TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

FIREWALLS STACKING: SERVICES DISTRIBUTION

Product concerned: SNS 2.x, SNS 3.x, SNS 4.x

Document last updated: December 9, 2019

Reference: sns-en-firewalls_stacking_services_distribution_technical_note

Table of contents

Introduction

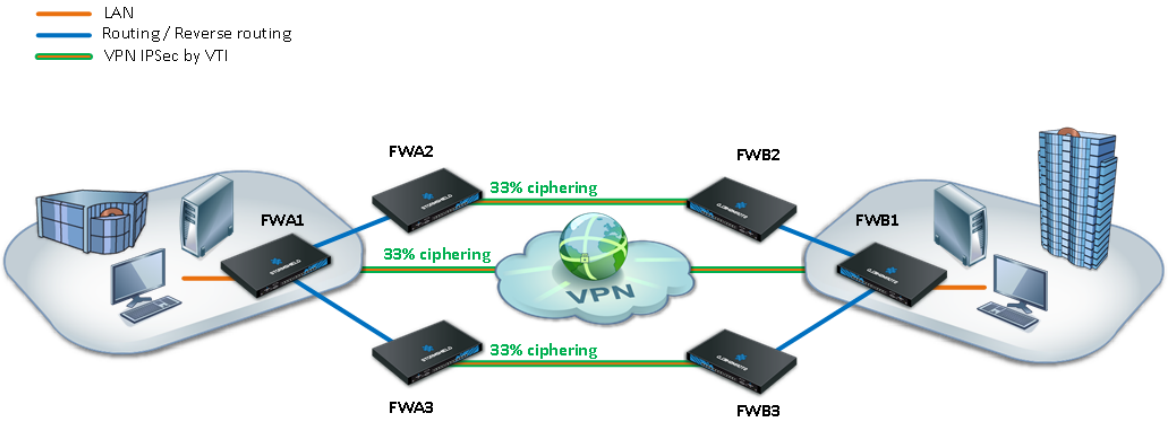
Ever since version 2 of the firmware, Stormshield Network firewalls have been enriched with two new features relating to the routing mechanism: router objects and return routes.

These features make the configuration of routing and load balancing much simpler and more intuitive, thereby allowing sophisticated architectures to be set up.

This technical note sets out two examples of how these features are implemented, in order to spread out traffic over several firewalls, optimizing as such performance and bandwidth use.

Architectures presented

Scenario 1: distribution of IPsec VPN tunnels

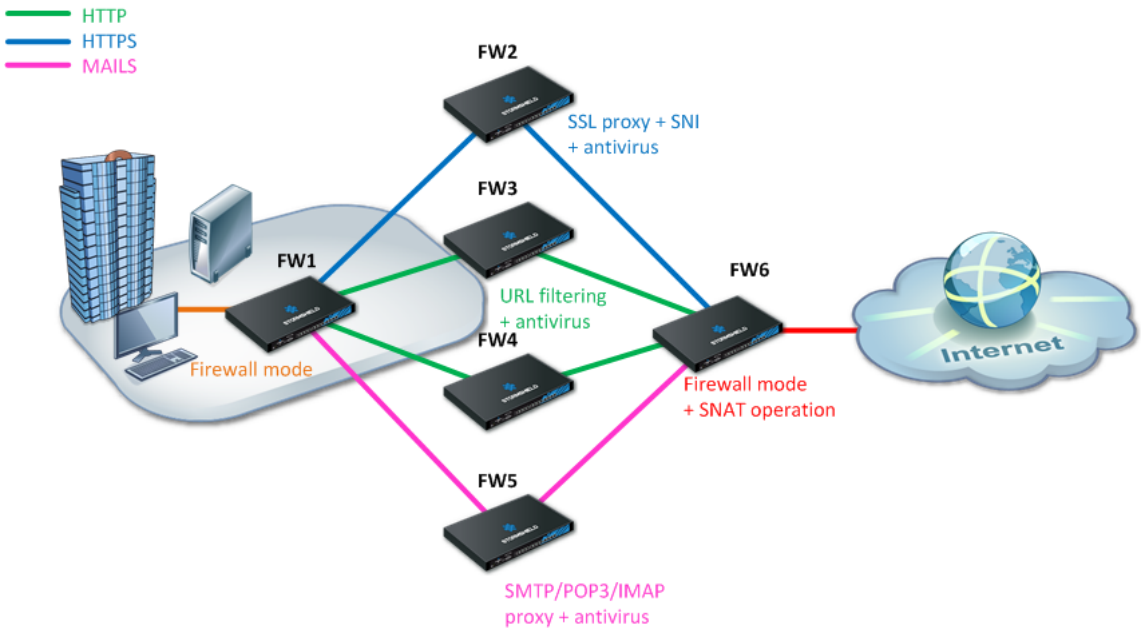


The first scenario shown in this technical note uses router objects and return routes in order to distribute IPsec tunnels over several firewalls, thereby spreading out the system resources needed for encrypting/decrypting data.

In this case, IPsec tunnels are based on virtual IPsec interfaces (VTI - see technical note *Virtual IPsec interfaces*) so that encryption decisions may be made based on routing instead of the Security Policy Database (SPD), thanks to the concept of router objects. As for return routes, they ensure that response packets are routed to the sending firewall.

The configuration examples shown in this technical note assume that traffic initiated from Site A is going to Site B.

Scenario 2: proxy distribution



The second scenario presented in this document uses router objects and return routes in order to distribute traffic according to type (SSL, HTTP and mail) to proxies enabled on separate firewalls.

Protocol-based routing in the filter policy in this case also relies on the use of router objects. As for return routes, they ensure that response packets are routed to the sending firewall.

Scenario 1: distribution of IPsec tunnels

Settings for firewall FWA1

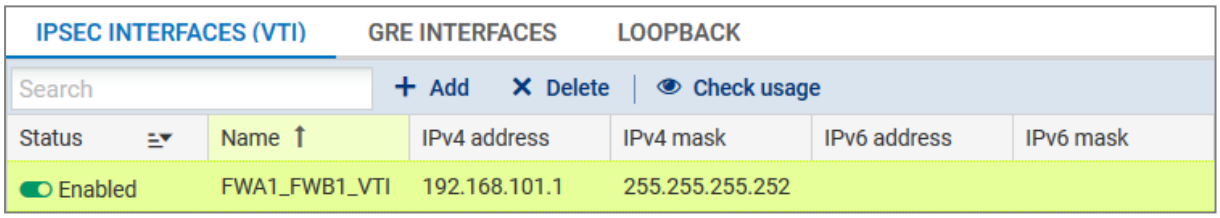
Virtual IPsec interface

Create the virtual interface on which the IPsec tunnel between firewall 1 on site A (FWA1) and firewall 1 on site B (FWB1) will be based.

