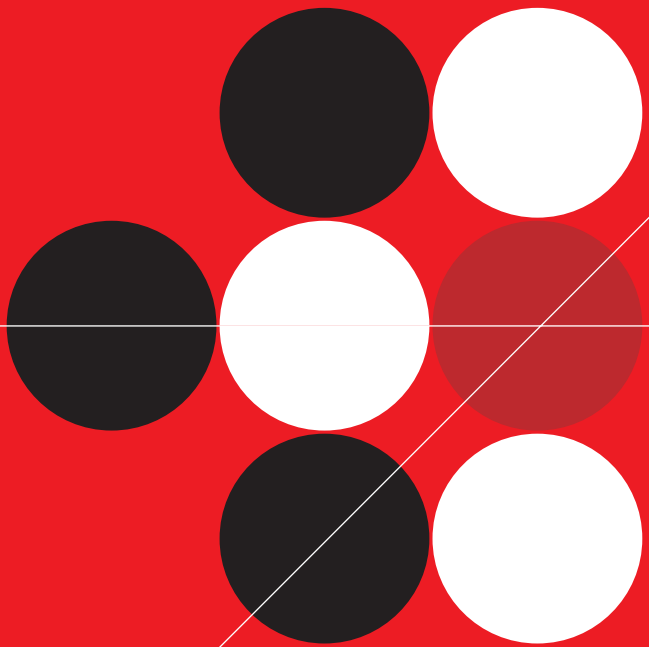
TREND MICRO™
Network VirusWall™ 2500

Getting Started Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

`www.trendmicro.com/download`

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. NVEM12218/50301

Release Date: May 2005

Protected by U.S. Patent No. 5,623,600 and pending patents.

The *Network VirusWall 2500 Getting Started Guide* is intended to provide deployment and preconfiguration instructions for your production environment. Read it prior to deploying or preconfiguring a Network VirusWall device.

For technical support, please refer to *Contacting Technical Support* for contact details. Detailed information about how to use specific features within Trend Micro Control Manager is available in the online help file and online Knowledge Base at Trend Micro's Web site. For more detailed installation and configuration instructions, refer to the *Network VirusWall 2500 Administrator's Guide* in PDF form on the *Trend Micro Solutions CD for Network VirusWall.*

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

`www.trendmicro.com/download/documentation/rating.asp`

Contents

Chapter 5: Preconfiguring Network VirusWall

Chapter 6: Troubleshooting Preconfiguration

Appendix A: System Checklists

Index

Preface

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

This preface discusses the following topics:

Network VirusWall Documentation

The Network VirusWall documentation consists of the following:

- Online Help—Web-based documentation that is accessible from the Control Manager management console

  The Network VirusWall Online Help is integrated with the Control Manager Online Help (*Managing the Control Manager Network* > *Managing Network VirusWall*). It contains explanations about the Network VirusWall components and features, which includes procedures needed to configure a Network VirusWall device from the Control Manager management console.

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

  This GSG contains instructions on deploying Network VirusWall, a task that includes planning and testing, preconfiguration, and Control Manager server installation. See *About This Getting Started Guide* for chapters available in this book.

  If you are planning a large-scale deployment of Network VirusWall or have a complex network architecture and need more details about product Network VirusWall and Control Manager architecture, refer to the *Network VirusWall Administrator's Guide* and *Control Manager Online Help and Getting Started Guide* available in the Solutions CD.

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

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

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

About This Getting Started Guide

The Network VirusWall Getting Started Guide discusses the following topics:

- *Introducing Network VirusWall 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*—recommendations to help you plan for the deployment of one or more Network VirusWall devices
- *Preconfiguring Network VirusWall*—step-by-step instructions on how to install Trend Micro Control Manager and the necessary patches, including considerations and procedures on how to perform Network VirusWall preconfiguration
- *Troubleshooting Preconfiguration*—troubleshooting tips for issues encountered during preconfiguration

In addition, *System Checklists* are available for readers to record relevant system information when preparing for a Control Manager and Network VirusWall deployment.

Audience

The Network VirusWall 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 Network VirusWall 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 ScanMail 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
INT	Network VirusWall interface connected to the protected network
EXT	Network VirusWall interface connected to the external or public network (usually the Internet)
FAILOVER	Network VirusWall interface connected to the device in a failover pair

TABLE 1. Conventions used in the Network VirusWall documentation

Chapter 1

Introducing Network VirusWall 2500

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

The topics discussed in this chapter include:

Trend Micro Network VirusWall™

Trend Micro™ Network VirusWall™ 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, 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.

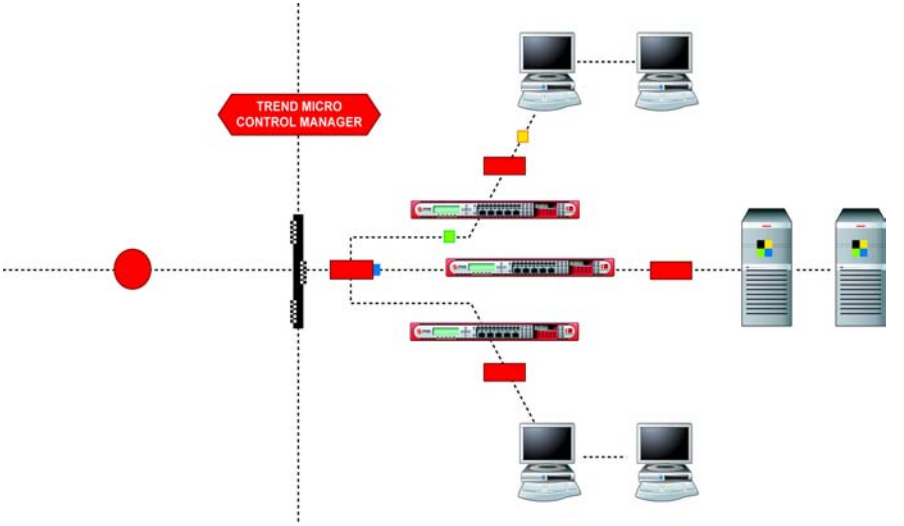


FIGURE 1-1. Network VirusWall monitors network packets and events that could indicate an attack against a network

A Control Manager server must be available to manage Network VirusWall devices. See *Trend Micro Control Manager™* on page 1-3 for more Control Manager information. *Deployment Overview* presents a sample Network VirusWall deployment.

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

Trend Micro Control Manager™

Trend Micro Control Manager™ is a central management console that manages Trend Micro antivirus and content security products, as well as services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager provides central management for one or more Network VirusWall devices on your network and gives you the tools to configure and enforce antivirus policies for an entire organization. This enables you to react quickly to network virus emergencies from nearly anywhere using the management console.

Network VirusWall makes use of a public encryption key (`E2EPublic.dat`) to register and communicate with the Control Manager server. See *Obtaining the Public Encryption Key* on page 4-7 for details on how to obtain the public key.

After registering a Network VirusWall device to a Control Manager server, the management console enables you to perform the following Network VirusWall administrative tasks:

- Update Network VirusWall components and settings
- Analyze your network's protection against viruses
- Enforce antivirus policies
- Monitor the network for suspicious activity
- Monitor Network VirusWall devices via SNMP
- Utilize Control Manager services

For instructions on installing Control Manager, see *Installing Control Manager for the First Time* on page 4-2.

For instructions on preparing an existing Control Manager server support for Network VirusWall 2500, see *Existing Control Manager Installation* on page 4-3.

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

Tip: Refer to the Control Manager *Online Help* or *Getting Started Guide* for details on the Control Manager features, deployment strategies, How To instructions, and troubleshooting tips.

Control Manager Management Console

The Control Manager management console is a Web-based console made available via the Microsoft™ Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any machine using a compatible Web browser and allows easy access to all Network VirusWall devices.

Figure 1-2 illustrates the main components of the Control Manager management console.

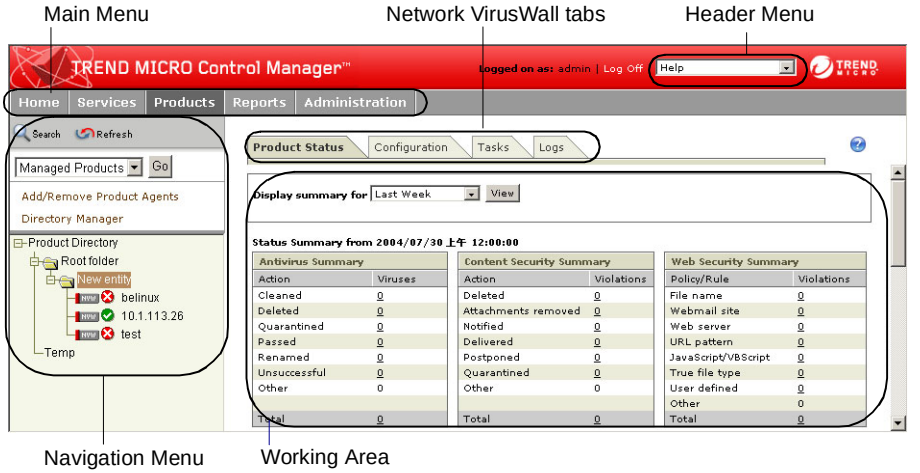


FIGURE 1-2. The Control Manager management console with registered Network VirusWall devices

See the following sections to:

- Prepare for and install Control Manager, *page 4-2*, *page 4-9* and *page 4-10*
- Register a Network VirusWall device through preconfiguration, *page 5-5*

Note: See the *Control Manager Online Help* for detailed Control Manager management console information.

Introducing Network VirusWall-specific Terms

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

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

The Network VirusWall documentation sometimes refers to *Ethernet ports* and fiber-optic ports as *ports* or *interfaces* (see *Understanding the Network VirusWall Interfaces* on page 1-6).

- **INT PORT** (RJ-45 or fiber-optic) – the Network VirusWall port/interface that connects to the protected network Depending on the Operation Mode, there can be a maximum of 4 INT ports set to a Network VirusWall device.
- **EXT PORT** (RJ-45 or fiber-optic) – the Network VirusWall port that connects to the public network. Depending on the Operation Mode, there can be a maximum of 2 EXT ports set to a Network VirusWall device.
- **FAILOVER** port (RJ-45 or fiber optic)– the Network VirusWall port that connects to the other Network VirusWall device used in a failover Operation Mode deployment

Operation Mode—the Network VirusWall Preconfiguration menu (menu number 3) that provides the options to configure the failopen, failover, and port redundancy settings

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

Failover—a backup operational mode in which the functions of a Network VirusWall device are assumed by a standby device when the Active device becomes

unavailable through either failure or scheduled downtime. The FAILOVER port becomes available when a high availability (HA)-based Operation Mode is set.

Protected network—the network segment separated and protected by Network VirusWall (see *Figure . Figure 1-4 illustrates a sample environment after a Network VirusWall deployment.* on page 1-9). It is the part of the network that is connected to INT.

Public network—the network segment that is not protected by Network VirusWall (see *Figure . Figure 1-4 illustrates a sample environment after a Network VirusWall deployment.* on page 1-9). A public network is usually the Internet or other LAN segments. This term is strictly relative to a specific Network VirusWall device. It is the part of the network that is connected to **EXT**.

Understanding the Network VirusWall Interfaces

Network VirusWall 2500 can support seven (7) user-configurable Ethernet ports—five (5) copper ports and two (2) fiber-optic ports. Depending on the Operation Mode setting, you can designate each copper port to become the **INT**, **EXT**, or **FAILOVER** port. Fiber ports can only serve as **INT** or **EXT** ports.

FIGURE 1-3. Network VirusWall 2500 Ethernet ports 1 through 6 with five copper ports and one multi-mode fiber-optic port

Note: Network VirusWall ships with one of two configurations: 1) No add-on PCI-X adapter with the PCI slot cover masked or 2) One multi-mode fiber-optic dual port with the PCI slot cover open (shown above).

Network VirusWall applies its protection features to packets that pass through the device. Table 1-1, "How INT and EXT apply Network VirusWall and Control Manager features," on page 1-7 defines how Network VirusWall applies its features, including Control Manager features, to the public and protected networks connected to **INT** and **EXT** ports.

NETWORK PROTECTION FEATURE	INT-INT*	INT-EXT*	EXT-INT*	EXT-EXT*
Network Outbreak Monitor	●	●	●	
Real-time Network Virus Scan	●	●	●	
Policy Enforcement		●		
Vulnerability Assessment		●		
Automatic Damage Cleanup Services	●	●		
Outbreak Prevention Service	●	●	●	

TABLE 1-1. How INT and EXT apply Network VirusWall and Control Manager features

* See Legend on *page 1-7* for details.

Legend:

INT-INT — refers to a network packet coming to and from a client in the protected network

INT-EXT — refers to a network packet coming from a client in the protected network and going to the public network

EXT-INT — refers to traffic coming from the public network and going to a client in the protected network

EXT-EXT — refers to traffic coming to and from a client in the public network

Configure Network VirusWall to automatically clean infected clients detected during real-time scan. Take note, however, that Network VirusWall only tries to clean clients connected to the **INT** port. To clean infected clients connected to the **EXT** port, use Damage Cleanup Services from the Control Manager management console.

Note: The **FAILOVER** port is reserved for connection to the failover device. It has no bearing as to how the Network VirusWall and Control Manager features apply their settings to the protected and public networks. See *Deploying Network VirusWall* starting on page 3-1 for details on how to allocate the Network VirusWall ports.

Refer to the *Control Manager documentation* for details about *Damage Control Services*.

Allocating Ports Based on Operation Mode

Designate each Network VirusWall port based on the Operation Mode settings. Network VirusWall 2500 supports an add-on fiber-optic adapter via PCI-X riser card.

Depending on the Operation Mode, designate a port as the **INT**, **EXT**, or **FAILOVER** port. For details on port allocation per Operation Mode, see *Deploying Network VirusWall* starting on page 3-1.

After preparing the Network VirusWall device (see *Getting Started*), proceed to *Deploying Network VirusWall* to learn how Network VirusWall works depending on the Operation Mode setting.

Deployment Overview

Network VirusWall deployment consists of the following steps:

1. Deciding on the deployment strategy

   Deploying Network VirusWall provides the basic deployment and strategies based on the four Operation Modes. This chapter aims to help you determine the strategy you will take to deploy Network VirusWall 2500.

2. Preparing for preconfiguration

   Preparing for Preconfiguration discusses the initial preconfiguration tasks that you need to perform to successfully deploy Network VirusWall and Control Manager in your environment.

3. Preconfiguring Network VirusWall

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

4. Configuring Network VirusWall

   Chapter 2 of the *Administrator's Guide* includes instructions to help you configure the basic Network VirusWall settings after preconfiguration.

Figure 1-4 illustrates a sample environment after a Network VirusWall deployment.

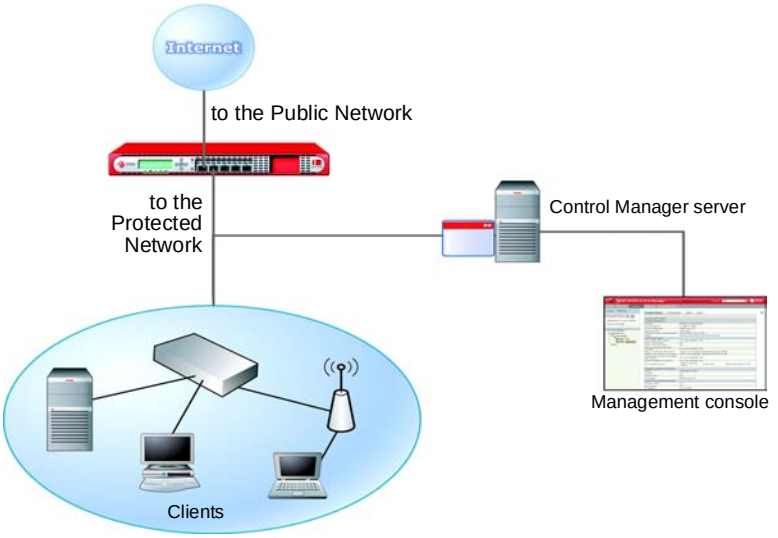


FIGURE 1-4. Network VirusWall and Control Manager after preconfiguration

Chapter 1 of the Network VirusWall *Administrator's Guide* provides details about the following concepts:

- Protected and public networks
- Clients
- Network VirusWall antivirus and outbreak monitoring capabilities

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

Chapter 2

Getting Started

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

This chapter contains the following topics:

After completing the procedures in this chapter, proceed by:

Package Contents

Figure 2-1 illustrates the Network VirusWall package contents.

FIGURE 2-1. The Network VirusWall package contents

Tip: After receiving the Network VirusWall package, refer to *Table 2-1*and *Table 2-10* to check whether the package is complete. Otherwise, please contact Trend Micro support (see *page 6-15*).

Table 2-1, “Network VirusWall package contents,” on page 2-3 specifies each item:

QUANTITY	ITEM	DESCRIPTION
1 unit	Network VirusWall 2500	The Network VirusWall device.
1 piece	Power cord	Used to supply power to a Network VirusWall device (length is 79in/200cm).
1 piece	Ethernet cable (RJ-45 crossover cable)	Used to connect two (2) Network VirusWall devices in a failover pair or connect a device to a computer used during Rescue Mode (length is 39in/100cm).
1 piece	Console cable (RS-232)	Used to connect the Network VirusWall device to the computer used during preconfiguration (length is 79in/200cm).
1 set	Rack kit	Used to mount a Network VirusWall to a standard 19in rack cabinet.
2 pieces	PCI-X slot covers	Used to cover the front panel slot for fiber, copper, and accessory cards. The original cover is already attached to the front panel when Network VirusWall 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 2500	The CD containing the Control Manager 3.0, patch, and hot fix installers, including the Network VirusWall tools and documentations available. The PDF documentation includes: • Network VirusWall Getting Started Guide • Network VirusWall Administrator’s Guide • Control Manager Getting Started Guide The Network VirusWall 2500 tools include: • Firmware Flash Utility • Rescue Utility **Note:** Refer to the *Administrator’s Guide* > *Troubleshooting* for instructions on how to use these tools.
1 book 1 sheet	Network VirusWall Getting Started Guide Network VirusWall Safety Sheet	Printed Network VirusWall Getting Started Guide and Safety Sheet.

TABLE 2-1. Network VirusWall package contents

Network VirusWall 2500 Front Panel

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

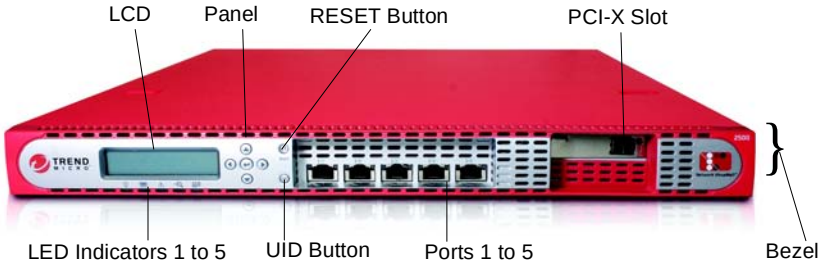


FIGURE 2-2. Network VirusWall 2500 front panel

The following table describes each front panel element:

ELEMENT	DESCRIPTION
Liquid Crystal Display (LCD)	A 2.6in x 0.6in (65mm x 16mm) 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**, **INSPECTION**, and **OUTBREAK** states. **POWER** and **UID** have one color each; **SYSTEM**, **POLICY**, and **OUTBREAK** have three colors each. See *page 2-5* for details.
Ports 1, 2, 3, 4, 5	Copper Gigabit LAN port designated as the INT, EXT, or FAILOVER port depending on the Operation Mode. The Network VirusWall documentation refers to each interface by its number (for example, port 1 or 2).
UID Button	Unique ID button that illuminates the LED, which helps administrators locate a device for troubleshooting or maintenance.
PCI-X Slot	Slot for fiber, copper, and accessory cards. See *page 2-10* for details on how to choose a fiber media converter (FMC).
Bezel	Detachable casing that covers and protects the front panel.

TABLE 2-2. 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 2500 has five (5) **l**ight-**e**mitting **d**iodes (LEDs) that indicate the **POWER**, **UID**, **SYSTEM**, **POLICY**, and **OUTBREAK** status.

FIGURE 2-3. Network VirusWall 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 Control Manager 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; see *page 6-3* for details.
	Yellow– flashing	Network VirusWall program file (firmware) is starting
	Yellow– steady	Network VirusWall program file (firmware) encountered a critical error
	Green– steady	Network VirusWall program file (firmware) is ready
INSPECTION	Green– flashing	Network Outbreak Monitor, Network Scan, or Policy Enforcement is enabled (Normal or high availability (HA) Active mode)
	Yellow– steady	Failover Standby mode is enabled

TABLE 2-3. Network VirusWall 2500 LED indicators

LED	STATE	DESCRIPTION
OUTBREAK	Green– steady	Outbreak Prevention Services (OPS) is disabled
	Red– flashing	OPS is enabled

TABLE 2-3. Network VirusWall 2500 LED indicators

Port Indicators

Network VirusWall has five (5) user-configurable Copper-based Ethernet ports. See *page 1-8* for the port functionality. Each Ethernet port has an indicator that allows you to determine the port's current state. *Figure 2-4* illustrates the indicators of a Network VirusWall port.

FIGURE 2-4. Port indicators 1 and 2

Table 2-4 lists the description for each port component.

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

TABLE 2-4. Port indicator description

Table 2-5 shows the possible states for each Network VirusWall 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 reserves ports 1 and 2 for failopen.
LINK 	Indicator 1– green, steady	Port speed is 10Mbps, 100Mbps, or 1Gbps
	Indicator 2– orange, flashing	Network packet transmission/receiving active

TABLE 2-5. Network VirusWall 2500 port indicators

Network VirusWall 2500 Back Panel

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

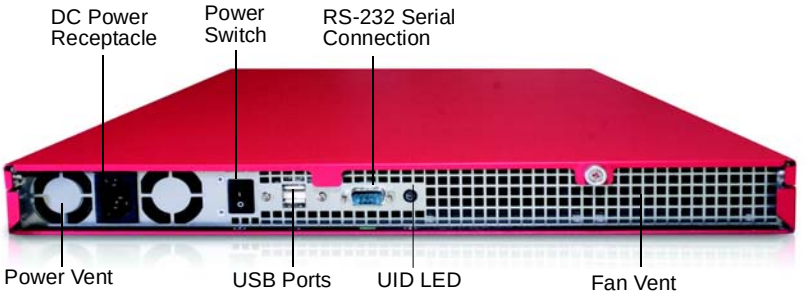


FIGURE 2-5. Network VirusWall 2500 back panel

The following table describes each back panel element:

ELEMENT	DESCRIPTION
DC Power Receptacle	Connects to the power outlet and Network VirusWall device using the power cord (included in the package, see *Package Contents* on page 2-2)
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 five (5) system fans
Power Vent	Cooling vent for the power receptacle
UID LED	LED at the back panel of a Network VirusWall device. When a user presses the UID button, the UID LED illuminates. The illuminated UID LED allows administrators to easily locate a Network VirusWall device for troubleshooting or maintenance.
USB Ports	USB ports, reserved for future releases

TABLE 2-6. Back panel description

Dimensions and Weight

The following specifications apply to Network VirusWall 2500:

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

TABLE 2-7. Network VirusWall 2500 dimensions and weights

Power Requirements and Environmental Specifications

The following settings apply to Network VirusWall 2500:

ELEMENT	SPECIFICATION
AC input voltage	90 to 264VAC
AC input current (90VAC)	8.0A
AC input current (180VAC)	4.0A
Frequency	47 to 63Hz (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 2-8. Network VirusWall 2500 power requirements and environmental specifications

Choosing a Fiber Media Connector for Fiber-based Networks

This release of Network VirusWall 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 connector. 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.

