STORMSHIELD

GUIDE

STORMSHIELD NETWORK SECURITY

PRODUCT PRESENTATION AND INSTALLATION 2023

Date : May 2023

Version du document : 2.0

Référence : sns-en-SNrange_installation_guide

Table of contents

FOREWORD

We strongly recommend that you read this whole document before installing a Stormshield Network firewall.

This installation guide presents the **Stormshield Network range** marketed by Stormshield. In this guide, we explain how to conduct the physical installation needed to integrate an appliance into your network architecture. It also provides the necessary details for adding transceivers and network modules to SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100, SN6100, SNi20 and SNi40 products.

The aim of this manual is to allow you to quickly integrate a Stormshield Network firewall into your network but does not provide any information on how to configure the product. For help in configuration, there is a full **User guide** in the form of online help, which you can look up on the **Stormshield Technical Documentation** website, at:
https://documentation.stormshield.eu

The *SNS user configuration manual,* an exhaustive help file, can be downloaded from the section **PDF download** (refer to the section DOCUMENTATION & ASSISTANCE).

Products concerned

SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100, SN6100, SNi20, SNi40 and Snxr1200 models.

NOTE
For earlier products in the **Stormshield Network range** (SN150, SN200, SN300, SN500, SN700, SN900, SN2000, SN3000 and SN6000), refer to the 2016 version of this *Product presentation and installation* guide.

Recommendations on the operating environment

DEFINITION

On an Evaluation Assurance Level or EAL scale of 1 to 7, the Common Criteria evaluate a product's capacity to provide security functions for which it had been designed, as well as the quality of its life cycle (development, production, delivery, operation, and updates).

Introduction

The installation of a firewall is often part of implementing a global security policy. To ensure optimal protection of your assets, resources and information, installing a firewall between your network and the Internet is only the first step. This is mainly because most attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.). And anyone would agree that installing a steel security door defeats its purpose when the walls are made of paper.

Stormshield Network therefore adopts and applies the usage recommendations defined in the Common Criteria in its administration suite and firewalls. These recommendations set out the usage requirements to meet to ensure that your firewall operates within the context of the common criteria certification.
For further information on Common Criteria compliance, go to:
https://documentation.stormshield.eu/common-criteria.html

Security watch

Check regularly for the Stormshield security advisories published on https://advisories.stomshield.eu.

Always apply updates if they fix security flaws on your firewall. Updates are available here: https://mystormshield.eu.

Physical security measures

Stormshield Network firewall-VPN appliances must be installed and stored in compliance with the state of the art regarding sensitive security devices: secured access to the premises, Shielded cables with twisted pairs, labeled cables, etc.

Organizational security measures

The default password of the “admin” user (super administrator) must be changed the very first time the product is used. In the web administration interface, this password can be changed in the Administrator module (System menu), under the Administrator account tab.

This password must be set according to the best practices described in the **User Guide**, in the section *Welcome*, sub-section *User awareness*, paragraph *User password management*, available at:https://documentation.stormshield.eu/

A particular administrative role – that of the super-administrator – has the following characteristics:

- Only the super-administrator is permitted to connect via the local console on firewall-VPN appliances, and only when installing the firewall or for maintenance operations, apart from actual use of the equipment.
- In charge of defining the profiles of other administrators,
- All access to the premises where the appliances are stored must be under this administrator's supervision, regardless of whether the purpose of the access is to conduct operations on the appliance or on other equipment. All operations conducted on any firewall-VPN appliance are under this administrator’s responsibility.

IT security environment

Stormshield Network firewall-VPN appliances must be installed in accordance with the current network interconnection policy and are the only passageways between the various networks on which the control policy for traffic must be applied. They are scaled according to the capacities of the adjacent devices or these devices restrict the number of packets per second, positioned slightly below the maximum processing capacities of each firewall-VPN appliance installed in the network architecture.

Regulations

WEEE (Waste Electrical and Electronic Equipment) directive
All Stormshield Network products that the WEEE directive concerns are marked with the mandated crossed-out wheelie bin symbol. This symbol means that the product meets the requirements laid down by the WEEE directive with regard to the destruction and reuse of waste electrical and electronic equipment.

RoHS (Restriction of Hazardous Substances) directive
For further information on RoHS compliance or on the Stormshield Network firewall recycling program (WEEE), refer to:
https://www.stormshield.com/about/recycling/

Certifications

Part 15 Subpart B

INTRODUCTION

Thank you for choosing Stormshield Network. Designed to protect networks of all sizes, **Stormshield Network - SN range** appliances are pre-configured: no hardware or software installation is needed and no UNIX knowledge is necessary, just a user-friendly configuration via a graphical interface.

The **Stormshield Network (SN)** range consists of twenty products:

SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN910, SN-M-SERIES-720, SN-M-SERIES-920, SN1100, SN2100, SN3100, SN6100, SNi20, SNi40 and SNxr1200.

The architecture of the new-generation SN range was specifically designed to maximize the performance of the Stormshield Network protection engine. Complex application traffic is therefore inspected at high speed at the heart of the network and without discernible latency (less than 1 millisecond).

Hardware acceleration for data encryption also anticipates multiple high-speed VPN sessions.

The SN firewall makes it possible to define incoming or outgoing access control rules. Its concept is simple: any incoming or outgoing transmission passing through the firewall is monitored, allowed or blocked according to the rules, packet by packet.

The SN firewall is based on a sophisticated packet filtering mechanism that provides a high level of security. All firewalls integrate the ASQ (Active Security Qualification) technology developed by Stormshield Network Security. This technology makes it possible detect and block hacking attempts in real time: illegal packets, denial of service attempts, anomalies in a connection, port scans, buffer overflows, etc.

In an intrusion attempt, depending on the instructions set in the security policy, the SN firewall blocks the transmission, generates an alarm and stores the information linked to the packet which set off the alarm. You will therefore be able to analyze the attack and trace its source.

The SN firewall not only allows you to prevent, or restrict to just certain services, incoming connections on your network, but also makes it possible to monitor the use of the Internet by your internal users (HTTP, FTP, SMTP, etc.). You can also monitor your users by authenticating them via an internal or external authentication database.

The SN firewall also manages port and address translation mechanisms. These mechanisms provide security (by masking your internal address range) and flexibility (by enabling the use of any private internal addressing range) and reduce costs (by enabling the provision of several servers on the Internet with a single public IP address).

Stormshield Network Vulnerability Manager, the risk management solution, is based on the detection of applications and the associated vulnerabilities. It allows you to quickly zero in on the most vulnerable hosts, identify affected applications and know which bug fixes to apply.

Lastly, the SN firewall includes VPN gateway functions allowing you to establish encrypted tunnels with other VPN equipment. In this way, your communications between sites or with your mobile users may be secured even while using an insecure communication infrastructure like the Internet.

Administration tools

Thanks to the web administration interface, you can administer your Stormshield Network firewall from the operating system of your choice. The new firewall configuration interface, accessible from a web browser, benefits from the latest breakthroughs in user friendliness and simplicity of use.

Monitoring tab

The **dashboard** gives an overview of information relating to the firewall's activity and its configuration.

The **Logs - Audit logs** module, available on firewalls equipped with storage media, allows you to read logs generated by appliances and stored locally. These logs are grouped by views, i.e., by alarm, connection, web log, etc. Advanced filters make it possible to analyze logs even deeper.

In the **Reports** module, you will be able to view how Internet access is used, which attacks your firewall blocked, and which hosts are vulnerable on your corporate network. Many interactive features allow you to modify the configuration of your firewall. These reports appear as Top 10 lists in Web, Security, Viruses, Vulnerabilities and Spam.

The **Monitoring** module shows graphs and data in real time, and history graphs can be added to these if this option is enabled in the **Report configuration** module.

Stormshield Management Center

With the SMC administration tool, you can manage and supervise a pool of SNS firewalls. Common or specific filter rules and VPN access can be set up to optimize configuration tasks. Always keep your firewall pool up to date, make regular backups and configure the privileges of your SMC administrators.

UPON RECEIVING YOUR FIREWALL

Several security mechanisms have been implemented to guarantee the integrity of the product that you receive, and confirm that your product has not been tampered with. **Check them carefully to avoid any ambiguity regarding the application of the warranty.**

If your product does not match your order, report it to your reseller within 48 hours after you receive the product.

Integrity of the product

Seals and labels on the packaging

Every firewall is delivered in a cardboard box sealed with one or two warranty seals. A label on the packaging indicates information that identifies the product it contains and its version. Check that this information matches your order.

Seals

Every firewall is sold in a closed cardboard box sealed with a "STORMSHIELD QUALITY SEAL".

IMPORTANT
If this seal is missing or has been tampered with, contact your distributor as soon as possible to find out why the packaging has been opened.

Figure 1: .
"Stormshield Quality seal" label

Identification labels

These labels indicate the information relating to the firewall (product reference, part number, serial number, software version installed, etc). Check that this information matches your order. You can also check whether the version installed has been certified.

Figure 2: Product labels on the cardboard box

Labels on the product

Warranty label

A warranty label is pasted on all firewalls. Once this label is torn, the warranty will be void.

Figure 3:
Warranty label

Serial number label

This label displays your product's serial number and registration password. It is pasted on:

- the underside of SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN2100 and SN3100 models,
- the back of the firewall on SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN6100 and SNxr1200 models,
- the side on SNi20 and SNi40 models.

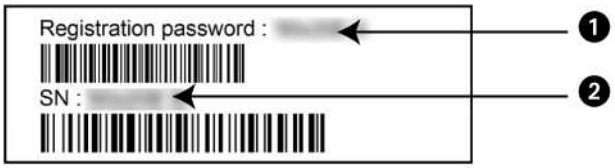


Figure 4: Serial number label

IMPORTANT
Take note of your registration password ❶ and your serial number ❷. You will be asked for these during the installation and registration of your product.

Product label

This label, found on your product, provides information relating to the firewall, such as the part number and the product's electrical power characteristics.

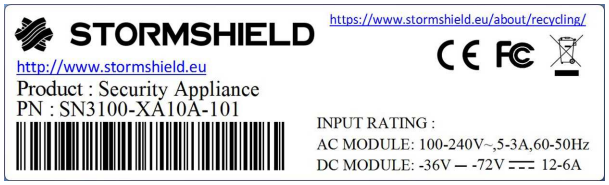


Figure 5: Product label

Contents of the packaging

Keep the cardboard packaging in a safe place in case you need it later to transport the firewall. The packaging is shock resistant to protect your SN firewall optimally.

Upon delivery, check that all the following components are included:

- Your Stormshield Network firewall,
- A power cord (two for SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models),
- A power adapter (SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320 models),
- A 6-pole screw connector (SNi20 and SNi40),
- A Category-5e RJ45 crossover cable,
- An “A to B” USB cable (SN160, SN160W, SN210, SN210W and SN310) or “A to C” USB cable (SN-S-Series-220, SN-S-Series-320, SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920),

- An RJ45 to DB9F serial DB9F (SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100, SN6100 and SNi20) or DB9F serial (SNi40 and SNxr1200 models),
- A micro USB cable: an "A" to “B” micro USB (SN1100),
- Three Wi-Fi antennae to be screwed to the back of the appliance (SN160W and SN210W).

For SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models, the packaging should also contain four non-slip rubber feet.

SN6100 models have brackets mounted by default so that they can be installed in a rack. Depending on the model, the following components are also included for racking:

- SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models: a set of brackets and screws,
- SN1100: a set of brackets, rails and screws,
- SN2100 and SN3100: a set of brackets, slide rails and screws,
- SN6100: a set of slide rails and screws.

SNi20 and SNi40 models are equipped with a fastener for a 35 mm-wide DIN rail (EN50022 standard).

NOTE
As SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 firewalls can be installed on a desk or in a rack, their non-slip rubber feet come separately. Only products that cannot be racked (SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320) are sold with the rubber feet already attached.

The documentation provided includes:

- General Conditions of Use and User License,
- Safety Rules and Installation Precautions,
- Quick Installation Guide,
- Installation guide for mounting the firewall in a rack (SN1100, SN2100, SN3100 and SN6100).

If any component is missing, contact your distributor immediately.

SAFETY RULES

Before installing anything, carefully read and follow the safety instructions.

All models except SNi20, SNi40 and SNxr1200

IMPORTANT
You must use the power adapter provided with the product.

Before plugging in any devices

- Ensure that neither your Stormshield product, the power cord nor power adapter is damaged.
- Ensure that the power supply or power adapter of your Firewall is compatible with the voltage of your power supply network.
- When the product's power cord or power adapter has a ground pin, it must be plugged into a properly grounded electrical outlet. Ensure that the connection is reliable and that the protective earth circuit of your installation complies with safety standards in force.
- To be able to disconnect the product, ensure that the connection to the power supply is always easily accessible.

Before connecting to a -48VDC power supply (SN1100, SN2100, SN3100 and SN6100)

Special considerations for equipment connected to a DC mains supply:

- Please follow IEC, NEC, ANSI/NFPA 70 and CEC, Part I, C22.1 for all relevant field wiring instructions and cautions. The equipement must be installed by a qualified electrician.
- Before using the equipment, the chassis must be permanently connected to earth using yellow/green wire rated a minimum of:
  - 1.5mm² (16 AWG) on SN1100, SN2100 and SN3100
  - 3.31mm² (12AWG) on SN6100
- The equipment shall be connected to the DC mains supply with an approved switch or breaker.
- Only wires with the following minimum ratings shall be used to connect the equipment to the DC mains supply:
  - 1.5mm² (16 AWG) on SN1100, SN2100 and SN3100
  - 3.31mm² (12AWG) on SN6100

Warranty and safety rules

Under no circumstances should you take apart a Stormshield Network appliance on your own. Only Stormshield, which markets the Stormshield Network range, and its approved maintenance agents are authorized to do so. A seal label protects all Stormshield Network Firewalls from being opened.

Your warranty will be rendered null and void should you dismantle a Stormshield Network Firewall on your own.

IMPORTANT
Never dismantle your Stormshield appliance, as doing so may cause hardware accidents and/or bodily harm.

IMPORTANT
Do not insert objects into the appliance's vents – this may hinder the rotation of an internal fan or damage it, causing the appliance to overheat. This may also cause a short-circuit that may lead to the breakdown of the appliance.

IMPORTANT
Copper Ethernet cables connected to your Stormshield Network Firewall must not be connected to other appliances located in other buildings.

As per legal safety requirements, anyone performing any operation on a Stormshield Network SN-range product must know and follow the safety indications below:

To the attention of maintenance teams:

WARNING
DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

Only qualified personnel from an approved maintenance center can perform operations on this component.

In the event of hardware problem with your Firewall or if one of the elements does not match its description, please contact your certified partner.

Installing an appliance outside a rack

Your product must be equipped with its non-slip rubber feet in order to reduce the possibility of your appliance slipping off the surface on which it has been installed.

These flexible non-slip rubber feet are to be attached to the underside of the chassis for SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models.
Please refer to the section INSTALLATION PRECAUTIONS for further information.

Assembly in a cabinet

For a racked installation, place heavier appliances in the lower section of the rack and lighter elements in the higher section.

Refer to the section INSTALLATION IN A 19" CABINET for details on how to install an appliance in a racking bay.

Precautions

- **Installation kit -** for rack mounting the original installation kit for this device has to be used.
- **Elevated Operating Ambient Temperature -** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- **Reduced Air Flow -** Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- **Mechanical Loading -** Mounting of the equipment in the rack should be such that hazardous conditions due to uneven mechanical loading are avoided.
- **Circuit Overloading -** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing -** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- **Leakage current -** considerations should be given to the summation of leakage currents when installing the equipment in a closed or multi-unit rack assembly.

SNi20, SNi40 and SNxr1200 models

Before plugging in any devices

- Ensure that your Stormshield product and its accessories are not damaged.
- Ensure that the electrical characteristics of your product indicated on the product label are compatible with those of your power supply network.
- The chassis of your product must be connected to a protective earth circuit, using rated minimum 16 AWG or 1.5mm² wire. Ensure that the connection is permanent and reliable, and that the protective earth circuit of your installation complies with safety standards in force.
- Before installing or removing your product, ensure that it has been turned off, and that all power supply connections have been removed.
- Equipment connected to a DC mains supply: please follow IEC, NEC, ANSI/NFPA 70 and CEC, Part I, C22.1 for all relevant field wiring instructions and cautions. The equipment must be installed by a qualified electrician. Only the CEI standard applies to the SNxr1200.
- The equipment shall be connected to the DC mains supply with an approved switch or breaker and easily accessible.
- Only wires rated minimum 16AWG or 1.5mm² shall be used to connect the equipment to the DC mains supply.

Warranty and safety rules

Under no circumstances should you take apart a Stormshield Network appliance on your own. Only Stormshield, which markets the Stormshield Network range, and its approved maintenance agents are authorized to do so. A seal label protects all Stormshield Network Firewalls from being opened.

Your warranty will be rendered null and void should you dismantle a Stormshield Network Firewall on your own.

IMPORTANT
Never dismantle your Stormshield appliance, as doing so may cause hardware accidents and/or bodily harm.

IMPORTANT
Copper Ethernet cables connected to your Stormshield Network Firewall must not be connected to other appliances located in other buildings.

As per legal safety requirements, anyone performing any operation on a Stormshield Network SN-range product must know and follow the safety indications below:

To the attention of maintenance teams:

WARNING
DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

Only qualified personnel from an approved maintenance center can perform operations on this component.

In the event of hardware problem with your Firewall or if one of the elements does not match its description, please contact your certified partner.

Assembly in a cabinet

- **Installation kit -** Only use the installation kit supplied with the product.
- **Elevated Operating Ambient -** If installed in a closed or multi-unit cabinet assembly, the operating ambient temperature of the cabinet environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- **Reduced Air Flow -** Installation of the equipment in a cabinet should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- **Mechanical Loading -** Mounting of the equipment in the cabinet should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading -** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing -** Reliable earthing of cabinet-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of terminal blocks).

INSTALLATION PRECAUTIONS

A firewall is a central device in your network, so it requires special attention. Install it under optimal conditions.

NOTE
Instructions on how to connect products are also given in the Poster **Quick Installation Guide** provided with the Firewall.

Conditions of use (all models except SNi20, SNi40 and SNxr1200)

The Stormshield Network firewall is designed to run continuously, in an office or in a server room. If you wish to install your appliance in an office, choose a flat and uncluttered surface. Add the non-slip rubber feet to SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, and SN-M-Series-920 models: stick a non-slip rubber foot to the underside of the appliance, close to each corner about 2 cm from the edges.
This will ensure the stability of the firewall and protect it from scratches.

IMPORTANT
When the Firewall is stored, it must be powered on for a period of 24 hours at least once every 2 years to allow internal electrolytic capacitors to be reformed. Failure to do so may lead to compromised reliability.

WARNING
The firewall must be installed in compliance with state-of-the-art conditions of secure installation, i.e., in a protected office or other premises with limited access. To guarantee the integrity of the product and to avoid compromising the security of your installation, all unauthorized access to the firewall must be prevented.

NOTE
Ensure that the cables do not obstruct passageways to prevent them from being pulled out or the product from falling.

Do not install and/or operate your Stormshield Firewall in any place that flammable objects are stored or used in. Your Stormshield Firewall is intended for indoor use (office environment or other IT environment), away from areas that may receive rainfall, floods or excessive humidity. It must be installed away from sources of shocks, vibrations, and dust, in an environment where the temperature conforms to the product's specifications.

The ideal ambient temperature is around 25°C. The tables below set out the operational temperature, storage temperature and humidity level for all models of SN range.

SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100 and SN3100 models

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
+0° to +40°C (+32° to +104°F)	0% to 95% at +40°C (+104°F) non-condensing	-30° to +65°C (-22° to +149°F)	5% to 95% at +60°C (+140°F) non-condensing

SN6100 model

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
+0° to +40°C (+32° to +104°F)	0% to 90% at +40°C (+104°F) non-condensing	-20° to +70°C (-4° to +158°F)	5% to 95% non-condensing

IMPORTANT
Avoid in particular direct exposure to sunlight. Always keep adequate distance around the appliance's vents in order to guarantee a free flow of air, thereby preventing the possibility of overheating.

IMPORTANT
Do not place objects on your Stormshield Network appliance.

IMPORTANT

The Stormshield Network Firewall has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the Firewall is operated in a commercial environment. The Stormshield Network Firewall generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this Firewall in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The Stormshield Network Firewall complies with the requirements set out in the European standard EN55032, Class A. In a residential environment, a Class A product may cause radioelectric interference, for which the user may need to take appropriate measures.

Conditions of use (SNi20, SNi40 and SNxr1200 models)

SNi20, SNi40 and SNxr1200 firewalls have been built to run continuously, in a server room for SNi20 and SNi40 appliances, or embedded for the SNxr1200.

IMPORTANT
When the Firewall is stored, it must be powered on for a period of 24 hours at least once every 2 years to allow internal electrolytic capacitors to be reformed. Failure to do so may lead to compromised reliability.

WARNING
The firewall must be installed in compliance with state-of-the-art conditions of secure installation, i.e., in protected premises with limited access. To guarantee the integrity of the product and to avoid compromising the security of your installation, all unauthorized access to the firewall must be prevented.

NOTE
Ensure that the cables do not obstruct passageways to prevent them from being pulled out or the product from falling.

Do not install and/or use your Stormshield firewall close to an area where inflammable objects are stored or used.

Your SNi20 or SNi40 Firewall is intended for indoor use, industrial environment (refer to product specifications), away from areas that may receive rainfall, floods or excessive humidity. It must be installed away from sources of shocks, vibrations, and dust, in an environment where the temperature conforms to the product's specifications.

Your SNxr1200 firewall is a built-in system that must be installed under conditions that meet the environmental qualifications provided by Stormshield (upon request).

The ideal ambient temperature is around 25°C. The tables below set out the operational temperature, storage temperature and humidity level for SNi20, SNi40 and SNxr1200 models.

SNi20, SNi40 and SNxr1200 models

Model	Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
SNi20 and SNxr1200	-40° to +70°C (-40° to +158°F)	0% to 95% non-condensing	-40° to +85°C (-40° to +185°F)	0% to 95% non-condensing
SNi40	-40° to +75°C (-40° to +167°F)			5% to 95% non-condensing

The tables below set out the operational temperature, storage temperature and humidity level for the power adapter, which is sold separately.