In the **Configuration** > **Network**>**Virtual interfaces** menu, select the *IPsec interfaces (VTI)* tab and click on **Add**.

Enter the following mandatory fields:

- **Name** (FWA1_FWB1_VTI in the example),
- **IP address** (192.168.101.1 in the example),
- **Mask** (255.255.255.252 in the example).



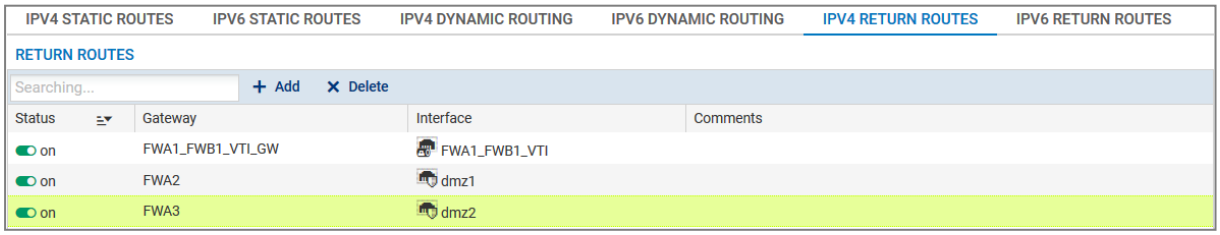
Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Create 3 routes that allow transporting return packets to the original firewall using the source MAC address:



Return route to firewall FWB1

In the **Configuration** > **Network** > **Routing** menu, in the *Return routes* tab, click on **Add** and fill in the mandatory fields:

- **Gateway**: create (icon) the network object corresponding to the virtual IPsec interface of firewall 1 on site B (FWA1_FWB1_VTI_GW with the IP address 192.168.101.2 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 1 on sites A and B (FWA1_FWB1_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWA2

- **Gateway**: create the network object corresponding to firewall 2 on site A (FWA2 in the example),

> **NOTE**
> The MAC address of firewall FWA2 must be declared in this network object.

- **Interface**: select the interface on firewall FWA1 through which return packets will be transported to firewall FWA2 (Dmz1 in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWA3

- **Gateway**: create the network object corresponding to firewall 3 on site A (FWA3 in the example),

> **NOTE**
> The MAC address of firewall FWA3 must be declared in this network object.

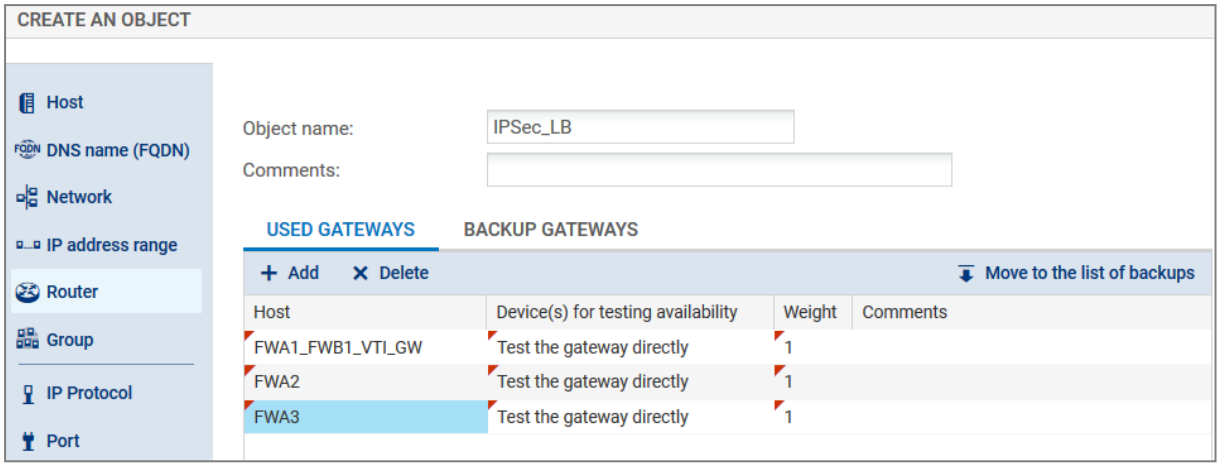
- **Interface**: select the interface on firewall FWA1 through which return packets will be transported to firewall FWA3 (Dmz2 in the example).

Enable the route by double-clicking in the **Status** column.

Load balancing

Packets meant to be encrypted in the 3 IPsec tunnels are balanced using a router object made up of firewalls FWA2, FWA3 and FWB1.

1. In the **Configuration** > **Objects** > **Network objects** menu, click on **Add** and choose *Router*:
2. Enter a name for this object (IPsec_LB in the example).
3. In the *Gateways used* tab, click on **Add** and select the virtual IPsec interface of FWB1 (FWA1_FWB1_VTI_GW). Leave the value **Test the gateway directly** for the column *Device(s) for testing availability*. Likewise, leave the value **1** in the *Weight* column.
4. Repeat this operation to add gateways FWA2 and FWA3.



5. In the Advanced properties panel, check that the various fields have been entered with the following values:
   - **Load balancing**: *By connection* (each new connection that needs to be encrypted in an IPsec tunnel will be sent to one of the gateways declared based on round robin scheduling),
   - **Enable backup gateways**: *When all gateways cannot be reached*,
   - **Enable all backup gateways when unavailable**: unselected
   - **If no gateways are available**: *Default route*.
6. Confirm the creation of the router object by clicking on **Create**.

Filter rule

In order for traffic to be shared evenly between the 3 firewalls (FWA1, FWA2 and FWA3) and to go through their respective IPsec tunnels, create a filter rule (**Configuration** > **Security policy** > **Filter and NAT** menu) that includes a routing directive based on the router object created earlier.

Status column

Double-click on the **Status** column to change the status of the rule to **On**.

Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the router object created for load balancing (IPsec_LB in the example).

Source column

- **Source hosts**: select the network object (host, host group, IP address range or network [LAN_Site_A in the example] at the source of the traffic that needs to be encrypted.

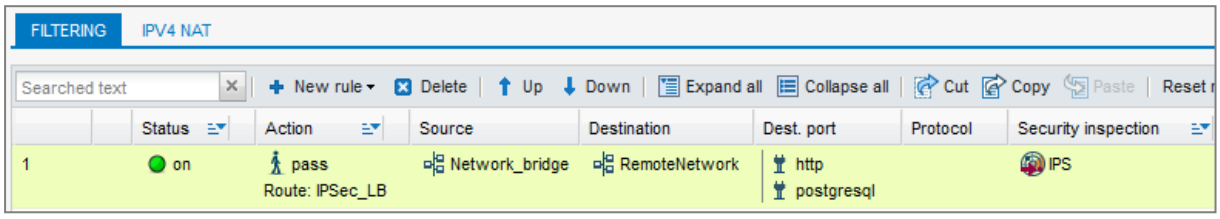
Destination column

- **Destination hosts**: select or create the network object (host, host group, IP address range or network [LAN_Site_B in the example] at the destination of the encrypted traffic.

