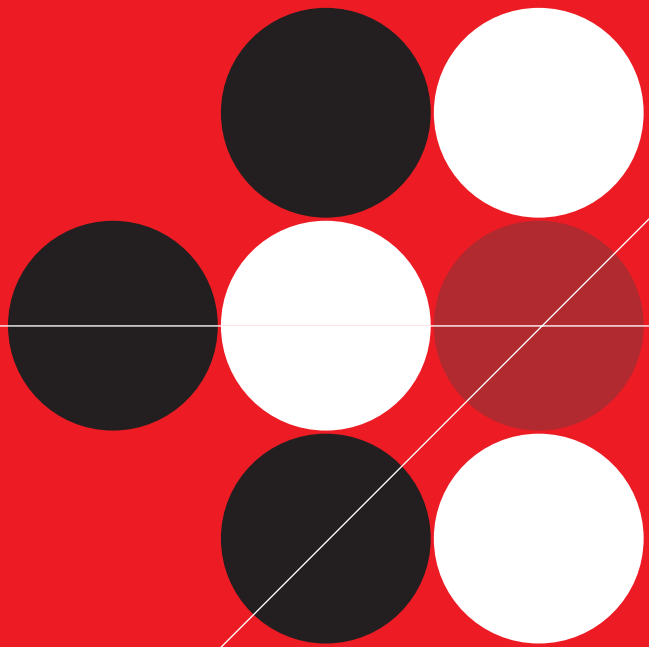
TREND MICRO™
Network VirusWall™ 2500

Administrator's 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 Administrator's Guide and 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 renewed on an annual basis at Trend Micro's then-current Maintenance fees. In order to use the Software and to receive Maintenance, You may be required to input a registration key and to register the Software at Trend Micro's Web site.

Document Part No. NVEM12219/50301

Release Date: May 2005

The Administrator's Guide for Network VirusWall 2500 discusses the features of Network VirusWall and provides administration instructions for your production environment. Read it prior to configuring the software.

For technical support, please refer to *Getting Support* on page 6-1 for technical support information and contact details. Detailed information about how to use specific features within the software is available in the online help file and online Knowledge Base at Trend Micro's Web site.

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 1: Understanding Network VirusWall—continued

Chapter 2: Configuring Scan, System, and Device Settings

Chapter 2: Configuring Scan, System, and Device Settings—continued

Chapter 3: Updating Components

Chapter 4: Viewing Status, Logs, and Summaries

Chapter 5: Troubleshooting and FAQs

Chapter 6: Getting Support

Preface

Welcome to the Administrator's Guide for Trend Micro™ Network VirusWall™ 2500. This book contains information about the tasks you need to configure Network VirusWall 2500. This book is intended for novice and experienced users of Trend Micro Control Manager™ and Network VirusWall who want to quickly configure, administer, and monitor the product.

The Network VirusWall package includes the Trend Micro Solutions CD for Network VirusWall. If you are planning large-scale deployment of Network VirusWall or have complex network architecture, refer to the *Control Manager Getting Started Guide* and the *Network VirusWall Getting Started Guide* PDF files on the Solutions CD.

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 a component of the Control Manager Online Help. It contains explanations on the Network VirusWall components and features, as well as 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 Trend Micro Solutions CD for Network VirusWall 2500 or downloadable from the Trend Micro Web site

  The GSG contains instructions on how to deploy Network VirusWall, which includes Control Manager server installation, common Network VirusWall deployment, Network VirusWall preconfiguration, port configuration, and post-installation configuration.

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

  This AG contains detailed instructions on how to configure and administer Network VirusWall from the applicable management tools, as well as explanations on the Network VirusWall concepts and features. See *About This Administrator's Guide* for chapters available in this book.

Note: Trend Micro recommends checking the Update Center for updates to the Network VirusWall documentation and program file.

About This Administrator's Guide

The Network VirusWall Administrator's Guide, which is in PDF, provides the following information:

- Overview of the product and its architecture, and description of all new features in Network VirusWall 2500, see *Understanding Network VirusWall* on page 1-1
- Procedures to configure and administer Network VirusWall from the applicable management tools, see *Configuring Scan, System, and Device Settings* on page 2-1
- Procedures to update Network VirusWall components, see *Updating Components* on page 3-1
- Instructions to access antivirus information to evaluate your organization's virus protection policies and identify clients that are at a high risk of infection, see *Viewing Status, Logs, and Summaries* on page 4-1
- Troubleshooting tips for issues encountered during device administration, which includes debug and error logs interpretation, see *Troubleshooting and FAQs* on page 5-1
- Guidelines to obtain more information, see *Getting Support* on page 6-1

In addition, this Administrator's Guide provides the following appendices:

- *Device Specifications* on page A-1
- *BMC Logs* on page B-1
- *Network VirusWall 1200 and 2500 Feature Comparison* on page C-1
- *Glossary* on page D-1

Audience

The Network VirusWall documentation assumes a basic knowledge of security systems and devices, as well as network administration.

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

Understanding Network VirusWall

This chapter introduces Network VirusWall 2500 and provides an overview of its technology, capabilities, and hardware connections.

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 including unprotected devices as they enter the network, using threat-specific knowledge from Trend Micro deployed at the network layer.

Unlike security solutions that only monitor threats or provide threat information, Network VirusWall helps organizations take precise outbreak security actions and proactively detect, prevent or contain, and eliminate outbreaks. By deploying Network VirusWall in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden. Network VirusWall supports the Trend Micro™ Enterprise Protection Strategy. Trend Micro Control Manager™ 3.0 manages Network VirusWall devices.

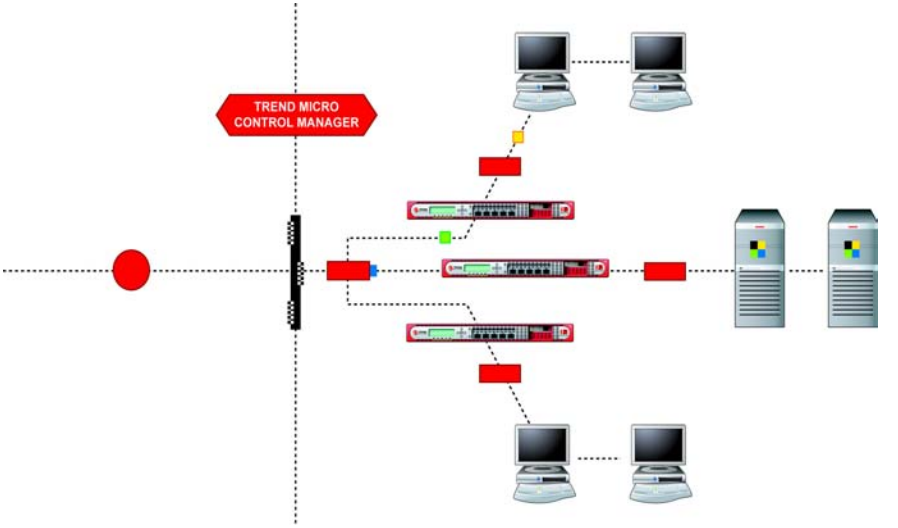


FIGURE 1-1. How Network VirusWall works

Network VirusWall monitors network packets and events that could indicate an attack against a network. The device scans all the traffic on a specific network segment. Deploy Network VirusWall in a hub or switched environment. A Control Manager server must be available to manage Network VirusWall devices.

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* in the Network VirusWall *Getting Started Guide* for instructions 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
- 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

A Control Manager server can manage up to 10,000 content security and antivirus products, including Network VirusWall devices. Use the Control Manager management console to monitor and report on Network VirusWall activities such as infections, security violations, or outdated components. You can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date.

Functions and Capabilities

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.

From the Control Manager management console, you can accomplish the following administrative tasks:

- *Analyze Your Network's Protection Against Viruses*
- *Update Your Protection*
- *Enforce Antivirus Policies*
- *Monitor the Network for Suspicious Activity*
- *Monitor Network VirusWall Devices via SNMP*
- *Utilize Control Manager Services*

Analyze Your Network's Protection Against Viruses

Network VirusWall generates various types of logs, including security and event logs. Use these logs to verify module updates and network outbreaks and view viruses found in network packets.

Update Your Protection

Virus writers write and release new viruses via different media every day, especially the Internet. To help ensure your protection against the latest threats is current, periodically update Network VirusWall components, including the network virus pattern file, network scan engine, network outbreak rule and program file.

Enforce Antivirus Policies

Network VirusWall monitors clients on the Protected Network and can determine the status of their antivirus protection. Based on this information, configure antivirus policy settings to block, pass, or redirect traffic, including traffic from specified TCP and UDP ports.

Monitor the Network for Suspicious Activity

A high number of simultaneous network sessions or connections on certain client ports can be a signal of an attack or virus infection. Enable and configure Network Outbreak Monitor to have Network VirusWall observe all sessions and connections on the Protected Network. In addition, configure the Control Manager Event Center to trigger an outbreak alert notification message when network conditions meet Network Outbreak Monitor criteria.

Monitor Network VirusWall Devices via SNMP

Network VirusWall supports Simple Network Management Protocol (SNMP) v2 and can send traps to specific network management stations. For added security, you can require network management stations to authenticate before gaining access to the Network VirusWall Management Information Base (MIB).

Utilize Control Manager Services

Control Manager services and products provide added benefits and capabilities when used in tandem with Network VirusWall. These include:

- Outbreak Prevention Services

  Network VirusWall can receive Outbreak alerts from the Control Manager server during a virus outbreak. Based on Outbreak Prevention Policy settings, Network VirusWall can block the following:

  - **IP addresses**—a single destination IP address or a range of addresses
  - **Protocols—**TCP, UDP, and ICMP
  - **Ports—**a single destination port or a range of ports
  - **Instant Message channels—**AOL™, ICQ™, MSN Messenger™, and Yahoo! Messenger™
  - **File transfers—**file names or extensions transferred via FTP, HTTP, and Windows™ Network File Sharing
  - **Websites—**a single Web site, or a group of Websites

- Trend Micro™ Vulnerability Assessment (VA)

  Network VirusWall can query Vulnerability Assessment™ (VA) to determine which computers on the Protected Network have vulnerabilities that may expose them to attacks and infections. Configure Network VirusWall to block or pass all traffic to and from vulnerable clients.

- Trend Micro™ Damage Cleanup Services (DCS)

  If clients on the Protected Network become infected, you can redirect them to access Damage Cleanup Services (DCS) to clean up their systems and remove virus remnants that could re-attack the network. Download the latest DCS damage cleanup template through Control Manager to help ensure you have the most up-to-date cleanup capabilities.

Tip: See the *Control Manager Getting Started Guide* and *Online Help* for detailed information.

Network VirusWall Architecture

This section describes the Network VirusWall components and antivirus defenses, which includes discussion about its antivirus technology and types of network threats.

Components

Two major components make up a Network VirusWall system:

- *Device(s)*
- *Management*

Device(s)

Unlike security solutions that only monitor threats or provide threat information, Network VirusWall helps organizations take precise outbreak security actions and proactively detect, prevent or contain, and eliminate outbreaks. By deploying Network VirusWall devices in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden.

Management

Network VirusWall provides the following management tools:

- Preconfiguration console
- Control Manager management console

Note: A Control Manager server must be available to manage Network VirusWall devices.

- LCD module (also known as LCM console)

Preconfiguration Console

The Preconfiguration console allows you to perform the network configuration and set the device settings by directly connecting to the Network VirusWall device using a terminal communication application. After completion of preconfiguration procedures, the Network VirusWall device will register itself as a managed product to the Control Manager server.

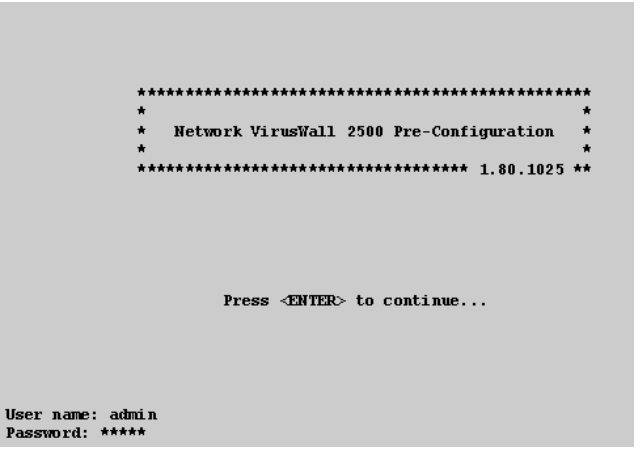


FIGURE 1-2. The Preconfiguration console login screen

Control Manager Management Console

A Control Manager server must be available to centrally manage Network VirusWall devices.

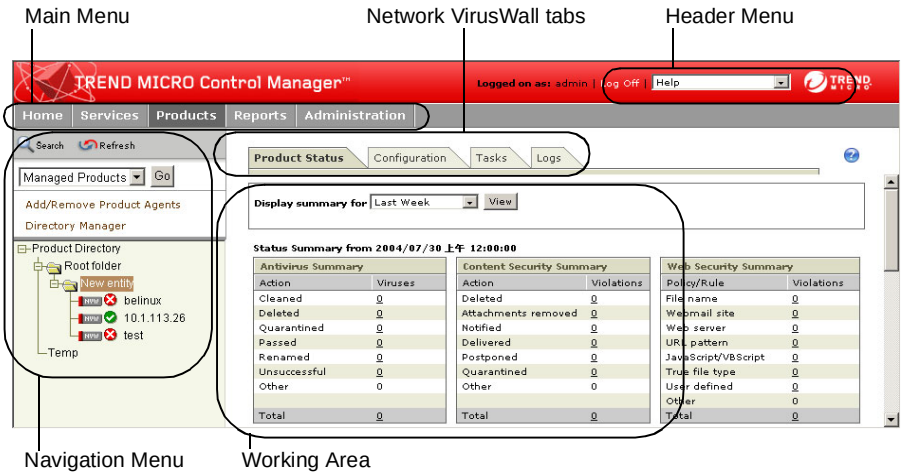


FIGURE 1-3. The Control Manager management console

The Control Manager management console allows you to administer managed Network VirusWall products remotely. Network VirusWall supports the Trend Micro™ Enterprise Protection Strategy.

Tip: Trend Micro recommends using Trend Micro Control Manager for centrally managing Network VirusWall. With Control Manager, you can manage groups of Network VirusWall devices at the same time, and take advantage of its Web-based management console's accessibility.

See *page 2-2* to access Network VirusWall devices from the Control Manager management console.

Refer to the Control Manager *Online Help* or *Getting Started Guide* for Control Manager information.

LCD module

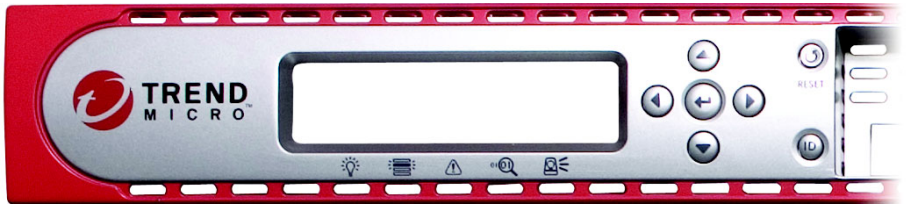


FIGURE 1-4. LCD and Control Panel make up the LCD module

This document uses the term "**LC**D **m**odule (LCM or LCM console)" to refer to the Liquid Crystal Display (LCD) and the control panel Network VirusWall front panel elements collectively. The best use of the LCM console is for simple, on-the-spot Network VirusWall settings adjustments, as well as for viewing hardware logs and system information.

The LCM console allows you to perform the following basic configuration:

- Configure device settings

  Device settings such as the Network VirusWall IP, netmask, gateway, and primary and secondary DNS servers, as well as the Control Manager IP address and root account.

- View and delete BMC logs

  BMC logs refer to the Board Management Control or hardware (H/W) logs. These logs report critical hardware status and error. Use the LCD module to purge BMC logs manually. See *page 4-25* for instructions on how to purge BMC logs.

- View system information

  Use the LCM console to view the Network VirusWall memory and CPU usages, as well as its concurrent activities.

The following table lists the differences between the management tools:

USAGE	PRECONFIG-URATION CONSOLE	CONTROL MANAGER MANAGEMENT CONSOLE	LCD MODULE
Register a Network VirusWall device to a Control Manager environment	●		●
Set network configuration (Operation Mode)	●		
Set interface speed and duplex mode	●		
Set advanced device settings	●		
Manage Network VirusWall user accounts	●		
Restart device	●		●
View network configuration	●	●	
Reset device	●	●	
Monitor Network VirusWall events, status, and summaries		●	
Update and deploy components		●	
Configure scan settings		●	
Configure device settings	●	●	●
View and delete BMC (device) logs			●
View device information (for example, CPU usage, memory usage)	●		●

TABLE 1-1. Comparison of the Network VirusWall management tools

To access Network VirusWall settings from the:

- Preconfiguration console, see *page 2-37*
- Control Manager management console, see *page 2-2*
- LCM console (LCD module), refer to the *Getting Started Guide* > *Preconfiguring Network VirusWall Using the LCD Module* section

Antivirus Technology

Network VirusWall is equipped with state-of-the-art antivirus technology that targets network viruses. Because it was designed to act as shield for a segment of your network, it not only can scan and drop infected network packets before they reach your clients, but also prevent vulnerable or infected clients from accessing the public network.

The number and complexity of virus threats are on the rise. Many organizations have put in place multi-layer virus protection in the form of a "security suite"– several antivirus installations that provide a patchwork virus defense. This type of virus protection, however, is effective only after servers or clients detect a virus; in other words, when a virus is already on your network.

Equipped with the Trend Micro™ network scan engine and network virus pattern file, Network VirusWall scans every packet entering and leaving a Protected Network segment in real-time (see *Network VirusWall 2500*). Trend Micro has specially designed Network VirusWall to recognize network viruses, drop infected packets before they enter the Protected Network, and prevent future attacks on your network caused by network virus infections. See *Understanding Threats* for more information on viruses, including network viruses.

Understanding Threats

Tens of thousands of viruses exist, with more coming into existence each day. Although once most common in DOS or Windows, computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and Web sites.

In general, computer viruses fall into the following categories:

- **ActiveX malicious code—**resides in Web pages that execute ActiveX controls
- **Boot sector viruses—**infects the boot sector of a partition or a disk
- **COM and EXE file infectors—**executable programs with *.com or *.exe extensions
- **Joke programs—**virus-like programs that often manipulate the appearance of things on a computer monitor
- **Java malicious code—**operating system-independent virus code written or embedded in Java

- **Macro viruses—**encoded as an application macro and often included in a document
- **Trojan horses—**executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter
- **VBScript, JavaScript or HTML viruses—**reside in Web pages and downloaded through a browser
- **Worms—**a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the malware mentioned above, such as worms, are actually network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

Protection

The principle function of Network VirusWall is to separate a segment of the network from the rest of public network (that is, the Internet, other LAN segments, and so on). Throughout, this document refers to this separated segment as the *Protected Network*.

Tip: Trend Micro recommends deploying a Network VirusWall device between switches or routers. Although the exact location of the device depends on the network topology, position the device between level 2 (L2) switches or level 3 (L3) routers.

Figure 1-5 depicts a representation of the Network VirusWall protection.

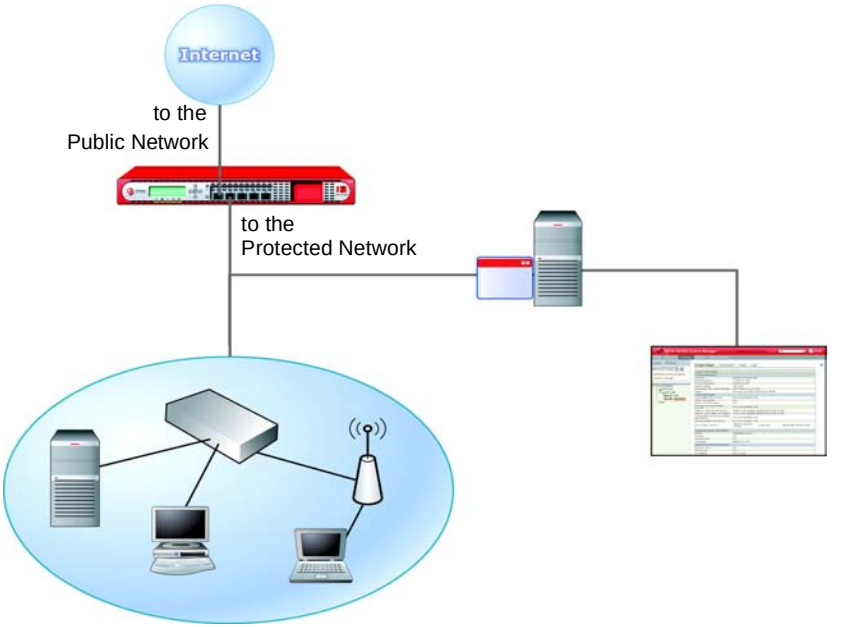


FIGURE 1-5. Protected and Public networks

Network VirusWall creates the Protected Network to accomplish these tasks:

- Scan network traffic to and from clients on the Protected Network
- Assess vulnerability on clients on the Protected Network
- Block clients on the Protected Network if they do not conform to the security policies of your organization
- Isolate infected clients to prevent viruses from spreading outside of the Protected Network

Antivirus and Outbreak Monitoring Components

Network VirusWall protects an organization through:

- Real-time network packet scanning
- Virus outbreak monitoring
- Policy Enforcement

Real-time Network Packet Scanning

Traditional antivirus software provides real-time scanning by monitoring an operating system's file I/O system. Such applications help prevent "traditional" viruses, which had to be on a computer's hard drive to launch an attack on the network.

Network VirusWall's proprietary Network Scan Engine is responsible for the packet analysis. It utilizes the following sub-components:

- Network Virus Pattern, which contains threat signatures and is updatable via manual or scheduled update
- Outbreak Prevention Policy (OPP) from the Outbreak Prevention Services available in the Control Manager server

  An OPP only applies when the Outbreak Prevention Services is in **Outbreak Prevention Mode**.

The real-time network packet scanning identifies and acts upon packets:

- With malicious code
- That violate outbreak prevention policies

When real-time scan detects any of these conditions, it can apply one of following actions configurable via the Control Manager management console Scan Options page:

- Pass infected packet
- Drop infected packet (that is, block an infected packet)
- Drop infected packet and Quarantine infected machine

Note: See *Quarantined and Blocked Clients* on page 1-26 to learn more about a client's behavior when Network VirusWall applies the 2nd or 3rd action.

- Damage Cleanup-related actions

Tip: Refer to the Control Manager *Getting Started Guide* or *Online Help* for details about Damage Cleanup actions.

Monitor the real-time packet scanning activities through the **Logs** > **Security Logs** > **Viruses found in network packets** option. In addition, enable Control Manager to send notifications about real-time packet scanning activities via the **Event Center** > **Network virus alert** option.

See the following sections to:

- Configure real-time network packet scanning, *page 2-7*
- Configure the safe sites list, *page 2-22*
- Determine whether the Real-time Network Packet Scanning acted upon a packet, *page 4-22*
- Allow Control Manager to send real-time packet scan notifications, refer to the *Control Manager Getting Started Guide* > *Use Event Center* section

Network Outbreak Monitoring

Network Outbreak Monitor (NOM) scans traffic to and from protected segments for telltale signs of an ongoing outbreak. It allows you to apply actions on outbreaks as they begin, thereby minimizing the extent of the damage. NOM is capable of monitoring the packet types from the following protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)

Network threats, such as the Slammer worm, tend to propagate as follows:

1. Infect a machine with specific software vulnerability.
2. From the infected machine, scan the network for other machines with a similar vulnerability, causing the following behavior on the network:
   - Unusual traffic direction
   - Unusually high network traffic
3. Copy the malware code to the vulnerable machines, and then repeat step i.

NOM can detect unusual changes in network traffic patterns, allowing you to react to the outbreak as it begins. It uses the following components to detect unusual events:

- Exception list
- Traffic volume rules
- Connection rules

Exception List

The Network VirusWall device does not monitor clients belonging to the NOM exception list for potential network outbreak-related activities. The device monitors clients that do not belong to the exception based on the traffic volume and connection rules. See *Exempted Clients* on page 1-24 for details about clients belonging to the exception list.

Traffic Volume Rules

NOM maintains a running count of all relevant packet types to determine whether traffic volume has increased. Consequently, NOM uses the traffic volume rules to

detect whether the overall traffic or traffic using any of the supported protocol increased over a specific period. NOM does this by comparing the running count against the benchmark count dictated by the traffic volume rules.

Connection Rules

NOM is able to detect computers that are:

- Being used as launching points for network virus infections
- Experiencing a Distributed Denial of Service (DDOS) attack

NOM monitors the packet-sending behavior between machines on the network over time. The connection rules use this information to detect whether connections from a machine or certain machines to other machine or groups of machines increase over a specific period.

Monitor the NOM activities through the **Logs** > **Event Logs**. In addition, enable Control Manager to send notifications about NOM activities via the **Event Center** > **Potential vulnerability attack detected** option.

See the following sections to:

- Configure network outbreak monitoring, *page 2-12*
- Configure the NOM exception list, *page 2-22*
- Determine whether NOM detected an outbreak, *page 4-19*
- Allow Control Manager to send NOM notifications, refer to the *Control Manager Getting Started Guide* > *Use Event Center* section

Policy Enforcement

Network VirusWall is capable of identifying a packet source, and then determining if it complies with the current antivirus and vulnerability-elimination policies. It can determine if the packet source (that is, the computer where the packet originated) has antivirus protection, service packs, and security patches installed, and so on. It helps ensure that machines sending inter-segment traffic comply with the network's antivirus policies. It verifies if the machines that send traffic through a Network VirusWall device have the:

- Functional antivirus protection
- Required security patches installed

Policy Enforcement assesses the status of client antivirus installations and vulnerabilities by using the following components:

- Exception list

  NVW does not monitor for policy violation those clients belonging to the Policy Enforcement exception list. NVW monitors clients that do not belong to the exception list based on the traffic volume and connection rules. See *Exempted Clients* on page 1-24 for details about clients belonging to the exception list.

- Six (6) antivirus and vulnerability-elimination policies

  These six policies invoke the actual Policy Enforcement process.

Table 1-2 enumerates the six (6) Policy Enforcement policies and their enforcement order.

ORDER	POLICY NAME	POLICY CONTENT
1	Policy 6	Vulnerabilities discovered by Vulnerability Assessment (VA)
2	Policy 1	Outdated virus pattern files for Trend Micro antivirus products
3	Policy 2	Outdated scan engine files for Trend Micro antivirus products
4	Policy 3	Identifiable third-party antivirus product
5	Policy 4	Windows-based clients with no identifiable antivirus products
6	Policy 5	All unidentifiable clients

TABLE 1-2. Antivirus and vulnerability-elimination policies and their execution order

Policy Enforcement can use the Vulnerability Assessment (VA) information in the Network VirusWall's Control Manager server to determine if a source of an inter-segment traffic already has the required patches and service packs.

Note: To use VA, you must activate the service on the Control Manager server using a valid Activation Code.

Policy Enforcement is able to detect the following products:

- Trend Micro™ OfficeScan Corporate Edition™ 5.5 SP1, 5.58, 6.0, and 6.5
- Trend Micro™ ServerProtect™ for Windows 5.5, 5.56, and 5.58
- Trend Micro PC-cillin™ Internet Security™ 11.35 and 12

Note: Enable Trend Micro Discover Protocol (TMDP) to allow Policy Enforcement to detect PC-cillin 11.35. See *page 2-20*.

- McAfee™ VirusScan with Orchestrator agent 3.0
- Norton™ Antivirus Corporate Edition 8.0 and 9.0

Note: Network VirusWall is unable to apply Policy Enforcement to OfficeScan or PC-cillin-based clients with Trend Micro Personal Firewall feature enabled. Verify that the Personal Firewall service is not running in the background to prevent this issue from occurring. See *page 5-29* for additional troubleshooting information.

Apply one of the following actions to non-compliant clients:

Tip: The Policy Enforcement action configurable through the Control Manager management console Policy Enforcement screen.

- Block—blocks all selected TCP and UDP services
- Pass—allows all traffic
- Redirect—redirects clients to another Web site when they make HTTP requests

The **Logs** > **Event Logs** (information) screen provides information on the Policy Enforcement configuration modification. In addition, enable **Windows Messenger Messages**, **HTTP Messages,** and **Blocking Pending Clients** to instruct Policy Enforcement to provide the following client notifications:

- Detection page (see *Figure 1-6*)
- Results page, which can be one of the following:
  - Redirect page—can be your organization's Intranet home page or a customized Web page detailing how to solve a client's threat or vulnerability issue (see *Figure 1-7*)
  - Blocking page—can include a URL that clients can go to solve its threat or vulnerability issue (see *Figure 1-8*)

Note: The Detection and Result pages only apply to clients whose packets originate from HTTP traffic. See *Pending Clients* on page 1-24 for details.
In addition, the Detection and Result pages only display if the **System Settings** > **HTTP Messages** option is enabled. See *page 2-27* to configure System Settings.

- Windows Messenger Service—use the Windows Messenger notification to notify Windows-based clients using any types of protocol (that is, HTTP, FTP, telnet, and so on) to access a public network resource (see *Figure 1-9*)

Note: This type of Network VirusWall client notification makes use of **Windows Messenger Service**. This feature does not require any Windows messaging server (for example, Windows Messenger Server or Live Communications Server) or instant messaging application (for example, Windows Messenger or MSN Messenger) to send popup notifications.

