TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SD-WAN: SELECTING THE BEST NETWORK LINK

Product concerned: SNS 4.3 LTSB, SNS 4.8 LTSB, SNS 5 and higher versions

Document last updated: December 4, 2025

Reference: sns-en-sd-wan_selecting_best_network_link-technical_note

Table of contents

Getting started ... 4

Understanding the various components of the SNS SD-WAN ... 5

Understanding monitoring parameters ... 5
Detection method and port ... 5
Timeout (s) ... 5
Interval (s) ... 5
Failures before degradation ... 5
Understanding the metrics of the SD-WAN SLA ... 6
Latency (ms) ... 6
Jitter (ms) ... 6
Packet loss rate (%) ... 6
Unavailability rate ... 6
Assessing the values to apply to each metric ... 6

Understanding the switch mechanism and how links are chosen ... 8

New incoming connections ... 8
Existing connections ... 11
Default route with failover (no load balancing) or static routing ... 11
Default route with load balancing or policy-based routing ... 11
Connections initialed by the firewall ... 12

Monitoring SD-WAN links from the firewall's administration interface ... 13

Overview: dashboard of health indicators ... 13
Detailed view: the SD-WAN monitoring module ... 13
Real time tab ... 13
Real time chart tab ... 14
History tab ... 15

Example 1: prioritizing VoIP traffic ... 17

Creating objects ... 18
Creating host objects for operator gateways ... 18
Creating host objects for VoIP servers ... 19
Creating the router object that will apply constraints for VoIP traffic ... 19
Creating the PBR rule for VoIP traffic ... 20

Example 2: IPsec VPN tunnel with link failover/load balancing ... 21

Tunnels based on the IPsec policy (PB - policy based) ... 21
Network architecture ... 21
IPsec architecture ... 21
Configuring the FW-LILLE firewall ... 22
Configuring the FW-LYON firewall ... 25
IPsec tunnels based on virtual IPsec interfaces (VTI) ... 28
Network architecture ... 28
IPsec architecture ... 28
Configuring the FW-LILLE firewall ... 29
Configuring the FW-PARIS firewall ... 35
IPsec tunnels based on virtual IPsec interfaces (VTI) in a hub and spoke configuration ... 41
Configuring the FW-LILLE firewall ... 42
Configuring the FW-PARIS firewall ... 44

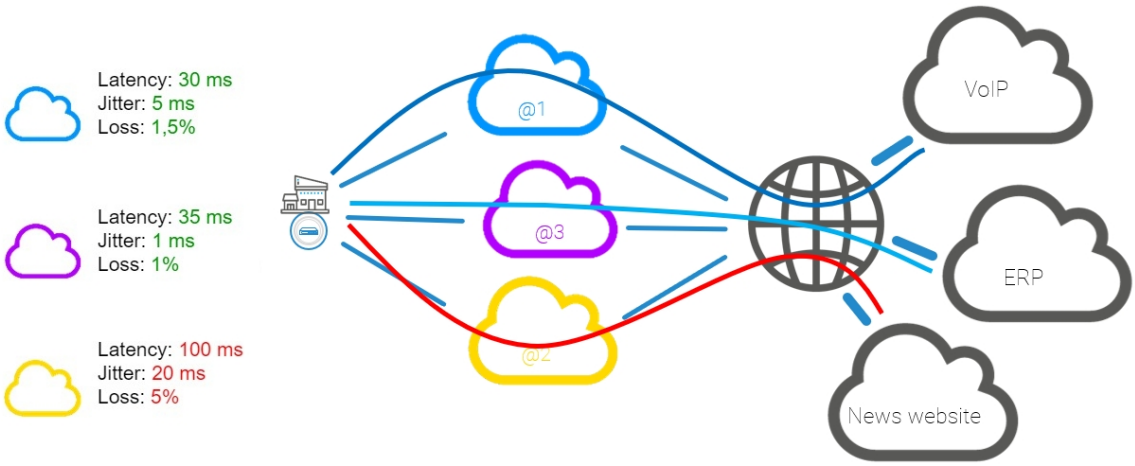
Example 3: NAT rules with a failover between the three outgoing links of the LILLE site 45
Creating the router object that will be the default route 45
Setting this router object as the FW-LILLE firewall's gateway 46
Creating the filter rule that allows internal networks to access the Internet 46
Creating address translation (NAT) rules for traffic towards the Internet 46
Example 4: using router objects in the SSL proxy 48
Routing principle 48
Creating the router object that will be used for routing 48
Default routing 49
Adding the router object as the default route 49
Creating an SSL inspection rule 49
Policy-based routing 49
Creating an SSL inspection rule 49
Further reading 51

Getting started

SD-WAN (software-defined wide area network) is a set of software features with which interconnected secure networks and multiple WAN links can be more easily managed.
One of the functional approaches in SD-WAN is its ability to automatically and transparently choose the network links to take depending on the traffic and its associated performance constraints, such as accepted latency, availability rate, etc.

This technical note is intended for organizations that have multiple WAN access links (Internet, branches, etc.) and want to optimize the selection of links based on traffic type (VoIP, Web, ERP, etc.).

To implement this approach, administrators must configure the available links and define router objects that factor in the desired service level agreement (SLA) constraints, which will be used, based on the intended configuration, as the default gateway in static routes or in the policy-based routing (PBR) rules of the traffic in question.



Understanding the various components of the SNS SD-WAN

Understanding monitoring parameters

Detection method and port

Two methods for detecting link availability and performance are offered on SNS firewalls:

- ICMP: in this method, ICMP Request packets are regularly sent over each link (two packets are sent during each detection request).
- TCP Probe: this method is based on requests to the TCP port used by the application server to be reached.
  The availability and performance of each link are therefore tested by initiating a connection to the TCP service from the firewall to the target object, by using the associated port (only one connection attempt is sent during each detection request).

NOTE
The ICMP method is preferred, unless ICMP is blocked by a device that is located between the SNS firewall and the target, or when the target does not accept ICMP requests.

If several application servers are used for traffic covered by an SD-WAN SLA, Stormshield recommends placing these servers in a network object group and using this group as the target of availability tests. In this case, the results of availability tests will be the average of the results of tests to each server.

Timeout (s)

This refers to the maximum length of time to wait for a response to a connection attempt with the chosen detection method.

Past this value, the connection attempt will be considered a failure and the number of attempts will be incremented by one unit, until it reaches the configured number of failures before the target object is declared unreachable or the link is declared degraded (only if SLA thresholds have been configured).

Interval (s)

This is the length of time between two connection attempts.

Failures before degradation

This refers to the maximum number of failed connection attempts before the target object is declared unreachable or the link is declared degraded (only if SLA thresholds have been configured).

Understanding the metrics of the SD-WAN SLA

Latency (ms)

SD-WAN latency on SNS firewalls represents the amount of time between when a packet is sent and when a response to it is received. It is therefore actually a round-trip time (RTT).
This parameter depends greatly on the type of traffic and ISPs.
The **Frequency (s)** parameter determines how much time passes between two latency measurements.
The latency shown in the SD-WAN real-time monitoring module corresponds to the last latency value measured for each gateway.

Jitter (ms)

Jitter represents how latency varies over time.
It is calculated based on all the latency values measured over the past 10 minutes.
The value shown in the SD-WAN real-time monitoring module therefore corresponds to the average jitter over the past 10 minutes.

Packet loss rate (%)

This is the ratio of the number of connection requests sent to the number of responses received.
On SNS firewalls, the percentage tolerated can be configured to the closest tenth.
It is calculated based on all packets lost during connection tests over the past 10 minutes.

The value shown in the SD-WAN real-time monitoring module therefore corresponds to the average packet loss rate over the past 10 minutes.

Unavailability rate

This is the ratio of how often the gateway is available to how often it is not available.
Strictly speaking, this is not an SD-WAN threshold; its main function is to show statistics about the availability of gateways.
There is therefore no need to enter a maximum value for this parameter.

The value shown in the SD-WAN real-time monitoring module therefore represents the average unavailability rate over the past 10 minutes.

Assessing the values to apply to each metric

It can be tedious and counterproductive to apply thresholds individually to objects used in a filter policy in a production environment due to traffic switching to different links regularly and for unwarranted reasons.

To assess the values to apply to each metric without disrupting production, Stormshield suggests proceeding as follows:

1. Create a test router object on which you have set the recommended metric values given by your ISPs and software solution vendors (VoIP, ERP, etc.).

2. Use this router object in a neutral filter rule, placed last in the security policy (before the *deny all* rule, if used), to trigger monitoring on the router and its gateways, and to observe behavior (changing links) relating to the values of the various metrics. To create this rule, refer to the section on Creating the filter rule for VoIP traffic.
3. Refine these values until you obtain the desired behavior with regard to the traffic in question.

By doing so, when the values of the metrics change, they do not affect production traffic at all, and you will then be able to refine values as often as you need before adopting them in the filter rule that applies to production traffic.

When you observe the values recorded for the various metrics (steps 2 and 3), do note that the data shown in the SD-WAN monitoring graphs in the SNS web administration interface are stored in a local database, and are then regularly aggregated to reduce the amount of disk space used.

You are therefore advised to use an SNMP-based monitoring solution (such as Zabbix, Centreon, etc.) and on the STORMSHIELD-ROUTE-MIB v4.3.x MIB - which can be downloaded from the **Downloads** menu in MyStormshield - to observe the real-time values of the various metrics and store these records over longer periods so that the appropriate values can be better refined.

More information on SD-WAN SLA metrics.

Understanding the switch mechanism and how links are chosen

When each metric is measured or calculated, each link is evaluated: this involves comparing the last measurement (latency) or last metric calculation (jitter or packet loss rate) with the value set in the SD-WAN SLA. If this measurement does not meet the thresholds that have been configured, the link will be considered degraded.

A link may therefore be described by 3 possible statuses:

- Optimal: the link is available and metric calculations/measurements meet the defined SLA thresholds.
- Degraded: one or several metrics do not meet the defined SLA thresholds.
- Unavailable: the link cannot be used following an incident.

The tables below show the link switching mechanisms, and the chosen links for the various possible types of connections.

In this document, the 3 possible statuses are represented by the following symbols:

- : optimal link,
- : degraded link,
- : unavailable link.

New incoming connections

In a four-link configuration (two main links and two backup links), the table below shows how the links will be chosen based on their respective status at a given moment, and based on the chosen configuration (whether there is load balancing, threshold values, etc.).

