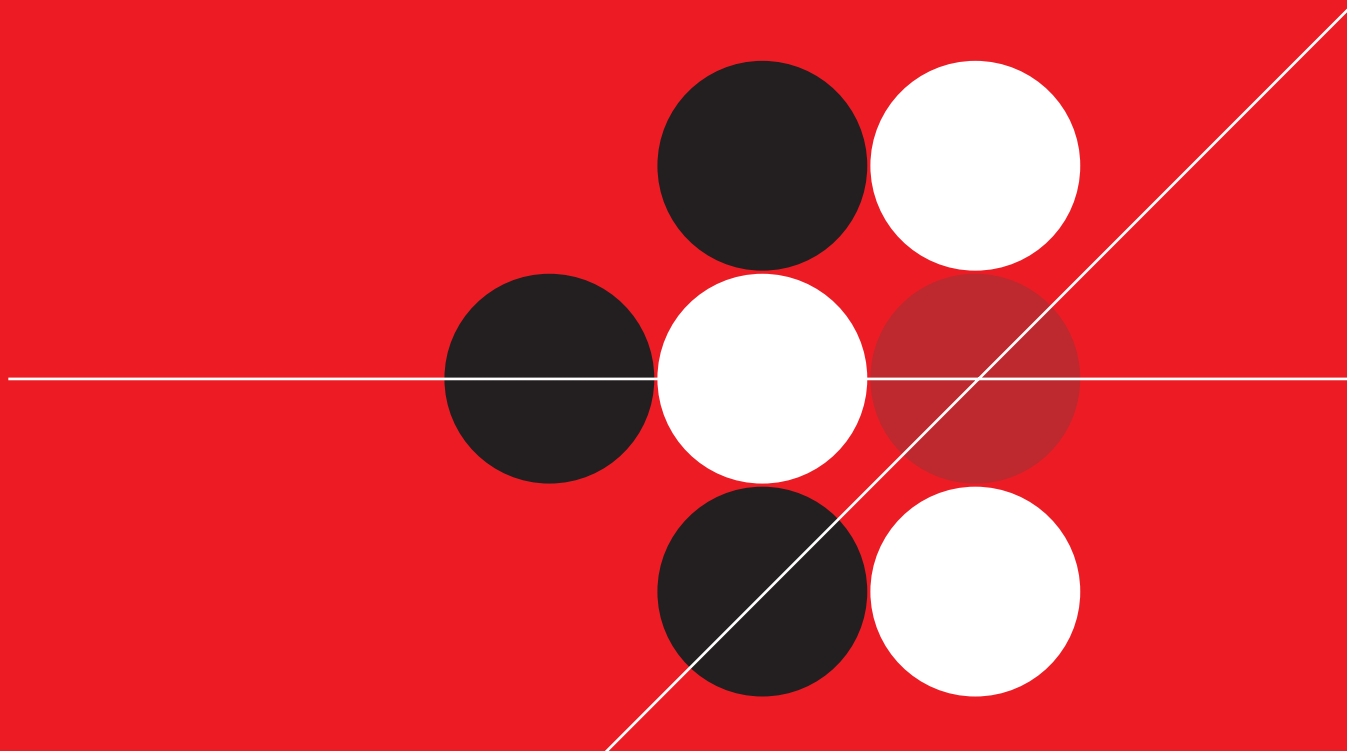
TREND MICRO™

Network VirusWall™ Enforcer 2500

Getting Started Guide



Document Part No. NVEM1267/60313

Release Date: July 2006

The user documentation for Trend Micro Network VirusWall Enforcer 2500 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site: http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Network VirusWall Enforcer 2500 Documentation vi
About This Getting Started Guide vii
Audience viii
Document Conventions viii

Chapter 1: Getting Started

Package Contents 1-2
Network VirusWall Enforcer 2500 Front Panel 1-4
LED Indicators 1-5
Port Indicators 1-6
Network VirusWall Enforcer 2500 Back Panel 1-7
Dimensions and Weight 1-8
Power Requirements and Environmental Specifications 1-8
Choosing a Fiber Media Connector for Fiber-based Networks 1-9
Mounting Network VirusWall Enforcer 2500 1-10
Recommended Tools 1-10
Rack Kit 1-11
Four-Post Rack Mounting 1-14
Preparing the Device 1-15
Assembling the Slide Sets 1-17
Installing the Slide Sets 1-21
Mounting the Device in the Rack 1-24
Installing a Fiber-Optic Card 1-26

Opening the Device 1-27
Installing the Card 1-30
Removing or Replacing a Fiber-Optic Card 1-34

Chapter 2: Introducing Trend Micro™ Network VirusWall™ Enforcer 2500

Network VirusWall Enforcer 2500 2-2
Introducing Network VirusWall Enforcer 2500-specific Terms 2-3
Trend Micro Network VirusWall Enforcer 2500 Web Console 2-5
Understanding Network VirusWall Enforcer Ports 2-6
Deployment Overview 2-6

Chapter 3: Deploying Network VirusWall™ Enforcer 2500

Planning for Deployment 3-2
Deployment Overview 3-2
Phase 1: Plan the Deployment 3-3
Phase 2: Perform Preconfiguration 3-3
Phase 3: Manage Network VirusWall Enforcer 2500 Devices ... 3-3
Deployment Notes 3-4
Identifying What to Protect 3-5
Remote Access Endpoints 3-5
Guest Endpoints 3-9
Key Network Segments/Important Network Assets 3-10
Dual-switch VLAN Environment 3-11
Single-switch VLAN Environment 3-14
Planning for Network Traffic 3-15
Determining the Number of Devices to Deploy 3-15
Conducting a Pilot Deployment 3-16
Choosing a Pilot Site 3-16
Creating a Contingency Plan 3-16
Deploying and Evaluating your Pilot 3-16
Redefining Your Deployment Strategy 3-17
Deploying Network VirusWall Enforcer 2500 3-17
A Basic Deployment Scenario 3-18
Multi-Protection Zone Configuration Without Failover 3-19
Failopen Considerations 3-20
User-defined Port Grouping with Failover Deployment 3-21

Failover Considerations 3-25
Deployment Scenario I: Single Pair Configuration with or without 802.1q VLAN (Only Dual Port Multi-mode Fiber) 3-26
User-defined Port Redundancy Deployment 3-28
User-defined Port Redundancy Considerations 3-30
Deployment Scenario II: Point-to-Point Links with Dual-Port Multi-mode Fiber-optic Server Adapter 3-31
Port Redundancy with Failover Deployment 3-33

Chapter 4: Preparing for Preconfiguration

Preparing for Preconfiguration 4-2
Network VirusWall Enforcer 2500 Initial Tasks 4-2
Verifying Network Support 4-3

Chapter 5: Preconfiguring Network VirusWall Enforcer 2500

Understanding Preconfiguration 5-2
Choosing the Preconfiguration Method 5-3
Using the Preconfiguration Console 5-3
Using the LCD Module 5-3
Performing Preconfiguration Using the Preconfiguration Console ... 5-5
Preparing the Preconfiguration Console 5-6
Logging on the Preconfiguration Console 5-7
Configuring Device Settings 5-11
Setting the Interface Speed and Duplex Mode 5-14
Logging off the Preconfiguration Console 5-15
Performing Preconfiguration Using the LCD Module 5-16
Connecting to the Network 5-18
Configuring Network VirusWall Enforcer 2500 5-19

Chapter 6: Troubleshooting Preconfiguration

Device Issues 6-2
Contacting Technical Support 6-3

Appendix A: Ethernet Cable Usage Guidelines

Network VirusWall Enforcer 2500 in Normal Mode A-2
Network VirusWall Enforcer 2500 in Failopen Mode with Standard Copper Ports 1 to 5 ..... A-4
Network VirusWall Enforcer 2500 in Failopen Mode with Bypass Card Copper Ports A-6

Index

Preface

Welcome to the Trend Micro™ Network VirusWall™ Enforcer 2500 Getting Started Guide. This book contains basic information about the tasks you need to perform to deploy the device. It is intended for novice and advanced users of Network VirusWall who want to plan, deploy, and preconfigure Network VirusWall Enforcer 2500.

This preface discusses the following topics:

- *Network VirusWall Enforcer 2500 Documentation* on page vi
- *About This Getting Started Guide* on page vii
- *Audience* on page viii
- *Document Conventions* on page viii

Network VirusWall Enforcer 2500 Documentation

The Network VirusWall Enforcer 2500 documentation consists of the following:

- Online Help—Web-based documentation that is accessible from the device Web console

  The Online Help contains explanations about device components and features.

- Upgrade Guide (UG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 2500 or downloadable from the Trend Micro Web site.

  The UG contains explanations about upgrading from Network VirusWall 2500 1.5 and 1.8 to Network VirusWall Enforcer 2500.

- Getting Started Guide (GSG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 2500 or downloadable from the Trend Micro Web site

  This GSG contains instructions on deploying the device, a task that includes planning, testing, and preconfiguration. See *About This Getting Started Guide* for chapters available in this book.

  If you are planning a large-scale deployment or have a complex network architecture and need more details about product architecture, refer to the *Network VirusWall Enforcer 2500 Administrator's Guide*.

- Administrator's Guide (AG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 2500 or downloadable from the Trend Micro Web site

  The AG contains explanation of device architecture and instructions on how to configure and administer the device using the applicable management tools. Topics include Frequently Asked Questions (FAQs), Troubleshooting, and Glossary chapters.

Tip: Trend Micro recommends checking the corresponding link from the Update Center (`http://www.trendmicro.com/download`) for updates to the device documentation and program file.

About This Getting Started Guide

The *Network VirusWall Enforcer 2500 Getting Started Guide* discusses the following topics:

- *Introducing Trend Micro™ Network VirusWall™ Enforcer 2500*—an overview of the device and its components
- *Getting Started*—details of the actual device and its specifications, including instructions for mounting and powering on the device
- *Deploying Network VirusWall™ Enforcer 2500*—recommendations to help you plan for the deployment of one or more devices
- *Preconfiguring Network VirusWall Enforcer 2500*—step-by-step instructions on how to install Trend Micro Control Manager and the necessary patches, including considerations and procedures on how to perform preconfiguration
- *Troubleshooting Preconfiguration*—troubleshooting tips for issues encountered during preconfiguration

Audience

The Network VirusWall Enforcer 2500 documentation assumes a basic knowledge of security systems, including:

- Antivirus and content security protection
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Network devices and their administration
- Network configuration (such as the use of VLAN, SNMP)

Document Conventions

To help you locate and interpret information easily, the documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided
FAILOVER	The Network VirusWall Enforcer 2500 interface connected to the device in a failover pair

TABLE 1. Conventions used in the documentation

Chapter 1

Getting Started

This chapter guides you through setting up and powering on a Network VirusWall™ Enforcer device.

This chapter contains the following topics:

- *Package Contents* on page 1-2
- *Choosing a Fiber Media Connector for Fiber-based Networks* on page 1-9
- *Mounting Network VirusWall Enforcer 2500* on page 1-10

After completing the procedures in this chapter, proceed by:

- *Conducting a Pilot Deployment* on page 3-16
- *Deploying Network VirusWall Enforcer 2500* on page 3-17
- *Redefining Your Deployment Strategy* on page 3-17
- *Performing Preconfiguration Using the Preconfiguration Console* on page 5-5

Package Contents

Figure 1-1 illustrates the package contents.

FIGURE 1-1. The package contents

Tip: Refer to *Table 1-1* and *Table 1-10* to check whether the package is complete. If any of the items are missing, please contact Trend Micro support (*See Contacting Technical Support* on page 6-3*)*.

Table 1-1 specifies each item:

QUANTITY	ITEM	DESCRIPTION
1 unit	Network VirusWall Enforcer 2500	The device.
1 piece	Power cord	Supplies power to the device (length is 79 in/200 cm).
1 piece	Ethernet cable (RJ-45 crossover cable)	Connects two (2) devices in a failover pair or connect a device to a computer used during Rescue Mode (length is 39 in/100 cm).
1 piece	Console cable (RS-232)	Connects the device to the computer used during preconfiguration (length is 79 in/200 cm).
1 set	Rack kit	Mounts a Network VirusWall Enforcer 2500 to a standard 19 in rack cabinet.
2 pieces	PCI-X slot covers	Covers the front panel slot for fiber, copper, and accessory cards. The original cover is already attached to the front panel when the device ships. Use the extra cover when a fiber-optic server adapter or Copper LAN adapter is installed on the riser card.
1 CD	Trend Micro Solutions CD for Network VirusWall Enforcer 2500	Contains patches, hot fix installers, tools, and documentation. The PDF documentation includes: • *Trend Micro Network VirusWall Enforcer 2500 Upgrade Guide* • *Trend Micro Network VirusWall Enforcer 2500 Getting Started Guide* • *Trend Micro Network VirusWall Enforcer 2500 Administrator's Guide* The Network VirusWall Enforcer 2500 tools include: • Appliance Firmware Flash Utility **Note:** Refer to *Troubleshooting* in the *Administrator's Guide* for instructions on how to use these tools.
2 books 1 sheet	*Trend Micro Network VirusWall Enforcer 2500 Upgrade Guide* *Trend Micro Network VirusWall Enforcer 2500 Getting Started Guide* Trend Micro Network VirusWall Enforcer 2500 Safety Sheet	Printed *Trend Micro Network VirusWall Enforcer 2500 Upgrade Guide, Trend Micro Network VirusWall Enforcer 2500 Getting Started Guide,* and Safety Sheet.

TABLE 1-1. Network VirusWall Enforcer 2500 package contents

Network VirusWall Enforcer 2500 Front Panel

The front panel of Network VirusWall Enforcer 2500 contains a Liquid Crystal Display (LCD), panel, ports, and LEDs.

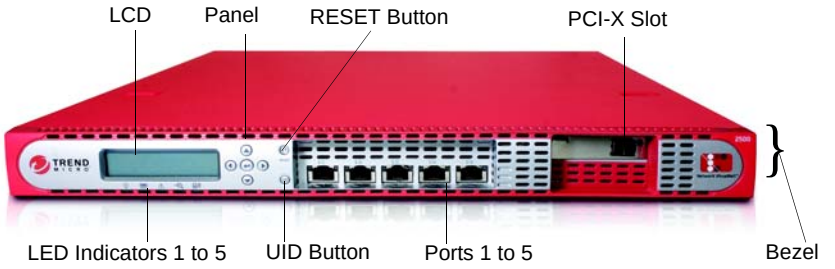


FIGURE 1-2. Network VirusWall Enforcer 2500 front panel

The following table describes each front panel element:

ELEMENT	DESCRIPTION
Liquid Crystal Display (LCD)	A 2.6 in x 0.6 in (65 mm x 16 mm) dot display LCD that is capable of displaying messages in 2 rows of 16 characters each.
Panel	5-button control panel that provides LCD navigation.
RESET Button	Resets the device.
LED Indicators 1 to 5	Indicates the **POWER**, **UID**, **SYSTEM**, **POLICY**, and **OUTBREAK** states. **POWER** and **UID** have one color each; **SYSTEM**, **POLICY**, and **OUTBREAK** have three colors each. See *page 1-5* for details.
Ports 1, 2, 3, 4, 5	Copper Gigabit LAN port that you designate as the MANAGEMENT, **MIRROR**, SNIFFER, REGULAR, or FAILOVER port. The Network VirusWall Enforcer 2500 documentation refers to each port by its number (for example, port 1 or 2).
UID Button	Unique ID button that illuminates the LED, which helps you locate a device for troubleshooting or maintenance.
PCI-X Slot	Slot for fiber, copper Ethernet, and accessory cards. See *page 1-9* for details on how to choose a fiber media converter (FMC).
Bezel	Detachable casing that covers and protects the front panel.

TABLE 1-2. Front panel description

Note: The LCD and Control Panel elements are collectively referred to as the LCD module (or LCM console).

LED Indicators

Network VirusWall Enforcer 2500 has five **l**ight-**e**mitting **d**iodes (LEDs) that indicate the **POWER**, **UID**, **SYSTEM**, **POLICY**, and **OUTBREAK** status.

FIGURE 1-3. POWER, UID, SYSTEM, POLICY, and OUTBREAK LED indicators

The following table shows the possible behavior for each LED element:

LED	STATE	DESCRIPTION
POWER	Yellow– steady	Device is operating normally.
	Off (no color)	Device is off.
UID	Blue– steady	The UID LED is illuminated because UID button is pressed.
	Blue– flashing	The Web console is sending the 'light on' command to turn on the UID LED.
	Off (no color)	The UID LED is not illuminated.
SYSTEM	Red– flashing	Device is booting.
	Red– steady	Power-On Self-Test (POST) error.
	Yellow– flashing	Network VirusWall Enforcer 2500 program file (firmware) is starting.
	Yellow– steady	Network VirusWall Enforcer 2500 program file (firmware) encountered a critical error.
	Green– steady	Network VirusWall Enforcer 2500 program file (firmware) is ready.
POLICY	Green– flashing	Network Scan, or Policy Enforcement is enabled
	Yellow– steady	Failover mode is enabled. (Non Management)
	Off (no color)	No multiple policy scan.
OUTBREAK	Green– steady	Outbreak Prevention Services (OPS) is disabled when Control Manager manages Network VirusWall Enforcer 2500.
	Red– flashing	OPS is enabled.

TABLE 1-3. Network VirusWall Enforcer 2500 LED indicators

Port Indicators

Network VirusWall Enforcer 2500 has five user-configurable copper-based Ethernet ports. Each Ethernet port has an indicator that allows you to determine the port's current state. *Figure 1-4* illustrates the indicators of a port.

FIGURE 1-4. Port indicators 1 and 2

Table 1-4 lists the description for each port component.

INDICATOR NUMBER	NAME	STATE	DESCRIPTION
1	10 Mbps / 100 Mbps /1Gbps LINK Status LED	Green– steady	10 Mbps LED
			100 Mbps LED
			1Gbps LED
2	ACT / BYPASS Status LED	Orange– steady	LAN Bypass LED
		Orange– flashing	Activity LED

TABLE 1-4. Port indicator description

Table 1-5 shows the possible states for each Network VirusWall Enforcer 2500 port based on the speed and duplex mode settings.

PORT	STATE	DESCRIPTION
BYPASS 	Indicators 1 and 2– orange, steady	Failopen (LAN bypass) enabled. **Note:** Network VirusWall Enforcer 2500 reserves ports 1 and 2 for failopen.
LINK 	Indicator 1– green, steady	Port speed is 10 Mbps, 100 Mbps, or 1 Gbps.
	Indicator 2– orange, flashing	Network packet transmission/receiving active.

