McAfee™
Together is power.

Revision A

McAfee Network Security Platform

(NS9500 Sensor Product Guide)

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

1 About Network Security Sensors

McAfee Network Security Sensors (Sensors) are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the McAfee® Network Security Manager (Manager). The process of configuring a Sensor and establishing communication with the Manager is described in subsequent chapters of this guide. For the details about the Manager, see the *McAfee Network Security Platform Manager Administration Guide.*

Contents

Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for McAfee® Network Security Sensor (Sensor) designed for high bandwidth links, to provide Next Generation IPS (NGIPS) capability, providing high aggregate throughput across various Sensor models. The NS9500 Sensor is a 1RU unit providing an aggregate throughput up to 30 Gbps.

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

Deployment of an NS-series Sensor

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of McAfee® ePolicy Orchestrator® (McAfee® ePO™) servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, McAfee® Network Security Platform (formerly McAfee® IntruShield®) provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Network Security Platform protects against Web and eCommerce mail server exploits.

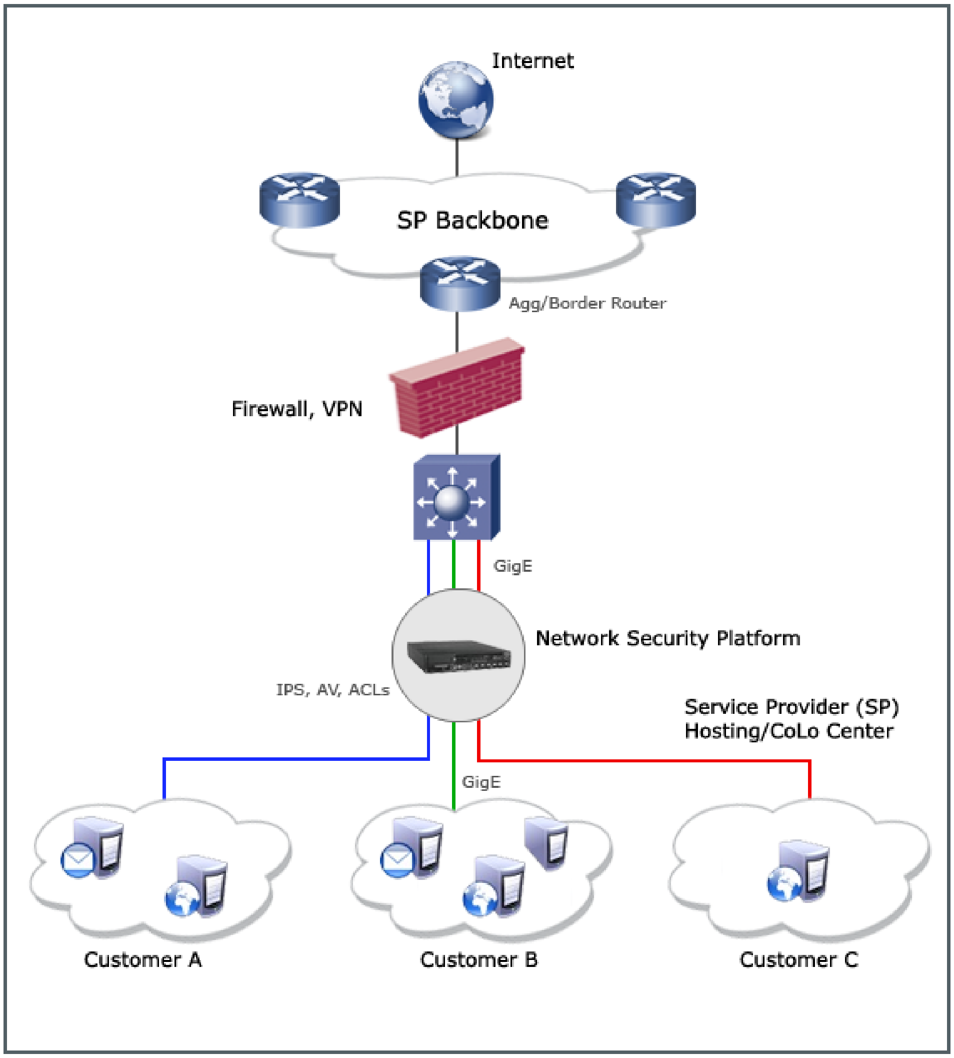


Figure 1-1 A sample Network Security Platform deployment

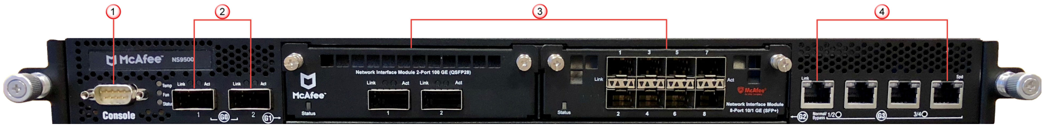
2 NS-series physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS-series Sensor.

Contents

Components of an NS-series Sensor

Correlate the pictures with the information following it to understand the components of an NS-series Sensor.