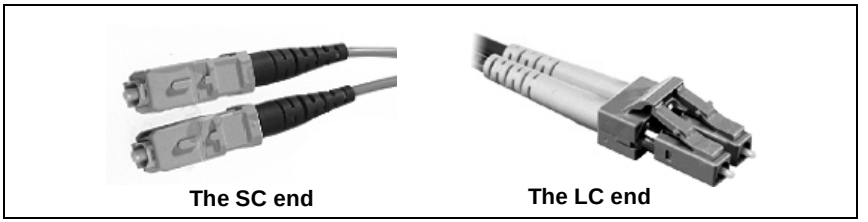


FIGURE 2-6. The two ends of an SC-LC fiber media patch cord

See Table 2-9, “Fiber media patch cords and connectors,” on page 2-10 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 2-9. Fiber media patch cords and connectors

Mounting Network VirusWall

Whenever possible, position and mount the Active and Standby devices in the same physical location (for example, "Server Room 101 on the 15th floor"). Doing so allows the network administrator to easily maintain the Network VirusWall devices.

Mount a Network VirusWall device:

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

  Network VirusWall requires 1 rack unit (RU) of vertical space in the rack.

  Tip: If you are mounting more than one Network VirusWall device, mount the first device in the lowest available position in the rack.

- On any stable surface as a freestanding device

  For freestanding installation, guarantee that the device has at least 2in (5.08cm) 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 a Network VirusWall 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 2-7 shows the contents of the Network VirusWall 2500 rack kit.

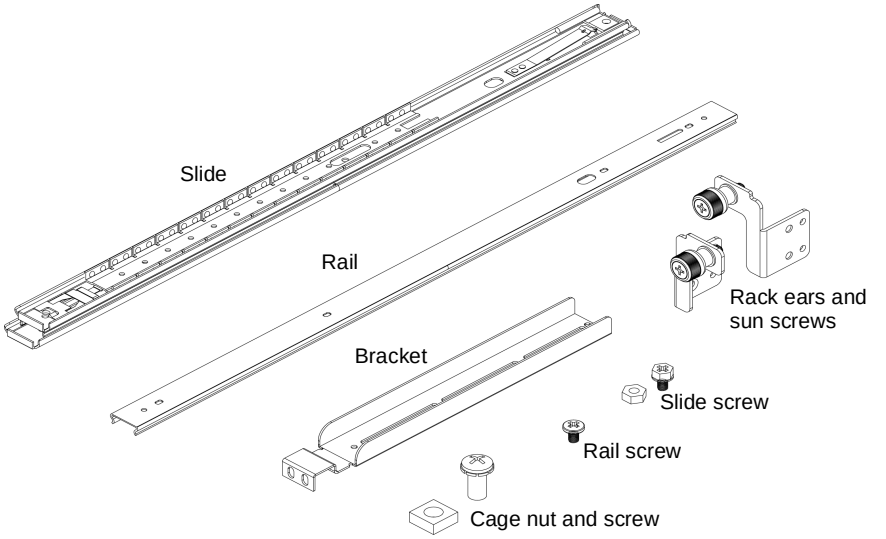


FIGURE 2-7. Rack kit contents

Table 2-10 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 Network VirusWall package is shipped. Remove the rail from the slide before mounting a 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 2-10. Network VirusWall 2500 rack kit contents

Figure 2-8 illustrates the positions of the slide set, rail, and cage screws.

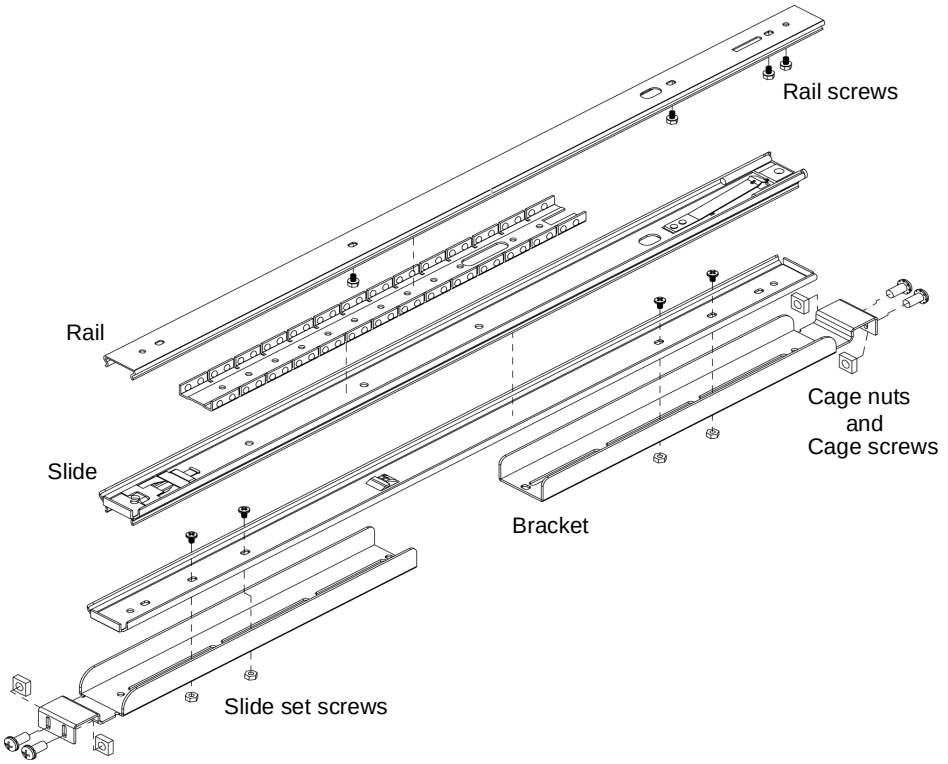


FIGURE 2-8. Positions of the slide set, rail, and cage screws

Four-Post Rack Mounting

You can mount a Network VirusWall 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 22*page 2-25* for illustration)
- Fixed mount– secures the device in one position (see *page 2-22* for illustration)

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

To mount Network VirusWall 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 device. Using the rack kit for another system may damage the device and cause injury to yourself and others.*

---

1. Prepare the Network VirusWall device (see *page 2-16*).
2. Assemble the slide sets (see *page 2-18*).
3. Install the slide sets (see *page 2-22*).
4. Mount the Network VirusWall device in the rack (see *page 2-25*).

Preparing the Network VirusWall Device

This task involves preparation of the Network VirusWall device.

To prepare the Network VirusWall device:

1. Attach the rack ear and sun screw set to each side on the front-end of the device (see *Figure 2-9*).

FIGURE 2-9. 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 2-10. 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 2-11*.

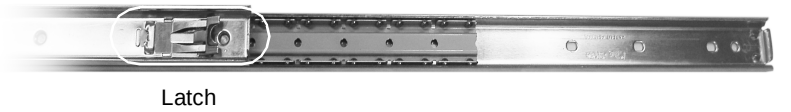


FIGURE 2-11. Rail is properly detached when the latch is raised

3. Attach a rail to the device side panel by using a minimum of four (4) slide screws (see *Figure 2-12*).

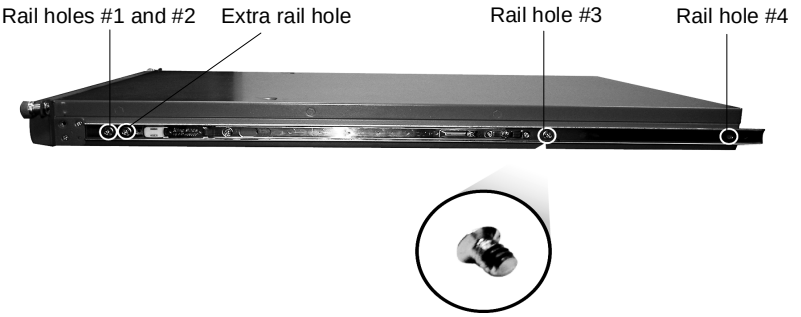


FIGURE 2-12. Attaching a rail to the side panel using slide screws

Tip: See *Figure 2-8* to for an illustration of the rail screws.

4. Repeat step 3 for the other side panel.

Figure 2-13 illustrates a device with rails and rack ears attached.

FIGURE 2-13. 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 2-14* for information about the slide set elements.

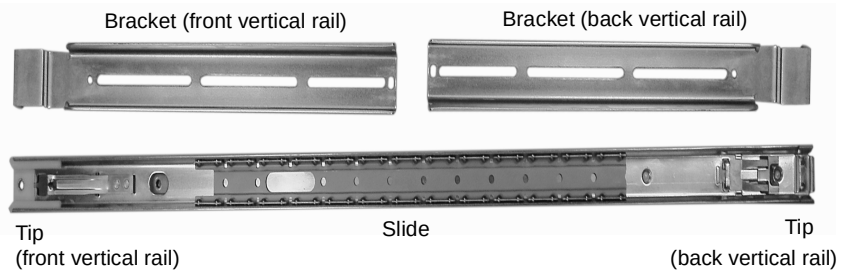


FIGURE 2-14. A slide set is composed of two brackets and a slide

Figure 2-15 illustrates how a slide set is mounted in a four-post rack.

FIGURE 2-15. 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 2-16* for the screw holes and positions.

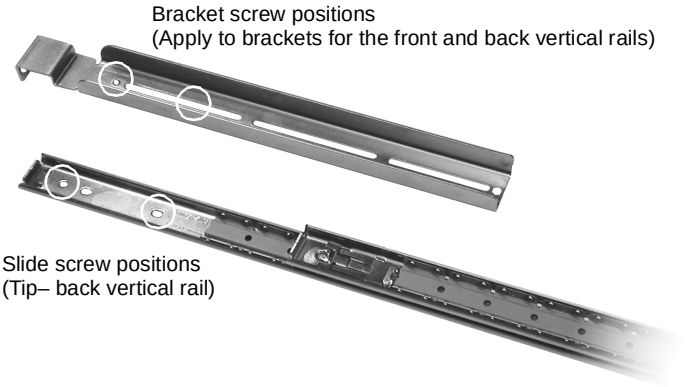


FIGURE 2-16. Screw positions for the back vertical rail

Tip: See *page 2-14* for illustration on the positions of the slide and bracket screws.

b. Insert the slide screws (see *Figure 2-17*).

FIGURE 2-17. Inserting two slide screws (bracket and slide pair for the back vertical rail)

Tip: See *page 2-14* 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.

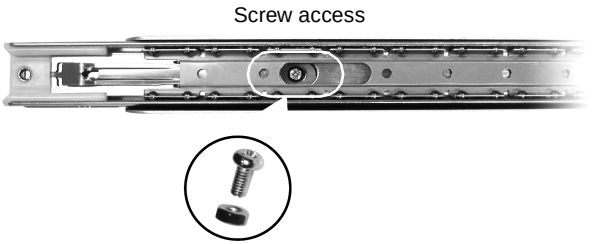


FIGURE 2-18. Inserting two slide screws (bracket and slide pair for the front vertical rail)

Tip: See *page 2-14* for an illustration of the slide set screws.

Figure 2-19 shows both ends and the back view of a completed slide set.

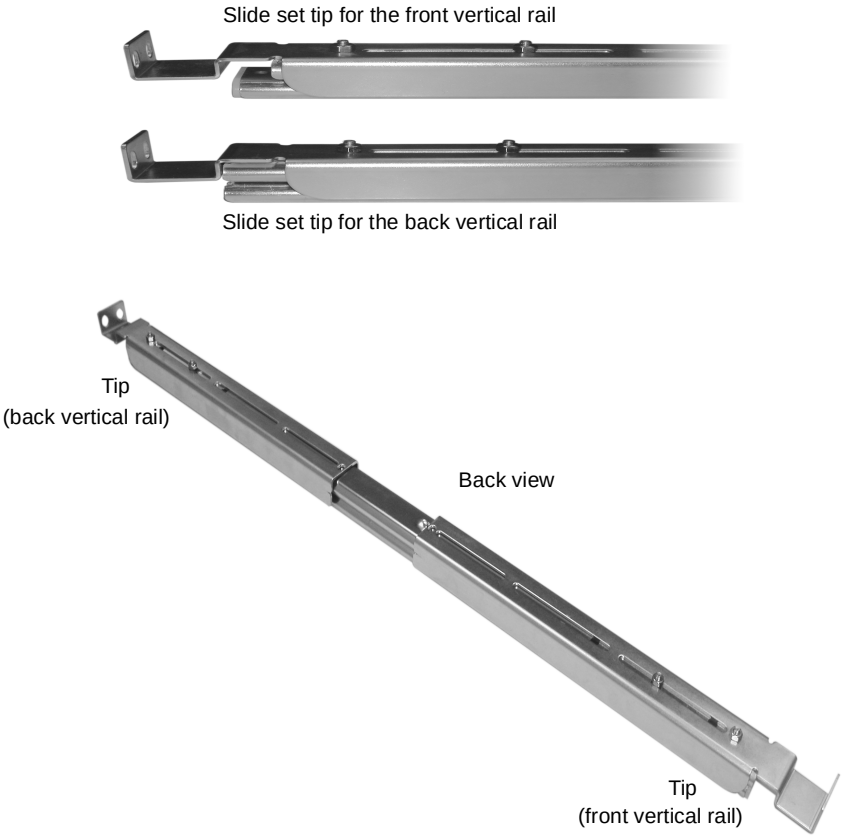


FIGURE 2-19. Completed slide set

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 Network VirusWall 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 Network VirusWall. *Figure 2-20* illustrates this step.

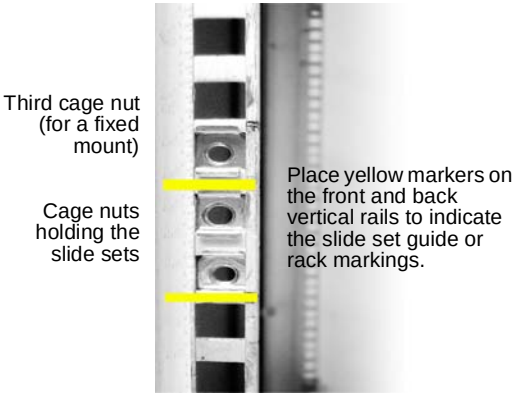


FIGURE 2-20. Graphical representation of the device position in the rack and slide set guides (rack markings)

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

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

---

4. Install one pair of cage nuts to occupy holes in between the marks you made on the front vertical rail (see *Figure 2-21*).

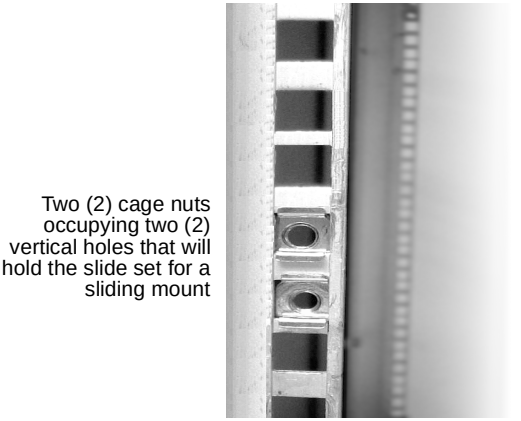


FIGURE 2-21. Cage nuts for a sliding mount

Note: Install a third cage nut above the cage nut pair for a fixed mount (see *Figure 2-22*).

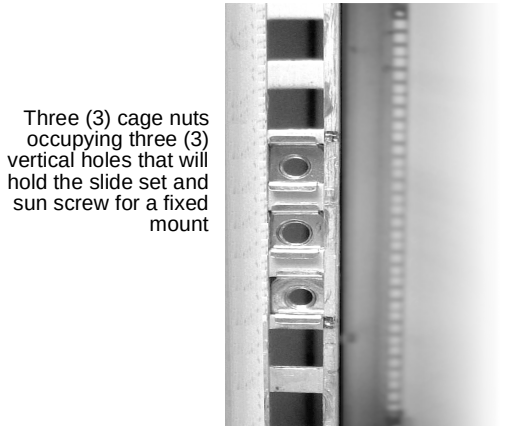


FIGURE 2-22. Cage nuts for a fixed mount

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 2-23*).

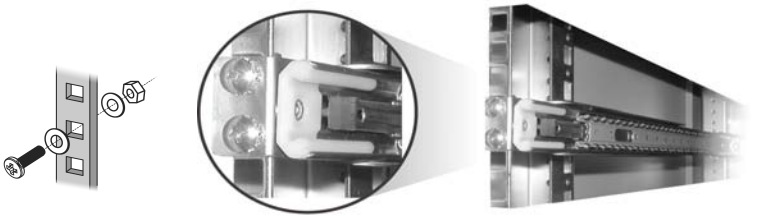


FIGURE 2-23. Installing the cage screws in the top and bottom holes of the slide set (front vertical rail view)

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 2-24*).

FIGURE 2-24. Mounted slide sets

Mounting the Network VirusWall Device in the Rack

This task involves installing the device in the rack.

Note: Because of the size and weight of Network VirusWall, never attempt to mount the device in the rack by yourself.

To mount the Network VirusWall 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 2-24* 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 2-25*).

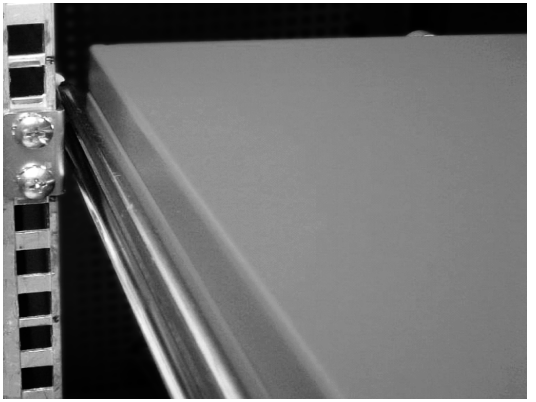


FIGURE 2-25. Mounted Network VirusWall device (sliding mount)

5. Install the sun screws to prevent the device from sliding in or out (see *Figure 2-26*).

FIGURE 2-26. Mounted Network VirusWall device (fixed mount)

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

- *Planning for Deployment* on page 3-2
- *Conducting a Pilot Deployment on page 3-21*
- *Understanding the Network VirusWall Preconfiguration* on page 5-2

Installing a Fiber-Optic Card

Network VirusWall 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 supports the following fiber-optic server adapters:

- Intel PRO/1000 MF Dual Port Server Adapter
- Intel PRO/1000 MF Single Port Server Adapter (LX)

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 Network VirusWall 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.

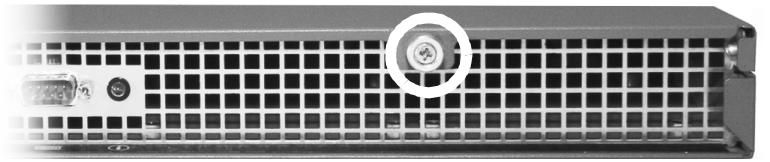


FIGURE 2-27. Back panel showing cover screw

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.

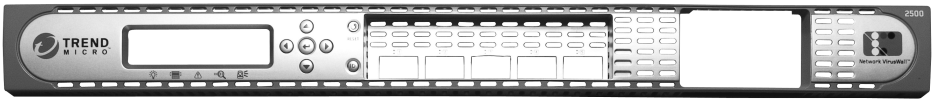


FIGURE 2-28. NVW 2500 front bezel panel, detached

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.

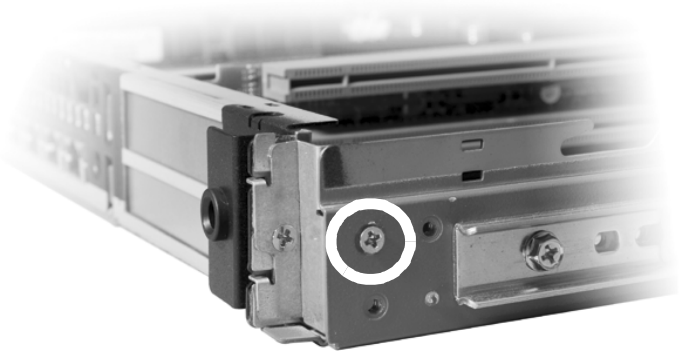


FIGURE 2-29. The screw to remove for step 6

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.

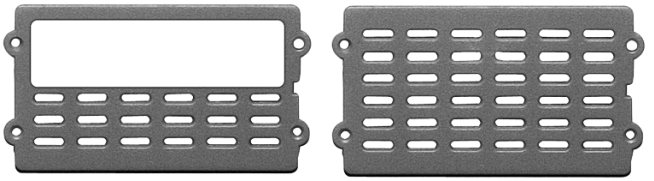


FIGURE 2-30. Two PCI slot covers. Left: open-area cover, Right: fully masked cover

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

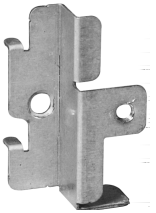


FIGURE 2-31. The silver metal side bracket

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.

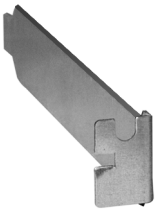


FIGURE 2-32. Blank metal expansion slot plate

The device is now ready to receive the fiber-optic card. See *To install a fiber-optic card in an open machine:* on page 2-30 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 2-27.)

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

1. Carefully remove the card from its plastic container.

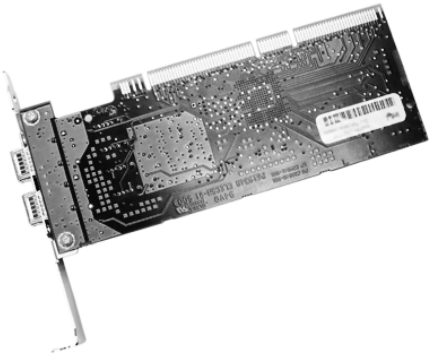


FIGURE 2-33. A duplex single-mode fiber-optic card

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

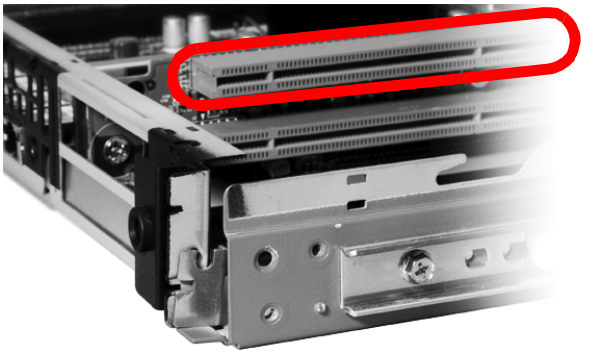


FIGURE 2-34. Insert card in top slot if only installing one card

4. Replace the silver metal side bracket and screw it back on.
5. 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.
6. Replace the front bezel, making sure that it snaps into place.
7. Replace the NVW2500 top cover and screw back in the Sun screw on the rear panel of the machine.
8. Plug the power cord back into the outlet on the rear panel of the machine.
9. Turn the power switch back on.