TABLE 1-5. Network VirusWall Enforcer 2500 port indicators

Network VirusWall Enforcer 2500 Back Panel

The back panel of Network VirusWall Enforcer 2500 contains a power receptacle, power switch, unused USB ports, serial connection, and fan vent.

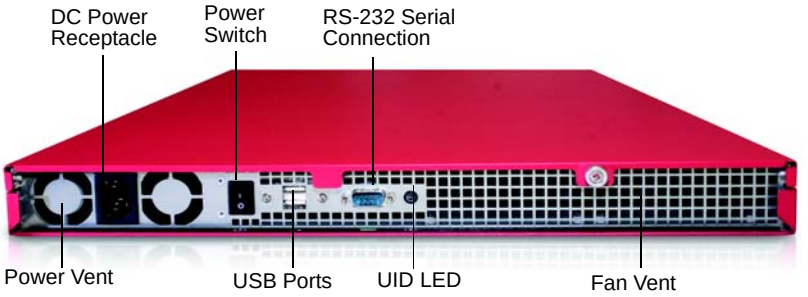


FIGURE 1-5. Network VirusWall Enforcer 2500 back panel

The following table describes each back panel element:

ELEMENT	DESCRIPTION
DC Power Receptacle	Connects to the power outlet and the device using the power cord (included in the package, see *Package Contents* on page 1-2).
Power Switch	Powers the device on and off.
RS-232 Serial Connection	Connects to a computer's serial port with an RS-232 type connection to perform preconfiguration.
Fan Vent	Cooling vent for 5 system fans.
Power Vent	Cooling vent for the power receptacle.
UID LED	LED at the back panel of a Network VirusWall Enforcer 2500 device. When a user presses the UID button, the UID LED illuminates. The illuminated UID LED allows you to easily locate the device for troubleshooting or maintenance.
USB Ports	USB ports, reserved for future releases.

TABLE 1-6. Back panel description

Dimensions and Weight

The following specifications apply to Network VirusWall Enforcer 2500:

ELEMENT	MEASUREMENT
Chassis dimension with bezel (D x W x H)	24.43 x 16.73 x 1.70 in (62.05 x 42.49 x 4.32 cm)
Carton dimension (D x W x H)	33.54 x 22.24 x 8.27 in (85.19 x 56.49 x 21.01 cm)
System weight	9 Kg (19.8 lbs)
System weight with package and accessory box	16.54 Kg (36.5 lbs)

TABLE 1-7. Network VirusWall Enforcer 2500 dimensions and weights

Power Requirements and Environmental Specifications

The following settings apply to Network VirusWall Enforcer 2500:

ELEMENT	SPECIFICATION
AC input voltage	90 to 264 VAC
AC input current (90 VAC)	8.0 A
AC input current (180 VAC)	4.0 A
Frequency	47 to 63 Hz (50/60 nominal)
NORMAL OPERATING AMBIENT TEMPERATURE (AT SEA LEVEL)	
Minimum (operating and idle)	41 °F (5 °C)
Maximum (operating, power supply on)	113 °F (45 °C)
Maximum (idle, AC power supply on, main power supply off)	104 °F (40 °C)
Maximum rate of change	50 °F per hour (10 °C per hour)
STORAGE TEMPERATURE (AT SEA LEVEL)	
Minimum	-40 °F (-40 °C)
Maximum	158 °F (70 °C)
Maximum rate of change	68 °F per hour (20 °C per hour)
HUMIDITY	
Maximum (operating)	80% non-condensing
Maximum (non-operating)	95% non-condensing

TABLE 1-8. Network VirusWall Enforcer 2500 power requirements and environmental specifications

Choosing a Fiber Media Connector for Fiber-based Networks

Network VirusWall Enforcer 2500 supports fiber-optic connectors. A fiber media converter is not necessary if your network environment is using fiber connectivity.

There are many types of fiber-optic connectors. The majority of GBIC network switches are SC type; only a few are LC type. However, since fiber-optic server adapters are LC type, you must be careful to choose the correct patch cord (optical fiber wiring) to ensure connectivity. If your network switch is SC type, you will need an SC-to-LC fiber adapter to be the bridge.

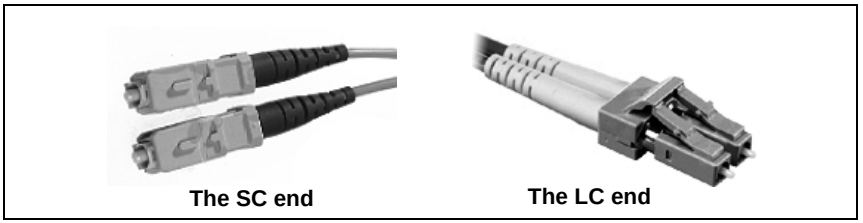


FIGURE 1-6. The two ends of an SC-LC fiber media patch cord

See *Table 1-9*, "Fiber media patch cords and connectors," for information on the connector type for single or multi-mode fiber-optic cable type.

PATCH CORD	SWITCH	MODE
Multi-mode duplex LC-LC connectors with fiber	GBIC, LC	Multi-mode, LC
Multi-mode duplex SC-LC connectors with fiber	GBIC, SC	Multi-mode, LC
Single-mode duplex SC-LC connectors with fiber	GBIC, SC	Single-mode, LC

TABLE 1-9. Fiber media patch cords and connectors

Mounting Network VirusWall Enforcer 2500

Mount a Network VirusWall Enforcer 2500 device:

- In a standard 19-inch four-post rack cabinet

  The device requires 1 rack unit (RU) of vertical space in the rack.

  Tip: If you are mounting more than one Network VirusWall Enforcer 2500 device, position and mount both devices in the same physical location (for example, "Server Room 101 on the 15th floor"). Doing so allows you to easily maintain the devices.

- On any stable surface as a freestanding device

  For freestanding installation, guarantee that the device has at least 2in (5.08 cm) of clearance on each side to allow for adequate airflow and cooling.

WARNING! *Ensure that the fan vent is not blocked.*

Recommended Tools

Trend Micro recommends using the following tools to mount the device:

- #2 Phillips screwdriver (or equivalent)
- Masking tape or felt-tip pen for marking the mounting holes where you will mount the device

Rack Kit

Figure 1-7 shows the contents of the Network VirusWall Enforcer 2500 rack kit.

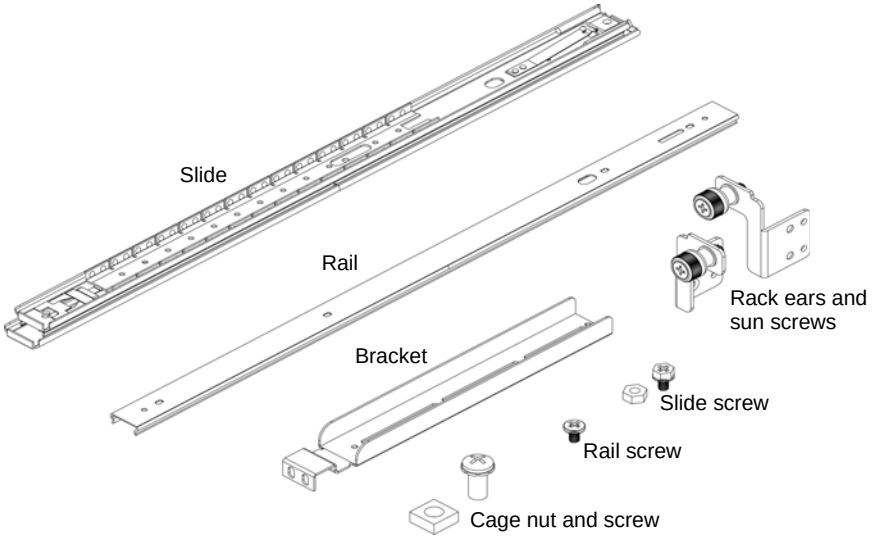


FIGURE 1-7. Rack kit contents

Table 1-10 specifies each item.

QUANTITY	ITEM	DESCRIPTION
2 sets (1 slide and 1 rail pair per each set)	Slide and rail sets	Secure the device (fixed mount) or use to secure and allow the device to slide in and out of a four-post rack (sliding mount **Note:** The rail is assembled with the slide when the package is shipped. Remove the rail from the slide before mounting the device.
4 pieces (2 pieces per pair)	Slide brackets	Hold the device on both sides of the panel of a four-post rack cabinet
1 pair	Rack ears	Secure the device in a fixed mount (when paired with sun screws) or use to serve as the handle when pulling the device out of or sliding it into a four-post rack for a sliding mount
1 pair	Sun screws	Secure the device in a fixed mount
10 pieces 8 pieces	Cage nuts Case screws	Hold the slide brackets and secure the device in both the front and back rack slots
14 pieces	Slide set screws	Secure the slide and bracket pair
14 pieces	Rail screws	Secure the rails on the both side panels of the device (one per side panel)

TABLE 1-10. Network VirusWall Enforcer 2500 rack kit contents

Figure 1-8 illustrates the positions of the slide set, rail, and cage screws.

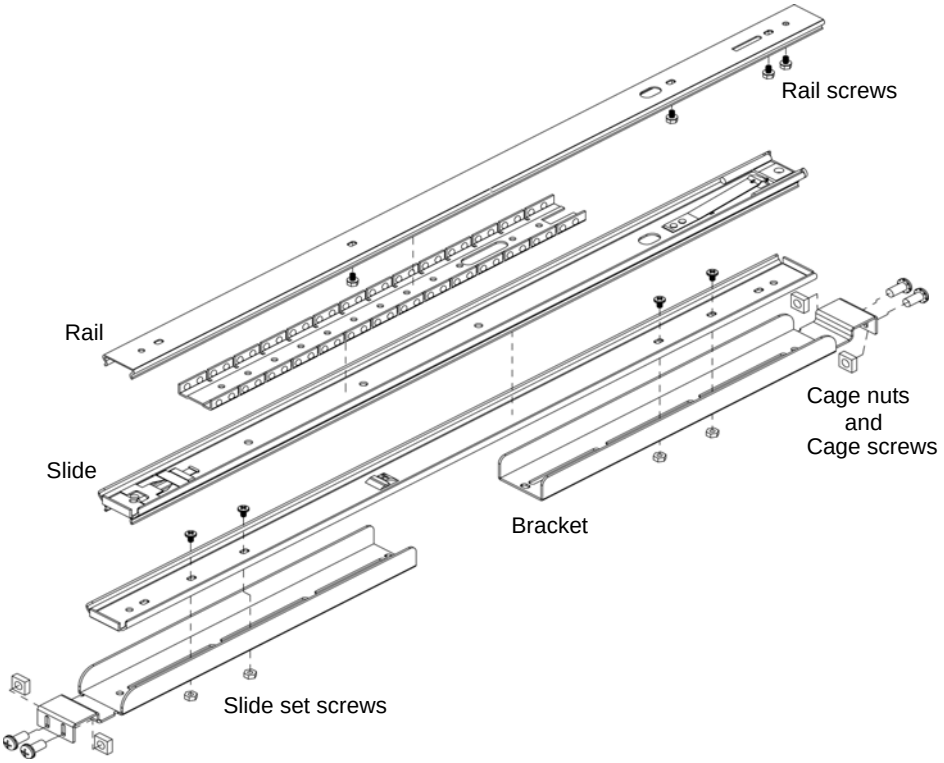


FIGURE 1-8. Positions of the slide set, rail, and cage screws

Four-Post Rack Mounting

You can mount the device in a 19" standard cabinet rack.

There are two types of mount setup:

- Sliding mount– allows you to slide the device in and out of the rack cabinet (see *page 1-24* for illustration)
- Fixed mount– secures the device in one position (see *page 1-21* for illustration)

Note: Ensure that the rack cabinet's side panel is longer than 25 in. (635mm).

To mount Network VirusWall Enforcer 2500 in a four-post rack cabinet:

WARNING! *Do not install rack kit components designed for another system. Use only the rack kit for your Network VirusWall Enforcer 2500 device. Using the rack kit for another system may damage the device and cause injury.*

1. Prepare the Network VirusWall Enforcer 2500 device (see *page 1-15*).
2. Assemble the slide sets (see *page 1-17*).
3. Install the slide sets (see *page 1-21*).
4. Mount the device in the rack (see *page 1-24*).

Preparing the Device

To prepare the device:

1. Attach the rack ear and sun screw set to each side on the front-end of the device (see *Figure 1-9*).

FIGURE 1-9. Attaching the rack ear with sun screw to the device

2. Holding a rail and slide set horizontally, with the slide's back facing you, detach the rail from the slide by pulling the rail lock to the right.

FIGURE 1-10. Detaching the rail from the slide

Tip: Check whether the rail is properly detached by checking the slide latch. If the rail is detached properly, the slide latch should be released. See *Figure 1-11*.

FIGURE 1-11. Rail is properly detached when the latch is raised

3. Attach a rail to the device side panel by using a minimum of four (4) slide screws (see *Figure 1-12*).

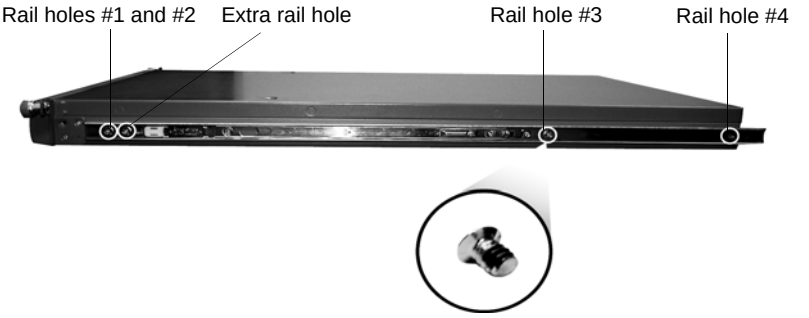


FIGURE 1-12. Attaching a rail to the side panel using slide screws

Tip: See *Figure 1-8* to for an illustration of the rail screws.

4. Repeat step 3 for the other side panel.
   Figure 1-13 illustrates a device with rails and rack ears attached.

FIGURE 1-13. Completed rack ear and rail preparation

Assembling the Slide Sets

This task involves preparation of two slide sets – one for each side panel. The following items compose a slide set:

- 1 slide
- 2 brackets, for each end
- 4 slide screws (2 slide screws per bracket)

To assemble a slide set:

1. Prepare one end of the slide set. See *Figure 1-14* for information about the slide set elements.

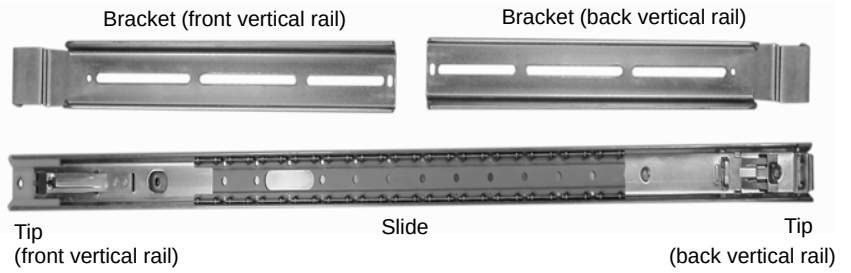


FIGURE 1-14. A slide set is composed of two brackets and a slide

Figure 1-15 illustrates how a slide set is mounted in a four-post rack.

FIGURE 1-15. A slide set installed in a four-post rack

a. Assemble the bracket and slide pair for the back vertical rail by locating the screw holes and aligning their positions. See *Figure 1-16* for the screw holes and positions.

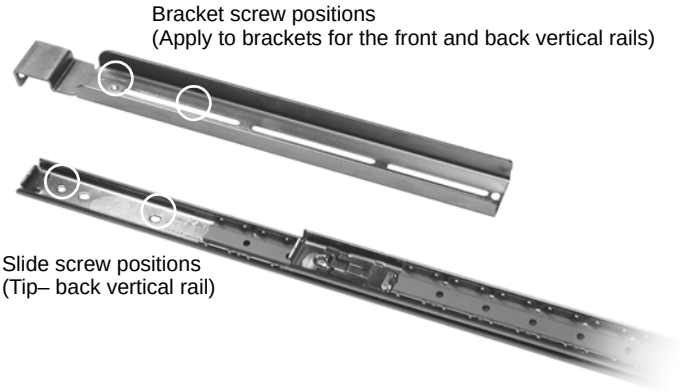


FIGURE 1-16. Screw positions for the back vertical rail

Tip: See *page 1-13* for illustration on the positions of the slide and bracket screws.

b. Insert the slide screws (see *Figure 1-17*).

FIGURE 1-17. Inserting two slide screws (bracket and slide pair for the back vertical rail)

Tip: See *page 1-13* for an illustration of the slide set screws.

2. Follow the instructions in step 1 to assemble the bracket and slide pair for the front vertical rail.

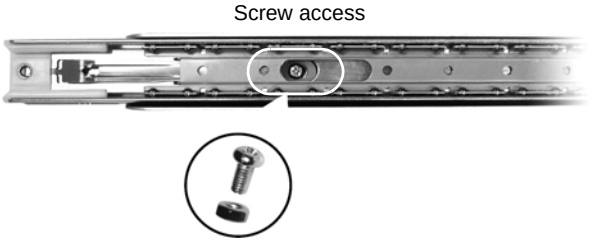


FIGURE 1-18. Inserting two slide screws (bracket and slide pair for the front vertical rail)

Tip: See *page 1-13* for an illustration of the slide set screws.

Figure 1-19 shows both ends and the back view of a completed slide set.

