and click on **Next**.
9. In the window that opens, providing a summary of the peer's settings, check the information, then click on **Finish**.
10. In the **Identification** section, fill in the following fields:
    - **Local ID** (optional): this is the local ID that was specified when the peer was created. If you fill in this field, you need to enter the same value in the **Peer ID** field on the hub.
    - **Peer ID** (optional): this is the ID that was assigned to the peer. We recommend specifying it to formally identify the mobile peer, and to associate the right IPsec policy with it during the tunnel negotiation. If you fill in this field, you need to enter the same value in the **Local ID** field on the hub.
11. Click on **Apply** to confirm the creation of the peer.



Creating the peer with pre-shared key authentication (PSK)

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**.

3. Select **New remote gateway**. A wizard will appear, prompting you to select the remote gateway.
4. Select the object **hub**.
5. By default, the name of the peer will be created by adding a prefix "Site_" to the object name, but this name can be customized (**hub** in the example). Confirm.
6. Select **IKEv2** as the IKE version, and click on **Next**.
7. Select the **pre-shared key (PSK)** as the authentication method.
8. In the **Identification** section, fill in the following fields:
   - **Local ID** (optional): this is the local ID that was specified when the peer was created. If you fill in this field, you need to enter the same value in the **Peer ID** field on the hub.
   - **Peer ID** (optional): this is the ID that was assigned to the peer. We recommend specifying it to formally identify the peer, and to associate the right IPsec policy with it during the tunnel negotiation. If you fill in this field, you need to enter the same value in the **Local ID** field on the hub.
   - **Pre-shared key**: click on **Edit** and in the fields **Pre-shared key** and **Confirm**, enter a complex key that will be exchanged between the hub and spoke to set up the IPsec tunnel.
     To define a sufficiently secure pre-shared key:
     - Keep to a minimum length of 15 characters,
     - Use uppercase and lowercase letters, numbers and special characters,
     - Do not use a word that can be found in a dictionary.
9. Click on **Apply**.

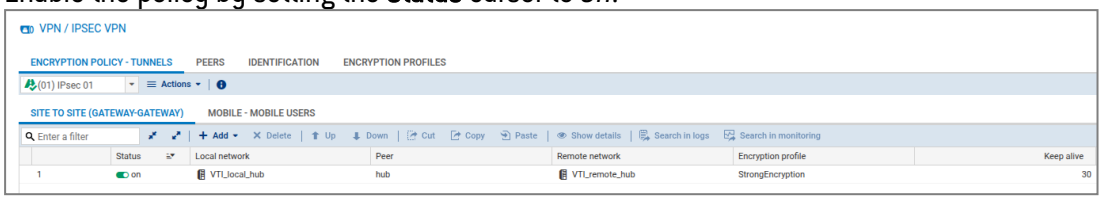


Configuring the IPsec policy

You will need to define the rules of the encryption policy to be applied to traffic.

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Site-to-site** tab.
2. Click on **Add**, then select **Standard site-to-site tunnel.**
3. Select **hub** as the **Peer selection**.
4. In the **Local network** field, select the object **VTI_local_hub**.
5. In the **Remote network** field, select the object **VTI_remote_hub**.

6. Enable the policy by setting the **Status** cursor to *On*.



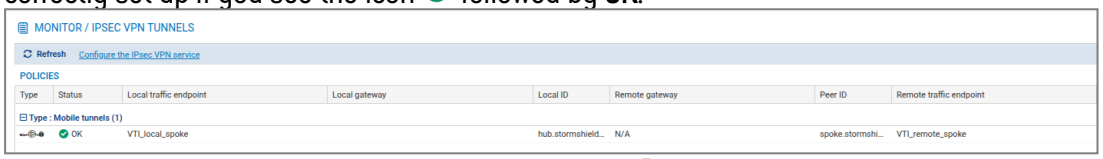
You have completed the configuration of the spoke, and can now proceed to checking the setup of the tunnels.

Verifying tunnel setup

You can check whether tunnels have been set up from the firewall's web administration interface.

Verifying tunnel setup on the hub

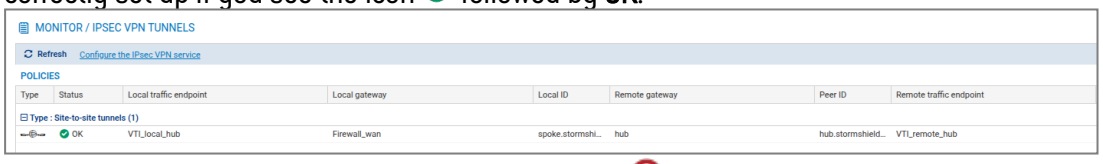
1. Go to **Monitoring > Monitoring > IPSec VPN tunnels.**
2. In the **Status** column, check the status of the tunnel: you will know that the tunnel has been correctly set up if you see the icon followed by **OK**.



If an issue occurred, it will be indicated with the icon followed by **No tunnels**. You can find out more information on the issue encountered by scrolling over the status.

Verifying tunnel setup on the spoke

1. Go to **Monitoring > Monitoring > IPSec VPN tunnels.**
2. In the **Status** column, check the status of the tunnel: you will know that the tunnel has been correctly set up if you see the icon followed by **OK**.



If an issue occurred, it will be indicated with the icon followed by **No tunnels**. You can find out more information on the issue encountered by scrolling over the status.

Further reading

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

documentation@stormshield.eu