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 2-27 and then proceed as follows.

To remove a fiber-optic card from Network VirusWall:

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 NVW2500 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 3

Deploying Network VirusWall

Before beginning to configure a Network VirusWall device, plan how to integrate Network VirusWall into your network. Determine which topology it will support and the type of operation mode it will apply.

This chapter explains how to plan for the deployment of Network VirusWall devices based on supported operating modes. It also provides application and deployment scenarios to facilitate understanding of the various ways Network VirusWall can help protect and secure your network.

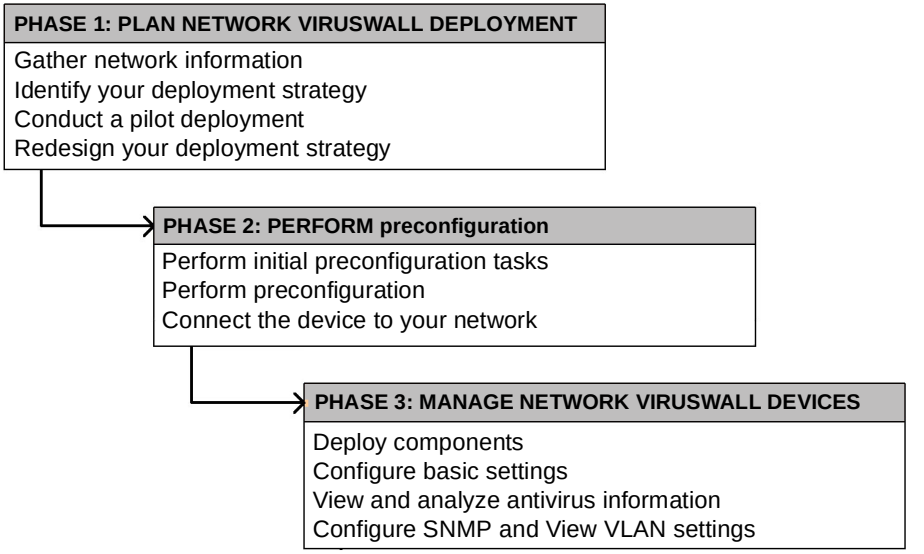
This chapter contains the following topics:

Planning for Deployment

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

Deployment Overview

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



Phase 1: Plan the Deployment

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

- Determine the segments of your network that are in the greatest need of protection (see *page 3-7*)
- Plan for network traffic, considering the location of devices critical to your operations such as email, Web, and application servers (see *page 3-20*)

- Determine both the number of Network VirusWall devices needed to meet your security needs and their locations on the network (see *page 3-20*)
- Conduct a pilot deployment on a test segment of your network (see *page 3-21*)
- Redefine your deployment strategy based on the results of the pilot deployment (see *page 3-22*)

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 *page 4-1*)
- Perform preconfiguration on the Network VirusWall device(s) to register the device to the Control Manager server (see *page 5-1*)
- Connect the device(s) to your network (see *page 5-24*)

Note: Trend Micro Control Manager™ 3.0 must be installed on your network before you can deploy Network VirusWall device(s).

Phase 3: Manage Network VirusWall Devices

During phase 3, manage Network VirusWall devices from the Control Manager management console. You can perform the following tasks:

- Deploy Network VirusWall components to help guarantee current protection for these devices
- Configure basic settings, including scan options, Network Outbreak Monitor, enforcement policies, exception lists, and component updates
- View and analyze antivirus information, including detailed summaries of clients on the Protected Network security logs, and event logs

---

Tip: This *Getting Started Guide* discusses phases 1 and 2. See *page 3-2*, *page 4-1*, and *page 5-1*.

Refer to the Network VirusWall 2500 *Administrator's Guide* > *Configuring the Scan, System, and Device Settings* section for instructions relating to phase 3.

Control Manager and Network VirusWall Integration

Network VirusWall is manageable through Control Manager. Install Control Manager before deploying Network VirusWall devices.

Before preconfiguring and integrating a Network VirusWall device with Control Manager, take note of the following integration notes:

- Deploy Control Manager and Network VirusWall on the same network segment

  Note: There is an exception to this guideline. Read the succeeding notes.

- If the Control Manager server on your network belongs to a VLAN, bind Network VirusWall to the same VLAN (tagged or non-tagged)

  Doing so will help guarantee effective communication between the Control Manager server and Network VirusWall.

- Network VirusWall supports networks using a Network Address Translation (NAT) device. In order to use Network VirusWall with NAT, set the NAT IP address and port in the Preconfiguration console. (See *Configuring Device Settings* on page 5-9 for details.)

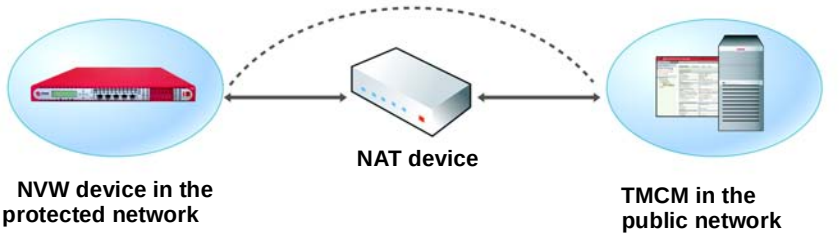


FIGURE 3-1. Network VirusWall deployment using a Network Address Translation device

Read the following procedures to learn how to configure Control Manager and Network VirusWall integration for similar scenarios as depicted on *page 3-9*.

Note: These instructions only apply to similar scenarios as depicted in Figure 3-1. *Network VirusWall deployment using a Network Address Translation device* on *page 3-4*.

To register Network VirusWall to a Control Manager Server:

1. Enable IP port forwarding on the NAT device with the following port settings:
   - **Time server UDP:** 123
   - **Control Manager server UDP:** 10319
   - **Control Manager Web server port:** 80

   Note: These are the default values. You can modify these port numbers on the **System Settings** screen of the Control Manager management console. Refer to the *Administrator's Guide* > *Configuring System Settings* for more information.

   - **Control Manager server TCP:** 10319
2. Perform one of the following to enable NAT mode on the Control Manager server:
   - Set the message routing path during a Control Manager installation
   - Modify the `tmi.cfg` configuration file for the existing Control Manager installation

Refer to the following documentation for details about Control Manager configuration and its integration with Network VirusWall:

- Control Manager 3.0 *Getting Started Guide* or Online Help
  - Planning and Implementing the Control Manager Deployment
  - Installing Control Manager
  - Getting Started with Control Manager

Note: For usability, Control Manager-related information is included in the *GSG*. Always refer to the latest Control Manager documentation available at http://www.trendmicro.com/download/.

Deployment Notes

Consider the following when planning for a Network VirusWall deployment:

- All traffic to and from a network segment has to go through Network VirusWall

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

- Each of the Network VirusWall 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 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 devices to have the same setting. Apply **1000Mbps x full-duplex** for both the switch and Network VirusWall device.

- Network VirusWall supports IP address 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 clients (see *page 1-6*)
- Network Outbreak Monitor does not support any action on a detected attack
  However, Control Manager can send notifications to inform you of the potential vulnerability attack.

Tip: Configure Control Manager server to send **Potential vulnerability attack detected** alerts through Event Center. Refer to the Control Manager *Online Help* or *Network VirusWall 2500 Administrator's Guide* for details.

Identifying What To Protect

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

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

- Remote clients that access your internal network resources (see *page 3-8*)
- Guest clients that temporarily connect to your network (see *page 3-11*)
- Key network segments/important network assets, such as places on the network that contain Email, Web, and application servers including client machines (see *page 3-12*)

Remote Access

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

There are two types of remote clients:

- **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.

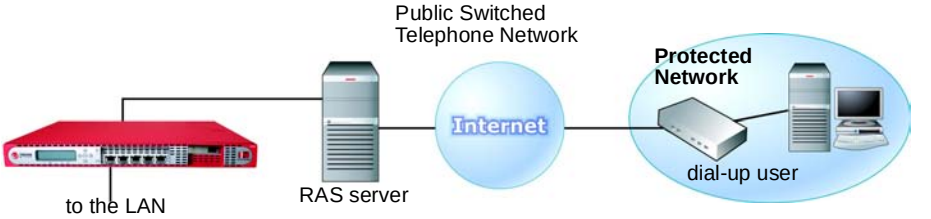


FIGURE 3-2 Dial-up service deployment scenario

Figure 3-2 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 the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the internal network. In this configuration, the home user's VPN connection is considered to be in the Protected Network. 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 3-23). The home user accesses both network resources and the Internet in the same way internal clients do.

Table 3-1 provides a summary of recommended Network VirusWall settings for this scenario.

FUNCTION	RECOMMENDED SETTINGS
Real-time network virus scan	Enabled: Drop Infected Packet and Quarantine Infected Machine
Network VirusWall Policy Enforcement	Enabled: Block traffic
Network Outbreak Monitor	Enabled
Vulnerability Assessment	Enabled
Damage Cleanup Services	Not enabled

TABLE 3-1. Recommended settings for dial-up deployment scenario

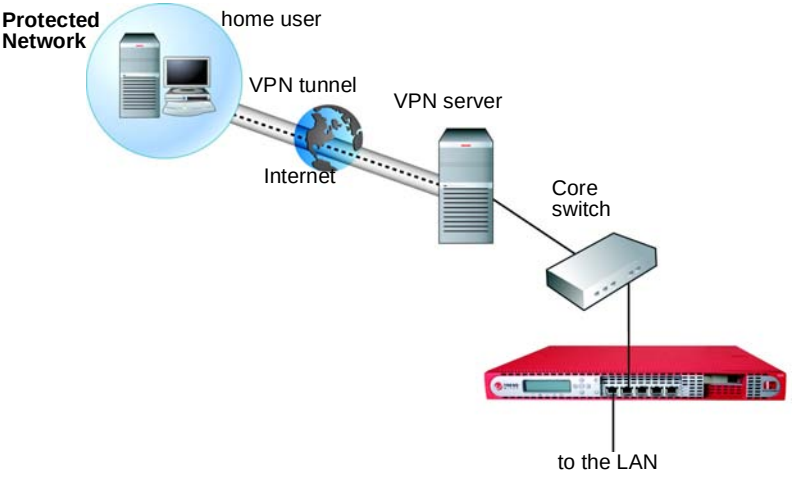


FIGURE 3-3 Client to site VPN deployment scenario

Figure 3-3 is similar to that under *Remote Access* on page 3-8. It illustrates a connection between a home user and an organization's internal network, only though a VPN server, which is connected to the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the internal network. In this configuration, the home user's VPN connection is considered to be in the Protected Network and it becomes part of the internal network.

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

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

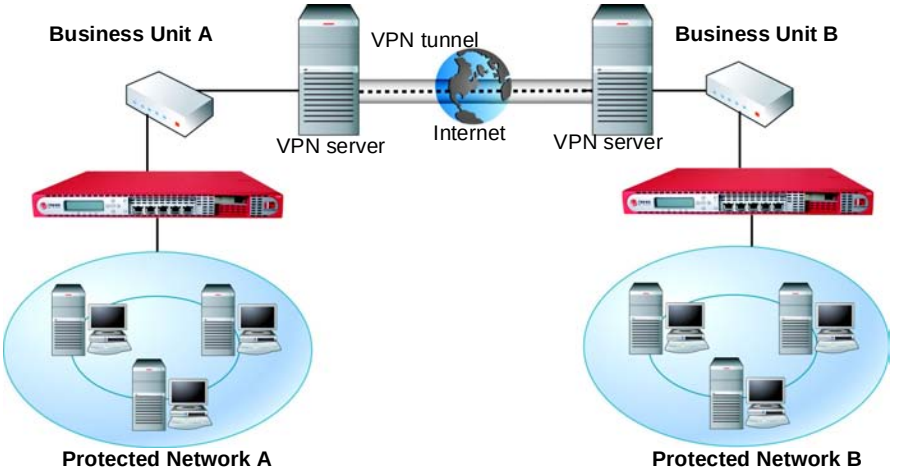


FIGURE 3-4 Site to site VPN deployment scenario

Figure 3-4 illustrates a VPN connection between two business units. As in the home user scenario, a VPN server is connected to the external (**EXT**) port of each Network VirusWall device, while the connection to each internal (**INT**) port leads to the internal network.

Guest Clients

Guest clients are clients that do not belong to an internal network domain. They are often visitors who temporarily access your network resources through their portable computers. Guest clients 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.

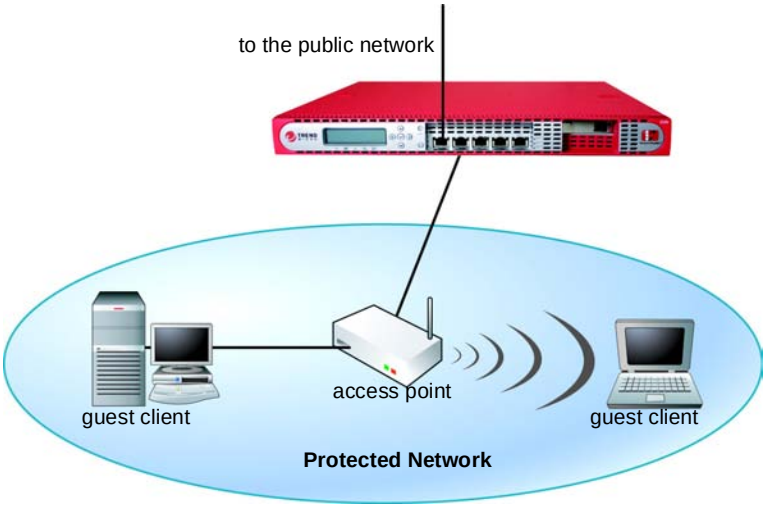


FIGURE 3-5. Guest network deployment scenario

Figure 3-5 illustrates a segment of an internal network especially for guest clients. A wireless access point, switch, or hub is connected to the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the public network. This type of topology ensures that Network VirusWall 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.

Table 3-2 provides a summary of recommended Network VirusWall settings for this scenario.

FUNCTION	RECOMMENDED SETTINGS
Real-time network virus scan	Enabled: Drop Infected Packet and Quarantine Infected Machine
Network VirusWall Policy Enforcement	Enabled: Pass traffic
Network Outbreak Monitor	Enabled
Vulnerability Assessment	Enabled
Damage Cleanup Services	Not enabled

TABLE 3-2. Recommended settings for guest network deployment scenario

Key Network Segments/Important Network Assets

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

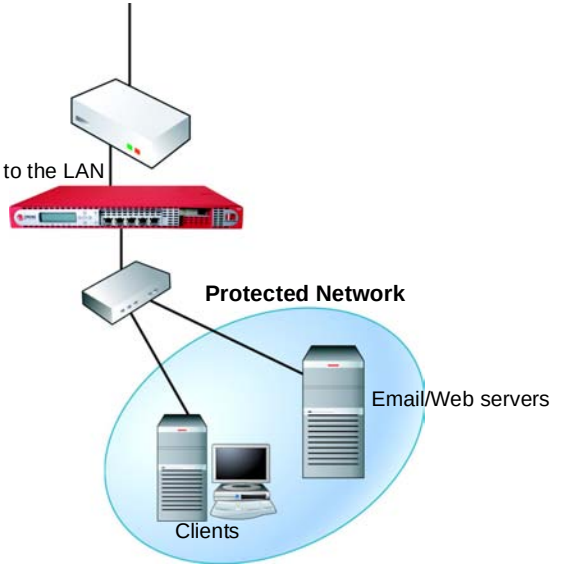


FIGURE 3-6. Key network segments scenario

Key Network Segments/Important Network Assets on page 3-12 illustrates a segment of an internal network containing email and Web servers, including clients. An internal switch or hub is connected to the Network VirusWall internal (**INT**) port, creating a Protected Network segment, while the connection to the external (**EXT**) port leads to the public network. Installing Network VirusWall 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 Network VirusWall before reaching the email and Web servers, Network VirusWall can scan and detect infected packets that come from clients on the LAN.

Table 3-3 provides a summary of recommended Network VirusWall settings for this scenario.

FUNCTION	RECOMMENDED SETTINGS
Real-time network virus scan	Enabled: Drop Infected Packet and Quarantine Infected Machine
Network VirusWall Policy Enforcement	Enabled: Pass traffic
Network Outbreak Monitor	Enabled
Vulnerability Assessment	Enabled
Damage Cleanup Services	Enabled

TABLE 3-3. Recommended settings for key network segments deployment scenario

Multiple VLAN Environment

If you are deploying Network VirusWall in a multiple VLAN environment, bind the Network VirusWall IP address to the VLAN ID that corresponds to the network segment on which the device is located. At the same time, position the Control Manager server on the same segment.

Figure 3-7 illustrates an example:

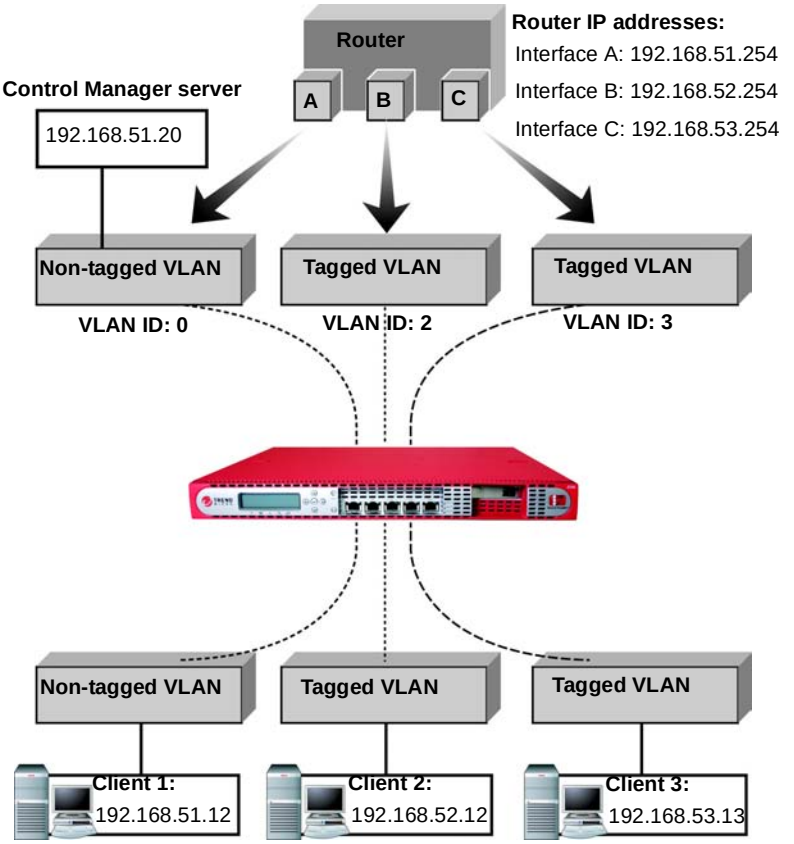


FIGURE 3-7. VLAN IP binding example

This network environment has three IP segments, each belonging to a VLAN:

- 192.168.51.0/24, VLAN ID:0 (non-tagged VLAN)
- 192.168.52.0/24, VLAN ID:2 (tagged VLAN)
- 192.168.53.0/24, VLAN ID:3 (tagged VLAN)

The Control Manager server is located on the non-tagged VLAN. Clients are also shown for reference.

Table 3-4 illustrates where you should bind the Network VirusWall IP address if you change it.

NETWORK VIRUSWALL IP ADDRESS	BIND TO THIS VLAN ID
192.168.51.11	VLAN ID 0
192.168.52.11	VLAN ID 2
192.168.53.11	VLAN ID 3

TABLE 3-4. VLAN IP binding example

Note: The only way to change VLAN settings is through the Preconfiguration console. *Configuring VLAN settings* on page 5-15 for more information.

Dual-switch VLAN Environment

Network VirusWall must be placed in line on the physical network to be able to provide security to the protected segment. 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 3-19. The figures in this section illustrate multiple downstream switches in a flat topology; however, a single in line configuration is also possible.

In *Figure 3-8*, Network VirusWall 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. The upstream switch carries traffic on VLANs 10, 20, and 30, and the downstream switches carry traffic for individual VLANs.

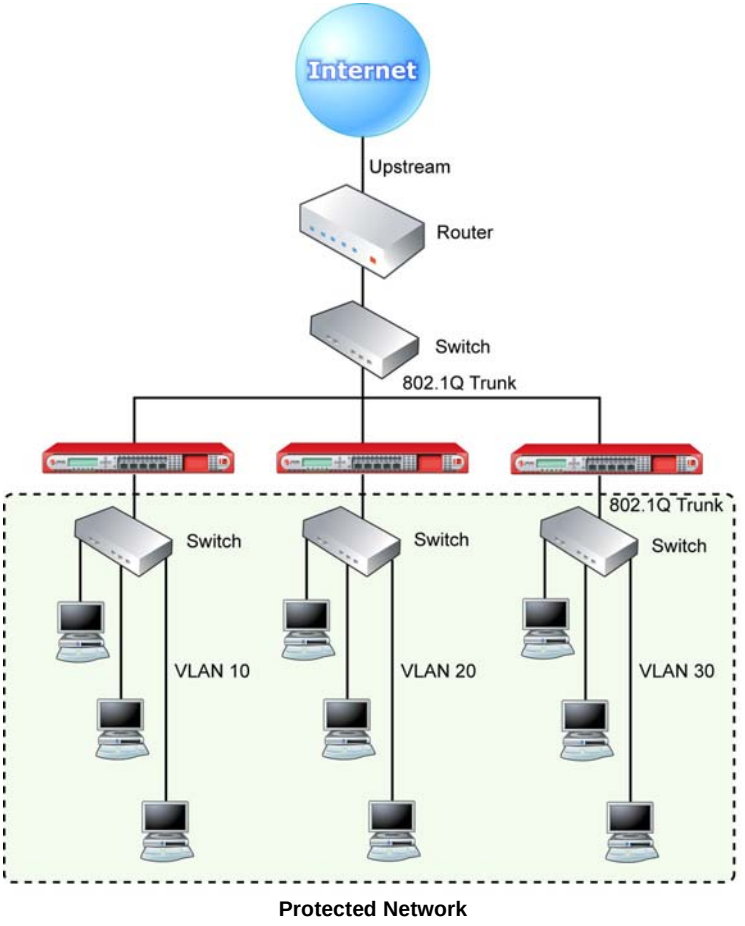


FIGURE 3-8. Multiple VLAN segments with each Network VirusWall protecting one segment

In *Figure 3-9*, Network VirusWall devices are installed on an 802.1Q trunk line between two switches. The upstream switch is configured to handle high-bandwidth traffic on VLANs 10, 20, and 30. Downstream switches handle lower bandwidth traffic on VLANs 10, 20, and 30. This configuration is appropriate when VLANs

span multiple physical local area networks or are defined logically for separating user groups.