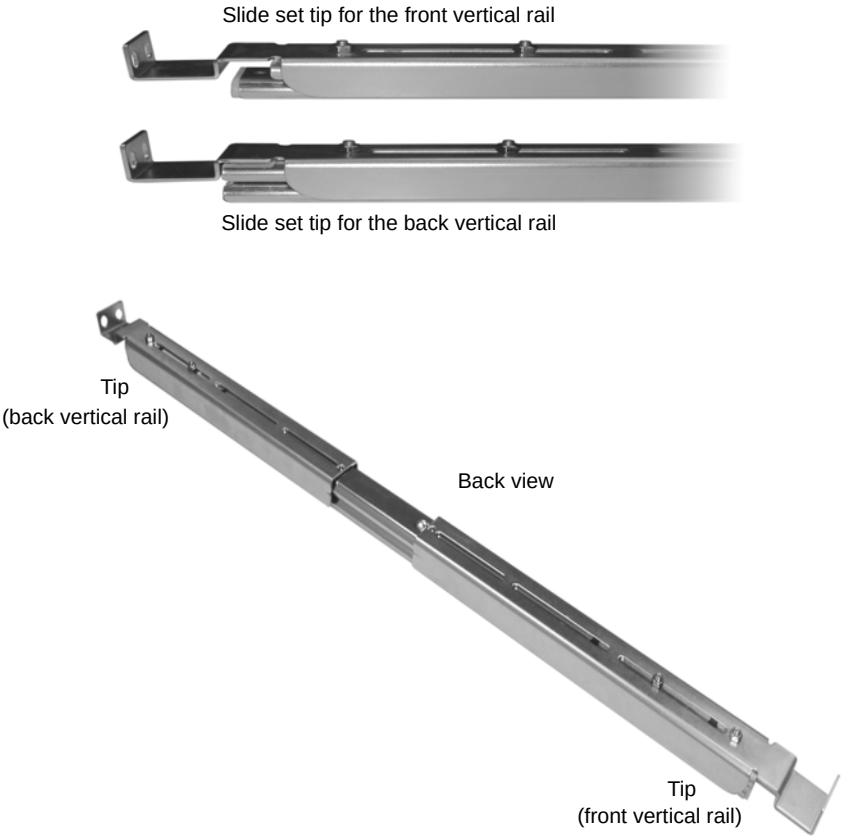


FIGURE 1-19. Completed slide set

Installing the Slide Sets

This task involves installation of the assembled slide sets to a four-post rack.

To install the slide sets:

1. Remove the rack doors if the rack doors are still covering the rack slots where you want to mount the device.

> **Tip:** Refer to documentation provided with the rack cabinet for details on how to remove the rack doors.

2. Using the masking tape or felt-tip pen, place a mark on the rack's front vertical rails where you want to position the bottom of the device. *Figure 1-20* illustrates this step.

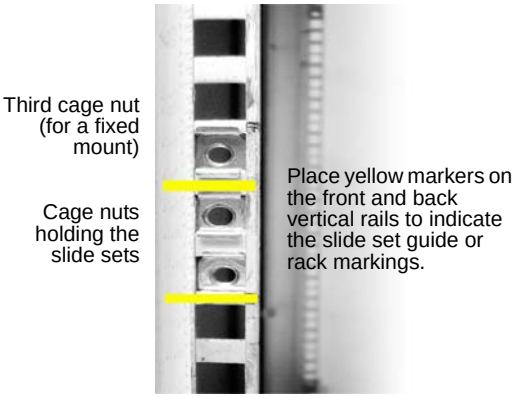


FIGURE 1-20. Graphical representation of the device position in the rack and slide set guides (rack markings)

3. Place a mark 1.70 in (4.32 cm) above the original mark you made (or count up two holes) and mark the rack's front vertical rails to indicate placement of the device's upper edge on the vertical rails.

> **Tip:** A Network VirusWall Enforcer 2500 device occupies 1 RU (1.70 in or 4.32 cm, three rack holes) of vertical space in the rack.

4. Install one pair of cage nuts to occupy holes between the marks you made on the front vertical rail (see *Figure 1-21*).

Two (2) cage nuts occupying two (2) vertical holes that will hold the slide set for a sliding mount

FIGURE 1-21. Cage nuts for a sliding mount

Note: Install a third cage nut above the cage nut pair for a fixed mount (see *Figure 1-22*).

Three (3) cage nuts occupying three (3) vertical holes that will hold the slide set and sun screw for a fixed mount

FIGURE 1-22. Cage nuts for a fixed mount

5. Starting with the front vertical rail, hold and position the slide set tip to align with the holes of the cage nuts.
6. Install two cage screws over the slide set and cage nuts' top and bottom holes to secure the slide set to the front vertical rail (see *Figure 1-23*).

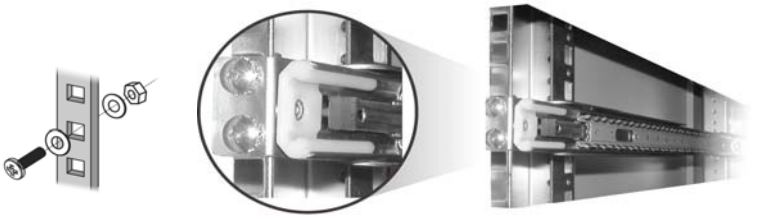


FIGURE 1-23. Installing the cage screws in the top and bottom holes of the slide set (front vertical rail view)

7. At the back of the cabinet, pull back the slide set until the mounting holes align with their respective cage nut holes on the back vertical rail.
8. Repeat steps 2 to 7 for the remaining slide set on the other side of the rack.
9. Guarantee that the slide sets are installed at the same position on the vertical rails on each side of the rack (see *Figure 1-24*).

FIGURE 1-24. Mounted slide sets

Mounting the Device in the Rack

To help ensure safety, do not attempt to mount the device in the rack by yourself.

To mount the device in the rack:

1. Pull the two slides out of the rack until the release latches lock in a fully extended position.
2. Lift the device into position in front of the extended slides.
3. Holding the top and bottom panels, align and fit the side panel rails on the left and right slide sets (see *Figure 1-24* for a sample of mounted slide sets).
4. Push the device into the rack until the front and back end slide set screws engage into their slots (see *Figure 1-25*).

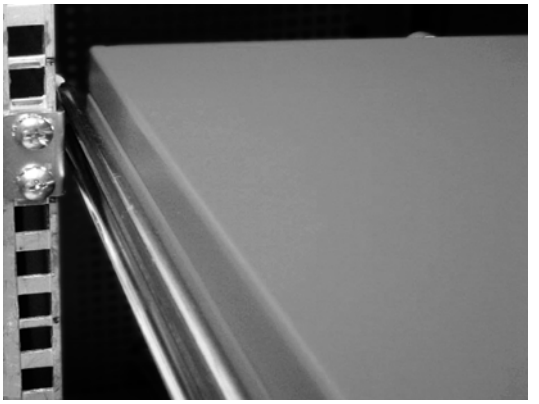


FIGURE 1-25. Mounted device (sliding mount)

5. Install the sun screws to prevent the device from sliding in or out (see *Figure 1-26*).

FIGURE 1-26. Mounted Network VirusWall Enforcer 2500 device (fixed mount)

After mounting the device, follow the directions in these sections:

- *Planning for Deployment* on page 3-2
- *Conducting a Pilot Deployment* on page 3-16
- *Understanding Preconfiguration* on page 5-2

Installing a Fiber-Optic Card

The device ships with one of two physical configurations:

- One dual-port multi-mode fiber-optic card pre-installed

  —or—

- No fiber-optic card pre-installed

Network VirusWall Enforcer 2500 supports the following fiber-optic server adapters:

- Intel PRO/1000 MF Dual Port Server Adapter
- Intel PRO/1000 MF Single Port Server Adapter (LX)
- Silicom Dual Port Fiber (SX) Gigabit Ethernet PIC-X Bypass Server Adapter
- Silicom Dual Port Fiber (LX) Gigabit Ethernet PCI-X Bypass Server Adapter
- Silicom Dual Port Copper Gigabit Ethernet PCI-X Bypass Server Adapter

Opening the Device

In order to install a fiber-optic card, first remove the device's top cover and front panel. If the device is mounted in a rack, unmount the device from the rack before attempting to install a fiber-optic card.

To prepare the device to receive a fiber-optic card:

1. Turn off the power switch on the back of the device.
2. Unplug the AC power cord.

WARNING! *Unplug the AC power cord after turning off the device. If the cord is still connected to the machine, there is risk of electric shock even if the power switch is in the off position.*

3. Unscrew the large cover screw on the rear panel of the machine.

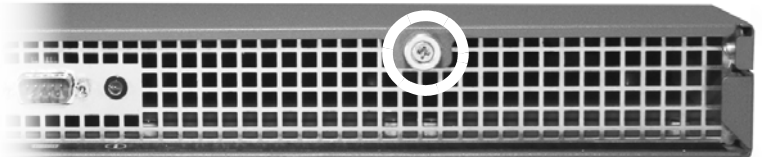


FIGURE 1-27. Back panel showing cover screw

4. Slide the top cover back, lift it off the machine, and set it aside.
5. Using both hands, grasp the top and bottom sides of the front bezel panel and gently squeeze the panel while pulling down. The bezel detaches from the front of the machine.

FIGURE 1-28. Network VirusWall Enforcer 2500 front bezel panel, detached

6. Using a Phillips-head screwdriver, unscrew the top left screw of the red metal bracket connected to the right side of machine, just around the right corner from the front panel.

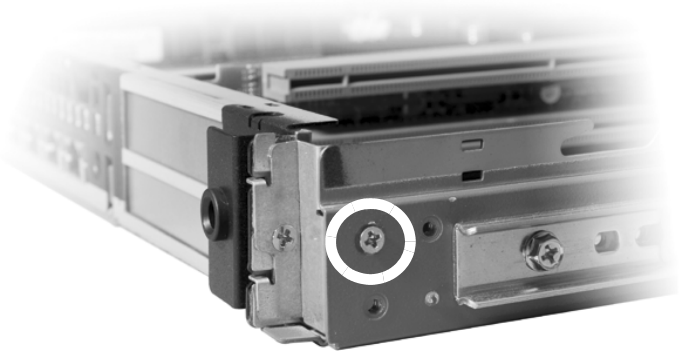


FIGURE 1-29. The screw to remove for step 6

7. Remove the PCI slot cover from the detached front bezel panel.
8. In the accessory box, locate the PCI slot cover designed to accommodate connectors on the top half. Attach the slot cover to the front bezel by inserting the plastic prongs into the receptacles on the front bezel. Note that the prongs and receptacles are designed so that the slot cover only clips into place in the correct direction, which is with the open area at the top.

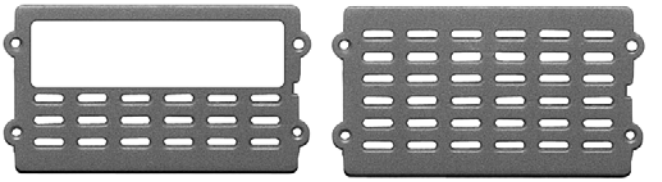


FIGURE 1-30. Two PCI slot covers. Left: open-area cover, Right: fully masked cover

9. Using a Phillips-head screwdriver, unscrew the silver metal side bracket that holds the blank metal expansion slot plates in place.

FIGURE 1-31. The silver metal side bracket

10. Remove the blank metal expansion slot plate from the back of the case at one end of the top slot (slot 1) and set it aside.

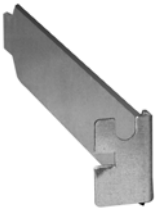


FIGURE 1-32. Blank metal expansion slot plate

The device is now ready to receive the fiber-optic card. See *To install a fiber-optic card in an open machine:* on page 1-30 for instructions on installing the card.

Note: If you are installing more than one fiber-optic card, install the card that will go into the bottom slot (slot 2) first. When installing two cards, no PCI slot cover is necessary.

Installing the Card

After you have removed the front panel and top cover from the device, you are ready to install the card into an available slot. (See *To prepare the device to receive a fiber-optic card:* on page 1-27.)

To install a fiber-optic card in an open machine:

1. Carefully remove the card from its plastic container.

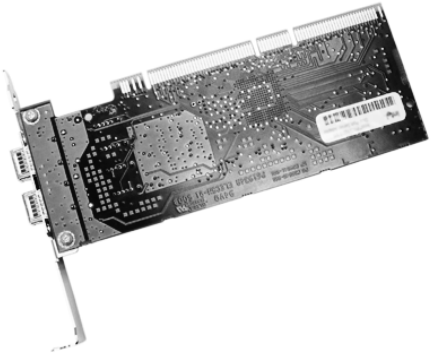


FIGURE 1-33. A duplex single-mode fiber-optic card

2. Remove any rubber "dummy" connector plugs from the connector sockets and orient the card so that its components are facing downward.

3. Insert the card at a 45 degree angle.

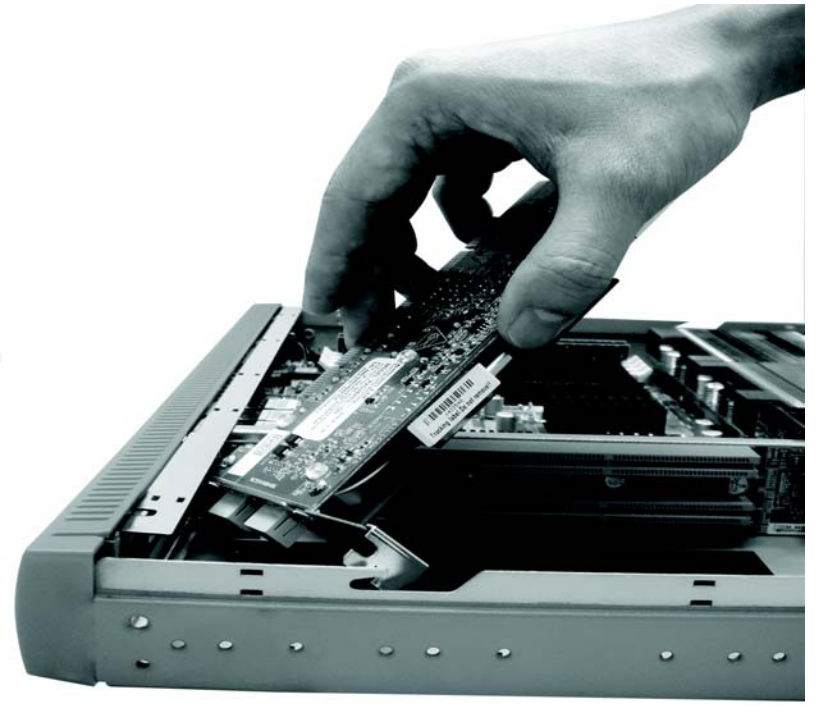


FIGURE 1-34. Insert the card at an angle

4. Slide the card to the fit in the front of the device.

FIGURE 1-35. Slide the card to the front of the device

5. Insert the card into the desired slot. (Insert card into the top slot if installing only one card.) Ensure that the card snaps solidly into place.

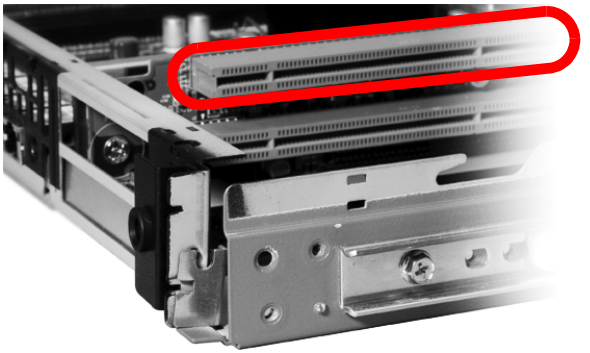


FIGURE 1-36. Insert card in top slot if only installing one card

6. Replace the silver metal side bracket and screw it back on.
7. Replace the top left screw in the red metal bracket connected to the right side of machine, just around the right corner from the front panel.
8. Replace the front bezel, making sure that it snaps into place.
9. Replace the top cover and screw back in the Sun screw on the rear panel of the machine.
10. Plug the power cord back into the outlet on the rear panel of the machine.
11. Turn the power switch back on.
12. Log on to the Web console to confirm installation of the card from the **Real-Time Status** screen. If installation is successful, the ports on the card display under **Interface Configuration Status**.

Removing or Replacing a Fiber-Optic Card

If you need to remove or replace an installed fiber-optic card, follow the instructions in *To prepare the device to receive a fiber-optic card:* on page 1-27 and then proceed as follows.

To remove a fiber-optic card from Network VirusWall Enforcer 2500:

1. Carefully remove the card from its PCI slot and set it aside.
2. Replace the blank metal slot plate at the back of the case at one end of the slot.
3. Replace the silver metal side bracket and screw it back on using a Phillips-head screwdriver.
4. Replace the top left screw in the red metal bracket connected to the right side of machine, just around the right corner from the front panel.
5. Remove the PCI slot cover from the detached front bezel panel.
6. In the accessory box, locate the original PCI slot cover designed to mask the PCI slot area. Attach the slot cover to the front bezel by inserting the plastic prongs into the receptacles on the front bezel.
7. Replace the front bezel, making sure that it snaps into place.
8. Replace the top cover and screw back in the cover screw on the rear panel of the machine.
9. Plug the power cord back into the outlet on the rear panel of the machine.
10. Turn the power switch back on.

Chapter 2

Introducing Trend Micro™ Network VirusWall™ Enforcer 2500

This chapter introduces Trend Micro Network VirusWall Enforcer 2500 and provides an overview of its components and deployment.

The topics discussed in this chapter include:

- *Network VirusWall Enforcer 2500* on page 2-2
- *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3
- *Trend Micro Network VirusWall Enforcer 2500 Web Console* on page 2-5
- *Understanding Network VirusWall Enforcer Ports* on page 2-6
- *Deployment Overview* on page 2-6

Network VirusWall Enforcer 2500

Network VirusWall Enforcer 2500 is an outbreak prevention appliance that helps organizations stop network viruses (Internet worms), block high-threat vulnerabilities during outbreaks, and quarantine and clean up infection sources. Network VirusWall Enforcer 2500, deployed at the network layer, uses threat-specific knowledge from Trend Micro to protect against threats as they enter the network. The device scans all the traffic on a specific network segment and applies one policy to an endpoint based on a first-match rule.

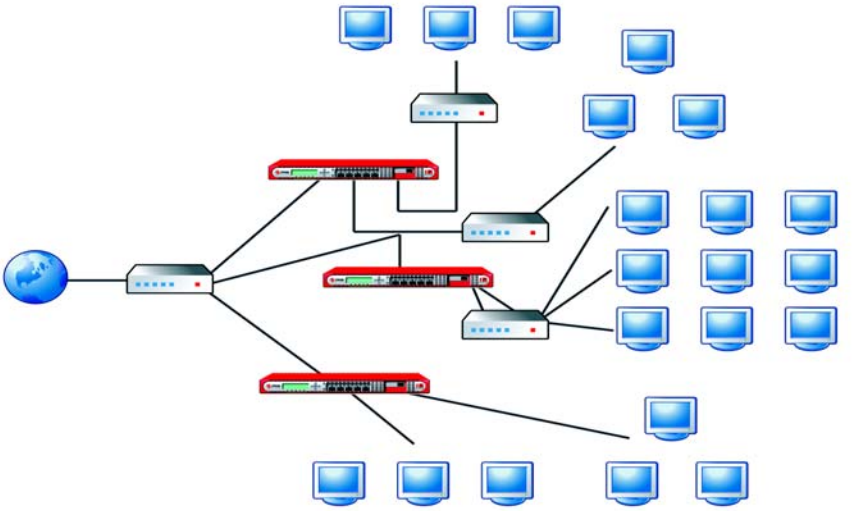


FIGURE 2-1. The device monitors network packets and events that could indicate an attack against a network

Refer to *Understanding Network VirusWall Enforcer 2500* in the *Administrator's Guide* for product function, architecture, and other details.

