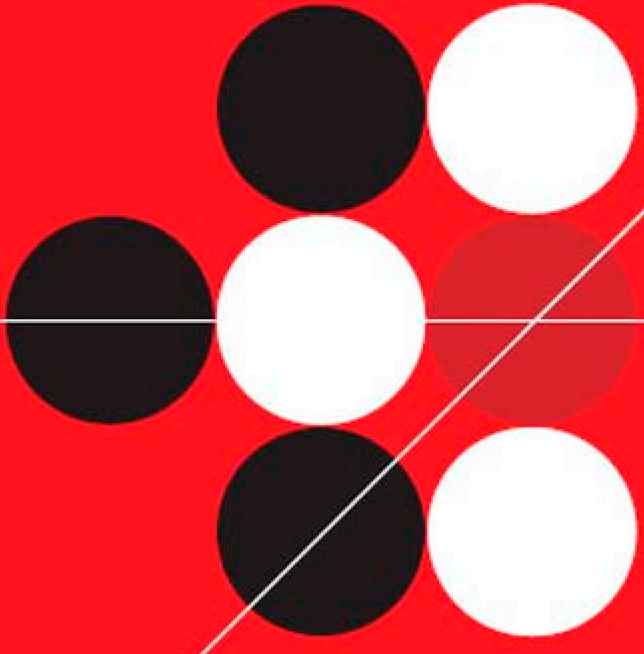
TREND MICRO™

Network VirusWall™ 1200

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. NVEM12104/41110

Release Date: November 2004

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

The Administrator’s Guide for Network VirusWall 1200 is intended to discuss the features of Network VirusWall and to provide instructions for preconfiguration, installation, and administration of this product for your production environment. Read it prior to configuring the software.

For technical support, please refer to *Technical Support, Troubleshooting and FAQs* on page 9-1 for technical support information and contact details. Detailed information about how to use specific features within the software are 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

Preface

Chapter 1: Introducing Network VirusWall 1200

Chapter 2: Deploying Network VirusWall 1200

Chapter 3: Performing Preconfiguration

Chapter 5: Configuring Basic Settings—continued

Chapter 6: Viewing and Analyzing Antivirus Information

Chapter 7: Performing Administrative Tasks

Chapter 8: SNMP and VLAN

Chapter 8: SNMP and VLAN—continued

Chapter 9: Technical Support, Troubleshooting and FAQs

Appendix A: Device Specifications

Appendix B: Box Contents

Index

Preface

Welcome to the Administrator's Guide for Trend Micro™ Network VirusWall™ 1200. This book contains information about the tasks you need to configure Network VirusWall 1200. 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 a 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* on page x
- *About this Administrator's Guide* on page xi
- *Audience* on page xi
- *Document Conventions* on page xii

Network VirusWall Documentation

The Network VirusWall documentation consists of the following:

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

  The Network VirusWall Online Help is integrated with the Control Manager Online Help. 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 1200 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 pre-configuration, port configuration, and post-installation configuration.

- Administrator’s Guide (AG)– PDF documentation that is accessible from the Trend Micro Solutions CD for Network VirusWall 1200 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 1200, see *Introducing Network VirusWall 1200* on page 1-1
- Procedures to configure and administer Network VirusWall from the applicable management tools, see *Configuring System Settings* on page 4-6
- Procedures to update Network VirusWall components, see *Updating Components* on page 5-19
- Troubleshooting tips for issues encountered during device administration, which includes debug and error logs interpretation, see *Technical Support, Troubleshooting and FAQs*
- Guidelines to obtain more information, see *Technical Support, Troubleshooting and FAQs* on page 9-1

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

- *Device Specifications*
- *Box Contents*

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 PREFACE-1. Conventions used in the Network VirusWall documentation

Chapter 1

Introducing Network VirusWall 1200

This chapter introduces Network VirusWall 1200 and provides an overview of its technology, capabilities, and hardware connections.

The topics discussed in this chapter include:

What Is 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 and is managed by Trend Micro Control Manager™ 3.0.

Network VirusWall 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.

Understanding the Protected Network

The principle function of Network VirusWall is to separate a segment of the network from the rest of the LAN. Throughout this document, this separated segment is referred to as the *Protected Network*.

Network VirusWall creates the Protected Network to accomplish these tasks:

- Scan network traffic to and from 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 Technology

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 *Understanding the Protected Network* on page 1-2). Network VirusWall is especially designed 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 Viruses* on page 1-3 for more information on viruses, including network viruses.