Dest. port column

- **Destination port**: select the port(s) corresponding to the protocols that need to be encrypted (Any in the example).

Confirm and apply. The filter rule will then look like this:

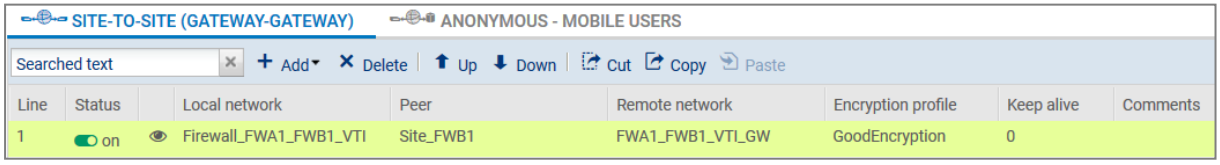


IPsec policy

Create an IPsec VPN policy for the encryption of traffic processed by firewall FWA1 (1/3 of the encrypted traffic, the rest being shared as well among routers FWA2 and FWA3).

1. In the *Site to site (gateway-gateway)* tab in the **Configuration** > **VPN** > **IPsec VPN** menu, click on **Add** and select **Site to site tunnel**.
2. Create a peer (IKEv1 or IKEv2) with the following characteristics:
   - **Remote gateway**: create an object bearing the public IP address of firewall 1 on site B (FWB1 in the example),
   - **Name**: you can either leave the name suggested by default (Site_FWB1 in the example) or customize it,
   - Select the certificate to be presented or indicate a pre-shared key depending on the chosen authentication method (for further detail, please read the relevant online documentation: *How to IPsec VPN - Pre-shared key authentication* and *How to IPsec VPN - Certificate authentication*
3. In the **Local network** field, select the object corresponding to the virtual IPsec interface on firewall FWA1 (Firewall_FWA1_FWB1_VTI in the example).
4. In the **Remote network** field, select the object corresponding to the virtual IPsec interface on firewall FWB1 (FWA1_FWB1_VTI_GW in the example).

The IPsec VPN policy on firewall FWA1 will then look like this:



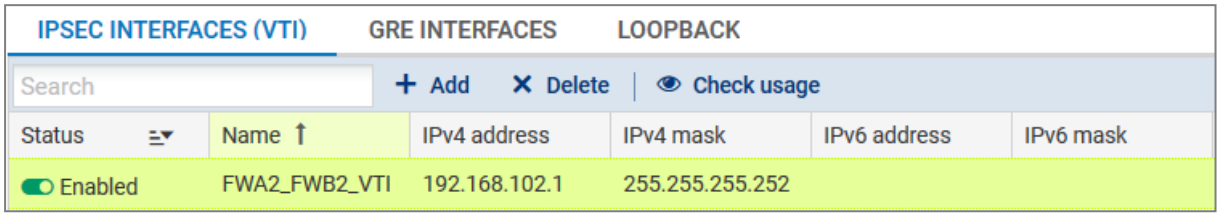
Save (**Save** button) and apply this policy (**Enable this policy** button).

Settings for firewall FWA2

Virtual IPsec interface

Following the method descibed for firewall FWA1, create a virtual IPsec interface (VTI) on which the IPsec tunnel between firewall 2 on site A (FWA2) and firewall 2 on site B (FWB2) will be based:

- **Name:** FWA2_FWB2_VTI in the example,
- **IP address:** 192.168.102.1 in the example,
- **Mask:** 255.255.255.252 in the example,



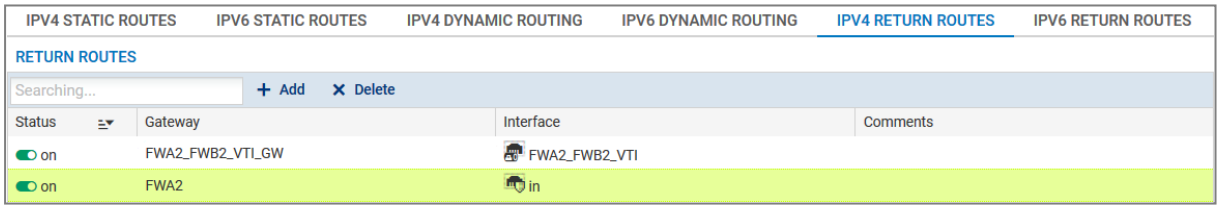
Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Following the method described for firewall FWA1, create 2 routes that allow transporting return packets to the original firewall using the source MAC address.



Return route to firewall FWB2

- **Gateway**: create the network object corresponding to the virtual IPsec interface of firewall 2 on site B (FWA2_FWB2_VTI_GW with the IP address 192.168.102.2 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 2 on sites A and B (FWA2_FWB2_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWA1

- **Gateway**: create the network object corresponding to firewall 1 on site A (FWA1 in the example),

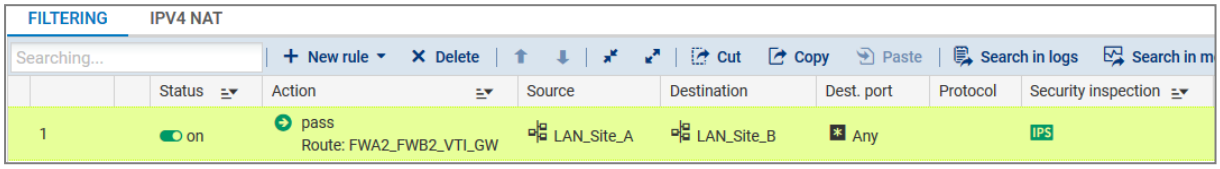
> **NOTE**
> The MAC address of firewall FWA1 must be declared in this network object.

- **Interface**: select the interface on firewall FWA2 through which return packets will be transported to firewall FWA1 ("In" in the example).

Enable the route by double-clicking in the **Status** column.

Filter rule

Following the method described for firewall FWA1, create a filter rule that will send encrypted traffic through the tunnel based on the virtual IPsec interface:



Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the virtual IPsec interface of firewall 2 on site B (object FWA2_FWB2_VTI_GW in the example),

Source column

- **Source hosts**: select the network at the source of the traffic that needs to be encrypted (LAN_Site_A in the example).

