STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

SD-WAN: SELECTING THE BEST NETWORK LINK

Product concerned: SNS 4.3 and higher versions

Document last updated: March 20, 2022

Reference: sns-en-sd-wan_selecting_best_network_link-technical_note

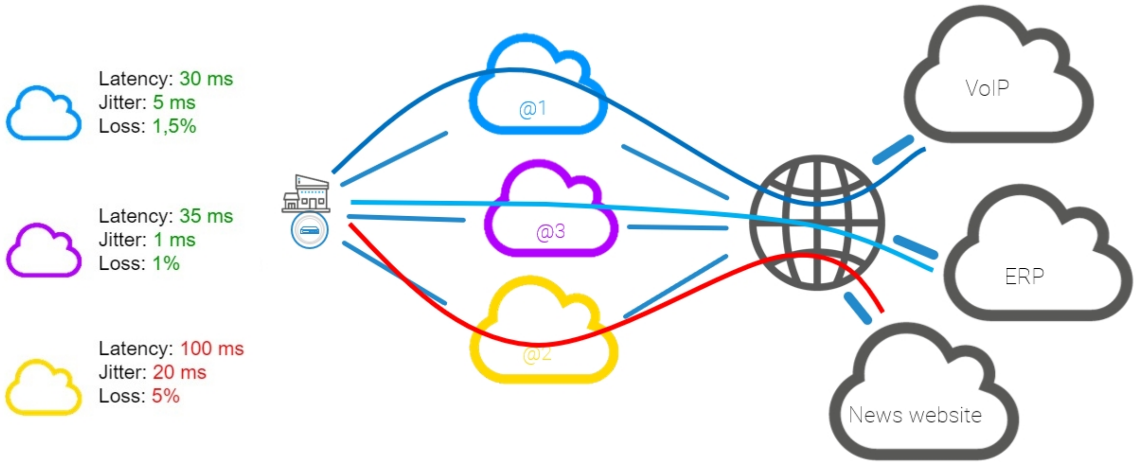
Table of contents

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 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:

- 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 by using the associated port.
- ICMP: in this method, ICMP Request packets are regularly sent over each link.

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.

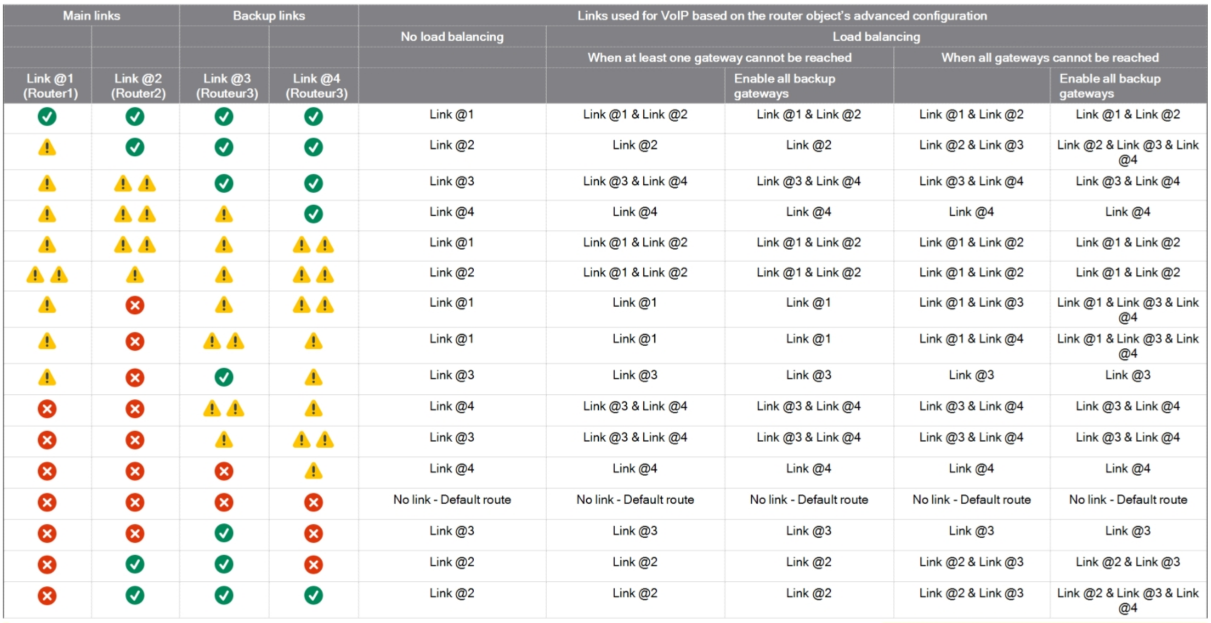
When you observe the values recorded for the various metrics (steps 2 and 3), do note that the data shown in the SD-WAN monitoring graphs in the SNS web administration interface are stored in a local database, and are then regularly aggregated to reduce the amount of disk space used.

