STORMSHIELD

TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

MANAGING BYPASS ON SNS FIREWALLS

Document last updated: January 15, 2025
Reference: sns-en-managing_bypass_technical_note

Table of contents

Change log

Date	Description
January 15, 2025	New document

Getting started

When the bypass function found on some SNS firewalls and network modules is enabled (ready to be triggered), during critical hardware and software failures, network traffic is channeled through the SNS firewall without being analyzed.

The bypass function ensures service continuity in sensitive environments. Do note, however, that due to the way they operate, the high availability feature on SNS firewalls is incompatible with the bypass function.

This technical note provides details on:

- Information regarding bypass components, their interactions and communication modes, as well as how bypass operates,
- The SNS firewalls and network modules that are equipped with bypass,
- Information on the interfaces of bypass segments, and on inserting the network module,
- The operation of Safety mode in bypass, and its configuration on SNS firewalls,
- How to check the bypass status on SNS firewalls.

Bypass operating principle

This section presents Information regarding bypass components, their interactions and communication modes, as well as how bypass operates.

Bypass components and interactions

Microcontroller

The microcontroller (or *uController*) is an essential component of the bypass. When it triggers the bypass mechanism, the bypass communication mode changes. This change is known as a "switch".

There are two possible types of switch:

- When the bypass mechanism is enabled (ready to be triggered), and a critical hardware or software failure occurs on the SNS firewall, the microcontroller triggers the bypass mechanism, which switches the communication mode from normal to bypass mode. Depending on the type of failure, the microcontroller will immediately trigger the bypass mechanism, or wait for the watchdog to time out.
- When the bypass mechanism has been triggered, the communication mode remains in bypass mode as long as the bypass mechanism has not been reset. Resetting the bypass mechanism switches the communication mode from bypass to normal mode.

Watchdog

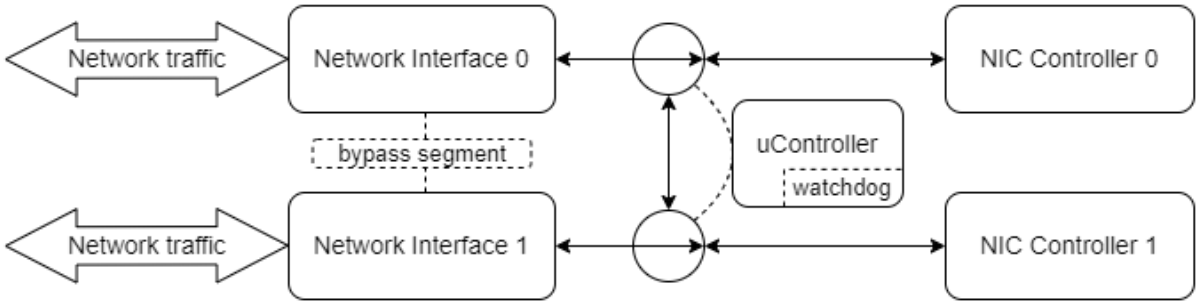
The watchdog, which is built into the microcontroller, serves as a timer, which can be configured in the SNS firewall's settings.

When the status of the watchdog can no longer be refreshed by the SNS firewall hardware manager, especially when the SNS firewall's operating system is no longer responding or is saturated, the timer will start counting down. When the timer is at zero, this means that the idle timeout has been reached, and the microcontroller triggers the bypass mechanism (switch to bypass mode).

Bypass segments

A bypass segment consists of two interfaces that are associated as a pair. This association is set in the hardware and cannot be changed.

When the bypass mechanism is triggered (switch to bypass mode), all network traffic from the bypass segment will be diverted from one interface to the other, and passes through the SNS firewall without being analyzed.



Bypass communication modes and switching

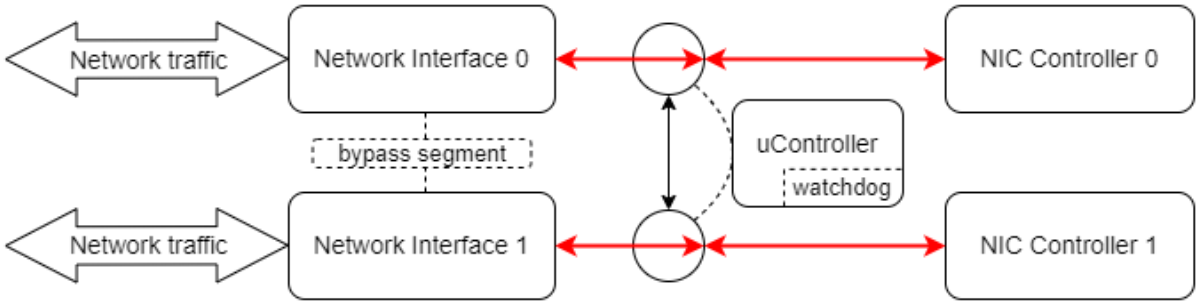
Bypass communication mode switching depends on the bypass mechanism. When the mechanism is triggered, the communication mode on the interfaces in the bypass segment switches from one mode to another.

There are two bypass communication modes.

