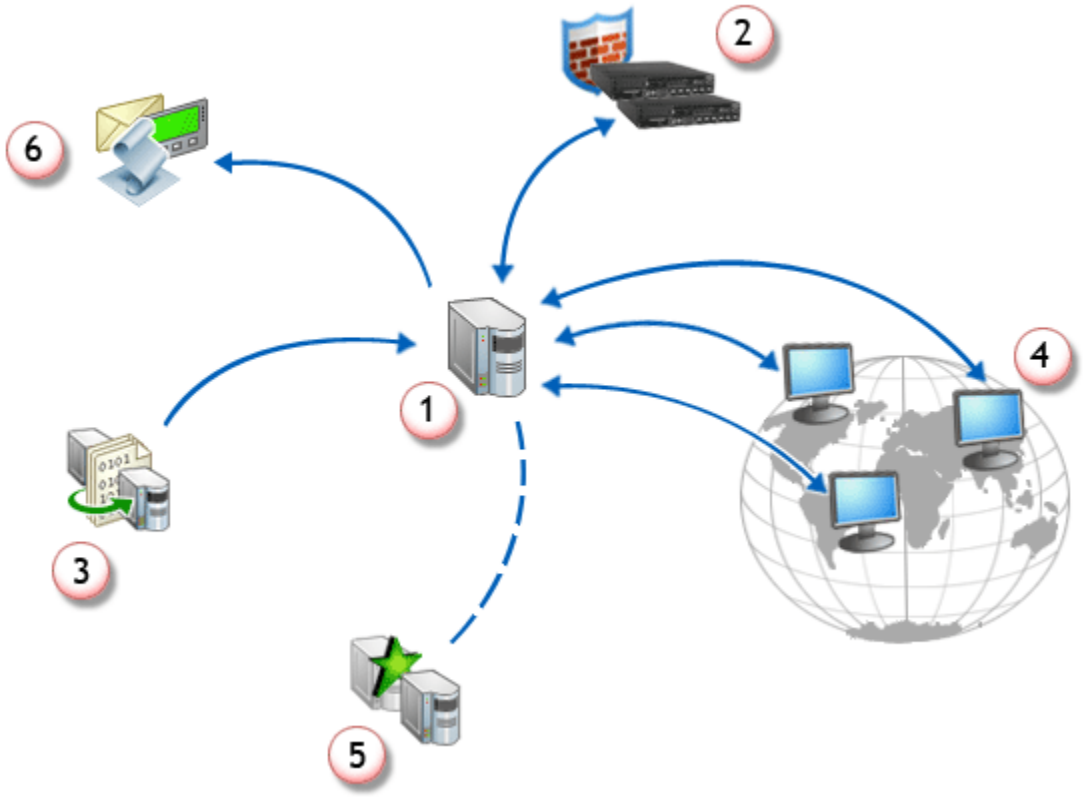
Quick Tour

Revision B

McAfee Network Security Platform

version 8.3

McAfee® Network Security Platform [formerly McAfee® IntruShield®] is a combination of network appliances and software that accurately detects and prevents intrusions, denial of service (DoS) and distributed denial of service (DDoS) attacks, and network misuse. McAfee Network Security Platform combines real-time intrusion detection and prevention for the most comprehensive and effective network security system.



The following table describes the figure in detail.

Item	Description
1	Network Security Manager (Manager)
2	Network Security Sensor (IPS Sensor)
3	McAfee Update Server
4	Web clients accessing the Manager server
5	Manager Disaster Recovery (MDR) server
6	Alert notification - email, pager, script generation

1 Ten Steps to using Network Security Platform

Step 1 	**Install the Manager software**. Install the Manager software on the server machine and ensure that you are able to log onto the Manager. For details, see *McAfee Network Security Platform Installation Guide*.
Step 2 	**Set up and configure the Sensor(s)**. Cable and install your Sensor(s) using a command line interface (CLI) and the Manager. For details, see the *McAfee Network Security Platform Sensor Product Guide*(s), *McAfee Network Security Platform Installation Guide*, and *McAfee Network Security Platform CLI Guide*.

Step 3	**Establish trust between the Manager and the Sensor(s)**.  The Sensor initiates all communication with the Manager server until secure communication is established between them. Later, configuration information is pushed from the Manager to the Sensor. • Verify on the appliance CLI that the Sensor has established communication with the Manager. • Verify in the Manager GUI that a node representing the Sensor appears in the Resource Tree under the Device List. For details, see *McAfee Network Security Platform Installation Guide*.
Step 4	**Configure policies in the Manager**.  Determine the IPS policies applicable to your network. Use the Manager GUI to set up policies. By default, the provided Default policy is applied to all of your Sensor ports. You can choose a specific policy to apply by default to the Root Admin Domain (and thus all monitoring interfaces on the Sensor). For details, see *McAfee Network Security Platform IPS Administration Guide*.
Step 5	**Configure the Update Server and download the latest signature sets**.  For your Network Security Platform to properly detect and protect against malicious activity, the Manager and the Sensors must be frequently updated with the latest signatures and software patches available - made available to you via the Update Server. Authenticate your credentials with the Update server and download the latest signature set for your Network Security Platform deployment. For details, see *McAfee Network Security Platform Manager Administration Guide*.
Step 6	**View alerts**.  The **Attack Log** page displays detected security events that violate your configured security policies. The page also provides powerful drill-down capabilities to enable you to see details on a particular alert like its type, source and destination addresses, and packet logs where applicable. View the alerts periodically and perform forensic analysis on the alert to help you tune Network Security Platform, and provide better responses to attacks. For details, see *McAfee Network Security Platform Manager Administration Guide*.
Step 7	**Tune your Network Security Platform deployment**.  Once you have configured and started using Network Security Platform, you can further enhance your deployment using the Manager GUI by utilizing some of the more advanced features like changing your deployment mode, creating multiple admin domains, defining specific user roles, applying multiple policies to multiple domains etc. For details, see *McAfee Network Security Platform Manager Administration Guide*.
Step 8	**Check the Operational Status**.  The Operational Status viewer in the Manager GUI details the functional status for all of your installed Network Security Platform system components, including the communication with integrated McAfee® Host Intrusion Prevention [formerly McAfee® Entercept] Management Servers. Check the Operational Status at regular intervals to view messages that detail system faults experienced by your Manager, appliances, or database. For details, see *McAfee Network Security Platform Manager Administration Guide*.

Step 9 	**Block malicious or unwanted traffic**. Analyze the attacks that your network is receiving on a regular basis and take actions, which can range from analyzing the impact and modifying policies, or blocking specific traffic from transmitting through your system. For details, see *McAfee Network Security Platform Manager Administration Guide, IPS Administration Guide*.
Step 10 	**Generate Reports**. The Report Generator enables a user to generate reports for the security events detected by the system and reports on system configuration. Configure your report settings to generate generated reports manually or automatically, save for later viewing, and/or email to specific individuals. For details, see *McAfee Network Security Platform Manager Administration Guide*.

2 Basics of Using Network Security Platform

This section provides a high-level overview of how to use Network Security Platform.

The process of setting up and running Network Security Platform falls into these basic stages:

a Deciding where to deploy Sensors and in what operating mode

b Setting up your Sensors

c Establish Sensor-to-Manager communication

d Configuring your deployment using the Manager

e Updating your signatures and software

f Viewing and working with data generated by Network Security Platform

g Tuning your deployment

Each of these stages consists of a number of tasks; some are simple, some are complex. You will generally perform steps 1 through 3 only once per Sensor.

3 Setting up your Sensors

The process of setting up a Sensor is described below at a high level.

a Position the Sensor.

1) Unpack the Sensor and place on a sturdy, level counter top.

2) Attach the provided rack mounting ears to the Sensor.

3) Install the Sensor in a rack. Sensors are either 1 or 2 RU, depending on model.

For detailed instructions on these tasks, see your Sensor model's *McAfee Network Security Platform Product Guide*.

b Install any additional hardware.

1) If your Sensor has Gigabit Ethernet (GE) Monitoring ports, install GBICs or XFP or SFP modules (not included) in the Sensor's GE ports.

Use only XFP or SFP modules and GBICs purchased either from McAfee or from an approved vendor. For a list of approved vendors, please see our Web site.

2) (Optional) If you have purchased a redundant power supply for your Sensor, install the power supply. Sensors that support a redundant power supply ship with only one power supply; the other must be purchased separately from McAfee. Other Sensor models have an internal power supply.

c Cable the Sensor for configuration.

1) Attach network cables to the Sensor as described in the Sensors' *McAfee Network Security Platform Product Guides*. You must first cable the Sensor to communicate with the console machine you will use to initialize the Sensor and then with the Manager server for Sensor configuration. You can cable the Sensor detection and response ports at a later time.

2) Power on the Sensor to start initialization.

4 Establish Sensor-to-Manager communication

The process of setting up a Sensor is described below at a high level.

a Set up the Manager software on the server machine.

1) Install the Manager software on the server machine. This process is described in detail in the *McAfee Network Security Platform Installation Guide.*

2) Start the Manager as described in the *McAfee Network Security Platform Installation Guide*. You can establish communication with a Sensor from the Manager server or from a remote client machine connected to the Manager server via Internet Explorer.

3) You can choose a specific policy to apply by default to the root admin domain (and thus all monitoring interfaces on the Sensor).

Whatever policy you have specified will apply until you make specific changes; this policy gets you up and running quickly. Most users tune their policies over time to best suit their environments and reduce the number of irrelevant alerts.

By default, the provided **Default Prevention** policy is applied to all of your Sensor ports. Note that this policy's behavior is to automatically block certain attacks upon detection. For more information on other provided policies, see Pre-configured rule sets and policies, *McAfee Network Security Platform IPS Administration Guide*.

1) Open the **Add New Device page** and add a Sensor, providing the Sensor with a name and a shared secret key value. For instructions on how to open the **Add New Device** page, see the *McAfee Network Security Platform Manager Administration Guide*. For instructions on how to add a Sensor to the Manager, see *McAfee Network Security Platform Installation Guide*.

b Configure the Sensor.

1) From a console connected physically or logically to the Sensor, configure the Sensor with network identification information (that is, an IP address, the IP address of the Manager server, and so on), and configure it with the same name and shared secret key value you provided in the Manager. For more information on Configuring the Sensor using the Sensor CLI, see *McAfee Network Security Platform CLI Guide*.

c Verify communication between the Sensor and the Manager.

There are three ways to check that the Sensor is configured and available:

1) In the **Manager** Dashboard, check the **System Health status**. (See if the Sensor is active. If the link is yellow, click on the cell to see the System Faults on the Sensor. For more information on this \process, see *McAfee Network Security Platform Manager Administration Guide*.

2) In the **Manager**, **click** | **Devices** | **<Device Name>** | **Setup** | **Physical Ports** | **Monitoring Ports**. Look at the color of the button(s) representing the ports on the Sensor, and check the color legend on the screen to see the status of the Sensor's ports. For more information on this process, see *McAfee Network Security Platform Manager Administration Guide*

3) Type `status` in the Sensor command line interface (CLI). Check the following line: `trust established between sensor and manager = yes`.

If the answer is `no`, re-check that your Sensor name and shared secret are the same on both the Sensor and the Manager.

d Troubleshoot any problems you run into.

1) If you run into any problems, check your configuration settings, and ensure that they are correct. For troubleshooting tips, see *McAfee Network Security Platform Troubleshooting Guide*.

e Verify the monitoring mode of the ports on your Sensor.

1) Your Network Security Platform Sensor ports are configured by default for monitoring in **Default Prevention** mode; that is, connected in-line on a network segment (for example, between a switch and a router or two switches). If you've cabled the Sensor to monitor in another monitoring mode, check your settings to make sure everything is correct. Some users choose instead to monitor in SPAN mode at first, and move to **tap** and/or **in-line** mode later.

For more information on verifying port configuration, see *McAfee Network Security Platform Installation Guide*.

5 Configuring your deployment using the Manager

Once you're up and running and reviewing the data generated by the Manager, you can further configure and maintain your Manager. For example, you can do the following:

- **Apply security policies to each interface of your multi-port Sensor** (instead of the **Default Inline IPS** policy applied to all interfaces). You can ensure all of your interfaces deploy policies specifically for the areas of your network they are monitoring. For example, you can apply the **Web Server** policy to one interface, the **Mail Server** policy to another, and the **Internal Segment** policy to another, and so on. For more on the provided policies, see Pre-configured rule sets and policies, *McAfee Network Security Platform IPS Administration Guide*.
- **Configure responses to alerts**. Developing a system of actions, alerts, and logs based on impact severity is recommended for effective network security. For example, you can configure Network Security Platform to send a page or an email notification, execute a script, disconnect a TCP connection, send an

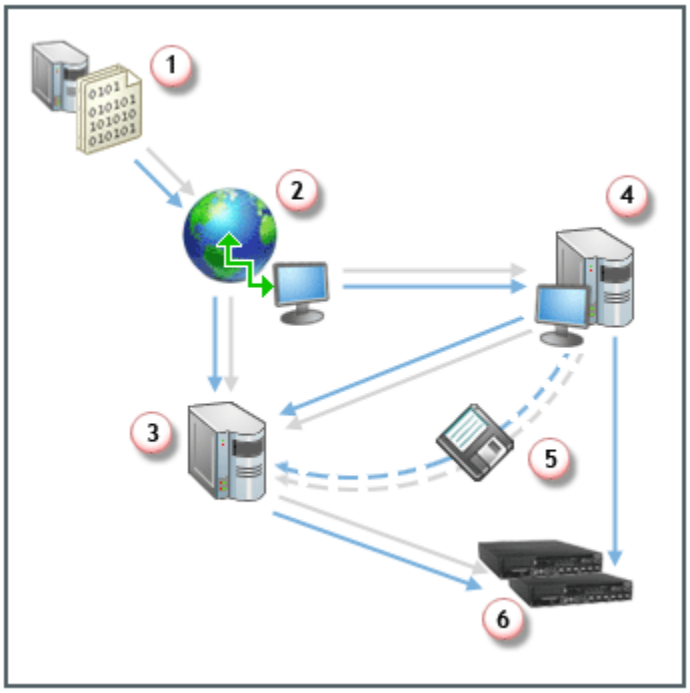
"ICMP Host Not Reachable" message to the attack source for ICMP transmissions, or send a block address filter to a host.

  - For information on response actions, see Sensor response actions, *McAfee Network Security Platform IPS Administration Guide*.
  - For information on configuring a pager, email, or script notification for alerts, see Alert notification options, *McAfee Network Security Platform Manager Administration Guide*.
  - For information on configuring a quarantine response, see Quarantining hosts, *McAfee Network Security Platform IPS Administration Guide*.
  - You can also send SNMP traps to a third-party management system. See Forward alerts to an SNMP server, and Forward faults to an SNMP server, *McAfee Network Security Platform Manager Administration Guide*.

- **Filter alerts**. The exception object feature limits the number of alerts generated by the system by excluding certain Source and Destination IP address parameters. If these address parameters are detected in a packet, the packet is allowed to finish transmission. For more information, see Managing exception objects and attack responses, *McAfee Network Security Platform IPS Administration Guide.*
- **View the Operational Status**. The Operational Status viewer details the functioning status for all of your installed Network Security Platform components. Messages are generated to detail system faults experienced by either your Manager, database, or Sensors. For more information, see *McAfee Network Security Platform Manager Administration Guide*.
- **View a Sensor's performance**. The **Devices** | **<Admin Domain>** | **Global** | **Common Device Settings** | **Performance Monitoring** | **Summary** action enables you to view performance data for a Sensor. The data collected is a reflection of the traffic that has passed through the Sensor. For more information, see *McAfee Network Security Platform IPS Administration Guide*.
- **Back up all or part of your Manager configuration information** to your server or other location. For more information, see Backing up data and settings,*McAfee Network Security Platform Manager Administration Guide*.

6 Updating your signatures and software

An essential element to a reliable IPS is updating the system signature and software images. McAfee periodically releases new Manager software and Sensor signature and software images, and makes these updates available via the Update Server to registered support customers.



Field	Description
1	McAfee Update Server
2	Internet
3	Network Security Manager Server
4	PC/tftp server
5	Import/disk
6	Network Security Sensor

There are several options for loading updates to your Manager and Sensors.

a Download latest software and signature updates from the Update Server to your Manager.

1) You can use the Manager interface to download Sensor software and signature updates from the Update Server to the Manager server, and then download the updates to the Sensor.

b Import update files from a remote workstation to your Manager.

1) If your Manager server is not connected to the Internet, you can download signature and software updates from the Update Server to any host, then do one of the following: Download the update to a host, then log in to the Manager and *import* the update to the Manager server. You can then download the update to the Sensor.

   Similar to above, download the update from the Update Server to any host, put it on a disk, take the disk to the Manager server, and then *import* the update and download it to the Sensor.

   For more information, see the *McAfee Network Security Platform Manager Administration Guide*.

c Download software from the Update Server to a TFTP client and then download to a Sensor.

1) You can download software images from the Update Server onto a TFTP server, and then download the software directly to the Sensor using Sensor CLI commands. This is useful if you prefer not to or are unable to update Sensor software via the Manager. This method is described in the *McAfee Network Security Platform Installation Guide*.

7 Tuning your deployment

Once you become familiar with the basics of the Manager, you can further enhance your deployment by utilizing some of the more advanced features. Network Security Platform is an extremely complex system and can be tuned on a highly granular level. You might try working with some of the following features as you tune your system:

- Cloning and modifying a provided policy. See Working with IPS policies, *McAfee Network Security Platform IPS Administration Guide*.
- Create Firewall policies to block specific traffic or pass specific traffic without sending it through the intrusion detection engine. See User-based access rules, *McAfee Network Security Platform IPS Administration Guide.*
- If you've started out in SPAN mode, you might try taking advantage of Network Security Platform's prevention capabilities by deploying your Sensor to monitor traffic in in-line mode. See Deployment of Sensors in in-line mode, *McAfee Network Security Platform IPS Administration Guide*.
- Adding users and assigning management roles. See Management of users and user roles, *McAfee Network Security Platform Manager Administration Guide*.
- Adding admin domains for resource management. See Create an admin domain, *McAfee Network Security Platform Manager Administration Guide*.
- Changing your interface type to CIDR or VLAN depending on your network configuration. See Managing interfaces, *McAfee Network Security Platform IPS Administration Guide*.

8 Network Security Platform documentation set

Unless otherwise noted, the product documentation is provided as Adobe Acrobat PDF files available on the McAfee Download Server and McAfee Service Portal.

The Network Security Platform documentation set is designed to provide you with the information you need during each phase of the product implementation from evaluating a new product to maintaining existing ones. After the product is released, additional information regarding the product is entered into the online Knowledge Base available on McAfee Service Portal.

Refer the following tables for a list of Network Security Platform software and hardware documentation:

Table 1 Network Security Platform software documentation

Guide	Description
Quick Tour	A high-level view of how to interact with Network Security Platform
Installation Guide	System requirements, installation of the Manager software, management of Network Security Sensors/failover pairs, and Upgrade steps

Table 1 Network Security Platform software documentation *(continued)*

Guide	Description
Manager Administration Guide	Management of admin domains, users, and roles Management of devices such as IPS Sensors and NTBA Appliances Obtaining updates from the McAfee Update Server Configuration of MDR Generation of reports Viewing status of your Network Security Platform components Monitoring alerts and hosts on your network Configuration and management of Central Manager
CLI Guide	List of all public and debug CLI commands for IPS Sensors and NTBA Appliances Initialization, upgrade or replacement of a Sensor, troubleshooting an issue, and performance monitoring for the Sensor
IPS Administration Guide	Management of policies and rule sets Management of exception objects and attack responses In-depth details for inline mode configuration Definition of failover pairs Achieving virtualization using Network Security Sensors Various IPS features supported up to the latest Network Security Platform release
Custom Attacks Definition Guide	Creation of custom attacks and signatures using the Custom Attack Editor Import of Snort signatures
XC Cluster Administration Guide	Configuration and administration of an XC 240 load balancer
Integration Guide	Integration with: • ePolicy Orchestrator • Global Threat Intelligence • Advanced Threat Defense • Threat Intelligence Exchange • Vulnerability Manager • Host Intrusion Prevention • Logon Collector • HP Network Automation • Third party SIEM products
NTBA Administration Guide	Configuring and managing NTBA Appliances Monitoring traffic usage patterns in real time Configuring NTBA virtual appliances Integration with Endpoint Intelligence Agent
Best Practices Guide	Recommended practices for using Network Security Platform most effectively

Table 1 Network Security Platform software documentation *(continued)*

Guide	Description
M-xx30 Best Practices Guide (Applicable to India and China only)	Recommended practices for using Network Security Platform M-xx30 most effectively
Troubleshooting Guide	Troubleshooting techniques for Network Security Platform

Table 2 Network Security Platform hardware documentation

Guide	Models
Sensor Product Guides	• NS7x00 and NS9x00 • M-1250/M-1450, M-2850/M-2950, M-3050/M-4050, M-6050, M-8000, and M-8000XC
Quick Start Guides	• NS7x00 and NS9x00 • M-1250/M-1450 , M-2850/M-2950, M-3050/M-4050, M-6050, M-8000, and M-8000XC • NTBA Appliance T-200, T-500, and T600 and T1200 • XC-240 Load Balancer Appliance
Slide Rail Assembly Procedure	• M-3050, M-4050, M-6050, M-8000
DC Power Supply Installation Procedure	• NS-series • M-series
Interface Modules Reference Guide	• NS-series
Transceiver Modules Reference Guide	• NS-series • M-series
GBIC Module for 1 Gigabit Ethernet Application ITV-2KLG-NA-100 Datasheet	• M-series
GBIC Module for 1 Gigabit Ethernet Application ITV-1KSG-NA-100 Datasheet	• M-series

Table 2 Network Security Platform hardware documentation *(continued)*

Guide	Models
Passive Fail-Open Bypass Kit Guides	• 10/100/1000 Copper Passive Fail-Open Kit • 1 Gigabit Optical Passive Fail-Open Kit • 10 Gigabit Passive Fail-Open Kit
Active Fail-Open Bypass Kit Guides	• 10/100/1000 Copper Active Fail-Open Kit • 10/100/1000 Copper Active Fail-Open Kit with SNMP • 1 Gigabit Optical Active Fail-Open Kit • 10 Gigabit Optical Active Fail-Open Kit • 40 Gigabit Active Fail-Open Kit