Introducing Network VirusWall Enforcer 2500-specific Terms

Before proceeding to the next section, take note of the following terms introduced in this chapter (also available in *Glossary* in the *Administrator's Guide*):

Ethernet and fiber-optic ports—residing on the device's front panel, these ports link to other devices (usually Layer 2 or Layer 3 devices)

The documentation sometimes refers to *Copper Gigabit Ethernet ports* and fiber-optic ports as *ports* or *interfaces* (see *Understanding Network VirusWall Enforcer Ports* on page 2-6). You can specify the following port types for each physical port:

- **MANAGEMENT** port (RJ-45 or fiber optic)—dedicated for management purposes. You can only specify one **MANAGEMENT** port.
- **MIRROR** port (RJ-45 or fiber optic)—sends all traffic going through the device to a computer to capture all data. The data can then be used for debugging purposes. You can specify one **MIRROR** port. (There may be an impact to performance if you use this port type.)
- **SNIFFER** port (RJ-45 or fiber optic)—receives and scans packets from the switch. You can specify multiple **SNIFFER** ports.
- **REGULAR** port (RJ-45 or fiber optic)—carries analyzed traffic to and from segments. You can specify multiple **REGULAR** ports.

Note: In previous versions of Network VirusWall, ports were separated into internal and external ports. However, in this version of Network VirusWall Enforcer 2500, the device does not differentiate internal and external ports.

- **FAILOVER** port (RJ-45 or fiber optic)—connects to another Network VirusWall Enforcer 2500 device used in a deployment with failover. You can specify one **FAILOVER** port.
- **SHARED** port (RJ-45 or fiber optic)—belongs to two port groups.

Failopen—a fault-tolerance solution, also known as LAN bypass, that allows the Network VirusWall Enforcer 2500 device to continue to pass traffic if a software or hardware failure occurs within the device.

Failover—a redundant setup in which the functions of a Network VirusWall Enforcer 2500 device are assumed by a second Network VirusWall Enforcer 2500 device when the first device becomes unavailable through either failure or scheduled downtime. Both devices perform the same function, but administrative tasks and management can only be performed using the Management device.

Link-state Failover—a port redundancy setting that enables this feature to turn off the working ports if a port fails in a port group. This allows all traffic to flow through the redundant port group and ensure that data transfers through the functioning port group. This feature cannot be enabled if there is a shared port in the port group.

Management device—a Network VirusWall Enforcer 2500 device that is used for management. All configurations from this device are replicated to the other device in the failover pair. You can select either the Primary or Secondary device to be the Management device in a failover pair.

Note: In previous versions of Network VirusWall, Active and Standby described the device that registers to Control Manager and the second device that receives all configuration from the first device. In Network VirusWall Enforcer 2500, both devices perform the same filtering functions. However, the Management device is the device that replicates configuration settings to the second device. By default, the Primary device is the Management device.

Primary device—a device in a failover pair. This is also the default Management device in a failover pair.

Secondary device—a device in a failover pair.

Trend Micro Network VirusWall Enforcer 2500 Web Console

The Network VirusWall Enforcer 2500 Web console provides central management for Network VirusWall Enforcer 2500 devices on your network. The Web console gives you the tools to configure and enforce security policies for an entire organization. This enables you to react quickly to network virus emergencies from nearly anywhere using the Web console.

After preconfiguration, the Web console enables you to perform the following Network VirusWall Enforcer 2500 administrative tasks:

- Analyze your network's protection against viruses
- Update components and settings
- Enforce security policies (following the first-match rule, only one policy applies to an endpoint at a time)
- View and manage logs
- Manage the device

For guidance on administering devices from the Web console, see the *Network VirusWall Enforcer 2500 Administrator's Guide.*

Understanding Network VirusWall Enforcer Ports

Network VirusWall Enforcer 2500 supports up to 9 ports—5 copper Ethernet ports and up to 4 additional copper gigabit ethernet or fiber-optic ports. The device applies its protection features to packets that pass through the device.

Note: The **FAILOVER** port is for connection to another identical device. See *Deploying Network VirusWall™ Enforcer 2500* starting on page 3-1 for details on how to allocate the Network VirusWall Enforcer 2500 ports.

Deployment Overview

Network VirusWall Enforcer 2500 deployment consists of the following steps:

1. Deciding on the deployment strategy

   Deploying Network VirusWall™ Enforcer 2500 provides the basic deployment and strategies. This chapter aims to help you determine the strategy you will take to deploy Network VirusWall Enforcer 2500.

2. Preparing for preconfiguration

   Preparing for Preconfiguration discusses the initial preconfiguration tasks that you need to perform to successfully deploy the device.

3. Preconfiguring Network VirusWall Enforcer 2500

   Preconfiguring Network VirusWall Enforcer 2500 provides instructions to guide you during device preconfiguration.

4. Configuring Network VirusWall Enforcer 2500

   Configuring Policy Enforcement and Device Settings of the *Administrator's Guide* includes instructions to help you configure the basic settings after preconfiguration.

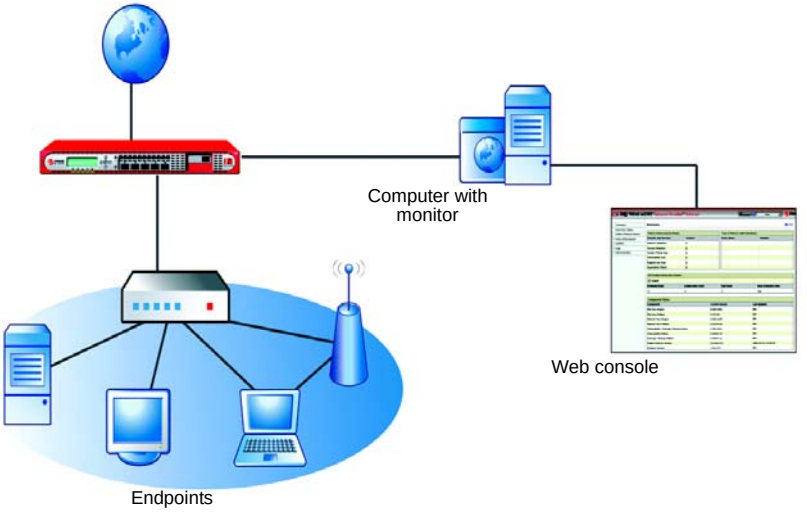


FIGURE 2-2. Network VirusWall Enforcer 2500 after preconfiguration

Understanding Network VirusWall Enforcer 2500 of the *Administrator's Guide* provides details about the following concepts:

- Antivirus capabilities
- Policy Enforcement using the first-match rule
- EndpointEndpoints

After checking the package contents and device's physical specifications in *Getting Started*, proceed to *Deploying Network VirusWall™ Enforcer 2500* for deployment considerations and sample deployment strategies.

Chapter 3

Deploying Network VirusWall™ Enforcer 2500

Before beginning to configure a Network VirusWall Enforcer 2500 device, plan how to integrate the device into your network. Determine which topology it will support.

This chapter explains how to plan for the deployment of Network VirusWall Enforcer 2500 devices. It also provides application and deployment scenarios to facilitate understanding of the various ways the device can help protect and secure your network.

This chapter contains the following topics:

- *Planning for Deployment* on page 3-2
- *Identifying What to Protect* on page 3-5
- *Planning for Network Traffic* on page 3-15
- *Conducting a Pilot Deployment* on page 3-16
- *Redefining Your Deployment Strategy* on page 3-17
- *Deploying Network VirusWall Enforcer 2500* on page 3-17

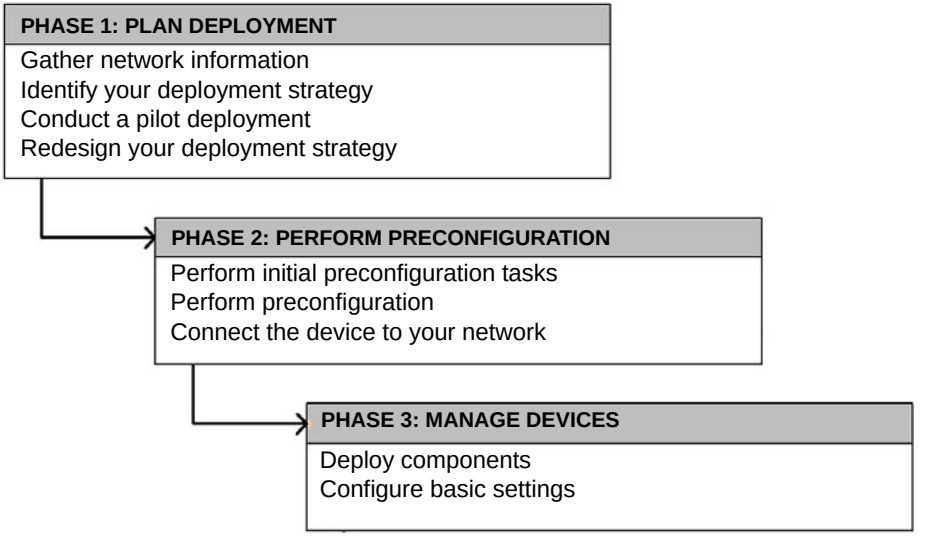
Planning for Deployment

To take advantage of the benefits Network VirusWall Enforcer 2500 can bring to your organization, you will need an understanding of the possible ways to deploy one or more devices. This section provides deployment overview and considerations.

Note: This version only supports EtherChannel in a single device environment with two port groups.

Deployment Overview

Follow three stages of deployment to successfully install the device(s).



Phase 1: Plan the Deployment

During phase 1, plan how to best deploy the device(s) by completing these tasks:

- Determine the segments of your network that are in the greatest need of protection
- Plan for network traffic, considering the location of devices critical to your operations such as email, Web, and application servers
- Determine both the number of devices needed to meet your security needs and their locations on the network
- Conduct a pilot deployment on a test segment of your network
- Redefine your deployment strategy based on the results of the pilot deployment

Phase 2: Perform Preconfiguration

During phase 2, start implementing the plan you created in phase 1. Perform the following tasks:

- Perform the initial preconfiguration tasks (See *Network VirusWall Enforcer 2500 Initial Tasks* on page 4-2)
- Perform preconfiguration on the device(s) (See *Configuring Network VirusWall Enforcer 2500* on page 5-19)
- Connect the device(s) to your network (See *Connecting to the Network* on page 5-18)

Phase 3: Manage Network VirusWall Enforcer 2500 Devices

During phase 3, manage Network VirusWall Enforcer 2500 devices from the Web console. You can perform the following tasks:

- Create and manage policies to protect your network
- Update device components
- View summaries and logs to analyze your network
- Configure device settings

Tip: This *Getting Started Guide* discusses phases 1 and 2. Refer to *Network VirusWall Enforcer 2500 Administrator's Guide* for instructions relating to phase 3.

Deployment Notes

Consider the following when planning for a deployment:

- All traffic to and from a network segment has to go through the device

  To protect an organization from network threats, position the device to key places on your network. The device should be able to scan all network traffic to prevent, detect, or contain threats.

- Each of the interfaces supports the following port speed and duplex mode settings:
  - 10Mbps x half-duplex
  - 10Mbps x full-duplex
  - 100Mbps x half-duplex
  - 100Mbps x full-duplex
  - 1000Mbps x full-duplex

Note: Both the connected L2/L3 and Network VirusWall Enforcer 2500 devices should have the same interface setting and duplex mode. Otherwise, the half-duplex mode setting will take effect. To help guarantee the correct interface setting and duplex mode implementation, modify both the L2/L3 and Network VirusWall Enforcer 2500 devices to have the same setting. Apply **1000Mbps x full-duplex** for both the switch and Network VirusWall Enforcer 2500 device.

- The device supports IP addresses belonging to any classes (that is, class A, B, or C)

Tip: Although each range is in a different class, you are not required to use any particular range for your internal network. It is a good practice, though, because it greatly diminishes the chance of an IP address conflict.

- Policy Enforcement and Real-time Packet Scan support various action for non-compliant or infected endpoints

Identifying What to Protect

Position Network VirusWall Enforcer 2500 between layer 2 (L2) or layer 3 (L3) devices. This way, Network VirusWall Enforcer 2500 can apply its protection to packets coming in or out of your network. Refer to *Glossary* in the *Administrator's Guide* for L2 and L3 definitions.

Identify segments of your network to protect by considering which kinds of endpoints may introduce viruses or violate security policies. Also, consider the location of resources that are critical to your organization. The following are examples:

- Remote endpoints that access your internal network resources
- Guest endpoints that temporarily connect to your network
- Key network segments/important network assets, such as places on the network that contain email, Web, and application servers including endpoint computers

Remote Access Endpoints

Remote endpoints access internal network resources in the same manner as the endpoints already on your network and comprise essentially another internal network segment. You must consider whether to protect remote endpoints as you do internal endpoints.

There are two types of remote endpoints:

- **Dial-up/home users** – often telecommuters who use a dial up or DSL connection to access your network
- **External business units** – offices located outside of the organization but who still need access to resources on your organization's main network

A home user could establish a dialup connection or a Virtual Private Network (VPN) connection to access a company's internal network resources. Most likely, business units would establish a VPN connection.

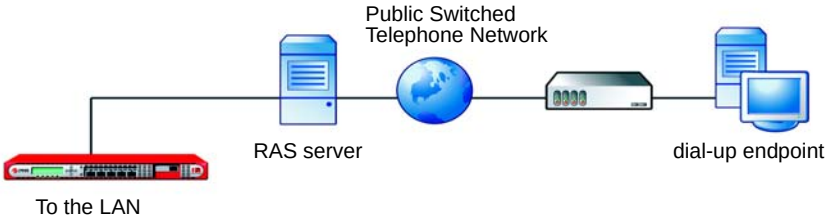


FIGURE 3-1 Dial-up service deployment scenario

Figure 3-1 illustrates a dialup connection between a home user and an organization's internal network. A RAS server, the point where the dialup connection terminates, is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3 for information about different types of ports). (For example, port 4.) This means that all packets going between the RAS server and the LAN pass through the device. Once the home user establishes a connection with the RAS server, it essentially becomes part of the internal network as illustrated in the basic deployment scenario (See *A Basic Deployment Scenario* on page 3-18). The home user accesses both network resources and the Internet in the same way internal endpoints do.

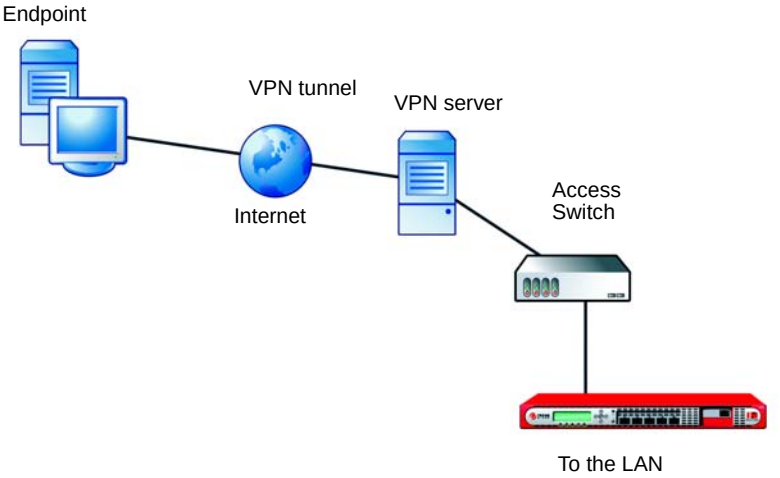


FIGURE 3-2 Endpoint to site VPN deployment scenario

Figure 3-2 illustrates a connection between a home user and an organization's internal network, only though a VPN server, which is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3 for information about different types of ports). In this configuration, the home user's VPN connection is considered to be part of the internal network.

Note: Network VirusWall Enforcer 2500 must be behind the VPN server, which encrypts and decrypts VPN traffic.

The recommended settings for this scenario are the same as the settings for the dial-up user scenario (see *Figure 3-1*).

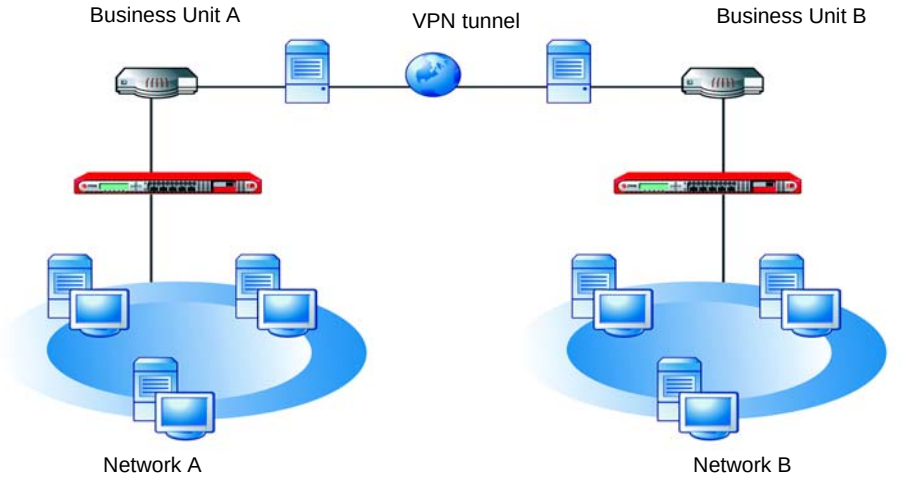


FIGURE 3-3. Site to site VPN deployment scenario

Figure 3-3 illustrates a VPN connection between two business units. As in the home user scenario, a VPN server is connected to a **REGULAR** port on each device (See *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3 for information about different types of ports).

Guest Endpoints

Guest endpoints are endpoints that do not belong to an internal network domain. They are often visitors who temporarily access your network resources through their portable computers. Guest endpoints represent an especially high risk because they are outside of your network security scope and therefore may inadvertently violate virus-protection policies and even introduce viruses to the network.

