STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

LEVEL 2 ENCAPSULATION

Product concerned: SNS 4.x

Document last updated: March 22, 2021

Reference: sns-en-level_2_encapsulation_technical_note

Table of contents

Getting started

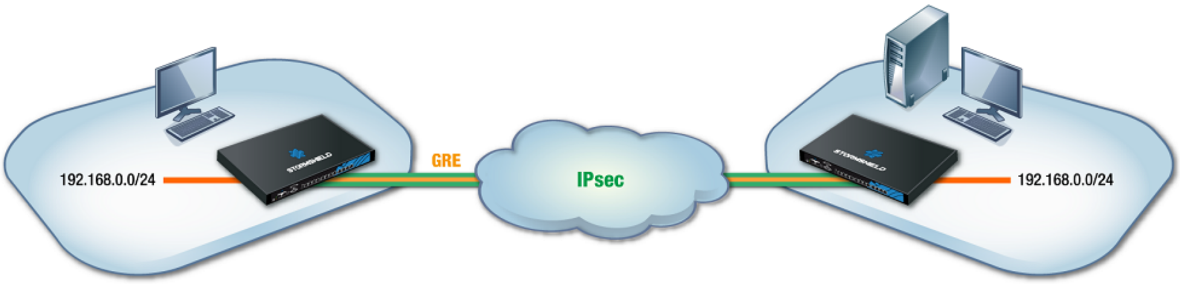
SNS firewalls can encapsulate level 2 traffic in GRE (Generic Routing Encapsulation) tunnels that rely on GRETAP interfaces. Since GRE tunnels are not natively encrypted, we strongly recommend that you secure communications by making GRE traffic go through IPsec.

By using GRE tunnels based on GRETAP interfaces, sites presenting the same address plan can be linked through a bridge. DHCP services can be shared between both sites in this way. This type of tunnel also makes it possible to transport shared VLANs between two sites, with or without filtering on these VLANs.

IMPORTANT
GRE tunnels can only be used with IPv4 in GRE over IPv4. The use of IPv6 packets in GRE tunnels, or of GRE tunnels encapsulated in IPv6, is not supported.

Architectures presented

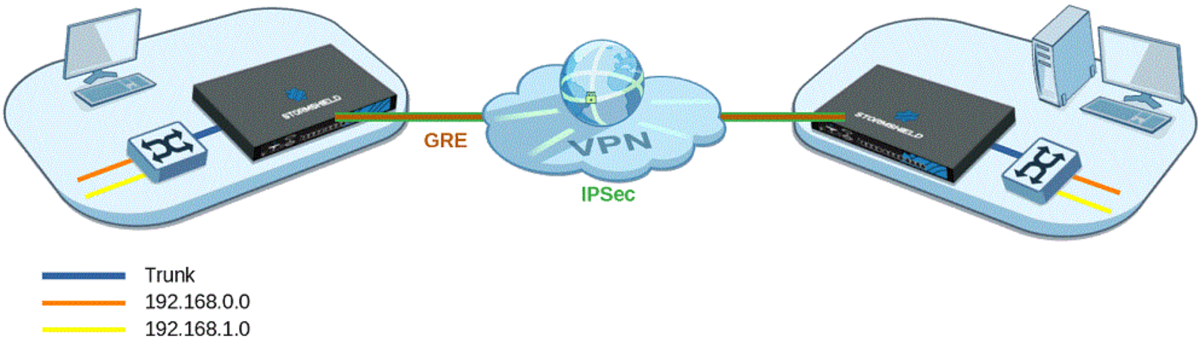
Scenario 1: joining two sites that share the same address plan



This section shows the scenario in which an organization uses a bridge to link two sites that share the same address plan. Services such as DHCP, for example, and shared network resources will therefore be treated as local services, regardless of which site the user is on. To secure such exchanges, GRE traffic will be encrypted in an IPsec tunnel.

> **NOTE**
> The IP addresses assigned to devices on both sites must of course be unique.

Scenario 2: transporting several VLANs through a GRE tunnel without inter-VLAN filtering/routing



This section shows the scenario in which an organization shares several VLANs between two sites through a GRE tunnel secured by encryption (IPsec).
This configuration **allows inter-VLAN communications through the GRE tunnel**.

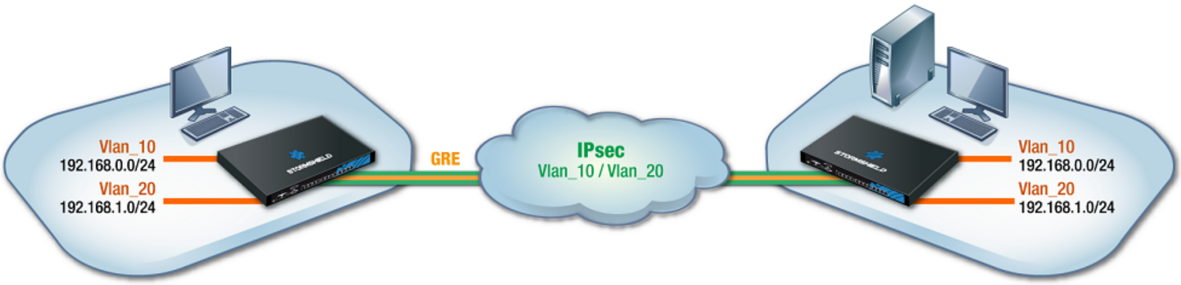
In this architecture, VLANs are not declared on firewalls – no specific operations that rely on VLAN interfaces can therefore be applied, and all VLANs are implicitly allowed to go through the GRE tunnel.
The firewall only knows the IP networks associated with VLANs, and these networks may be specifically filtered, for example.

Level 3 switches located on the LANs of each site route traffic. In this configuration, the link between firewalls and switches is a trunk link, and all VLAN tags are sent back through the tunnel.

We will cover the creation of GRETAP interfaces and the configuration of physical interfaces associated with GRETAP interfaces (advanced settings **Keep VLAN IDs** and **Keep initial routing**), as well as the creation of the IPsec tunnel.

> **IMPORTANT**
> If your configuration requires specific filtering to be applied to VLANs before going through the GRE tunnel, refer to Scenario 3.
> Do note that this scenario can be applied to architectures that contain more than two firewalls (star configuration), but can never apply to a full mesh topology.