Understanding Viruses

Tens of thousands of viruses are known to exist, with more being created 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.

Computer viruses can be roughly classified 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, can be referred to as 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.

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

New viruses are written and released via different media every day, especially the Internet. To 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. Also configure the Control Manager Event Center to trigger an outbreak alert notification message when Network Outbreak Monitor criteria are met.

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, Vulnerability Assessment, and Trend Micro™ Damage Cleanup Services. See the *Control Manager Getting Started Guide* and online help for detailed information.

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 protocols
- **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

Vulnerability Assessment

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.

Damage Cleanup Services

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 ensure you have the most up-to-date cleanup capabilities.

Hardware and Connections

This section explains the Network VirusWall front and back panel ports, connections, and LEDs. It also provides step-by-step information on connecting the device to your network. See *Box Contents* on page B-1 for a description of all items included in the Network VirusWall box.

See *Connecting to the Network* on page 1-9 for instructions on how to connect the device to your network.

Network VirusWall 1200 Front Panel

The front panel of Network VirusWall 1200 contains a Liquid Crystal Display (LCD) module, panel, ports, and LEDs.

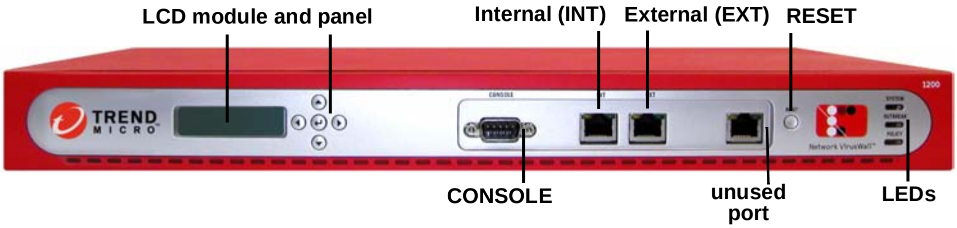


FIGURE 1-1. Front panel.

Element	Description
CONSOLE port	Connects to a computer’s serial port with an RS-232 type connection to perform preconfiguration.
Internal (**INT**) network port	Connects to the Protected Network – the segment of the network that Network VirusWall protects.
External (**EXT**) network port	Connects to the section of the LAN that leads to the public network.
Reserved port (not labeled)	Unused.
RESET button	Resets the device.

TABLE 1-1. Front panel description

LED	LED Color	Description
SYSTEM	Green- steady	Device is operating normally.
	Red- flashing	Device is rebooting.
	Red- steady	Device not ready.
OUTBREAK	Green- steady	Outbreak Prevention Services is not enabled.
	Yellow- flashing	Network Outbreak Monitor detects an abnormal amount of simultaneous network sessions or connections.
	Red- flashing	Outbreak Prevention Services is enabled.
POLICY	Off	Real-time network virus scan and Network VirusWall Policy Enforcement are disabled.
	Green- steady	Real-time network virus scan or Network VirusWall Policy Enforcement are enabled.
	Yellow- flashing	Client(s) on Protected Network violated Antivirus policy enforcement and/or Vulnerability Assessment policies.
	Red- flashing	Network virus detected and client(s) on Protected Network quarantined.
	Red- steady	Antivirus policy enforcement and Vulnerability Assessment not operational due to a memory problem. Network VirusWall drops all network packets. If this LED illuminates, reset Network VirusWall

TABLE 1-2. Front panel LED description

Network VirusWall 1200 Back Panel

The back panel of Network VirusWall 1200 contains a power receptacle, power switch and fan.vent.

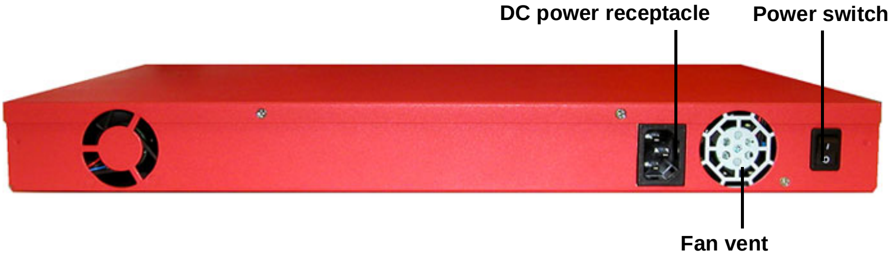


FIGURE 1-2. Back panel

Element	Description
Power switch	Power on and off the device.
Fan vent	Cooling fan for the device.
DC power receptacle	Connects to the included power cord.

