TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC VIRTUAL INTERFACES

Product concerned: SNS 2.1 and higher versions, SNS 3.x, SNS 4.x

Document last updated: January 11, 2021

Reference: sns-en-ipsec_virtual_interfaces_technical_note

Table of contents

Introduction

Version 2.x of the Stormshield Network firewall firmware offers the possibility of implementing routed IPsec VPN tunnels. Routing instructions (static or dynamic routing defined by the filter policy) instead of the information defined in the Security Policy Database (SPD) is now used to determine whether packets need to go through this IPsec tunnel.

When defining a routed IPsec tunnel, virtual interfaces act as traffic endpoints. There is no longer the need to specify remote networks in the IPsec policy.

The combined use of router objects and routed tunnels in filter rules therefore allows implementing several types of configurations.

Failover

When a link fails, traffic (encrypted or unencrypted) going through an MPLS network for example, can now be redirected to a backup VPN tunnel set up between sites via the Internet.

Load balancing

Router objects allow in particular implementing load balancing on several Internet access gateways. Load balancing by type of traffic can also be configured using instructions for routing packets to differentiated IPsec tunnels.

Quality of Service (QoS)

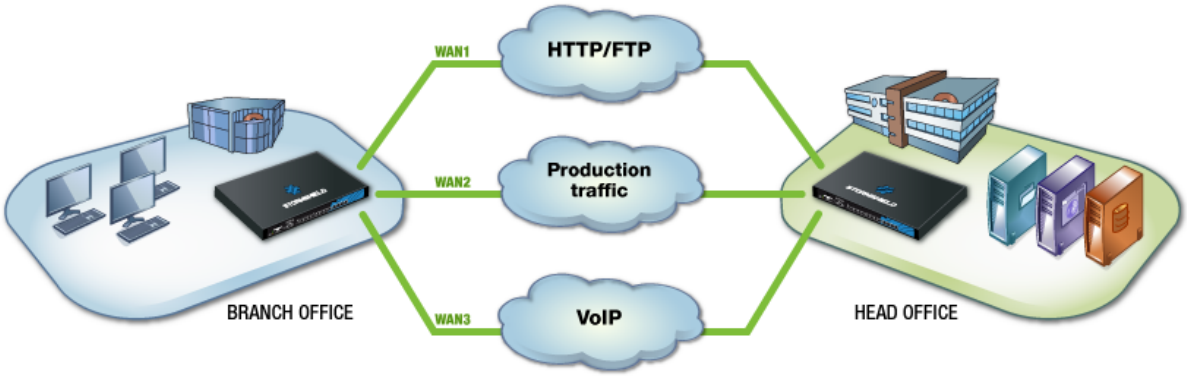
The value of the DSCP (Differentiated Services Code Point) field assigned to IP packets makes it possible to direct them to differentiated IPsec tunnels based on the routing instructions defined.

Securing unencrypted traffic

Unencrypted traffic (e.g.: HTTP) can therefore be secured using an IPsec tunnel based on routing, whereas encrypted traffic (HTTPS) going to the same server does not go through a tunnel.

Architecture

This document describes the configuration stages needed for setting up the following architecture:



Overview

A company has two sites linked to each other by 3 access routers: The agency, exclusively comprising client workstations, accesses server resources hosted at the head office in this way:

- Access to intranet web portals and file transfers via FTP,
- Usage of "production" applications (e.g.: access to SQL database servers),
- Communication by VoIP via the head office's PBX servers.

The company wishes to secure these three types of traffic using encryption in IPsec tunnels. It has also chosen to implement redundancy between the 3 links in order to ensure service continuity for "production" traffic and VoIP.

Detailed presentation

In the architecture shown, traffic between the agency's client workstations and servers at the remote head office is shared between several links depending on their nature. These links are managed by external interfaces (unprotected) on both firewalls (each of these interfaces has a dedicated IP address). Traffic is distributed following routing instructions specified in the filter rules (Policy Based Routing):

- HTTP and FTP traffic go through the link named WAN1,
- "Production" traffic goes through the link named WAN2,
- the link named WAN3 is used for VoIP traffic.

Configuring the firewall on the client side

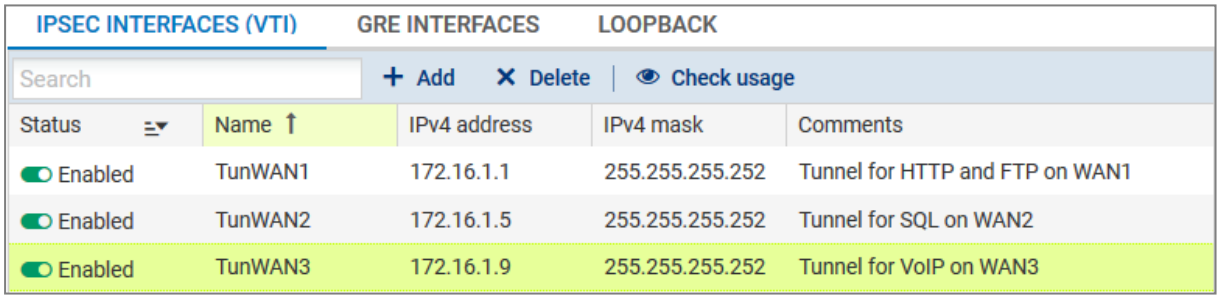
The tunnels through which various streams of traffic travel are defined by IPsec virtual interfaces.