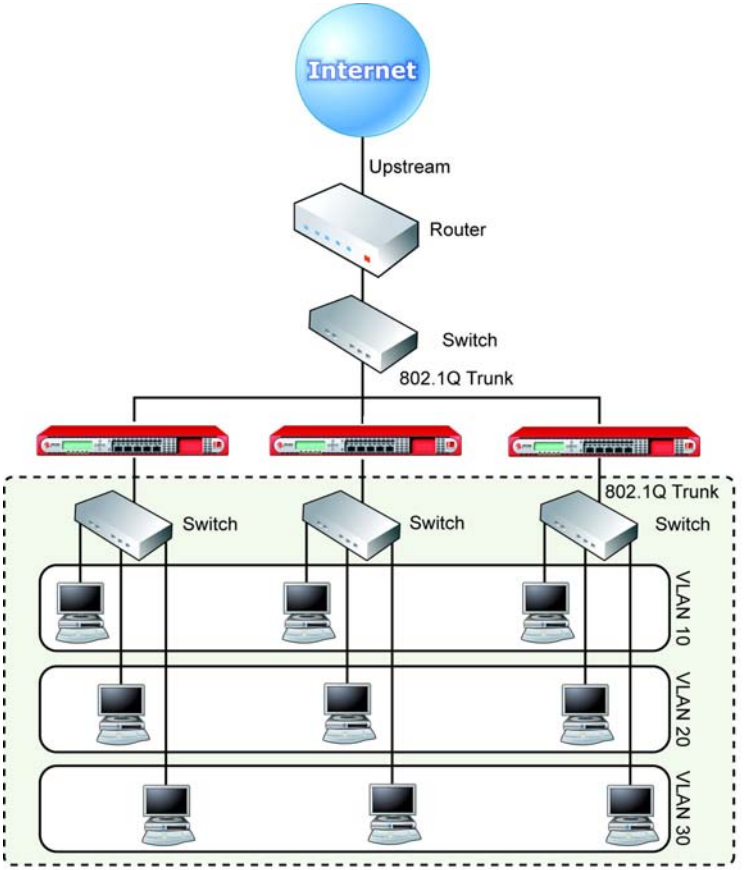


FIGURE 3-9. Multiple VLAN segments with each Network VirusWall protecting all segments

Single-switch VLAN Environment

The single-switch configuration that appears in *Figure 3-10* is only possible when using a switch that can be configured to carry individual VLAN traffic on specific physical ports. In *Figure 3-10*, VLAN 200 is assigned to ports 1 and 2, and VLAN 20 is assigned to ports 3 and 4. The upstream network is connected to port 4, the **EXT** port on Network VirusWall connected to port 3, The **INT** port on Network VirusWall is connected to port 2, and the downstream network connected to port 1.

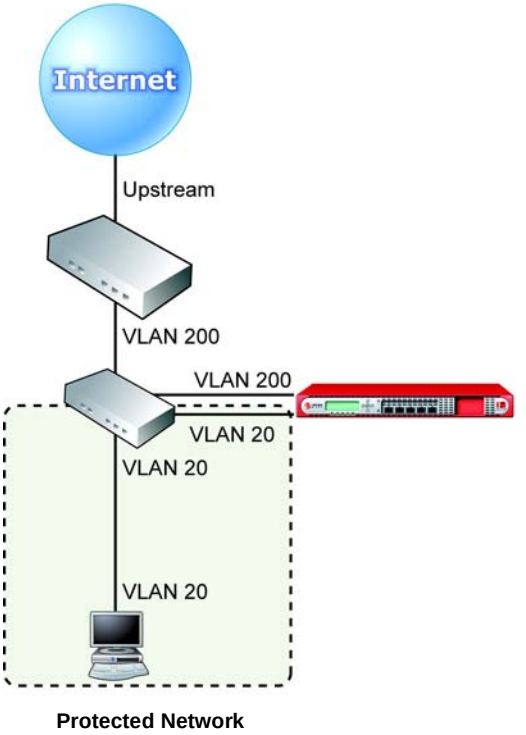


FIGURE 3-10. Single-switch configuration

Planning for Network Traffic

The scenario presented in *Key Network Segments/Important Network Assets* on page 3-12 is also a good example of how to plan for network traffic. There is a strategic advantage to positioning Network VirusWall in front of resources that clients access on a frequent and regular basis, 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 Network VirusWall significantly reduces the risk of virus infection. Identify other places on your network through which large amounts of traffic pass and consider positioning Network VirusWall at points where it can scan the most amount of traffic.

Determining the Number of Devices to Deploy

Determine the number of Network VirusWall 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 Network VirusWall to protect (see *Identifying What To Protect* on page 3-7)
- **Existing network device interfaces**– because Network VirusWall 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 devices
- **Desired effectiveness of protection**– to lower the risk of a virus outbreak spreading, segment several sections of your network with Network VirusWall devices
- **Desired degree of performance**– consider the number of clients and the amount of traffic Network VirusWall can handle (refer to the *Administrator's Guide > Network VirusWall 1200 and 2500 Feature Comparison* section for details)

Conducting a Pilot Deployment

Trend Micro recommends conducting a pilot deployment in a controlled environment to help you understand how Network VirusWall features work, determine how Network VirusWall 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™, and the Control Manager 3.0 services you plan to use. 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 Network VirusWall and/or other Control Manager services or components. 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 Network VirusWall performed with the antivirus installations on your network. This pilot evaluation can be rolled into the overall production and deployment plan.

Deploying Network VirusWall Based on an Operation Mode

A deployment plan is dependent upon the operating mode that you select. With the five (5) user-definable Copper Gigabit LAN ports and two (2) fiber-optic ports, more Network VirusWall deployment options are now available. This section provides the basic deployment scenario (see *page 3-22*) and deployment strategies based on the four (4) Operation Modes:

- Port Grouping (see *page 3-24*)
- Port Grouping with Failover (see *page 3-29*)
- Port Redundancy (see *page 3-35*)
- Port Redundancy with Failover (see *page 3-40*)

Tip: See *Network VirusWall Initial Tasks* on page 4-4 and *Verifying Network Support* on page 4-5 for checklists on how to prepare a Network VirusWall device for deployment.

A Basic Deployment Scenario

Network VirusWall can be installed on a network that contains Ethernet devices such as hubs, switches, and routers. Deploy Network VirusWall between a core switch that leads to the public network and an edge switch that protects a segment of the Local Area Network (LAN). It can also be installed between an edge switch and a hub.

Tip: Trend Micro recommends setting the **Port Grouping** Operation Mode and testing

---

Figure 3-11 illustrates a basic deployment scenario.

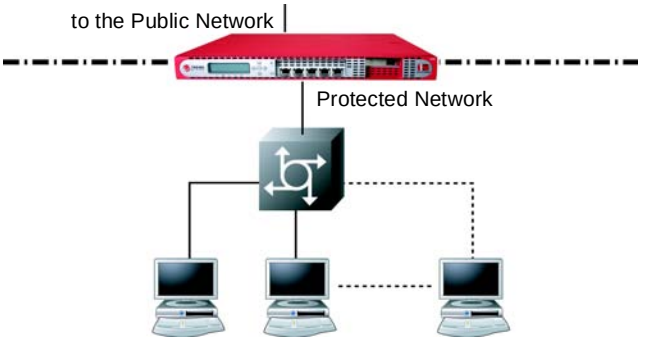


FIGURE 3-11. Basic deployment

A layer 2 (L2) or layer 3 (L3) device is connected to the Network VirusWall internal (**INT**) port, creating a Protected Network segment, and the connection to the external (**EXT**) port leads to the public network.

Network VirusWall protects your network as follows:

- Scans traffic to and from clients on the Protected Network
- Prevents clients that violate your security policies from gaining access to resources outside of the Protected Network
- Isolates the clients 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 Network VirusWall 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 *Port Grouping Deployment* and *Port Redundancy Deployment*
- Failover, proceed to *Port Redundancy Deployment* and *Port Redundancy with Failover Deployment*

Port Grouping Deployment

Port grouping, also referred to as port-based virtual LAN (VLAN), allows you to deploy a Network VirusWall device that will handle up to four (4) port-based VLANs. The port grouping Operation Mode makes use of all five interfaces.

Tip: Network VirusWall supports up to 50 IEEE 802.1Q-compliant VLAN tags.

Figure 3-12 illustrates how to set the Network VirusWall interfaces for this type of deployment.

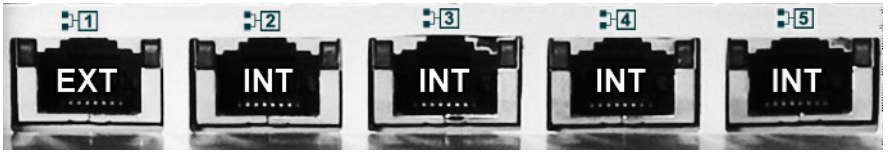


FIGURE 3-12. Interface allocation for a port grouping deployment

Figure 3-13 illustrates a port grouping deployment.

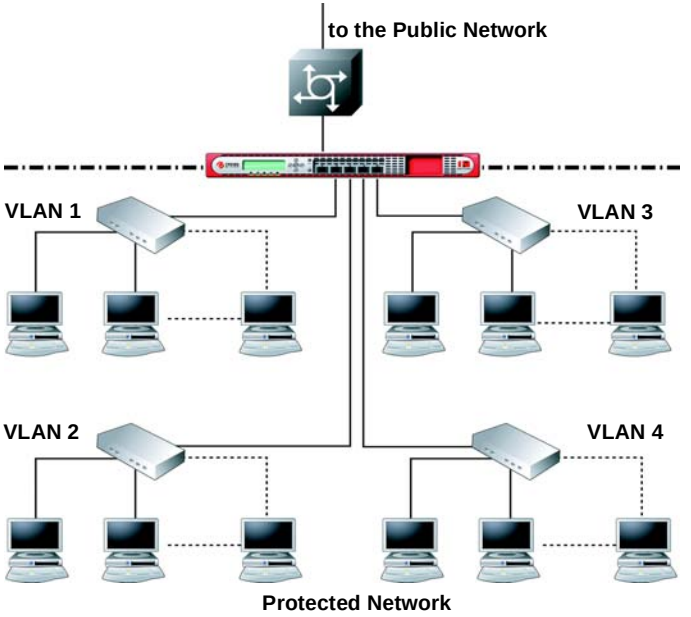


FIGURE 3-13. Port grouping deployment

Both types of fiber-optic server adapter configurations can apply to this mode.

Table 3-5, “Supported operation modes for a single-port fiber card,” on page 3-25 shows the various possible port configurations using a single-port LX fiber card.

	On Board					Single Port LX Card
	Port 1	**Port 2**	**Port 3**	**Port 4**	**Port 5**	**Fiber**
1	External	Internal	Internal	Internal	Internal	n/a
2	Disabled	Internal	Internal	Internal	Internal	External
3	External	Internal	Internal	Internal	**Failover**	n/a
4	Disabled	Internal	Internal	Internal	**Failover**	External

TABLE 3-5. Supported operation modes for a single-port fiber card

Table 3-6, “Supported operation modes for a dual-port fiber card installed,” on page 3-26 lists the various possible port configurations using a dual-port SX card.

	On Board					Dual Port SX Card	
	Port 1	**Port 2**	**Port 3**	**Port 4**	**Port 5**	**Fiber 1**	**Fiber 2**
1	External	Internal	Internal	Internal	Internal	n/a	n/a
2	Disabled	Disabled	Disabled	Disabled	Disabled	External	Internal
3	Disabled	Internal	Internal	Internal	Internal	External	Disabled
4	Disabled	Internal	Internal	Internal	Internal	Disabled	External
5	External	Internal	Internal	Internal	**Failover**	n/a	n/a
6	Disabled	Disabled	Disabled	Disabled	**Failover**	External	Internal
7	Disabled	Internal	Internal	Internal	**Failover**	External	Disabled
8	Disabled	Internal	Internal	Internal	**Failover**	Disabled	External

TABLE 3-6. Supported operation modes for a dual-port fiber card installed

The following points apply to a port grouping deployment strategy:

- A VLAN can represent one network segment
- Network VirusWall protects each VLAN provided that you set all VLAN tags in the **VLAN Settings**
- Set all the VLAN tags in the Preconfiguration console > **VLAN Settings** menu.
- Only one EXT exists, which all four INT share
- Each INT is connected to the access switch for each VLAN
- With Network VirusWall, an infected packet detected in one segment does not crossover other LAN segments
- A Network VirusWall device in a Port Grouping mode can enable failopen (LAN bypass) when it encounters a hardware or system error that prevents it from filtering network packets

Multi-Protection Zone Configuration Without Failover

In this sample deployment scenario Network VirusWall 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.

- **External port** — Fiber 1 (or Fiber 2)
- **Internal port** — Copper 2, Copper 3, Copper 4, Copper 5 (or Fiber 2)

Figure 3-14. *Port grouping without failover, multi-protection zone configuration, 1 external fiber port* on page 3-27 illustrates this deployment scenario.

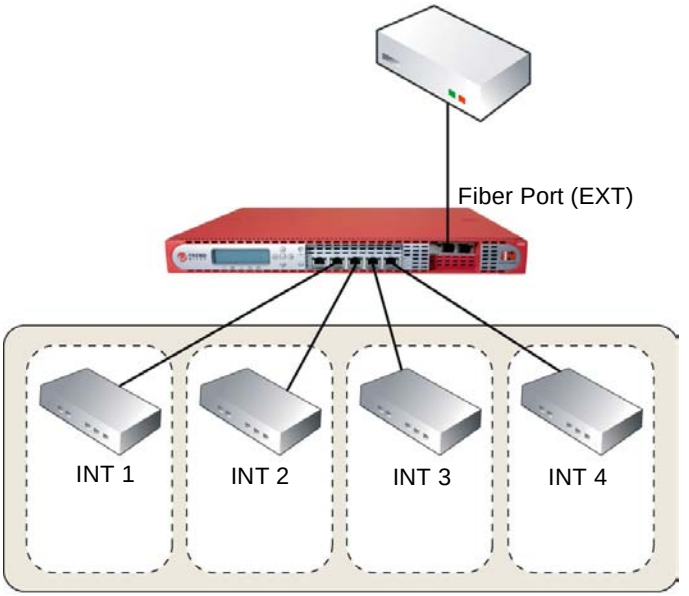


FIGURE 3-14. Port grouping without failover, multi-protection zone configuration, 1 external fiber port

Failopen Considerations

Consider the following points when implementing Port Grouping or Port Redundancy Operation Mode:

- Network VirusWall reserves ports 1 and 2 for failopen

  If the switches used in your network do not support auto MDI/MDI-X, use a crossover and non-crossover cable combination for ports 1 and 2. This configuration enables failopen to work. Otherwise, an invalid cable type combination prevents Network VirusWall to failopen and can result in network issues. Refer to the device documentation to determine whether your L2 switches support auto MDI/MDI-X.
- If there is no power supplying a Network VirusWall device (that is, the AC power receptacle is disconnected from the power outlet or actual device), failopen will not work
- The total length of the network cable connecting the Network VirusWall ports 1 and 2 and other devices must not be more than 100 meters (328 feet)

Note: This constraint only applies to failopen deployments. The network cable connecting port 1 should be equal to or shorter than 50 m. Consequently, the network cable connecting port 2 should be equal to or shorter than 50 m. 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** Operation Mode, Network VirusWall automatically disables failopen

See *Setting the Operation Mode* on page 5-17 for details on how to set the Operation Mode.

Port Grouping with Failover Deployment

There are two Network VirusWall 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 program file version.

Tip: Network VirusWall operates in active-active failover mode. An active-active failover deployment consists of one Primary Network VirusWall device and one Secondary device processing traffic.

Refer to the *Administrator's Guide* for details on failover and other high availability concepts.

Figure 3-15 illustrates how to set the Network VirusWall interfaces for this type of deployment.

FIGURE 3-15. Interface allocation for a port grouping with failover deployment

Figure 3-16 illustrates a port grouping with failover deployment applied to a partial mesh topology.

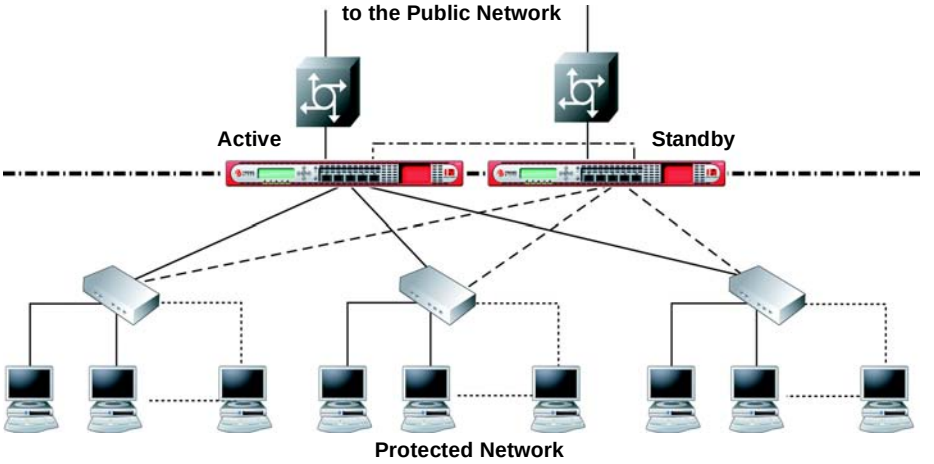


FIGURE 3-16. Port grouping with failover deployment, partial mesh

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

- Only one **EXT** port exists, which a maximum of three **INT** share
- One **FAILOVER** port exists, which connects to the other device in a failover pair via an RJ-45 crossover cable

Note: In this mode, port 5 can be allocated as the **FAILOVER** port.

- The failover pair has one Active and one Standby device

Note: The Active and Standby roles are for Control Manager management purposes only. These roles do not refer to whether a device can filter packets.

- Both devices filter network packets
- If the Active device fails, the Standby device changes its role to Active and communicates with the Control Manager server

- A Control Manager server manages the Active device
- The managed product representing the Active device appears on the Control Manager management console
- A Standby device cannot be configured through the Preconfiguration or Control Manager management console

  The former will replicate the configuration setting and update the antivirus components (except the program file) to the latter.
- 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 *Administrator's Guide > Understanding the Network VirusWall Security Components* for details on Network VirusWall components.

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

See *Setting the Operation Mode* on page 5-17 for details on how to set the Operation Mode.

In partial mesh design only the connection between Access L2 and distribution L3 switches has redundant links (see Figure 3-17. *Port grouping with failover, multi-protection zone configuration, 1 external fiber port* on page 3-32). The connection between distribution L3 and core L3 switches has only single link.

A network administrator can install two Network VirusWall (NVW) devices between L2 and L3 switches or distribution L3 and core L3 switches by linking them together using a failover link. In this deployment scenario, the two NVW devices start to synchronize the information and the administrator can manage the "Active" NVW device (can send commands and set command/logs) using the Trend Micro Control Manager server.

- **External port** — Fiber 1 (or Fiber 2)
- **Internal port** — Copper 2, Copper 3, Copper 4
- **Failover port** — Copper 5

Figure 3-17. *Port grouping with failover, multi-protection zone configuration, 1 external fiber port* on page 3-32 illustrates this deployment scenario.

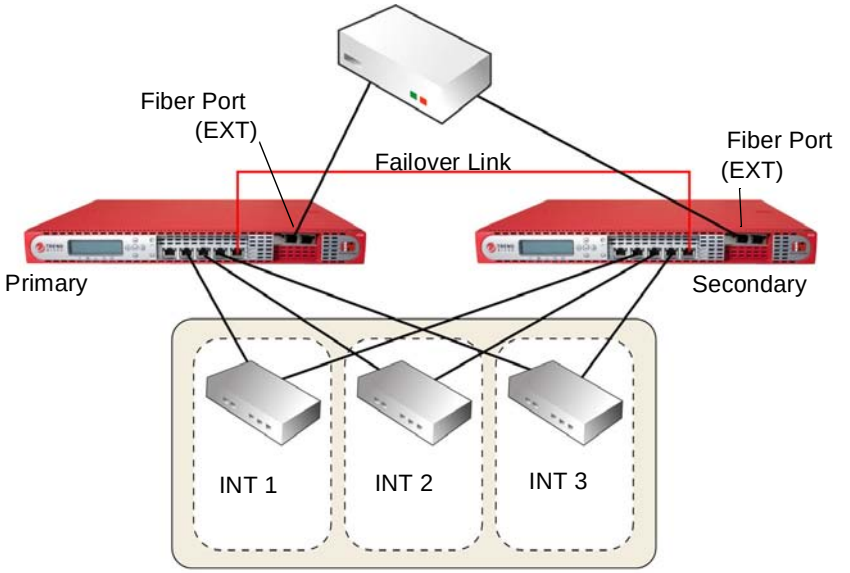


FIGURE 3-17. Port grouping with failover, multi-protection zone configuration, 1 external fiber port

Failover Considerations

Consider the following points when implementing a failover-based Operation Mode:

- Network VirusWall recognizes port 5 as the FAILOVER port
- A Network VirusWall failover pair must have identical devices– same model and running the same Network VirusWall program file version

  Otherwise, the failover solution cannot work.
- Check whether the core and LAN switches connected to the Network VirusWall devices have Spanning Tree Protocol (STP) enabled

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

- Do not automatically update 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 the *Administrator's Guide* > *Updating the Program File Manually in a Failover Deployment* for instructions to manually update the program file.

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

Deployment Scenario: 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 (internal) connects to an L2 switch (or segment) via a VLAN trunked link as the protection zone. The fiber-optic port (external) connects to an external L2 or L3 switch.

- External port — Fiber 1
- Internal port — Fiber 2

Figure 3-18. *Single pair configuration with or without 802.1q VLAN* on page 3-34 illustrates this deployment scenario.