TABLE 1-3. Back panel description

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

Connecting to the Network

This section explains how to connect Network VirusWall to your network. For a comprehensive collection of deployment scenarios, see *Deployment Planning Details* on page 2-4.

Note: Ensure Trend Micro Control Manager 3.0 is installed on your network before installing Network VirusWall.

To connect Network VirusWall to your network:

1. Connect one end of a 10/100 Mbps Ethernet cable to the **INT** (Internal) port and the other to the segment of the network that Network VirusWall will protect (the Protected Network).
2. Connect one end of another 10/100 Mbps Ethernet cable to the **EXT** (External) port and the other end to the part of the network that leads to the public network.
3. Connect one end of the power adapter to the **PWR** port and the other end to an electrical outlet.
4. Perform preconfiguration. See *Performing Preconfiguration* on page 3-1 for detailed instructions.

Note: Network VirusWall 1200 can handle only 10/100 Mbps traffic.

Chapter 2

Deploying Network VirusWall 1200

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

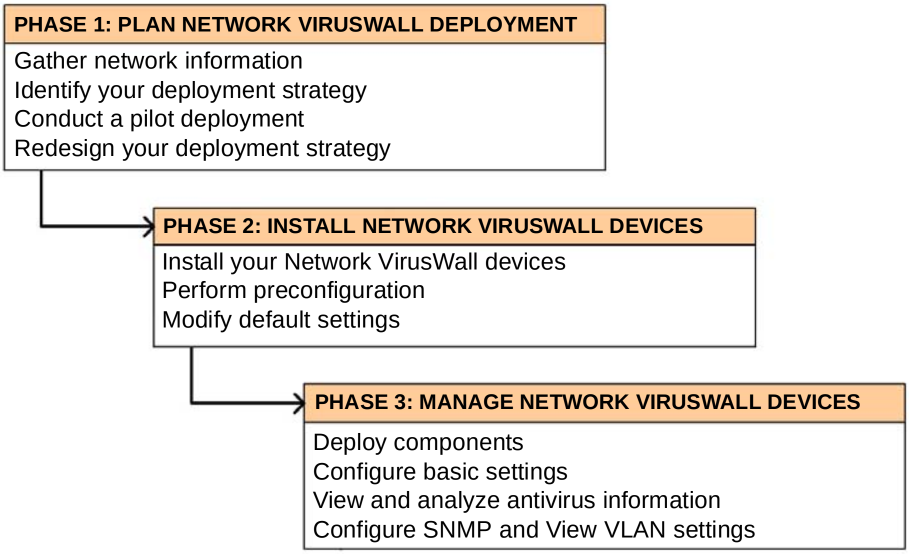
The topics discussed in this chapter include:

Planning for Deployment

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

Overview of Deployment Planning

There are three stages involved in deploying the Network VirusWall device(s).



PHASE 1: PLAN NETWORK VIRUSWALL DEPLOYMENT

Gather network information
Identify your deployment strategy
Conduct a pilot deployment
Redesign your deployment strategy

PHASE 2: INSTALL NETWORK VIRUSWALL DEVICES

Install your Network VirusWall devices
Perform preconfiguration
Modify default settings

PHASE 3: MANAGE NETWORK VIRUSWALL DEVICES

Deploy components
Configure basic settings
View and analyze antivirus information
Configure SNMP and View VLAN settings

Phase 1 Summary

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

- Determine the segments of your network that are in the greatest need of protection
- Plan for network traffic, considering the location of devices critical to your operations such as email, Web, and application servers

- Determine both the number of Network VirusWall devices needed to meet your security needs and their locations on the network
- Conduct a pilot deployment on a test segment of your network
- Redesign your deployment strategy based on the results of the pilot deployment

Phase 2 Summary

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

- Connect the device(s) to your network (see *Hardware and Connections* on page 1-7 for more information)
- Perform preconfiguration on the Network VirusWall device(s) to register the device to the Control Manager server (see *Performing Preconfiguration* on page 3-1 for more information)
- Modify the default settings to create the security policies you want to implement (see *Getting Started with Network VirusWall 1200* on page 4-1 for more information