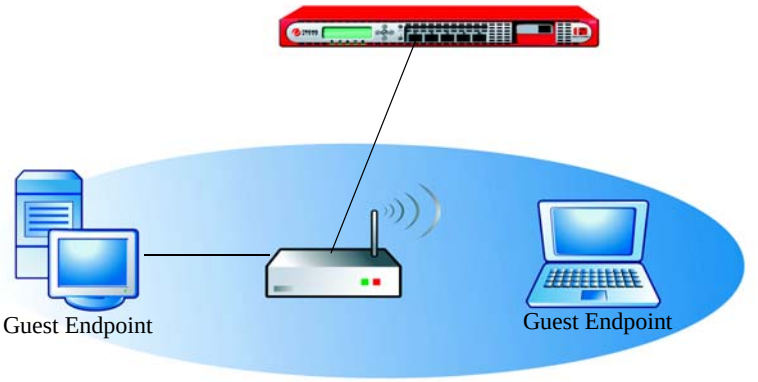


FIGURE 3-4. Guest network deployment scenario

Figure 3-4 illustrates a segment of an internal network especially for guest endpoints. A wireless access point, switch, or hub is connected to the **REGULAR** port (See *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3 for information about different types of ports). This type of topology ensures that the device scans all traffic before it leaves the guest network segment and makes isolation of the guest segment possible in the event of a virus outbreak.

Key Network Segments/Important Network Assets

Key network segments need to be protected from network-based threats. This may include a group of endpoint machines or network resources that are critical to the functioning of your organization, such as email, Web, and application servers.

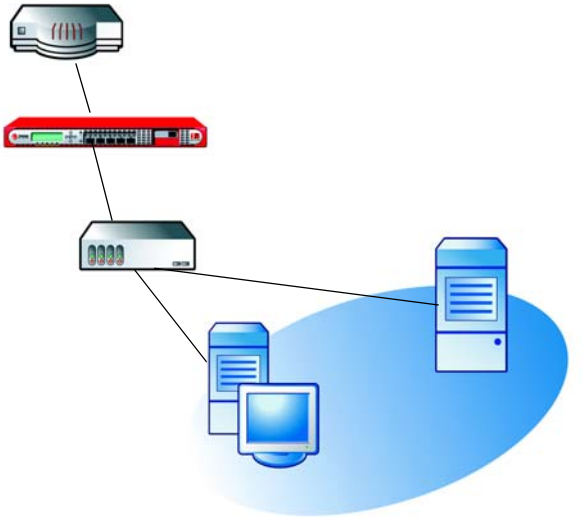


FIGURE 3-5. Key network segments scenario

Key Network Segments/Important Network Assets on page 3-10 illustrates a segment of an internal network containing email and Web servers, including endpoints. An internal switch or hub is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 2500-specific Terms* on page 2-3 for information about different types of ports), creating a segment where all packets going in and out of the segment can be scanned. Installing the device in this position adds the benefits of virus scanning and segment isolation in the event of a virus outbreak.

Another advantage is that it can guard against attacks that not only originate on the Internet, but also attacks that may originate from within your organization's network. Since traffic first passes through the device before reaching the email and Web servers, the device can scan and detect infected packets that come from endpoints on the LAN.

Dual-switch VLAN Environment

Network VirusWall Enforcer 2500 must be placed in line on the physical network to be able to provide security. In most situations, this means between an upstream switch and one or more downstream switches.

Most VLAN configurations will utilize two switches. Single-switch VLAN configurations are possible; for more information refer to *Single-switch VLAN Environment* on page 3-14. The figures in this section illustrate multiple downstream switches in a flat topology; however, a single in line configuration is also possible.

In *Figure 3-6*, The devices are installed between an upstream switch and downstream switches. This configuration is appropriate when multiple VLANs carry moderate network traffic, and the upstream switch carries high-bandwidth traffic.

Note: Ensure that Spanning Tree Protocol (STP) is enabled. If STP is not enabled, packets may loop for an indefinite period.

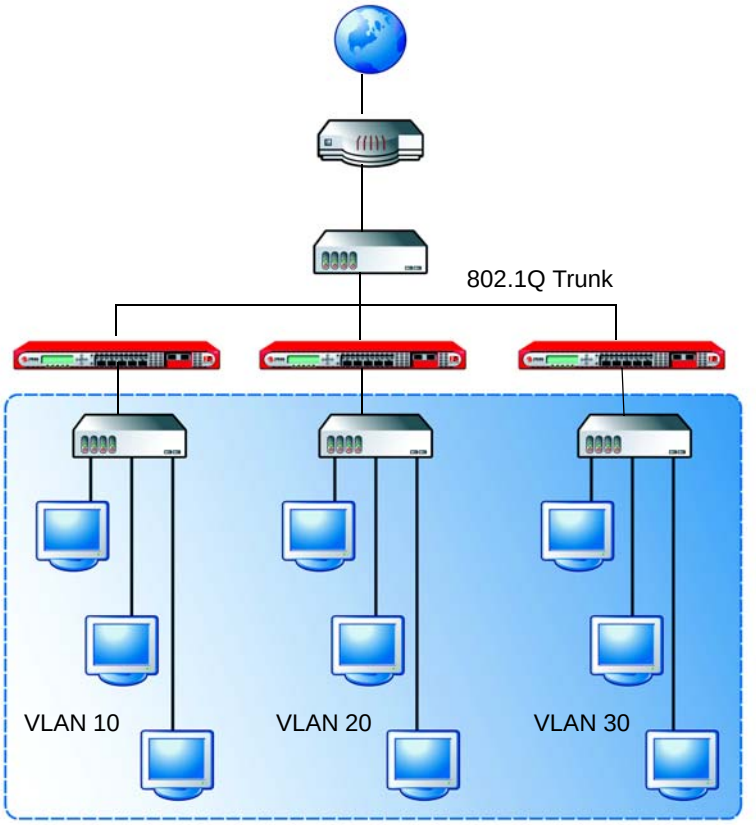


FIGURE 3-6. Multiple VLAN segments with each device protecting one segment

In *Figure 3-6*, the devices are installed on an 802.1Q trunk line between two switches.

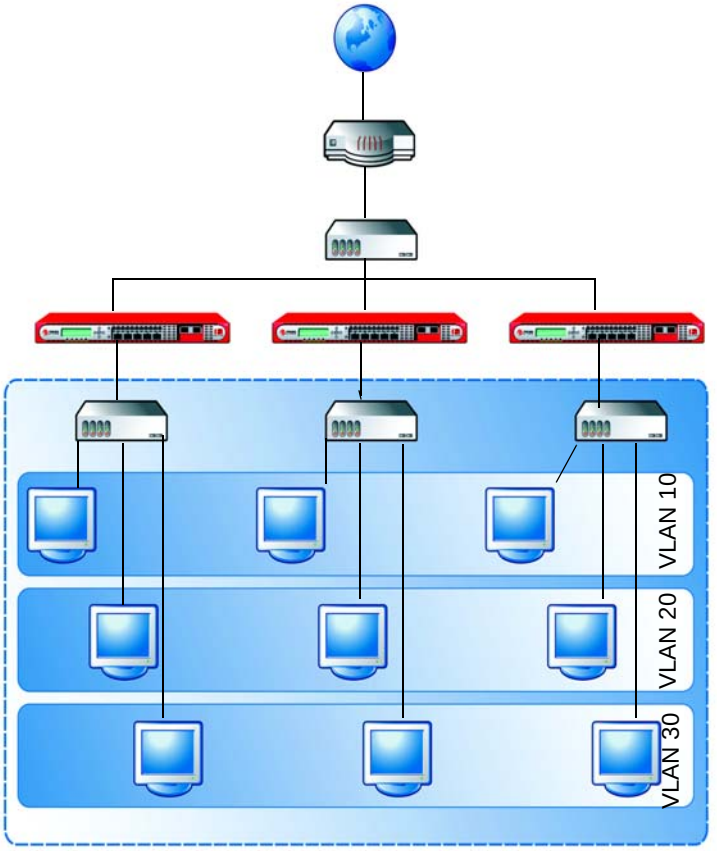


FIGURE 3-7. Multiple VLAN segments with each device protecting all segments

Single-switch VLAN Environment

An example of a single switch configuration may have the following properties:

- Is only possible when using a switch that can be configured to carry individual VLAN traffic on specific physical ports
- VLAN 20 is assigned to ports 1 and 2 on the switch
- The upstream network is connected to port 2 on the switch
- The **REGULAR** port on Network VirusWall Enforcer 2500 is connected to port 1 on the switch
- Endpoints are connected to other **REGULAR** ports on Network VirusWall Enforcer 2500

FIGURE 3-8. Single-switch VLAN environment

Planning for Network Traffic

The scenario presented in *Key Network Segments/Important Network Assets* on page 3-10 is also a good example of how to plan for network traffic. There is a strategic advantage to positioning the device in front of resources that endpoints access regularly, such as an email or Web server. Because many viruses make their way onto networks through email attachments and Web browsers, forcing traffic to pass through the device significantly reduces the risk of virus infection. Identify other places on your network through which large amounts of traffic pass and consider positioning the device at points where it can scan the most amount of traffic.

Determining the Number of Devices to Deploy

Determine the number of devices that best meets your security requirements. This depends upon many factors, including the following:

- **Existing Network topology**– based on your network topology, identify the segments you want the device to protect (see *Identifying What to Protect* on page 3-5)
- **Existing network device interfaces**– because the device handles 10/100Mbps or 1Gbps Fast Ethernet traffic, identify the network device interfaces that handle the same type of traffic and can therefore connect to Network VirusWall Enforcer 2500 devices
- **Desired effectiveness of protection**– to lower the risk of a virus outbreak spreading, segment several sections of your network with Network VirusWall Enforcer 2500 devices
- **Desired degree of performance**– consider the number of endpoints and the amount of traffic the device can handle

Conducting a Pilot Deployment

Trend Micro recommends conducting a pilot deployment in a controlled environment to help you understand how the device features work, determine how the device can help your organization accomplish its security goals, and estimate the level of support you will likely need after a full deployment. A pilot deployment also provides feedback to help you redesign your deployment plan.

Perform the following tasks to conduct a pilot deployment:

- Choose a pilot site
- Create a contingency plan
- Deploy and evaluate your pilot

Choosing a Pilot Site

Choose a pilot site that matches your planned deployment. This includes other devices on your network such as switches and firewalls, other antivirus installations, such as Trend Micro™ OfficeScan™ 5.0 or later, and Control Manager™ 3.5. Try to simulate the type of topology that would serve as an adequate representation of your production environment.

Creating a Contingency Plan

Trend Micro recommends creating a contingency plan in case there are issues with the installation, operation, or upgrade of the device. Consider your network's vulnerabilities and how you can retain a minimum level of security if issues arise.

Deploying and Evaluating your Pilot

Deploy and evaluate the pilot based on expectations regarding both security enforcement and network performance. Create a list of items that meet and do not meet the expected results experienced through the pilot process.

Redefining Your Deployment Strategy

Identify the potential pitfalls and plan accordingly for a successful deployment. Consider especially how the device performed with the antivirus installations on your network. This pilot evaluation can be rolled into the overall production and deployment plan.

Deploying Network VirusWall Enforcer 2500

A deployment plan is dependent upon the options you create and select. With the 5 user-definable copper gigabit LAN ports and up to 4 fiber-optic or copper gigabit ethernet ports, more deployment options are now available. This section provides an example of a few basic deployment scenarios (see *page 3-18*) and deployment strategies:

- User-defined Port Grouping (see *page 3-18*)
- User-defined Port Grouping with Failover (see *page 3-21*)
- User-defined Port Redundancy (see *page 3-28*)
- User-defined Port Redundancy with Failover (see *page 3-33*)

Tip: See *Network VirusWall Enforcer 2500 Initial Tasks* on page 4-2 and *Verifying Network Support* on page 4-3 for checklists on how to prepare a device for deployment.

A Basic Deployment Scenario

The device can be installed on a network that contains Ethernet devices such as hubs, switches, and routers. Deploy Network VirusWall Enforcer 2500 between a switch that leads to the public network and a switch that protects a segment of the Local Area Network (LAN). It can also be installed between an edge switch and a hub. *Figure 3-9* illustrates a basic deployment scenario.

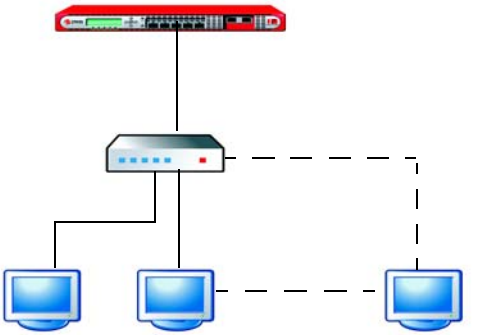


FIGURE 3-9. Basic deployment

A layer 2 (L2) or layer 3 (L3) device is connected to a **REGULAR** port.

Network VirusWall Enforcer 2500 protects your network as follows:

- Scans traffic to and from endpoints
- Prevents endpoints that violate your security policies from gaining access to resources
- Isolates the endpoints in the event of a virus infection.

In this deployment setup, you may opt to enable failopen. With failopen enabled, traffic can still pass through the device if the device encounters a hardware or system error that prevents it from filtering network packets.

See the following sections for details about:

- Failopen, proceed to *User-defined Port Redundancy Deployment*
- Failover, proceed to *User-defined Port Redundancy Deployment* and *Port Redundancy with Failover Deployment*

Multi-Protection Zone Configuration Without Failover

In this sample deployment scenario internal ports connect to four different L2 Switches (or port segments) to create the protection zone, and the fiber-optic port connects to an external L2 or L3 switch as the external port. *Figure 3-10* illustrates this deployment scenario.

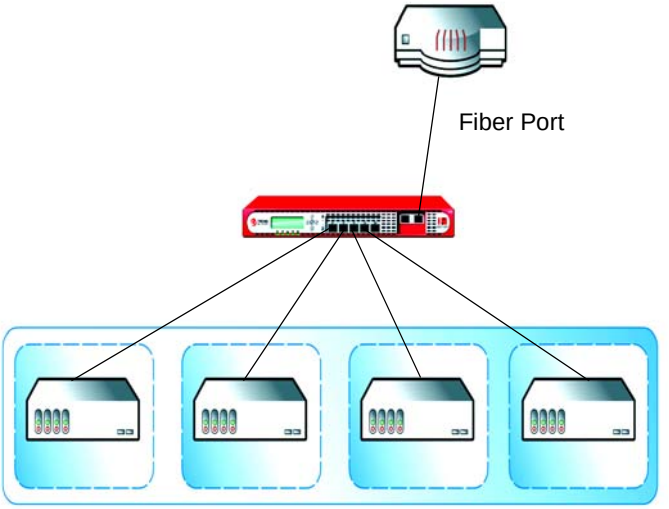


FIGURE 3-10. Port grouping without failover, multi-protection zone configuration, and 1 fiber port

Failopen Considerations

Consider the following points when implementing port grouping or port redundancy:

- If there is no power supplying a device (that is, the AC power receptacle is disconnected from the power outlet or actual device), failopen will not work. However, if you have 2 fiber bypass cards installed, the failopen function on these bypass cards will continue to work without power.
- The total length of the network cable connecting ports 1 and 2 to other devices must not be more than 100 meters (328 feet) for copper port connections.

Note: This constraint only applies to failopen deployments. The network cable connecting port 1 should be equal to or shorter than 50 meters. Consequently, the network cable connecting port 2 should be equal to or shorter than 50 meters. Otherwise, a cable that is longer than the maximum length will prevent failopen from working (because the natural electrical resistance of a copper wire of that length would slow down the signal too much).

- If you implemented port grouping with failover or port redundancy with failover, the device automatically disables failopen.
- If you configure failopen with the fiber bypass cards, failopen settings must be in the following pairs:
  - Ports 1 and 2
  - Ports 6 and 7
  - Ports 8 and 9

  You cannot split the pairs. For example, setting port 1 and port 6 to failopen does not work.

User-defined Port Grouping with Failover Deployment

There are two devices in a failover pair. These devices enforce the same security policy and share the same configuration settings. A failover pair must have the same model and be running the same Network VirusWall Enforcer 2500 program file version.

Tip: In a failover pair, if the one device fails, all traffic goes through the other device. Refer to the *Administrator's Guide* for details on failover and other high availability concepts.

Figure 3-11 illustrates how to set the interfaces for this type of deployment. In this example, port 3 is the failover port.

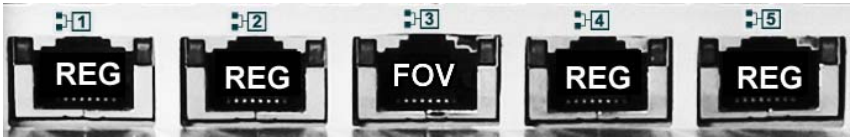


FIGURE 3-11. Interface allocation for a port grouping with failover deployment

Figure 3-12 illustrates a port grouping with failover deployment applied to a partial mesh topology.

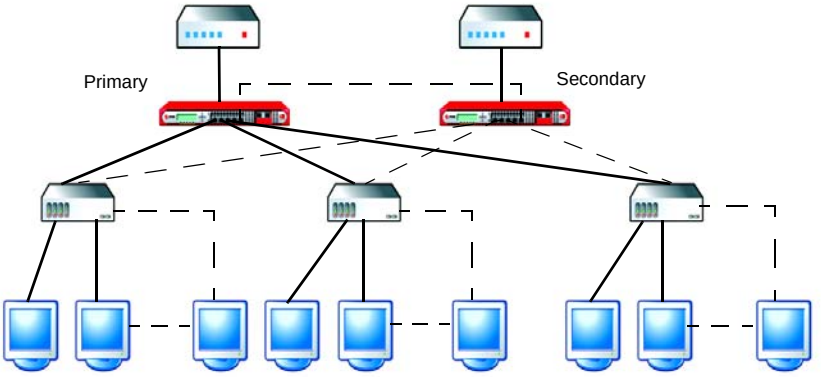


FIGURE 3-12. Port grouping with failover deployment, partial mesh

The following points apply to a port grouping with failover deployment:

- One **FAILOVER** port exists, which connects to the other device in a failover pair via an RJ-45 crossover cable
- The failover pair has one **PRIMARY** device and one **SECONDARY** device
- Both devices filter network packets
- If the Primary device is the Management device and it fails, the Secondary device becomes the device that filters all traffic
- A device that is not the **MANAGEMENT** device cannot be configured through the Preconfiguration or the Web console

  The **MANAGEMENT** device replicates the configuration setting and updates the antivirus components (except the program file) to the other device.
- The failover link allows both devices to have identical configuration settings

---

Note: However, stateful failover does not apply to the Network Scan Engine component. Refer to *Understanding the Network VirusWall Enforcer 2500 Security Components* in the *Administrator's Guide* for details on components.