Three local virtual interfaces therefore need to be created, allowing three separate IPsec tunnels to be set up. In the example, these interfaces are named **TunWAN1**, **TunWAN2**and **TunWAN3** (the associated remote interfaces will be named **RemoteTunWAN1**, **RemoteTunWAN2** and **RemoteTunWAN3** respectively).

Creating local virtual interfaces

Select the *IPsec interfaces* tab in the **Configuration > Network > Virtual interfaces** module. Click on **Add** to create the first virtual interface. Three fields must be entered:

- **Name**: specify the name of the virtual interface created (**TunWAN1** in the example),
- **IP address**: indicate the IP address assigned to the interface (172.16.1.1 in the example),
- **Network mask**: the value suggested by default is a 255.255.255.252 mask that allows defining an address for the local virtual interface, and an address for the remote virtual interface. In this example, the mask keeps its default value. The IP address of the associated remote virtual interface will therefore be 172.16.1.2.



Repeat this operation to define the interfaces **TunWAN2** (IP address / mask: 172.16.1.5 / 255.255.255.252) and **TunWAN3** (IP address / mask: 172.16.1.9 / 255.255.255.252).

Defining remote virtual interfaces

The virtual interfaces on the remote firewall can be defined with the help of network objects. They will be used as gateways in routers and can be used in the definition of IPsec tunnels.

In the given example, remote interfaces are named **RemoteTunWAN1**, **RemoteTunWAN2** and **RemoteTunWAN3**.

To create the object corresponding to the first virtual interface on the remote firewall, go to the **Configuration > Objects > Network objects** module and click on Add and on the **Host** icon of the upper banner.

Assign a name to the object (**RemoteTunWAN1** in this example) and indicate the associated IP address. For this object, you will need to indicate the IP address of the IPsec interface associated with the WAN1 link of the remote firewall, i.e. 172.16.1.2 in the example. Confirm to create the object.

Following the same method, create the objects **RemoteTunWAN2** (172.16.1.6) and **RemoteTunWAN3** (172.16.1.10).

Creating IPsec tunnels

An IPsec tunnel that goes through virtual interfaces has the particularity of using these local and remote interfaces as traffic endpoints. The IPsec peer is defined ordinarily by its public IP address.

- In the **IPsec VPN** module, create a new tunnel by clicking on **Add** then selecting **Site to site**.
- For the **Local network** field, select the local virtual interface **Firewall_TunWAN1**,
- For the **Remote network** field, select the object **RemoteTunWAN1**,

Create (or select it if it exists) a peer whose remote gateway will be an object representing the public IP address dedicated to the WAN1 link of the remote firewall.
Note that the version of the IKE protocol must be the same for all peers used in the IPsec VPN policy.

Following the same method, create two other tunnels with the following values:

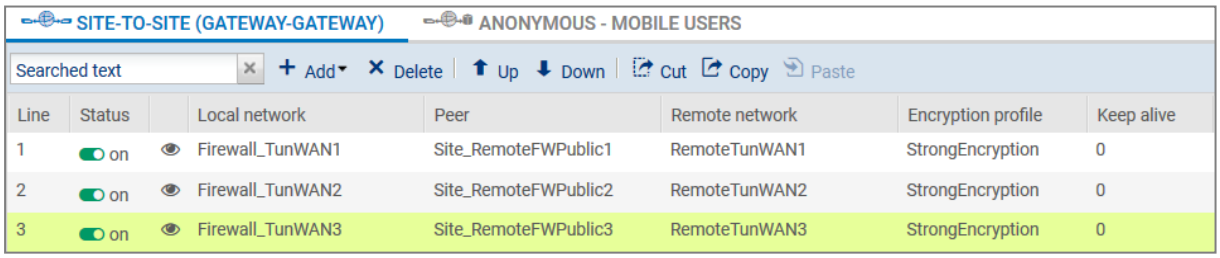
Tunnel for the WAN2 link

- **Local network**: virtual interface **Firewall_TunWAN2**,
- **Remote network**: object **RemoteTunWAN2**,
- **Peer's gateway**: host object with the same public IP Address dedicated to the WAN2 link of the remote firewall.

