

# NSFOCUS NFNX3 Firewall Series Installation Guide

NSFOCUS Technologies, Inc.

Document version: 6W100-20230111

---

■ Copyright © 2022 NSFOCUS Technologies, Inc. All rights reserved.

---

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

---

# Preface

This document describes the installation procedure for the NSFOCUS NFNX3 Firewall Series. It covers preparing for installation, installing the firewall, accessing the firewall, hardware replacement, hardware management and maintenance, and troubleshooting.

This preface includes the following topics about the documentation:

- [Audience](#).
- [Conventions](#).

## Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

## Conventions

The following information describes the conventions used in the documentation.





### Command conventions

Convention	Description
<b>Boldface</b>	<b>Bold</b> text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... }*	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[ x   y   ... ]*	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.













### GUI conventions

Convention	Description
<b>Boldface</b>	Window names, button names, field names, and menu items are in Boldface. For example, the <b>New User</b> window opens; click <b>OK</b> .
>	Multi-level menus are separated by angle brackets. For example, <b>File &gt; Create &gt; Folder</b> .

## Symbols

Convention	Description
 <b>WARNING!</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 <b>CAUTION:</b>	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 <b>IMPORTANT:</b>	An alert that calls attention to essential information.
<b>NOTE:</b>	An alert that contains additional or supplementary information.
 <b>TIP:</b>	An alert that provides helpful information.

## Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

## Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

# Contents

<b>1</b>	<b>Preparing for installation</b>	<b>1</b>
	Safety recommendations	1
	Safety symbols	1
	General safety recommendations	1
	Electrical safety	2
	Laser safety	2
	Handling safety	2
	Examining the installation site	3
	Weight support	3
	Temperature and humidity	3
	Cleanliness	3
	Cooling system	4
	ESD prevention	5
	EMI	5
	Lightning protection	5
	Power supply	6
	Installation tools	6
	Accessories	6
	Pre-installation checklist	7
<b>2</b>	<b>Installing the firewall</b>	<b>9</b>
	Installation flow	9
	Mounting the firewall on a workbench	10
	Installing the firewall in a standard 19-inch rack	10
	Rack-mounting the firewall by using front mounting brackets	11
	Rack-mounting the firewall by using front and rear mounting brackets	12
	Grounding the firewall	15
	Grounding the firewall with a grounding strip	16
	Grounding the firewall with the grounding terminal on the rack	16
	Installing a Micro SD card	17
	Installing a power supply	17
	Installing an interface module	19
	Installing a drive	20
	Installing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall	20
	Installing a drive for other firewalls than the NFNX3-HDB1080, NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280	20
	Connecting Ethernet cables	21
	Connecting a copper Ethernet port	21
	Connecting a fiber port	21
	Connecting power cords	23
	Connecting an AC power cord	23
	Connecting a DC power cord	24
	Connecting the power adapter for an NFNX3-HDB680 firewall	25
	Verifying the installation	25
<b>3</b>	<b>Accessing the firewall</b>	<b>3-26</b>
	Starting the firewall	3-26
	Pre-start checking	3-26
	Starting the firewall and observing the initial startup conditions	3-26
	Logging in to the firewall	3-27
	Logging in from the Web interface	3-27
	Logging in from the console port	3-28
	Logging in through Telnet	3-28
<b>4</b>	<b>Hardware replacement</b>	<b>4-30</b>
	Replacing a power supply	4-30
	Replacing an interface module	4-30

Replacing a drive .....	4-31
Replacing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall.....	4-31
Replacing a drive for the NFNX3-HDB1080, NFNX3-HDB1780, NFNX3-HDB3080, or NFNX3-HDB3280 firewall .....	4-32
Replacing a transceiver module.....	4-32
<b>5 Hardware management and maintenance .....</b>	<b>5-34</b>
Displaying detailed information about the firewall.....	5-34
Displaying the software and hardware version information for the firewall .....	5-34
Displaying the electrical label information for the firewall.....	5-35
Displaying the CPU usage of the firewall.....	5-35
Displaying the memory usage of the firewall.....	5-36
Displaying the temperature information of the firewall .....	5-36
Displaying the operational statistics of the firewall.....	5-37
Displaying transceiver module information .....	5-38
Rebooting the firewall.....	5-38
<b>6 Troubleshooting .....</b>	<b>6-40</b>
Power supply failure.....	6-40
Configuration terminal display issue .....	6-40
Password loss .....	6-40
Cooling system failure.....	6-41
Software loading failure.....	6-41
<b>7 Appendix A Chassis views and technical specifications.....</b>	<b>6-42</b>
Chassis views .....	6-42
NFNX3-HDB680.....	6-42
NFNX3-HDB1080.....	6-43
NFNX3-HDB1180/NFNX3-HDB1480.....	6-43
NFNX3-HDB1780/NFNX3-HDB3080 .....	6-44
NFNX3-HDB3280.....	6-45
Interface modules.....	6-46
NIC-NF-GE-SFP4 .....	6-47
NIC-NF-10GE-SFPP6.....	6-47
Drives .....	6-47
Power supplies.....	6-48
AC power supplies .....	6-48
DC power supplies .....	6-48
Dimensions and weights .....	6-49
Chassis .....	6-49
Interface modules.....	6-49
Drives .....	6-49
Storage media.....	6-50
Power consumption.....	6-50
Chassis .....	6-50
Interface modules.....	6-50
Drives .....	6-51
Power supply specifications.....	6-51
Port specifications .....	6-51
Console port.....	6-51
GE copper port.....	6-52
GE fiber port.....	6-52
10 GE fiber port.....	6-52
<b>8 Appendix B LEDs.....</b>	<b>6-53</b>
NFNX3-HDB680.....	6-53
NFNX3-HDB1080.....	6-53
NFNX3-HDB1180/NFNX3-HDB1480 .....	6-54
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB3280 .....	6-55
<b>9 Appendix C Cables .....</b>	<b>6-56</b>
Console cable .....	6-56

Ethernet twisted pair cable.....	6-57
Introduction .....	6-57
Making an Ethernet twisted pair cable .....	6-60
Optical fiber.....	6-60

# 1 Preparing for installation

This document is applicable to the following firewall models:


- NFNX3-HDB680
- NFNX3-HDB1080
- NFNX3-HDB1180
- NFNX3-HDB1480
- NFNX3-HDB1780
- NFNX3-HDB3080
- NFNX3-HDB3280


## Safety recommendations

To avoid any equipment damage or bodily injury, read the following safety recommendations before installation. Note that the recommendations do not cover every possible hazardous condition.

## Safety symbols

When reading this document, note the following symbols:

 **WARNING** means an alert that calls attention to important information that if not understood or followed can result in personal injury.





 **CAUTION** means an alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.

## General safety recommendations

- Do not place the firewall on an unstable case or desk. The firewall might be severely damaged in case of a fall.
- Make sure the ground is dry and flat and anti-slip measures are in place.
- Keep the chassis and installation tools away from walk areas.
- Keep the chassis clean and dust-free.
- Do not place the firewall near water or in a damp environment. Prevent water or moisture from entering the firewall chassis.
- Ensure good ventilation of the equipment room and keep the air inlet and outlet vents of the firewall free of obstruction.
- Make sure the operating voltage is in the required range.
- Use a screwdriver, rather than your fingers, to fasten screws.
- Stack devices according to the sizes of and packing symbols on the packages.



Figure1-1 Packing symbols

Symbol	Description
	Stored with a maximum stack of n units.
	Transported and stored with the arrows up.
	Transported and stored with care.
	Transported and stored avoiding humidity, rains and wet floor.

## Electrical safety

- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Locate the emergency power-off switch in the room before installation. Shut the power off at once in case accident occurs.
- Do not work alone when the firewall has power.
- Always verify that the power has been disconnected.

## Laser safety

---

**⚠ WARNING!**

Disconnected optical fibers or transceiver modules might emit invisible laser light. Do not stare into beams or view directly with optical instruments when the firewall is operating.

---

The firewall is a Class 1 laser device.

- Before you disconnect the fiber connector, execute the **shutdown** command in interface view to disable the optical source.
- Install dust caps to disconnected optical fiber connectors and ports on disconnected transceiver modules to avoid damage caused by built-up dust.
- Insert a dust plug into empty fiber ports.

## Handling safety

When you move the firewall, follow these guidelines:

- Move and unpack the firewall carefully to avoid firewall damage.
- Unpack the firewall at least half an hour and power on the firewall at least two hours after you move it from a place below 0°C (32°F) to the equipment room. This prevents condensation and even damage to the firewall.
- Use a safety hand truck when you move multiple firewalls.

- Before you move the firewall, remove all cables and mounting brackets.
- For long-distance transportation, remove all the removable components, such as power supplies and interface modules, and package them separately, and install the filler panels supplied with the firewall. For short-distance transportation, make sure all the removable components are securely seated in the slots and the screws are fastened.
- When you move or lift the firewall chassis, support the bottom of the chassis, rather than holding any removable component. Make sure the accessories of the firewall are not lost or damaged during firewall moving.

## Examining the installation site

The firewall can only be used indoors. To make sure the firewall operates correctly and to prolong its service lifetime, the installation site must meet the following requirements.

### Weight support

Make sure the floor can support the total weight of the rack, chassis, modules, and all other components. For more information, see "Dimensions and weights."

### Temperature and humidity

Maintain appropriate temperature and humidity in the equipment room.

- Lasting high relative humidity can cause poor insulation, electricity leakage, mechanical property change of materials, and metal corrosion.
- Lasting low relative humidity can cause washer contraction and ESD and bring problems including loose captive screws and circuit failure.
- High temperature can accelerate the aging of insulation materials and significantly lower the reliability and lifespan of the firewall.

For the temperature and humidity requirements of the firewall, see [Table1-1](#).

**Table1-1 Temperature/humidity requirements**

Temperature	Relative humidity
<ul style="list-style-type: none"> <li>• Operating:               <ul style="list-style-type: none"> <li>○ Without drives: 0°C to 45°C (32°F to 113°F)</li> <li>○ With drives: 5°C to 40°C (41°F to 104°F)</li> </ul> </li> <li>• Storage: -40°C to +70°C (-40°F to +158°F)</li> </ul>	<ul style="list-style-type: none"> <li>• Operating:               <ul style="list-style-type: none"> <li>○ Without drives: 5% to 95%, noncondensing</li> <li>○ With drives: 10% to 90%, noncondensing</li> </ul> </li> <li>• Storage: 5% to 95%, noncondensing</li> </ul>

### Cleanliness

Dust buildup on the chassis might result in electrostatic adsorption, which causes poor contact of metal components and contact points, especially when indoor relative humidity is low. In the worst case, electrostatic adsorption can cause communication failure.

**Table1-2 Dust concentration limit in the equipment room**

Substance	Concentration limit (particles/m <sup>3</sup> )
Dust particles	$\leq 3 \times 10^4$ (No visible dust on desk in three days)

Substance	Concentration limit (particles/m <sup>3</sup> )
<b>NOTE:</b>	
Dust particle diameter ≥ 5 μm	

The equipment room must also meet strict limits on salts, acids, and sulfides to eliminate corrosion and premature aging of components, as shown in [Table1-3](#).

**Table1-3 Harmful gas limits in an equipment room**

Gas	Max. (mg/m <sup>3</sup> )
SO <sub>2</sub>	0.2
H <sub>2</sub> S	0.006
NH <sub>3</sub>	0.05
Cl <sub>2</sub>	0.01
NO <sub>2</sub>	0.04

## Cooling system

For adequate cooling of the firewall, follow these guidelines:

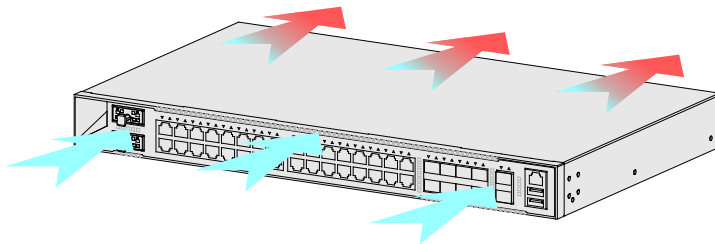
- Plan the firewall installation position for the airflow direction of the firewall to match the ventilation designs at the installation site.
- Reserve a minimum clearance of 80 mm (3.15 in) around the inlet and outlet air vents.
- Make sure the installation site has a good cooling system.
- When installing the firewall in a standard 19-inch rack, reserve a distance of 1U (44.45 mm, or 1.75 in) between the chassis and other devices.

The NFNX3-HDB680 and NFNX3-HDB1080 firewalls use passive cooling.

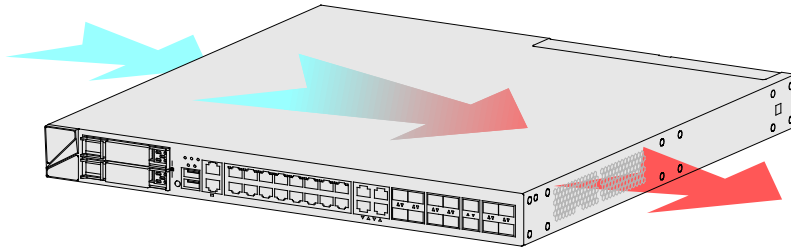
The NFNX3-HDB1180 and NFNX3-HDB1480 firewalls provide front side-intake and rear side-exhaust airflow for heat dissipation.

The NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280 firewalls provide left side-intake and right side-exhaust airflow for heat dissipation.

**Figure1-2 Airflow through the NFNX3-HDB1180/NFNX3-HDB1480 firewall chassis**



**Figure1-3 Airflow through the NFNX3-HDB1780/NFNX3-HDB3080/NFNX3-HDB3280 firewall chassis**



## ESD prevention

To prevent electrostatic discharge (ESD), follow these guidelines:

- Make sure the firewall, the workbench, and the rack are reliably grounded.
- Take dust-proof measures for the equipment room. For more information, see "[Cleanliness](#)."
- Maintain the humidity and temperature at an acceptable level. For more information, see "[Temperature and humidity](#)."
- Put the removed interface modules away on an ESD workbench, with the PCB upward, or put them in ESD bags for future use.
- Always wear ESD clothing, ESD gloves, and an ESD wrist strap.

## EMI

All electromagnetic interference (EMI) sources, from outside or inside of the firewall and application system, adversely affect the firewall in the following ways:

- A conduction pattern of capacitance coupling.
- Inductance coupling.
- Electromagnetic wave radiation.
- Common impedance (including the grounding system) coupling.

To prevent EMI, use the following guidelines:

- If AC power is used, use a single-phase three-wire power receptacle with protection earth (PE) to filter interference from the power grid.
- Keep the firewall far away from radio transmitting stations, radar stations, and high-frequency devices.
- Use electromagnetic shielding, for example, shielded interface cables, when necessary.
- To prevent signal ports from getting damaged by overvoltage or overcurrent caused by lightning strikes, route interface cables only indoors. If part of the network cable of an Ethernet port must be routed outdoors, connect a lightning arrester to the cable before you plug the cable into the port.

## Lightning protection

To protect the firewall from lightning better, follow these guidelines:

- Make sure the grounding cable of the chassis is reliably grounded.
- Make sure the grounding terminal of the AC power receptacle is reliably grounded.









- Install a lightning arrester at the input end of the power supply to enhance the lightning protection capability of the power supply.

## Power supply


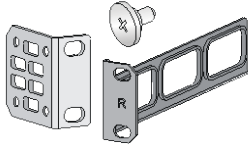









Verify that the power system at the installation site meets the requirements of the power supplies, including the input method and rated input voltage. For more information, see "Appendix A Chassis views and technical specifications."

## Installation tools

All installation tools are user supplied.