Normal communication mode

This is the default communication mode for the bypass.

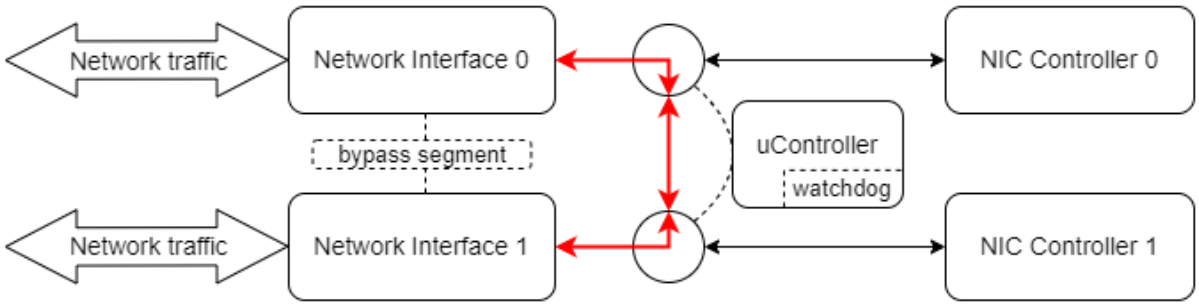
In this mode, network interface connections on the bypass segment are connected to network controllers. The SNS firewall's security rules then apply to the network traffic.



Bypass communication mode

This mode is used only when the bypass mechanism has been triggered.

In this mode, network interface connections on the bypass segment are disconnected from network controllers, and diverted to the other interface to create a looped crossover connection. All network traffic is then diverted from one interface to the other, and passes through the SNS firewall without being analyzed.



Switch time

This is the time that the bypass mechanism needs to switch from one communication mode to another. This takes approximately 100 ms.

IMPORTANT
The switch time does not correspond to the recovery time as other elements have to be taken into consideration. This duration is explained in the section Configuring bypass in Safety mode.

Bypass operating modes

Two operating modes enable interaction with bypass's communication modes.

Security mode	Safety mode
Prioritizes network security and protection.	Prioritizes service continuity.
Default operating mode when Safety mode is not enabled.	Operating mode that needs to be manually enabled in the SNS firewall configuration.
The bypass function remains **permanently disabled**. The bypass communication mode permanently remains in normal mode.	The bypass mechanism is enabled, meaning that it is ready to be triggered. When a triggering event occurs, the bypass mechanism is then triggered, which will switch the bypass mechanism's communication mode.

NOTE
Safety mode is explained in the section Configuring bypass in Safety mode.

SNS firewalls and network modules equipped with the bypass function

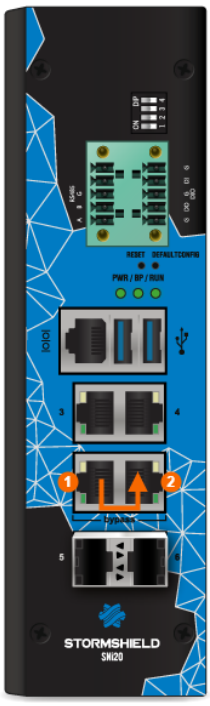
This section lists the SNS firewalls and network modules that are equipped with the bypass function.

NOTE
On SNS firewalls that require a network module, only the slot for inserting the module is indicated. For further information, refer to the Procedures for inserting or removing extension modules in the *SNS presentation and installation guide*.

SNi40

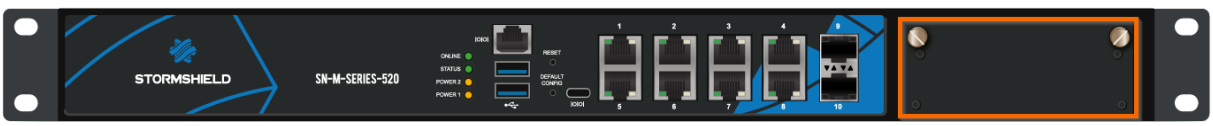
- Number of bypass: 1,
- Bypass included,
- The "in" and "out" interfaces are paired, and form a bypass segment.

SNi20



- Number of bypass: 1,
- License option required,
- The "in" and "out" interfaces are paired, and form a bypass segment.

SN-M-Series-520 (SN520)

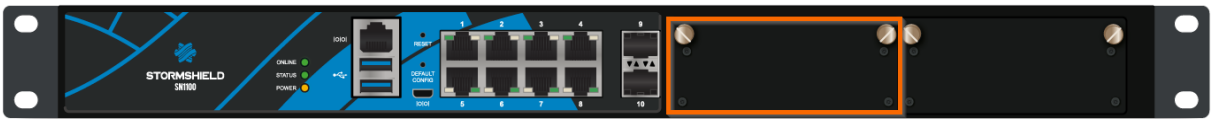


- A network module is required in order to benefit from the bypass function. It has to be inserted in the extension slot intended for this purpose.