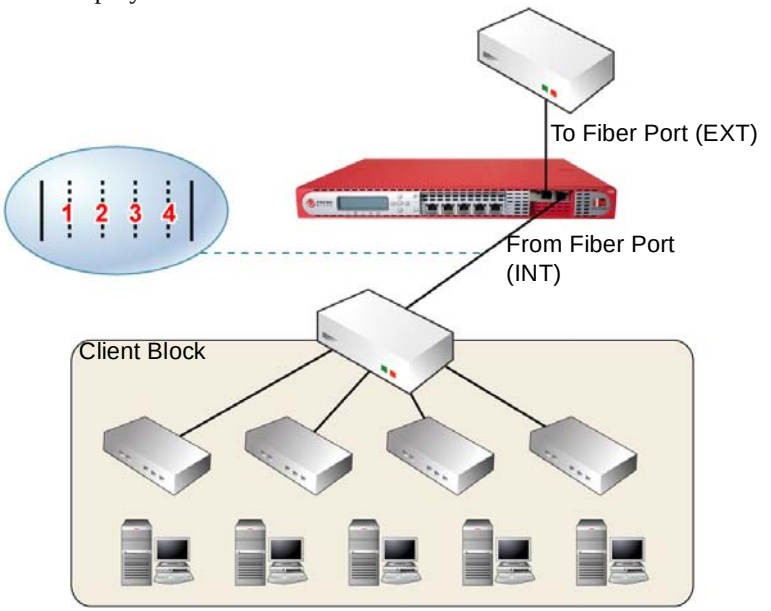


FIGURE 3-18. Single pair configuration with or without 802.1q VLAN

Case 2: With Failover

In this scenario two L2 or L3 switches configure as a port-to-port channel (see Figure 3-19. *Case 2: Failover pair with single-switch dual-port multi-mode fiber* on page 3-35). The redundant uplinks of the L2 switch connect to two individual NVW devices.

- External port — Fiber 1
- Internal port — Fiber 2
- Failover port — Copper 5

Figure 3-19. *Case 2: Failover pair with single-switch dual-port multi-mode fiber* on page 3-36 illustrates this deployment scenario.

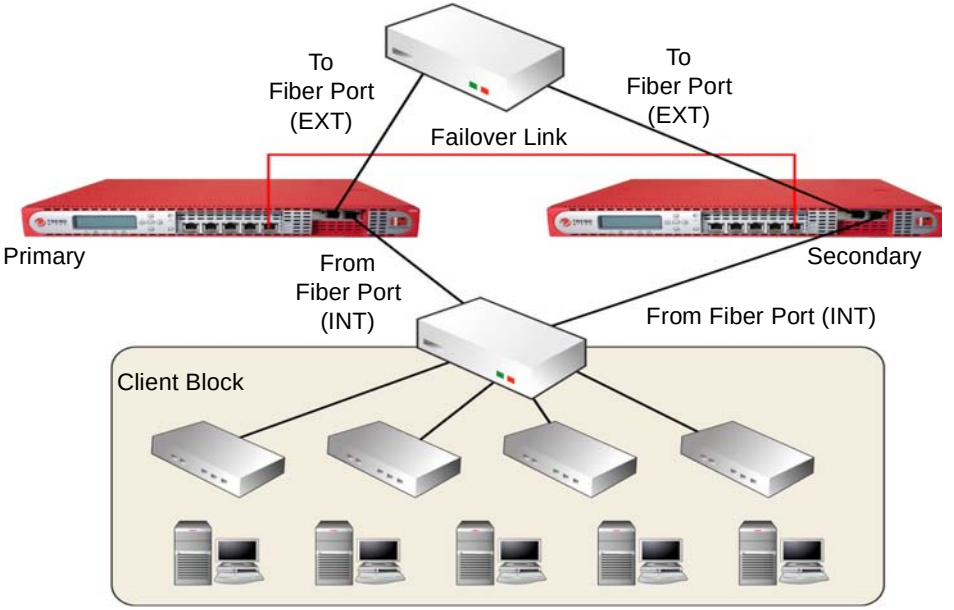


FIGURE 3-19. Case 2: Failover pair with single-switch dual-port multi-mode fiber

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. Two pairs of **INT/EXT** make up the port groups.

Figure 3-20 illustrates how to allocate the Network VirusWall interfaces for this type of deployment.

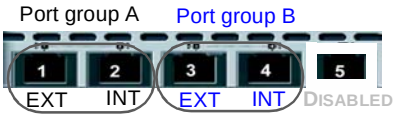


FIGURE 3-20. Interface allocation for a port redundancy deployment

Using a redundant physical link implementation allows Network VirusWall 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 3-21 represents a port redundancy deployment.

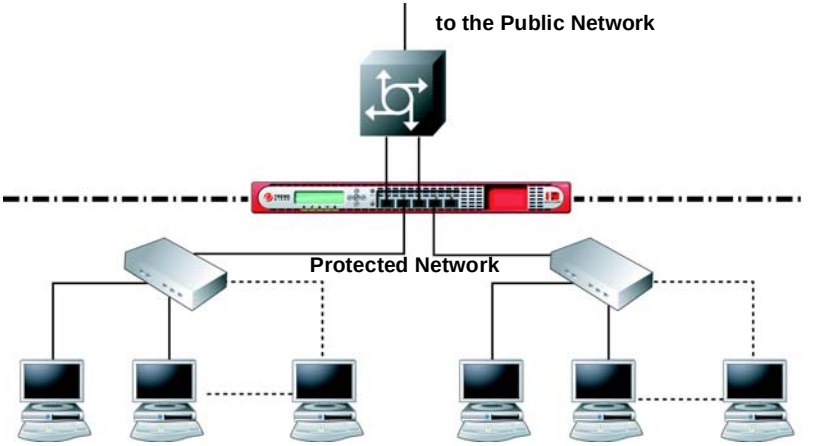


FIGURE 3-21. Port redundancy deployment

	On Board					Dual Port SX Card	
	Port 1	Port 2	Port 3	Port 4	Port 5	Fiber 1	Fiber 2
1	External 1	Internal 1	External 2	Internal 2	Disabled	n/a	n/a
2	Disabled	Internal 1	Disabled	Internal 2	Disabled	External 1	External 2
3	External 1	Internal 1	Disabled	Disabled	Disabled	External 2	Internal 2
4	External 1	Internal 1	External 2	Internal 2	Failover	n/a	n/a
5	Disabled	Internal 1	Disabled	Internal 2	Failover	External 1	External 2
6	External 1	Internal 1	Disabled	Disabled	Failover	External 2	Internal 2

TABLE 3-7. Supported operation modes for a dual-port fiber-optic card installed

The following points apply to a port redundancy deployment strategy:

- Two port groups are available– port group A (**INT A/EXT A**) and port group B (**INT B/EXT B**)
- If you enable failopen, Network VirusWall 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 device
- Network VirusWall supports the spanning tree protocol (STP). As described in 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, Network VirusWall 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.

Network VirusWall 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 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 3-28 for more information.

- Network VirusWall 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.

Port Redundancy Considerations

Consider the following points when implementing a port redundancy deployment:

- A redundant group must include two port groups with different EXT and INT ports
- A port group consists of one EXT port and one INT port
- 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
- The INT port cannot be shared between port groups; the EXT port can be shared between port groups
- 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 3-32 for details)

See *Setting the Operation Mode* on page 5-17 for details on how to set the Operation Mode.

Deployment Scenario: 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.

- **External port** — Fiber 1, Fiber 2
- **Internal port** — Copper 2, Copper 4

Figure 3-22. *Point-to-Point Links Using Two Pairs of Fiber-Copper Ports* on page 3-39 illustrates this deployment scenario.

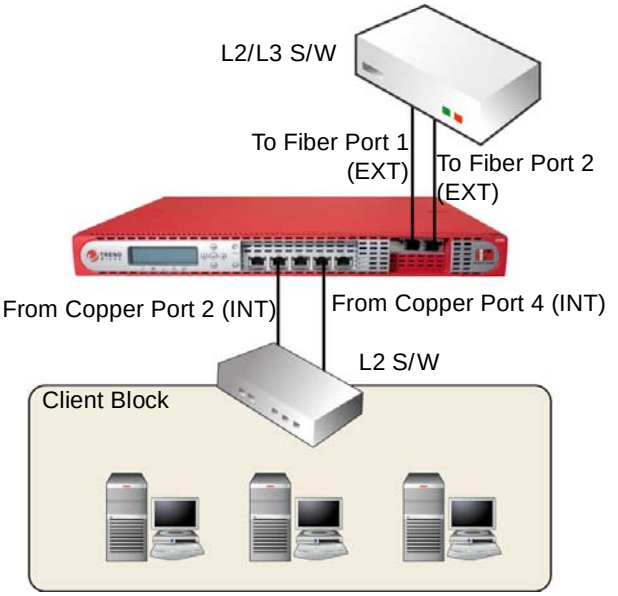


FIGURE 3-22. Point-to-Point Links Using Two Pairs of Fiber-Copper Ports

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

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

- **External port** — Copper 1, Fiber 1
- **Internal port** — Copper2, Fiber 2

Figure 3-23. *Point-to-Point Links - One Pair of Copper Ports with One Pair of Fiber Ports* on page 3-40 illustrates this deployment scenario.

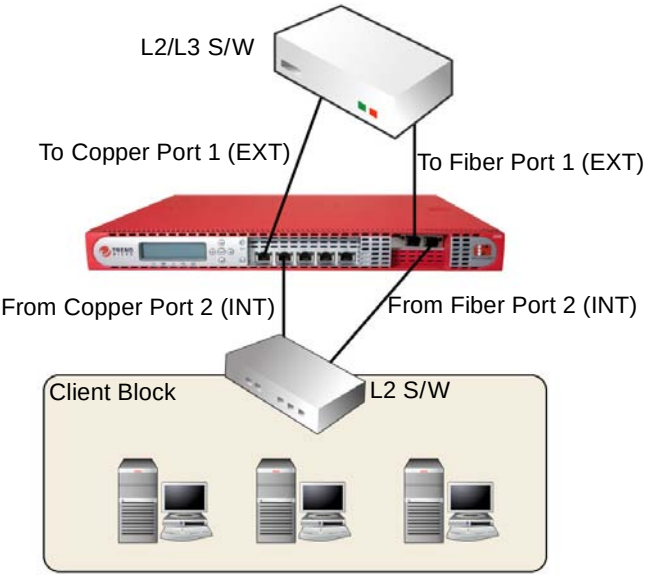


FIGURE 3-23. Point-to-Point Links - One Pair of Copper Ports with One Pair of Fiber Ports

Port Redundancy with Failover Deployment

To maximize the benefit of Port Redundancy operating mode, configure high availability along with the port groups. Doing so helps guarantee that if one of the Network VirusWall device fails, all functions of the matching devices are maintained. This option allows uninterrupted packet filtering and outbreak monitoring capabilities.

Port redundancy with failover deployment requires two port groups and a failover port. *Figure 3-24* illustrates the interface allocation.

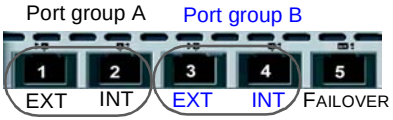


FIGURE 3-24. Interface allocation for a port redundancy with failover deployment

Trend Micro recommends implementing a port redundancy with failover deployment in a full mesh topology. *Figure 3-25* illustrates this strategy.

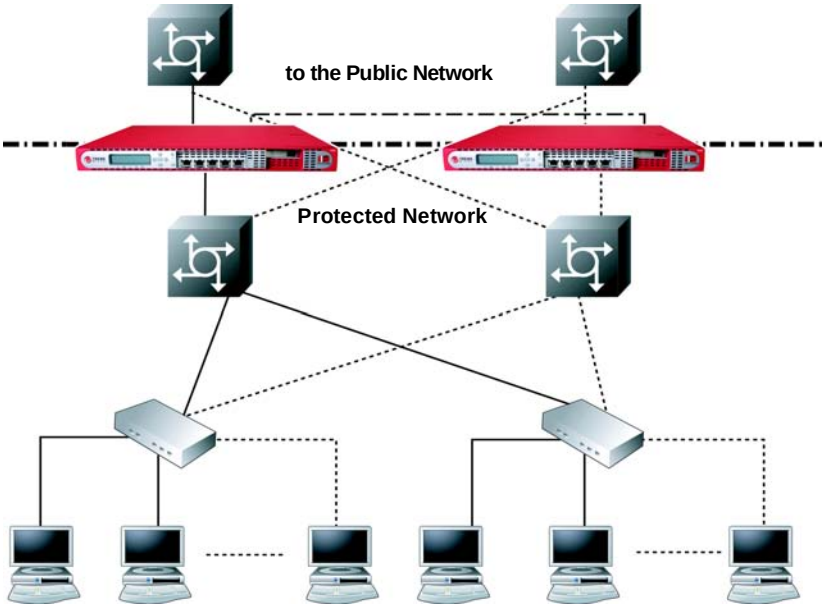


FIGURE 3-25. Port redundancy with failover deployment on a full mesh topology

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

- Two port groups and a failover port are available—port group A (**INT1/EXT1**), port group B (**INT2/EXT2**), and the **FAILOVER** port
- The two devices in a failover pair must be the same model and running the same Network VirusWall image
- If one device in the failover pair fails, the L2 or L3 device blocks the port connected to the failed Network VirusWall device and redirects traffic to the Standby pair
- This strategy applies the active-active failover mode—both devices can filter network packets
- However, each device has a role—Active or Standby, which determines how Control Manager manages a device
- Only the Active device is configurable from the preconfiguration or management console. (There is only one managed product representing the failover pair.)

Note: Standby device settings are viewable through the Preconfiguration console when using the monitor account.

- To determine each others' failover status, each device polls the other every one (1) second

Tip: See *Failover Considerations* on page 3-32 for more information about failover.

When NVW configures to port redundancy mode with failover, assign the fifth port as the failover port and connect the device to another NVW device.

- **External port** — Fiber 1, Fiber 2
- **Internal port** — Copper 2, Copper 4
- **Failover port** — Copper 5

Figure 3-26. *L2 Redundant Links: Two Pairs of Fiber-Copper Ports with Failover* on page 3-43 illustrates this deployment scenario.

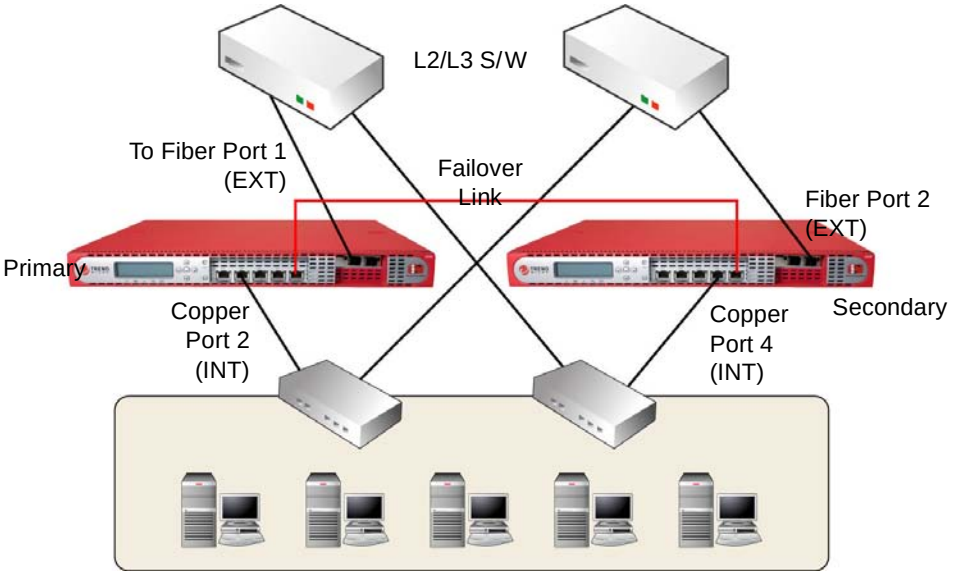


FIGURE 3-26. L2 Redundant Links: Two Pairs of Fiber-Copper Ports with Failover

Administrators can also configure NVW to port redundancy mode by using two fiber ports as another pair for redundancy.

- **External port** — Copper 1, Fiber 1
- **Internal port** — Copper 2, Fiber 2

Figure 3-27. *L2 Redundant Links: One Pair of Copper Ports with One Pair of Fiber-optic Ports Without Failover* on page 3-44 illustrates this deployment scenario.

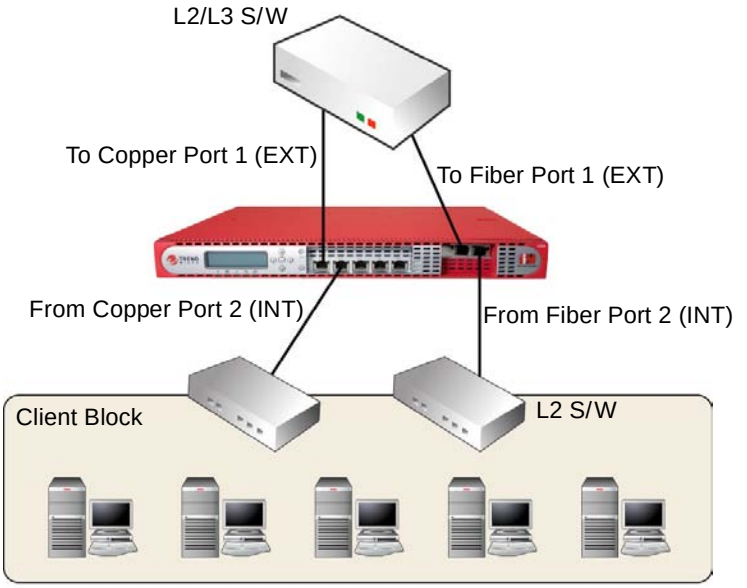


FIGURE 3-27. L2 Redundant Links: One Pair of Copper Ports with One Pair of Fiber-optic Ports Without Failover

When configuring NVW to port redundancy mode, an administrator can use two fiber ports as another port pair for redundancy and the fifth port to connect to another NVW device.

- **External port** — Copper 1, Fiber 1
- **Internal port** — Copper 2, Fiber 2
- **Failover port** — Copper 5

Figure 3-28. *L2 Redundant Links: One Pair of Copper Ports with One Pair of Fiber Ports with Failover* on page 3-45 illustrates this deployment scenario.

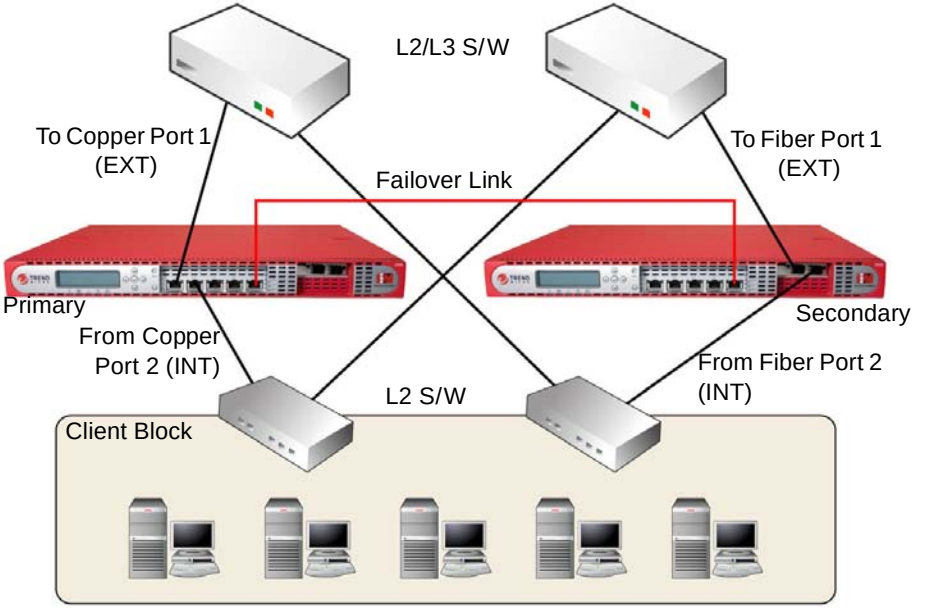


FIGURE 3-28. L2 Redundant Links: One Pair of Copper Ports with One Pair of Fiber Ports with Failover

See *Setting the Operation Mode* on page 5-17 for details on how to set the Operation Mode.

Chapter 4

Preparing for Preconfiguration

Preconfiguring Network VirusWall requires the completion of Control Manager and Network VirusWall-related tasks.

To perform preconfiguration:

1. Plan and determine the deployment strategy (see *page 3-2*).
2. Prepare the Control Manager server and Network VirusWall device (see *page 4-2*).
3. Perform preconfiguration (see *page 4-20*).

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

This chapter contains the following topics:

Preparing for Preconfiguration

Complete the following tasks before installing a Control Manager server and preconfiguring Network VirusWall:

- Control Manager pre-installation tasks (see *page 4-2*)
- Network VirusWall initial tasks (see *page 4-4*)

Control Manager Pre-installation Tasks

Note: For usability, Control Manager-related information is appended in this section. Always refer to the latest Control Manager documentation available at `http://www.trendmicro.com/download/`.

Installing Control Manager for the First Time

Complete the following pre-installation tasks:

- Determine and obtain the following information
  - Control Manager Registration Key and Activation Code (see *page 4-6*)
  - An Internet connection to obtain the Activation Code
  - Relevant target server address and port information
  - Security Level you want to use for the Control Manager server and Network VirusWall or other managed product communication

    Note: To communicate, Control Manager requires exclusive use of ports 10319 and 10198 (see *page A-4*).
    For more information about the Control Manager security levels, refer to the Control Manager *Online Help*.

- Consider the following Control Manager database-related points:
  - Select if you want to use an SQL server with Control Manager

    If the SQL server is located on a server other than the Control Manager server, obtain its IP address, FQDN, or NetBIOS name. If there are multiple instances of the SQL server, identify the one that you intend to use.

- Prepare the following information about the SQL database to be used for Control Manager:
  - User name for the database
  - Password
- Determine the number of managed products Control Manager will handle

  If an SQL server is not detected on your server, Control Manager will install MSDE, which can only handle a limited number of connections.

Tip: Refer to the Microsoft MSDN Website for additional MSDE information (`http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnmsde/html/msderoadmap.asp`).

- Use the *System Checklists* on page A-1 to help you with the Control Manager server installation

Proceed to *page 4-9* and *page 4-10* for Control Manager requirements and installation procedures.

Existing Control Manager Installation

If you already have Control Manager 3.0 installed, complete the following tasks before performing a Network VirusWall preconfiguration:

- Apply the Control Manager Patch 1 for Service Pack 2 (see *page 4-16*)
- Check whether the following Control Manager and other application services are running:
  - SQL Server Agent service
  - Trend Micro Common CGI service
  - Trend Micro Control Manager
  - Trend Micro Management Infrastructure
  - Trend Micro Network Time Protocol service

Proceed to *page 4-16* for Control Manager patch and hot fix instructions.