Power adapter for SNi20 models (optional)

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
-30° to +60°C (-22° to +140°F)	20% to 90% non-condensing	-40° to +85°C (-40° to 185°F)	10% to 95% non-condensing

Power adapter for SNi40 models (optional)

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
0° to +40°C (+32° to +104°F)	10% to 90% non-condensing	-20° to +70°C (-4° to +158°F)	10% to 90% non-condensing

Power adapter for SNxr1200 models (optional)*

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
-30° to +70°C (-22° to +158°F)	20% to 90% non-condensing	-40° to +85°C (-40° to +185°F)	10% to 95% non-condensing

**approved only for pre-production*

IMPORTANT
Avoid in particular direct exposure to sunlight. Always keep an adequate distance around the appliance (at least 50 mm for the SNxr1200 model) in order to guarantee a free flow of air, thereby preventing the possibility of overheating.

IMPORTANT
Do not place objects on your Stormshield Network appliance.

IMPORTANT

The Stormshield Network Firewall has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the Firewall is operated in a commercial environment. The Stormshield Network Firewall generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this Firewall in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The Stormshield Network Firewall complies with the requirements set out in the European standard EN55032, Class A. In a residential environment, a Class A product may cause radioelectric interference, for which the user may need to take appropriate measures.

Connecting to the mains

The supported voltage ranges from 100V to 240V.

NOTE
You are strongly advised to connect all appliances to a UPS device. As SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN3100 and SN6100 models are equipped with redundant power supplies (option offered on SN-S-Series-220, SN-S-Series-320, SN1100 and SN2100 models), plugging them into two separate mains circuits is recommended.

NOTE
In the event of an accidental power cut, the product will automatically start up once it is powered up again.

NOTE
For SN1100, SN2100, SN3100 and SN6100 models, -48V DC power supply modules may be provided separately upon request.

For SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320 models, insert or screw the connector of the power adapter into the power socket on the rear panel of the Firewall.
Next, connect the adapter to an appropriate mains socket using the power cord provided.

For SN510, SN710, SN910 and SN1100 models, insert the plug of the power cord (provided with the product) into the power socket on the rear panel of the appliance. Next, plug the other end of the power cord into an appropriate mains socket.

For SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN3100 and SN6100 models, insert the plugs of both power cords provided into both power sockets located on the rear panel of the appliance. Next, plug in the other ends of the power cords into appropriate mains sockets.

Connecting a DC power supply unit (SNi20, SNi40 and SNxr1200)

On SNi20 models, the supported voltage ranges from 12VDC to 48VDC. On SNi40 and SNxr1200 models, the supported voltage ranges from 12VDC to 36VDC.

REMINDER
Equipment has to be installed by a qualified electrician.

NOTE
You are strongly advised to connect all appliances to a UPS device. SNi20 and SNi40 models are equipped with a redundant power supply unit, so we recommend that you connect it to two independent sources of power.

NOTE
If the power supply is disrupted, the appliance will automatically start up once it is powered up again.

NOTE
A power adapter may be ordered separately.

Connecting to the network

All models except the SNxr1200 are fitted with **RJ45** Gigabit Ethernet ports by default.
On the SNxr1200 model, **RJ45** Gigabit Ethernet is offered as an option via breakout cables.

SN910, SNi20 and SNi40 models offer by default two SFP sockets, which make it possible to insert **SFP** transceivers, provided as an option.

The SN1100 and SN6100 models also have by default two SFP+ sockets, making it possible to insert **SFP**+ transceivers provided as an option.

SN710, SN910, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models also offer one or several slots for various types of extension modules, depending on the module reference ordered, that allow Ethernet ports to be added:

- **RJ45** copper,
- or module for **SFP** transceivers,
- or module for **SFP+** transceivers,
- or module for **QSFP+** transceivers,

A slot is available on SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models, two on the SN1100, three on SN2100 and SN3100 appliances, and eight on the SN6100.

IMPORTANT
Use only **Stormshield Network-approved SFP (1Gbps), SFP+ (1Gbps/10Gbps)** or **QSFP+ (40Gbps)** transceivers available in the catalogue.

For information on the type of network cable to choose according to the network port and the selected connectors, see the sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

INSTALLATION IN A 19" RACK AND CABINET

All Stormshield Network appliances can be installed in 19-inch cabinets (except SNi20, SNi40 and SNxr1200). A fastening system for placing the appliance in a rack, in the form of a rack mount shelf, can be included by special order for SN160, SN160W, SN210, SN210W and SN310 models. Two SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 or SN-S-Series-320 firewalls can be installed on the same shelf.

SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN2100 and SN3100 models come with a set of brackets. The SN1100 model is sold with a set of brackets et rails. SN2100, SN3100 and SN6100 appliances are sold with a set of slide rails.

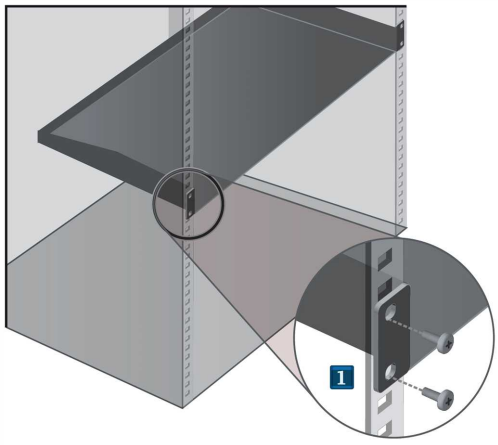
REMINDER
Ensure that the cabinet complies with temperature and humidity conditions indicated in the section Conditions of use.

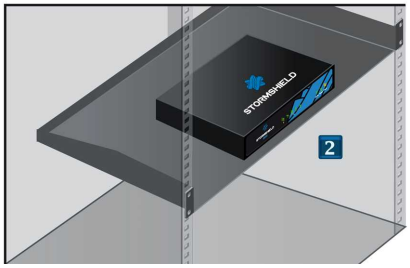
NOTE
SN160 and SN160W models can also be installed vertically (screws and fasteners not provided).

Installing SN160, SN160W, SN210, SN210, SN310, SN-S-Series-220 and SN-S-Series-320 models on a 19" cabinet shelf

In this non-standard installation, allow a height of more than 1U due to the thickness of the shelf, the presence of rubber feet below the appliance as well as antennae on Wi-Fi products. The procedure is as follows:

1. Using screws and caged nuts (not provided with the appliance), fasten the shelf to the vertical rails located at the front of the cabinet.
2. Once the shelf has been installed, you can place one or two appliances on it (no additional fastening is needed).





WARNING
If you are installing two Firewalls on the same rack mount shelf, you will need to leave enough space between the Firewalls to avoid obstructing the flow of air from the sides.

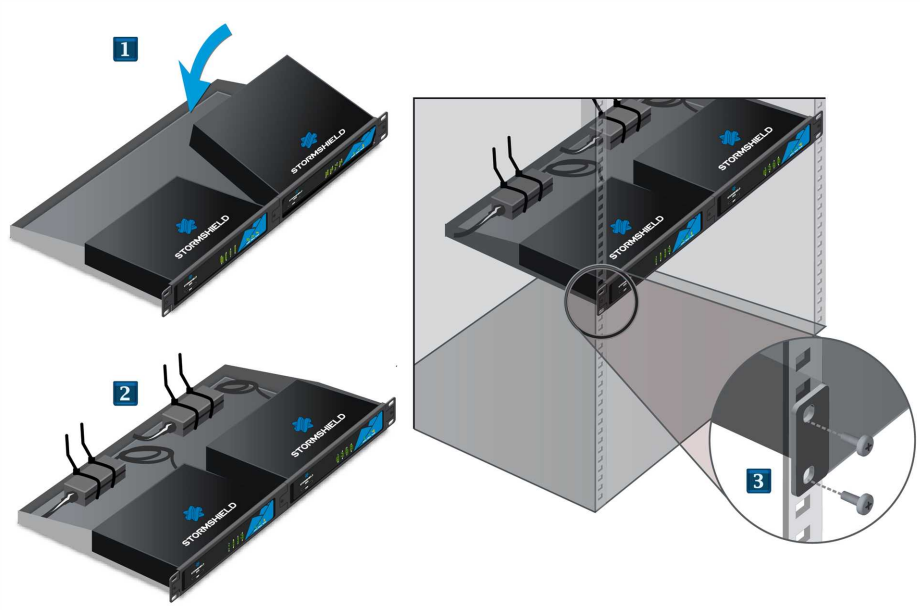
Installing SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320 models on a 19" cabinet 1U shelf

The minimum vertical space needed for installing the shelf is 1U. In this configuration, the shelf makes it possible to **install one or two products**. There are indentations to ensure that products and power adapters are held securely in place.

WARNING
Before any installation, ensure that you have removed the four non-slip rubber feet under each product.

NOTE
Fasteners for two power adapters are provided with the shelf.

1. Place your firewall in front of its slot at the front of the shelf, then set it upright until it is firmly in place.
2. Install and fasten the power adapter on the shelf. Connect it to the firewall.
3. Using screws and caged nuts (not provided with the appliance), fasten the shelf to the vertical rails located at the front of the cabinet.



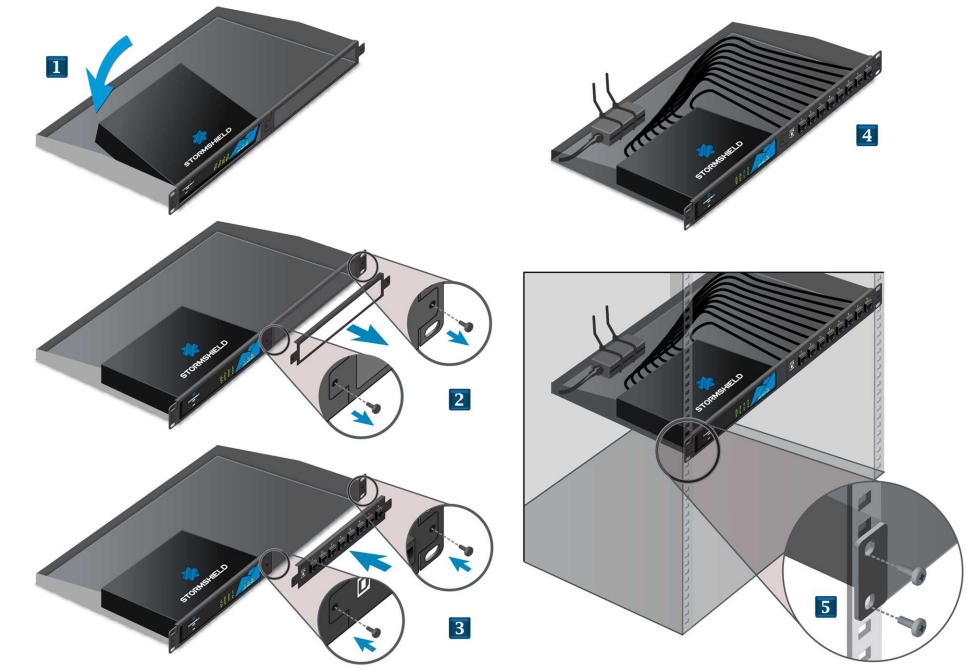
Kit for USB and network interfaces on the front panel option

In this configuration, the shelf makes it possible to **install one product**. There are indentations to ensure that product and power adapter are held securely in place.

NOTE
This kit must be ordered separately.

NOTE
This kit allows you to connect the console, via a USB port, and network interfaces on the front panel of the shelf (cables provided).

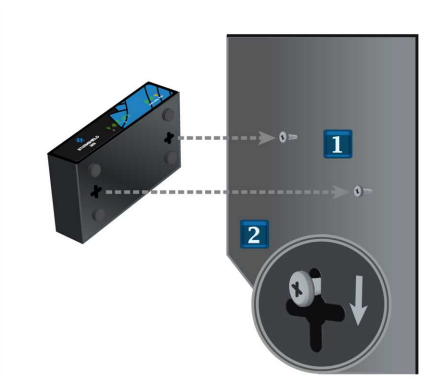
1. Place your firewall in front of its slot at the front left of the shelf, then set it upright until it is firmly in place.
2. Unscrew the right side of the front panel (two screws).
3. Position the kit, then fasten it to the front panel with both screws.
4. Install and fasten the power adapter on the shelf. Connect the power adapter to the firewall, as well as the USB and network ports from the kit.
5. Using screws and caged nuts (not provided with the appliance), fasten the shelf to the vertical rails located at the front of the cabinet.



Fastening SN160 and SN160W models to a wall

SN160 and SN160W models can also be installed vertically using screws and fasteners (not provided). The screw heads must be narrower than 8mm in diameter and the diameter of the shank must not exceed 4mm.

The procedure is as follows:

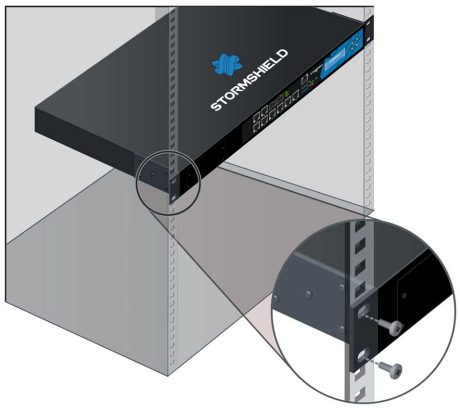


1. Place against the wall the 2 screws aligned horizontally, leaving a space of 12cm (center to center) between them and letting them protrude slightly to take into account the thickness of the non-slip rubber feet.
2. Once the screws have been drilled into the wall, you can insert the screw heads into the indentations meant for this purpose, then gently bring the appliance downwards in order to insert the screws.

Installing SN510, SN-M-Series-520, SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models in a 19" cabinet

The minimum vertical space needed for installing an SN Firewall is 1U.

Once the brackets have been installed, you can fasten the Firewall to the vertical rails located at the front of your cabinet using screws and the caged nuts (not provided with the appliance).



Installing SN1100, SN2100, SN3100 and SN6100 models in a 19" cabinet

The minimum vertical space needed to install an SN1100, SN2100 or SN3100 Firewall is 1U, and for an SN6100, 2U is required. The processes of mounting lateral rails and installing appliances in racks are described in **SN1100_rack mounting, SN2100-SN3100_rack mounting** and **SN6100_rack mounting**. These documents are provided with SN2100, SN3100 and SN6100 products, and available on the Stormshield Technical Documentation website, under the section **PDF download**, under *Installation guides*.

The rails that come with the product enable installation in a 19" rack – the depth between the vertical rails located in the front and back are:

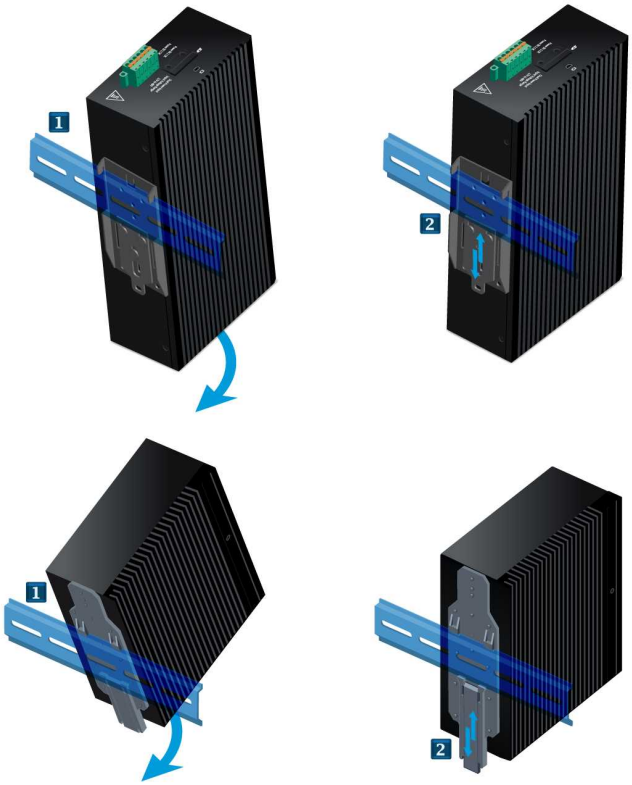
- SN1100: between 655 and 745mm
- SN2100/SN3100: between 735 and 850mm
- SN6100: between 620 and 808mm

Installing SNi20 and SNi40 models on DIN rails

To install the appliance in a cabinet, SNi20 and SNi40 models have a fastener on a 35mm-wide DIN rail (EN50022 standard).

REMINDER
Ensure that the cabinet complies with temperature and humidity conditions indicated in the section Conditions of use. Equipment has to be installed by a qualified electrician.

NOTE
SNi20 and SNi40 models must be installed vertically.



The procedure is as follows:

1. Hold the appliance facing the DIN rail, then insert the upper part of the rail into the notch in the fastener. Set the appliance upright.
2. Push the appliance against the DIN rail until you hear a click. Ensure that the position of the appliance has been locked.

PRESENTATION OF SN MODELS

Stormshield Network SN range models rely on the most advanced technologies to provide high performance and optimum protection.

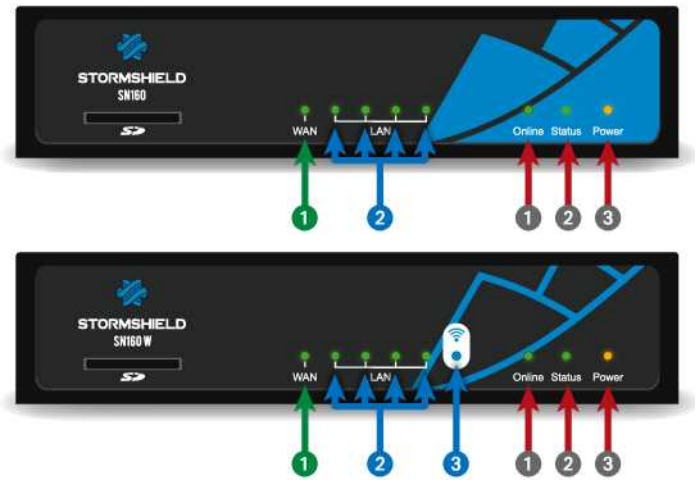
NOTE
For more information on Ethernet interfaces, refer to the section Connecting to the network under INSTALLATION PRECAUTIONS.

SN160 and SN160W models

SN160 and SN160W firewalls are fanless. The products come with an external power adapter.

Front panel: LEDs

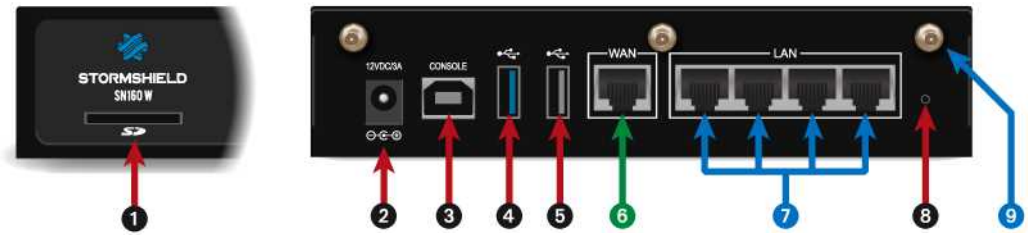
This model has its LEDs on the front panel as shown below:



1. *Online* LED (green)
2. *Status* LED (green)
3. *Power* LED (yellow)

1. **OUT** interface
2. **IN** interface
3. **Wi-Fi** interface

Connectors



The connectors on SN160 and SN160W models are located on the front and rear panels.

1. This is the slot for the **SD card*.**
2. Plugging in the mains adapter automatically starts this product.

❸ **The USB port** makes it possible access the product in console mode**; the firewall can be connected directly from a computer. The default baud rate on these models is 115200 baud (8N1).

❹ **The USB 3.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

❺ **The USB 2.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

SN160 and SN160W models hold five 1Gbps ports:

❻ The first zone is the **EXTERNAL (OUT)** interface, in external mode by default. It makes up the zone that is needed for connecting to the internet.

❼ The second zone is by default identified in **INTERNAL (IN)**mode. It is made up of 4 switched ports.

❽ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

❾ **Sockets** for Wi-Fi antennae.

** The recommended type of SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in a full-size physical SD format, in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB. Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32Go.*

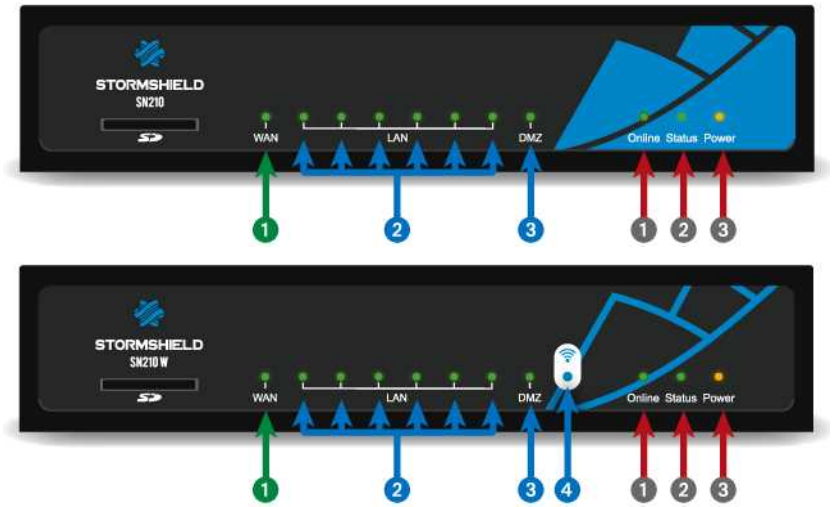
*** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

SN210 and SN210W models

SN210 and SN210W firewalls are fanless. The products come with an external power adapter.

Front panel: LEDs

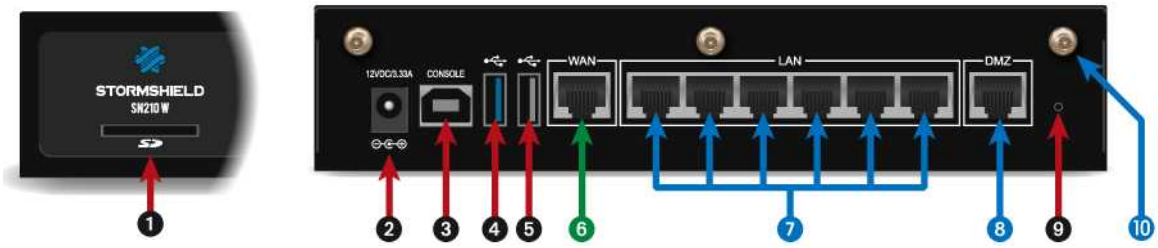
This model has its LEDs on the front panel as shown below:



1 *Online* LED (green)
2 *Status* LED (green)
3 *Power* LED (yellow)

1 **OUT** interface
2 **IN** interface
3 **DMZ** interface
4 **Wi-Fi** interface

Connectors



The connectors on SN210 and SN210W models are located on the front and rear panels.