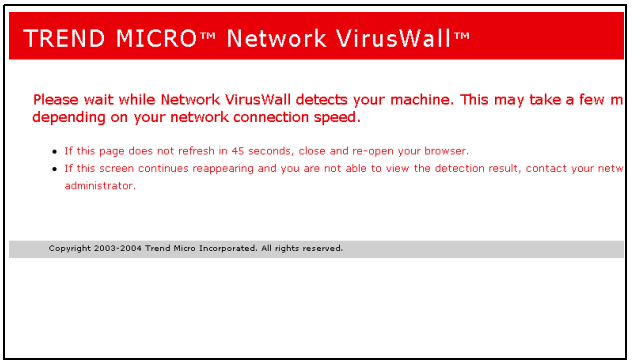


FIGURE 1-6. Sample Policy Enforcement Detection page

FIGURE 1-7. Sample Policy Enforcement Redirect page

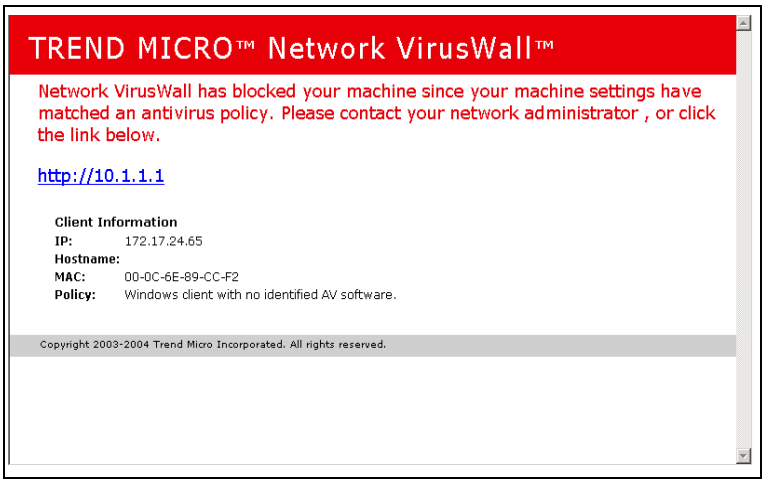


FIGURE 1-8. Sample Policy Enforcement Blocking page with a redirect URL

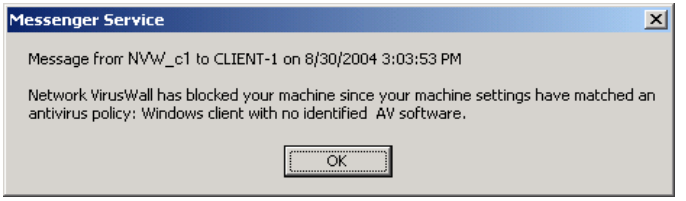


FIGURE 1-9. Sample Policy Enforcement Windows Messenger Service popup message

See the following sections to:

- Configure Policy Enforcement, *page 2-12*
- Configure the Policy Enforcement exception list, *page 2-22*
- Instruct Policy Enforcement to inform clients of its detection through the Detection and Results page, *page 2-18*
- Enable Windows Messenger Service popup message, see *page 2-29*

Understanding Clients

A packet source (that is, a machine) can have more than one network interface card (NIC) and therefore can have more than one IP address. Network VirusWall considers each IP address a separate client.

The following types of clients apply to Network VirusWall depending on the antivirus or outbreak-monitoring component and action:

- Pending clients
- Exempted clients
- Quarantined and blocked clients

Pending Clients

Pending clients refer to IP addresses that Network VirusWall detects for Policy Enforcement compliancy. You can decide to inform users of this task by enabling the **Blocking Pending Clients** and **System Settings** > **HTTP Messages** options. When enabled, the Blocking Pending Clients option displays a Detection Web page (as in *Figure 1-6*).

To display the Detection page to pending clients, see *page 2-18*.

Exempted Clients

Exempted clients are clients that belong to the following:

- Policy Enforcement exception list
- Network Outbreak Monitor exception list

Potential exempted clients include:

- Trusted machines owned by the organizations CEO, which should not be delayed
- Proxy servers that clients use to access the Internet
- DNS servers
- Machines to which Network VirusWall redirects traffic
- Machines generating high-volume traffic, such as servers hosting an antivirus product that deploy components to its clients

Tip: Add non-Windows machines with IP addresses (for example, Linux or Netware servers, IP Phones, or network printers) in the Policy Enforcement and Network Outbreak Monitor exception lists. This prevents Network VirusWall from blocking these resources.

Policy Enforcement Exception List

This list is configurable via the **Exceptions Lists** > **Enable exceptions for Network VirusWall Policy Enforcement** option. NVW does not monitor for policy violation those clients belonging to the Policy Enforcement exception list. Therefore, Policy Enforcement will never monitor these clients for violation of the six antivirus and vulnerability-elimination policies (see *Table 1-2*).

Network Outbreak Exception List

This list is configurable via the **Exceptions Lists** > **Enable exceptions for Network Outbreak Monitor** option. NVW does not monitor for potential network outbreak-related activities those clients belonging to the Network Outbreak Monitor exception list. Therefore, NOM will never monitor these clients for violation of traffic volume or connection rules (see *page 1-17*).

See the following sections to:

- Enable exceptions for Network VirusWall Policy Enforcement, *page 2-22*
- Enable exceptions for Network Outbreak Monitor, *page 2-22*

Quarantined and Blocked Clients

Network VirusWall allows you to quarantine infected clients and block clients that violate enforcement policies. Quarantining clients and blocking clients are not the same.

Blocked clients are clients that Network VirusWall performed the **Drop infected packet** real-time packet scan action on. Network VirusWall will only block malicious packets and the blocked client can still send traffic through Network VirusWall.

Quarantined clients are clients that Network VirusWall performed the **Drop infected packet and Quarantine infected machine** real-time packet scan action on. Network VirusWall blocks the malicious packet and prevents the infected packet source from sending traffic through Network VirusWall.

See the following sections to:

- Configure Network VirusWall real-time scan action, *page 2-7*
- Configure Network VirusWall Policy Enforcement setting, *page 2-12*
- Configure the Safe Sites list accessible to blocked and quarantined clients, see *page 2-22*
- View quarantined and blocked clients, *page 4-16*
- View real-time scan logs, *page 4-22*

SNMP

Simple **N**etwork **M**anagement **P**rotocol (SNMP) is set of communications specifications for managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

In the SNMP management architecture, one or more computers on the network act as a network management station (NMS) and poll the managed devices to gather information about their performance and status. Each managed device has a software module, known as an agent, which communicates with the NMS.

See *page 4-27* for details on how to configure the Network VirusWall SNMP settings.

MIBs

On the agents, information resides in the form of objects. Each object is essentially data about a particular aspect of the managed device, such as the number of packets received or memory utilization statistics. Together, the objects comprise a Management Information Base (MIB). By modifying the contents of an MIB, an NMS can change the settings of a managed device and perform actions on the device, such as a reboot.

Traps

The NMS is not the only side that can initiate communication. The managed devices can send notifications, known as traps, to the NMS when certain events occur, such as a shutdown or authentication error.

Communication

Communication between the NMS and the agent take place through the following basic commands:

- Get—NMS reads data from the agent MIB
- Set—NMS writes data to the agent MIB
- Trap—agent notifies NMS when important events occur

Note: Advanced versions of SNMP include variations of these commands to perform functions that are more specific.

Security

Managed devices can protect their MIBs by granting only specific network management stations access. One way of doing this is through authentication. Managed devices can require that all NMS's belong to a community, the name of which acts as a password that the managed devices use to authenticate management stations attempting to gain access. Additionally, the settings for a community can include access privileges, such as READ-ONLY and READ-WRITE, that are granted to network management stations.

Specifications

Table 1-3 and *Table 1-4* enumerate the supported Network VirusWall SNMP specifications:

VERSION	v1, v2c
ACCESS PRIVILEGES	READ ONLY (the GET command)
MANAGEMENT INFORMATION BASE (MIB)	MIB II, with the following standard objects: • System group • Interfaces group • Enterprise group, including system status and memory utilization
ACCEPTED COMMUNITY NAMES	Community names with the following characteristics: • Default name– public • Access privileges- READ ONLY (the get command) • Maximum number of community names- 5 • Maximum length of community name- 33 alphanumeric characters
TRUSTED NETWORK MANAGEMENT STATIONS (NMS)	Allows up to 255 specific network management station IP addresses to access the agent

TABLE 1-3. Supported SNMP Agent specifications

<table>
<tr><td>COMMUNITY NAMES</td><td>One community name allowed</td></tr>
<tr><td>DESTINATION NETWORK MANAGEMENT STATION (NMS) IP ADDRESSES</td><td>One NMS IP address allowed per community name</td></tr>
<tr><td>GENERIC AND NORMAL TRAPS</td><td>Includes the following:
<table><tr><th>ID #</th><th>TRAP NAME</th><th>TRAP DESCRIPTION*</th></tr><tr><td>0</td><td>Coldstart</td><td>Enable SNMP agent</td></tr><tr><td>2</td><td>Linkdown</td><td>Network connection is broken</td></tr><tr><td>3</td><td>Linkup</td><td>Network connection is established</td></tr><tr><td>4</td><td>Authentication failure</td><td>Wrong user name or password when logging on the Preconfiguration console</td></tr><tr><td>none</td><td>NotifyShutdown</td><td>SNMP agent disabled</td></tr></table>
TRAP DESCRIPTION refers to the event that triggers Network VirusWall to send the trap.</td></tr>
</table>

TABLE 1-4. Supported SNMP Traps specifications

SNMP Trap Limitations

The following SNMP traps limitations exist:

- **Version supported:** 2c
- **Community Names:** one community name allowed
  - **Community name character limitations:** 1–33 alphanumeric characters (including underscore: "_")
- **Destination Network Management Station (NMS) IP addresses:** one NMS IP address allowed per community name
- **System location and System contact:** 0–254 characters (ASCII 32–126, excluding "&")

VLAN

A **V**irtual **L**ocal **A**rea **N**etwork (VLAN) is a network consisting of clients that are not on the same segment of a Local Area Network (LAN) but behave as if they were. These clients comprise a network in a virtual sense, through software residing on a networking device, such as a switch, which filters traffic using client MAC addresses (layer 2) or IP addresses (layer 3). VLANs reduce network congestion by managing the flow of traffic between clients that communicate often, even if they are not on the same network segment.

Tagged and Non-tagged Frames

When a local switch on the network receives a packet, it can use the destination port, destination MAC address, or protocol to determine to which VLAN the packet belongs. When other switches receive the packet, they determine VLAN membership either implicitly (using the MAC address) or explicitly (using a tag that the first switch added to the MAC address header).

Network VirusWall recognizes both tagged and non-tagged of IEEE 802.1Q VLAN frames, thereby preserving the VLAN structure on your network. Using the existing VLAN membership settings on your network, configure Network VirusWall to recognize up to 4094 VLAN IDs. Network VirusWall supports fifty (50) tagged VLANs and one (1) non-tagged VLAN. VLAN configuration can only be done while performing preconfiguration. Refer to the *Getting Started Guide* for instructions on how to set the Network VirusWall **VLAN Settings** and other preconfiguration tasks.

Tip: If the Control Manager server on your network belongs to a VLAN, bind Network VirusWall to the same VLAN (tagged or non-tagged). This will help ensure effective communication between the Control Manager server and Network VirusWall.

To view VLAN settings, see *page 4-2*.

Network VirusWall 2500

Network VirusWall 2500 is a high capacity, gigabit-capable device added to the Network VirusWall (NVW) product line. This model provides the following new features:

- Gigabit connectivity
- Support for High Availability (see *page 1-34*)

  Network VirusWall 2500 achieves high availability (HA) using the following solutions:
  - Redundant ports
  - Redundant devices
  - Fault tolerance solutions
- Support for up to four different internal network segments

  Network VirusWall 2500 can run in Port Grouping Operation Mode using up to four on-board ports. This mode enables a single Network VirusWall device to support and protect up to four different internal network segments.
- Configurable interface speed and duplex mode

  Refer to the *Getting Started Guide > Setting the Interface Speed and Duplex Mode* section for details.

In addition, Network VirusWall 2500 provides the following enhancements from Network VirusWall 1200:

- Ability to import and export the Network VirusWall configuration file through the Preconfiguration console (see *page 2-39*)
- Allow ICMP request from other computers for device troubleshooting

  Send a ping request to the Network VirusWall device to determine whether the device is running (see *page 2-38*).
- Support for additional identifiable Trend Micro products

  Network VirusWall can now identify Trend Micro PC-cillin Internet Security version 11.35 or 12 installation (see *page 2-17*).
- Additional device and system options

  Use the Control Manager management console to specify whether to display Windows Messenger Service popup messages when Network VirusWall blocks a client's access attempts (see *page 1-21*). In addition, use the applicable management tools to easily locate a NVW 2500 device for troubleshooting or maintenance by turning on the UID (see *page 2-30*).

Seven (7) User-definable LAN Ports

Network VirusWall offers high-performance gigabit connectivity via its seven (7) user-definable LAN ports (five (5) copper ports and two (2) fiber-optic ports). This number of ports allows a Network VirusWall device to support up to four (4) virtual LANs (VLANs).

Note: A fiber media converter (FMC) is not necessary if your network environment is using fiber connectivity. Network VirusWall 2500 supports direct fiber connectivity. Network VirusWall supports fifty (50) tagged VLANs and one (1) non-tagged VLAN.

The gigabit platform has both copper and fiber-optic interface connectivity that allows full-duplex operation in 1000Mbps mode. This high bandwidth helps protect network continuity through failopen, failover, and port and device redundancies.

The new hardware design helps Network VirusWall to:

- Achieve high availability
- Support up to 1 million concurrent sessions and 4,096 concurrent clients during policy enforcement. See *Network VirusWall 1200 and 2500 Feature Comparison* on page C-1 for more comparison information between the new and old Network VirusWall models.

Table 1-5 lists the system port names:

PORT NUMBER	SYSTEM PORT NAME
1	eth3
2	eth2
3	eth1
4	eth0
5	eth4
6	ext0
7	ext1

TABLE 1-5. System port names

The Network VirusWall Log Viewer refers to each port using the system port name. *Figure 1-10* provides an example.

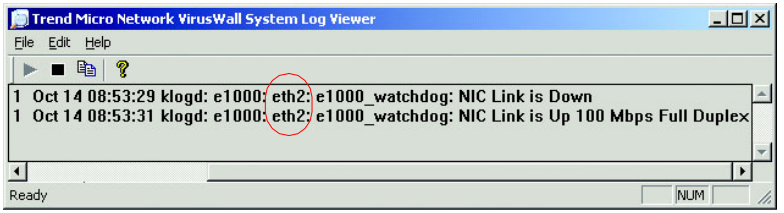


FIGURE 1-10. Viewing logs generated by the Network VirusWall ports from the Log Viewer main window

See *page 4-26* for instructions on how to use the Network VirusWall Log Viewer.

Consider the following points when setting the Network VirusWall ports:

- Network VirusWall reserves ports 1 and 2 for a failopen deployment
- Depending on the Operation Mode, there can be a maximum of four (4) INT ports or two (2) EXT ports
- Network VirusWall reserves port 5 for a failover deployment
- Use port 5 when running the Rescue Utility or Firmware Flash Utility (see *page 5-2*)
- Port 5 is also known as the FAILOVER port

High Availability

Network VirusWall 2500 achieves high availability (HA) using the following solutions:

- Redundant ports and devices
- Failover
- Failopen

Tip: Refer to the *Getting Started Guide* > *Understanding and Testing the Network VirusWall Deployment* section for details on how to apply a failover and failopen solution in a Network VirusWall deployment.

Redundant Ports and Devices

Port redundancy allows you to use a redundant physical link implementation for securing maximum network uptime and reliability. A mesh network is the target topology for the redundant port solution.

In a port redundancy solution, Network VirusWall provides two pairs of internal and external ports to connect to the up-link and downlink switches in dual paths.

Applying a port redundant solution requires the completion of the following tasks:

1. Allocation of port group A with two (2) ports— one external port, one internal port
2. Allocation of port group B with two (2) ports— one external port, one internal port
3. Configuration of the redundancy port group with port groups A and B

To enable the failover fault-tolerance solution, redundant devices usually accompany the port redundancy configuration. In a port-redundant NVW implementation, multiple connection paths exist, each with redundant devices, to help ensure that the connection is still viable even if one (or more) paths fail. The capacity for automatic failover means that the device can maintain normal functions despite the inevitable interruptions caused by problems with equipment. In a failover deployment, if one of the devices in a failover pair fails, the other Network VirusWall device maintains all settings, connections, and sessions.

Port Redundancy Considerations

1. Consider the following points when implementing a port redundancy deployment:
2. A redundant group must include two port groups with different EXT and INT ports
3. A port group consists of one EXT port and one INT port
4. Each port group can contain:
   - Ports and port attribute
   - Other port groups
5. Each port group can possess configurable attributes– you can choose whether to configure settings for a port group
6. Port groups cannot share the INT port; they can share the EXT port
7. Packets cannot be routed into different port groups
8. Configure the FAILOVER port as a separate port, which should not belong to any port group (see *Failover Considerations* for details)

Refer to the *Getting Started Guide* > *Deploying Network VirusWall* > *Deploying Network VirusWall Based on an Operation Mode* section for additional information.

Failover

The failover solution involves two (2) Network VirusWall devices– Active and Standby. It is a backup operation that automatically switches to a standby Network VirusWall device if the active device fails or is temporarily shut down for servicing.

Applying a failover solution requires the completion of the following tasks:

1. Selection between the following Operation Modes:
   - Port Grouping with Failover
   - Port Redundancy with Failover
2. Allocation of the Active Network VirusWall interface based on the Operation Mode
3. Allocation of the Standby Network VirusWall interface based on the Operation Mode
4. Establishment of the failover link between Active and Standby
5. Establishment of Network VirusWall connection to other network devices

Failover Considerations

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

1. Network VirusWall recognizes port 5 as the FAILOVER port.
2. A Network VirusWall failover pair must have identical devices—same model and running the same Network VirusWall program file and boot loader. Otherwise, the failover solution cannot work.
3. Check whether the core and LAN switches connected to the Network VirusWall devices have Spanning Tree Protocol (STP) enabled.
4. If STP is not enabled and there is a Network VirusWall failover pair in the network, Network VirusWall will send heavy UDP traffic broadcasts.
5. Network VirusWall disables failopen (LAN bypass) in a failover environment.
6. 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 disconnects the failover link. See *page 3-5* for instructions on how to update the program file in a failover deployment.

Refer to the *Getting Started Guide > Deploying Network VirusWall > Deploying Network VirusWall Based on an Operation Mode* section for information on how to set a failover Operation Mode.

Failopen

The failopen or LAN bypass solution involves one Network VirusWall device. Failopen is a fault-tolerance solution that allows the Network VirusWall device to continue to pass traffic in an event when a software or hardware failure occurs within the device.

Applying a failover solution requires the completion of the following tasks:

- Selection between the following Operation Mode:
  - Port grouping
  - Port redundancy
- Allocation of the Network VirusWall interface based on the Operation Mode selection
- Establishment of Network VirusWall connection to other network devices

Failopen Considerations

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

1. Network VirusWall reserves ports 1 and 2 for failopen.

   If the switches that your network uses do not support auto MDI/MDI-X, use a crossover and non-crossover combination for Ports 1 and 2. This configuration will enable failopen to work. Otherwise, invalid cable type combination prevents Network VirusWall from using failopen and can result in a network issue. Refer to the device documentation to determine whether your L2 switches support auto MDI/MDI-X.

2. 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.
3. The network cable connecting Network VirusWall and other devices must not be longer than 100 meters (328 feet).
4. If you have a failover-based Operation Mode, Network VirusWall automatically disables failopen.
5. Resetting a Network VirusWall device with failopen enabled temporarily blocks the network connection.
6. Failopen does not work when the speed of the EXT connection and the INT connection are different. Enable auto-negotiation for the devices connected to the Ethernet cables.

Table 1-6 describes the behavior of failopen ports (ports 1 and 2) during a device reset.

Note: The thirty-second (30s) delay occurs only when resetting the device. Powering on or off the device does not cause this delay.

TIME (SECONDS)	PROCESS	PORTS 1 AND 2 STATUS (FAILOPEN ENABLED)	PORTS 1 AND 2 STATUS (FAILOPEN DISABLED)
30	BIOS Power-On Self Test (POST)	Disconnected	Disconnected
60	Loading GRand Unified Bootloader (GRUB)	Connected	Disconnected
	Rescue Mode	Connected	Disconnected
	Validating the boot partition flag	Connected	Disconnected
	Validating the system configuration file	Connected	Disconnected
	Booting Network VirusWall	Connected	Disconnected
10	Disabling failopen	Disconnected	Disconnected
n/a	Preconfiguring Network VirusWall	Connected	Connected

TABLE 1-6. Ports 1 and 2 status when resetting a device

Refer to the *Getting Started Guide > Deploying Network VirusWall > Deploying Network VirusWall Based on an Operation Mode* section for information on how to set a failopen Operation Mode.

Operation Mode

Network VirusWall 2500 introduces Operation Mode. Operation Mode is a preconfiguration option accessible from the Preconfiguration console. It allows you to configure the failopen, failover, and port redundancy settings.

You can set one of the following Operation Modes per device:

- **Port Grouping**—involves one external port and four internal ports
- **Port Grouping with Failover**—involves one external port, three internal ports, and one failover port
- **Port Redundancy**—involves two pairs of one internal and one external port
- **Port Redundancy with Failover**—involves two pairs of one external, one internal port, and one failover port

Refer to the following topics in the Network VirusWall 2500 *Getting Started Guide* for details on how to allocate the Network VirusWall interface and set the Operation Mode:

- *Allocating Ports Based on the Operation Mode Setup*
- *Deploying Network VirusWall Based on the Operation Mode*
- *Setting the Operation Mode*

Chapter 2

Configuring Scan, System, and Device Settings

This chapter describes the management tools that you can use to take advantage of Network VirusWall 2500 virus-scanning capabilities, which include scan options, Network Outbreak Monitor, enforcement policies, system settings, and system tasks.

Network VirusWall provides three management tools that let you easily configure its settings. See Table 1-1, “Comparison of the Network VirusWall management tools,” on page 1-11 to understand the configuration options allowable from the available management tools.

The topics discussed in this chapter include:

Getting Started with Network VirusWall

Trend Micro recommends performing the following tasks after preconfiguring a Network VirusWall device and testing a successful deployment:

- Access and check Network VirusWall devices via the Trend Micro Control Manager management console (see *page 2-2*)
- Update components (see *page 3-1*)
- Modify the Preconfiguration console accounts (see *page 2-36*)
- View Operation Mode and VLAN settings (see *page 4-2*)

Tip: Refer to the *Getting Started Guide* for details on how to preconfigure and test a successful Network VirusWall deployment.

Accessing Network VirusWall Devices

The Trend Micro Control Manager management console is a Web-based console published on the Internet 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.

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

To access Network VirusWall devices:

1. Open the Control Manager management console.
2. In the main menu, click **Products**.

   On the navigation menu, the Product Directory appears. The Product Directory lists all the managed products, which the Control Manager server manages.

   Tip: The host name of each registered Network VirusWall device appears next to the  icon.

3. Perform one of the following:
   - Click **Root folder** > **New entity** > *Network VirusWall host name* to administer a newly registered device
   - Click **Root folder** > *specific Network VirusWall folder* containing a group of managed devices with the same model (for example, **Network VirusWall 2500**) to manage a group of managed products

     Note: Control Manager provides limited options when configuring a group of devices. See *page 2-4* for details.

   - Click **Root folder** > *specific Network VirusWall folder* > *Network VirusWall host name* to administer a previously registered device

FIGURE 2-1. Accessing Network VirusWall devices, individually or grouped

When accessing a single device, the Product Status showing the **System Information** table appears. Alternatively, accessing a group of devices through a **Product Directory** folder, the Product Status screen showing the Status Summary for the last seven (7) days appears. Administer the device(s) using the **Product Status**, **Configuration**, **Tasks**, and **Logs** tabs.

Understanding the Network VirusWall Status

Control Manager has a status verification mechanism to update the operating status of products on the network. The Control Manager agent on Network VirusWall

periodically sends a notification message, known as a heartbeat, to the Control Manager server. If the Control Manager server does not receive a heartbeat after the maximum heartbeat delay time (180 minutes by default), it verifies the connection by sending a heartbeat request to the Network VirusWall. If Control Manager still does not receive a heartbeat, then it changes the Network VirusWall connection status from **active** to **abnormal**.

The following Network VirusWall status icons can appear on the navigation menu of the Control Manager management console:

- — active (functioning properly)
- — abnormal (turned off, disconnected from network or is no longer recognized by Control Manager)

Configuring a Group of Devices

Access a group of similar Network VirusWall device models (for example, groups of Network VirusWall 2500 devices) using the Product Directory grouping. To access a group of devices, see Step 3 on *page 2-3*.

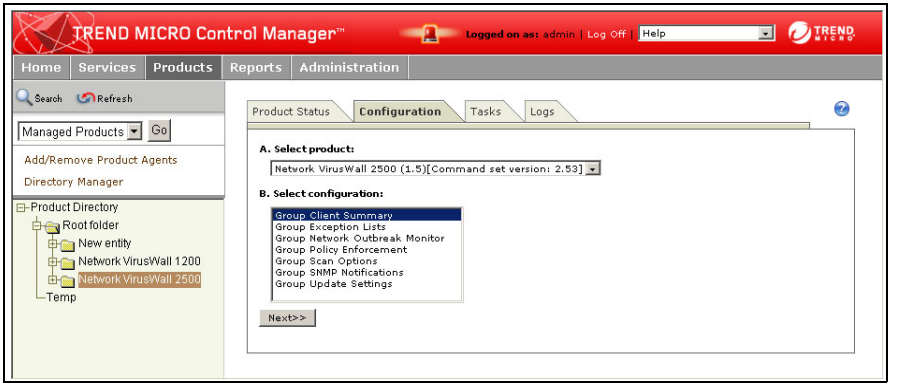


FIGURE 2-2. Accessing and configuring a group of Network VirusWall devices

Control Manager allows you to configure a group of devices with the following options:

- View the Client Summary
- Enable and add client IP addresses in the Exception Lists

- Enable and configure Network Outbreak Monitor
- Enable and configure Policy Enforcement
- Enable and configure Scan Options
- Enable and configure SNMP notifications
- Enable a scheduled update and configure the update source settings

As for the rest of the options available from the **Configuration** tab > **Select configuration** list, these are applicable per Network VirusWall device. That is, group configuration is not possible.

Note: The instructions in this documentation assume that you are configuring a single Network VirusWall device. Access a Network VirusWall Product Directory folder (see Step 3 on *page 2-3*), and then follow the instructions provided to configure a group of devices.

Replicating Configuration Settings

If you have more than one Network VirusWall 2500 device on your network and want them to have the same settings, it is not necessary to configure them separately. Configure one device and replicate the settings onto other Network VirusWall 2500 devices.

To replicate Network VirusWall 2500 settings:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Tasks** tab.
3. Under **Select task**, select **Configuration Replication**.
4. Click **Network VirusWall 2500** under **Supported products**.

   Note: The Control Manager server on your network may be managing products other than Network VirusWall 2500.

5. Click **Next>>**.
6. In the Product Directory, select the Network VirusWall device to receive the configuration settings.

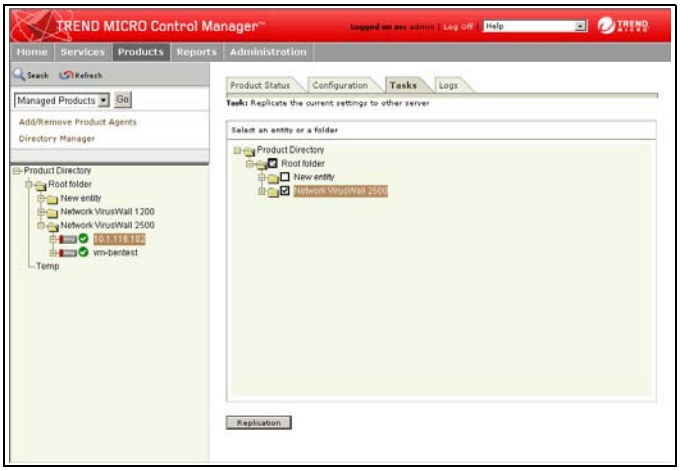


FIGURE 2-3. Replicating Network VirusWall configuration

7. Click **Replication**.

Tip: Alternatively, access a group of Network VirusWall devices and perform a group configuration. See *page 2-4* for details.

In addition, refer to the *Control Manager Online Help* > *Understanding Directory Manager* to plan how you will customize the Product Directory organization to suit your administration model needs.

Configuring Scan Settings and Policies

This section includes the following topics:

Configuring Real-time Scan Options

Use the **Scan Options** screen to enable the scanning of network traffic in real-time, select an action to take on infected packets and clients, and enable Damage Cleanup Services. See the *Control Manager Getting Started Guide* for more information on Damage Cleanup Services.

Enabling Real-time Network Virus Scan

Enable Real-time network virus scan to have Network VirusWall scan all network traffic at the packet level.

To enable Real-time network virus scan and choose a scan action:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Scan Options**.
4. Click **Next>>**. The Scan Options screen appears.

FIGURE 2-4. The Real-time Scan Options screen

5. Select the **Enable Real-time Network Virus Scan** check box to have Network VirusWall 2500 scan all network traffic passing through it.
6. Under **Scan Action**, select an action to take on infected packets:
   - **Drop infected packet:** click to prevent Network VirusWall 2500 from forwarding any packets it finds containing malicious code (selected by default)
   - **Pass infected packet:** click to allow Network VirusWall 2500 to forward all packets, even if they contain malicious code
   - **Drop infected packet and Quarantine infected machine:** click to prevent Network VirusWall 2500 from forwarding any packets, and quarantine the client from where the infected packet originated. Network VirusWall 2500 disallows all traffic to and from a quarantined client.

Tip: For maximum security, select **Drop infected packet and Quarantine infected machine**. This will reduce the chances of spreading a network virus and allow you to immediately isolate and treat any infected machines.

---

7. Click **Save**.

Note: Network VirusWall quarantines a maximum of 4096 clients and drops all network traffic from additional clients (over 4096) whose packets are infected.

Enabling Damage Cleanup Services

Use the Scan Options screen to enable Damage Cleanup Services (DCS). Enabling DCS from this screen instructs Network VirusWall to notify Trend Micro Control Manager (TMCM) to start DCS when TMCM detects an infected packet.

To enable Damage Cleanup Services:

1. On the **Scan Options** screen, select the **Enable Damage Cleanup Services** check box.
2. Click **Save**.

Note: You must activate Damage Cleanup Services on your Control Manager server before you can use DCS. See the *Control Manager Getting Started Guide* for information on installing and configuring Damage Cleanup Services.

To configure a list of safe sites that Network VirusWall allows quarantined clients to access, click the **Exception Lists** link under **Exceptions**. See *page 2-22* for more information.

Automating the Removal of Infected Clients from Quarantine

Network VirusWall can automatically remove infected clients from quarantine. To do this, add the client to the Control Manager server with the **Account Manager Tool** (see the *Control Manager Getting Started Guide* and online help for more information).

If you do not add the client to the Control Manager server with the **Account Management Tool**, the only way to remove infected clients from quarantine is on the **Virus Infections Summary** screen (see *page 4-16* for more information).

Enabling Network Outbreak Monitor

A high number of simultaneous network sessions or connections on certain client ports are often a signal of an attack or virus infection. Use Network Outbreak Monitor to trigger an outbreak alert notification message.

To enable and configure Network Outbreak Monitor:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Network Outbreak Monitor**.
4. Click **Next>>**. The Network Outbreak Monitor screen appears.