			
Flat-head screwdriver	Phillips screwdriver	Needle-nose pliers	Marker
			
Diagonal pliers	ESD wrist strap	Wire stripper	Crimping tool

## Accessories

			
NFNX3-HDB680/NFNX3-HDB1080/NFNX3-HDB1180/NFNX3-HDB1480 mounting bracket	NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB3280 mounting brackets (including M4 shoulder screws)	Cage nut	M6 screw
			
M4 screw	Rubber feet	Grounding cable	Console cable
			
Power adapter for the NFNX3-HDB680	Power cord for the NFNX3-HDB1080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB3280	Power cord retainer	

# Pre-installation checklist

**Table1-4 Checklist before installation**

Item		Requirements	Result
Installation site	Ventilation	<ul style="list-style-type: none"> <li>There is a minimum clearance of 80 mm (3.15 in) around the inlet and outlet air vents for heat dissipation of the firewall chassis.</li> <li>A good ventilation system is available at the installation site.</li> <li>When installing the firewall in a standard 19-inch rack, reserve a distance of 1U (44.45 mm, or 1.75 in) between the chassis and other devices.</li> </ul>	
	Temperature	<ul style="list-style-type: none"> <li>Operating:               <ul style="list-style-type: none"> <li>Without drives: 0°C to 45°C (32°F to 113°F)</li> <li>With drives: 5°C to 40°C (41°F to 104°F)</li> </ul> </li> <li>Storage: -40°C to +70°C (-40°F to +158°F)</li> </ul>	
	Relative humidity	<ul style="list-style-type: none"> <li>Operating:               <ul style="list-style-type: none"> <li>Without drives: 5% RH to 95% RH, noncondensing</li> <li>With drives: 10% RH to 90% RH, noncondensing</li> </ul> </li> <li>Storage: 5% RH to 95% RH, noncondensing</li> </ul>	
	Cleanness	<ul style="list-style-type: none"> <li>Dust concentration <math>\leq 3 \times 10^4</math> particles/m<sup>3</sup></li> <li>No dust on desk within three days</li> </ul>	
	ESD prevention	<ul style="list-style-type: none"> <li>The equipment, workbench, and rack are reliably grounded.</li> <li>The equipment room is dust-proof.</li> <li>The humidity and temperature are at an acceptable level.</li> <li>Wear an ESD wrist strap and make sure it makes good skin contact and is reliably grounded when installing removable components.</li> <li>Put the removed interface modules away on an ESD workbench, with the PCB upward, or put them in ESD bags for future use.</li> <li>Touch only the edges, instead of electronic components when observing or moving a removed interface module.</li> </ul>	
	EMI prevention	<ul style="list-style-type: none"> <li>Take effective measures to protect the power system from the power grid system.</li> <li>Separate the protection ground of the firewall from the grounding device or lightning protection grounding device as far as possible.</li> <li>Keep the firewall far away from radio stations, radar and high-frequency devices working in high current.</li> <li>Use electromagnetic shielding when necessary.</li> </ul>	
	Lightning protection	<ul style="list-style-type: none"> <li>The grounding cable of the chassis is reliably grounded.</li> <li>The grounding terminal of the AC power receptacle is reliably grounded.</li> <li>(Optional.) A power lightning arrester is installed.</li> </ul>	
	Electricity safety	<ul style="list-style-type: none"> <li>Equip a UPS.</li> </ul>	

Item		Requirements	Result
		<ul style="list-style-type: none"> <li>Locate the power switch in the equipment room. In case of emergency during operation, switch off the power switch.</li> </ul>	
	Rack-mounting requirements	<ul style="list-style-type: none"> <li>Make sure the cabinet is equipped with a good ventilation system.</li> <li>The rack is sturdy enough to support the weight of the firewall and installation accessories.</li> <li>The size of the rack is appropriate for the firewall.</li> <li>The front and rear of the rack are a minimum of 0.8 m (31.50 in) away from walls or other devices.</li> </ul>	
Safety precautions	<ul style="list-style-type: none"> <li>The firewall is far away from any moist area and heat source.</li> <li>The emergency power switch in the equipment room is located.</li> </ul>		
Tools and accessories	<ul style="list-style-type: none"> <li>Installation accessories supplied with the firewall</li> <li>User-supplied tools</li> </ul>		
Reference	<ul style="list-style-type: none"> <li>Documents shipped with the firewall</li> <li>Online documents</li> </ul>		

# 2 Installing the firewall

**⚠ WARNING!**

Keep the tamper-proof seal on a mounting screw on the chassis cover intact, and if you want to open the chassis, contact NSFOCUS for permission. Otherwise, NSFOCUS shall not be liable for any consequence.

The installation procedure is similar for the NFNX3-HDB680, NFNX3-HDB1080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280 firewalls.

The firewall appearance varies by model. The following figures are for illustration only.

## Installation flow

**Table2-1 Installation flow for the firewall**

Step	Description
1. Start	Before installation, make sure all requirements on the checklist are met and the firewall is powered off.
2. Mounting the firewall on a workbench	Verify that the workbench is sturdy and reliably grounded. Ensure a minimum clearance of 80 mm (3.15 in) around the air inlet and outlet vents of the chassis.
3. Installing the firewall in a standard 19-inch rack	To avoid bodily injury and device damage, use a minimum of two people to rack-mount the firewall.
4. Grounding the firewall	Before installation, make sure the firewall and rack are grounded correctly and you wear an ESD wrist strap.
5. Installing a Micro SD card	Install a Micro SD card on the firewall.
6. Installing a power supply	Before you install a power supply, make sure the power supply is not connected to any power source and the grounding cable of the firewall is connected reliably.
7. Installing an interface module	Install compatible interface modules on the firewall.
8. Installing a drive	Install compatible drives on the firewall.
9. Connecting Ethernet cables	The firewall provides various ports. Choose compatible transceiver modules and cables as required. To avoid bodily injury or device damage, read the restrictions and guidelines carefully before connection.
10. Connecting power cords	Connect compatible power cords to the power supplies.
11. Verifying the installation	Verify that the firewall is installed securely and reliably grounded, and that the power supplies are as required.



# Mounting the firewall on a workbench

---

## ⚠ IMPORTANT:

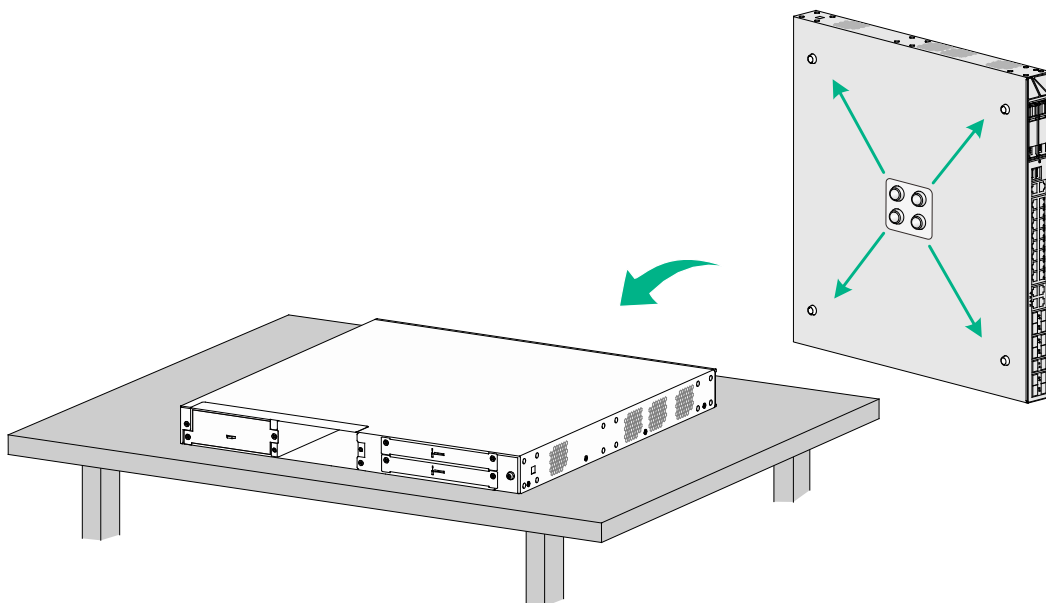
- Ensure good ventilation and a minimum clearance of 80 mm (3.15 in) around the chassis for heat dissipation.
  - Avoid placing heavy objects on the firewall.
  - To stack firewalls, make sure a minimum distance of 15 mm (0.59 in) is available between two adjacent firewalls.
- 

If a standard 19-inch rack is not available, you can place the firewall on a workbench.

To mount the firewall on a workbench:

1. Verify that the workbench is sturdy and reliably grounded.
2. Place the firewall upside down on the workbench and clean the four round holes in the chassis bottom with a dry cloth.
3. Attach the four rubber feet to the round holes in the chassis bottom.
4. Place the firewall with upside up on the workbench.

**Figure2-1 Mounting the firewall on a workbench**



# Installing the firewall in a standard 19-inch rack

---

## ⚠ WARNING!

To avoid bodily injury and device damage, use a minimum of two persons to rack-mount the firewall.

---

## ⚠ CAUTION:

For adequate heat dissipation, ensure a minimum clearance of 80 mm (3.15 in) around the air inlet and outlet vents of the chassis and a distance of 1U (44.45 mm, or 1.75 in) between the chassis and other devices in the rack.

---

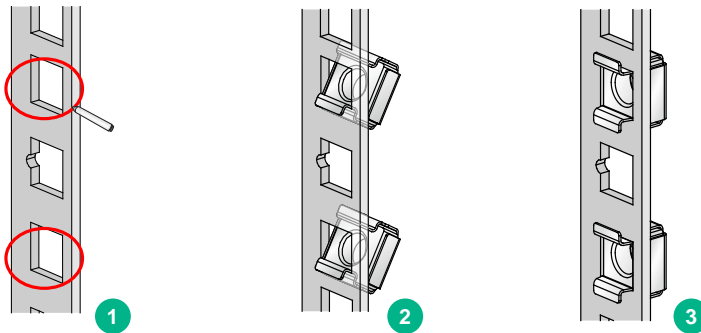
# Rack-mounting the firewall by using front mounting brackets

The NFX3-HDB680, NFX3-HDB1080, NFX3-HDB1180, and NFX3-HDB1480 firewalls support this installation method.

To install the firewall in a standard 19-inch rack by using front mounting brackets:

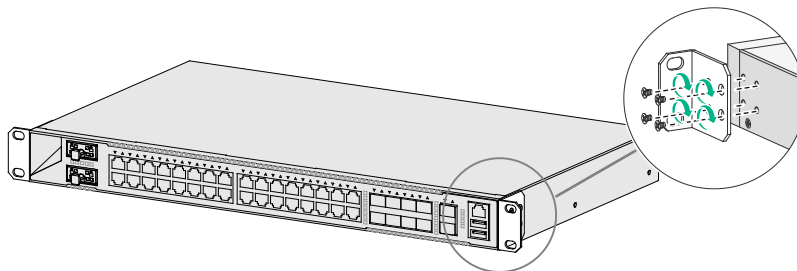
1. Wear an ESD wrist strap and make sure the wrist strap makes good skin contact and is reliably grounded.
2. Unpack the firewall and accessories.
3. Mark the cage nut installation positions on the rack posts by using the mounting brackets.
4. Install cage nuts.

**Figure2-2 Installing cage nuts**



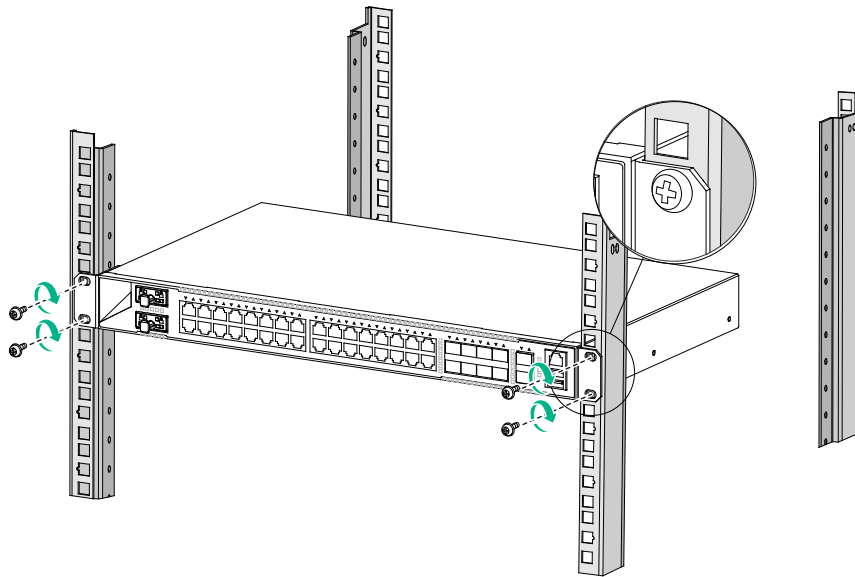
5. Attach the front mounting brackets to both sides of the firewall with M4 screws provided with the firewall.

**Figure2-3 Attaching the front mounting brackets to the firewall**



6. Mount the firewall in the rack. Use M6 screws to secure the mounting brackets to the front rack posts.

**Figure2-4 Mounting the firewall in the rack**



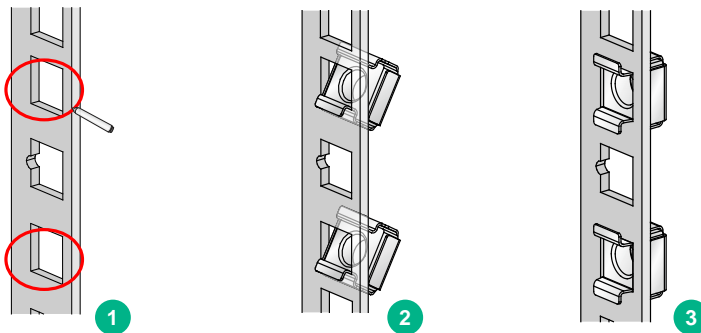
## Rack-mounting the firewall by using front and rear mounting brackets

The NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280 firewalls support this installation method.

To install the firewall in a standard 19-inch rack:

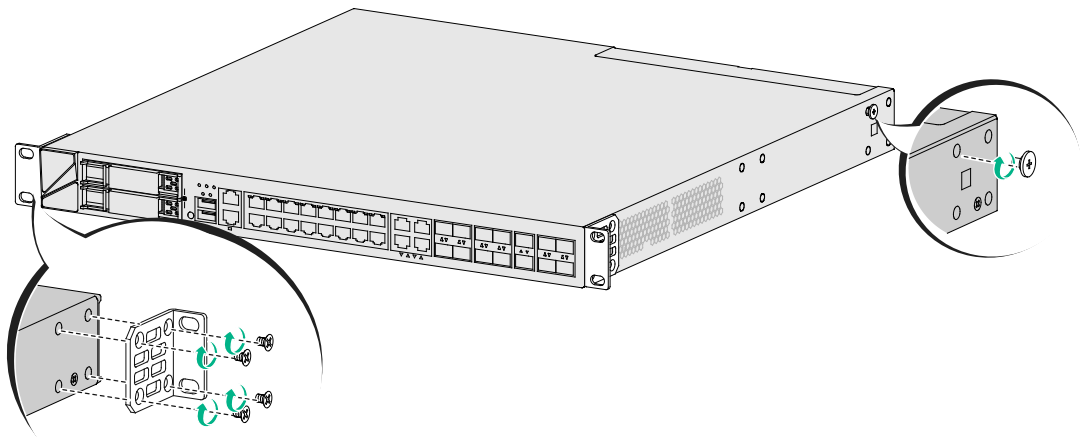
1. Wear an ESD wrist strap and make sure the wrist strap makes good skin contact and is reliably grounded.
2. Unpack the firewall and accessories.
3. Mark the cage nut installation positions on the rack posts by using the mounting brackets.
4. Install cage nuts.

**Figure2-5 Installing cage nuts**



5. Attach the front mounting brackets and shoulder screws to both sides of the firewall with M4 screws provided with the firewall.

**Figure2-6 Attaching mounting brackets and shoulder screws to the firewall**

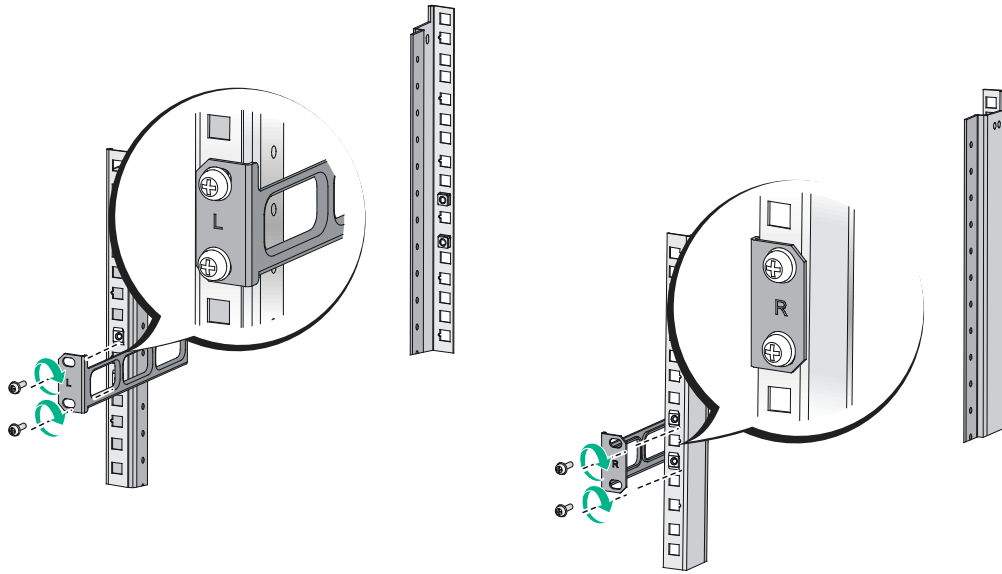


6. Attach the rear mounting brackets to the rear rack posts. The rear mounting brackets can be attached to the rear rack posts with the wide flange inside or outside the rack.