1. This is the slot for the **SD card*.**
2. Plugging in the mains adapter automatically starts this product.
3. **The USB port** makes it possible access the product in console mode**; the firewall can be connected directly from a computer. The default baud rate on these models is 115200 baud (8N1).
4. **The USB 3.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.
5. **The USB 2.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

SN210 and SN210W models hold eight 1GbE ports:

6. The first zone is the **EXTERNAL (OUT)** interface, in external mode by default. It makes up the zone that is needed for connecting to the internet.
7. The second zone is by default identified in **INTERNAL (IN)**mode. It is made up of 6 switched ports.
8. The third zone is by default identified in **INTERNAL (IN)**mode.
9. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
10. **Sockets** for Wi-Fi antennae.

** The recommended type of SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in a full-size physical SD format, in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB. Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32Go.*

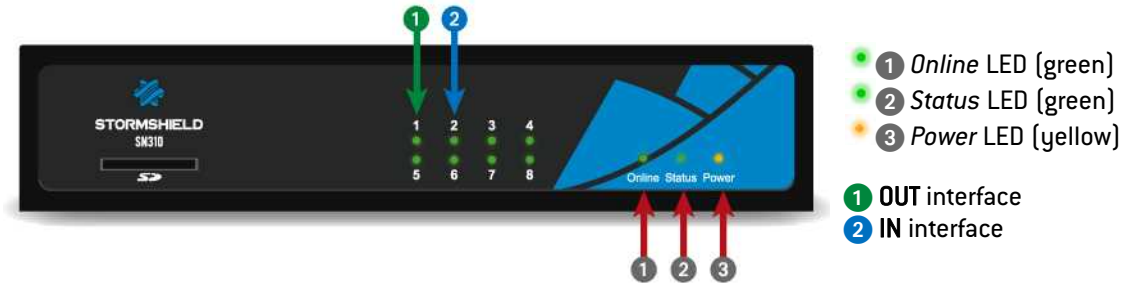
*** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

SN310 model

The SN310 firewall is fanless. The product comes with an external power adapter.

Front panel: LEDs

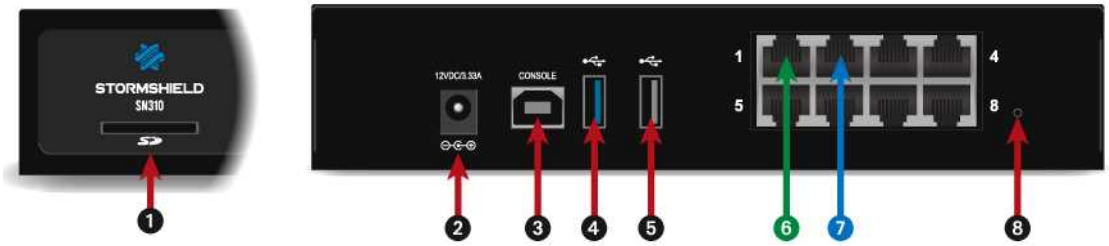
This model has its LEDs on the front panel as shown below:



1. *Online* LED (green)
2. *Status* LED (green)
3. *Power* LED (yellow)

1. **OUT** interface
2. **IN** interface

Connectors



The connectors on the SN310 model are located on the front and rear panels.

1. This is the slot for the **SD card*.**
2. Plugging in the mains adapter automatically starts this product.
3. **The USB port** makes it possible access the product in console mode**; the user can connect to the firewall directly from a computer. The default baud rate on these models is 115200 baud (8N1).
4. **The USB 3.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.
5. **The USB 2.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

The SN310 model offers 8 1Gbps ports:

6. The first zone is the **EXTERNAL (OUT)** interface, in external mode by default. It makes up the zone that is needed for connecting to the internet.
7. The second zone is the **INTERNAL (IN)** interface.
8. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

** The recommended type of SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in a full-size physical SD format, in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB. Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32Go.*

*** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

SN-S-Series-220 and SN-S-Series-320 models

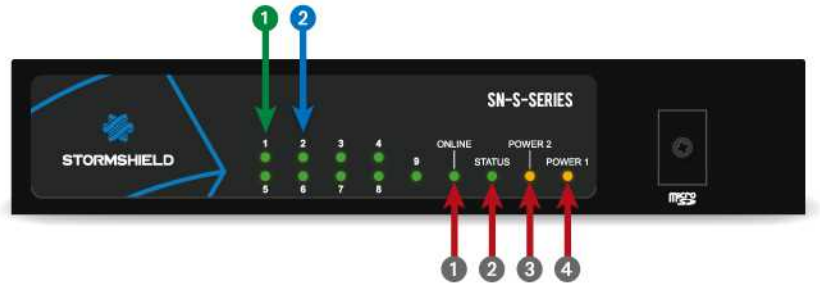
Depending on the license, the SN-S-Series platform (physical appliance) may either be an SN-S-Series-220 or SN-S-Series-320 model.

Temporary licenses correspond to the SN-S-Series-220 model by default. A license must be installed in order to upgrade to an SN-S-Series-320 model. For further information on upgrading licenses, refer to the module UPDATING THE LICENSE.

The SN-S-Series firewall is fanless. The product comes with an external power adapter.

Front panel: LEDs

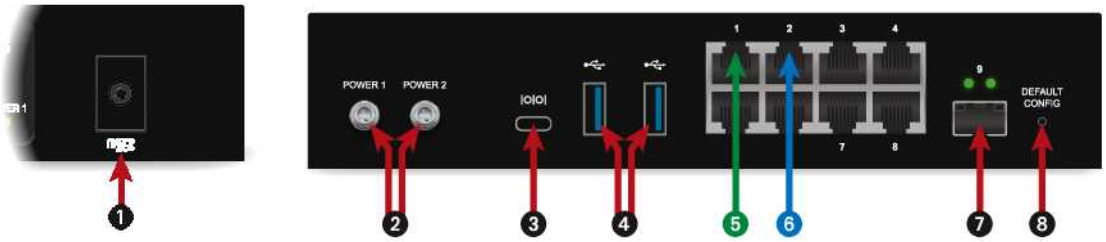
This model has its LEDs on the front panel as shown below:



1. *Online* LED (green)
2. *Status* LED (green)
3. *Power* 2 LED (yellow)
3. *Power* 1 LED (yellow)

1. **OUT** interface
2. **IN** interface

Connectors



The connectors on the SN-S-Series model are located on the front and rear panels.

1. This is the slot for the **SD card*.**
2. **Two mains sockets** to be screwed in for redundant power supplies. Plugging in a mains adapter automatically starts this product.
3. **The USB port** makes it possible access the product in console mode**; the firewall can be connected directly from a computer. The default baud rate on this model is 115200 baud (8N1).
4. **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.

The SN-S-Series model holds 8 Gigabit Ethernet interfaces.

5. The first zone is the **EXTERNAL (OUT)** interface, in external mode by default. It makes up the zone that is needed for connecting to the internet.
6. The second zone is the **INTERNAL (IN)** interface.

❼ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115200 baud (8N1).

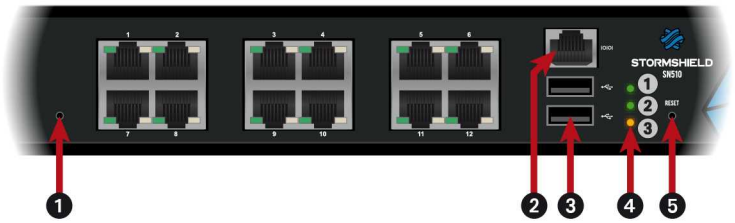
❽ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

** The recommended type of micro SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB.*
*Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32Go.*

*** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

SN510 and SN710 models

Front panel: connectors and LEDs



① *Online* LED (green)
② *Status* LED (green)
③ *Power* LED (yellow)

❶ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

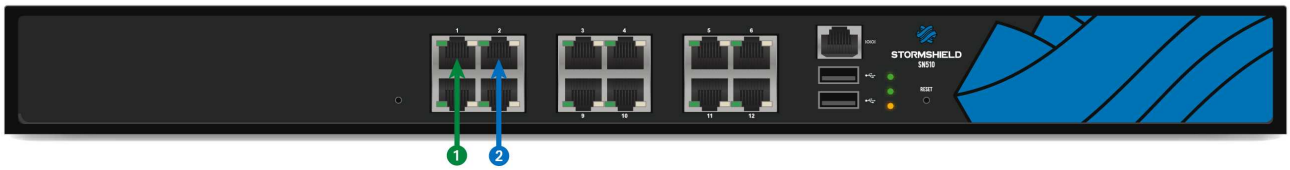
❷ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on these models is 115200 baud (8N1).

❸ **Two USB 2.0 ports** that can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

❹ The *Power*, *Status* and *Online* (from bottom to top) LEDs.

❺ **The *Reset* button:** resets the firewall's electrical power supply.

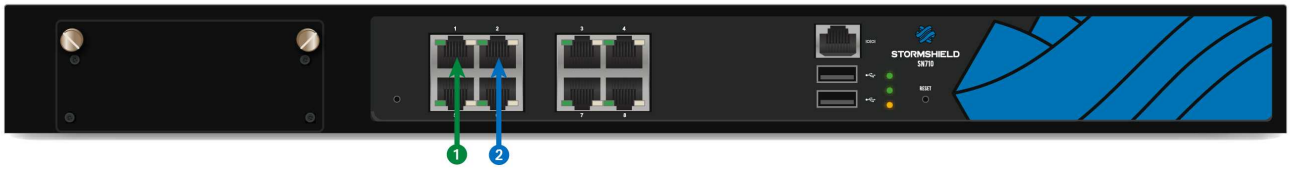
SN510 model



This model is fitted with a multi-core CPU, making it possible to increase processing power.
This product has an internal power supply.
The SN510 model offers 12 1Gbps ports:

① **OUT** interface
② **IN** interface

SN710 model



This model is fitted with a multi-core CPU, making it possible to increase processing power.

① **OUT** interface
② **IN** interface

This product has an internal power supply.
The SN710 model offers 8 1Gbps ports: It allows the addition of one extension module with RJ45 (1Gbps) or fiber (1Gbps or 10Gbps) connectors.
Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

The socket for the power cord is located on the rear panel of the product. A switch makes it possible to turn the product on or off.

SN-M-Series-520 models

Front panel: connectors and LEDs

① *Online* LED (green)
② *Status* LED (green)
③ *Power 2* LED (yellow)
④ *Power 1* LED (yellow)

❶ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115200 baud (8N1).

❷ **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.

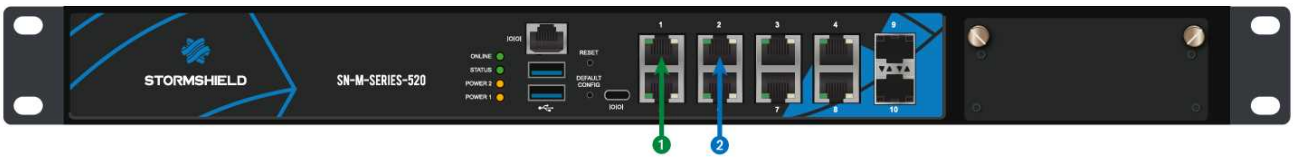
❸ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

❹ **The *Reset* button:** resets the firewall's electrical power supply.

❺ **The USB-C port** makes it possible to access the product in console mode*; the firewall can be connected directly from a computer. The default baud rate on this model is 115200 baud (8N1).

** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

Description



This model is fitted with a multi-core CPU, making it possible to increase processing power.

It has two internal power supply units to provide a redundant power supply.

① **OUT** interface
② **IN** interface

The SN-M-Series platform holds 8 2.5Gbps interfaces by default (backward compatible between 1Gbps/100Mbps) and 2 SFP+ sockets for adding 1Gbps/10Gbps transceivers. On this model, 1 extension module can be added with RJ45 (1Gbps, 2.5Gbps or 10Gbps) or fiber (1Gbps or 10Gbps) connectors.

Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

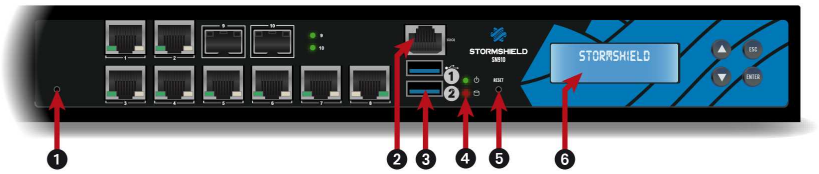
Rear panel: connectors

❶ **Two Power button** to switch the firewall on or off.

❷ **Two mains sockets** for redundant power supplies.

SN910 model

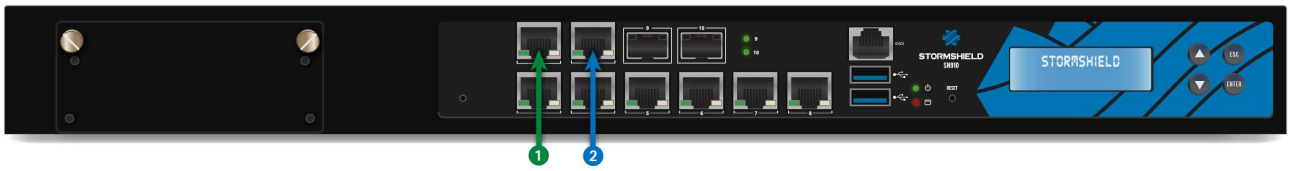
Front panel: connectors and LEDs



① *Online* LED (green)
② *SSD activity* LED (red)

1. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
2. **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on these models is 9600 baud (8N1).
3. **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
4. The *Power* and *SSD activity* LEDs (from top to bottom).
5. **The *Reset* button:** resets the firewall's electrical power supply.
6. **LCD screen**: indicates the version of the firmware installed, the active partition, the serial number of the product as well as the HA status if it has been enabled.

Description



1. **OUT** interface
2. **IN** interface

This model is fitted with a multi-core CPU, making it possible to increase processing power.

This product has an internal power supply.

The SN910 model holds 8 1Gbps Ethernet interfaces and 2 SFP sockets for adding 1Gbps Ethernet transceivers. It allows the addition of one extension module with RJ45 (1Gbps) or fiber (1Gbps or 10Gbps) connectors.

Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

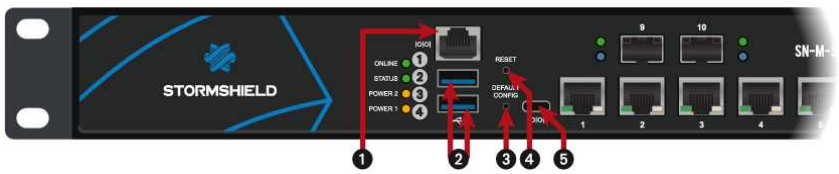
1. A mains socket.
2. The product's on/off switch.
3. **The USB 2.0 port** can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
4. **The VGA port** allows connecting a monitor.

SN-M-Series-720 and SN-M-Series-920 models

Depending on the license, the SN-M-Series platform (physical appliance) may either be an SN-M-Series-720 or SN-M-Series-920 model.

Temporary licenses correspond to the SN-M-Series-720 model by default. A license must be installed in order to upgrade to an SN-M-Series-920 model. For further information on upgrading licenses, refer to the module UPDATING THE LICENSE.

Front panel: connectors and LEDs



① *Online* LED (green)
② *Status* LED (green)
③ *Power 2* LED (yellow)
④ *Power 1* LED (yellow)

❶ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115200 baud (8N1).

❷ **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.

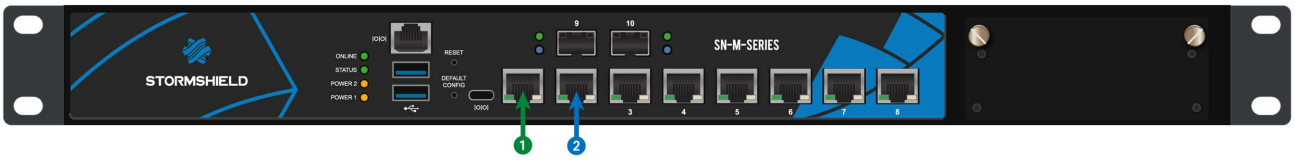
❸ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

❹ **The *Reset* button:** resets the firewall's electrical power supply.

❺ **The USB-C port** makes it possible to access the product in console mode*; the firewall can be connected directly from a computer. The default baud rate on this model is 115200 baud (8N1).

** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

Description



This model is fitted with a multi-core CPU, making it possible to increase processing power.

It has two internal power supply units to provide a redundant power supply.

1 **OUT** interface
2 **IN** interface

The SN-M-Series platform holds 8 2.5-Gigabit SFP 1 GbE ports by default (backward compatible between Gigabits/100 Megabits) and 2 SFP+ sockets for adding 1 Gbps/ 10 Gbps transceivers. On this model, 1 extension module can be added with RJ45 (Gigabit or 10 Gigabit) or fiber (Gigabit or 10 Gigabit) connectors.

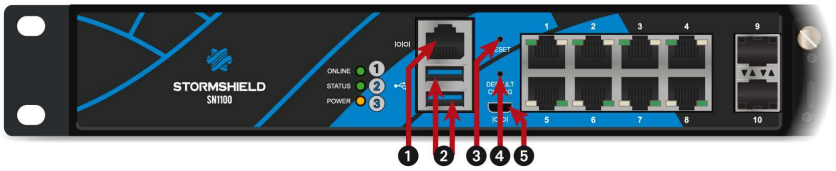
Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

1. **Two Power button** to switch the firewall on or off.
2. **Two mains sockets** for redundant power supplies.

SN1100 model

Front panel: connectors and LEDs

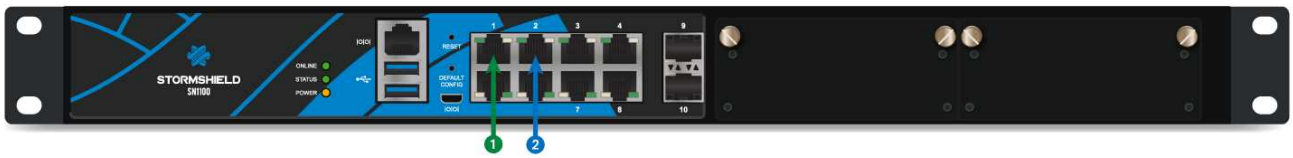


① *Online* LED (green)
② *Status* LED (green)
③ *Power* LED (yellow)

1. **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115200 baud (8N1).
2. **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
3. **The *Reset* button:** resets the firewall's electrical power supply.
4. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
5. **The micro USB port** makes it possible access the product in console mode*; the user can connect to the firewall directly from a computer. The default baud rate on this model is 115200 baud (8N1).

** This connection in console mode requires the installation of a driver. Depending on your operating system, you can download a driver from: http://www.ftdichip.com/Drivers/VCP.htm*

Description



This model is fitted with a multi-core CPU, making it possible to increase processing power.

This product has a removable power supply.

A second power supply module can be ordered separately for redundant power supply.

1 **OUT** interface
2 **IN** interface

The SN1100 model holds 8 1Gbps ports by default and 2 SFP+ sockets for adding 1Gbps/10Gbps transceivers. On this model, 2 extension modules can be added with RJ45 (1Gbps or 10Gbps) or fiber (1Gbps or 10Gbps) connectors.

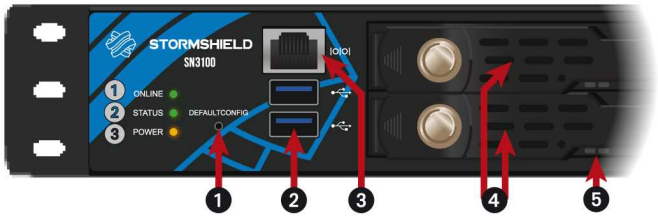
Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

1. **The HDMI port** allows connecting a monitor.
2. **The USB 3.0 port** can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
3. The **Power button** switches the firewall on or off.
4. A **mains socket.** Modules are hot-swappable on products with a redundant power supply.
5. **The Alarm off button**. The alarm rings when a power supply module is missing or when there is a power failure on either module. Press this button to deactivate the alarm.

SN2100 and SN3100 models

Front panel: connectors and LEDs



① *Online* LED (green)
② *Status* LED (green)
③ *Power* LED (yellow)

❶ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

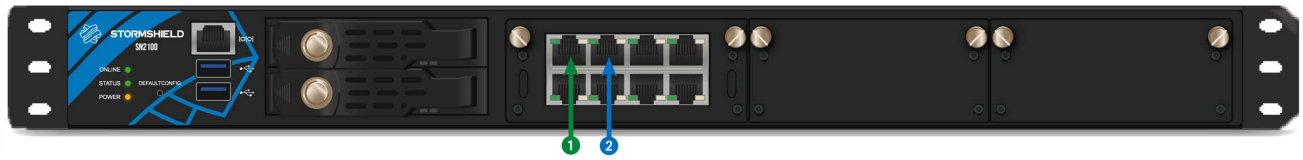
❷ **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.

❸ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on these models is 115 200 baud (8N1).

❹ **SSD racks for log storage** (1 SSD by default on SN2100 models, RAID available as an option, 2 in RAID 1 on SN3100 models). Disks are hot-swappable on products in a RAID setup.

❺ **The LEDs on SSD racks** confirm whether the SSD has been accessed (blue LED on the right) and installed (green LED on the left).

SN2100 model



This model is fitted with a multi-core CPU, making it possible to increase processing power.

This product has an internal removable power supply and is equipped with an SSD.

1 **OUT** interface
2 **IN** interface

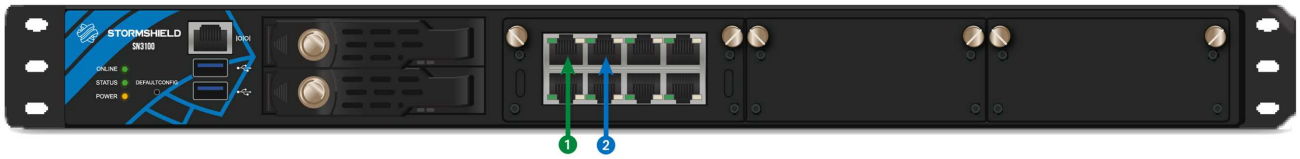
A second power supply module can be ordered separately for redundant power supply. You can also order a second SSD for a RAID installation.