- The device disables failopen (LAN bypass) in a failover environment.

In partial mesh design only the connection between Access L2 and distribution L3 switches has redundant links (*Figure 3-17*). The connection between distribution L3 and L3 access switches has only single link.

You can install two Network VirusWall Enforcer 2500 devices between L2 and L3 switches or distribution L3 switches and L3 access switches by linking them together using a failover link. In this deployment scenario, the two devices start to synchronize the information and you manage the **MANAGEMENT** device through the Web console. *Figure 3-13* illustrates this deployment scenario.

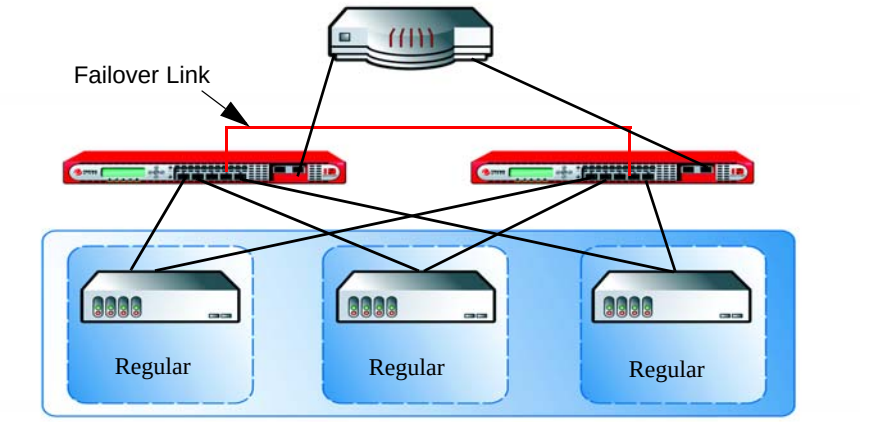


FIGURE 3-13. Port grouping with failover, multi-protection zone configuration, and 1 fiber port

Failover Considerations

Consider the following points when implementing a failover-based deployment:

- A Network VirusWall Enforcer 2500 failover pair must consist of identical devices– same model and running the same Network VirusWall Enforcer 2500 program file version

  Otherwise, the failover solution cannot work.

- Check whether the switches connected to the devices have Spanning Tree Protocol (STP) enabled

  If STP is not enabled and a failover pair is deployed in the network, packets would loop for an indefinite period in networks with physically redundant links.

- Do not automatically update the program file for the devices in a failover pair

  Doing so alters the identical settings for the failover devices, which consequently causes the failover link to be disconnected. Refer to *Updating the Program File Manually in a Failover Deployment* in the *Administrator's Guide* for instructions to manually update the program file.

Network VirusWall Enforcer 2500 disables failopen (LAN bypass) in a failover environment

Deployment Scenario I: Single Pair Configuration with or without 802.1q VLAN (Only Dual Port Multi-mode Fiber)

Case 1: Without Failover

In this deployment scenario an NVW fiber-optic port connects to an L2 switch (or segment) through a VLAN trunked link as the protection zone. The fiber-optic port connects to an external L2 or L3 switch.

Figure 3-14 illustrates this deployment scenario.

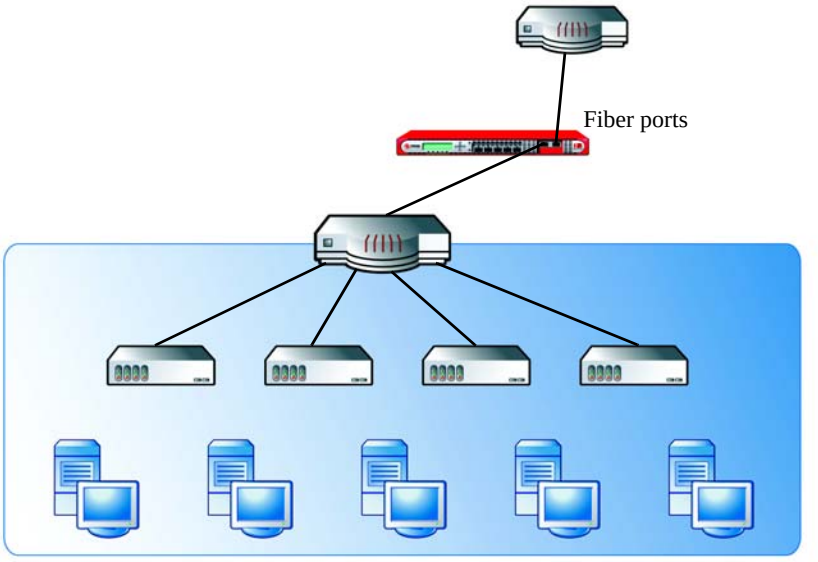


FIGURE 3-14. Single pair configuration with or without 802.1q VLAN

Case 2: With Failover

In this scenario two L2 or L3 switches configure as a port-to-port channel. The redundant uplinks of the L2 switch connect to two individual NVW devices. Failover port—for example, copper 5.

Figure 3-15 illustrates this deployment scenario.

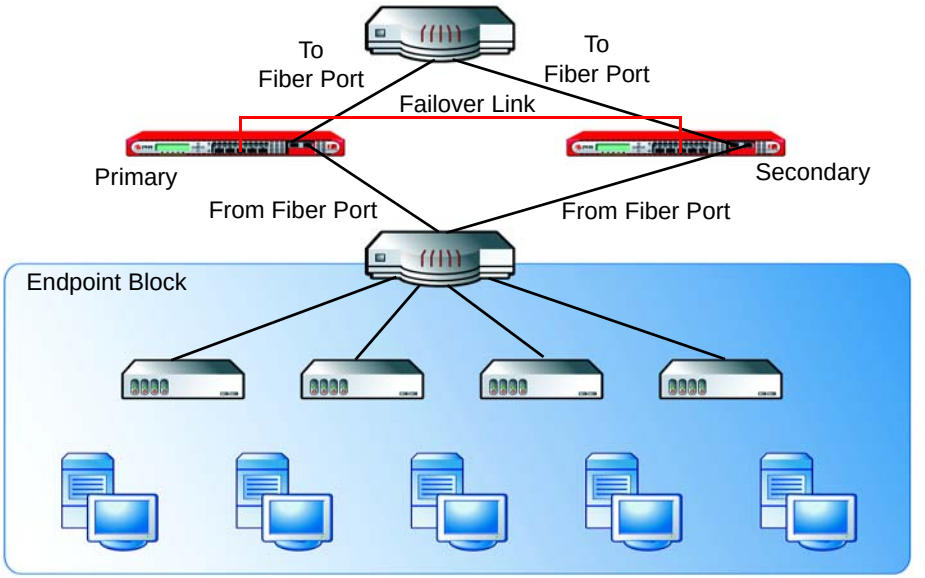


FIGURE 3-15. Case 2: Failover pair with single-switch dual-port multi-mode fiber

User-defined Port Redundancy Deployment

Port redundancy deployment supports topologies with switches that have redundant links to a public network. Two port groups compose a redundant connection.

Figure 3-16 illustrates how to allocate the interfaces for this type of deployment.

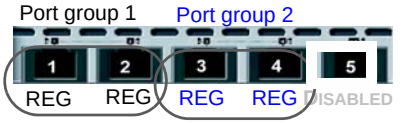


FIGURE 3-16. Interface allocation for a port redundancy deployment

Using a redundant physical link implementation allows the device to help secure maximum network uptime and reliability. For example, you could have the following port configuration:

- Port 1 is the default port that interfaces to the switch connecting to an external network
- Port 2 is the default port that interfaces to the switch connecting to an internal network
- Port 3 is the redundant interface to the external network
- Port 4 is the redundant interface to the internal network

Figure 3-17 represents a port redundancy deployment.

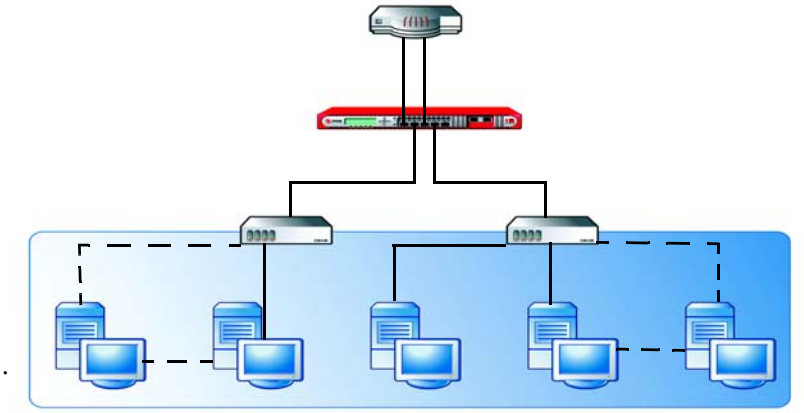


FIGURE 3-17. Port redundancy deployment

The following points apply to a port redundancy deployment strategy:

- Two port groups are available– port group 1and port group 2
- If you enable failopen, the device automatically applies failopen in this mode
- If a Layer 2 or Layer 3 device fails, the network traffic is still routed to same Network VirusWall Enforcer 2500 device
- Network VirusWall Enforcer 2500 supports the spanning tree protocol (STP). As described in the STP standard, STP allows only one active path at a time between any two network devices but establishes a redundant link as a backup. In other words, if one of the links fails, the device can still keep the network connection alive through the redundant link.

  Note: Verify whether the switches deployed in the network have STP enabled. Refer to the device documentation for details on how to enable STP. The device does not refresh its MAC address table if one of the links fails. This results to a temporary delay in the packet delivery.

- If the device fails, Network VirusWall Enforcer 2500 enables ports 1 and 2 for failopen

- Port Redundancy can support failopen. Enable or disable failopen through the Preconfiguration console

  See *Failopen Considerations* on page 3-20 for more information.

- the device needs to adjust its settings whenever the STP table is changed

  As a result, the network traffic may be blocked. The length of time when the network is blocked depends on the L2 or L3 device's MAC address timeout.

User-defined Port Redundancy Considerations

Consider the following points when implementing a port redundancy deployment:

- A redundant group must include two port groups
- Each port group can contain ports and port attributes
- Each port group can possess configurable attributes—you can choose whether to configure settings for a port group
- Packets cannot be routed into different port groups
- Configure the **FAILOVER** port as a separate port, which should not belong to any port group (see *Failover Considerations* on page 3-25 for details)

Deployment Scenario II: Point-to-Point Links with Dual-Port Multi-mode Fiber-optic Server Adapter

Two Pairs of Fiber-Copper Port Without Failover

In this deployment scenario two fiber ports replace the on-board copper external ports and external and internal ports connect to the uplink and downlink switches via two individual links.

Figure 3-18 illustrates this deployment scenario.

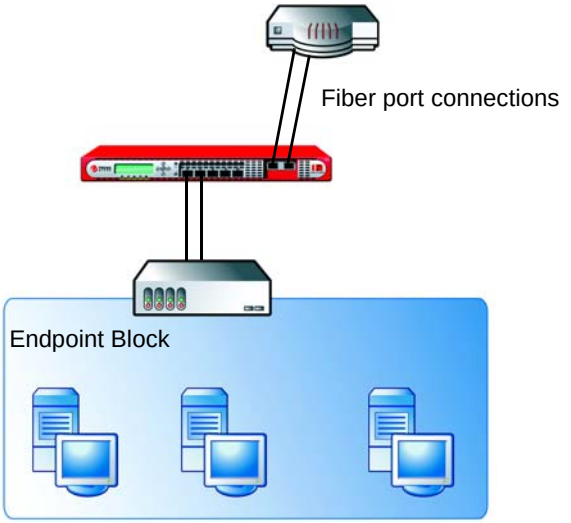


FIGURE 3-18. Point-to-point links using two pairs of fiber-copper ports

One Pair of Copper Ports with One Pair of Fiber Ports Without Failover

Two fiber ports can act as another port pair for redundancy.

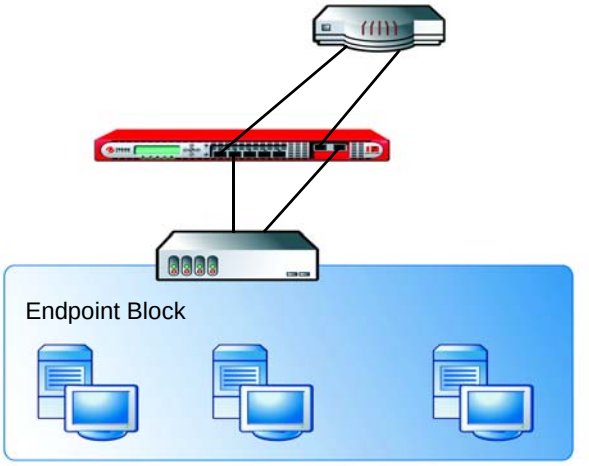


FIGURE 3-19. Point-to-point links—one pair of copper ports with one pair of fiber ports

Port Redundancy with Failover Deployment

To maximize the benefit of port redundancy, configure high availability along with the port groups. Doing so helps guarantee that if one of the device fails, all functions of the matching devices are maintained. This option allows uninterrupted packet filtering capabilities.

Port redundancy with failover deployment requires two port groups and a failover port. The following figure illustrates the interface allocation.

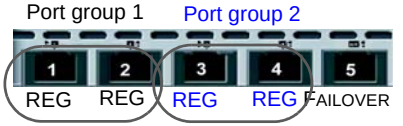


FIGURE 3-20. Interface allocation for a port redundancy with failover deployment

Trend Micro recommends implementing a port redundancy with failover deployment in a full mesh topology. *Figure 3-21* illustrates this strategy.

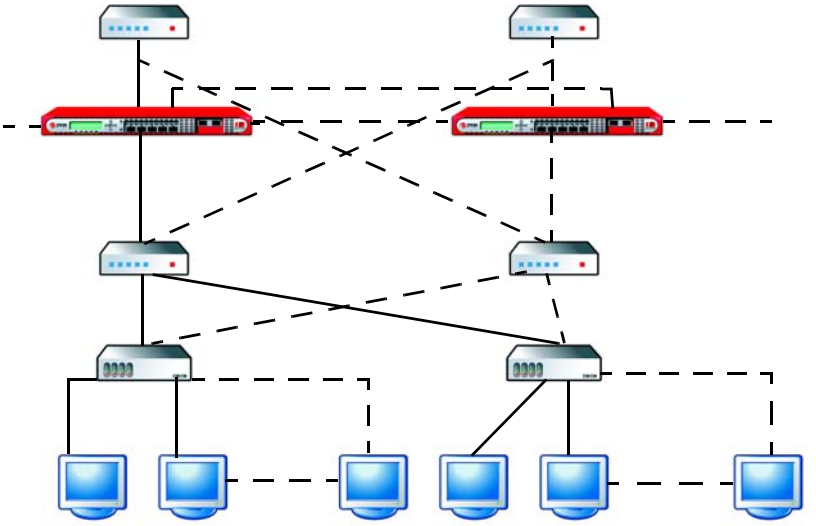


FIGURE 3-21. Port redundancy with failover deployment on a full mesh topology

The following points apply to a port redundancy with failover deployment:

- Two port groups and a failover port are available—port group 1, port group 2, and the **FAILOVER** port
- The two devices in a failover pair must be the same model and running the same image
- If one device in the failover pair fails, the L2 or L3 device blocks the port connected to the failed Network VirusWall Enforcer 2500 device and redirects traffic to the other device
- Both devices can filter network packets
- You can only configure the **MANAGEMENT** device and the device replicates the configuration to the other device
- To view the non-**MANAGEMENT** device status, log in to the Web console for that device
- To determine the failover status of both devices, each device polls the other every one (1) second

Tip: See *Failover Considerations* on page 3-25 for more information about failover.

To configure port redundancy with failover, assign the fifth port as the failover port and connect the device to another NVW device. For example, **FAILOVER** port—copper 5.

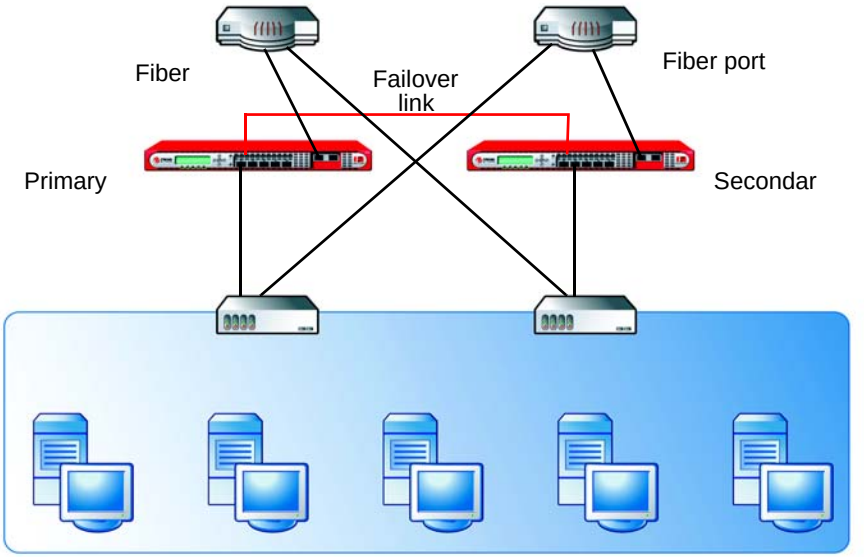


FIGURE 3-22. L2 redundant links: two pairs of fiber-copper ports with failover

You can also configure the device to have port redundancy by using two fiber ports as another pair for redundancy.