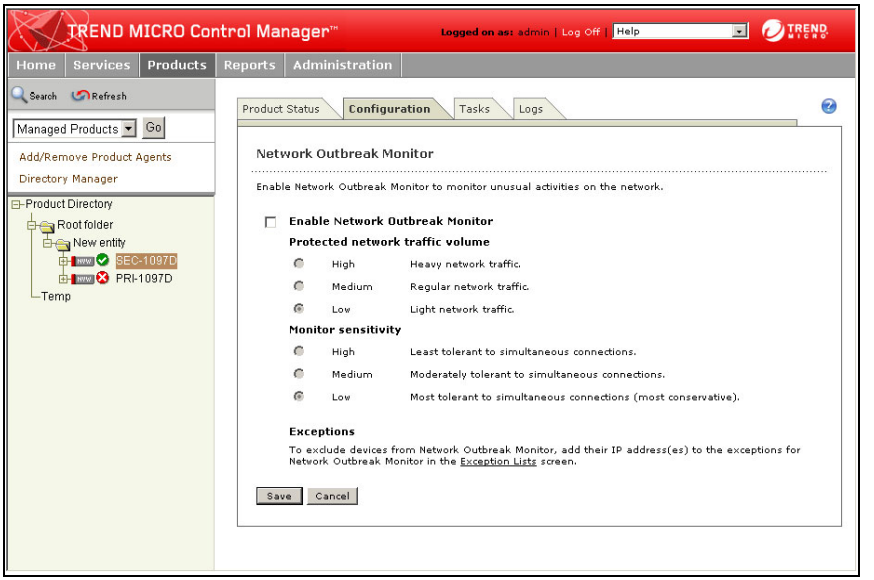


FIGURE 2-5. The Network Outbreak Monitor screen

5. Select the **Enable Network Outbreak Monitor** check box.
6. Under **Protected network traffic volume**, select a volume that represents the amount of traffic typically generated on your network:

- **High:** Heavy network traffic due to a large number of clients or servers and frequent use of network resources
- **Medium:** A regular amount of network traffic
- **Low:** Light network traffic, due to a small number of clients or infrequent use of network resources (selected by default)

7. Under **Monitor sensitivity**, select a sensitivity level that represents the NVW device's level of tolerance for simultaneous network connections. The following options are available:
   - **High:** click to enable the most sensitive setting. Network VirusWall 2500 checks the network most often and does not tolerate many simultaneous network connections
   - **Medium:** click to enable a moderately sensitive setting. Network VirusWall 2500 only tolerates some simultaneous network connections
   - **Low:** click to enable the least sensitive setting. Network VirusWall 2500 checks the network least often and tolerates many simultaneous network connections (selected by default)

   To exclude devices from Network Outbreak Monitor, click the **Exception Lists** link under **Exceptions**. See *Creating Exception Lists* on page 2-22 for more information.
8. Click **Save**.

Note: Configure Control Manager server to send Network Outbreak Monitor alerts to specified recipients. See the *Control Manager Getting Started Guide* for more information.

Configuring Policy Enforcement Settings

Enable Network VirusWall Policy Enforcement to assess the status of client antivirus installations and client vulnerabilities. Based on this assessment, configure settings to pass, block, or redirect different types of client traffic.

WARNING! *For network environments using Network Address Translation (NAT), with a NAT device between Control Manager (TMCM) and a Network VirusWall device, Trend Micro recommends that you disable scheduled Vulnerability Assessments from within TMCM (from the Services page). When used with a NAT device, this service could allow traffic to flow to a vulnerable client.*

To enable and configure Network VirusWall Policy Enforcement:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Policy Enforcement**.
4. Click **Next>>**. The Network VirusWall Policy Enforcement screen appears.

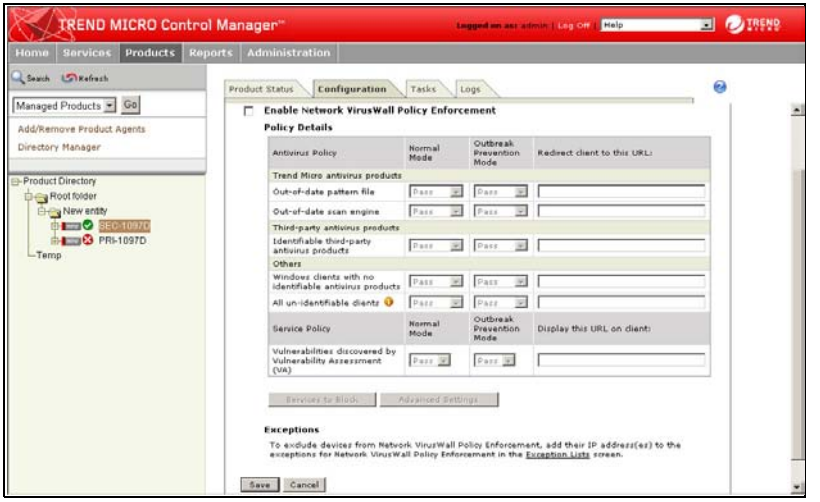


FIGURE 2-6. The Network VirusWall Policy Enforcement screen

5. Select the **Enable Network VirusWall Policy Enforcement** check box.
6. Under **Policy Details**, select actions to take when Network VirusWall 2500 discovers clients with the following:
   - **Trend Micro antivirus products**– includes the following component status:
     - **Out-of-date pattern file**
     - **Out-of-date scan engine**
   - **Identifiable third-party products**– includes the following:
     - **McAfee™ VirusScan™ with Orchestrator agent**
     - **Norton Antivirus™ Corporate Edition™**
   - **Windows clients with no identifiable antivirus products**
   - **All unidentifiable clients**—this includes the following:
     - Computers with non-Windows operating systems, such as Unix™ and Linux™, regardless of antivirus protection
     - Other operating systems without antivirus installations
     - Computers that are behind a firewall and are invisible

   Choose from these actions to take on clients whose antivirus installations match the above criteria:
   - **Block**—block specified traffic (to specify which types of traffic to block, select ports associated with TCP and UDP services. See *Configuring TCP and UDP Services To Block* on page 2-14 for more information)
   - **Pass**—allow all traffic
   - **Redirect—**redirect clients to another Web site when they make an HTTP request

   Choose actions to take when Network VirusWall 2500 is not in outbreak prevention mode (normal mode) and when it is in outbreak prevention mode.
7. Select actions to take when Trend Micro Vulnerability Assessment (VA) discovers vulnerability:
   - **Block**—block specified traffic (to specify which types of traffic to block, select ports associated with TCP and UDP services. See *Configuring TCP and UDP Services To Block* on page 2-14 for more information)

     If you select **Block**, the option exists to redirect clients to another URL. Type the URL in the text box under **Display this URL on client**.

- **Pass**—allow all traffic

Choose actions to take when Network VirusWall 2500 is not in outbreak prevention mode (normal mode) and when it is in outbreak prevention mode.

Note: By default, Network VirusWall Policy Enforcement is off. See the *Control Manager Getting Started Guide* for detailed information on Vulnerability Assessment.

To exempt specified clients from Network VirusWall Policy Enforcement, click the **Exception Lists** link under **Exceptions**. See *Creating Exception Lists* on page 2-22 for more information.

8. Click **Save**.

   To block ports associated with certain services, click **Services to Block**. See *Configuring TCP and UDP Services To Block* on page 2-14 for more information.

   To configure advanced settings, which include client assessment frequency and policy tolerance, click **Advanced Settings**. See *Configuring Advanced Settings* on page 2-16 for more information.

Configuring TCP and UDP Services To Block

When clients meet the antivirus Policy Enforcement criteria you specified on the Policy Enforcement screen and the action is set to **Block**, Network VirusWall 2500 can block TCP and UDP traffic destined for ports that you specify.

To block TCP and UDP service ports:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Policy Enforcement**.
4. Click **Next>>**. The Network VirusWall Policy Enforcement screen appears.
5. Ensure that **Enable Network VirusWall Policy Enforcement** is on and click **Services to Block**. The Block TCP and UDP Services screen appears.

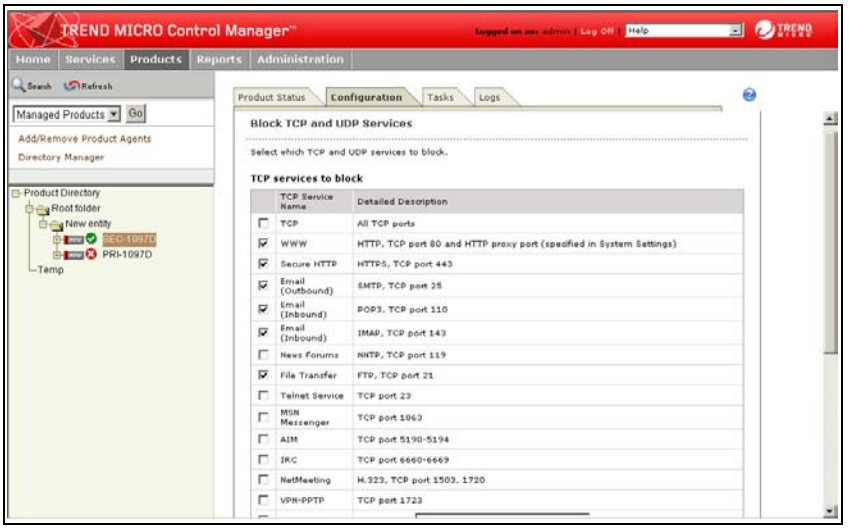


FIGURE 2-7. The Block TCP and UDP Services screen

6. Select ports to block that are associated with TCP and UDP services.
7. Click **Save**. The **Network VirusWall Policy Enforcement** screen displays.
8. Click **Save**.

The following services are selected by default:

- **WWW:** all http traffic
- **Secure HTTP:** all https traffic using Secure Socket Layer (SSL)
- **Email (Outbound):** all email sent from the client
- **Email (Inbound):** all email addressed to the client using the POP3 protocol
- **Email (Inbound):** all email addressed to the client using the IMAP protocol
- **File Transfer:** all File Transfer Protocol (FTP) traffic

Tip: Trend Micro recommends blocking the default-selected services at minimum. Most client traffic uses these services. Blocking them will help ensure that virus infections do not spread to/from vulnerable or infected clients.

Configuring Advanced Settings

Set assessment intervals and policy tolerance on the policy enforcement **Advanced Settings** screen. In addition, specify which ports identifiable antivirus software installations are using on your clients.

To configure advanced settings:

1. Access a managed Network VirusWall product (see *Accessing Network VirusWall Devices* on page 2-2).
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Policy Enforcement**.
4. Click **Next>>**. The Network VirusWall Policy Enforcement screen appears.
5. Ensure the **Network VirusWall Policy Enforcement** check box is enabled, and then click **Advanced settings**. The **Advanced Settings** screen appears.

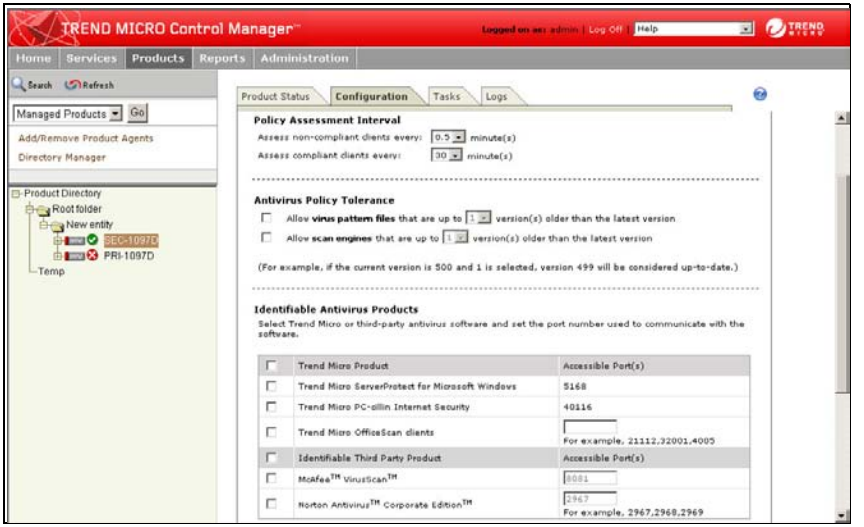


FIGURE 2-8. The Advanced Settings screen

6. Under **Policy Assessment Interval**, select a frequency to assess both clients that are compliant with the policy and clients that are not. Network VirusWall 2500

determines each client's compliance every time it performs a policy assessment. The first time Network VirusWall 2500 performs an assessment, it considers all clients as compliant.

Tip: Trend Micro recommends the default settings of **0.5** minutes for **noncompliant clients** and **30** minutes for **compliant clients**. These settings help ensure that Network VirusWall checks noncompliant clients as often as possible but does not use excessive network bandwidth checking compliant clients.

---

7. There may be occasions when you want to allow clients to have virus pattern files and scan engines that are one or more versions out-of-date. Network VirusWall 2500 gives you the option of taking action on clients only when the versions of their virus pattern files and/or scan engines are out-of-date by more than one version number.

   To do this, select the check boxes under **Antivirus Policy Tolerance** and specify the number of old versions to allow.

Note: Network VirusWall recognizes a total of four scan engine versions and eight versions of virus pattern files. After a scan engine update, Network VirusWall treats a new scan engine as the up-to-date version and treats the replaced version as one version out-of-date, and so on. Similarly, after a virus pattern file update, NVW replaces the eight out-of-date versions with the most recent eight versions and treats the most recent version as the up-to-date version. See *Deploying Network VirusWall Components* on page 3-16 to view the version numbers of the current scan engine and virus pattern file.

---

8. To carry out the enforcement actions specified when Network VirusWall 2500 identifies Trend Micro or third-party antivirus installations, it is necessary to enter the port number(s) these installations use under **Identifiable Antivirus Products**. Network VirusWall 2500 can identify the following antivirus installations:
   - Trend Micro™ ServerProtect™ for Microsoft™ Windows™
   - Trend Micro OfficeScan clients
   - Trend Micro PC-cillin Internet Security
   - McAfee™ VirusScan™ with Orchestrator agent
   - Norton Antivirus™ Corporate Edition™

WARNING! *Network VirusWall cannot detect antivirus installations other than those listed above. Network VirusWall will not enforce a policy on clients with other antivirus installations.*

If any of these installations are on your network, do the following:

a. Type the port number(s) they use under **Accessible port(s)**.

b. From the list next to **Antivirus software detection timeout**, select the number of seconds after which Network VirusWall 2500 will stop scanning the specified port(s) for antivirus installations.

9. To block all clients when Network VirusWall is unable to retrieve Vulnerability Assessment information from Control Manager, select the checkbox under **Blocking Policy for Vulnerability Assessment Timeout**.

10. To display the Detection page while Policy Enforcement analyzes a client accessing a public network resource via HTTP, select the **Blocking Pending Clients** option.

11. Click **Save**. The **Network VirusWall Policy Enforcement** screen displays.

12. Click **Save**.

Enabling or Disabling the Policy Enforcement Detection Page

Use the Blocking Pending Clients option to enable or disable the Policy Enforcement Detection page.

Enabling the Blocking Pending Clients option notifies pending clients of the Network VirusWall's detection tasks. In doing so, clients will experience a delay in accessing an HTTP resource for a maximum of 45 seconds while Network VirusWall searches for possible violations of antivirus and vulnerability-elimination policies. On the other hand, displaying the Detection page informs the client of this process and helps educate the user about keeping his or her machine compliant with the network policies.

Disabling the Blocking Pending Clients option prevents the display of the Detection page. Network VirusWall allows pending clients to access the public network resource while it is searching for policy violations. During this time, pending clients

can access and use the public network resource normally. However, when Network VirusWall detects a policy violation, it takes the set Policy Enforcement action.

Use the Policy Enforcement Advanced Settings screen to enable or disable display of the Policy Enforcement Detection page.

See *Pending Clients* on page 1-24 for details about the Detection page.

To display the Policy Enforcement Detection page:

1. Access the Policy Enforcement Advanced Settings screen (see *Configuring Advanced Settings* on page 2-16).
2. Select the option under **Blocking Policy for Pending Clients**.

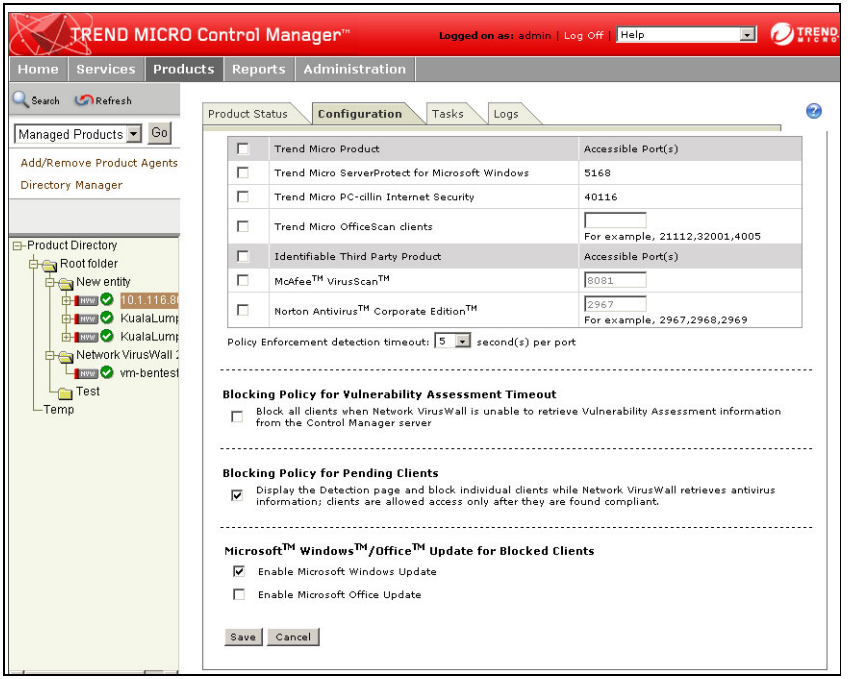


FIGURE 2-9. Blocking Policy for Pending Clients

Note: Network VirusWall displays HTTP messages if the administrator has selected the **HTTP Messages** option on the System Settings screen (see *page 2-29*).

Windows/Office Update for Blocked Clients

A possible reason for blocking a client machine is that the machine lacks the most recent Microsoft Windows™ update or Microsoft Office™ update. Through the Policy Enforcement Advanced Settings screen, you can set Network VirusWall to give a blocked machine access to these update resources.

To enable Windows/Office update for blocked clients:

1. Access the Policy Enforcement Advanced Settings screen. (See *Configuring Advanced Settings* on page 2-16.)
2. In the Windows/Office Update for Blocked Clients section, near the bottom of the screen, select **Enable Windows Update**, **Enable Office Update**, or both.
3. Click **Save** to save these settings.

Note: 1) If a client that is blocked by VA policy is still presented with a blocking page and is unable to access the Windows Update component, you may need to set the gateway IP in the System Settings screen of the Control Manager console for NVW (see *Configuring System Settings* on page 2-27).

2) A blocked client can access the Windows/Office Update site only if it has violated a Vulnerability Assessment policy. If the client is blocked because of an antivirus policy, it cannot access the Windows/Office Update site (or any other site).

Allowing Policy Enforcement to Detect PC-cillin 11.35 Clients

Enable Trend Micro Discover Protocol (TMDP) to allow Policy Enforcement to detect PC-cillin 11.35.

Tip: PC-cillin 12 enables TMDP by default. Therefore, Policy Enforcement can detect clients with PC-cillin 12 installed.

To allow PC-cillin 11.35 clients detection by enabling TMDP:

1. On the PC-cillin client, stop all PC-cillin services.

   Tip: Use PCCTool.exe to stop the PC-cillin services (see *page 2-21*). Refer to the PC-cillin documentation for more details on how to stop and restart its services.

