GUIDE

STORMSHIELD NETWORK SECURITY

PRODUCT PRESENTATION AND INSTALLATION 2016

SN Range

Date	Version	Details
August 2014	V1.0	Creation
November 2014	V1.1	Update
May 2015	V1.2	Update (SN910)
October 2015	V1.3	Update (SN510 and SN710)
January 2016	V1.4	Update (Stormshield GCU and UL)
May 2016	V1.5	Update (SNi40)
December 2020	V1.6	Update (Conditions of use)

Reference: sns-en-SNrange_installation_guide-2016

Table of contents

FOREWORD

You are strongly advised to read this whole document before installing a Stormshield Network Firewall.

This installation guide presents the **Stormshield Network range** marketed by Stormshield. This guide explains how to conduct the physical installation needed for integrating an appliance into your network architecture. It also provides the necessary details for adding transceivers and network modules to SN710, SN900, SN910, SN2000, SN3000, SN6000 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 at

http://documentation.stormshield.eu

Alternatively, you can download a document that contains the full help file from **the Document Base,** accessible from **your Secure area** (please refer to the chapter DOCUMENTATION AND ASSISTANCE).

Products concerned

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000, SN6000 and SNi40.

General conditions of use and user license

To view the current version of the General conditions of use and User license or to access translated versions, please go to the DOCUMENT BASE section in your Secure area.

(version 1.0 - January 2016)

STORMSHIELD NETWORK SECURITY GENERAL CONDITIONS OF USE AND USER LICENSE

Preamble

These conditions (points 1-8) are intended to define the terms and conditions applicable to the use of the Stormshield Network Security hardware solution(s) (hereinafter the "Product(s)") by the Customer.

These Conditions of Use apply to the range of Products distributed by Stormshield and their possible modifications and updates.

By opening the packaging of the Product(s), installing the administration software and/or registering the Product(s), the Customer acknowledges full acceptance of these General Conditions of Use and the User License for the Product(s).

1. Contractual documents

These Conditions, supplemented by the Stormshield General Sales Terms and Conditions and the Technical Support Charter, define the scope of the obligations that exist between Stormshield and the Customer. They supersede any prior oral or written commitment that may be contradictory pertaining to the subject of the Conditions.

These Conditions have been drafted by taking into account the current state of Stormshield technology at the time of these were written.

However, Stormshield applies a policy of ongoing development in order to continuously upgrade the Products to better protect Customers. Therefore, these Conditions of Use may become obsolete. Accordingly, Stormshield disclaims any liability for inaccuracies that may appear in this document and the damage that could result from such inaccuracies.

Stormshield reserves the right:

- to make changes and improvements to any Product described in this document, without any prior notice
- to modify or replace these Conditions at any time

2. Warranties and Liability

1. As of the date of activation of the Product(s), notwithstanding any legal warranty available to the Client, Stormshield guarantees the hardware of the Product(s) against defects (parts and labor) for a period of twelve (12) months.
   As of the date of activation of the Product(s), and unless a maintenance contract has been signed, Stormshield only guarantees the software of the Product(s), hereinafter referred to as "the Software", for a period of ninety (90) days against serious defects and malfunctions compared to the manual as it exists on the date of delivery and exclusively in environments that conform to the prerequisites.
   In case of hardware and/or Software defects, Stormshield will exercise its discretion to:
   - Either repair,
   - Or replace the Product.

   Beyond the ninety-day (90) Software warranty period and without signing a maintenance contract, the Product(s) is (are) provided "as is" without any kind of warranty, either express or implied.
   The signing of a maintenance contract is necessary for the proper functioning of the Product (s), insofar as maintenance enables updating the security Software associated with the Product(s). Without maintenance, the Customer is warned that the security functions of the Product(s) **will not provide protection against the most recent threats.**
   It is advisable to refer to the terms of the maintenance contract in the case where such a contract has been signed.
2. In addition, in the case where the Customer is proven to be at fault, Stormshield shall only be held responsible for repairing the financial consequences of any direct and foreseeable damage resulting from the use of the Product(s).
   The responsibility of Stormshield for any direct damage is limited to the amount received by Stormshield for the purchase of the Product that actually caused the damage.
   In no event can Stormshield be held responsible for damage indirectly related to the use of the Product(s), including any operating losses due to an interruption in service or any other cause, suffered by the Customer or by any other third parties, even if Stormshield has been advised of the possibility of such damage.
   Stormshield can in no way be held responsible for any loss of data or revenue, as well as any particular, incidental, consequential or indirect damage arising from the use of the Product(s) and its associated documentation.
3. The Customer is solely responsible for ensuring that the Product(s) meet(s) his or her needs.
4. Stormshield does not guarantee that the use of the Product(s) can be uninterrupted or free of any errors.

5. Similarly, Stormshield disclaims any liability for improper installation, setup, configuration and/or improper use of the Product(s). Stormshield does not guarantee use by the Customer that does not comply with the prerequisites and conditions of use described herein. The same holds for all the consequences of an action, inaction, error, omission or default attributed to the Customer or any service provider commissioned by the Customer. All of the installation, setup and configuration tasks must be performed by the Customer according to the state of the art and the regulations in force.
   When the Customer or any service provider commissioned by the Customer takes the initiative to download, launch, install or perform any other procedure for updating the Product (s), Stormshield cannot be responsible for the Customer's failure to activate the updates or for failure to do so by any service provider authorized by the Customer.
   The Customer or any service provider commissioned by the Customer must comply with the requirements of the documentation for the installation of the Product(s), including the safety rules, precautions for installation and the prerequisites for connections that are communicated herein. The Customer shall be held exclusively responsible for any failure to comply with these rules.
6. Furthermore, the Customer shall be held exclusively responsible for any fraudulent or illegal use of the Product (s), including any such use by its agents or service provider commissioned by the Customer, both with regard to that of Stormshield as well as third parties who have suffered damage due to this fact.

3. User license

By this license, Stormshield grants the Customer who has registered the Product the personal, non-exclusive, non-transferable and non-assignable right to use the Product for the duration of subscription.

The Customer may only use the Product(s) in accordance with its documentation. In particular, the license related to the Product(s) is granted for the sole purpose of enabling the Customer to use the Product, and for no other purpose. Thus, the Customer agrees to use the Product(s) according to its intended purpose.

This license applies to updates.

In addition, the Customer agrees not to make any temporary or permanent copy of the Product(s) or instructions associated with the Product by any means whatsoever, as well as any translation, adaptation, arrangement, decompilation or modification, particularly for the purpose of creating similar solutions.

Stormshield guarantees that it holds all the intellectual property rights or the authorizations, assignments or licenses of any rights of third parties, on the Product(s), allowing it to grant the Customer use of said Product(s).

4. Intellectual Property

Patent

The Product(s) include(s) ASQ technology, for which Stormshield holds international patents.

5. Data

1. Some Products enable retrieving and analyzing the history of connections and logs. The data thus analyzed enables monitoring the activity of the internal users and can provide personal information. The laws in force in the Customer's country may impose certain measures such as administrative declarations, for instance. The Customer acknowledges that it is its responsibility to comply with the legal obligations in force in its own country.
2. Certain Products provide data encryption mechanisms, the use of which may be prohibited or restricted by the laws in force in the Customer's country. The Customer acknowledges that it has a responsibility to comply with the legal obligations applicable for this type of device.
3. Stormshield disclaims all liability for any use of the Product(s) which does not comply with the local laws of the Customer's country. Stormshield cannot be responsible for the Customer's failure to comply with the law.
4. In general, the Customer guarantees Stormshield that it has met all of its obligations in terms of its national laws and with regard to personal data, and that, where appropriate, it has informed the physical individuals concerned by the use made of said personal data. As such, the Customer guarantees Stormshield against any claims or complaints from a person whose personal data are replicated and communicated to Stormshield.
5. In no event shall Stormshield be held responsible for the quality, integrity, completeness and accuracy of the data provided by the Customer, nor by the content and data that may be available on the Product(s).

6. Force majeure

Neither party may be held liable for a breach of any of its obligations, if such breach is due to any of the following: a government decision, including any withdrawal or suspension of authorizations whatsoever, a full or partial internal or external strike at the company, a fire, a natural disaster, a state of war, a total or partial interruption or blockage of telecommunication or electrical networks, an act of computer hacking or, in general, any other event of force majeure as defined by the courts.

The party affected by the event shall immediately inform the other party of its inability to render its service. The suspension of obligations or delay shall in no case be a cause of liability for non-performance of the obligation in question, or result in the payment of damages or late penalties.

7. Exporting

Stormshield informs that the Products may contain technology and Software subject to US and EU laws on the control of exports, as well as subject to the laws of the country where the Products are delivered or used. In accordance with these laws, the Products may not be sold, leased or transferred to users or countries subject to restriction. The Retailer, Customer, or any other service provider commissioned by the Customer agrees to abide by and comply with these laws.

The Products fall into the category of dual-use Products, which means that they can be used in a civilian or military context. As dual-use Products, they are subject to (EU) Regulation No. 428/2009 of the European Council on May 5, 2009, amended by EU Regulation No. 1232/2011 and Regulation No. 388/2012 of the European Parliament and the European Council, respectively, on November 16, 2011 and April 19, 2012.

In order to comply with the international obligations of the European Union as well as those of its member states, the export of dual-use goods is subject to control and authorization.

Stormshield has taken all the steps required by the French authorities to obtain the export licenses and authorizations for each country to which it exports. This means that Stormshield is allowed to export its Products, but that does not mean that a third party and/or Stormshield partner can export Products to the recipient countries indicated in the export licenses granted to Stormshield only.

Any Distributor, Retailer or other Stormshield Partner, regardless of the name given to it, is warned that if it exports Products outside the European Union, it must file its own requests with the competent authorities in order to obtain an export license. If a Product has been exported outside the EU without authorization, Stormshield recommends that the Distributor, Retailer, Partner or other party concerned immediately contact the competent authority in order to regularize the situation.

Due to the nature of the Products, cryptology processes are implemented. Stormshield has obtained the required authorizations. It is the responsibility of the Distributor, Retailer, Partner or other to proceed with all statutory and/or regulatory formalities and procedures locally applicable to the Products. Stormshield agrees to provide the information and assistance that may be reasonably required for the guarantees necessary in order to obtain these authorizations.

8. Applicable Law - Assignment of Jurisdiction

ANY DISPUTE RELATING TO ALLEGED DEFECTS IN THE SOFTWARE AND/OR THE PRODUCT(S) AND/OR RELATING TO THE INTERPRETATION OR THE APPLICATION OF THE PRESENT GENERAL CONDITIONS OF USE AND USER LICENSE MUST BE SUBMITTED TO THE JURISDICTION OF THE COURTS IN THE PLACE WHERE THE STORMSHIELD HEADQUARTERS ARE LOCATED, AND FRENCH LAW IS EXCLUSIVELY APPLICABLE.

Recommendations on the operating environment

DEFINITION

The common criteria evaluate (on an Evaluation Assurance Level or EAL scale of 1 to 7) 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, putting into service, updates).

Introduction

The installation of a Firewall often comes within the scope of setting up a global security policy. To ensure optimal protection of your assets, resources or information, it is not only a matter of installing a Firewall between your network and the Internet. This is namely because the majority of attacks come from the inside (accidents, disgruntled employees, dismissed employee having retained internal access, etc.). And one would also agree that installing a steel security door defeats its purpose when the walls are made of paper.

Backed by the Common Criteria, Stormshield Network advises taking into consideration the recommendations of use for the Administration Suite and Firewall product stated below. These recommendations set out the usage requirements by which to abide in order to ensure that your Firewall operates within the context of the common criteria certification.