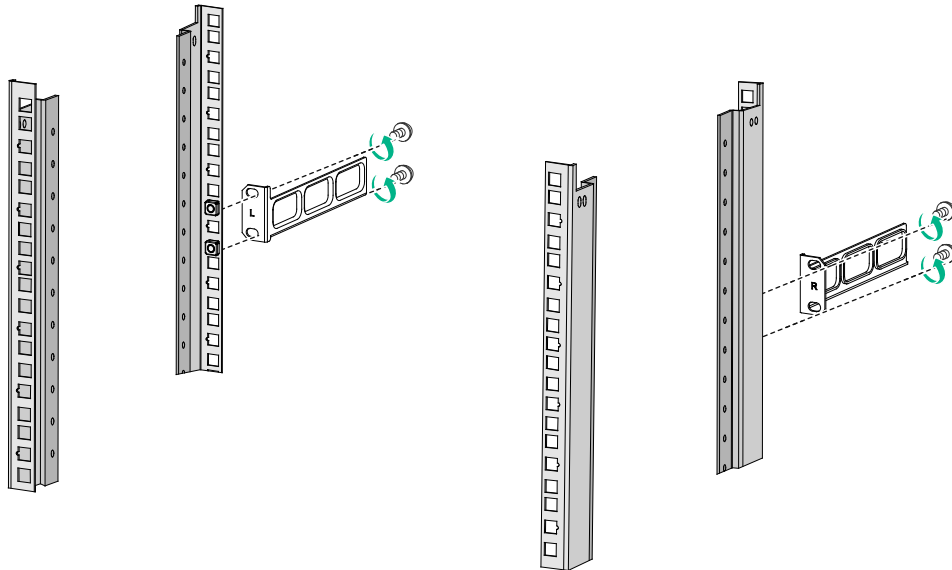
**Table2-2 Installation methods for rear mounting brackets**

Distance between the front and rear rack posts	Rear mounting bracket installation method
405 to 569 mm (15.94 to 22.40 in)	With the wide flange inside the rack.
247 to 411 mm (9.72 to 16.18 in)	With the wide flange outside the rack. <b>Caution:</b> To prevent the rear mounting brackets from obstructing the closing of the rack door, ensure a distance greater than 153 mm (6.02 in) between the rear rack posts and the interior side of the rack door.

**Figure2-7 Attaching the rear mounting brackets to the rear rack posts (with the wide flange inside the rack)**

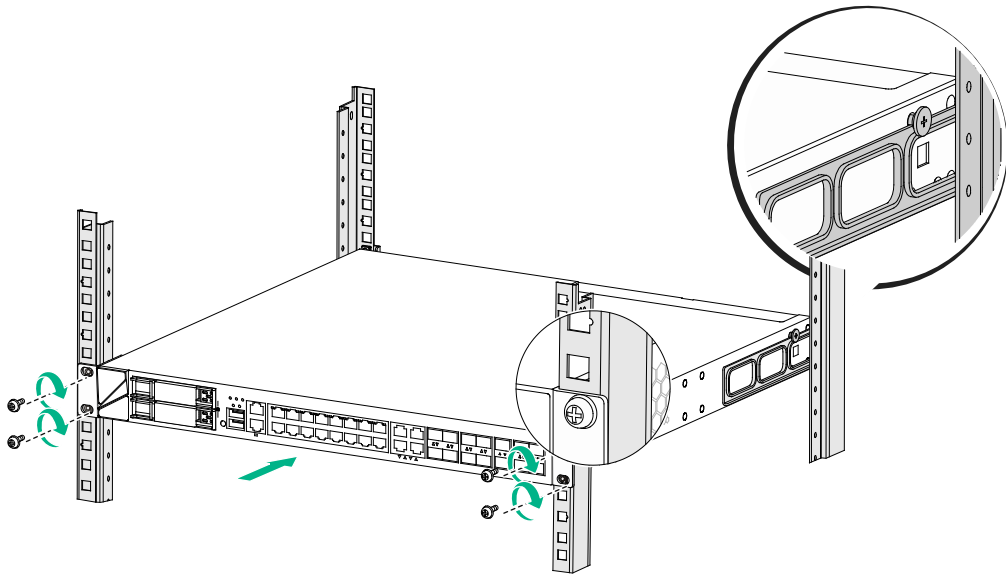


**Figure2-8 Attaching the rear mounting brackets to the rear rack posts (with the wide flange outside the rack)**

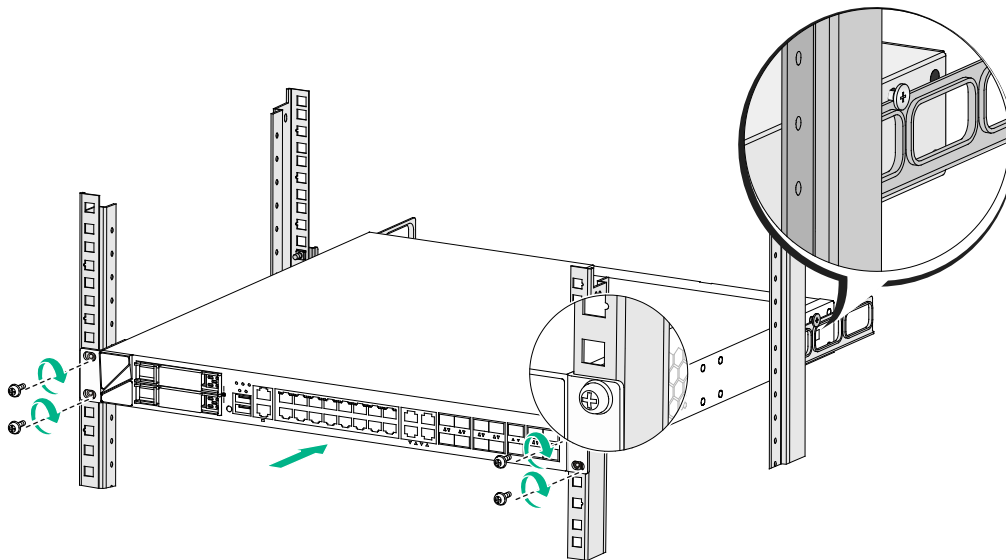


7. Mount the firewall in the rack. Use M6 screws to secure the mounting brackets to the front rack posts and make sure the shoulder screws rest firmly on the upper edge of the rear mounting brackets.

**Figure2-9 Mounting the firewall in the rack (with the wide flange of the rear mounting brackets inside the rack)**



**Figure2-10 Mounting the firewall in the rack (with the wide flange of the rear mounting brackets outside the rack)**



## Grounding the firewall

---

**⚠ WARNING!**

- Correctly connecting the firewall grounding cable is crucial to lightning protection and EMI protection.
  - Do not connect the firewall grounding cable to a fire main or lightning rod.
-

You can ground the firewall in one of the following ways, depending on the grounding conditions available at the installation site.

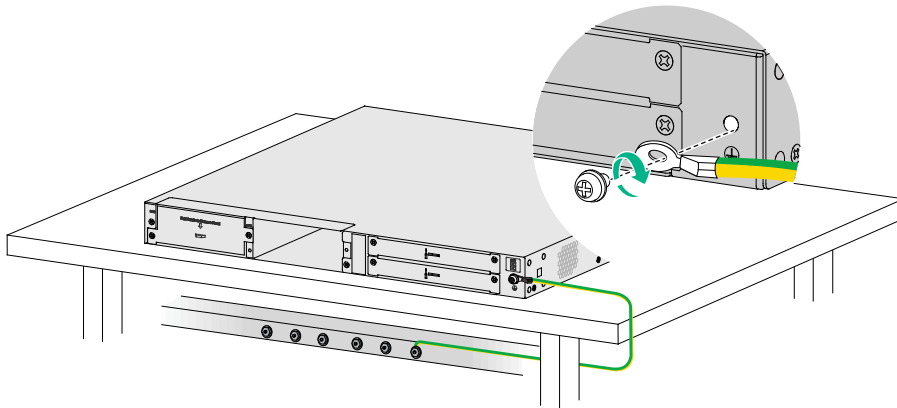
## Grounding the firewall with a grounding strip

If a grounding strip is available at the installation site, connect the grounding cable through the grounding strip.

To connect the grounding cable:

1. Remove the grounding screw from the firewall chassis.
2. Attach the grounding screw to the ring terminal of the grounding cable.
3. Use a Phillips screwdriver to fasten the grounding screw into the grounding hole on the firewall.
4. Remove the hex nut from the grounding strip.
5. Use a pair of needle-nose pliers to bend a hook at the other end of the grounding cable. Attach the hook to the grounding point, and secure the hook with a screw.

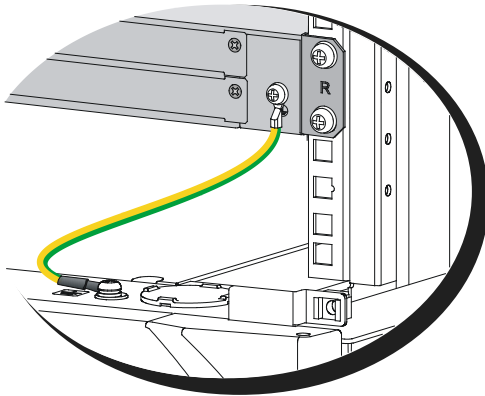
**Figure2-11 Grounding the firewall with a grounding strip**



## Grounding the firewall with the grounding terminal on the rack

1. Remove the grounding screw from the firewall chassis.
2. Attach the grounding screw to the ring terminal of the grounding cable.
3. Use a Phillips screwdriver to fasten the grounding screw into the grounding hole on the firewall.
4. Remove the grounding screw from the grounding point on the rack.
5. Use a pair of needle-nose pliers to bend a hook at the other end of the grounding cable. Attach the hook to the grounding post, and secure the hook with a screw.

**Figure2-12 Grounding the firewall with the grounding terminal on the rack**



## Installing a Micro SD card

**△ CAUTION:**

To avoid damaging the Micro SD card slot, do not use excessive force when you install a Micro SD card.

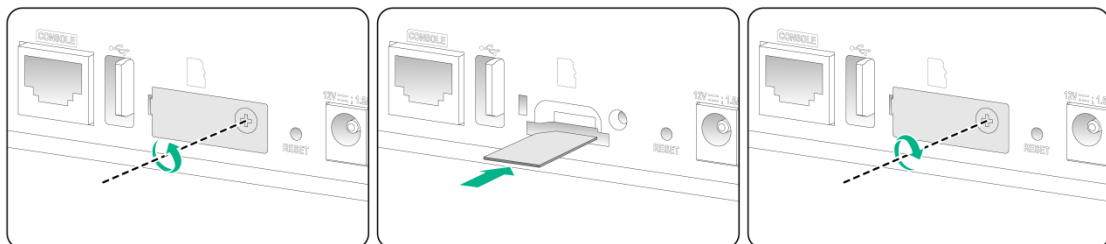
Only the NFNX3-HDB680 firewall supports Micro SD cards.

No Micro SD card is provided with the firewall. Purchase one as required.

To install a Micro SD card:

1. Face the front panel of the firewall. Use a Phillips screwdriver to remove the screw on the Micro SD card slot cover and take off the cover.
2. Push the Micro SD card into the slot until it clicks into place.
3. Reinstall the cover and fasten the screw on the cover.

**Figure2-13 Installing a Micro SD card**



## Installing a power supply

**△ CAUTION:**

- Before installing a power supply, make sure the power supply is powered off and the grounding cable is correctly connected.
- Do not install AC and DC power supplies on the same firewall.

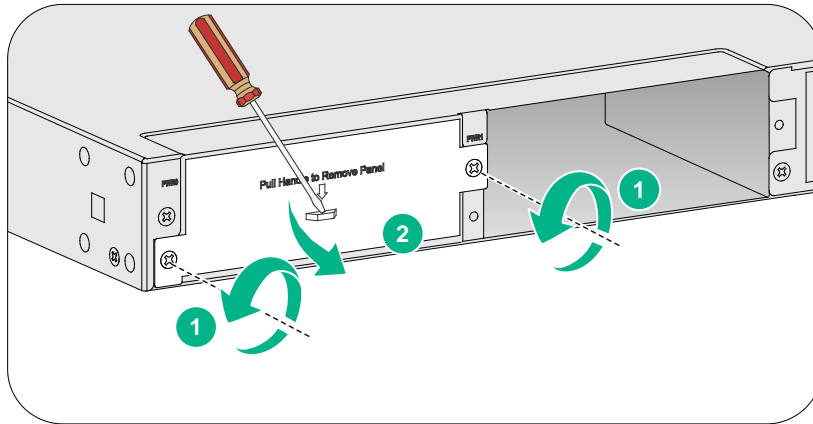
The NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280 firewalls support removable power supplies.



To install a power supply:

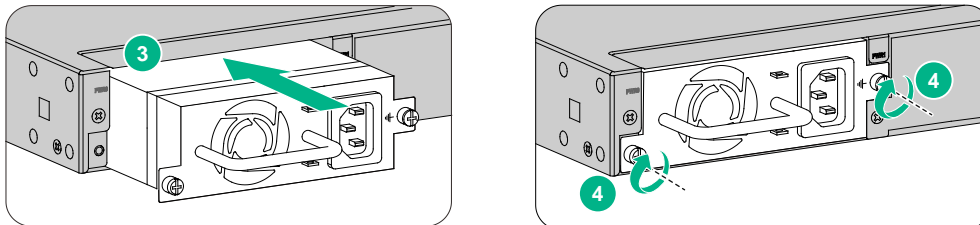
1. Face the rear panel of the firewall.
2. Remove the filler panel (if any) from the target power supply slot.  
The firewall comes with the PWR1 slot empty and the PWR0 slot installed with a filler panel.

**Figure2-14 Removing the filler panel**

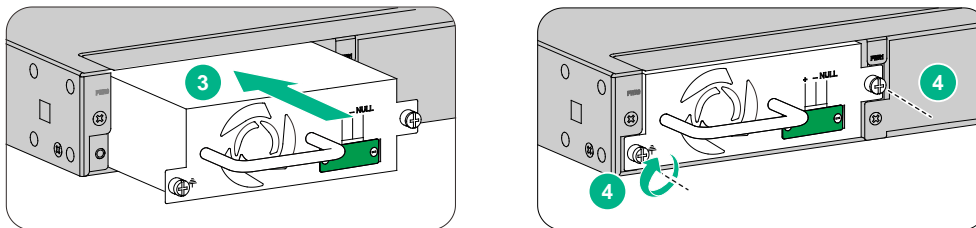


3. Orient the power supply with its handle at the left. Holding the handle of the module with one hand and supporting the module bottom with the other, slide the power supply slowly into the slot along the guide rails.
4. Use a Phillips screwdriver to fasten the captive screws on the power supply to secure the power supply in place.

**Figure2-15 Installing an AC power supply**



**Figure2-16 Installing a DC power supply**



# Installing an interface module

## ⚠ CAUTION:

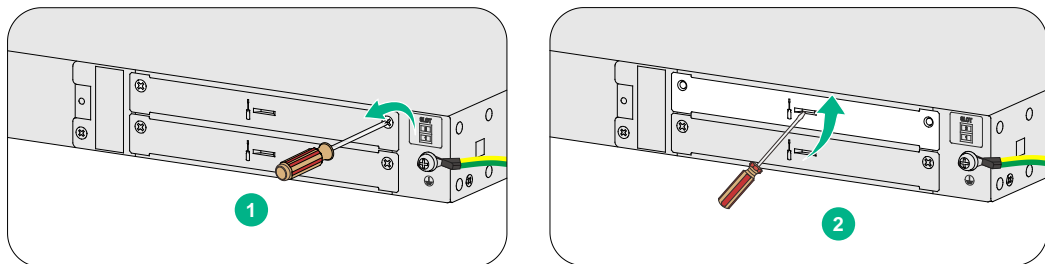
- Do not hot swap interface modules.
- For smooth interface module installation in the two interface module slots, use subslot 2 prior to subslot 1 as a best practice. If you are to install an interface module in subslot 2 after an interface module has been installed in subslot 1, you must press down the ejector levers of the interface module before inserting it into the Subslot 2.
- No interface modules are provided with the firewall. Purchase them as needed. For interface module compatibility with the firewalls, see "Appendix A Chassis views and technical specifications."

The NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280 firewalls support removable interface modules. The installation procedure is the same for all interface modules.

To install an interface module:

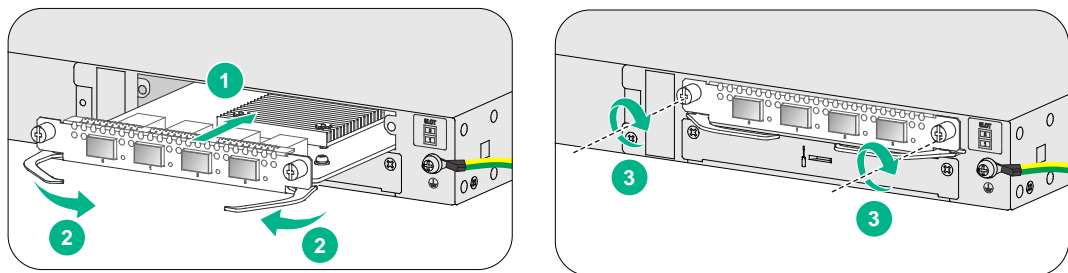
1. Face the rear panel of the firewall.
2. Use a Phillips screwdriver to remove the screws on the filler panel and then remove the filler panel.  
Keep the filler panel for future use.

**Figure2-17 Removing the filler panel**



3. Pull the ejector levers on the module outward and slide the module slowly into the slot along the guide rails.
4. Press the ejector levers inward until they touch the panel tightly and the module seats into the slot securely.
5. Use a Phillips screwdriver to fasten the captive screws on the module.

**Figure2-18 Installing an interface module**



# Installing a drive

## ⚠ CAUTION:

- Do not hot swap drives.
- To avoid damage to drives, always hold a drive by its sides. Do not touch any components and do not squeeze, vibrate, or strike a drive.
- Install a filler panel in empty drive slots to prevent dust and ESD damage.

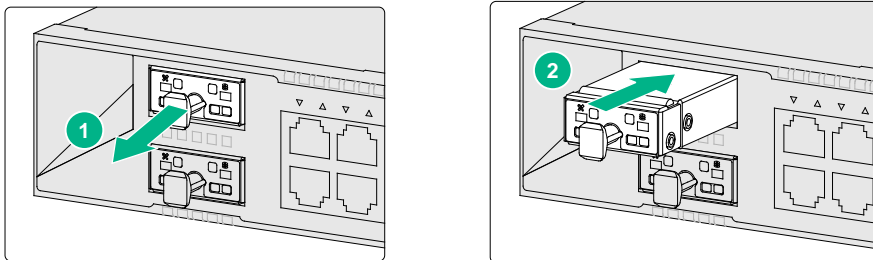
## ⚠ IMPORTANT:

- The device does not come with any drives. Purchase drives for the device as needed. For the drives to be identified by the system, purchase the drives from NSFOCUS.
- Before using the drive, execute the `fdisk` and `format` commands from the CLI to partition and format the drive.

## Installing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall

1. Wear an ESD wrist strap and make sure it makes good skin contact and is reliably grounded.
2. Remove the filler panel from the drive slot.
3. Push the drive into the slot slowly along the guide rails.

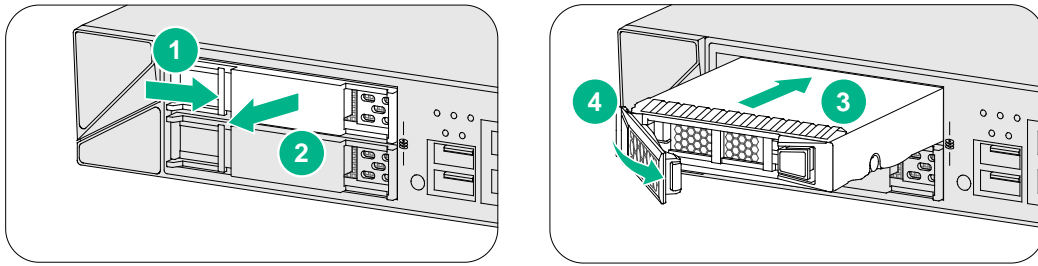
Figure2-19 Installing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall



## Installing a drive for other firewalls than the NFNX3-HDB1080, NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280

1. Wear an ESD wrist strap. Make sure it makes good skin contact and is reliably grounded.
2. Remove the filler panel from the drive slot.
3. Press the button on the drive panel to release the locking lever.
4. Hold the locking lever and push the drive into the slot slowly along the guide rails.
5. Close the locking lever.

Figure2-20 Installing a drive



## Connecting Ethernet cables

### Connecting a copper Ethernet port

You can use either a straight-through or a cross-over network cable. For more information about Ethernet twisted pair cables, see "Ethernet twisted pair cable."

To connect a copper Ethernet port:

1. Connect one end of the Ethernet cable to the copper Ethernet port of the firewall, and the other end to the Ethernet port of the peer device.
2. Examine whether the LEDs of the Ethernet port are normal. For more information about LEDs, see "Appendix B LEDs."

After connecting the firewall to the network, you can use the `ping` or `tracert` command to examine network connectivity. For more information, see the related command reference.

### Connecting a fiber port

---

**⚠ WARNING!**

Disconnected optical fibers or transceiver modules might emit invisible laser light. Do not stare into beams or view directly with optical instruments when the firewall is operating.

---

**⚠ CAUTION:**

- Never bend or curve a fiber excessively. The bend radius of a fiber must be not less than 100 mm (3.94 in).
  - Keep the fiber end clean.
  - Make sure the fiber connector matches the transceiver module.
  - Before connecting a fiber, make sure the optical power at the receiving end does not exceed the transceiver module's upper threshold of the optical receive power. If the optical power at the receiving end exceeds the threshold, the transceiver module might be damaged.
  - Do not install a transceiver module connected with a fiber into a fiber port. To connect an optical fiber, first install the transceiver module in the fiber port and then connect the fiber.
  - Insert a dust plug into any open fiber port.
  - Make sure the Tx and Rx ports on a transceiver module are connected to the Rx and Tx ports on the peer end, respectively.
- 

The firewall supports GE SFP transceiver modules and 10GE SFP+ transceiver modules. For the transceiver module specifications, see "Appendix A Chassis views and technical specifications."

**Figure2-21 GE SFP transceiver module**



**Figure2-22 10GE SFP+ transceiver module**

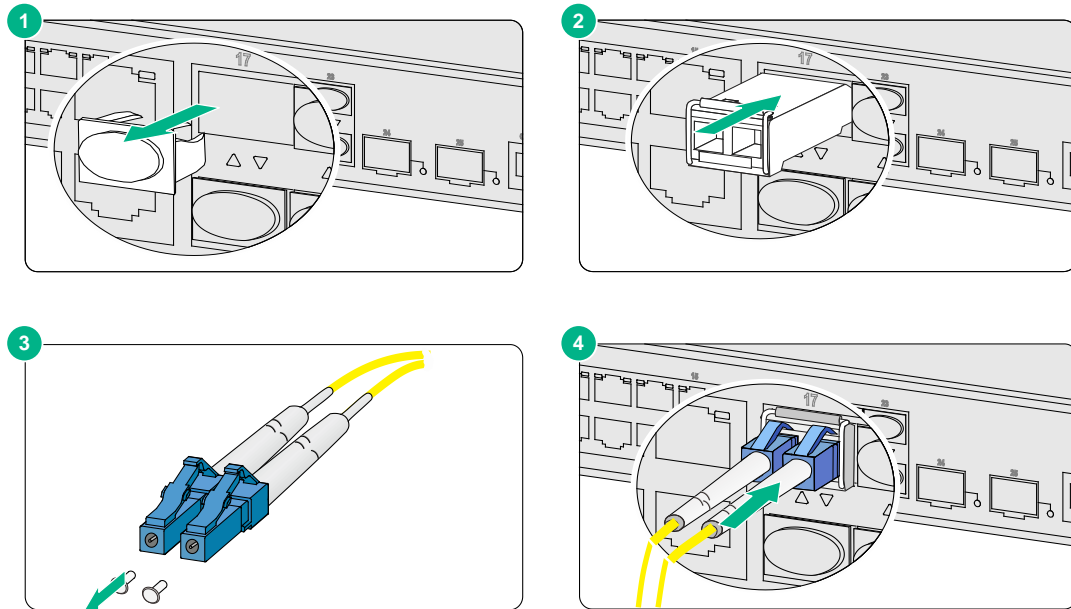


To connect the firewall to the network through an optical fiber:

1. Remove the dust plug from the fiber port.
2. Remove the dust cap from the transceiver module and insert it into the fiber port.
3. Remove the dust cap of the optical fiber connector, and use dust free paper and absolute alcohol clean the end face of the fiber connector.
4. Identify the Rx and Tx ports on the transceiver module. Plug one end of the optical fiber into the transceiver module in the firewall, and plug the other end into the transceiver module in the peer device.

Make sure the Rx port and the Tx port are connected to the Tx port and the Rx port on the peer device, respectively.

Figure2-23 Installing and connecting an optical fiber



## Connecting power cords

**△ CAUTION:**

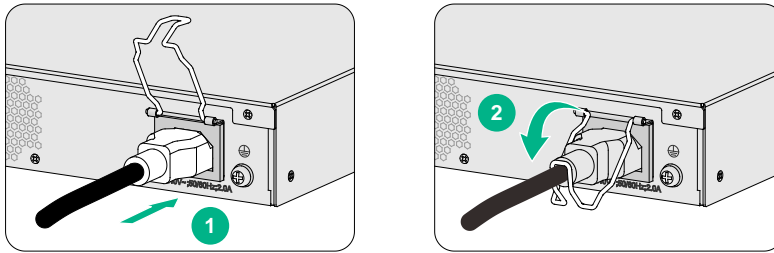
Make sure the grounding cable of the firewall is correctly connected and the power source is powered off before connecting the power cord.

## Connecting an AC power cord

### Connecting an AC power cord for an NFX3-HDB1080, NFX3-HDB1180, or NFX3-HDB1480 firewall

1. Attach the hooks of the power cord retainer clip into the holes on the top of the AC-input power receptacle, and pull the power cord retainer clip upwards.
2. Connect one end of the AC power cord to the AC-input power receptacle on the firewall.
3. Pull the power cord retainer clip downwards and secure the connector to the power receptacle.
4. Connect the other end of the power cord to an AC power source.

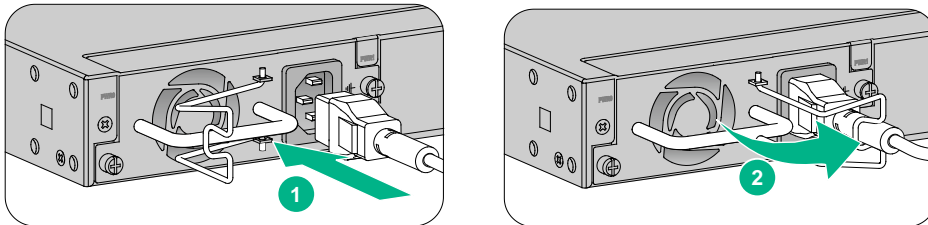
**Figure2-24 Connecting an AC power cord for an NFNX3-HDB1080, NFNX3-HDB1180, or NFNX3-HDB1480 firewall**



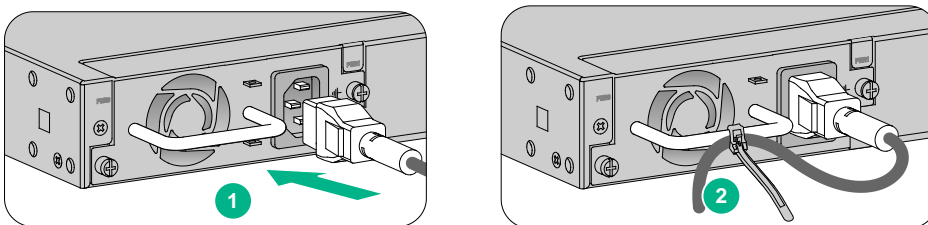
### Connecting an AC power cord for an NFNX3-HDB1780, NFNX3-HDB3080, or NFNX3-HDB3280 firewall

1. Attach the hooks of the power cord retainer clip into the holes next to the AC-input power receptacle, and pull the power cord retainer clip leftwards.
2. Connect the connector of the AC power cord to the target AC power receptacle on the rear panel of the chassis. Then use a power cord retainer clip (see [Figure2-25](#)) or a releasable cable tie (see [Figure2-26](#)) to secure the power cord.
3. Connect the other end of the power cord to an AC power source.

**Figure2-25 Connecting an AC power cord (using a power cord retainer clip to secure the power cord)**



**Figure2-26 Connecting an AC power cord (using a releasable cable tie to secure the power cord)**

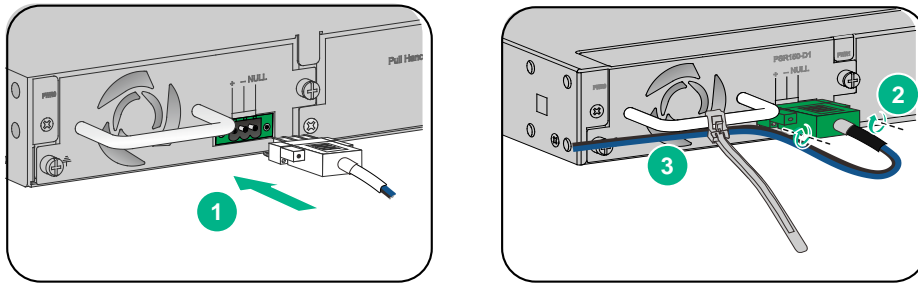


## Connecting a DC power cord

1. Correctly orient the DC power cord connector. Insert the connector into the power receptacle on the power supply.
2. Fasten the captive screws on the power cord connector with a flat-head screwdriver to secure the power cord connector.
3. Use a releasable cable tie to secure the power cord to the handle.

4. Connect the other end of the power cord to a DC power source.

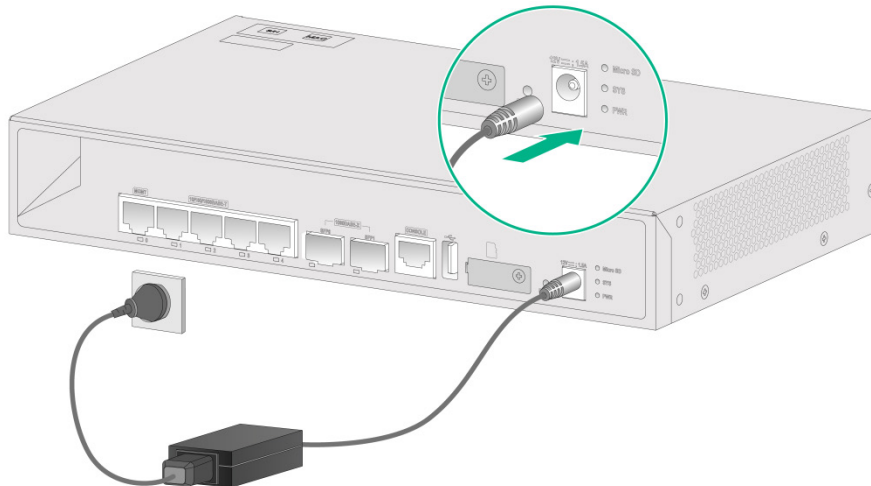
**Figure2-27 Connecting and securing a DC power cord**



## Connecting the power adapter for an NFNX3-HDB680 firewall

1. Make sure the firewall is reliably grounded.
2. Connect the power adapter to an external power source.
3. Connect the DC output plug of the power adapter to the power adapter receptacle on the firewall.

**Figure2-28 Connecting the power adapter for an NFNX3-HDB680 firewall**



## Verifying the installation

Verify the following items to ensure correct installation:

- There is enough space for heat dissipation around the firewall.
- The firewall and its components are installed securely. The screws are fastened tightly.
- The power source specifications are as required by the firewall.
- The grounding cable and power cords are connected correctly.