Main links		Backup links		Order of links used according to the configuration				
				No load balancing	With load balancing			
					When at least one gateway cannot be reached		When all gateways cannot be reached	
Link 1	Link 2	Link 3	Link 4			Enable all backup gateways		Enable all backup gateways
✓	✓	✓	✓	1	1 and 2	1 and 2	1 and 2	1 and 2
⚠	✓	✓	✓	2	2	2	2, 3 and 4	2 and 3
⚠	⚠	✓	✓	3	3 and 4	3 and 4	3 and 4	3 and 4
⚠	⚠	⚠	✓	4	4	4	4	4
⚠	⚠	⚠	⚠	1	1 and 2	1 and 2	1 and 2	1 and 2
⚠	✗	⚠	⚠	1	1	1	1, 3 and 4	1 and 3
⚠	✗	✓	⚠	3	3	3	3	3
✗	✓	⚠	⚠	2	2	2	2	2
✗	✗	⚠	⚠	3	3 and 4	3 and 4	3 and 4	3 and 4
✗	✗	✗	⚠	4	4	4	4	4

Main links		Backup links		Order of links used according to the configuration				
				No load balancing	With load balancing			
					When at least one gateway cannot be reached		When all gateways cannot be reached	
Link 1	Link 2	Link 3	Link 4			Enable all backup gateways		Enable all backup gateways
✗	✗	✗	✗	The policy defined in the router object's **If no gateways are available** field is applied: • Default routing (*OnFailPolicy = pass*), • Do not route (*OnfailPolicy = block*).				
✗	✗	✓	✗	3	3	3	3	3
✗	✓	✓	✗	2	2	2	2 and 3	2 and 3
✗	✓	✓	✓	2	2	2	2, 3 and 4	2 and 3
✓	✓	✓	✓	1	1 and 2	1 and 2	1 and 2	1 and 2

Existing connections

Default route with failover (no load balancing) or static routing

What happens to passing connections when the gateway is changed	
Address translation (NAT)	**When the gateway changes***
No NAT	Connections are kept during the switch
With NAT (NAT policy, or via a proxy)	RST packet is sent to the client of a TCP connection, and the connection table is purged (UDP and TCP)

*depending on the rules described in the table New incoming connections.

Default route with load balancing or policy-based routing

<table>
<tr><th colspan="7">What happens to passing connections when the gateway is changed</th></tr>
<tr><th rowspan="2">Address translation (NAT)</th><th colspan="6">When the gateway status changes</th></tr>
<tr><th> </th><th> </th><th> </th><th> </th><th> </th><th> </th></tr>
<tr><td>No NAT</td><td rowspan="2">Connections are kept</td><td colspan="2">Connections are kept during the switch</td><td rowspan="2">Connections are kept</td><td colspan="2" rowspan="2">None</td></tr>
<tr><td>With NAT (NAT policy, or via a proxy)</td><td colspan="2">RST packet is sent to the client of a TCP connection, and the connection table is purged (UDP and TCP)</td></tr>
</table>

Connections initialed by the firewall

What happens to connections initialed by the firewall when the gateway is changed
When the gateway changes*
The connection table is purged (UDP and TCP) and service resumes

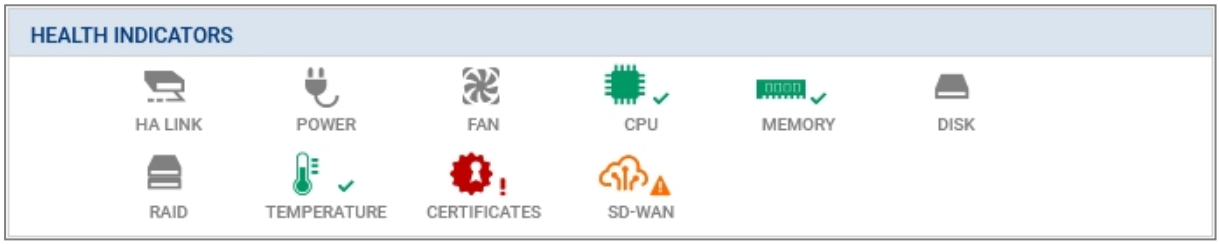
*depending on the rules described in the table New incoming connections.

Monitoring SD-WAN links from the firewall's administration interface

The monitoring module makes it possible to show the status of SD-WAN gateways as well as the values of the metrics relating to SLA thresholds.

Overview: dashboard of health indicators

The SD-WAN dashboard, available in the **Monitoring** tab > **Dashboard** module > **Health indicators** section, offers a quick view of the status of all SD-WAN objects:



The color of the SD-WAN icon varies according to the status of the routers and gateways used in the firewall configuration:

- Green: all router gateways are functional and meet the defined SD-WAN SLA criteria,
- Orange: a router has a degraded status as one of its gateways has a degraded status, or cannot be reached,
- Rouge: a router cannot be reached as all its gateways are unreachable.

Clicking on this icon will take you directly back to **Monitoring** > **SD-WAN**.

Detailed view: the SD-WAN monitoring module

The **SD-WAN** module, which can be accessed from **Monitoring** > **Monitoring**, shows details of routers and gateways used in the firewall's routing settings (default route, static routes and policy-based routing).

Real time tab

The **Real time** tab shows information about the status of monitored routers and gateways, as well as the SD-WAN SLA values of these gateways.

The values may be as follows:

Type	Status	SLA status
Gateway	• **Enabled**, • **Standby** (redundant), • **Unreachable**.	• **Good**, • **Degraded**, • **Unreachable**.

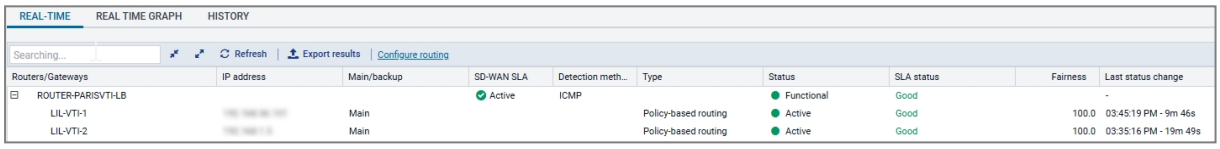
Router	• **Functional** (load balancing), • **Functional** (redundant - at least one gateway is on standby), • **Degraded**, • **Unreachable**.	• **Good**, • **Degraded**, • **Unreachable**.

Example of a router with load balancing

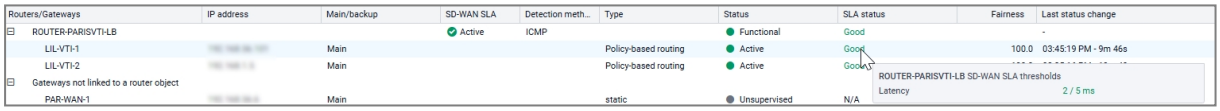
For more details on the values that the various indicators may show, refer to the module on SD-WAN monitoring in the Stormshield SNS v4 user guide.

In this example, both gateways have been enabled.

Load balancing values between both gateways are shown: they depend on the weight assigned to each gateway. When all gateways have a weight of 1, this means that each of them have been assigned 100% load balancing:



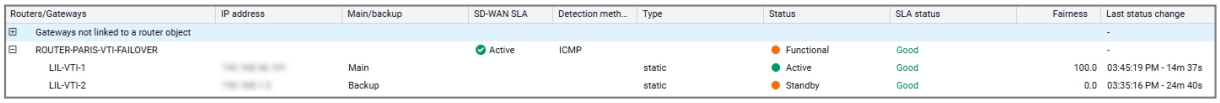
By scrolling over the SLA status of a gateway, the last measured indicator value will be shown:



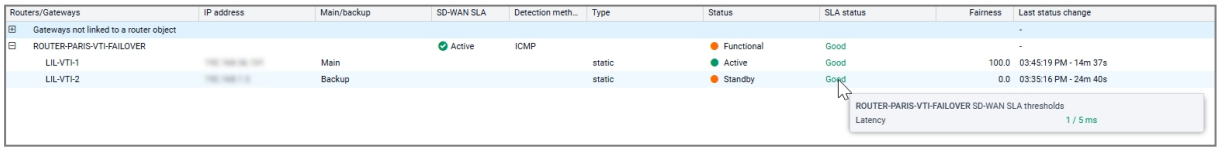
Example of a router with failover

One gateway is active, while the other is on standby.

Load balancing between both gateways is indicated: the active gateway indicates 100%, while the standby gateway is at 0%.



By scrolling over the SLA status of a gateway, the last measured indicator value will be shown:

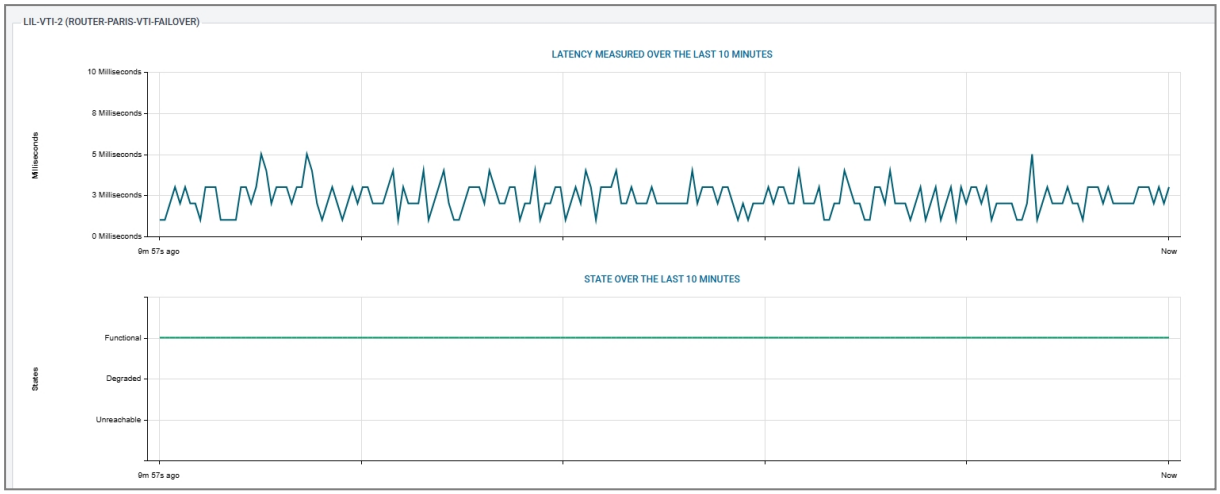


Real time chart tab

In this tab, a router gateway can be selected to display curves that show changes to the following SLA indicators over the past 10 minutes:

- Latency,
- Percentage of time spent in the various possible statuses (functional, degraded and unreachable).