Network VirusWall Initial Tasks

Complete the following tasks before you preconfigure Network VirusWall:

- Verify whether your network will support Network VirusWall and the designated Operation Mode (see *page 4-5*)
- Test the Network VirusWall failopen functionality by setting the **Port Grouping** Operation Mode (see *page 3-24*)

  This ensures network traffic can still pass through the Network VirusWall device when the later encounters a hardware or system error that prevents it from filtering network packets.
- Select the Operation Mode (see *page 3-22*)
- Determine the Network VirusWall `admin` account password

Tip: There are two accounts available in Network VirusWall– `admin` and `monitor`. Both accounts use `admin` and `monitor`, respectively, as their default password. If you have misplaced or forgotten the account's password, see *page 6-2*.

- Determine the managed product host name for the Network VirusWall device or devices in a failover pair
- Prepare a machine that has a terminal communications software, such as HyperTerminal for a Windows server or Minicom for a Linux server (see *page 5-5*)
- Guarantee that network connection is present in the environment running the Control Manager server

  From the computer that you will use for preconfiguration, send an ICMP request to the Control Manager server to check the network connection. For example:

  ```
  # ping {CM server host name or IP address}
  ```

Tip: Use the host name if the Control Manager server is using DHCP.

- Obtain the public encryption key (see *page 4-7*)
- Determine the Control Manager server IP address and host name
- Determine the Control Manager server `root` account, which will be used to register the device to the Control Manager server

Verifying Network Support

Use the following list to verify whether your environment can support Network VirusWall and the designated Operation Mode:

- Position Network VirusWall on the part of the network where it can communicate with the Control Manager server (see *page 3-4*)
- Enable STP (spanning tree protocol) for switches deployed in the network if you will set **Port Redundancy** Operation Mode

  When one of the links fails, Network VirusWall 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.
- The network connection between the Control Manager server and Network VirusWall device is present

  From the Control Manager server, ping the Network VirusWall device to check whether the connection between the two products can be established.

  Tip: Enable the Preconfiguration console > **Advanced Settings** > **Allow ICMP requests from other computers** option to send a ping request and get a ping response to and from the Network VirusWall device.

  In a failover deployment, the failover pair will not switch roles if the Active pair is unable to connect to the Control Manager server. In this situation, the Active device still works. However, the logs will not be delivered to the Control Manager server due to network connection issues. Consequently, you cannot configure an Active device from the Control Manager server if the connection between the two products cannot be established. Manually switch the Active/Standby roles through the Preconfiguration console > **Operation Mode** menu if the Active device is unable to connect to the Control Manager server due to network connection problem. See *page 3-32* for additional failover considerations.
- If the Control Manager server on your network belongs to a VLAN, bind Network VirusWall to the same VLAN

  This ensures effective communication between the Control Manager server and Network VirusWall.

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

  Otherwise, a cable that is longer than the maximum length will prevent failopen from working. See *page 3-28* for additional failopen considerations.

Obtaining the Activation Code

The Trend Micro sales team or sales representative provides the Control Manager Registration Key. Use the Registration Key to obtain a full version Activation Code.

Note: If you already have a Control Manager Activation Code, ignore these instructions and proceed to Control Manager activation (see *page 4-10*).

To obtain a full version Activation Code:

1. Go to the Trend Micro Online Registration Website (`https://olr.trendmicro.com/registration`). The Online Registration page of the Trend Micro Website opens.
2. Perform one of the following:
   - If you are an existing Trend Micro customer, log on using your **logon ID** and **password**
   - Otherwise, if you are a new customer, click **Register Your Product** under **New customer** registration
3. On the Enter Registration Key page, type or copy the **Control Manager Registration Key**, and then click **Continue**.
4. On the Confirm License Terms page, read the license agreement, and then click **I accept to the terms of the license agreement**.
5. On the Confirm Product Information page, click **Continue Registration**.
6. Fill out the online registration form, and then click **Submit**.
7. Click **OK** twice.

After the registration is complete, Trend Micro sends an Activation Code via email, which you can then use to activate Control Manager and other applicable Trend Micro services.

Obtaining the Public Encryption Key

Network VirusWall makes use of a public encryption key (E2EPublic.dat) to register and communicate with the Control Manager server. Without this key, Network VirusWall is unable to register to Control Manager. Without Control Manager, you cannot administer a Network VirusWall device. See *page 1-3*

Define how Network VirusWall obtains the public encryption key using the **Device Settings** menu available in the Preconfiguration console (see *page 5-11*).

To obtain the public encryption key:

- Manually download and import the public key from an existing Control Manager server

  Tip: Save a copy of `E2EPublic.dat` and note its location on the preconfiguration machine.

- Automatically import the public encryption key during preconfiguration

  Tip: Trend Micro recommends importing `E2EPublic.dat` automatically. Network VirusWall automatically downloads the public key when it registers with Control Manager.

Preparing Other Trend Micro Products

When your network has Trend Micro™ OfficeScan Corporate Edition™ or ServerProtect™ for Windows™ servers installed, complete the following tasks before preconfiguring Network VirusWall:

- Check whether the OfficeScan and ServerProtect servers are applying the New Pattern File Numbering Format (NPF) Service Pack
- Otherwise, visit `http://www.trendmicro.com/en/support/npf/overview.htm` for more information on how to apply the applicable NPF Service Pack to the OfficeScan or ServerProtect server

---

Tip: Network VirusWall supports OfficeScan Corporate Edition 5.5 SP1 (or newer) and ServerProtect 5.5 for Windows (or newer). Refer to the *Administrator's Guide* > *Policy Enforcement* topic for the list of supported antivirus products and other Policy Enforcement details.

Network VirusWall 2500 blocks OfficeScan or ServerProtect clients that have not applied the NPF Service Pack. If this happens, Trend Micro recommends the following workaround:

- Include the IP address of `www.trendmicro.com` in the Safe Sites list

  Configure the Network VirusWall Safe Sites list via the Control Manager management console > **Configuration** > **Exception List** screen. See *Enabling Safe Sites for Blocked and Quarantined Clients* topic in the Administrator's Guide for instructions.

- Temporarily include the IP address of the OfficeScan or ServerProtect client in the Policy Enforcement Exception list

  Configure the Network VirusWall Policy Enforcement Exception list via the Control Manager management console > **Configuration** > **Exception List** screen. Doing so allows the blocked or quarantined OfficeScan or ServerProtect client to temporarily access `http://www.trendmicro.com/en/support/npf/overview.htm`, obtain, and install NPF Service Pack package to comply with the antivirus and vulnerability-elimination policies. See *Enabling the Policy Enforcement Exception List* topic in the Administrator's Guide for instructions.

Note: Remove the OfficeScan or ServerProtect client from the Policy Enforcement Exception list if it does not originally belong to the list. Refer to the *Potential Exception Clients list* in the *Administrator's Guide* for characteristics of an ideal exempted client.

Control Manager System Requirements

The following table lists the minimum system requirements for a Control Manager server.

SPECIFICATIONS	MINIMUM REQUIREMENTS
CPU	Intel Pentium™ III Processor 450MHz or higher
Memory	256MB RAM
Disk space	300MB for Control Manager Standard Version 300MB for MSDE 2000 (Optional)
Operating system	Microsoft™ Windows™ Server 2003 Standard / Enterprise Edition, Microsoft Windows 2000 Server / Advanced Server with Service Pack 3, Microsoft Windows NT 4 with Service Pack 6a
Web server	Microsoft Internet Information Server (IIS) 4.0 or higher
Database	Microsoft SQL Server Desktop Engine (MSDE) 1.0 / 2000 (2000 + SP3 is recommended) Microsoft SQL Server 7.0 Microsoft SQL Server 2000 (2000 + SP3 is recommended)
Others	SQL ODBC driver 3.7 or higher Windows Installer (included in Control Manager package)
Management console	Browser- Microsoft Internet Explorer 5.5 with SP2 or higher Java VM- Microsoft Version 5.0.0.3805 or higher

TABLE 4-1. Minimum system requirements for a Control Manager server

Note: For recommended system requirements and sizing recommendations, refer to the *Trend Micro Control Manager Getting Started Guide*, available in Portable Document Format (PDF) on the *Trend Micro Solutions CD for Network VirusWall 2500*.

Installing Control Manager 3.0

Once you have verified that the target server is ready (see *Control Manager Pre-installation Tasks* on page 4-2), install Control Manager.

To install Control Manager 3.0:

Step 1. Register and activate the product and services (see *page 4-10*).

Step 2. Specify Control Manager server file location and communications settings (see *page 4-10*).

Step 3. Choose and configure database information (see *page 4-11*).

Step 4. Set up root account and configure proxy server (see *page 4-12*).

Step 5. Configure notification settings (see *page 4-13*).

Step 1: Register and activate the product and services

1. Obtain the Activation Code.

   See *page 4-6* for instructions on how to obtain the Activation Code. Otherwise, if you already have an Activation Code, proceed to *Step 2*.

2. From the target Control Manager server, insert the *Trend Micro Solutions CD for Network VirusWall 2500*. The setup program starts.
3. Click **Trend Micro Control Manager** and click **Install**. The Control Manager installer starts.

Step 2: Specify Control Manager server file location and communications settings

1. From the **Product Activation (Step 2)** screen, click **Next**. Specify a location for Control Manager files. The default location is `C:\Program Files\Trend Micro`.
2. Click **Next**. Select a security level and network address. This is the network address you use during Network VirusWall preconfiguration.

Note: If you use the host name or FQDN to identify your server, check whether this name can be resolved on Network VirusWall 2500, otherwise Network VirusWall 2500 cannot communicate with the Control Manager server.

---

3. Click **Next**. The **Choose Destination Location** screen appears.
4. Specify the location of the Control Manager backup and authentication files. Click **Browse** to specify an alternate location.
5. Click **Next**. The **Specify Web Server Information** screen appears.
6. From the **IP address** list, select the IP address or FQDN/host name you want to use for the Control Manager management console.

Step 3: Choose and configure database information

1. Click **Next**. The **Setup Control Manager Database** screen appears.
2. Select a database to use with Control Manager.
   - **Install Microsoft Data Engine (MSDE)**

     The Microsoft SQL Server Desktop Engine (MSDE) is suitable only for a small number of connections. An SQL server is preferable for large Control Manager networks.

     Note: Installing MSDE requires restarting the server after Setup finishes. See *page 4-14*.

   - **SQL Server**– the setup program automatically selects this option if an SQL server is detected on your server. Provide the following information:
     - **SQL Server (\Instance)**
     - **SQL Server Authentication**

     WARNING! *For security reasons, do not use an SQL database that is not password protected.*

3. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is “db_ControlManager”.
4. Click **Next** to create the required database.

Step 4: Set up root account and configure proxy server

1. Click **Next**. The **Create Root Account** screen appears:

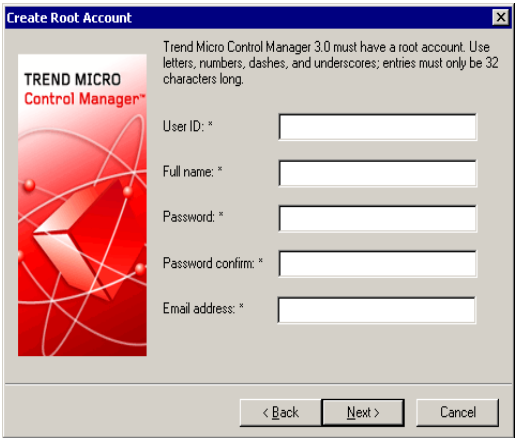


FIGURE 4-1. Creating the Control Manager *root* account

2. Provide the following account information:
   - User ID– **this is the root ID you use when setting the Device Settings through preconfiguration** (see *page 5-9*.)
   - Full Name
   - Password
   - Password confirmation
   - Email address
3. Click **Next**.

   If you use a proxy server to connect to the Internet, select the **Enable proxy server** check box, and then set the following:
   - Proxy server– type the FQDN, IP address, or NetBIOS name of the server
   - Port– type the proxy port number
   - Proxy type– click the appropriate proxy type: HTTP or SOCKS
   - User name
   - Password

4. Click **Next**. The system verifies the proxy settings you entered. The proxy configuration screen for Trend VCS agents appears. If you are using legacy versions of Control Manager, refer to the *Trend Micro Control Manager Getting Started Guide* on the *Trend Micro Solutions CD for Network VirusWall*.

Step 5: Configure notification settings

1. Click **Next**. The **Notification Settings** screen appears.
2. Configure the settings used for the Control Manager notification functions.
3. Click **Next**. The **Specify Message Routing Path** screen appears.
4. These settings allow you to adapt Control Manager to your company's existing security systems. Select the appropriate route.

   Message routing settings are only set during installation. Proxy configurations made here are not related to the proxy settings used for Internet connectivity–though the same proxy settings are used by default.

   Note: If your network topology includes a NAT device, see *page 3-4* for details on how to configure the Control Manager routing path settings.

   Source of incoming messages:

   - **Direct from registered agents**– Control Manager can directly receive incoming messages
   - **Proxy server**– use a proxy server when receiving messages
   - **IP port forwarding**– this feature configures Control Manager to work with the IP port forwarding function of your company's firewall

     Provide the firewall server's FQDN, IP address or NetBIOS name, and then type the port number that Control Manager opened for communication.

   Route for outgoing messages:

   - **Direct to registered agents**– Control Manager sends outgoing messages directly to Network VirusWall
   - **Proxy server**– Control Manager sends outgoing messages via a proxy server
5. Click **Next**. Specify the Start menu program folder that will contain the Control Manager shortcut. The default is **Trend Micro Control Manager**. Click **Next**.
6. Perform one of the following tasks:

- If an SQL server is detected on your server, proceed to the Control Manager 3.0 Patch 1 for Service Pack 2 and hot fix 2047 installation by clicking **OK** on the prompt that follows.

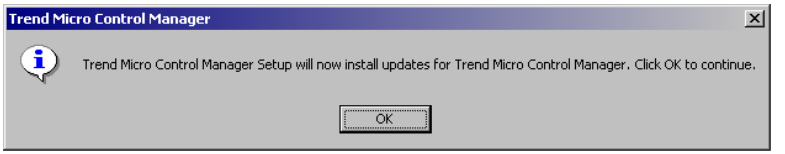


FIGURE 4-2. Installing Control Manager Patch 1 for Service Pack 2 and hot fix 2047

- If you are installing MSDE on the server for the first time, the following prompt appears after Setup finishes the Control Manager installation:

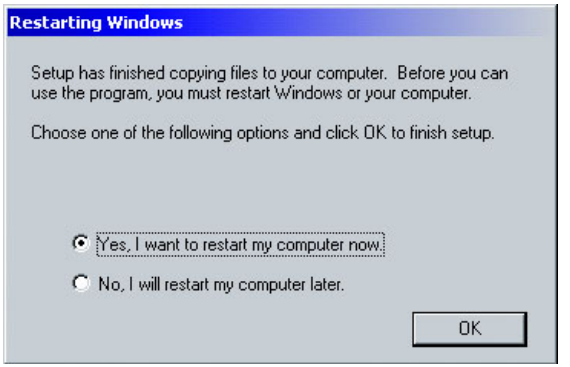


FIGURE 4-3. Select whether to restart the server after installing Control Manager and MSDE

  - If you select **Yes, I want to restart my computer now.**, the Control Manager server restarts

    After restarting the server, manually install Patch 1 for Service Pack 2 and hot fix 2047 to enable Control Manager support for Network VirusWall 2500 (see *page 4-16*).

- If you want to restart the server later, select **No, I will restart my computer later.** and perform the following steps to finish the Control Manager setup:

  i. Click **OK** on the prompt that follows.

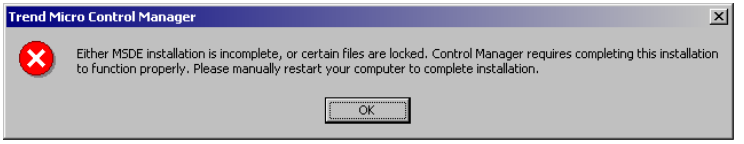


FIGURE 4-4. Skip restarting the server

ii. Click **OK** to install the Control Manager updates.

iii. Restart the server to complete the Control Manager installation.

The Control Manager server installation is finished. If you launch the Setup program from the Solutions CD, the Solutions CD Welcome window re-appears.

See *page 4-19* for details on how to verify a successful Control Manager server installation.

Installing Control Manager Patch 1 for Service Pack 2 and Hot Fix 2047

Along with enhancements and bug fixes, the Control Manager Patch 1 for Service Pack 2 (SP2) enables the Control Manager server support for Network VirusWall 2500 devices. In addition, hot fix 2047 allows you to view the latest Network VirusWall 2500 documentation.

Tip: Refer to the What's New section in the patch and hot fix readme for additional enhancements included in these releases.

Visit `http://www.trendmicro.com/download` for the latest Control Manager releases.

Table 4-2 shows all applicable Control Manager setup scenarios for the Control Manager patch and hot fix releases.

SCENARIO	ACTION
Running Control Manager 3.0 for the first time	The Control Manager Setup will install Control Manager Patch 1 for SP2 if you select **Install** from the Patch 1 for SP2 prompt.
Running an existing Control Manager 3.0 server with build 2035 (or older)	Install the following releases: • Patch 1 for SP2 • Hot fix 2047
Running an existing Control Manager 3.0 server with build version 2035 up to 2046	Install hot fix 2047.
Running an existing Control Manager 3.0 server with build 2047 (or newer)	No action necessary. The Control Manager build can support Network VirusWall 2500.

TABLE 4-2. Control Manager 3.0 Patch 1 for SP2 setup scenarios

The patch and hot fix setup files are available in the following location in the Network VirusWall 2500 Solutions CD:

```
root\Programs\TMCM3\Patch
```

To install Control Manager 3.0 Patch 1 for SP2:

1. Perform any of the following task to obtain the Setup program (`CM30_EN_SP2_Patch1.exe`):
   - Download the Setup program from the **Update Center** to a directory on the Control Manager server
   - Copy `CM30_EN_SP2_Patch1.exe` from the Solutions CD to a directory on the Control Manager server.
2. Using Microsoft Windows Explorer, double-click `CM30_EN_SP2_Patch1.exe`.

The message *Installation successful!* will display after a complete and successful installation.

FIGURE 4-5. Successful Control Manager Patch 1 for SP2 installation

To install Control Manager 3.0 hot fix 2047:

1. Copy `CM30B2047_en.exe` from the Solutions CD to a directory on the Control Manager server.
2. Using Microsoft Windows Explorer, double-click `CM30B2047_en.exe`.

The message *Installation successful!* will display after a complete installation.

Registering and Activating Control Manager

After you have successfully installed Control Manager, check the license status and expiration date on the management console.

To check the license status on the management console:

1. Access the Control Manager management console.
2. On the menu header, click **Administration**. The Administration screen appears.
3. On the navigation menu, click **Registration** > **License Information**. The License Status screen appears.

If the status is not activated or expired, obtain an Activation Code and activate Control Manager.

To activate Control Manager:

1. Obtain an Activation Code.

   If you already have a full version Activation Code, skip this step and proceed to step 2.

   To obtain a full version Activation Code, follow these steps:

   a. Point a Web browser to the following Web page:

      `https://olr.trendmicro.com/registration`

      The Online Registration page of the Trend Micro Website opens.

   b. If you are an existing Trend Micro customer, log on using your **logon ID** and **password**. If you are a new customer, click **Register Your Product** under **New customer registration**.

   c. On the Enter Registration Key page, type or copy the Control Manager Registration Key, and then click **Continue**.

   d. On the Confirm License Terms page, read the license agreement and then click **I accept the terms of the license agreement**.

   e. On the Confirm Product Information page, click **Continue Registration**.

   f. Fill out the online registration form, and then click **Submit**.

   g. Click **OK** twice.

After you have completed the registration process, Trend Micro sends an Activation Code via email, which you can then use to activate Control Manager.

2. On the Control Manager management console > **License Status** screen, click **Activate the product**.
3. Type or copy the Control Manager **Activation Code**.

The activation is finished. Refer to *Verifying a Successful Control Manager Installation* for details on how to verify a successful Control Manager server installation.

If you experience issues with your Activation Code, please contact technical support (see *page 6-14* for more information).

After readying Control Manager, you are now ready to preconfigure Network VirusWall.

Verifying a Successful Control Manager Installation

Check whether the following services are running to verify a successful Control Manager installation on a server with at least the minimum system requirements:

- Trend Micro Control Manager
- Trend Micro Common CGI
- Trend Micro Management Infrastructure
- Trend Micro Network Time Protocol

Tip: Use the Windows **Services** panel to check the Control Manager services.

The following folder structure and process list becomes available after a successful Control Manager installation:

- The following folder structure appears under the directory Program Files\Trend Micro:
  - `Common\TMI`
  - `Common\CCGI`
  - `Control Manager`

- The following processes are running:
  - CCGI processes:
    - `Jk_nt_service.exe`
    - `Java.exe`
  - IIS process:
    - `Inetinfo.exe` (Internet Information Services)
  - TMI processes:
    - `CM.exe` (TMI-CM)
    - `MRF.exe` (Message Routing Framework Module)
    - `DMServer.exe` (TMI-DM full-function)
  - Control Manager processes:
    - `ProcessManager.exe`
    - `LogReceiver.exe`
    - `MsgReceiver.exe`
    - `EntitiyEmulator.exe`
    - `LogRetriever.exe`
    - `CmdProcessor.exe`
    - `UIProcessor.exe`
    - `ReportServer.exe`
    - `NTPD.exe`
    - `DCSprocessor.exe`
    - `Casprocessor.exe`

Chapter 5

Preconfiguring Network VirusWall

Preconfiguring a Network VirusWall 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 5-5*).
3. Configure device settings (see *page 5-9*).
4. If your network is configured to use one or more VLANs, configure VLAN settings (see *page 5-15*).
5. Set the Operation Mode (see *page 5-17*).
6. Set the interface speed and duplex mode (see *page 5-23*).

This chapter discusses the above-mentioned steps in detail and contains the following topics:

Understanding the Network VirusWall Preconfiguration

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

To perform preconfiguration:

1. Plan and determine the deployment strategy (see *Deploying Network VirusWall* on page 3-1).
2. Prepare for and install Control Manager and necessary patch (see *Control Manager Pre-installation Tasks* on page 4-2 and *Installing Control Manager 3.0* on page 4-10).
3. Perform preconfiguration (see instructions starting on *Using the Preconfiguration Console* on page 5-3).
4. Perform configuration tasks (see chapter 2 of the *Network VirusWall 2500 Administrator's Guide*).

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

Preconfiguration configures Network VirusWall for your network and allows Network VirusWall to establish communication with Control Manager upon connection to the network. It allows you to modify basic Network VirusWall default settings and perform network configuration.

After the preconfiguration procedure of the Network VirusWall device is complete, the device registers itself to the Control Manager server as a managed product. You can then administer Network VirusWall device from the Control Manager management console. Refer to *chapter 2* of the *Administrator's Guide*.

Choosing the Preconfiguration Method

Preconfigure Network VirusWall 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—

- Operation Mode
- Passwords
- Interface
- Network and Control Manager settings
- System logs
- VLAN tags

Examples of a terminal interface are HyperTerminal for Windows or Minicom for Linux.