Destination column

- **Destination hosts**: select or the network object (host, host group, IP address range or network [LAN_Site_B in the example] at the destination of the encrypted traffic.

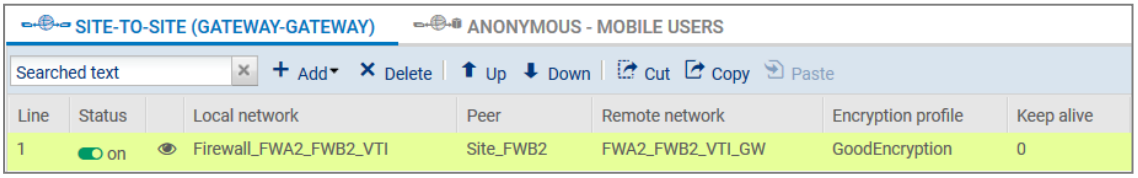
Dest. port column

- **Destination port**: select the port(s) corresponding to the protocols that need to be encrypted (Any in the example).

IPsec policy

Following the method described for firewall FWA1m create an IPsec VPN policy for the encryption of traffic processed by following FWA2:

- **Peer**: create an object corresponding to the public IP address of firewall FWB2,
- **Local network**: select the object corresponding to the local virtual IPsec interface (Firewall_FWA2_FWB2_VTI in the example),
- **Remote network**: select the object corresponding to the remote virtual IPsec interface (FWA2_FWB2_VTI_GW in the example).

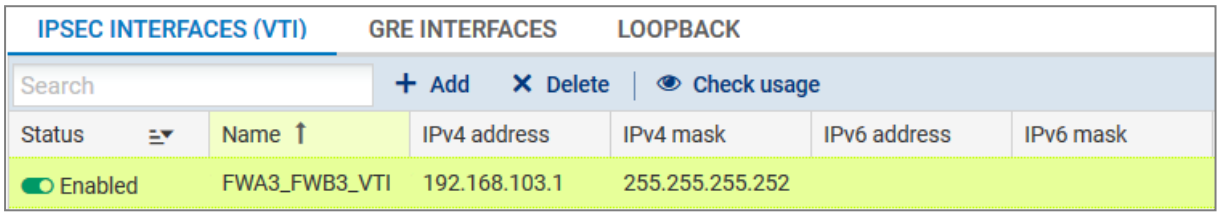


Settings for firewall FWA3

Virtual IPsec interface

Following the method descibed for firewall FWA1, create a virtual IPsec interface (VTI) on which the IPsec tunnel between firewall 3 on site A (FWA3) and firewall 3 on site B (FWB3) will be based:

- **Name:** FWA3_FWB3_VTI in the example,
- **IP address:** 192.168.103.1 in the example,
- **Mask:** 255.255.255.252 in the example,



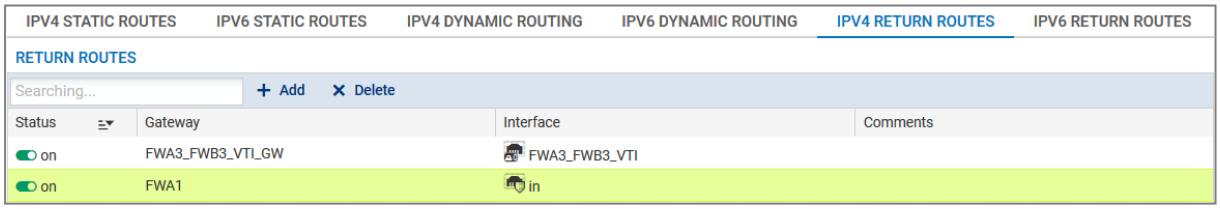
Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Following the method described for firewall FWA1, create 2 routes that allow transporting return packets to the original firewall using the source MAC address.



Return route to firewall FWB3

- **Gateway**: create the network object corresponding to the virtual IPsec interface of firewall 3 on site B (FWA3_FWB3_VTI_GW with the IP address 192.168.103.2 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 3 on sites A and B (FWA3_FWB3_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWA1

- **Gateway**: create the network object corresponding to firewall 1 on site A (FWA1 in the example),

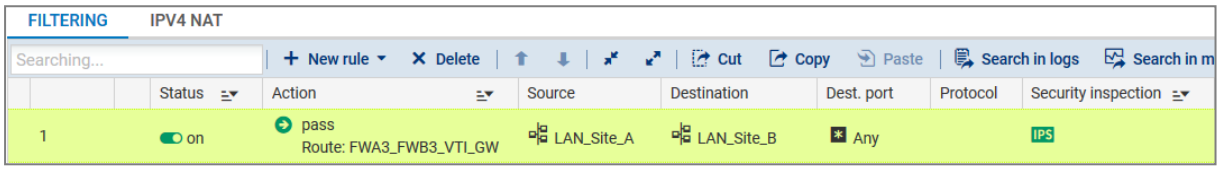
> **NOTE**
> The MAC address of firewall FWA1 must be declared in this network object

- **Interface**: select the interface on firewall FWA3 through which return packets will be transported to firewall FWA1 ("In" in the example).

Enable the route by double-clicking in the **Status** column.

Filter rule

Following the method described for firewall FWA1, create a filter rule that will send encrypted traffic through the tunnel based on the virtual IPsec interface:



Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the virtual IPsec interface of firewall 3 on site B (object FWA3_FWB3_VTI_GW in the example),

Source column

- **Source hosts**: select the network at the source of the traffic that needs to be encrypted (LAN_Site_A in the example).

Destination column

- **Destination hosts**: select or the network object (host, host group, IP address range or network [LAN_Site_B in the example] at the destination of the encrypted traffic.

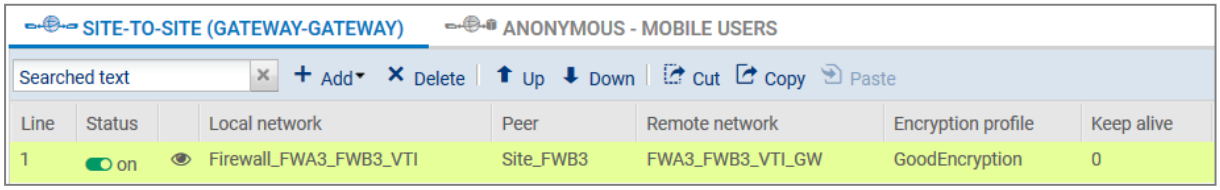
Dest. port column

- **Destination port**: select the port(s) corresponding to the protocols that need to be encrypted (Any in the example).

IPsec policy

Following the method described for firewall FWA1m create an IPsec VPN policy for the encryption of traffic processed by following FWA3:

- **Peer**: create an object corresponding to the public IP address of firewall FWB3,
- **Local network**: select the object corresponding to the local virtual IPsec interface (Firewall_FWA3_FWB3_VTI in the example),
- **Remote network**: select the object corresponding to the remote virtual IPsec interface (FWA3_FWB3_VTI_GW in the example).