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

Phase 3 Summary

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

- Deploy Network VirusWall components to ensure the devices have current protection (see *Deploying Network VirusWall Components* on page 4-5)
- Configure basic settings, including scan options, Network Outbreak Monitor, enforcement policies, exception lists, and component updates (see *Configuring Basic Settings* on page 5-1)
- View and analyze antivirus information, including detailed summaries of clients on the Protected Network security logs, and event logs (see *Viewing and Analyzing Antivirus Information* on page 6-1)

- Configure optional SNMP settings and view the VLAN settings you configured during preconfiguration (see *SNMP and VLAN* on page 8-1)

Modify the default settings to create the security policies you want to implement (see *Getting Started with Network VirusWall 1200* on page 4-1 for more information

Deployment Planning Details

This section provides information needed to understand how Network VirusWall can protect your network and details of Phase 1 deployment.

A Basic Network VirusWall Deployment Scenario

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

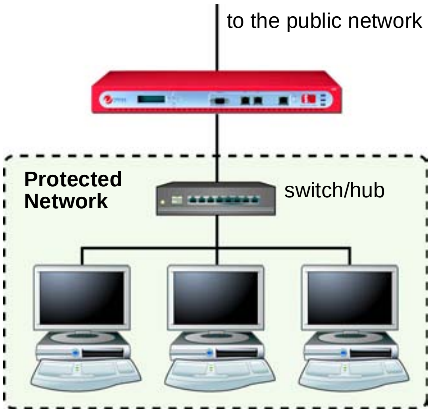


FIGURE 2-1. Basic Network VirusWall deployment scenario

Figure 2-1 on page 2-4 illustrates a basic deployment scenario. An internal switch or hub is connected to the Network VirusWall internal (**INT**) port, creating a Protected

Network segment, while the connection to the external (**EXT**) port leads to the public network. Network VirusWall scans traffic to and from clients on the Protected Network, prevents clients that violate your security policies from gaining access to resources outside of the Protected Network, and isolates the clients in the event of a virus infection.

Identifying What To Protect

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

- Remote clients that access your internal network resources
- Guest clients that temporarily connect to your network
- Key network segments/important network assets, such as places on the network that contain Email, Web, and application servers as well as client machines

Remote Access

Remote clients access internal network resources in the same manner as the clients already on your network and comprise essentially another internal network segment. You must consider whether or not to protect remote clients as you do internal clients.

There are two types of remote clients:

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

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

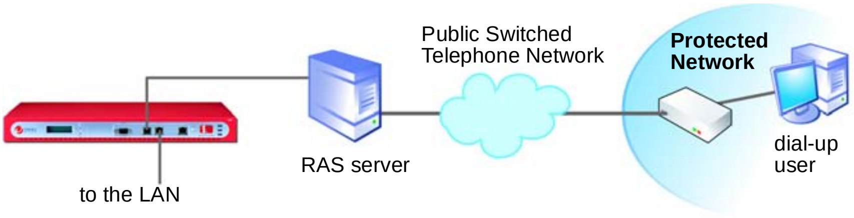


FIGURE 2-2. Dial-up service deployment scenario

Figure 2-2 on page 2-6 illustrates a dialup connection between a home user and an organization's internal network. A RAS server, the point where the dialup connection terminates, is connected to the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the internal network. In this configuration, the home user's VPN connection is considered to be in the Protected Network. Once the home user establishes a connection with the RAS server, it essentially becomes part of the internal network as illustrated in the basic deployment scenario (see Figure 2-1 on page 2-4). The home user accesses both network resources and the Internet in the same way internal clients do.

Table 2-1 provides a summary of recommended Network VirusWall settings for this scenario.

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

TABLE 2-1. Recommended settings for dial-up deployment scenario

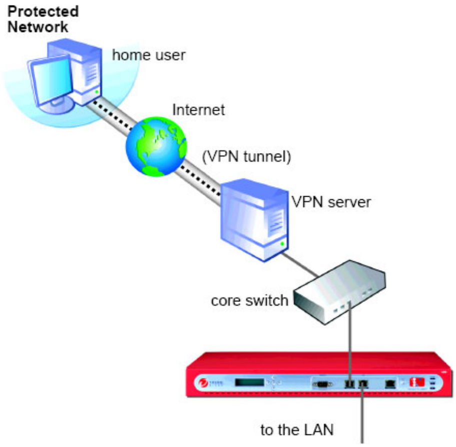


FIGURE 2-3. Client to site VPN deployment scenario

Figure 2-3 on page 2-7 is similar to Figure 2-2 on page 2-6. It illustrates a connection between a home user and an organization’s internal network, only though a VPN server, which is connected to the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the internal network. In this configuration, the home user’s VPN connection is considered to be in the Protected Network and it becomes part of the internal network.