Scenario 3: transporting VLANs through a GRE tunnel with VLAN filtering



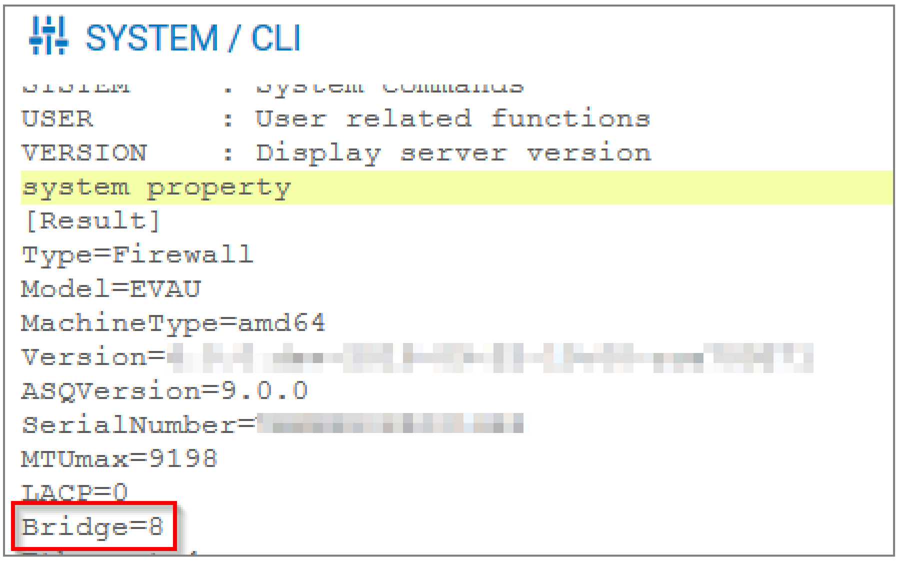
This section shows the scenario in which an organization shares two VLANs between two sites through a GRE tunnel secured by encryption (IPsec).
This architecture **does not allow inter-VLAN communications through the GRE tunnel**.

It covers the specific configurations of GRETAP interfaces, IPsec tunnels, VLAN settings and their connection to GRETAP interfaces.

Associating a bridge to each VLAN makes it possible to filter VLANs through the tunnel – only VLANs declared on firewalls are allowed to go through the tunnel.

> **IMPORTANT**
>
> - This configuration generates routing between the VLANs transported through the tunnel and if the machines from both VLANs attempt to communicate with one another through the tunnel, the firewall hosting the GRE tunnel will detect IP spoofing.
>   If your configuration requires inter-VLAN communication, refer to Scenario 2.
> - As a bridge is used for each transported VLAN, ensure that the firewall supports the number of bridges planned.

The `system property` command (**Configuration** > **System** > **CLI** module) makes it possible to identify the number of bridges that the firewall supports:



```
SYSTEM       : System commands
USER         : User related functions
VERSION      : Display server version
system property
[Result]
Type=Firewall
Model=EVAU
MachineType=amd64
Version=[redacted]
ASQVersion=9.0.0
SerialNumber=[redacted]
MTUmax=9198
LACP=0
Bridge=8
```

Scenario 1: joining two sites that share the same address plan

Creating the GRETAP interface

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **Network** > **Interfaces**:

1. Click on **Add**.
2. Select **GRETAP interface**.
   The configuration window of the interface appears.
3. In **General configuration** > **General settings**:
   - Assign a **Name** to the GRETAP interface (*gretap_FW* in the example).
   - In the **This interface is** field, select **Internal (protected)**.
4. In the **General configuration** tab > **GRETAP tunnel addresses**:
   - **Tunnel source**: select the physical interface that GRE traffic will pass through on its way out of the firewall. In the example shown, this will be the **Firewall_out** interface.
   - **Tunnel destination**: select an object bearing the public IP address of the remote firewall (**Remote_FW** in the example).
5. In **General configuration** > **Address range**:
   - Select **Address range inherited from the bridge**,
   - Next, select the **Bridge** to which the interface must be connected.
     This can be a bridge generated by the default configuration or a bridge created for this purpose.

> **NOTES**
>
> - I Bridges cannot be created in the GRETAP interface creation wizard.
> - It is possible to not select any bridge for the GRETAP interface by forcing the status of the interface to OFF. The interface can then be enabled later by moving it to a bridge.

6. Click on **Apply** to confirm the creation of the GRETAP interface.

Creating the IPsec tunnel

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

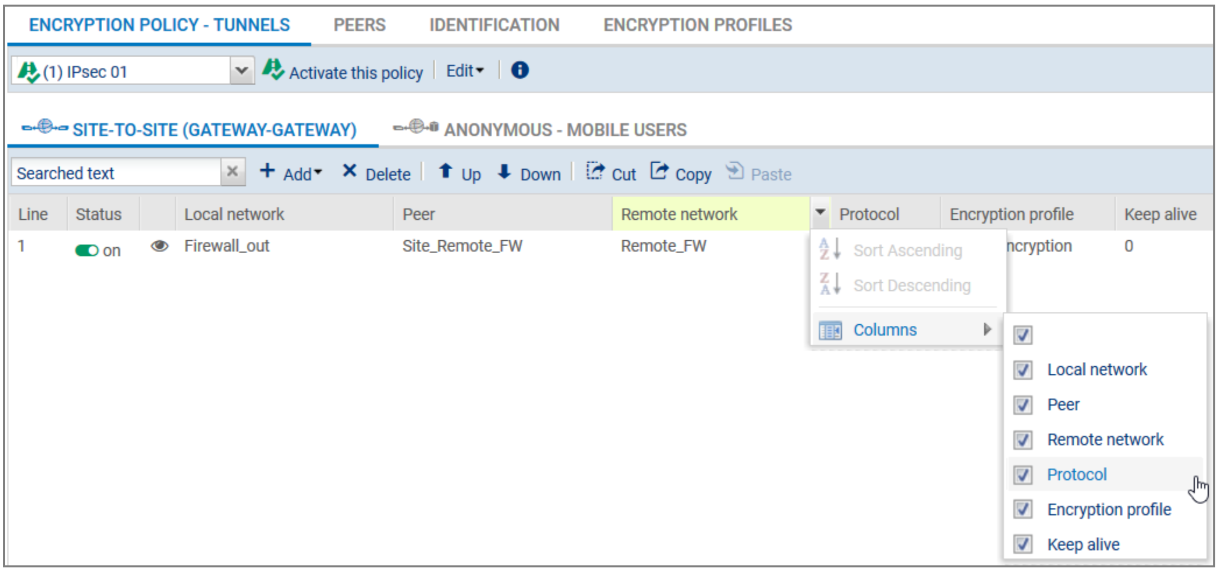
1. Click on **Add**.
2. Select **Site-to-site tunnel**.
3. For the **Local network** field: select the physical interface that hosts the GRE tunnel (**Firewall_out** in the example).
4. For the **Remote network** field: select an object bearing the public IP address of the remote firewall (**Remote_FW** in the example).
5. For the **Peer selection** field: create (or select if it already exists) a peer with a remote

gateway that will be an object bearing the public IP address of remote firewall.