Settings for firewall FWB1

The configuration of firewall FWB1 is symmetrical with regard to the one created for firewall FWA1.

Following the method described for configuring firewall FWA1, define the elements below:

Virtual IPsec interface

- **Name** (FWB1_FWA1_VTI in the example),
- **IP address** (192.168.101.2 in the example),
- **Mask** (255.255.255.252 in the example).

Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Return route to firewall FWA1

- **Gateway**: create ( icon) the network object corresponding to the virtual IPsec interface of firewall 1 on site A (FWB1_FWA1_VTI_GW with the IP address 192.168.101.1 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 1 on sites B and A (FWB1_FWA1_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWB2

- **Gateway**: create the network object corresponding to firewall 2 on site B (FWB2 in the example),

> **NOTE**
> The MAC address of firewall FWB2 must be declared in this network object.

- **Interface**: select the interface on firewall FWB1 through which return packets will be transported to firewall FWB2 (Dmz1 in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWB3

- **Gateway**: create the network object corresponding to firewall 3 on site B (FWB3 in the example),

> **NOTE**
> The MAC address of firewall FWB3 must be declared in this network object.

- **Interface**: select the interface on firewall FWB1 through which return packets will be transported to firewall FWB3 (Dmz2 in the example).

Enable the route by double-clicking in the **Status** column.

Filter rule

- **Status:***On*,
- **Action**: *Pass*,
- **Source hosts**: LAN_Site_A in the example,
- **Destination hosts**: LAN_Site_B in the example,
- **Destination port**: Any in the example,

IPsec policy

- **Peer**: Site_FWA1 in the example,
- **Local network**: select the object corresponding to the virtual IPsec interface on firewall FWB1 (Firewall_FWB1_FWA1_VTI in the example),
- **Remote network**: select the object corresponding to the virtual IPsec interface on firewall FWA1 (FWB1_FWA1_VTI_GW in the example).

Settings for firewall FWB2

The configuration of firewall FWB2 is symmetrical with regard to the one created for firewall FWA2.

Following the method described for configuring firewall FWA1, define the elements below:

Virtual IPsec interface

- **Name:** FWB2_FWA2_VTI in the example,
- **IP address:** 192.168.102.2 in the example,
- **Mask:** 255.255.255.252 in the example,

Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Following the method described for firewall FWA1, create 2 routes that allow transporting return packets to the original firewall using the source MAC address.

Return route to firewall FWA2

- **Gateway**: create the network object corresponding to the virtual IPsec interface of firewall 2 on site A (FWB2_FWA2_VTI_GW with the IP address 192.168.102.1 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 2 on sites B and A (FWB2_FWA2_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWB1

- **Gateway**: create the network object corresponding to firewall 1 on site B (FWB1 in the example),

> **NOTE**
> The MAC address of firewall FWB1 must be declared in this network object.

- **Interface**: select the interface on firewall FWB2 through which return packets will be transported to firewall FWB1 ("In" in the example).

Enable the route by double-clicking in the **Status** column.

Filter rule

- **Action**: *Pass*,
- **Source hosts**: LAN_Site_A in the example,
- **Destination hosts**: LAN_Site_B in the example,
- **Destination Port**: Any in the example,

IPsec policy

- **Peer**: create an object corresponding to the public IP address of firewall FWA2,
- **Local network**: select the object corresponding to the local virtual IPsec interface (Firewall_FWB2_FWA2_VTI in the example),
- **Remote network**: select the object corresponding to the remote virtual IPsec interface (FWB2_FWA2_VTI_GW in the example).

Settings for firewall FWB3

The configuration of firewall FWB3 is symmetrical with regard to the one created for firewall FWA3.

Following the method described for configuring firewall FWA1, define the elements below:

Virtual IPsec interface

- **Name:** FWB3_FWA3_VTI in the example,
- **IP address:** 192.168.103.2 in the example,
- **Mask:** 255.255.255.252 in the example,

Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Return route to firewall FWA3

- **Gateway**: create the network object corresponding to the virtual IPsec interface of firewall 3 on site A (FWB3_FWA3_VTI_GW with the IP address 192.168.103.1 in the example),
- **Interface**: select the local virtual interface defined for the IPsec tunnel between firewalls 3 on sites B and A (FWB3_FWA3_VTI in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FWB1

- **Gateway**: create the network object corresponding to firewall 1 on site B (FWB1 in the example),

> **NOTE**
> The MAC address of firewall FWB1 must be declared in this network object.

- **Interface**: select the interface on firewall FWB3 through which return packets will be transported to firewall FWB1 ("In" in the example).

Enable the route by double-clicking in the **Status** column.

Filter rule

- **Action**: *Pass*,
- **Source hosts**: LAN_Site_A in the example,
- **Destination hosts**: LAN_Site_B in the example,
- **Destination port**: Any in the example,

IPsec policy

- **Peer**: create an object corresponding to the public IP address of firewall FWA3,
- **Local network**: select the object corresponding to the local virtual IPsec interface (Firewall_FWB3_FWA3_VTI in the example),
- **Remote network**: select the object corresponding to the remote virtual IPsec interface (FWB3_FWA3_VTI_GW in the example).

Scenario 2: proxy distribution

Settings for Firewall FW1

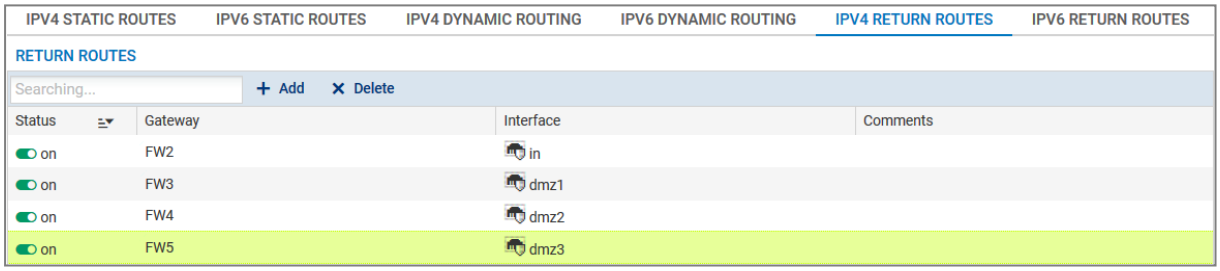
Static routing

Even though the firewall performs routing in the filter policy (Policy Based Routing) in this configuration, **a default route or an explicit static route to the remote network needsto be defined**.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return routes

Create 4 routes that allow transporting return packets to the original firewall using its source MAC address:



Return route to firewall FW2

In the *Return routes* tab in the **Configuration** > **Network** > **Routing** menu, click on **Add** and fill in the mandatory fields:

- **Gateway**: create (icon) the network object corresponding to firewall 2 on the site (FW2 in the example),

> **NOTE**
> The MAC address of firewall FW2 must be declared in this network object.