1
2
3
4
McAfee NS9500
Console
Temp
Fan
Status
Link
Act
G0
G1
Network Interface Module 2-Port 100 GE (QSFP28)
McAfee
Status
Network Interface Module 8-Port 10/1 GE (SFP+)
Spd
Normal/Bypass 1/2
G2
G3
3/4

Figure 2-1 Sensor front panel

1 Console port (1)

2 QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2)

3 Two slots for I/O modules (Any combination of the interface modules can be used)

- QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2)
- QSFP+ 40 Gigabit Ethernet ports (4)
- QSFP+ 40 Gigabit Ethernet ports (2)
- SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8)
- RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6)
- RJ-45 100/1000/10000 Gigabit Ethernet Monitoring ports (4)
- 1/10 Gigabit Ethernet Monitoring ports (4)

4 RJ-45 100/1000/10000 Mbps Ethernet Monitoring ports (4)

The supported transceiver modules are QSFP28, QSFP+, SFP+ (MM and SM), SFP Fiber (MM and SM) and SFP Copper.

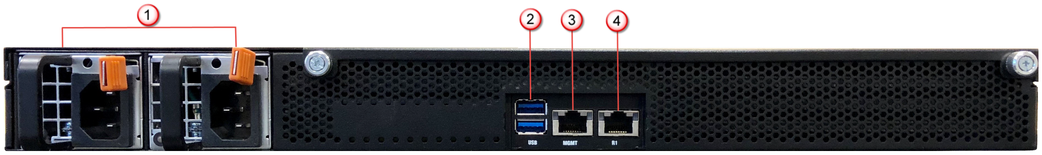


Figure 2-2 Sensor rear panel

1 Power supply A/B (Pwr A/Pwr B)

2 USB ports (2)

3 RJ-45 1000/10000 Management port (Mgmt) (1)

4 RJ-45 1000/10000 Response port (R1) (1)

Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. Also indicates system bad health if the LED is on for longer duration.
Fan	Green Amber	All five fans are operating. One or more of the fans has failed.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK.) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot.)
Gigabit Ports Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The port speed is 100 Mbps.
Gigabit Ports Link	Green Off	The link is up. The link is down.
RJ45 FailOpen/ Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/Span/Tap Mode. The Port Pair is in the Bypass Mode.

Rear panel LEDs

LED	Status	Description
Pwr A (Power A)	Solid Green Blinking Green Solid Amber	Power Supply A is functioning. Power Supply A is stand-by. Power Supply A is not functioning or the unit has no power feed.
Pwr B (Power B)	Solid Green Blinking Green Solid Amber	Power Supply B is functioning. Power Supply B is stand-by. Power Supply B is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps.
Management Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.
Response Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps.
Response Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.

3 Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

Contents

Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

- You should not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- The Sensor appliance is not a general purpose workstation.
- McAfee prohibits the use of the Sensor appliance for anything other than operating Network Security Platform.
- McAfee prohibits the modification or installation of any hardware or software on the Sensor appliance that is not part of the normal operation of Network Security Platform.

Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector and compatible cable types are below:

Connector	Cable
QSFP28	MPO/MTP and LC
QSFP+	LC-duplex and MPO/MTP
SFP/SFP+	LC-duplex

Note the following:

- Fiber-optic ports (for example, SFP/SFP+/QSFP+/ QSFP28, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

> To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/QSFP+/QSFP28 laser transceivers are acceptable for use with the Sensor.

Contents of the box

The following accessories are shipped in the NS-series Sensor crate:

- Sensor
- Power supply (x2)
- Power cords. McAfee provides a standard and international power cables.

- Set of rack mounting rails
- Printed Quick Start Guide
- Serial Console Cable (DB9-DB9)
- QSFP28 Direct Attach Copper (DAC) cable

Unpack the Sensor

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts.

   These parts are listed on the packing list and in the section, Contents of the box.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts.

   These parts are listed on the packing list and in the section, Contents of the box.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

4 Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

Contents

Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install the supported interface modules as per your requirement.
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

How to position the Sensor

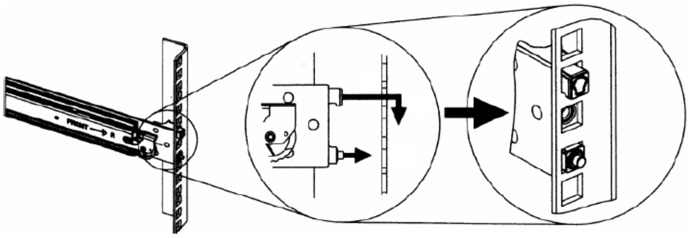
Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

Install the slide rails and rack mount the Sensor

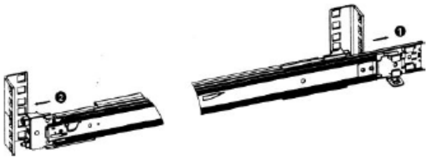
Follow this procedure to assemble the slide rails and position the Sensor on it.

Task

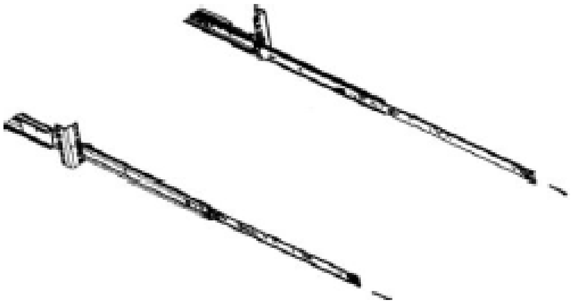
1. Disassemble inner slide rail members from cabinet sections.
   a. Pull inner member out until it comes to a lock position.
   b. Depress the QD latch to fully disconnect inner members.



2. Mount inner members to the chassis unit.
   a. Place each inner member on both sides of the chassis unit. Position the bottom mounting holes of the inner member with matching mounting holes on chassis unit.
   b. Use screws to secure inner members in place. Apply to both sides of chassis unit.



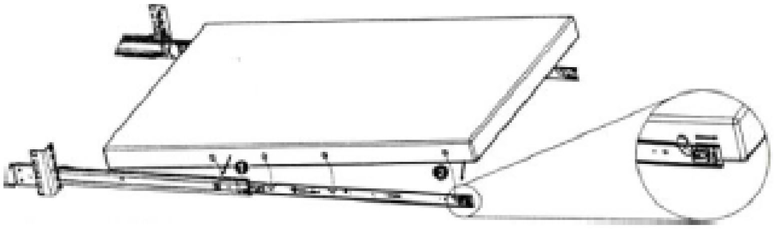
3. Mount slide cabinet sections to the rack.
   a. Install the front end of each slide cabinet section to rack using the slide tool-less features. The tool-less latch rotates when the bracket is pressed up against the rack rails.
   b. Align, adjust, and attach the rear brackets to the rack rail.



4 Mount chassis unit into mounted cabinet sections.

a Guide the chassis unit into the pre-installed cabinet sections. Allow the pre-installed inner members to slide into the outer members until they lock in place.

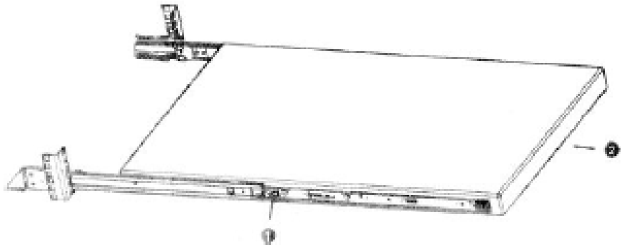
b Depress the QD latch on both sides and continue to push the chassis unit in until fully closed.



5 Secure the chassis unit through the rack rails.

a With the chassis unit in fully closed position, secure using two truss head screws.

b Drive the screws through the inner member flange and through the rack rails. The screws thread directly to the cabinet slide members. Tighten the screws.



5 NS-series interface modules

The NS9500 Sensors support the 2-port, 4-port, 6-port, and 8-port Network Interface Modules. These modules need to be installed in the respective slots on the Sensor.

For more information, see the *Network Security Platform NS-series Interface Modules Reference Guide*.

Contents

2-port QSFP28 100 Gigabit Network Interface Module

The 2-port QSFP28 (Quad Small Form-Factor Pluggable 28) Network Interface Module provides 100 Gigabit Ethernet performance on each port.

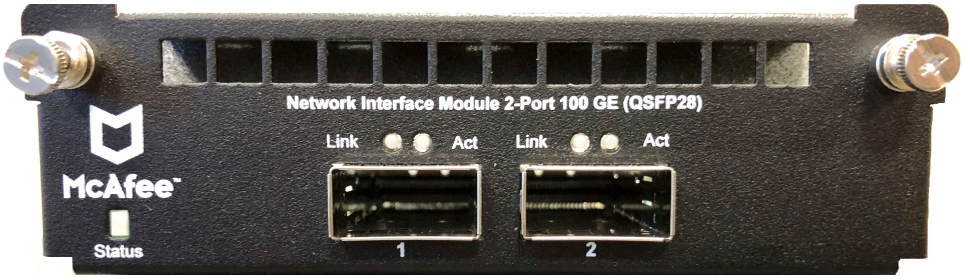


Figure 5-1 2-port QSFP28 100 Gigabit interface module

2-port QSFP+ 40 Gigabit Network Interface Module

The 2-Port QSFP+ (Quad Small Form-Factor Pluggable Plus) Network Interface Module provides 40 Gigabit Ethernet performance on each port.

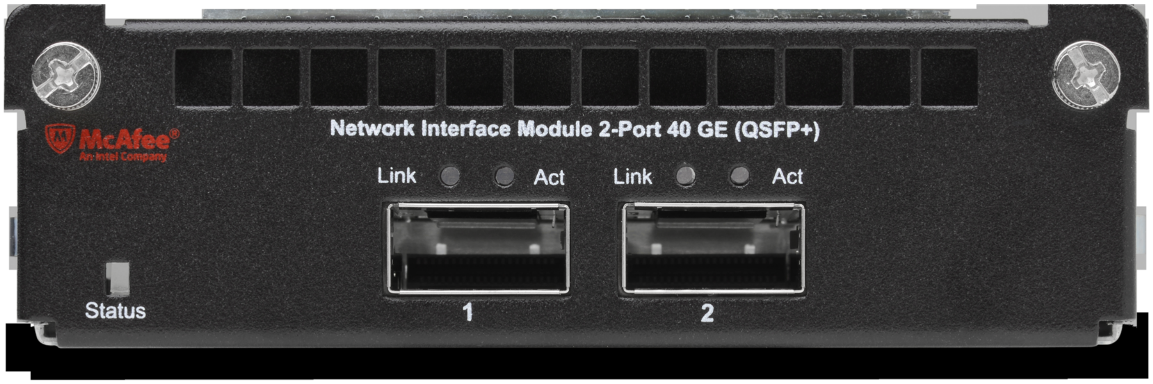


Figure 5-2 2-Port QSFP+ 40 Gigabit interface module

4-port QSFP+ 40 Gigabit Network Interface Module

The 4-port QSFP+ (Quad Small Form-Factor Pluggable Plus) Network Interface Module provides 40 Gigabit Ethernet performance on each port.

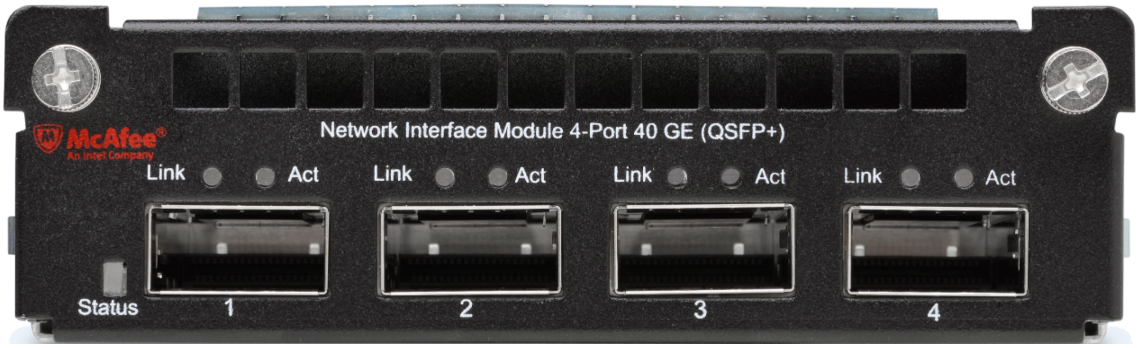


Figure 5-3 4-port QSFP+ 40 Gigabit interface module

4-port 10/1 GigE SM 8.5 µm with internal fail-open Network Interface Module

The 4-port SM 8.5 µm Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

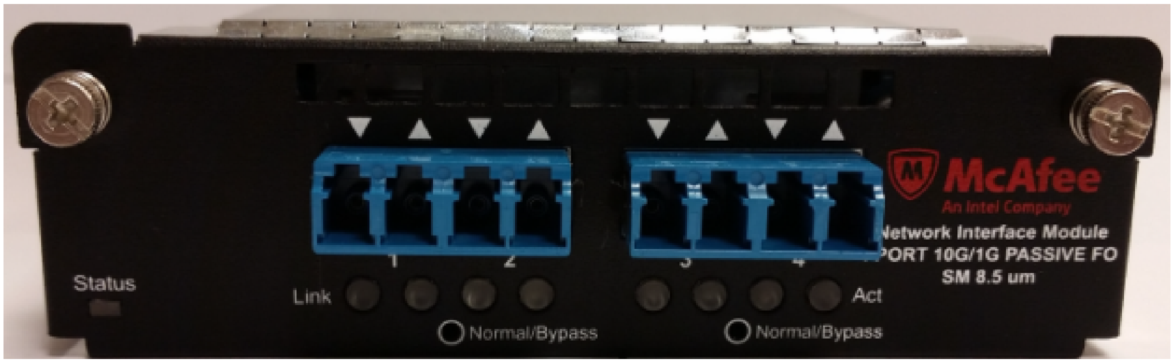


Figure 5-4 4-port 10/1 GigE SM 8.5 µm with internal fail-open interface module

4-port 10/1 GigE MM 50 µm with internal fail-open Network Interface Module

The 4-port MM 50 µm Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

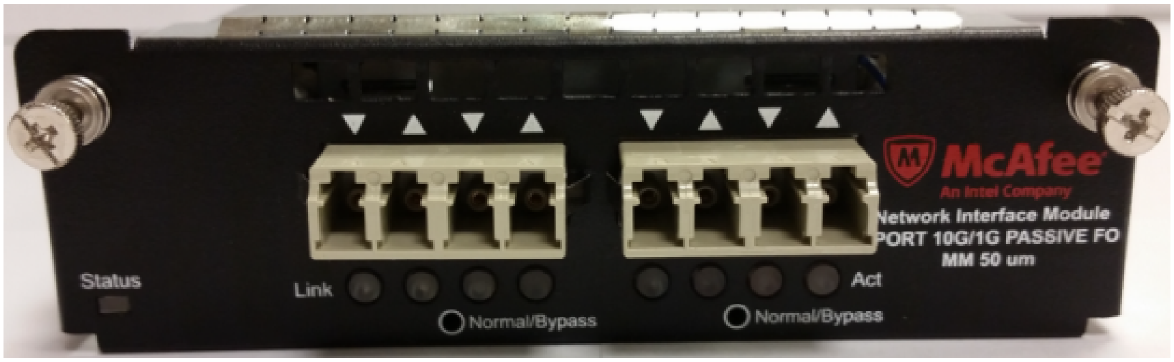


Figure 5-5 4-port 10/1 GigE SM 50 µm with internal fail-open interface module

4-port 10/1 GigE MM 62.5 µm with internal fail-open Network Interface Module

The 4-port MM 62.5 µm Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

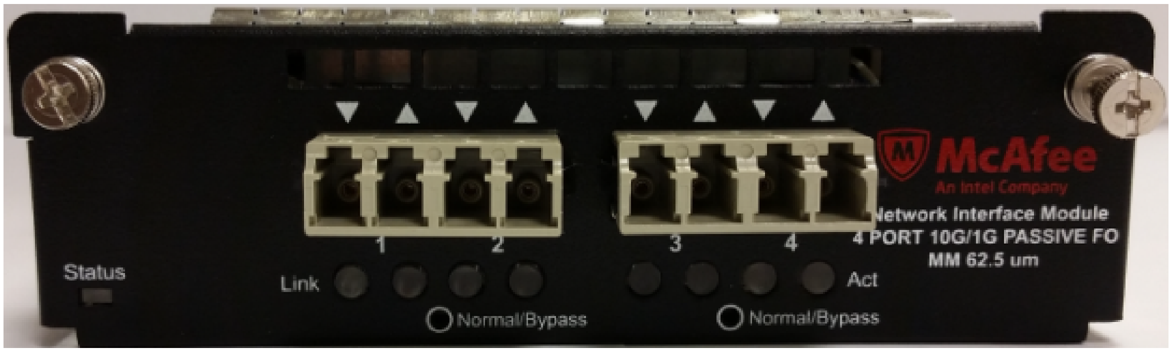


Figure 5-6 4-port 10/1 GigE SM 62.5 µm with internal fail-open interface module

4-port RJ-45 10 Gbps/1 Gbps/100 Mbps Network Interface Module

The 4-port RJ-45 Network Interface Module provides 10 Gbps/1 Gbps/100 Mbps Ethernet performance on each port.

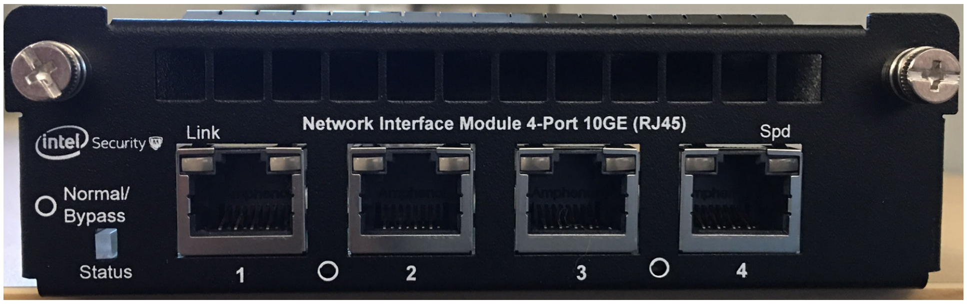


Figure 5-7 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps interface module

6-port RJ-45 10/100/1000 Mbps Network Interface module

The 6-port RJ-45 Network Interface Module provides 10/100/1000 Mbps Ethernet performance on each port.

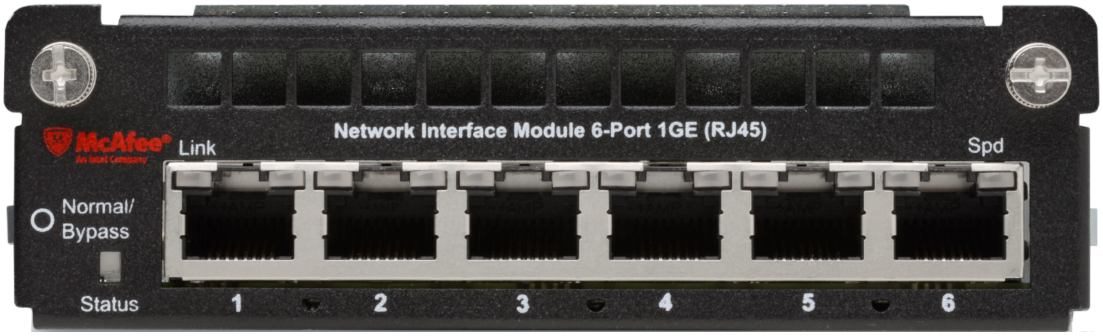


Figure 5-8 6-port RJ-45 10/100/1000 Mbps interface module

8-port SFP/SFP+ 1/10 Gigabit Network Interface Module

The 8-Port SFP/SFP+ (Small Form-Factor Pluggable Plus) Network Interface Module provides 1/10 Gigabit Ethernet performance on each port.

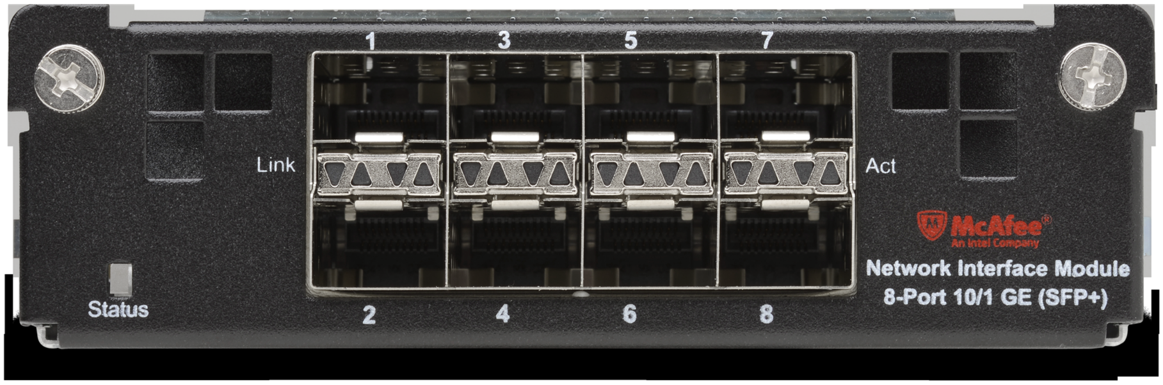


Figure 5-9 8-Port SFP+/SFP 10/1G Gigabit interface module

Installation of the interface module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Manager and Sensor.

Task

1 Remove the module from its protective packaging.

> It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Manager has not been established.

2 Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

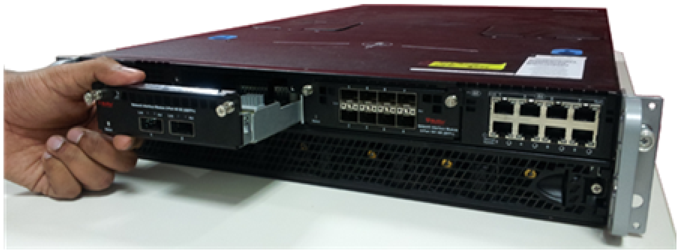


Figure 5-10 Install an interface module

3 Drive in the screws fixed on the sides of the module to attach it to the Sensor.

4 Turn on the Sensor.

5 Establish trust between the Sensor and the Manager.

Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

Task

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

Remove an interface module

Perform these steps if you need to remove an interface module.

Task

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

6 Small form-factor pluggable transceiver modules

The NS-series Sensors use three types of small form-factor pluggable modules as shown in the following table. For more information, see *McAfee Network Security Platform NS-series Transceiver Modules Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	10 Gbps (fiber optic)
QSFP+	40 Gbps (fiber optic)
QSFP28	100 Gbps (fiber optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, McAfee supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through McAfee or from a McAfee-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at http://mysupport.mcafee.com/Eservice/. Click **Search the KnowledgeBase.**

These installation instructions provide information for installing SFP, SFP+, QSFP+ and QSFP28 modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

> ! To prevent eye damage, do not stare into open laser apertures.

Contents

SFP transceiver modules

An SFP module is a protocol-independant, compact, optical receiver, which allows for greater port density than the standard GBIC. This module operates at varying speeds for up to 1 gigabit per second on SONET/SDH, Fibre Channel, Gigabit Ethernet and other applications. An SFP module operates in multimode. Additionally, this module transmits on a 850-nanometer wavelength on short reach (SR).

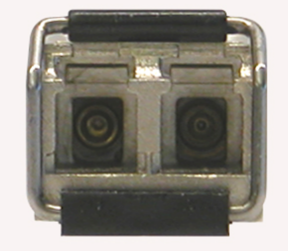


Figure 6-1 An SFP module

SFP+ transceiver modules

The **enhanced small form-factor pluggable** (**SFP+**) is an enhanced version of the SFP that supports data rates up to 10 Gbps. 850nm SFP+ 1310nm SFP+Transceiver modules are supported.

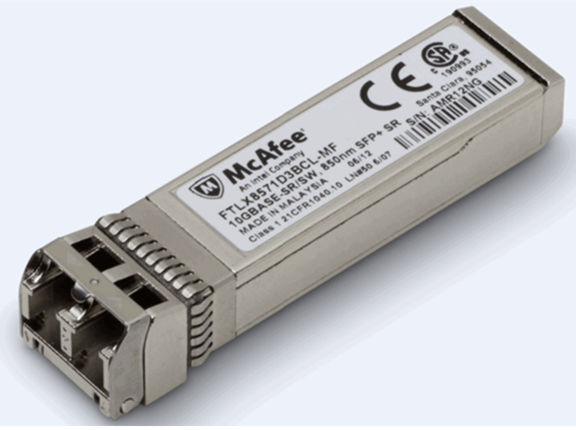


Figure 6-2 850nm SFP+ transceiver module

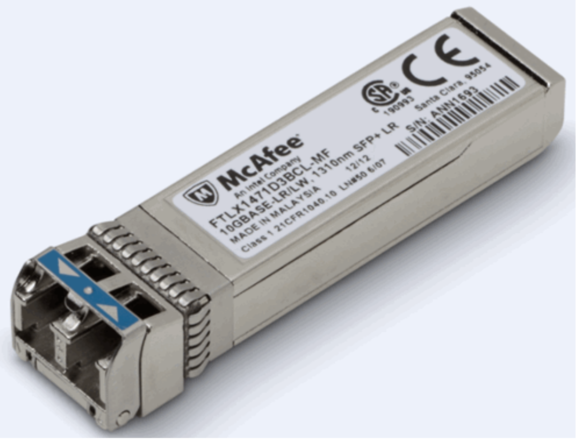


Figure 6-3 1310nm SFP+ transceiver module

QSFP+ transceiver modules

The Quad Small Form-factor Pluggable (QSFP+) is a compact, hot-pluggable, protocol-independant transceiver used for data communications applications. It interfaces a network device (switch, router, media converter or similar device) to a fiber optic cable. It is a industry format jointly developed and supported by many network component vendors. QSFP+ transceivers are designed to support Serial Attached SCSI, 40G Ethernet, 20G/40G Infiniband, and other communications standards. 850nm QSFP+ transceiver module is supported.

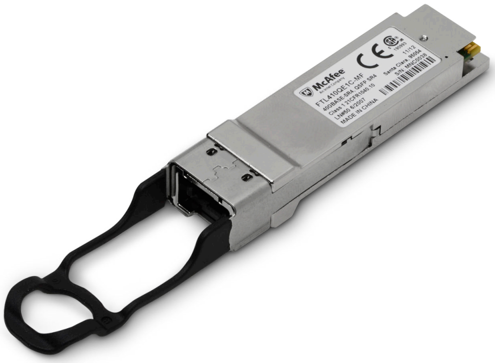


Figure 6-4 850nm QSFP+ transceiver module

QSFP28 transceiver modules

The Quad Small Form-factor Pluggable (QSFP28) is a compact, hot-pluggable, transceiver used for data communications applications. It interfaces a network device (switch, router, media converter or similar device) to a fiber optic cable. It is an industry format jointly developed and supported by many network component vendors. QSFP28 transceivers are specifically designed to support 100G Ethernet.

Install a transceiver module

Task

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket.

Modules are keyed to prevent incorrect insertion.

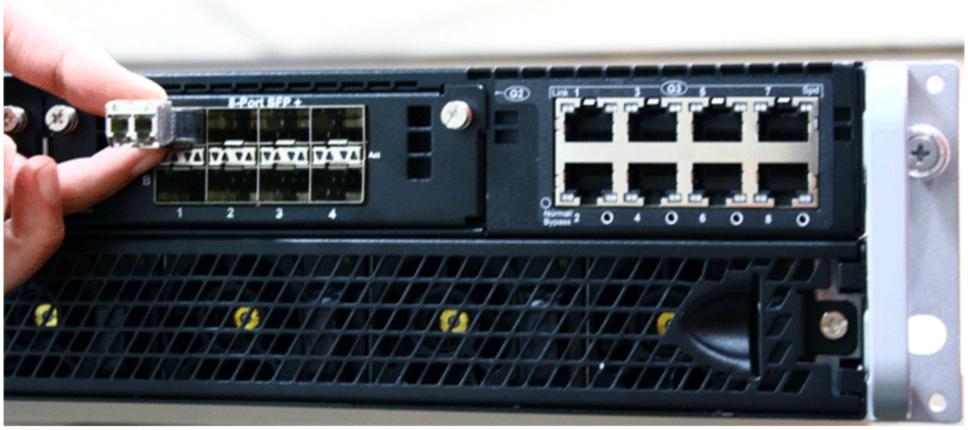


Figure 6-5 Insert a transceiver module

In the following scenarios you need to reboot the Sensor to detect the new speed:

- 100 Gbps Copper transceiver to 40 Gbps transceiver Copper or vice versa
- 100 Gbps Fiber transceiver to 40 Gbps Fiber transceiver or vice versa

Remove a transceiver module

Perform these tasks if you need to remove a module.

Task

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

7

Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

Contents

Connect the cable to the Console port

The Console port on the NS-series Sensor is used for setup and configuration of the Sensor.

Task

1. For console connections, plug the DB9 Console cable supplied by McAfee into the Console port on the Sensor.

   This port is labeled **Console** in the Sensor front panel.

2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer running correctly configured Windows HyperTerminal software.

   You must connect directly to the console for initial configuration, you cannot configure the Sensor remotely. Terminal servers are provided for console access. Required settings for HyperTerminal are:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

Task

1. Plug a Cat-5e Ethernet cable into the Response port.

   This port is labeled **R1** on the Sensor rear panel.

2. Connect the other end of the cable to the network device such as a hub, switch, or a router, through which you want to respond to attacks.

Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

Task

1. Plug a Category 5e Ethernet cable into the Management port.

   This port is labeled **Mgmt** in the rear panel of the NS-series Sensor.

2. Plug the other end of the cable into the network device connected to your Manager server.

> ℹ To isolate and protect your management traffic, McAfee strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode

Tasks

- *Connect the cables for in-line mode* on page 31
- *Connect the cables for tap mode* on page 32
- *Connect the cables for SPAN or hub mode* on page 32
- *Connect the cable for Sensor failover* on page 32
- *Connect the cables for Sensor Fail-Open* on page 33

How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.

The following Ethernet ports are coupled and must be used together.

- On NS9500 Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is the 2-port QSFP28 1000G interface module, G2 is the 8-Port SFP+/SFP 1/10G interface module, G5 is the 4-port QSFP+ 40G interface module and G6 is the 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

You cannot disable auto-negotiation in G3 slots.

Port Pairs	Sensor
G0/1 and G0/2	NS9500
G1/1 and G1/2	NS9500
G2/1 and G2/2	NS9500
G2/3 and G2/4	NS9500
G2/5 and G2/6	NS9500
G2/7 and G2/8	NS9500
G3/1 and G3/2	NS9500
G3/3 and G3/4	NS9500

Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the SFP/SFP+/QSFP+ monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to SFP/SFP+/QSFP+ monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and have a fail-open function built-in as well.

All other monitoring ports require the use of external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

Task

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/2.
3. Connect the other end of each cable to the network devices that you want to monitor.

   For example, if you plan to monitor traffic between a switch and a router, connect the cable connected to 1 to the switch and the one connected to 2 to the router.

Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

> For a list of McAfee-approved third party vendors, see the KnowledgeBase at http://mysupport.mcafee.com/Eservice/. Click **Search the KnowledgeBase** and locate the relevant KnowledgeBase article.

Task

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

Connect the cable for Sensor failover

For Sensor failover, connect two NS-series Sensors using the appropriate cables. These two Sensors must be running the same software version. Failover cables are the only additional hardware required to support failover communication between two NS-series Sensors.

Refer the following table before you configure a failover pair:

Sensor Model	Port to connect the failover pair	Cable requirements for failover
NS9500	G0/1	QSFP28/QSFP+ Direct Attach Copper (DAC)

The system ships with a 1m QSFP28 DAC cable. This can be used for failover connection if the failover sensors are placed within 1m.

If you need to configure failover pair between sensors kept at distance greater than 1m, consider the following options:

- For distances up to 3m, purchase QSFP28 DAC from external source
- For distances greater than 3m, purchase 40G SR4 transceivers from McAfee and fiber cables from external source

Task

1. Plug the cable(s) appropriate for use with your QSFP+ or QSFP28 module into port G0/1 (NS9500) of the active NS-series Sensor.
2. Connect the other end of the cable(s) into port G0/1 (NS9500) of the standby NS-series Sensor.

Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits, 10 Gigabit Fail-Open Kits and 40 Gigabit Fail-open Kits are available for the 1, 10, and 40 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which have the fail-open function built-in as well, for the Monitoring ports to fail-open, you use the optional external bypass switch provided in an Active Fail-Open Kit.

While the Sensor is operating, the Active Fail-Open kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "on" state, once again enabling in-line monitoring.

> ❗ Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

> ❗ A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.
>
> The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the following guides:

- *1 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *10 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *40 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *Active Fail-Open Kit Quick Start Guide*
- *Passive Fail-Open Kit Quick Start Guide*

Turning the Sensor on and off

Before you begin

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

Task

1. Connect the power cable to the Sensor power supply.
2. Connect the power cable to a power source.

> If you are installing a redundant power supply, you should install it as described in Install the power supply. For true redundant operation with the optional redundant power supply, McAfee recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source.

McAfee recommends that you use the `shutdown` CLI command to halt the Sensor before turning it off. For more information on CLI commands, see *McAfee Network Security Platform CLI Guide* for specific Sensor software version you are running.

Managing licenses for NS9500 Sensors

The NS9500 Sensor license requires a license to activate the baseline throughput of 10 Gbps. Additional license is required to increase the throughput from 10 Gbps to 20 Gbps or 30 Gbps. The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details for the throughput for the Sensors.

> You must first purchase a license to enable traffic inspection in the NS9500 Sensor. To obtain a license, contact McAfee Sales.

You can upload the license from the **Licenses** page in the Manager. In the Manager, select **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.

The following details are displayed in the **Capacity** tab:

Option	Definition
Required	**Model** – Sensor model compatible with the license **Capacity** – Throughput limit for the license **Device Count** – Number of devices that can be assigned to the license
Assigned To	Name of the Sensor assigned to the license.
License Details	**Customer** – Customer for whom the license file was generated **Grant ID** – The McAfee Grant ID of the corresponding customer **Key** – The license key number. **Expiration** – The expiration date and time of the license.

Option	Definition
Added	**Time** – Date in <mmm-yy> format, and time when the license was added **By** – Name of the user who added the license
Comments	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved.

The following actions can be performed in the **Capacity** tab:

- Add a license
- Assign a license to a Sensor
- Unassign a license to a Sensor
- Remove a license
- Export the license list in CSV format

Add license to the Manager

Task

To upload the license, perform the following steps:

1 Go to **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.

2 Click the **Capacity** tab.

3 Click **Add License**.

The **Add License** pop-up window opens.

4 Click **Browse**.

Navigate to the location where the license is saved. Select the license and click **Open**.

The supported license formats are zip and jar.

5 Click **Add**.

The license is uploaded to the Manager.

6 (Optional) Click **Save as CSV** to export the license usage details as .csv file.

Assign a license to a Sensor

Task

To assign the license, perform the following steps:

1 Go to **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.

2 Click the **Capacity** tab.

3 Click **Assign**.

The **Assign License** pop-up window opens.

4 Click the **Assign To** drop down and select the Sensor.

5 Click **Assign** to assign the license to the Sensor.

You must reboot the device for the changes to take effect.

Unassign a license from a Sensor

Task

To unassign the license, perform the following steps:

1. Go to **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.
2. Click the **Capacity** tab.
3. Select the license you wish to unassign.
4. Click **Other Actions** | **Unassign**.
5. Click **Ok**.

   Once a license is unassigned from a Sensor it will not be able to deploy pending changes, including new signature sets and policy updates.

Remove a license from the Manager

Task

To remove a license, perform the following steps:

1. Go to **Manager** | **<Admin Domain Name>** | **Setup** | **Licenses**.
2. Click the **Capacity** tab.
3. Select the license you wish to unassign.
4. Click **Other Actions** | **Remove**.
5. Click **Ok**.

   Once a license is removed from the Manager, the Sensor to which the license was assigned will not be able to deploy pending changes, including new signature sets and policy updates.

8 Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems.	Improper cabling or port configuration.	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers.	Improper cabling or port configuration.	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The system fault "Switch absent" appears in the Manager Status page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

9 Sensor technical specifications

The following table lists the specifications of for NS9500 Sensors.

Sensor Specifics	NS9500
Dimensions	17 ¼" (W) x 29 1/16" (D) x 1 ¾" (H)
Weight	28.55 lbs
Storage	2 x 240 GB M.2 drive
System Heat Dissipation	
Maximum BTU	2038 BTU/hr
Typical BTU	1790 BTU/hr
Maximum Power Consumption	598 W
Typical Power Consumption	525 W
Redundant Power Supply	Yes
Power	100 - 240 VAC (50 - 60 Hz)
DC Power Supply	Optional
Temperature	Operating: 0° to 35° C , Non-operating: - 40° to 70° C
Relative humidity (non-condensing)	Operational: 10% to 90%, Non-operational: 5% to 95%
Altitude	0 to 10,000 feet
Safety Certification	UL 60950-1 (USA); CSA 22.1.No. 60950-1 (Canada); EN 60950-1 (Europe); CNS 14336-1 (Taiwan), GB 4943-1 (China); IEC 60950-1 (International) - CB Scheme certificate and test report covering all applicable country deviations; IEC 60825 and 21CFR1040
EMI Certification	FCC Part 15 Subpart B Class A (USA); CAN ICES-3 Class A (Canada); EN 55022, EN 55032, EN 55024, EN61000-3-2, EN61000-3-3 (Europe and International); VCCI Class A (Japan); AS/NZS CISPR 32 (Australia and New Zealand); CNS 13438 (Taiwan); GB 9254-2008 (China); KN32 and KN35 (South Korea); GB 17625.1 (China)