Example:

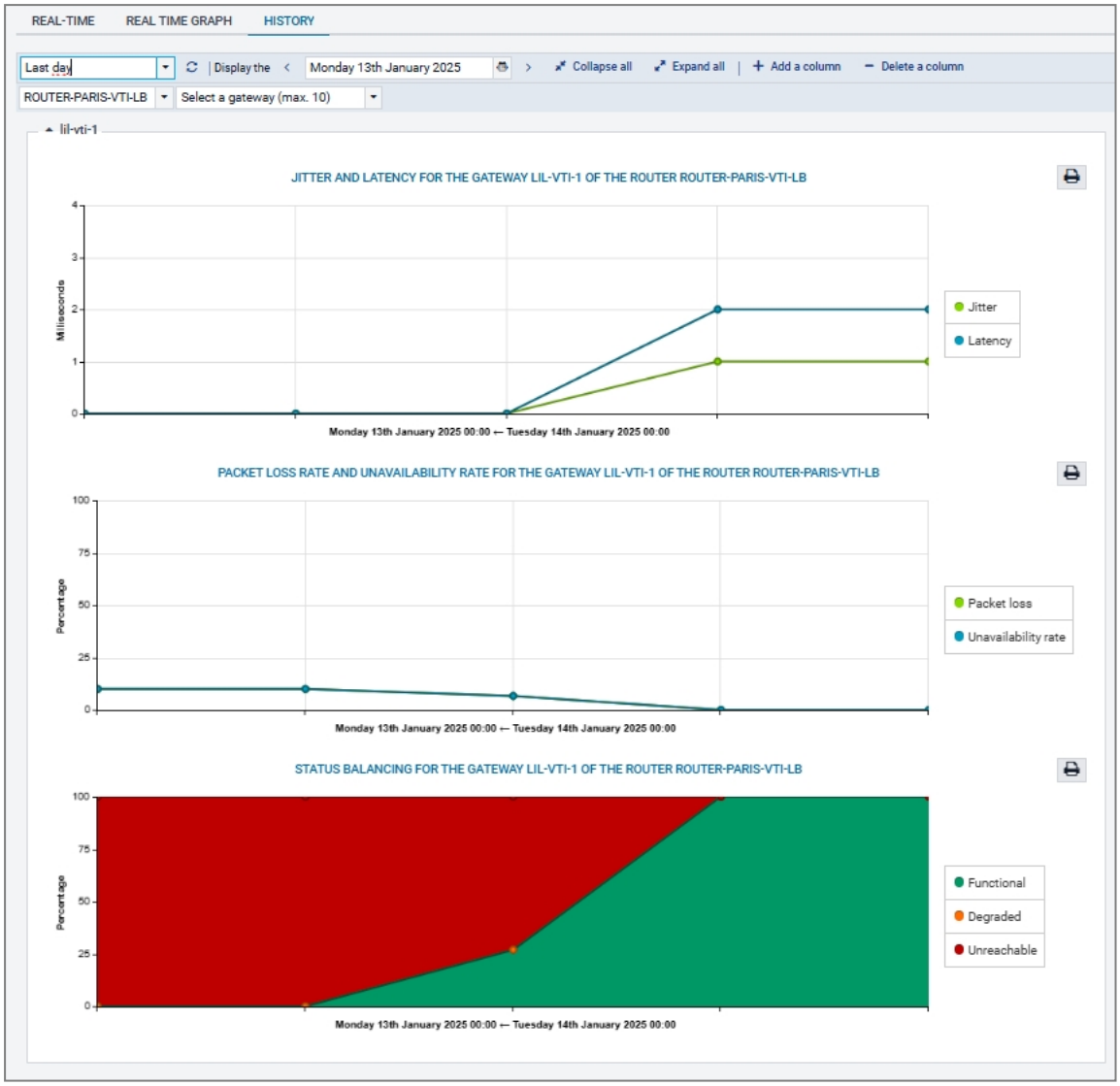


History tab

In this tab, up to five router gateways can be selected to display curves that show changes to the various SLA indicators over the selected period:

- Jitter and latency,
- Packet loss rate and unavailability rate,
- Percentage of time spent in the various possible statuses (functional, degraded and unreachable).

Example:


REAL-TIME
REAL TIME GRAPH
HISTORY
Last day
Display the
Monday 13th January 2025
Collapse all
Expand all
Add a column
Delete a column
ROUTER-PARIS-VTI-LB
Select a gateway (max. 10)
lil-vti-1
JITTER AND LATENCY FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Milliseconds
Jitter
Latency
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00
PACKET LOSS RATE AND UNAVAILABILITY RATE FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Percentage
Packet loss
Unavailability rate
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00
STATUS BALANCING FOR THE GATEWAY LIL-VTI-1 OF THE ROUTER ROUTER-PARIS-VTI-LB
Percentage
Functional
Degraded
Unreachable
Monday 13th January 2025 00:00 — Tuesday 14th January 2025 00:00

Example 1: prioritizing VoIP traffic

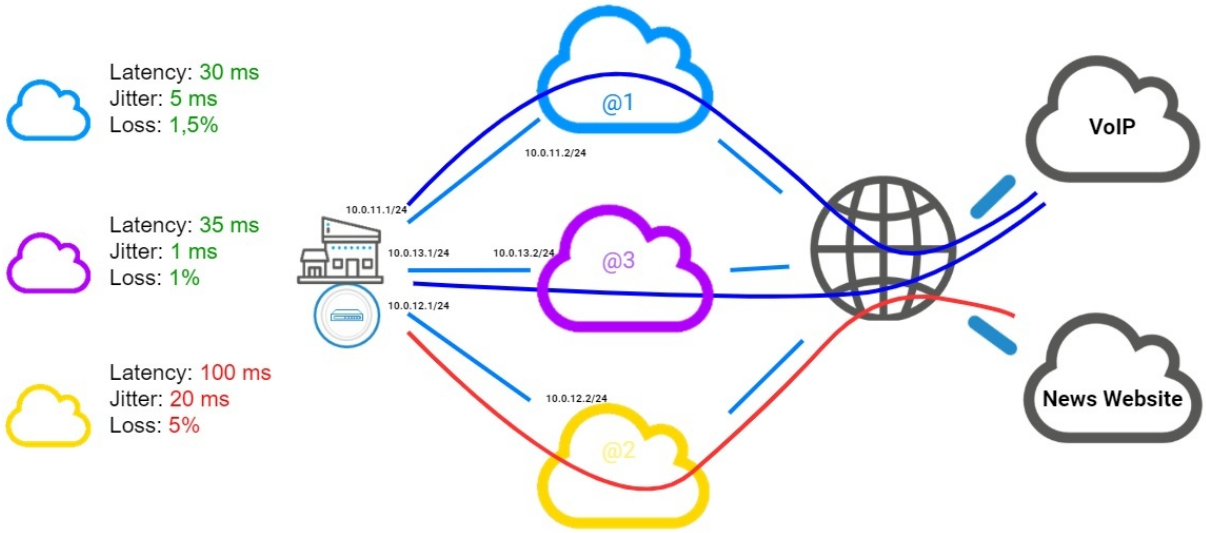
The configuration used in this technical note illustrates the example of an organization that has three remote access links:

- Two links associated with two routers (named *Router1* and *Router2* in this technical note) from an ISP,
- One link associated with one router (named *Router3* in this technical note) from another ISP,

Both links from the first ISP are used as main links, while the one from the second ISP is designated as a backup link.

Load balancing is set on active links.

The SD-WAN configuration described must allow VoIP traffic to transparently go through the network links with the highest performance at any given moment, which web traffic goes through the other link.



The table below shows how links will be chosen based on their respective statuses at a given moment:

Link 1 (Router1) Main	Link 2 (Router2) Main	Link 3 (Routeur3) Backup	Links used for VoIP with: • Load balancing • Backup gateways enabled when at least one gateway cannot be reached
✓	✓	✓	1.2
⚠	✓	✓	2.3
⚠	⚠	✓	3
⚠	⚠	⚠	1.2

Link 1 (Router1) Main	Link 2 (Router2) Main	Link 3 (Routeur3) Backup	Links used for VoIP with: • Load balancing • Backup gateways enabled when at least one gateway cannot be reached
⚠	✗	✓	3
⚠	✗	⚠	1.3
✗	✗	⚠	3
✗	✗	✗	No link - Default route
✗	✗	✓	3
✗	✓	✓	2.3

Creating objects

This step consists of creating the objects that will be needed in the configuration:

- Host objects corresponding to operator gateways (if these objects do not already exist),
- Host objects corresponding to VoIP servers (if these objects do not already exist),
- A router object that uses operator gateways and makes it possible to set constraints relating to VoIP traffic.
  This router object will be used in filter rules for VoIP traffic.

In this technical note, we will assume that three interfaces on the firewall are linked to three operator routers:

- One interface is connected to the first operator's first router (*Router1*).
  In this example, the IP address of this interface is 10.0.11.1/24.
- One interface is connected to the first operator's second router (*Router2*).
  In this example, the IP address of this interface is 10.0.12.1/24.
- One interface is connected to the second operator's router (*Router3*).
  In this example, the IP address of this interface is 10.0.13.1/24.

Creating host objects for operator gateways

In **Configuration** > **Objects** > **Network objects**:

1. Click on **Add**.
   This opens a window to create and edit objects.
2. In the menu on the left, select **Host**.
3. Name the host (first operator's first router: *Router1*).
4. Enter its IPv4 address (e.g., 10.0.11.2).
5. Click on **Create and duplicate**.
6. Repeat steps 3 to 5 for the next gateway (first operator's second router). The values chosen in this example are:

- Name: *Router2*,
- IP address: 10.0.12.2.

7. Repeat steps 3 to 4 for the last gateway (second operator's router). The values chosen in this example are:

- Name: *Router3*,
- IP address: 10.0.13.2.

8. Click on **Create**.

Creating host objects for VoIP servers

Following the steps in the section on Creating host objects for operator gateways, create the objects corresponding to the VoIP servers.

As shown in the section on Understanding monitoring parameters, if you have several VoIP servers, you are advised to place them all together in a group that will be used as the target of availability tests.

To create a group with VoIP servers

In **Configuration** > **Objects** > **Network objects**:

1. Click on **Add**.
   This opens a window to create and edit objects.
2. In the menu on the left, select **Group**.
3. Name this group (e.g., *Remote_VoIP*).
4. In the grid on the left, select the servers to include in this group (press [Ctrl] to select several objects).
5. Click on the arrow ➡ to move servers in the group being created.
6. Confirm the creation of the group by clicking on **Create**.

Creating the router object that will apply constraints for VoIP traffic

In **Configuration** > **Objects** > **Network objects**:

1. Click on **Add**.
   This opens a window to create and edit objects.
2. In the menu on the left, select **Router**.

General properties

3. Name the object (e.g., *SD-WAN_VoIP*).

Monitoring

4. For the **Detection method**, select **ICMP**.
5. Adjust the **Timeout (s)** as needed.
6. Adjust the **Interval (s)** as needed.
7. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

8. Select **SD-WAN SLA (thresholds)**.
9. Adjust the **Latency (ms)** as needed.

10. Adjust the **Jitter (ms)** as needed.
11. Adjust the **Packet loss rate (%)** as needed.
12. Do not enter an **Unavailability rate (%)**.

Gateways

13. In the **Gateways used** tab, click on **Add**.
14. In the **Gateway** column, select the object LIL-WAN-1.
15. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
16. Repeat steps 15 to 17 to add the object LIL-WAN-2.
17. In the **Backup gateways** tab, click on **Add**.
18. In the **Gateway** column, select the object LIL-WAN-3.
19. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

20. In **Advanced properties**, select **Load balancing** *No load balancing*.
21. For **Enable backup gateways**, select *When all gateways cannot be reached*.
22. Click on **Apply** then **Save**.