- **Interface**: select the interface on firewall FW1 through which return packets will be transported to firewall FW2 ("In" interface in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FW3

- **Gateway**: create the network object corresponding to firewall 3 on the site (FW3 in the example),

> **NOTE**
> The MAC address of firewall FW3 must be declared in this network object

- **Interface**: select the interface on firewall FW1 through which return packets will be transported to firewall FW3 ("dmz1" interface in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FW4

- **Gateway**: create the network object corresponding to firewall 4 on the site (FW4 in the example),

> **NOTE**
> The MAC address of firewall FW4 must be declared in this network object.

- **Interface**: select the interface on firewall FW1 through which return packets will be transported to firewall FW4 ("dmz2" interface in the example).

Enable the route by double-clicking in the **Status** column.

Return route to firewall FW5

- **Gateway**: create the network object corresponding to firewall 5 on the site (FW5 in the example),

> **NOTE**
> The MAC address of firewall FW5 must be declared in this network object.

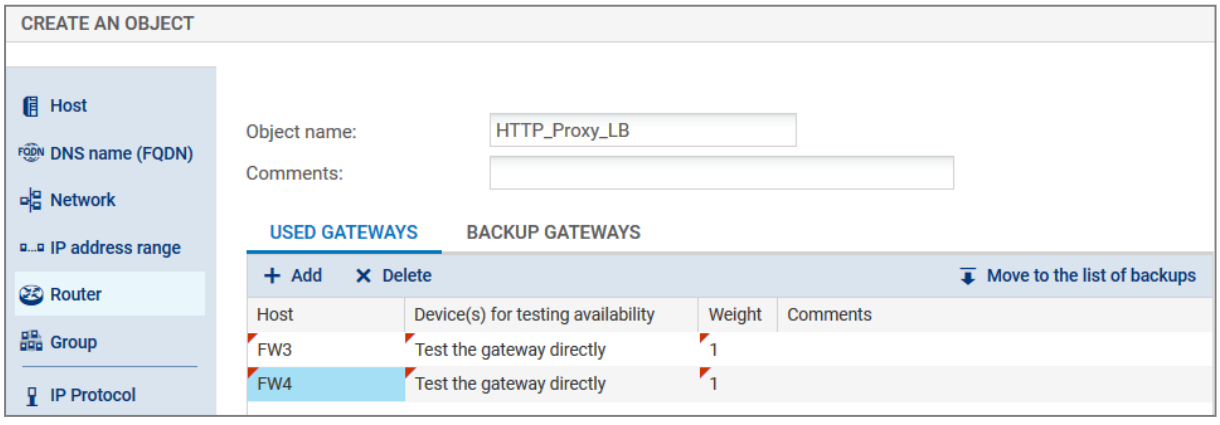
- **Interface**: select the interface on firewall FW1 through which return packets will be transported to firewall FW5 ("dmz3" interface in the example).

Enable the route by double-clicking in the **Status** column.

Load balancing

Packets going to two firewalls on which the HTTP proxy has been enabled will be balanced on a router object made up of firewalls FW3 and FW4.

1. In the **Configuration** > **Objects** > **Network objects** menu, click on **Add** and choose *Router*.
2. Enter a name for this object (HTTP_Proxy_LB in the example).
3. In the *Gateways used* tab, click on **Add** and select firewall 3 on the site (FW3). Leave the value **Test the gateway directly** for the column *Device(s) for testing availability*. Likewise, leave the value **1** in the *Weight* column.
4. Repeat this operation to add gateway FW4:



5. In the Advanced properties panel, check that the various fields have been entered with the following values:
   - **Load balancing**: *By connection* (each new HTTP connection will be sent to one of the gateways declared based on round robin scheduling),
   - **Enable backup gateways**: *When all gateways cannot be reached*,
   - **Enable all backup gateways when unavailable**: unselected
   - **If no gateways are available**: *Default route*.
6. Confirm the creation of the router object by clicking on **Create**.

Filter rules

In order for traffic (HTTP, SSL, IMAP and POP3) to be directed to firewalls on which the right proxy has been enabled, create three filter rules (**Configuration** > **Security policy** > **Filter and NAT** menu) including a routing directive:

- HTTPS to firewall FW2 in order to request action from its SSL proxy,
- HTTP to the object HTTP_Proxy_LB in order to balance the load between the HTTP proxies on firewalls FW3 and FW4,
- SMTP/POP3/IMAP to firewall FW5 in order to request action from its SMTP proxy,

Since security inspections are conducted on firewalls that have enabled various proxies, security rules on firewall FW1 may be in Firewall mode.

HTTPS traffic

Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the object corresponding to the firewall that has enabled the SSL proxy (FW2 in the example).

Source column

- **Source hosts**: select the network at the source of the HTTPS traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select the Internet object.

Dest. port column

- **Destination port**: select the https object.

Security inspection column

- **Inspection level**: select the Firewall mode.

HTTP traffic

Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the router object made up of firewalls FW3 and FW4 which have enabled the HTTP proxy (HTTP_Proxy_LB in the example).

Source column

- **Source hosts**: select the network at the source of the HTTP traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select the Internet object.

Dest. port column

- **Destination port**: select the http object.

Security inspection column

- **Inspection level**: select the Firewall mode.

SMTP/IMAP/POP traffic

Action column

- **Action**: set the action to **Pass**,
- **Gateway - router**: select the object corresponding to the firewall that has enabled the SMTP proxy (FW5 in the example).

Source column

- **Source hosts**: select the network at the source of the mail traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select the Internet object.

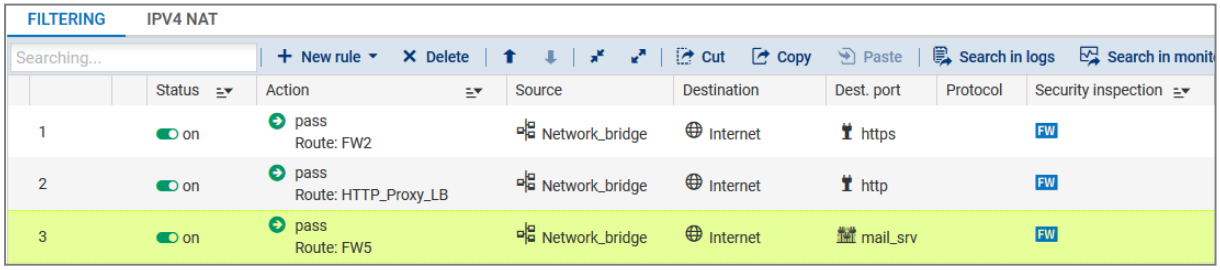
Dest. port column

- **Destination port**: select the object mail_srv (this object covers SMTP, IMAP and POP3).