Using the terminal interface, you can preconfigure all Network VirusWall settings. If you do not have access to a computer with terminal communications software, use the Network VirusWall LCD module panel to perform preconfiguration. See *Preconfiguring Network VirusWall 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 network settings, such as the IP address. See *Preconfiguring Network VirusWall Using the LCD Module* on page 5-27 for details on how to use the LCD module.

When completed, either method allows Network VirusWall to register to the Control Manager server.

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

WHAT YOU CAN DO	PRECONFIGURATION CONSOLE	LCD MODULE
Change account passwords	●	
Set Network VirusWall IP address, netmask, Gateway address, and DNS addresses	●	●
Configure the Control Manager settings	●	●
Create and edit Virtual LAN (VLAN) tags	●	
Lock/unlock LCD module panel controls	●	
View system logs	●	
Initialize Network VirusWall to default settings	●	
Reset Network VirusWall	●	●
Restore default settings (factory settings)	●	
Set the Operation Mode	●	
Configure the interface speed and duplex mode	●	
View device settings	●	
Allow changes to take effect immediately	Need to log off	●
Change Network Address Translation (NAT) settings	●	

TABLE 5-1. Comparison of available consoles for preconfiguration

Tip: Trend Micro recommends using the Preconfiguration console when preconfiguring Network VirusWall for the first time. Doing so allows you to easily preconfigure a device.

Preconfiguring Network VirusWall Using the Preconfiguration Console

Preconfiguring Network VirusWall using the Preconfiguration console requires the completion of the following tasks:

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

1. Prepare the Preconfiguration console (see *page 5-5*).
2. Log on to the Preconfiguration console (see *page 5-6*).
3. Configure the device settings (see *page 5-9*).
4. Configure the VLAN settings (see *page 5-15*).
5. Set the Operation Mode (see *page 5-17*).
6. Set the interface speed and duplex mode (see *page 5-23*).

Preparing the Preconfiguration Console

Before you preconfigure Network VirusWall, designate a computer for preconfiguration. Network VirusWall requires the following connections for preconfiguration:

- A console connection to the computer you use for preconfiguration

  Use a computer with terminal configuration software such as HyperTerminal for Windows or Minicom for Linux.

  Note: Importing or exporting the Network VirusWall configuration is not possible when using Minicom.

- A network connection to the server running Control Manager

  Tip: You can use the Control Manager server for preconfiguration.

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 enter 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

Logging on to 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 2-9 for Network VirusWall 2500 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** when the terminal interface displays *Network VirusWall 2500 preconfiguration, Press <ENTER> to continue...*

   After connection, the terminal screen appears blank.

3. Press **Enter**. The **User name** logon prompt displays.

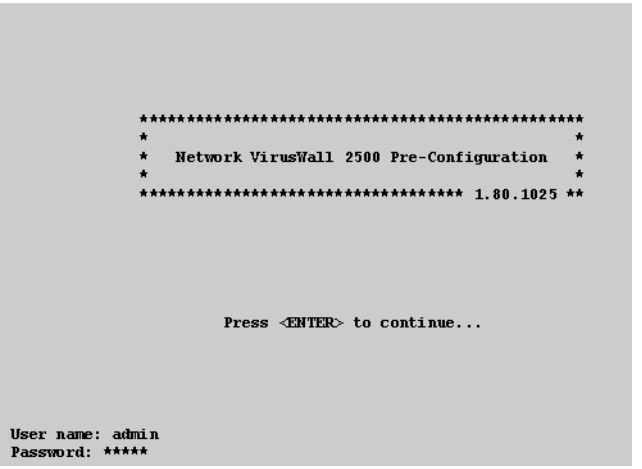


FIGURE 5-1. The Preconfiguration console logon prompt

4. 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.

   Use this login for full access to all Network VirusWall preconfiguration features.

   Tip: See *admin password misplaced or forgotten* on page 6-2 for tips on how to troubleshoot a missing or forgotten password. In addition, the *Administrator's Guide* > *Modifying the Preconfiguration Console Accounts* topic provides details about the `admin` and `monitor` account.

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

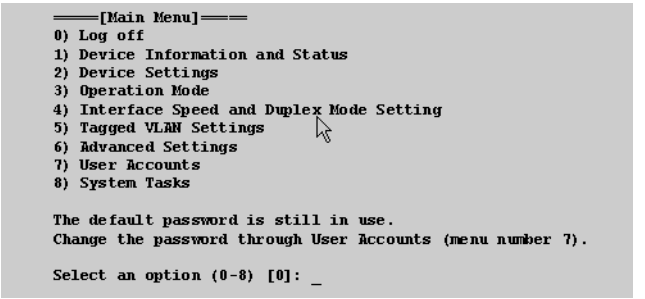


FIGURE 5-2. The Preconfiguration console main menu

Note: The Preconfiguration console has a timeout value of three (3) minutes. If the console is idle for three minutes, it automatically logs off the account.

For instructions on how to on how to log off the Preconfiguration console, see *page 5-26*.

Tip: Proceed by configuring the Network VirusWall settings, which include the device host name and IP settings and the Control Manager server settings.

Configuring Device Settings

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

To configure the Network VirusWall device settings:

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

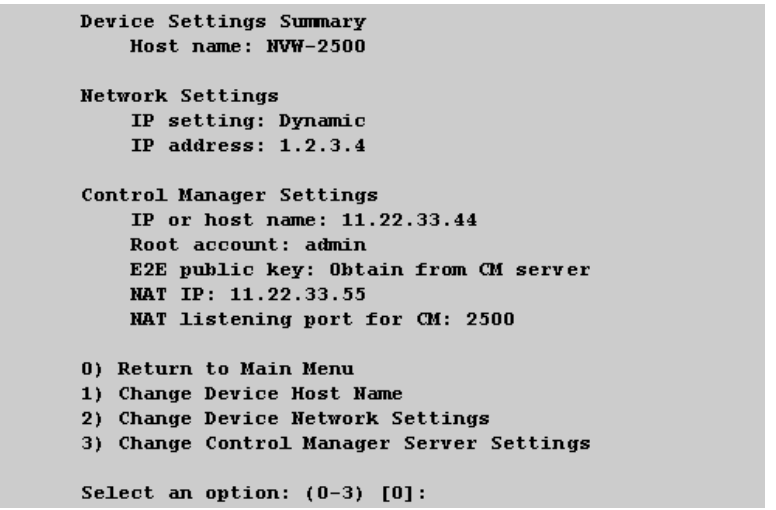


FIGURE 5-3. The Device Settings submenu

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

2. Type `1` to change the Network VirusWall host name.
3. Type a host name that properly represents the Network VirusWall device in the network and on the Control Manager management console.

Note: When Network VirusWall is registered without a host name, the Communicator name on the Control Manager management console > **Products** > **Computers** screen appears blank.

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

Tip: Host names may be up to 63 alphanumeric characters (spaces not allowed). Trend Micro recommends a unique descriptive host name to represent and identify the Network VirusWall 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.

4. Press **Enter.** The console returns to the **Device Settings** menu.
5. Type `2` to change the Network VirusWall network settings. A prompt displays asking you if you want to use a dynamic IP setting.
6. Type `Y` to have a DHCP server on your network determine the Network VirusWall IP address, netmask, gateway address, and DNS server addresses.

   Alternatively, type `N` and configure these settings manually.

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

7. After specifying the network settings, press **Enter**. The console returns to the **Device Settings** menu.
8. Type `3` to configure the Control Manager settings.
9. Type `N` when prompted to manually import the Control Manager public key.

   Have Network VirusWall automatically download the public key when it registers with Control Manager. The public key ensures secure communication between Network VirusWall and Control Manager during registration and managed product administration.

Tip: To successfully register a device to a Control Manager server, check whether the network connection between the computer used during preconfiguration and Control Manager server is present. See *page 4-5* for additional network support information.

---

10. Type the Control Manager IP address or host name and the root user name.

Note: The Control Manager IP address, host name, and root user name is set during the Control Manager installation (see *page 4-10*).

---

11. If a Network Address Translation (NAT) device is present in your network, type the NAT IP and NAT listening port for Control Manager. The NAT IP is its public IP and the NAT listening port is the port that NAT configures for NVW.

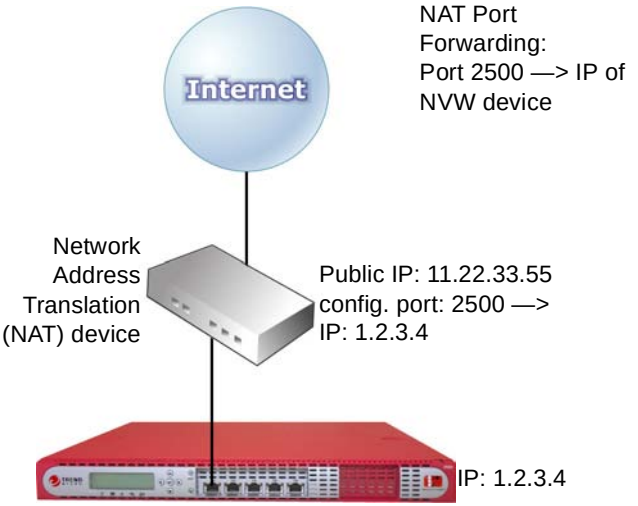


FIGURE 5-4. NVW 2500 deployment in a network environment using a NAT device (with sample IP address and port)

Note: The network administrator needs to configure the port forwarding on the NAT device. Configure port forwarding according to the Network VirusWall settings. See Figure 5-5. *The Change Control Manager Server Settings submenu of the Preconfiguration console* on page 5-12, below.

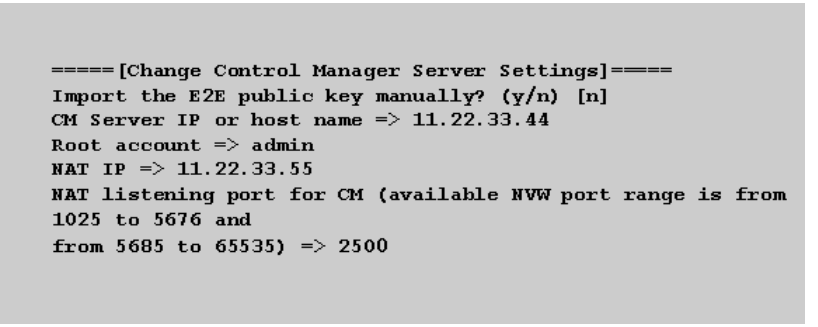


FIGURE 5-5. The Change Control Manager Server Settings submenu of the Preconfiguration console

---

Tip: Use a host name if the Control Manager server obtains an IP address from a DHCP server. Test the connection to the Control Manager server by using the command `ping {host name or IP address}` from the command prompt, where `{host name}` is the Control Manager server domain name.

---

12. Press `0` to return to the **Main Menu**, and press `0` again to log off from the Preconfiguration console.

Note: If your network is configured to use one or more VLANs, refer to the instructions on configuring VLAN settings *page 5-15*.

---

13. Log back on to the Network VirusWall console using the administrator name and password.

Tip: View system logs to see the progress of Control Manager registration. See succeeding steps.

---

14. Type `8` in the **Main Menu** to select **System Tasks**.

15. On the System Tasks screen, type `1` to **View System Logs**. The system logs appear showing the following information:
    - Date and time of log entry
    - Log entry

```
====[System Tasks]====

0) Return to Main Menu
1) View System Logs
2) Import Configuration File
3) Export Configuration File
4) Reset Device
5) Restore Default Settings

Select an option (0-5) [0] 1

====[View System Logs]====
Product version [1.8.1025]
At any time, press <ENTER> to return to the Main Menu.

Jul 16 11:11:36 NVW2500_NY syslogd 1.3-3: Restart...
Jul 16 11:11:37 NVW2500_NY udhcpc: Sending discover...

Return to Main Menu? (y/n) [y]
```

FIGURE 5-6. Viewing system logs

Note: System logs contain information useful for troubleshooting. If you experience issues with Network VirusWall and contact Trend Micro support, you may be asked to view the system log.

Refer to the Network VirusWall *Administrator's Guide* > *Viewing Status, Logs, and Summaries* and *Troubleshooting* sections for more details about troubleshooting.

---

16. Press **Enter** to stop the log report.
17. At the prompt, type `Y` to return to the main menu.

You are now ready to set the VLAN, Operation Mode, and interface settings.

Configuring VLAN settings

Create and edit Virtual Local Area Network (VLAN) tags that conform to the existing VLAN rules on your network. Network VirusWall supports up to 50 tagged VLANs and 1 non-tagged VLAN.

Tip: If the Control Manager server is a member of a VLAN, Trend Micro recommends binding the Network VirusWall IP address to the same VLAN; otherwise, Network VirusWall may experience communication problems with the Control Manager server.

Refer to the *Administrator's Guide* for more information on VLANs.

To add a new VLAN ID:

1. On the **Main Menu** of the Preconfiguration console, type `5` to select **Tagged VLAN Settings**.

```
====[Tagged VLAN Settings]====

 VLAN ID    VLAN Name                      Tagged      IP
-------------------------------------------------------------
 Default     Default VLAN                   No         v
  258        HR                             Yes
  368        Support                        Yes


0) Return to Main Menu
1) Add VLAN
2) Remove VLAN
3) Rename VLAN
4) Change IP Binding

Select an option: (0-4) [0] _
```

FIGURE 5-7. The VLAN Settings submenu

2. Type `1` in the **Tagged VLAN Setting** menu to **add** a new tagged-VLAN.
3. At the **New VLAN ID** prompt, type an ID number from 1 to 4094.
4. The **VLAN name** prompt displays a default name. Press **Enter** to accept the default name or type a new name (VLAN names may be up to 31 alphanumeric characters long).

5. If you want to bind the Network VirusWall IP address to the current VLAN, type `Y` at the next prompt.

Note: To allow Network VirusWall to filter VLAN traffic, you must bind the Network VirusWall IP address to at least one VLAN.

The VLAN Settings screen refreshes and includes the newly added VLAN.

To remove an existing VLAN:

1. On the **Main Menu** of the Preconfiguration console, type `5` to select **VLAN Settings**.
2. Type `2` in the **VLAN Setting** menu to **remove** an existing tagged VLAN.
3. At the prompt, type the ID number of the VLAN to delete.

Note: You cannot remove a VLAN to which the Network VirusWall IP address is bound.

The VLAN Settings screen refreshes showing a list that does not include the deleted tagged VLAN.

To rename an existing VLAN:

1. On the **Main Menu** of the Preconfiguration console, type `5` to select **VLAN Settings**.
2. Type `3` in the **VLAN Setting** menu to rename an existing VLAN.
3. At the prompt, type the ID number of the VLAN to rename.
4. Type the new name.

The VLAN Settings screen refreshes and displays the renamed VLAN.

To modify the IP binding selection of a VLAN:

1. On the **Main Menu** of the Preconfiguration console, type `5` to select **VLAN Settings**.
2. Type `4` in the **VLAN Setting** menu to select **Change IP Binding**.
3. At the prompt, type the ID number of the VLAN whose IP binding setting you want to change.

The VLAN Settings screen refreshes and displays the new IP binding setting.

Setting the Operation Mode

After deciding on the Network VirusWall deployment strategy, use the Operation Mode option in the Network VirusWall Preconfiguration console to configure the failopen, failover, and port redundancy settings.

To set the Operation Mode:

1. On the **Main Menu** of the Preconfiguration console, type `3` to select **Operation Mode**.

```
=====[Operation Mode]=====
Port Grouping
1 fiber-optic port(s) detected.

    Failopen: Disabled
    Failover: Disabled

0) Return to Main Menu
1) Change Operation Mode

Select an option: (0-1) [0]: 1
```

FIGURE 5-8. The Operation Mode submenu

2. On the Operation Mode submenu, type `1` to set the Operation Mode configuration.
3. On the Change Operation Mode screen, select from the available operating modes and then type the menu number.

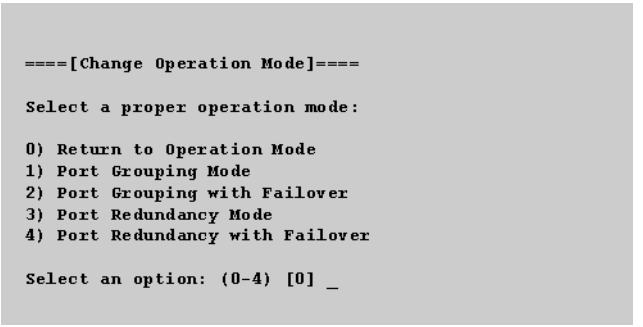


FIGURE 5-9. The Operation Mode submenu (failover is not set)

Tip: See *Deploying Network VirusWall Based on an Operation Mode* on page 3-22 to learn more about the deployment strategies based on the four (4) operating modes.

- To set port-based VLAN grouping, type `1`

  Type `y` to enable failopen.
- To set port-based VLAN grouping with failover, type `2`
  - **i.** Type `y` to assign the original attribute setting to **Primary**.
  - **ii.** Type `y` to set the failover environment to **Switch-back** mode.
- To set port redundancy, type `3`

  Type `y` to enable failopen.
- To set port redundancy with failover, type `4`
  - **i.** Type `y` to assign the original attribute setting to **Primary**.
  - **ii.** Type `y` to set the failover environment to **Switch-back** mode.

Tip: For explanations about the original attribute setting, failover environment, and other high availability concepts, refer to the *Administrator's Guide > Understanding Network VirusWall > Network VirusWall 2500 > High Availability.*

---

4. Type `0` to return to the Operation Mode submenu. The new settings appear.

```
=====[Operation Mode]=====
Port Grouping with Failover
1 fiber-optic port has been detected.

    Failopen: Disabled
    Failover: Secondary; Non-switch-back

NOTE: Log off to apply new settings.

0) Return to Main Menu
1) Change Operation Mode
2) Change Failover Status

Select an option: (0-2) [0]: 1
```

FIGURE 5-10. The Operation Mode submenu (failover set)

Note: By default, the Operation Mode submenu provides two (2) menu options. When failover is set, the third option (**Change Failover Status**) becomes available.

---

5. To apply the new settings, type `0` twice to return to the main menu and log off from the Preconfiguration console.
6. Log back on and then type `3` to view the current operating mode.

WARNING! *For network environments using Network Address Translation (NAT): When failover is activated, the standby Network VirusWall device may not work in a NAT environment, because two devices (IP addresses) cannot share the same port. To resolve any such failure, reconfigure the NAT settings in the standby device once failover has occurred and the standby device is running.*

---

7. View the current Operation Mode from the Control Manager management console.

Note: Modifying the Operation Mode causes the Network VirusWall to re-register to the Control Manager server, resulting in two (2) managed product icons listed in the **Product Directory**. See *page 6-8* for additional troubleshooting instructions.

You can use the Preconfiguration console to change operation settings. If you are using a fiber port, your options are different than if not.

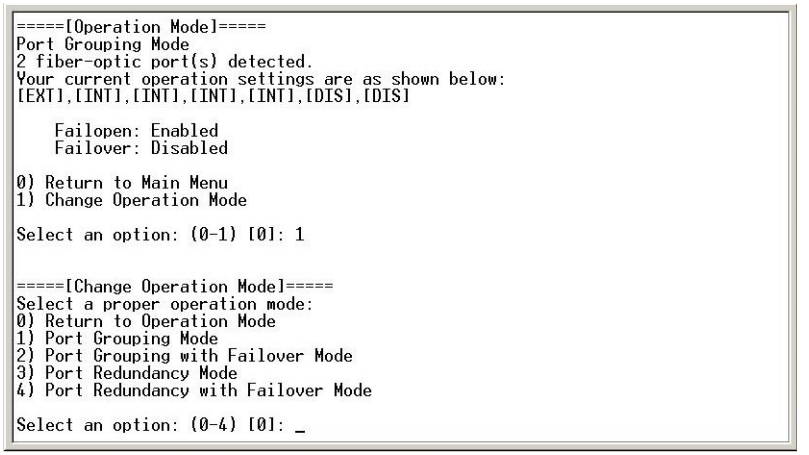


FIGURE 5-11. The Change Operation Mode menu when using fiber ports

For a Network VirusWall device using fiber-optic ports in a port grouping mode, the following configurations are available:

```
1) Change Operation Mode

Select an option: (0-1) [0]: 1


=====[Change Operation Mode]=====
Select a proper operation mode:
0) Return to Operation Mode
1) Port Grouping Mode
2) Port Grouping with Failover Mode
3) Port Redundancy Mode
4) Port Redundancy with Failover Mode

Select an option: (0-4) [0]: 1


=====[Change Operation Settings]=====
0) Return to the Main Menu
1) [EXT],[INT],[INT],[INT],[INT],[DIS],[DIS]
2) [DIS],[INT],[INT],[INT],[INT],[EXT],[DIS]
3) [DIS],[INT],[INT],[INT],[INT],[DIS],[EXT]
4) [DIS],[DIS],[DIS],[DIS],[DIS],[EXT],[INT]

Select an option: (0-4) [0]:
```

FIGURE 5-12. Port Grouping configuration options for a Network VirusWall device with fiber-optic ports

For a Network VirusWall device using fiber-optic ports in a *port grouping with failover* mode, the following configurations are available:

```
1) Change Operation Mode

Select an option: (0-1) [0]: 1


=====[Change Operation Mode]=====
Select a proper operation mode:
0) Return to Operation Mode
1) Port Grouping Mode
2) Port Grouping with Failover Mode
3) Port Redundancy Mode
4) Port Redundancy with Failover Mode

Select an option: (0-4) [0]: 2


=====[Change Operation Settings]=====
0) Return to the Main Menu
1) [EXT],[INT],[INT],[INT],[FOV],[DIS],[DIS]
2) [DIS],[INT],[INT],[INT],[FOV],[EXT],[DIS]
3) [DIS],[INT],[INT],[INT],[FOV],[DIS],[EXT]
4) [DIS],[DIS],[DIS],[DIS],[FOV],[EXT],[INT]

Select an option: (0-4) [0]:
```

FIGURE 5-13. Port Gouping with Failover configuration options for a Network VirusWall device with fiber-optic ports

For a Network VirusWall device using fiber-optic ports in a port redundancy mode, the following configurations are available:

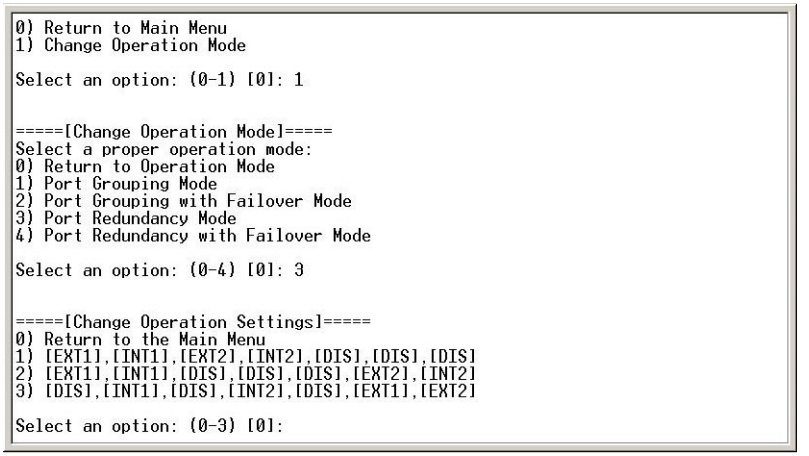


FIGURE 5-14. Port Redundnacy configuration options for a Network VirusWall device with fiber-optic ports

For a Network VirusWall device using fiber-optic ports in a *port redundancy with failover* mode, the following configurations are available:

```
0) Return to Main Menu
1) Change Operation Mode

Select an option: (0-1) [0]: 1


=====[Change Operation Mode]=====
Select a proper operation mode:
0) Return to Operation Mode
1) Port Grouping Mode
2) Port Grouping with Failover Mode
3) Port Redundancy Mode
4) Port Redundancy with Failover Mode

Select an option: (0-4) [0]: 4


=====[Change Operation Settings]=====
0) Return to the Main Menu
1) [EXT1],[INT1],[EXT2],[INT2],[FOV],[DIS],[DIS]
2) [EXT1],[INT1],[DIS],[DIS],[FOV],[EXT2],[INT2]
3) [DIS],[INT1],[DIS],[INT2],[FOV],[EXT1],[EXT2]

Select an option: (0-3) [0]:
```

FIGURE 5-15. Port Redundnacy with Failover configuration options for a Network VirusWall device with fiber-optic ports

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 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 devices to have the same setting. Apply **100Mbps x full-duplex** for both the switch and Network VirusWall device.