Tunnel for the WAN3 link

- **Local network**: virtual interface **Firewall_TunWAN3**,
- **Remote network**: object **RemoteTunWAN3**,
- **Peer's gateway**: host object with the same public IP Address dedicated to the WAN3 link of the remote firewall.

The IPsec VPN policy will therefore resemble:



Creating router objects

The use of router objects makes it possible to provide redundancy between WAN links. Indeed, these routers are made up of different gateways that can be defined as active or backup.

To test the availability of these gateways, a series of ICMP requests (pings) will be sent. They are carried out over regular intervals ("frequency" setting, expressed in seconds).

Once a request has been sent to a gateway, the firewall will wait for its response for the defined period ("wait" setting, expressed in seconds). If it does not receive a response, it will send a new request until it reaches the maximum number of unsuccessful times defined ("tries" setting). Once it has reached the number of tries, and if no response has been received, the firewall will consider the gateway uncontactable. One or several backup gateways will then become the main gateway(s).

The "frequency", "wait" and "tries" settings can only be configured in the CLI:

```
CONFIG OBJECT ROUTER NEW name=<router name> [tries=<int>] [wait=<seconds>]
[frequency=<seconds>] update=1.
```

The recommended values for these settings are:

- "frequency": 15 (seconds),
- "wait": 2 (seconds),
- "tries": 3.

In the configuration shown, three router objects need to be created:

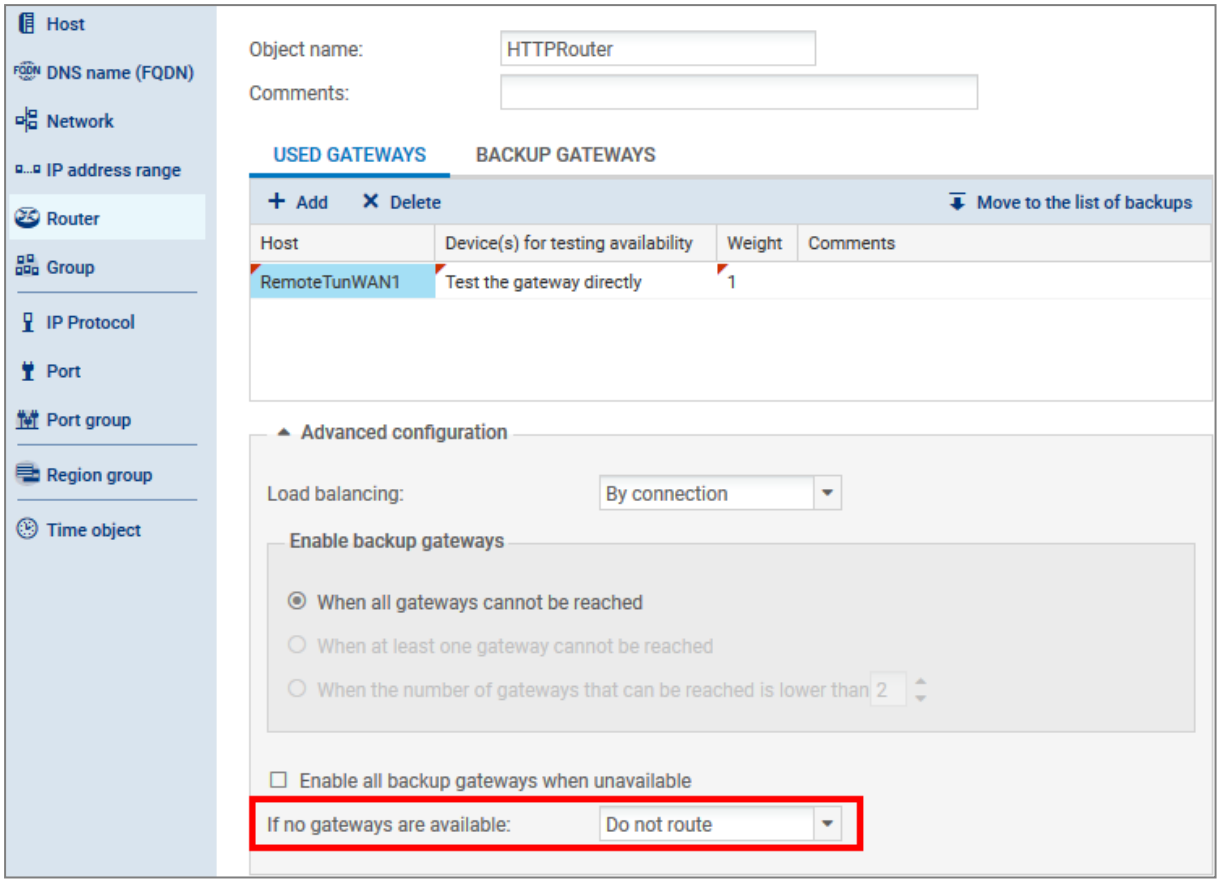
- The first (**HTTPRouter** in the example) is used for transporting HTTP/FTP traffic on WAN1, without redundancy,
- The second (**ProductionRouter**) allows guaranteeing the redundancy of production traffic going from WAN2 to the two other links WAN1 and WAN3,
- The third (**VoIPRouter**) ensures the transfer of traffic from WAN3 to WAN2.