Creating the PBR rule for VoIP traffic

In **Configuration > Security policy > Filter - NAT**:

1. Select the rule above which you want to add the rule for VoIP traffic.
2. Click on **New rule**.
3. Select **Single rule**.
4. A new inactive rule is added to the filter policy.
   This rule is selected by default.
5. Double-click on this rule.
   The configuration window of the rule opens.
6. Click on the **General** menu on the left.
7. In the **Status** field, set the value to *On*.
8. Click on the **Action** menu on the left.
9. In the **General** tab:

- In the **Action** field, select *pass*,
- In the **Gateway - router** field, select *SD-WAN_VoIP*.

10. Click on the **Destination** menu on the left.
11. In the **General** tab, for the **Destination hosts** tab, click on **Add** and select the server or server group *Remote_VoIP*.
12. Click on the **Port - Protocol** menu on the left.
13. In the **Destination port** field, click on **Add** and select *sip_tcp*.
14. Confirm the configuration of the rule by clicking on **OK**, then on **Apply** to enable the modified filter policy.

This filter rule will then look like this:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
	on	pass Route: SD-WAN_VoIP	Any	Remote_VoIP	sip_tcp		IPS

Example 2: IPsec VPN tunnel with link failover/load balancing

This example illustrates two scenarios in which IPsec tunnels are managed through router objects:

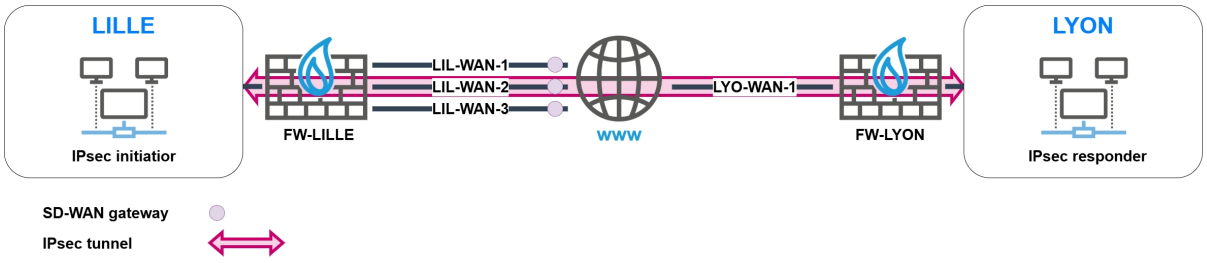
- Tunnels based on the IPsec policy (PB - policy based),
- Tunnels based on virtual IPsec interfaces (VTI).

Tunnels based on the IPsec policy (PB - policy based)

Network architecture

- The main LILLE site hosts three WAN links, two of which are main links (LIL-WAN-1 and LIL-WAN-2), and one backup link (LIL-WAN-3),
- The secondary LYON site hosts a WAN link (LYO-WAN-1).

IPsec architecture



The LILLE and LYON sites communicate through a tunnel that is based on the IPsec policy in line with the configurations described below.

LILLE site

There are several routing options for setting up the IPsec tunnel with the LYON site:

- One default route with load balancing through a router object,
- One default route with failover balancing through a router object,
- One static route with failover through a router object.

NOTE
Policy-based routing (PBR) cannot be directly used in filter rules in such configurations.

In this example, the FW-LILLE firewall uses a router object as the default gateway with failover: when the link used is degraded, the tunnel has to be kept alive by switching to another available link.

LYON site

There are several routing options for setting up the IPsec tunnel with the LILLE site:

- A default route,
- A static route.

NOTE
Policy-based routing (PBR) cannot be directly used in filter rules in such configurations.

IPsec settings:

- The IPsec peer that has been defined on the FW-LYON firewall has to be mobile (fastest solution to set up) or configured in Responder-only mode, as the FW-LYON firewall does not know which WAN access link the LILLE site will take to set up the tunnel,
- The FW-LYON firewall configuration has to allow FW-LILLE's three public IP addresses to set up site-to-site IPsec tunnels. This requires the configuration of three pre-shared keys or three certificates for the LILLE site's WAN links.

This document describes how a mobile peer is used with pre-shared key authentication.

Configuring the FW-LILLE firewall

Creating objects corresponding to LANs at the LILLE and LYON sites

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Network**.
4. Specify the **Object name** (LIL-LAN in this example).
5. Enter the **Network IP address** in the form of a network/mask. The network mask can be entered in CIDR or decimal format.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object LYO-LAN.
8. Click on **Create**.

Creating 3 objects corresponding to the LILLE WAN gateways/links

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (LIL-WAN-1 in this example).
5. Enter its **IPv4 address**.
6. Click on **Create and duplicate**.
7. Repeat steps 4 to 6 to create the object LIL-WAN-2.

8. Repeat steps 4 and 5 to create the object LIL-WAN-3.
9. Click on **Create**.

Creating the object corresponding to the FW-LYON firewall

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (FW-LYON in this example).
5. Enter the public **IPv4 address** of the LYON site's WAN link.
6. Click on **Create**.

Creating the router object that will be the default route

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Rrouter**.

General properties

4. Name the object (e.g., DEFAULT-ROUTER-LILLE).

Monitoring

For more information on monitoring parameters and SLA thresholds, refer to the SNS user guide.

5. For the **Detection method**, select **ICMP**.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** as needed.
8. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

9. Select **SD-WAN SLA (thresholds)**.
10. Adjust the **Latency (ms)** as needed.
11. Adjust the **Jitter (ms)** as needed.
12. Adjust the **Packet loss rate (%)** as needed.
13. Do not enter an **Unavailability rate (%)**.

Gateways

14. In the **Gateways used** tab, click on **Add**.
15. In the **Gateway** column, select the object LIL-WAN-1.
16. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
17. Repeat steps 14 to 16 to add the object LIL-WAN-2.
18. In the **Backup gateways** tab, click on **Add**.
19. In the **Gateway** column, select the object LIL-WAN-3.
20. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

21. In **Advanced properties**, select **Load balancing** *No load balancing*.
22. For **Enable backup gateways**, select *When all gateways cannot be reached*.
23. Click on **Apply** then **Save**.

Setting this router object as the FW-LILLE firewall's gateway

1. Go to **Configuration > Network > Routing.**
2. In the **Default gateway** field, select the router object that was created earlier (DEFAULT-ROUTER-LILLE in this example).
3. Click on **Apply** then **Save**.

Setting the IPsec peer for the LYON site

This peer is a remote gateway.

In this example, pre-shared key authentication is used.

1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**, then on **New remote gateway**.
3. In the **Remote gateway** field, select the object corresponding to the FW-LYON firewall's public IP address (LYO-WAN-1 in the example).
4. Enter a name for this peer (FW-LYON in the example).
5. Select the **IKEv2** version.
6. Choose the **IKE profile** to use.
7. Click on **Next**.
8. For the **Authentication type**, select **Pre-shared key (PSK)**.
9. Set the **Pre-shared key** and confirm it.
10. Click on **Next**.
    You will be shown a summary of the peer's details.
11. Click on **Finish**.
    Details on the peer are shown.
12. Ensure that the value of the **Local address** is **Any**.

> **NOTE**
> In order for one of the 3 FW-LILLE WAN links to be used, the value of the **Local address** field has to be **Any**.

13. In the **Advanced properties** section, set the **DPD** field to **High**.

> **NOTE**
> The **DPD** (Dead Peer Detection) option has to be set to **High** to force the IPsec tunnel to be renegotiated as quickly as possible when the link is down.

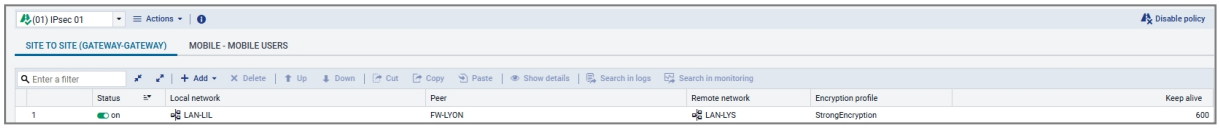
14. Confirm changes by clicking on **Apply** then on **Save**.
15. Changes can be applied immediately by clicking on **Yes, activate the policy**.

Creating the IPsec policy to set up the tunnel with the FW-LYON peer

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Site-to-site (gateway-gateway)** tab.
2. Click on **Add**, then on **Standard site-to-site tunnel.**
3. In the **Local resources** field, select the traffic endpoint of the LILLE site (network object LIL-LAN in the example).
   The endpoint may be a network group.

4. In the **Peer selection** field, select the peer that was created for the LYON firewall (host object FW-LYON in the example).
5. In the **Remote networks** field, select the traffic endpoint of the LYON site (network object LYO-LAN in the example).
   The endpoint may be a network group.
6. Click on **Finish**.
7. Click in the **Keepalive** column and select a duration from the drop-down menu (600 ms in the example).
   This setting determines how long to keep the tunnel up even when it is not in use.
8. Double-click in the **Status** column to enable this rule in the IPsec policy.
9. Click on **Apply**, then **Save** to save the changes made to the configuration.
10. Changes can be applied immediately by clicking on **Yes, activate the policy**.

On the FW-LILLE firewall, the IPsec policy between the LILLE and LYON sites is therefore:



Creating the filter rule to enable dialogue between the LILLE and LYON sites

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: select the object corresponding to the LYON local network (LYO-LAN in this example).
7. **Destination** menu on the left: select the object corresponding to the LILLE local network (LIL-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the **Destination ports** of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Repeat steps 2 to 10 with the LIL-LAN object as the source, and the LYO-LAN object as the destination.
12. Click on **Apply**.

Configuring the FW-LYON firewall

Creating objects corresponding to LANs at the LILLE and LYON sites

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Network**.
4. Specify the **Object name** (LIL-LAN in this example).
5. Enter the **Network IP address** in the form of a network/mask. The network mask can be entered in CIDR or decimal format.

6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object LYO-LAN.
8. Click on **Create**.

Creating the object corresponding to the LYON WAN gateway/link

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (LYO-WAN-1 in this example).
5. Enter its **IPv4 address**.
6. Click on **Create**.

Setting this router object as the FW-LYON firewall's gateway

1. Go to **Configuration** > **Network** > **Routing.**
2. In the **Default gateway** field, select the host object that was created earlier (LYO-WAN-1 in this example).
3. Click on **Apply** then **Save**.

Setting the IPsec peer for the LILLE site

This is a mobile peer, as the FW-LYON firewall cannot predict the address that the FW-LILLE firewall will use to set up the tunnel.

Similarly to the FW-LILLE firewall, the **DPD** (Dead Peer Detection) option has to be set to **High** to force the IPsec tunnel to be renegotiated immediately when the link is down.