6. Click on **Finish**.

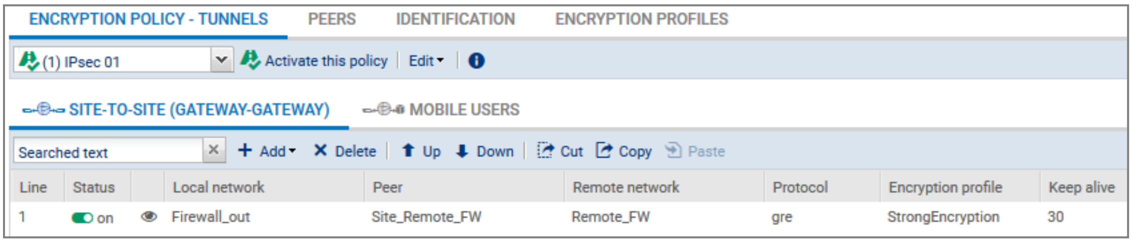
> **NOTES**
> For more details on creating peers that use pre-shared key or certificate-based authentication, refer to IPsec VPN - Authentication by pre-shared key and IPsec VPN - Authentication by certificate.
>
> The version of the IKE protocol for this peer must be the same as:
>
> - The version used on the remote firewall,
> - The version on peers used in the other rules of the IPsec policy in question.

7. To prevent IPsec tunnels from being set up for protocols other than GRE, and to prevent the encryption of traffic such as ICMP (pings), we recommend that you specify the GRE protocol in the **Protocol** column.
   If this column does not appear, scroll over the title of any column and expand the right-click menu by clicking on the arrow. Click on **Column** then select the **Protocols** checkbox.



Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on	👁	Firewall_out	Site_Remote_FW	Remote_FW		ncryption	0

The IPsec VPN policy will then look like this:



Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on	👁	Firewall_out	Site_Remote_FW	Remote_FW	gre	StrongEncryption	30

> **NOTE**
> Since the firewall started sending GRE network packets, filter rules therefore do not need to be created for this protocol.

Verifying tunnels

GRE tunnels

To check whether the unencrypted GRE tunnel is functioning between both firewalls:

1. Disable the IPsec rule on each site by turning it **off.**
2. Activate the IPsec policy.
3. From a workstation on the local network of site A, ping a host located on the local network of site B.
   This host should respond to requests.

Encrypted GRE tunnel in an IPsec tunnel

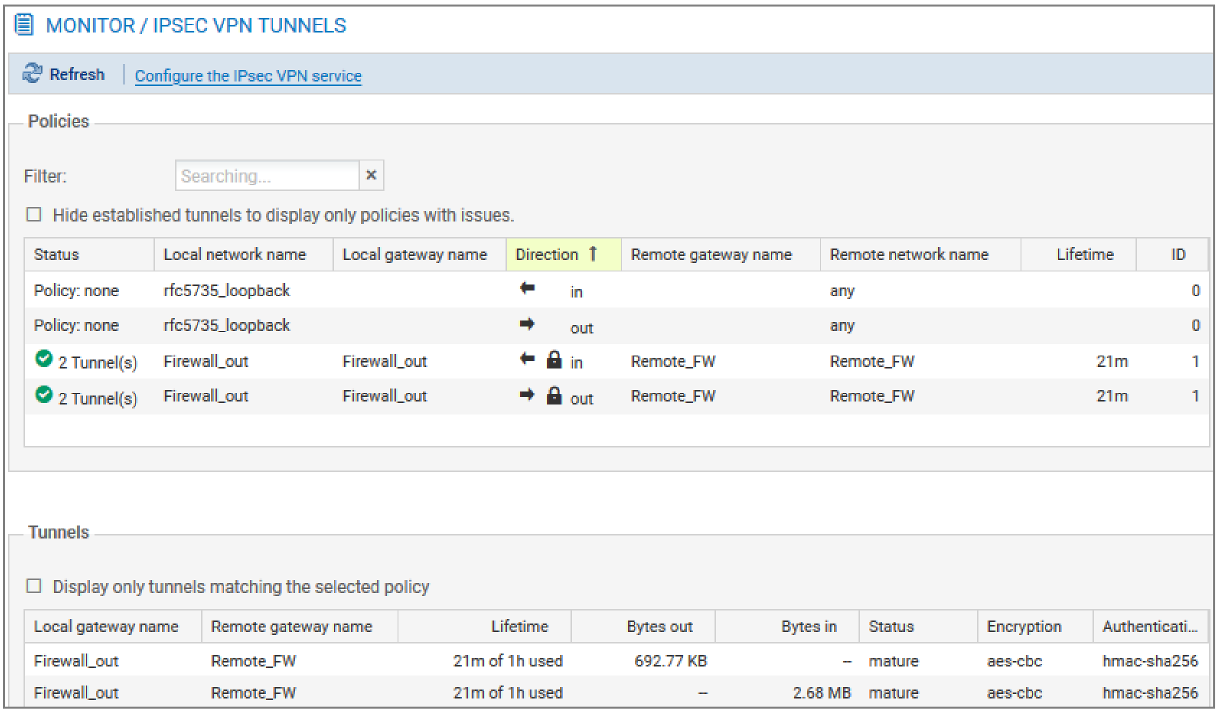
On each firewall:

1. Enable the IPsec rule by turning it **on**:
2. Activate the IPsec policy.
3. From a workstation on the local network of site A, ping from a host located on the local network of site B.
   This host should respond to requests.

Verification from the web interface on firewalls

In the firewall web administration interface, click on **Monitoring** > **IPsec VPN tunnel monitoring**. The window displays tunnels that have been set up as well as details about these tunnels:

- Name of the tunnel's local endpoint,
- Name of the tunnel's remote endpoint,
- Lifetime,
- Bytes in,
- Bytes out,
- Status of the tunnel,
- Encryption algorithm used,
- Authentication algorithm used.



MONITOR / IPSEC VPN TUNNELS

Refresh | Configure the IPsec VPN service

Policies

Filter: Searching...