# 3 Accessing the firewall

## Starting the firewall

### Pre-start checking

**⚠ WARNING!**

Locate the emergency power-off switch in the room before powering on the firewall so you can quickly shut power off when an electrical accident occurs.

Before powering on the firewall, verify that the following conditions are met:

- The power cord and grounding cable are connected correctly.
- The power source specifications meet the firewall requirements.
- The firewall is connected correctly to a configuration terminal (a PC for example). The configuration terminal has been started and the parameters have been set correctly. For more information, see "[Logging in from the console port.](#)"
- The interface modules (if any) are installed correctly.

## Starting the firewall and observing the initial startup conditions

1. Turn on the circuit breakers to power on the firewall.
2. Observe the initial startup conditions to verify that the firewall starts up correctly.
  - o The LEDs on the front panel indicate that the device is operating correctly. For more information about LEDs, see "Appendix B LEDs."
  - o The fan blades are rotating and air is exhausted from the air outlet vents.
  - o The configuration terminal displays the following information:

The output on the configuration terminal varies by device software version.

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing.....Done.

*****
*
*                               BootWare, Version 1.03
*
*****

Copyright (c) 2021 NSFOCUS. All rights reserved.

Compiled Date       : May  8 2021
Memory Type        : DDR4 SDRAM
Memory Size        : 4096MB
```

```
Memory Speed      : 1600MHz
flash Size        : 3728MB
CPLD 1 Version    : 4.0
CPLD 2 Version    : 2.0
PCB 1 Version     : Ver.A
PCB 2 Version     : Ver.B
```

```
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
Loading the main image files...
Loading file flash:/main-cmwv6-BOOT-AXXXX.bin...Done.
Loading file flash:/main-cmwv6-SYSTEM-AXXXX.bin...Done.
Loading file flash:/main-cmwv6-BOOT-AXXXX.bin...Done.

Image file flash:/main-cmwv6-BOOT-AXXXX.bin is self-decompressing...
.....
.....Done.
System image is starting...
Cryptographic algorithms tests passed.
Line con0 is available.

Press ENTER to get started...
```

---

**NOTE:**

To access the EXTENDED-BOOTWARE menu, press **Ctrl + B** within four seconds at the prompt "Press Ctrl+B to access EXTENDED-BOOTWARE MENU." If you do not press **Ctrl+B** at the prompt, the system starts to read and decompress program files. To enter the EXTENDED-BOOT menu afterwards, you need to reboot the device.

---

## Logging in to the firewall

---

**!** **IMPORTANT:**

After accessing the device with the default account, immediately modify the password of the default account, or create a new administrator account and delete the default account as a best practice.

---

You can use the following methods to access and manage the firewall. For more information about logging in to the firewall, see the configuration guides and command references for the firewall.

- [Logging in from the Web interface](#)
- [Logging in from the console port](#)
- [Logging in through Telnet](#)

## Logging in from the Web interface

At the first login from the Web interface, you can use the default account or use an account created from the CLI. [Table3-1](#) shows the default Web interface login information.

**Table3-1 Default Web interface login information**

Item	Default configurations
Username	admin
Password	admin
Management Ethernet port	<ul style="list-style-type: none"><li>• NFNX3-HDB680/NFNX3-HDB1080: GigabitEthernet 1/0/0, 192.168.0.1/24</li><li>• NFNX3-HDB1180/NFNX3-HDB1480: 0/MGMT</li><li>• NFNX3-HDB1780/NFNX3-HDB3080/NFNX3-HDB3280:<ul style="list-style-type: none"><li>○ 0/MGMT</li><li>○ 1/MGMT</li></ul></li></ul>
IP address of the management Ethernet port	<ul style="list-style-type: none"><li>• <b>0/MGMT</b>—192.168.0.1/24</li><li>• <b>1/MGMT</b>—192.168.1.1/24</li></ul>

To log in to the firewall from the Web interface by using the default account:

1. Use an Ethernet cable to connect a PC to the management Ethernet port on the firewall.
2. Configure an IP address in subnet 192.168.0.0/24 for the PC. Make sure the PC and the firewall are reachable to each other.  
The PC must use a different IP address than the management Ethernet port.
3. Start a browser, enter **192.168.0.1** in the address bar, and press **Enter**.
4. Enter the default username **admin** and password **admin** and then click **Login**.
5. Modify the login information.

At the first login from the Web interface, change the password as required in the pop-up window, and then click **OK**.

Keep the new password secure.

## Logging in from the console port

By default, the firewall uses the scheme access authentication mode. The username and password are both **admin**.

To configure and manage the firewall from the console port, you must run a terminal emulator program, TeraTermPro or PuTTY, on your configuration terminal and configure the following settings for the terminal. For more information about the terminal emulator programs, see the user guides for these programs.

- **Bits per second**—9600.
- **Data bits**—8.
- **Stop bits**—1.
- **Parity**—None.
- **Flow control**—None.

## Logging in through Telnet

1. Log in to the firewall through the console port, and enable the Telnet function in system view by using the **telnet server enable** command.
2. Enter VTY user line view, and configure the authentication mode, user role, and common properties in VTY user line view.  
By default, the authentication mode is scheme, and the username and password are **admin**.
3. Connect a PC to the management Ethernet port M-GigabitEthernet1/0/0 on the firewall.

4. Specify an IP address for the network port of the PC. The IP address must be in subnet 192.168.0.0/24 and cannot be **192.168.0.1**.
5. Run the Telnet client on the PC and enter the default login information.

# 4 Hardware replacement

---

**△ CAUTION:**

Wear an ESD wrist strap or ESD gloves for hardware maintenance. They are not provided with the firewall. Prepare them yourself.

---

## Replacing a power supply

---

**△ CAUTION:**

Before you replace a power supply, turn off the circuit breaker and then remove the power cord.

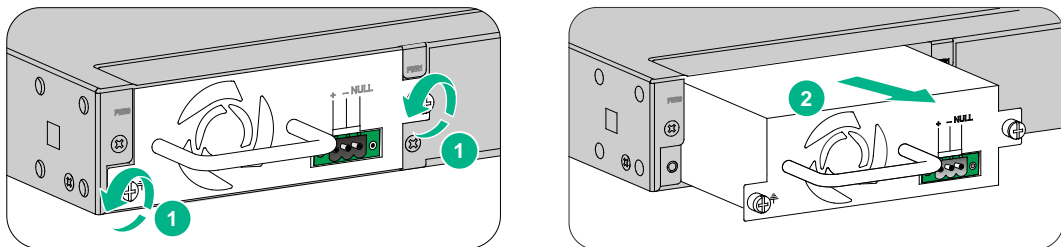
---

The replacement procedure is the same for an AC power supply and a DC power supply. This section takes a DC power supply as an example.

To replace a power supply:

1. Face the rear panel of the firewall.
2. Use a Phillips screwdriver to loosen the captive screws of the power supply.
3. Hold the power supply with one hand and pull the power supply part way out of the slot.
4. Supporting the bottom of the power supply with the other hand, gently pull the power supply out of the slot along the slide rails.

**Figure4-1 Removing a power supply**



5. Put the removed power supply on a workbench or into an antistatic bag.
6. Install a new power supply. If you do not install a new power supply in the slot, install a filler panel. For the installation procedure, see "[Installing a power supply.](#)"

## Replacing an interface module

---

**△ CAUTION:**

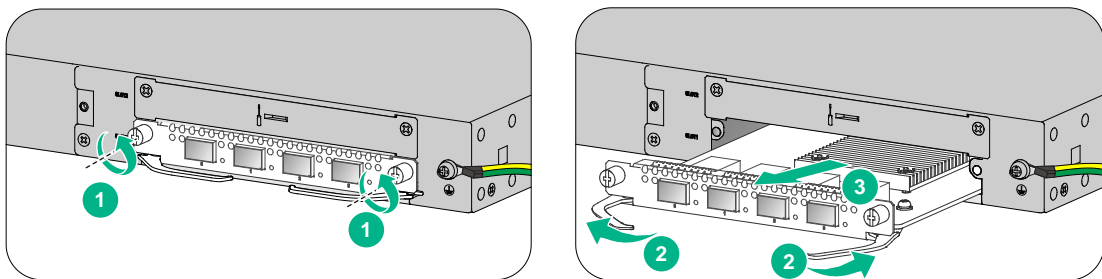
- Do not hot swap interface modules. Power off the firewall before you replace an interface module.
  - For smooth interface module installation in the two interface module slots, use subslot 2 prior to subslot 1 as a best practice. If you are to install an interface module in subslot 2 after an interface module has been installed in subslot 1 you must press down the ejector levers of the interface module before inserting it into subslot 2.
-

To replace an interface module:

1. Power off the firewall.
2. Use a Phillips screwdriver to loosen the captive screws of the interface module.
3. Holding the ejector levers of the interface module with both hands, pull the ejector levers outward, and pull the interface module part way out of the slot along the slide rails. Supporting the bottom of the interface module with one hand, gently pull the interface module out of the slot with the other.
4. Put the removed interface module (with the circuit board facing upward) on an antistatic workbench or into an antistatic bag.
5. Install a new interface module. For the installation procedure, see "[Installing an interface module](#)."

If you are not to install a new interface module, install a filler panel in the slot to ensure good ventilation in the firewall.

**Figure4-2 Removing an interface module**



## Replacing a drive

### ⚠ CAUTION:

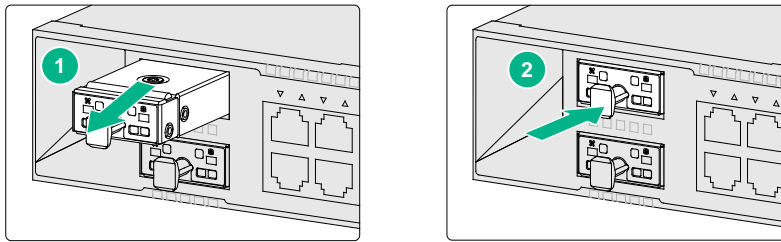
- To avoid storage medium damage, execute the `umount` command from the CLI to unmount all the file systems before removing a drive.
- Do not hot swap drives.

## Replacing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall

1. Log in to the Web interface. Click the **Unmount** button on the **Storage settings** page.
2. Wear an ESD wrist strap and make sure it makes good skin contact and is reliably grounded.
3. Pull the drive slowly out of the slot along the guide rails.
4. Install a new drive. For the installation procedure, see "[Installing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall](#)."

If you are not to install a new drive in the slot, install a filler panel in the slot to prevent dust and ensure good ventilation.

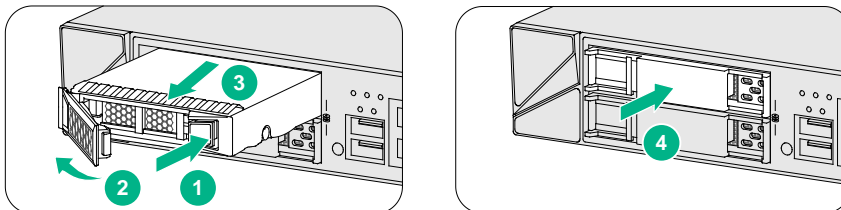
Figure4-3 Replacing a drive for an NFNX3-HDB1180 or NFNX3-HDB1480 firewall



## Replacing a drive for the NFNX3-HDB1080, NFNX3-HDB1780, NFNX3-HDB3080, or NFNX3-HDB3280 firewall

1. Log in to the Web interface. Click the **Unmount** button on the **Storage settings** page.
  2. Wear an ESD wrist strap and make sure it makes good skin contact and is reliably grounded.
  3. Press the button on the drive panel to release the locking lever.
  4. Hold the locking lever and pull the drive out of the slot.
  5. Install a new drive. For the installation procedure, see "[Installing a drive for other firewalls than the NFNX3-HDB1080, NFNX3-HDB1780, NFNX3-HDB3080, and NFNX3-HDB3280.](#)"
- If you are not to install a new drive in the slot, install a filler panel in the slot to prevent dust and ensure good ventilation.

Figure4-4 Removing a drive



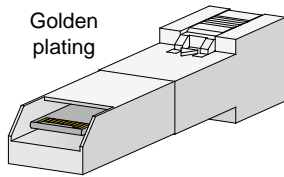
## Replacing a transceiver module

### **⚠ WARNING!**

Disconnected optical fibers or transceiver modules might emit invisible laser light. Do not stare into beams or view directly with optical instruments when the firewall is operating.

When you replace a transceiver module, make sure the two transceiver modules connected by the same optical fiber are the same type. Do not touch the golden plating of the transceiver module.

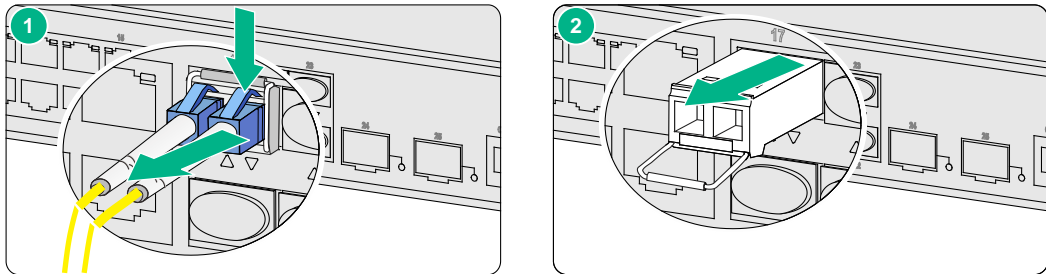
**Figure4-5 Transceiver module golden plating**



To replace a transceiver module:

1. Use the **shutdown** command in interface view at the CLI to shut down the optical source before you remove the fiber connector.
2. Remove the LC connectors with the optical fiber from the transceiver module, and install dust caps to the LC connectors.
3. Pivot the clasp of the transceiver module down to the horizontal position, and gently pull the transceiver module out.

**Figure4-6 Removing the transceiver module**



4. Install dust caps to the removed transceiver module, and put it into the package.
5. Install a new transceiver module. If you do not install a new transceiver module in the slot, install a dust cap. For information about installing a transceiver module, see "[Connecting a fiber port.](#)"



# 5 Hardware management and maintenance

---

**NOTE:**

The output depends on your firewall model. For more information about the commands used in this chapter, see the configuration guides and command references for the firewall.

---

## Displaying detailed information about the firewall

Use the **display device verbose** command to display detailed information, including the running status and hardware version, about the firewall and its interface modules.

```
Slot 1 SubSlot 0 info:
Status           : Normal
Type             : NF
PCB 1 Ver        : VER.A
Software Ver     : 8860P16
CPU Ver          : 1.0
CPLD_A           : 4.0
CPLD_B           : 2.0
CFCard Num       : 0
```

## Displaying the software and hardware version information for the firewall

Use the **display version** command to display software and hardware version information for the firewall.

```
<Sysname> display version
NSFOCUS NF Software, Version 6.0, Ess 8860P16
Copyright (c) 2021 NSFOCUS. All rights reserved.
NSFOCUS NF uptime is 0 weeks, 0 days, 0 hours, 5 minutes
Last reboot reason: User reboot

Boot image: flash:/main-cmwv6-BOOT-AXXXX.bin
Boot image version: 7.1.064, Test XXXX
  Compiled Jul 14 2021 15:00:00
System image: flash:/main-cmwv6-SYSTEM-AXXXX.bin
System image version: 7.1.064, Test XXXX
  Compiled Jul 14 2021 15:00:00
SLOT 1
CPU type:           Multi-core CPU
DDR4 SDRAM Memory: 8192M bytes
FLASH:             3728M bytes
CPLD_A              Version:128.0
```

## Displaying the electrical label information for the firewall

Use the **display device manuinfo** command to display the electrical label information for the firewall.

```
Slot 1 CPU 0:  
DEVICE_NAME               : NFNX3-HDB3280  
DEVICE_SERIAL_NUMBER     : 210235A45Q9196Q0000B  
MAC_ADDRESS               : 0868-8DBC-3B73  
MANUFACTURING_DATE       : NONE  
VENDOR_NAME               : NONE
```

**Table5-1 Output description**

Field	Description
DEVICE_NAME	Firewall name.
DEVICE_SERIAL_NUMBER	Firewall serial number.
MAC_ADDRESS	MAC address of the firewall.
MANUFACTURING_DATE	Manufacturing date of the firewall.
VENDOR_NAME	Vendor name.

## Displaying the CPU usage of the firewall

Use the **display cpu-usage** command to display the CPU usage of the firewall.