For further information on Common Criteria compliance, please go to: http://documentation.stormshield.eu/common-criteria.html

Security watch

Please regularly check Stormshield security advisories published on https://advisories.stomshield.eu.

Always update your firewall if it allows fixing a security flaw. 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. The wizard will prompt the user to change his password during the initial installation, in the Administration of the appliance window. 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 UserGuide, in the chapter Welcome, under the section User awareness, sub- section User password management, available at: http://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.
- He is in charge of defining the profiles of other administrators,
- All access to the premises where the appliances are stored has to be under his supervision, regardless of whether the access is due to an intervention on the appliance or on other equipment. He is responsible for all interventions carried out on appliances.

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 different networks on which the control policy for traffic has to 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 treatment capacities of each firewall-VPN appliance installed in the network architecture.

Regulations

WEEE (Waste Electrical and Electronic Equipment) directive
All Stormshield Network products that are subject to the WEEE directive will be 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 regards 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 recycling program of Stormshield Network Firewalls (WEEE), please refer to:
https://www.stormshield.eu/about/recycling/

Certifications

CE

FC
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 thirteen products:

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000, SN6000 and SNi40.

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 the multiplication of high-speed VPN access.

The SN Firewall allows the definition of incoming or outgoing access control rules. Its concept is simple: any incoming or outgoing transmission passing through the Firewall is monitored, authorized or denied 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 allows detecting and blocking hacking attempts in real time illegal packets, denial of service attempts, anomalies in a connection, port scans, buffer overflows, etc.

In the event of an intrusion attempt, depending on the instructions given in the security policy, the SN Firewall blocks the transmission, generates an alarm and stores the information linked to the packet which had set off the alarm. As such, you would be able to analyze the attack and trace its source.

The SN Firewall not only allows preventing, or restricting to just certain services, incoming connections on your network, but also allows monitoring the use of the Internet by your internal users (HTTP, FTP, SMTP...). You may 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.

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

Through SN Activity Reports, available from a dedicated portal, you can view how Internet access is used, the various attacks that your Firewall has blocked and the vulnerable hosts in your network. Furthermore, numerous interactions allow you to directly take action on the configuration of your Firewall.

Stormshield Network Administration Suite

SN GLOBAL ADMINISTRATION allows you to safely update several Firewalls locally or remotely. You can administer up to five appliances simultaneously without an additional license.

SN REAL-TIME MONITOR is the application that analyzes security events in real time and allows you to view your Firewall's activity simply. The dashboard in particular allows you to monitor all your SN Firewalls. This application is an excellent tool for the security of your network thanks to the wide array of information displayed.

The SN Firewall is also equipped with advanced tracking features. In the event of an intrusion attempt, the network administrator can access all the data sent before the attacks and understand how it had been prepared. SN EVENT REPORTER gives a graphic view and detailed analysis of logs generated on the Firewall.

UPON RECEIVING YOUR FIREWALL

Several security mechanisms have been implemented to guarantee the integrity of the product that you receive. They also validate the fact that your product has not been tampered with. **Check them carefully in order to avoid disputes later regarding the application of the warranty.**

Any abnormality must be reported within 48 hours from receipt of the product, to your reseller if your product is not as per order.

Integrity of the product

Seals and labels on the packaging

Every Firewall is delivered in a cardboard box sealed by one or two warranty seals. On this packaging, there is a label indicating information identifying the product it contains and its version. Check that this information corresponds to your order.

Seals

Every Firewall is delivered in a cardboard box on which one seal (SN150, SN510, SN710, SN910, SN2000 and SN3000) or two "STORMSHIELD QUALITY SEAL" seals affixed.

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 corresponds to your order. You can also check whether the version installed has been certified.

Figure 2: Identification labels

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: .
SN6000 warranty label

Figure 4:
Warranty label for other models

Serial number label

This label, pasted on the back panel of the product (on the underside for SN150, SN2000, SN3000 and SN6000 models, and on the side for SNi40), displays the serial number and the password for registering your product.

Figure 5: 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 the underside of your product, provides information relating to the Firewall, such as the *part number* and the product's electrical power characteristics.

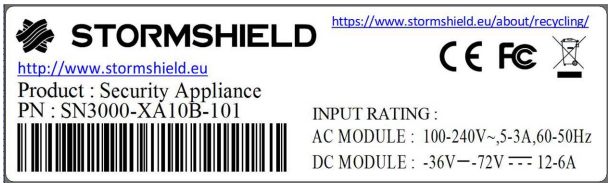


Figure 6: Product label

Contents of the packaging

Keep the cardboard packaging in a safe place in case you need it later for transporting the Firewall. It has been designed to give your SN Firewall optimum protection (shock resistance, etc.).

Upon delivery, check that the following have been included in the packaging:

- Your Stormshield Network Firewall,
- A power cord (two for SN3000 and SN6000 appliances)

- A power adapter (SN150, SN200 and SN300),
- A 6-pole screw connector (SNi40),
- A Category-5e RJ45 crossover cable,
- A DB9F serial cable (SN200, SN300, SN500, SN700, SN900 and SNi40), or an RJ45 to DB9F serial cable (SN510, SN710, SN910, SN2000 and SN3000) or an "A to B" USB cable (SN150).

For SN500, SN510, SN700, SN710, SN900 and SN910 models, the packaging should also contain:

- A set of brackets and screws for mounting the Firewall in a rack,
- 4 non-slip rubber feet.

For SN510, SN710, SN910, SN2000 and SN3000 models, the brackets are mounted.

For SN2000, SN3000 and SN6000 models, the packaging should also contain a set of rails and screws for mounting the Firewall in a rack.

The SNi40 model is equipped with a 35mm DIN Rail mounting bracket (EN50022 standard).

NOTE
As SN500, SN510, SN700, SN710, SN900 and SN910 Firewalls can be installed on a desk or in a rack, their non-slip rubber feet are delivered separately. Only products that cannot be racked (SN150, SN200 and SN300) 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 the set of rails (SN2000, SN3000 and SN6000).

If any element is missing, contact your distributor immediately.

SAFETY RULES

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

All models except SNi40

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 48VDC power supply (SN3000 and SN6000)

Special considerations for equipments 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 rated minimum 16 AWG or 1.5 mm² yellow/green wire.
- The equipment shall be connected to the DC mains supply with an approved switch or breaker.
- Only wires rated minimum 16AWG or 1.5 mm² 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
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 then 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 SN500, SN510, SN700, SN710, SN900 and SN910 models. Please refer to the chapter 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 chapter 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.

SNi40 model

Before plugging in any devices

- Ensure that neither your Stormshield product nor its accessories are damaged.
- Ensure that the input rating of your Firewall, printed on the product label, is compatible with the characteristics of your DC mains supply.
- The chassis of your product must be connected to a protective earth circuit, using rated minimum 16 AWG or 1 mm² 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 is turned off, and that all power supply connections are 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 equipement must be installed by a qualified electrician.
- 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 1mm² 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.

Precautions for assembly in a cabinet

- **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, therefore do not neglect it – install it in the best way possible, under the best 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 SNi40)

The Stormshield Network Firewall has been 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 SN500, SN510, SN700, SN710, SN900 and SN910 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 has to be installed in compliance with the state of the art corresponding to the practical terms of secure installation, namely: in a protected office or other premises with limited access. In order to guarantee the integrity of the product and to avoid compromising the security of your installation, all unauthorized access to the Firewall has to be avoided.

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

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.

SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000 and SN3000 models:

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
5° to 40°C (41° to 104°F)	20% to 90% 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

SN6000 Model:

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
10° to 35°C (50° to 95°F)	8% to 90% non-condensing	-30° to 65°C (-22° to 149°F)	5% to 95% at 60°C (140°F) non-condensing

IMPORTANT
Avoid in particular direct exposure to sunlight. Always keep an 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 (SNi40 model)

The SNi40 firewall has been designed to run continuously in a technical room.

WARNING
The Firewall has to be installed in compliance with the state of the art corresponding to the practical terms of secure installation, namely: in protected premises with limited access. In order to guarantee the integrity of the product and to avoid compromising the security of your installation, all unauthorized access to the Firewall has to be avoided.

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

Your Stormshield 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. The ideal ambient temperature is around 25°C. The table below sets out the operational temperature, storage temperature and humidity level.

Operating temperature	Relative humidity operating (%)	Storage temperature	Relative humidity storage (%)
-40° to 75°C (-40° to 167°F)	0% to 90% non-condensing	-40° to 85°C (-40° to 185°F)	5% to 95% non-condensing

IMPORTANT
Avoid in particular direct exposure to sunlight. Always keep an adequate distance around the appliance 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 SN3000 and SN6000 models are equipped with redundant power supplies, plugging them into 2 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 SN3000 and SN6000 models, 48V DC power supply modules may be provided separately upon request.

For SN150, SN200 and SN300 models, insert 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 SN500, SN510, SN700, SN710, SN900, SN910 and SN2000 models, insert the connector 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 SN3000 and SN6000 models, insert the connector of both power cords provided into both power sockets located on the rear panel of the Firewall. Next, plug in the other ends of the power cords into appropriate mains sockets.

Connecting to a 24VDC power supply unit (SNi40)

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. The SNi40 model is equipped with a redundant power supply unit, so you are advised to connect it to 2 independent sources of power.

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

NOTE
An AC power adapter may be ordered separately.

Connecting to the network

All models are fitted with RJ45 Gigabit Ethernet ports by default.

The SN900, SN910 and SNi40 models offer by default, two SFP sockets, allowing the insertion of **SFP** transceivers, provided as an option.

SN710, SN910, SN2000, SN3000 and SN6000 models also offer one or several slots for different types of extension modules: optional network modules that allow either adding RJ45 Gigabit Ethernet ports or inserting SFP or SFP+ transceivers depending on the module ordered. A slot is available on SN710 and SN910 models, two on SN2000 and SN3000 appliances, and seven on the SN6000.

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

For the choice of the type of network cable according to the network port and the selected connectors, see the chapters EXTENSION MODULES (SN710, SN910, SN2000, SN3000, SN6000) and Fiber Ethernet connectors.

INSTALLATION IN A 19" RACK AND CABINET

All Stormshield Network appliances can be installed in 19-inch cabinets (except SNi40). 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 SN150, SN200 and SN300 models. Two SN150, SN200 or SN300 Firewalls can be installed on the same shelf.

SN500, SN700, SN900 and SN910 appliances are sold with an installation kit containing brackets. On SN510, SN710, SN910, SN2000 and SN3000 models, the brackets are mounted by default. SN2000, SN3000 and SN6000 appliances are sold with a set of rails.