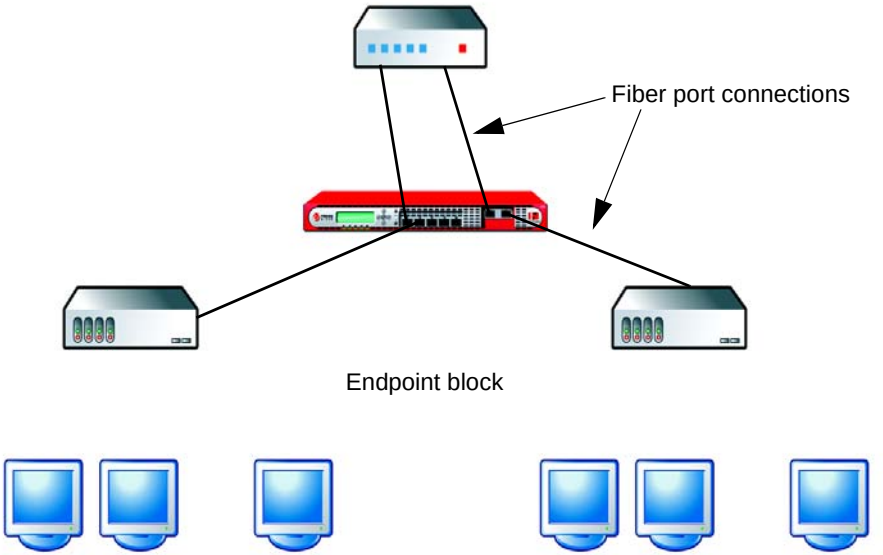


FIGURE 3-23. L2 redundant links: one pair of copper ports with one pair of fiber-optic ports without failover

When configuring the device to have port redundancy, you can use two fiber ports as another port pair for redundancy and the fifth port to connect to another identical device. For example, **FAILOVER** port—Copper 5.

Chapter 4

Preparing for Preconfiguration

Preconfiguring the device requires that you are connected to Network VirusWall Enforcer 2500.

This chapter contains the following topics:

- *Preparing for Preconfiguration* on page 4-2
- *Network VirusWall Enforcer 2500 Initial Tasks* on page 4-2

Preconfiguring Network VirusWall Enforcer 2500 requires the completion of related tasks.

To perform preconfiguration:

1. Plan and determine the deployment strategy (see *page 3-2*).
2. Prepare the device (see *page 4-2*).
3. Perform preconfiguration (see *page 5-1*).

Deploying Network VirusWall™ Enforcer 2500 on page 3-1 discusses step 1, the succeeding sections discuss step 2, and *Preconfiguring Network VirusWall Enforcer 2500* on page 5-1 provides instructions for step 3.

Preparing for Preconfiguration

Complete the following tasks before preconfiguring the device:

- If you are upgrading from a previous version of Network VirusWall refer to the *Network VirusWall Enforcer 2500 Upgrade Guide* before continuing.
- Network VirusWall Enforcer 2500 initial tasks (See *Network VirusWall Enforcer 2500 Initial Tasks* on page 4-2).

Network VirusWall Enforcer 2500 Initial Tasks

Complete the following tasks before you preconfigure Network VirusWall Enforcer 2500:

- Test the failopen functionality
  This ensures network traffic can still pass through the device when the later encounters a hardware or system error that prevents it from filtering network packets.
- Determine the `admin` account password

Tip: There are three accounts available– `Admin`, `PowerUser`, and `Operator`. All accounts use `admin`, `poweruser`, and `operator`, respectively, as their default password.

- Determine the managed product host name for the device or devices in a failover pair.
- Prepare a computer that has terminal communications software, such as HyperTerminal for Windows (See *Preparing the Preconfiguration Console* on page 5-6).

Verifying Network Support

Use the following list to verify whether your environment can support Network VirusWall Enforcer 2500:

- Enable STP (spanning tree protocol) for switches deployed in the network if you will configure port grouping.

  When one of the links fails, the device will be able to determine which path to take through the spanning tree protocol (STP). Refer to the documentation that comes with your STP device for details on how to enable STP.

- In a failopen deployment, the total length of the network cable connecting ports 1 and 2 to other devices must not be longer than 100 meters (328 feet).

  A cable that is longer than the maximum length will prevent failopen from working. See *page 3-20* for additional failopen considerations.

Chapter 5

Preconfiguring Network VirusWall Enforcer 2500

This chapter contains the following topics:

- *Understanding Preconfiguration* on page 5-2
- *Choosing the Preconfiguration Method* on page 5-3
- *Performing Preconfiguration Using the Preconfiguration Console* on page 5-5
- *Performing Preconfiguration Using the LCD Module* on page 5-16
- *Connecting to the Network* on page 5-18
- *Configuring Network VirusWall Enforcer 2500* on page 5-19

Preconfiguring a Network VirusWall Enforcer 2500 device requires the completion of the following tasks:

1. Select the console to use during preconfiguration (see *page 5-3*).
2. Prepare and access the Preconfiguration console (see *page 5-6*).
3. Configure device settings (see *page 5-11*).
4. Set the interface speed and duplex mode (see *page 5-14*).

Understanding Preconfiguration

As stated in *Preparing for Preconfiguration* starting on page 4-1, preconfiguring the device requires the completion of Network VirusWall Enforcer 2500-related tasks.

To perform preconfiguration:

1. Plan and determine the deployment strategy (see *Deploying Network VirusWall™ Enforcer 2500* on page 3-1).
2. Perform preconfiguration (see instructions starting on *Using the Preconfiguration Console* on page 5-3).
3. Perform configuration tasks (see *Configuring Policy Enforcement and Device Settings* in the *Administrator's Guide*).

After completing the initial configuration tasks (see *Preparing for Preconfiguration* on page 4-1), use the Preconfiguration console to proceed with preconfiguration.

After the preconfiguration procedure of the device is complete, you can then administer Network VirusWall Enforcer 2500 using the Web console. Refer to *Configuring Policy Enforcement and Device Settings* of the *Administrator's Guide*.

Choosing the Preconfiguration Method

Preconfigure the device through the:

- Preconfiguration console
- LCD module (also known as the LCM console)

Using the Preconfiguration Console

The Preconfiguration console is a terminal communications program that allows you to configure or view any preconfiguration setting. These settings include:

- Interface settings
- Network settings
- System logs

Examples of a terminal interface are HyperTerminal for Windows. To access the Preconfiguration console remotely using SSH, use Putty or Secure Shell Client applications.

Using the terminal interface, you can preconfigure all device settings. If you do not have access to a computer with terminal communications software, use the LCD module panel to perform preconfiguration. See *Performing Preconfiguration Using the Preconfiguration Console* on page 5-5 for details on how to use the Preconfiguration console.

Using the LCD Module

Use the LCD and control panel on the front of the device to configure only Network VirusWall Enforcer 2500 network settings, such as the IP address. See *Performing Preconfiguration Using the LCD Module* on page 5-16 for details on how to use the LCD module.

For a comparison of these two methods, see *Table 5-1*.

WHAT YOU CAN DO	PRECONFIGURATION CONSOLE	LCD MODULE
Set the Network VirusWall Enforcer 2500 IP address, netmask, Gateway address, and DNS addresses	•	•
Lock/unlock LCD module panel controls	•	
View system logs	•	
Initialize the device to default settings	•	
Reset the device	•	•
Restore default settings (factory settings)	•	
Configure the interface speed and duplex mode	•	
View device settings	•	
Enable/disable SSH access	•	
Enable/disable failover	•	
Pattern/Engine rollback	•	
Allow changes to take effect immediately	(Need to log off)	•
Register to Control Manager	•	
Configure Native VLAN ID	•	

TABLE 5-1. Comparison of available consoles for preconfiguration

Performing Preconfiguration Using the Preconfiguration Console

Preconfiguring the device using the Preconfiguration console requires the completion of the following tasks:

Tip: Check whether you have completed the *Network VirusWall Enforcer 2500 Initial Tasks* on page 4-2 before starting with the following steps.

1. Prepare the Preconfiguration console (see *page 5-6*).
2. Log on to the Preconfiguration console (see *page 5-7*).
3. Configure the device settings (see *page 5-11*).
4. Set the interface speed and duplex mode (see *page 5-14*).

Preparing the Preconfiguration Console

The computer you choose for preconfiguration must have terminal configuration software such as HyperTerminal for Windows.

To prepare the Preconfiguration console:

1. Connect one end of the included console cable to the **CONSOLE** port on the back panel of the device and the other end to the serial port (COM1, COM2, or other COM port) on a computer.
2. Open HyperTerminal.
   a. Click **Start > Programs > Accessories > Communications > HyperTerminal**.

      HyperTerminal prompts you for location information.

   b. Click **Cancel** when prompted for dial-up location information.

   c. Type the information and press **ENTER** to type information in the terminal interface.

      Tip: Trend Micro recommends configuring HyperTerminal properties so that the backspace key is set to delete.

   d. On the HyperTerminal window, click **File** > **Properties**.

   e. Click the **Settings** tab.

   f. Under **Backspace key sends**, select **Del**.
3. To prepare HyperTerminal for optimal use, set the following properties:
   - **Bits per second:** 115200
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop bits:** 1
   - **Flow control:** None
   - **Emulation**: VT100

Logging on the Preconfiguration Console

After preparing the terminal application, you are ready to access the Preconfiguration console.

To access the Preconfiguration console:

1. Power on the device and wait for a welcome message to appear on the LCM panel (approximately 1-2 minutes).

   To power-on a device:

   a. Connect the power cord to the DC power receptacle.

   b. Connect the power cord to an electrical outlet.

   Tip: See *Power Requirements and Environmental Specifications* on page 1-8 for device power requirements and environmental specifications.

   c. Push the power switch to the **On** position. The Welcome message appears when the system is successfully powered on.

2. Press **ENTER**. The **User name** logon prompt displays. If the screen does not display, type Ctrl + 'R' or Ctrl + 'L'.

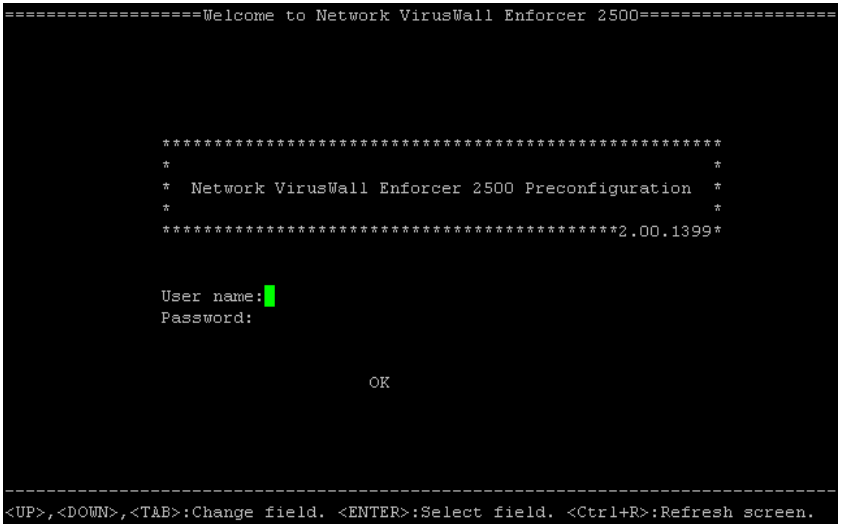


FIGURE 5-1. The Preconfiguration console logon prompt

3. Type the default administrator user name and its corresponding password:

   User name: `admin`

   Password: `admin`

   Note: Change the default password to a secure password immediately after logging for the first time. Only administrators and power users can login to the Preconfiguration console. *Modifying the Preconfiguration Console Accounts* in the *Administrator's Guide* provides details about the `admin` and `poweruser` accounts.

   Use this login for full access to all preconfiguration features.

   Tip: See *admin password misplaced or forgotten* on page 6-2 for tips on how to troubleshoot a missing or forgotten password.

4. After logging on, the **Main Menu** appears.

Note: The Preconfiguration console has a timeout value of 3 minutes. If the console is idle for three minutes, it automatically logs off the account. After 3 attempts to login, there will be a short time period before you can try again.

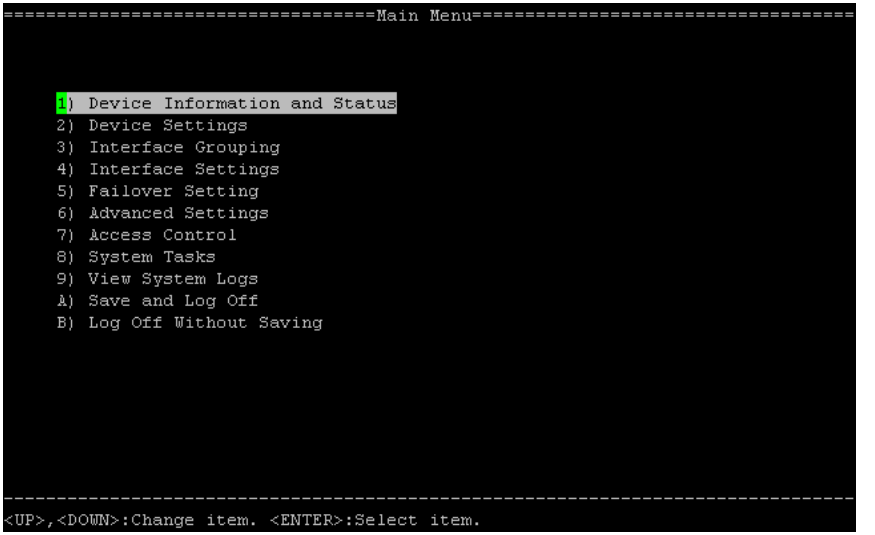


FIGURE 5-2. The Preconfiguration console Main menu

For instructions on how to log off the Preconfiguration console, see *page 5-15*.

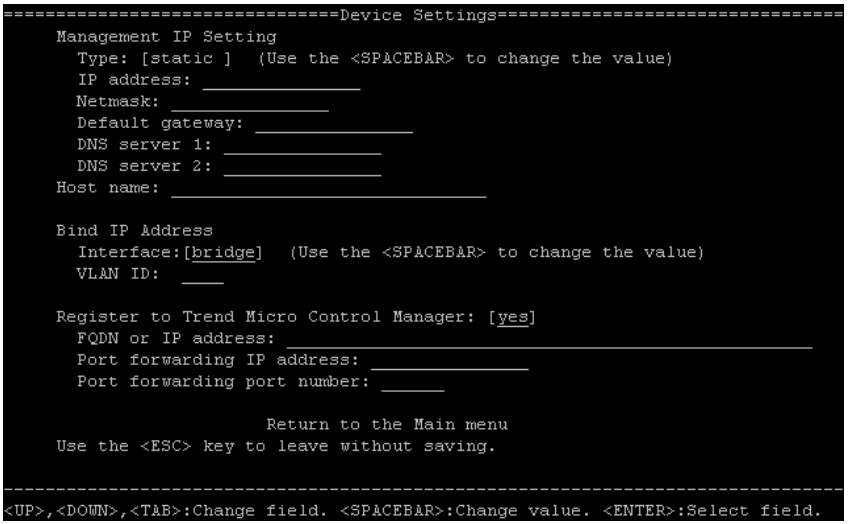
Tip: Proceed by configuring the device settings, which include the device host name and IP settings.

Configuring Device Settings

Immediately after logging onto the Preconfiguration console for the first time, change the default password to a secure password from the Web console. After changing the password, use the **Device Settings** menu to configure the Network VirusWall Enforcer 2500 host name that appears on the Web console and the Network VirusWall Enforcer 2500 network settings.

To configure the device settings:

1. On the **Main Menu** of the Preconfiguration console, type 2 to select **Device Settings**. The Device Setting Summary appears.



Note: When configuring the device for the first time, the factory default settings appear.

2. Type a host name that properly represents the device in the network.

   Each device on your network must have a unique host name. Control Manager uses this unique host name during registration and as the managed product name.

   Host names may be up to 30alphanumeric characters (spaces not allowed). Trend Micro recommends a unique descriptive host name to represent and identify the device or devices in a failover pair locally (through the front panel LCD module) or remotely (through the management console). For example, designate NVW2500-NY-main as the host name for the failover pair protecting the New York main office.

3. Type or select the Management IP setting details under Management IP settings.

WARNING! *If there is a NAT device in your environment, Trend Micro recommends assigning a static IP address to the device. Because different port settings are assigned from your NAT, your device may not work properly if dynamic IP addresses are used.*

---

4. After specifying the network settings, press **ENTER**.

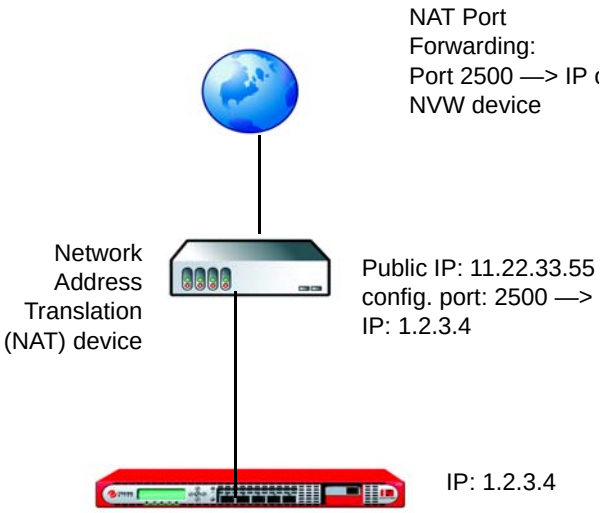


FIGURE 5-3. Network VirusWall Enforcer 2500 deployment in a network environment using a NAT device (with sample IP address and port)

Note: You need to configure the port forwarding on the NAT device. Configure port forwarding according to the settings.

---

5. Log back on to the Web console using the administrator name and password.

Note: System logs contain information useful for troubleshooting. If you experience issues with the device and contact Trend Micro support, you may be asked to view the system log. Refer to *Viewing Status, Logs, and Summaries* and *Troubleshooting* in the *Administrator's Guide* for more details about troubleshooting.

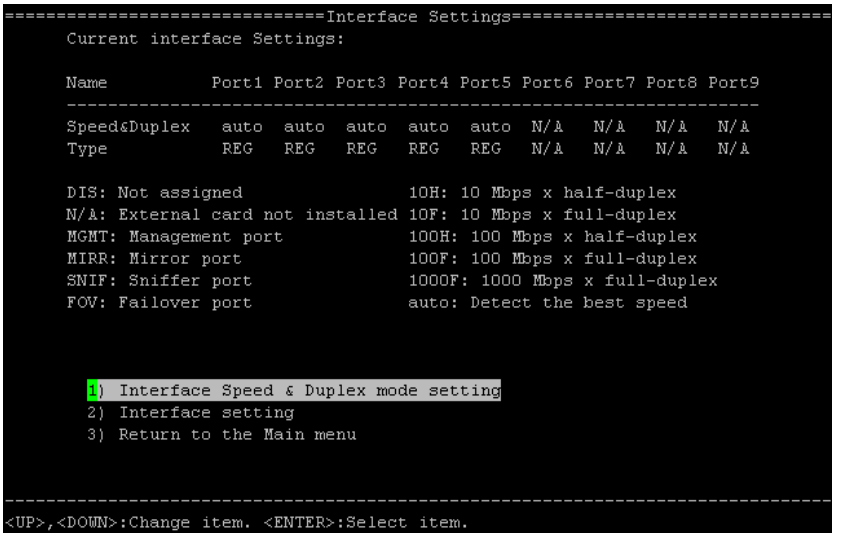
Setting the Interface Speed and Duplex Mode

Use the Preconfiguration console to configure the interface speed and duplex mode.