□ Hide established tunnels to display only policies with issues.

Status	Local network name	Local gateway name	Direction	Remote gateway name	Remote network name	Lifetime	ID
Policy: none	rfc5735_loopback		← in		any		0
Policy: none	rfc5735_loopback		→ out		any		0
✓ 2 Tunnel(s)	Firewall_out	Firewall_out	← 🔒 in	Remote_FW	Remote_FW	21m	1
✓ 2 Tunnel(s)	Firewall_out	Firewall_out	→ 🔒 out	Remote_FW	Remote_FW	21m	1

Tunnels

□ Display only tunnels matching the selected policy

Local gateway name	Remote gateway name	Lifetime	Bytes out	Bytes in	Status	Encryption	Authenticati...
Firewall_out	Remote_FW	21m of 1h used	692.77 KB	–	mature	aes-cbc	hmac-sha256
Firewall_out	Remote_FW	21m of 1h used	–	2.68 MB	mature	aes-cbc	hmac-sha256

Logs about the setup of the IPsec tunnel can be looked up in the **Monitoring** > **Logs - Audit logs** > **VPN** tab.

Scenario 2: transporting VLANs through a GRE tunnel with delegated inter-VLAN routing

Before you start this configuration, do note that this configuration does not make it possible to filter by VLANs transported through the GRE tunnel. If your configuration requires VLAN filtering, refer to Scenario 3.

Getting started

To set up the suggested infrastructure, each firewall that participates in the GRETAP/IPsec tunnel must be configured in five steps:

- Create the bridge dedicated to the GRETAP interface,
- Choose and verify the additional settings of the physical interface that will be associated with the GRETAP interface (*in* interface in this example).
- Create and configure the GRETAP interface,
- Group both of these interfaces in a bridge dedicated to the GRETAP tunnel,
- Set the IPsec tunnel.

Creating the bridge for the GRETAP interface

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **Network** > **Interfaces**:

1. Click on **Add**, then select **Bridge** > **No members**.
   A bridge named *new_bridge1* by default is created.
   This name can be changed later.
2. In **General configuration** > **Address range**, depending on your network configuration, select **Dynamic IP (obtained by DHCP)** or **Fixed IP** to assign to the bridge an IP address in the network that has access to the internet.
3. Click on **Apply**.
4. Confirm by clicking on **Save**.

Creating and activating a GRETAP interface

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **Network** > **Interfaces**:

1. Click on **Add**.
2. Select **GRETAP interface**.
   The configuration window of the interface appears.
3. Go to the **General configuration** tab.
4. In the **Status** section, put the cursor on **ON**.
5. In **General settings** > **Name** field, name the GRETAP interface (*GretapVLAN* in the example).
6. In **General settings** > **This interface is** field, select **External (public)**.
7. In **GRETAP tunnel addresses** > **Tunnel source** field: select the physical interface that GRE traffic will pass through on its way out of the firewall to go through the IPsec tunnel.
   In the example shown, this will be the **Firewall_out** interface.
8. In **GRETAP tunnel addresses** > **Tunnel destination** field: select (or create) an object with the public IP address of the remote firewall (**Remote_FW** in the example).

9. In **Address range** > **Address range** field, select **Address range inherited from the bridge**.
10. In **Address range** > **Bridge** field, select the bridge created earlier (*new_bridge1* in the example).
    The interface is automatically placed in the bridge *new_bridge1*.
11. Go to the **Advanced properties** tab.
12. In **Routing by interface**, select **Keep initial routing**.
    A **Keep VLAN IDs** check box appears. Select it.
13. Click on **Apply**, then **Save** to confirm the creation of the GRETAP interface.

Changing the settings of the traffic's source physical interface and moving it to the bridge

On each firewall that is part of the GRETAP tunnel:

1. In the **Configuration** > **Network** > **Interfaces** module, double-click on the source physical interface of the traffic that needs to go through the tunnel.
   In the example shown, this will be the **in** interface.
2. In **General settings** > **This interface is** field, select **External (public)**.
3. In **Address range** > **Address range** field, select **Address range inherited from the bridge**.
4. In **Address range** > **Bridge** field, select the bridge created earlier (*new_bridge1* in the example).
   The interface is automatically moved to the bridge *new_bridge1*.
5. Go to the **Advanced properties** tab.
6. In **Routing by interface**, select **Keep initial routing**.
   A **Keep VLAN IDs** check box appears. Select it.
7. Click on **Apply** to confirm the creation of the GRETAP interface.

Renaming the bridge (optional)

If you wish to change the name of the bridge in which the GRETAP interface was placed, in **Configuration > Network > Interfaces**, double-click on this bridge (*new_bridge1* in this example):

1. In **General configuration > General settings > Name** field, give the bridge a name (*gretap_bridge* in the example).
2. Click on **Apply** then on **Save**.

Creating the IPsec tunnel

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

1. Click on **Add**.
2. Select **Site-to-site tunnel**.
3. For the **Local network** field: select the physical interface that hosts the GRE tunnel (**Firewall_out** in the example).
4. For the **Remote network** field: select an object bearing the public IP address of the remote firewall (**Remote_FW** in the example).
5. For the **Peer selection** field: create (or select if it already exists) a peer with a remote gateway that will be an object bearing the public IP address of remote firewall.
6. Click on **Finish**.