SN-M-Series-720 (SN720) and SN-M-Series-920 (SN920)

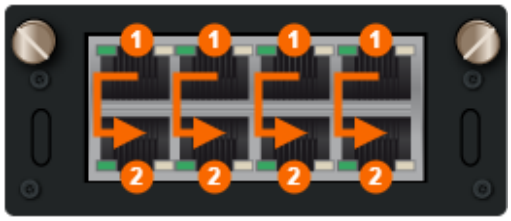
- A network module is required in order to benefit from the bypass function. It has to be inserted in the extension slot intended for this purpose.

SN1100



- A network module is required in order to benefit from the bypass function. It has to be inserted in the extension slot **on the left**.
- The SNS firewall BIOS has to be in version R1.01 or higher to ensure the proper operation of the bypass function. For more information, refer to the technical note SN1100 - Updating BIOS to version R1.01.

8-port 1Gbps copper network module (NA-EX-CARD-BP-8xG-C)



- Number of bypass: 4,
- Compatible SNS firewalls: SN-M-Series-520, SN-M-Series-720, SN-M-Series-920 and SN1100,
- Lowest SNS version required: 4.8.1,
- Interfaces are paired vertically, and form bypass segments.

Configuring interfaces on a bypass segment

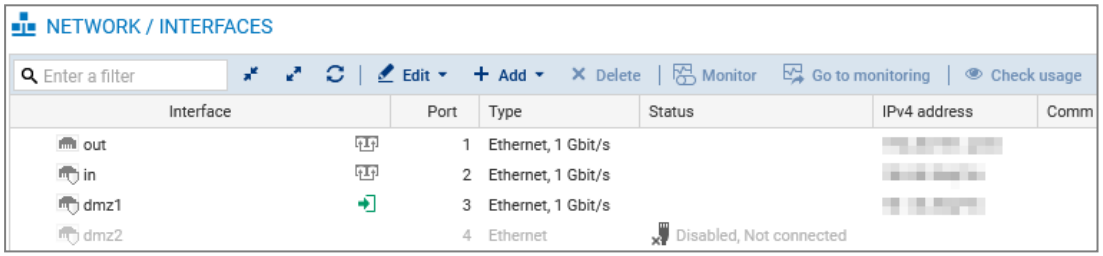
This section shows how to configure interfaces on a bypass segment in the SNS firewall web administration interface.

Accessing interface configuration panel

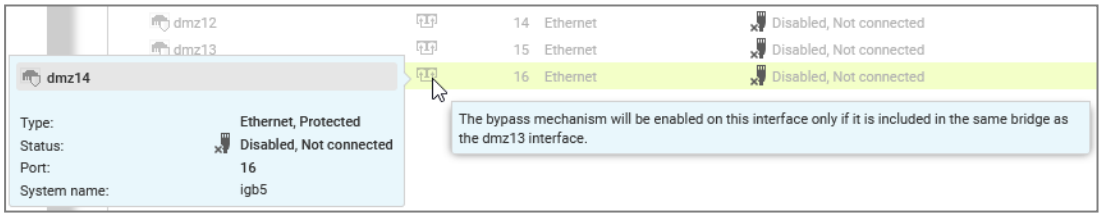
Go to **Configuration > Network > Interfaces**.

In the grid:

- The icon indicates the SNS firewall connection interface. If the IP address of this interface is changed during configuration, the connection to the SNS firewall will be lost, and you will need to use the new IP address to connect again.



- The icon indicates that an interface is associated with a bypass segment. This icon does not appear in SNS 4.3 LTSB versions. If several bypass segments are available, you can scroll over the icon to display the name of the other interface in the bypass segment.



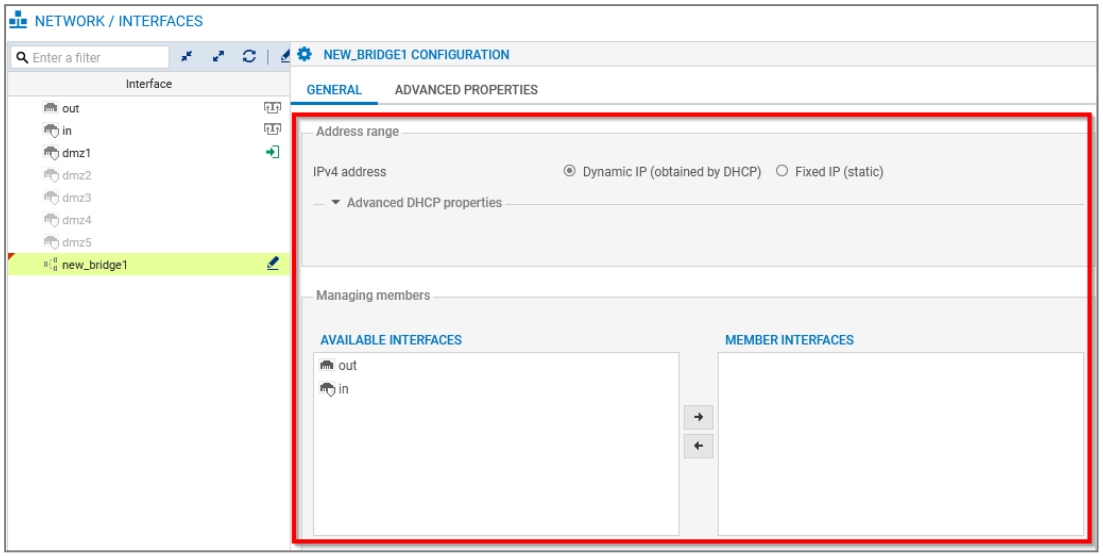
Grouping interfaces from the bypass segment into a bridge

To enable the bypass mechanism on a bypass segment, you will need to group both of its interfaces into a bridge. Although this grouping is not mandatory on SNi40 and SNi20 firewalls, it is strongly recommended.