1. Go to **Configuration** > **VPN** > **IPsec VPN** > **Peers** tab.
2. Click on **Add**, then on **New mobile peer**.
3. Enter a name for this peer (FW-LILLE in the example).
4. Select the **IKEv2** version.
5. Choose the **IKE profile** to use.
   It has to be the same as the one used on the FW-LILLE firewall.
6. Click on **Next**.
7. For the **Authentication type**, select **Pre-shared key (PSK)**.
8. Click on **Next**.
9. Click on **Add**:
   a. For the **ID**, enter the public IP address of the LILLE site's first WAN link.
      Enter the **Pre-shared key** and confirm it.
      It has to be the same one defined on the FW-LILLE firewall.
   b. Click on **Apply**.
   c. Repeat steps A to C to set the pre-shared keys used for the two other WAN links on the LILLE site.
      They have to be the same ones defined on the FW-LILLE firewall.
10. Click on **Next**.
    You will be shown a summary of the peer's details.
11. Click on **Finish**.
    Details on the peer are shown.
12. Ensure that the value of the **Local address** is **Any**.

13. In the **Advanced properties** section, set the **DPD** field to **High**.

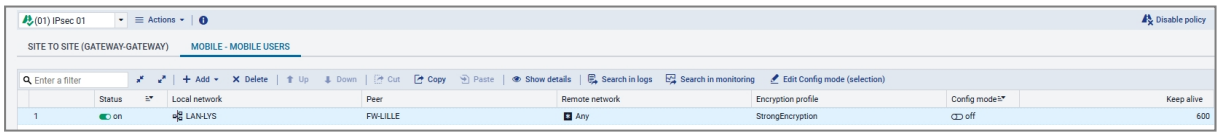
> **NOTE**
> As the peer is mobile, it is automatically set to *Responder-only* mode.

14. Click on **Apply** then on **Save**.
15. Changes can be applied immediately by clicking on **Yes, activate the policy**.

Creating the IPsec policy to set up the tunnel with the FW-LILLE peer

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Mobile – Mobile users** tab.
2. Click on **Add**, then on **New standard mobile policy**.
3. In the **Local resources** field, select the traffic endpoint of the LYON site (network object LYO-LAN in the example).
   The endpoint may be a network group.
4. In the Peer selection field, select the peer that was created for the LILLE firewall (host object FW-LILLE in the example).
5. Click on **Finish**.
6. Click in the **Keepalive** column and select a duration from the drop-down menu (600 ms in the example).
   This setting determines how long to keep the tunnel up even when it is not in use.
7. Double-click in the **Status** column to enable this rule in the IPsec policy.
8. Click on **Apply** then **Save**.
9. Changes can be applied immediately by clicking on **Yes, activate the policy**.

On the FW-LYON firewall, the IPsec policy between the LYON and LILLE sites is therefore:



Creating the filter rule to enable dialogue between the LYON and LILLE sites

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: select the object corresponding to the LILLE local network (LIL-LAN in this example).
7. **Destination** menu on the left: select the object corresponding to the LYON local network (LYO-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the **Destination ports** of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Repeat steps 2 to 10 with the LYO-LAN object as the source, and the LIL-LAN object as the

destination.

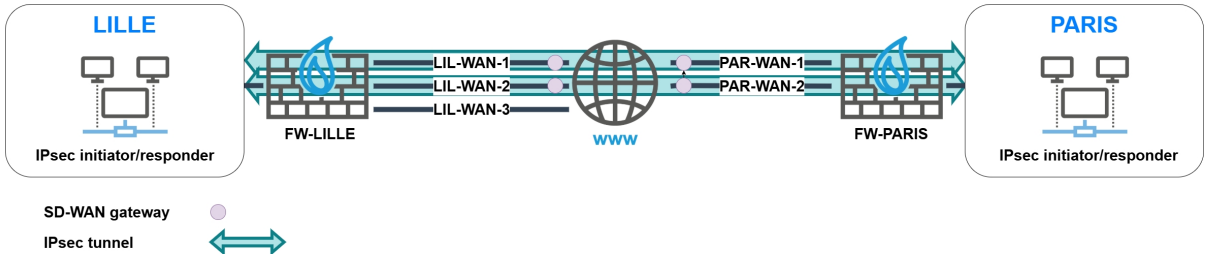
12. Click on **Apply**.

IPsec tunnels based on virtual IPsec interfaces (VTI)

Network architecture

- The main LILLE site hosts three WAN links (LIL-WAN-1, LIL-WAN-2 and LIL-WAN-3),
- The secondary PARIS site hosts two main WAN links (PAR-WAN-1 and PAR-WAN-2).

IPsec architecture



- The LILLE and PARIS sites communicate through two IPsec tunnels that are based on virtual IPsec interfaces (VTI).
- One of the sites can be configured as responder only.

LILLE site

The FW-LILLE firewall uses two static routes to set up IPsec tunnels with the PARIS site through WAN access link pairs LIL-WAN-1/PAR-WAN-1 and LIL-WAN-2/PAR-WAN-2. These tunnels are based on virtual IPsec interfaces.

This configuration imposes communication exclusively between LIL-WAN-1 and PAR-WAN-1, and between LIL-WAN-2 and PAR-WAN-2.

> **NOTE**
> As the PARIS site has one WAN link less than the LILLE site, the LIL-WAN-3 access link will not be used to set up the IPsec tunnels with the PARIS site.

A route has to be defined to set up tunnels with the PARIS site: this can be done with a router object that uses both virtual IPsec interfaces on the PARIS site.

This route can be defined:

- Through policy-based routing (PBR). This option enables load balancing and failover between both router object gateways.
- Through static routing. This option **imposes** failover to be defined between both router object gateways. Load balancing cannot be used in this case.

> **NOTE**
> If the PARIS site had only one WAN link, the configuration can still be deployed by using an alias or a second public IP address to define PAR-WAN-1.

PARIS site

The configuration of the PARIS site mirrors the LILLE site.

Configuring the FW-LILLE firewall

Creating objects corresponding to LANs at the PARIS and LILLE sites

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Network**.
4. Specify the **Object name** (LIL-LAN in this example).
5. Enter the **Network IP address** in the form of a network/mask. The network mask can be entered in CIDR or decimal format.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object PAR-LAN.
8. Click on **Create**.

Creating objects corresponding to the LILLE WAN gateways/links

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (LIL-WAN-1 in this example).
5. Enter its **IPv4 address**.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object LIL-WAN-2.
8. Click on **Create**.

Creating objects corresponding to the PARIS WAN gateways/links

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (PAR-WAN-1 in this example).
5. Enter the public **IPv4 address** of the PARIS site's WAN-1 link.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object PAR-WAN-2 with the public IPv4 address of the PARIS site's WAN-2 link.
8. Click on **Create**.

Creating virtual IPsec interfaces for the LILLE site

1. Go to **Configuration > Network > Virtual interfaces.**
2. Click on **Add**.
3. Switch the **Status** of the interface to **Enabled**.
4. Indicate the **Name** of the virtual IPsec interface (LIL-VTI-1 in this example).
5. Indicate the **IPv4 address** and **network mask** of this interface (10.255.1.1/255,255,255,252 in this example).
6. Click on **Apply**.
7. Repeat steps 2 to 6 to create the second virtual IPsec interface (LIL-VTI-2 and 10.255.2.1/255.255.255.252 in this example).
8. Click on **Apply**.

Creating objects corresponding to the virtual IPsec interfaces of the PARIS firewall

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (PAR-VTI-1 in this example).
5. Enter the **IPv4 address** of the virtual IPsec interface (10.255.1.2/255,255,255,252 in this example).
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object PAR-VTI-2 with the IP address 10.255.2.2/255.255.255.252 in this example.
8. Click on **Create**.

Creating return routes for the FW-LILLE virtual IPsec interfaces

1. Go to **Configuration** > **Network** > **Routing, IPv4 return routes** tab.
2. Click on **Add**.
3. Switch the **Status** of the return route to **Enabled**.
4. Indicate the remote **Gateway** of this return route (PAR-VTI-1 in this example).
5. Indicate the local virtual IPsec **interface** to be used for this return route (LIL-VTI-1 in this example).
6. Repeat steps 2 to 5 with the following elements:
   - **Gateway**: PAR-VTI-2,
   - **Interface**: LIL-VTI-2.
7. Click on **Apply**.

Creating the static routes required for setting up IPsec tunnels

This step involves defining a static route to each physical remote interface in such a way that:

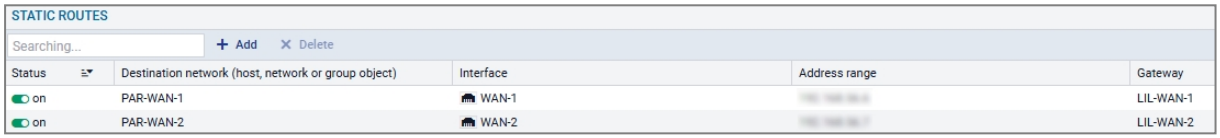
- The first tunnel sets up between the links LIL-WAN-1 and PAR-WAN-1,
- The second tunnel sets up between the links LIL-WAN-2 and PAR-WAN-2.

To do so:

1. Go to **Configuration** > **Network** > **Routing** > **Static routing** tab.
2. Click on **Add**.
3. Switch the **Status** of the route to **On**.

4. For the **Destination network**, select the object corresponding to the PARIS site's WAN 1 access link (PAR-WAN-1 in the example).
5. For the local **Interface** that needs to be used for this route, select the interface corresponding to the LILLE WAN 1 access link (WAN-1 in this example).
6. For the gateway that needs to be used for this route, select the object LIL-WAN-1.
7. Repeat steps 2 to 6 with the following elements:
   - **Destination network**: PAR-WAN-2,
   - **Interface**: WAN-2,
   - **Gateway**: LIL-WAN-2.
8. Click on **Apply**.

These routes will then resemble the following:



Creating the router object to use in the route to the PARIS site's LAN

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Rrouter**.

General properties

4. Name the object (e.g., ROUTER-LILLE-VTI-FAILOVER or ROUTER-LILLE-VTI-LB depending on the chosen routing option).

Monitoring

5. For the **Detection method**, select **ICMP**.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** as needed.
8. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

9. Select **SD-WAN SLA (thresholds)**.
10. Adjust the **Latency (ms)** as needed.
11. Adjust the **Jitter (ms)** as needed.
12. Adjust the **Packet loss rate (%)** as needed.
13. Do not enter an **Unavailability rate (%)**.

Gateways

14. In the **Gateways used** tab, click on **Add**.
15. In the **Gateway** column, select the object PAR-VTI-1.
16. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
17. If you select the load balancing option: repeat steps 14 to 16 to add the object PAR-VTI-2.

18. If you select the failover option:
    a. In the **Backup gateways** tab, click on **Add**.
    b. In the **Gateway** column, select the object PAR-VTI-2.
    c. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

19. In **Advanced properties**, for the **Load balancing** field value:
    a. Depending on your requirements, select **By connection** or **By source IP address** if you have chosen the load balancing option.
    b. Select **No load balancing** if you have chosen the failover option.
20. For **Enable backup gateways,** select **When all gateways cannot be reached**.

> **IMPORTANT**
> For the **If no gateways are available** field, select **Do not route** regardless of your routing choice.
> This will prevent unencrypted traffic from being sent to unprotected networks, such as the Internet if no gateways are available.