2. Open the registry, and then add the following key and value:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillin\TMSS\EnableAgent=1 (REG_DWORD)
   ```

   WARNING! *Before editing the registry, make sure you understand how to restore it if a problem occurs. For more information, view the **Restoring the Registry** Help topic in regedit.exe or **Restoring a Registry Key** Help topic in regedt32.exe.*

   Making incorrect changes to your registry can cause serious system problems. Always make a back up copy before making any registry changes.

3. Restart PC-cillin services by performing any of the following tasks:
   - Reboot the PC-cillin client
   - Run `PCCTool.exe` to restart all services

   To run `PCCTool.exe`:

   a. Using Windows Explorer, double-click PCCTool.exe, which is available at `<root>:\Program Files\Trend Micro\Internet Security`.

   b. Click **Quit All Modules**, and then click **Start All Modules**.

4. From the PC-cillin main console, access the Personal Firewall configuration window and check whether it lists UDP port 40116. Otherwise, add the UDP port 40116 to allow Policy Enforcement to detect PC-cillin 11.35 clients.

Note: If you have installed PC-cillin 11.35 for the first time, the UDP port 40116 is already included in the Personal Firewall configuration window. Otherwise, manually add the rule if you update from an earlier version.

Network VirusWall should be able to detect PC-cillin 11.35 once you have enabled TMDP.

Creating Exception Lists

Under certain circumstances, you may need to exempt clients from Network VirusWall Policy Enforcement, or from the Network Outbreak Monitor. You may also need to add certain computers or servers to a safe site list that remains accessible to all blocked and quarantined clients.

To enable and configure exception lists:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Exception and Safe Site Lists**.
4. Click **Next>>**. The **Exception Lists** screen displays the following exception lists:
   - **Enable Exceptions for Network VirusWall Policy Enforcement:** configure a list of computers exempted from Policy Enforcement (see *Configuring Policy Enforcement Settings* on page 2-12 for more information)
   - **Enable safe sites for blocked and quarantined clients:** configure the safe site list that quarantined and blocked clients can access
   - **Enable Exceptions for Network Outbreak Monitor:** configure a list of computers exempted from Network Outbreak Monitor (see *Configuring Policy Enforcement Settings* on page 2-12 for more information)

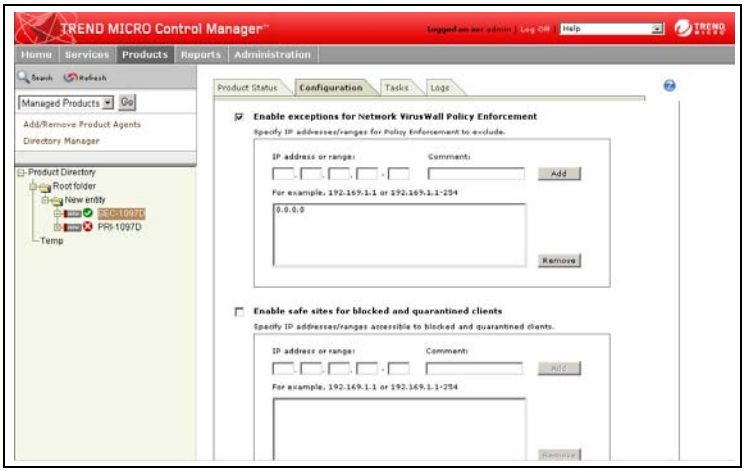


FIGURE 2-10. The Exception Lists screen

5. Enable any of the exception lists by selecting the check box at the top of the list.
6. Add a class C client IP address or a range of IP addresses under **IP address or range**.
7. Click **Add**.

   To remove addresses from the list, click them in the list and click **Remove**. Use the `CTRL` or `SHIFT` keys to make multiple selections.
8. Click **Save**.

Network VirusWall implements the exception lists.

Note: Network VirusWall ignores the last item in the Network Outbreak Monitor exception list if the value is an IP range with comments (for example: `192.193.191.10 - 15 Segment B`). As a workaround, avoid specifying an IP range with comment as the last value in the NOM exception list.

In the safe sites exception list for blocked and quarantined clients, consider adding the following:

- Server components of Trend Micro products (for example, OfficeScan or ServerProtect), which periodically deploy updates to their clients

- Proxy servers that clients use to access the Internet
- DNS servers
- Machines to which Network VirusWall redirects traffic

Note: Network VirusWall automatically allows blocked and quarantined clients to access the Control Manager server. It is not necessary to add the Control Manager server to the safe sites list for blocked and quarantined clients.

Setting a Blocking Policy for Vulnerability Assessment

Network VirusWall advanced settings allows you to block clients when Network VirusWall is unable to retrieve Vulnerability Assessment (VA) information from the Control Manager server.

Seta blocking policy for Vulnerability Assessment through the—

- Control Manager management console > **Policy Enforcement** > **Advanced Settings** option
- Preconfiguration console > **Advanced Settings**

To set a blocking policy for VA through the management console:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab, and then select **Policy Enforcement** from the list.
3. On the bottom of the Policy Enforcement screen, click **Advanced Settings**. The Advanced Settings screen appears.
4. Under the **Blocking Policy for Vulnerability Assessment Timeout** section, select **Block all clients when Network VirusWall is unable to retrieve Vulnerability Assessment information from the Control Manager server**.

FIGURE 2-11. Setting blocking policy for VA

5. Click **Save**.

To set blocking policy for VA through the Preconfiguration console:

1. Type `6` in the **Main Menu** to select **Advanced Settings**. The **Advanced Settings** screen appears. The value of the current blocking policy setting appears under the Advanced Settings summary.
2. Type `1` to change the blocking policy for VA setting.

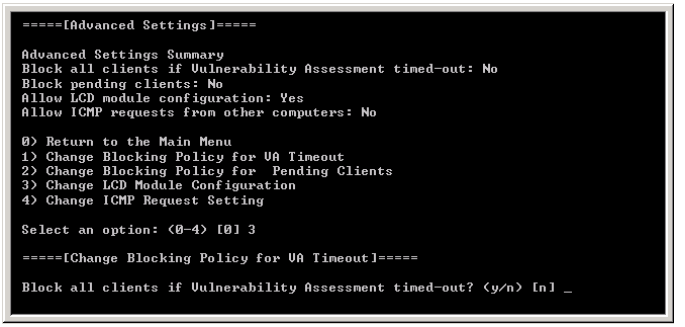


FIGURE 2-12. Setting blocking policy for VA

3. On the option prompt, type `y` to block all clients if VA times-out. Otherwise, type `n` to allow clients even if VA timed-out.

The Advanced Settings summary displays the new setting.

Tip: Blocking clients when VA times out helps ensure that VA prevents vulnerable clients from being the source of infected network packets.

Configuring Device and System Settings

This section includes the following topics:

Configuring System Settings

Network VirusWall 2500 automatically registers to the Control Manager server with the device settings you selected during preconfiguration. Change these settings at any time on the System Settings screen.

To modify system settings:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.

   Under **Select configuration**, click **System Settings.**

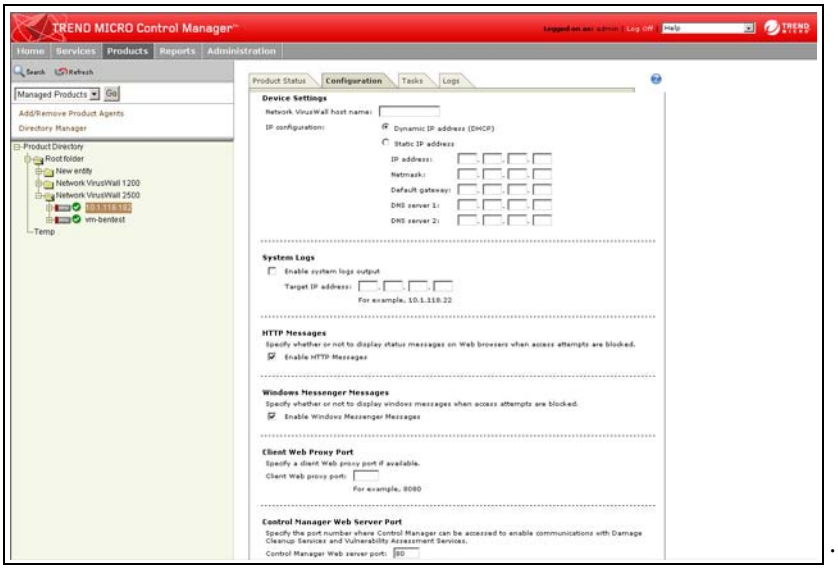


FIGURE 2-13. System Settings screen

3. Click **Next>>**. The **System Settings** screen displays the following options:
   - **Device Settings:** configure Network VirusWall 2500 host name and network settings, including IP address, netmask, gateway address, and DNS server addresses.

     To modify device settings, do the following:

     a. Type a new host name.

     b. Next to **IP configuration**, select the type of IP address for Network VirusWall 2500. If there is a DHCP server on your network and you want it to dynamically assign an IP address to Network VirusWall 2500, select **Dynamic IP address (DHCP)**. Otherwise, select **Static IP address** and type the IP address, netmask, default gateway address, and DNS server addresses.

Note: Users cannot change NAT IP and port number from within Control Manager. You can change NAT settings only from within the Preconfiguration console. (See *Getting Started Guide*, Chapter 5: "Preconfiguring Network VirusWall," Configuring Device Settings, for more information.)

- **System logs**—send the system log to a specified computer

  To enable a system log:

  a. Select the **Enable System Logs output** check box.

  b. Type the IP address of the machine that will receive a system log.

Tip: Use the Network VirusWall 2500 System Log Viewer, a user-friendly, Windows-based application, to view logs. See *Using the Log Viewer* on page 4-26 for more information.

- **HTTP messages**—select the **Enable HTTP messages** check box (selected by default) to enable Web browser messages to display on client machines when NVW blocks access attempts (this applies to quarantined and blocked clients, see *page 2-7*)
- **Windows Messenger Messages**– select the **Enable Windows Messenger Messages** check box (selected by default) to enable Windows-based client machines to display Windows Messenger Service messages

  This type of Network VirusWall client notification makes use of Windows Messenger Service. This feature does not require any Windows messaging server (for example, Windows Messenger Server or Live Communications Server) or instant messaging application (for example, Windows Messenger or MSN Messenger) to send popup notifications.

Tip: Trend Micro recommends keeping the default **Enable HTTP messages** setting. This helps ensure that clients will know why NVW has blocked their machines when attempting to access the Internet. Client host names will not appear on the status messages unless you configure existing DNS server(s) on your network.

- **Client Web Proxy Port**—type the port number the client Web proxy uses for connection to the Internet
- **Control Manager Web Server Port**– to enable communications between Damage Cleanup Services and Vulnerability Assessment through the Control Manager server, type the Web server port the Control Manager server uses for HTTP communication (default is 80)

  This port number must be the same as the Web server port number entered during Control Manager installation. See the *Control Manager Getting Started Guide* for more information.

4. Click **Save**.

Control Manager sends the command to the Network VirusWall device. The Network VirusWall device then performs a quick "network refresh" to apply the modified system settings.

Performing System Tasks

If an emergency arises whereby you want to isolate the Protected Network, you can lock Network VirusWall to block all traffic that would normally pass through the device. Likewise, if you are experiencing problems with Network VirusWall, you can power on the UID LED or perform a reset.

Turning On the UID LED

Use the System Tasks screen to turn on the UID LED. Turning on the UID LED allows you to identify a Network VirusWall device to maintain or troubleshoot. This option is useful especially if you have multiple Network VirusWall devices mounted on a rack wall.

Turn on the UID LED through the:

- Control Manager management console
- UID button on the front panel of the device

To turn on the UID LED through the Control Manager management console.

1. Access a managed Network VirusWall product (see *page 2-2*).
2. On the working area, click the **Configuration** tab.
3. Under Select configuration, select **System Tasks**.

4. Click **Next>>**. The System Tasks screen appears.
5. Under UID LED, select **Turn ON** to turn on the UID LED.

   Select **Turn OFF** to turn off the UID LED.

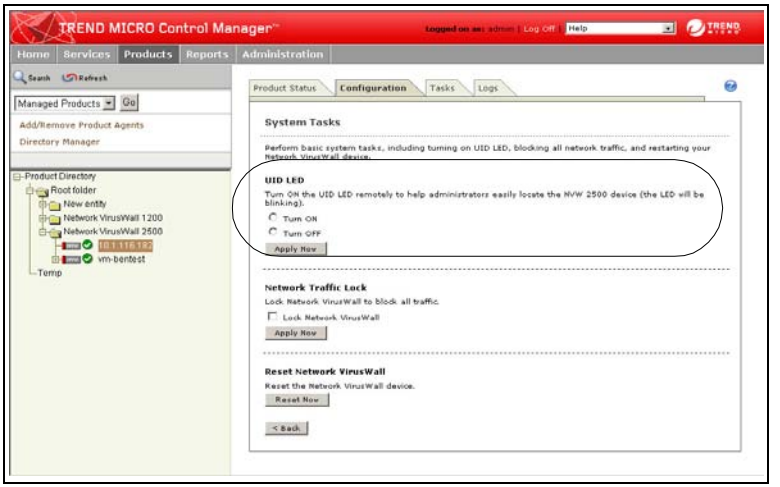


FIGURE 2-14. System Tasks > UID LED option

6. Click **Apply Now**.

The UID LED becomes blue if the UID LED is pressed. See *UID LED and button* on page 2-31.

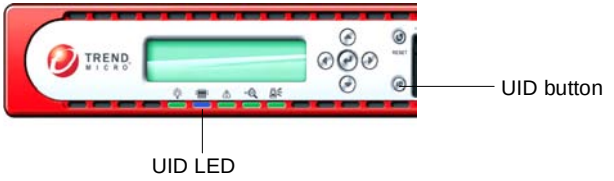


FIGURE 2-15. UID LED and button

To turn on the UID LED through the UID button:

Press the **UID** button on the front panel of the device. The UID LED becomes blue.

Locking Network VirusWall

The **System Tasks** screen allows you to lock Network VirusWall, which performs the same function as physically disconnecting the device from the network. Unlock Network VirusWall later to bring the device back online.

To set the network traffic lock:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **System Tasks**.
4. Click **Next>>**.
5. Select the **Lock Network VirusWall** check box to block all traffic.

   To unblock all traffic, clear the check box.

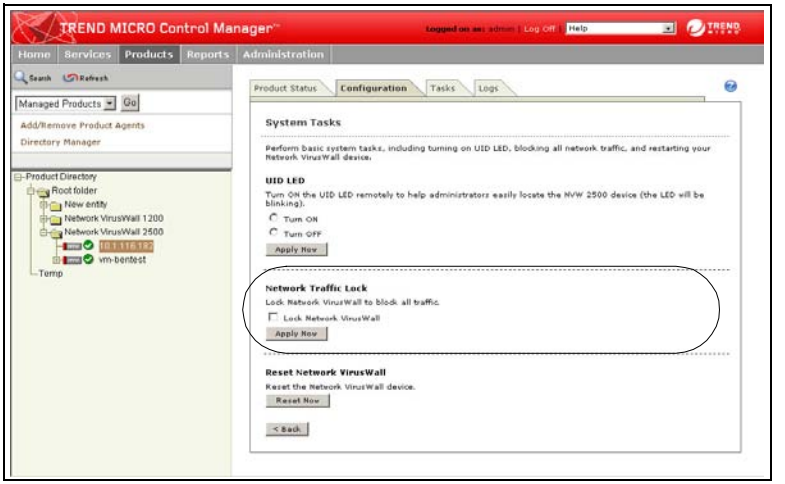


FIGURE 2-16. System Tasks > Network Traffic Lock option

6. Click **Apply Now**.

Take note of the following scenarios:

- If Network VirusWall is powered *off*, failopen is enabled, and network traffic lock is enabled, traffic passes through the failopen ports (ports 1 and 2)

- If Network VirusWall is powered *on*, failopen is enabled, and network traffic lock is enabled, traffic is not allowed to pass through the device

Resetting Network VirusWall

Reset Network VirusWall 2500 if you experience any problems or if the Control Manager management console prompts you to perform a reset.

Reset Network VirusWall through the:

- Preconfiguration console (see *page 2-34*)
- **RESET** button on the front panel of the device (see *page 2-34*)
- Control Manager management console (see *page 2-34*)

Any of the following actions invokes a device reset:

- Manually resetting the device by following one of the procedures listed in *page 2-34*, *page 2-34*, and *page 2-34*
- Importing the configuration file through the Preconfiguration console
- Automatically or manually updating Network VirusWall components through the Control Manager server

If NVW detects any of the above actions and failopen is in use, Network VirusWall temporarily disconnects ports 1 and 2 for approximately thirty seconds (30s). See *Table 1-6* for details.

Note: The thirty-second (30s) delay only occurs when resetting the device. Powering on or off the device does not cause this delay.

To reset Network VirusWall 2500 through the preconfiguration menu:

1. Access the Network VirusWall 2500 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type `8` in the main menu. The System Tasks submenu appears.
3. Type `4` to reset the device. A confirmation screen appears.

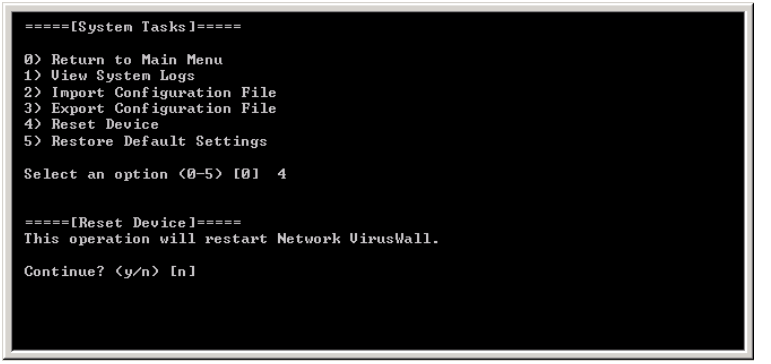


FIGURE 2-17. Resetting Network VirusWall

4. Type `y` to continue.

Note: Refer to the Getting Started for detailed information on using the preconfiguration menu through the Preconfiguration console.

To reset Network VirusWall 2500 with the Reset button:

Press the **Reset** button on the front panel of the device. Network VirusWall 2500 resets.

To reset Network VirusWall 2500 through the Control Manager management console:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **System Tasks**.

4. Click **Next>>.**

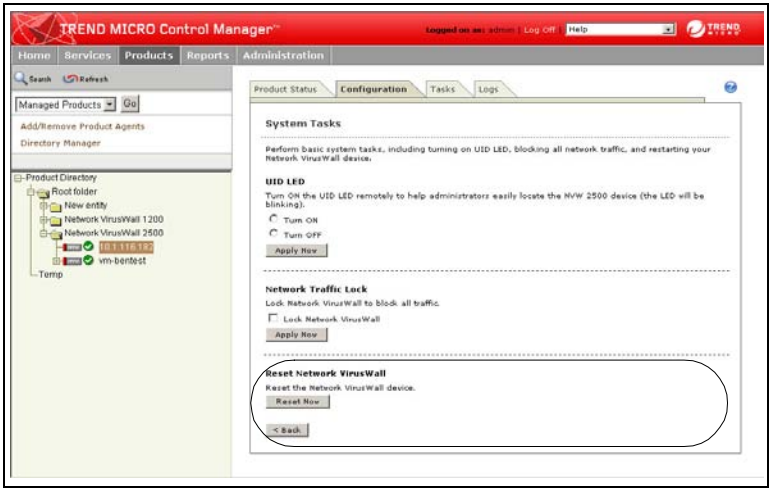


FIGURE 2-18. System Tasks > Reset Network VirusWall option

5. Click **Reset Now**.
6. Confirm the reset when prompted.

Control Manager sends the command to Network VirusWall to perform a system reset.

Modifying the Preconfiguration Console Accounts

The admin and monitor accounts provide different access levels. *Table 2-1* lists the possible access levels for each account:

ACCESS LEVEL	admin	monitor
Preconfigure Network VirusWall	●	
Modify account settings	●	
Log on to the Preconfiguration console of the Active device	●	
Modify settings of the Active device through the Preconfiguration console	●	
Read-only access		●
Log on to the Preconfiguration console of the Standby device		●
Modify settings of the Standby device through the Preconfiguration console	Not possible	Not possible

TABLE 2-1. Access levels for the Preconfiguration console accounts

Trend Micro highly recommends modifying the default passwords for both the admin and monitor accounts. Use the Preconfiguration console to change the user password.

To change the default password:

1. Log on to the Preconfiguration console.

> **Tip:** Refer to the *Getting Started Guide* > *Logging on the Preconfiguration Console* for instructions.

2. Type `7` in the **Main Menu** to select **User Accounts**. The user name and its corresponding permissions appear.

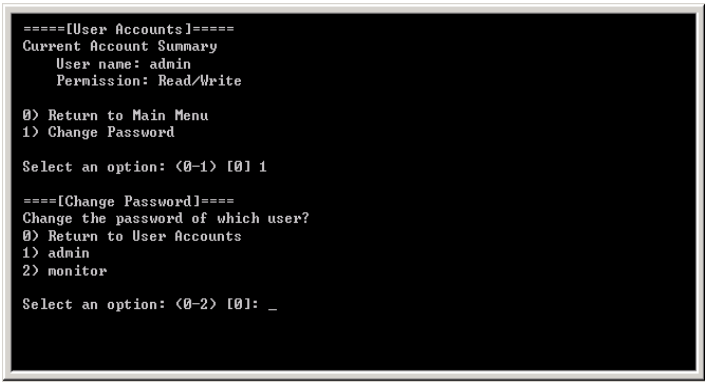


FIGURE 2-19. The User Accounts submenu

3. Type `1` to select **Change Password**.
4. Type the number corresponding to the user password to change.

> **Note:** If you logged on as **monitor**, you can only change the **monitor** password.

5. Type both the current and new passwords. Passwords must be between 5 and 12 alphanumeric characters in length (spaces not allowed).

Use the new password the next time you log on to the Preconfiguration console.

Allowing ICMP Requests

Network VirusWall 2500 has a built-in firewall that protects it from attacks. You can configure Network VirusWall to prevent or allow ICMP packets requests from reaching the device. This setting is configurable via the Preconfiguration console.

To allow ICMP requests to reach a Network VirusWall device.

1. Access the Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type `6` to open the Advanced Settings menu. The Advanced Settings Summary screen displays.
3. Type `4` to toggle the ICMP request setting.

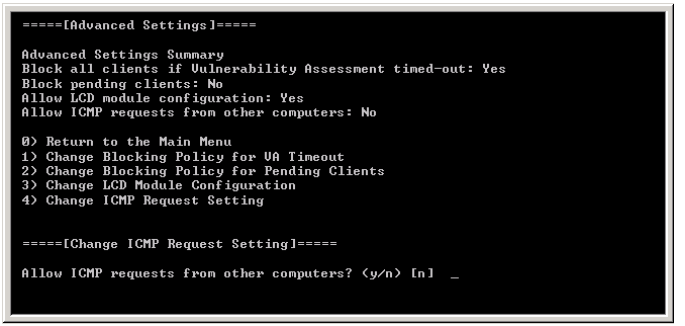


FIGURE 2-20. Allowing ICMP requests

4. Type `y` to allow ICMP requests from reaching a Network VirusWall device. Otherwise, type `n`.

The Advanced Settings Summary screen refreshes and displays the current ICMP request setting.

Importing and Exporting the Configuration File

Use the Preconfiguration console to import and export the Network VirusWall configuration. This allows easy replication of existing Network VirusWall settings from one Network VirusWall 2500 to other devices of the same model and locale settings.

Note: Importing or exporting the Network VirusWall configuration is not possible when using Minicom (available in Linux servers).

To import the configuration file:

1. Access the Network VirusWall 2500 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type `8` in the main menu. The System Tasks submenu appears.
3. Type `2` to import the configuration file. A confirmation screen appears.

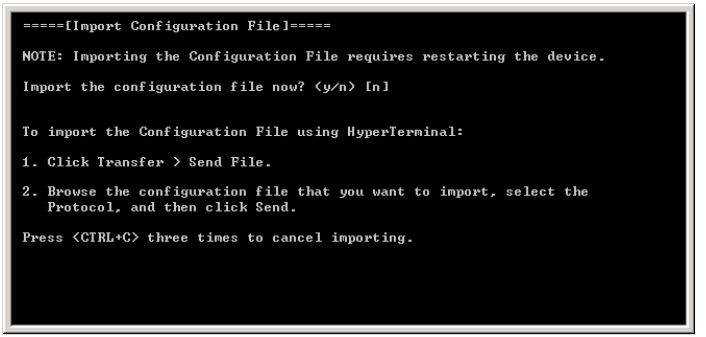


FIGURE 2-21. Importing the Network VirusWall configuration file

4. Type `y` to continue.

Note: Refer to the Getting Started for detailed information on using the preconfiguration menu through the Preconfiguration console.

To export the configuration file:

1. Access the Network VirusWall 2500 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type `8` in the main menu. The System Tasks submenu appears.
3. Type `3` to import the configuration file. A confirmation screen appears.

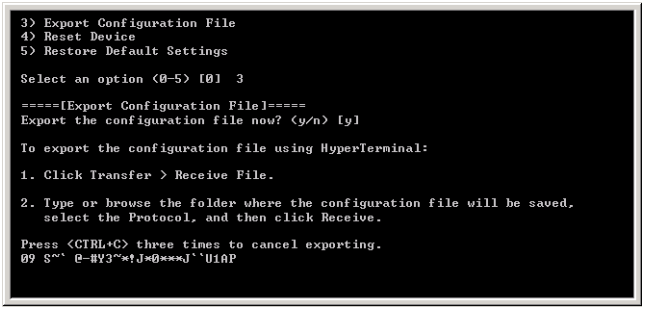


FIGURE 2-22. Exporting the Network VirusWall configuration file

4. Type `y` to continue.

Note: Refer to the Getting Started for detailed information on using the preconfiguration menu through the Preconfiguration console.

Restoring Default Settings

If you experience any issues during preconfiguration, you have the option of initializing Network VirusWall, which restores settings to the factory defaults.

WARNING! *You will lose all changes to preconfiguration settings when you perform initialization.*

To initialize Network VirusWall:

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

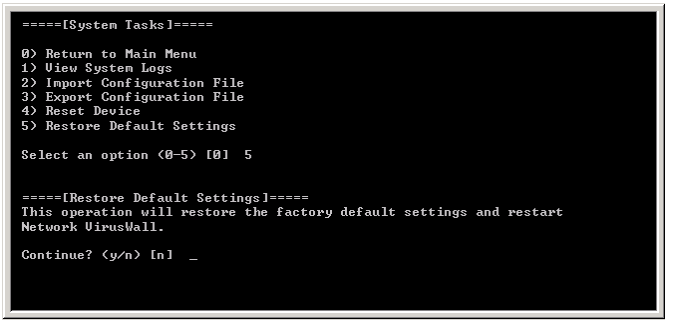


FIGURE 2-23. Restoring the default settings

2. On the System Tasks submenu, type `5` to restore the default settings.

WARNING! *Use care when restoring the default settings. Doing so erases the configurations you have set.*

3. Type `y` to continue.

The Network VirusWall device will reset and restore factory defaults.

Table 2-2 lists the default settings:

SETTING	DEFAULT VALUE
Network VirusWall host name	none
IP address type	Static
IP address	none
Netmask	none
Default gateway	none
Primary DNS server	none
Secondary DNS server	none
Operation Mode	none
Interface speed and duplex mode	Auto

TABLE 2-2. Network VirusWall default settings

Table 2-3 lists the default hardware specifications:

HARDWARE COMPONENT	SPECIFICATION
Memory	2 512MB DDR-II
Processor	2 CPU (Nocona 2.8GHz)
DOM (IDE **D**isk **O**n **M**odule)	1 256MB flash disk
Fans	5 cooling fans

TABLE 2-3. Network VirusWall default hardware specifications

Changing the LCD Module Configuration

LCD Module (LCM) configuration controls the status of the touch panel on the Network VirusWall front bezel. If the touch panel is locked, you can make preconfiguration settings only by using the Preconfiguration console.

To change the LCM Configuration:

1. Type `6` in the **Main Menu** to select **Advanced Settings**.
2. On the Advanced Settings submenu, type 3 to set the toggle the LCD module configuration setting between **ON** and **OFF**.

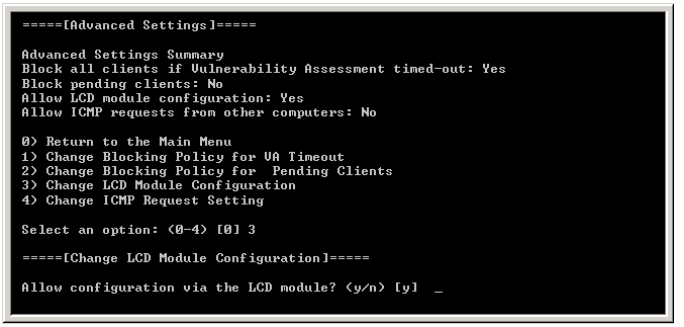


FIGURE 2-24. The Advanced Settings submenu

3. Type `y` to allow configuration via the LCD module. Otherwise, type `n` to lock the LCD module.

The Advanced Settings submenu displays again, showing the new LCM configuration status. Confirm that the status is correct.

Chapter 3

Updating Components

This chapter describes how to access Network VirusWall devices from the Control Manager management console, view system information, deploy Network VirusWall components, and modify device settings.

The topics discussed in this chapter include:

Understanding Updatable Components

Network VirusWall uses the following components to detect, prevent or contain, and eliminate malware outbreaks:

- Network Scan Engine– scans all traffic passing through Network VirusWall at the packet level

  The network scan engine specifically searches for network viruses.

- Network Virus Pattern– contains a regularly updated database of packet-level network virus patterns

  Trend Micro often updates the network virus pattern file to help ensure Network VirusWall can identify any new network viruses.

  Note: Visit http://www.trendmicro.com/download/ to view the latest Network Virus Pattern information.

- Network outbreak rule– contains a regularly updated collection of behavior-based network threat rules
- Program file– the Network VirusWall program, also referred to as the image, which includes the operating system, system programs, and all components necessary to get Network VirusWall functioning properly

  Note: Update the program file manually in a failover deployment. See *page 3-5*.

Depending on the device role in a failover environment, the Active Network VirusWall device always communicates with the Control Manager server for updates, logs, and various configuration commands. The Standby device polls the Active device for the latest components.

Updating Components

Network VirusWall components are software modules that comprise the Network VirusWall operating system. To help ensure up-to-date protection, update the network scan engine, network virus pattern file, network outbreak rule, and program file after connecting to the network or during virus outbreaks.

Network VirusWall provides the following methods to update and deploy the latest components to its managed products and devices:

- Automatically or manually, from the update source

  Either of these methods instructs Network VirusWall to connect directly to the update source, download, and then apply the latest components. Use the **Update Settings** or **Manual Update** option from the **Configuration** tab of the management console to set this type of update.

  Tip: Trend Micro recommends updating components manually after finishing with the Network VirusWall preconfiguration.

- Automatically or manually, from the Control Manager server

  Either of these methods instructs Network VirusWall to wait for updates from the Control Manager server. The Control Manager server connects and downloads the latest components from the update source, and then deploys them to managed Network VirusWall. Use the **Administration** menu from management console to set these types of update.

  Note: Refer to the Control Manager *Online Help* or *Getting Started Guide* for details on how to configure a scheduled or manual download and deployment plan.

  For Network VirusWall failover deployments, refrain from using the Control Manager Deployment Plan to update the Network VirusWall program file. Doing so disconnects the failover link between the Primary and Secondary devices, causing a non-working failover deployment. See *page 3-5* for instructions to update the program file.

Updating Components Manually from the Update Source

After preconfiguring Network VirusWall, download the latest components (Network Virus Pattern, Cleanup templates, Network Virus Engine) to help maintain the highest security protection.

To download the latest components:

1. Click a Network VirusWall device from the navigation menu of the Control Manager management console.
2. In the working area, click the **Configuration** tab, and then select **Manual Update** from the **Select configuration** list.
3. Under **Select components to update**, select the components to update.

Tip: Ensure the **Update Source** is set.
Trend Micro recommends selecting **Network scan engine**, **Network virus pattern file**, and **Network outbreak rule** to download and apply the latest antivirus and vulnerability-elimination components.

---

4. Click **Update Now**.

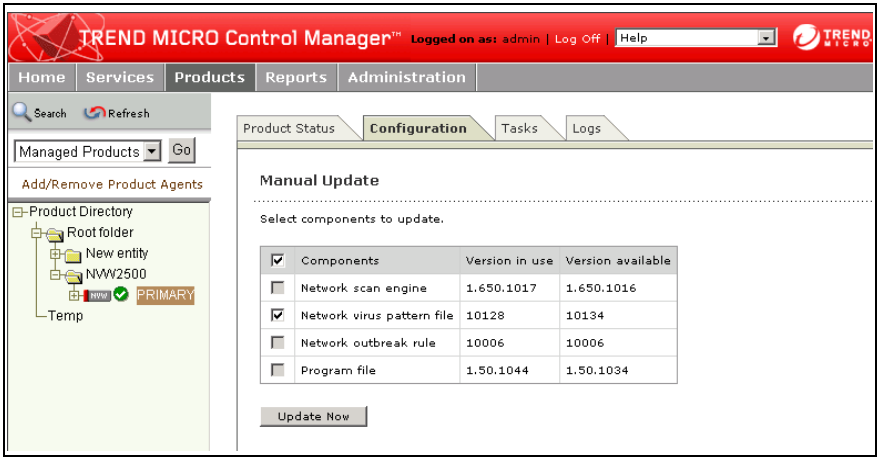


FIGURE 3-1. Updating Network VirusWall components manually

Use the **Logs** tab > **Event Logs** or **Command Tracking** screen to verify whether Control Manager updates the selected components during manual update.

Tip: Visit http://www.trendmicro.com/download/product.asp?productid=45 to view the latest Network Virus Pattern information.

Updating the Program File Manually in a Failover Deployment

Updating the Network VirusWall program file using the Control Manager deployment plan disconnects the failover link between the Primary and Secondary devices. Thus causing a non-working failover deployment.

One of the following conditions occurs if the failover link is disconnected:

- 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.

- Instead of having the Active device as the only managed device registered on the Control Manager management console, two managed product icons appear– Active and Standby

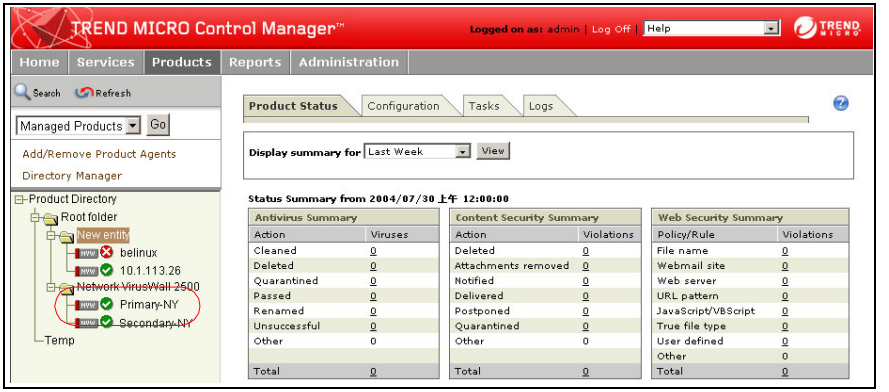


FIGURE 3-2. Both devices in a failover pair register to Control Manager

Perform the following tasks to prevent these conditions from occurring:

- Update the Network VirusWall program file through the **Configuration** tab > **Manual Update** option

  See *page 3-6* for details on how to update the program file of devices in a failover pair.

- If you are implementing automatic or manual Network VirusWall component update from Control Manager server, see *page 3-8*

To manually update the program file in a failover deployment:

Note: The following steps require access to the physical Network VirusWall 2500 Active and Standby devices. Turn on the UID LED to locate the Active device. Position and mount the Active and Standby devices in the same physical location (for example, the Server Room 101 on the 15th floor).

---

1. Access the Active device from the Control Manager management console.
2. Use the **Configuration** tab > **Manual Update** option to check for and manually update the Network VirusWall program file.

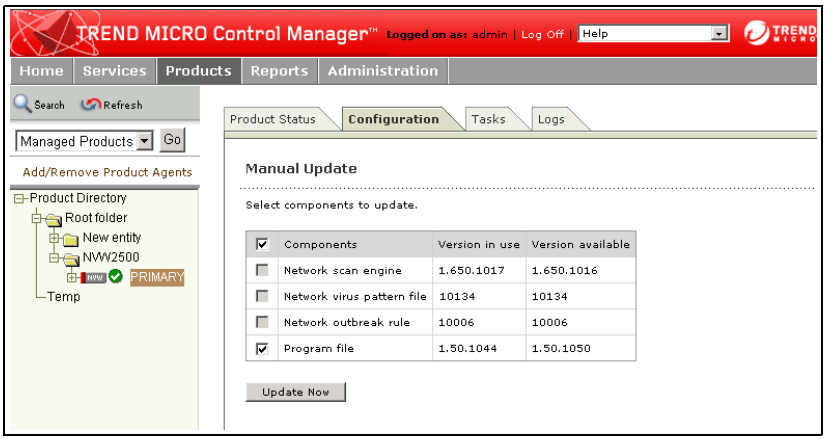


FIGURE 3-3. Manually updating the program file of an Active Network VirusWall 2500 device

3. Wait for the following message to appear on the LCD of the Active device:

   ```
   Booting NVW...
   ```

   As soon as the above message appears on the LCD, power off the Active device. This allows the Standby device to switch to Active. Determine whether the host name displayed on the Control Manager management console is that of the Standby device.
4. Repeat steps 2 and 3 for the newly registered Active device.
5. After updating the program file and Network VirusWall restarts the device, power on the original Active device.

Note: If you enable Switch-back, the Active (original Standby) device will switch to its original failover status and vice-versa. Alternatively, if you enable Non-switch-back, the original Active device will keep its new status (Standby).

Check the failover status after updating the program file:

- Open the management console and check whether the Active device is registered
- Log on to the Preconfiguration console of the Standby device

  You can only log on using the `monitor` account. The `monitor` account allows you to view the current Preconfiguration console settings.

To prevent Control Manager from automatically updating the program file in a failover deployment:

1. Remove the registered Active device from the Deployment Plan in use.

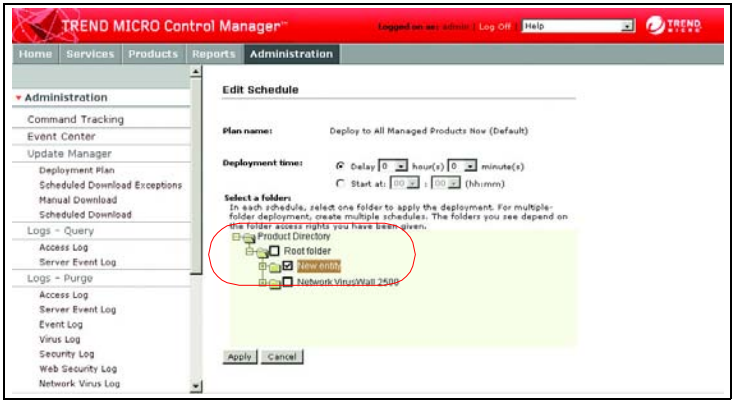


FIGURE 3-4. Excluding Active Network VirusWall 2500 devices from the default Deployment Plan

2. To continue updating the network scan engine and network virus pattern, create a new deployment plan that will deploy updated components to Active Network VirusWall devices.

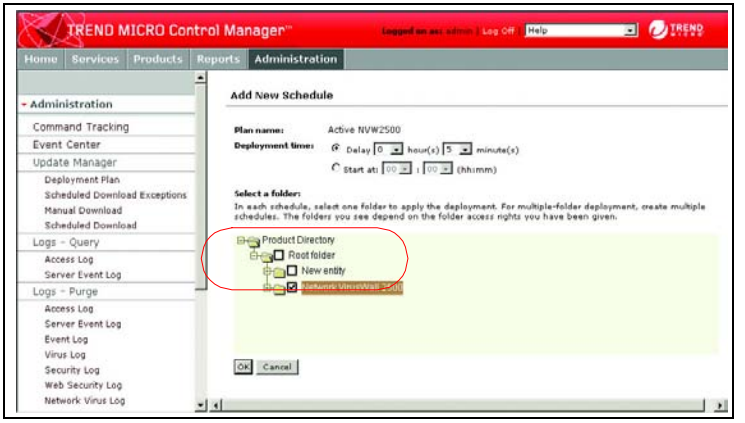


FIGURE 3-5. Creating a new deployment plan for Active Network VirusWall 2500 devices

3. Specify the newly created deployment plan (for example, `Active NVW2500`) in the **Manual Download** or **Scheduled Download** > **Automatic deployment settings** screen.

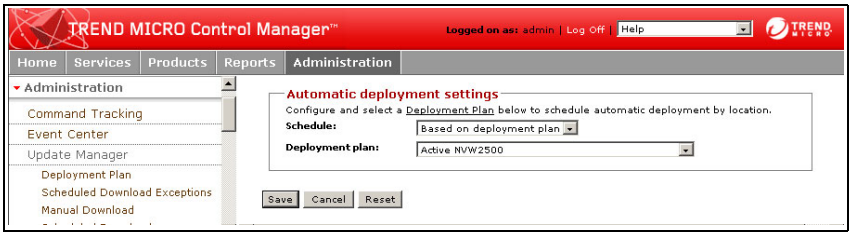


FIGURE 3-6. Setting the network scan engine and network virus pattern deployment plan for Active Network VirusWall 2500 devices

Updating Components Automatically from the Update Source

Set a scheduled update to instruct Network VirusWall to update and obtain the latest components directly from the update source. Use the Update Settings screen to schedule update settings.

To update components automatically

1. Click a Network VirusWall device or groups of Network VirusWall devices from the navigation menu of the Control Manager management console.
2. In the working area, click the **Configuration** tab, and then select **Update Settings** or **Group Update Settings** from the **Select configuration** list.
3. Under **Scheduled Updates** in the Update Settings or Group Update Settings screen, select the **Enable scheduled update** check box.
4. Under **Select update components**, select the components to update.

Tip: Trend Micro recommends selecting **Network virus pattern file** and **Network outbreak rule** as Trend Micro frequently updates these components.

---

5. Under **Configure an update schedule**, specify a schedule to perform the updates.
6. Specify when to perform the scheduled update in the **Start time** lists.
7. Click **Save**.

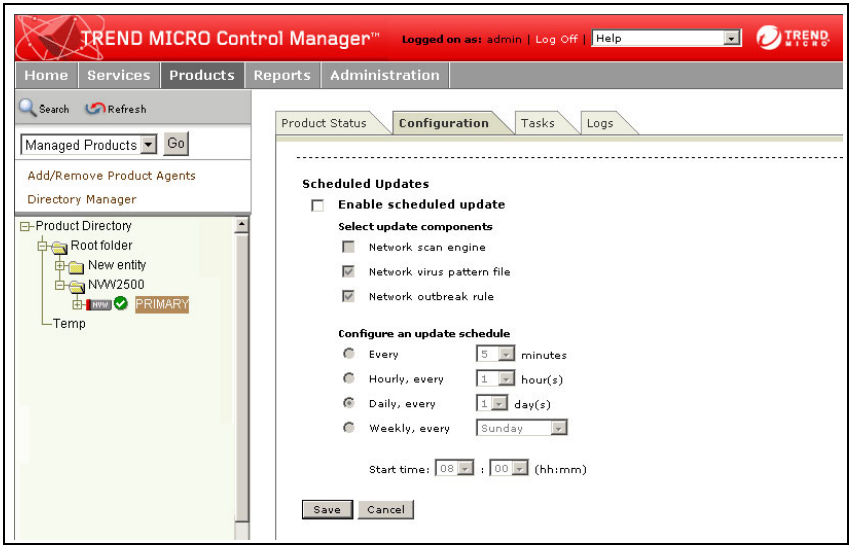


FIGURE 3-7. Updating Network VirusWall components automatically via a scheduled update

Use the **Logs** tab > **Event Logs** or **Command Tracking** screen to verify whether Control Manager updates the selected components at the specified schedule.

Setting the Update Source

Use the Update Settings screen to set the update source from which Network VirusWall will obtain the latest components, including the proxy settings if your network has a proxy server to connect to the Internet.

To set the update source:

1. Access a managed Network VirusWall product (see *page 2-2*).
2. On the working area, click the **Configuration** tab.
3. Under **Select configuration**, select **Update Settings**.
4. Click **Next>>**. The Update Settings screen appears.
5. Choose whether to receive updates from the **Trend Micro ActiveUpdate server** or from **another source**, and then type the **source URL**.

Note: Trend Micro ActiveUpdate server is the default selection.

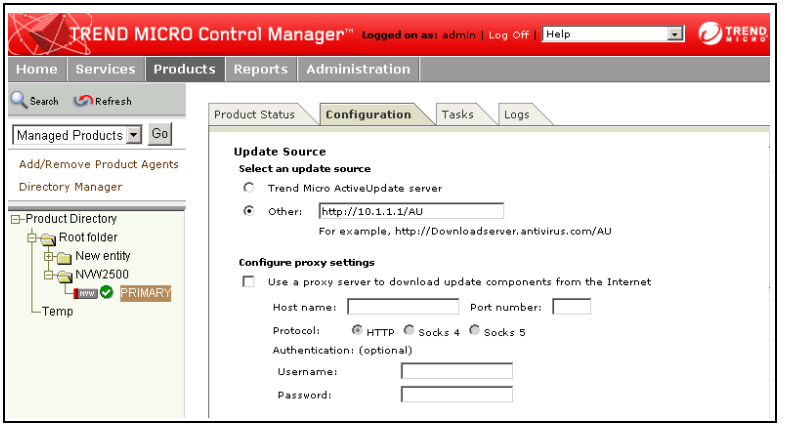


FIGURE 3-8. Using another update source (for example, your company's Intranet server)

6. Configure the **proxy server settings** if you are using a proxy server to connect to the Internet.
   a. Click **Use a proxy server to download update components from the Internet**.
   b. Specify the proxy server **host name** and **port**.
   c. Select the proxy server protocol– HTTP, SOCKS 4, or SOCKS 5.
   d. Type the **user name** and **password** used for proxy authentication.
7. Click **Save**.

The Network VirusWall Manual and Scheduled Update will obtain the latest components from the update source.

Updating Components from the Control Manager Server

Using the Control Manager server as the source of Network VirusWall components requires the completion of the following tasks:

- Downloading components
- Deploying downloaded components

To update components manually from the Control Manager server:

1. Obtain the latest components via scheduled or manual download.

   To download components manually:

   a. From the Control Manager management console main menu, click **Administration**.

   b. In the left-hand menu under **Update Manager**, click **Manual Download**.

   c. Click **Download Now** in the working area, and then click **OK** to confirm. The download response screen opens. The progress bar shows the download status.

   d. View details from the **Command Details** screen.

   e. Click **OK** to return to the Manual Download screen.

   To download components automatically through a scheduled update:

   a. From the Control Manager management console main menu, click **Administration**.

   b. In the left-hand menu under **Update Manager**, click **Scheduled Download**.

   c. Click the **Edit** link of the component that you want to modify.

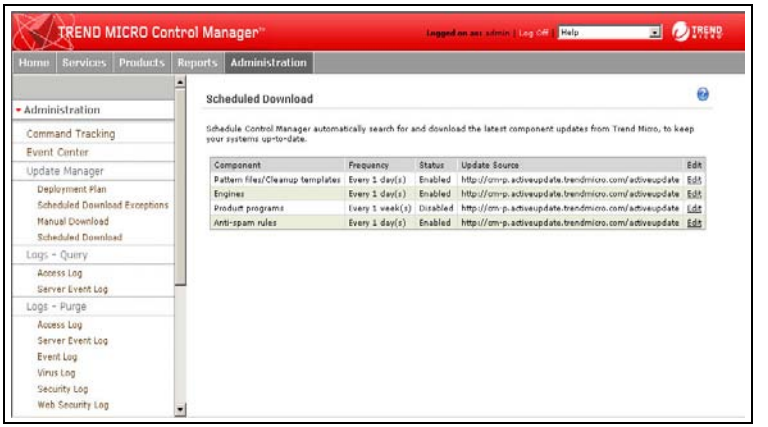


FIGURE 3-9. Setting the Control Manager scheduled component download

---

Tip: Click the **Pattern files/Cleanup templates** and **Engines** links to update the corresponding Network VirusWall components.

---

d. Under **Schedule and frequency**:

i. Define the **download schedule**. Select a **frequency**, and use the appropriate drop down menu to specify the desired **schedule**. You may schedule a download every **minute**, **hour**, **day**, or **week**.

ii. Use the **Start time** drop-down menus to specify **time** when the schedule starts to take effect.

c. Click **Save**.

2. Deploy the downloaded components through a **Deployment Plan** or **Deploy** task.

To deploy components through a Deployment Plan:

a. From the Control Manager management console main menu, click **Administration**.

b. In the left-hand menu under **Update Manager**, click **Deployment Plan**.

c. Select whether to update the existing deployment plans or create a new one.

Tip: The Control Manager installation creates two deployment plans. One of these plans, **Deploy to All Managed Products Now (Default)** is the default plan used during component updates. This plan instructs Control Manager to deploy the latest component to applicable managed products once the component download is finished.

Trend Micro recommends using this default plan.

To deploy components manually:

a. Access a managed Network VirusWall product (see *page 2-2*).

b. Click the **Tasks** tab.

c. Under **Select task**, select the component to deploy to the selected Network VirusWall 2500 device:

- **Deploy engines:** deploy the network scan engine
- **Deploy pattern files/cleanup templates:** deploy the network virus pattern file and network outbreak rule
- **Deploy program files:** deploy the program file

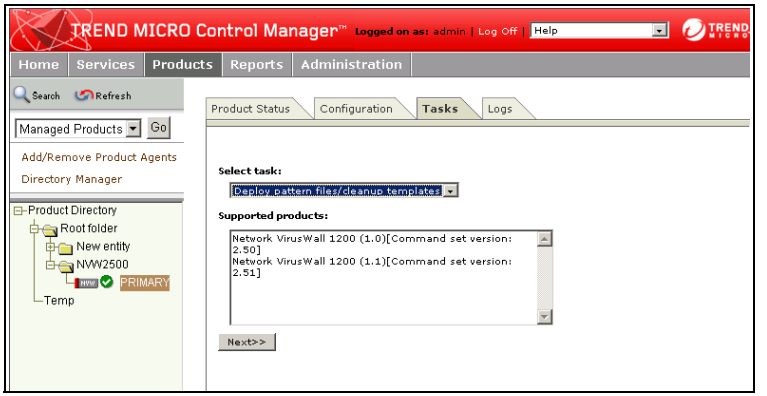


FIGURE 3-10. Deploying components from the Control Manager server to Network VirusWall

d. Click **Next>>.**

e. Click the **Deploy Now** link at the bottom of the screen to deploy the component(s).

Tip: Trend Micro recommends deploying the latest network virus pattern file immediately after a new one becomes available following a virus outbreak. This will help ensure your network has the most up-to-date antivirus protection. Verify that you first perform a Manual Download on the Control Manager server (see the *Control Manager Getting Started Guide* for more information.)

Deploying Network VirusWall Components

Deploying components instructs Network VirusWall to obtain the latest components from the Control Manager server. The Control Manager server should have the latest component to help ensure up-to-date protection from the current network threats.

To deploy components to Network VirusWall:

1. Access Network VirusWall devices from the Control Manager management console.
2. Click the **Tasks** tab.
3. Under **Select task**, select the component to deploy to the selected Network VirusWall 2500 device:
   - **Deploy engines:** deploy the network scan engine
   - **Deploy pattern files/cleanup templates:** deploy the network virus pattern file and network outbreak rule
   - **Deploy program files:** deploy the program file
4. Click the **Next** button.
5. Click the **Deploy Now** link at the bottom of the screen to deploy the component(s).

Tip: Trend Micro recommends deploying the latest network virus pattern file immediately after a new one becomes available following a virus outbreak. This will help ensure your network has the most up-to-date antivirus protection. Verify that you first perform a Manual Download on the Control Manager server (see the *Control Manager Getting Started Guide* for more information.)

Chapter 4

Viewing Status, Logs, and Summaries

This chapter explains how to access antivirus information to evaluate your organization's virus protection policies and identify clients that are at a high risk of infection. Network VirusWall 2500 logs a wide variety of information about events that occur on your network, such as client infections and policy violations, virus outbreaks, and component updates.

The topics discussed in this chapter include:

Viewing Operation Mode and VLAN Settings Summary

Use the Operation Mode and VLAN Information screen to view information about the existing Operation Mode and VLAN settings.

Tip: See *page 1-27* and *page 1-39* for details about SNMP and Operation Mode.

View the Operation Mode and VLAN Settings summary from any of the following:

- Control Manager management console, see *page 4-3*
- Preconfiguration console, see *page 4-3*

Operation Mode Summary

The read-only summary table provides the following information:

- Operation Mode
- Failopen (Disabled or Enabled)– whether or not failopen is enabled
- Failover (Primary or Secondary, Switch-back or Non-switch-back)– provides the failover environment (Switch-back or Non-switch-back mode) and "original attribute setting" (Primary or Secondary)
- Status– determines whether the device role is Active or Standby

VLAN Setting Summary

The summary table provides the following details:

- Number of tagged/non-tagged VLANs– the total number of both tagged and non-tagged VLANs
- VLAN ID– the ID number given to the VLAN given during configuration
- VLAN Name– the name of the VLAN given during configuration
- Tag (Yes or No)– whether or not the VLAN is tagged or non-tagged
- IP Binding (Yes or No)– whether or not the Network VirusWall IP address is bound to this VLAN (by default, the Network VirusWall IP address is bound to a non-tagged VLAN)

Tip: Change the Operation Mode and VLAN settings via the Preconfiguration console. Refer the Network VirusWall 2500 Getting Started Guide for more information on preconfiguration.

To view Operation Mode and VLAN information from the management console:

1. Access Network VirusWall from the Control Manager management console (see *page 2-2*).
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Operation Mode and VLAN Information**.
4. Click **Next >>**.

The read-only Operation Mode and VLAN Information screen appears.

To view Operation Mode and VLAN information from the Preconfiguration console:

1. Access the Preconfiguration console (see *page 2-37*).
2. Perform one of the following:
   - To view the Operation Mode summary, type `3` in the main menu
   - To view the VLAN Settings, type `5` in the main menu

Tip: Refer to the Network VirusWall *Getting Started Guide* for instructions to set the Operation Mode and VLAN settings.

Understanding Logs

Logs provide information about the performance of managed Network VirusWall devices. They allow you to monitor the Network VirusWall activities and help you to troubleshoot an issue.

This section provides the following information:

- Types of Network VirusWall logs
- Ways to view Network VirusWall logs
- Network VirusWall log format and interpretation

Types of Network VirusWall Logs

Network VirusWall generates the following log types:

- Network Outbreak Monitor and Policy Enforcement logs
- Real-time scan logs
- Debug or system logs
- Baseboard Management Controller (BMC) logs

Network Outbreak Monitor and Policy Enforcement Logs

Network Outbreak Monitor and Policy Enforcement logs refer to recorded actions initiated by either a user or the computer to a Network VirusWall device. Network VirusWall generates different severity levels for event logs. These include:

- Information– provides details about changes made to the Network VirusWall configuration through the management console
- Critical– provides details about determinative information relating to Network VirusWall settings, such as outdated components
- Error– provides details about error information relating to Network VirusWall processes, such as being unable to update components due to unresponsive device

Network Outbreak Monitor and Policy Enforcement logs are accessible from the **Logs** > **Event Logs** screen on the Control Manager management console. See *page 4-19* to view event logs.

Real-time Scan Logs

Network virus logs refer to recorded actions that involve the detection of virus and other types of threat in a network packet.

The following processes enumerate how Network VirusWall stores and delivers its virus logs:

i. Network VirusWall stores the virus logs in its queue.

ii. Network VirusWall sends the virus logs to Control Manager:

- Every 30 seconds
- When the virus log queue reaches 200 records within 30 seconds

---

Note: The queue does not save identical logs to prevent "log spamming." Identical logs refer to logs having the exact threat information detected in the same client. This means, Network VirusWall will only log the first instance of multiple identical detections.

For example, Network VirusWall detects and writes a virus log about `worm_ABC` in `client1`, `trojan456` in `client1`, and `backdoor_XYZ` in `client2`. NVW saves all three detections as logs in the queue. For details about clients, see *page 1-24*.

iii. After sending the virus logs, Network VirusWall then purges the queue to provide space for new logs.

Real-time scan logs are accessible from the **Logs** > **Security Logs > Viruses found in network packets** screen on the Control Manager management console. See *page 4-22* to view Network VirusWall real-time scan logs.

Debug or System Logs

Debug or system logs refer to recorded actions that involve notifications and information that allow you to determine the cause of Network VirusWall issues. These logs help you to troubleshoot errors in or malfunctions of Network VirusWall components, commands, and functions.

Debug or system logs are accessible from the following interfaces:

- Preconfiguration console > **System Tasks** > **View System Logs** option
- Remote host set through the Control Manager Management console > **System Logs** option
- **Network VirusWall System Log Viewer** tool

See *page 4-26* to view Network VirusWall debug logs.

Note: Network VirusWall cannot store its virus and debug logs in the device. If the device cannot connect to the Control Manager when sending logs, it retries for three (3) times. If after the third try the server is still unreachable, Network VirusWall deletes the logs in the queue. In addition, the following debug log appears:

CMAgent Unable to send status log to Control Manager (-109), Retry timeout (60) due to communications problem. Ensure that Control Manager is online and your network is functioning properly.

Baseboard Management Controller (BMC) Logs

BMC logs, also called as hardware (H/W) logs, refer to recorded actions that involve the actual Network VirusWall hardware components. BMC is a microcontroller responsible for the Intelligent Platform Management Interface (IPMI). IPMI is an interface or gateway between the host system (that is, server management software) and the periphery devices.

BMC logs are only accessible from the LCM console (LCD module). See *page 4-12* for more details about Network VirusWall BMC logs.

Where Logs Are Displayed

Table 4-1 lists the interfaces where you can view Network VirusWall logs.

TYPE OF LOGS	INTERFACE
Network Outbreak Monitor / Policy Enforcement logs	• Control Manager management console > **Logs** tab > **Event Logs**
Real-time Scan logs	• Control Manager management console > **Logs** tab > **Security Logs** > **Viruses Found in network packets**
Debug/System	• **Preconfiguration console** > **System Tasks** > **View System Logs** option • Remote host set through the Control Manager Management console > **System Logs** option • **Network VirusWall System Log Viewer** tool
BMC logs	• LCD module

TABLE 4-1. Interfaces where Network VirusWall displays logs

System Log Format and Interpretation

Except for the logs displayed on the LCD console, Network VirusWall logs viewable from the Preconfiguration console and Control Manager management console have the following format:

```
{time} {host name} {process} {log level} {module name} {message}
```

where:

- `{time}` is the log generate time, which follows `Month Day HH:MM:SS` convention
- `{host name}` is the Network VirusWall client host name or IP address

Note: If you are using the Network VirusWall System Log View, the log displays the device IP address instead of the host name.

- `{process}` is the Network VirusWall process name and process ID

Note: Some processes do not log their process ID.

- `{log level}` defines the log condition
- `{module name}` is the Network VirusWall function generating the log
- `{message}` is the log content

For example:

```
Aug 9 15:03:20 NVW2500_NY cavit[8w3r4]: INFO: AVE(IPRANGE):
Invalid IP address. Check the IP and then input a valid IP
address format. Refer to the Administrator's Guide for details
on the valid IP, netmask, default gateway, and DNS server
addresses.
```

Real-time Scan Log Format and Interpretation

The Network VirusWall real-time scan generates logs and sends them to Control Manager server whenever it detects malicious packets. View the real-time scan log from the following interfaces:

- Preconfiguration console > **View System Logs** screen
- Control Manager management console > **Logs** > **Security Logs**/**Event Logs** screen

Real-time scan logs available from the **Security Logs** screen have the following format:

```
{Time} {Computer Name} {Infection Source} {Viruses found in network packets} {Scan Action} {Engine Type} {Engine Version} {Virus Pattern File Version}
```

Where:

- `{time}` is the log generate time, which follows `Month Day HH:MM:SS` convention
- `{Computer Name}` is the Network VirusWall client host name or IP address
- `{Infection Source}` is the client where the infection originated
- `{Viruses found in network packets}` is the name of the virus or other threats detected
- `{Scan Action}` is the scan action code

  Network VirusWall uses the following scan action code:

CODE	SCAN ACTION
6	Pass
8	Drop
9	Quarantine

TABLE 4-2. Network VirusWall Real-time Scan Action Codes

- `{Engine Type}` is the Trend Micro Network Scan Engine
- `{Engine Version}` is the network scan engine version number
- `{Virus Pattern File Version}` is the Trend Micro Virus Pattern file version number

For example:

	A	B	C	D	E	F	G	H
1	Generated	Computer Name	Infection Source	Viruses found in network packets	Scan Action	Engine Type	Engine Version	Virus Pattern File Version
2	9/28/2004 0:03	HIETEST	111.123.123.123	WORM_SQLP1434.A	8	Network VirusWall engine	1.5401012	10140
3	9/28/2004 2:28	HIETEST	10.123.123.123	MS03-026_RPC_DCOM_EXPLOIT	8	Network VirusWall engine	1.5401012	10140
4	9/28/2004 3:27	HIETEST	11.123.11.111	MS04-011_LSASS_EXPLOIT	8	Network VirusWall engine	1.5401012	10140

FIGURE 4-1. Sample Network VirusWall real-time scan logs exported in *.CSV format

LCD Module Log Format and Interpretation

Logs displayed on the LCD console fall into the following categories:

- Asset tag error logs
- H/W logs
- LCD module error logs

Asset Tag Logs

Asset tag logs refer to logs that record the Network VirusWall device validity checking. When booting up or restarting (resetting) the device, Network VirusWall checks whether the device hosting the NVW software components are valid. An invalid casing or hardware component results to an asset tag log.

An asset tag log has the following format:

```
[Error #]
Invalid device
```

Where `#` indicates the error code and `Invalid device` indicates that a Network VirusWall software or hardware component is mounted on an invalid platform.

Table 4-3 enumerates all possible asset tag logs:

ERROR CODE	DESCRIPTION
0	Invalid asset tag.
-1	**Action**: Issue GET_FRU_INFO command GET_FRU_INFO is the function that obtains the Field Replaceable Unit. FRU is the component responsible for the actual device information. **Result**: The response data length does not match or the completion code is incorrect
-2	FRU size is equal to 0. The FRU size should not be equal to 0.
-3	**Action**: Issue GET_FRU_DATA command **Result**: The response data length does not match or the completion code is incorrect
-4	The FRU header version is not equal to 1. The FRU header version should be equal to 1.
-6	Missing product offset.

TABLE 4-3. Asset tag logs

Having any of the above error codes can only mean that someone has tampered with the Network VirusWall device. Someone has altered or replaced the original components included with shipment of the product. The error codes help listed above help Trend Micro engineers to troubleshoot and pinpoint the exact device issue.

Hardware Logs

Hardware (H/W) logs refer to logs generated by the Network VirusWall devices. An H/W log can pertain to almost anything related to the Network VirusWall hardware-related events (such as the fan speed, memory capacity, or current temperature).

H/W logs have the following format:

```
{hardware component} {critical level} {activity}
```

Where:

- `{hardware component}` refers to the hardware component generating the log

  The following hardware components generate H/W logs:

  - Temperature
  - Processor
  - Voltage
  - CPU VRD PWRGD
  - Vcore
  - Fan
  - Platform security violation attempt
  - Power unit
  - Memory
  - System Firmware Progress (POST Error)
  - Disabled event logging
  - PCI error
  - Button or switch
  - Boot error
  - Watchdog
  - Storage

- `{critical level}` refers to lower or upper critical component threshold

  The following are the possible critical level:

  - Lower Critical– the lower critical component threshold
  - Upper Critical– the upper critical component threshold

- `{activity}` refers to the increasing or decreasing of the component's activity

  The following are the possible critical level:

  - going low Assert– the component has started to decrease its activity
  - going high Assert– the component has started to increase its activity

- going high Deassert– the component has started to stop from increasing its activity
- going low Deassert– the component has started to stop from decrease its activity

For example:

```
CPU 1 Temp Upper Critical - going high Assert
```

The above example indicates that the first processor's temperature is starting to reach the upper critical threshold temperature.

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

Appendix B enumerates all possible H/W logs and their descriptions.

LCD Module Error Logs

LCD module error logs refer to logs generated by and displayed on the LCD module.

Tip: The LCD and control panel make up the LCD module.

An LCD module error log has the following format:

```
[Error #{code}]
{message}
```

Where:

- `[Error #{code}]` refers to the error code (use *Table 4-4* to determine the meaning and possible solution for an LCD module error message)
- `{message}` indicates the short message description

Table 4-4 enumerates all possible LCD module error logs:

ERROR CODE AND MESSAGE	CAUSE AND POSSIBLE WORKAROUND/SOLUTION
100 Corrupted image	The Network VirusWall firmware is corrupted. Reload the Network VirusWall image.
101 Missing file	Missing boot file. Network VirusWall will try to boot from the second partition.
102 Device failure	Missing boot file or physically damaged boot partition. Contact technical support.
200 Corrupted file	Corrupted configuration file. Reload the Network VirusWall image.
407 Cannot open file	Unable to open the configuration file. The file may be missing or corrupted. Reload the Network VirusWall image.
409 Cannot read file	Unable to read the configuration file. The file may be missing or corrupted. Reload the Network VirusWall image.
203 Missing CM server	Cannot register the Network VirusWall device to the Control Manager server. Check the network and Control Manager server status.
205 No connection	Network connection unavailable. Check the network cable, as well as the network status.
206 Cannot get key	Unable to obtain the public encryption key. The Network VirusWall device cannot register to the Control Manager server. Check the E2EPublic.dat through LCD module or Preconfiguration console.
207 Cannot sync time	Unable to synchronize time with the Control Manager time server. The Network VirusWall device cannot register to the Control Manager server. Ensure that the Control Manager time service is running.
208 Cannot register	Unable to register the NVW device to the Control Manager server. Check the network and Control Manager settings.
209 Unknown error	The LCD module is unable to obtain the error from the Network VirusWall function. The LCD module may be corrupted or damaged. Contact technical support.
210 Cannot restore	Unable to restore the Network VirusWall factory default settings. The Network VirusWall image may be corrupted. Reload the image.
300 Cannot proceed	A network interface card (NIC) error occurred. Check the Network VirusWall port and network card. Contact Trend Micro support if the issue persists.

TABLE 4-4. LCD module error logs

ERROR CODE AND MESSAGE	CAUSE AND POSSIBLE WORKAROUND/SOLUTION
400 Invalid IP	Invalid IP address. Ensure the address specified belongs to the valid IP class and device. Check and modify the address through the LCD module or Preconfiguration console.
401 Same as local IP	The IP address used is the same as the IP address of a machine located in the same network. Check and modify the address through the LCD module or Preconfiguration console.
402 Invalid netmask	Invalid netmask. Ensure the address specified is the address belonging to the subnet mask. Check and modify the address through the LCD module or Preconfiguration console.
403 Gateway not set	The gateway address was not set. Ensure the address specified is a valid gateway server address. Check and set the IP address through the LCD module or Preconfiguration console.
404 Invalid address	Unusable address. Ensure the address specified is a valid address. Check and modify the address through the LCD module or Preconfiguration console.
405 Duplicate DNS IP	Duplicate DNS server IP address. Ensure the address specified the address belonging to the DNS server. Check and modify the address through the LCD module or Preconfiguration console.
406 Different subnet	The subnet address set is on a different network. Ensure the subnet address specified is a valid subnet address. Check and modify the address through the LCD module or Preconfiguration console.
408 Cannot write	Unable to write to the configuration file. The file may be missing or corrupted. Reload the Network VirusWall image.
410 Cannot save file	Unable to save the changes to the configuration file. The file may be missing or corrupted. Reload the Network VirusWall image.
411 LCD H/W error	Physical damage to the LCD module. Contact technical support.
412 Cannot reset	Unable to reset the Network VirusWall device. The firmware may be corrupted. Reload the image.

TABLE 4-4. LCD module error logs

Viewing Client Summary Information

The **Client Summary** screen provides an overview of network-virus infections, policy violations, and existing Trend Micro antivirus component details. From these summaries:

- View which clients have been infected and which have violated policies
- Un-quarantine infected clients
- Add or remove clients from the exception list for policy enforcement

To view client summary information:

1. Access a Network VirusWall device from the Control Manager management console.
2. In the main window, click the **Configuration** tab. Under **Select configuration**, click **Client Summary**.
3. Click **Next>>**.

   The following tables appear:

   - **Violation Summary** – virus infections, Network VirusWall Policy violations, and Outbreak Prevention Policies violations
   - **Component Enforcement Summary** – the latest (most recent available) and baseline (currently used) version numbers for the virus pattern file and two types of Windows-based virus scan engines:
     - **VxD**– for machines running Windows 95 (95, 98, and Me)
     - **NTDK** – for machines running Windows NT (NT, 2000, XP)

   Note: The baseline versions may be older than the latest versions. Determine how many versions older than baseline versions can be by enabling and configuring Network VirusWall Policy Enforcement (see *Configuring Advanced Settings* on page 2-16).

   The following icons represent client status:

   - NVW had quarantined client because of an infection
   - NVW has blocked a client because of a violation of Network VirusWall Policy Enforcement or Outbreak Prevention Policies (see *Configuring Policy Enforcement Settings* on page 2-12 for more information on

enforcement policies and see the Control Manager online help for information on Outbreak Prevention Policies)

- client would normally be blocked, but is not because it is on the **Policy Exception List** (see *Creating Exception Lists* on page 2-22 for more information)

To view client infections:

1. Click the **Virus infections** link in the **Count** column. The **Virus Infections Summary** screen appears showing a table with quarantined client IP address(es), host name(s), and MAC address(es), time and date of infection, and the virus name(s).

   Note: Configure Network VirusWall 2500 to quarantine clients on the **Scan Options** screen (see *Configuring Real-time Scan Options* on page 2-7 for more information).

2. Do the following:
   - Sort the table by clicking on a column heading.
   - Un-quarantine infected clients by doing the following:
     - Select the client(s) to remove from quarantine and click **Release**.
   - Save the client violation information as a CSV file by right clicking **Export summary into CSV**. Alternatively, view the information in the Control Manager management console window by left clicking **Export summary into CSV**.

To view Network VirusWall Policy violations:

1. Click the link in the **Count** column for **Network VirusWall Policy violations**. The **Network VirusWall Policy Violations** screen shows a table with clients that violated policy enforcement and their corresponding IP address, host name, and MAC address, time and date of violation, and violation details.
2. Do the following:
   - Click a column heading to sort the table.

- Unblock clients and add them to the exception list for Network VirusWall Policy Enforcement by doing the following:
  - Select the client(s) to unblock and click **Add to exceptions**.
- Block clients and remove them from the exception list for Network VirusWall Policy Enforcement by selecting the client(s) to unblock, and then clicking **Remove from exceptions**
- Save the client violation information as a CSV file by right clicking **Export summary into CSV**. Alternatively, view the information in the Control Manager management console window by left clicking **Export summary into CSV**.

To view Outbreak Prevention Policies violations:

1. Click the **Outbreak Prevention violations** link in the **Count** column. The **Outbreak Prevention Violations Summary** screen appears showing a table with clients that violated Outbreak Prevention Policies and their corresponding IP address, host name, and MAC address, time and date of violation, and violation details.
2. The following options are available on this screen:
   - Sort the table by clicking on a column heading.
   - Save the client violation information as a CSV file by right clicking **Export summary into CSV**.

Note: Use a spreadsheet application, such as Microsoft Excel, to view *.csv files.

Viewing Event Logs

When Network VirusWall 2500 detects an event, such as a virus outbreak, or performs an action, such as a reset or component update, it creates an event log entry. Query and view the following types of Network VirusWall 2500-related information from the event logs:

- **Module updates:** updates to the Network VirusWall 2500 scan engine and virus pattern file
- **Network outbreaks:** any type of virus detection on the network
- **All events:** all events available from the Control Manager server

To query any type of event log:

1. Access Network VirusWall 2500 from the Control Manager management console.
2. Click the **Logs** tab.
3. Click **Event Logs**.
4. Next to **Severity**, select **Information**.

Note: The Control Manager server on your network reports event logs with several types of event severity. Only logs with the even severity **Information** report Network VirusWall 2500-related information. Select other types of severity to include non-Network VirusWall-related event logs.

---

5. In the **Incidents** list, select an event type.

Note: The Control Manager server on your network reports several types of event logs. Only the logs **Module updates**, **Network outbreaks**, and **All events** contain Network VirusWall 2500-related information. Select other types of logs to include non-Network VirusWall-related event logs.

---

6. Next to **Product**, select the Network VirusWall device whose logs you want to query.
7. Next to **Logs for**, select a period. Network VirusWall displays log entries created during this period.

To select a period between two specific dates, select **Specified range**, and then select the **start** and **end dates**.

8. Next to **Sort logs by**, select one of the following ways to sort the logs:
   - **Event date/time:** Control Manager sorts logs by the date and time Network VirusWall 2500 discovered the virus or violation
   - **Computer name:** Control Manager sorts logs by the host name of the client
   - **Product:** Control Manager sorts logs by the name of the product

---

Note: The Control Manager server on your network may be managing products other than Network VirusWall 2500. Sort the logs by product to group the Network VirusWall-related logs together.

---

9. Next to **Sort order**, select either ascending or descending.
10. Click **Display Logs**.

    To save the result as a CSV file, click **Export Logs into CSV**, select a place to save the file, and click **Save**.

    To create a new query, click **New Query**.

Note: Use a spreadsheet application, such as Microsoft Excel, to view *.csv files.

Internet Explorer displays the exported logs in normal text format if there is no Microsoft Excel installed on the computer. Install Microsoft Excel to view exported logs in CSV format when using the Export Logs into CSV option from the Control Manager management console > Client Summary screen.

Viewing Network VirusWall System Information

View Network VirusWall system information for a summary of device details. The read-only **System Information** screen displays the following information:

- **Product Information** – Network VirusWall device details, including the product version number, Control Manager agent version number, the date and time the device was registered to the Control Manager server, and the current device status
- **Component Status** – Network VirusWall device components, including the version numbers for the network outbreak rule, network virus pattern file, and scan engine
- **Operating System Information** – the Network VirusWall operating system name, version, service pack number and language
- **Agent Environment Information** – the Network VirusWall domain name, host name, IP address, and MAC address

---

Note: Not all the information on the **System Information** screen relates directly to Network VirusWall 2500. Some information relates to other Control Manager services and products. For a detailed explanation of every field on the **System Information** screen, see the Control Manager online help.

To view Network VirusWall status:

1. Access a Network VirusWall device from the Control Manager management console (see *Accessing Network VirusWall Devices* on page 2-2).
2. When you click the Network VirusWall host name to manage, the **System Information** screen displays. At any time, click the **Product Status** tab on the main window of the management console to return to the **System Information** screen.

Viewing Security Logs

When Network VirusWall 2500 detects a virus or security violation, it creates a security log entry. Query and view the following types of Network VirusWall 2500-related information from the security logs:

- **Viruses found in network packets:** the infection source, the virus name, and scan engine and virus pattern file versions, and so on.

Note: The Control Manager server on your network reports several types of security logs. Only the logs listed above contain information about Network VirusWall. Select other types of logs to include non-Network VirusWall-related event logs.

To query any type of security log:

1. Access Network VirusWall 2500 from the Control Manager management console.
2. Click the **Logs** tab.
3. Click **Security Logs**.
4. Select a query by clicking the link adjacent to it.
5. Next to **Logs for**, select the **time**. Network VirusWall will display log entries created during this period.

   To select a time between two specific dates, select **Specified range**, and then select the **start** and **end** dates.
6. Next to **Sort logs by**, select one of the following ways to sort the logs:
   - **Event date/time:** the date and time Network VirusWall 2500 discovered the virus or violation
   - **Computer name:** the host name of the client
   - **Product:** the name of the product

   Note: The Control Manager server on your network may be managing products other than Network VirusWall 2500. Sort the logs by product to group the Network VirusWall-related logs together.

   ---
7. Next to **Sort order**, select either ascending or descending.

8. Click **Display Logs**.

   To save the result as a CSV file, click **Export Logs into CSV**, select a place to save the file, and click **Save**.

   To create a new query, click **New Query**.

Note: Use a spreadsheet application, such as Microsoft Excel, to view *.csv files.

Viewing Device Information and Status

The System Information screen, which is accessible via the Preconfiguration console, provides the Network VirusWall information, memory and CPU usage, as well as the number of concurrent users and scan sessions.

To device information and status:

1. Access the Preconfiguration console (see *page 2-37*).
2. Type `1` in the **Main Menu** to view the system information.

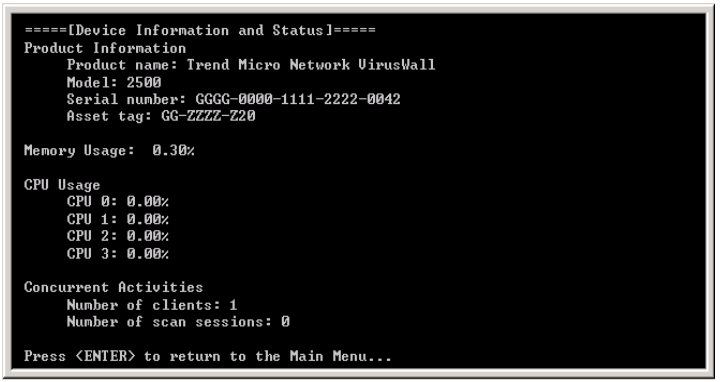


FIGURE 4-2. Viewing system information

The System Information screen displays.

Tip: The serial number identifies the Network VirusWall device. Each unit has a unique serial number. The asset tag, on the other hand, is identical to all Network VirusWall 2500 models.

Viewing System Logs

System logs contain information useful for troubleshooting. If you experience problems with Network VirusWall and contact Trend Micro support, your support provider may ask you to view the system log.

To view system logs through the Preconfiguration console:

1. Access the Preconfiguration console (see *page 2-37*).
2. Type `8` in the **Main Menu** to open the System Tasks submenu.
3. On the System Tasks submenu, type `1` to view system logs. The system logs appear showing the following information:
   - Date and time of log entry
   - Log entry

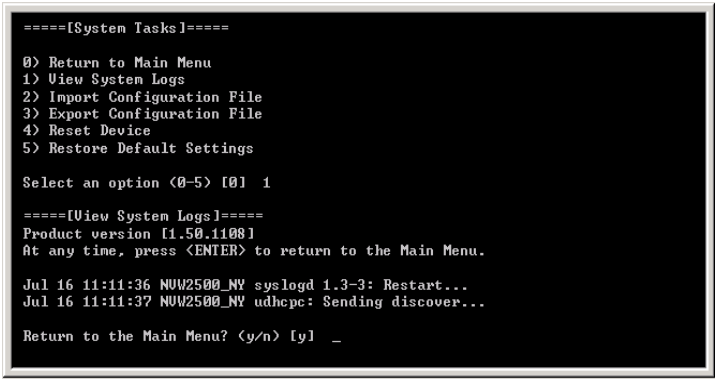


FIGURE 4-3. Viewing system logs

4. Press **Enter** to stop the log report.
5. At the prompt, type `y` to return to the main menu.

Viewing BMC Logs

You can only view BMC (H/W) logs from the LCD module of a running Network VirusWall device. See *page 4-12* for details about BMC logs.

To view BMC logs:

1. From the Network VirusWall control panel, press **Enter**. The Main Menu appears.
2. Use the **Down** arrow to select **View H/W Logs**.

Tip: The LCM console will timeout in 3 minutes if there is no activity initiated on the Control Panel.

---

3. The LCD screen refreshes and displays the available BMC logs. Otherwise, the following message appears if there are no available BMC logs:

   No H/W logs

Tip: Use the Left and Right arrows to scroll and be able to read the H/W logs.

See *page 4-12* for details about H/W logs.

Purging BMC Logs

You can only view and delete BMC logs from the LCD module of a running Network VirusWall device.

To purge BMC logs:

1. From the Network VirusWall control panel, press **Enter**. The Main Menu appears.
2. Use the **Down** arrow to select **Purge H/W Logs**. A prompt displays asking if you want to purge the BMC logs.
3. To continue, ensure the * is next to `Yes`; otherwise, move it next to `No`.
4. Press **Enter**.
5. If you selected `Yes`, the following message displays:

   ```
   H/W logs purged
   ```

Using the Log Viewer

Network VirusWall 2500 System Log Viewer (NVW System Log Viewer) is a user-friendly, stand-alone application that displays system debug log information in real-time as Network VirusWall creates log entries. Use NVW System Log Viewer to view system debug log entries and save them to a text file.

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

Note: The log viewer can only run on the computer configured to receive system logs. See *Configuring Device and System Settings* on page 2-27 for more information.

To download and use the System Log Viewer:

1. Open the Control Manager management console.
2. Click **Administration** in the main menu.
3. Click **Tools** in the navigation menu on the left. The **Tools** screen displays.
4. Click the **NVW System Log Viewer** link to download the `nvw_view.zip` file.
5. Unzip the file and double click `TMNVW.EXE`. The **System Log Viewer** window opens.
6. To start viewing the system logs, click ▶ . Log entries will display in the main window.

FIGURE 4-4. Viewing logs from the Log Viewer main window

7. To save the log, click **File** > **Capture to file**. Type a file name with extension, select a location to save the file, and click **Save**.

   NVW System Log Viewer continues to append any additional log entries to the file as Network VirusWall 2500 generates them.

   To stop the NVW System Log Viewer from receiving log entries, click ■ .

Configuring SNMP Notifications

Configure Simple Network Management Protocol (SNMP) notification settings to allow a network management station to receive traps from Network VirusWall. In addition, enable the SNMP agent, which adds security to SNMP communications. See *page 1-27* for more information on SNMP.

Tip: Trend Micro recommends enabling all SNMP agent community options for added security. This helps ensure only specific network management stations are able to access Network VirusWall 2500 after authenticating to the device.

To enable SNMP traps:

1. Access Network VirusWall 2500 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **SNMP Notifications**.
4. Click **Next>>**.
5. Select the **Send traps to the following network management station** check box.
6. Type the community name and IP address of the network management station to which Network VirusWall 2500 will send traps.
7. Click **Save**.

To enable SNMP agent:

1. Access Network VirusWall 2500 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **SNMP Notifications**.
4. Click **Next>>**.
5. Select the **Enable SNMP agent** check box.
6. Type the optional system location and contact person details under **System information**. This information appears on the network management station console.
7. Under **Security settings**, there are two lists to configure:

- **Set accepted community name:** community names of network management stations that Network VirusWall 2500 will accept before allowing access (maximum 5 names)
- **Set trusted network management station IP address:** IP addresses of specific network management stations that can access Network VirusWall 2500 (maximum 255 NMS IP addresses)

Note: The default accepted community name is **public**. If no community names or trusted network management station IP addresses are set, Network VirusWall 2500 grants any network management station access with this community name. The only allowable access privilege is READ ONLY.

To configure the lists, do the following:

a. Type a case-sensitive acceptable community name (maximum 33 alphanumeric characters) or IP address in the corresponding text boxes.

b. Click **Add**.

To remove a community name or IP address, click it in the list and click **Remove**. Use the CTRL or SHIFT keys to make multiple selections.

8. Click **Save**.

Downloading the Network VirusWall SNMP MIB II File

The SNMP MIB II file allows one or more computers on the network that act as a network management station (NMS) to poll the managed devices and gather information about their performance and status. Configure this setup by downloading the Network VirusWall SNMP MIB II file. You can download the Network VirusWall SNMP MIB II file from the Control Manager server.

To download the SNMP MIB II file:

1. Access the Control Manager management console.

2. Click **Administration** in the main menu.

3. Click **Tools** in the navigation menu on the left.

4. On the working area, click the **NVW SNMPv2 MIB file** link to download the `nvw_mib2.zip` file.

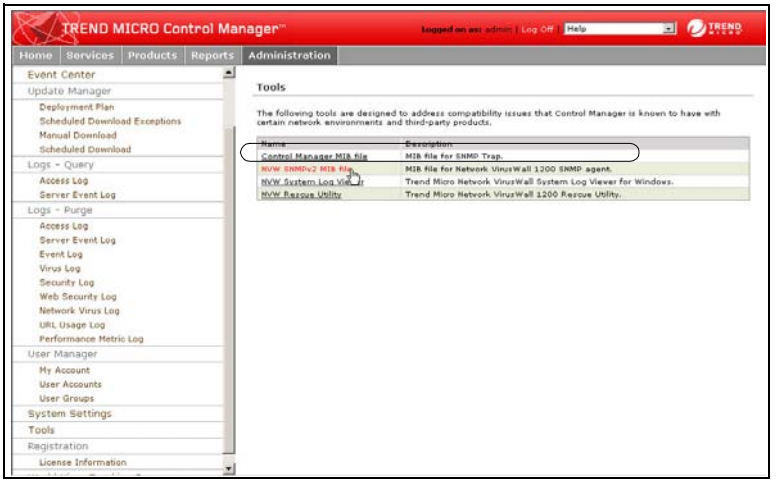


FIGURE 4-5. System Tasks > NVW SNMPv2 MIB file download

5. Unzip the file.

Chapter 5

Troubleshooting and FAQs

This chapter addresses troubleshooting issues that may arise and answers frequently asked questions.

The topics discussed in this chapter include:

Using Network VirusWall Utilities

Network VirusWall provides two (2) utilities:

- Rescue Utility– is a Windows-based tool that allows you to upgrade the Network VirusWall program and boot loader firmware
- Firmware Flash Utility– is a Windows-based tool that allows you to flash the Network VirusWall BIOS, BMC, and LCM firmware

These utilities are available in the *Trend Micro Solutions CD for Network VirusWall 2500* under the `\Programs` folder.

See the following sections for instructions on how to run the Network VirusWall utilities:

- Uploading the latest program file (firmware) and boot loader, see *page 5-4*
- Flashing the BIOS, BMC, and LCM firmware, see *page 5-8*

Entering Rescue Mode

If you are experiencing problems that prohibit the normal functioning of Network VirusWall, enter rescue mode to upload the program file or boot file via Trivial File Transfer Protocol (tftp). While in rescue mode, Network VirusWall has a default static IP address to which you will need to establish a tftp session. See *Table 5-1* for a summary of rescue mode settings.

WARNING! *Use rescue mode for troubleshooting only. Under normal circumstances, you do not need to enter rescue mode. See Troubleshooting on page 5-14 and the troubleshooting section in the* Getting Started Guide *for more information on common troubleshooting issues.*

RESCUE MODE SETTING	VALUE
Network VirusWall host name	Blank
IP address type	Reset
IP address	192.168.252.1
Netmask:	255.255.255.0
Default gateway	192.168.252.254
DNS server 1	Blank
DNS server 2	Blank

TABLE 5-1. Rescue mode settings

Note: The Rescue Utility or Firmware Flash Utility will hang and fail to function if any of these settings is not set. Use the Windows **Task Manager** to close the non-responsive utility.

Enter rescue mode through the:

- LCD module
- Preconfiguration console

To enter rescue mode with the LCD module panel:

1. Reset Network VirusWall by pressing the **RESET** button.
2. When the device resets, a message appears on the LCD display prompting you to enter rescue mode.
3. Press the **Enter** button. A message appears on the LCD display showing that the device is in rescue mode.

To enter rescue mode through the Preconfiguration console:

1. Reset Network VirusWall while logged on the Preconfiguration console.
2. When the device resets, a message appears prompting you to enter rescue mode.
3. Type `r` at the prompt. The Network VirusWall rescue mode settings appear.

Note: To exit rescue mode at any time, reset Network VirusWall by pressing the **RESET** button on the front panel.

Uploading the Program File and Boot Loader

The Network VirusWall program file (firmware) contains all the components necessary to prepare Network VirusWall devices for preconfiguration. This includes the operating system, network scan engine, network virus pattern file, and system programs.

Note: Uploading the program file will restore the Network VirusWall default factory settings.

To preserve the existing settings, back up the Network VirusWall configuration using the **System Tasks** > **Import Configuration File** option. After uploading the new or default program file, reconfigure the device settings through the Preconfiguration console > **Device Settings** menu or import the original configuration using the **System Tasks** > **Import Configuration File** option.

Note: After new firmware deploys to Network VirusWall, the device will automatically reboot.

The program file name is as follows:

`NVW_image.x.yy.zzzz.en_US.R`

Where:

- **x** is the major version
- **yy** is the minor version
- **zzzz** is the build number
- **en_US** is the program language version
- **R** denotes the nature of the file (that is, the Network VirusWall program file)

The boot loader contains information necessary for the Network VirusWall operating system to function. The boot loader file name is as follows:

NVW_image.x.yy.zzzz.en_US.B

Where:

- **x** is the major version
- **yy** is the minor version
- **zzzz** is the build number
- **en_US** is the program language version
- **B** denotes the nature of the file (that is, the Network VirusWall boot loader file)

You can obtain these files from the following locations:

- **Trend Micro download Web site**—contains the most up-to-date versions (www.trendmicro.com/download)
- **Trend Micro Solutions CD for Network VirusWall 2500**—the included CD contains the program file with factory defaults (see *page 2-42*) and the original boot loader. These files are located in the following path (replace D: with the path used by your CD-ROM drive):

  D:\Programs\NVW_Rescue

There are two methods for uploading the program file and boot loader:

- **The command line**—execute Trivial File Transfer Protocol (tftp) commands from computers running Windows or Linux (see *page 5-6*)
- **Network VirusWall 2500 Rescue Utility**—utilize a user-friendly Windows-based utility (see *page 5-7*)

Uploading with the Command Line

Use Windows or Linux commands to upload the program file or boot file.

To upload the program file from the command line:

1. To use the most up-to-date program file and boot loader, download them from the Trend Micro Web site to your computer; otherwise, use the program file with factory defaults and the original boot loader located on the *Trend Micro Solutions CD for Network VirusWall 2500*.
2. Configure the computer to use a static IP in the range 192.168.252.2 to 192.168.252.254 with a subnet mask 255.255.255.0.
3. Enter rescue mode (see *Entering Rescue Mode* on page 5-2).
4. Connect one end of the included crossover Ethernet cable that came with the device to your computer's LAN port and the other end to port **5** of the Network VirusWall device.
5. At the command prompt, type the following command(s). There are different commands for Windows and Linux operating systems:
   - For Windows machines, type the following:

     ```
     tftp -i 192.168.252.1 PUT [file name]
     ```

   - For Linux machines, type the following:

     ```
     tftp 192.168.252.1
     tftp> bin
     tftp> put [file name]
     ```

Note: `[file name]` is the name of the file to upload. See *Uploading the Program File and Boot Loader* on page 5-4 for exact file names.

If you uploaded the program file, Network VirusWall resets automatically after upload is complete. You must perform preconfiguration before the device can register to the Control Manager server (see *Performing Preconfiguration* on *Preconfiguring Network VirusWall* in the Network VirusWall *Getting Started Guide*).

Uploading with the Network VirusWall Rescue Utility

Uploading with the Trend Micro Network VirusWall Rescue Utility performs the same function as uploading through the command line interface. The utility, however, is a user-friendly, Windows based option for those who prefer to use a graphical user interface.

Note: The Network VirusWall Rescue Utility supports only Windows operating systems. If you are using a Linux-based computer, you can only upload the program and boot files from the command prompt (see *Uploading with the Command Line* on page 5-6).

The utility is included on the *Trend Micro Solutions CD for Network VirusWall 2500*. You can also download the utility from the Control Manager server.

To run the rescue utility from the CD:

1. Insert the Trend Micro Solutions CD for Network VirusWall 2500 into your CD-ROM drive. The autorun program loads.
2. Select **Network VirusWall Rescue Utility** from the menu on the left.
3. Click **Launch** to run the Network VirusWall Rescue Utility.

To download the rescue utility and run it from your computer:

1. Access the Control Manager management console.
2. Click **Administration** in the main menu.
3. Click **Tools** in the navigation menu on the left.
4. Click the **NVW Rescue Utility** link to download the `nvw_rescue.zip` file.
5. Unzip the file.
6. Browse to the location of the utility and double-click `NVWRESCUE.EXE` to run the program.

To upload with the rescue utility:

1. To use the most up-to-date program file and boot loader, download them from the following Website to your computer:

   `www.trendmicro.com/download`. Locate the Network VirusWall files.

Otherwise, use the program file with factory defaults and the original boot loader located on the *Trend Micro Solutions CD for Network VirusWall 2500*.

2. Configure the computer to use a static IP in the range 192.168.252.2 to 192.168.252.254 with a subnet mask 255.255.255.0.

Note: If you are running PC-cillin™ 2002 or later, set the Personal Firewall settings to "low" or "medium" when using the utility.

3. Enter rescue mode (see *Entering Rescue Mode* on page 5-2).
4. Connect one end of the included crossover Ethernet cable to your computer's LAN port and the other end to port **5** of the Network VirusWall device.
5. Run the program from your computer or from the CD.
6. Click **Browse** and locate the file you want to upload.
7. Click **Open**.
8. Click **Update** to begin the update process.

WARNING! *During the update, do not turn off, reset the device, or modify any device settings. If you uploaded the program file, wait for the device to finish the automatic reset.*

Flashing the BIOS, BMC, and LCM Firmware

Use the Network VirusWall 2500 Firmware Flash Utility (FFU) to flash the BIOS, BMC, or LCM firmware. Run the utility on computers that can access a Network VirusWall 2500 device.

Before Running the Firmware Flash Utility

Prepare the following before running the utility:

- A computer running Microsoft™ Windows™ with a LAN port and configurable IP address, as well as a CD drive
- An account belonging to the Administrator's group of the local computer on which the tool will run

- The included crossover Ethernet cable
- The *Trend Micro Solutions CD for Network VirusWall 2500*, which contains the Firmware Flash Utility

Complete the following tasks before flashing a Network VirusWall firmware:

- Obtain a copy of the Network VirusWall 2500 Solutions CD

  The `\Programs` folder in the CD contains the Firmware Flash Utility executable.

- Obtain the latest copies of the Network VirusWall BIOS, BMC, or LCM firmware save them on the computer on which the Firmware Flash Utility will run

  To use the most up-to-date BIOS, BMC, and LCM firmware, locate and download them from the following Web site to your computer:

  `http://www.trendmicro.com/downloads.`

  The Network VirusWall firmware uses the following naming convention:

  - BIOS firmware– `S25_####.rom`
  - BMC firmware– `BMS25###.bin`
  - LCM firmware– `PICFW##.hex`

  Where `####`, `###`, or `##` is the firmware's version number. For example, `BMS25110.bin` denotes that the BMC firmware version is 1.10.

Note: Remember the location of the directory with the latest firmware. If you want to roll back to the factory defaults, use the versions available in the Solutions CD.

- Disconnect the device from the network and enter rescue mode (see *page 5-2*)
- Prepare a Windows-based computer on which to run the Firmware Flash Utility During Rescue Mode, Network VirusWall enables failopen and allows network traffic to pass through the device.

Tip: Trend Micro recommends using a standalone Windows 2000 server to run the Firmware Flash Utility.

To prepare the computer:

a. Log on to the computer used when running FFU using an Administrator account.

Note: The account used to log on to the computer on which the Firmware Flash Utility will run must have administrator rights or should belong to the Administrators group. Otherwise, the utility cannot successfully execute.

---

b. Configure the Local Area Connection properties to use the following settings:

- IP address– 192.168.252.100
- Netmask– 255.255.255.0
- Default Gateway– blank
- DNS– blank
- Firewall– disabled

c. Connect one end of a crossover Ethernet cable to the computer's LAN port and the other end to Port 5 of the Network VirusWall device.

Note: In a failover deployment, disconnect the failover cable from Port 5 to connect the Network VirusWall device to the computer on which this tool will run.

After completing these tasks, you are now ready to run the Network VirusWall 2500 Firmware Flash Utility.

Running the Firmware Flash Utility

Ensure that you have completed the initial tasks described in *page 5-8* before running this utility.

To run the Firmware Flash Utility:

1. Insert the *Trend Micro Solutions CD for Network VirusWall 2500*, select the Network VirusWall Firmware Flash Utility, and then click **Launch**.

The Firmware Flash Utility main console appears and automatically searches for connected Network VirusWall devices.

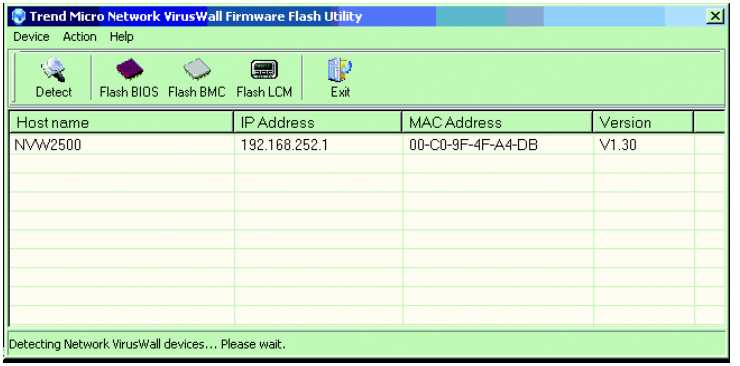


FIGURE 5-1. The Firmware Flash Utility main console with detected Network VirusWall device

2. If the utility has not yet detected the Network VirusWall device, click **Detect** on the toolbar menu. The utility detects the Network VirusWall device connected to the computer and lists it in the detection table.
3. Click the first row to select the detected device from the detection table.
4. Click one of the following buttons to flash the corresponding firmware:
   - **Flash BIOS**
   - **Flash BMC**

     Updating the BMC firmware disrupts the LAN connection temporarily. This disruption happens if the utility runs while the Network VirusWall device is still connected to the LAN. To prevent this disruption from happening, disconnect the Network VirusWall device from its LAN connection before entering rescue mode.

     WARNING! *If the BMC update is unsuccessful, using the Firmware Flash Utility, will no longer work. Contact Trend Micro support if this issue occurs.*

   - **Flash LCM**

The Flash screen appears.

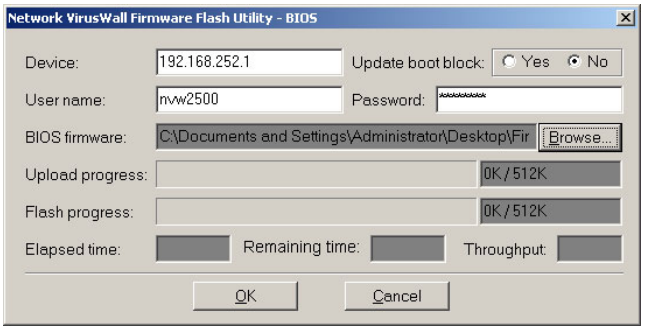


FIGURE 5-2. Sample BIOS dialog box

5. On the Flash dialog box, perform the following:

Note: The "Device" field value corresponds to the fixed Network VirusWall device IP in rescue mode.

---

a. Select **Yes** for **Update Boot Block**.

This option is only applicable when flashing the BIOS.

WARNING! *If a power loss interrupts the BIOS boot block update, BIOS will no longer be able to operate. See the Known Issues list below for more information.*

---

b. Type the following user name and password in the corresponding fields:

User name: `nvw2500`

Password: `qZTSpdum`

Note: These values are the default fixed values and the system cannot accept any changes to them.

---

c. Type or click **Browse** to determine the location of the target firmware.

d. Click **OK**.

e. On the warning message that displays, click **OK** to continue and start the Firmware Flash Utility process.

WARNING! *During the Firmware Flash Utility process, do not turn off, reset, or modify any device settings.*

The Firmware Flash Utility console displays the progress and informs you of a successful firmware flash.

While refreshing the settings, Network VirusWall enables failopen and allows network traffic to pass through the device. However, there is approximately 30 seconds of downtime when the Network VirusWall ports are disconnected from the network. After NVW refreshes the settings, it establishes the network connection.

Note: After successfully flashing the BIOS or BMC firmware, the Network VirusWall device shuts down. On the other hand, after successfully flashing the LCM firmware, the device remains powered on.

Refer to the next section for post-installation configuration.

After Running Firmware Flash Utility

Perform the applicable tasks from the following list after running the Firmware Flash Utility:

- Disconnect the Ethernet cable connecting the computer and Network VirusWall device
- Restore the original interface setup (for example, reconnect the port 5 failover pair connecting the Primary and Secondary devices)
- Restart the Network VirusWall device manually after flashing the LCM firmware

  To do so, press the **RESET** button on the front panel of the device.
- Power on the Network VirusWall device after flashing the BIOS or BMC firmware

Troubleshooting

The section covers the following troubleshooting topics:

To help troubleshoot a Network VirusWall issue:

- Use the Network VirusWall System Log viewer (see *page 4-26*)
- Access and view the system information via the Preconfiguration console > **System Information** menu (see *page 4-23*)
- Access and view the system log information via the Preconfiguration console > **System Tasks** > **View System Logs** option (see *page 4-24*)