NOTE
On SNS firewalls that are equipped with a network module, the bypass mechanism cannot be enabled on aggregated module interfaces.

1. Go to the interface configuration panel.
2. Click on **Add > Bridge > No members**.
3. Give the bridge a name, then click on **Apply**.
4. The bridge configuration window appears. In the **Address range** section, define the desired address range.

5. In **Managing members**, select the interfaces of the bypass segment in question.

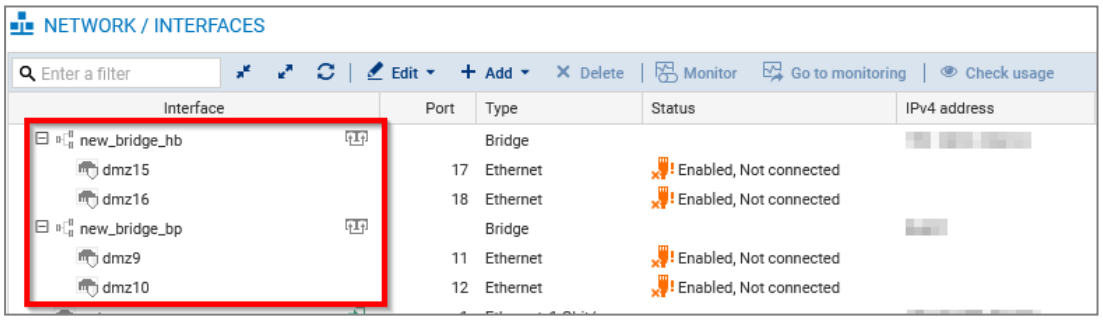


6. Click on **Apply**.

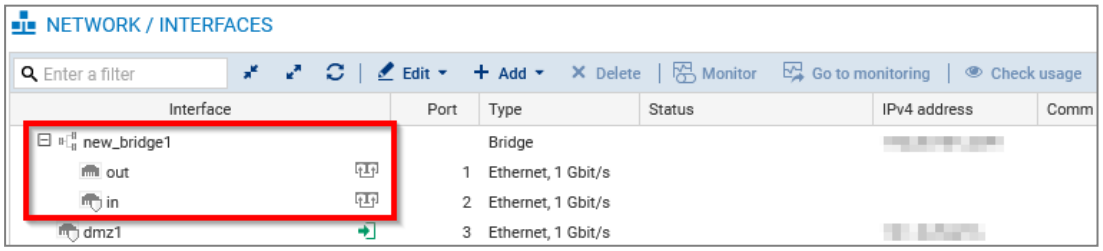
If the interfaces in question and/or address range entered are already being used in the SNS firewall configuration, errors will appear in the **Verification of the configuration** section. In this case, you need to adapt the SNS firewall configuration and/or select another address range before you can group the interfaces into a bridge.

Once you have created the bridge with the interfaces from the bypass segment:

- On SNS firewalls that have several bypass segments, the icon is now next to the bridge,



- On SNi40 and SNi20 firewalls, the icon remains next to the interfaces from the bypass segment.

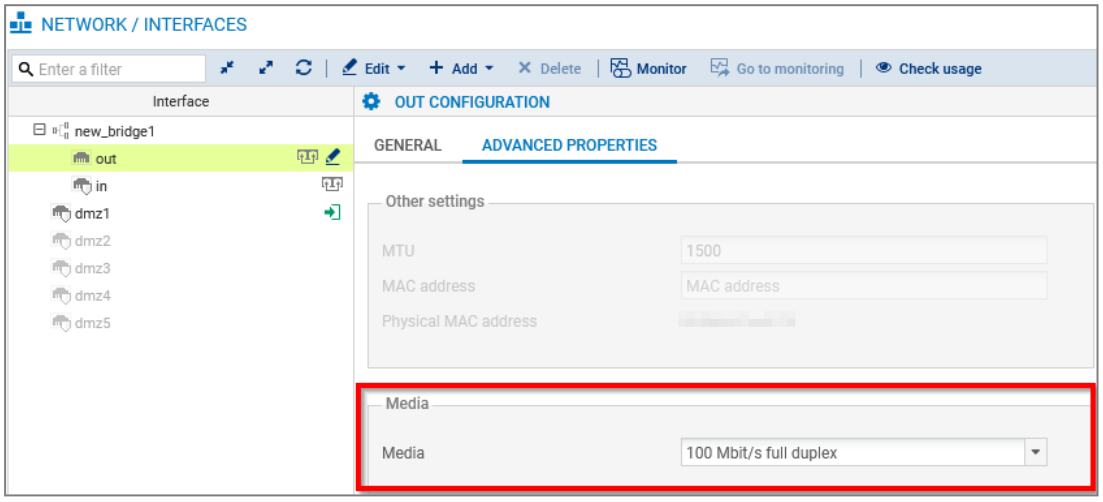


Optimizing interface and bridge configuration

You can optimize the configuration of interfaces from the bypass segment and the bridge to speed up the bypass process. These optimizations are recommended.