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

The recommended Network VirusWall settings for this scenario are the same as the settings for the dial-up user scenario (see Table 2-1).

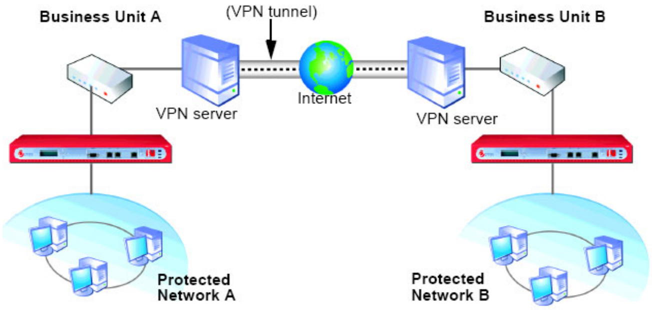


FIGURE 2-4. Site to site VPN deployment scenario

Figure 2-4 on page 2-8 illustrates a VPN connection between two business units. As in the home user scenario (see Figure 2-3 on page 2-7), a VPN server is connected to the external (**EXT**) port of each Network VirusWall device, while the connection to each internal (**INT**) port leads to the internal network.

Guest Clients

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

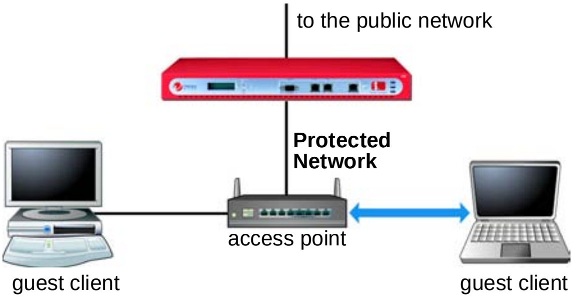


FIGURE 2-5. Guest network deployment scenario

Figure 2-5 on page 2-9 illustrates a segment of an internal network especially for guest clients. A wireless access point, switch, or hub is connected to the Network VirusWall internal (**INT**) port, while the connection to the external (**EXT**) port leads to the public network. This type of topology ensures that Network VirusWall scans all traffic before it leaves the guest network segment and makes isolation of the guest segment possible in the event of a virus outbreak.

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

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

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

Key Network Segments/Important Network Assets

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

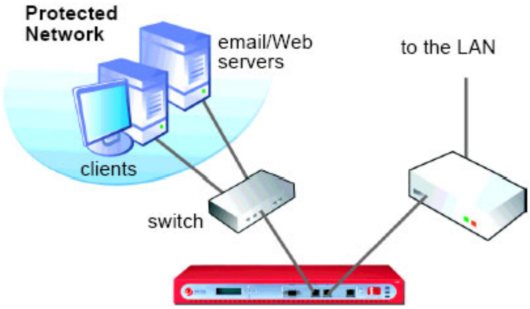


FIGURE 2-6. Key network segments scenario

Figure 2-6 on page 2-10 illustrates a segment of an internal network containing email and Web servers, as well as clients. An internal switch or hub is connected to the Network VirusWall internal (**INT**) port, creating a Protected Network segment, while the connection to the external (**EXT**) port leads to the public network. Installing Network VirusWall in this position adds the benefits of virus scanning and segment isolation in the event of a virus outbreak.

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

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

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

TABLE 2-3. Recommended settings for key network segments deployment scenario

Planning for Network Traffic

The scenario presented in Figure 2-6 on page 2-10 is also a good example of how to plan for network traffic. There is a strategic advantage to positioning Network VirusWall in front of resources that clients access on a frequent and regular basis, such as an email or Web server. Because many viruses make their way onto networks through email attachments and Web browsers, forcing traffic to pass through Network VirusWall significantly reduces the risk of virus infection. Identify other places on your network through which large amounts of traffic pass and consider positioning Network VirusWall at points where it can scan the most amount of traffic.