- View the BMC logs (or H/W logs) from the LCD module (see *page 4-25*)

Hardware Issues

#	ISSUE	CORRECTIVE ACTION
1	LEDs do not illuminate	Verify secure power cable and network cable connections (see *Network VirusWall 2500 Getting Started Guide* for more information). If the error persists, there may be a hardware problem. Contact your vendor.
2	Unable to access the Preconfiguration console	Verify secure console port connections and terminal communications software settings (refer to the *Getting Started Guide* > *Preconfiguring Network VirusWall Using the Preconfiguration Console*).
3	Unable to change settings with the LCD module panel	To change settings with the LCD module panel, you must first press and hold down the <ENTER> button . If a problem with any LCD module buttons persist, there may be a hardware problem. Contact your vendor.
4	Failopen does not work when the speed of the EXT connection and the INT connection are different.	Enable auto-negotiation for the devices connected to the Ethernet cables.

TABLE 5-2. Troubleshooting Network VirusWall 2500 hardware issues

Configuration Issues

#	ISSUE	CORRECTIVE ACTION
ISSUES WITH CONTROL MANAGER		
1	Network VirusWall is unable to register with the Control Manager server	Check all network connections and ensure you have correctly performed preconfiguration (refer to the *Getting Started Guide* > *Preconfiguring Network VirusWall* section for more information). If the OS on which Control Manager 3.0 resides is 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 problem, 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.
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 problem, 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 problem persists and Network VirusWall is in a multiple VLAN environment, ensure that the Network VirusWall IP address is bound to the correct VLAN ID (refer to the *Getting Started Guide* > *Understanding and Testing the Network VirusWall Deployment* section for an example).

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
3	Communication between the Network VirusWall agent 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 (see the *Control Manager Getting Started Guide* and online help for more information on the Communicator scheduler).
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 updating 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.
5	Network VirusWall is unable to communicate with Vulnerability Assessment (VA)	Ensure that VA is activated (see the *Control Manager Getting Started Guide*) and the Control Manager server is accessible. Verify that the Control Manager Web server port is correct. This port is configured during Control Manager installation (see *Configuring Device and System Settings* on page 2-27).

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
6	Vulnerability Assessment (VA) settings are set to block, but Network VirusWall does not block vulnerable clients	To remedy this problem *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 problem *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 Preconfiguration console and press <ENTER> or until you press on the control panel.
8	Blocked clients are not able to access Damage Cleanup Services (DCS) to issue a cleanup request	Ensure that DCS is activated (see the *Control Manager Getting Started Guide*) and enabled (see *Configuring Real-time Scan Options* on page 2-7).
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. Remove the Network VirusWall device (see the *Control Manager Getting Started Guide* and online help for information on adding and removing products).

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
10	In Failover mode, when active NVW crashes, the standby NVW cannot take over and register to TMCM successfully.	Issue can occur if standby NVW lacks some files that registration needs. Active NVW generates those files after registering to TMCM and must synchronize them with standby NVW. 1. Configure an NVW device as primary NVW and then register it to TMCM properly. (See the NVW *Getting Started Guide*, Preconfiguration chapter for detailed instructions.) The primary NVW will serve as the active NVW after registering to TMCM. 2. Configure a second NVW device as "secondary" to pair with the "primary" NVW. (See the NVW *Getting Started Guide*, Preconfiguration chapter for detailed instructions.) The primary NVW synchronizes data to the secondary NVW device, which serves as the "standby" device.
11	Network VirusWall may not be able to register to the Control Manager server after NVW is upgraded from version 1.5 to version 1.8.	1. Make sure that the TMCM 3.0 Release Build 1417 is installed. Do the following to verify that the build is installed: a. Log on to the TMCM management console. b. Click **About** in the upper-right menu. The **About Trend Micro Control Manager** screen appears. The following information is part of the Trend Micro Control Manager Product Version 3.0 information that is shown: `Version: 3.0 (build 1417)` 2. Install the `CM30_MergeProfile_EN` tool for Merge Profile. a. Download the `CM30_MergeProfile_EN` tool (from http://solutionfile.trendmicro.com/SolutionFile/24197/en/mergeprofile.zip) and extract the `CM30_MergeProfile_EN.exe` file to the folder where TMCM server is installed. b. Run the `CM30_MergeProfile_EN.exe` file. A dialog box confirming the success of the installation appears.

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
ISSUES WITH QUARANTINING AND BLOCKING CLIENTS		
12	Network VirusWall is not quarantining clients whose packets are infected	Check your scan options settings (see *Configuring Real-time Scan Options* on page 2-7). Network VirusWall quarantines a maximum of 4096 clients and drops all network traffic from additional clients (over 4096) whose packets are infected. Reconsider your deployment plan to take into consideration the number of clients on the Protected Network.
13	Network VirusWall continues to block Yahoo! Messenger on clients after Outbreak Prevention Policies blocking has been lifted	On the blocked client, open a Web browser and surf to the Yahoo! homepage: www.yahoo.com. Press the "mail" icon. A screen shows that the Yahoo! ID is locked. Follow the directions on the screen to unlock the ID.
14	Clients violating Policy Enforcement are still able to use MSN Messenger even though **MSN Messenger** is selected under **TCP Services to Block**	MSN Messenger uses HTTP and HTTPS services. Select **WWW** and **Secure HTTP** on the **Block TCP and UDP services** screen (see *Configuring TCP and UDP Services To Block* on page 2-14 for more information).
15	Network VirusWall continues to identify clients as vulnerable and blocks them even though the machine has been released from blocking	There may be a communication problem between Network VirusWall and the Control Manager server. By default, Network VirusWall blocks vulnerable clients. Check to ensure that Network VirusWall is registered with the Control Manager server.
16	A client that is blocked by VA policy is unable to access the Windows Update component	Set the gateway IP in the System Settings screen of the Control Manager console for NVW (see *Configuring System Settings* on page 2-27).

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
17	A client that was blocked because it does not have the latest Windows patch remains blocked even after running Windows Update.	Connect to "Microsoft Security Bulletin Search" (http://www.microsoft.com/technet/security/current.aspx) and search for the vulnerability name (for example, MS01-059) shown in the blocking page. Download that specific patch and install it on the blocked client.
18	No page (or a blank page) displays when client tries to access Windows Update.	Try to refresh current page, or close it and reconnect to the Windows Update site. If doing so still does not solve the problem, use another computer and connect to http://support.microsoft.com and search for your problem.
ISSUES WITH ENFORCING POLICIES		
19	When downloading Windows or Office updates, sometimes the update is unexpectedly interrupted by the display of a Pending page and the update process restarts from the beginning.	On the **Policy Enforcement** > **Advanced Settings** screen, disable **Blocking Policy for Pending Clients.**
20	Network VirusWall Policy Enforcement does detect client information	If the client IP addresses and the Network VirusWall IP address are not on the same subnet and there is no routing device to route network traffic, Network VirusWall cannot detect client information. Consider the design of your network configuration regarding subnets and the placement of routing devices.
21	Clients blocked due to violating Policy Enforcement are unable to redirect their browsers to the redirect site	This problem occurs if the client is attempting to access a proxy server located on the segment of the network connected to the **EXT** port. Add the redirect URL to your Web browser's Proxy Setting Exceptions List (see your Web browser's help for more information). Otherwise, consider redesigning your network so that the proxy server is located on the Protected Network (the segment of the network connected to the **INT** port).

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
22	Clients blocked because Vulnerability Assessment assessed them as vulnerable are unable to start a vulnerability re-assessment.	Same as above.
23	Administrator cannot remove some clients on the Network VirusWall Policy Violations Summary screen from the exception list	If a client's IP address is included in a range of IP addresses added to the exception list for Network VirusWall Policy Enforcement, you cannot release the client machine by clicking **Remove from exception lists** on the **Network VirusWall Policy Violations Summary** screen. Reconfigure the exception list so that the clients you want to release are not included (see *Creating Exception Lists* on page 2-22 for more information).
24	Network VirusWall Policy Enforcement does not correctly identify incompliant clients	An HTTP proxy server located between Network VirusWall and clients on the Protected Network may prevent Network VirusWall from correctly identifying client status. Reconsider your deployment plan to take into consideration proxy servers on the Protected Network. **Note:** If a SYN flood attack with fake source IP address occurs on your network, Network VirusWall Policy Enforcement may not be able to detect the status of clients on the Protected Network.
25	IP addresses of printers on the network appear on security violations summary lists	Network VirusWall may identify network printers as clients. Add the IP addresses of these printers to the exception lists for Network VirusWall Policy Enforcement and Network Outbreak monitor.
26	Netware servers running Trend Micro ServerProtect on the network are judged as unidentifiable clients in policy enforcement	Network VirusWall does not recognize Netware servers. Add the IP addresses of these servers to the exception lists for Network VirusWall Policy Enforcement and Network Outbreak monitor.

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
27	Network VirusWall is unable to implement Outbreak Prevention Policies to block client ports	If a client routes its traffic through a proxy server, the machine actually sends packets to the proxy using a proxy port; the proxy is responsible for actual packet delivery. Unless the proxy itself is within the Protected Network, Network VirusWall does not block the client traffic.
OTHER ISSUES		
28	Clients are unable to access the update source for component updates	If there is a proxy server on your network, ensure that your proxy settings are correct (see *page 3-12*). If you want quarantined or blocked clients to access the update source, add the IP address of the update source to the safe sites exception list (see *Creating Exception Lists* on page 2-22).
29	Network Outbreak Monitor is identifying normal network activity as suspicious	The Network Outbreak Monitor settings are too sensitive for the amount of traffic on your network. Consider increasing the **Protected network traffic volume** setting and lowering the **Monitor sensitivity** (see *Configuring Policy Enforcement Settings* on page 2-12).
30	Network VirusWall is either unable to obtain, or gets incorrect, DNS server information	This occurs if the DHCP server that assigns the Network VirusWall IP address does not specify a DNS server. Confirm your network DHCP and DNS server settings are correct (see *Configuring Device and System Settings* on page 2-27).
31	Third-party vulnerability scanners are not detecting certain vulnerabilities	Network VirusWall is not compatible with some vulnerability scanners and may render them unable to detect NIMDA-related vulnerabilities. Tentatively disable Real-time network virus scan or set the scan option to pass while other vulnerability scanners on your network are performing vulnerability scans.
32	Exporting the configuration file displays garbage characters	This is a known issue. The garbage characters do not cause any adverse effects on the exported configuration file.
33	The Control Manager event log query result displays *WARNING: unexpected IO-API C, please mail to linux-smp@vger.kernel.org*	Network VirusWall generates the following event log whenever it starts up: WARNING: unexpected IO-API C, please mail to linux-smp@vger.kernel.org This is a known issue. However, the message does not mean a system error during Network VirusWall start up.

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
34	When a NAT device resides between Control Manager server and EXT port of NVW, if NVW uses dynamic IP to register to CM, the network administrator may need to change port forwarding settings each time.	Set Network VirusWall by static IP.
35	When a NAT is between CM server and EXT port of NVW, TMCM/Vulnerability Assessment cannot actively check the vulnerability status for clients manually or automatically.	When the client is blocked by Vulnerability Assessment (VA), user can run the Manual Assessment Tool (ActiveX module of VA) from the clients.
36	When a NAT is between CM server and EXT port of NVW, TMCM/Damage Cleanup Services cannot actively deploy the DCE/DCT to clients manually or automatically.	When the client is quarantined by Network Virus Scan, user can run the Manual Cleanup Tool (ActiveX module of DCS) from the client.

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

#	ISSUE	CORRECTIVE ACTION
37	When exporting NVW configuration from Preconfiguration console, console displays error message: "Unable to create configuration file: compress error", and returns user to main menu without prompting for exporting.	One possible cause is when a user has installed a fiber card and is attempting to change the operation mode from pure copper to pure fiber connection at a time when NVW is not in contact with the Control Manager server. (User may have forgotten to connect the fiber cable, or there may be some other network connectivity. problem.) NVW cannot export its configuration if it is not connected to Control Manager. **Solution:** Ensure that all cables are connected properly and that NVW can communicate with Control Manager, and try again.
38	User cannot see popup messages on a Windows XP SP2 client.	There are two possible causes: 1. By default in Windows XP SP2 the "Messenger" service is disabled. To resolve the problem, enable the "Messenger" service. 2. The necessary ports in the Windows Firewall Exceptions list may be disabled. NVW2500 uses ports TPC 139 and UDP 137 to deliver popup messages through Windows Messenger. In Windows XP SP2 by default the firewall is enabled. However, if at any point a user clicks **Restore Defaults**, the necessary Exceptions ports become disabled. **To re-enable the necessary ports:** a. Go to **Windows Security Center** > **Windows Firewall** > **Exceptions** > **File and Printer Sharing**. b. Check to see if "TCP 139 Port" and "UDP 137 Port " are selected in the Windows Firewall Exceptions. If these ports are not selected, select them now. c. Click **Save** to save your change.

TABLE 5-3. Troubleshooting Network VirusWall 2500 configuration issues

Control Manager and Network VirusWall Communication Issues

Tip: Refer to the *Getting Started Guide* > *Control Manager and Network VirusWall Integration* for additional information.

When troubleshooting the Control Manager and Network VirusWall integration and communication:

- Check the Network Time Protocol (NTP) used (see *page 5-26*)
- Determine whether the Control Manager server uses multiple network interface cards (NICs) (see *page 5-26*)
- Check whether the network connection between the Control Manager server and Network VirusWall device is present (see *page 5-27*)
- Check whether the VLAN name was modified (see *page 5-27*)
- Determine whether the Network VirusWall IP was modified (see *page 5-28*)

Check the Network Time Protocol (NTP) in Use

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

If your Control Manager server does not have ADS, you must disable Windows NTP and enable Control Manager NTP because Windows NTP does not work without ADS. To enable Control Manager NTP, start the **Trend Micro Network Time Protocol** from the Windows Services panel.

If your Control Manager server has ADS, use Windows NTP. Network VirusWall can work (and register) with Control Manager successfully in this situation.

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 Network VirusWall Device Is Present

From the Control Manager server, ping the Network VirusWall device to check whether the two products can establish a connection.

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, NVW cannot deliver the 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 two products cannot establish a connection. 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 1-36* 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.

To resolve this issue, restart the Network VirusWall by pressing the RESET button on the front panel. This enables the device to re-register to the Control Manager server.

Tip: When configuring the VLAN settings, decide on the final VLAN name and ID. Standardizing the VLAN naming convention in your organization helps prevent frequent modification, which can lead to this issue.

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.

Client Issues

After a successful deployment, Network VirusWall should be able to filter network packets directed to clients in the protected network. When troubleshooting client-related issues, consider the following checklists:

- Understand how the Network VirusWall interfaces implements the network protection features

  Table 5-4 defines how Network VirusWall applies its features, as well as the 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 5-4. How INT and EXT apply Network VirusWall and Control Manager features

* See Legend on *page 5-29* 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

Tip: Refer to the *Getting Started Guide > Understanding the Network VirusWall Interfaces* section for details.

- Check whether the Trend Micro Personal Firewall feature is running

  Network VirusWall is unable to apply Policy Enforcement to OfficeScan or PC-cillin-based clients with Trend Micro Personal Firewall feature enabled. Verify that the Personal Firewall service is not running in the background to prevent this issue from occurring.

  Note: Even if you have disabled Personal Firewall in the product's user interface, the service may still be working in the background. Refer to the OfficeScan or PC-cillin documentation for detailed instructions on how to disable Personal Firewall and its service.

- Determine the connection between the Network VirusWall and L2/L3 device, and clients available in the network

  A broken or disconnected network cable may prevent Network VirusWall or L2/L3 device from reaching the client. Consequently, this prevents Network VirusWall from detecting unwanted packets or vulnerabilities originating from the disconnected client. If such client is able to reconnect to the network, its vulnerabilities may cause potential network outbreaks.

  Tip: Create an IT policy that will require users in your organization to always keep track and apply the latest security patches and components to his/her computers. This helps prevent vulnerabilities from occurring in Network VirusWall clients.

See *page 1-24* for additional discussion about Network VirusWall clients.

Frequently Asked Questions (FAQs)

This section answers the following common questions about Network VirusWall:

- Does Network VirusWall 2500 support gigabit interface speed?
- Does this release support fiber-based networks?
- Where does Network VirusWall store its logs, and how can I access them?
- What are the functions of the seven (7) Network VirusWall ports?
- Can I connect more than one Network VirusWall 2500 devices or stack them together to improve throughput?
- If a malfunction prevents Network VirusWall 2500 from operating, will the Protected Network traffic still be able to flow?
- Can I PING Network VirusWall 2500 to see if it is on the network?
- Can I enable SSL Web browser security with Damage Cleanup Services (DCS) and Vulnerability Assessment (VA)?
- Is Network VirusWall compatible with Network Address Translation (NAT)?
- Can Network VirusWall block Instant Messaging services that utilize a proxy server?
- Can the length of the network cable affect the failopen functionality of Network VirusWall?
- Do I need to register the Standby device in a failover pair?
- Can I register a Network VirusWall device to more than one Control Manager server?
- Does Network VirusWall support spanning tree protocol (STP)?
- Will modifying the duplex settings from half-duplex to full duplex have any adverse effect on Network VirusWall?
- Will changing the Network VirusWall IP address prevent it from communicating with the Control Manager server?
- Why does a Network VirusWall device appear as two (2) managed products in the Product Directory?
- If Network VirusWall is bridging an 802.1Q trunk with multiple VLANS, is it able to do policy enforcement on all VLANS or only on the one to which the NVW IP address is bound?
- What happens if one of the Network VirusWall devices fails to function?

- Can I perform extensive Network VirusWall configuration settings locally through the Network VirusWall front panel?
- How can I back up the Network VirusWall 2500 configuration before modifying the firmware?
- Why is it that I cannot find any preconfiguration information in the Administrator's Guide?
- Will the Windows NTP service prevent NVW from registering to the Control Manager server?
- How does NVW 2500 handle trunked gigabit lines?
- Will Network VirusWall bridge all non-IP traffic?
- Can I import and export the Network VirusWall configuration?
- Aside from ports 1 to 5, does Network VirusWall refer to its interfaces using another naming convention?
- Can I create a new account to access the Preconfiguration console?
- Does Network VirusWall support networks with an Etherchannel solution?
- Can I use another Control Manager account to register and manage Network VirusWall devices?
- Do I need to send an email to `linux-smp@vger.kernel.org` whenever I receive the following message?

  WARNING: unexpected IO-API C, please mail to linux-smp@vger.kernel.org
- Why does a client that has a vulnerability show up as "risk free"?
- I have enabled Windows Update and Office Update, but my client is still blocked by an antivirus policy when trying to connect to the Windows/Office Update site. Why is that?
- Does Network VirusWall 2500 support a load-balancing configuration?
- Does Network VirusWall support Spanning Tree Protocol /Rapid Spanning Tree Protocol?
- Can Network VirusWall 2500 be installed on Cisco EtherChannel links?

Does Network VirusWall 2500 support gigabit interface speed?

Yes. Network VirusWall 2500 has five (5) user-configurable Copper Gigabit LAN ports referred to as ports 1 to 5 and designated as the INT, EXT, or FAILOVER port depending on the Operation Mode. It also supports fiber-optic ports.

Does this release support fiber-based networks?

Yes, Network VirusWall supports fiber-based networks. The device ships with one of two physical configurations: one duplex multimode fiber-optic card installed and no fiber-optic card installed. For more information on the supported fiber-optic media cards, refer to the *Network VirusWall 2500 Getting Started Guide > Choosing a Fiber-Optic Media Connector for Fiber-based Networks* section.

Where does Network VirusWall store its logs, and how can I access them?

Network VirusWall 2500 only uses a 256 IDE Disk On Module (DOM) flash disk for storage. Consequently, it does not have memory space available to store log files. Network VirusWall sends its normal logs to the Control Manager server. Alternatively, NVW can send system logs (which also include debug information) to any computer on the network. See *Configuring Device and System Settings* on page 2-27 and *Understanding Logs* on page 4-4 for more information.

What are the functions of the seven (7) Network VirusWall ports?

The Network VirusWall 2500 device comes with up to seven network ports. Depending on the Operation Mode, these ports can be set as the INT, EXT, or FAILOVER port. Refer to the *Getting Started Guide > Understanding the Network VirusWall Interfaces* for details.

Can I connect more than one Network VirusWall 2500 devices or stack them together to improve throughput?

Yes. With the new Network VirusWall 2500 platform, Network VirusWall achieves high availability (HA) using redundant devices. See *High Availability* on page 1-34 for details.

If a malfunction prevents Network VirusWall 2500 from operating, will the Protected Network traffic still be able to flow?

Network VirusWall 2500 has a built-in LAN bypass (failover) feature. This feature helps ensure that in the event of a hardware or software failure, all network traffic will pass freely through the device. During a failover period, NVW will not block traffic from the Protected Network. Failover is enabled when **Port Grouping** or **Port Redundancy** operating mode is set. See *Failopen* on page 1-36 for details.

Can I PING Network VirusWall 2500 to see if it is on the network?

Network VirusWall 2500 has a built-in firewall that protects it from attacks. You can configure Network VirusWall to prevent or allow ICMP packets requests from reaching the device. See *page 2-38* for instructions on how to allow ICMP requests.

Can I enable SSL Web browser security with Damage Cleanup Services (DCS) and Vulnerability Assessment (VA)?

Although the Control Manager server supports SSL security, Network VirusWall does not when communicating with Vulnerability Assessment. See the Control Manager Getting Started Guide for more information.

Is Network VirusWall compatible with Network Address Translation (NAT)?

If Network VirusWall 2500 is on a different network segment from the Control Manager server and a NAT device is between them, you must do the following to enable Network VirusWall to register with the Control Manager server:

1. Enable IP port forwarding on the NAT device.
2. Enable NAT mode on the Control Manager server.

Tip: Refer to the *Network VirusWall 2500 Getting Started Guide > Control Manager and Network VirusWall Integration* for detailed instructions.

Can Network VirusWall block Instant Messaging services that utilize a proxy server?

Network VirusWall 2500 is unable to block Instant Messaging (IM) services if those services utilize a proxy server.

Can the length of the network cable affect the failopen functionality of Network VirusWall?

Yes. The network cable connecting Network VirusWall and other devices must not be longer than 100 meters (328 feet). Otherwise, Network VirusWall failopen will not work.

Do I need to register the Standby device to a Control Manager server?

No, there is need to register the Standby device to a Control Manager server. You only need to register the Active device of the failover pair. See *page 1-35* for details.

Can I register a Network VirusWall device to more than one Control Manager server?

No, you cannot register a device to more than one Control Manager server. Register a device to only one Control Manager server. Register a device to a Control Manager server through the Network VirusWall preconfiguration **Device Settings** option.

Does Network VirusWall support spanning tree protocol (STP)?

Yes. However, ensure that STP is enabled in your L2 or L3 device. Otherwise, if one of the links fails in a port redundancy deployment, Network VirusWall is unable to determine the path to take through the spanning tree protocol (STP). Refer to the *Getting Started Guide* for details.

Will modifying the duplex settings from half-duplex to full-duplex have any adverse effect on Network VirusWall?

Modifying the interface speed and duplex mode setting from the Preconfiguration console causes Network VirusWall to refresh its settings and perform a *network refresh*. During this time, the network connection is disconnected for a short time.

Will changing the Network VirusWall IP address prevent it from communicating with the Control Manager server?

Yes, changing the Network VirusWall IP address through the Preconfiguration console Device Settings menu will temporary disconnect the Network VirusWall device from the Control Manager server while it refreshes its network settings. See

Determine Whether the Network VirusWall IP address, VLAN settings, or Operation Mode Was Modified on page 5-28 for details.

Why does a Network VirusWall device appear as two (2) managed products in the Product Directory?

Modifying the Operation Mode causes the Network VirusWall to re-register to the Control Manager server. This result to two (2) managed product icons listed in the Product Directory.

Delete the managed product with the abnormal status ( ) using Directory Manager. Doing so will not adversely affect control of the product via the new managed product.

Refer to the *Getting Started Guide* > *Troubleshooting* > *Configuration Issues* for additional information.

If Network VirusWall is bridging an 802.1Q trunk with multiple VLANS, is it able to do policy enforcement on all VLANs or only on the one to which the NVW IP address is bound?

Policy enforcement can work on all VLANs, provided you set all VLAN tags in the **VLAN Settings**. Set all the VLAN tags in the Preconfiguration console > **VLAN Settings** menu.

What happens if one of the Network VirusWall devices fails to function?

When a Network VirusWall device encounters a hardware or system error that prevents it from filtering network packets, Network VirusWall will implement its LAN bypass function. This is true, however, only when failopen is enabled. Implementing the **Port Grouping** or **Port Redundancy** Operation Mode allows you to enable failopen. See *page 1-37* for failopen considerations.

Can I perform extensive Network VirusWall configuration settings locally through the Network VirusWall front panel?

No, you cannot perform extensive configuration settings using the device itself.

The Network VirusWall front panel interface only allows you to configure the **Device Settings**, view System Information and hardware logs, reset the device, and turn on

the UID LED. In addition, the back panel interface has a serial port that allows you to complete the preconfiguration tasks.

To perform extensive configuration changes, use a Control Manager management console.

See Table 1-1, “Comparison of the Network VirusWall management tools,” on page 1-11 for a comparison of the available Network VirusWall management tools.

How can I back up the Network VirusWall 2500 configuration before modifying the firmware?

Use the Preconfiguration console > **System Tasks** > **Export Configuration File** option to back up the Network VirusWall configuration. In addition, the Preconfiguration console > **System Tasks** > **Import Configuration File** option allows you to import settings from an identical Network VirusWall devices.

Why is it that I cannot find any preconfiguration information in the Administrator’s Guide?

This Administrator’s Guide includes instructions and details that you will need when configuring and administering a device from the available management tools. For preconfiguration instructions, please refer to the printed or PDF *Getting Started Guide*.

Will the Windows NTP service prevent Network VirusWall from registering to the Control Manager server?

If your Control Manager server does not have ADS, you must disable Windows NTP and enable Control Manager NTP because Windows NTP does not work without ADS. To enable Control Manager NTP, start the **Trend Micro Network Time Protocol** from the Windows Services panel.

If your Control Manager server has ADS, use Windows NTP. Network VirusWall can work (and register) with Control Manager successfully in this situation.

How does Network VirusWall 2500 handle trunked gigabit lines?

This release of Network VirusWall does not support port channel configurations.

Does Network VirusWall bridge all non-IP traffic?

Yes, Network VirusWall bridges all non-IP traffic.

Can I import and export the Network VirusWall configuration?

Yes, the Network VirusWall 2500 Preconfiguration console > **System Tasks** option allows you to import and export the Network VirusWall configuration when accessed through a HyperTerminal session. However, importing or exporting the Network VirusWall configuration is not possible when using Minicom (available in Linux servers).

Note: Export configuration files only for backup purposes. This feature is not intended for copying the configuration of one NVW device to another.

Aside from *ports 1* to *5*, does Network VirusWall refer to its interfaces using another naming convention?

Yes. Table 5-3, "NVW 2500 system names for seven ports," on page 5-38 shows the actual system names of each Network VirusWall port:

FIGURE 5-3. NVW 2500 system names for seven ports

See *Seven (7) User-definable LAN Ports* on page 1-32 for details.

Can I create a new account to access the Preconfiguration console?

The `admin` and `monitor` accounts are the predefined Preconfiguration console accounts. The `admin` account allows full access of the Preconfiguration console. Alternatively, the `monitor` account allows you to read the current settings in the Preconfiguration console menus. See *Table 2-1* for details.

You can modify the passwords for these accounts. However, you cannot create additional accounts to access the Preconfiguration console.

Does Network VirusWall support networks with an Etherchannel solution?

As of this release, Network VirusWall 2500 does not support networks with an Etherchannel solution.

Can I use another Control Manager account to register and manage Network VirusWall devices?

You can use any Control Manager account in lieu of the root account User ID. However, Trend Micro recommends using the root account because if you delete the User ID specified during agent installation, you will have difficulty managing the agent.

Do I need to send an email to linux-smp@vger.kernel.org whenever I receive the following message?

WARNING: unexpected IO-API C, please mail to linux-smp@vger.kernel.org

Network VirusWall generates the following event log during startup:

> *WARNING: unexpected IO-API C, please mail to linux-smp@vger.kernel.org*

This is a known issue and does not require sending an email to `linux-smp@vger.kernel.org`. The message does not represent a system error or any other error.

Why does a client that has a vulnerability show up as "risk free"?

When an unsupported client does a Windows update, although it may be risk free before downloading a specific update, the update itself could conceivably introduce a vulnerability. If a client is re-assessed before downloading such an update, it may

have its "risk free" status recorded in Control Manager even though it acquires a vulnerability later. Such a client would not be blocked by Vulnerability Assessment.

I have enabled Windows Update and Office Update, but my client is still blocked by an antivirus policy when trying to connect to the Windows/Office Update site. Why is that?

The feature that allows access to Windows Update and Office Update only applies to violations of vulnerability assessment policy. If a machine is blocked by an antivirus policy (for example, Pattern/Engine Out-of-Date or No Antivirus Software Installed) it will not be able to access the Windows/Office Update site.

Does Network VirusWall 2500 support a load-balancing configuration?

No, it does not.

Does Network VirusWall support Spanning Tree Protocol /Rapid Spanning Tree Protocol?

No. Network VirusWall is designed to be a transparent L2 device in the network, so it will pass those packets through.

Can Network VirusWall 2500 be installed on Cisco EtherChannel links?

No, Network VirusWall 2500 is not designed for that use.

Chapter 6

Getting Support

Trend Micro is committed to providing service and support that exceeds our user's expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try to find a solution to your problem:

- **Check your documentation**– the Administrator's Guide, Getting Started Guide, and Online Help provide comprehensive information about Network VirusWall. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site**– our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit

  `http://kb.trendmicro.com/solutions/solutionSearch.asp`

Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- Email support

  `support@trendmicro.com`

- Help database- configuring the product and parameter-specific tips
- Readme- late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base- technical information procedures provided by the Support team:

  `http://kb.trendmicro.com/solutions/solutionSearch.asp`

- Product updates and patches

  `http://www.trendmicro.com/download/`

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- Network VirusWall model and image (firmware) version (if possible)
- Operation Mode
- Interface speed and duplex mode setting
- Exact text of the error message, if any
- Steps to reproduce the problem

Sending Infected Files to Trend Micro

You can send viruses, infected files, Trojan horse programs, and other malware to Trend Micro. More specifically, if you have a file that you think is some kind of malware but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following Web address:
`subwiz.trendmicro.com`

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any viruses it may contain and return the cleaned file to you within 48 hours.

Introducing TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of hundreds of engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Lake Forest, CA, ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 — one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