IMPORTANT
For the configuration of routed IPsec tunnels, the routes defined in the filter rules must use remote gateways. Router objects used in this example are therefore based on remote virtual IPsec interfaces.

Router for HTTP and FTP traffic

In the **Configuration > Objects > Network objects** menu, click on **Add** and on the **Router** icon in the upper banner.

- Enter the name of the object (**HTTPRouter** in the example),
- In the list of gateways used, select the remote router associated with WAN1 (**RemoteTunWAN1** object in this example),
- In the object's advanced configuration, select the option **Do not route** for the field **If no gateways are available**. As such, if WAN1 fails, HTTP/FTP traffic will not be taken into account by the routing instructions defined by default. The firewall will simply ignore such traffic.



Click on **Create and duplicate** to confirm this configuration.

Router for production traffic

- Enter the name of the object (**ProductionRouter** in the example),
- In the list of gateways used, select the remote IPsec interface associated with WAN2, i.e. the **RemoteTunWAN2** object in this example),
- In the list of backup gateways, add both remote IPsec interfaces that are likely to receive production traffic if WAN2 is unavailable, i.e. **RemoteTunWAN1** and **RemoteTunWAN3,**
- In the object's advanced configuration, select the option **Enable all backup gateways when unavailable**: both backup gateways **RemoteTunWAN1** and **RemoteTunWAN3** will then be simultaneously enabled when the main link WAN2 becomes unavailable:

NOTE
If different weights are assigned to both backup gateways, load balancing for new connections will be applied when the main gateway fails.

EXAMPLE
A weight value of 50 is assigned to the gateway **RemoteTunWAN1**.
A weight value of 10 is assigned to the gateway **RemoteTunWAN3**.
When both of these gateways become active, the gateway **RemoteTunWAN1** will absorb 50/(50+10)=83% of connections. The remaining 17% of connections will be managed by the gateway**RemoteTunWAN3**.

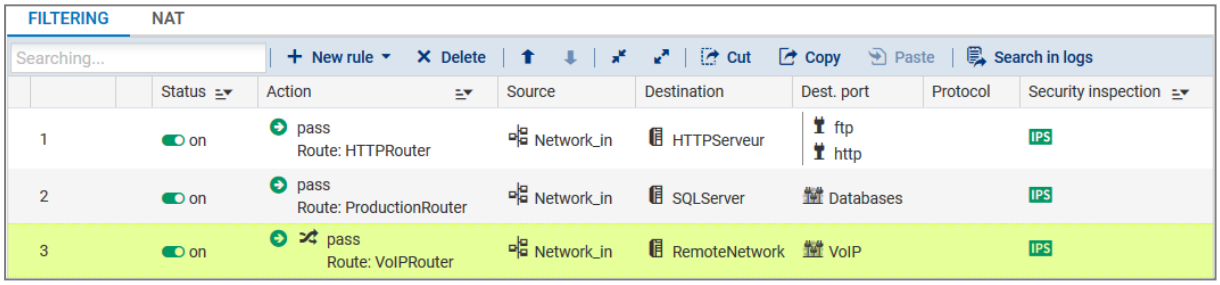
Router for VoIP traffic

In the **Configuration > Objects > Network objects** menu, click on **Add** and on the **Router** icon in the upper banner:

- Enter the name of the object (**VoIPRouter** in the example),
- In the list of gateways used, select the remote router absorbing WAN3 (**RemoteTunWAN3** object in this example),
- In the list of backup gateways, add the gateway that is likely to receive VoIP traffic if WAN3 is unavailable, (**RemoteTunWAN2** in the example):

Filter rules

Three policy-based routing (PBR) rules are needed in order to allow traffic through their respective IPsec tunnels.



- The first rule allows HTTP and FTP traffic to go from the internal network to the server (**HTTPServer** object in the example). These streams of traffic go through the router **HTTPRouter** (WAN1 link),
- The second rule allows production traffic (SQL traffic in the example) to go from the internal network to the server (**SQLServer** object in the example). These streams of traffic are directed to the gateway **ProductionRouter** (WAN2 link),
- The third rule is dedicated to VoIP traffic going from the internal network to the remote network. These streams of traffic go through the router **VoIPRouter** (WAN3 link),

Since routing to the server network was defined in the filter rules, there is no need to create a static route.