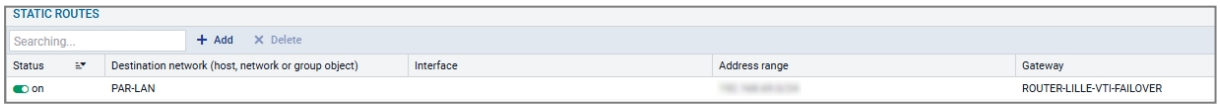
21. Click on **Apply** then **Save**.

Using this object in routing to reach the PARIS site's LAN

Static routing with failover

1. Go to **Configuration** > **Network** > **Routing** > **Static routing** tab.
2. Click on **Add**.
3. Switch the **Status** of the return route to **Enabled**.
4. For the **Destination network**, select the object corresponding to the PARIS site's LAN (PAR-LAN in the example).
5. Do not select any **interface**.
6. For the gateway that needs to be used for this route, select the router object that was configured with failover (ROUTER-LILLE-VTI-FAILOVER in this example).
7. Click on **Apply**.

This route will then look like this:



Policy-based routing with load balancing

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu on the left, **General** tab:
    a. **General** section: set the **Action** to **pass**.
    b. **Routing** section: select the router object that was configured earlier (ROUTER-LILLE-VTI-LB in this example).

6. **Source** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local network of the LILLE site (LIL-LAN in this example).
7. **Destination** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local network of the PARIS site (PAR-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the Destination ports of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Click on **Apply**.

This filter rule will then look like this:

Setting the IPsec peers of the PARIS site

These peers are remote gateways.

In this example, pre-shared key authentication is used.

In order for one of the two FW-LILLE WAN links to be used when the tunnel is initialized, the value of the **Local address** field has to be **Any**. Similarly, the **DPD** (Dead Peer Detection) option has to be set to **High** to force the IPsec tunnel to be renegotiated as quickly as possible when the link is down.

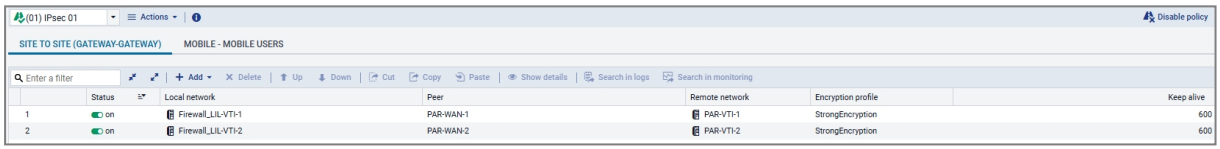
1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**, then on **New remote gateway**.
3. In the **Remote gateway** field, select the object corresponding to the FW-PARIS firewall's first public IP address (PAR-WAN-1 in the example).
4. Enter a name for this peer (PAR-WAN-1 in the example).
5. Select the **IKEv2** version.
6. Choose the **IKE profile** to use.
7. Click on **Next**.
8. For the **Authentication type**, select **Pre-shared key (PSK)**.
9. Set the **Pre-shared key** and confirm it.
10. Click on **Next**.
    You will be shown a summary of the peer's details.
11. Click on **Finish**.
    Details on the peer are shown.
12. Ensure that the value of the **Local address** is **Any**.
13. In the **Advanced properties** section, set the **DPD** field to **High**.
14. Confirm changes by clicking on **Apply** then on **Save**.
15. Repeat steps 2 to 14 to create the peer based on the FW-PARIS firewall's second public IP address (PAR-WAN-2 in this example).
16. Changes can be applied immediately by clicking on **Yes, activate the policy**.

Creating the IPsec policy to set up tunnels with the PARIS site

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Site-to-site (gateway-gateway)** tab.
2. Click on **Add**, then on **Standard site-to-site tunnel.**

3. In the **Local resources** field, select the traffic endpoint of the LILLE site: this is FW-LILLE's first virtual IPsec interface (network object Firewall_LIL-VTI-1 in the example).
4. In the **Peer selection** field, select the first peer that was created for the PARIS firewall (host object PAR-WAN-1 in the example).
5. In the **Remote networks** field, select the traffic endpoint of the PARIS site: this is FW-PARIS's first virtual IPsec interface (network object PAR-VTI-1 in the example).
6. Click on **Finish**.
7. Click in the **Keepalive** column and select a duration from the drop-down menu (600 ms in the example).
   This setting determines how long to keep the tunnel up even when it is not in use.
8. Double-click in the **Status** column to enable this rule in the IPsec policy.
9. Repeat steps 2 to 8 to create the tunnel between LIL-VTI-2 and PAR-VTI-2.
10. Click on **Apply**, then **Save** to save the changes made to the configuration.
11. Changes can be applied immediately by clicking on **Yes, activate the policy**.

On the FW-LILLE firewall, the IPsec policy between the LILLE and PARIS sites is therefore:



Creating the filter rule to enable monitoring of VTIs at the PARIS site

1. Go to **Configuration** > **Security policy** > **Filter - NAT, Filtering** tab.
2. Click on **New rule** > **Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: leave the **Any** object suggested by default.
7. **Destination** menu on the left: double-click on the **Any** object and replace it with the objects corresponding to the VTIs of the PARIS site (PAR-VTI-1 and PAR-VTI-2 in this example).
8. **Port/Protocol** menu on the left: for the **IP protocol** field in the **Protocol** section, select the **icmp** object.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Click on **Apply**.

Creating the filter rule to enable dialogue between the LILLE and PARIS sites

1. Go to **Configuration** > **Security policy** > **Filter - NAT, Filtering** tab.
2. Click on **New rule** > **Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local PARIS network (PAR-LAN in this example).
7. **Destination** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local LILLE network (LIL-LAN in this example).

8. **Port/Protocol** menu on the left: add to the grid the **Destination ports** of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Repeat steps 2 to 10 with the LIL-LAN object as the source, and the PAR-LAN object as the destination.

> **NOTE**
> The second rule does not need to be created if you have used policy-based routing to reach the PARIS LAN.

12. Click on **Apply**.

Configuring the FW-PARIS firewall

Creating objects corresponding to LANs at the PARIS and LILLE sites

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Network**.
4. Specify the **Object name** (LIL-LAN in this example).
5. Enter the **Network IP address** in the form of a network/mask. The network mask can be entered in CIDR or decimal format.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object PAR-LAN.
8. Click on **Create**.

Creating objects corresponding to the PARIS WAN gateways/links

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (PAR-WAN-1 in this example).
5. Enter its **IPv4 address**.
6. Click on **Create and duplicate**.
7. Repeat steps 4 and 5 to create the object PAR-WAN-2.
8. Click on **Create**.

Creating objects corresponding to the LILLE WAN gateways/links

1. Go to **Configuration** > **Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (LIL-WAN-1 in this example).
5. Enter the public **IPv4 address** of the LILLE site's WAN-1 link.
6. Click on **Create and duplicate**.

7. Repeat steps 4 to 5 to create the object LIL-WAN-2 with the public IPv4 address of the LILLE site's WAN-2 link.
8. Click on **Create**.

Creating objects corresponding to the virtual IPsec interfaces of the LILLE firewall

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Host**.
4. Specify the **Object name** (LIL-VTI-1 in this example).
5. Enter the **IPv4 address** of the virtual IPsec interface (10.255.1.1/ 255.255.255.252).
6. Click on **Create and duplicate**.
7. Repeat steps 4 to 5 to create the object LIL-VTI-2 with the IP address 10.255.2.1/255.255.255.252 in this example.
8. Click on **Create**.

Creating virtual IPsec interfaces for the PARIS site

1. Go to **Configuration > Network > Virtual interfaces.**
2. Click on **Add**.
3. Switch the **Status** of the interface to **Enabled**.
4. Indicate the **Name** of the virtual IPsec interface (PAR-VTI-1 in this example).
5. Indicate the **IPv4 address** and **network mask** of this interface (10.255.1.2/255,255,255,252 in this example).
6. Click on **Apply**.
7. Repeat steps 2 to 6 to create the second virtual IPsec interface (PAR-VTI-2 and 10.255.2.2/255.255.255.252 in this example).
8. Click on **Apply** at the bottom of the module to save this configuration.

Creating return routes for the FW-PARIS virtual IPsec interfaces

1. Go to **Configuration** > **Network** > **Routing, IPv4 return routes** tab.
2. Click on **Add**.
3. Switch the **Status** of the return route to **On**.
4. Indicate the remote **Gateway** of this return route (LIL-VTI-1 in this example).
5. Indicate the local virtual IPsec **interface** to be used for this return route (PAR-VTI-1 in this example).
6. Repeat steps 2 to 5 with the following elements:
   - **Gateway**: LIL-VTI-2,
   - **Interface**: PAR-VTI-2.
7. Click on **Apply** at the bottom of the module to save this configuration.

Creating the static routes required for setting up IPsec tunnels

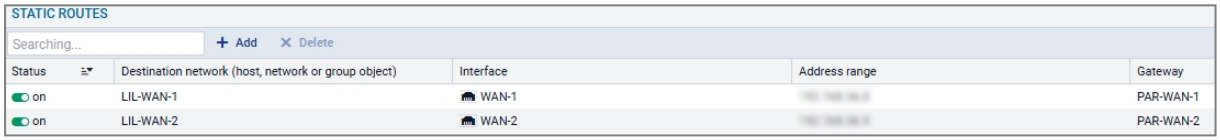
This step involves defining a static route to each physical remote interface in such a way that:

- The first tunnel sets up between the links LIL-WAN-1 and PAR-WAN-1,
- The second tunnel sets up between the links LIL-WAN-2 and PAR-WAN-2.

To do so:

1. Go to **Configuration** > **Network** > **Routing** > **Static routing** tab.
2. Click on **Add**.
3. Switch the **Status** of the route to **On**.
4. For the **Destination network**, select the object corresponding to the LILLE site's WAN 1 access link (LIL-WAN-1 in the example).
5. For the local **Interface** that needs to be used for this route, select the interface corresponding to the PARIS WAN 1 access link (WAN-1 in this example).
6. For the gateway that needs to be used for this route, select the object PAR-WAN-1.
7. Repeat steps 2 to 6 with the following elements:
   - **Destination network**: LIL-WAN-2,
   - **Interface**: WAN-2,
   - **Gateway**: PAR-WAN-2.
8. Click on **Apply** at the bottom of the module to save this configuration.

These routes will then resemble the following:



Creating the router object to use in the route to the LILLE site's LAN

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Rrouter**.

General properties

4. Name the object (e.g., ROUTER-PARIS-VTI-FAILOVER or ROUTER-PARIS-VTI-LB depending on the chosen routing option).

Monitoring

5. For the **Detection method**, select **ICMP**.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** as needed.
8. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

9. Select **SD-WAN SLA (thresholds)**.
10. Adjust the **Latency (ms)** as needed.
11. Adjust the **Jitter (ms)** as needed.
12. Adjust the **Packet loss rate (%)** as needed.
13. Do not enter an **Unavailability rate (%)**.

Gateways

14. In the **Gateways used** tab, click on **Add**.
15. In the **Gateway** column, select the object LIL-VTI-1.
16. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
17. If you select the load balancing option: repeat steps 14 to 16 to add the object LIL-VTI-2.