> 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.

Understanding the switch mechanism and how links are chosen

When each metric is measured or calculated, a score is calculated for every link: 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.
The link that obtains the best score is chosen to transport traffic.

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		Links used for VoIP based on the router object's advanced configuration				
				No load balancing	Load balancing			
					When at least one gateway cannot be reached		When all gateways cannot be reached	
Link @1 (Router1)	Link @2 (Router2)	Link @3 (Routeur3)	Link @4 (Routeur3)			Enable all backup gateways		Enable all backup gateways
✓	✓	✓	✓	Link @1	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2
⚠	✓	✓	✓	Link @2	Link @2	Link @2	Link @2 & Link @3	Link @2 & Link @3 & Link @4
⚠	⚠⚠	✓	✓	Link @3	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4
⚠	⚠⚠	⚠	✓	Link @4	Link @4	Link @4	Link @4	Link @4
⚠	⚠⚠	⚠	⚠⚠	Link @1	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2
⚠⚠	⚠	⚠	⚠⚠	Link @2	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2	Link @1 & Link @2
⚠	✖	⚠	⚠⚠	Link @1	Link @1	Link @1	Link @1 & Link @3	Link @1 & Link @3 & Link @4
⚠	✖	⚠⚠	⚠	Link @1	Link @1	Link @1	Link @1 & Link @4	Link @1 & Link @3 & Link @4
⚠	✖	✓	⚠	Link @3	Link @3	Link @3	Link @3	Link @3
✖	✖	⚠⚠	⚠	Link @4	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4
✖	✖	⚠	⚠⚠	Link @3	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4	Link @3 & Link @4
✖	✖	✖	⚠	Link @4	Link @4	Link @4	Link @4	Link @4
✖	✖	✖	✖	No link - Default route	No link - Default route	No link - Default route	No link - Default route	No link - Default route
✖	✖	✓	✖	Link @3	Link @3	Link @3	Link @3	Link @3
✖	✓	✓	✖	Link @2	Link @2	Link @2	Link @2 & Link @3	Link @2 & Link @3
✖	✓	✓	✓	Link @2	Link @2	Link @2	Link @2 & Link @3	Link @2 & Link @3 & Link @4

Legend

✓	Optimal link
⚠	Degraded link (does not meet SLA thresholds)
⚠⚠	Highly degraded link (when several links are degraded : link with the lowest score)
✖	Link not available

Architecture presented

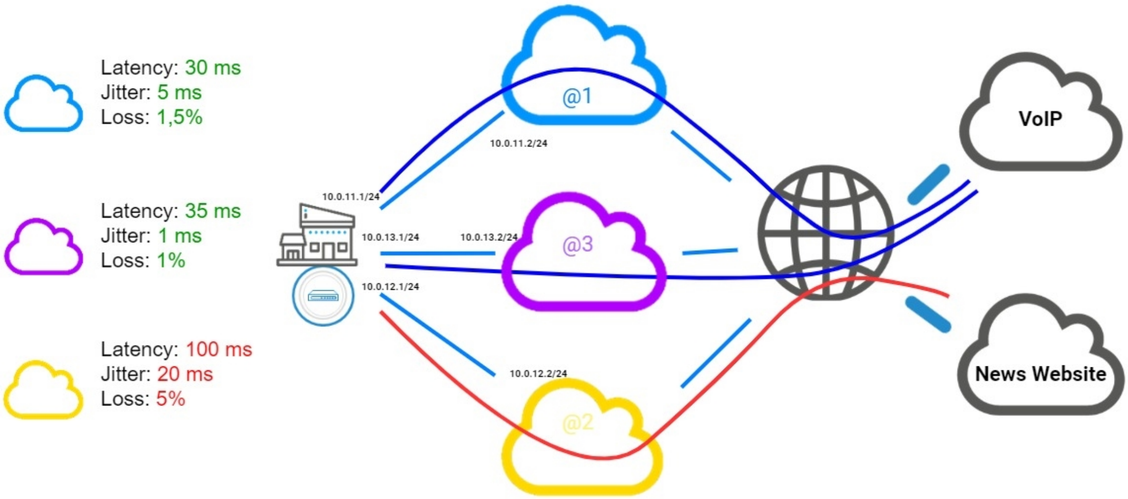
The configuration used in this technical note illustrates the example of an organization that has three remote access links:

- 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,

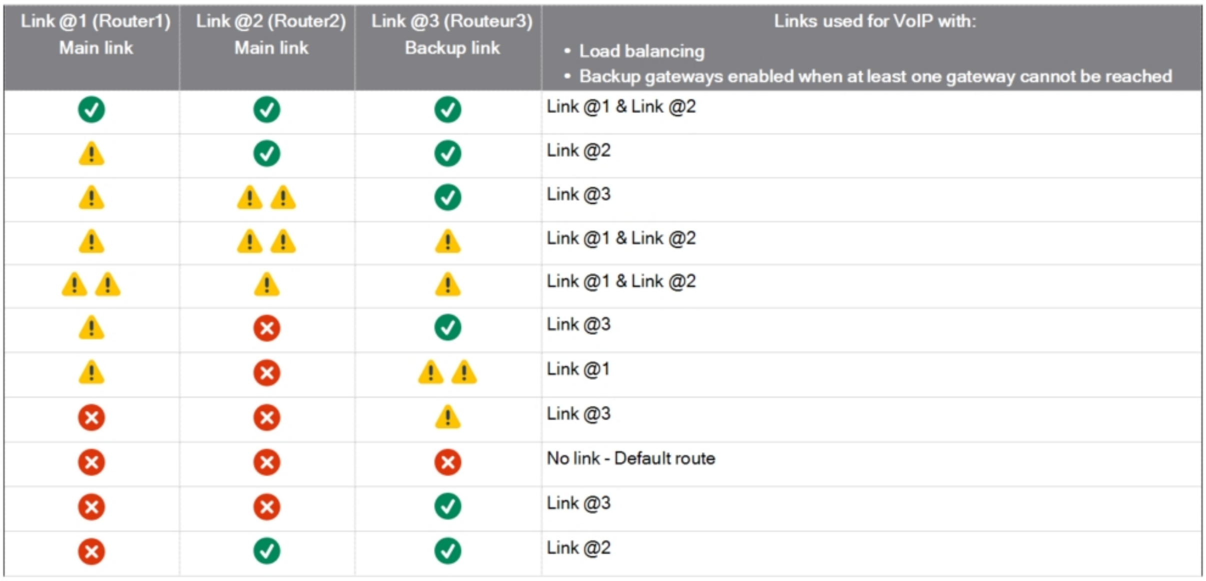
Both links from the first ISP are used as main links, while the one from the second ISP is designated as a backup link.

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

Legend

✓	Optimal link
⚠	Degraded link (does not meet SLA thresholds)
⚠⚠	Highly degraded link (when several links are degraded : link with the lowest score)
✗	Link not available

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 is the router object that 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 object(s) corresponding to the VoIP server(s).

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 the example described in this document, TCP port 5060, corresponding to the SIP protocol, is used.
The availability and performance of each link are therefore tested by initiating a connection to the remote VoIP server from the firewall by using TCP port 5060.

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 *TCP Probe*.
5. For the **Port**, select *sip_tcp*.
6. Adjust the **Timeout (s)** as needed.
7. Adjust the **Interval (s)** of availability tests as needed.
8. Adjust the **Failures before degradation** (5 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 **Used gateways** tab, click on **Add**.
15. In the **Gateway** column, select the object Router1.
16. In the **Device(s) for testing availability** column, select the remote VoIP server or group of remote VoIP servers (*Remote_VoIP* object in this technical note).
17. Repeat steps 14 to 16 to add the object Router2.