Rule for HTTP and FTP traffic via the WAN1 link

Add a rule using the same following elements:

- **Action** (**General** tab)
  In the **Action** field, select the value **Pass**. In the **Route** field, select the router object **HTTPRouter.**
- **Source** (**General** tab)
  In the **Source** field, select the host, host group or network allowed to set up HTTP and FTP connections to the server. In the example, the selected object is **Network_in**.
- **Destination** (**General** tab)
  In the **Destination** field, select the host or host group hosting HTTP and FTP services. In the example, the selected object is **HTTPServer.**
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, HTTP and FTP have been selected.

Rule for production traffic via the WAN2 link

Add a rule using the same following elements:

- **Action** (**General** tab)
  In the **Action** field, select the value **Pass**. In the **Route** field, select the router object **ProductionRouter.**
- **Source** (**General** tab)
  In the **Source** field, select the host, host group or network allowed to set up connections to the production server(s). In the example, the selected object is **Network_in**.
- **Destination** (**General** tab)
  In the **Destination** field, select the host or host group hosting production services. In the example, the selected object is **SQLServer.**
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, the **Databases** group is used, which includes various ports for connecting to the SQL database (PostgreSQL, MySQL,etc.).

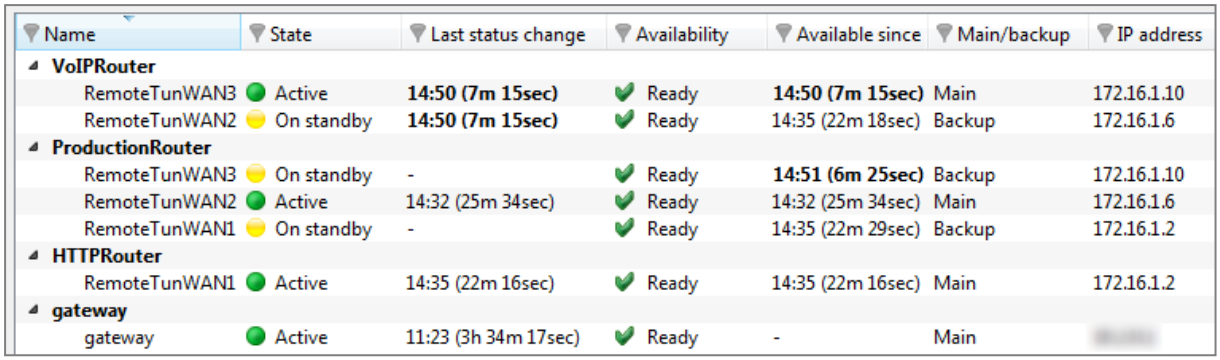
Rule for VoIP traffic via the WAN3 link

Create a filter rule using the same following elements:

- **Action** (**General** tab)
  In the **Action** field, select the value **Pass**. In the **Route** field, select the router object **VoIPRouter**.
- **Action** (**Quality of service** tab)
  The DSCP field can be imposed on packets. To do so, select the option **Impose value** and in the **New DSCP value** field, you may set a customized DSCP field (18 Class 2 in the example).
- **Source** (**General** tab)
  In the Source field, select the host, host group or network allowed to set up connections to the production server(s). In the example, the selected object is Network_in.
- **Destination** (**General** tab)
  In the **Destination** field, select the host, host group or network with which connections will be set up. In the example, the selected object is **RemoteNetwork**.
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, a **VoIP** group is used, containing different ports needed for VoIP.

Verifying the status of routers

The **Routers** module on Stormshield Network Real-Time Monitor displays the status of the default gateway and other gateways that make up each router used in the firewall's configuration:



Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	**14:50 (7m 15sec)**	Ready	**14:50 (7m 15sec)**	Main	172.16.1.10
RemoteTunWAN2	On standby	**14:50 (7m 15sec)**	Ready	14:35 (22m 18sec)	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	On standby	-	Ready	**14:51 (6m 25sec)**	Backup	172.16.1.10
RemoteTunWAN2	Active	14:32 (25m 34sec)	Ready	14:32 (25m 34sec)	Main	172.16.1.6
RemoteTunWAN1	On standby	-	Ready	14:35 (22m 29sec)	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	14:35 (22m 16sec)	Ready	14:35 (22m 16sec)	Main	172.16.1.2
gateway						
gateway	Active	11:23 (3h 34m 17sec)	Ready	-	Main	[redacted]

The following information will be displayed:

- **Name:** name given to the router or gateway in the firewall's configuration.
- **State**: Gateway status The three possible values are: **Active** (gateway used), **On standby** (backup gateway) or **Unavailable** (pings to this gateway failed).
- **Last status change:** date on which the status of the gateway last changed (e.g.: switching from **On standby** to **Active**) The duration since the last status change is also specified in brackets.
- **Availability:** this refers to the results of the last ping. The possible values are **Ready** (gateway operational) or **Unavailable** (the gateway did not respond).
- **Available since:** time at which the gateway became available. The duration since the first successful ping is also specified in brackets.
- **Main/backup:** this refers to the gateway's default role in the router. The values are either **Main** or **Backup**.
- **IP Address:** IP address of the gateway.
- **Distribution:** In load balancing, this refers to the gateway's rate of use in the router (percentage).