```
<Sysname> display cpu-usage  
Slot 1 CPU 0 CPU usage:  
    3% in last 5 seconds  
    3% in last 1 minute  
    3% in last 5 minutes
```

**Table5-2 Output description**

Field	Description
Slot 1 CPU 0 CPU usage	CPU 0 usage information for the interface module in slot 1.
3% in last 5 seconds	Average CPU usage in the last 5 seconds. (After the firewall boots, the firewall calculates and records the average CPU usage at the interval of 5 seconds.)
3% in last 1 minute	Average CPU usage in the last minute. (After the firewall boots, the firewall calculates and records the average CPU usage at the interval of 1 minute.)
3% in last 5 minutes	Average CPU usage in the last 5 minutes. (After the firewall boots, the firewall calculates and records the average CPU usage at the interval of 5 minutes.)

# Displaying the memory usage of the firewall

Use the **display memory** command to display the memory information of the firewall.

```
<Sysname> display memory
```

Memory statistics are measured in KB:

Slot 1:

```

                Total      Used      Free      Shared  Buffers  Cached  FreeRatio
Mem:           8212672  4655360  3557312         0   17152   549952    43.9%
-/+ Buffers/Cache:  4088256  4124416
Swap:           0         0         0

```

**Table5-3 Output description**

Field	Description
Slot	Slot number of the interface module
Mem	Memory usage information.
Total	Total size of the physical memory space that can be allocated. The memory space is virtually divided into two parts. Part 1 is used for kernel codes, kernel management, and ISSU functions. Part 2 can be allocated and used for such tasks as running service modules and storing files. The size of part 2 equals the total size minus the size of part 1.
Used	Used physical memory.
Free	Free physical memory.
Shared	Physical memory shared by processes.
Buffers	Physical memory used for buffers.
Cached	Physical memory used for caches.
FreeRatio	Free memory ratio.
-/+ Buffers/Cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which indicates the physical memory used by applications. -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates the physical memory available for applications.
Swap	Swap memory.

# Displaying the temperature information of the firewall

Use the **display environment** command to display the temperature information of the firewall.

```
<Sysname> display environment
```

System Temperature information (degree centigrade):

```

-----
-----
Slot      Sensor  Temperature LowerLimit Warning-UpperLimit Alarm-UpperLimit
Shutdown-UpperLimit
1         inflow  1          31           0                47                52
60

```

1	outflow 1	39	0	68	80
	88				
1	hotspot 1	47	0	63	68
	75				
1	hotspot 2	54	0	84	97
	102				

**Table5-4 Output description**

Field	Description
Sensor	Temperature sensor: <ul style="list-style-type: none"> <li><b>inflow</b>—Air inlet vent temperature sensor.</li> <li><b>outflow</b>—Air outlet vent temperature sensor.</li> <li><b>hotspot</b>—Hotspot temperature sensor.</li> </ul>
Temperature	Current temperature.
LowerLimit	Low temperature alarm threshold.
Warning-UpperLimit	Warning-level high temperature alarm threshold.
Alarm-UpperLimit	Alarm-level high temperature alarm threshold.
Shutdown-Upperlimit	Shutdown-level high temperature alarm threshold. The firewall automatically powers off when the temperature exceeds this threshold.

## Displaying the operational statistics of the firewall

When you perform routine maintenance or the system fails, you might need to view the operational information of each functional module for locating failures. Typically you need to run **display** commands one by one. To collect more information one time, you can execute the **display diagnostic-information** command in any view to display or save the operational statistics of multiple functional modules of the firewall.

- Save the operational statistics of each functional module of the firewall:

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_NF_20211029-112744.tar.gz]:
Diagnostic information is outputting to flash:/diag_NF_20211029-112744.tar.gz.
Please wait...
Save successfully.
To view the diag.gz file:
a. In user view, execute the tar extract archive-file diag.tar.gz command and then the gunzip diag.gz command to decompress the file.
b. Execute the more diag command.
c. Press Pg Up and Pg Down.
```
- Display the operational statistics for each functional module of the firewall:

```
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
=====
=====display clock=====
11:28:55 UTC Fri 10/29/2021
=====
=====dir core/=====
```

```

The file or directory doesn't exist.
=====
=====display version=====
NSFOCUS NF Software, Version 6.0, Ess 8860P16
Copyright (c) 2021 NSFOCUS. All rights reserved.
NSFOCUS NF uptime is 0 weeks, 0 days, 0 hours, 9 minutes
Last reboot reason: User reboot
...

```

## Displaying transceiver module information

### Identifying transceiver modules

To identify transceiver modules, you can use the following command to view the key parameters of the transceiver modules, including transceiver module type, connector type, central wavelength of the laser sent, transmission distance, and vendor name or name of the vendor who customizes the transceiver modules.

To display transceiver module information:

Task	Command	Remarks
Display key parameters of the transceiver module in a specific interface.	<b>display transceiver interface</b> [ <i>interface-type</i> <i>interface-number</i> ]	Available for all transceiver modules.

### Troubleshooting transceiver modules

The system outputs alarm information for you to locate and troubleshoot faults of transceiver modules.

To display the alarming information or fault detection parameters of a transceiver module:

Task	Command	Remarks
Display the current alarm information of the transceiver module in a specific interface.	<b>display transceiver alarm interface</b> [ <i>interface-type</i> <i>interface-number</i> ]	Available for all transceiver modules.

## Rebooting the firewall

### ⚠ CAUTION:

- If the main system software image file does not exist, do not use the **reboot** command to reboot the firewall. Specify the main system software image file first, and then reboot the firewall.
- The precision of the rebooting timer is 1 minute. 1 minute before the rebooting time, the firewall prompts "REBOOT IN ONE MINUTE" and reboots in one minute.
- If you are performing file operations when the firewall is to be rebooted, the system does not execute the reboot command for security.

To reboot a firewall, use one of the following methods:

- Use the **reboot** command to reboot the firewall immediately.

- Enable the scheduled reboot function at the CLI. You can set a time at which the firewall can automatically reboot, or set a delay so that the firewall can automatically reboot within the delay.
- Power on the firewall after powering it off, which is also called hard reboot or cold start. As a best practice, do not use this method because it might cause data loss and hardware damages.

To reboot the firewall immediately:

Task	Command	Remarks
Reboot the firewall immediately.	<b>reboot</b>	Available in user view.

To enable the scheduled reboot function:

Task	Command	Remarks
Enable the scheduled reboot function.	<ul style="list-style-type: none"> <li>• Enable the scheduled reboot function and specify a specific reboot time and date: <b>scheduler reboot at</b></li> <li>• Enable the scheduled reboot function and specify a reboot waiting time: <b>scheduler reboot delay</b></li> </ul>	<p>Use either approach.</p> <p>The scheduled reboot function is disabled by default.</p> <p>Available in user view.</p>

# 6 Troubleshooting

## Power supply failure

### Symptom

The firewall cannot be powered on, and the power LED (PWR0/PWR1) on the front panel is off.

### Solution

To solve the issue:

1. Power off the firewall.
2. Verify that the power supply is as required by the firewall.
3. Verify that the power cords of the firewall are firmly connected.
4. Verify that the power cords are not damaged.
5. If the issue persists, contact your local sales agent.

## Configuration terminal display issue

### Symptom

The configuration terminal displays nothing or garbled text when the firewall is powered on.

### Solution

To solve the issue:

1. Verify that the power supply system is operating correctly.
2. Verify that the console cable is correctly connected.
3. Verify that the console cable is connected to the serial port configured on the configuration terminal.
4. Verify that the configuration terminal parameters are configured as follows:
  - **Baud rate**—9600.
  - **Data bits**—8.
  - **Parity**—None.
  - **Stop bits**—1.
  - **Flow control**—None.
  - **Terminal emulation**—VT100.
5. Verify that the console cable is in good condition.
6. If the issue persists, contact your local sales agent.

## Password loss

To deal with loss of the password used for accessing the firewall through the console port, see the release notes for the firewall.

# Cooling system failure

## Symptom

The temperature of the firewall is higher than the normal operating temperature (45°C or 113°F).

## Solution

To solve the issue:

1. Verify that the fans are operating correctly.
2. Verify that the operating environment of the firewall has good ventilation.
3. If the following alarm information is generated, the temperature of the firewall has reached the warning-level high temperature alarm threshold.

```
%Nov 28 20:02:59:085 2022 NSFOCUS DEV/4/TEMPERATURE_WARNING: -Context=1; Temperature is greater than the high-temperature warning threshold on slot 1 sensor outflow 1. Current temperature is 58 degrees centigrade.
```

Use the **display environment** command to examine whether the temperature of the firewall keeps rising. If the temperature has reached the alarming-level high temperature alarm threshold, power off the firewall, and contact your local sales agent. If the temperature has reached the shutdown-level high temperature alarm threshold, the device will shut down automatically.

Information about the firewall temperature in the **display environment** command output varies by firewall model.

4. If the issue persists, contact your local sales agent.

# Software loading failure

## Symptom

Software loading fails and the system runs the software of the previous version.

## Solution

To solve the issue:

1. Verify that the physical ports are correctly connected.
2. Verify that no parameter is configured incorrectly during the loading process. You can examine the software loading process displayed on the HyperTerminal for configuration errors. The following errors can lead to software loading failure.
  - When XMODEM is used to load software, a baud rate other than 9600 bps is selected, but the baud rate for the HyperTerminal is not reset.
  - When TFTP is used to load software, an incorrect IP address, software name, or TFTP serve path is configured.
  - When FTP is used to load software, an incorrect IP address, software name, username, or password is entered.
3. If the issue persists, contact your local sales agent.



# 7 Appendix A Chassis views and technical specifications

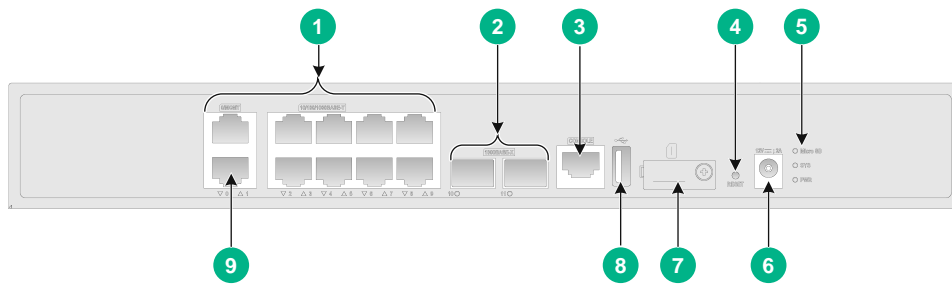
## Chassis views

### NFNX3-HDB680

The NFNX3-HDB680 firewall provides the following ports on the front panel:

- Two 1000BASE-X Ethernet fiber ports.
- Five 10/100/1000BASE-T autosensing Ethernet copper ports (including one management Ethernet port).
- One USB port.
- One console port.
- One Micro SD card slot.

**Figure7-1 Front panel**



(1) 10/100/1000BASE-T copper ports	(2) 1000BASE-X fiber ports
(3) Console port	(4) Reset button
(5) Micro SD card, system status (SYS), and power status (PWR) LEDs	
(6) DC-input power receptacle	(7) Micro SD card slot
(8) USB port (host mode, Type A)	(9) Management Ethernet port (MGMT)

**NOTE:**

The reset button restarts the firewall. It does not restore the factory defaults.

**Figure7-2 Rear panel**



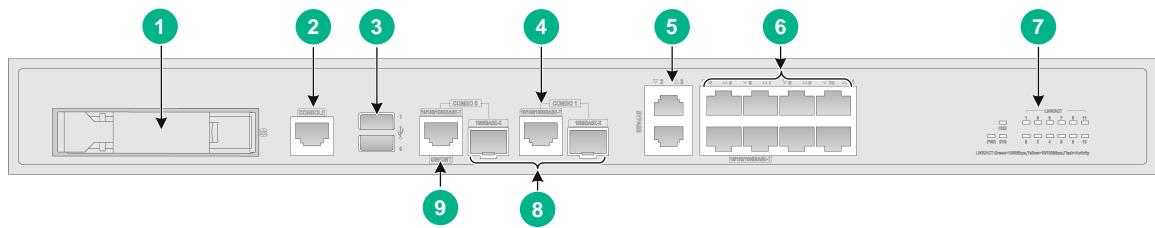
(1) Grounding screw
---------------------

# NFNX3-HDB1080

The NFNX3-HDB1080 firewall provides the following ports on the front panel:

- Eight 10/100/1000BASE-T autosensing Ethernet copper ports.
- Two combo interfaces.
- Two bypass ports.
- One USB port.
- One console port.
- One drive slot.

**Figure7-3 Front panel**



(1) Drive slot	(2) Console port
(3) USB port (host mode, type A)	(4) 10/100/1000BASE-T copper port (combo interface)
(5) Bypass ports	(6) 10/100/1000BASE-T copper ports
(7) LEDs	(8) 1000BASE-X fiber ports (combo interfaces)
(9) Management Ethernet port (0/MGMT, combo interface)	

**Figure7-4 Rear panel**



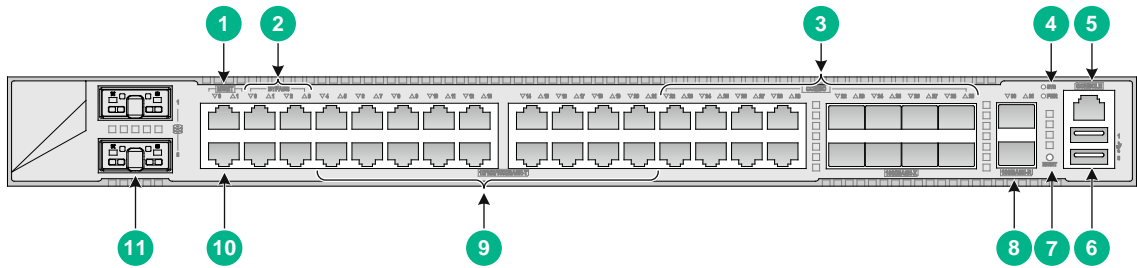
(1) Grounding screw	(2) Power receptacle
---------------------	----------------------

# NFNX3-HDB1180/NFNX3-HDB1480

The NFNX3-HDB1180/NFNX3-HDB1480 firewall provides the following ports on the front panel:

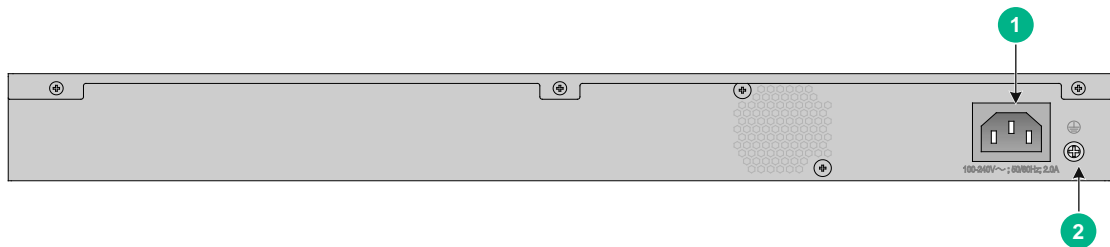
- Eighteen 10/100/1000BASE-T autosensing Ethernet copper ports.
- Two 10GBASE-R fiber ports.
- Two management Ethernet ports.
- Four bypass ports.
- Eight combo interfaces.
- One console port.
- Two USB ports.
- One reset button.
- Two drive slots.