Configuring the same media on both bypass segment interfaces

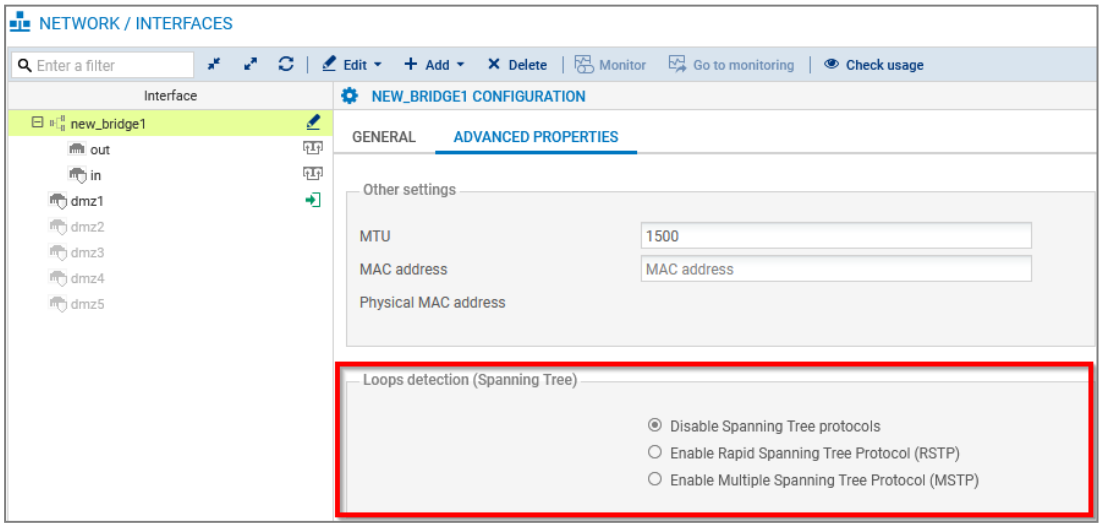
1. Go to the interface configuration panel.
2. Double-click on the first interface in the bypass segment.
3. In the **Advanced properties** tab, select the appropriate **Media** for your environment.
4. Click on **Apply**.



5. Double-click on the second interface in the bypass segment.
6. In the **Advanced properties** tab, select the same **Media**.
7. Click on **Apply**.

Disabling Spanning Tree protocols on the bridge

1. Go to the interface configuration panel.
2. Double-click on the bridge that groups both bypass segment interfaces.
3. In the **Advanced properties** tab, under **Loops detection (Spanning Tree)**, ensure that **Disable Spanning Tree protocols** has been selected.
4. Click on **Apply**.



Configuring bypass in Safety mode

This section explains how bypass in Safety mode functions, and how to configure it in the SNS firewall web administration interface.

Understanding how Safety mode functions

Safety mode prioritizes service continuity. When this mode is enabled:

- The bypass mechanism is enabled (ready to be triggered) on all bypass segments that have been configured to use it,
- When a triggering event occurs, the bypass mechanism is triggered, which switches the bypass's communication mode to *bypass*,
- Once the bypass mechanism has been triggered, the only way to switch the communication mode from *bypass* to *normal* is to reset the bypass mechanism.

If the Safety mode is not enabled, Security mode will be used. In this mode, the bypass function remains **permanently disabled**, even during a critical failure.

Events that trigger the bypass mechanism in Safety mode

The bypass mechanism is triggered whenever one of the following events occurs:

- When the SNS firewall experiences an electrical failure or power outage,
- When the SNS firewall restarts, once the BIOS has been initialized.

> **NOTE**
> The bypass mechanism will be automatically reset once the SNS firewall restarts.

- During a software failure, especially when the SNS firewall's operating system has stopped responding or is saturated, after the watchdog has timed out.