Configuring the firewall on the server side

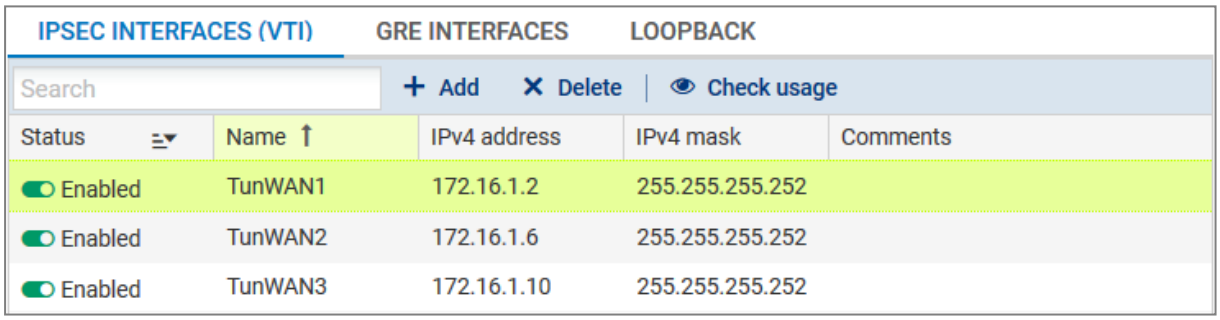
The tunnels through which various streams of traffic travel are defined by IPsec virtual interfaces.

Three local virtual interfaces therefore need to be created, allowing three separate IPsec tunnels to be set up. In the example, these interfaces are named **TunWAN1**, **TunWAN2**and **TunWAN3** (the associated remote interfaces will be named **RemoteTunWAN1**, **RemoteTunWAN2** and **RemoteTunWAN3** respectively).

Creating local virtual interfaces

By following the method described for the firewall that protects client workstations, define 3 local virtual interfaces. In order to obtain the network mask chosen in the example, these interfaces will have the following IP addresses:

- **TunWAN1** interface: 172.16.1.2 (mask 255.255.255.252),
- **TunWAN2** interface: 172.16.1.6 (mask 255.255.255.252),
- **TunWAN3** interface: 172.16.1.10 (mask 255.255.255.252).



Defining remote virtual interfaces

By following the method described for the firewall that protects client workstations, define 3 remote virtual interfaces. Since these are the firewall's local virtual interfaces on the client side, the IP addresses to use will be the following:

- **RemoteTunWAN1** interface: 172.16.1.1,
- **RemoteTunWAN2** interface: 172.16.1.5,
- **RemoteTunWAN3** interface: 172.16.1.9,

Creating IPsec tunnels

By following the method described for configuring IPsec tunnels on the firewall that protects client workstations, define 3 IPsec tunnels using the values below:

Tunnel on the WAN1 link

- **Local network**: select the local virtual interface **Firewall_TunWAN1**,
- **Remote network**: select the object **RemoteTunWAN1**,
- Create (or select it if it exists) a peer whose remote gateway will be an object representing the public IP address dedicated to the WAN1 link of the remote firewall. The version of the IKE protocol has to be the same as the one used on the firewall that protects clients.

Tunnel on the WAN2 link

- **Local network**: virtual interface **Firewall_TunWAN2**,
- **Remote network**: object **RemoteTunWAN2**,
- **Peer's gateway**: host object with the same public IP Address dedicated to the WAN2 link of the remote firewall.

Tunnel on the WAN3 link

- **Local network**: virtual interface **Firewall_TunWAN3**,
- **Remote network**: object **RemoteTunWAN3**,
- **Peer's gateway**: Host object with the same public IP Address dedicated to the WAN3 link of the remote firewall.

Return routes

When the firewall that protects servers receives traffic from a virtual remote interface, it does not yet know the route through which return packets should be correctly directed. 3 return routes therefore need to be created on this firewall corresponding to the three remote IPsec interfaces.

In the *Return routes* tab in the **Configuration** > **Network** > **Routing** module, click on **Add** and fill in the fields as follows for the WAN1 link:

- **Status**: **On**,
- **Gateway**: select (or create directly from this field) the object corresponding to the first virtual remote interface (**RemoteTunWAN1** in the example).
- **Interface**: select the associated local virtual IPsec interface (**TunWAN1** in the example),
- **Comments**: you may write a short description about the role of this route.

Click on **Apply** to enable this return route.