```
www.trendmicro.com/en/security/trendlabs/overview.htm
```

Other Useful Resources

Trend Micro offers a host of services via its Web site, www.trendmicro.com.

Internet-based tools and services include:

- Virus Map—monitors virus incidents around the world
- HouseCall™ — Trend Micro online virus scanner
- Virus risk assessment—the Trend Micro online virus protection assessment program for corporate networks

Appendix A

Device Specifications

This appendix provides general system and hardware specifications for Network VirusWall 2500.

COMPONENT	SPECIFICATIONS
CHASSIS DIMENSION WITH BEZEL (L X W X H)	24.43" x 16.73" x 1.70" (620.6 x 425 x 42.4mm)
CARTON DIMENSION (L X W X H)	33.54" x 22.24" x 8.27" (852 x 565 x 210mm)
SYSTEM WEIGHT	9Kg
SYSTEM WEIGHT WITH PACKAGE AND ACCESSORY BOX	16.54Kg [3.9Kg (packing) + 9Kg (system) + 1Kg (accessory box) + 2.64Kg (rails)]
PROCESSOR	Nocona 800 2.8 GHz X 2
LAN	Intel 82546 NIC X 2 Intel 82545 NIC X 1
MEMORY	DDR-II 400 DIMM X 4
SATA	Serial ATA 1.5Gbps channel X 2
SERIAL PORT	Serial port X 1 (9 Pin Header)
USB	USB 2.0 port X 2

TABLE A-1. Network VirusWall 2500 device specifications

COMPONENT	SPECIFICATIONS
UID FUNCTION (REAR SIDE)	Indicator LED X 1
UID FUNCTION (FRONT SIDE)	UID button X 1 indicator LED X 1
BMC FUNCTION	Hitachi 2168
COOLING FAN	Dual motor system fan X 5
BIOS ROM	ST M50FW040
FORM FACTOR	10.5 x 13.5'' PCB
S25 PCI-X RISER BOARD FEATURE	PCI-X 64bit Slot X 2
LCD MODULE FEATURE	• LCD display for server message • 5 control panel buttons for display control • LED display for server status • UID button • System reset button

TABLE A-1. Network VirusWall 2500 device specifications

Appendix B

BMC Logs

The LCD module displays the following hardware-related logs:

Temperature Logs

BMC EVENT LOG	DESCRIPTION
CPU 1 Temp Upper Critical - going high Assert	**CPU 1 and CPU 2**– the temperature reading relating to the first and second processor **DIMM**– the temperature reading relating to dual in-line memory module **VRD 1 and VRD 2**– the temperature reading relating to onboard processors **Ambient temperature**– the temperature reading relating to all sides of the device **Lower Critical**– the lower critical temperature threshold (cold) **Upper Critical**– the upper critical temperature threshold (hot) **going low Assert**– the temperature has started to decrease **going high Assert**– the temperature has started to increase
CPU 1 Temp Upper Non-critical - going high Assert	
CPU 1 Temp Upper Critical - going low Deassert CPU 1 Temp Upper Non-critical - going low Deassert	
CPU 2 Temp Upper Critical - going high Assert	
CPU 2 Temp Upper Non-critical - going high Assert	
CPU 2 Temp Upper Critical - going low Deassert CPU 2 Temp Upper Non-critical - going low Deassert	
DIMM Temp Upper Critical - going high Assert	
DIMM Temp Upper Non-critical - going high Assert	
DIMM Temp Upper Critical - going low Deassert DIMM Temp Upper Non-critical - going low Deassert	
VRD 1 Temp Upper Critical - going high Assert	
VRD 1 Temp Upper Non-critical - going high Assert	
VRD 1 Temp Upper Critical - going low Deassert VRD 1 Temp Upper Non-critical - going low Deassert	
VRD 2 Temp Upper Critical - going high Assert	
VRD 2 Temp Upper Non-critical - going high Assert	
VRD 2 Temp Upper Critical - going low Deassert VRD 2 Temp Upper Non-critical - going low Deassert	
Ambient Temp Upper Critical - going high Assert	

TABLE B-1. Temperature logs

BMC EVENT LOG	DESCRIPTION
Ambient Temp Upper Non-critical - going high Assert	See descriptions on *page B-2*.
Ambient Temp Upper Critical - going low Deassert Ambient Temp Upper Non-critical - going low Deassert	

TABLE B-1. Temperature logs

Processor Temperature Logs

BMC EVENT LOG	DESCRIPTION
Processor 1 Hot Assert	**Processor 1 and Processor 2**– refers to the first and second device processor **Hot Assert**– the internal CPU temperature is starting to get too hot **Deassert**– the internal CPU temperature has stopped to get too hot
Processor 1 Hot Deassert	
Processor 2 Hot Assert	
Processor 2 Hot Deassert	

TABLE B-2. Processor Temperature Logs

Voltage Logs

BMC EVENT LOG	DESCRIPTION
Lan AB 1.5V STB Lower Critical - going low Assert Lan AB 1.5V STB Upper Critical - going high Assert	**Lan AB**– ports1 and 2 **Lan CD**– ports 3 and 4 **LAN E**– port 5 **CPU1**– processor 1 **CPU2**– processor 2 **Vcc**– main power **#V STB**– refers to the voltage input **Lower Critical**– the lower critical voltage threshold **Upper Critical**– the upper critical voltage threshold **going low Assert**– the voltage has started to decrease **going high Assert**– the voltage has started to increase **going high Deassert**– the voltage has started to stop from increasing **going low Deassert**– the voltage has started to stop from decreasing
Lan AB 1.5V STB Lower Non-critical - going low Assert Lan AB 1.5V STB Upper Non-critical - going high Assert	
Lan AB 1.5V STB Lower Non-critical - going high Deassert Lan AB 1.5V STB Lower Critical - going high Deassert Lan AB 1.5V STB Upper Non-critical - going low Deassert Lan AB 1.5V STB Upper Critical - going low Deassert	
Lan CD 1.5V STB Lower Critical - going low Assert Lan CD 1.5V STB Upper Critical - going high Assert	
Lan CD 1.5V STB Lower Non-critical - going low Assert Lan CD 1.5V STB Upper Non-critical - going high Assert	
Lan CD 1.5V STB Lower Non-critical - going high Deassert Lan CD 1.5V STB Lower Critical - going high Deassert Lan CD 1.5V STB Upper Non-critical - going low Deassert Lan CD 1.5V STB Upper Critical - going low Deassert	
Lan E 1.5V STB Lower Critical - going low Assert Lan E 1.5V STB Upper Critical - going high Assert	
Lan E 1.5V STB Lower Non-critical - going low Assert Lan E 1.5V STB Upper Non-critical - going high Assert	
Lan E 1.5V STB Lower Non-critical - going high Deassert Lan E 1.5V STB Lower Critical - going high Deassert Lan E 1.5V STB Upper Non-critical - going low Deassert Lan E 1.5V STB Upper Critical - going low Deassert	
CPU1 12V Lower Critical - going low Assert CPU1 12V Upper Critical - going high Assert	
CPU1 12V Lower Non-critical - going low Assert CPU1 12V Upper Non-critical - going high Assert	
CPU1 12V Lower Non-critical - going high Deassert CPU1 12V Lower Critical - going high Deassert CPU1 12V Upper Non-critical - going low Deassert CPU1 12V Upper Critical - going low Deassert	

TABLE B-3. Voltage logs

BMC EVENT LOG	DESCRIPTION
CPU2 12V Lower Critical - going low Assert CPU2 12V Upper Critical - going high Assert	See descriptions on *page B-5*.
CPU2 12V Lower Non-critical - going low Assert CPU2 12V Upper Non-critical - going high Assert	
CPU2 12V Lower Non-critical - going high Deassert CPU2 12V Lower Critical - going high Deassert CPU2 12V Upper Non-critical - going low Deassert CPU2 12V Upper Critical - going low Deassert	
Vcc 3.3V Lower Critical - going low Assert Vcc 3.3V Upper Critical - going high Assert	
Vcc 3.3V Lower Non-critical - going low Assert Vcc 3.3V Upper Non-critical - going high Assert	
Vcc 3.3V Lower Non-critical - going high Deassert Vcc 3.3V Lower Critical - going high Deassert Vcc 3.3V Upper Non-critical - going low Deassert Vcc 3.3V Upper Critical - going low Deassert	
Vcc 5V Lower Critical - going low Assert Vcc 5V Upper Critical - going high Assert	
Vcc 5V Lower Non-critical - going low Assert Vcc 5V Upper Non-critical - going high Assert	
Vcc 5V Lower Non-critical - going high Deassert Vcc 5V Lower Critical - going high Deassert Vcc 5V Upper Non-critical - going low Deassert Vcc 5V Upper Critical - going low Deassert	
Vcc 12V Lower Critical - going low Assert Vcc 12V Upper Critical - going high Assert	
Vcc 12V Lower Non-critical - going low Assert Vcc 12V Upper Non-critical - going high Assert	
Vcc 12V Lower Non-critical - going high Deassert Vcc 12V Lower Critical - going high Deassert Vcc 12V Upper Non-critical - going low Deassert Vcc 12V Upper Critical - going low Deassert	
Vcc 1.5V Lower Critical - going low Assert Vcc 1.5V Upper Critical - going high Assert	
Vcc 1.5V Lower Non-critical - going low Assert Vcc 1.5V Upper Non-critical - going high Assert	

TABLE B-3. Voltage logs

BMC EVENT LOG	DESCRIPTION
Vcc 1.5V Lower Non-critical - going high Deassert Vcc 1.5V Lower Critical - going high Deassert Vcc 1.5V Upper Non-critical - going low Deassert Vcc 1.5V Upper Critical - going low Deassert	See descriptions on *page B-5*.
DDR 1.8V Lower Critical - going low Assert DDR 1.8V Upper Critical - going high Assert	
DDR 1.8V Lower Non-critical - going low Assert DDR 1.8V Upper Non-critical - going high Assert	
DDR 1.8V Lower Non-critical - going high Deassert DDR 1.8V Lower Critical - going high Deassert DDR 1.8V Upper Non-critical - going low Deassert DDR 1.8V Upper Critical - going low Deassert	
Vtt GTL 1.2V Lower Critical - going low Assert Vtt GTL 1.2V Upper Critical - going high Assert	
Vtt GTL 1.2V Lower Non-critical - going low Assert Vtt GTL 1.2V Upper Non-critical - going high Assert	
Vtt GTL 1.2V Lower Non-critical - going high Deassert Vtt GTL 1.2V Lower Critical - going high Deassert Vtt GTL 1.2V Upper Non-critical - going low Deassert Vtt GTL 1.2V Upper Critical - going low Deassert	
Vcc -12V Lower Critical - going low Assert Vcc -12V Upper Critical - going high Assert	
Vcc -12V Lower Non-critical - going low Assert Vcc -12V Upper Non-critical - going high Assert	
Vcc -12V Lower Non-critical - going high Deassert Vcc -12V Lower Critical - going high Deassert Vcc -12V Upper Non-critical - going low Deassert Vcc -12V Upper Critical - going low Deassert	
Vcc 3.3V STB Lower Critical - going low Assert Vcc 3.3V STB Upper Critical - going high Assert	
Vcc 3.3V STB Lower Non-critical - going low Assert Vcc 3.3V STB Upper Non-critical - going high Assert	
Vcc 3.3V STB Lower Non-critical - going high Deassert Vcc 3.3V STB Lower Critical - going high Deassert Vcc 3.3V STB Upper Non-critical - going low Deassert Vcc 3.3V STB Upper Critical - going low Deassert	

TABLE B-3. Voltage logs

CPU VRD Logs

BMC LOG	DESCRIPTION
CPU VRD PWRGD Assert	**VRD**– Voltage Regulator Down. It provides an adjustment of voltage from the main to the CPU power **CPU VRD PWRGD**– indicates a working VRD **Assert**– the VRD voltage current status is OK **Deassert**– the VRD voltage current status fails
CPU VRD PWRGD Deassert	

TABLE B-4. CPU VRD logs

Vcore Logs

BMC LOG	DESCRIPTION
Vcore 1 Assert	Vcore 1– the core voltage for CPU1 Vcore 2– the core voltage for CPU2 Assert– the core voltage current status is OK Deassert– the core voltage current status fails
Vcore 1 Deassert	
Vcore 2 Assert	
Vcore 2 Deassert	

TABLE B-5. Vcore logs

System Fan Logs

BMC LOG	DESCRIPTION
System Fan 1A not present or stop	**System Fan #A/#B**– # indicates the system fan number and A/B indicates the system fan location (front or rear position) **Not present or stop**– the system fan is either missing or stopped **Lower Critical**– the lower critical fan speed threshold **Upper Critical**– the upper critical fan speed threshold **going low Assert**– the fan has started to slow down the speed **going high Assert**– the fan has started to increase speed
System Fan 1A Lower Critical - going low Assert	
System Fan 1A Upper Critical - going high Assert	
System Fan 1A Lower Critical - going high Deassert System Fan 1A Upper Critical - going low Deassert	
System Fan 1B not present or stop	
System Fan 1B Lower Critical - going low Assert	
System Fan 1B Upper Critical - going high Assert	
System Fan 1B Lower Critical - going high Deassert System Fan 1B Upper Critical - going low Deassert	
System Fan 2A not present or stop	
System Fan 2A Lower Critical - going low Assert	
System Fan 2A Upper Critical - going high Assert	
System Fan 2A Lower Critical - going high Deassert System Fan 2A Upper Critical - going low Deassert	
System Fan 2B not present or stop	
System Fan 2B Lower Critical - going low Assert	
System Fan 2B Upper Critical - going high Assert	

TABLE B-6. System fan logs

BMC LOG	DESCRIPTION
System Fan 2B Lower Critical - going high Deassert System Fan 2B Upper Critical - going low Deassert	See descriptions on *page B-9*.
System Fan 3A not present or stop	
System Fan 3A Lower Critical - going low Assert	
System Fan 3A Upper Critical - going high Assert	
System Fan 3A Lower Critical - going high Deassert System Fan 3A Upper Critical - going low Deassert	
System Fan 3B not present or stop	
System Fan 3B Lower Critical - going low Assert	
System Fan 3B Upper Critical - going high Assert	
System Fan 3B Lower Critical - going high Deassert System Fan 3B Upper Critical - going low Deassert	
System Fan 4A not present or stop	
System Fan 4A Lower Critical - going low Assert	
System Fan 4A Upper Critical - going high Assert	
System Fan 4A Lower Critical - going high Deassert System Fan 4A Upper Critical - going low Deassert	
System Fan 4B not present or stop	
System Fan 4B Lower Critical - going low Assert	
System Fan 4B Upper Critical - going high Assert	

TABLE B-6. System fan logs

BMC LOG	DESCRIPTION
System Fan 4B Lower Critical - going high Deassert System Fan 4B Upper Critical - going low Deassert	See descriptions on *page B-9*.
System Fan 5A not present or stop	
System Fan 5A Lower Critical - going low Assert	
System Fan 5A Upper Critical - going high Assert	
System Fan 5A Lower Critical - going high Deassert System Fan 5A Upper Critical - going low Deassert	
System Fan 5B not present or stop	
System Fan 5B Lower Critical - going low Assert	
System Fan 5B Upper Critical - going high Assert	
System Fan 5B Lower Critical - going high Deassert System Fan 5B Upper Critical - going low Deassert	

TABLE B-6. System fan logs

Platform Security Violation Attempt Logs

BMC LOG	DESCRIPTION
Auth. Security Front Panel Lockout Violation Assert	The system has detected a security violation.
Auth. Security Out-of-band password Violation Assert	A remote connection is trying to access and compromise the system with an invalid password.

TABLE 2-7. Platform security violation attempt logs

IERR, Thermal Trip, and Processor Availability Logs

BMC LOG	DESCRIPTION
Processor x IERR Assert	**Processor x IERR**– indicates a failure or error in the CPU self-test **Processor x Thermal Trip**– indicates that the internal CPU temperature is too hot (this state is more critical than processor temperature logs, see *page B-4*.) **Assert**– sensor is present **Deassert**– sensor is absent
Processor x Thermal Trip Assert	
Processor x Processor present detected Assert Processor x Processor present detected Deassert	

TABLE B-8. IERR, thermal trip, and processor availability logs

System Power and AC Power State Logs

BMC LOG	DESCRIPTION
Power Off/Power Down Assert	**Assert**– Network VirusWall is powered off **Deassert**– Network VirusWall is powering on
Power Off/Power Down Deassert	
Power Unit AC lost Assert	
Power Unit AC lost Deassert	

TABLE B-9. Power state logs

Memory Logs

BMC LOG	DESCRIPTION
DIMM x Correctable ECC Assert	Memory: single-bit error A single bit error occurred and can be recovered
DIMM x Uncorrectable ECC Assert	Memory: multi-bit error A multi-bit error occurred and cannot be recoverable
DIMM Presence detected Deassert	Indicates that the memory module is absent

TABLE B-10. Memory logs

POST Error Logs

BMC LOG	DESCRIPTION
POST Error channel 2 timer error Assert	Channel 2 timer error.
POST Error CMOS battery failure Assert	CMOS battery failure.
POST Error CMOS system options not set Assert	CMOS system options not set.
POST Error CMOS checksum error Assert	CMOS checksum error.
POST Error CMOS time not set Assert	CMOS time not set.
POST Error PCI memory conflict Assert	PCI memory conflict.
POST Error PCI I/O conflict Assert	PCI I/O conflict.
POST Error PCI IRQ conflict Assert	PCI IRQ conflict.
POST Error static resource conflict Assert	Static resource conflict.
POST Error NVRAM checksum error, NVRAM cleared Assert	NVRAM checksum error, NVRAM cleared.
POST Error system board device resource conflict Assert	System board device resource conflict.
POST Error NVRAM data invalid, NVRAM cleared Assert	NVRAM data invalid, NVRAM cleared.
POST Error Memory read/write test fail Assert	Memory conflict

TABLE B-11. Power-On Self Test (POST) error logs

Event Recording Logs

BMC LOG	DESCRIPTION
Eventlog All event logging disable Assert	Event logging disabled.
Eventlog All event logging disable Deassert	Event logging enabled.

TABLE B-12. Event recording logs

Various Logs

BMC LOG	DESCRIPTION
Critical INT Software NMI Assert	A non-maskable interrupt (NMI) error occurred.
Critical INT PCI PERR Assert	A parity (PERR) error occurred.
Critical INT PCI SERR Assert	A system (SERR) error occurred.
Button Power button pressed Assert Button Reset button pressed Assert Button Power button pressed Deassert Button Reset button pressed Deassert	Indicates the Power button activity.
Boot Error No bootable media Assert	Network VirusWall cannot boot. There is no boot component.
Watchdog Timer expired, status only Assert	Timer expired– the component for detecting the watchdog timer timeouts Basic Input/Output System (BIOS)/Power-On Self Test (POST), OS, Server Management Software (SMS/OS) timeout Hard Reset Assert– the device will restart Power Down Assert– the device will turn off Power Cycle Assert– the device will power off and then power on after a short time delay
Watchdog Hard Reset Assert	
Watchdog Power Down Assert	
Watchdog Power Cycle Assert	
Watchdog Timer expired, status only Assert	
Watchdog Hard Reset Assert	
Watchdog Power Down Assert	
Watchdog Power Cycle Assert	
Watchdog Timer expired, status only Assert	
Watchdog Hard Reset Assert	
Watchdog Power Down Assert	
Watchdog Power Cycle Assert	
System Panic Assert	Indicates a system kernel panic.
HDD Smart Failure Assert	Indicates hard disk drive SMART feature failure.

TABLE B-13. Logs generated by various components

Appendix C

Network VirusWall 1200 and 2500 Feature Comparison

The following table presents a comparison of Trend Micro Network VirusWall 1200 and 2500 devices.

FEATURE	1200	2500
HARDWARE SPECIFICATIONS		
Form Factor	1U Small Size	1U Middle Size
Interface	FE x 2	GE x 5
Processor	1	2
Memory	256MB	IGB
Storage	CF/128MB	DOM/256MB
Hardware status monitor	No	Yes
CONNECTIVITY		
Number of LAN port (on board)	2/Copper	5/Copper, 0-2 fiber
Ability to add-on Fiber Optic LAN Adapter	No	Yes
Ability to add-on Gigabit Ethernet Adapter	No	Yes
Concurrent connections (in-line scan)	68,000	1,000,000

TABLE C-1. Network VirusWall 1200 and 2500 Feature Comparison

FEATURE	1200	2500
Current users (Policy Enforcement)	256	4,096
Virtual segment	802.1Q	802.1Q
Port segment	n/a	Port Grouping
Fault tolerance, high availability solutions	Failopen (LAN bypass)	Failopen Failover Port and device redundancy
ANTIVIRUS AND MANAGEMENT FEATURES		
Antivirus defenses	Real-time network packet filtering Virus Outbreak monitoring Policy Enforcement (Antivirus, Vulnerability Assessment, Threats, Outbreak Prevention)	Real-time network packet filtering Virus Outbreak monitoring Policy Enforcement (Antivirus, Vulnerability Assessment, Threats, Outbreak Prevention)
Reporting	Threat and outbreak	Threat and outbreak
Management	Control Manager management console Preconfiguration console LCM console	Control Manager management console Preconfiguration console LCM console
PHYSICAL SPECIFICATIONS		
Height	1.75in	1.70in
Depth	12.6in	24.43in
Width	16.8in	16.73in
Weight	4.5Kg	9Kg
Operating temperature	32°–104°F (0°–40°C)	41°–113°F (5°–45°C)
Storage temperature	-4°–167°F (-20°–75°C)	-40°–158°F (-40°–70°C)

TABLE C-1. Network VirusWall 1200 and 2500 Feature Comparison

The following references provide additional Network VirusWall 2500 information:

- The Network VirusWall *Getting Started Guide* > *Getting Started* > *Package Contents* section provides dimensions, weight, power requirements, and environmental specifications
- The chapter *Understanding Network VirusWall* starting on page 1-1 includes discussions about Network VirusWall architecture, components, antivirus technology, and Network VirusWall 2500 overview
- The topic *Restoring Default Settings* starting on page 2-41 includes details on the factory default settings and hardware specifications

Glossary

Tip: For a faster glossary search when viewing this appendix online, use the Acrobat Reader's **Find** option to search for a term.

A **B** **C** **D** **E** **F** G **H** **I**

J K **L** **M** **N** **O** **P** Q **R**

S **T** **U** **V** **W** X Y Z

A

Top

Active
In a failover solution, it refers to the device that is currently in use.

ActiveUpdate
ActiveUpdate server. The Trend Micro server hosting the Network VirusWall components. The ActiveUpdate server can be set as the update source.

B

Top

Baseboard management controller
Short for BMC. It is a microcontroller responsible for the Intelligent Platform Management Interface (IPMI).

BMC logs
Short for Board Management Control logs. These type of logs report critical hardware status and error.

BPDU
Short for **b**ridge **p**rotocol **d**ata **u**nit. BPDUs are data messages that travel across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where the sender intended it to go. BPDU messages go back and forth across bridges to detect loops in a network topology. The protocol then removes the loops by shutting down selected bridge interfaces and places redundant switch ports in a backup, or blocked, state.

C

Top

Client
Refers to an IP address, which Network VirusWall scans for unwanted packets.

D

Top

Device role
A device identifies its role after assigning the original attribute setting (Primary or Secondary).

DHCP
Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DIMM
Short for dual in-line memory module, a small circuit board that holds memory chips. A single in-line memory module (SIMM) has a 32-bit path to the memory chips whereas a DIMM has 64-bit

path. Because the Pentium processor requires a 64-bit path to memory, you need to install SIMMs two at a time. With DIMMs, you can install memory one DIMM at a time.

Directory Manager
Allows you to customize the Product Directory organization to suit your administration model needs.

E

Top

Ethernet
One of the most widely implemented local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10Mbps, 100Mbps (100Base-T or Fast Ethernet), or 1,000Mbps or 1Gbps.

External network
See public network (see *Page -5*).

External port
Also referred to as EXT. The Network VirusWall port/interface that connects to the public network.

F

Top

Failopen
A fault-tolerance solution allows the Network VirusWall device to continue to pass traffic in an event when a software or hardware failure occurs within the device.

Failover
A backup operational mode in which a standby device assumes the functions of a NVW device when the Active device becomes unavailable through either failure or scheduled down time.

Fault tolerance
The ability of a system to respond gracefully to an unexpected hardware or software failure.

H

Top

HA
See high availability.

High availability
Refers to the ability of a Network VirusWall device to be continuously operational for a desirably long length of time. Administrators usually measure availability relative to "100% operational" or "never failing."

I

Top

IETF
Short for Internet Engineering Task Force, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

IGMP
Short for Internet Group Management Protocol. It is the standard protocol for IP multicasting in the Internet.

The purpose of IGMP is to establish host memberships in particular multicast groups on a single network. Its mechanism allows a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group.

Image
Refers to the Network VirusWall firmware or program file.

Intelligent Platform Management Interface
Short for IPMI. IPMI is an interface or gateway between the host system (that is, server management software) and the periphery devices.
Internal port

Also referred to as INT. The Network VirusWall port/interface that connects to the protected network.

Internet Control Message Protocol
Short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

IP multicasting
Sending out data to distributed servers on the MBone. For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic, which requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source, transmitting just one set of packets for all the destinations.

IPsec
Short for IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec is a widely used method of implementing Virtual Private Networks (VPNs).

L Top

L2 devices
Short for layer 2 devices. These devices refer to hardware devices connected to the Data Link layer of the OSI model. Switches are examples of L2 devices.

L3 devices
Short for layer 3 devices. These devices refer to hardware devices connected to the Network layer of the OSI model. Routers are examples of L3 devices.

L2TP
Short for Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).

LAN
Short for local area network. A computer network that spans a relatively small area. Most LANs reside in a single building or a group of buildings.

LCD module
See LCM console.

LCD
Short for Liquid Crystal Display. A 5x7 dot display LCD on the Network VirusWall front panel that is capable if displaying 2x16 character messages.

LCM console
Also referred to as the LCD module. It is composed of the LCD and Control Panel, which is located on the Network VirusWall front panel. This allows basic Network VirusWall device settings configuration. See *Table 1-1, "Comparison of the Network VirusWall management tools," on page 11*.

M Top

Managed product
Refers to any software or hardware application managed by a Control Manager server.

Management console
Short for Control Manager management console. A Web-based console published via IIS from the Control Manager server, which administrators use to administer managed products and devices registered to Control Manager.

MBone
Short for Multicast Backbone. MBone is an extension to the Internet to support IP multicasting -- two-way transmission of data between multiple sites.

Mesh network
A mesh network is a network that employs one of two connection arrangements: full mesh topology or partial mesh topology. In the full mesh topology, each node connects directly to each of the others. In the partial mesh topology, nodes e connect to only some, not all, of the other nodes.

MIB
Management Information Base (MIB). Groups

the SNMP information organized in the form of objects. Each object is an essential data about a particular aspect of the managed Network VirusWall device, such as the number of packets received or memory utilization statistics.

N

Top

NAT
See Network Address Translation.

Network Address Translation
Also known as NAT. The term refers to an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT device located where the LAN meets the Internet makes all necessary IP address translations.

Network Interface Card
Also known as NIC. The term refers to an expansion board inserted into a computer so the computer can connect to a network. Most NICs work only with a particular type of network, protocol, and media, although some can serve multiple networks.

Network segment
A section of a network that falls within the bounds of bridges, routers, or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN. If segmented correctly, most network traffic remains within a single segment, enjoying the full 10 Mbps bandwidth. Hubs and switches connect each segment to the rest of the LAN.

Network Time Protocol
Also known to NTP. The term refers to an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

Network virus
The type of threat that Network VirusWall devices can detect, eliminate, and contain.

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the known malware programs, such as worms, are actually network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

NIC
See network interface card.

NMS
In the SNMP management architecture, one or more computers on the network act as a network management station (NMS) and poll the managed devices to gather information about their performance and status.

Non-switch-back
A mode that prevents the Standby device to automatically switch-back to the Active device once it becomes online. The network administrator manually switches the link to the Active device.

NTKD
Refers to scan engine used by products running on Windows NT, 2000, or XP machines.Operation Mode

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

NTP
See Network Time Protocol.

O

Top

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

Short for Open System Interconnection model. This model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. Network VirusWall works with L2 and L3 devices.

P

Top

Port-based VLAN
A type of virtual LAN setup wherein each physical switch port has an access list specifying membership in a set of VLANs.
Network VirusWall supports port-based VLAN through Port Grouping Operation Mode.

PPPoE
Short for Point-to-Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device, or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

PPTP
Short for Point-to-Point Tunneling Protocol, a new technology for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum.

Preconfiguration console
The console used to preconfigure a Network VirusWall device.

Preconfiguring a Network VirusWall device allows you to modify the basic Network VirusWall default settings, perform network configuration, and set the Operation Mode. See *Table 1-1, "Comparison of the Network VirusWall management tools," on page 11*.

Primary port
Describes the Network VirusWall ports used to establish redundant connections to the protected and public network.

Primary
Primary device. Identifies the original attribute of a device to support the failover switchback mode. The Primary Network VirusWall device is automatically assigned the Active role.

Product Directory
The Product Directory is a logical grouping of managed products accessible from the Control Manager management console.

Protected network
Also referred to as INT. It refers to a network segment separated and protected by Network VirusWall. It is the part of the network connected to the Network VirusWall internal port(s).

Public network
Refers to the part of the network that the external port(s) connect to. This term is strictly relative to a specific Network VirusWall device.

R

Top

Redundant device
Describes Network VirusWall devices whose purpose is to back up primary devices in case they fail.

Redundant ports
Describes Network VirusWall ports used when the primary port fails.

S

Top

Scan engine
Trend Micro Network Virus Scan Engine. The antivirus component that filters network packets for threats and other viruses.

Secondary
Identifies the original attribute of a device to sup-

port the failover switchback mode. The Secondary Network VirusWall device automatically takes on the Standby role.

Segment
A section of a network that is bounded by bridges, routers, or switches.

SNMP agent
A software module in a managed device, which communicates with the NMS.

SNMP
Simple Network Management Protocol (SNMP) is set of communications specifications for managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

Spanning Port
Spanning Port indicates the ability to copy traffic from all the ports to a single port but also typically disallows bi-directional traffic on the port. In the case of Cisco, SPAN stands for Switch Port ANalyzer.

Spanning tree protocol
Also known as STP. This terms refers to a link management protocol that is part of the IEEE 802.1 standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing undesirable loops in a network. Multiple active paths between stations create such loops, which occur when there are alternate routes between hosts. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

Standby
In a failover solution, it refers to the device that is idle and waiting switch as the Active device once the Active device fails.

STP
See spanning tree protocol.

Switch
A device that filters and forwards packets between LAN segments.

Switch-back
A mode that allows the Standby device to automatically switch-back to the Active device once it becomes online.

Switched Ethernet LANs
Ethernet networks that use switches to join segments.

Switched LANs
LANs that use switches to join segments.

T Top

Tagged VLAN
A type of VLAN that uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag can indicate VLAN and QoS (Quality of Service) priority identification.

TCP
Short for Transmission Control Protocol, and pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks.

Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and guarantees packet delivery in the same order in which the originating machine sends them.

Traps
Notifications sent by managed devices to the NMS when certain events occur, such as a shutdown or authentication error.

U Top

UDP
Short for User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. Its primary use is for broadcasting messages over a network.

V

Top

Virus pattern file
Trend Micro Network Virus Pattern (NVP). The antivirus component that provides rules and signatures to detect network threats and other vulnerabilities. Network VirusWall uses both the Network Virus Scan Engine and Network Virus Pattern to detect known threats.

VLAN
Short for virtual LAN. A network consisting of clients that are not on the same segment of a Local Area Network (LAN) but behave as if they are.

VPN
Short for virtual private network, a network that makes use of public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanism to ensure only authorized users can access the network and unauthorized users cannot intercept information.

VxD
Refers to scan engine used by Trend Micro products running on Windows 95, 98, or ME machines.

W

Top

Worms
A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email.

Index

O

P