Security inspection column

- **Inspection level**: select the Firewall mode.

The filter policy will then look like this:



Settings for Firewall FW2

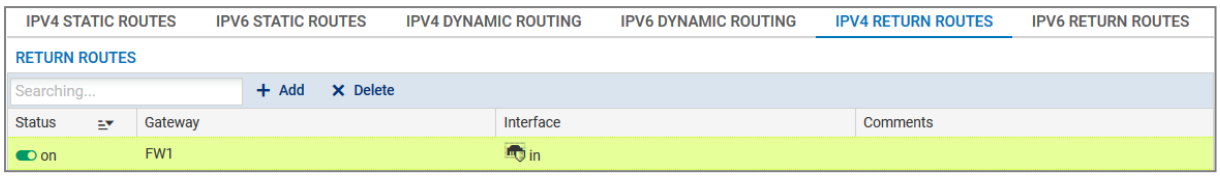
Static routing

A default route or an explicit static route to the remote network needsto be defined.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return route

Create a route that would allow transporting return packets to the original firewall using its MAC address:



Return route to firewall FW1

- **Gateway**: create the network object corresponding to firewall 1 on the site (FW1 in the example),

> **NOTE**
> The MAC address of firewall FW1 must be declared in this network object.

- **Interface**: select the interface on firewall FW2 through which return packets will be transported to firewall FW1 ("In" interface in the example).

Enable the route by double-clicking in the **Status** column.

Enabling the SSL proxy

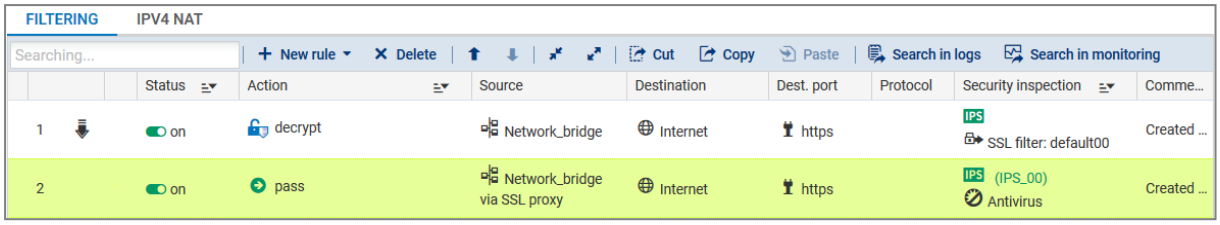
In the **Configuration** > **Security policy** > **Filter and NAT** menu, expand the **New rule** menu and select

SSL inspection rule:

Fill in the fields in the wizard with the following values:

- **Source hosts**: select the object representing the hosts or network at the source of the HTTPS traffic (object Network_bridge in the example),
- **Destination**: select Internet,
- **Destination port**: leave it as the https object.
- **Inspection profile**: choose the inspection profile to apply (the choice suggested by default applies the profile IPS_00 to incoming traffic and the profile IPS_01 to outgoing traffic),
- **SSL filter policy**: select the SSL filter policy to apply (default00 in the example),
- **Antivirus**: enable the antivirus by selecting the value **On**,
- **Source hosts**: select the object representing the hosts or network at the source of the HTTPS traffic (object Network_bridge in the example),
- **Destination**: select Internet,
- **Destination port**: leave it as the https object.
- **Inspection profile**: choose the inspection profile to apply (the choice suggested by default applies the profile IPS_00 to incoming traffic and the profile IPS_01 to outgoing traffic),
- **SSL filter policy**: select the SSL filter policy to apply (default00 in the example),
- **Antivirus**: enable the antivirus by selecting the value **On**,

The filter policy will then look like this:



Settings for Firewalls FW3 and FW4

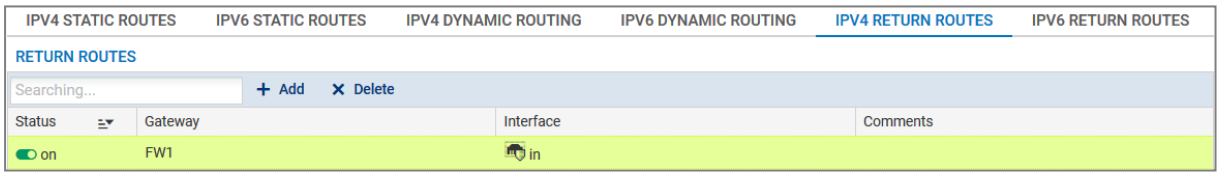
Static routing

A default route or an explicit static route to the remote network needsto be defined.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return route

Create a route that would allow transporting return packets to the original firewall using its MAC address:



Return route to firewall FW1

On each of the firewalls (FW3 and FW4), create the following return route:

- **Gateway**: create the network object corresponding to firewall 1 on the site (FW1 in the example),

> **NOTE**
> The MAC address of firewall FW1 must be declared in this network object.

- **Interface**: select the interface on firewall FW3 (respectively for firewall FW4) through which return packets will be transported to firewall FW1 ("In" interface in the example).

Enable the route by double-clicking in the **Status** column.

Enabling the HTTP proxy

In the **Configuration** > **Security policy** > **Filter and NAT** menu, expand the **New rule** menu and select **Single rule**.

Action column

- **Action**: set the action to **Pass**,

Source column

- **Source hosts**: select the network at the source of the electronic mail traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select Internet.

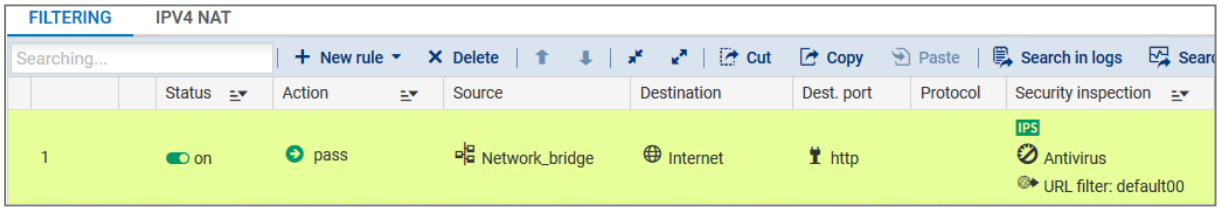
Dest. port column

- **Destination port**: select the http object.