Perform the same operation to create traffic going through the WAN2 and WAN3 links using the following values:

For the WAN2 link

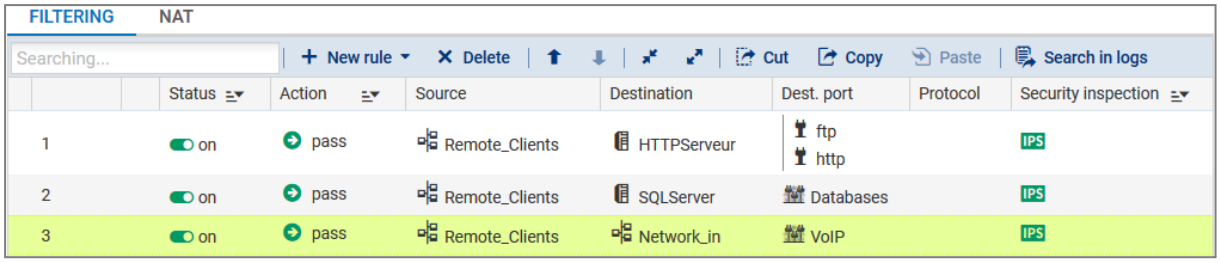
- **Status**: **On**,
- **Gateway**: object **RemoteTunWAN2**,
- **Interface**: object **TunWAN2**.

For the WAN3 link

- **Status**: **On**,
- **Gateway**: object **RemoteTunWAN3**,
- **Interface**: object **TunWAN3**.

Filter rules

Create the three rules needed to allow authorized traffic to reach the local network:



Rule for HTTP and FTP traffic

Add a rule using the same following elements:

- **Action** (**General** tab)
  In the **Action** field, select the value **Pass**
- **Source** (**General** tab)
  In the **Source** field, select the host, host group or network allowed to set up HTTP and FTP connections to the server. In the example, the selected object is the network **Remote_clients**.
- **Destination** (**General** tab)
  In the **Destination** field, select the host or host group hosting HTTP and FTP services. In the example, the selected object is **HTTPServer.**
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, **HTTP** and **FTP** have been selected.

Rule for production traffic via the WAN2 link

Add a rule using the same following elements:

- **Action** (**General** tab)
  In the **Action** field, select the value **Pass**
- **Source** (**General** tab)
  In the **Source** field, select the host, host group or network allowed to set up connections to the production server(s). In the example, the selected object is the network **Remote_clients**.
- **Destination** (**General** tab)
  In the **Destination** field, select the host or host group hosting production services. In the example, the selected object is **SQLServer.**
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, the **Databases** group is used, which includes various ports for connecting to the SQL database (PostgreSQL, MySQL,etc.).

Rule for VoIP traffic

Create a filter rule using the same following elements:

- **Action** (**General** tab)
  In the Action field, select the value **Pass**
- **Source** (**General** tab)
  In the **Source** field, select the host, host group or network allowed to set up connections to the production server(s). In the example, the selected object is **Remote_clients**.

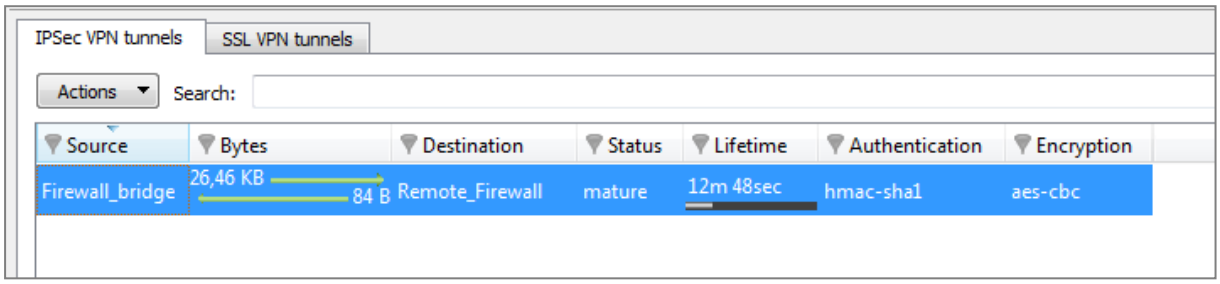
- **Destination** (**General** tab)
  In the **Destination** field, select the host, host group or network with which connections will be set up. In the example, the selected object is **Network_in**.
- **Port – Protocol**
  Select the objects corresponding to the authorized ports. In the example, a **VoIP** group is used, containing different ports needed for VoIP.

The configuration of the firewall protecting client workstations is now complete. We will check whether this configuration is operational.