Recovery time

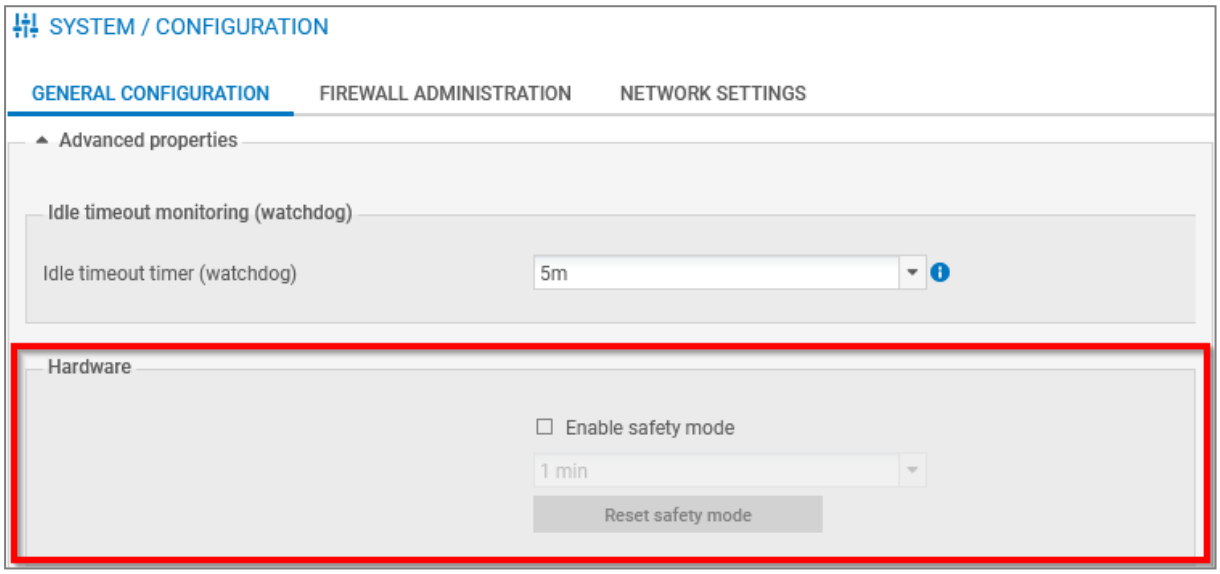
This is the time required to ensure service continuity. Depending on the triggering event, you need to add up all the times in the table, or only some to determine the theoretical recovery time.

Item	Time required for recovery (to be added up)
Watchdog timer	1 to 4 minutes, depending on the duration set in the Safety mode configuration. The timer starts when the status of the watchdog can no longer be refreshed by the SNS firewall hardware manager, especially during a software failure. When the timer is at zero, this means that the idle timeout has been reached, and the bypass mechanism will be enabled (communication in bypass mode).
Switch time	Approximately 100 ms. This is the time required to switch the bypass's communication mode.
Remote device detection time	Generally between 3 and 10 seconds. After a switch, this is the time that remote devices need to detect the change in status ("*DOWN*" or "*UP*") on interfaces in the bypass segment. The duration varies by remote device and the version installed on the SNS firewall.

Accessing Safety mode configuration

1. Go to **Configuration > System > Configuration, General configuration** tab.
2. Expand the **Advanced properties** section.
   Safety mode settings can be found in the **Hardware** section.

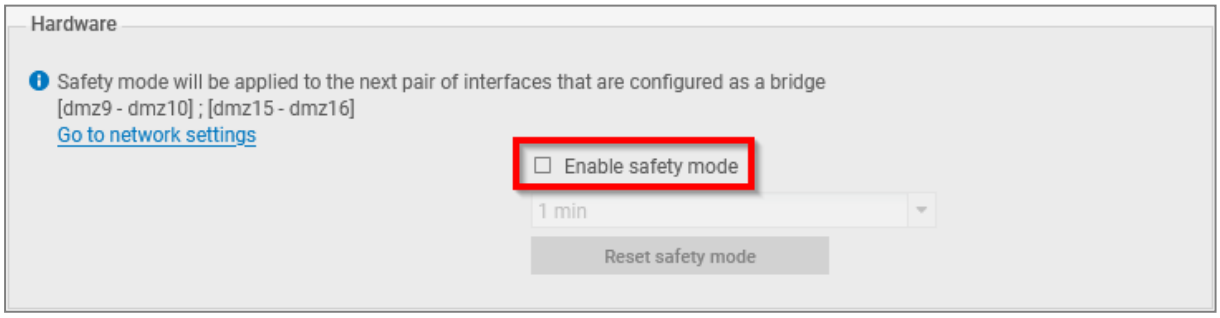
On SNS 4.3 LTSB versions, the interface is slightly different, but Safety mode is configured in the same way.



Enabling or disabling Safety mode

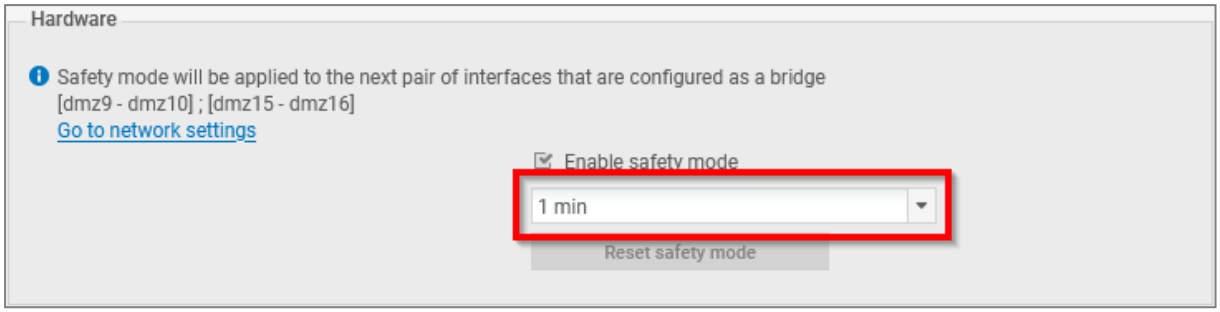
Reminder: Safety mode cannot be enabled on SNS firewalls in high availability.