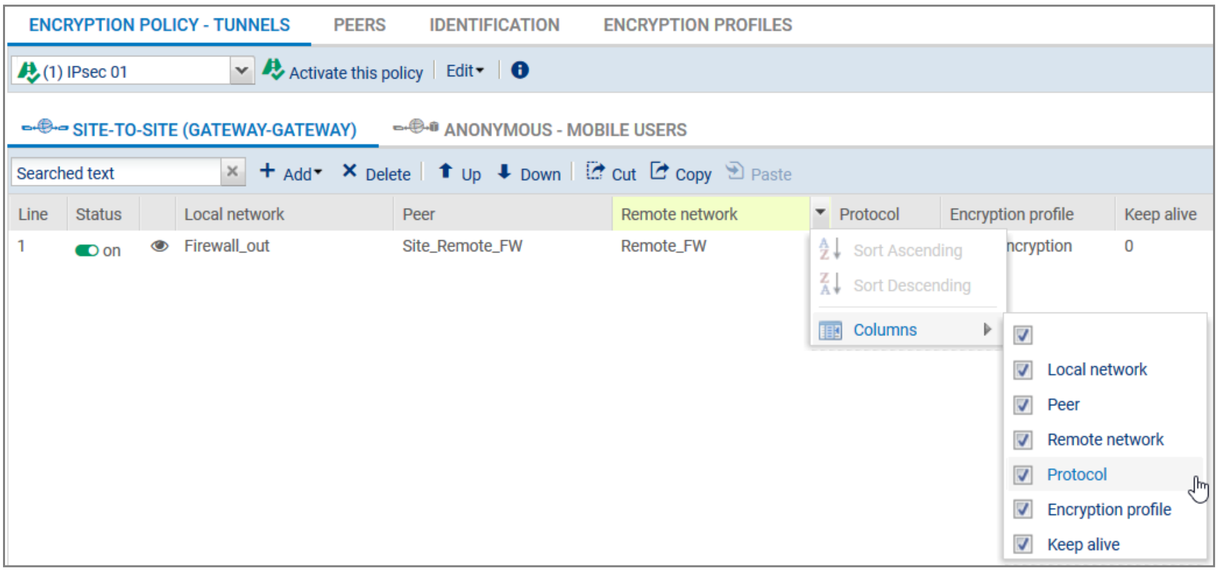
NOTES

For more details on creating peers that use pre-shared key or certificate-based authentication, refer to IPsec VPN - Authentication by pre-shared key and IPsec VPN - Authentication by certificate.

The version of the IKE protocol for this peer must be the same as:

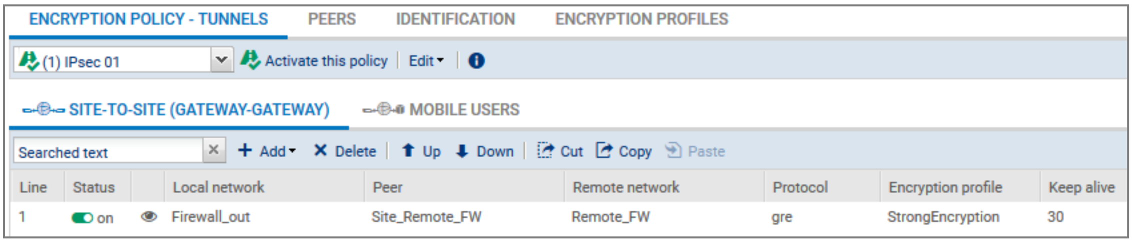
- The version used on the remote firewall,
- The version on peers used in the other rules of the IPsec policy in question.

7. To prevent IPsec tunnels from being set up for protocols other than GRE, and to prevent the encryption of traffic such as ICMP (pings), we recommend that you specify the GRE protocol in the **Protocol** column.
   If this column does not appear, scroll over the title of any column and expand the right-click menu by clicking on the arrow. Click on **Columns** then select the **Protocols** checkbox.



Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on		Firewall_out	Site_Remote_FW	Remote_FW		ncryption	0

8. To allow the tunnel to set up without initial traffic and to stay up even when traffic is disrupted for a short period, click in the **Keepalive** column and select a duration (30 seconds in the example).
   The IPsec VPN policy will then look like this:



Line	Status	Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on	Firewall_out	Site_Remote_FW	Remote_FW	gre	StrongEncryption	30

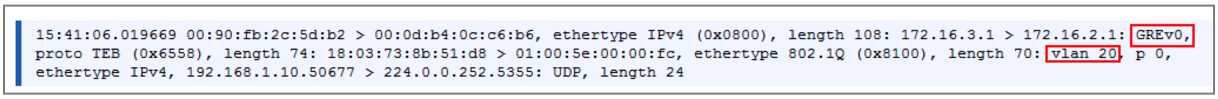
NOTE

Since the firewall started sending GRE network packets, filter rules therefore do not need to be created for this protocol.

Checking operation

From a host on site A that belongs to one of the VLANs, ping a host on site B belonging to the same VLAN. The host on site B should respond to requests.

You can also check whether VLANs are being transported in the tunnel by making a network capture on the incoming interface of the tunnel on site B's firewall. In this case, captured network packets will show the GRE protocol that encapsulates the transported VLAN (VLAN 20 in the example):



```
15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0,
proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20, p 0,
ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24
```

Scenario 3: transporting VLANs through a GRE tunnel with VLAN filtering

Before you start this configuration, do note that:

- This configuration does not allow routing between VLANs transported in the GRE tunnel. If your configuration requires routing between VLANs, refer to Scenario 2.
- A bridge is needed for each VLAN transported. It is therefore essential that you ensure the firewall supports the number of bridges planned.
- Associating a bridge to a VLAN makes it possible to filter VLANs through the tunnel – only VLANs associated with bridges are allowed to go through the tunnel.

Getting started

To set up the suggested infrastructure, each firewall that participates in the GRETAP/IPsec tunnel must be configured in four steps:

- Create and configure the GRETAP interface,
- Create the VLANs,
- Group these VLANs in a dedicated bridge,
- Set the IPsec tunnel.