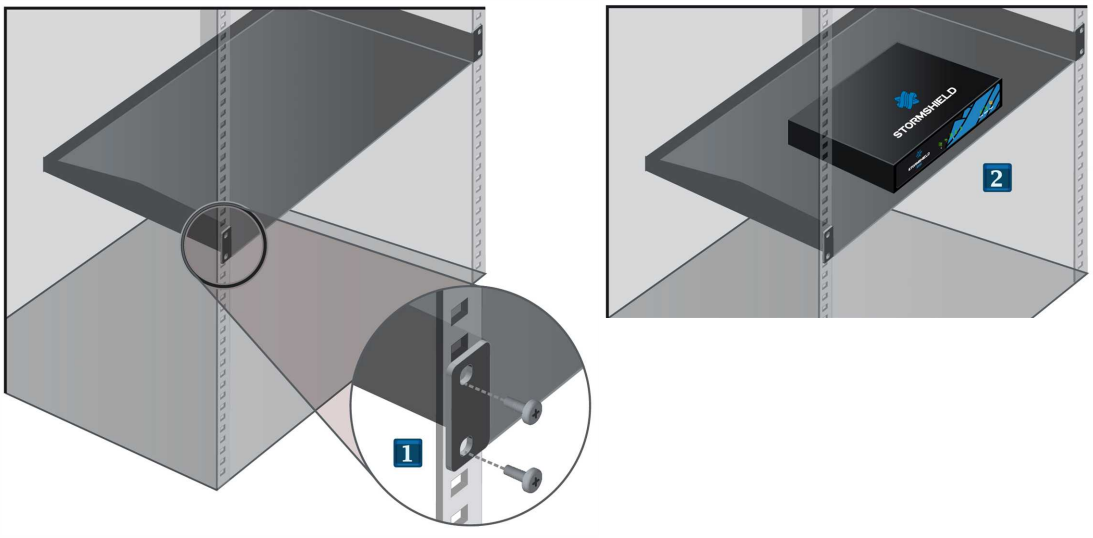
REMINDER
Ensure that the cabinet complies with temperature and humidity conditions indicated in the section Conditions of use.

NOTE
The SN150 model can also be installed vertically (screws and fasteners not provided).

Installing SN150, SN200 and SN300 models in a 19" rack mount shelf

In this non-standard installation, allow a height of more than 1U due to the thickness of the shelf and the presence of rubber feet below the appliance. 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).



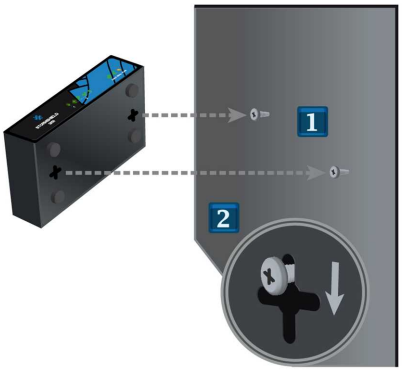
WARNING
If you are installing two Firewalls on the same rack mount shelf, you will need to leave enough space between the Firewalls to avoid obstructing the flow of air from the sides.

Attaching the SN150 model appliance to the wall

The SN150 model can also be fastened vertically with screws and fasteners (not provided with the appliance). 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:

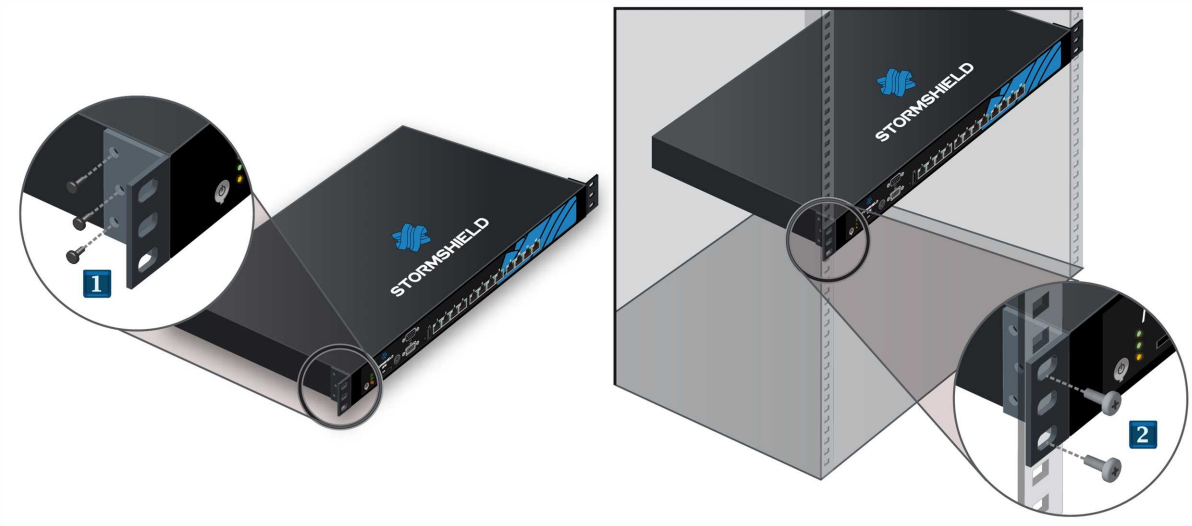
1. Place against the wall the 2 screws aligned horizontally, leaving a space of 12cm (center to center) between them and letting them protrude slightly to take into account the thickness of the non-slip rubber feet.
2. Once the screws have been drilled into the wall, you can insert the screw heads into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



Installing SN500, SN700 and SN900 models in a 19" cabinet

The minimum vertical space needed for installing an SN Firewall is 1U. The procedure is as follows:

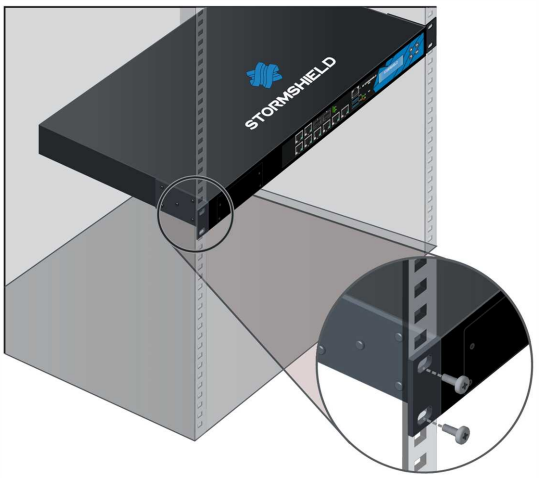
1. Screw the brackets to the sides of the Firewall.
2. Once the brackets have been installed, you can fasten the Firewall to the vertical rails located at the front of your cabinet using screws and the caged nuts (not provided with the appliance).



Installing SN510, SN710 and SN910 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 SN2000, SN3000 and SN6000 models in a 19" cabinet

The minimum vertical space needed for installing an SN2000 or SN3000 Firewall is 1U and for installing an SN6000, this space is 2U. The procedures for mounting lateral rails and installing appliances in racks are described in **SN2000-SN3000_rack mounting** and SN6000 _rack mounting. These documents are delivered with the SN2000/3000 and SN6000 products and are available in the Document base section in your Secure area (*Product > Stormshield Network Firewall > User Guide > Hardware*).

Installing an SNi40 model appliance on a DIN rail

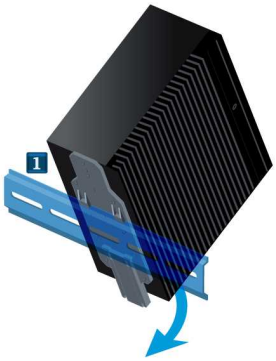
To install the appliance in a cabinet, the SNi40 model is equipped with a 35mm DIN Rail mounting bracket (EN50022 standard).

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

The SNi40 model has to be installed vertically.



The procedure is as follows:

1. Hold the SNi40 facing the DIN rail, then insert the upper part of the rail intothe notch in mounting bracket. Straighten up the SNi40.
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.

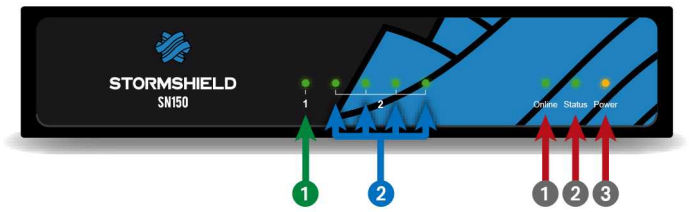
NOTE
For more information on Ethernet interfaces, please refer to the section Connecting to the network in the chapter INSTALLATION PRECAUTIONS.

SN150 model

The SN150 firewall is fanless. The product comes with an external power adapter.

LEDs Front panel:

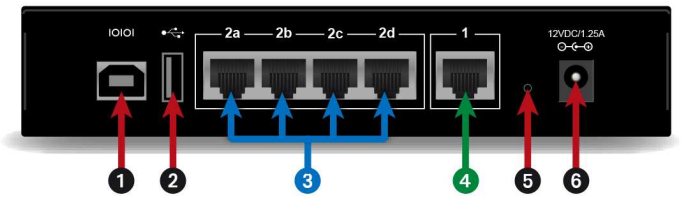
This model has its LEDs on the front panel as shown below:



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

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

Rear panel: connectors



The connectors on the SN150 model are located on the rear panel.

1. **The USB port** allows accessing 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. **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 SN150 model offers five 1GbE ports:

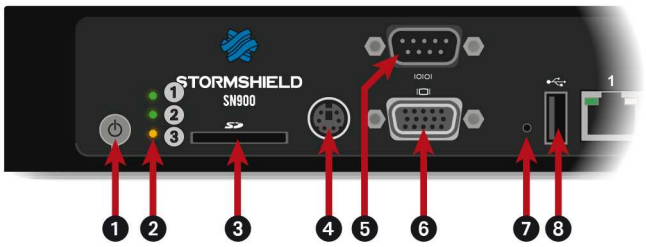
3. The first zone is defined by default in **INTERNAL 2 (IN)** mode. It is made up of 4 switched ports.
4. The second zone is the **EXTERNAL 1 (OUT)** interface, in external mode by default. It makes up the zone that is needed for connecting to the internet.
5. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
6. Plugging in the mains adapter automatically starts this product.

** 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*

SN200, SN300, SN500, SN700 and SN900 models

Front panel: connectors and LEDs

The main connectors on these models are located on the front panel.



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

1. The **Power button** allows switching the Firewall on or off.
2. The *Power, Status* and *Online* (from bottom to top) LEDs.
3. This is the slot for the **SD card*.**
4. **The mini-din PS2 port** allows connecting a keyboard.
5. **The serial port** allows accessing 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).
6. **The VGA port** allows connecting a monitor.
7. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
8. **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.

** The recommended type of SD card is at least Class 6, SDHC standard.*

SN200 model

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

The SN200 multi-function Firewall is fanless.

The product comes with an external power adapter.

The SN200 model holds five 1GbE ports spread out in three zones:

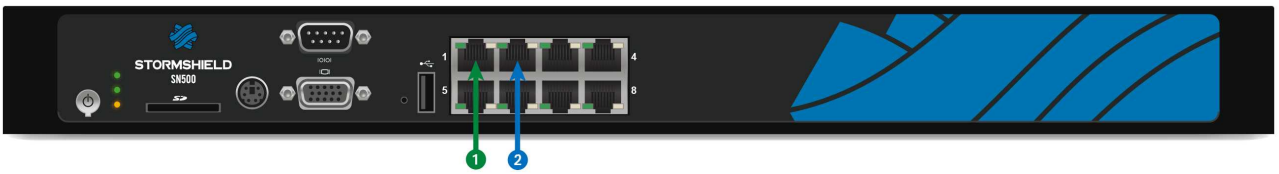
- The first zone is defined by default in external (OUT) mode. It makes up the zone that is needed for connecting to the internet.
- The second zone is by default identified in internal mode (IN). It is made up of 2 switched ports,
- The third zone allows you to define a third protection sector (DMZ). It is made up of 2 switched ports.

SN300 model

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

The SN300 multi-function Firewall is fitted with a very quiet fan. The noise generated by the appliance, expressed in sound power levels, does not exceed 22dB(A) over the distance of a meter.
The product comes with an external power adapter.
The SN300 model holds eight 1GbE ports.