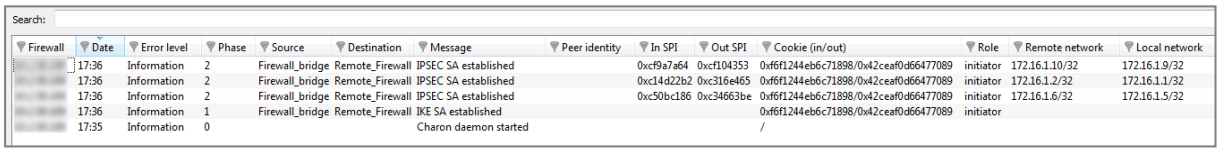
Verifying tunnels

Verifying in SN Real-Time Monitor

When connections using WAN links have been set up, the status of the corresponding tunnels can be viewed in the *IPsec VPN tunnels* tab in the **VPN Tunnels** module:



Logs regarding the setup of the various tunnels can be looked up in the **Logs > VPN** module:



Verifying in the firewall web interface

In the firewall's web administration interface, you can display logs in the **Monitoring** > **Audit Logs** module (VPN view / VPN IPsec logs) to verify that your configuration operates correctly.

Switching to a backup link

When a WAN link fails, the corresponding remote gateway will become uncontactable. The backup gateway(s) defined in the router dedicated to this WAN link will then be enabled. Its change in status can be viewed in the **Routers** module in SN Real-Time Monitor. The example described below explains the router's behavior **ProductionRouter** when the WAN2 link fails.

All WAN links are operational

In line with the definition of routers described in the paragraph Creating router objects, SN Real-Time Monitor shows that production traffic has to go through the WAN2 link (main gateway: **RemoteTunWAN2**). If this link fails, this traffic must then be distributed between the WAN1 and WAN3 links (backup gateways: **RemoteTunWAN1** and **RemoteTunWAN3**).

Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	**14:50 (7m 15sec)**	Ready	**14:50 (7m 15sec)**	Main	172.16.1.10
RemoteTunWAN2	On standby	**14:50 (7m 15sec)**	Ready	14:35 (22m 18sec)	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	On standby	-	Ready	**14:51 (6m 25sec)**	Backup	172.16.1.10
RemoteTunWAN2	Active	14:32 (25m 34sec)	Ready	14:32 (25m 34sec)	Main	172.16.1.6
RemoteTunWAN1	On standby	-	Ready	14:35 (22m 29sec)	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	14:35 (22m 16sec)	Ready	14:35 (22m 16sec)	Main	172.16.1.2
gateway						
gateway	Active	11:23 (3h 34m 17sec)	Ready	-	Main	[redacted]

The WAN2 link is defective

In the illustration above, the WAN2 link no longer functions The gateway **RemoteTunWAN2** then appears as uncontactable and therefore unavailable. For the router **ProductionRouter**, both gateways **RemoteTunWAN1** and **RemoteTunWAN3** have been enabled and production traffic will then go through tunnels set up on the WAN1 and WAN3 links.

Name	State	Last status change	Availability	Available since	Main/backup	IP address
VoIPRouter						
RemoteTunWAN3	Active	-	Ready	-	Main	172.16.1.10
RemoteTunWAN2	Unreachable	-	Unavailable	-	Backup	172.16.1.6
ProductionRouter						
RemoteTunWAN3	Active	-	Ready	-	Backup	172.16.1.10
RemoteTunWAN2	Unreachable	-	Unavailable	-	Main	172.16.1.6
RemoteTunWAN1	Active	-	Ready	-	Backup	172.16.1.2
HTTPRouter						
RemoteTunWAN1	Active	-	Ready	-	Main	172.16.1.2
gateway						
gateway	Active	-	Ready	-	Main	[redacted]

Resolving incidents - Common errors

Further on in this section, the firewall that protects clients (which initiated the setup of tunnels) will be referred to as the *initiator*. The remote firewall will be referred to as the *responder*.

Symptom: The tunnel cannot be set up.

- A message "Remote seems to be dead" in phase 1 appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the "initiator".
- No message appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the "responder".

Solutions: check that:

- the physical interfaces on which the corresponding WAN link relies are indeed available,
- the virtual IPsec interfaces that define the tunnel have been enabled,
- the filter rule matching the traffic that needs to go through this tunnel has been correctly defined and that the router used in this rule is relying on the right virtual interfaces.

Symptom: The tunnel cannot be set up.

- A message "IKE SA establishment failed: received AUTHENTICATION_FAILED notify error" in phase 1 appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the *initiator*.
- A message "Tried 1 shared key but MAC mismatched" in phase 1 appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the *responder*.

Solution: the pre-shared key (peer settings) is different on the *initiator* and *responder* firewalls.

Symptom: The tunnel cannot be set up.

- A message "Invalid major version X" appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the *initiator*.
- A message "Invalid major version Y" appears in the **Logs** > **VPN** module in SN Real-Time Monitor for the *responder*.

Solution: the version of the IKE protocol (peer settings) is different on the *initiator* and *responder* firewalls.

Further reading

Stormshield Knowledge Base

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

STORMSHIELD

documentation@stormshield.eu