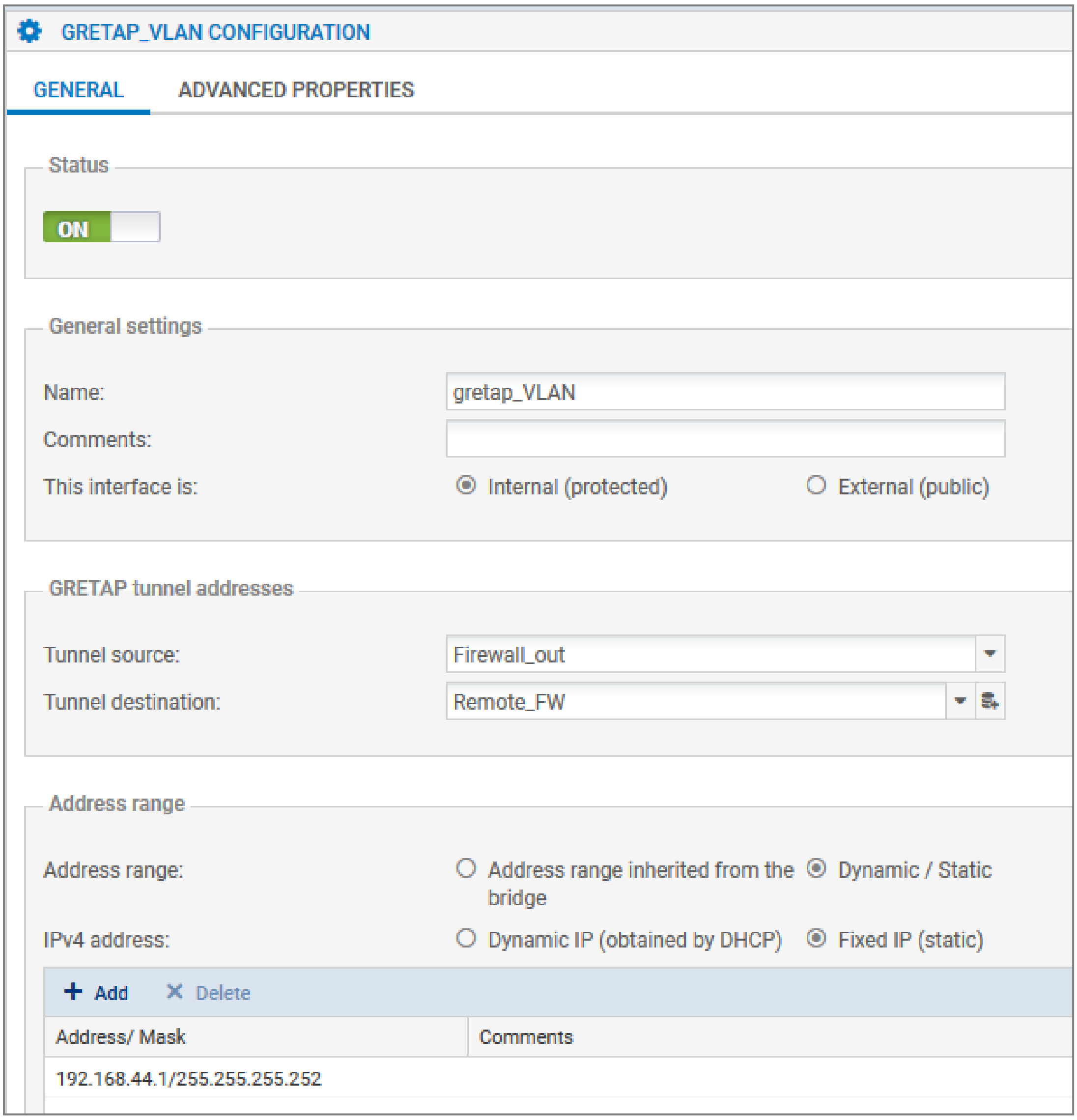
Creating and activating a GRETAP interface

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **Network** > **Interfaces**:

1. Click on **Add**.
2. Select **GRETAP interface**.
   The configuration window of the interface appears.
3. Go to the **General configuration** tab.
4. In the **Status** section, put the cursor on **ON**.
5. In **General settings** > **Name** field, name the GRETAP interface (GretapVLAN in the example).
6. In **General settings** > **This interface is** field, select **External (public)**.
7. In **GRETAP tunnel addresses** > **Tunnel source** field: select the physical interface that GRE traffic will pass through on its way out of the firewall. In the example shown, this will be the **Firewall_out** interface.
8. In **GRETAP tunnel addresses** > **Tunnel destination** field: select (or create) an object with the public IP address of the remote firewall (**Remote_FW** in the example).
9. In **Address range** > **Address range** field, select **Dynamic / Static**.

> **NOTE**
> Not attaching the GRETAP interface to a bridge makes it possible to allow only network packets through the GRE tunnel from VLANs attached to this interface (VLAN10 and 20 in the example).

10. In **Address range** > **IPv4 address** field, select **Fixed IP (static).**
11. Click on **Add**, and enter the IP address and network mask of the GRETAP interface.
    In this example, the IP address and network selected have the values 192.168.44.1 (192.168.44.2 on the remote firewall) and 255.255.255.252 respectively:



GRETAP_VLAN CONFIGURATION

Status

ON

General settings

Name: gretap_VLAN

Comments:

This interface is: ● Internal (protected) ○ External (public)

GRETAP tunnel addresses

Tunnel source: Firewall_out

Tunnel destination: Remote_FW

Address range

Address range: ○ Address range inherited from the bridge ● Dynamic / Static

IPv4 address: ○ Dynamic IP (obtained by DHCP) ● Fixed IP (static)

Address/ Mask	Comments
192.168.44.1/255.255.255.252	

12. Click on **Apply**, then **Save** to confirm the creation of the GRETAP interface.

Creating VLANs

VLANs are first created outside bridges before being connected to a bridge specifically created to allow them to pass through the tunnel.

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **Network** > **Interfaces**:

Creating the incoming VLAN 10

In **Configuration > Network > Interfaces**:

1. Click on **Add**.
2. Select **VLAN > No parent interface**.
3. Go to the **General configuration** tab.
4. In the **Status** section, put the cursor on **ON**.
5. In **General settings** > **Name** field, name the VLAN (*vlan_10_1* in the example).
6. In **General settings** > **Parent interface** field, select the interface that hosts the incoming VLAN (*in* interface in the example).

7. In **General settings** > **ID** field, select the 802.1q identifier associated with the VLAN (*10* in the example).
8. In **General settings** > **This interface is** field, select **Internal (protected)**.
9. In **Address range**: leave the **Address range** field as **Dynamic / Static** and the **IPv4 address** field as **Dynamic IP (obtained by DHCP)**.
10. Click on **Apply**.

Creating the outgoing VLAN 10

In **Configuration > Network > Interfaces**:

1. Click on **Add**.
2. Select **VLAN > No parent interface**.
3. Go to the **General configuration** tab.
4. In the **Status** section, put the cursor on **ON**.
5. In **General settings** > **Name** field, name the VLAN (*vlan_10_2* in the example).
6. In **General settings** > **Parent interface** field, select the interface that hosts the outgoing VLAN (*Gretap_VLAN* interface in the example).
7. In **General settings** > **ID** field, select the 802.1q identifier associated with the VLAN (*10* in the example).
8. In **General settings** > **This interface is** field, select **Internal (protected)**.
9. In **Address range**: leave the **Address range** field as **Dynamic / Static** and the **IPv4 address** field as **Dynamic IP (obtained by DHCP)**.
10. Click on **Apply**.