**Figure7-5 Front panel**



(1) Management Ethernet port (0/MGMT)	(2) Bypass ports
(3) Combo interfaces	(4) LEDs
(5) Console port	(6) USB port (host mode, type A)
(7) Reset button	(8) 10GBASE-R fiber port
(9) 10/100/1000BASE-T copper ports	(10) Management Ethernet port (1/MGMT)
(11) Drive slots	

**Figure7-6 Rear panel**



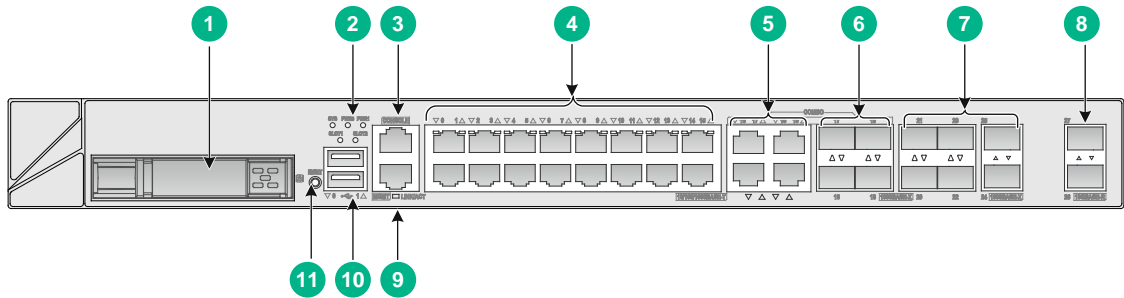
(1) Power receptacle 1	(2) Grounding screw
------------------------	---------------------

## NFNX3-HDB1780/NFNX3-HDB3080

The NFNX3-HDB1780/NFNX3-HDB3080 firewall provides the following ports on the front panel:

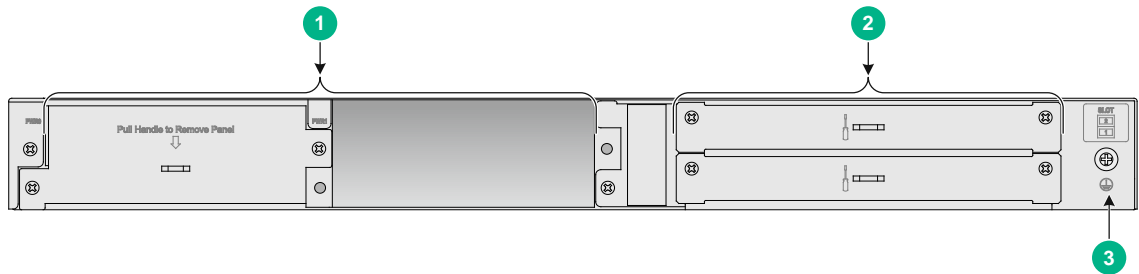
- Sixteen 10/100/1000BASE-T autosensing Ethernet copper ports.
- Four combo interfaces.
- Six 1000BASE-X fiber ports.
- Two 10GBASE-R fiber ports.
- Two USB ports.
- One console port.
- One drive slot.
- One management Ethernet port.

**Figure7-7 Front panel**



(1) Drive slot	(2) LEDs
(3) Console port	(4) 10/100/1000BASE-T copper ports
(5) 10/100/1000BASE-T copper ports (combo interfaces)	(6) 1000BASE-X fiber ports (combo interfaces)
(7) 1000BASE-X fiber ports	(8) 10GBASE-R fiber port
(9) Management Ethernet port (MGMT)	(10) USB port (host mode, Type A)
(11) Reset button	

**Figure7-8 Rear panel**



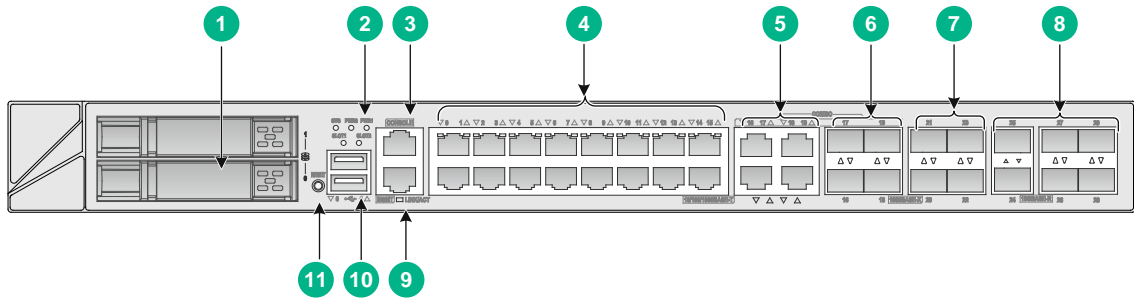
(1) Power supply slots	(2) Interface module slots
(3) Grounding screw	

## NFNX3-HDB3280

The NFNX3-HDB3280 firewall provides the following ports on the front panel:

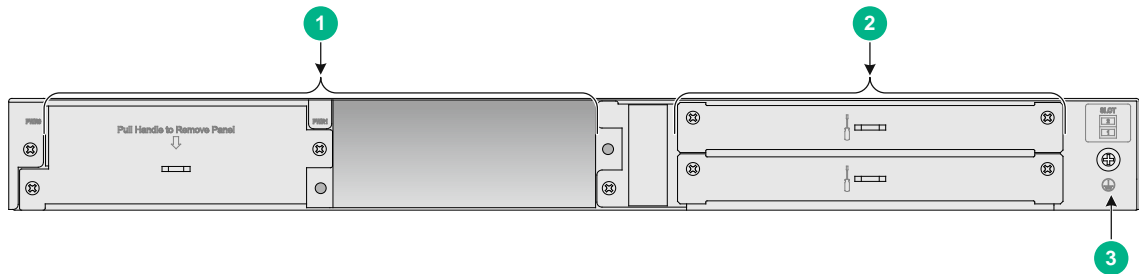
- Sixteen 10/100/1000BASE-T autosensing Ethernet copper ports.
- Four combo interfaces.
- Four 1000BASE-X fiber ports.
- Six 10GBASE-R fiber ports.
- Two USB ports.
- One console port.
- Two drive slots.
- One management Ethernet port.

**Figure7-9 Front panel**



(1) Drive slot	(2) LEDs
(3) Console port	(4) 10/100/1000BASE-T copper ports
(5) 10/100/1000BASE-T copper ports (combo interfaces)	(6) 1000BASE-X fiber ports (combo interfaces)
(7) 1000BASE-X fiber ports	(8) 10GBASE-R fiber ports
(9) Management Ethernet port (MGMT)	(10) USB port (host mode, Type A)
(11) Reset button	

**Figure7-10 Rear panel**



(1) Power supply slots	(2) Interface module slots
(3) Grounding screw	

## Interface modules

**CAUTION:**  
Do not hot swap interface modules.

Table7-1 displays the compatible slots for the interface modules.

**Table7-1 Interface module and device slot compatibility**

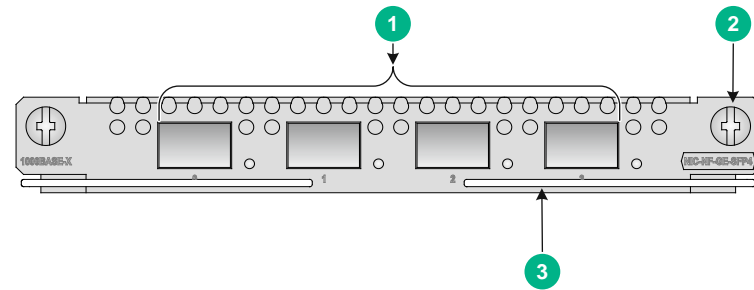
Firewall model	Slot number	Slot speed	Compatible interface module
NFNX3-HDB680/NFNX3-HDB1080/NFNX3-HDB1180/NFNX3-HDB1480	N/A	Not supported	Not supported
NFNX3-HDB1780/NFNX3-HDB3080	SUBSLOT 1, SUBSLOT 2	Low speed	NIC-NF-GE-SFP4
NFNX3-HDB3280	SUBSLOT 1	High speed	NIC-NF-10GE-SFP6

Firewall model	Slot number	Slot speed	Compatible interface module
	SUBSLOT 2	Low speed	NIC-NF-GE-SFP4

## NIC-NF-GE-SFP4

The NIC-NF-GE-SFP4 interface module provides four 1000BASE-X fiber ports.

**Figure7-11 Front panel of the NIC-NF-GE-SFP4 interface module**



(1) 1000BASE-X fiber ports

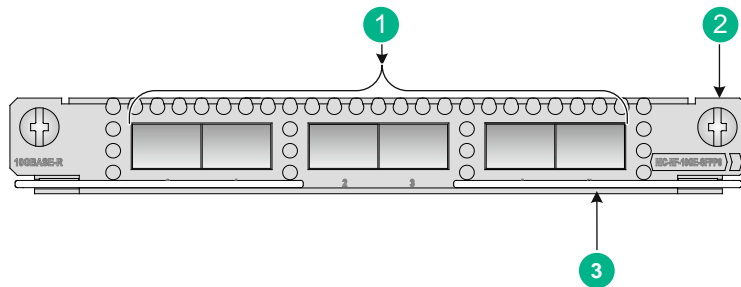
(2) Captive screw

(3) Ejector lever

## NIC-NF-10GE-SFPP6

The NIC-NF-10GE-SFPP6 interface module provides six 10GBASE-R fiber ports.

**Figure7-12 Front panel of the NIC-NF-10GE-SFPP6 interface module**



(1) 10GBASE-R fiber ports

(2) Captive screw

(3) Ejector lever

## Drives

### △ CAUTION:

Do not hot swap drives.

Table7-2 displays drive compatibility with the firewalls.

**Table7-2 Drive compatibility with the firewalls**

Drive model	NFNX3-HDB1180/NFNX3-HDB1480	NFNX3-HDB1080/NFNX3-HDB1780/NFNX3-HDB3080/NFNX3-HDB3280
SSD-M.2-480G	Supported	Not supported
SSD-2.5inch-SATA-480G	Not supported	Supported

## Power supplies

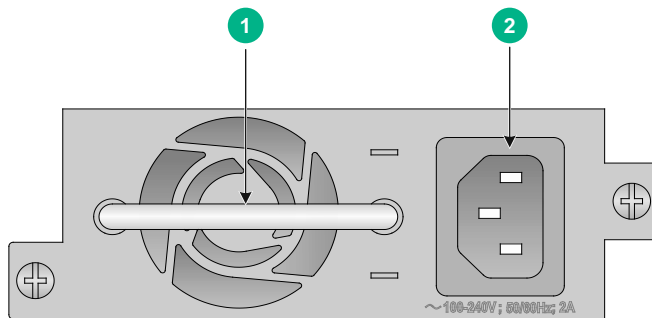
The firewall provides two power supply slots PWR0 and PWR1 and supports both AC and DC removable power supplies. No power supplies are provided with the firewall. Prepare power supplies for the firewall yourself as required.

The firewall supports 1+1 power supply redundancy. To install two power supplies for the firewall, make sure they are the same model.

### AC power supplies

The device supports the PW-150W-AC AC power supply that provides a maximum output power of 150 W.

**Figure7-13 PW-150W-AC AC power supply**



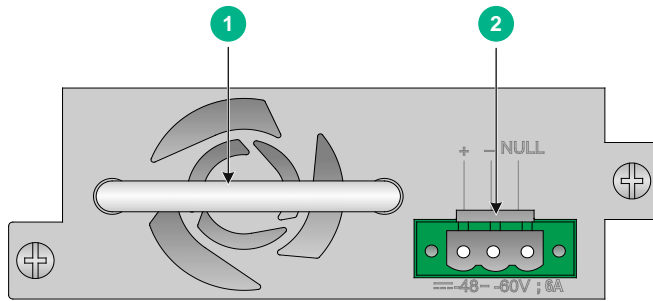
(1) Handle

(2) AC-input power receptacle

### DC power supplies

The device supports the PW-150W-DC DC power supply that provides a maximum output power of 150 W.

Figure7-14 PW-150W-DC DC power supply



(1) Handle

(2) DC-input power receptacle

## Dimensions and weights

The weight of the firewall includes the chassis and its removable components.

### Chassis

Table7-3 Chassis dimensions and weights

Firewall model	Dimensions (H x W x D), excluding rubber feet and mounting brackets	Net weight (chassis only)
NFNX3-HDB1080	44 x 440 x 230 mm (1.73 x 17.32 x 9.06 in)	3 kg (6.61 lb)
NFNX3-HDB1180/NFNX3-HDB1480	43.6 x 440 x 260 mm (1.72 x 17.32 x 10.24 in)	3.7 kg (8.16 lb)
NFNX3-HDB1780/NFNX3-HDB3080	44.2 x 440 x 435 mm (1.74 x 17.32 x 17.13 in)	5.4 kg (11.90 lb)
NFNX3-HDB3280	44.2 x 440 x 435 mm (1.74 x 17.32 x 17.13 in)	5.6 kg (12.35 lb)

### Interface modules

Table7-4 Interface module dimensions and weights

Interface module model	Dimensions (H x W x D)	Weight
NIC-NF-GE-SFP4	19 x 150 x 172.9 mm (0.75 x 5.91 x 6.81 in)	0.40 kg (0.88 lb)
NIC-NF-10GE-SFPP6	19 x 150 x 172.9 mm (0.75 x 5.91 x 6.81 in)	0.40 kg (0.88 lb)

### Drives

Table7-5 Drive dimensions and weights

Drive model	Dimensions (H x W x D)	Weight
SSD-M.2-480G	12.1 x 27.1 x 99.4 mm (0.48 x 1.07 x 3.91 in)	0.05 kg (0.11 lb)
SSD-2.5inch-SATA-480G	19 x 75.7 x 118.4 mm (0.75 x 2.98 x 4.66 in)	0.07 kg (0.15 lb)



# Storage media

**Table7-6 Storage media specifications**

Firewall model	Memory
NFNX3-HDB680/NFNX3-HDB1080/NFNX3-HDB1180/NFNX3-HDB1480	2GB DDR4
NFNX3-HDB1780/NFNX3-HDB3080	4GB DDR4
NFNX3-HDB3280	8GB DDR4

**Table7-7 Memory specifications of drives**

Drive model	Memory
SSD-M.2-480G	480 GB
SSD-2.5inch-SATA-480G	480 GB

# Power consumption

The system power consumption includes the power consumptions of the chassis and the removable components.

# Chassis

**Table7-8 Chassis power consumption**

Firewall model	Maximum power consumption
NFNX3-HDB680	12 W
NFNX3-HDB1080	30 W
NFNX3-HDB1180/NFNX3-HDB1480	39 W
NFNX3-HDB1780/NFNX3-HDB3080	23 W
NFNX3-HDB3280	46 W

# Interface modules

**Table7-9 Interface module power consumption**

Interface module model	Power consumption
NIC-NF-GE-SFP4	10.4 W
NIC-NF-10GE-SFP6	11 W

# Drives

**Table7-10 Drive power consumption**

Drive model	Power consumption
SSD-M.2-480G	4.5 W
SSD-2.5inch-SATA-480G	3 W

# Power supply specifications

**Table7-11 AC power supply specifications**

Item	Specifications
Model	PW-150W-AC
Rated input voltage range	100 VAC to 240 VAC @ 50 Hz or 60 Hz
Maximum input current	2 A
Maximum power	150 W

**Table7-12 DC power supply specifications**

Item	Specifications
Model	PW-150W-DC
Rated input voltage range	-48 VDC to -60 VDC
Maximum input current	6 A
Maximum power	150 W

# Port specifications

## Console port

**Table7-13 Console port specifications**

Item	Specification
Connector	RJ-45
Standard compliant	RS-232
Baud rate	9600 bps (default) to 115200 bps
Cable type	Common asynchronous serial port cable
Transmission distance	≤ 15 m (49.21 ft)
Services	<ul style="list-style-type: none"><li>• Connection to an ASCII terminal</li><li>• Connection to the serial port of a local PC running the terminal emulation program</li><li>• CLI</li></ul>

## GE copper port

**Table7-14 GE copper port specifications**

Item	Specification
Connector	RJ-45
Standard compliance	802.3, 802.3u, and 802.3ab
Interface type	MDI/MDI-X autosensing
Cable type	Category 5 or higher twisted pair cable
Transmission distance	100 m (328.08 ft)
Interface speed and duplex mode	10 Mbps, half/full-duplex 100 Mbps, half/full-duplex 1000 Mbps, full-duplex

**NOTE:**

The interfaces on a network interface card are typically media dependent interface (MDI) interfaces. The interfaces on a hub or LAN switch are typically media dependent interface crossover (MDI-X) interfaces.

## GE fiber port

**Table7-15 GE fiber port specifications**

Item	Specification
Connector type	LC
Transceiver module type	SFP
Standard compliance	1000BASE-X
Interface speed	1000 Mbps
Duplex mode	Full duplex

## 10 GE fiber port

**Table7-16 10 GE fiber port specifications**

Item	Specification
Connector type	LC
Transceiver module type	SFP+
Standard compliance	10GBASE-R
Interface speed	LAN PHY: 10.3125 Gbps

# 8 Appendix B LEDs

## NFNX3-HDB680

**Table8-1 LED description for the NFNX3-HDB680 firewall**

LED	Mark	Status	Description
10/100/1000BASE-T copper port LED	10/100/1000BASE-T	Off	No link is present.
		Steady green	A link is present.
		Flashing green	The port is receiving and sending data.
1000BASE-X fiber port LED	1000BASE-X	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
Micro SD card LED	Micro SD	On	A Micro SD card is present.
		Off	No Micro SD card is detected.
Power status LED	PWR	Off	The power system is faulty.
		Steady green	The power system is operating correctly.
System status LED	SYS	Off	The firewall is not powered on or has failed.
		Slow flashing green	The firewall is operating correctly.
		Fast flashing green	The firewall is loading software.