The SN2100 model offers 2 1Gbps interfaces and allows the addition of 3 extension modules with RJ45 (1Gbps or 10Gbps) or fiber (1Gbps, 10Gbps or 40Gbps) connectors.

NOTE
For this model, network extension modules are sold separately and must be ordered.

Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

SN3100 model



This model is fitted with a multi-core CPU, making it possible to increase processing power. This product has redundant internal power supplies. Two removable SSDs are installed in a RAID configuration.

1. **OUT** interface
2. **IN** interface

The SN3100 model offers 2 1Gbps interfaces and allows the addition of 3 extension modules with RJ45 (1Gbps or 10Gbps) or fiber (1Gbps, 10Gbps or 40Gbps) connectors.

> **NOTE**
> For this model, network extension modules are sold separately and must be ordered.

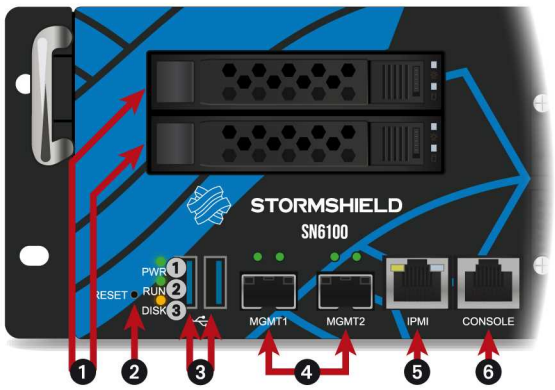
Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

1. The **Power button** switches the firewall on or off.
2. **Three independent hot-swappable fans** in the event of a breakdown.
3. **The Reset button:** resets the firewall's electrical power supply.
4. Two ports dedicated to the management of the appliance (**MGMT1** and **MGMT2**).
5. **The HDMI port** allows connecting a monitor.
6. **A mains socket** (SN2100) or **two mains sockets** (SN3100) for redundant power supplies. Modules are hot-swappable on products with a redundant power supply.
7. **The Alarm off button**. The alarm rings when a power supply module is missing or when there is a power failure on either module. Press this button to deactivate the alarm.

SN6100 model

Front panel: connectors and LEDs



① *Power* LED (green)
② *Run* LED (green)
③ *SSD activity* LED (yellow)

❶ **SSD racks** for log storage (2 SSD in RAID 1 and hot-swappable). The LEDs on racks confirm that installation (green LED at the top) and access (yellow LED at the bottom) have been successful.

❷ **The *Reset* button:** resets the firewall's electrical power supply.

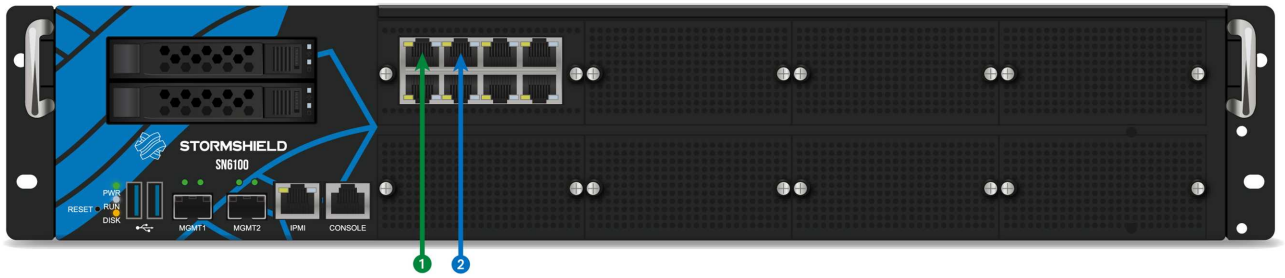
❸ **Two USB 3.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.

❹ **MGMT1 and MGMT2:** Two SFP+ sockets, allowing the insertion of SFP+ transceivers, provided as an option. Both of these ports are dedicated to the management of the appliance or the configuration of high availability.

❺ **The IPMI network port** dedicated to the administration of the appliance via IPMI. Refer to the appendix CONFIGURATION AND ADMINISTRATION VIA IPMI (SN6100).

❻ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115 200 baud (8N1).

Description



This model is fitted with two multi-core CPUs, making it possible to increase processing power. This product has redundant internal power supplies. Two removable SSDs are installed in a RAID configuration.

1 **OUT** interface
2 **IN** interface

The SN6100 model holds 8 1Gbps ports by default and 2 SFP+ sockets for adding 1Gbps/10Gbps transceivers. On this model, 8 extension modules can be added with RJ45 (1Gbps or 10Gbps) or fiber (1Gbps, 10Gbps or 40Gbps) connectors.

Specifications of Stormshield Network-approved extension modules and transceivers are set out in sections Extension modules (SN710 and upwards) and Fiber Ethernet connectors.

Rear panel: connectors

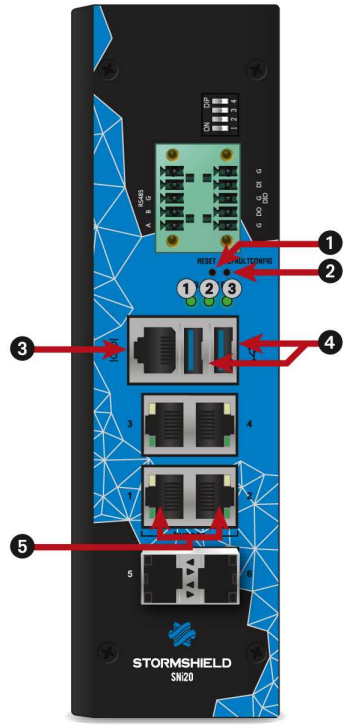
1. **The USB 2.0 port** can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
2. **Four independent hot-swappable fans** in the event of a breakdown.
3. **The VGA port** allows connecting a monitor.
4. The **Power button** switches the firewall on or off.
5. **The Alarm off button**. The alarm rings when a power supply module is missing or when there is a power failure on either module. Press this button to deactivate the alarm.
6. **Two mains sockets** for redundant power supplies. These modules are hot-swappable.

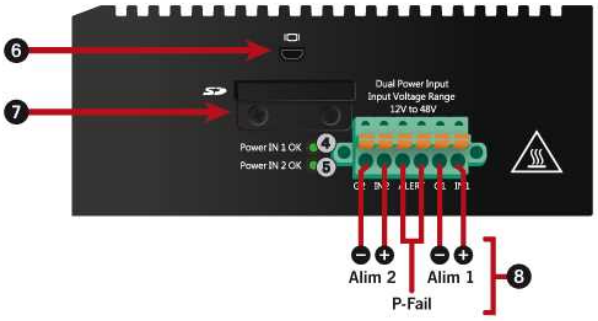
SNi20 model

In order to ensure service continuity in an industrial setting, the SNi20 firewall is equipped with a hardware bypass function, which when enabled, allows network traffic to pass through in the event of a power outage or appliance breakdown.

This feature, available from version 4.1 onwards, is disabled by default. If you want to allow bypass to be enabled, high availability must not be configured on the appliance.

Connectors and LEDs





- ① *Power* LED (green)
- ②*Bypass* LED (Off/green/red)
- ③ *Run* LED (green)
- ④*Power supply 1* LED (green)
- ⑤*Power supply 2* LED (green)

❶ **The *Reset* button** (underside): resets the firewall's electrical supply.

❷ This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).

❸ **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115 200 baud (8N1).

❹ **USB 3.0 ports** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.

❺ Two network ports dedicated to **Ethernet Bypass** (may vary by license).

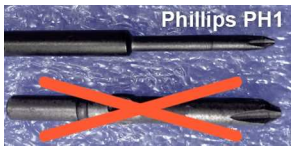
❻ **The HDMI port** makes it possible to connect a monitor.

❼ This is the slot for the **SD card*.**

❽ This 6-pole screw terminal connector enables connection to a 48VDC redundant power supply and a **P-Fail relay.**

** The recommended type of SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in a full-size physical SD format, in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB. Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32 GB. .*

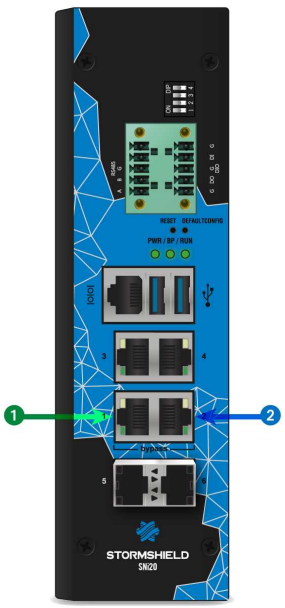
IMPORTANT
On SNi20 appliances, use a Phillips PH1 screwdriver to remove the screws from the SD card reader cache. Insert the SD card, then put back the SD card reader cache to guarantee that the SNi20 is airtight.



Bypass LED

Color	Status	Status
	Off	*Bypass* feature disabled (default status, **Security mode**)
Green	On	*Bypass* feature configure in **Safety mode**. The *Bypass* mechanism will be enabled whenever the appliance breaks down or there is a power outage.
Red	On	*Bypass* mechanism enabled.

Description



1. **OUT** interface
2. **IN** interface

The SNi20 multi-function firewall is fanless.

This model is fitted with a multi-core CPU, making it possible to increase processing power.

This appliance is equipped with a 48VDC redundant power supply; the 6-pole screw terminal connector provided allows connecting to two independent sources of power.

The SNi20 model holds 4 1Gbps Ethernet interfaces and 2 SFP* sockets for adding 1Gbps Ethernet transceivers.

Specifications of Stormshield Network-approved transceivers are set out in the sections Optional Ethernet Transceivers and Fiber Ethernet connectors.

** may vary by license.*

Redundant power supply and P-Fail (Power Failure) relay

REMINDER
Before plugging any equipment into a DC power supply module, read the SAFETY RULES carefully and follow them.

Both electrical power supplies can be connected to the SNi20 to provide a redundant power source. Connect the power supplies according to the diagram shown in Connectors and LEDs

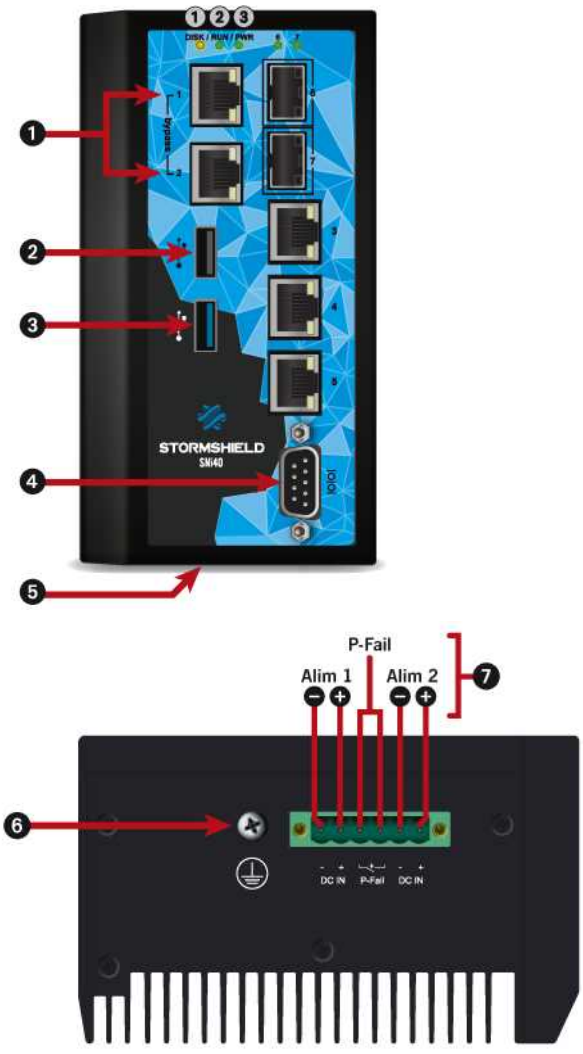
A P-Fail relay makes it possible to detect an abnormal status on a power supply. You can connect this relay to a sound or light alarm, such as a buzzer or a LED, equipped with an independent power supply. To do so, connect the external power supply of the alarm to the third and fourth pins. If both power supplies run at the same time, the alarm will be short-circuited. If either power supply is defective, the alarm will go off. The highest intensity that this relay supports is 1A.

SNi40 model

In order to ensure service continuity in an industrial setting, the SNi40 firewall is equipped with a hardware bypass function, which when enabled, allows network traffic to pass through in the event of a power outage or appliance breakdown.

This feature, available from version 3.0 onwards, is disabled by default. If you want to allow bypass to be enabled, high availability must not be configured on the appliance.

Connectors and LEDs



① *SSD activity* LED (yellow)
② *Run* LED (green)
③ *Power* LED (green)

1. Two network ports dedicated to **Ethernet Bypass**
2. **The USB 2.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.
3. **The USB 3.0 port** can be used for secure configurations or upgrades. You can also plug a USB key or an approved USB modem into it.
4. **The serial port** makes it possible access the product in console mode; it is possible to connect the firewall directly from a computer. The default baud rate on this model is 115 200 baud (8N1).
5. **The *Reset* button** (underside): resets the firewall's electrical supply.
6. Connection of the **protective earth circuit.**
7. This 6-pole screw terminal connector enables connection to a 24VDC redundant power supply and a **P-Fail relay.**

Description

1 **OUT** interface
2 **IN** interface

The SNi40 multi-function firewall is fanless.

This model is fitted with a multi-core CPU, making it possible to increase processing power.

This appliance is equipped with a 24VDC redundant power supply; the 6-pole screw terminal connector provided allows connecting to 2 independent sources of power.

The SNi40 model holds 5 1Gbps Ethernet interfaces and 2 SFP sockets for adding 1Gbps Ethernet transceivers.

Specifications of Stormshield Network-approved transceivers are set out in the sections Optional Ethernet Transceivers and Fiber Ethernet connectors.

Redundant power supply and P-Fail (Power Failure) relay

REMINDER
Before plugging any equipment into a DC power supply module, read the SAFETY RULES carefully and follow them.

Both electrical power supplies can be connected to the SNi40 to provide a redundant power source. Connect the power supplies according to the diagram shown in Connectors and LEDs

A P-Fail relay makes it possible to detect an abnormal status on a power supply. You can connect this relay to a sound or light alarm, such as a buzzer or a LED, equipped with an independent power supply. To do so, connect the external power supply of the alarm to the third and fourth pins. If both power supplies run at the same time, the alarm will be short-circuited. If either power supply is defective, the alarm will go off. The recommended intensity for this relay is 30VDC, 2A or 60W.

SNxr1200 model

Connectors and LEDs

LEDs

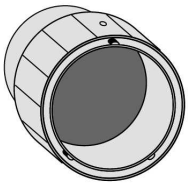
1 *Power* LED (green)

1 Connection of the **protective earth circuit.**

Plugging in connectors

To access your firewall from a client workstation, you will need to connect on the **IN** or "Internal" port, or on another port (except the **OUT** port) located on connectors **J3** or **J4**.
For further information, refer to the section on **NETWORK CONNECTORS**, under IN/OUT definition.

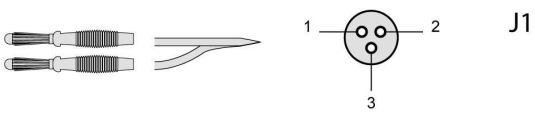
For testing purposes, an IT connection kit (breakout cables) is available as an option. This kit is not intended for use in a production environment.
To connect the cables, engage the coded pins according to the diagram opposite (coded pins specific to each connector), then screw firmly to ensure that the product is watertight.



J1 connectors

J1 connectors, which cater to the product's power supply, are described below.
The power adapter (provided as an option) is plugged into the breakout cable ("IT connection kit" provided as an option) corresponding to this connector.

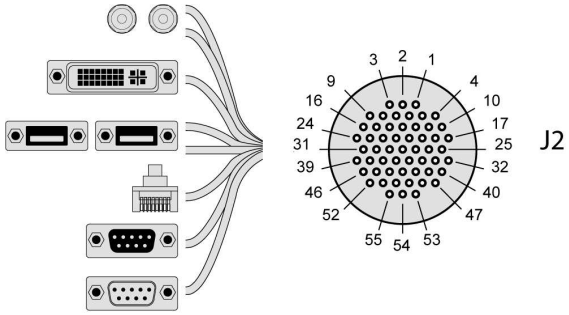
Pin	Signal
J1.1	VIN 28+
J1.2	VIN 28-
J1.3	n/a



J2 connectors

J2 connectors correspond to the following connectors:

- 2 push buttons: ON/OFF switch and Reset button (resets the firewall's electrical supply)
- 1 DVI output port
- 2 USB 2.0 ports
- 1 RJ45 1Gbps Ethernet port
- 1 RS232 serial port
- 1 RS422 serial port



"IT connection kit" connectors

2 push buttons: ON/OFF switch and Reset button (electrically resets the firewall)

Details	Pin	Signal
ON	J2.10	POWER BUTTON+
OFF	J2.11	POWER BUTTON-
RESET	J2.17	RESET BUTTON+
	J2.18	RESET BUTTON-

1 DVI output port

Pin	Signal
J2.2	DVI DATA2+
J2.3	DVI DATA2-
J2.4	DVI DDCCLK
J2.5	DVI DDCDATA
J2.6	DVI HPD
J2.2	DVI DATA2+

2 USB 2.0 ports

Details	Pin	Signal
USB no. 1	J2.47	USB0 5VDC
	J2.48	USB0-
	J2.49	USB0+
	J2.50	USB0 GND
USB no. 2	J2.51	USB1 GND
	J2.53	USB1 5VDC
	J2.54	USB1-
	J2.55	USB1+

1 Ethernet port RJ45 1Gbps

Details	Pin	Signal
OUT 1	J2.32	ETH1 MDI0+
	J2.33	ETH1 MDI0-
	J2.34	ETH1 MDI1+
	J2.35	ETH1 MDI1-
	J2.36	ETH1 MDI2+
	J2.37	ETH1 MDI2-
	J2.38	ETH1 MDI3+
	J2.39	ETH1 MDI3-

1 RS232 serial port

Pin	Signal
J2.45	RS232 SER0 TX
J2.46	RS232 SER0 RX

1 RS422 serial port

Pin	Signal
J2.40	RS422 SER0 RXN
J2.41	RS422 SER0 RXP
J2.42	RS422 SER0 TXN
J2.43	RS422 SER0 TXP

Overview of J2 connectors

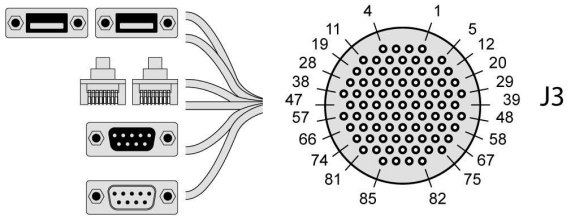
Pin	Signal	Pin	Signal	Pin	Signal
J2.1	GND	J2.21	n/a	J2.41	RS422 SER0 RXP
J2.2	DVI DATA2+	J2.22	GND	J2.42	RS422 SER0 TXN
J2.3	DVI DATA2-	J2.23	DVI CLK+	J2.43	RS422 SER0 TXP
J2.4	DVI DDCCLK	J2.24	DVI CLK-	J2.44	GND
J2.5	DVI DDCDATA	J2.25	n/a	J2.45	RS232 SER0 TX
J2.6	DVI HPD	J2.26	n/a	J2.46	RS232 SER0 RX
J2.7	GND	J2.27	n/a	J2.47	USB0 5VDC
J2.8	DVI DATA1+	J2.28	n/a	J2.48	USB0-
J2.9	DVI DATA1-	J2.29	n/a	J2.49	USB0+
J2.10	POWER BUTTON+	J2.30	n/a	J2.50	USB0 GND
J2.11	POWER BUTTON-	J2.31	n/a	J2.51	USB1 GND
J2.12	GND	J2.32	ETH1 MDI0+	J2.52	GND
J2.13	DVI 5VDC	J2.33	ETH1 MDI0-	J2.53	USB1 5VDC
J2.14	GND	J2.34	ETH1 MDI1+	J2.54	USB1-
J2.15	DVI DATA0+	J2.35	ETH1 MDI1-	J2.55	USB1+
J2.16	DVI DATA0-	J2.36	ETH1 MDI2+		
J2.17	RESET BUTTON+	J2.37	ETH1 MDI2-		
J2.18	RESET BUTTON-	J2.38	ETH1 MDI3+		
J2.19	+5VDC STANDBY (*1)	J2.39	ETH1 MDI3-		
J2.20	GND	J2.40	RS422 SER0 RXN		

*(*1) +5VDC STANDBY limited to 0.2A*
*(*2) VBUS0, VBUS1: 0.5A for each voltage (0.8A max)*

J3 connectors

J3 connectors correspond to the following connectors:

- 2 USB 2.0 ports
- 2 RJ45 1Gbps Ethernet ports
- 1 RS232 serial port
- 1 RS422 serial port



"IT connection kit" connectors

2 USB 2.0 ports

Details	Pin	Signal
USB no. 1	J3.75	USB2 GND
	J3.76	USB2-
	J3.77	USB2+
	J3.78	USB2 5VDC
USB no. 2	J3.82	USB3 5VDC
	J3.83	USB3+
	J3.84	USB3-
	J3.85	USB3 GND

2 Ethernet ports RJ45 1Gbps

Details	Pin	Signal
DMZ2	J3.1	ETH4 MDI0+
	J3.2	ETH4 MDI0-
	J3.3	ETH4 MDI1+
	J3.4	ETH4 MDI1-
	J3.11	ETH4 MDI2+
	J3.10	ETH4 MDI2-
	J3.9	ETH4 MDI3+
	J3.8	ETH4 MDI3-
DMZ3	J3.31	ETH5 MDI0+
	J3.32	ETH5 MDI0-
	J3.33	ETH5 MDI1+
	J3.34	ETH5 MDI1-
	J3.35	ETH5 MDI2+
	J3.36	ETH5 MDI2-
	J3.37	ETH5 MDI3+
	J3.38	ETH5 MDI3-

1 RS232 serial port

Pin	Signal
J3.70	RS232 1 RX
J3.71	RS232 1 TX

1 RS422 serial port

Pin	Signal
J3.73	RS422 1 RX+
J3.74	RS422 1 RX-
J3.80	RS422 1 TX-
J3.81	RS422 1 TX+