To set the interface speed and duplex mode:

1. On the **Main Menu** of the Preconfiguration console, type `4` to select **Interface Speed and Duplex Mode Setting**.

```
=====[Interface Speed and Duplex Mode Setting]=====
Interface Speed and Duplex Mode Setting Summary
    Network Port 1 (00:C0:9F:46:9A:00): Auto
    Network Port 2 (00:C0:9F:46:9A:01): Auto
    Network Port 3 (00:C0:9F:46:9A:02): Auto
    Network Port 4 (00:C0:9F:46:9A:03): Auto
    Network Port 5 (00:C0:9F:46:99:42): Auto
    Fiber Port 1 (slot A) (00:04:23:9F:54:51): Auto

----Fiber card information----
Slot A: Intel PRO/1000 MF Single Port Server
Adapter

0) Return to Main Menu
1) Change Network Port 1
2) Change Network Port 2
3) Change Network Port 3
4) Change Network Port 4
5) Change Network Port 5
6) Change Fiber Port1 (Slot A)

Select an option: (0-6) [0]:
```

FIGURE 5-16. The Port Configuration (Interface Speed and Duplex Mode) submenu

2. On the Interface Speed and Duplex Mode Setting screen, select the port you want to configure and type the menu number. For example, to configure the interface speed and duplex mode of port 1, type 1. To change port settings for the fiber ports, type the number of the port as shown in Figure 5-13. *Changing interface speed and duplex mode for Network Port 1* on page 5-20.To change port settings for copper port 1, type 1:

```
======[Change Interface Speed and Duplex Mode Setting]=====
Choose a proper configuration for Fiber Port 1 (slot A):
(Current setting for Fiber Port 1 (slot A) is: Auto)

0) Return to Interface Speed and Duplex Mode Setting
1) Set auto

Select an option: (0-1) [0]:
```

FIGURE 5-17. The Interface Speed and Duplex Mode Setting submenu

```
=====[Change Interface Speed and Duplex Mode Setting]=====
Choose a proper configuration for Network Port 1:
(Current setting for Network Port 1 is: Auto)
0) Return to Interface Speed and Duplex Mode Setting
1) Set auto
2) Set 10 Mbps x half-duplex
3) Set 10 Mbps x full-duplex
4) Set 100 Mbps x half-duplex
5) Set 100 Mbps x full-duplex
6) Set 1000 Mbps x full-duplex

Select an option: (0-6) [0]:
```

FIGURE 5-18. Changing interface speed and duplex mode for Network Port 1

The Change Port Setting screen appears, displaying the port's current interface speed and duplex setting.

3. Select from the available interface speed and duplex mode, and then type the menu number.
4. Log off the Preconfiguration console for changes to take effect (see *page 5-26*).

The Port Configuration menu appears, displaying the current port configuration summary.

Logging off the Preconfiguration Console

Log off the Preconfiguration console after completing preconfiguration or modifying settings (for example, Operation Mode, VLAN, and 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, type `0` to select **Log off**. A confirmation message appears.

```
=====[Main Menu]=====
0) Log off
1) Device Information and Status
2) Device Settings
3) Operation Mode
4) Interface Speed and Duplex Mode Setting
5) Tagged VLAN Settings
6) Advanced Settings
7) User Accounts
8) System Tasks

The default password is still in use.
Change the password through User Accounts (menu number 7).

NOTE: Log off to apply new settings.

Select an option (0-8) [0]:
Exit the Network VirusWall Pre-configuration? (y/n) [n]
```

FIGURE 5-19. Logging off the Preconfiguration console

2. Type `y` and press Enter to log off.

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

Save the settings when prompted on the display.

Preconfiguring Network VirusWall Using the LCD Module

Tip: Check *page 5-4* for comparison between the consoles you can use for preconfiguration.

With the LCD console, you can only configure the Network VirusWall 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 Network VirusWall 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 Network VirusWall 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 Control Manager server **IP address**.

   c. Type the Control Manager root account **user name**.

   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 Network VirusWall **IP address**, **netmask**, **Gateway address**, and **DNS server addresses**.

   c. Type the Control Manager server **IP address**.

   d. Type the Control Manager root account **user name**.

Note: The Control Manager IP address, host name, and root user name is set during Control Manager installation.

---

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

Network VirusWall restarts to apply the new settings.

Connecting to the Network

Be sure to install Control Manager and preconfigure Network VirusWall before attempting to connect the device or devices in a failover pair.

Note: Check whether Trend Micro Control Manager 3.0 and Patch 1 for Service Pack 2 are installed (see *page 4-17*) and the necessary OfficeScan or ServerProtect patches are applied before connecting Network VirusWall (see *page 4-8*).

The figure on page 3-22 illustrates a typical deployment. Note that the Control Manager server may be within or outside of the protected network, as long as the host name or IP address can be resolved between the two.

To connect Network VirusWall to your network:

Note: After preconfiguration, switch off the device before connecting it to the network.

1. Connect one end of a 10/100Mbps Ethernet cable to the **INT** port and the other to the segment of the network that Network VirusWall will protect (the Protected Network).
2. Connect one end of another 10/100 Mbps Ethernet cable to the **EXT** port and the other end to the part of the network that leads to the public network.
3. In a failover deployment, establish the failover pair by connecting the provided Ethernet cable (RJ-45 crossover or a regular LAN cable) to port 5 of the Primary and Secondary devices.
4. Power on the device if it is turned off (see *page 5-7*).

Note: Network VirusWall 2500 can handle various interface speed and duplex mode network traffic. See *Setting the Interface Speed and Duplex Mode* on page 5-23.

Testing a Successful Deployment

Perform any of the following tasks to test whether you have successfully deployed Network VirusWall.

To test a successful deployment:

- From the Control Manager server, ping the Network VirusWall device

  A ping response should come from the device if the **Advanced Settings** > **Allow ICMP requests from other computers** option is enabled. By default, this option is disabled.

  Refer to the *Administrator's Guide* > *Configuring Device and System Settings* section for instructions on how to enable this option.
- Using the management console, check whether the registered device has the active ( ) status
- In a failover deployment, determine whether the failover pair is established by logging on to the Preconfiguration console of the Standby device

  The Preconfiguration console of a Standby device is not configurable. The `monitor` account allows only read-only access to the Standby device settings.

Configuring Network VirusWall

After installing Control Manager and preconfiguring Network VirusWall, you are ready to configure the Network VirusWall device and commence network protection.

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

- Update components
- Change user password
- View Operation Mode

Refer to the following documentation for related instructions:

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

See the *Configuring Scan, System, and Device Settings > Getting Started with Network VirusWall* section in the *Administrator's Guide* for recommended instructions.

- *Network VirusWall Online Help*– provides instructions on how to configure Network VirusWall devices using the Control Manager management console

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

Chapter 6

Troubleshooting Preconfiguration

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

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

This chapter contains the following topics:

Note: The *Network VirusWall Administrator's Guide* > *Troubleshooting* section has more details regarding Control Manager and Network VirusWall integration troubleshooting.

Hardware Issues

	Issue	Corrective Action/Explanation
1	`admin` password misplaced or forgotten	Use the Rescue Utility to reload the Network VirusWall image. **Note:** Reloading the Network VirusWall 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 2-5 for details on the Network VirusWall 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 5-5 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 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 the Administrator's Guide > Changing the LCD Module Configuration topic 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 does not refresh its MAC address table if one of the links fails. The result is a temporary delay in packet delivery.

	Issue	Corrective Action/Explanation
6	POST error is encountered	**Power-On Self Test (POST Error)** The following events may result in a POST error (**SYSTEM** LED is red– steady): • CPU internal error (IERR) • All memory not present • Memory single-bit error • Memory multi-bit error • PCI system error (SERR) • PCI parity error (PERR) • Fan speed abnormal • Temperature abnormal • Voltage abnormal • Boot device absent • PCI memory conflict • PCI I/O conflict • PCI IRQ conflict • Memory read/write test fail • OS Load watchdog timeout Reset Network VirusWall by pressing the RESET button on the front panel of the device. If a particular POST error persists, contact support (see *page 6-14*).

Configuration Issues

	ISSUE	CORRECTIVE ACTION
1	Network VirusWall is unable to register with the Control Manager server	Check all network connections and check whether you have correctly performed preconfiguration. If you changed the Network VirusWall IP address, manually reset the device to allow it to register to the Control Manager server. If Control Manager 3.0 is installed on a server running Windows Server 2003, Network VirusWall may not be able to use the Control Manager time service to synchronize with the server, and will therefore be unable to register to the Control Manager service. **To remedy this issue, choose one of the following:** • Install Active Directory on the Windows Server 2003 server so Network VirusWall can synchronize with the Windows Server 2003 time service • Disable the Windows Server 2003 time service and enable **Trend Micro Network Time Protocol** so Network VirusWall can synchronize with the Control Manager server time service See *page 6-9* for more Control Manager and Network VirusWall communication troubleshooting tips.

	ISSUE	CORRECTIVE ACTION
2	Network VirusWall displays a **sync time** error and is unable to register to CM server	A sync time error displays when Network VirusWall is unable to synchronize with the Control Manager server. **To remedy this issue, do the following:** 1. On the computer acting as the Control Manager server, open **Services** under the Windows **Administrative Tools**. Click **Start** > **Programs** > **Administrative Tools** > **Services**. 2. Stop the **Windows Time** service. 3. Start the **Trend Micro Network Time Protocol** service. 4. Reset the Network VirusWall device. If the issue persists and Network VirusWall is in a multiple VLAN environment, check whether the Network VirusWall IP address is bound to the correct VLAN ID.
3	Communication between the Network VirusWall device and the Control Manager server is not taking place according to the Communicator Scheduler settings	Network VirusWall supports only GMT system time; it is not possible to configure other time settings. The schedule you configure on the Control Manager Communicator Scheduler must take into account any time difference between the time settings on the Control Manager server and GMT time.
4	The Network VirusWall icon on the Control Manager management console appears as active even when the device is offline	When Network VirusWall 2500 is turned off, or is disconnected from the network, the Control Manager agent for Network VirusWall is not given the opportunity to inform Control Manager that it is going offline. As a result, it relies on Control Manager's status verification mechanism to update its operating status. If the default heartbeat settings are used, Control Manager may require up to 180 minutes to update the status. The actual time would depend on when Network VirusWall sent its last heartbeat. See the *Control Manager Getting Started Guide* and online help for information on changing Heartbeat settings.

	ISSUE	CORRECTIVE ACTION
5	Network VirusWall is unable to communicate with Vulnerability Assessment (VA)	Check whether VA is activated (see the *Control Manager Getting Started Guide*). Verify that the Control Manager Web server port is correct. This port is configured during Control Manager installation (see *Installing Control Manager 3.0* on page 4-10).
6	Vulnerability Assessment (VA) settings are set to block, but Network VirusWall does not block vulnerable clients	To remedy this issue *before* performing a Vulnerability Assessment, do the following: 1. Access the Control Manager management console. 2. Click **Services** > **Vulnerability Assessment** > **Global Settings**. 3. Click the check boxes for the machines to block under **Auto Enforcement Settings**. 4. Under **Action Settings for Manual Vulnerability Assessment Tool**, click **Assess by all vulnerability names**. 5. Click **Enable enforcement on machines that are { }**, and select a vulnerability from the list. To remedy this issue *after* performing a Vulnerability Assessment, do the following: 1. Access the Control Manager management console. 2. Click **Services** > **Vulnerability Assessment** > **Security Summary**. 3. In the **Enforcement Status** table, click the number of blocked clients under **Machine Count**. 4. Click **Block**.
7	The message 'cannot get key' displays on the LCD module	The LCD module display shows 'cannot get key' until you log on the terminal interface and press Enter or until you press the enter button on the front panel.
8	Blocked clients are not able to access Damage Cleanup Services (DCS) to issue a cleanup request	Check whether DCS is activated (see the *Control Manager Getting Started Guide*) and enabled.

	ISSUE	CORRECTIVE ACTION
9	The icon and user name for a Network VirusWall device that was removed from the network still appears on Control Manager	Access the Product Directory on the Control Manager management console. Use Directory Manager to remove the Network VirusWall device from the Product Directory listing. Refer the *Control Manager Getting Started Guide* and online help for information on adding and removing products.

	ISSUE	CORRECTIVE ACTION
10	Two (2) identical Network VirusWall managed products with the active status ( ) appear on the **Product Directory**	Modifying the Operation Mode causes the Network VirusWall to re-register to the Control Manager server, resulting in two (2) managed product icons listed in the **Product Directory**. **To determine which of the active managed products is the current registered device:** • From the Control Manager management console, check the **Product Status** > **System Information** table The current registered device should have the latest date and time value in the **Registered with Control Manager** field. • From the Control Manager management console, run any configuration option from the **Configuration** tab > **Select configuration** list When trying to configure the original registered device, the management console displays *Unable to load...* message. Depending on the heartbeat setting, it may take some time before the management console displays the latest Communicator status. For short-interval heartbeats, the Product Directory listing will refresh in less than sixty (60) minutes. During this time, the original managed product icon will display the abnormal status ( ). With this status, it is now safe to delete the duplicated icon from the **Product Directory** using **Directory Manager**. Deleting the original managed product will not adversely affect control of the product via the new managed product. **Tip:** The following topics available in the Control Manager Online Help provide additional information: • Determining the right heartbeat setting • Recover managed products removed from the Product Directory • Using the Directory Manager • Why does a managed product appear twice in the Product Directory?

Troubleshooting Control Manager and Network VirusWall Integration

After a successful Control Manager and Network VirusWall integration, both applications should be able to communicate with each other.

Tip: See *Control Manager and Network VirusWall Integration* on page 3-4 for more information regarding Control Manager and Network VirusWall integration.

Consider the following points when troubleshooting the Control Manager and Network VirusWall communication:

- Check the Network Time Protocol (NTP) used (see *page 6-10*)
- Determine whether the Control Manager server uses multiple network interface cards (NICs) (see *page 6-10*)
- Check whether the network connection between the Control Manager server and Network VirusWall device is present (see *page 6-11*)
- Check whether the VLAN name was modified (see *page 6-11*)
- Determine whether the Network VirusWall IP address, VLAN settings, or Operation Mode was modified (see *page 6-12*)

Check the Network Time Protocol (NTP) in Use

Windows NTP and Control Manager NTP are both time servers, but Windows NTP may provide some other features for Active Directory Server (ADS) clients. However, Windows NTP does not work unless you have installed ADS.

If the Control Manager Windows server does not have ADS, disable Windows NTP and enable TMCM-NTP because Windows NTP does not work without ADS. Otherwise, if the Control Manager Windows server has ADS, use Windows NTP. NVW can work (and register) with TMCM successfully in this scenario.

Check the Number of NICs in Use

Determine whether the Control Manager server uses multiple network interface cards (NICs).

To determine whether the Control Manager server uses multiple NICs:

1. Open the TMI.cfg file located in the TMCM server.
2. Search for and verify the `HostID` value. It should contain the IP address that Network VirusWall wants to connect.

   For example:

   ```
   HostID={Control Manager server IP address}:10319
   ```

   where `{Control Manager server IP address}` is the server's IP address.

If the Control Manager server does use multiple NICs, set the `HostID` with the IP address configured in the Network VirusWall preconfiguration > **Device Settings** option.

Check Whether the Network Connection Between the Control Manager Server and the Network VirusWall Device Is Present

From the Control Manager server, ping the Network VirusWall device to check whether the connection between the two products can be established.

Tip: Enable the Preconfiguration console > **Advanced Settings** > **Allow ICMP requests from other computers** option to send a ping request and get a ping response to and from the Network VirusWall device.

In a failover deployment, the failover pair will not switch roles if the Active pair is unable to connect to the Control Manager server. In this situation, the Active device still works. However, the device does not deliver logs to the Control Manager server due to network connection issues. Consequently, you cannot configure an Active device from the Control Manager server if the connection between the two products cannot be established. Manually switch the Active/Standby roles through the Preconfiguration console > **Operation Mode** menu if the Active device is unable to connect to the Control Manager server due to network connection problems. See *page 3-32* for additional failover considerations.

Check Whether the VLAN Name Was Modified

Changing the VLAN name through the Preconfiguration console VLAN Settings menu causes the Control Manager management console Command Details page to display a message similar to the following:

> *The entity service is not running. Verify the entity server status. Contact your system administrator if the issue persists.*

The Control Manager server is unable to communicate with the Network VirusWall device due to the modified VLAN name. Take note, however, that changing the IP or VLAN tag does not cause this issue.

When configuring the VLAN settings, determine the final VLAN name and ID. Standardizing the VLAN naming convention in your organization helps prevent frequent modification, which can lead to this unwanted message.

Determine Whether the Network VirusWall IP Address, VLAN Settings, or Operation Mode Was Modified

Modifying one of the following settings causes the device to temporarily disconnect from the Control Manager server:

- Network VirusWall device IP address
- VLAN settings
- Operation Mode

These tasks are available through the Preconfiguration console **Device Settings** menu. Any of these tasks prevents the Control Manager server from sending any command to the Network VirusWall device and vice versa. The communication between the two systems is disrupted for approximately 13 seconds while the NVW device is refreshing its network connection.

Refresh the Control Manager management console view to determine whether the communication is already established and new IP address is applied.

Tip: Assign a static IP address to Network VirusWall. If the IP address changes often, communication issues may arise between the Control Manager server and Network VirusWall depending on your network topology, architecture, VLAN settings, and so on.

Troubleshooting Failover Deployments

Failover Issue with Network Address Translation

When failover is activated, the standby Network VirusWall device may not work in a NAT environment, because two devices (IP addresses) cannot share the same port.

To resolve any such failure, try one of the following solutions:

- Reconfigure the NAT settings in the standby device once failover has occurred and the standby device is running.
- Deploy Network VirusWall in a network environment that does not use NAT.

Unable to Establish Failover Pair

The following message appears if Network VirusWall cannot establish a failover pair:

> *One of the devices in the failover pair has been idle for 2 seconds. Check the status of both devices.*

To resolve this issue, check whether:

- The failover pair devices are powered ON

  The LCD of the Active device displays the following message:

  ```
  Trend Micro Inc.
  <Network VirusWall IP address / host name>
  ```

  The LCD of the Standby device displays the following message:

  ```
  On Standby
  Settings...
  ```

  In addition, the INSPECTION LED ( ) of the Standby device steadily lights up in Yellow.

- Both devices are registered to the Control Manager server

  In a successful failover deployment, only the Active device should be registered and configurable from the Control Manager management console

- Both devices have matching device model, language, and program image version
- Both devices have the correct failover settings

Check whether:

- One device is the Primary, and the other one is the Secondary
- Both devices have the same switch-back settings (Switch-back or Non-switch-back)
- Both devices have the same Operation Mode (Port Grouping with Failover or Port Redundancy with Failover)

Use the Preconfiguration console > **Device Information and Status** and **Operation Mode** options to check for the last two items.

Contacting Technical Support

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

Appendix A

System Checklists

Use the following checklists to record relevant system information:

- *Control Manager Server Address Checklist* on page A-2
- *Control Manager Server Ports Checklist* on page A-4
- *Network VirusWall Deployment Checklist* on page A-5

You will need them from time to time.

Control Manager Server Address Checklist

The following server address information is required during installation and for configuring the Control Manager server to work with your network. Record this information here for easy reference.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
CONTROL MANAGER SERVER INFORMATION		
IP address	10.1.104.255	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Registration Key (RK) and Activation Code (AC)	RK: AC:	
WEB SERVER INFORMATION		
IP address	10.1.104.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
SQL-BASED CONTROL MANAGER DATABASE INFORMATION		
IP address	10.1.114.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	sqlserver	
PROXY SERVER FOR COMPONENT DOWNLOAD		
IP address	10.1.174.225	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
PROXY SERVER FOR TREND VCS AGENT		
IP address	10.1.177.225	

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Fully Qualified Domain Name (FQDN)	firewall.company.com	
NetBIOS (host) name	firewall	
SMTP SERVER INFORMATION (OPTIONAL; FOR EMAIL NOTIFICATIONS)		
IP address	10.1.123.225	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP TRAP INFORMATION (OPTIONAL; FOR SNMP TRAP NOTIFICATIONS)		
Community name	trendmicro	
IP address	10.1.194.225	

Control Manager Server Ports Checklist

Control Manager uses the following ports for the indicated purposes.

PORT	SAMPLE	YOUR VALUE
SMTP	25	
Pager COM	COM1	
Management Console and Update/Deploy components	80	
Firewall, 'forwarding' port (Optional; used during Control Manager Agent installation)	224	
Trend Micro Management Infrastructure (TMI) external process communication (for remote products)	10319	
TMI internal process communication	10198	
Entity emulator	10329	

Note: Control Manager requires exclusive use of ports 10319 and 10198.

Network VirusWall Deployment Checklist

The following information is used during agent installation.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Terminal software	HyperTerminal, tw-win2k-spare	
Public encryption key location	C:\MyDocu-ments\E2EPulic.dat	
Network VirusWall account	Account: admin Password: ***** **WARNING!** *Keep the written password in a secure place.*	
Control Manager server IP address or host name	NJ-cm1 / 10.1.111.10	
Control Manager server root account	Account: root Password: *****	
Network VirusWall managed product name	NVW2500-NY	

Index