## NFNX3-HDB1080

**Table8-2 LED description**

LED	Mark	Status	Description
Drive status LED	HDD	Fast flashing green	Data is being read from or written to the drive.
		Steady green	The drive is present and operating correctly.
10/100/1000BASE-T copper port LED	10/100/1000BASE-T	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
10/100/1000BASE-T	10/100/1000BASE-T	Off	No link is present.

LED	Mark	Status	Description
copper port LED (combo interfaces)		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
1000BASE-X fiber port LED (combo interfaces)	1000BASE-X	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
System status LED	SYS	Off	The firewall is not powered on or has failed.
		Flashing green at 0.5 Hz	The firewall is operating correctly.
		Flashing green at 4 Hz	The firewall is loading software.
Power supply status LED	PWR	Off	No power supply is present or the power supply has failed.
		Steady green	The power supply is operating correctly.

## NFNX3-HDB1180/NFNX3-HDB1480

**Table8-3 LED description**

LED	Mark	Status	Description
10/100/1000BASE-T copper port LED	10/100/1000BASE-T	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
10/100/1000BASE-T copper port LED (combo interfaces)	10/100/1000BASE-T	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
1000BASE-X fiber port LED (combo interfaces)	1000BASE-X	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending

LED	Mark	Status	Description
			data at 1000 Mbps.
10GE fiber port LED	10GBASE-R	Off	No link is present.
		Steady green	A 10 Gbps link is present.
		Flashing green	The port is receiving and sending data at 10 Gbps.
System status LED	SYS	Off	The firewall is not powered on or has failed.
		Flashing green at 0.5 Hz	The firewall is operating correctly.
		Flashing green at 4 Hz	The firewall is loading software.
Power supply status LED	PWR	Off	No power supply is present or the power supply has failed.
		Steady green	The power supply is operating correctly.

## NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB3280

**Table8-4 LED description**

LED	Mark	Status	Description
System status LED	SYS	Off	The firewall is not powered on or has failed.
		Flashing green at 0.5 Hz	The firewall is operating correctly.
		Flashing green at 4 Hz	The firewall is loading software.
Power supply status LED	PWR0, PWR1	Off	No power supply is present or the power supply has failed.
		Steady green	The power supply is operating correctly.
10/100/1000BASE-T copper port LED	10/100/1000BASE-T	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
1000BASE-X fiber port LED	1000BASE-X	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.

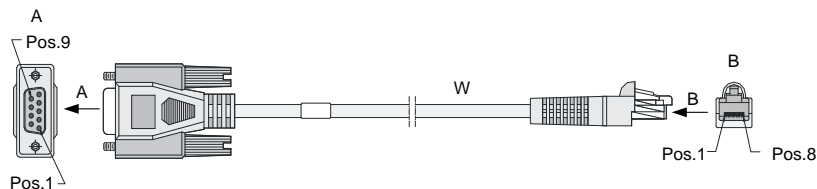
LED	Mark	Status	Description
10GE fiber port LED	10GBASE-R	Off	No link is present.
		Steady green	A 10 Gbps link is present.
		Flashing green	The port is receiving and sending data at 10 Gbps.
1000BASE-X fiber port LED (combo interfaces)	1000BASE-X	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
10/100/1000BASE-T copper port LED (combo interfaces)	10/100/1000BASE-T	Off	No link is present.
		Steady green	A 1000 Mbps link is present.
		Flashing green	The port is receiving and sending data at 1000 Mbps.
		Steady yellow	A 10/100 Mbps link is present.
		Flashing yellow	The port is receiving and sending data at 10 Mbps or 100 Mbps.
Interface module status LED	Slot1, Slot2	Off	No interface module is present or the interface module has failed.
		Steady green	The interface module is operating correctly.

# 9 Appendix C Cables

## Console cable

A console cable is an 8-core shielded cable with a crimped RJ-45 connector at one end and a DB-9 female connector at the other end. The RJ-45 connector is for connecting to the console port of the firewall, and the DB-9 female connector is for connecting to the serial port on the configuration terminal.

**Figure9-1 Console cable**



**Table9-1 Console cable pinouts**

RJ-45	Signal	Direction	DB-9
1	RTS	←	7
2	DTR	←	4
3	TXD	←	3

RJ-45	Signal	Direction	DB-9
4	CD	→	1
5	GND	-	5
6	RXD	→	2
7	DSR	→	6
8	CTS	→	8

# Ethernet twisted pair cable

## Introduction

An Ethernet twisted pair cable consists of four pairs of insulated copper wires twisted together. Every wire uses a different color, and has a diameter of about 1 mm (0.04 in). A pair of twisted copper cables can cancel the electromagnetic radiation of each other, and reduce interference of external sources. An Ethernet twisted pair cable mainly transmits analog signals and is advantageous in transmitting data over shorter distances. It is the commonly used transmission media of the Ethernet. The maximum transmission distance of the Ethernet twisted pair cable is 100 m (328.08 ft). To extend the transmission distance, you can connect two twisted pair cable segments with a repeater. At most four repeaters can be added, which means five segments can be joined together to provide a transmission distance of 500 m (1640.42 ft).

Ethernet twisted pair cables can be classified into category 3, category 4, category 5, category 5e, category 6, and category 7 cables based on performance. In LANs, category 5, category 5e, and category 6 are commonly used.

**Table9-2 Description for commonly used Ethernet twisted pair cables**

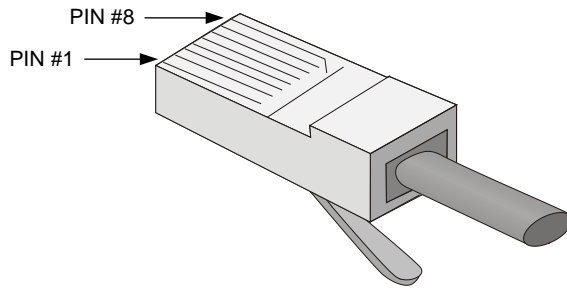
Type	Description
Category 5	Suitable for data transmission at a maximum speed of 100 Mbps
Category 5e	Suitable for data transmission at a maximum speed of 1000 Mbps
Category 6	Suitable for data transmission at a speed higher than 1 Gbps

Based on whether a metal shielding is used, Ethernet twisted pair cables can be classified into shielded twisted pair (STP) and unshielded twisted pair (UTP). An STP cable provides a metallic braid between the twisted pairs and the outer jacket. This metallic braid helps reduce radiation, prevent information from being listened, and eliminate external electromagnetic interference (EMI) of external sources. STPs have strict application requirements and are expensive although they provide better EMI prevention performance than UTPs, so in most LANs, UTPs are commonly used.

An Ethernet twisted pair cable connects network devices through the RJ-45 connectors at the two ends. [Figure9-2](#) shows the pinouts of an RJ-45 connector.



**Figure9-2 RJ-45 connector pinout**



**NOTE:**

The RJ-45 Ethernet ports of the firewall use category 5 or higher Ethernet twisted pair cables for connection.

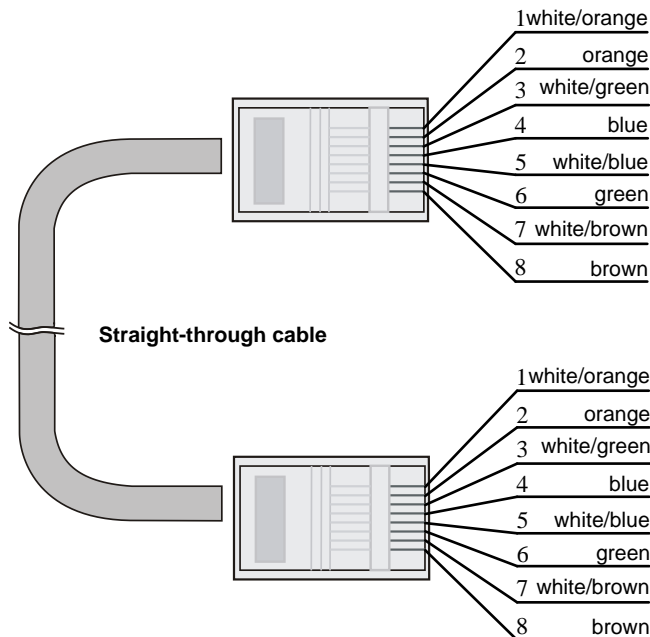
EIA/TIA cabling specifications define two standards, 568A and 568B, for cable pinouts.

- **Standard 568A**—pin 1: white/green stripe, pin 2: green solid, pin 3: white/orange stripe, pin 4: blue solid, pin 5: white/blue stripe, pin 6: orange solid, pin 7: white/brown stripe, pin 8: brown solid.
- **Standard 568B**—pin 1: white/orange stripe, pin 2: orange solid, pin 3: white/green stripe, pin 4: blue solid, pin 5: white/blue stripe, pin 6: green solid, pin 7: white/brown stripe, pin 8: brown solid.

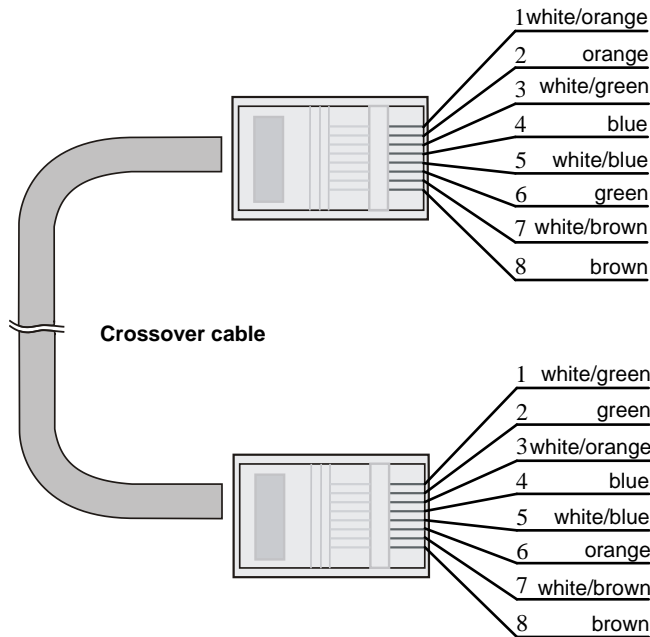
Ethernet twisted pair cables can be classified into straight-through and crossover cables based on their pinouts.

- **Straight-through**—The pinouts at both ends are T568B compliant, as shown in [Figure9-3](#).
- **Crossover**—The pinouts are T568B compliant at one end and T568A compliant at the other end, as shown in [Figure9-4](#).

**Figure9-3 Straight-through cable**



**Figure9-4 Crossover cable**



Select an Ethernet twisted pair cable according to the RJ-45 Ethernet port type on your device. An RJ-45 Ethernet port can be MDI (for routers and PCs) or MDIX (for switches). [Table9-3](#) and [Table9-4](#) show their pinouts.

**Table9-3 RJ-45 MDI port pinouts**

Pin	10BASE-T/100BASE-TX		1000BASE-T	
	Signal	Function	Signal	Function
1	Tx+	Sends data	BIDA+	Bi-directional data cable A+
2	Tx-	Sends data	BIDA-	Bi-directional data cable A-
3	Rx+	Receives data	BIDB+	Bi-directional data cable B+
4	Reserved	N/A	BIDC+	Bi-directional data cable C+
5	Reserved	N/A	BIDC-	Bi-directional data cable C-
6	Rx-	Receives data	BIDB-	Bi-directional data cable B-
7	Reserved	N/A	BIDD+	Bi-directional data cable D+
8	Reserved	N/A	BIDD-	Bi-directional data cable D-

**Table9-4 RJ-45 MDIX port pinouts**

Pin	10BASE-T/100BASE-TX		1000BASE-T	
	Signal	Function	Signal	Function
1	Rx+	Receives data	BIDB+	Bi-directional data cable B+
2	Rx-	Receives data	BIDB-	Bi-directional data cable B-
3	Tx+	Sends data	BIDA+	Bi-directional data cable A+
4	Reserved	N/A	BIDD+	Bi-directional data cable D+
5	Reserved	N/A	BIDD-	Bi-directional data cable D-

Pin	10BASE-T/100BASE-TX		1000BASE-T	
	Signal	Function	Signal	Function
6	Tx-	Sends data	BIDA-	Bi-directional data cable A-
7	Reserved	N/A	BIDC+	Bi-directional data cable C+
8	Reserved	N/A	BIDC-	Bi-directional data cable C-

To ensure normal communication, the pins for sending data on one port must correspond to the pins for receiving data on the peer port. When both of the ports on the two devices are MDI or MDIX, use a crossover Ethernet cable; when one port is MDI and the other is MDIX, use a straight-through Ethernet cable. To summarize, straight-through and crossover cables connect the following devices:

- Straight-through cables connect devices of different types—for example, router to PC and router to switch.
- Crossover cables connect devices of the same type—for example, switch to switch, router to router, and PC to PC.

If an RJ-45 Ethernet port is enabled with MDI/MDIX autosensing, it can automatically negotiate pin roles.

---

**NOTE:**

The RJ-45 Ethernet ports on the firewall support MDI/MDIX autosensing.

---

## Making an Ethernet twisted pair cable

1. Cut the cable to a required length with the crimping tool.
2. Strip off an appropriate length of the cable sheath. The length is typically that of the RJ-45 connector.
3. Untwist the pairs so that they can lay flat, and arrange the colored wires based on the wiring specifications.
4. Cut the top of the wires even with one another. Insert the wires into the RJ-45 connector and make sure the wires extend to the front of the RJ-45 connector and make good contact with the metal contacts in the RJ-45 connector and in the correct order.
5. Crimp the RJ-45 connector with the crimping tool until you hear a click.
6. Use a cable tester to verify the connectivity of the cable.

## Optical fiber

Optical fibers feature low loss and long transmission distance.

Optical fibers can be classified into single mode fibers and multi-mode fibers. A single mode fiber (with yellow jacket) carries only a single ray of light; a multi-mode fiber (with orange jacket) carries multiple modes of lights.

**Table9-5 Characteristics of single mode and multi-mode optical fibers**

Item	Single mode fiber	Multi-mode fiber
Core	Small core (10 micrometers or less)	Larger core than single mode fiber (50 micrometers, 62.5 micrometers or greater)
Dispersion	Less dispersion	Allows greater dispersion and therefore, signal loss exists.
Light source and	Uses lasers as the light source often	Uses LEDs as the light source often within

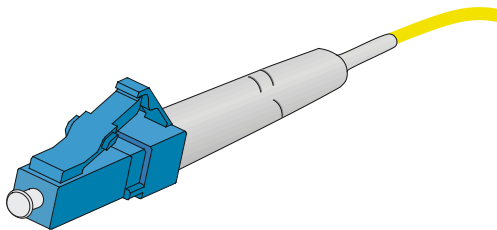
Item	Single mode fiber	Multi-mode fiber
transmission distance	within campus backbones for distance of several thousand meters	LANs or distances of a couple hundred meters within a campus network

**Table9-6 Allowed maximum tensile force and crush load**

Period of force	Tensile load (N)	Crush load (N/mm)
Short period	150	500
Long term	80	100

Fiber connectors are indispensable passive components in an optical fiber communication system. They allow the removable connection between optical channels, which makes the optical system debugging and maintenance more convenient. There are multiple types of fiber connectors. [Figure9-5](#) shows an LC connector.

**Figure9-5 Appearance of an LC connector**



Follow these guidelines when you connect an optical fiber:

- Before connecting an optical fiber, make sure the connector and cable type match the interface module.
- The fiber Ethernet port of the firewall supports only the LC connector.
- Fiber connectors are fitted with dust caps. Keep the dust caps secure when the fiber connectors are in use. Install dust caps when the fiber connectors are not in use to avoid damage to their end face. Replace the dust cap if it is loose or polluted.
- Before connecting an optical fiber, use dust free paper and absolute alcohol to clean the end face of the two fiber connectors. You can brush the end faces only in one direction.
- Never bend or curve a fiber when connecting it.
- If the fiber has to pass through a metallic board hole, when passing through a metallic board hole or bending along the acute side of mechanical parts, the fiber must wear jackets or cushions.