18. If you select the failover option:
    a. In the **Backup gateways** tab, click on **Add**.
    b. In the **Gateway** column, select the object LIL-VTI-2.
    c. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

19. In **Advanced properties**, for the **Load balancing** field value:
    a. Depending on your requirements, select **By connection** or **By source IP address** if you have chosen the load balancing option.
    b. Select **No load balancing** if you have chosen the failover option.
20. For **Enable backup gateways,** select **When all gateways cannot be reached**.

> **IMPORTANT**
> For the **If no gateways are available** field, select **Do not route** regardless of your routing choice.
> This will prevent unencrypted traffic from being sent to unprotected networks, such as the Internet if no gateways are available.

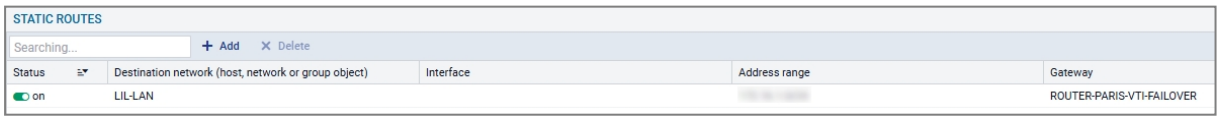
21. Click on **Apply** then **Save**.

Using this object in routing to reach the LILLE site's LAN

Static routing with backup

1. Go to **Configuration** > **Network** > **Routing** > **Static routing** tab.
2. Click on **Add**.
3. Switch the **Status** of the return route to **Enabled**.
4. For the **Destination network**, select the object corresponding to the LILLE site's LAN (LIL-LAN in the example).
5. Do not select any **interface**.
6. For the gateway that needs to be used for this route, select the router object that was configured with failover (ROUTER-PARIS-VTI-FAILOVER in this example).
7. Click on **Apply** at the bottom of the module to save this configuration.

This route will then look like this:



Policy-based routing with load balancing

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu on the left, **General** tab:
    - **General** section: set the **Action** to **pass**.
    - **Routing** section: select the router object that was configured earlier (ROUTER-PARIS-VTI-LB in this example).

6. **Source** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local network of the PARIS site (PAR-LAN in this example).
7. **Destination** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local network of the LILLE site (LIL-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the Destination ports of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Click on **Apply**.

This filter rule will then look like this:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass Route: ROUTER-PARIS-VTI-LB	PAR-LAN	LIL-LAN	Any		IPS

Setting the IPsec peers of the LILLE site

This peer is a remote gateway.

In this example, pre-shared key authentication is used.

In order for one of the two FW-PARIS WAN links to be used when the tunnel is initialized, the value of the **Local address** field has to be **Any**. Similarly, the **DPD** (Dead Peer Detection) option has to be set to **High** to force the IPsec tunnel to be renegotiated as quickly as possible when the link is down.

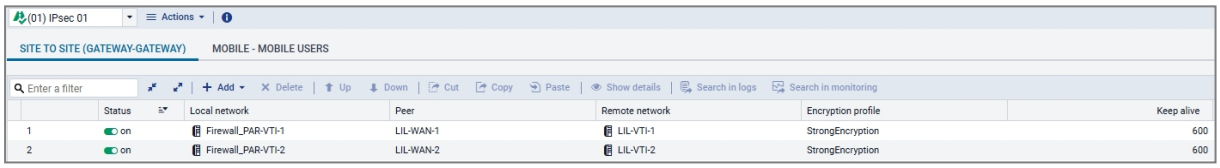
1. Go to **Configuration > VPN > IPsec VPN > Peers** tab.
2. Click on **Add**, then on **New remote gateway**.
3. In the **Remote gateway** field, select the object corresponding to the FW-LILLE firewall's first public IP address (LIL-WAN-1 in the example).
4. Enter a name for this peer (LIL-WAN-1 in the example).
5. Select the **IKEv2** version.
6. Choose the **IKE profile** to use.
7. Click on **Next**.
8. For the **Authentication type**, select **Pre-shared key (PSK)**.
9. Set the **Pre-shared key** and confirm it.
10. Click on **Next**.
    You will be shown a summary of the peer's details.
11. Click on **Finish**.
    Details on the peer are shown.
12. Ensure that the value of the **Local address** is **Any**.
13. In the **Advanced properties** section, set the **DPD** field to **High**.
14. Click on **Apply** then on **Save**.
15. Repeat steps 2 to 14 to create the peer based on the FW-LILLE firewall's second public IP address (LIL-WAN-2 in this example).
16. Changes can be applied immediately by clicking on **Yes, activate the policy**.

Creating the IPsec policy to set up tunnels with the LILLE site

1. Go to **Configuration > VPN > IPsec VPN > Encryption Policy - Tunnels** tab > **Site-to-site (gateway-gateway)** tab.
2. Click on **Add**, then on **Standard site-to-site tunnel.**

3. In the **Local resources** field, select the traffic endpoint of the PARIS site: this is FW-PARIS's first virtual IPsec interface (network object Firewall_PAR-VTI-1 in the example).
4. In the **Peer selection** field, select the first peer that was created for the PARIS firewall (host object LIL-WAN-1 in the example).
5. In the **Remote networks** field, select the traffic endpoint of the PARIS site: this is FW-PARIS's first virtual IPsec interface (network object LIL-VTI-1 in the example).
6. Click on **Finish**.
7. Click in the **Keepalive** column and select a duration from the drop-down menu (600 ms in the example).
   This setting determines how long to keep the tunnel up even when it is not in use.
8. Double-click in the **Status** column to enable this rule in the IPsec policy.
9. Repeat steps 2 to 8 to create the tunnel between LIL-VTI-2 and PAR-VTI-2.
10. Click on **Apply** then on **Save**.
11. Changes can be applied immediately by clicking on **Yes, activate the policy**.

On the FW-PARIS firewall, the IPsec policy between the LILLE and PARIS sites is therefore:



Creating the filter rule to enable monitoring of VTIs at the LILLE site

1. Go to **Configuration** > **Security policy** > **Filter - NAT, Filtering** tab.
2. Click on **New rule** > **Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: leave the **Any** object suggested by default.
7. **Destination** menu on the left: select the objects corresponding to the PARIS site's VTIs (LIL-VTI-1 and LIL-VTI-2 in this example).
8. **Port/Protocol** menu on the left: for the **IP protocol** field in the **Protocol** section, select the **icmp** object.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Click on **Apply**.

Creating the filter rule to enable dialogue between the LILLE and PARIS sites

1. Go to **Configuration** > **Security policy** > **Filter - NAT, Filtering** tab.
2. Click on **New rule** > **Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local LILLE network (LIL-LAN in this example).

7. **Destination** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local PARIS network (PAR-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the **Destination ports** of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
10. Click on **OK**.
11. Repeat steps 2 to 10 with the PAR-LAN object as the source, and the LIL-LAN object as the destination.

> **NOTE**
> The second rule does not need to be created if you have used policy-based routing to reach the LILLE LAN.

12. Click on **Apply**.

IPsec tunnels based on virtual IPsec interfaces (VTI) in a hub and spoke configuration

This example is a variation of the scenario in which tunnels are based on virtual IPsec interfaces (VTI) between the LILLE and PARIS sites. In addition to encrypted exchanges between the LILLE and PARIS sites, the PARIS site uses IPsec tunnels to access the Internet via one of the LILLE WAN access links.

The architecture is the same as the one used for tunnels based on virtual IPsec interfaces (VTI) between the LILLE and PARIS sites. As such, it will not be explained in this section.

Only the imperative settings relating to the type of router object to be used for routing on each site, as well as the NAT rules to create on the LILLE site, will be described in this section.

LILLE site

In a hub & spoke configuration, traffic on the LILLE site can be routed:

- Over a default route through a router object that uses failover between both its gateways,
- Over policy-based routing (PBR) through a router object that uses failover between both its gateways,
- Over a static route through a router object that uses failover between both its gateways,

Load balancing cannot be used in the router object in this case: it is not compatible with unprotected source interfaces, which is the default setting for virtual IPsec interfaces.

PARIS site

In a hub & spoke configuration, traffic on the PARIS site can be routed:

- Over a default route through a router object that uses failover between both its gateways,
- Over a static route through a router object that uses failover between both its gateways,
- Over policy-based routing (PBR) through a router object that uses failover between both its gateways,

- Over policy-based routing through a router object that uses load balancing, on the condition that the virtual IPsec interfaces of the PARIS site have been declared unprotected, which is the default configuration. Setting up load balancing with gateways that are based on protected interfaces will raise identity spoofing alarms that will block packets on the LILLE firewall.

Configuring the FW-LILLE firewall

Follow all the steps required to configure the LILLE firewall, as described in the section Configuring the FW-LILLE firewall from the example that deals with IPsec tunnels based on virtual IPsec (VTI) interfaces.

As indicated in the header of this section, the failover option is imperative when creating the router object that is used in the route to the PARIS site's LAN.

The following paragraphs explain the specific settings in a hub and spoke configuration.

Using the router object in routing to reach the PARIS site's LAN

Default route option

1. Go to **Configuration > Network > Routing.**
2. In the **Default gateway** field, select the router object that was created earlier.
3. Click on **Apply** then **Save**.

Static routing option

1. Go to **Configuration** > **Network** > **Routing** > **Static routing** tab.
2. Click on **Add**.
3. Switch the **Status** of the return route to **Enabled**.
4. For the **Destination network**, select the object corresponding to the PARIS site's LAN (PAR-LAN in the example).
5. Do not select any **interface**.
6. For the gateway that needs to be used for this route, select the router object that was created earlier.
7. Click on **Apply**.

Policy-based routing (PBR) option

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu on the left, **General** tab:
   a. **General** section: set the **Action** to **pass**.
   b. **Routing** section: select the router object that was created earlier.
6. **Source** menu on the left: select the object corresponding to the LILLE site's local network (LIL-LAN in this example).
7. **Destination** menu on the left: select the object corresponding to the PARIS site's local network (PAR-LAN in this example).
8. **Port/Protocol** menu on the left: add to the grid the Destination ports of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.

10. Click on **OK**.
11. Click on **Apply**.

Creating address translation (NAT) rules for traffic towards the Internet

1. Go to **Configuration > Security policy > Filter - NAT, NAT** tab.

First LILLE WAN access link

2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Original source** menu on the left, **Source hosts** grid: double-click on the **Any** object and replace it with the object corresponding to the PARIS LAN (PAR-LAN in this example).
6. **Original destination** menu on the left:
   a. In the **General** tab, **Destination hosts** grid: double-click on the object **Any** and replace it with the object **Internet**.
   b. In the **Advanced properties** tab, **Outgoing interface** field: select the object corresponding to the first LILLE WAN interface (WAN-1 in the example).
7. **Translated source** menu on the left:
   a. **Translated source host** field: select the object corresponding to the first public IP address of the firewall (Firewall_WAN-1 in this example).
   b. **Translated source port** field: select the object **ephemeral_fw**.
   c. Select **Choose random translated source port**.
8. **Options** menu on the left: select **NAT inside IPsec tunnel (before encryption, after decryption)**.
9. Click on **OK**.