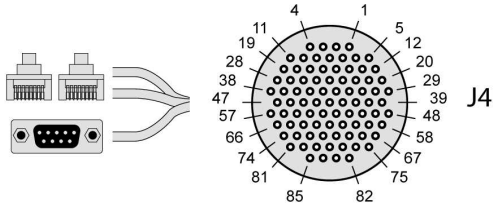
Overview of J3 connectors

Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal
J3.1	ETH4 MDI0+	J3.21	n/a	J3.41	n/a	J3.61	LINE OUTn/a L	J3.81	RS422 1 TX+
J3.2	ETH4 MDI0-	J3.22	n/a	J3.42	n/a	J3.62	LINE OUTn/a GND	J3.82	USB3 5VDC
J3.3	ETH4 MDI1+	J3.23	n/a	J3.43	n/a	J3.63	LINE OUTn/a R	J3.83	USB3+
J3.4	ETH4 MDI1-	J3.24	n/a	J3.44	n/a	J3.64	n/a	J3.84	USB3-
J3.5	n/a	J3.25	n/a	J3.45	n/a	J3.65	n/a	J3.85	USB3 GND
J3.6	n/a	J3.26	n/a	J3.46	n/a	J3.66	n/a		
J3.7	n/a	J3.27	n/a	J3.47	n/a	J3.67	n/a		
J3.8	ETH4 MDI3-	J3.28	n/a	J3.48	n/a	J3.68	LINE IN L		
J3.9	ETH4 MDI3+	J3.29	n/a	J3.49	n/a	J3.69	LINE IN R		
J3.10	ETH4 MDI2-	J3.30	n/a	J3.50	n/a	J3.70	RS232 1 RX		
J3.11	ETH4 MDI2+	J3.31	ETH5 MDI0+	J3.51	n/a	J3.71	RS232 1 TX		
J3.12	n/a	J3.32	ETH5 MDI0-	J3.52	n/a	J3.72	GND		
J3.13	n/a	J3.33	ETH5 MDI1+	J3.53	n/a	J3.73	RS422 1 RX+		
J3.14	n/a	J3.34	ETH5 MDI1-	J3.54	n/a	J3.74	RS422 1 RX-		
J3.15	n/a	J3.35	ETH5 MDI2+	J3.55	n/a	J3.75	USB2 GND		
J3.16	n/a	J3.36	ETH5 MDI2-	J3.56	n/a	J3.76	USB2-		
J3.17	n/a	J3.37	ETH5 MDI3+	J3.57	n/a	J3.77	USB2+		
J3.18	n/a	J3.38	ETH5 MDI3-	J3.58	n/a	J3.78	USB2 5VDC		
J3.19	n/a	J3.39	n/a	J3.59	GND	J3.79	GND		
J3.20	n/a	J3.40	n/a	J3.60	LINE IN Cn/aOM	J3.80	RS422 1 TX-		

J4 connectors

J4 connectors correspond to the following connectors:

- 2 RJ45 1Gbps Ethernet ports
- 1 GPIO COM port



"IT connection kit" connectors

2 Ethernet ports RJ45 1Gbps

Details	Pin	Signal
IN 2	J4.1	ETH2 MDI0+
	J4.2	ETH2 MDI0-
	J4.3	ETH2 MDI1+
	J4.4	ETH2 MDI1-
	J4.11	ETH2 MDI2+
	J4.10	ETH2 MDI2-
	J4.9	ETH2 MDI3+
	J4.8	ETH2 MDI3-
DMZ1	J4.55	ETH3 MDI0+
	J4.56	ETH3 MDI0-
	J4.57	ETH3 MDI1+
	J4.66	ETH3 MDI1-
	J4.65	ETH3 MDI2+
	J4.64	ETH3 MDI2-
	J4.63	ETH3 MDI3+
	J4.62	ETH3 MDI3-

1 GPIO COM port

Pin	Signal
J4.20	GPO3
J4.29	GPO2
J4.48	GPI2
J4.58	GPI3

Overview of J4 connectors

Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal
4.1	ETH2_MDI0+	J4.21	n/a	J4.41	n/a	J4.61	n/a	J4.81	n/a
J4.2	ETH2_MDI0-	J4.22	n/a	J4.42	n/a	J4.62	ETH3_MDI3-	J4.82	n/a
J4.3	ETH2_MDI1+	J4.23	n/a	J4.43	n/a	J4.63	ETH3_MDI3+	J4.83	n/a
J4.4	ETH2_MDI1-	J4.24	n/a	J4.44	n/a	J4.64	ETH3_MDI2-	J4.84	n/a
J4.5	n/a	J4.25	n/a	J4.45	n/a	J4.65	ETH3_MDI2+	J4.85	n/a
J4.6	n/a	J4.26	n/a	J4.46	n/a	J4.66	ETH3_MDI1-		
J4.7	n/a	J4.27	n/a	J4.47	n/a	J4.67	n/a		
J4.8	ETH2_MDI3-	J4.28	n/a	J4.48	GPI2	J4.68	n/a		
J4.9	ETH2_MDI3+	J4.29	GPO2	J4.49	n/a	J4.69	n/a		
J4.10	ETH2_MDI2-	J4.30	n/a	J4.50	n/a	J4.70	n/a		
J4.11	ETH2_MDI2+	J4.31	n/a	J4.51	n/a	J4.71	n/a		
J4.12	n/a	J4.32	n/a	J4.52	n/a	J4.72	n/a		
J4.13	n/a	J4.33	n/a	J4.53	n/a	J4.73	n/a		
J4.14	n/a	J4.34	n/a	J4.54	n/a	J4.74	n/a		
J4.15	n/a	J4.35	n/a	J4.55	ETH3_MDI0+	J4.75	n/a		
J4.16	n/a	J4.36	n/a	J4.56	ETH3_MDI0-	J4.76	n/a		
J4.17	n/a	J4.37	n/a	J4.57	ETH3_MDI1+	J4.77	n/a		
J4.18	n/a	J4.38	n/a	J4.58	GPI3	J4.78	n/a		
J4.19	n/a	J4.39	GND	J4.59	n/a	J4.79	n/a		
J4.20	GPO3	J4.40	n/a	J4.60	n/a	J4.80	n/a		

Overview of RJ45 Ethernet connectors

To summarize, RJ45 Ethernet ports are arranged as follows:

Port	Signal	Pin	Port	Signal	Pin
OUT 1	ETH1_MDI0+	J2.32	IN 2	ETH2_MDI0+	J4.1
	ETH1_MDI0-	J2.33		ETH2_MDI0-	J4.2
	ETH1_MDI1+	J2.34		ETH2_MDI1+	J4.3
	ETH1_MDI1-	J2.35		ETH2_MDI1-	J4.4
	ETH1_MDI2+	J2.36		ETH2_MDI2+	J4.11
	ETH1_MDI2-	J2.37		ETH2_MDI2-	J4.10
	ETH1_MDI3+	J2.38		ETH2_MDI3+	J4.9
	ETH1_MDI3-	J2.39		ETH2_MDI3-	J4.8

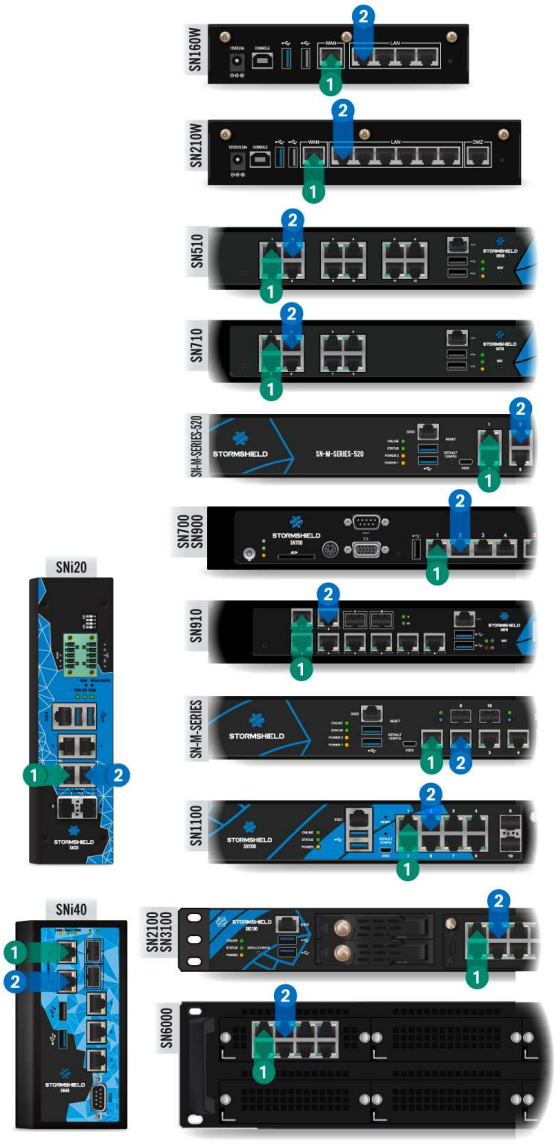
Port	Signal	Pin	Port	Signal	Pin	Port		Pin
DMZ1	ETH3_MDI0+	J4.55	DMZ2	ETH4_MDI0+	J3.1	DMZ3	ETH5_MDI0+	J3.31
	ETH3_MDI0-	J4.56		ETH4_MDI0-	J3.2		ETH5_MDI0-	J3.32
	ETH3_MDI1+	J4.57		ETH4_MDI1+	J3.3		ETH5_MDI1+	J3.33
	ETH3_MDI1-	J4.66		ETH4_MDI1-	J3.4		ETH5_MDI1-	J3.34
	ETH3_MDI2+	J4.65		ETH4_MDI2+	J3.11		ETH5_MDI2+	J3.35
	ETH3_MDI2-	J4.64		ETH4_MDI2-	J3.10		ETH5_MDI2-	J3.36
	ETH3_MDI3+	J4.63		ETH4_MDI3+	J3.9		ETH5_MDI3+	J3.37
	ETH3_MDI3-	J4.62		ETH4_MDI3-	J3.8		ETH5_MDI3-	J3.38

NETWORK CONNECTORS

RJ45 Ethernet connectors

These interfaces have to be connected to other network appliances with an RJ45 Ethernet cable. Details on how to connect SNxr1200 model firewalls are given in the section RJ45 Ethernet cabling on the SNxr1200 model below.

NOTE
A crossover cable is delivered with the Stormshield Network Firewall. This is a Category 5e cable, for running in 10Mbps, 100Mbps, 1Gbps or 2.5Gbps. Check the compatibility of your devices.



Connectors

The Ethernet (1Gbps, 2.5Gbps or 10Gbps) ports of the Stormshield Network SN range are configured in auto-sense mode, meaning that they adapt to the configuration of the Ethernet port on the appliance to which they are connected.
These ports are therefore compatible with straight or crossover RJ45 Ethernet cables.

On SN710, SN910, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models, Ethernet RJ45 ports can be added by inserting extension modules.

WARNING
Keep data cables some distance away from any source of electromagnetic interference such as mains cables, radio transmitters, fluorescent tubes, etc.

IN/OUT definition

The **OUT** 1 or "External" network port is reserved for the modem or Internet router.

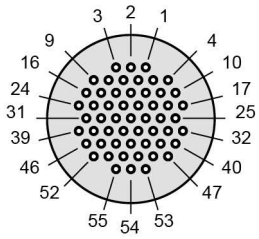
Access to this interface is blocked by default, you will therefore not be able to access the configuration interface from this port.

To access your Firewall from a client workstation, you will need to connect on the **IN** 2 or "Internal" port, or on another port (except port 1).

For further information regarding the startup procedure of your firewall, refer to the section INITIAL CONNECTION TO THE PRODUCT.

Ethernet cabling on the SNxr1200 model

WARNING
To access your Firewall from a client workstation, you will need to connect on the **IN** 2 or "Internal" port, or on another port (except port 1). Refer to the previous section IN/OUT definition.



J2

Port	Signal	Pin	Port	Signal	Pin
OUT 1	ETH1_MDI0+	J2.32	IN 2	ETH2_MDI0+	J4.1
	ETH1_MDI0-	J2.33		ETH2_MDI0-	J4.2
	ETH1_MDI1+	J2.34		ETH2_MDI1+	J4.3
	ETH1_MDI1-	J2.35		ETH2_MDI1-	J4.4
	ETH1_MDI2+	J2.36		ETH2_MDI2+	J4.11
	ETH1_MDI2-	J2.37		ETH2_MDI2-	J4.10
	ETH1_MDI3+	J2.38		ETH2_MDI3+	J4.9
	ETH1_MDI3-	J2.39		ETH2_MDI3-	J4.8

LEDs of interfaces (all models except SNxr1200)

LEDs associated with Ethernet interfaces provide indications on the status of the connection. following information on the connection:

SN160, SN160W, SN210, SN210W and SN310 models

Name	Color	Status	Status
Front panel LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.

SN160W and SN210W models

Name	Color	Status	Status
Front panel Wi-Fi LED ACT/LINK	Blue	On	Wi-Fi interface on.
		Off	Wi-Fi interface off.
		Blinking	The Wi-Fi interface is sending or receiving data. The blinking speed varies according to the volume of traffic.

SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN910, SN1100, SN-M-Series-720, SN-M-Series-920, SN2100 and SN3100 models

1Gbps Ethernet ports

Name	Color	Status	Status
Left LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.
	Green	On	Media speed negotiated at 100Mbps.
		Off	Media speed negotiated at 10Mbps.

2.5Gbps Ethernet ports (except SN510)

IMPORTANT
For the 2.5 Gbps extension module to be compatible with the SN1100 model, the BIOS must be updated to version R1.01 or higher.

Name	Color	Status	Status
Left LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Orange	On	Media speed negotiated at 2.5Gbps.
	Green	On	Media speed negotiated at 1Gbps.
		Off	Media speed negotiated at 100Mbps.
		Off	Media speed negotiated at 10Mbps.

10Gbps Ethernet ports

Name	Color	Status	Status
Left LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Green	On	Media speed negotiated at 10Gbps.
	Yellow	On	Media speed negotiated at 1Gbps.
		Off	Media speed negotiated at 100Mbps.

SN6100 model

1Gbps Ethernet ports (including IPMI)

Name	Color	Status	Status
Left LED ACT/LINK	Yellow	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.
	Green	On	Media speed negotiated at 100Mbps.
		Off	Media speed negotiated at 10Mbps.

10Gbps Ethernet ports

Name	Color	Status	Status
Left LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Green	On	Media speed negotiated at 10Gbps.
	Yellow	On	Media speed negotiated at 1Gbps.
		Off	Media speed negotiated at 100Mbps.

SNi20 model

Name	Color	Status	Status
Lower LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Upper LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.
	Green	On	Media speed negotiated at 100Mbps.
		Off	Media speed negotiated at 10Mbps.

SNi40 model

Name	Color	Status	Status
Upper LED ACT/LINK	Yellow	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Lower LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.
	Green	On	Media speed negotiated at 100Mbps.
		Off	Media speed negotiated at 10Mbps.

Fiber Ethernet connectors (all models except SN160, SN210, SN310 and SNxr1200)

These Ethernet ports are available by default on the following models:

- SN-M-Series-520 and SN910: ports 9 and 10 (via two sockets for SFP transceivers),
- SNi20: ports 5 and 6 (via two sockets for SFP transceivers)*,
- SNi40: ports 6 and 7 (via two sockets for SFP transceivers),
- SN-M-Series-720, SN-M-Series-920 and SN1100: ports 9 and 10 (via two sockets for SFP+ transceivers),
- SN6100: ports MGMT1 and MGMT2 (via two sockets for SFP+ transceivers).

* *may vary by license.*

On SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models, Ethernet fiber connectors can be added by inserting extension modules.

In both cases it is necessary to install a transceiver. **SFP** transceivers are used for **1Gbps** connections, **SFP+** for **1Gbps/10Gbps** connections or **QSFP+** for **40Gbps** connections (on SN2100, SN3100 and SN6100).

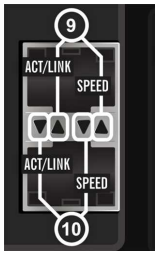
IMPORTANT
Use only Stormshield Network-approved transceivers found in the catalogue.

LEDs

The LEDs indicate the following information:

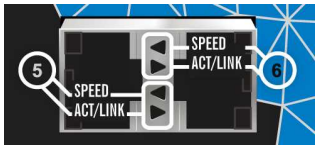
1Gbps connectors with SFP transceivers

- Default ports on SN- S-Series-220, SN- S-Series-320, SN-M-Series-520, SN910 and SNi40 models:
  A green LED will light up when the link is established and blink depending on the volume of traffic.
  For SN-M-Series-520 models, the position of LEDs is shown in the diagram on the right.



SN-M-Series-520: LEDs on ports 9 and 10

- Extension modules for SN710, SN910, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100 and SN3100 models:
  A green LED will light up when the link is established and blink depending on the volume of traffic.
- Default ports on SNi20* models:
  Both lower LEDs correspond to port 5 and both upper LEDs correspond to port 6.
  The position of LEDs is shown in the diagram on the right.



SNi20: LEDs on ports 5 and 6

Name	Color	Status	Status
Upper LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.
Lower LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.

* *may vary by license.*

- Extension modules for SN6100:

Name	Color	Status	Status
Left LED ACT/LINK	Yellow	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Yellow	On	Media speed negotiated at 1Gbps.

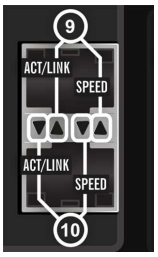
10Gbps connectors with SFP+ transceivers

- Extension modules for SN710, SN910, SN-M-Series-720 and SN-M-Series-920 models:

Name	Color/State	Status
Left LED ACT/LINK	Green/Blinking	Link established between the Ethernet port and the connected appliance. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Blue	Media speed negotiated at 10Gbps.
	Yellow	Media speed negotiated at 1Gbps.

- Default ports and extension modules for SN-M-Series-720, SN-M-Series-920, SN1100, SN2100 and SN3100 models:
  For SN1100 models, the position of LEDs is shown in the diagram below.

Name	Color/State	Status
Left LED ACT/LINK (Upper LED on SN-M-Series-720 and SN-M-Series-920)	Green/Blinking	Link established between the Ethernet port and the connected appliance. The blinking speed varies according to the volume of traffic.
Right LED SPEED (Lower LED on SN-M-Series-720 and SN-M-Series-920)	Blue	Media speed negotiated at 10Gbps.
	Off	Media speed negotiated at 1Gbps.



SN1100: LEDs on ports 9 and 10

- Default ports and extension modules for SN6100:

Name	Color	Status	Status
Left LED ACT/LINK	Green	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Green	On	Media speed negotiated at 10Gbps.
		Off	Media speed negotiated at 1Gbps.

40Gbps connectors with QSFP+ transceivers

- Extension modules for SN2100 and SN3100:

Name	Color	Status	Status
Left LED ACT/LINK	Green/Blinking	On	Link established between the Ethernet port and the connected appliance.
		Blinking	The blinking speed varies according to the volume of traffic.
Right LED SPEED	Green	On	Media speed negotiated at 40Gbps.

- Extension modules for SN6100:

Name	Color	Status	Status
Left LED ACT/LINK	Yellow	On	Link established between the Ethernet port and the connected appliance.
		Off	Ethernet port switched off or link not established with the connected appliance.
		Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
Right LED SPEED	Yellow	On	Media speed negotiated at 40Gbps.

Optional Ethernet transceivers

Ethernet fiber transceivers (SN710 and upwards, SNi20 and SNi40)

For 1 Gbps transmission, two types of transceivers are available according to the length of the cable and the type of fiber used:

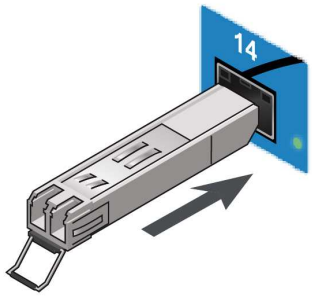
- SFP SX: short distance
- SFP LX: long distance.

For 10 Gbps transmission, two types of transceivers are available according to the length of the cable and the type of fiber used:

- SFP+ SR: short distance
- SFP+ LR: long distance.

For 40 Gbps transmission, two types of transceivers are available according to the length of the cable and the type of fiber used:

- QSFP+ SR4: short distance
- QSFP+ LR4: long distance



NOTE
Only **LC** fiber optic connectors are supported (or 1x12 MPO for QSFP+ SR4).

Ethernet copper transceivers (SN710 and upwards, SNi20 and SNi40)

For 1 Gbps transmissions, such RJ45 over SFP transceivers (1000/100/10Base-T) require copper Ethernet RJ45 cables. These must be Category 5e cables, for running in 10 Mbps, 100 Mbps or 1 Gbps. Check the compatibility of your devices.

Stormshield Network-approved Ethernet transceivers

		SN-S-Series-220 SN-S-Series-320 SN-M-Series-520, SNi20 and SNi40	SN710, SN910 SN-M-Series-720 SN-M-Series-920 SN1100	SN2100 SN3100 SN6100
FIBER CONNECTOR				
1Gbps SFP	SFP transceiver, **1000Base-SX** (black extraction lever) Requires a multi-mode fiber (the connector is usually orange). Wavelength: 850nm Typical maximum distance supported: 550m	supported	supported	supported
	SFP transceiver, **1000Base-LX** (blue extraction lever) Ethernet 1000Base-LX, requires a single-mode fiber (the connector is usually yellow). Wavelength: 1310nm. Typical maximum distance supported: 10km	supported	supported	supported
10Gbps SFP+	SFP+ Transceiver, **10GBASE-SR/1000Base-SX**, (beige extraction lever): Ethernet 10GBASE-SR/1000Base-SX, requires a multi-mode fiber (the connector is usually orange). Wavelength: 850nm Typical maximum distance supported: 300m on 10Gbps, 550m on 1Gbps.	not supported	supported	supported
	SFP+ transceiver, **10GBASE-LR/1000Base-LX** (blue extraction lever) Ethernet 10GBASE-LR/1000Base-LX, requires a single-mode fiber (the connector is usually yellow). Wavelength: 1310nm Typical maximum distance supported: 10km	not supported	supported	supported
40Gbps QSFP+	QSFP+ Transceiver, **40GBASE-SR4** (beige extraction lever) Ethernet 40GBASE-LM4, requires a multi-mode fiber with 1x12 MPO female connector. Wavelength: 850nm Typical maximum distance supported*: 150m with a multi-mode fiber	not supported	not supported	supported
	QSFP+ transceiver, **40GBASE-LR4** (blue extraction lever) Ethernet 40GBASE-LR4, requires a single-mode fiber (the connector is usually yellow). Wavelength: 1310nm Typical maximum distance supported: 10km with a single-mode fiber	not supported	not supported	supported
COPPER CONNECTOR				
1Gbps SFP	RJ45 over SFP transceiver, **1000/100/10Base-T** Requires a Category 5e RJ45 Ethernet cable. Typical maximum distance supported: 100m	supported	supported	supported

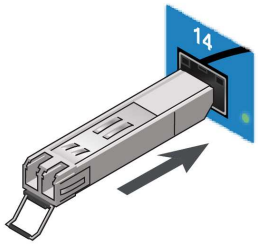
On condition of optimum quality

Installation

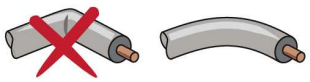
SFP/SFP+/QSFP+ transceivers are hot-swappable. Proceed as follows to install your transceiver:

1. If the socket in which you would like to install the transceiver has a protective cover, remove it.
2. Insert the transceiver, then plug in the cable corresponding to this transceiver.

IMPORTANT
The fiber transceiver and the optic fiber are equipped with a connector plug. When you plug this optic fiber into the transceiver, remove the connector plugs and keep them away from dust for later use.



IMPORTANT
Do not exceed the bending radius indicated in your optic fiber specifications.



Extension modules (SN710 and upwards)

There are three main steps to remove or insert extension modules on SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 or SN6100 firewalls:

1. **Step 1** Shut down firewall.
2. **Step 2** Remove or insert the module.
3. **Step 3** Restart the firewall

SFP/SFP+/QSFP+ transceivers for fiber extension modules have to be ordered separately.

SFP/SFP+/QSFP+ transceivers are hot-swappable (they can be inserted and removed while the appliance is powered on).

Description of extension modules for SN710 models and upwards

SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models accept the following extension modules:

- **8-port 1Gbps copper module**
  - RJ45 connectors
  - 1000/100/10Base-T
- **8-port 2.5Gbps copper module (SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN2100 and SN31000 models)**
  - RJ45 connectors
  - 2500/1000/100/10Base-T
- **4-port 10Gbps copper module (SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models)**
  - RJ45 connectors
  - 10G/1000/100Base-T

- **4-port 1Gbps fiber module (not available on SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models)**
  4 SFP+ sockets, supporting the following transceivers:
  - SFP fiber transceiver, 1000Base-SX (1Gbps Ethernet, short distance).
  - SFP fiber transceiver, 1000Base-LX (1Gbps Ethernet, long distance).
  - RJ45 over SFP copper transceiver, 1000/100/10Base-T
- **8-port 1 GbE fiber module**
  8 SFP+ sockets, supporting the following transceivers:
  - SFP fiber transceiver, 1000Base-SX (1Gbps Ethernet, short distance).
  - SFP fiber transceiver, 1000Base-LX (1Gbps Ethernet, long distance).
  - RJ45 over SFP copper transceiver, 1000/100/10Base-T
- **2-port 10 GbE fiber module (not available on SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models)**
  2 SFP+ sockets, supporting the following transceivers:
  - SFP+ fiber transceiver, 10GBase-SR (10Gbps Ethernet, short distance) / 1000BASE-SX (1Gbps Ethernet, short distance).
  - SFP+ fiber transceiver, 10GBase-LR (10Gbps Ethernet, long distance) / 1000BASE-LX (1Gbps Ethernet, long distance).
- **4-port 10Gbps fiber module**
  4 SFP+ sockets, supporting the following transceivers:
  - SFP+ fiber transceiver, 10GBase-SR (10Gbps Ethernet, short distance) / 1000BASE-SX (1Gbps Ethernet, short distance).
  - SFP+ fiber transceiver, 10GBase-LR (10Gbps Ethernet, long distance) / 1000BASE-LX (1Gbps Ethernet, long distance).
- **2-port 40Gbps fiber module (SN2100, SN3100 and SN6100)**
  2 QSFP+ sockets, supporting the following transceivers:
  - QSFP+ fiber transceiver, 40GBASE-SR4 (40Gbps Ethernet, short distance).
  - QSFP+ fiber transceiver, 40GBASE-LR4 (40Gbps Ethernet, long distance).

Sequence of modules

When extension modules are added or removed, ports will be reordered according to the order shown below.

SN-M-Series-520 model:

SN710 model:

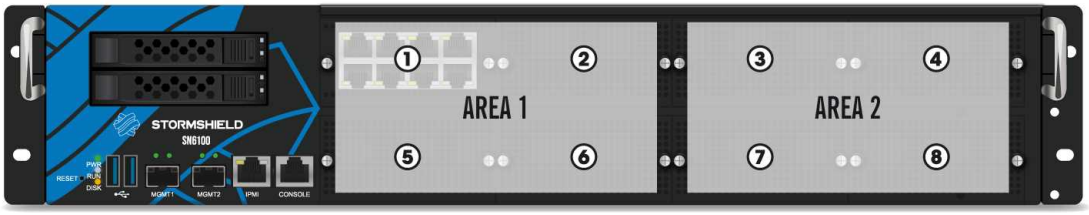
SN910 model:

SN-M-Series-720 and SN-M-Series-920 models:

SN1100 model:

SN2100 and SN3100 models:

SN6100 model:



Procedure for inserting or removing extension modules

No specific licenses are required for adding extension modules.

IMPORTANT
Extension modules must only be removed or inserted on appliances that have fully shut down and which must be unplugged from any electrical power supply.

On SN6100 models, spreading out network modules between both areas is recommended in order to enhance your product's performance. This makes it possible to balance the loads of both CPUs. The first set of modules and the 2 network ports located on the front of the appliance are managed as a priority by the first CPU and the second set by the second CPU.

IMPORTANT
The theoretical bandwidth available for each network slot is:
- **SN710 models:** 30Gbps, full-duplex
SN2100 and SN3100 models: 30Gbps, full-duplex on slot ❶
SN2100 and SN3100 models: 60Gbps, full-duplex on slots ❷ and ❸
SN-M-Series-520, SN910, SN-M-Series-720, SN-M-Series-920, SN1100 and SN6100 models: 60Gbps, full-duplex

REMINDER
In cases where modules are added subsequently in row 1, the interfaces of the modules in row 2 will be automatically re-ordered.

Inserting an extension module on SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 or SN6100 models

- Shut down the firewall by using the Power button on the front panel of SN1100, SN2100 and SN3100 models and on the rear panel of SN6100 models. On SN710, SN-M-Series-520, SN910, SN-M-Series-720 and SN-M-Series-920 models, shut down the firewall from the administration interface,
- Once it has fully shut down, ensure that you unplug it from any electrical power supply,
- Remove the filler panel by unscrewing the 2 knurled screws and extract it by pulling on both screws,
- Present the module to be inserted, push it all the way in (push harder towards the end), then screw in the 2 knurled screws,
- Reconnect the Firewall to the power supply,
- Using the Power button on the front panel, start the Firewall.

Removing an extension module on SN-M-Series-520, SN710, SN910, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 or SN6100 models

- Using the Power button on the front panel (rear panel for SN6100 appliances), or from the administration interface, proceed to shut down the Firewall,
- Once it has fully shut down, ensure that you unplug it from any electrical power supply,
- Unscrew the 2 knurled screws and extract the extension module by pulling on both screws,
- Put back the filler panel by screwing in the 2 knurled screws,
- Reconnect the Firewall to the power supply,
- Using the Power button on the front panel, start the Firewall.

INITIAL CONNECTION TO THE PRODUCT

By default, the product is managed through its INTERNAL interface. On all models, this interface is identified by the number 2 (IN).

For the description of the interfaces, refer to the section PRESENTATION OF THE SN RANGE.

Requirements

Minimum configuration to manage a Stormshield Network firewall

Lowest version of the OS (firmware)

For the following models, the lowest firmware versions required are:

- **SN160, SN160W, SN210, SN210W and SN310:** v3.1.1
- **SN-S-Series-220 and SN-S-Series-320:** v4.3.15
- **SN510 and SN710**: v1.4.1 in version 1 and v2.2.0 in version 2
- **SN-M-Series-520:** v4.3.15
- **SN910:** v1.2.3
- **SN-M-Series-720 and SN-M-Series-920:** v4.3.13
- **SN1100:** v4.2.4
- **SN2100 and SN6100:** v3.7.0
- **SN3100:** v3.7.5
- **SNi40:** v2.3.4
- **SNi20**: v4.1.0 in version 4 and v3.11.0 in version 3
- **SNxr1200:** v4.3.4

Web administration interface

In order for the firewall administration interface to operate optimally, you are advised to use the latest versions of Microsoft Edge, Google Chrome and Mozilla Firefox (ESR version - Extended Support Release). For further information on these versions, please refer to the relevant vendors for the life cycles of their products.

Preparing the Internet access

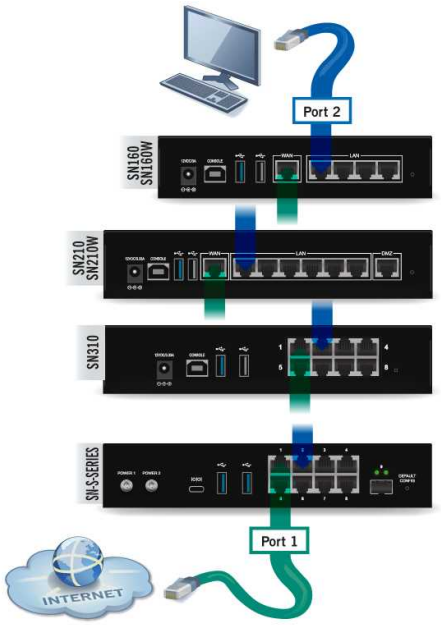
Before installing the SN firewall, ensure that the devices that connect to the Internet (if the firewall has to be connected to the Internet) have been appropriately installed and configured.

Connections

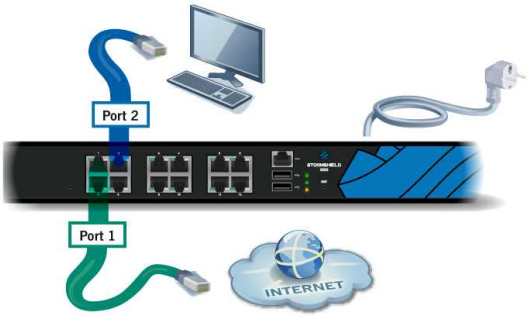
Connect the network ports as follows:

- INTERNAL interface 2 (IN): Workstation
- EXTERNAL interface 1 (OUT): Internet access device

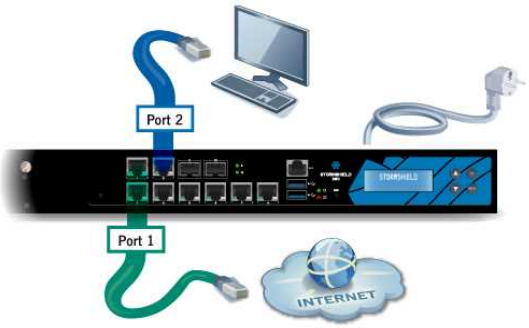
The client workstation can either be linked directly to the firewall's internal interface or connected to the local network, which is itself connected to the firewall's internal interface. For a direct connection of the workstation to the firewall, use the crossover Ethernet cable provided with the product. Details on how to connect SNxr1200 model firewalls are given in the section Cabling on the SNxr1200 model below.



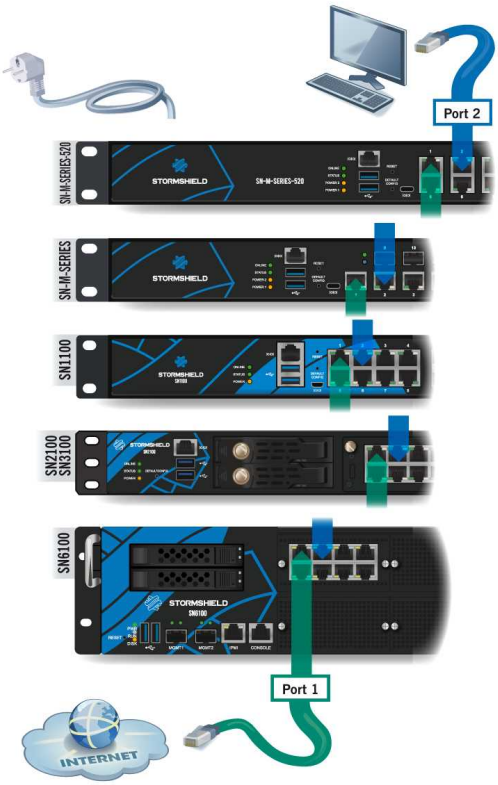
SN160, SN160W, SN210, SN210W, SN310 and SN-S-Series models



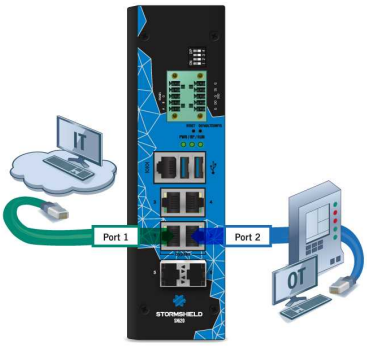
SN510 and SN710 models



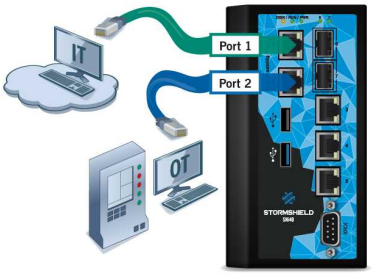
SN910 model



SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100, SN3100 and SN6100 models



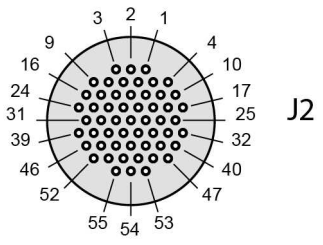
SNi20 model



SNi40 model

Cabling on the SNxr1200 model

WARNING
To access your Firewall from a client workstation, you will need to connect on the **IN** 2 or "Internal" port, or on another port (except port 1). Refer to the section on **NETWORK CONNECTORS**, under IN/OUT definition.



Port	Signal	Pin	Port	Signal	Pin
OUT 1	ETH1_MDI0+	J2.32	IN 2	ETH2_MDI0+	J4.1
	ETH1_MDI0-	J2.33		ETH2_MDI0-	J4.2
	ETH1_MDI1+	J2.34		ETH2_MDI1+	J4.3
	ETH1_MDI1-	J2.35		ETH2_MDI1-	J4.4
	ETH1_MDI2+	J2.36		ETH2_MDI2+	J4.11
	ETH1_MDI2-	J2.37		ETH2_MDI2-	J4.10
	ETH1_MDI3+	J2.38		ETH2_MDI3+	J4.9
	ETH1_MDI3-	J2.39		ETH2_MDI3-	J4.8

Configuration

When you first receive your firewall, it will run in transparent (bridge) mode and will have the IP address **10.0.0.254** with a subnetwork mask **255.0.0.0**. These parameters might not match your network configuration, but they are however necessary for the pre-configuration phase.

To connect to the firewall, you will need to use a workstation on which DHCP has been enabled, or its IP address has to be in the same address range as your firewall (10.0.0.0/8). DHCP is enabled by default on Windows platforms If this is not the case, refer to the section **Network configuration of your client workstation**. If you do not know what these parameters mean, we strongly advise you to read up on TCP/IP as it would be very difficult for you to configure your Stormshield Network firewall without some of the basics.

NOTE
For a manual configuration, we suggest that you use the IP address 10.0.0.1 and the subnet mask 255.0.0.0.

Network configuration of your client workstation

If DHCP has not been enabled on your client workstation, or for manual configurations, modify the **Network connection** parameters of your operating system.

In Windows, you generally need to select "Internet Protocol (TCP/IP)" from the list, then "Properties", and select the option **Obtain an IP address automatically**.

To manually configure this network, enter the necessary address information. During the initial connection, the IP address of this workstation will need to belong to the same address range as the firewall, 10.0.0.0/8 by default.

Startup

WARNING
You **must not** unplug the product when it is **starting, shutting down or being upgraded.**
Except for SN910 appliances, these phases are indicated when the following LEDs are lit:

- *Power* 3 and *Status* 2 LEDs for SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN1100, SN2100 and SN3100 models.
- *Power* 3 LED for SN6100, SNi20, SNi40 and SNxr1200 models.

For S SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320, SN510, SN-M-Series-520, SN710, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100 and SN3100 models, upon startup, the LEDs light up in the following order:
Power 3 ***+ Status*** 2 ***=> Online*** 1.
The *Power* and *Status* LEDs will light up first. After a few minutes, the *Online* LED will light up, followed by a beep (on SN510, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100, SN2100 and SN3100 models) once your product is up and running.

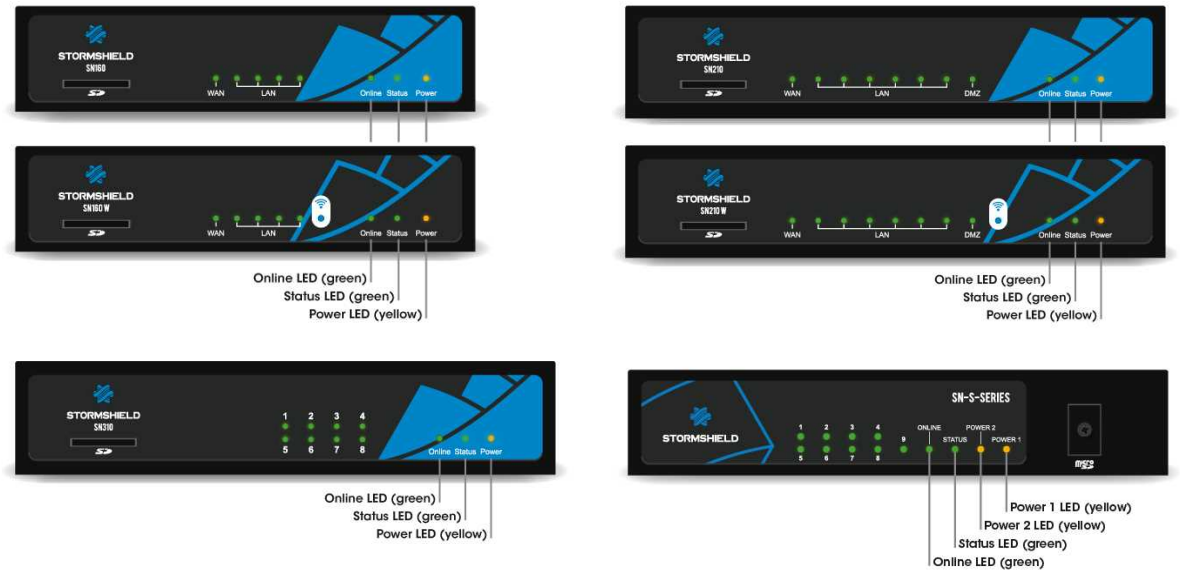
For SNi20, SNi40 and SN6100 models, upon startup, the LEDs light up in the following order:
Power => Run 1
The *Power* LED lights up first. After a few minutes, the *Online* LED will light up, followed by a beep on SN6100 models once your product is up and running.

Starting up SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320 models

Plug your firewall into its power supply; it will start automatically. Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* (2 *Power* LEDs on SN-S-Series-220 and SN-S-Series-320 models) to light up.

NOTE
If necessary during startup, you can insert a USB key containing a configuration. Console mode will display the following message: "*Please insert your USB token to continue*".

The lit *Online* LED will indicate the end of the product's startup phase.



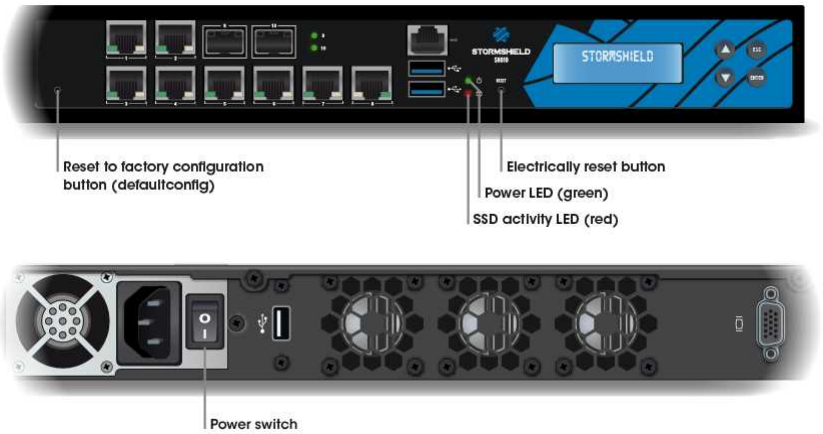
Starting up SN510 and SN710 models

Plug your SN firewall into the mains power supply, it will automatically start up. Ensure that the power supply switch is "ON". Your firewall will then automatically start running. Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to light up.

NOTE
When you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary. Console mode will display the following message: "*Please insert your USB token to continue*".

Two consecutive beeps and the lighted up *Online* LED indicate the end of the product's startup sequence.

Starting up SN910 models

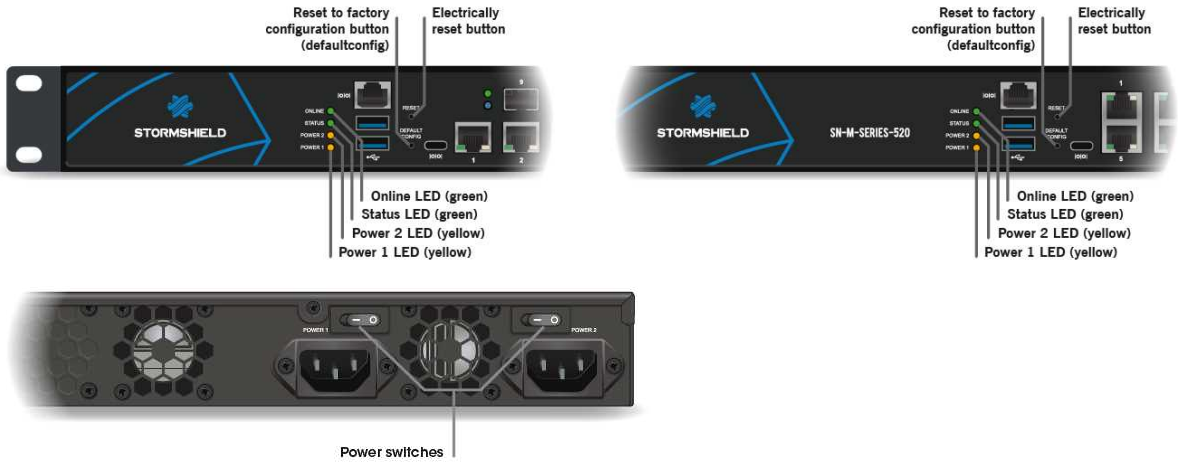


Plug your SN firewall into the mains power supply, it will automatically start up. Ensure that the power supply switch is "ON". Your firewall will then start running automatically, the Power LED will light up. Then wait several minutes.

NOTE
When you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary. Console mode will display the following message: "Please insert your USB token to continue".

Two consecutive beeps indicate the end of the product's startup sequence.

Starting SN-M-Series-520, SN-M-Series-720 and SN-M-Series-920 models



Plug your SN firewall into the mains power supply, it will automatically start up. Ensure that both power supply switches are "ON". Your firewall will then start running automatically, the Power LED will light up. Wait a few minutes for all 4 LEDs – *Online*, *Status*, *Power 1* and *Power 2* to light up.

> **NOTE**
> When you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary. Console mode will display the following message: “Please insert your USB token to continue”.

A beep indicates the end of the product’s startup sequence.

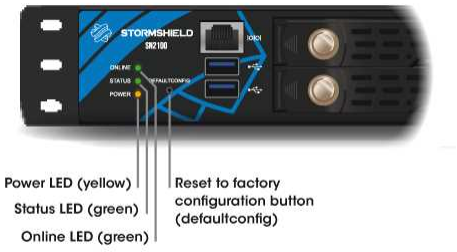
Starting up SN1100, SN2100 and SN3100 models

As soon as the appliance is powered up, press once on the Power button (rear panel). Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to light up.

> **NOTE**
> When you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary. Console mode will display the following message: “Please insert your USB token to continue”.

Two consecutive beeps and the lighted up *Online* LED indicate the end of sequence.

SN1100 model



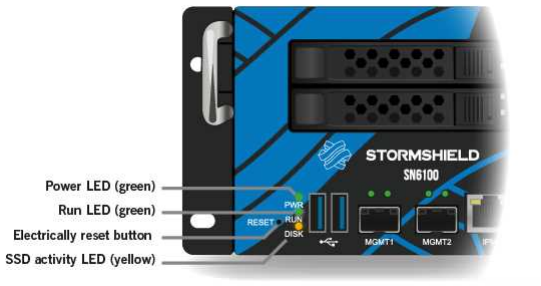
SN2100 and SN3100 models

Starting up SN6100 models

As soon as the appliance is powered up, press once on the Power button (rear panel). Wait a few minutes for both LEDs – *Power* and *Run* to light up.

> **NOTE**
> When you hear 8 consecutive beeps, you will be able to insert a USB key containing a configuration if necessary. Console mode will display the following message: "*Please insert your USB token to continue*".

Two consecutive beeps indicate the end of the product's startup sequence.

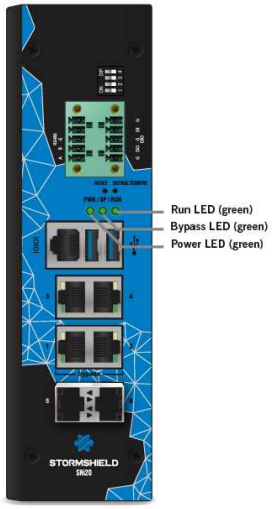


Starting up SNi20 and SNi40 models

Once your firewall has been powered up, it will automatically start up. Wait a few minutes for both LEDs – *Power* and *Run* to light up.

> **NOTE**
> If necessary during startup, you can insert a USB key containing a configuration. Console mode will display the following message: "*Please insert your USB token to continue*".

The lit *Run* LED will indicate the end of the product's startup phase.



Starting up SNxr1200 models

Once your firewall has been powered up, it will automatically start running and the *Power* LED will light up. Then wait several minutes.

Initial connection to the appliance

A security procedure must be followed if the initial connection to the appliance takes place through an untrusted network. This operation is not necessary if the administration workstation is plugged in directly to the product.

Access to the administration portal is secured through the SSL/TLS protocol. This protection allows authenticating the portal via a certificate, thereby assuring the administrator that he is indeed logged in to the desired appliance. This certificate can either be the appliance's default certificate or the certificate entered during the configuration of the appliance (*Authentication* > *Captive portal*). Depending on the model, it is signed by default by the authority with the name:

- **NETASQ:** CN=serial number of the appliance, O=Secure Internet Connectivity, OU=NETASQ firewall Certification Authority.
- **Stormshield**: CN=Stormshield Products Root CA, O=Stormshield, OU=Cloud Services, C=FR, L=Issy-Les-Moulineaux.

To confirm a secure access, the browser must trust the certification authority that signed the certificate used, which must belong to the browser's list of trusted certification authorities. Therefore, to confirm the integrity of the appliance, before the initial connection, you need to add the authority to the list of the browser's trusted authorities. Depending on the model, the corresponding authority is available on these links:
http://pki.stormshieldcs.eu/netasq/root.crt
http://pki.stormshieldcs.eu/products/root.crt

If a certificate signed by another authority has been configured on the appliance, this authority will need to be added instead of the default authority.

As a result, the initial connection to the appliance will no longer raise an alert in the browser regarding the trusted authority. However, a message will continue to warn the user that the certificate is not valid. This is because the certificate defines the firewall by its serial number instead of its IP address. To stop this warning from appearing, you will need to indicate to the DNS server that the serial number is associated with the IP address of the firewall.

Administration graphical interface

On your client workstation, type the following address in your browser:
https://10.0.0.254/admin
Enter "**admin**" as the login and password.

IMPORTANT
If you have connected your client workstation on port 1, you will no longer be able to access the web administration interface You will need to connect your computer to port 2 (or on another port), and reboot your firewall.

NOTE
The default password of the "admin" user (super administrator) must be changed the very first time the product is used. In the web administration interface, this password can be changed in the **Administrator** module (**System** menu), under the *Administrator account* tab.
The definition of this password must observe the best practices described in the **User Guide**, in the section *Welcome*, sub-section *User awareness*, paragraph *User password management*, available at https://documentation.stormshield.eu
This password must never be saved in the browser.

For further information on downloading and installing your license, refer to the section UPDATING THE LICENSE.

Shutting down

SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220 and SN-S-Series-320

Log on to the configuration interface. Go to the **Maintenance** module (**System** menu) and click on "Shut down the firewall". Then wait for several minutes until the *Online* and *Status* LEDs go out. For this model, the LEDs shut off in the following order:

Online (1) ***=> Status*** (2)

The *Power* LED will stay lit if the product is powered up.

SN510, SN-M-Series-520, SN710, SN-M-Series-720 and SN-M-Series-920

Log on to the configuration interface. Go to the **Maintenance** module (**System** menu) and click on "Shut down the firewall". Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to go off.

For these models, upon shutdown, the LEDs shut off in the following order:

Online (1) ***+ Status*** (2) ***=> Power*** (3)

A beep will indicate that the appliance is in the process of shutting down.

SN910

Log on to the configuration interface. Go to the **Maintenance** module (**System** menu) and click on "Shut down the firewall".

A beep will indicate that the appliance is in the process of shutting down. Wait for several minutes until the *Power* LED goes out.

SN1100, SN2100 and SN3100

To shut down your firewall, press once on the Power button located on the rear panel. Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to go off.

For these models, upon shutdown, the LEDs shut off in the following order:

Online (1) ***+ Status*** (2) ***=> Power*** (3)

A beep will indicate that the appliance is in the process of shutting down.

SN6100

To shut down your firewall, press once on the Power button located on the rear panel. Wait a few minutes for the 2 LEDs (*Run* and *Power*) to go off. For this model, the LEDs shut off in the following order:

Run (1) ***=> Power*** (2)

A beep will indicate that the appliance is in the process of shutting down.

SNi20

Log on to the configuration interface. Go to the **Maintenance** module (**System** menu) and click on "Shut down the firewall". Wait several minutes until the Run LED goes off and the Power LED turns to yellow. For this model, the LEDs shut off in the following order:

Run (1) ***=> Power*** (2)

The Power LED will stay yellow if the product is powered up.

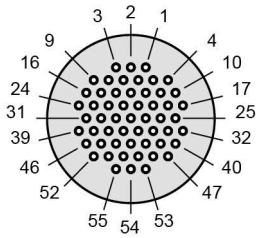
SNi40

Log on to the configuration interface. Go to the Maintenance module (System menu) and click on "Shut down the firewall". Wait a few minutes for the 2 LEDs (*Run* and *Power*) to go off. For this model, the LEDs shut off in the following order:

Run (1) ***=> Power*** (2)

SNxr1200

Log on to the configuration interface. Go to the Maintenance module (System menu) and click on "Shut down the firewall". Then wait for several minutes until the *Power* LED goes out.



J2

ON/OFF switch

Details	Pin	Signal
ON	J2.10	POWER_BUTTON+
OFF	J2.11	POWER_BUTTON-

General remarks

- The *Status* LED (2) (Run for SN6100, SNi20 and SNi40 models) will blink in red (green for SN510 and SN710 models) in the event of a major failure on the product (hardware anomaly, faulty network interface, etc.). Contact your reseller in this case.
- During startup, shutdown or upgrading, only the LEDs *Status* (2) and *Power* (3) will light up.
- In High Availability mode, when the firewall is in passive mode, the *Online* (1) or *Run* LED on SN6100, SNi20 and SNi40 models will blink (about 2 seconds off for every 1 second it is on).
- During the reset phase (*defaultconfig*), the *Online* and *Status* LEDs will blink (*Run* for SN6100, SNi20 and SNi40).
- To reboot an SN160, SN160W, SN210, SN210W, SN310 or SNi20 appliance that is still powered up (only the *Power* LED is on), you will need to unplug and plug the firewall back into the mains socket. It is also possible to reboot in console mode by pressing on any key as suggested.
- To reboot an SNi20 appliance that has been shut down (*Run* LED off and Power LED in yellow), proceed as follows: unplug it, wait for thirty seconds, then plug the firewall back into its power supply source.
- To reboot an SNi40 appliance that has been shut down (*Power* and *Run*LEDs off), proceed as follows: unplug it, wait for thirty seconds, then plug the firewall back into its power supply source.
- To reboot an SN510, SN710, SN910, SN-M-Series-720 or SN-M-Series-920 model (*Power* LED is off), proceed as follows: unplug it, wait for thirty seconds, then plug it back into the mains socket.
- You may also shut down your firewall by logging on in console mode and by typing the following command: `halt`

UPDATING THE LICENSE

Your appliance is delivered with a temporary license that must be updated. If you have acquired additional options or a security pack, you must update your product with the license that will allow you to use this option.

Maintenance packs are valid from the date on which the associated SNS products are registered on MyStormshield. If the product remains unregistered, this period will begin automatically three months from the billing date. Reminder: products must be registered to receive updates and be entitled to technical support.

WARNING
Options that require the firewall to be rebooted are listed in the **User Manual**, under the License section, at *https://documentation.stormshield.eu*

Refer to the procedure below to find out how to update your product license:

Retrieving the license

1. Go to your Secure Area at https://mystormshield.eu/
   The registration step allows you to obtain the password to access your **Secure area**.
2. Enter your login and password then confirm or register in order to receive them. The client secure area homepage will appear.
3. Click on “product management”. You will then see a list of all the Stormshield Network products registered in this area.
4. Select the product for which you wish to retrieve the license, by clicking on the product’s serial number. Details of the license will be displayed.

NOTE
Before you download the license, you will need to know your product’s version. If you do not know it, it is indicated on a label affixed to the product’s cardboard packaging. If you no longer have the packaging, or if you have since updated your product, connect to your product via the web administration interface. The product’s version will be indicated in the dashboard of the web application.

Installing the license

If you have never installed a license on the product, the details of the license will be of the temporary license. To install the license that had been downloaded from the client secure area, proceed as follows:

Via the web administration interface, go to the General tab of the **License** module.

- To manually install a license, insert the downloaded file in the relevant field. It is however possible to configure an automatic search and installation of the license.
- The full procedure is set out in the **User Manual**, under the License section, at *http://documentation.stormshield.eu*.

DOCUMENTATION & ASSISTANCE

DOCUMENTATION

The documentation for SN Multi-function Firewalls is available online at https://documentation.stormshield.eu

This website allows you to look up or download various technical documents such as user guides, technical notes, etc. The INSTALLATION AND FIRST-TIME CONFIGURATION GUIDE explains how to configure your firewall. This guide can be found at: https://documentation.stormshield.eu/SNS/first-config

SECURE AREA

The registration step allows you to obtain the password to access your **Secure area**. Your Secure area allows you to:

- Activate licenses and software options, and download the latest updates,
- Manage your licenses,
- Subscribe to technical and marketing mailing lists,
- Access the knowledge base.

Log in to the following address to access or obtain the access codes to your Secure area at https://mystormshield.eu/.

KNOWLEDGE BASE

The technical support department's knowledge base centralizes various technical entries relating to the use of Stormshield Network products. Its aim is to give a better understanding of how they work. The ***Knowledge base*** is in your **Secure area**.

ASSISTANCE

When you encounter hardware issues on your firewall or if any of the components does not match its description, contact your certified partner.

For Stormshield Network products, there are different product return procedures called RMAs (return merchandise authorization). The various types of RMA are as follows:

1. RMA WITH STANDARD EXCHANGE:
   If the appliance has a valid **Standard** maintenance package
2. RMA WITH EXPRESS EXCHANGE:
   If the appliance has a valid **Express exchange** maintenance package
3. RMA WITH DOA EXCHANGE:
   If the product was registered **less than 30 days** before the RMA was activated.

The procedures and documents relating to these exchanges can be found on the MyStormshield online help website at https://mystormshield.eu/documentation

In compliance with Common Criteria assumptions, clients must subscribe to the **Secure Exchange** option and follow the procedure for this type of exchange. This option ensures the confidentiality of the configuration elements imported into the Stormshield Network product before it is sent for repairs.

APPENDIX A: RESETTING THE FIREWALL

The default factory settings can be restored on a Stormshield Network firewall. This operation will bring the product back to its initial configuration. It does not modify the firmware version and only affects the active partition.

WARNING
Resetting a firewall will completely erase the settings configured on the product. This operation is irreversible, so do not apply this procedure unless absolutely necessary. You are therefore advised to make a backup beforehand.

WARNING
The product must not be unplugged while is it reinitializing.

After a few minutes the initial settings will be recovered and the firewall will reboot. This reset operation may take **up to 10 minutes**, so do wait until the end of the reboot procedure before reconnecting to the firewall.

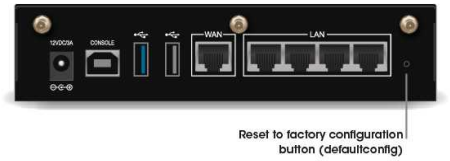
NOTE
The *Online* and *Status* (*Run* on SN6100, SNi20 and SNi40) LEDs will blink throughout the entire initialization phase. Two consecutive beeps (except on SN160, SN160W, SN210, SN210W, SN310, SNi20 and SNi40 models) and the lighted up *Online* (*Run* on SN6100, SNi20 and SNi40) LED indicate the end of the product's startup sequence.

WARNING
This operation will also reinitialize the administrator's password. The login and password are "admin" by default.

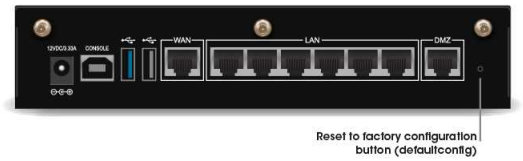
All models except SN6100, SNi40 and SNxr1200

Use a pointed object to reset your firewall. A small pushbutton is accessible through a hole in the following locations:

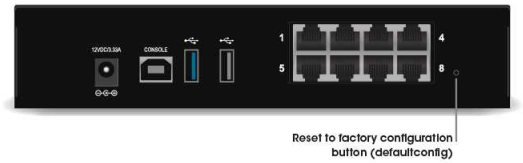
- on SN160, SN160W, SN210, SN210W and SN310 models, on the rear panel of the product, to the right of the Ethernet interfaces.
- on SN510 models, on the front panel of the product, to the left of the Ethernet interfaces.
- on SN710 and SN910 models, on the front panel of the product, between the extension module slot and the Ethernet interfaces.
- On SN-M-Series-720, SN-M-Series-920 and SN1100 models, on the front panel of the product, between the USB ports and the Ethernet interfaces,
- on SN2100 and SN3100 models, on the front panel of the product, between the LEDs and USB ports,
- on SNi20 models, on the front panel of the product, to the right above the LEDs.



SN160 and SN160W models



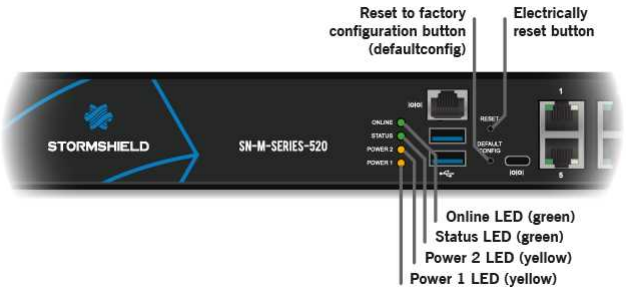
SN210 and SN210W models



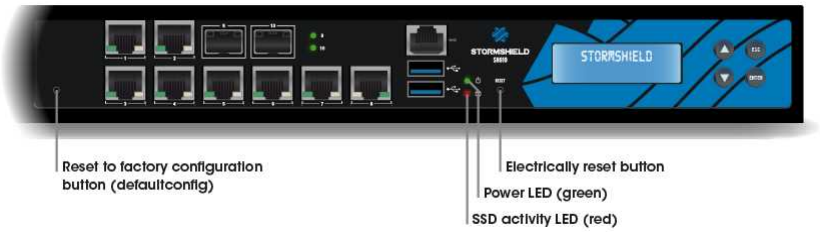
SN310 model

SN-S-Series-220 and SN-S-Series-320

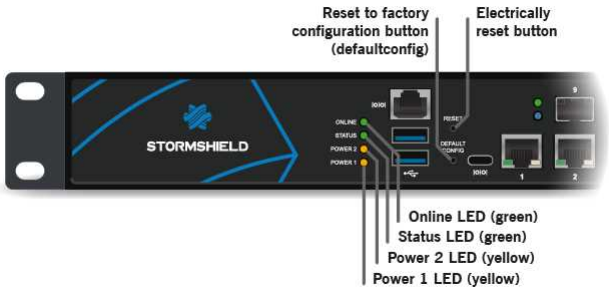
SN510 and SN710 models



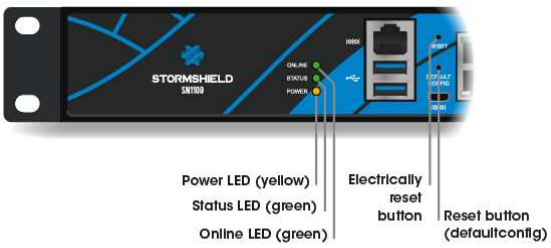
SN-M-Series-520 model



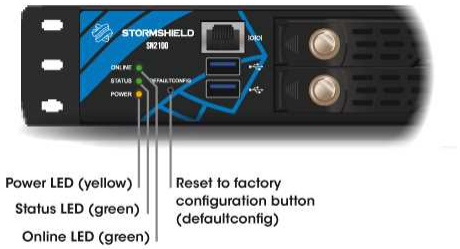
SN910 model



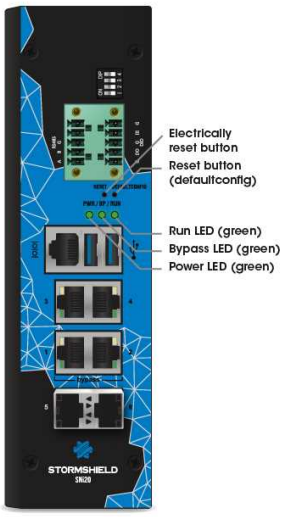
SN-M-Series-720 and SN-M-Series-920 models



SN1100 model



SN2100 and SN3100 models



SNi20 model

Hold down the button for about 5 seconds, until you see the *Online* and *Status* (*Run* on SNi20 models) LEDs blink and/or until you hear an audible signal. The reset procedure will automatically launch. After a few minutes, the initial settings will be recovered and the firewall will reboot.

SN6100, SNi40 and SNxr1200 models

The factory configuration on SN6100, SNi40 and SNxr1200 appliances can only be restored by connecting in console mode. Type the following command: `defaultconfig -f -r -p`

The reset procedure will automatically launch. After a few minutes, the initial settings will be recovered and the firewall will reboot.

APPENDIX B: LOG STORAGE

For models equipped with a hard disk or SSD, the log storage service is enabled by default, except on SNi40 models. To enable it, refer to the section *Enable log storage* below.

External log storage on SD cards (SN160, SN160W, SN210, SN210W, SN310, SN-S-Series-220, SN-S-Series-320 and SNi20)

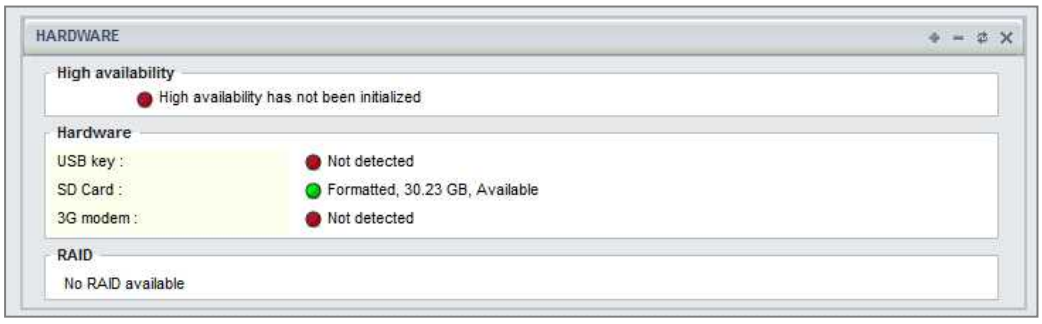
NOTE
Logs can only be stored externally on SD cards. This service is not compatible with other media such as a USB key or an external hard disk.