18. In the **Backup gateways** tab, click on **Add**.
19. In the **Gateway** column, select the object Router3.
20. In the **Device(s) for testing availability** column, select the remote VoIP server or group of remote VoIP servers (*Remote_VoIP* object in this technical note).

Advanced configuration

To maintain optimal link quality in as many cases as possible, the VoIP router object is configured with load balancing between the links used. Likewise, it is configured to use a backup link as soon as a main link is degraded or inaccessible.

21. In **Advanced configuration**, select **Load balancing** *By connection*.
22. For **Enable backup gateways**, select*When at least one gateway cannot be reached*.
23. Click on **Apply** then **Save**.

Creating the PBR rule for VoIP traffic

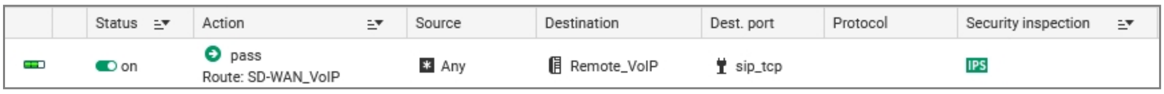
In **Configuration** > **Security policy** > **Filter - NAT**:

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:



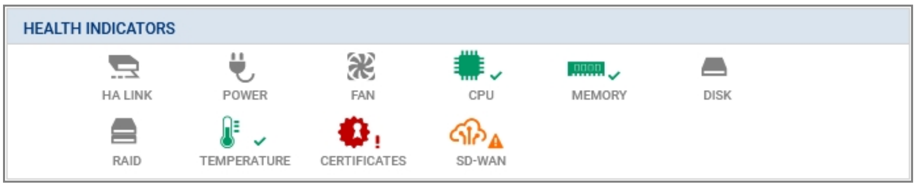
		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
		on	pass Route: SD-WAN_VoIP	Any	Remote_VoIP	sip_tcp		IPS

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 gateways are functional and meet the defined SD-WAN SLA criteria,
- Orange: (at least) one gateway is degraded,
- Red: (at least) one gateway cannot be reached.

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 as the default gateway and in policy-based routing (PBR) rules.

Real time tab

The **Real time** tab shows information about the SD-WAN SLA on monitored gateways and routers.

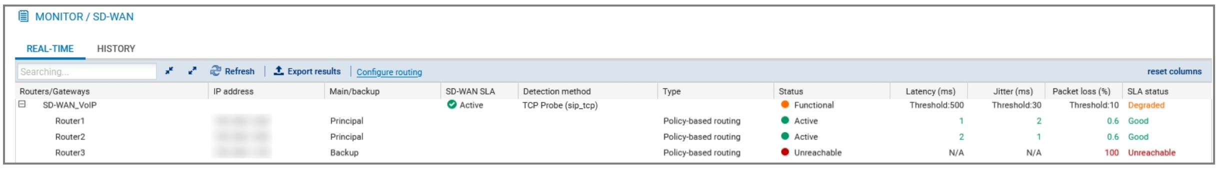
On the line corresponding to a router, you will see:

- The status of the router associated with a color code based on the same criteria as in the dashboard (**green, orange** or **red**).
- The thresholds set for each metric (latency, jitter and packet loss rate),
- The router's SLA status.

On the line corresponding to a gateway that makes up this router, you will see:

- The status of the gateway associated with a color code (green: operational, orange: degraded or red: unreachable),
- The value of each metric associated with a color code (**green, orange** or **red**) making it easier to know whether they meet the set thresholds.
- The gateway's SLA status.

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.