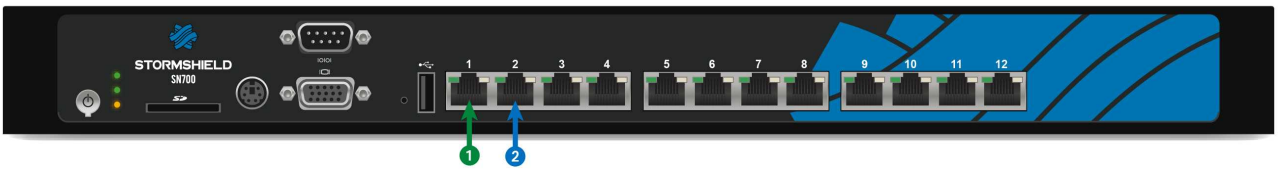
SN500 model



This product has an internal power supply.
The SN500 model holds eight 1GbE ports.

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

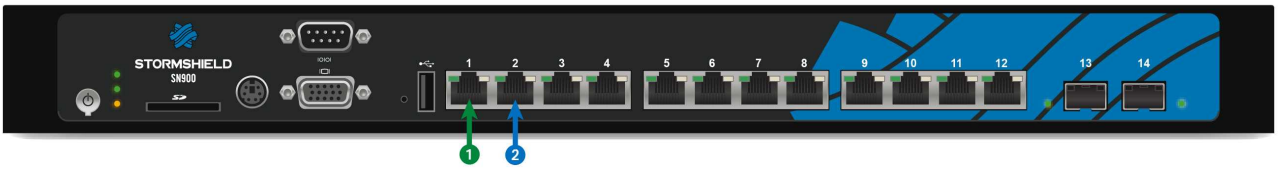
SN700 model



This model is fitted with a multi-core CPU, making it possible to increase processing power.
This product has an internal power supply.
The SN700 model holds twelve 1GbE ports.

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

SN900 model



This model is fitted with a multi-core CPU, making it possible to increase processing power.
This product has an internal power supply.

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

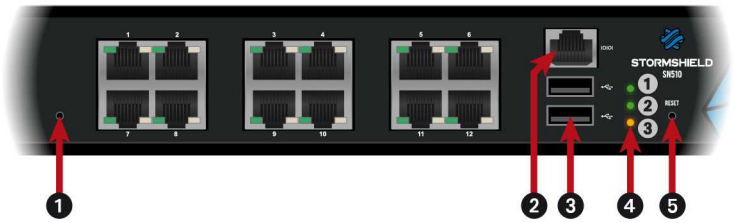
The SN900 model holds 12 1GbE ports and 2 SFP sockets for adding 1GbE transceivers.
Specifications of Stormshield Network-approved transceivers are set out in chapter Fiber Ethernet connectors.

Rear panel: connectors

The socket for the power cord or the power adapter is located on the rear panel of the product. The rear panel has two additional USB ports that allow access to the same features as USB ports located on the front panel.

SN510 and SN710 models

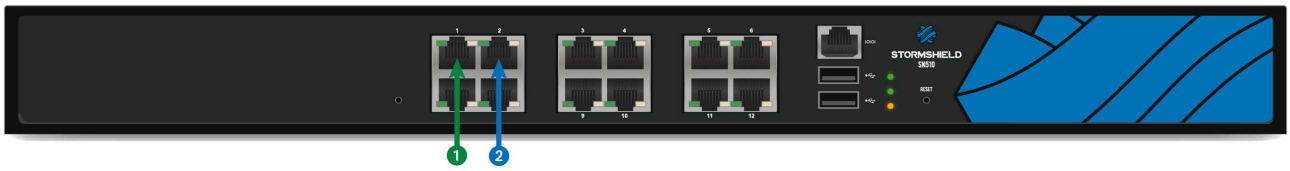
Front panel: connectors and LEDs



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

1. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
2. **The serial port** allows accessing 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).
3. **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.
4. The *Power, Status* and *Online* (from bottom to top) LEDs.
5. **The Reset button:** electrically resets the Firewall.

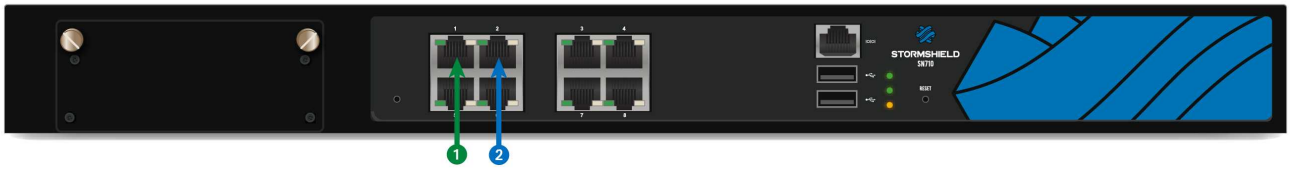
SN510 model



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 holds twelve 1GbE 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

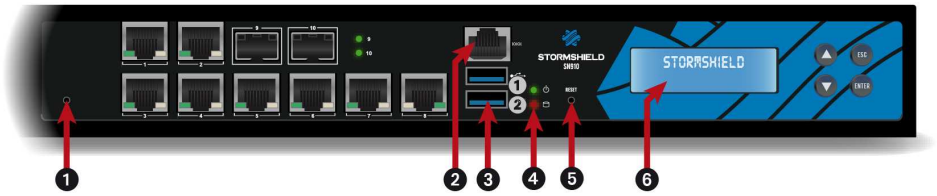
This product has an internal power supply.
The SN710 model holds eight 1GbE ports. It allows the addition of one extension module with RJ45 (1GbE) or fiber (1GbE or 10GbE) connectors.
Specifications of Stormshield Network-approved extension modules and transceivers are set out in chapters Extension modules (SN710, N910, SN2000, SN3000, SN6000) 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.

SN910 model

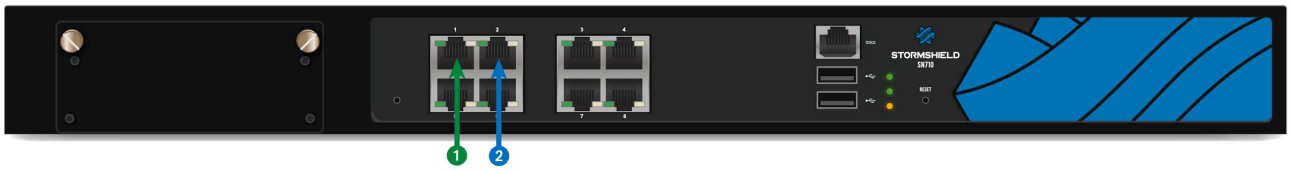
Front panel: connectors and LEDs



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** allows accessing 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:** electrically resets the Firewall.
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 1GbE ports and 2 SFP sockets for adding 1GbE transceivers. It allows the addition of one extension module with RJ45 (1GbE) or fiber (1GbE or 10GbE) connectors.

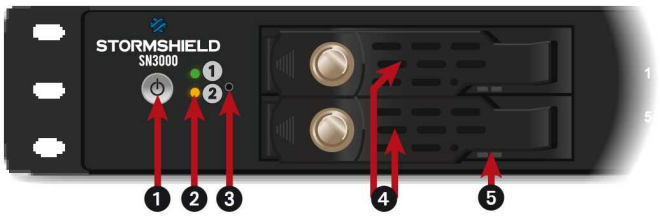
Specifications of Stormshield Network-approved extension modules and transceivers are set out in chapters Extension modules (SN710, N910, SN2000, SN3000, SN6000) and Fiber Ethernet connectors.

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.

SN2000 and SN3000 models

Front panel: connectors and LEDs



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

1. The **Power button** allows switching the Firewall on or off.
2. The *Power* and *Online* LEDs (from bottom to top).
3. This is the button for **resetting the appliance** to its factory settings (*defaultconfig*).
4. **SSD racks for log storage** (1 on SN2000 models, 2 in RAID 1 on SN3000 models).
5. **The LEDs on SSD racks** confirm whether the SSD has been accessed (blue LED on the right) and installed (green LED on the left).

SN2000 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 and a removable SSD.

The SN2000 model offers ten 1GbE ports and allows the addition of two extension modules with RJ45 (1GbE) or fiber (1GbE or 10GbE) connectors.
Specifications of Stormshield Network-approved extension modules and transceivers are set out in chapters Extension modules (SN710, N910, SN2000, SN3000, SN6000) and Fiber Ethernet connectors.

SN3000 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

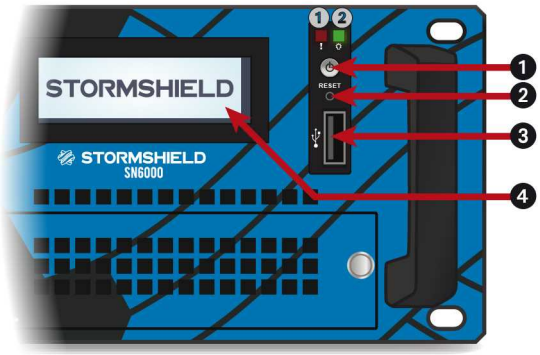
The SN3000 model offers ten 1GbE ports and allows the addition of two extension modules with RJ45 (1GbE) or fiber (1GbE or 10GbE) connectors.
Specifications of Stormshield Network-approved extension modules and transceivers are set out in chapters Extension modules (SN710, N910, SN2000, SN3000, SN6000) and Fiber Ethernet connectors.

Rear panel: connectors

1. Two ports dedicated to the management of the appliance or a High Availability configuration (MGMT1 and MGMT2)
2. **The serial port** allows accessing 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. **Four 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 VGA port** allows connecting a monitor.
5. **The mini-din PS2 port** allows connecting a keyboard.
6. The product's on/off switch (SN2000 only).
7. A mains socket (SN2000) or two mains sockets (SN3000) for redundant power supplies.

SN6000 model

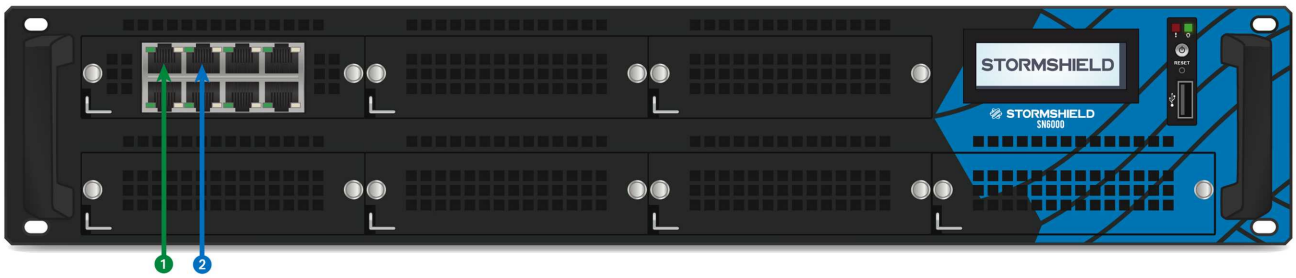
Front panel: connectors and LEDs



1. ***Hardware alert* LED (red):** indicates overheating or hardware failure (e.g.: fans)
2. **Green *Power* LED:** indicates whether the Firewall is powered up.

1. The **Power button** allows switching the Firewall on or off.
2. **The Reset button:** electrically resets the Firewall.
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. **LCD screen**: indicates the version of the firmware installed, the active partition, the serial number of the product, the IP address of the IPMI as well as the HA status (if enabled), RAID and power supplies.