Connecting both VLANs to a dedicated bridge

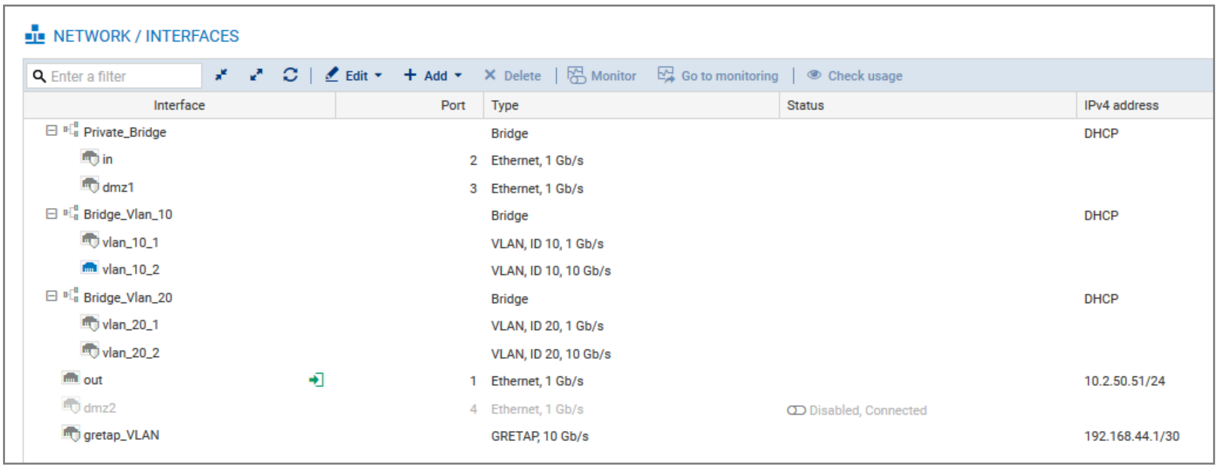
In **Configuration > Network > Interfaces**:

1. Select vlan_10_1 and vlan_10_2 from the list of interfaces.
2. Click on **Add**.
3. Select **Bridge** > **With vlan_10_1, vlan_10_2**.
4. **Name**: enter the name of the bridge (BridgeVlan10 in the example).
5. **IPv4 address**: leave it as **Dynamic IP (obtained by DHCP).**
6. Click on **Apply**.

Creating VLAN 20

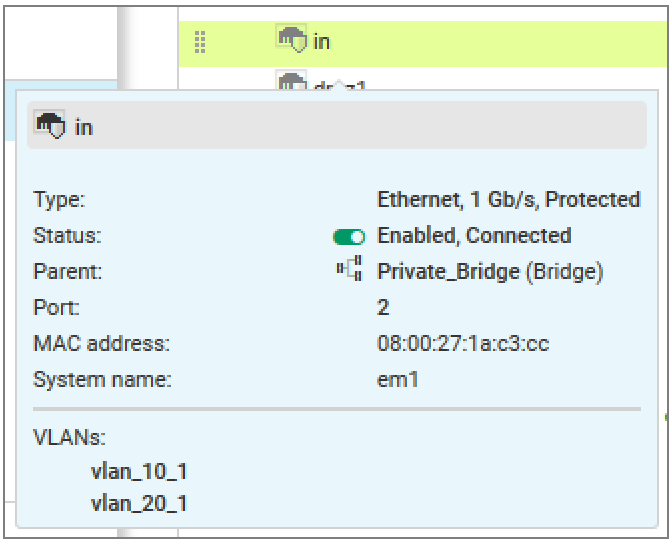
Following the method described earlier, create vlan_20_1 and vlan_20_2 with the ID *20*, connected respectively to the *in* and *gretap_VLAN* interfaces, then placed under a new dedicated bridge named *BridgeVlan20* in the example.

The bridges and their connected VLANs will then appear in the list of interfaces:



Interface	Port	Type	Status	IPv4 address
Private_Bridge		Bridge		DHCP
in	2	Ethernet, 1 Gb/s		
dmz1	3	Ethernet, 1 Gb/s		
Bridge_Vlan_10		Bridge		DHCP
vlan_10_1		VLAN, ID 10, 1 Gb/s		
vlan_10_2		VLAN, ID 10, 10 Gb/s		
Bridge_Vlan_20		Bridge		DHCP
vlan_20_1		VLAN, ID 20, 1 Gb/s		
vlan_20_2		VLAN, ID 20, 10 Gb/s		
out	1	Ethernet, 1 Gb/s		10.2.50.51/24
dmz2	4	Ethernet, 1 Gb/s	Disabled, Connected	
gretap_VLAN		GRETAP, 10 Gb/s		192.168.44.1/30

By scrolling over the *in* interface, you will be able to check whether VLANs *vlan_10_1* and *vlan_20_1* have been attached to it:

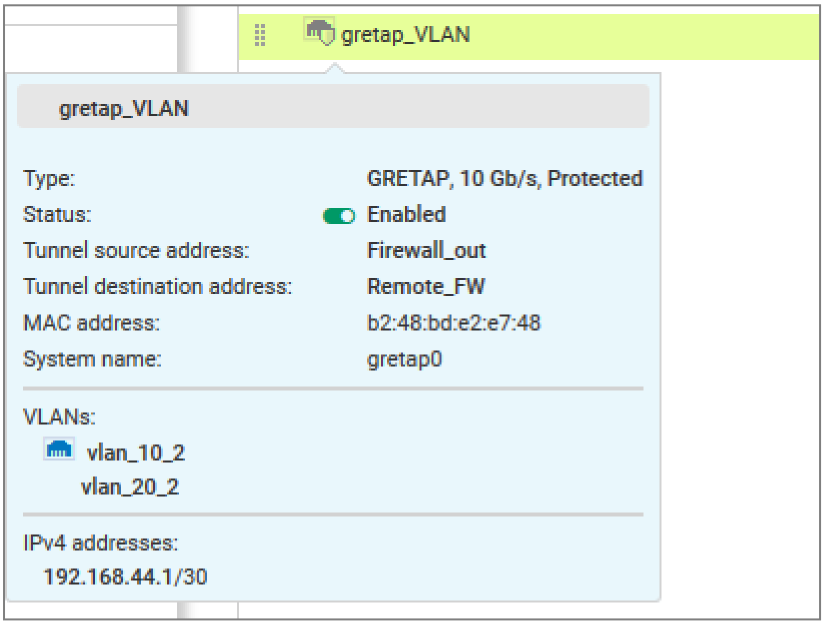


in

Type:	Ethernet, 1 Gb/s, Protected
Status:	Enabled, Connected
Parent:	Private_Bridge (Bridge)
Port:	2
MAC address:	08:00:27:1a:c3:cc
System name:	em1