Security inspection column

- **Inspection profile**: choose the inspection profile to apply (the choice suggested by default applies the profile IPS_00 to incoming traffic and the profile IPS_01 to outgoing traffic),
- **Antivirus**: enable the antivirus by selecting the value **On**,
- **URL filter**: select the URL filter policy to apply (default00 in the example),

The filter policy will then look like this:



Settings for Firewall FW5

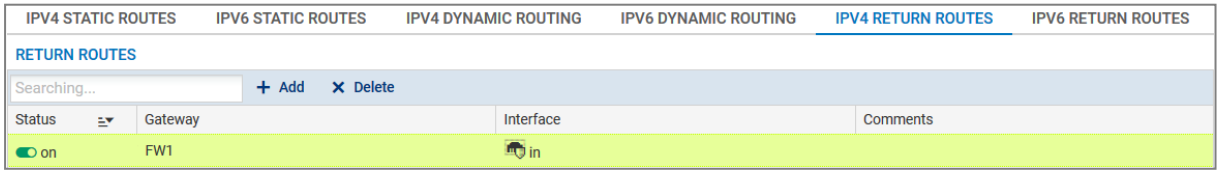
Static routing

A default route or an explicit static route to the remote network needsto be defined.

The first action that the firewall performs is indeed to check that it has a route to the remote site before looking up its filter policy. The absence of a route will result in packets being rejected.

Return route

Create a route that would allow transporting return packets to the original firewall using its MAC address:



Return route to firewall FW1

- **Gateway**: create the network object corresponding to firewall 1 on the site (FW1 in the example),

NOTE
The MAC address of firewall FW1 must be declared in this network object.

- **Interface**: select the interface on firewall FW2 through which return packets will be transported to firewall FW1 ("In" interface in the example).

Enable the route by double-clicking in the **Status** column.

Enabling the SMTP proxy

In the **Configuration** > **Security policy** > **Filter and NAT** menu, expand the **New rule** menu and select **Standard rule**.

Action column

- **Action**: set the action to **Pass**,

Source column

- **Source hosts**: select the network at the source of the electronic mail traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select Internet.

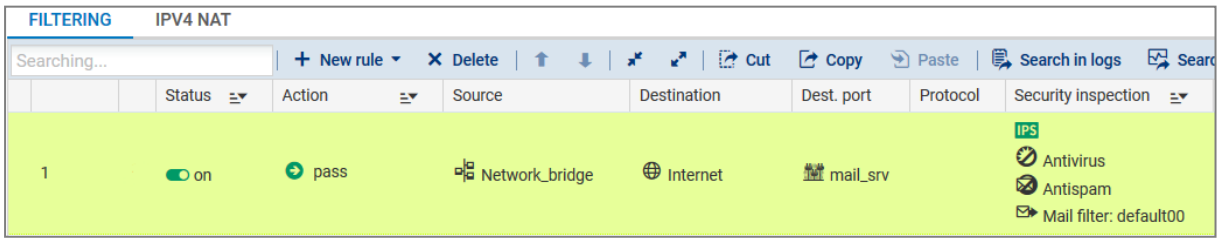
Dest. port column

- **Destination port**: select the object mail_srv containing SMTP, IMAP and POP3.

Security inspection column

- **Inspection profile**: choose the inspection profile to apply (the choice suggested by default applies the profile IPS_00 to incoming traffic and the profile IPS_01 to outgoing traffic),
- **Antivirus**: enable the antivirus by selecting the value **On**,
- **Antispam**: enable the antispam by selecting the value **On**,
- **SMTP filter**: select the SMTP filter policy to apply (default00 in the example),

The filter policy will then look like this:



Settings for Firewall FW6

Return routes

Return routes do not need to be defined on this firewall: since the various proxies enabled on firewalls FW2 to FW5 (SSL, HTTP, SMTP/POP3/IMAP) perform address translation by default

(**Keep original source IP address** option unselected in the settings of each of these protocols), firewall FW6 therefore knows the source of source packets for each traffic stream.

Filter rule

Create a filter rule that allows HTTP, HTTPS, SMTP, IMAP and POP3 traffic going to the Internet. Since security inspections are conducted on firewalls that have enabled various proxies, the security rule on firewall FW6 may be in Firewall mode.

Action column

- **Action**: set the action to **Pass**,

Source column

- **Source hosts**: select the network at the source of the traffic (Network_bridge in the example).

Destination column

- **Destination hosts**: select the Internet object.

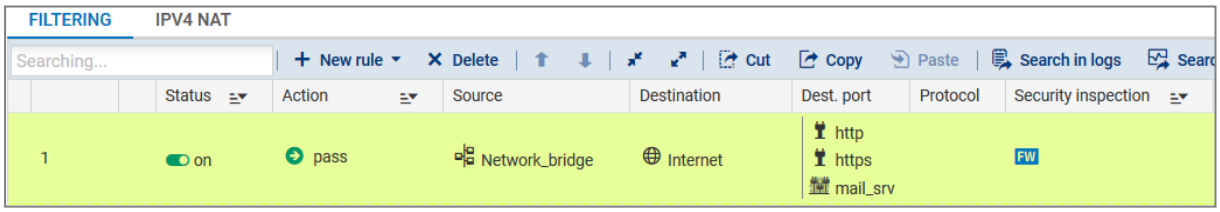
Dest. port column

- **Destination port**: select the http, https and srv_mail objects.

Security inspection column

- **Inspection level**: select the Firewall mode.

The filter rule will then look like this:



NAT rule

NAT rule

Create a NAT rule meant to mask internal networks behind the public address of firewall FW6.

In the *NAT* tab in the **Configuration** > **Security policy** > **Filter and NAT** menu, expand the **New rule** menu and select **Standard rule**:

Status column

- Enable the rule by switching its status to **On**.

Original traffic column

Source column

- **Source hosts**: select the network at the source of the traffic (**Network_bridge** in the example).

Destination column

- **Destination hosts** (*general* tab): select the **Internet** object.
- **Out interface** (*Advanced properties* tab): select the outgoing interface to the Internet (**out** interface in the example).

Dest. port column

- **Destination port**: select the **Any** object.

Traffic after translation column

Source column

- **Translated source host**: select the network object corresponding to the public address of firewall FW6 (**Firewall_out** in the example),
- **Translated source port**: choose the **ephemeral** object and select the option **select a random translated source port**.

Destination column

- **Translated destination host**: leave the **Any** object suggested by default.

The NAT rule will then look like this:

		Original traffic (before translation)				Traffic after translation			
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	on	Network_bridge	Internet interface: out	Any	→	Firewall_out	ephemeral	Any	

Further reading

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

documentation@stormshield.eu