Description



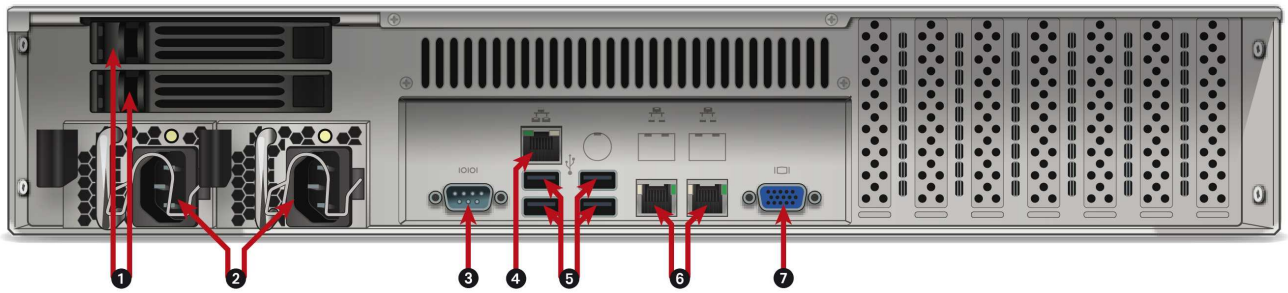
This model is fitted with two multi-core CPUs, making it possible to increase processing power. This product has redundant internal power supplies. Two removable SSDs are installed in a RAID configuration.

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

The SN6000 model offers ten 1GbE ports by default and allows the replacement and addition of seven extension modules with RJ45 (1GbE) or fiber (1GbE or 10GbE) connectors.

Specifications of Stormshield Network-approved extension modules and transceivers are set out in chapters Extension modules (SN710, N910, SN2000, SN3000, SN6000) and Fiber Ethernet connectors.

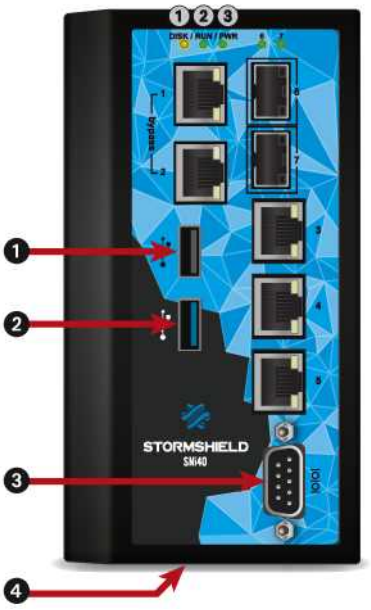
Rear panel: connectors



1. **SSD racks for log storage** (2 in RAID 1). The LEDs on SSD racks confirm whether the SSD has been accessed (bottom blue LED) and installed (top green LED).
2. **Two mains sockets** for redundant power supplies.
3. **The serial port** allows accessing the product in console mode; it is possible to connect the Firewall directly from a computer. The default baud rate on this model is 9600 baud (8N1).
4. A network port dedicated to the administration of the appliance via IPMI. Please refer to the appendix for information on CONFIGURATION AND ADMINISTRATION VIA IPMI (SN6000).
5. **Four USB 2.0 ports** that can be used for secure configurations or upgrades. You may also plug in a USB key, USB keyboard or approved USB modem.
6. Two network ports dedicated to the management of the appliance or a High Availability configuration (from left to right: MGMT1 and MGMT2).
7. **The VGA port** allows connecting a monitor.

SNi40 model

Connectors and LEDs



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

1. **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.
2. **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.
3. **The serial port** allows accessing 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).
4. **The Reset button** (underside): electrically resets the Firewall.

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 24VDC redundant power supply, the 6-Pole screw terminal connector provided allows a connection to 2 independent sources of power.

The SNi40 model holds 5 1GbE ports and 2 SFP sockets for adding 1GbE transceivers.

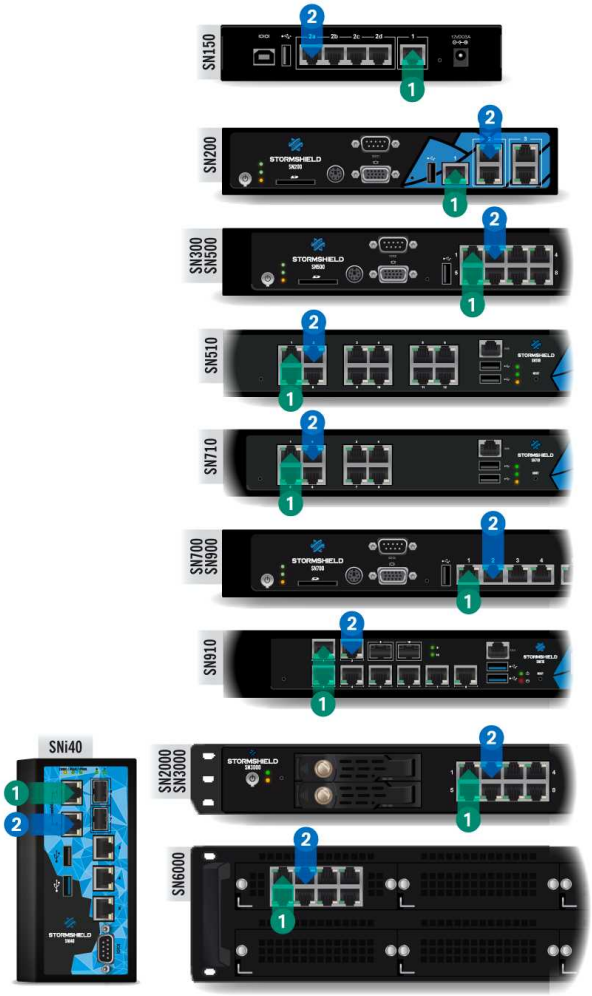
Specifications of Stormshield Network-approved transceivers are set out in the chapters Optional Fiber Ethernet Transceivers and Fiber Ethernet connectors.

NETWORK CONNECTORS

RJ45 Ethernet connectors

These interfaces have to be connected to other network appliances with an RJ45 Ethernet cable.

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



Connectors

The Ethernet (Gigabit) 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, SN2000, SN3000 and SN6000 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 chapter INITIAL CONNECTION TO THE PRODUCT.

LEDs of interfaces

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

SN150 model

Name	Color	State	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.

SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000 and SN3000 models:

Name	Color	State	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 1 Gbps.
	Green	On	Media speed negotiated at 100 Mbps.
		Off	Media speed negotiated at 10 Mbps.

SN6000 model

Front panel

Name	Color	State	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 1 Gbps.
	Green	On	Media speed negotiated at 100 Mbps.
		Off	Media speed negotiated at 10 Mbps.

Rear panel

IPMI

Name	Color	State	Status
Left LED LINK	Green	On	Link established between the Ethernet port and the connected appliance (100 Mbps).
		Off	Ethernet port switched off or link not established with the connected appliance.
Right LED ACTIVITY	Yellow	Blinking	The Ethernet port is sending or receiving data. The blinking speed varies according to the volume of traffic.
		Off	Ethernet port switched off or link not established with the connected appliance.

MGMT1/2

Name	Color	State	Status
Right 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.
Left LED SPEED	Yellow	On	Media speed negotiated at 1 Gbps.
	Green	On	Media speed negotiated at 100 Mbps.
		Off	Media speed negotiated at 10 Mbps.

SNi40 model

Name	Color	State	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 1 Gbps.
	Green	On	Media speed negotiated at 100 Mbps.
		Off	Media speed negotiated at 10 Mbps.

Fiber Ethernet connectors

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

- SN900: ports 13 and 14,
- SN910: ports 9 and 10,
- SNi40: ports 6 and 7,

On SN710, SN910, SN2000, SN3000 and SN6000 models, fiber Ethernet connectors can be added by inserting extension modules.

In both cases it is necessary to install a transceiver. This transceiver is in **SFP** format for **1Gbps** connections or **SFP+** for **1Gbps/10Gbps** connections.

LEDs

The LEDs indicate the following information:

- SN900, SN910 and SNi40 models equipped with SFP transceivers (available by default on fiber Ethernet ports): a green LED will light up when the link is established and blink depending on the volume of traffic.
- SN710, SN910, SN2000 and SN3000 models equipped with 1Gbps extension modules with SFP+ transceivers: a green LED will light up when the link is established and blink depending on the volume of traffic.
- SN6000 model equipped with 1Gbps extension modules with SFP transceivers:

Name	Color/State	Status
Right LED SPEED	Yellow	Media speed negotiated at 1 Gbps.
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.

- SN710, SN910, SN2000, SN3000 and SN6000 models equipped with 10Gbps extension modules with SFP+ transceivers:

Name	Color/State	Status
Right LED SPEED	Blue	Media speed negotiated at 10 Gbps.
	Yellow	Media speed negotiated at 1 Gbps.
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.

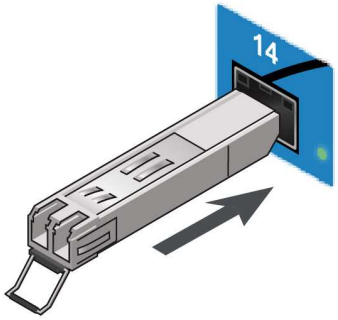
Optional Ethernet fiber transceivers (SN710, SN900, SN910, SN2000, SN3000, SN6000 and SNi40)

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.



NOTE

- SN900, SN910 and SNi40 models offer two sockets for **SFP** transceivers by default.
- Use only Stormshield Network-approved **SFP (1Gbps)** or **SFP+ (1/10Gbps)** transceivers available in the catalogue.
- Only **LC** fiber optic connectors are supported.

Stormshield Network-approved Ethernet transceivers

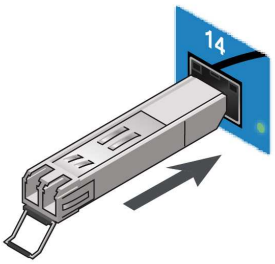
		SN900 and SNi40	SN710, SN910, SN2000, SN3000, and SN6000
	FIBER CONNECTOR		
GIGA - SFP	SFP Transceiver, 1000Base-SX: Requires multi-mode fiber. Maximum typical distance supported (subject to optimum quality): 550m	supported	supported
	SFP Transceiver, 1000Base-LX: Ethernet 1000Base-LX, requires single-mode fiber. Maximum typical distance supported (subject to optimum quality): 10km	supported	supported
10 GIGA - SFP+	SFP+ transceiver, 10GBASE-SR/1000Base-SX: Ethernet 10GBASE-SR/1000Base-SX, requires multi-mode fiber. Maximum typical distance supported (subject to optimum quality): 300m on 10Gbps, 550m on 1Gbps.	not supported	supported
	SFP+ transceiver, 10GBASE-LR/1000Base-LX: Ethernet 10GBASE-LR/1000Base-LX, requires single-mode fiber. Maximum typical distance supported (subject to optimum quality): 10 km	not supported	supported

Installation

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 optic cable corresponding to this transceiver.

IMPORTANT
The 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, SN910, SN2000, SN3000 and SN6000)

The procedure for removing or inserting an extension module on SN710, SN910, SN2000, SN3000 or SN6000 Firewalls takes place in three main steps:

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

NOTE
The extension modules for SN710 / SN910 / SN2000 / SN3000 appliances are not mechanically compatible with those on SN6000 appliances.

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

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

Description of extension modules for SN710, SN910, SN2000, SN3000 and SN6000 appliances

SN710, SN910, SN2000, SN3000 and SN6000 models accept the following extension modules:

- **8-port 1 GbE copper module**
  - RJ45 connectors
  - 1000/100/10Base-T
- **4-port 1 GbE fiber module**
  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).
- **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).