1. Go to the Safety mode settings.
   On SNS firewalls that have several bypass segments, a list shows the bypass segments on which Safety mode will be enabled.
2. Select or unselect the **Enable safety mode** checkbox.
3. Click on **Apply**.



Setting the watchdog timer (idle timeout)

1. Go to the Safety mode settings.
2. In the drop-down list below the **Enable safety mode** checkbox, select the desired timeout.
   The selectable values range from 1 to 4 minutes.
3. Click on **Apply**.



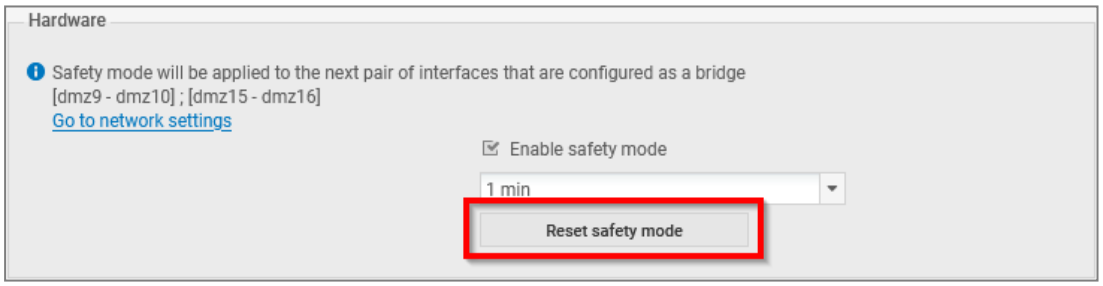
Resetting the bypass mechanism (resetting Safety mode)

Once the bypass mechanism is triggered, the only way for the SNS firewall to analyze traffic again is to reset the bypass mechanism. Resetting the bypass mechanism switches the communication mode to normal mode, which will then involve a recovery time that corresponds to the switch time and remote device detection time.

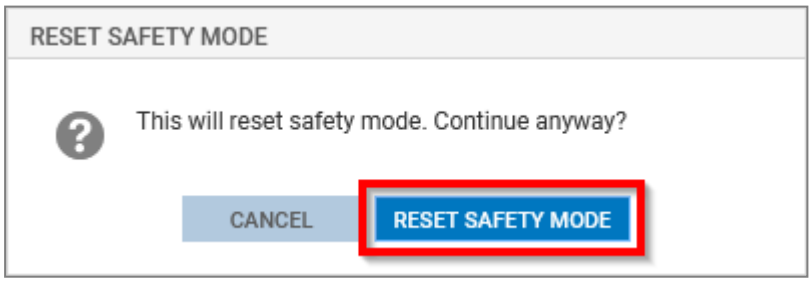
The bypass mechanism will be automatically reset when the SNS firewall completes its startup phase.

You can manually reset the bypass mechanism in the SNS firewall web administration interface.

1. Go to the Safety mode settings.
2. Click on **Reset safety mode**.



3. In the window that appears, confirm that you want to reset Safety mode.



IMPORTANT
After a manual reset, check whether network traffic is functioning properly, as connections that are initiated during the active phase of the bypass mechanism will be shut down, and have to be set up again by remote devices.

Checking bypass status

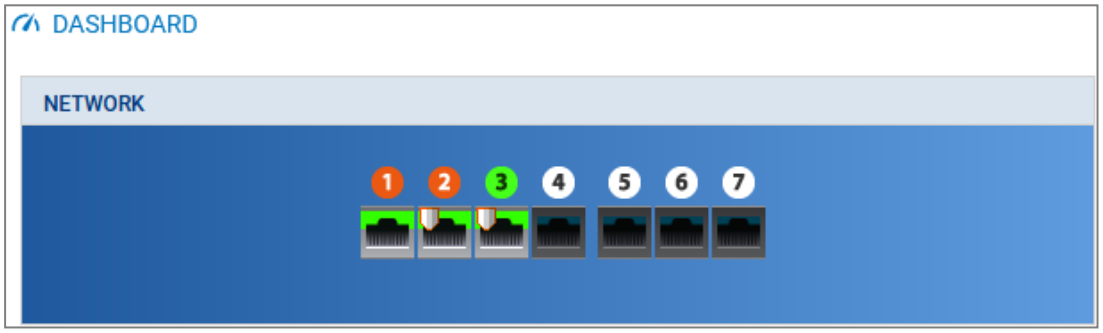
This section explains how to check the bypass status on the bypass segments of an SNS firewall (Safety mode enabled, bypass mechanism triggered, etc.).