Repeat steps 2 to 9 to create the NAT rules corresponding to the two other WAN access links of the LILLE site with the following objects:

Second LILLE WAN access link

Field	Value
Original source - Destination hosts	PAR-LAN
Original destination - Destination hosts	Internet
Original destination - Outgoing interface	WAN-2
Translated source - Translated source host	Firewall_WAN2

Third LILLE WAN access

Field	Value
Original source - Destination hosts	PAR-LAN
Original destination - Destination hosts	Internet
Original destination - Outgoing interface	WAN-3
Translated source - Translated source host	Firewall_WAN3

The translation rules on the LILLE firewall will therefore look like this:

Status	Original traffic (before translation)				Traffic after translation				Protocol	Options
	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port		
on	PAR-LAN	Internet interface: WAN-1	Any		Firewall_WAN-1		Any			NAT inside IPsec tunnel
on	PAR-LAN	Internet interface: WAN-2	Any		Firewall_WAN-2		Any			NAT inside IPsec tunnel
on	PAR-LAN	Internet interface: WAN-3	Any		Firewall_WAN-3		Any			NAT inside IPsec tunnel

Configuring the FW-PARIS firewall

Follow all the steps required to configure the PARIS firewall, as described in the section Configuring the FW-PARIS firewall from the example that deals with IPsec tunnels based on virtual IPsec (VTI) interfaces.

As indicated in the header of this section, the failover option is imperative when creating the router object that is used in the route to the PARIS site's LAN.

The following paragraphs explain the specific settings in a hub and spoke configuration.

This example shows the policy-based routing option on the PARIS site.

Using the router object in routing to access the Internet

1. Go to **Configuration** > **Security policy** > **Filter - NAT, Filtering** tab.
2. Click on **New rule** > **Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu on the left, **General** tab:
   a. **General** section: set the **Action** to **pass**.
   b. **Routing** section: select the router object that was created earlier.
6. **Source** menu on the left: double-click on the **Any** object and replace it with the object corresponding to the local network of the PARIS site (PAR-LAN in this example).
7. **Destination** menu on the left: double-click on the object **Any** and replace it with the **Internet** object.
8. **Inspection** menu on the left: we recommend leaving the default **Inspection level**, **IPS**.
9. Click on **OK**.
10. Click on **Apply**.

The policy-based routing rule will then look like this:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass Route: ROUTER-PARIS-VTI-FAILOVER	PAR-LAN	Internet	Any		IPS

Example 3: NAT rules with a failover between the three outgoing links of the LILLE site

This example illustrates a setup with failover between the three Internet access WAN links of the LILLE site through a router object.

Creating the router object that will be the default route

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Rrouter**.

General properties

4. Name the object (e.g., ROUTER-LILLE-WAN-FAILOVER).

Monitoring

5. For the **Detection method**, select **ICMP**.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** as needed.
8. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

9. Select **SD-WAN SLA (thresholds)**.
10. Adjust the **Latency (ms)** as needed.
11. Adjust the **Jitter (ms)** as needed.
12. Adjust the **Packet loss rate (%)** as needed.
13. Do not enter an **Unavailability rate (%)**.

Gateways

14. In the **Gateways used** tab, click on **Add**.
15. In the **Gateway** column, select the object LIL-WAN-1.
16. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
17. In the **Backup gateways** tab, click on **Add**.
18. In the **Gateway** column, select the object LIL-WAN-2.
19. Repeat steps 17 and 18 to add the object LIL-WAN-3.
20. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

21. In **Advanced properties**, select **No load balancing** for the **Load balancing** field.
22. For **Enable backup gateways,** select **When all gateways cannot be reached**.
23. Click on **Apply** then **Save**.

Setting this router object as the FW-LILLE firewall's gateway

1. Go to **Configuration > Network > Routing.**
2. In the **Default gateway** field, select the router object that was created earlier (ROUTER-LILLE-WAN-FAILOVER in this example).
3. Click on **Apply** then **Save**.

Creating the filter rule that allows internal networks to access the Internet

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Action** menu, **General** tab: set the **Action** to **pass**.
6. **Source** menu on the left: double-click on the object **Any** and replace it with the object **Network_internals**.
7. **Destination** menu on the left: double-click on the object **Any** and replace it with the object **Internet**.
8. **Port/Protocol** menu on the left: add to the grid the **Destination ports** of the various objects corresponding to the ports to be allowed in this filter rule.
9. **Inspection** menu on the left: we recommend leaving the default **Inspection level, IPS**.
10. Click on **OK**.
11. Click on **Apply**.

Creating address translation (NAT) rules for traffic towards the Internet

1. Go to **Configuration > Security policy > Filter - NAT, NAT** tab.

First LILLE WAN access link

2. Click on **New rule > Single rule**.
3. Double-click in any column in this rule.
4. **General** menu on the left: switch the **Status** of the rule to **On**.
5. **Original source** menu on the left, **Source hosts** grid: double-click on the object **Any** and replace it with the object **Network_internals**.
6. **Original destination** menu on the left:
   a. In the **General** tab, **Destination hosts** grid: double-click on the object **Any** and replace it with the object **Internet**.
   b. In the **Advanced properties** tab, **Outgoing interface** field: select the object corresponding to the first LILLE WAN interface (WAN-1 in the example).
7. **Translated source** menu on the left:
   a. **Translated source host** field: select the object corresponding to the first public IP address of the firewall (Firewall_WAN-1 in this example).
   b. **Translated source port** field: select the object **ephemeral_fw**.
   c. Select **Choose random translated source port**.
8. Click on **OK**.

Repeat steps 2 to 9 to create the NAT rules corresponding to the two other WAN access links of the LILLE site with the following objects:

Second LILLE WAN access link

Field	Value
Original source - Destination hosts	**Network_internals**
Original destination - Destination hosts	Internet
Original destination - Outgoing interface	WAN-2
Translated source - Translated source host	Firewall_WAN-2

Third LILLE WAN access

Field	Value
Original source - Destination hosts	**Network_internals**
Original destination - Destination hosts	Internet
Original destination - Outgoing interface	WAN-3
Translated source - Translated source host	Firewall_WAN-3

These NAT rules will then look like this:

Status	Original traffic (before translation)				Traffic after translation			
	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
on	Network_internal	Internet interface: WAN-1	Any	→	Firewall_WAN-1	ephemeral_fw	Any	
on	Network_internal	Internet interface: WAN-2	Any	→	Firewall_WAN-2	ephemeral_fw	Any	
on	Network_internal	Internet interface: WAN-3	Any	→	Firewall_WAN-3	ephemeral_fw	Any	

Example 4: using router objects in the SSL proxy

This example shows how a router object is used to provide failover in the SSL proxy: the first two links, WAN-1 and WAN-2, are set as the main gateways, with WAN-3 set as a failover gateway.

Do note that a router object can also be used with load balancing between its gateways.

For more information on filtering SSL traffic, refer to the technical note Filtering HTTPS connections.

Routing principle

The SSL proxy may use:

- A default route through a router object that provides failover,
- Policy-based routing.

When a gateway in the router object becomes unreachable, an RST packet is sent to the client's web browser, which establishes a new connection via the SSL proxy over one of the available WAN links.

Creating the router object that will be used for routing

1. Go to **Configuration > Objects** > **Network**.
2. Click on **Add**.
3. In the column on the left side of the object creation window, select **Rrouter**.

General properties

4. Name the object (e.g., ROUTER-LILLE-WAN-FAILOVER).

Monitoring

5. For the **Detection method**, select **ICMP**.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** as needed.
8. Adjust the number of **Failures before degradation** (3 by default).

SD-WAN SLA (thresholds)

9. Select **SD-WAN SLA (thresholds)**.
10. Adjust the **Latency (ms)** as needed.
11. Adjust the **Jitter (ms)** as needed.
12. Adjust the **Packet loss rate (%)** as needed.
13. Do not enter an **Unavailability rate (%)**.

Gateways

14. In the **Gateways used** tab, click on **Add**.
15. In the **Gateway** column, select the object LIL-WAN-1.
16. In the **Device(s) for testing availability** column, select **Test the gateway directly**.
17. In the **Backup gateways** tab, click on **Add**.
18. In the **Gateway** column, select the object LIL-WAN-2.

19. Repeat steps 17 and 18 to add the object LIL-WAN-3.
20. In the **Device(s) for testing availability** column, select **Test the gateway directly**.

Advanced properties

21. In **Advanced properties**, select **No load balancing** for the **Load balancing** field.
22. For **Enable backup gateways,** select **When all gateways cannot be reached**.
23. Click on **Apply** then **Save**.

Default routing

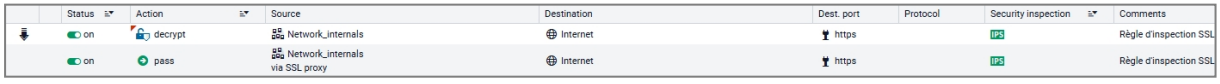
Adding the router object as the default route

1. Go to **Configuration > Network > Routing.**
2. In the **Default gateway** field, select the router object that was created earlier (ROUTER-LILLE-WAN-FAILOVER in this example).
3. Click on **Apply** then **Save**.

Creating an SSL inspection rule

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > SSL inspection rule**.
3. In the **Source hosts** field: leave the default object **Network_internals**, or select an object corresponding to your client hosts.
4. In the **Dest port** field: select the **https** object.
5. If you have not set any specific **Inspection profile** or **SSL filter policy**, you can leave the other default values as they are. Otherwise, select your inspection profile and/or SSL filter policy.
6. Click on **Finish**.
7. Click on **Apply** to confirm these changes to the filter policy.
8. Click on **Activate now** if you wish to enable this policy immediately, or **Later**.

The SSL inspection rule will then look like this:



Policy-based routing

Creating an SSL inspection rule

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Click on **New rule > SSL inspection rule**.
3. In the **Source hosts** field: leave the default object **Network_internals**, or select an object corresponding to your client hosts.
4. In the **Dest port** field: select the **https** object.

5. If you have not set any specific **Inspection profile** or **SSL filter policy**, you can leave the other default values as they are. Otherwise, select your inspection profile and/or SSL filter policy.
6. Click on **Finish**.
7. Double-click in the **Action** column of the newly created decryption rule.
8. In the **General** tab, for the **Gateway - router** field, select the router object that will be used for routing (ROUTER-LILLE-WAN-FAILOVER in this example).
9. Click on **OK**, then **Apply** to confirm these changes to the filter policy.
10. Click on **Activate now** if you wish to enable this policy immediately, or **Later**.

The SSL inspection rule will then look like this:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
	on	decrypt Route: ROUTER-LILLE-WAN-FAILOVER	Network_internals	Internet	https		IPS	Règle d'inspection SSL
	on	pass	Network_internals via SSL proxy	Internet	https		IPS	Règle d'inspection SSL

Further reading

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

documentation@stormshield.eu

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

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.