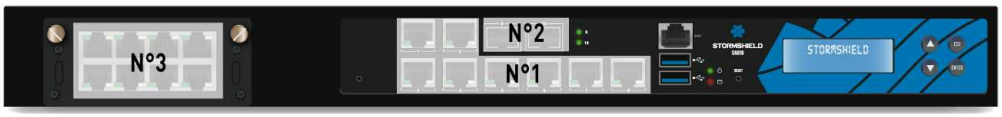
- **2-port 10 GbE fiber module (not available on SN6000)**
  2 SFP+ sockets, supporting the following transceivers:
  - SFP+ fiber transceiver, 10GBase-SR (10Gbps Ethernet, short distance) / 1000BASE-SX (1Gbps Ethernet, short distance).
  - SFP+ fiber transceiver, 10GBase-LR (10Gbps Ethernet, long distance) / 1000BASE-LX (1Gbps Ethernet, long distance).
- **4-port 10 GbE 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).

Sequencing of modules

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

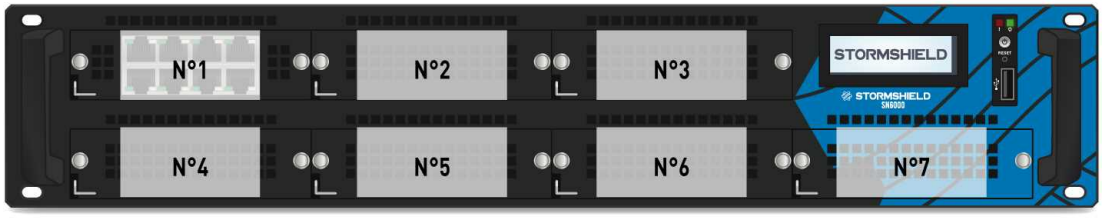
SN710 Model:

SN910 Model:



SN2000 and SN3000 Models:

SN6000 Model:



Procedure for removing/ inserting 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.

Specific instructions on the location of modules are as follows:

- Modules have to be inserted from left to right starting with the top row.
- There must not be any empty slots between two modules in the same row.

Furthermore, on the SN6000 model, in order to enhance your product's performance, you are advised to spread out the network modules over 2 rows, without leaving any empty slots between two modules in the same row. This makes it possible to balance the two CPUs' load. The first row of modules and the 2 network ports located on the rear of the appliance are managed as a priority by the first CPU and the second row by the second CPU.

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 SN710, SN910, SN2000 or SN3000 models

- Using the Power button on the front panel, 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,
- 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.

Extracting an extension module on SN710, SN910, SN2000 or SN3000 models

- Using the Power button on the front panel, 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.

Inserting an extension module on SN6000 models

- Using the Power button on the front panel, 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,

- Unlock and remove the empty module in place by lifting the small catch on the bottom left, while pulling on both handles,
- Insert the extension module all the way in (until you hear a click to indicate that it has been locked),
- Reconnect the Firewall to the power supply,
- Using the Power button on the front panel, start the Firewall.

Extracting an extension module on SN6000 models

- Using the Power button on the front panel, 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,
- Unlock and remove the module in place by lifting the small catch on the bottom left, while pulling on both handles,
- Put back the empty module to be inserted all the way in (until you hear a click to indicate that it has been locked),
- 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 administered through its INTERNAL interface. On all models, this interface is identified by the number 2 (IN).

To obtain the description of the interfaces, refer to the chapter PRESENTATION OF THE SN RANGE.

Requirements

Minimum configuration for administering a Stormshield Network Firewall

Lowest version of the OS (firmware)

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

- **SN150, SN200, SN300, SN500, SN700, SN900, SN2000 and SN3000:** V1.1.0
- **SN510 and SN710:** V1.4.1 in version 1 and V2.2.0 in version 2
- **SN910:** V1.2.3
- **SN6000:** V1.1.1
- **SNi40:** V2.3.4

Web administration interface

The configuration interface on Stormshield Network Firewalls can be accessed via a web browser and benefits from the latest breakthroughs in user friendliness and simplicity of use. It is compatible with the following browsers:

- Internet Explorer 7 and +
- Firefox 3.6 and +

Stormshield Network administration suite

Stormshield Network supports the execution of the Stormshield Network Administration Suite software in the following environments:

- Microsoft Windows 7 and 8,
- Microsoft Windows Server 2008 and 2012.

Preparing the Internet access

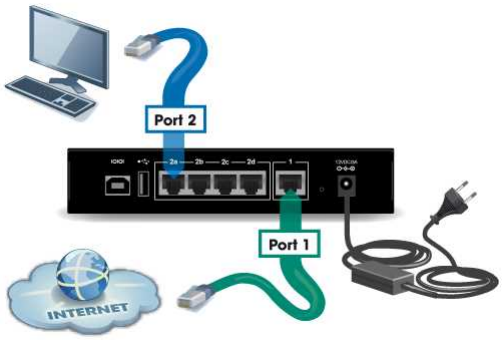
Before installing the SN Firewall, ensure that the devices that connect to the Internet (if the Firewall has to be connected to the Internet) have been appropriately installed and configured.

Connections

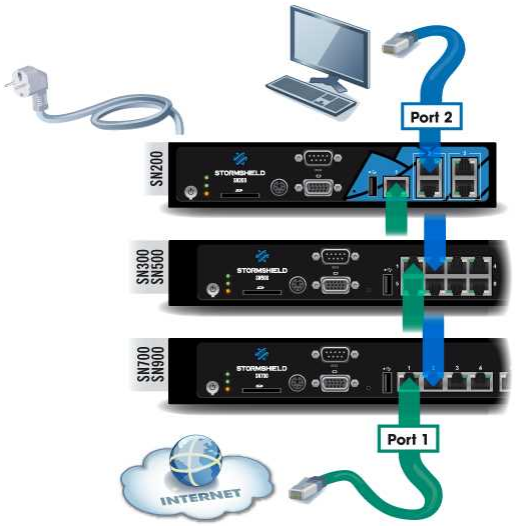
Connect the network ports as follows:

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

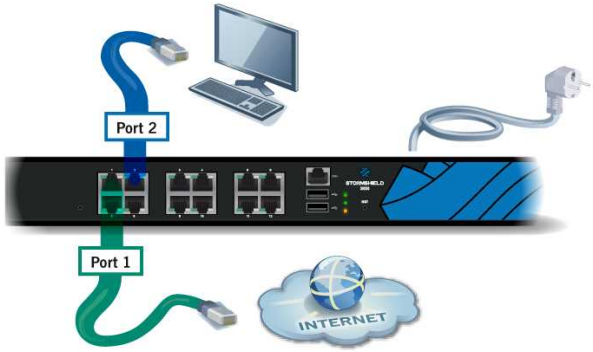
The client workstation can either be linked directly to the Firewall's internal interface or connected to the local network, which is itself connected to the Firewall's internal interface.
For a direct connection of the workstation to the Firewall, use the crossover Ethernet cable provided with the product.



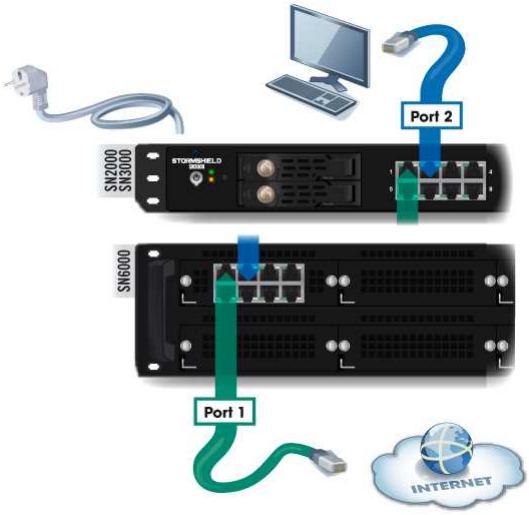
SN150 model



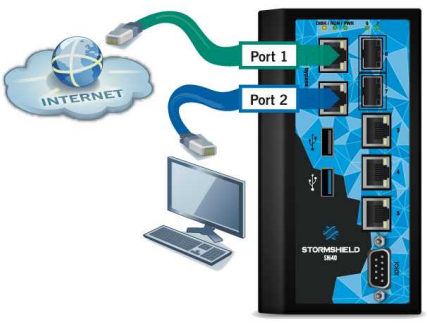
SN200, SN300, SN500, SN700 and SN900 models



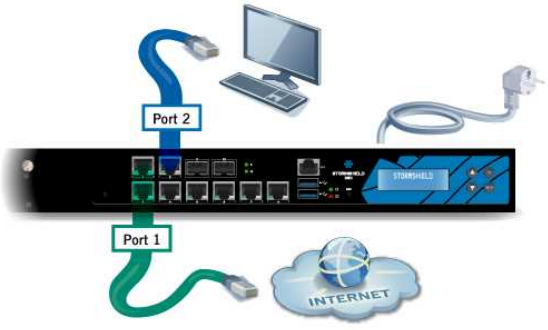
SN510 and SN710 models



SN2000, SN3000 and SN6000 models



SNi40 model



SN910 model

IMPORTANT
In factory settings, the network port 1 is reserved for the modem or Internet router. In this case, you cannot access the configuration interface from this port.

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 at least this knowledge.

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.

Starting

WARNING
You **must not** unplug the product when it is **starting, shutting down or being upgraded.**

Except for SN910 and SN6000 appliances, these phases are indicated when the following LEDs are lit:

- *Power* 3 and *Status* 2 LEDs for SN510, SN710 and SN150 to SN900 models,
- *Power* 3 LED for SN2000, SN3000 and SNi40 models.

For SN150, SN200, SN300, SN500, SN510, SN700, SN710 and SN900 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* once your product is up and running.

**For all models except the SN150.*

For SN2000 and SN3000, upon startup, the LEDs light up in the following order:

Power => Online 1

The *Power* LED lights up first. After a few minutes, the *Online* LED will light up, followed by a beep* once your product is up and running.

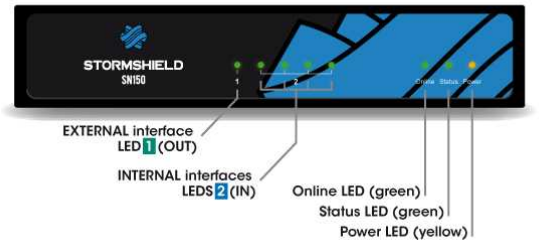
For the SNi40, upon startup, the LEDs light up in the following order:

Power => Run 1

The *Power* LED lights up first. After a few minutes, the *Run* LED will light up once your product is up and running.

Starting up SN150

Plug your SN Firewall into into the mains power supply, it will automatically start up. Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to light up.



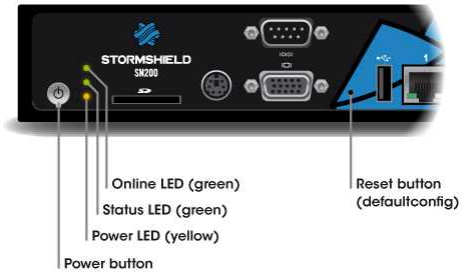
NOTE

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 SN200, SN300, SN500, SN700 and SN900 models

Plug your Stormshield Network Firewall into the mains power supply. Press once on the **Power button** then wait several minutes for the 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 SN510 and SN710 models

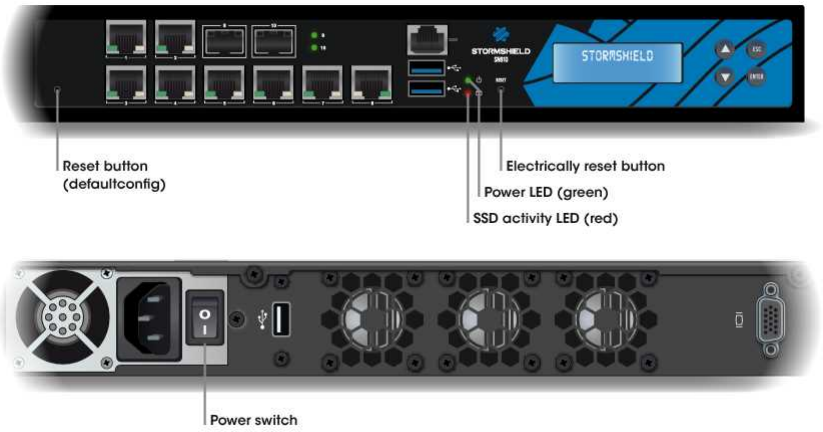
Plug your Stormshield Network Firewall into the mains power supply. Make sure the power switch is set to the position "ON". Your firewall will then automatically start running. Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to light up.

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



Plug your Stormshield Network Firewall into the mains power supply. Make sure the power switch is set to the position "ON". Your Firewall will then start running automatically, the Power LED will light up. Then wait several minutes.

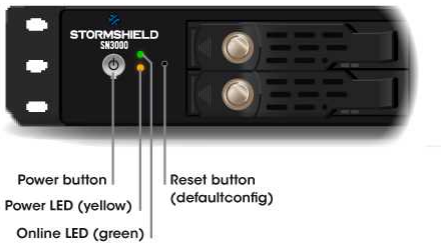
NOTE

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 up SN2000 and SN3000 models

Press once on the Power button then wait several minutes for the 2 LEDs Online and Power to light up.



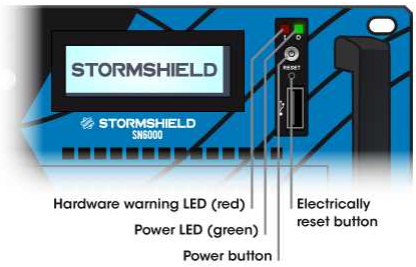
NOTE

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 SN6000

Press once on the **Power** button and the *Power* LED will light up. Wait for a few minutes while the appliance starts.



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 SNi40

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.

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*). The name (CN) of the appliance's default certificate is the appliance's serial number and it is signed by the authority called "NETASQ - Secure Internet Connectivity ("O") / NETASQ Firewall Certification Authority ("OU").

To confirm a secure access, the browser must trust the certificate authority that signed the certificate used, which must belong to the browser's list of trusted certificate authorities. Therefore, to confirm the integrity of the appliance, before the initial connection, you need to add the NETASQ authority to the list of the browser's trusted authorities. This authority can be accessed at:

http://www.netasq.com/pki/netasq-firewall-ca.crt.

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

Initial installation wizard

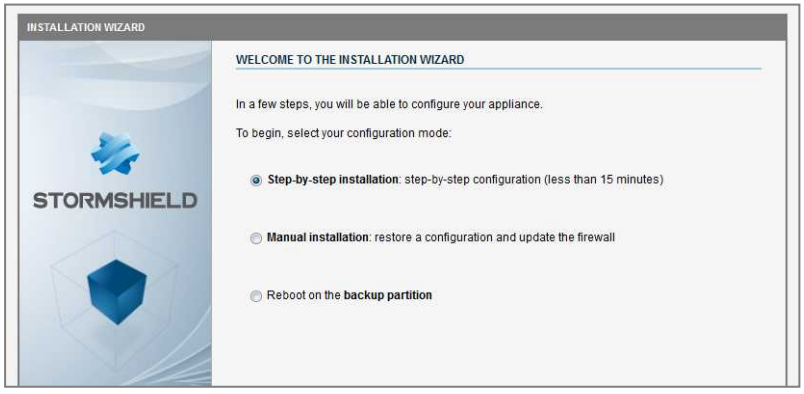
From your client workstation, type the following address in your browser: https://10.0.0.254/install

Enter the **"admin"** password.

IMPORTANT

If you have connected your client workstation on port 1, you will no longer be able to access the installation wizard. You will need to connect your computer to port 2 (or on another port), and reboot your Firewall.

An installation wizard will guide you through the configuration of your Firewall.



NOTE

The default password of the "admin" user (super administrator) must be changed the very first time the product is used. The wizard will prompt the user to change his password during the initial installation, in the *Administration of the appliance* window. 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 chapter **Welcome**, under the section *User awareness*, sub-section *User password management*, available at: http://documentation.stormshield.eu

This password must never be saved in the browser.

Thanks to this wizard, you can:

- Configure the network in order to define the network architecture in which your product is located,
- Configure your security policy,
- Register your product in order to obtain upgrades,
- Perform the first upgrades,
- Download and install your license. For more information on this subject, please refer to APPENDIX A: UPDATING THE LICENSE

The registration step allows you to obtain the password to access your **Secure area**. Once the installation is complete, you can log on to the **configuration graphical interface** at the following address: https://10.0.0.254/admin

Stormshield Network administration suite

The Stormshield Network Administration Suite, which groups the GLOBAL ADMINISTRATION, REALTIME MONITOR and EVENT REPORTER software programs, can be downloaded from your Secure area.

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

You can also obtain this suite at: http://gui.stormshield.eu/last-version

Shutting down

SN150

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, upon shutdown, the LEDs shut off in the following order:

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

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

SN200, SN300, SN500, SN700, and SN900

To shut down your Firewall, press once on the ON button.

Wait a few minutes for all 3 LEDs – *Online*, *Status* and *Power* to go off.

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

Online ❶ **+** ***Status*** ❷ **=>** ***Power*** ❸

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

SN510 and SN710

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 ❶ **+** ***Status*** ❷ **=>** ***Power*** ❸

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.

SN2000, SN3000 and SN6000

To shut down your Firewall, press once on the ON button.

For SN2000 and SN3000 models, the procedure is the same as the one described in the paragraph relating to SN200, SN300, SN500, SN700, and SN900, without the *Status* LED.

For SN6000 models, the only indication that the product has shut down is an extinguished *Power* LED.

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 ❶ **=>** ***Power*** ❷

General remarks

- The *Status* 2 LED will blink in the event of a major product failure (hardware component failure, 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 (HA), when the Firewall is in passive mode, the *Online* 1 or *Run* LED for the SNi40 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 the SNi40).
- To reboot an SN150 appliance that is still powered up (only the *Power* LED is lit), 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 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 or SN910 appliance that is still powered up (*Power* LED is off), proceed as follows: unplug it, wait for thirty seconds, then plug the Firewall 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`.
- 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 or SN910 appliance that is still powered up (*Power* LED is off), proceed as follows: unplug it, wait for thirty seconds, then plug the Firewall back into the mains socket.

DOCUMENTATION & ASSISTANCE

ONLINE HELP

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

SECURE AREA

Your Secure area allows you to:

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

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

DOCUMENT BASE

This base, which can be accessed from the Secure area, allows you to look up or download various technical documents (user guides, technical notes, etc.). Go to the ***Document base*** in your **Secure area**.

KNOWLEDGE BASE

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

ASSISTANCE

In the event of a hardware issue on your Firewall or if one of the elements does not match its description, please 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 **Initial** maintenance package,
2. RMA WITH EXPRESS EXCHANGE:
   If the appliance has a valid **Privilege** maintenance package,
3. RMA WITH DOA EXCHANGE:
   If the product was registered **less than 30 days** before the RMA was activated.

Documents relating to these procedures and their implementation are available in the *Document Base* (*Operational* folder) in your **Secure area**.

In order to comply with the hypotheses of the common criteria evaluation, clients have to 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: UPDATING THE LICENSE

Your appliance is sold with a temporary license. You will therefore need to update this license.

NOTE
The license update step is suggested in the initial installation wizard.

If you have acquired an additional option, you will need to update your product with the license that will allow you to use this option.

WARNING
Options that require you to reboot the Firewall are specified in the **online help**, in the chapter License.

Please 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/
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 online help, in the chapter License.

APPENDIX B: RESETTING THE FIREWALL

It is possible to restore the default factory settings of a Stormshield Network Firewall. This operation will bring the product back to its initial configuration. This reinitialization does not modify the firmware version and only affects the active partition.

WARNING
Resetting a Firewall will completely remove the configuration made on the product. This operation is irreversible, so do not apply this procedure unless absolutely needed. You are therefore advised to make a prior backup.

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.

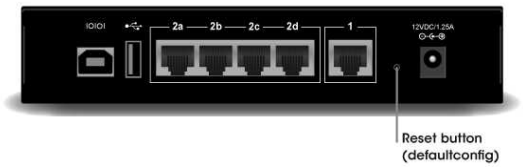
NOTE
The *Online* and *Status* (*Run* on SNi40) LEDs will blink throughout the entire initialization phase. 2 consecutive beeps (except on SN150 and SNi40 models) and the lighted up *Online* (*Run* on SNi40) LED indicate the end of the product's startup sequence.

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

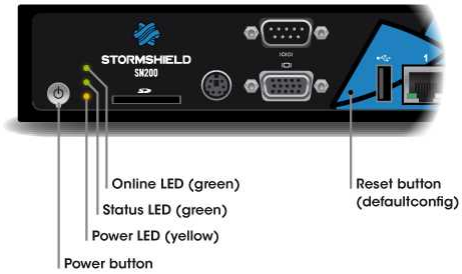
All models except SN6000 and SNi40

In order to reset your Firewall, take a pointed object. A small pushbutton is accessible through a hole located in the following places:

- on SN150 model, on the rear panel of the product, between the Ethernet interfaces and the plug of the mains adapter
- on SN200, SN300, SN500, SN700 and SN900 models, on the front panel of the product, between the USB port and VGA port.
- 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 SN2000 and SN3000 models, on the front panel of the product, between the LEDs and SSD racks.

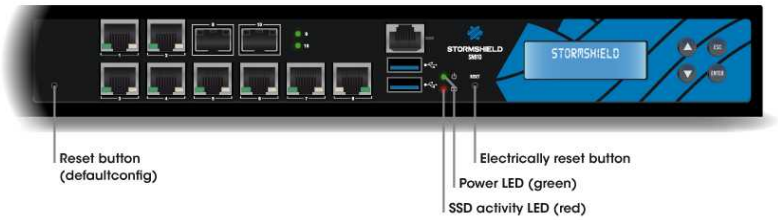


SN150 model



SN200, SN300, SN500, SN700 and SN900 models

SN510 and SN710 models



SN910 model

SN2000 and SN3000 models

Hold down the button for about 5 seconds, until you see the *Online* and *Status* LEDs blink and/or until you hear an audible signal. The reset procedure will automatically be launched. After a few minutes, the initial settings will be recovered and the Firewall will reboot.

SN6000 and SNi40 models

The factory configuration of SN6000 and SNi40 appliances can only be restored by connecting in console mode. Type the following command: `defaultconfig -f -r -p`

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

APPENDIX C: 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, please refer to the chapter *Enable log storage* below.

On SN200, SN300, SN500, SN700 and SN900 models, you can subscribe to the **External storage** option allowing you to store logs externally on an SD card.

External storage option - storing logs externally on an SD card

NOTE
Storing logs on an external medium can only be done on an SD card. This service is not compatible with other media such as a USB key or an external hard disk.

The type of SD card must be at least Class 6 and compliant with the **SDHC standard**. The maximum memory size supported is 32GB.

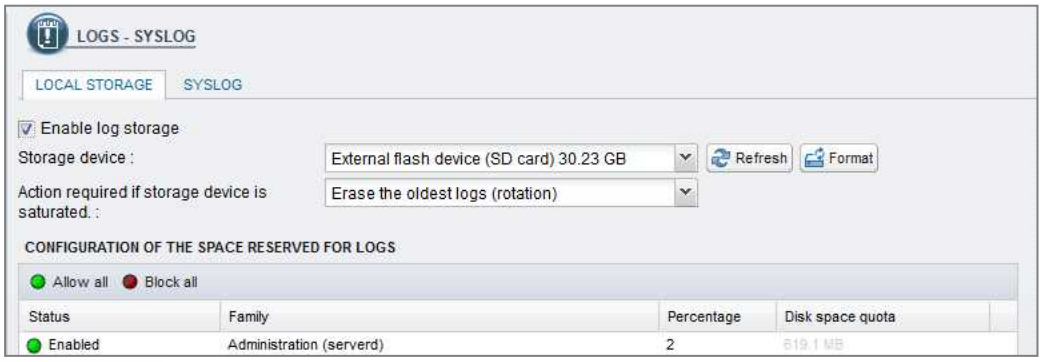
Insert the SD card, as described in the diagram to the right, with the connector facing downwards.

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

You will then need to enable and format the SD card - please refer to the following chapter.

Enable 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.



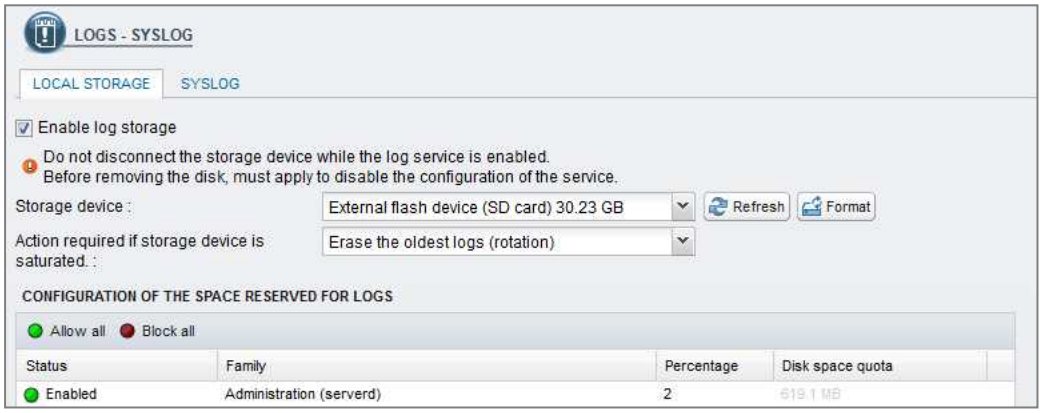
If you wish to save logs on an SD card, hard disk or SSD, select *Enable log storage*, then select your medium from the list of storage media. A message will prompt you to format it.

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

Changing the storage medium

IMPORTANT
Before ejecting the SD card from the drive or removing the SSD from an SN2000 (to change media, for example), you must first shut down the service by unselecting the option to enable log storage, in the **Logs - Syslog** module.

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



Log consultation

These logs can be read in the **SN Activity Reports** web interface in the form of reports, as well as in the **SN Event Reporter** application.

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 with the "External storage" option.

Please refer to the online help, Chapter *SN Activity Reports* for more information.

APPENDIX D: MANAGING SSDs

The SSD (Solid State Drive) on the SN2000 model is removable.

By default on SN3000 and SN6000 models, both SSDs are installed in RAID (RAID 1). These two SSDs are also removable.

NOTE
On SN2000 models, 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 may 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, SN2000 and SNi40 models, the SMART status of the SSD is available in the Hardware section of the **Hardware** widget.

On SN3000 and SN6000 models, 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.

Adding and extracting SSDs

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

- SN2000:

This procedure is to be carried out on an appliance that has been powered off. After having extracted the defective SSD, insert the new SSD, which you would have obtained from your partner. Once you have inserted the new SSD, it will be detected the next time you start the appliance.

- SN3000 and SN6000 (SSD in RAID1):

This procedure is to be carried out on an appliance that is running. After having extracted the defective SSD, insert the new SSD, which you would have obtained from your partner, then type the following command to scan the newly inserted SSD: `nraid -z`.

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

Big Data Option

If you have subscribed the *Big Data* option (available on SN3000 and SN6000 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. Next, insert the new SSDs, which will be detected the next time you start the appliance.

APPENDIX E: CHANGING A POWER SUPPLY MODULE (SN3000 AND SN6000)

REMINDER

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

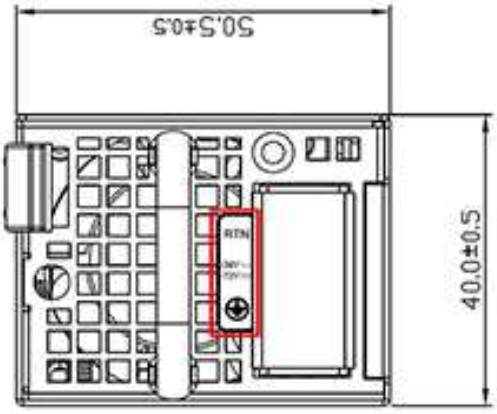
SN3000

WARNING

Certain Stormshield Network SN3000 appliances are not compatible with 48VDC power supply modules and must not use them.

Affected products have the following Part number: SN3000-XA10A-101

If your SN3000 is one of such appliances, and you wish to use a 48VDC power supply module, please contact your partner or reseller in order to replace your appliance.



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).

- SN3000 (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.

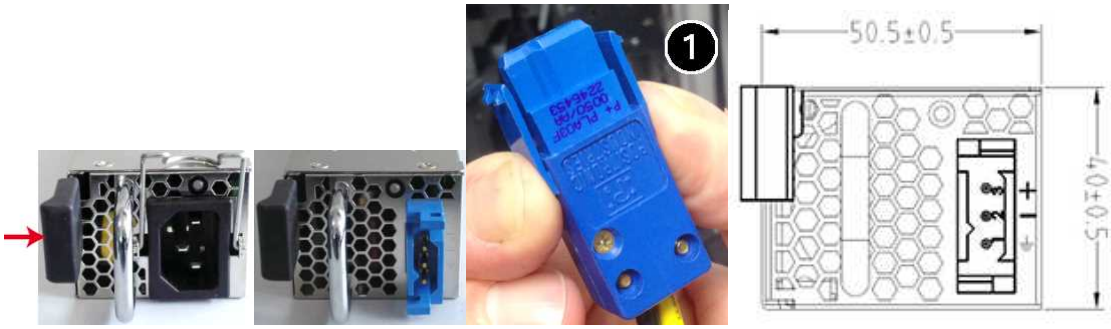
- SN3000 (running):

- 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.

SN6000



1. Disconnect the module from the electrical supply:
   - **AC mains supply:** disconnect the mains cable.
   - **48VDC module:** disconnect the supply cable from the module - squeeze the connecter vertically ❶, and pull.
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 supply cable's connector ❶. Verify that the connector is locked in place by pulling it gently.

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.

- SN6000 (halted):

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

- SN6000 (running):

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

• Module not functioning correctly

- module connected to a power source: red, not blinking.

APPENDIX F: CONFIGURATION AND ADMINISTRATION VIA IPMI (SN6000)

IPMI (Intelligent Platform Management Interface) is a network protocol and allows obtaining hardware information remotely, monitoring certain components and controlling appliances (control, reboot, interruption, etc.).

Configuration

When starting the product, once the *Stormshield* logo appears, press <del> to access the BIOS.

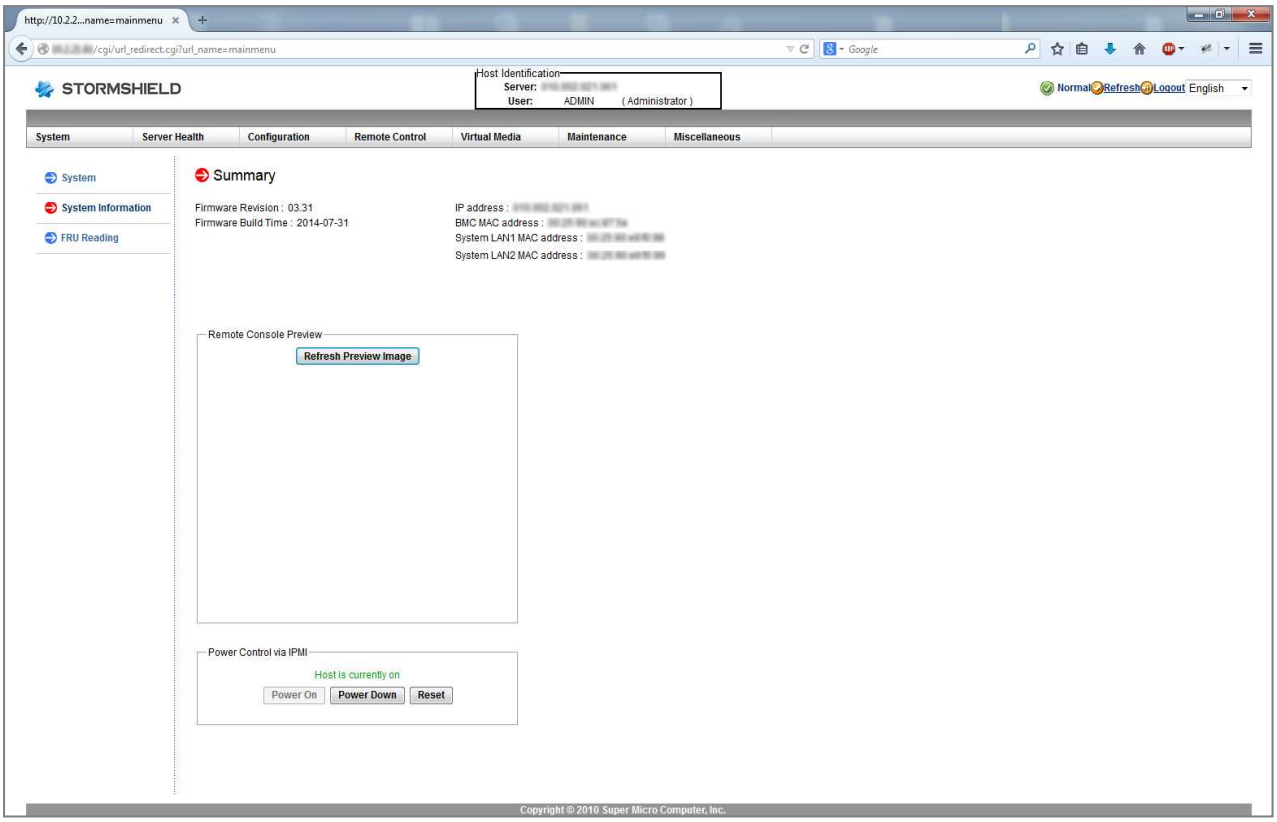
Next, go to the section "IPMI/BMC network configuration" in the IPMI menu in order to configure the network interface dedicated to IPMI, then save and quit.

Connection

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

Launch your browser and log on to the dedicated interface by entering the address: **http://<*ip_if_ipmi*>**
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 in the menu *Configuration/Users*. You are further advised to place the IPMI interface on a dedicated administration network.

If necessary, the following Supermicro documentation will provide a detailed description of the motherboard (page 23, section 1-9): http://www.supermicro.com/manuals/motherboard/C606_602/MNL-1306.pdf

For the full description of IPMI, please refer to this document:

http://www.supermicro.com/manuals/other/SMT_IPMI_Manual.pdf

STORMSHIELD

documentation@stormshield.eu