In the dashboard module

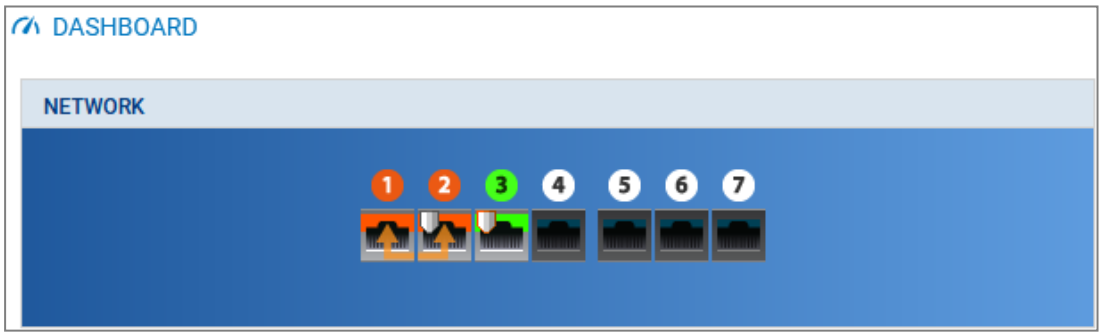
This use case is exclusive to SNS 4.8 and higher versions.

In the web administration interface, go to **Monitoring > Dashboard**. The **Network** widget provides a graphical representation of the interfaces on an SNS firewall:

- When Safety mode is enabled (bypass mechanism ready to be triggered), interface numbers on bypass segments appear in an orange circle,



- When the bypass mechanism has been triggered, interfaces on bypass segments appear in orange with a two-way arrow that links them.



In the CLI/Serverd console

You can interact with the bypass by using the command set `SYSTEM BYPASS` and the command `MONITOR BYPASS`.

In the CLI/SSH console

The bypass operating mode appears in a message after authentication:

- "*Operating mode : Security*" indicates that Security mode is in use,
- "*Operating mode : Safety*" indicates that Safety mode is enabled,
- "*Operating mode : Bypass*" indicates that the bypass mechanism has been triggered.

In the CLI/SSH console, you can interact with the bypass by using the command `enbypass`.

```
Last login: Tue Dec 10 12:46:09 2024 from [redacted]
[redacted]: FW SNi40 (M / EUROPE)
Firewall software version 4.8.4 RELEASE

port       name       NS-BSD   state  addressIPv4         addressIPv6
   1        out         igb0 no-link  [redacted]
   2         in         igb1 no-link  [redacted]
   3       dmz1         igb4      up  [redacted]
   4       dmz2         igb5    down
   5       dmz3         igb6    down
   6       dmz4         igb2    down
   7       dmz5         igb3    down
Operating mode : Bypass

[redacted]>
```

With the status of LEDs on RJ45 network port connectors

By going to the physical location of the SNS firewall, you can check the status of LEDs on the RJ45 network port connectors of bypass segments.

SNi40 and SNi20

When the bypass mechanism has been triggered, LEDs on RJ45 network port connectors of bypass segments are switched off on SNi40 and SNi20 firewalls.

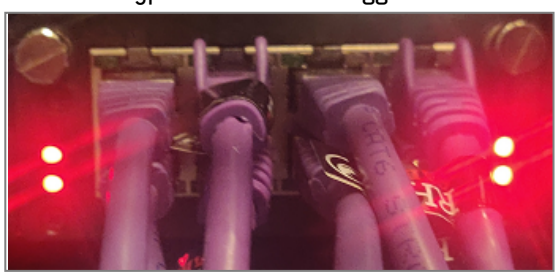
8-port 1Gbps copper network module (NA-EX-CARD-BP-8xG-C)

On SNS firewalls that are equipped with an 8-port 1Gbps copper network module (NA-EX-CARD-BP-8xG-C), when the bypass mechanism has been triggered:

- LEDs on RJ45 network port connectors of bypass segments are switched off,
- LEDs indicating the status of the network module, which are usually green, are red.

Bypass mechanism not triggered

Bypass mechanism triggered



With logs

Several bypass-related logs can be generated. Here are a few examples:

Bypass mechanism triggered as the watchdog has timed out

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz=+0200 startime="YYYY-MM-DD HH:MM:SS" pri=6
service=hardwared msg="Bypass mode triggered: timer expired"
```

Bypass Safety mode enabled (bypass mechanism ready to be triggered)

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz=+0200 startime="YYYY-MM-DD HH:MM:SS" pri=5
service=enbypass msg="Bypass activated on segments 0,1,2,3"
```

On SNi40 and SNi20 firewalls, the bypass segments in question do not appear.

Bypass mechanism reset (Safety mode reset)

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz=+0200 startime="YYYY-MM-DD HH:MM:SS" pri=5
service=enbypass msg="Run-time bypass watchdog rearmed"
```

With MIBs and SNMP traps

Information on the status of the bypass on the SNS firewall's bypass segments can be retrieved with the MIB **STORMSHIELD-SYSTEM-MONITOR-MIB**, SNMP table **snsBypassTable**.

To do so:

- Download the SNMP MIBs from your MyStormshield personal area, in **Downloads > Downloads > Stormshield Network Security > SNMP MIBs**.
- Configure the **SNMP agent** module in the SNS firewall web administration interface.

For more information, refer to the SNMP agent section in the *SNS user manual*.

Further reading

Additional information and answers to some of your questions may be found in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu