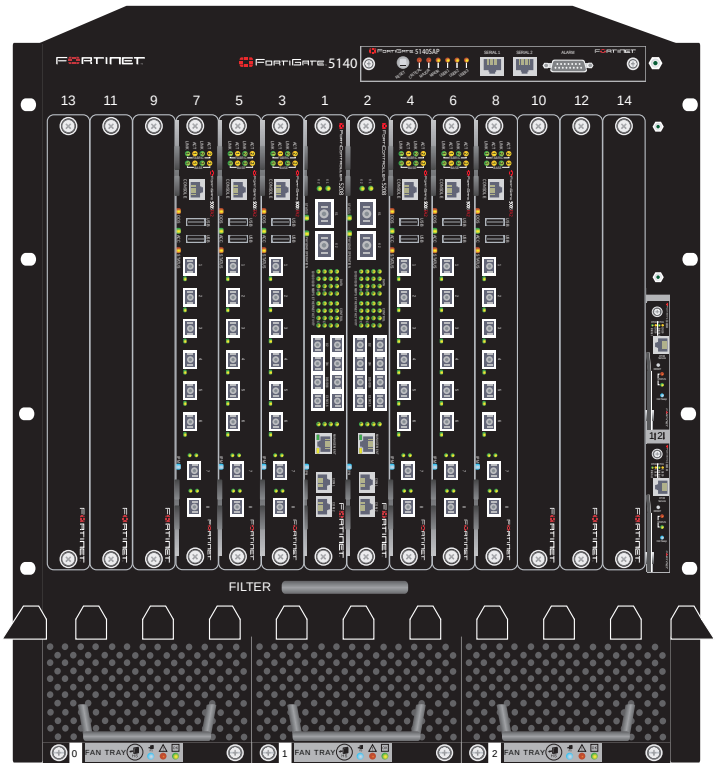
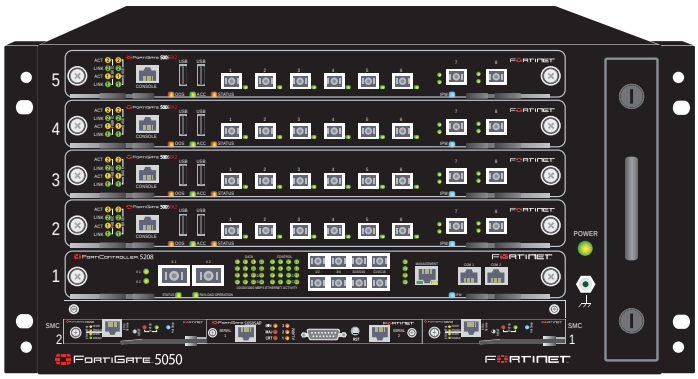
# Administration Guide

## FortiGate-5005-DIST Security System




Visit http://support.fortinet.com to register your FortiGate-5005-DIST Security System. By registering you can receive product updates, technical support, and FortiGuard services.

FORTINET

www.fortinet.com

*FortiGate-5005-DIST Security System Administration Guide*

15 June 2007
01-30003-0358-20070615



**Trademarks**
Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**Regulatory compliance**
FCC Class A Part 15 CSA/CUS

**CAUTION:** Risk of Explosion if Battery is replaced by an Incorrect Type.
Dispose of Used Batteries According to the Instructions.

# Contents

# Introduction

This *FortiGate-5005-DIST Security System Administration Guide* contains the information you need to install, configure, and operate a FortiGate-5005-DIST security system. The document begins with a description of the capabilities and some applications of the FortiGate-5005-DIST security system, describes how to install FortiGate-5005-DIST security system hardware components, how to configure FortiGate-5005-DIST systems onto your network, and also describes FortiGate-5005-DIST web-based manager and CLI options and procedures.

The following topics are included in this section:



## Revision history

**Table 1: Revision History**

| Version | Description of changes |
|---|---|
| Draft-01-00000-0358-20061117 | First draft. Still lots of work to do for this document, but this first draft has lots of useful information that may not may not be correct depending on how the product changes before it is released. |
| Draft-01-30003-0358-20070110 | Second draft. The product information included is still subject to change. Plenty to be included hasn't yet been finalized. |

## Warnings and cautions

Only trained and qualified personnel should be allowed to install or maintain FortiGate-5000 series equipment. Read and comply with all warnings, cautions and notices in this document.

**Caution:** You should be aware of the following cautions and warnings before installing FortiGate-5000 series hardware.

- Turning off all power switches may not turn off all power to the FortiGate equipment. Except where noted, disconnect the FortiGate equipment from all power sources, telecommunications links and networks before installing, or removing FortiGate components, or performing other maintenance tasks. Failure to do this can result in personal injury or equipment damage. Some circuitry in the FortiGate equipment may continue to operate even though all power switches are off.
- An easily accessible disconnect device, such as a circuit breaker, should be incorporated into the data center wiring that connects power to the FortiGate equipment.
- Install FortiGate chassis at the lower positions of a rack to avoid making the rack top-heavy and unstable.
- Do not insert metal objects or tools into open chassis slots.
- Electrostatic discharge (ESD) can damage FortiGate equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiGate chassis.
- Some FortiGate components may overload your supply circuit and impact your overcurrent protection and supply wiring. Refer to nameplate ratings to address this concern.
- Make sure all FortiGate components have reliable grounding. Fortinet recommends direct connections to the branch circuit.
- If you install a FortiGate component in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Make sure the operating ambient temperature does not exceed the manufacturer's maximum rated ambient temperature.
- Installing FortiGate equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- This equipment is for installation only in a Restricted Access Location (dedicated equipment room, service closet or the like), in accordance with the National Electrical Code.
- Per the National Electrical Code, sizing of a Listed circuit breaker or branch circuit fuse and the supply conductors to the equipment is based on the marked input current rating. A product with a marked input current rating of 25 A is required to be placed on a 40 A branch circuit. The supply conductors will also be sized according to the input current rating and also derated for the maximum rated operating ambient temperature, Tma, of the equipment.
- FortiGate equipment shall be installed and connected to an electrical supply source in accordance with the applicable codes and regulations for the location in which it is installed. Particular attention shall be paid to use of correct wire type and size to comply with the applicable codes and regulations for the installation / location. Connection of the supply wiring to the terminal block on the equipment may be accomplished using Listed wire compression lugs, for example, Pressure Terminal Connector made by Ideal Industries Inc. or equivalent which is suitable for AWG 10. Particular attention shall be given to use of the appropriate compression tool specified by the compression lug manufacturer, if one is specified.

# About this document

This document contains the information you require to install, configure, and operate a FortiGate-5005-DIST system. This document includes the following chapters:

- The FortiGate-5005-DIST Security System provides an overview of the functionality and capabilities of the FortiGate-5005-DIST Security system and also describes FortiGate-5005-DIST hardware components.
- Installing hardware components provides the information you need to install FortiGate-5005-DIST hardware components and to make sure that they are all functioning properly. Once you have completed the procedures in this chapter you can configure the FortiGate-5005-DIST system onto your network.
- Quick Configuration Guide a quick start guide to configuring a FortiGate-5005-DIST security system for your network.
- IO module administration describes how to administer FortiGate-5005-DIST I/O modules using both the web-based manager and the CLI.
- Hardware procedures describes procedures that you may be required to perform from time to time with your FortiGate-5005-DIST system.

# Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com. All FortiGate-5000 information is available from the *FortiGate-5000* page.

## Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at http://docs.forticare.com.

## Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

The *FortiGate Log Message Reference* is available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.

## Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

# Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

# The FortiGate-5005-DIST Security System

This section provides an overview of the functionality and capabilities of the FortiGate-5005-DIST Security system. This section also describes the FortiGate-5000 series hardware components that are part of the FortiGate-5005-DIST security system and how to install and configure these hardware components to create different FortiGate-5005-DIST hardware configurations.

The FortiGate-5005-DIST security system is very similar to a single FortiGate unit, but with much higher capacity and with support for failover protection and scalability. The FortiGate-5005-DIST security system consists of a FortiGate-5050 or FortiGate-5140 chassis with one or two Input/Output or I/O modules (FortiController-5208 modules) and one or more worker modules (FortiGate-5005FA2 modules running in DIST mode). The I/O modules provide network connections and distribute traffic to the worker modules. The worker modules provide FortiGate security system functions including firewall, VPN, IPS, antivirus, antispam, and so on.

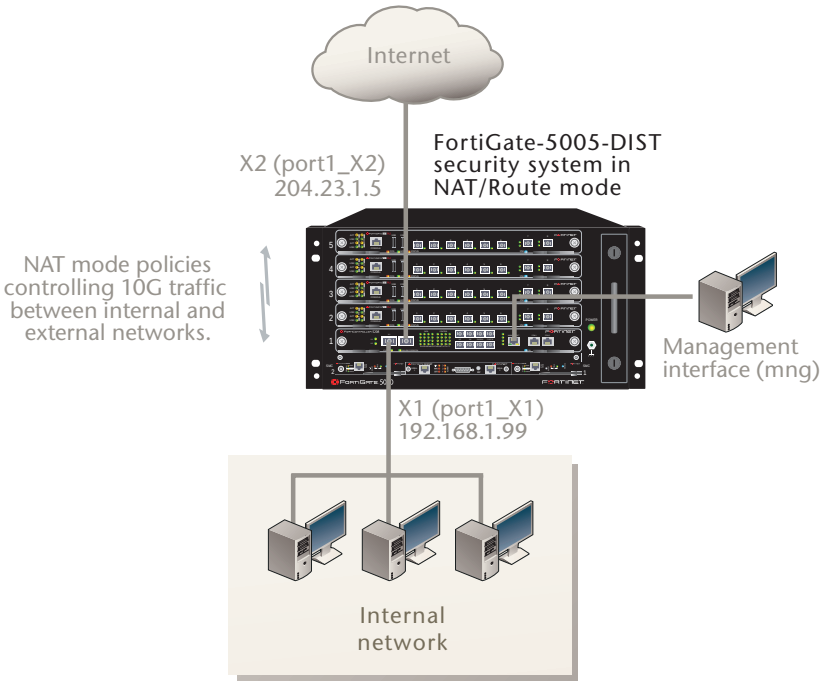
The following topics are included in this section:



## Basic FortiGate security system configuration

A basic FortiGate security system consists of a single FortiController-5208 module and four FortiGate-5005 modules installed in a FortiGate-5050 or FortiGate-5140 chassis (see Figure 1 on page 12). This system can be installed in NAT/Route mode between the Internet and a private network. In this configuration, the FortiGate-5005-DIST security system can provide FortiGate services to 10 gigabit traffic passing between the private network and the Internet.

**Figure 1: Example basic FortiGate-5005-DIST security system**

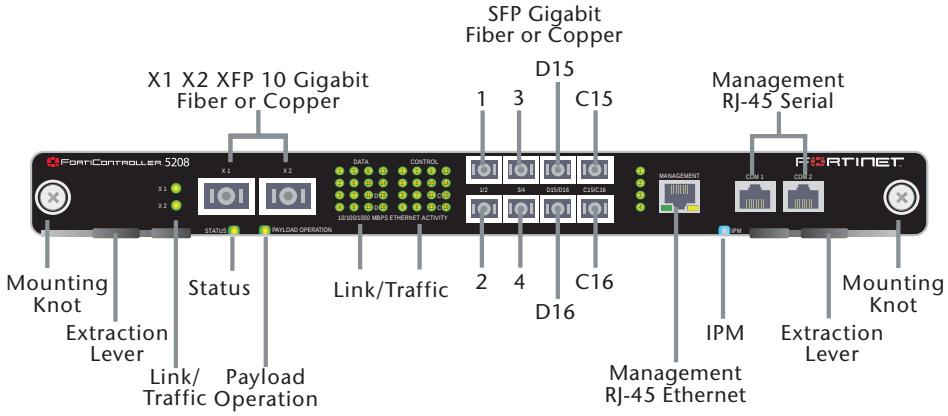



# FortiController-5208 I/O modules

Data flows into and out of the FortiGate-5005-DIST system through the I/O modules. The I/O modules are FortiController-5208 modules installed in chassis slots 1 and 2 in a FortiGate-5050 or FortiGate-5140 chassis. The I/O module installed in slot 1 is configured as the primary I/O module. The optional I/O module installed in slot 2 becomes the secondary I/O module. A FortiGate-5005-DIST system can include one or two I/O modules.

As the I/O module, the FortiController-5208 provides all FortiGate-5005-DIST network connections. The FortiController-5208 module provides two 10 gigabit interfaces and four 1 gigabit interfaces for network traffic. The FortiController-5208 front panel also contains four 1 gigabit interfaces. Two of these interfaces support inter-chassis HA and two are for future use. Adding a second FortiController-5208 module doubles the number of FortiGate-5005-DIST network interfaces.

**Figure 2: FortiController-5208 front panel**



In addition to network interfaces, the FortiController-5208 modules distribute traffic to the worker modules and administrators connect to the FortiController-5208 management interface or console port to manage the FortiGate-5005-DIST Security System. See the *FortiController-5208 System Guide* for more details about the FortiController-5208 system.

As I/O modules, the FortiController-5208 modules manage data flow between networks and among the worker modules installed in the chassis. All network connections are made to the I/O module front panel interfaces. Each I/O module uses a load distribution algorithm to distribute traffic evenly among the worker modules. The load distribution algorithm distributes traffic according to traffic source/destination address pairs to provide basic optimization of the distribution of traffic to the worker modules.

The secondary I/O module provides more interfaces for the FortiGate-5005-DIST system and is connected to different networks than the primary I/O module. The secondary I/O module is not used for failover protection and will not take the place of the primary I/O module if the primary I/O module fails. If either the primary or secondary I/O module fails, the entire FortiGate-5005-DIST system stops processing traffic.

The primary I/O module also provides all administrative connections to the FortiGate-5005-DIST system. You use the primary I/O module front panel Management RJ-45 Ethernet interface to connect to the FortiGate-5005-DIST web-based manager or CLI. You use the primary I/O module Com 2 console port to connect to the FortiGate-5005-DIST CLI. The secondary I/O module Management interface and Com 1 port are only used for a few things, such as for upgrading the secondary I/O module firmware.

## Bridge mode

Normally the FortiGate-5005-DIST system stops all network traffic if all of the worker modules fail or are unable to process traffic. The system fails closed. If you want the FortiGate-5005-DIST system to fail open, to maintain traffic flow if the worker modules fail, you can enable bridge mode. If you enable bridge mode, the I/O modules will bridge traffic between interfaces X1, X2, 1, 2, 3, and 4 when all the worker modules fail. Each I/O module functions as a hub. In this state, traffic is allowed to flow with no security restrictions or inspection of any kind.

Bridge mode is available in both transparent and NAT operating modes, though no address translation will occur if a FortiGate-5005-DIST system operating in NAT mode enters bridge mode.

If a DIST system equipped with two I/O modules enters bridge mode, each I/O module will bridge only its own interfaces. The two I/O modules are isolated from each other even if firewall policies allow traffic between interfaces on different I/O modules.

**Caution:** In bridge mode, traffic can pass between FortiGate-5005-DIST network interfaces with no security restrictions.

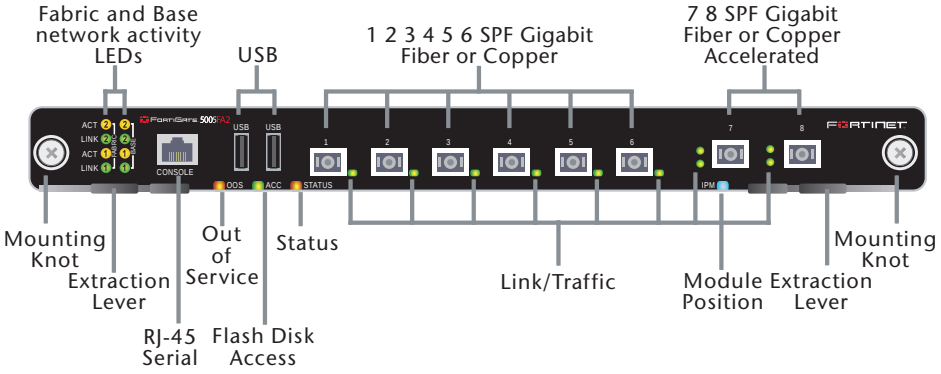
The I/O modules continue to check for available worker modules while in bridge mode. If the I/O module detects an operating worker module, the I/O module leaves bridge mode and resumes normal operation.

# FortiGate-5005FA2 worker modules

The FortiGate-5005FA2 security system serves as the worker module for the FortiGate-5005-DIST security system. Worker modules are identically configured and administered as a single unit from the primary I/O module. Workers are typically installed in slots 3 and above, though FortiGate-5005FA2 security systems with only one I/O module can also have a worker installed in slot 2.

The worker modules apply all of the FortiGate security system functionality to traffic passing through the FortiGate-5005-DIST security system. Traffic is distributed to the worker modules by the I/O modules. The worker modules perform FortiGate functions such as applying firewall policies, virus scanning, IPS and routing to distributed traffic.

**Figure 3: FortiGate-5005FA2 front panel**




Communication between I/O modules and worker modules takes place over the chassis backplane. In a FortiGate-5005-DIST system, the FortiGate-5005FA2 front panel network connectors are not used. You also cannot connect to the FortiGate-5005FA2 CLI using the FortiGate-5005FA2 front panel console port. In addition, FortiGate-5005FA2 accelerated packet forwarding and policy enforcement is not used.

See the *FortiGate-5005FA2 Security System Guide* for more details about the FortiGate-5005FA2 security system.

You can add worker modules to increase the capacity of the FortiGate-5005-DIST system. Control overhead increases at a moderate rate as more worker modules are added. Also, control traffic is separated from data traffic. As a result, FortiGate-5005-DIST load balancing architecture provides an almost linear increase in capacity as you add worker modules. A FortiGate-5050 chassis can contain up to 4 worker modules and a FortiGate-5140 chassis can contain up to 12.

Multiple worker modules also provide failure protection. If one worker module fails, the I/O modules distribute new sessions to the worker modules that are still operating. All sessions being processed by the failed worker module are stopped and must be restarted. Some service interruption does occur if a worker module fails, but the interruption is only temporary.

## Synchronizing the worker module firmware and configuration

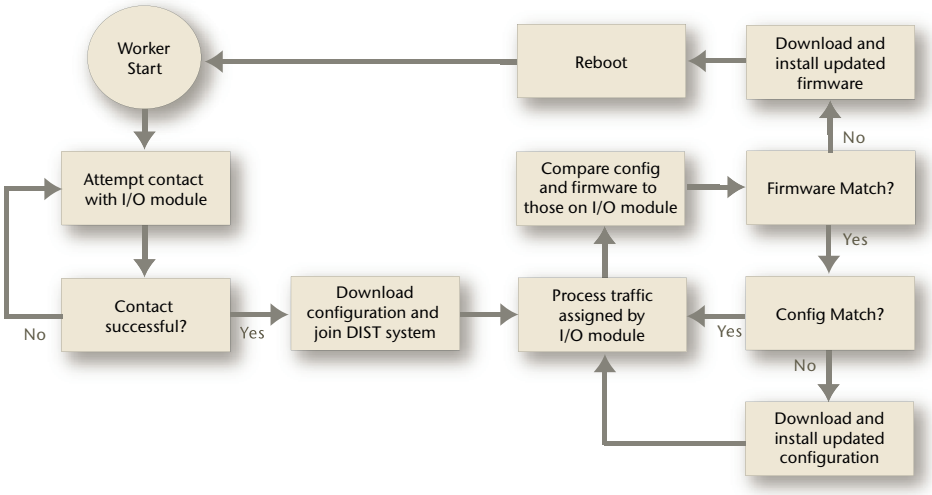
When you restart or replace a failed worker module or when you add a new worker module to a FortiGate-5005-DIST system, if the worker module is operating with DIST mode firmware the I/O module automatically recognizes the worker module and adds it to the FortiGate-5005-DIST system. Before the worker module can be added to the FortiGate-5005-DIST system the worker module must be operating with the same firmware version and configuration as the other worker modules. This section describes how the I/O module synchronizes the firmware version and configuration of new worker modules and maintains the synchronization for all worker modules.

The I/O module stores a copy of the worker module firmware and worker module configuration. During normal operation of a FortiGate-5005-DIST system, when a worker module starts (whether it's newly installed, rebooting, or powering up), it downloads a copy of the worker configuration from the I/O module and joins the FortiGate-5005-DIST system. The I/O module will recognize the worker is ready and begin sending it traffic to process.

Once part of the FortiGate-5005-DIST system, each worker will compare its own firmware and configuration to those stored on the primary I/O module every two seconds. This check is part of routine management communication and does not interfere with traffic processing.

If a changed configuration appears, each worker downloads and installs it. If a changed firmware is detected, the worker will download the firmware, install it, and reboot to complete the procedure. Once restarted, the worker downloads the config file and joins the FortiGate-5005-DIST system again.

**Figure 4: Worker startup and operating sequence**



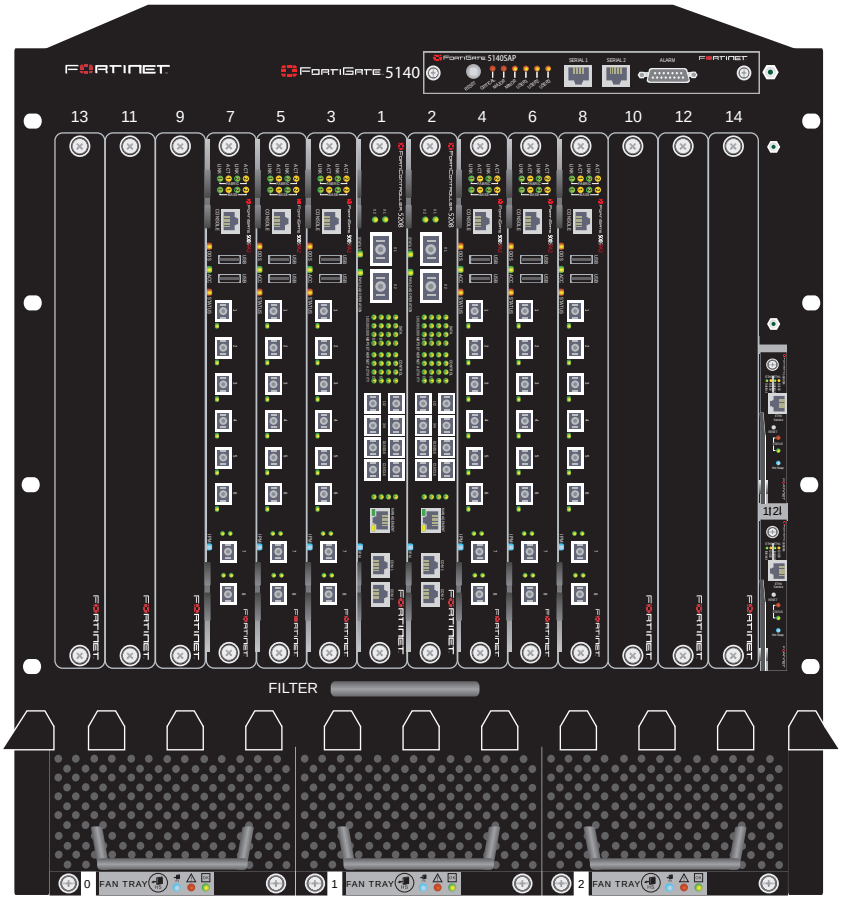
# FortiGate-5005-DIST security system chassis

FortiGate-5005-DIST security systems can be installed in FortiGate-5050 or FortiGate-5140 chassis.

## FortiGate-5140 chassis

You can install one or two I/O modules in slot 1 and 2 of the FortiGate-5140 ATCA chassis. You can also install up to 12 worker modules in slots 3 to 14 if two I/O modules are used, or up to 13 worker modules in slots 2 to 14 if one I/O module is used. The FortiGate-5140 is a 12U chassis that contains two redundant hot swappable DC power entry modules that connect to -48 VDC Data Center DC power. The FortiGate-5140 chassis also includes three hot swappable cooling fan trays. For details about the FortiGate-5140 chassis see to the *FortiGate-5140 Chassis Guide*.

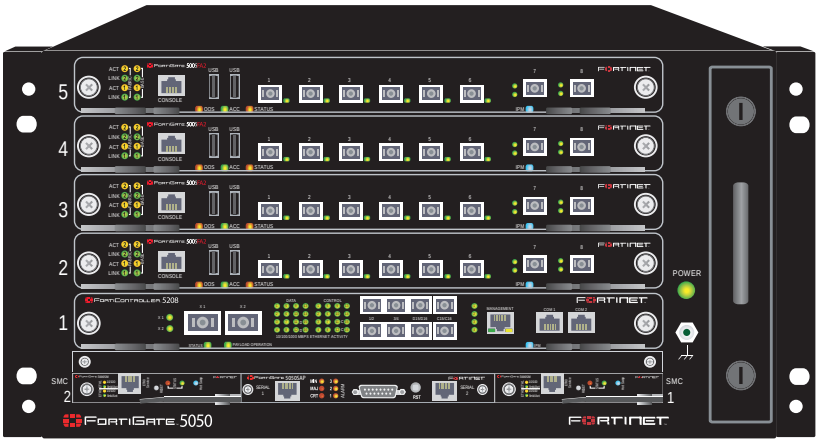
**Figure 5: FortiGate-5005-DIST components installed in a FortiGate-5140 chassis**



## FortiGate-5050 chassis

You can install one or two I/O modules in slot 1 and 2 of the FortiGate-5050 ATCA chassis. You can also install up to three worker modules in slots 3 to 5 if two I/O modules are being used, or four worker modules in slots 2 to 5 if one I/O module is used. The FortiGate-5050 is a 5U chassis that contains two redundant DC power connections that connect to -48 VDC Data Center DC power. The FortiGate-5050 chassis also includes a hot swappable cooling fan tray. For details about the FortiGate-5050 chassis, see the *FortiGate-5050 Chassis Guide*.

**Figure 6: FortiGate-5005-DIST components installed in a FortiGate-5050 chassis**




## Adding standalone modules to a FortiGate-5005-DIST chassis

You can add standalone FortiGate-5000 series modules to empty slots in a FortiGate-5140 or FortiGate-5050 chassis that contains a FortiGate-5005-DIST system. If your FortiGate-5005-DIST system only contains a single I/O module, you can also add a FortiSwitch-5003 module and more than one FortiGate-5000 module to FortiGate-5005-DIST chassis and create an HA configuration.

To add standalone modules to a chassis containing a FortiGate-5005-DIST system you should keep the following principles in mind:

- Any connection to the chassis fabric could potentially conflict with the operation of the FortiGate-5005-DIST use of the backplane fabric. To prevent conflicts, do not enable connections to the backplane fabric. For example, if you are adding one or two FortiGate-5005FA2 systems operating in standalone mode, do not enable the fabric backplane interfaces.
- You can add any FortiGate-5000 series modules to chassis slots numbered 3 and up as long as these modules are not configured to use the fabric or base backplane interfaces.
- If the FortiGate-5005-DIST system includes one I/O module (installed in slot 1) the FortiGate-5005-DIST system uses base backplane channel 1. You should not configure any FortiGate-5000 series modules to use backplane channel 1. But, you can install a FortiSwitch-5003 module in slot 2 and use backplane channel 2 for communication between standalone FortiGate-5000 series modules in slots 3 and above. For example, this could mean using the port10 interfaces for communication between two FortiGate-5001SX modules. You can also create an HA configuration using the FortiSwitch-5003 module and the second base backplane interface for HA heartbeat communications.

- If the FortiGate-5005-DIST system includes two I/O modules you cannot use base backplane communications. You should not configure any FortiGate-5000 series modules to use base backplane interfaces.

# FortiGate-5005-DIST backplane communications

All networks are connected to the I/O module front panel interfaces. All communication between the I/O modules and the worker modules takes place over the chassis backplane. Data traffic uses the base backplane interfaces. The primary I/O module sends and receives data from the worker modules using base backplane interface 1. The secondary I/O module sends and receives data from worker modules using base backplane interface 2.

Both I/O modules and all worker modules use the backplane mesh fabric for management communication. The worker modules also use the backplane mesh fabric for session correction between worker modules.

## Base backplane data communications

Data communication across the base backplane interfaces between FortiGate-5005-DIST modules uses a proprietary layer 2 protocol. This protocol tags packets so:

- For incoming packets, the system knows which I/O module interface received an incoming packet.
- For outgoing packets, the system knows which I/O module interface should be used to send an outgoing packet.

The following sequence describes base backplane communication for a FortiGate-5005-DIST system consisting of one I/O module and multiple worker modules.

Using a proprietary layer 2 protocol, the 5208 tags each packet that it receives so that the system knows which interface it is received on. The tag is sort of like a vlan tag.

The 5208 then uses a load distribution algorithm to determine which 5005FA2 to send the packet to.

The packet is sent over the chassis base backplane interface. If 5208 is in slot 1 so it sends the packet using the first base backplane interface.

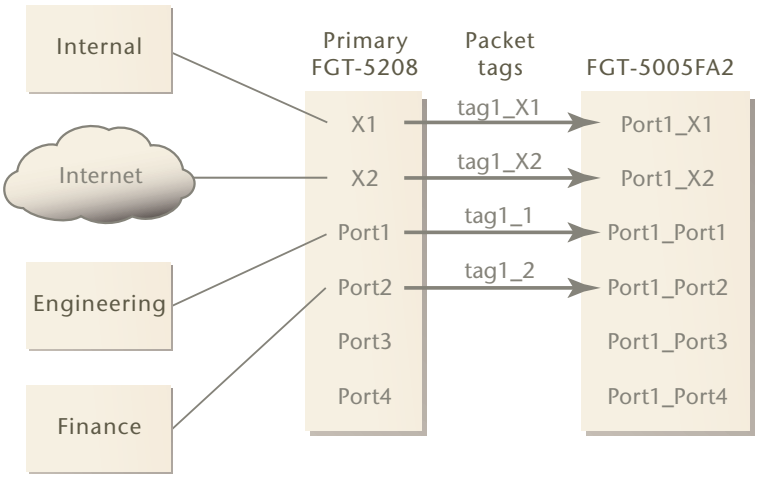
The 5005FA2 receives the packet and reads the tag to get the source interface for the packet. For example, if the 5208 receives the packet on the X1 interface the 5005 understands that the packet source interface is port1_X1.

The 5005FA2 then routes and processes the packet according to the 5005FA2 routing table and firewall policies. Routing determines the destination interface of the packet.

The 5005 forwards the processed packet back to the 5208 over the base backplane interface. The packet is tagged so that the 5208 knows its destination interface. The 5208 sends the packet out the destination interface to its destination on the network.

Figure 7 shows four networks connected to a FortiGate-5005_DIST system made up of one I/O module and one worker module. In this simple example, the I/O module tags incoming traffic packets before forwarding them to the worker module. The packet tag tells the worker module on what interface the traffic entered the DIST system. All traffic is processed by the only installed worker module.

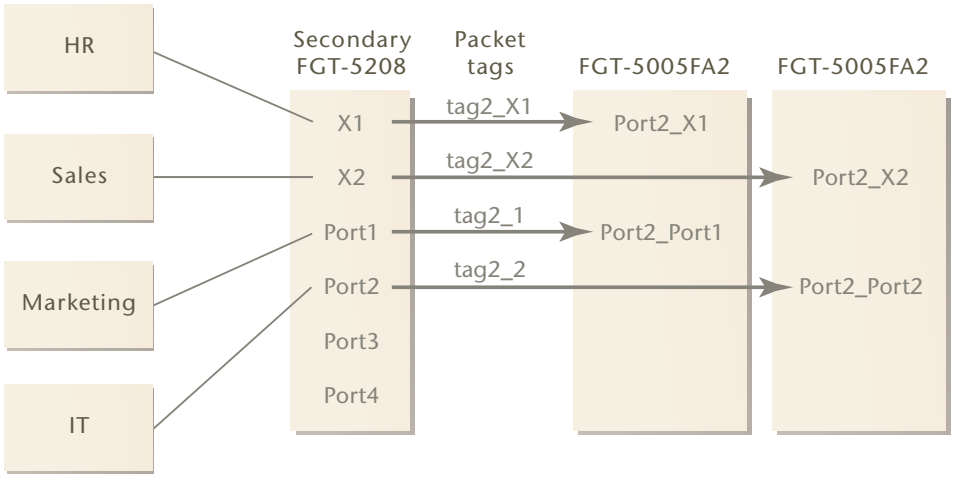
**Figure 7: Data path and packet tags with one I/O module and one worker module**




**Note:** Packet tag values in Figure 7 and Figure 8 are for illustration only. Actual tags are binary values.

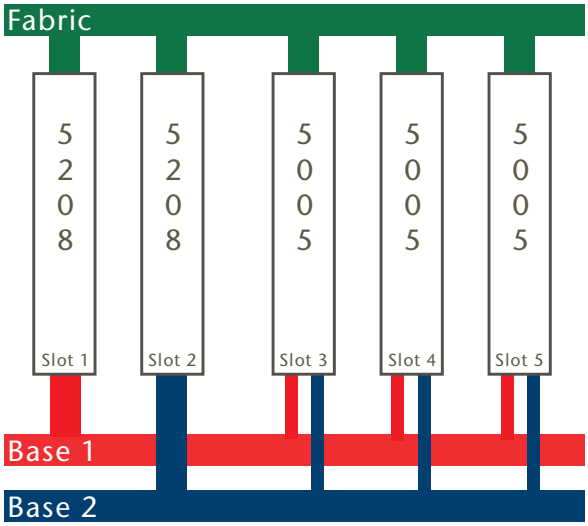
In the two-worker FortiGate-5005-DIST system illustrated in Figure 8 the primary I/O module is not displayed but it is connected to the same networks as shown in Figure 7. Both the primary and secondary I/O modules distribute traffic to the worker modules for processing.

**Figure 8: Data path and packet tags with two I/O modules and multiple workers.**




The 5208 in slot 2 uses the second base backplane interface and its front interfaces are labelled differently.

**Figure 9: Backplane connections in a FortiGate-5005-DIST system**




# Available FortiGate features

The FortiGate-5005-DIST security system supports most FortiGate security system features including basic firewall, VPN, and content screening features. The FortiGate-5005-DIST security system also supports high-end FortiGate security system features such as multiple virtual domains, vlans, redundant interfaces, 802.3ad aggregate interfaces, and dynamic routing. These features are configured in the same way for a FortiGate-5005-DIST system as for a standalone FortiGate unit.

The first version of the FortiGate-5005-DIST has the following limitations:

- Only IPSec interface mode VPN is supported. The following VPN features are not supported: SSL VPN, PPTP, and L2TP, Dialup VPN, and VPN concentrator.
- I/O module interfaces cannot be configured to use PPPoE or DHCP to acquire IP addresses.
- DHCP server and DHCP relay features are not available.
- All FortiGate user and authentication features including FSAE, local users, RADIUS users, LDAP users, and Windows AD users are not supported.
- Logging to memory or hard disk is not supported. Log messages can only be saved to a FortiAnalyzer unit or to an external syslog device. See “FortiAnalyzer logging and alert email” on page 22.
- The FortiUSB key cannot be used when the system is operating in DIST mode. The FortiUSB key can be used to upgrade the firmware on a standalone FortiGate-5005FA2 module.
- RIP, OSPF, and BGP dynamic routing is supported. However, Protocol Independent Multicast (PIM) is not supported. Dynamic and static routing can be configured between FortiGate-5005-DIST interfaces and between connected networks similar to configuring static and dynamic routing for a standalone FortiGate unit.

- Standard FortiGate HA has been replace by the HA features described in "FortiGate-5005-DIST HA and failover" on page 49.
- Management and monitoring of the FortiGate-5005-DIST system by FortiManager devices is not currently supported.

## Administration

All administration and configuration of the FortiGate-5005-DIST security system is done through the primary I/O module (the FortiController-5208 module installed in slot 1). This includes configuration of the I/O module, configuration of the worker modules, and upgrading I/O module and worker module firmware.

To connect to the FortiGate-5005-DIST web-based manager and CLI you must connect to the primary FortiController-5208 Ethernet management interface. You can also connect to the FortiGate-5005-DIST CLI using the primary FortiController-5208 serial Com 2 console port.

The FortiGate-5005-DIST web-based manager includes separate I/O module and worker module web-based managers and CLIs. When you first connect to the Ethernet management interface using HTTP or HTTPS you connect to the I/O module web-based manager. From the I/O module web-based manager you can configure the FortiGate-5005-DIST mng (management) interface and associated routing, configure system time and other basic settings, upgrade I/O module and worker module firmware, and get status information about the FortiGate-5005-DIST system.

You also access the worker module web-based manager from the I/O module web-based manager. You use the worker module web-based manager to configure all FortiGate-5005-DIST security settings, similar to configuring a standalone FortiGate system. All worker module configuration changes that you make are synchronized to all worker modules. Some worker module configuration settings also affect the operation of the I/O module. Most notably, administrative accounts for accessing the I/O module are configured from the worker module web-based manager.

The FortiGate-5005-DIST CLI works in much the same way. When you connect to the CLI using a console connection to the primary I/O module or using SSH to connect to the Management interface, you first connect to the primary I/O module CLI. From here you can use the command `execute worker manage` to connect to the worker module CLI.

## FortiGate-5005-DIST interface names

The FortiGate-5005-DIST worker web-based manager and CLI use an internal naming convention to name FortiGate-5005-DIST interfaces. The interface names indicate the I/O module containing the interface and also include the I/O module front panel interface name. The naming convention is:

`port<I/O_module_number>_<I/O_module_interface_name>`

where:

`<I/O_module_number>` is 1 for the interfaces of the primary I/O module installed in chassis slot 1 and 2 for the interfaces of the secondary I/O module installed in chassis slot 2. The interfaces for the secondary I/O module only appear in the web-based manager and CLI when a secondary I/O module is installed.

<I/O_module_interface_name> is the name of the interface as shown on the FortiController-5208 front panel.

Table 2 on page 22 shows the relationship between the names of the primary and secondary module front panel interfaces and the interface names that appear on the FortiGate-5005-DIST worker web-based manager and CLI.

**Table 2: FortiGate-5005-DIST interface naming**

| FortiController-5208 location | FortiController-5208 front panel interface names | Web-based manager and CLI interface names |
|---|---|---|
| Primary FortiController-5208 module installed in chassis slot 1 | X1 | port1_X1 |
| | X2 | port1_X2 |
| | 1 | port1_1 |
| | 2 | port1_2 |
| | 3 | port1_3 |
| | 4 | port1_4 |
| | Management | mng |
| Secondary FortiController-5208 module installed in chassis slot 2 | X1 | port2_X1 |
| | X2 | port2_X2 |
| | 1 | port2_1 |
| | 2 | port2_2 |
| | 3 | port2_3 |
| | 4 | port2_4 |
| | Management | Not used. |

## FortiAnalyzer logging and alert email

You should configure remote logging using a FortiAnalyzer unit or a syslog server to view and analyze FortiGate-5005-DIST log messages. Each worker module and I/O module creates separate log messages. Each module sends its own log messages through the primary I/O module Management interface to the FortiAnalyzer unit or to a remote syslog server. The FortiAnalyzer or remote syslog server must be accessible from the network that the management interface is connected to.

For your FortiAnalyzer unit to receive all FortiGate-5005-DIST system log messages, you must all add of the worker modules and I/O modules to your FortiAnalyzer configuration.

Each worker module also sends its own alert email messages. The FortiGate-5005-DIST system also sends alert email from the primary I/O module Management interface. Your mail server must be accessible from the network that the management interface is connected to.

## Quarantine and content archiving

Because the FortiGate-5005-DIST system does include hard disks, you must use a FortiAnalyzer device for file quarantine and content archiving. All worker modules have the same quarantine and content archiving configuration. Each worker module sends data to the same FortiAnalyzer unit. Just as for log messages, you must add all of the worker modules to your FortiAnalyzer configuration.

## FortiGuard services

The FortiGate-5005-DIST system supports all FortiGuard services. Only the worker modules require FortiGuard subscriptions because only the worker modules use FortiGuard services. You must have FortiGuard subscriptions for each worker module. All the worker module FortiGuard subscriptions must be the same because all the worker modules will share the same FortiGuard configuration settings.

The FortiGate-5005-DIST system communicates with the FortiGuard Distribution Network (FDN) through the I/O module Management interface. Make sure the management interface is connected to a network that has access to the Internet or to an internal FortiGuard server.

Database updates (antivirus and IPS) and lookup requests (web filtering and antispam) are handled differently.

### FortiGuard Web Filtering and Antispam

FortiGuard Web Filtering and FortiGuard Antispam lookup requests are submitted by any worker module processing traffic requiring a lookup. The FortiGuard servers answers the worker's request with the results of the lookup. Each worker module maintains its own FortiGuard WebFilter and AntiSpam caches.

### FortiGuard Antivirus and IPS

FortiGuard servers will deliver Antivirus and IPS database and engine updates to only one worker, called the master worker. The master worker will apply the update to its own database and also send a copy of the database update to the primary I/O module. The next time each worker makes its regular check with the primary I/O module for configuration changes, the database update will be downloaded and applied. This saves network resources and ensures all workers receive the same update.

## SNMP

Only the worker modules support SNMP. Each worker module runs its own SNMP agent, responds to SNMP queries, and sends its own SNMP traps. All SNMP traps, queries, and responses to queries use the primary I/O module Management interface.

## FortiManager

At this time, the FortiGate-5005-DIST system does not support management by the FortiManager devices.

## Virtual domains

The FortiGate-5005-DIST system supports virtual domains in much the same way as standalone FortiGate units. You enable virtual domain configuration, add virtual domains, configure global settings, and configure virtual domain settings from the FortiGate-5005-DIST worker module web-based manager or CLI.

The number of virtual domains that a FortiGate-5005-DIST system supports is determined by virtual domain licensing of the worker modules. Each worker module must be licensed separately and each worker module must be licensed for the same number of virtual domains. The maximum number of virtual domains that a FortiGate-5005-DIST system supports is the maximum number of virtual domains supported by a single worker module. Worker modules support 10, 25, 50, 100 or 250 virtual domains.

### Changing virtual domain licensing of a FortiGate-5005-DIST system

The following procedure describes how to obtain a virtual domain license key for each FortiGate-5005FA2 module in your FortiGate-5005-DIST system so that you can increase the number of virtual domains that your FortiGate-5005-DIST system is licensed for.

**To change the virtual domain licensing of a FortiGate-5005-DIST system**

1. Record the serial number of each FortiGate-5005FA2 module in the FortiGate-5005-DIST system.

   You can find the serial number in the web-based manager on the System Status page.
2. Send the serial numbers to Fortinet customer support and request a license key for 25, 50, 100 or 250 VDOMs for each FortiGate-5005FA2 module.
3. When you receive your license keys, go to the worker module web-based manager.
4. Go to **System > Maintenance > License**.
5. In the License Key field, enter the 32-character license keys you received from Fortinet.
6. Select Apply.

## Hardware and network configuration examples

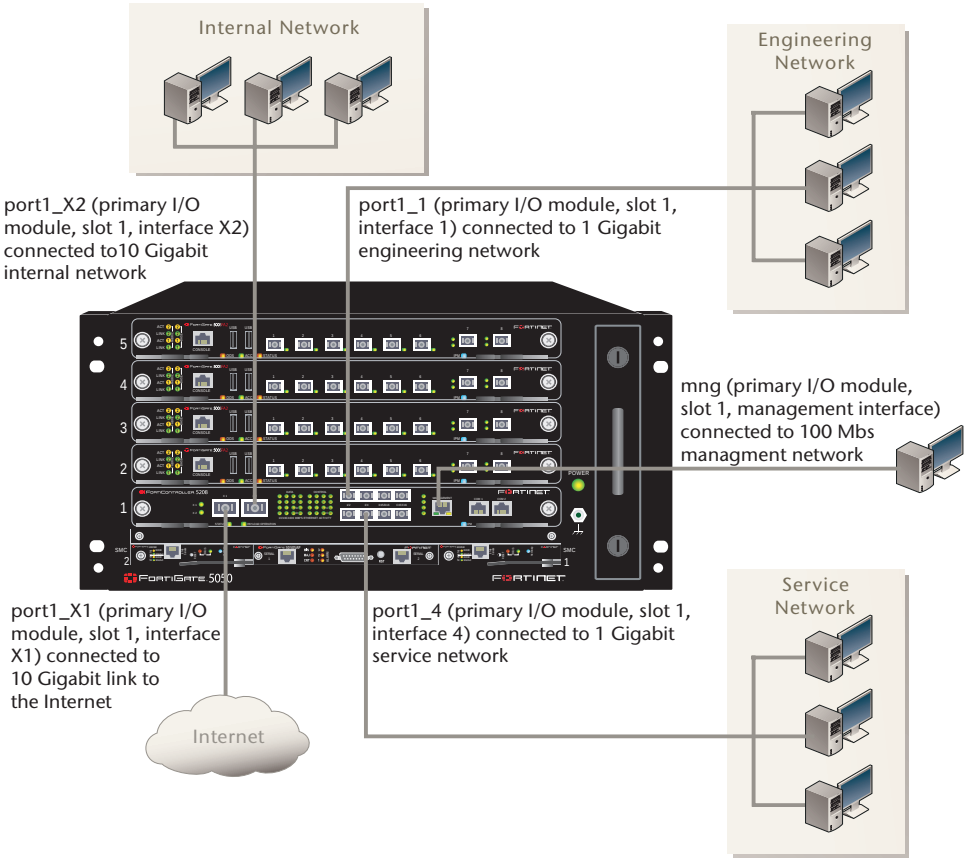
This section describes some typical FortiGate-5005-DIST hardware and network configuration examples.

### Example FortiGate-5050 chassis configuration

The example shown in Figure 10 consists of a FortiGate-5005-DIST security system installed in a FortiGate-5050 chassis. The FortiGate-5005-DIST security system includes two FortiGate-5005A2 worker modules installed in slots 3 and 4 and a single FortiController-5208 I/O module installed in slot 1.

The I/O module is connected to two 10 Gigabit networks (internal and the Internet) and two 1 Gigabit networks (the engineering network and the service network). As well, the I/O module management interface is connected to a management network.

**Figure 10: Example 5005-DIST system with one 5208 module in a 5050 chassis**




You can increase the processing capacity of this FortiGate-5005-DIST configuration by installing one or two more FortiGate-5005FA2 modules in the empty slots. This FortiGate-5005-DIST configuration can also process traffic for one or two more Gigabit networks. To connect more than 6 networks to the system or to increase the number of 10 Gigabit networks, you can install a second FortiController-5208 I/O module in slot 2. The second I/O module would reduce the maximum number of worker modules to three, however.

Table 3 shows how the FortiController-5208 I/O module front panel interface names map to FortiGate-5005-DIST web-based manager and CLI interface names and shows the networks that each of the interfaces is connected to.

**Table 3: Example configuration FortiGate-5208 network interface naming**

| FortiController-5208 front panel interface name | Web-based manager and CLI interface name | Network that the interface is connected to |
|---|---|---|
| X1 | port1_X1 | 10 Gigabit connection to the Internet. |
| X2 | port1_X2 | 10 Gigabit connection to the internal network. |
| 1 | port1_1 | 1 Gigabit connection to the engineering network. |
| 2 | port1_2 | Not connected. |
| 3 | port1_3 | Not connected. |
| 4 | port1_4 | 1 Gigabit connection to the service network. |
| Management | mng | 100 Mbit management network. |

Table 4 shows some examples of the source and destination interfaces to select to create different firewall policies.

**Table 4: Example configuration firewall policies**

| Source network | Destination network | Firewall policy | |
|---|---|---|---|
| | | Source interface | Destination interface |
| Internal | Internet | port1_X2 | port1_X1 |
| Internal | Engineering | port1_X2 | port1_1 |
| Internal | Service | port1_X2 | port1_4 |
| Engineering | Internal | port1_1 | port1_X2 |
| Engineering | Internet | port1_1 | port1_X1 |
| Service | Engineering | port1_4 | port1_1 |
| Service | Internal | port1_4 | port1_X2 |

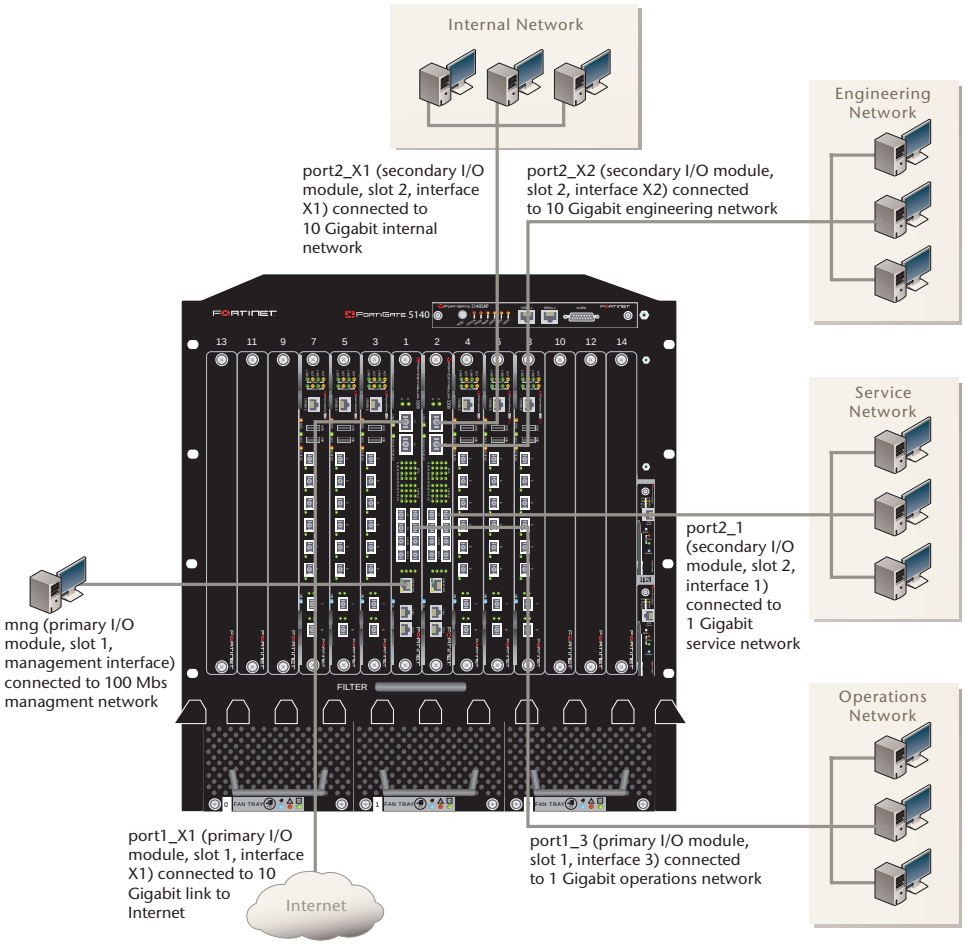
## Example FortiGate-5140 chassis configuration

The example shown in Figure 11 consists of a FortiGate-5005-DIST security system installed in a FortiGate-5140 chassis. The FortiGate-5005-DIST system includes two FortiController-5208 I/O modules installed in chassis slots 1 and 2 as well as six FortiGate-5005FA2 worker modules installed in slots 3 to 8.

The primary I/O module is connected to one 10 Gigabit network (the Internet) and one 1 Gigabit network (operations). As well, the primary I/O module management interface is connected to a management network.

The secondary I/O module is connected to two 10 Gigabit networks (internal and engineering) and one 1 Gigabit network (service).

**Figure 11: Example 5005-DIST system with two I/O modules in a FortiGate-5140 chassis**




You can increase the processing capacity of this FortiGate-5005-DIST configuration by installing more worker modules in slots 9 to 14. This FortiGate-5005-DIST configuration can also process traffic for one more 10 Gigabit network and up to six more 1 Gigabit networks.

Table 5 and Table 6 shows how the primary and secondary FortiController-5208 front panel interface names map to FortiGate-5005-DIST web-based manager and CLI interface names and shows the networks that each of the interfaces is connected to.

**Table 5: Example configuration primary FortiGate-5208 I/O module network interface naming**

| FortiController-5208 front panel interface name | Web-based manager and CLI interface name | Network that the interface is connected to |
|---|---|---|
| X1 | port1_X1 | 10 Gigabit connection to the Internet. |
| X2 | port1_X2 | Not connected. |
| 1 | port1_1 | Not connected. |
| 2 | port1_2 | Not connected. |
| 3 | port1_3 | 1 Gigabit connection to the operations network. |
| 4 | port1_4 | Not connected. |
| Management | mng | 100 Mbit management network. |

**Table 6: Example configuration secondary FortiGate-5208 I/O module network interface naming**

| FortiController-5208 front panel interface name | Web-based manager and CLI interface name | Network that the interface is connected to |
|---|---|---|
| X1 | port2_X1 | 10 Gigabit connection to the internal network. |
| X2 | port2_X2 | 10 Gigabit connection to the engineering network. |
| 1 | port2_1 | 1 Gigabit connection to the service network. |
| 2 | port2_2 | Not connected. |
| 3 | port2_3 | Not connected. |
| 4 | port2_4 | Not connected. |
| Management | mng | Not connected. |

Table 7 shows some examples of the source and destination interfaces to select to create different firewall policies.

**Table 7: Example firewall policies**

| Source network | Destination network | Firewall policy | |
|---|---|---|---|
| | | Source interface | Destination interface |
| Internal | Internet | port2_X1 | port1_X1 |
| Internal | Engineering | port2_X1 | port2_X2 |
| Internal | Service | port2_X1 | port2_1 |
| Engineering | Internal | port2_X2 | port2_X1 |
| Engineering | Internet | port2_X2 | port1_X1 |
| Service | Engineering | port2_1 | port2_X2 |
| Service | Internal | port2_1 | port2_X1 |
| Operations | Engineering | port1_3 | port2_X2 |
| Operations | Internal | port1_3 | port2_X1 |

# Installing hardware components

This section provides the information you need to install FortiGate-5005-DIST hardware components and to make sure that they are all functioning properly. Once you have completed the procedures in this chapter, you can configure the FortiGate-5005-DIST system onto your network using the procedures in “Quick Configuration Guide” on page 39.

FortiGate-5005-DIST hardware components include a FortiGate-5140 or FortiGate-5050 chassis, one or two FortiController-5208 I/O modules, and one or more FortiGate-5005FA2 modules. The chassis must be installed and connected to power and the modules must be inserted into the proper chassis slots and be operating in the correct modes before you can begin configuring your FortiGate-5005-DIST security system.

You can install and power up the FortiGate-5005-DIST hardware components in any order. If all of the components are installed in the correct slots, power is connected correctly, and all components are operating in the correct mode, the primary I/O module will connect with all components, and after a few minutes the system will be operational.

However, the first time you install a FortiGate-5005-DIST system you should follow the procedures in this chapter in order. The procedures in this chapter describe a systematic process for making sure that all hardware components are installed and functioning properly.

When all FortiGate-5005-DIST hardware components are installed and functioning correctly, you can establish a management connection to the primary I/O module CLI using the Com 2 console port. You can also establish a management connection to the primary I/O module web-based manager using the Management ethernet interface. No other management connections are possible. You cannot connect to the FortiGate-5005FA2 console port or any interface. All management is done through the primary I/O module.

The following topics are included in this section:



## Getting started

To complete the procedures in this chapter, you need:

- A FortiGate-5140 or 5050 chassis
- A rack to install the chassis in with enough space for the chassis
- DC power for the chassis
- One or two FortiController-5208 I/O modules
- SFP and XFP connectors for the interfaces you will be using

- One or more FortiGate-5005-DIST worker modules
- An electrostatic discharge (ESD) preventive wrist or ankle strap with connection cord

The procedures in this chapter reference detailed hardware install information available in the following documents. You should have these documents available before installing your FortiGate-5005-DIST security system.

- *FortiGate-5140 Chassis Guide*
- *FortiGate-5050 Chassis Guide*
- *FortiController-5208 System Guide*
- *FortiGate-5005FA2 Security System Guide*

**Caution:** FortiGate-5000 hardware components must be protected from static discharge and physical shock. Only handle or work with FortiGate-5000 components at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist or ankle strap when handling FortiGate-5000 components.

# Installing the chassis

Begin by installing your FortiGate-5140 or FortiGate-5050 chassis using the information in the *FortiGate-5140 Chassis Guide* or the *FortiGate-5050 Chassis Guide*.

**To install the chassis**

1. Install the chassis in an equipment rack.
2. Connect the chassis to DC power.
3. Turn on the power to the chassis.
4. Verify that the chassis is operating normally.

# Installing FortiController-5208 modules

If your FortiGate-5005-DIST security system includes one FortiController-5208 module it must be installed in slot 1 of your chassis. The FortiController-5208 module installed in slot 1 becomes the primary I/O module.

If your system includes two FortiController-5208 modules the second one is installed in slot 2. Use the following steps to install each FortiController-5208 module. The FortiController-5208 module installed in slot 2 becomes the secondary I/O module.

See the *FortiController-5208 System Guide* for complete information about how to insert the FortiController-5208 module into a chassis slot.

- Installing FortiController-5208 modules
- Connecting to the FortiController-5208 CLI or web-based manager
- Configuring the primary I/O module

## Installing FortiController-5208 modules

This procedure describes how to install one or two FortiController-5208 modules in a FortiGate-5005-DIST chassis. This procedure also describes how to confirm that the front panel LEDs indicate that the FortiController-5208 modules are operating normally.

### To install the FortiController-5208 modules

1 Insert the FortiController-5208 module into chassis slot 1.

See the *FortiController-5208 System Guide* for complete details.

If the chassis is powered on, the FortiController-5208 module starts up. After a few minutes, verify that the FortiController-5208 module normal operating LEDs are lit.

**Table 8: FortiController-5208 normal operating LEDs**

| LED | State |
|---|---|
| **PAYLOAD OPERATION** | Green |
| **STATUS** | Green |
| **IPM** | Off |

2 If your FortiGate-5005-DIST system includes a second FortiController-5208 module, install it in slot 2.

After a few minutes verify that the second FortiController-5208 module normal operating LEDs show normal operation.

3 Install SFP and XFP transceivers in the front panel interfaces of your FortiController-5208 I/O module as required.

## Connecting to the FortiController-5208 CLI or web-based manager

The following procedures describe how to confirm that a FortiController-5208 module is operating normally by connecting to the FortiController-5208 CLI or web-based manager.

### To connect to the FortiController-5208 console port

You can confirm that the FortiController-5208 module is operating normally if you can connect to the CLI using the Com 2 front panel console port.

1 Use the serial cable supplied with your FortiController-5208 module to connect the FortiController-5208 Com 2 port to a management computer serial port.

2 Start a terminal emulation program (HyperTerminal) on the management computer.

Use these settings: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

3 Press Enter a few times on the management computer.

If the FortiController-5208 is operating normally the `login:` prompt appears. You can type admin and press Enter twice (no password required) to log into the CLI.

Enter the command `get system status`. The output similar to the following is displayed if the FortiController-5208 is operating normally.

```
Version:Fortigate-5208 3.00,build039,061031
Serial-Number:123456789012345
Bios version:04000002
Hostname:FTG5K-IO
System time: Tue Nov 7 09:30:18 2006
```

If you cannot connect to the CLI make sure your connections are good and that your terminal emulation settings are correct. You could also try connecting to the web-based manager using the following procedure.

If you still cannot connect, contact Fortinet Support.

**To connect to the FortiController-5208 web-based manager**

You can confirm that the FortiController-5208 module is operating normally if you can connect to the web-based manager using the Management front panel Ethernet interface.

1. Connect the Management ethernet interface of the FortiController-5208 module to the same hub, switch, or network as a management computer.
2. The default IP address of the FortiController-5208 Management interface is 192.168.1.99. Configure the management computer to be on the same subnet as the Management interface. For example, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. To access the web-based manager, start Internet Explorer on the management computer and browse to https://192.168.1.99 (remember to include the “s” in https://).

   If the FortiController-5208 is operating normally, the FortiGate login page appears.
4. Type admin in the Name field and select Login (no password required).

   The FortiController-5208 System Status page (also called the dashboard) is displayed (for example, see Figure 12 on page 36).

   If you cannot connect to the web-based manager make sure your connections are good and that the management computer IP address is correct. The Management interface should also respond to pings at 192.168.1.99. You could also try connecting to the CLI using the previous procedure.

   If you still cannot connect, contact Fortinet Support.

## Configuring the primary I/O module

Once the FortiController-5208 modules are installed you must configure the FortiController-5208 module installed in slot 1 to be the primary I/O module. All FortiController-5208 modules default to operating as a secondary I/O module, and wait for communication from the primary FortiController-5208 module.

You must always configure the FortiController-5208 module installed in slot 1 to be the primary I/O module. This is true if the FortiGate-5005-DIST system contains one or two FortiController-5208 modules.

If your system contains two FortiController-5208 modules an extra step is required on the primary I/O module.

This section also contains an optional procedure for enabling bridge mode. Bridge mode provides fail open protection for the FortiGate-5005-DIST system. If you enable bridge mode, the FortiController-5208 modules will function similar to network hubs and continue to pass traffic if all FortiGate-5005FA2 modules fail.

If your FortiGate-5005-DIST system only contains one I/O module, you can use the procedure "To add a secondary I/O module to a functioning FortiGate-5005-DIST system" on page 87 to add a secondary I/O module.

**To configure the primary I/O module**

1 Connect to the CLI of the FortiController-5208 module installed in slot 1.

Use the Com 2 port as described in "To connect to the FortiController-5208 console port" on page 31.

2 Enter the following commands to set the FortiController-5208 module to be the primary I/O module.

- If there is only one FortiController-5208 module, enter the following command:

```
config system global
    set io-primary enable
end
```

- If there are two FortiController-5208 modules, enter the following commands:

```
config system global
    set io-primary enable
    set io-num double
end
```

The FortiController-5208 module in slot 1 becomes the primary I/O module. If you have installed a FortiController-5208 module in slot 2, the module in slot 2 recognizes that the FortiController-5208 module in slot 1 is the primary I/O module. The FortiController-5208 module in slot 2 becomes the secondary I/O module.

**To enable bridge mode (optional)**

1 Connect to the CLI of the FortiController-5208 module installed in slot 1.

Use the Com 2 port as described in "To connect to the FortiController-5208 console port" on page 31.

2 Enter the following command to enable bridge mode.

```
config system global
    set io-bridge enable
end
```

# Installing FortiGate-5005FA2 worker modules

When configured as a FortiGate-5005-DIST system, the FortiGate-5050 chassis will support up to four FortiGate-5005FA2 modules in slots 2 to 5 with a single FortiController-5208 module in slot 1, or up to three FortiGate-5005FA2 modules in slots 3 to 5 with two FortiController-5208 modules in slots 1 and 2. When using a FortiGate-5140 chassis, the FortiGate-5005-DIST system supports any arrangement of FortiGate-5005FA2 modules in slots 3 to 14. You cannot install a FortiGate-5005FA2 module in chassis slots 1 or 2 using the FortiGate-5140 chassis.

See the *FortiGate-5005FA2 Security System Guide* for complete information about how to insert the FortiGate-5005FA2 module into a chassis slot.

FortiGate-5005FA2 modules can operate in normal mode or in DIST mode depending on the firmware installed on the module. A FortiGate-5005FA2 module must be running DIST mode firmware before it can join a FortiGate-5005-DIST system.

The procedures in this section describe how to install FortiGate-5005FA2 modules. These procedures also describe how to determine the mode that the FortiGate-5005FA2 module is operating in and if required how to install DIST firmware so that the module operates in DIST mode.

- Installing FortiGate-5005FA2 modules
- Verifying that FortiGate-5005FA2 modules can communicate with the primary I/O module
- Installing DIST firmware on a FortiGate-5005FA2 module

## Installing FortiGate-5005FA2 modules

This procedure describes how to install FortiGate-5005FA2 modules in a FortiGate-5005-DIST chassis. This procedure also describes how to confirm that the front panel LEDs indicate that the FortiGate-5005FA2 modules are operating normally.

### To install FortiGate-5005FA2 modules

1 Install a FortiGate-5005FA2 module in any slot numbered 2 or higher in a single I/O module FortiGate-5005-DIST system, or slot 3 or higher in a dual I/O module FortiGate-5005-DIST system.

See the *FortiGate-5005FA2 Security System Guide* for details.

If the chassis is powered on, the FortiGate-5005FA2 module starts up. After a few minutes, verify that the FortiGate-5005FA2 module normal operating LEDs are lit.

**Table 9: FortiGate-5005FA2 normal operating LEDs**

| LED | State |
|---|---|
| **OOS** | Off |
| **ACC** | Off (Or flashing green when the system accesses the FortiGate-5005FA2 flash disk.) |
| **STATUS** | Green |
| **IPM** | Off |

2 Repeat this procedure for each FortiGate-5005FA2 module to be installed.

## Verifying that FortiGate-5005FA2 modules can communicate with the primary I/O module

From the primary I/O module CLI or web-based manager you can display information about the status of the FortiGate-5005FA2 modules that are operating in DIST mode. If the FortiGate-5005FA2 modules are operating in normal mode they are not visible from primary I/O module CLI or web-based manager. Use the procedures in this chapter to verify that the FortiGate-5005FA2 modules that you have installed are operating in DIST mode or not.

### To view FortiGate-5005FA2 module status from the primary I/O module CLI

1 Connect to the primary I/O module CLI.

See "To connect to the FortiController-5208 console port" on page 31.

2 Enter the command `execute worker list`. If the FortiGate-5005FA2 modules are operating in DIST mode, a message similar to the following is displayed:

```
2 workers are found
Found a worker at Slot-10 with IP address-192.168.100.26
Found a worker at Slot-6 with IP address-192.168.100.22
```

This message could be displayed by a FortiGate-5005-DIST system running in a FortiGate-5140 chassis with worker modules installed in chassis slots 6 and 10. The message indicates that both worker modules are operating in DIST mode and have successfully connected to the primary I/O module and become worker modules in the DIST configuration. The FortiGate-5005FA2 modules listed in this message are working properly and have been successfully installed.

If some or all of the worker modules do not appear in the list, use the procedure "To view the status of FortiGate-5005FA2 modules from the FortiGate-5005FA2 CLI" on page 36 to verify the status of each module and determine a course of action for changing the module to operate in DIST mode.

**Note:** I/O and worker modules are assigned IP addresses for control communication over the chassis backplane fabric interfaces. These IP addresses are assigned automatically and cannot be changed. A special invisible virtual domain is used for backplane fabric control communication. Because these IP addresses are in a separate virtual domain, they will not conflict with the IP addresses that you assign to other FortiGate-5005-DIST interfaces.

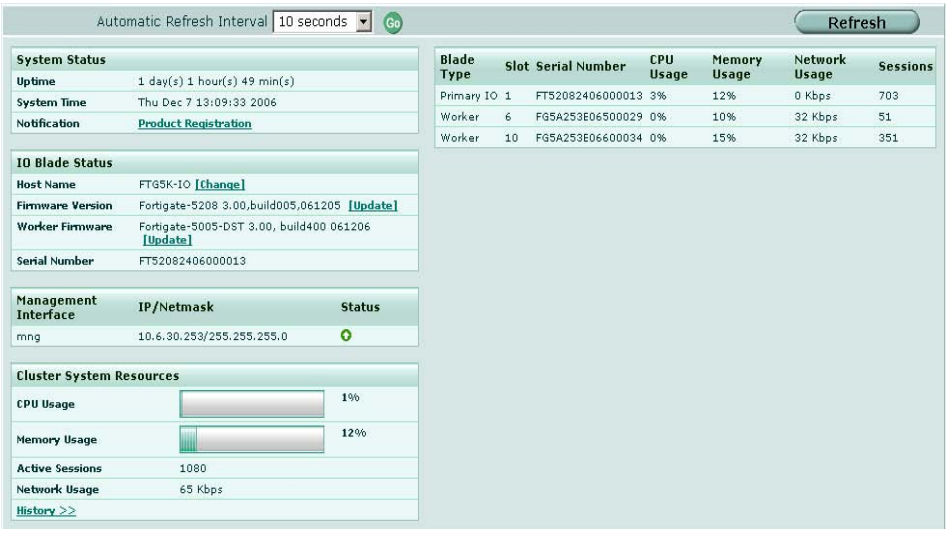
### To view worker module status from the primary I/O module web-based manager

1 Log into the primary I/O module web-based manager.

See "Connecting to the FortiController-5208 CLI or web-based manager" on page 31.

The I/O blade system status page (also called the dashboard) is displayed (see Figure 12).

**Figure 12: FortiController-5208 I/O module system status**




2 Check to see if the installed FortiGate-5005FA2 modules appear in the Blade Type list on the dashboard.

Each FG5005 entry in the list indicates a FortiGate-5005FA2 module that has successfully connected to the primary I/O module and become worker a module in the DIST configuration. The FortiGate-5005FA2 modules in this list are working properly and have been successfully installed.

If some or all of the worker modules do not appear in the list, use the procedure "To view the status of FortiGate-5005FA2 modules from the FortiGate-5005FA2 CLI" on page 36 to verify the status of each module and determine a course of action for changing the module to operate in DIST mode.

### To view the status of FortiGate-5005FA2 modules from the FortiGate-5005FA2 CLI

Use the following procedure to connect to the CLI of individual FortiGate-5005FA2 modules to verify that the module has started up and to determine the mode that the module is operating in.

1 Use the serial cable supplied with your FortiGate-5005FA2 module to connect the FortiGate-5005FA2 Console port to a management computer serial port.

2 Start a terminal emulation program (HyperTerminal) on the management computer.

Use these settings: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

3 Press Enter a few times on the management computer.

- If the message `Console access disabled` appears after the system starts, the FortiGate-5005FA2 module is operating with DIST firmware installed. The FortiGate-5005FA2 is operating in DIST mode and you should be able to view information about the FortiGate-5005FA2 module from the primary I/O module CLI or web-based manager. If the FortiGate-5005FA2 module does not appear on the primary I/O module CLI or web-based manager after a few minutes, contact Fortinet Support.
- If the `login:` prompt appears after the system starts, the FortiGate-5005FA2 module is operating with standard firmware. You can type admin and press Enter twice (no password required) to log into the CLI. You must install DIST firmware so that the FortiGate-5005FA2 module can communicate with the primary I/O module and form a DIST system. See "Installing DIST firmware on a FortiGate-5005FA2 module" on page 37.
- If the following message appears after the system starts and repeats every 30 seconds:

  ```
  wkcfg_open_retry() failed to connect to IO blade, still
  trying. Please config IO blade if it has not been
  configured yet
  ```

  The FortiGate-5005FA2 module is operating with DIST firmware and cannot connect to the primary I/O module. Check to make sure the primary I/O module is installed and configured correctly. In particular, confirm the I/O module in slot 1 is configured as the primary. For details, see "To configure the primary I/O module" on page 33. If this does not solve the problem, contact Fortinet Support.

## Installing DIST firmware on a FortiGate-5005FA2 module

Most new FortiGate-5005FA2 modules are shipped with normal firmware installed in the default partition of the FortiGate-5005FA2 boot device and DIST mode firmware installed on the boot device backup partition. If your FortiGate-5005FA2 module has DIST mode firmware installed on the boot device backup partition, you can use the procedure below to switch the DIST mode firmware to the default partition so that the FortiGate-5005FA2 module operates in DIST mode.

Alternatively, you can skip this procedure and just download and install the latest FortiGate-5005FA2 DIST mode firmware using any of the firmware procedures described in the *FortiGate-5005FA2 Security System Guide*.

### To install DIST firmware from the backup partition

Use the following procedure to switch firmware from the boot device backup partition to the boot device default partition. If DIST firmware is installed in the backup partition, at the end of this procedure the FortiGate-5005FA2 module starts up in DIST mode. If DIST firmware is not installed in the backup partition, you can download and install the latest FortiGate-5005FA2 DIST firmware.

1 Use the serial cable supplied with your FortiGate-5005FA2 module to connect the FortiGate-5005FA2 console port to a management computer serial port.

Use these settings: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

2 Press Enter a few times on the management computer.

If the FortiGate-5005FA2 module is operating normally, the `login:` prompt appears. You can type admin and press Enter twice (no password required) to log into the CLI.

3 Enter the following command to restart the FortiGate-5005FA2 module.

```
execute reboot
```

The FortiGate-5005FA2 module responds with the following message:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

4 Type y.

As the FortiGate-5005FA2 module starts, a series of system startup messages is displayed. When the following messages appears:

```
Press any key to display configuration menu.....
......
```

Immediately press any key to interrupt the system startup.

**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following menu appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,I,Q,or H:
```

5 Enter B.

The FortiGate-5005FA2 module exchanges the backup and default firmware and then restarts. If the DIST firmware was installed in the backup partition, the FortiGate-5005FA2 module starts up running the DIST firmware.

- If the message `Console access disabled` appears the FortiGate-5005FA2 is operating in DIST mode and has successfully connected to the primary I/O module.
- If the a message similar to the following appears:

  ```
  wkcfg_open_retry() failed to connect to IO blade, still
  trying. Please config IO blade if it has not been
  configured yet
  ```

  The FortiGate-5005FA2 module is operating with DIST firmware and cannot connect to the primary I/O module. Check to make sure the primary I/O module is installed and configured correctly. If this does not solve the problem, contact Fortinet Support.
- If the `login:` prompt appears, the FortiGate-5005FA2 module is still running in normal mode and you need to use any of the firmware procedures described in the *FortiGate-5005FA2 Security System Guide* to install DIST firmware on the FortiGate-5005FA2 module.

# Quick Configuration Guide

This section is a quick start guide to configuring a FortiGate-5005-DIST security system for your network.

Before using this section:

- Your FortiGate-5000 series chassis should be mounted and connected to your power system
- A FortiController-5208 module should be installed in slot 1
- If required, a secondary FortiController-5208 module should be installed in slot 2
- The FortiGate-5005FA2 modules should be installed in the remaining slots (slot 3 and above is the system has two I/O modules installed, or slot 2 and above if one I/O module is installed)
- The FortiController-5208 module(s) should also have the appropriate XFP and SFP transceivers installed.
- The modules should also be powered up with the front panel LEDs indicating that the modules are functioning normally.

The following topics are included in this section:



## Planning the configuration

Before beginning to configure your FortiGate-5005-DIST security system, you need to plan how to integrate the unit into your network. Your configuration plan depends on the operating mode that you select: NAT/Route mode (the default) or Transparent mode.

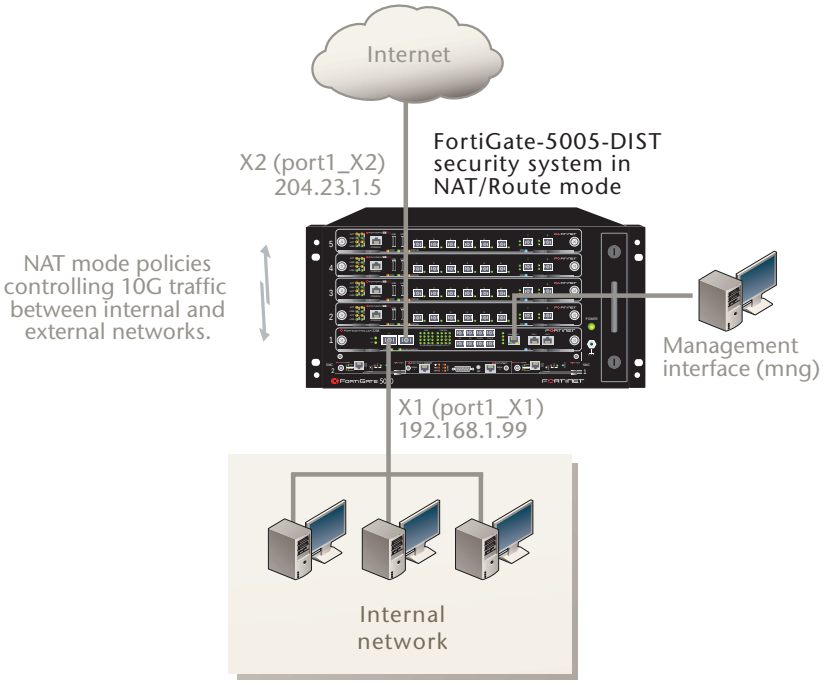
## NAT/Route mode

In NAT/Route mode, the FortiGate security system is visible to the networks that it is connected to. Each interface connected to a network must be configured with an IP address that is valid for that network. In many configurations, in NAT/Route mode all of the FortiGate security system interfaces are on different networks, and each network is on a separate subnet.

You would typically use NAT/Route mode when the FortiGate security system is deployed as a gateway between private and public networks. In the default NAT/Route mode configuration, the FortiGate security system functions as a firewall. Firewall policies control communications through the FortiGate security system. No traffic can pass through the FortiGate security system until you add firewall policies.

In NAT/Route mode, firewall policies can operate in NAT mode or in Route mode. In NAT mode, the FortiGate firewall performs network address translation before IP packets are sent to the destination network. In Route mode, no translation takes place.

**Figure 13: Example FortiGate-5005-DIST system operating in NAT/Route mode**

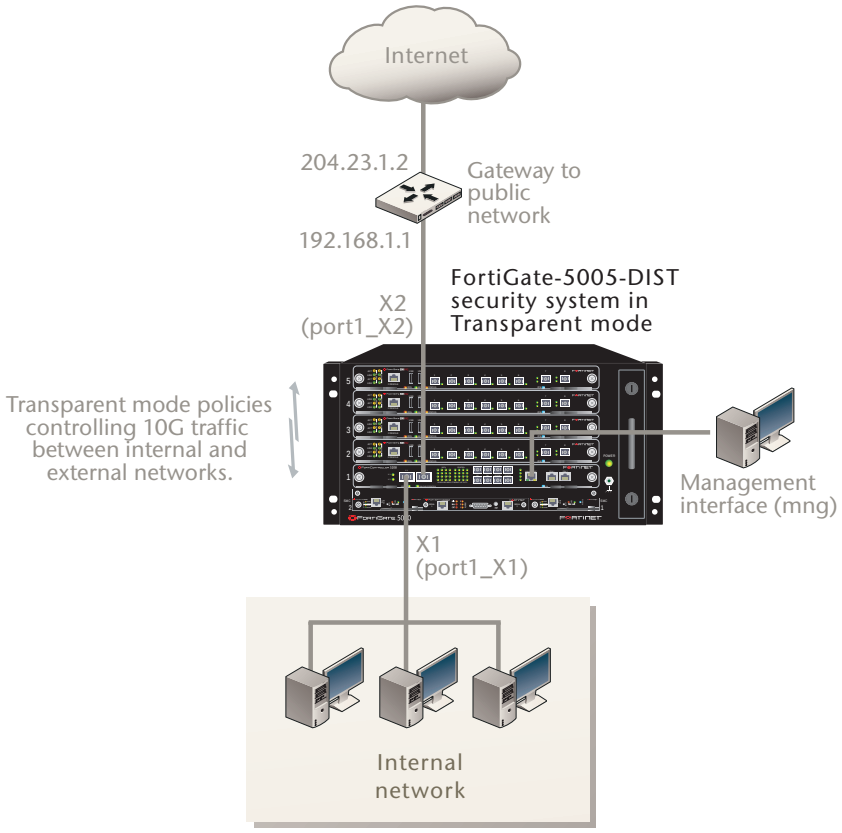


### Transparent mode

In Transparent mode, the FortiGate security system is invisible to the network. All of the FortiGate interfaces are connected to different segments of the same network. In Transparent mode you only have to configure a management IP address so that you can connect to the FortiGate security system to make configuration changes and so the FortiGate security system can connect to external services such as the FortiGuard Distribution Network (FDN).

You would typically deploy a FortiGate security system in Transparent mode on a private network behind an existing firewall or behind a router. In the default Transparent mode configuration, the FortiGate security system functions as a firewall. No traffic can pass through the FortiGate module until you add firewall policies.

**Figure 14: Example FortiGate-5005-DIST system operating in Transparent mode**




## Choosing the configuration tool

You can use either the web-based manager or the Command Line Interface (CLI) to configure the FortiGate module.

### Web-based manager

The FortiGate web-based manager is an easy to use management tool. Use the web-based manager to configure the FortiGate administrator password, the interface addresses, the default gateway, and the DNS server addresses.

Requirements:

- An Ethernet connection between the FortiController-5208 module and management computer.
- Internet Explorer 6.0 or higher on the management computer.

### Command Line Interface (CLI)

The CLI is a full-featured management tool. Use it to configure the administrator password, the interface addresses, the default gateway, and the DNS server addresses.

Requirements:

- The serial connector that came packaged with your FortiController-5208 module.
- Terminal emulation application (for example, HyperTerminal for Windows) on the management computer.

**Note:** Connections to the management computer must be made to the Com 2 interface of the primary FortiController-5208 module rather than the secondary FortiController-5208 or any of the individual FortiGate-5005FA2 modules.

## Factory default settings

The FortiGate-5005-DIST security system unit ships with a factory default configuration. The default configuration allows you to connect to the console interface and use the CLI to configure the FortiGate security system for your network. To configure the FortiGate security system for your network, add an administrator password, change the network interface IP addresses, add DNS server IP addresses, and, if required, configure basic routing.

**Table 10: FortiGate-5005-DIST factory default settings**

| | |
|---|---|
| **Operation Mode** | NAT/Route |
| **Administrator Account** | User Name: admin<br>Password: (none) |
| **X1 (port1_X1) IP/Netmask** | 192.168.1.99/24 |
| **X2 (port1_X2) IP/Netmask** | 192.168.100.99/24 |
| **All other interfaces** | 0.0.0.0/0.0.0.0 |
| **Management (mng)** | 192.168.1.99/24 |
| **Default route** | Gateway: 192.168.100.1<br>Device: port1_X2 |
| **Primary DNS Server:** | 65.39.139.53 |
| **Secondary DNS Server:** | 65.39.139.53 |

**Note:** At any time during the configuration process, if you run into problems, you can reset the FortiGate security system to the factory defaults and start over. From the web-based manager go to **System > Status**, find System Operation at the bottom of the page, and select Reset to Factory Default. From the CLI enter `execute factory reset`.

# Configuring NAT/Route mode

Use Table 11 to gather the information you need to customize NAT/Route mode settings for the FortiGate-5005-DIST security system. You can use one table to record the configuration of each FortiController-5208 module.

**Table 11: FortiGate-5005-DIST module NAT/Route mode settings**

| | | |
|---|---|---|
| **Admin Administrator Password:** | | |
| **X1 (port1_X1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **X2 (port1_X1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **1 (port1_1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **2 (port1_2)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **3 (port1_3)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **4 (port1_4)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **Management (mng)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **Secondary I/O module interfaces** | | |
| **X1 (port2_X1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **X2 (port2_X1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **1 (port2_1)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **2 (port2_2)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **3 (port2_3)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **4 (port2_4)** | IP:<br>Netmask: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |
| **Default Route** | Device (Name of the Interface connected to the external network):<br>Default Gateway IP address: | <br>_____ . _____ . _____ . _____ |
| | The default route consists of the name of the interface connected to an external network (usually the Internet) and the default gateway IP address. The default route directs all non-local traffic to this interface and to the external network. | |
| **DNS Servers** | Primary DNS Server:<br>Secondary DNS Server: | _____ . _____ . _____ . _____<br>_____ . _____ . _____ . _____ |

## Using the web-based manager to configure NAT/Route mode

1. Connect the Management interface of the primary FortiController-5208 module to the same hub or switch as the computer you will use to configure the FortiGate-5005-DIST security system.
2. Configure the management computer to be on the same subnet as the Management interface of the FortiController-5208 module. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. To access the FortiGate-5005-DIST web-based manager, start Internet Explorer and browse to https://192.168.1.99 (remember to include the “s” in https://).
4. Type admin in the Name field and select Login.

**To change the admin administrator password**

1. Go to **System > Admin > Administrators**.
2. Select Change Password for the admin administrator and enter a new password.

**To configure the management interface**

1. From the I/O module web-based manager go to **System > Network > Interface**.
2. Select the edit icon for the mng interface.
3. Enter the IP address and netmask for the interface.

**To configure interfaces**

1. Go to **Worker Blade > System > Network > Interface**.
2. Select the edit icon for each interface to configure.
3. Enter the IP address and netmask for the interface.

**To configure the Primary and Secondary DNS server IP addresses**

1. Go to **System > Network > DNS**.
2. Enter the Primary and Secondary DNS IP addresses as required and select Apply.

**To configure the Default Gateway**

1. Go to **Router > Static** and select Edit icon for the static route.
2. Select the Device that you recorded in Table 11.
3. Set Gateway to the Default Gateway IP address you recorded in Table 11.
4. Select OK.

## Using the CLI to configure NAT/Route mode

1. Use the serial cable supplied with your FortiController-5208 module to connect the FortiController-5208 Com 2 port to the management computer serial port.
2. Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings:

   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
3. At the Login: prompt, type admin and press Enter twice (no password required).
4. Configure the management interface.

```
config system interface
      edit mng
          set ip <intf_ip>/<netmask_ip>
      end
  exit
```

5 Change the administrator password.

```
execute worker manage
  config system admin
      edit admin
          set password <password>
      end
  exit
```

6 Configure the port1_X1 interface.

```
execute worker manage
  config system interface
      edit port1_X1
          set ip <intf_ip>/<netmask_ip>
      end
  exit
```

7 Repeat to configure each interface as required, for example, to configure the port1_X2 interface.

```
config system interface
  edit port1_X2
  ...
```

8 Configure the primary and secondary DNS server IP addresses.

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
  end
```

9 Configure the default gateway.

```
config router static
  edit 1
      set device <interface_name>
      set gateway <gateway_ip>
  end
```

# Configuring Transparent mode

Use Table 12 to gather the information you need to customize Transparent mode settings.

**Table 12: Transparent mode settings**

| | | |
|---|---|---|
| **Admin Administrator Password:** | | |
| **Management IP** | IP: | _____.____.____.____ |
| | Netmask: | _____.____.____.____ |
| | The management IP address and netmask must be valid for the network where you will manage the FortiGate unit. | |
| **Default Route** | Default Gateway IP address: | _____.____.____.____ |
| | In Transparent mode the default route requires the default gateway IP address. The default route directs all non-local traffic to the external network. | |
| **DNS Servers** | Primary DNS Server: | _____.____.____.____ |
| | Secondary DNS Server: | _____.____.____.____ |

## Using the web-based manager to configure Transparent mode

1. Connect the Management interface of the FortiController-5208 module to the same hub or switch as the computer you will use to configure the FortiGate module.
2. Configure the management computer to be on the same subnet as the port1 interface of the FortiGate-5005FA2 module. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. To access the FortiGate web-based manager, start Internet Explorer and browse to https://192.168.1.99 (remember to include the “s” in https://).
4. Type admin in the Name field and select Login.

### To switch from NAT/Route mode to transparent mode

1. Go to **Worker Blade > System > Status** and select the Change link beside Operation Mode: NAT.
2. Set Operation Mode to Transparent.
3. Set the Management IP/Netmask to 192.168.1.99/24.
4. Set the default Gateway to 192.168.100.1 and select Apply.
5. When complete, select **I/O Blade** to return to the FortiController-5208 interface.

### To change the admin administrator password

1. Go to **Worker Blade > System > Admin > Administrators**.
2. Select Change Password for the admin administrator, enter a new password, and select OK.
3. When complete, select **I/O Blade** to return to the FortiController-5208 interface.

**To change the management interface address**

1. Go to **Worker Blade > System > Config > Operation**.
2. Enter the Management IP address and netmask that you recorded above and select Apply.
3. When complete, select **I/O Blade** to return to the FortiController-5208 interface.

**To configure the Primary and Secondary DNS server IP addresses**

1. Go to **System > Network > DNS**.
2. Enter the Primary and Secondary DNS IP addresses as required and select Apply.

## Using the CLI to configure Transparent mode

1. Use the serial cable supplied with your FortiController-5208 module to connect the FortiController-5208 Com 2 port to the management computer serial port.
2. Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings:

   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
3. At the Login: prompt, type admin and press Enter twice (no password required).
4. Change from NAT/Route mode to Transparent mode. Configure the Management IP address and default gateway.

```
execute worker manage
  config system settings
      set opmode transparent
      set manageip <mng_ip>/<netmask>
      set gateway <gateway_ip>
      end
  exit
```

5. Configure the primary and secondary DNS server IP addresses.

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
  end
```

# Powering off the FortiGate-5005-DIST system

To avoid potential hardware problems or data loss, always shut down the modules before powering down the chassis.

**Note:** Executing a shutdown command will shut down the module's operating system. The module itself will still receive power from the chassis and indicator lights on the module may remain lit after a successful shut down operation.

### Using the CLI to shut down the FortiGate-5005-DIST system

1 Connect to the primary I/O module and shut down the worker modules.

```
execute worker shutdown
```

2 If present, shut down the secondary I/O module.

```
execute secondary-io
  execute shutdown
exit
```

3 Shut down the primary I/O module.

```
execute shutdown
```

You can now safely turn off power to the chassis.

# FortiGate-5005-DIST HA and failover

The FortiGate-5005-DIST security system supports active-passive high availability (HA) between two identical FortiGate-5005-DIST chassis. HA redundancy of DIST modules within the same chassis is not supported.

During HA operation, the primary chassis processes all traffic and the backup chassis monitors the status of the primary chassis. If one or both of the I/O modules in the primary chassis fails or if all of the worker modules in the primary chassis fails, an HA failover occurs. All new connections fail over to the backup chassis. All sessions that are active at the time of the failover are lost and have to be restarted.

To support failover, instead of connecting the I/O module network interfaces directly to their networks, the matching network interfaces from the I/O modules in each chassis are connected to switches. These switches are then connected to the appropriate networks.

The D15 and D16 front panel interfaces of the primary I/O module are used for HA communication between chassis. The minimum requirement for HA communication between the primary and backup chassis is a single 1 Gigabit ethernet connection between the D15 interface of the primary FortiController-5208 in one chassis and the D15 interface of the primary FortiController-5208 in the other chassis. You can create redundant HA communication channels between chassis by also connecting the D16 interfaces.



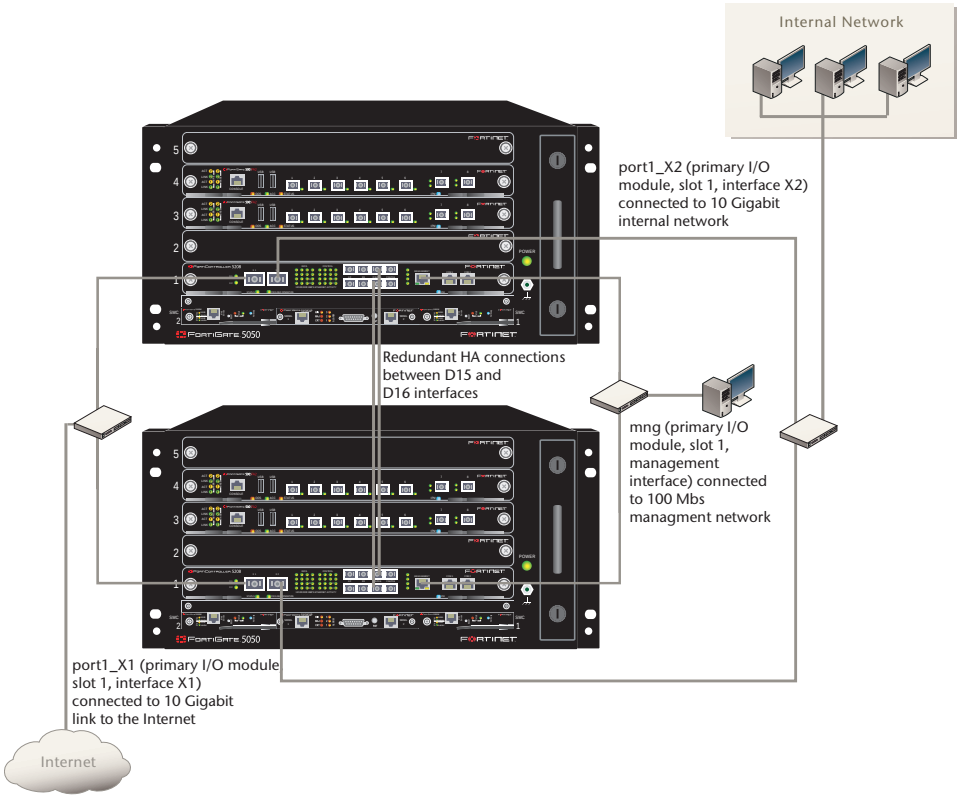
## Example HA configuration

The example shown in Figure 15 consists of two identical FortiGate-5005-DIST security systems installed in two FortiGate-5050 chassis in an HA configuration. Each chassis includes one FortiController-5208 I/O module installed in chassis slot 1 as well as 2 FortiGate-5005FA2 worker modules installed in slots 3 and 4.

In each chassis, the I/O module is connected to two 10 Gigabit networks (internal and the Internet) and one 1 Gigabit network (operations). As well, the primary I/O module management interface is connected to a management network.

The chassis in the HA configuration are connected together using the FortiController-5208 D15 and D16 front panel 1 Gigabit interfaces.

**Figure 15: Example HA configuration**




You can increase the processing capacity of this FortiGate-5005-DIST configuration by installing one or two more FortiGate-5005FA2 modules in the empty slots. This FortiGate-5005-DIST configuration can also process traffic for four 1 Gigabit networks. To connect more than 6 networks to the system or to increase the number of 10 Gigabit networks you can install a second FortiController-5208 in slot 2. The second I/O module would reduce the maximum number of worker modules to three, however.

# Configuring HA

A FortiGate-5005-DIST system will continue to function should a worker module fail. The processing power of the failed module is lost, but traffic will continue to be processed. If all the workers fail, or any installed I/O module, traffic will be halted. A High Availability (HA) configuration has a second identically configured FortiGate-5005-DIST system standing by to take over should the primary system suffer any failure severe enough to stop traffic flow.

The FortiGate-5005-DIST system HA mode is very similar to the HA mode supported by current FortiGate appliances, with a few limitations.

- Only active-passive mode is supported. The secondary unit in the HA cluster will stand by and handle no traffic until the primary fails.
- Configuration and firmware synchronization is not supported. Any changes made to the configuration of the primary unit must be manually duplicated on the secondary unit. Similarly, any firmware changes must be applied to both units.

- A maximum of four FortiGate-5005-DIST systems can be included in an HA cluster.

**Using the CLI to create an HA cluster**

1. Assemble the components of one of the cluster units. For details on how to assemble the FortiGate-5005-DIST system components, see the chapter "Installing hardware components" on page 29.
2. Connect the primary I/O module's management interface of the first cluster unit to a network accessible to your management computer.
3. If necessary, update this first cluster unit with the current I/O module and worker module firmware.
4. Configure the first cluster unit to operate as needed in your network. This includes operating mode, all routes, policies, profiles, etc.
5. Enable HA mode by entering the following CLI commands from the primary I/O module.

```
config system global
  set io-ha enable
end
```

6. Save the primary I/O configuration and keep a copy of the I/O module and worker module firmware installed on the first cluster unit.
7. Disconnect the first cluster module from the network.
8. Assemble the secondary unit to mirror the primary. Install the same module models in the same slots of the same chassis model.
9. Connect the primary I/O module's management interface of the second cluster unit to a network accessible to your management computer.
10. Update the I/O modules and worker modules to the same firmware versions as the primary cluster unit.
11. Take the first cluster unit's configuration backup file and restore it to this second cluster unit. When complete, you will have identically configured FortiGate-5005-DIST systems.
12. Log into the second cluster unit and change the management IP address to another IP address accessible from the management computer. The remaining second cluster unit interface IP addresses will mirror those of the first cluster unit.

    Since the cluster configuration is not automatically synchonized across all cluster members, you must manually make any configuration changes to each cluster member. With each system having a uniquely addressed management interface, you can log into each cluster member individually.
13. Reconnect the first cluster unit to the management computer network.
14. Connect the D15 interfaces of each primary I/O module directly together. This link will be used by the clustered units to exchange heartbeat information. The D16 interfaces can be connected to each other to form a redundant heartbeat link.
15. With a heartbeat connection established, the two cluster members will negotiate a relationship and determine which will act as the primary unit and which will act as the secondary unit.

16 Instead of directly connecting your networks to the I/O blade interfaces, connect the same port on the primary and secondary cluster units to a switch, then connect the network to the same switch. Each cross-connected interface requires its own switch, as shown in the example HA configuration in Figure 15 on page 50.

# IO module administration

This section describes how to administer the FortiGate-5005-DIST I/O module using both the web-based manager and the CLI.

The following topics are included in this section:



**Note:** Administering the FortiGate-5005-DIST worker module is very similar to administering any FortiGate-5005-DIST Security System unit. For information about the differences, see "Worker module administration" on page 67.

## Configuring the I/O module

To configure the I/O module, log in to the FortiGate-5005-DIST system web-based manager or CLI.

To return to the I/O module when configuring the worker module, from the worker module web-based manager, select **I/O Blade**. To return to the I/O module CLI from the worker module CLI, enter the command `exit`.

## Configuring worker modules

To configure worker modules from the web-based manager, log into the FortiGate-5005-DIST web-based manager and select **Worker Blade**. To return to the I/O module configuration, select **I/O Blade**.

To configure the worker modules from the CLI, log into the FortiGate-5005-DIST system web-based manager and enter `execute worker manage`.

# System Status

This section describes the System Status page, the dashboard of your FortiGate unit. At a glance you can view the current system status of the FortiGate unit including component serial numbers, uptime, FortiGuard™ license information, system resource usage, alert messages and network statistics.

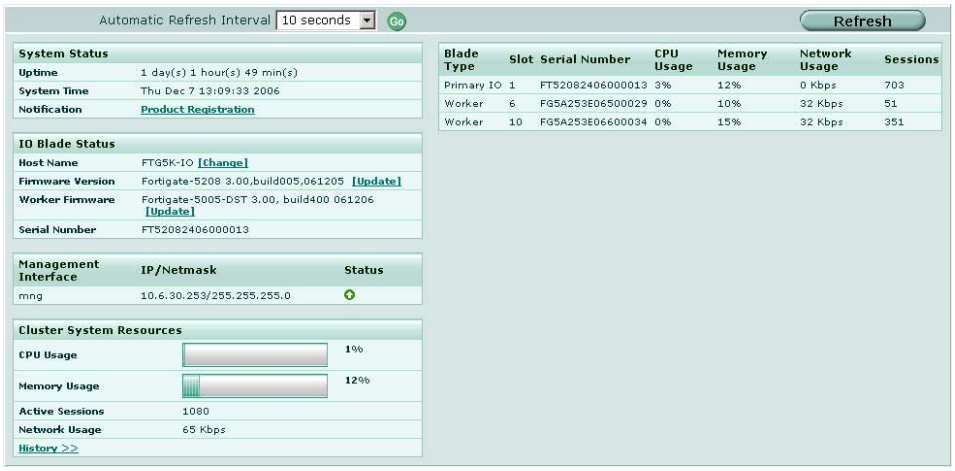
**Note:** Your browser must support Javascript to view the System Status page.

## Viewing I/O module system status

Go to **System > Status** to view the status of the I/O module. View the System Status page, also known as the system dashboard, for a snapshot of the current operating status of the I/O module. Administrators whose access profiles permit read access to system configuration can view system status information.

Administrators whose access profiles permit write access to system configuration can change or update I/O Blade Status information.

**Figure 16: I/O module system status**




## Automatic Refresh Interval

Select how often the Status page automatically updates from none to 30 seconds. Selecting none indicates the Status page will not be updated.

You can select the Refresh button to update the Status page immediately.

## System status

**Figure 17: Example FortiController-5208 System Status**

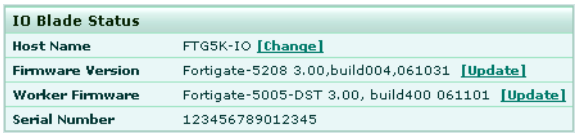
**Uptime** The time in days, hours, and minutes since the I/O module was last started.

**System Time** The current date and time according to the FortiGate unit internal clock.
Select Change to change the time or configure the FortiGate unit to get the time from an NTP server. See “Configuring system time” on page 67.

**Notification** Notification messages, such as a reminder to register the I/O module, appear here.

## I/O blade status

**Figure 18: Example FortiController-5208 I/O Blade Status**




**Host Name** The I/O module host name. Select Change to change the host name. See ““Changing the I/O module host name” on page 56”.

**Firmware Version** The version of the firmware installed on the I/O module.
Select Update to change the I/O module firmware.
See ““Changing the I/O module firmware” on page 57.

**Worker Firmware** The version of the worker firmware stored on the I/O module. This firmware version is automatically synchronized to all worker modules.
Select Update to change the worker module firmware.
See ““Changing the worker module firmware” on page 60.

**Serial Number** The serial number of the I/O module. The serial number identifies the I/O module and does not change with firmware upgrades.

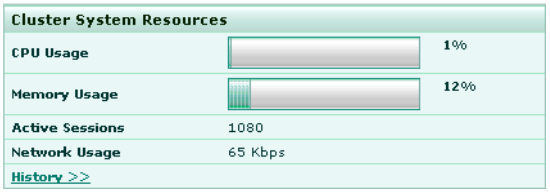
## Management interface

**Figure 19: Example FortiController-5208 Management Interface display**


**mng** The IP address, subnet mask, and status of the management interface.

## System resources

**Figure 20: Example FortiController-5208 System Resources display**



| | |
|---|---|
| **CPU Usage** | The current CPU usage as a percentage of maximum, displayed as a bar graph.<br>The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded. |
| **Memory Usage** | The current memory usage as a percentage of maximum, displayed as a bar graph.<br>The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded. |
| **Active Sessions** | The number of active communications sessions being processed by the I/O module. |
| **Network Utilization** | Network bandwidth being used by all sessions. |
| **History icon** | Select to view a graphical representation of the last minute of CPU, memory, sessions, and network usage. This page also shows the virus and intrusion detections over the last 20 hours. For more information see “Viewing operational history” on page 63. |

## Component inventory

**Figure 21: Example FortiGate-5005-DIST component inventory display**

| Blade Type | Slot | Serial Number | CPU Usage | Memory Usage | Network Usage | Sessions |
|---|---|---|---|---|---|---|
| Primary IO | 1 | FT52082406000013 | 3% | 13% | 0 Kbps | 698 |
| Worker | 6 | FG5A253E06500029 | 0% | 10% | 33 Kbps | 45 |
| Worker | 10 | FG5A253E06600034 | 0% | 15% | 33 Kbps | 343 |

| | |
|---|---|
| **Blade Type** | Every module installed in the chassis and correctly configured to operate as part of the FortiGate-5005-DIST system will be listed here, including any FortiController-5208 modules. |
| **Slot** | The slot number in which each module is installed. |
| **Serial Number** | The serial number of each module. |
| **CPU Usage** | The percentage of the CPU processing power currently in use for each module. |
| **Memory Usage** | The percentage of the total memory currently in use for each module. |
| **Network Usage** | The network bandwidth currently in use for each module, in kilobits per second. |
| **Sessions** | The number of open sessions each module is servicing. |

**Note:** The module information listed in the component inventory table is not continuously updated. The values are retrieved from the modules and displayed when the status page is updated. Setting an Automatic Refresh Interval of 10 seconds will have the module information values updated every 10 seconds, for example.

## Changing the I/O module host name

The I/O module host name appears on the Status page and in the I/O module CLI prompt.

The default host name is the I/O module serial number.

Administrators whose access profiles permit system configuration write access can change the I/O module host name.

**Note:** If the I/O module is part of a FortiGate-5005-DIST intern-chassis HA cluster, you should enter a unique hostname for the I/O module to identify this chassis.

**To change the I/O module host name using the web-based manager**

1 Go to **System > Status**.

2 In the Host Name field of the IO Blade Status section, select Change.

3 In the New Name field, type a new host name.

4 Select OK.

The new host name is displayed in the Host Name field, and in the CLI prompt.

**To change the I/O module host name using the CLI**

1 Enter the following in a terminal program logged into the I/O module:

```
config system global
  set hostname <hostname>
  end
```

2 The host name is changed and the I/O module prompt returns.

## Changing the I/O module firmware

Administrators whose access profiles permit maintenance read and write access can change the I/O module firmware.

Firmware changes either upgrade to a newer version or revert to an earlier version. Follow the appropriate procedure for the firmware change you want to perform:

- Upgrading to a new I/O module firmware version
- Reverting to a previous I/O module firmware version

### Upgrading to a new I/O module firmware version

Use the following procedure to upgrade the I/O module to a newer firmware version.

**To upgrade the I/O module firmware using the web-based manager**

1 Copy the firmware image file to your management computer.

2 Log into the I/O module web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.

3 Go to **System > Status**.

4 In the IO Blade Status section, select Update on the Firmware Version line.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

The I/O module uploads the firmware image file, upgrades to the new firmware version, closes all sessions, restarts, and displays the FortiGate login. This process takes a few minutes.

7 Log into the web-based manager.

8 Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade is successfully installed.

### To upgrade the I/O module firmware using the CLI

To use the following procedure, you must have a TFTP server the I/O module can connect to.

**Note:** To use this procedure, you must log in using the admin administrator account, or an admin account that has system configuration read and write privileges.

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the I/O module can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```
5. Enter the following command to copy the firmware image from the TFTP server to the I/O module:

   ```
   execute restore image io <name_str> <tftp_ip4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image io image.out 192.168.1.168
   ```

   The I/O module responds with the message:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type y.

   The I/O module uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
7. Reconnect to the CLI.
8. To confirm the firmware image is successfully installed, enter:

   ```
   get system status
   ```

## Reverting to a previous I/O module firmware version

Use the following procedure to revert your I/O module to a previous firmware version. This also reverts the I/O module to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages. Back up your I/O module configuration to preserve this information. For information, see “Backing up and restoring the configuration” on page 77.

### To revert to a previous I/O module firmware version using the web-based manager

1. Copy the firmware image file to the management computer.
2. Log into the I/O module web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.

3 Go to **System > Status**.

4 In the IO Blade Status section, select Update on the Firmware Version line.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

The I/O module uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

7 Log into the web-based manager.

8 Go to **System > Status** and check the Firmware Version to confirm that the firmware is successfully installed.

**To revert to a previous I/O module firmware version using the CLI**

1 Make sure the TFTP server is running

2 Copy the firmware image file to the root directory of the TFTP server.

3 Log into the I/O module CLI.

4 Make sure the I/O module can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 Enter the following command to copy the firmware image from the TFTP server to the I/O module:

```
execute restore image io <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `v3image.out` and the IP address of the TFTP server is 192168.1.68, enter:

```
execute restore image io v3image.out 192.168.1.168
```

The I/O module responds with this message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type y.

The I/O module uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7 Type y.

The I/O module reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

8 Reconnect to the CLI.

9 To confirm the new firmware image has been loaded, enter:

```
get system status
```

## Changing the worker module firmware

Administrators whose access profiles permit maintenance read and write access can change the worker module firmware.

To change worker firmware, the new firmware file must first be uploaded to the I/O module. Once completed, the workers will automatically detect the new firmware and download a copy from the I/O module and install it. The installation procedure ends with a reboot of all worker blades. This will interrupt network traffic.

Firmware can be changed to either a newer version, or to an older version. Follow the appropriate procedure for the firmware change you want to perform:

- Upgrading to a new I/O module firmware version
- Reverting to a previous I/O module firmware version

### Upgrading to a new worker module firmware version

Use the following procedure to upgrade the worker module firmware version.

**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware make sure that antivirus and attack definitions are up to date.

**To upgrade the worker module firmware using the web-based manager**

1. Copy the firmware image file to your management computer.
2. Log into the web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.
3. Go to **System > Status**.
4. In the IO Blade Status section, select Update on the Worker Firmware line.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.

   The I/O module uploads the firmware image file, the worker modules upgrade to the new firmware version, close all sessions, and restart.
7. After the worker modules reboot, log into the web-based manager.
8. Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade is successfully installed.

   Update antivirus and attack definitions.

**To upgrade the worker module firmware using the CLI**

To use the following procedure, you must have a TFTP server the I/O module can connect to.

**Note:** To use this procedure, you must log in using the admin administrator account, or an admin account that has system configuration read and write privileges.

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.

3 Log into the CLI.

4 Make sure the I/O module can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 Enter the following command to copy the firmware image from the TFTP server to the I/O module:

```
execute restore image worker <name_str> <tftp_ip4>
```

Where <name_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image worker image.out 192.168.1.168
```

The I/O module responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type y.

The I/O module uploads the firmware image file and upgrades the worker modules automatically. This process takes a few minutes.

7 To confirm the firmware image is successfully installed, enter:

```
execute worker manage
get system status
```

8 After confirming the workers are running the updated firmware, return to the I/O module CLI by entering:

```
execute primary-io
```

## Reverting to a previous worker module firmware version

Use the following procedure to revert your worker module to a previous firmware version. This also reverts the worker modules to their factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages. Back up your worker module configuration to preserve this information. For information, see “Backing up and restoring the configuration” on page 77.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware make sure that antivirus and attack definitions are up to date.

### To revert to a previous worker module firmware version using the web-based manager

1 Copy the firmware image file to the management computer.

2 Log into the web-based manager as the super admin, or an administrator account that has system configuration read and write privileges.

3 Go to **System > Status**.

4 In the IO Blade Status section, select Update on the Worker Firmware line.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

The I/O module uploads the firmware image file, the worker modules install the firmware from the I/O module, close all sessions, and restart.

7 Log into the web-based manager.

8 Go to **System > Status** and check the Firmware Version to confirm that the firmware is successfully installed.

9 Restore your configuration.

10 Update antivirus and attack definitions.

**To revert to a previous worker module firmware version using the CLI**

1 Make sure the TFTP server is running

2 Copy the firmware image file to the root directory of the TFTP server.

3 Log into the I/O module CLI.

4 Make sure the I/O module can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 Enter the following command to copy the firmware image from the TFTP server to the I/O module:

```
execute restore image worker <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `v3image.out` and the IP address of the TFTP server is 192168.1.68, enter:

```
execute restore image worker v3image.out 192.168.1.168
```

The I/O module responds with this message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type y.

The I/O module uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7 Type y.

The I/O module uploads the firmware image file, the worker modules install the firmware from the I/O module, close all sessions, and restart.

8 To confirm the firmware image is successfully installed, enter:

```
execute worker manage
get system status
```

9 To restore your previous configuration, if needed, use the command:

```
execute restore allconfig <name_str> <tftp_ip4>
```

10 Update antivirus and attack definitions.

For information, see the *FortiGate Administration Guide*, or from the CLI, enter:

```
execute update-now.
```

11 To return to the I/O module CLI, enter:

```
execute primary-io
```

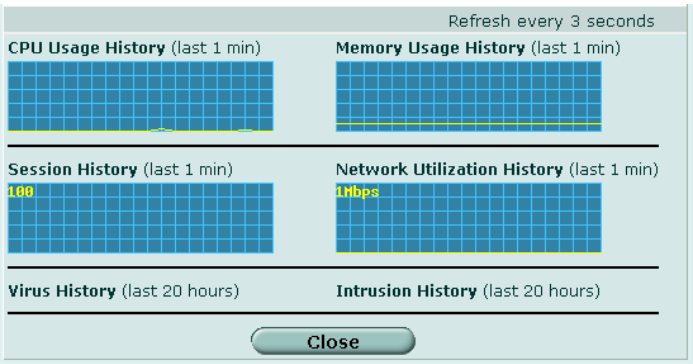
## Viewing operational history

The System Resource History page displays six graphs representing system resources and protection activity.

1 Go to **System > Status**.

2 Select History at the bottom of the System Resources section.

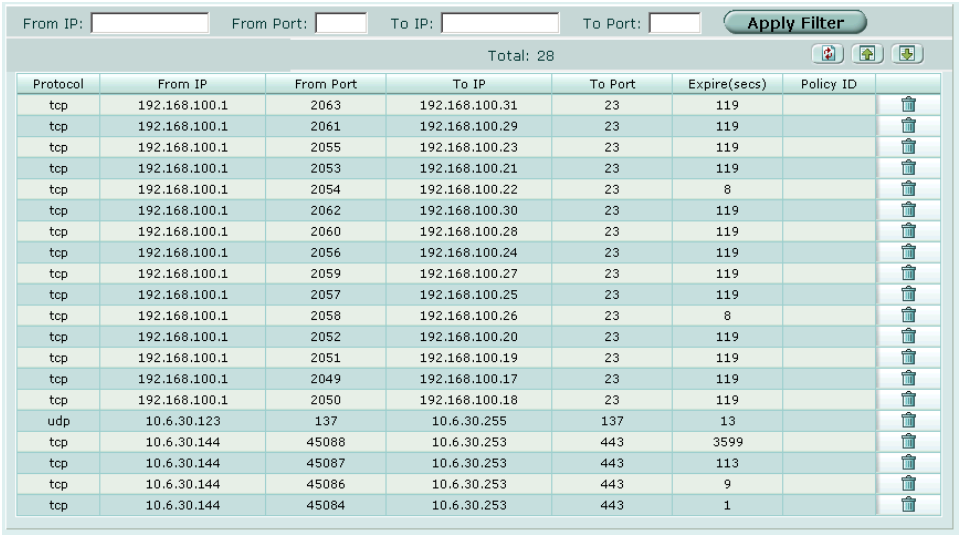
**Figure 22: Sample system resources history**




| | |
|---|---|
| **CPU Usage History** | CPU usage for the preceding interval. |
| **Memory Usage History** | Memory usage for the preceding interval. |
| **Session History** | Number of sessions over the preceding interval. |
| **Network Utilization History** | Network utilization for the preceding interval. |
| **Virus History** | Number of Viruses detected over the preceding interval. |
| **Intrusion History** | Number of intrusion attempts detected over the preceding interval. |

## Viewing session information

Go to **System > Status > Session** to view information about management sessions on the FortiGate module.




| Protocol | From IP | From Port | To IP | To Port | Expire(secs) | Policy ID | |
|---|---|---|---|---|---|---|---|
| tcp | 192.168.100.1 | 2063 | 192.168.100.31 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2061 | 192.168.100.29 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2055 | 192.168.100.23 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2053 | 192.168.100.21 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2054 | 192.168.100.22 | 23 | 8 | | |
| tcp | 192.168.100.1 | 2062 | 192.168.100.30 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2060 | 192.168.100.28 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2056 | 192.168.100.24 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2059 | 192.168.100.27 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2057 | 192.168.100.25 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2058 | 192.168.100.26 | 23 | 8 | | |
| tcp | 192.168.100.1 | 2052 | 192.168.100.20 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2051 | 192.168.100.19 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2049 | 192.168.100.17 | 23 | 119 | | |
| tcp | 192.168.100.1 | 2050 | 192.168.100.18 | 23 | 119 | | |
| udp | 10.6.30.123 | 137 | 10.6.30.255 | 137 | 13 | | |
| tcp | 10.6.30.144 | 45088 | 10.6.30.253 | 443 | 3599 | | |
| tcp | 10.6.30.144 | 45087 | 10.6.30.253 | 443 | 113 | | |
| tcp | 10.6.30.144 | 45086 | 10.6.30.253 | 443 | 9 | | |
| tcp | 10.6.30.144 | 45084 | 10.6.30.253 | 443 | 1 | | |

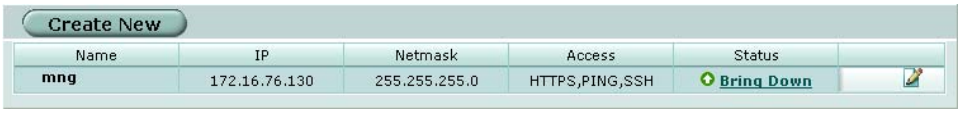
| | |
|---|---|
| **From IP:**<br>**From Port:**<br>**To IP:**<br>**To Port:** | Optionally, enter criteria for session source and destination and select the Apply Filter button to display only the sessions that match. |
| **Apply Filter** | Filter session display according to criteria in From IP, From Port, To IP and To Port. |
| **Filtered Results** | This is available only if filtering is in effect, showing the number of sessions that meet the filter criteria. |
| **Total** | The total number of management sessions. |
| **Refresh** | Update the session list. |
| **Page up** | View previous page in the session list. |
| **Page down** | View the next page in the session list. |
| **Protocol** | The service protocol of the connection, for example, udp, tcp, or icmp. |
| **From IP** | The source IP address of the connection. |
| **From Port** | The source port of the connection. |
| **To IP** | The destination IP address of the connection. |
| **To Port** | The destination port of the connection. |
| **Expiry (sec)** | The time, in seconds, before the connection expires. |
| **Policy ID** | The number of the firewall policy allowing this session or blank if the session involves only one FortiGate interface. |
| **Delete icon** | Stop an active communication session. Your access profile must include read and write access to System Configuration. |

# System Network

This section describes how to configure your FortiController-5208 unit to operate in your management network. Basic network settings include configuring the management interfaces and FortiController-5208 DNS settings. More advanced configuration includes adding VLAN subinterfaces.

## Viewing the configuration of the I/O module management interface

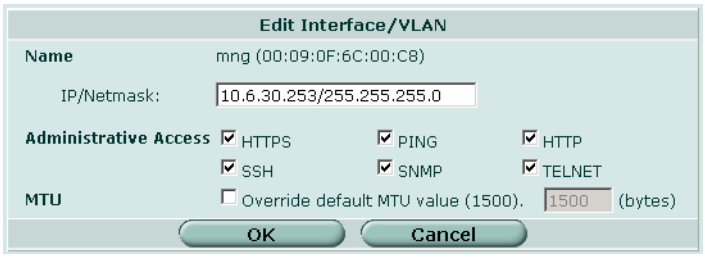
You initially configured the management interface using the CLI so that you could connect to the web-based manager. Go to **System > Network > Management Interface** to modify this configuration.




| | |
|---|---|
| **Name** | The names of the management interface on your FortiGate unit and VLANs on the management interface. |
| **IP** | The current IP address of the management interface. |
| **Netmask** | The current netmask of the management interface. |
| **Access** | The administrative access configuration for the interface. HTTPS access is required to connect to the web-based manager. SSH access is required for access to the CLI. |
| **Status** | The administrative status for the interface.<br>If the administrative status is a green arrow, the interface is up and can accept network traffic. If the administrative status is a red arrow, the interface is administratively down and cannot accept traffic. To change the administrative status, select Bring Down or Bring Up. |
| **Delete, edit, and view icons** | Delete, edit, or view an entry. |

## Changing the configuration of the I/O module management interface

Go to **System > Network > Interface**. Configure the management interface or select Create New to create a VLAN interface. To edit an existing interface, select the Edit icon for that interface.



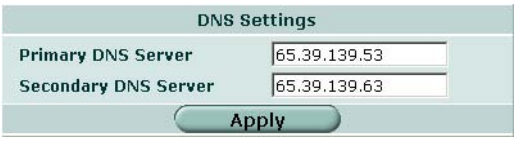

| | |
|---|---|
| **Name** | Enter a name for the interface. You cannot change the name of an existing interface. |
| **Interface** | Select the name of the physical interface on which to create the VLAN. Once created, the VLAN subinterface is listed below its physical interface in the Interface list.<br>You cannot change the interface of an existing VLAN subinterface.<br>This field is only displayed when Type is set to VLAN. |

| | |
|---|---|
| **VLAN ID** | Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. You cannot change the VLAN ID of an existing VLAN subinterface.<br>The VLAN ID can be any number between 1 and 4096 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface.<br>This field is only displayed for a VLAN interface. |
| **IP/Netmask** | Enter the IP address/subnet mask in the IP/Netmask field. The IP address must be on the same subnet as the network to which the interface connects.<br>Two interfaces cannot have IP addresses on the same subnet.<br>This field is only available when Manual addressing mode is selected. |
| **Administrative Access** | Select the types of administrative access permitted on this interface. |
| **HTTPS** | Allow secure HTTPS connections to the web-based manager through this interface. |
| **PING** | Interface responds to pings. Use this setting to verify your installation and for testing. |
| **HTTP** | Allow HTTP connections to the web-based manager through this interface. HTTP connections are not secure and can be intercepted by a third party. |
| **SSH** | Allow SSH connections to the CLI through this interface. |
| **SNMP** | Allow a remote SNMP manager to request SNMP information by connecting to this interface. See “Configuring SNMP” on page 68. |
| **TELNET** | Allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party. |
| **MTU** | To change the MTU, select Override default MTU value and enter the MTU size based on the addressing mode of the interface<br>• 68 to 1 500 bytes for static mode<br>• 576 to 1 500 bytes for DHCP mode<br>• 576 to 1 492 bytes for PPPoE mode<br>• up to 16 110 bytes for jumbo frames (FortiGate models numbered 3000 and higher)<br>This field is available only on physical interfaces. VLANs inherit the parent interface MTU size. |

# Configuring management DNS settings

Several FortiGate unit I/O module functions use DNS. You can specify the IP addresses of the DNS servers to which the I/O module connects. DNS server IP addresses are usually supplied by your ISP.

Go to **System > Network > DNS** to configure DNS settings.




Enter the primary DNS server IP address and optionally a secondary DNS server IP address in the fields provided.

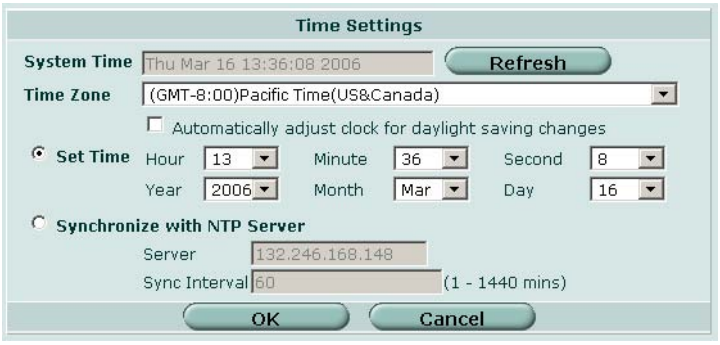
# System Config

This section describes the configuration of several non-network features, such as system time and SNMP.

## Configuring system time

1. Go to **System > Config > Time**.
2. Select the time zone and then either set the date and time manually or configure synchronization with an NTP server.

**Figure 23: Time Settings**




| | |
|---|---|
| **System Time** | The current FortiGate system date and time. |
| **Refresh** | Update the display of the current FortiGate system date and time. |
| **Time Zone** | Select the current FortiGate system time zone. |
| **Automatically adjust clock for daylight saving changes** | Select to automatically adjust the FortiGate system clock when your time zone changes between daylight saving time and standard time. |
| **Set Time** | Select to set the FortiGate system date and time to the values you set in the Hour, Minute, Second, Year, Month, and Day fields. |
| **Synchronize with NTP Server** | Select to use an NTP server to automatically set the system date and time. You must specify the server and synchronization interval. |
| **Server** | Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org. |
| **Sync Interval** | Specify how often the FortiGate unit should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the FortiGate unit to synchronize its time once a day. |

## Configuring administration language and timeout

Go to **System > Config > Options** to set the idle timeout for administrators and the language used in the web-based manager. Change the settings as needed and then select Apply.

**Timeout Settings**

| | |
|---|---|
| **Idle Timeout** | The administrator is automatically logged out when the Idle Timeout period expires. The default setting is 5 minutes. You can set the timeout to any value from 1 to 480 minutes. |

**Web Administration**

| | |
|---|---|
| **Language** | Select the language of the web-based manager. This release supports only English. |

# SNMP

Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, or FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager is a computer running an application that can read the incoming traps from the agent and track the information. Using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access.

**Note:** Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiGate unit, or be able to query it.

The FortiGate SNMP implementation is read-only. SNMP v1 and v2c compliant SNMP managers have read-only access to FortiGate system information and can receive FortiGate traps. To monitor FortiGate system information and receive FortiGate traps you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager.

RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II) (for more information, see "Fortinet MIBs" on page 71.

## Configuring SNMP

Go to **System > Config > SNMP v1/v2c** to configure the SNMP agent.

**Figure 24: Configuring SNMP**


| | |
|---|---|
| **SNMP Agent** | Enable the FortiGate SNMP agent. |
| **Description** | Enter descriptive information about the FortiGate unit. The description can be up to 35 characters long. |
| **Location** | Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long. |
| **Contact** | Enter the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters. |
| **Apply** | Save changes made to the description, location, and contact information. |
| **Create New** | Select Create New to add a new SNMP community.<br>See "Configuring an SNMP community" on page 69. |
| **Communities** | The list of SNMP communities added to the FortiGate configuration. You can add up to 3 communities. |
| **Name** | The name of the SNMP community. |
| **Queries** | The status of SNMP queries for each SNMP community. The query status can be enabled or disabled. |

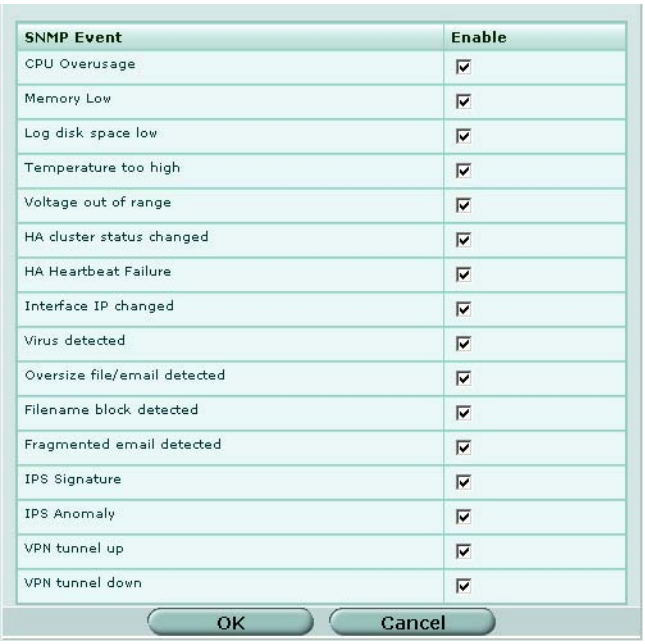
| | |
|---|---|
| **Traps** | The status of SNMP traps for each SNMP community. The trap status can be enabled or disabled. |
| **Enable** | Select Enable to activate an SNMP community. |
| **Delete icon** | Select Delete to remove an SNMP community. |
| **Edit/View icon** | Select to view or modify an SNMP community. |

## Configuring an SNMP community

An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities so that SNMP managers can connect to the FortiGate unit to view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

**Figure 25: SNMP community options (part 1)**

**Figure 26: SNMP community options (part 2)**




**Community Name** Enter a name to identify the SNMP community.

**Hosts** Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.

- **IP Address** The IP address of an SNMP manager than can use the settings in this SNMP community to monitor the FortiGate unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
- **Interface** Optionally select the name of the interface that this SNMP manager uses to connect to the FortiGate unit. You only have to select the interface if the SNMP manager is not on the same subnet as the FortiGate unit. This can occur if the SNMP manager is on the Internet or behind a router.
- **Delete** Select a Delete icon to remove an SNMP manager.
- **Add** Add a blank line to the Hosts list. You can add up to 8 SNMP managers to a single community.

**Queries** Enter the Port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the Enable check box to activate queries for each SNMP version.

**Traps** Enter the Local and Remote port numbers (port 162 for each by default) that the FortiGate unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Select the Enable check box to activate traps for each SNMP version.

**SNMP Event** Enable each SNMP event for which the FortiGate unit should send traps to the SNMP managers in this community.

"Temperature too high" and "Voltage out of range" event traps are available only on FortiGate 5001.

**To configure an interface for SNMP access**

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

1 Go to **System > Network > Interface**.
2 Choose an interface that an SNMP manager connects to and select Edit.
3 In Administrative Access, select SNMP.
4 Select OK.

**To configure SNMP access in Transparent mode**

1 Go to **System > Config > Operation Mode**.
2 Enter the IP address that you want to use for management access and the netmask in the Management IP/Netmask field.
3 Select Apply.

## Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

The FortiGate MIB is listed in Table 13 along with the two RFC MIBs. You can obtain these MIB files from Fortinet technical support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager.

Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

**Table 13: Fortinet MIBs**

| MIB file name or RFC | Description |
|---|---|
| **fortinet.3.00.mib** | The proprietary Fortinet MIB includes detailed FortiGate system configuration information and trap information. Your SNMP manager requires this information to monitor FortiGate configuration settings and receive traps from the FortiGate SNMP agent. See “FortiGate traps” on page 72 and “Fortinet MIB fields” on page 74. |
| **RFC-1213 (MIB II)** | The FortiGate SNMP agent supports MIB II groups with the following exceptions.<br>• No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).<br>• Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB. |
| **RFC-2665 (Ethernet-like MIB)** | The FortiGate SNMP agent supports Ethernet-like MIB information with the following exception. |
| | No support for the dot3Tests and dot3Errors groups. |

## FortiGate traps

The FortiGate agent can send traps to SNMP managers that you have added to SNMP communities. To receive traps, you must load and compile the Fortinet 3.0 MIB into the SNMP manager.

All traps include the trap message as well as the FortiGate unit serial number and hostname.

**Table 14: Generic FortiGate traps**

| Trap message | Description |
|---|---|
| ColdStart<br>WarmStart<br>LinkUp<br>LinkDown | Standard traps as described in RFC 1215. |

**Table 15: FortiGate system traps**

| Trap message | Description |
|---|---|
| CPU usage high (fnTrapCpuHigh) | CPU usage exceeds 90%. This threshold can be set in the CLI using `config system global`. |
| Memory low (fnTrapMemLow) | Memory usage exceeds 90%. This threshold can be set in the CLI using `config system global`. |
| Interface IP change (fnTrapIfChange) | Change of IP address on a FortiGate interface. The trap message includes the name of the interface, the new IP address and the serial number of the FortiGate unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE. |
| Temperature too high (fnTrapTempHigh) | Hardware sensor detects high temperature.<br>This is available only for FortiGate 5001. |
| Voltage out of range (fnTrapVoltageOutOfRange) | Hardware sensor detects abnormal power levels.<br>This is available only for FortiGate 5001. |
| (fnFMTrapIfChange) | No message. Interface changes IP. Only sent to monitoring FortiManager. |
| (fnFMTrapConfChange) | Any configuration changes made to FortiGate unit, excluding any changes made by a connected FortiManager unit. |

**Table 16: FortiGate VPN traps**

| Trap message | Description |
|---|---|
| VPN tunnel is up (fnTrapVpnTunUp) | An IPSec VPN tunnel started. |
| VPN tunnel down (fnTrapVpnTunDown) | An IPSec VPN tunnel shuts down. |

**Table 17: FortiGate IPS traps**

| Trap message | Description |
|---|---|
| IPS Anomaly fnTrapIpsAnomaly | IPS anomaly detected. |
| IPS Signature fnTrapIpsSignature) | IPS signature detected. |

**Table 18: FortiGate antivirus traps**

| Trap message | Description |
|---|---|
| Virus detected (fnTrapAvEvent) | The FortiGate unit detects a virus and removes the infected file from an HTTP or FTP download or from an email message. |
| Oversize file/email detected (fnTrapAvOversize) | The FortiGate unit antivirus scanner detects an oversized file. |
| Filename block detected (fnTrapAvPattern) | The FortiGate unit antivirus scanner blocks a file matching a pattern. |
| Fragmented email detected (fnTrapAvFragmented) | The FortiGate unit antivirus scanner detects a fragmented file or attachment. |

**Table 19: FortiGate logging traps**

| Trap message | Description |
|---|---|
| Log full (fnTrapLogFull) | On a FortiGate unit with a hard drive, hard drive usage exceeds 90%. On a FortiGate unit without a hard drive, log to memory usage exceeds 90%.<br>This threshold can be set in the CLI using config `system global`. |

**Table 20: FortiGate HA traps**

| Trap message | Description |
|---|---|
| HA switch (fnTrapHaSwitch) | The primary unit in an HA cluster fails and is replaced with a new primary unit. |
| HA Heartbeat Failure (fnTrapHaHBFail) | HA monitored interface fails heartbeat. |

**Table 21: FortiBridge traps**

| Trap message | Description |
|---|---|
| FortiBridge detects fail (fnTrapBridge) | A FortiBridge unit detects a FortiGate unit failure. |

## Fortinet MIB fields

The Fortinet MIB contains fields reporting current FortiGate unit status information. The tables below list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the fortinet.3.00.mib file into your SNMP manager and browsing the Fortinet MIB fields.

**Table 22: System MIB fields**

| MIB field | Description |
|---|---|
| **fnSysModel** | FortiGate model number, for example, 400 for the FortiGate-400. |
| **fnSysSerial** | FortiGate unit serial number. |
| **fnSysVersion** | The firmware version currently running on the FortiGate unit. |
| **fnSysVersionAv** | The antivirus definition version installed on the FortiGate unit. |
| **fnSysVersionNids** | The attack definition version installed on the FortiGate unit. |
| **fnSysHaMode** | The current High-Availability (HA) mode (standalone, A-A, A-P) |
| **fnSysOpMode** | The FortiGate unit operation mode (NAT or Transparent). |
| **fnSysCpuUsage** | The current CPU usage (as a percent). |
| **fnSysMemUsage** | The current memory utilization (in MB). |
| **fnSysDiskCapacity** | The hard disk capacity (MB) |
| **fnSysDiskUsage** | The current hard disk usage (MB) |
| **fnSysSesCount** | The current IP session count. |

**Table 23: HA MIB fields**

| MIB field | Description | |
|---|---|---|
| **fnHaSchedule** | Load balancing schedule for A-A mode. | |
| **fnHaStatsTable** | Statistics for the individual FortiGate unit in the HA cluster. | |
| | **fnHaStatsIndex** | The index number of the unit in the cluster. |
| | **fnHaStatsSerial** | The FortiGate unit serial number. |
| | **fnHaStatsCpuUsage** | The current FortiGate unit CPU usage (%). |
| | **fnHaStatsMemUsage** | The current unit memory usage (MB). |
| | **fnHaStatsNetUsage** | The current unit network utilization (Kbps). |
| | **fnHaStatsSesCount** | The number of active sessions. |
| | **fnHaStatsPktCount** | The number of packets processed. |
| | **fnHaStatsByteCount** | The number of bytes processed by the FortiGate unit |
| | **fnHaStatsIdsCount** | The number of attacks that the IPS detected in the last 20 hours. |
| | **fnHaStatsAvCount** | The number of viruses that the antivirus system detected in the last 20 hours. |

**Table 24: Administrator accounts**

| MIB field | Description | |
|---|---|---|
| **fnAdminNumber** | The number of administrators on the FortiGate unit. | |
| **fnAdminTable** | Table of administrators. | |
| | **fnAdminIndex** | Administrator account index number. |
| | **fnAdminName** | The user name of the administrator account. |
| | **fnAdminAddr** | An address of a trusted host or subnet from which this administrator account can be used. |
| | **fnAdminMask** | The netmask for fnAdminAddr. |

**Table 25: Local users**

| MIB field | Description | |
|---|---|---|
| **fnUserNumber** | The number of local user accounts on the FortiGate unit. | |
| **fnUserTable** | Table of local users. | |
| | **fnUserIndex** | Local user account index number. |
| | **fnUserName** | The user name of the local user account. |
| | **fnUserAuth** | The authentication type for the local user:<br>**local** - a password stored on the FortiGate unit<br>**radius-single** - a password stored on a RADIUS server<br>**radius-multiple** - any user who can authenticate on the RADIUS server can log on<br>**ldap** - a password stored on an LDAP server |
| | **fnUserState** | Whether the local user is enabled or disabled. |

**Table 26: Options**

| MIB field | Description |
|---|---|
| **fnOptIdleTimeout** | The idle period in minutes after which the administrator must re-authenticate. |
| **fnOptAuthTimeout** | The idle period in minutes after which a user must re-authenticate with the firewall. |
| **fnOptLanguage** | The web-based manager language. |
| **fnOptLcdProtection** | Whether an LCD PIN has been set. |

**Table 27: Logging**

| MIB field | Description |
|---|---|
| **fnLogOption** | Logging preferences. |

**Table 28: Custom messages**

| MIB field | Description |
|---|---|
| **fnMessages** | The number of custom messages on the FortiGate unit. |

**Table 29: Virtual domains**

| MIB field | Description | |
|---|---|---|
| **fnVdNumber** | The number of virtual domains on the FortiGate unit. | |
| **fnVdTable** | Table of virtual domains. | |
| | **fnVdIndex** | Internal virtual domain index number on the FortiGate unit. |
| | **fnVdName** | The name of the virtual domain. |

**Table 30: Active IP sessions**

| MIB field | Description |
|---|---|
| **fnIpSessIndex** | The index number of the active IP session. |
| **fnIpSessProto** | The IP protocol (TCP, UDP, ICMP, etc.) of the session. |
| **fnIpSessFromAddr** | The source IP address of the active IP session. |
| **fnIpSessFromPort** | The source port of the active IP session. |
| **fnIpSessToPort** | The destination IP address of the active IP session. |
| **fnIpSessToAddr** | The destination port of the active IP session. |
| **fnIpSessExp** | The expiry time or time-to-live in seconds for the session. |

**Table 31: Dialup VPNs**

| MIB field | Description |
|---|---|
| **fnVpnDialupIndex** | The index of the dialup VPN peer. |
| **fnVpnDialupGateway** | The remote gateway IP address. |
| **fnVpnDialupLifetime** | VPN tunnel lifetime in seconds. |
| **fnVpnDialupTimeout** | Time remaining until the next key exchange (seconds). |
| **fnVpnDialupSrcBegin** | Remote subnet address. |
| **fnVpnDialupSrcEnd** | Remote subnet mask. |
| **fnVpnDialupDstAddr** | Local subnet address. |

**Table 32: VPN Tunnels**

| MIB field | Description |
|---|---|
| **fnVpnTunEntIndex** | The unique index of the VPN tunnel. |
| **fnVpnTunEntPhase1Name** | The descriptive name of the Phase1 configuration. |
| **fnVpnTunEntPhase2Name** | The descriptive name of the Phase2 configuration. |
| **fnVpnTunEntRemGwyIp** | The IP of the remote gateway. |
| **fnVpnTunEntRemGwyPort** | The port of the remote gateway. |
| **fnVpnTunEntLocGwyIp** | The IP of the local gateway. |
| **fnVpnTunEntLocGwyPort** | The port of the local gateway. |
| **fnVpnTunEntSelectorSrcBeginIp** | Beginning of the address range of a source selector. |
| **fnVpnTunEntSelectorSrcEndIp** | Ending of the address range of a source selector. |
| **fnVpnTunEntSelectorSrcPort** | Source selector port |
| **fnVpnTunEntSelectorDstBeginIp** | Beginning of the address range of a destination selector |
| **fnVpnTunEntSelectorDstEndIp** | Ending of the address range of a destination selector. |
| **fnVpnTunEntSelectorDstPort** | Destination selector port. |
| **fnVpnTunEntSelectorProto** | Protocol number for the selector. |
| **fnVpnTunEntSelectorLifeSecs** | Lifetime of the tunnel in seconds. |
| **fnVpnTunEntSelectorLifeBytes** | Lifetime of the tunnel in bytes. |
| **fnVpnTunEntTimeout** | Timeout of the tunnel in seconds. |
| **fnVpnTunEntInOctets** | Number of bytes received on the tunnel. |
| **fnVpnTunEntOutOctets** | Number of bytes sent out on the tunnel. |
| **fnVpnTunEntStatus** | Current status of the tunnel - either up or down. |

# System Maintenance

This section describes how to back up and restore your system configuration.

## Backing up and restoring the configuration

Go to **System > Maintenance > Backup & Restore** to backup or restore the FortiGate system configuration using files on the management computer. In this release, you can back up the entire system configuration as a password protected file. This backup will include the configuration of the I/O module, the worker firmware image stored on the I/O module, and the worker configuration stored on the I/O module.

**Note:** The I/O module checks the workers for configuration changes every 20 seconds. If a change is detected, a copy of the updated configuration is saved to the I/O module. If a change is made to the worker module configuration and a configuration backup started within this 20 second window, the backup will not include the worker changes.

**To back up the system configuration using the web-based manager**

1 Go to **System > Maintenance > Backup & Restore**.
2 Select the Backup icon.
3 Optionally enter a password for the backup file
4 Select OK.
5 Save the file on the management computer.

**To back up the system configuration using the CLI**

To use the following procedure, you must have a TFTP server the I/O module can connect to.

**Note:** To use this procedure, you must log in using the admin administrator account, or an admin account that has system configuration read and write privileges.

1 Make sure the TFTP server is running
2 Log into the I/O module CLI.
3 Make sure the I/O module can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

4 Enter the following command to copy the configuration backup file from the I/O module to the TFTP server:

```
execute backup allconfig <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the backup file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the backup configuration file name is `backup.out` and the IP address of the TFTP server is 192168.1.68, enter:

```
execute backup allconfig backup.out 192.168.1.168
```

The I/O module responds with this message:

**`<output to be added>`**

5 The I/O module sends the backup image file to the TFTP server. After the file is delivered, a message similar to the following is displayed:

**`<output to be added>`**

**To restore the system configuration using the web-based manager**

1 Go to **System > Maintenance > Backup & Restore**.
2 Select the Restore icon.
3 If you entered a password when creating the backup file, enter it.
4 In the Upload File field, select Browse, navigate to the backup file, and then select OK.

The FortiGate system restarts after it reads the configuration file.

**To restore the system configuration using the CLI**

To use the following procedure, you must have a TFTP server the I/O module can connect to.

**Note:** To use this procedure, you must log in using the admin administrator account, or an admin account that has system configuration read and write privileges.

1. Make sure the TFTP server is running
2. Log into the I/O module CLI.
3. Make sure the I/O module can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```
4. Enter the following command to copy the backup file from the I/O module to the TFTP server:

   ```
   execute restore allconfig <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the backup file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the configuration backup file name is `backup.out` and the IP address of the TFTP server is 192168.1.68, enter:

   ```
   execute restore allconfig backup.out 192.168.1.168
   ```

   The I/O module responds with this message:

   **`<output to be added>`**
5. The I/O module retrieves the backup configuration file from the TFTP server. After the file is retrieved, the I/O module reverts to the saved configuration, and reboots. This process takes a few minutes.

### Shutdown and other maintenance operations

Go to **System > Maintenance > Shutdown** to do any of the following:

- Log out from the web-based manager
- Shot down the FortiGate system.
- Reboot the FortiGate system.
- Restore all settings on the FortiGate system to factory defaults.

Select the desired operation from the list and select Apply.

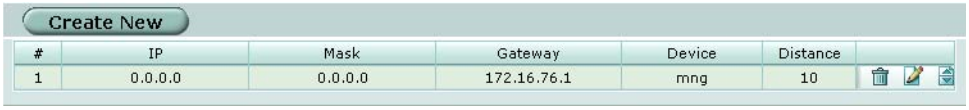
## Router Static

This section describes how to configure routing for management access through the management interface of the primary I/O module.

### Configuring administrative static routing

The Static Route list shows the routes configured on the management interface (mng) or VLAN subinterfaces created on the management interface.

**Note:** The routing shown here is for management only. Routing for traffic on the FortiGate-5000-DIST system is configured on the worker modules.

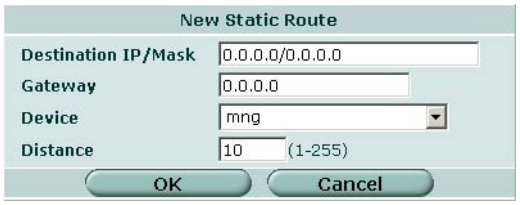



| | |
|---|---|
| **Create New** | Add a static route to the Static Route list. See "Adding an administrative static route" on page 80. |
| **#** | The row IDs of entries in the Static Route list. |
| **IP** | The destination IP addresses of packets that the FortiGate unit intercepts. |
| **Mask** | The network masks associated with the IP addresses. |
| **Gateway** | The IP addresses of the next-hop routers to which intercepted packets are forwarded. |
| **Device** | The I/O modules management interface (mng) and VLANs created on the management interface. |
| **Distance** | The administrative distances associated with each route. The values represent distances to next-hop routers. |
| **Delete, Edit, and Move To icons** | Delete or edit an entry, or move an entry to a new position on the list. |

## Adding an administrative static route

Go to **Router > Static > Static Route** and select Create New to add a static route on the I/O module for management use.

**Note:** The routing shown here is for management only. Routing for traffic on the FortiGate system is configured on the worker modules.




| | |
|---|---|
| **Destination IP/Mask** | Type the destination IP address and network mask of packets that the FortiGate unit has to intercept. The value `0.0.0.0/0.0.0.0` is reserved for the default route. |
| **Gateway** | Type the IP address of the next-hop router to which the FortiGate unit will forward intercepted packets. |
| **Device** | Select the name of the FortiGate interface through which the intercepted packets may be routed to the next-hop router. |
| **Distance** | Type an administrative distance for the route. The distance value is arbitrary and should reflect the distance to the next-hop router. A lower value indicates a more preferred route. The value can be an integer from 1 to 255. |

### Moving an administrative static route

Go to **Router > Static > Static Route** and select the Move To icon for the static route you want to move.

**Note:** The routing shown here is for management only. Routing for traffic on the FortiGate system is configured on the worker modules.


**Current Order** The current list position of the route to be moved.

**Move To** Select the location in the list to which the static route will be moved.

## Router Monitor

Go to **Router > Monitor > Routing Monitor** to view the status of routes on the I/O module.

**Note:** The routes monitored here are for the I/O module only. Routes for traffic on the FortiGate system are monitored on the worker modules.

**Type** The type of route (Static or Connected).

**Network** The IP addresses and network masks of destination networks that the FortiGate unit can reach.

**Distance** The administrative distance associated with the route. A lower value indicates a preferable route. To modify the administrative distance, see “Adding an administrative static route” on page 80.

**Gateway** The IP addresses of gateways to the destination networks.

**Interface** The interface through which packets are forwarded to the gateway of the destination network. For the I/O module, the available interfaces are mng, VLANs created on mng, and swdev.

# Hardware procedures

This section describes procedures that you may be required to perform from time to time with your FortiGate-5005-DIST system.

The following topics are included in this section:



## Starting a configured FortiGate-5005-DIST system

There are no special requirements for starting a configured FortiGate-5005-DIST system that has been shut down and powered off. As long as the chassis has power, as the modules start up they automatically find each other and form the FortiGate-5005-DIST system. It may take a few minutes for all components to start up and establish communications with the primary I/O blade. During this startup time the FortiGate-5005-DIST system cannot process traffic.

**To start a configured FortiGate-5005-DIST system**

1. Connect and turn on power to the chassis.
2. Fully insert all modules into the correct chassis slots.
3. Wait a few minutes for the FortiGate-5005-DIST system to start up and begin processing traffic.
4. Review the LEDs on your FortiGate-5005-DIST system components to make sure that all components are operating correctly.

   The following documents describe normal operating status LEDs for FortiGate-5005-DIST components.

   - *FortiGate-5140 Chassis Guide*
   - *FortiGate-5050 Chassis Guide*
   - *FortiController-5208 System Guide*
   - *FortiGate-5005FA2 Security System Guide*

## Installing FortiGate-5005-DIST firmware

In a functioning FortiGate-5005-DIST system, you install FortiController-5208 firmware on the primary I/O module. The primary I/O module synchronizes this same firmware version to the secondary FortiController-5208 module if one is present. This synchronization happens even if the secondary I/O module is running a newer firmware version than the primary I/O module.

You also install FortiGate-5005FA2 DIST firmware on the primary I/O module. The primary I/O module synchronizes this firmware to all FortiGate-5005FA2 modules. This happens even if the FortiGate-5005FA2 modules are running newer firmware versions. Also, if different FortiGate-5005FA2 modules are running different firmware versions, the system synchronizes them all to run the worker firmware version installed on the primary I/O module.

FortiController-5208 modules are shipped with FortiController-5208 and FortiGate-5005FA2 firmware installed. So, as you are installing your FortiGate-5005-DIST hardware, the system synchronizes all firmware to the versions installed on the primary I/O module.

If the FortiGate-5005FA2 firmware is missing from the primary I/O module, the FortiGate-5005FA2 modules will keep running their current firmware versions until you install FortiGate-5005FA2 worker module firmware on the primary I/O module.

You can view the current FortiController-5208 and FortiGate-5005FA2 firmware versions installed on the primary I/O module from the primary I/O module CLI or web-based manager.

**To view the current firmware versions from the web-based manager**

1 From the I/O module web-based manager go to **System > Status**.

2 On the IO Blade status list view the I/O blade firmware version and the worker firmware version.

**To view the current firmware versions from the CLI**

1 To view the FortiController-5208 firmware version enter the command:

```
get system status
```

2 To view the FortiGate-5005FA2 firmware version enter the following command to connect to the worker CLI:

```
execute worker manage
```

3 Then to view the FortiGate-5005FA2 DIST firmware version enter the following command:

```
get system status
```

**To install new I/O module or worker module firmware**

For FortiGate-5005-DIST firmware upgrade procedures, see “Changing the I/O module firmware” on page 57 and “Changing the worker module firmware” on page 60.

# Adding and removing modules from a FortiGate-5005-DIST system

The FortiGate-5005FA2 and FortiController-5208 modules in a functioning FortiGate-5005-DIST security system are interdependent and constantly exchanging information with each other. Because of this interdependence, adding new or removing currently operating modules may cause a service disruption. This section describes recommended procedures for adding and removing modules from a functioning FortiGate-5005-DIST system.

Performing any of the procedures in this section will temporarily disrupt FortiGate-5005-DIST traffic processing. To minimize the effect of these disruptions, you should perform these procedures during off peak hours.

## Adding FortiGate-5005FA2 modules

You can add additional FortiGate-5005FA2 modules to a functioning FortiGate-5005-DIST system if any slots numbered 2 and above in your chassis are empty. When you add a FortiGate-5005FA2, some of the current active communications may be lost. This happens because when you add a new Fortigate-5005FA2 module, the primary I/O module redistributes all active sessions among all FortiGate-5005FA2 modules (including the new one). When this happens, the new FortiGate-50005FA2 module may get sessions that were being processed by other FortiGate-5005FA2 modules. The new FortiGate-5005FA2 module will drop these in-process sessions.

**To add a FortiGate-5005FA2 module to an operating FortiGate-5005-DIST system**

1. Remove the cover from any empty chassis slot numbered 2 or higher.
2. Insert the FortiGate-5005FA2 module into the slot.

   See the *FortiController-5005FA2 System Guide* for complete details.
3. If required, install FortiGate-5005-DIST firmware.

   See “Installing DIST firmware on a FortiGate-5005FA2 module” on page 37.

   The FortiGate-5005FA2 module starts up in DIST mode and connects with the primary I/O module to download and install the worker configuration file. The FortiGate-5005FA2 module then joins the DIST system and compares its firmware version with the version installed on the I/O module.
   - If the versions are the same, the FortiGate-5005FA2 module is ready to process traffic assigned by the I/O module
   - If the versions are different, the worker module firmware is downloaded from the I/O module and installed. The worker reboots to complete the firmware installation.

   The I/O modules then add the new worker module to the load distribution configuration and begins distributing traffic to the new worker module.

## Removing FortiGate-5005FA2 modules

To remove a FortiGate-5005FA2 module you must use the CLI to shut down the FortiGate-5005FA2 module to be removed. The FortiGate-5005FA2 module should then be removed from its chassis slot as quickly as possible. While the FortiGate-5005FA2 module is shut down and still installed in the chassis slot the I/O modules will continue to send traffic to it because I/O modules cannot detect that a FortiGate-5005FA2 module has stopped functioning until it is removed from its chassis slot.

**To remove a FortiGate-5005FA2 module from a functioning FortiGate-5005-DIST system**

1 Shut down the FortiGate-5005FA2 module to be removed.

From the CLI enter the command `execute worker manage <slot_number>`. Where `<slot_number>` is the number of the chassis slot containing the FortiGate-5005FA2 module to be removed. Enter the command `execute shutdown` to shut down the FortiGate-5005FA2.

2 The FortiGate-5005FA2 module may be safely removed from the chassis when the shutdown procedure is completed. In the CLI, the FortiGate-5005FA2 will indicate the shutdown is complete with this message:

```
The system is halted.
```

Once removed, the I/O modules redistribute traffic to the remaining FortiGate-5005FA2 modules.

## Adding and removing FortiController-5208 modules

Adding and removing FortiController-5208 modules always disrupts the operation of the FortiGate-5005-DIST system. Because of this disruption you should only add or remove FortiController-5208 modules while the FortiGate-5005-DIST system is not processing traffic.

**To replace the primary I/O module**

Replacing a primary I/O module involves backing up the primary I/O module configuration, removing the primary I/O module and installing a new one and then restoring the configuration to the new primary I/O module

1 Log into the primary I/O module CLI and enter the following command.

```
execute worker shutdown
```

The master worker will update the primary I/O with a copy of the current worker configuration and all worker modules will shut down.

2 If the DIST system has two I/O modules, shut down the secondary I/O module by entering the following CLI commands.

```
execute secondary-io manage
    execute shutdown
```

The secondary I/O module will shut down and the CLI session will close. Log in to the primary I/O module again to continue.

3 Save the I/O configuration by logging into the DIST system GUI and going to **System > Maintenance > Backup & Restore**.

4 Select the Backup icon, optionally enter a password, and select OK.

5 Save the file to your local computer.

6 Shut down the primary I/O module by entering the following CLI command.

```
execute shutdown
```

The primary I/O module will shut down and the CLI session will close.

7 Remove the primary I/O module.

See the *FortiController-5208 System Guide* for complete information about how to remove the FortiController-5208 module from a chassis slot.

8 Insert the replacement primary I/O module into chassis slot 1.

See the *FortiController-5208 System Guide* for complete information about how to insert the FortiController-5208 module into a chassis slot.

9 Cycle power to the chassis. All the installed modules will reboot.

10 Log into the primary I/O module and go to **System > Maintenance > Backup & Restore** and select the restore icon.

**Note:** If the I/O has not been used before, the accounts, passwords, and interface IP addresses will be set to the factory defaults. See the *FortiController-5208 System Guide* for complete information.

11 Select the configuration backup file and enter the password if one was specified.

12 Select OK. The configuration file will be installed.

13 Once the configuration is restored, the DIST modules will reboot.

14 The FortiGate-5005-DIST system will be able to process traffic after a few minutes.

### To add a secondary I/O module to a functioning FortiGate-5005-DIST system

If a FortiGate-5005-DIST system only contains a primary I/O module, adding a secondary I/O module causes all worker modules to reboot because this operation adds network interfaces port2_X1, port2_X2, port2_1, port2_2, port2_3 and port2_4 to the FortiGate-5005-DIST system configuration.

1 Insert the second FortiController-5208 module in slot 2.

See the *FortiController-5208 System Guide* for complete information about how to insert the FortiController-5208 module into a chassis slot.

2 Make sure the new FortiController-5208 module is running the same firmware build as the primary I/O module.

Upgrade the firmware installed on the new FortiController-5208 module if required.

3 Enter the following command from the primary I/O module CLI (the FortiController-5208 module slot 1).

```
config system global
    set io-num double
end
```

The FortiController-5208 module in slot 2 becomes the secondary I/O module. All worker modules reboot to add the secondary I/O module interfaces to their configuration. The FortiGate-5005-DIST system will be able to process traffic after a few minutes.

### To remove the secondary I/O module from a functioning FortiGate-5005-DIST system

Removing the a secondary I/O module causes all worker modules to reboot because this operation removes network interfaces to the FortiGate-5005-DIST system configuration. Because removing the secondary I/O module removes interfaces from the configuration, it is recommended that you delete all configuration elements for port2_X1, port2_X2, port2_1, port2_2, port2_3 and port2_4 interfaces from the worker module configuration before removing the secondary I/O module. You should remove, routes, firewall policies, firewall addresses, and other configuration elements for these interfaces.

1 Shut down the secondary FortiController-5208 module to be removed.

Use the CLI command `execute secondary-io` to connect to the secondary I/O module. Enter the command `execute shutdown` to shut down the secondary I/O module.

2 Remove the FortiController-5208 module from chassis slot 2.

3 Configure the primary I/O module to operate without a secondary I/O module. Enter the CLI command:

```
config system global
    set io-num single
end
```

The worker modules reboot and after a few minutes the FortiGate-5005-DIST system can start processing traffic.

### To replace a secondary I/O module

Replacing the secondary I/O module involves shutting down the worker modules, optionally backing up the primary I/O module configuration, and shutting down the secondary I/O module. The secondary I/O module can then be removed and replaced.

1 Log into the primary I/O module CLI and enter the following command.

```
execute worker shutdown
```

The master worker will update the primary I/O module with a copy of the current worker configuration. All worker modules will then shut down.

2 Optionally, save the I/O configuration by logging into the DIST system GUI and going to **System > Maintenance > Backup & Restore**.

3 Shut down the secondary I/O module by entering the following CLI commands.

```
execute secondary-io manage
    execute shutdown
```

The secondary I/O module will shut down and the CLI session will return to the primary I/O module.

4 Shut down the primary I/O module by entering the following CLI command.

```
execute shutdown
```

The primary I/O module will shut down and the CLI session will close.

5 Remove the secondary I/O module.

See the *FortiController-5208 System Guide* for complete information about how to remove the FortiController-5208 module from a chassis slot.

6 Insert the replacement secondary I/O module into chassis slot 2.

See the *FortiController-5208 System Guide* for complete information about how to insert the FortiController-5208 module into a chassis slot.

7 Cycle power to the chassis. All the installed modules will reboot.

8 The FortiGate-5005-DIST system will be able to process traffic after a few minutes.

# Upgrading FortiController-5208 NPU firmware

Under normal circumstances you will never have to upgrade the FortiController-5208 NPU firmware. However, in exceptional circumstances when recommended by Fortinet Customer Support, you can use the following information to upgrade the firmware operating on FortiController-5208 module. You must perform this procedure separately for each FortiController-5208 module installed in your FortiGate-5005-DIST system.

**Caution:** The following procedure is for advanced users only. You should contact Fortinet Customer Support before upgrading FortiController-5208 NPU firmware. A failed burn can render the FortiController-5208 unusable and may require returning the module to Fortinet for repair.

**Note:** The NPU firmware is entirely separate from the FortiController-5208 firmware and is not effected by burning I/O module or worker module firmware, or by formatting the FortiController-5208 boot device, or anything else done from FortiOS or the BIOS.

**To upgrade FortiController-5208 NPU firmware**

Before you start the FortiController-5208 must be operating as a primary FortiController-5208. You must also have a TFTP server that the FortiController-5208 module can connect to from the FortiController-5208 Management interface.

1 Copy the NPU firmware image to the TFTP server

2 Connect to the FortiController-5208 CLI

3 Enter the following command:

```
diag npu flash <npu_image_name> <tftp_server_IP> port1
```

The FortiController-5208 requests a password.

4 Enter `qwerty` and press Enter.

The FortiController-5208 copies the firmware image from the TFTP server and installs the image on the FortiController-5208 NPU.

5 Once the firmware has been installed you must restart the FortiController-5208.

If the 5208 does not restart properly, or the NPU behaves strangely the firmware may not have burned properly. Contact Fortinet Customer Support for assistance in restoring the NPU firmware.

# Index

www.fortinet.com