VLANs:
vlan_10_1
vlan_20_1

Likewise for the interface *gretap_VLAN* and VLANs *vlan_10_2* and *vlan_20_2*:



gretap_VLAN

Type:	GRETAP, 10 Gb/s, Protected
Status:	Enabled
Tunnel source address:	Firewall_out
Tunnel destination address:	Remote_FW
MAC address:	b2:48:bd:e2:e7:48
System name:	gretap0

VLANs:
vlan_10_2
vlan_20_2

IPv4 addresses:
192.168.44.1/30

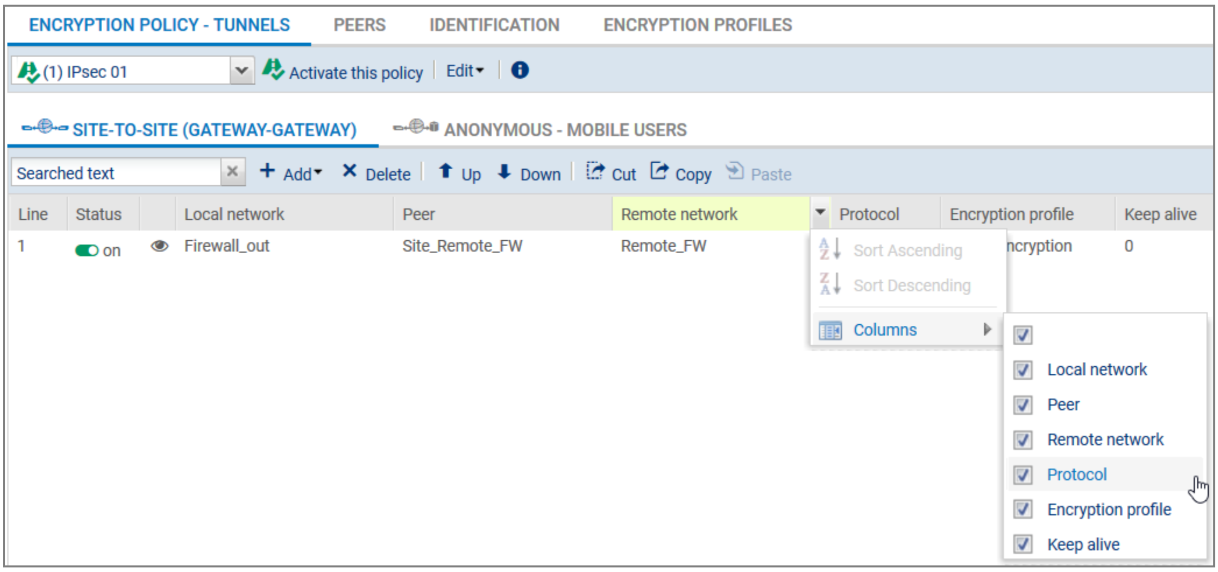
Creating the IPsec tunnel

On each firewall that is part of the GRETAP tunnel, in **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

1. Click on **Add**.
2. Select **Site-to-site tunnel**.
3. For the **Local network** field: select the physical interface that hosts the GRE tunnel (**Firewall_out** in the example).
4. For the **Remote network** field: select an object bearing the public IP address of the remote firewall (**Remote_FW** in the example).
5. For the **Peer selection** field: create (or select if it already exists) a peer with a remote gateway that will be an object bearing the public IP address of remote firewall.
6. Click on **Finish**.

> **NOTES**
> For more details on creating peers that use pre-shared key or certificate-based authentication, refer to IPsec VPN - Authentication by pre-shared key and IPsec VPN - Authentication by certificate.
>
> The version of the IKE protocol for this peer must be the same as:
>
> - The version used on the remote firewall,
> - The version on peers used in the other rules of the IPsec policy in question.

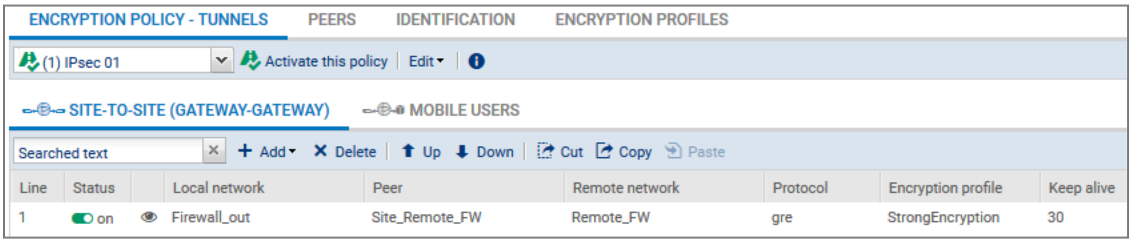
7. To prevent IPsec tunnels from being set up for protocols other than GRE, and to prevent the encryption of traffic such as ICMP (pings), we recommend that you specify the GRE protocol in the **Protocol** column.
   If this column does not appear, scroll over the title of any column and expand the right-click menu by clicking on the arrow. Click on **Columns** then select the **Protocols** checkbox.



Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on		Firewall_out	Site_Remote_FW	Remote_FW		ncryption	0

8. To allow the tunnel to set up without initial traffic and to stay up even when traffic is disrupted for a short period, click in the **Keepalive** column and select a duration (30 seconds in the example).

The IPsec VPN policy will then look like this:



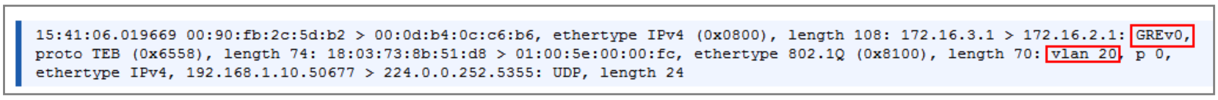
Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile	Keep alive
1	on		Firewall_out	Site_Remote_FW	Remote_FW	gre	StrongEncryption	30

NOTE
Since the firewall started sending GRE network packets, filter rules therefore do not need to be created for this protocol.

Checking operation

From a host on site A that belongs to one of the VLANs, ping a host on site B belonging to the same VLAN. The host on site B should respond to requests.

You can also check whether VLANs are being transported in the tunnel by making a network capture on the incoming interface of the tunnel on site B's firewall. In this case, captured network packets will show the GRE protocol that encapsulates the transported VLAN (VLAN 20 in the example):



```
15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0,
proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20, p 0,
ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24
```

Further reading

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

STORMSHIELD

documentation@stormshield.eu

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