Note: Both the connected L2/L3 and Network VirusWall Enforcer 2500 devices should have the same interface setting and duplex mode. Otherwise, the half-duplex mode setting will take effect. Apply **100Mbps x full-duplex** for both the switch and Network VirusWall Enforcer 2500 device.

To set the interface speed and duplex mode:

1. On the **Main Menu** of the Preconfiguration console, type 4 to select **Interface Speed**. The Interface Settings Screen appears.



2. Type 1 to select **Interface speed & duplex mode setting**.

   The **Interface speed & duplex mode setting** screen displays the current interface speed and duplex setting for all ports.
3. Select the port by using the up and down arrows.
4. Select the speed by using the space bar to scroll through the speed options.

5. Select **Return to the previous menu**. The **Interface Settings** screen displays.
6. Type 3 to select **Return to Main menu**. The **Main Menu** displays.
7. Select **Save and Log Off** for changes to take effect.

Logging off the Preconfiguration Console

Log off the Preconfiguration console after completing preconfiguration or modifying settings (for example, device settings) that require logging off for changes to take effect.

To log off the Preconfiguration console:

1. On the **Main Menu** of the Preconfiguration console, select **Save and Log Off**. A confirmation message appears.
2. Select **OK** and press **ENTER** to log off.

Note: In order to apply new settings, you must log off Network VirusWall Enforcer 2500.

Performing Preconfiguration Using the LCD Module

With the LCD console, you can only configure the device's IP address. Use the terminal interface for access to all preconfiguration options (see *Comparison of available consoles for preconfiguration*).

There are five buttons on the LCD console:

- **Up arrow** – cycle forward through the alphanumeric characters displayed on the LCD
- **Down arrow** – cycle backward through the alphanumeric characters displayed on the LCD
- **Left arrow** – move the focus or cursor to the left
- **Right arrow** – move the focus or cursor to the right

Tip: Use the **Left** and **Right** arrows to read the logs displayed on the LCD module.

- **ENTER** – confirm selection or input

Note: The LCD module and keypad do not work when the system is powered off (even if the device is plugged in to an AC power source).

To configure the IP address through the LCD module:

1. Press **ENTER** ( ). The Main Menu appears.
2. Use the down arrow ( ) to select **Configure NVW**. A prompt displays asking if you want to change settings.

Tip: The LCD module times out in three (3) minutes if there is no activity initiated using the Control Panel.

---

3. To continue, ensure that a star (*) is next to `Yes`. To abort, move the star (*) to the `No` position:

   ```
   (*) Yes  ( ) No
   ```

4. Press **ENTER** ( ).
5. If you selected `Yes`, a prompt displays asking to have the IP address dynamically assigned.

   To use a dynamic IP address, do the following:

   a. Ensure that a star (*) is next to `Yes` and press **ENTER** ( ):

   ```
   (*) Yes  ( ) No
   ```

   b. Type the Management server **IP address**.

   To manually enter a static IP address, do the following:

   a. Ensure that a star (*) is next to `No` and press **ENTER** ( ):

   ```
   ( ) Yes  (*) No
   ```

   b. Type the new **IP address**, **netmask**, **Gateway address**, and **DNS server addresses**.

   c. Type the Management server **IP address**.

6. Press **ENTER** ( ) to save the settings when prompted.

The device restarts to apply the new settings.

Connecting to the Network

Be sure to preconfigure the device before attempting to connect the device or devices in a failover pair. After preconfiguration, switch off the device before connecting it to the network.

To connect the device to your network:

1. Connect one end of a 10/100Mbps Ethernet cable to a **REGULAR** port and the other to a segment of your network
2. In a failover deployment, establish the failover pair by connecting the provided Ethernet cable (RJ-45 crossover or a regular LAN cable) to the designated failover port of both devices.
3. Power on the device (see *page 5-7*).

Note: Network VirusWall Enforcer 2500 can handle various interface speed and duplex mode network traffic. See *Setting the Interface Speed and Duplex Mode* on page 5-14.

Configuring Network VirusWall Enforcer 2500

After preconfiguring Network VirusWall Enforcer 2500, you are ready to configure the device and commence network protection.

Trend Micro recommends performing the following tasks after preconfiguring a device:

- Update components
- Change user password
- Configure Policy Enforcement

Refer to the following documentation for related instructions:

- *Network VirusWall Enforcer 2500 Administrator's Guide*– includes instructions on how to configure and administer the device from the applicable management tools

  See *Getting Started with Network VirusWall Enforcer 2500* in the *Administrator's Guide* for recommended instructions.
- *Network VirusWall Enforcer 2500 Online Help*– provides instructions on how to configure Network VirusWall Enforcer 2500 devices Web console

See *Preface* on page v for a complete description of Network VirusWall Enforcer 2500 documentation.

Chapter 6

Troubleshooting Preconfiguration

This chapter addresses troubleshooting issues that may arise during the device preconfiguration.

Tip: Refer to the *Network VirusWall Enforcer 2500 Administrator's Guide* in the *Trend Micro Solutions CD for Network VirusWall Enforcer 2500* for additional FAQs and troubleshooting.

This chapter contains the following topics:

- *Device Issues* on page 6-2
- *Contacting Technical Support* on page 6-3

Note: *Troubleshooting* in the *Administrator's Guide* has more details regarding Control Manager and Network VirusWall Enforcer 2500 integration troubleshooting.

Device Issues

#	Issue	Corrective Action/Explanation
1	`admin` password misplaced or forgotten	Use the Application Firmware Flash Utility to reload the Network VirusWall Enforcer 2500 image. **Note:** Reloading the Network VirusWall Enforcer 2500 image will restore the default settings. Trend Micro recommends exporting the configuration first before reloading the image.
2	LEDs do not illuminate	Verify secure power cable and network cable connections. If the error persists, there may be a hardware issue. Contact your vendor. See *LED Indicators* on page 1-5 for details on the Network VirusWall Enforcer 2500 LED.
3	Unable to access the Preconfiguration console	Verify secure console port connections and terminal communications software settings. See *Preparing the Preconfiguration Console* on page 5-6 for details on setting the terminal communications software settings.
4	Unable to change settings with the LCD module panel	Verify whether the LCD module configuration is set to ON. Otherwise, the OFF LCD module configuration state will prevent you from configuring Network VirusWall Enforcer 2500 through the LCD module. In addition, to change settings with the LCD module panel, you must first press and hold down the return button  . **Tip:** Refer to *Changing the LCD Module Configuration* in the *Administrator's Guide* for instructions on how to toggle this setting. If an issue with any LCD module buttons persists, the hardware may need to be repaired. Contact your vendor.
5	The network packet delivery is too slow and seems to be blocked	Network VirusWall Enforcer 2500 does not refresh its MAC address table if one of the links fails. The result is a temporary delay in packet delivery.

Contacting Technical Support

If the issue still persists despite following the troubleshooting tips provided in *Troubleshooting Preconfiguration*, refer to *Getting Support* in the *Administrator's Guide* for instructions on how obtain technical support.

Appendix A

Ethernet Cable Usage Guidelines

This chapter describes the different cable combinations you must use with different deployments.

This chapter contains the following topics:

- *Network VirusWall Enforcer 2500 in Normal Mode* on page A-2
- *Network VirusWall Enforcer 2500 in Failopen Mode with Standard Copper Ports 1 to 5* on page A-4
- *Network VirusWall Enforcer 2500 in Failopen Mode with Bypass Card Copper Ports* on page A-6

Network VirusWall Enforcer 2500 in Normal Mode

This section lists the cables to use when Network VirusWall Enforcer 2500 is not set to failopen.

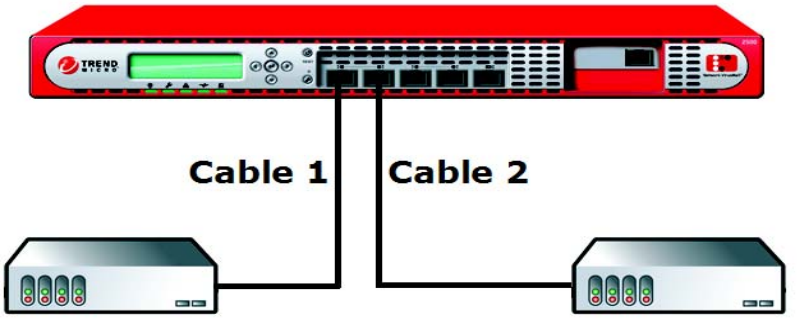


FIGURE A-1. Network VirusWall Enforcer 2500 in Normal Mode

Switch Configuration								
			Copper					
Speed			Auto	10	10	100	100	1000
Duplex				Half	Full	Half	Full	Full
Device copper port configuration			↕	↕	↕	↕	↕	↕
	Speed	**Duplex**						
Copper	Auto		1000 Full Both	10 Half Both	10 Full Both	100 Half Both	100 Full Both	1000 Full Both
	10	Half	10 Half Both	10 Half Straight				
	10	Full	10 Half Both		10 Full straight			
	100	Half	100 Half Both			100 Half Straight		
	100	Full	100 Half Both				100 Full Straight	
	1000	Full	1000 Full both					1000 Full straight

TABLE A-2. Network VirusWall Enforcer 2500 in Normal Mode

An explanation of the terms used in the table:

- Both—Use straight through cables or crossover cables for cable 1 and cable 2
- Straight—Use straight through cables only for cable 1 and cable 2
- Crossover—Use crossover cables for cable 1 and cable 2

Network VirusWall Enforcer 2500 in Failopen Mode with Standard Copper Ports 1 to 5

This section lists the cables to use when Network VirusWall is set to failopen with switches connected to standard factory copper ports 1 to 5.

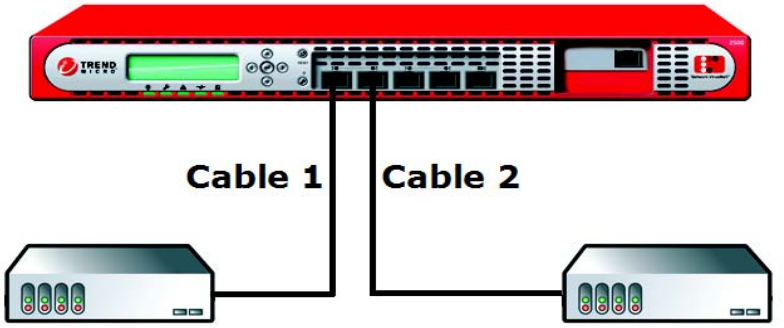


FIGURE A-3. Network VirusWall Enforcer 2500 in Failopen Mode

Switch Configuration								
			Copper					
Speed			Auto	10	10	100	100	1000
Duplex				Half	Full	Half	Full	Full
Device copper port configuration			↕	↕	↕	↕	↕	↕
	Speed	Duplex						
Copper	Auto		1000 Full Both	10 Half S&C	10 Full S&C	100 Half S&C	100 Full S&C	1000 Full S&C
	10	Half	10 Half Both	10 Half S&C				
	10	Full	10 Half Both		10 Full S&C			
	100	Half	100 Half Both			100 Half S&C		
	100	Full	100 Half Both				100 Full S&C	
	1000	Full	1000 Full both					1000 Full S&C

TABLE A-4. Network VirusWall Enforcer 2500 in Normal Mode

An explanation of the terms used in the table:

- Both—Use straight through cables or crossover cables for cable 1 and cable 2
- S&C—One of the cables must be either straight through or crossover for cable 1 and cable 2

Network VirusWall Enforcer 2500 in Failopen Mode with Bypass Card Copper Ports

This section lists the cables to use when Network VirusWall Enforcer 2500 is set to failopen with switches connected to bypass card copper ports.

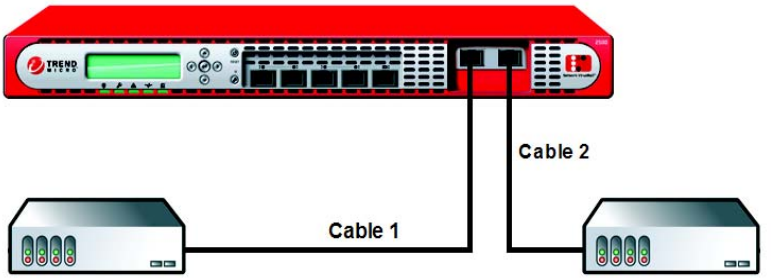


FIGURE A-5. Network VirusWall Enforcer 2500 in Failopen Mode with bypass card copper ports

Switch Configuration								
			Copper					
Speed			Auto	10	10	100	100	1000
Duplex				Half	Full	Half	Full	Full
Device copper port configuration			↕	↕	↕	↕	↕	↕
	Speed	Duplex						
Copper	Auto		1000 Full Both	10 Half S or C	10 Full S or C	100 Half S or C	100 Full S or C	1000 Full S or C
	10	Half	10 Half Both	10 Half S or C				
	10	Full	10 Half Both		10 Full S or C			
	100	Half	100 Half Both			100 Half S or C		
	100	Full	100 Half Both				100 Full S or C	
	1000	Full	1000 Full both					1000 Full S or C

TABLE A-6. Network VirusWall Enforcer 2500 in Normal Mode

An explanation of the terms used in the table:

- Both—Use straight through cables or crossover cables for cable 1 and cable 2
- S or C—Use straight through or crossover cables for both cable 1 and cable 2

Index

A

Administrator's Guide ii
appliance 2-2
architecture 2-2
audience iv

C

cable
  Ethernet 1-3
connections
  to the network 5-18
connectors
  ports 1-7
considerations
console
  cable 1-3
contingency plan 3-16

D

deploying Network VirusWall Enforcer
  overview 2-6
deployment
  number of devices 3-15
  planning 3-2
  port grouping with failover 3-21, 3-28
  port redundancy 3-28
  port redundancy with failover 3-33
  scenario 3-18
  strategy redesign 3-17
device 2-2
device settings
  configuring 5-11
document conventions iv
documentation ii
duplex mode 5-18

E

ethernet cable 1-3
evaluating your pilot 3-16

F

failopen 2-3
  considerations
    network cable length 3-20
    power supply 3-20
failover 2-3–2-4, 3-21, 3-33
  considerations
    disabling failopen 3-25
    failover pair 3-25
    Spanning Tree Protocol 3-25
    STP 3-25
Firmware Flash Utility 1-3

G

Getting Started Guide ii
  about iii
Glossary 2-3
GSG. See Getting Started Guide.
guest clients 3-9

H

HyperTerminal 4-2

I

interface speed 5-18
IP address
  static 5-12
issues
  accessing Preconfiguration console 6-2
  delayed delivery 6-2
  forgotten passwords 6-2
  MAC address table 6-2
  misplaced passwords 6-2
  password 6-2
  port redundancy 6-2
  Preconfiguration console 6-2
issues
  LCD module configuration 6-2
  LED 6-2

M

mounting 1-10

N

Network VirusWall Enforcer
- device settings 5-11
- mounting 1-10

Network VirusWall Enforcer 2500
- about the appliance 2-2
- Administrator's Guide ii
- components 2-2
- documentation ii
  - audience iv
  - conventions iv
- Getting Started Guide ii
- how it works 2-2
- introduction 2-2
- online help ii
- printed documentation iii
- protection 2-2
- tools 1-3

notes
- assembling rails 1-12
- cage nut 1-22
- control panel 5-16
- deployment with VPN 3-7
- duplex mode 5-14, 5-18
- failopen 3-20, 3-30
- failopen and port redundancy 3-30
- FAILOVER port 2-6, 3-23
- fixed mount 1-22
- image 6-2
- installing cage nuts 1-22
- interface speed 5-14, 5-18
- LCD module 1-4, 5-16
- LCM console 1-4, 5-16
- mounting 1-14
- network cable 3-20
- panel 5-16
- port 5 3-23
- port redundancy 3-29
- port redundancy and STP 3-29
- power supply 3-20
- Preconfiguration console 5-10
- rack cabinet length 1-14
- rail assembly 1-12
- reloading image 6-2
- saving configurations 5-15
- stateful failover 3-23
- STP 3-29
- system logs 5-13
- timeout 5-10
- Update Center ii
- updating Network Scan Engine 3-23
- using control panel 5-16
- using LCD module 5-16
- VPN 3-7

O

OLH ii

Online help ii

P

panel
- back 1-7
- front 1-4

password
- default 5-9

Pilot
- choosing a site 3-16
- conducting a pilot deployment 3-16

port grouping with failover 3-21

port redundancy 3-28

port redundancy with failover 3-33

power vent 1-7

Preconfiguration method 5-3

Preface i

R

rack mounting 1-10

remote clients 3-5

S

setting interface speed and duplex mode 5-14

Solutions CD 1-3

Speed 5-18

Static IP address 5-12

T

tips
- about this GSG 3-3

addresses 3-4
admin 4-2
before preconfiguring Network VirusWall Enforcer 5-5
checking package 1-2
control panel 5-16
documentation ii
FAQs 6-1
full mesh topology 3-34
glossary 2-3
host names length 5-12
HyperTerminal 5-6
LCD module timeout 5-17
monitor 4-2
mounting Network VirusWall Enforcer 1-10, 1-21
Network VirusWall Enforcer
  accounts 4-2
  host names 5-12
  initial tasks 5-5
  IP address 5-12
  mounting 1-10
positioning Network VirusWall Enforcer 3-5
powering on device 5-7
  preconfiguring 5-10
  rack space 1-21
  reading LCD module 5-16
  removing rack doors 1-21
  required rack cabinet space 1-21
  static IP address 5-12
  timeout 5-17
  troubleshooting 6-1
  using HyperTerminal 5-6
tools 1-3

U

unit 2-2
Update Center ii

V

vent
  power 1-7

W

who should read this document
  audience iv