The recommended type of SD card is at least **Class 10 (C10) UHS Class 1 (U1) or App Performance 2 (A2)**. The memory card must be in **SDHC or SDXC standard**. Only adapters provided with the card must be used. The maximum memory size supported is 2 TB.

Stormshield recommends the use of **high-endurance/industrial** cards or preferably, those that have a built-in **MLC** flash chip developed by major brands (e.g., SanDisk, Western Digital, Innodisk, Transcend, etc.) and with at least 32Go.

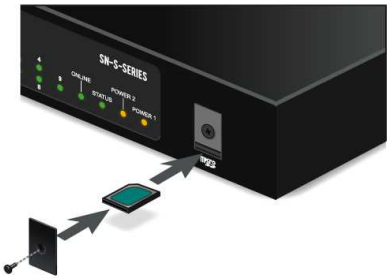
Insert the SD card, as described in the diagram to the right, with the connector facing downwards.

When you insert the SD card for the first time, the *Hardware* component (widget) on the **Dashboard** will display the following information:

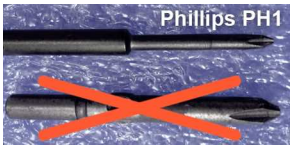


IMPORTANT
In order to remove the screws from the SD card reader cache, use these specific screwdrivers:
- **SNi20 models:** Phillips PH1 screwdriver
- **SN-S-Series-220 and SN-S-Series-320:** Phillips PH0 screwdriver
Insert the SD card, then put back the SD card reader cache to guarantee that the product is airtight.

SNi20 model



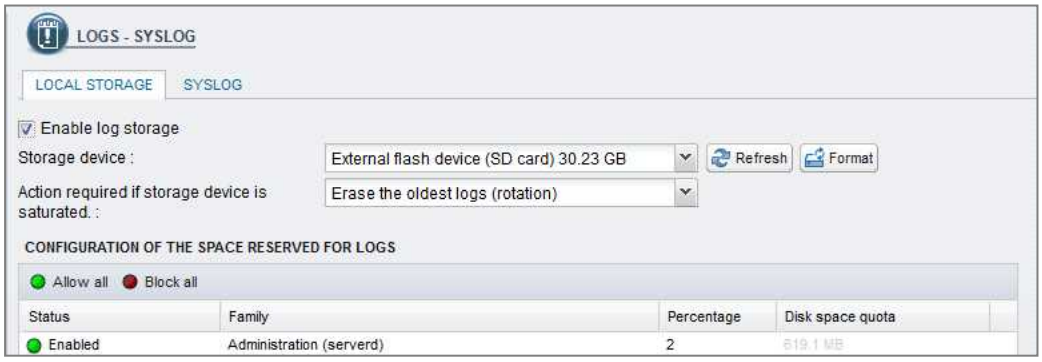
SN-S-Series-220 and SN-S-Series-320 models



You must then enable and format the SD card - refer to the following section.

Enabling log storage

To enable the service, go to the **Notifications** menu, then to the **Logs – Syslog** module. In the *Local storage* tab, select the *Enable log storage* option.



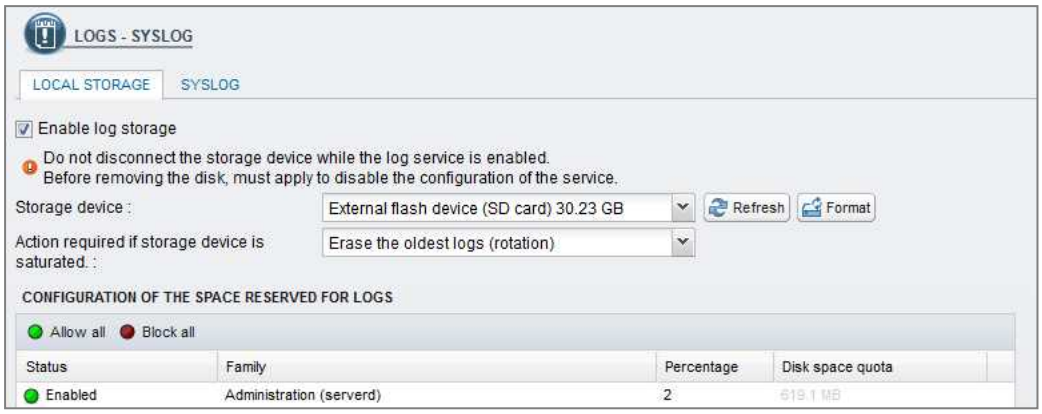
If you wish to save logs on an SD card, hard disk or SSD, select *Enable log storage*, then select your medium from the list of storage media. A message will prompt you to format it.

After this operation, your SD card, hard disk or SSD will be ready to receive all logs.

Loading the SD card

IMPORTANT
Before ejecting the SD card from the drive, to change media, for example, you must first shut down the service by unselecting the option that enables log storage, in the **Logs - Syslog** module.

To eject the SD card, press lightly and horizontally on it, then let go.



Reading logs

These logs can be read in the **SN Activity Reports** web interface in the form of reports.

In **SN Activity Reports,** 5 reports are enabled by default. The number of reports enabled can be increased on models that are equipped with hard disks or an SSD or with the help of an SD card.

Refer to the **User Manual**, under the *Reports* section, at https://documentation.stormshield.eu

APPENDIX C: MANAGING SSDs

An SSD is installed by default on the SN2100 model. A second SSD can be added to it by subscribing to the RAID option (RAID1).

By default on SN3100 and SN6100 models, both SSDs are installed in RAID (RAID 1). Both of these SSDs are also hot-swappable.

NOTE
On SN2100 models without the RAID option, the replacement of the SSD would cause logs and static reports saved on the log partition to be lost, as well as data memorized using the HTTP Cache option if it has been enabled.

Detecting issues

The SMART (Self-Monitoring, Analysis and Reporting Technology system) status of SSDs can be monitored. SMART technology monitors and informs about the status of certain reliability indicators such as the temperature, number of sectors allocated, errors while locating sectors, etc. It therefore helps to anticipate failures.

On SN910, SN-M-Series-520, SN-M-Series-720, SN-M-Series-920, SN1100 and SN2100 models without the RAID option, and SNi20 and SNi40 models, the SMART status of the SSD is available in the *Hardware* section of the **Hardware** widget.

On SN2100, SN3100 and SN6100 models with the RAID option, the *RAID* section in the **Hardware** widget informs you about the SMART status of the SSDs, as well as the RAID status.

You may also log on to the appliance in console mode or via an SSH connection and obtain the information with the following commands:

- SMART status of the SSDs: `smartinfo`
- If SSDs are installed in RAID: `nraid -s`

If an issue arises with the log partition, report it using the Properties widget either in console mode or via an SSH connection, using the command: `logdisk -c`, the partition can be rebuilt using the following command: `logdisk -f`

IMPORTANT
This command permanently erases data saved earlier on the log partition.

If the SMART status of an SSD shows errors, or if rebuilding your log partition fails, you can contact your certified partner to replace your SSD.

Replacing an SSD

Depending on the model, the respective procedures are as follows:

- SN2100, without RAID option:

This procedure is to be carried out on an appliance that has been powered off. To remove the SSD, unlock the rack with the lever, then pull out the canister with the defective SSD. Insert the new canister with the replacement SSD obtained from your partner, until you hear a click. Once you have inserted the new SSD, it will be detected the next time you start the appliance.

- SN2100 with RAID option, SN3100 and SN6100 (SSD in RAID 1):

This procedure is to be carried out on an appliance that is running. To remove the SSD, unlock the rack with the lever, then pull out the canister with the defective SSD. Insert the new canister with the replacement SSD obtained from your partner, until you hear a click. Once you have inserted the new SSD, type the following command to scan this new SSD: `nraid -z`.

Next, type the command to rebuild the RAID: `nraid -r`

RAID option (SN2100)

On the SN2100 model, the RAID option can be subscribed in order to add a second SSD and build a RAID1 on it.

This procedure is to be carried out on an appliance that is running:

- In console mode, type the following command to build the RAID: `nraid -c`
- Unlock the rack with the lever, then pull out the empty canister (lower canister, LEDs off). Insert the new canister with the optional SSD obtained from your partner, until you hear a click.
- Once you have inserted the new SSD, type the following command to scan this new SSD: `nraid -z`
- Then type the following command to replicate the data on the RAID: `nraid -r`

Big Data option (SN2100, SN3100 and SN6100)

If you have subscribed the *Big Data* option(available on SN2100, SN3100 and SN61000 models), the original SSDs will be replaced with SSDs of greater capacity.

After you have shut down the appliance, you will be able to extract the SSDs. Unlock the rack with the levers, then pull out both SSD canisters. Insert the new canisters with the replacement SSDs obtained from your partner, until you hear a click. They will be detected the next time you start the appliance.

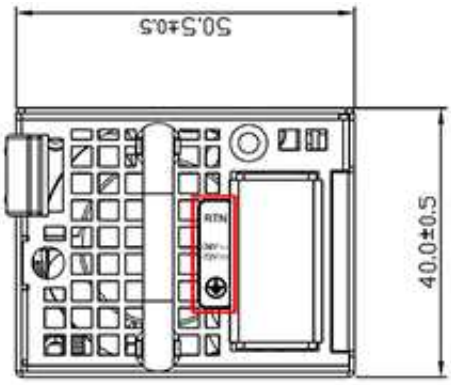
APPENDIX D: CHANGING A POWER SUPPLY MODULE (SN1100, SN2100, SN3100 AND SN6100)

REMINDER
Before plugging any equipment into a 48VDC power supply module, read the SAFETY RULES carefully and follow them.

SN1100, SN2100 and SN3100

NOTE
On SN1100 and SN2100 models, a second AC mains supply or -48VDC module can be ordered separately for redundant power supply. Modules are hot-swappable on products with a redundant power supply.

SN1100, SN2100 and SN3100 models



1. Disconnect the module from the electrical supply:
   - **AC mains supply:** disconnect the mains cable.
   - **-48VDC supply:** first, disconnect the power cord from the 48VDC source. Next, on the module, remove the protective cover ❶, then use a screwdriver to disconnect the three supply wires.
2. Remove the module: push the release lever sideways toward the extraction handle, and use the handle to pull the module. Take hold of the case of the module and remove it completely.
3. Insert the new module with the product label facing upwards. When the module is fully inserted, push until you hear a "click" that indicates that the module is locked in place. Verify that the module is locked in place by pulling gently on the extraction handle: the module must not move.
4. Attach the new module to the electrical supply:
   - **AC mains supply:** connect the mains cable.
   - **-48VDC supply:** with the power cord disconnected from the 48VDC supply, use a screwdriver to attach the three wires of the power cord to the module ❶ then reattach the protective cover. The wires must be connected to the 48VDC module as shown above. Next, connect the power cord to the 48VDC source.

Each PSU module is equipped with a light showing its state (two colors: green/red for the AC mains module, blue/red for the -48VDC module):

- **Module working correctly**
  - module connected to a power source but not installed in a firewall: green (AC mains)/blue (-48VDC).

- SN1100, SN2100 and SN3100 (halted):

  - module installed but not connected to a power source, and the other module is installed and connected: green (AC mains)/blue (-48VDC), blinking.
  - module installed and connected to a power source: green (AC mains)/blue (-48VDC), blinking.

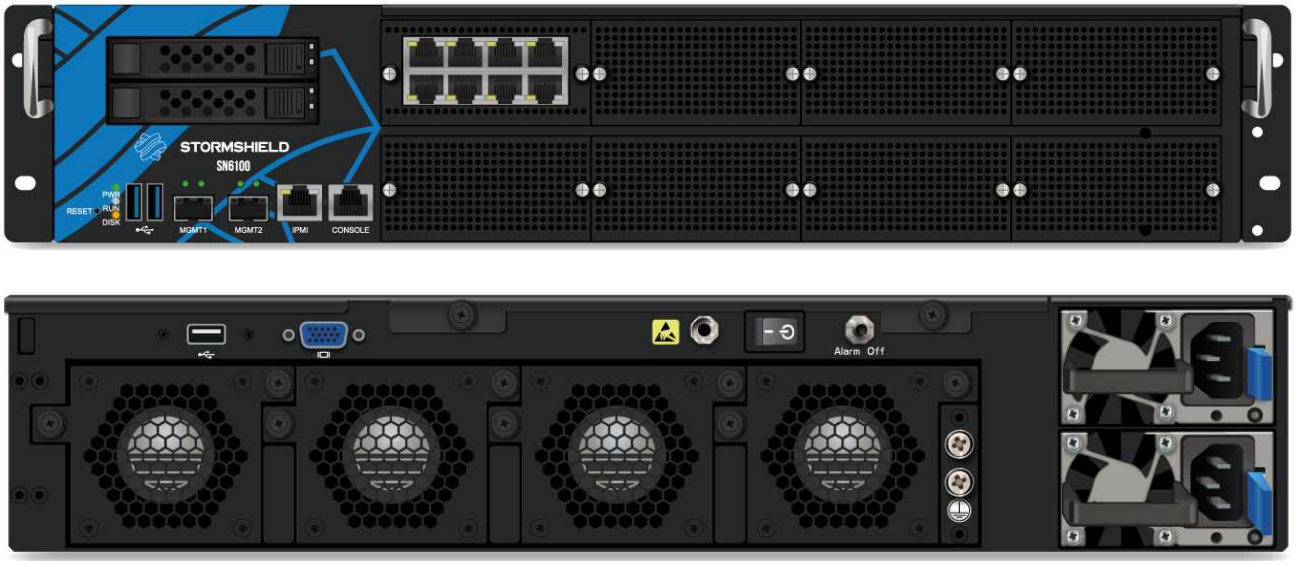
- SN1100, SN2100 and SN3100 running:

  - module installed and connected to a power source: green (AC mains)/blue (-48VDC), not blinking.
  - module installed and not connected to a power source: red, blinking (+ buzzer).

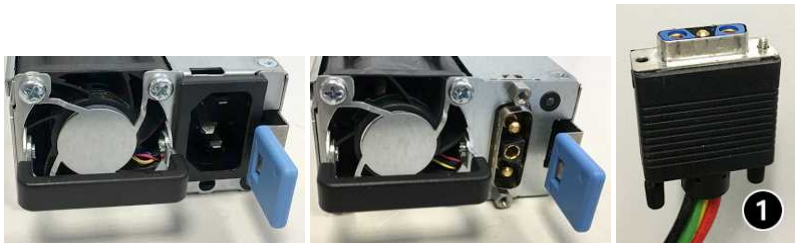
- **Module not functioning correctly**
  - module connected to a power source: red, not blinking.

SN6100

> **NOTE**
> This model is equipped with an internal redundant power supply and its modules are hot-swappable.



SN6100 model



1. Disconnect the module from the electrical supply:
   - **AC mains supply:** disconnect the mains cable.
   - **-48VDC supply**: unscrew the knurled screw, then unplug the power cord on the module side.
2. Remove the module: push the release lever sideways toward the extraction handle, and pull the handle. Take hold of the case of the module and remove it completely.

> **WARNING**
> The module's metal case serves as a heat sink and its temperature can reach +60°C at full power. It is therefore advisable to use a glove to hold the case.

3. Insert the new module with the product label facing upwards. When the module is fully inserted, push until you hear a “click” that indicates that the module is locked in place. Verify that the module is locked in place by pulling gently on the extraction handle: the module must not move.
4. Attach the new module to the electrical supply:
   - **AC mains supply:** connect the mains cable.
   - **-48VDC supply:** plug in the power cord's connector ❶ Screw in the knurled screw.

Each PSU module is equipped with a light showing its state (two colors: green/red):

- **Module working correctly**
  - module connected to a power source but not installed in a firewall: green, blinking.

- SN6100 (halted):

  - module installed but not connected to a power source, and the other module is installed and connected: red, not blinking.
  - module installed and connected to a power source: green, blinking.

- SN6100 (running):

  - module installed and connected to a power source: green, not blinking.
  - module installed and not connected to a power source: red, not blinking (+ buzzer).

- **Module not functioning correctly**
  - module connected to a power source: red, not blinking.

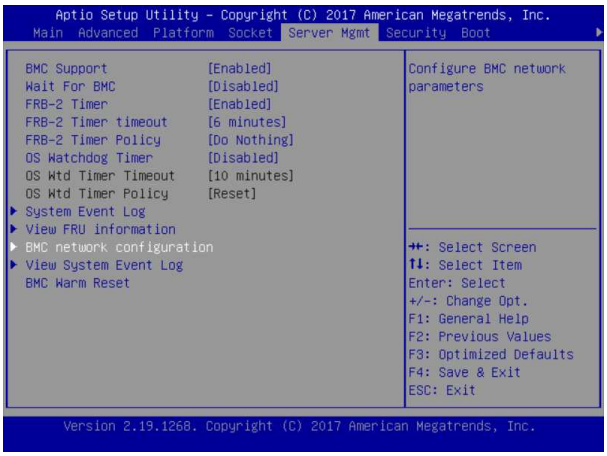
APPENDIX E: CONFIGURATION AND ADMINISTRATION VIA IPMI (SN6100)

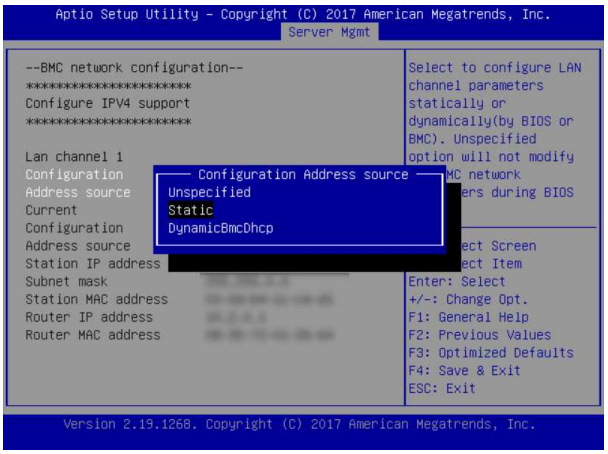
IPMI (Intelligent Platform Management Interface) is a network protocol that makes it possible to obtain hardware information remotely, monitor certain components and control appliances (control, reboot, interruption, etc.).

SN6100

Configuration

When the product is starting up, once the Stormshield logo appears, press <del> to access the BIOS. Next, go to the section "BMC network configuration" in the Server Mgmt menu in order to configure the network interface dedicated to IPMI, then save and quit.

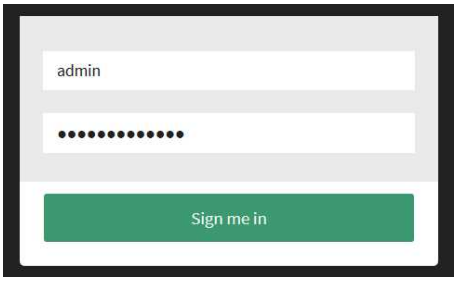




Connection

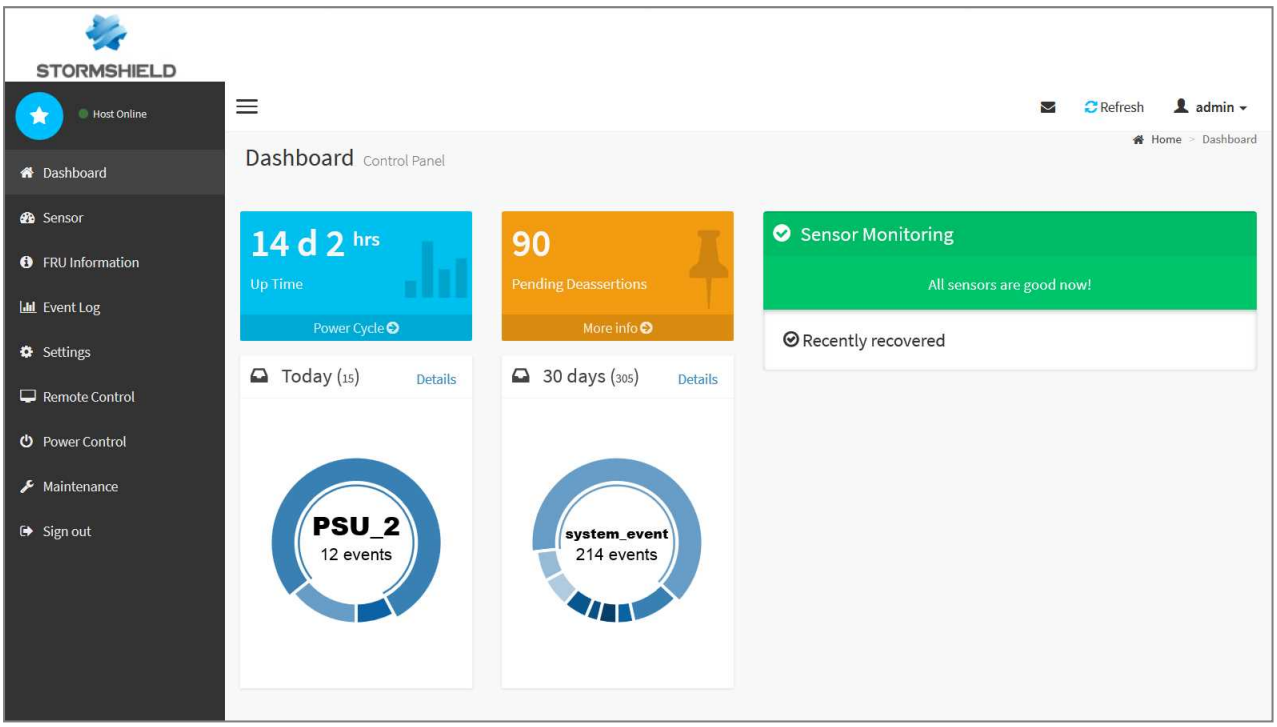
Plug the network cable into the dedicated network interface on the front of the appliance.

Launch your browser and connect to the dedicated interface by entering the address: http://<ip_if_ipmi>.
If an address has not yet been configured, the default IP address of the IPMI interface will be 192.168.0.100/24



The login and password are “admin” by default.

The dashboard of the web interface will look like this:



IMPORTANT

Change the “admin” administration password immediately. You will be asked to change it during the initial connection. You are also advised to place the IPMI interface on a dedicated administration network.

documentation@stormshield.eu