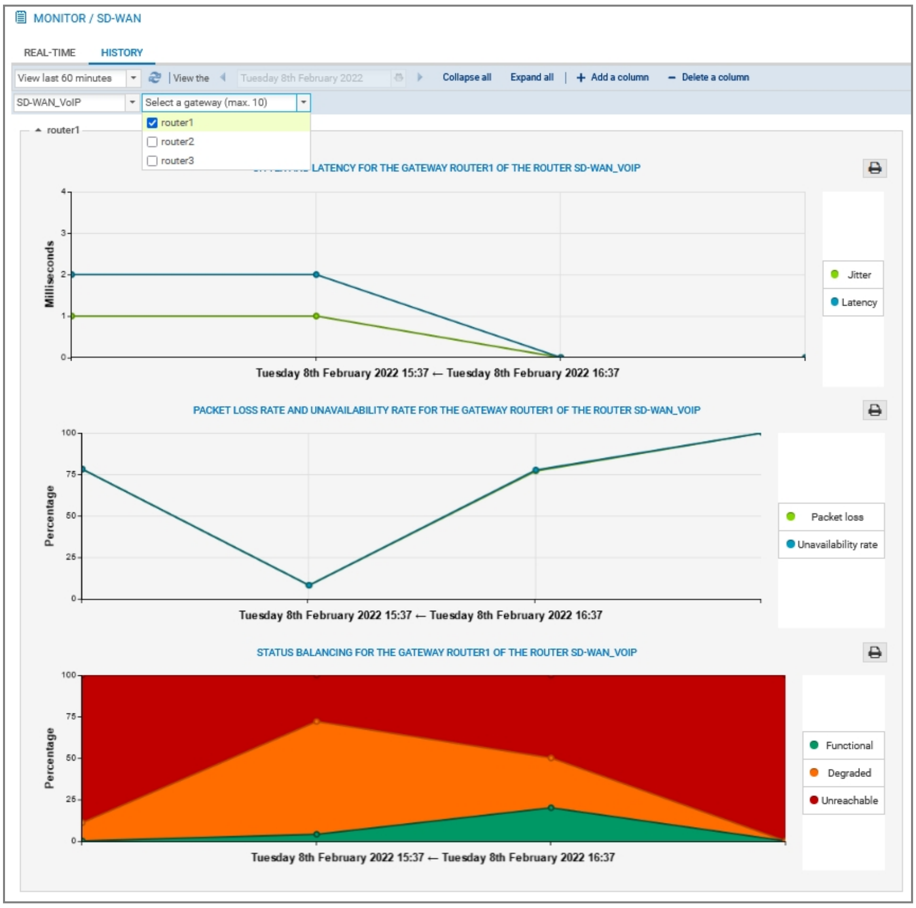


Routers/Gateways	IP address	Main/backup	SD-WAN SLA	Detection method	Type	Status	Latency (ms)	Jitter (ms)	Packet loss (%)	SLA status
⊟ SD-WAN_VoIP			✓ Active	TCP Probe (sip_tcp)		● Functional	Threshold:500	Threshold:30	Threshold:10	Degraded
Router1	[redacted]	Principal			Policy-based routing	● Active	1	2	0.6	Good
Router2	[redacted]	Principal			Policy-based routing	● Active	2	1	0.6	Good
Router3	[redacted]	Backup			Policy-based routing	● Unreachable	N/A	N/A	100	Unreachable

History tab

In this tab, up to five gateways can be selected for a given router to display curves that show changes in latency, jitter, packet loss rate, availability and proportion of time each selected gateway spent in the various states.

Example for the *Router1* gateway of the router *SD-WAN_VoIP*:


MONITOR / SD-WAN
REAL-TIME
HISTORY
View last 60 minutes
View the
Tuesday 8th February 2022
Collapse all
Expand all
Add a column
Delete a column
SD-WAN_VoIP
Select a gateway (max. 10)
☑ router1
☐ router2
☐ router3
router1
LATENCY FOR THE GATEWAY ROUTER1 OF THE ROUTER SD-WAN_VOIP
Milliseconds
4
3
2
1
0
Tuesday 8th February 2022 15:37 — Tuesday 8th February 2022 16:37
Jitter
Latency
PACKET LOSS RATE AND UNAVAILABILITY RATE FOR THE GATEWAY ROUTER1 OF THE ROUTER SD-WAN_VOIP
Percentage
100
75
50
25
0
Tuesday 8th February 2022 15:37 — Tuesday 8th February 2022 16:37
Packet loss
Unavailability rate
STATUS BALANCING FOR THE GATEWAY ROUTER1 OF THE ROUTER SD-WAN_VOIP
Percentage
100
75
50
25
0
Tuesday 8th February 2022 15:37 — Tuesday 8th February 2022 16:37
Functional
Degraded
Unreachable

Further reading

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

STORMSHIELD

documentation@stormshield.eu

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