Determining the Number of Devices To Deploy

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

- **Existing Network topology** – based on your network topology, identify the segments you want Network VirusWall to protect (see *Identifying What To Protect* on page 2-5)
- **Existing network device interfaces** – because Network VirusWall handles 10/100 Mbps Fast Ethernet traffic, identify the network device interfaces that handle the same type of traffic and can therefore connect to Network VirusWall devices

- **Desired effectiveness of protection** – to lower the risk of a virus outbreak spreading, segment several sections of your network with Network VirusWall devices
- **Desired degree of performance** – consider the number of clients and the amount of traffic Network VirusWall can handle (see *Device Specifications* on page A-1)

Conducting a Pilot Deployment

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

Perform the following tasks to conduct a pilot deployment:

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

Choosing a Pilot Site

Choose a pilot site that matches your planned deployment. This includes other devices on your network such as switches and firewalls, other antivirus installations, such as Trend Micro™ OfficeScan™, and the Control Manager 3.0 services you plan to use. Try to simulate the type of topology that would serve as an adequate representation of your production environment.

Creating a Contingency Plan

Trend Micro recommends creating a contingency plan in case there are issues with the installation, operation, or upgrade of Network VirusWall and/or other Control Manager services or components. Consider your networks vulnerabilities and how you can retain a minimum level of security if issues arise.

Deploying and Evaluating Your Pilot

Deploy and evaluate the pilot based on expectations regarding both security enforcement and network performance. Create a list of successes and failures encountered through the pilot process.

Redesigning Your Deployment Strategy

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

Chapter 3

Performing Preconfiguration

This chapter explains how to perform preconfiguration, which is necessary to activate Network VirusWall and perform management functions through the Control Manager management console. Preconfiguration allows you to modify basic Network VirusWall default settings and perform network configuration. After completion of preconfiguration procedures, the Network VirusWall device registers itself as a managed product to the Control Manager server.

The topics discussed in this chapter include:

Preconfiguration Overview

Note: Control Manager 3.0 server must be installed on the network before an administrator can perform preconfiguration.

There are two methods to perform preconfiguration:

- **The terminal interface** – use terminal communications software to configure or view any preconfiguration settings, including passwords, network and Control Manager settings, system logs and VLAN tags (see *Comparison of preconfiguration methods* on page 3-2)
- **The LCD module panel** – use the LCD module panel on the front of the device to configure only Network VirusWall network settings, such as the IP address (see *Using the LCD Module Panel* on page 3-31)

When completed, either method allows Network VirusWall to register to the Control Manager server. For a comparison of these two methods, see Table 3-1.

What you can do	Terminal interface	LCD module panel
Change account passwords	Yes	No
Set Network VirusWall IP address, netmask, Gateway address, and DNS addresses	Yes	Yes
Configure Trend Micro Control Manager public key settings	Yes	Yes
Create and edit Virtual LAN (VLAN) tags	Yes	No
Lock/unlock LCD module panel controls	Yes	No
View system logs	Yes	No
Initialize Network VirusWall to default settings	Yes	No
Reset Network VirusWall	Yes	RESET button on front panel
NAT settings	Yes	No

TABLE 3-1. Comparison of preconfiguration methods

Using the Terminal Interface

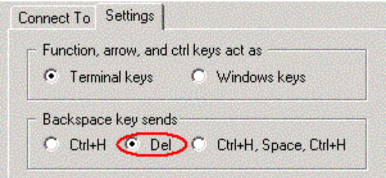
With the terminal interface, you can configure all Network VirusWall preconfiguration settings. If you need only to set the device's IP address, you can use the Network VirusWall LCD module panel to perform preconfiguration (see *Using the LCD Module Panel* on page 3-31).

Note: Changes to Network VirusWall preconfiguration settings will not take effect until you log off the terminal interface. See *Entering Rescue Mode* on page 3-30 for more information.

Logging On to the Terminal Interface

Use any terminal communications software, such as hyperterminal, to access the terminal interface. Linux users can use Minicom. To enter information in the terminal interface, type the information and press **ENTER**.

Tip: Trend Micro recommends configuring HyperTerminal properties so that the backspace key is set to delete. This enables you to erase text in the terminal window by pressing the backspace key. To do this, click **File** in the HypeTerminal window and select **Properties**. Click the **Settings** tab. Under **Backspace key sends**, select **Del** (see Figure 3-1.)



Function, arrow, and ctrl keys act as

● Terminal keys ○ Windows keys

Backspace key sends

○ Ctrl+H [✓ ● Del] ○ Ctrl+H, Space, Ctrl+H

FIGURE 3-1. Setting the backspace key to delete

To log on to the terminal interface:

1. Connect one end of the included console cable to the **CONSOLE** port on the front panel of the device and the other end to the serial port (COM1, COM2, or other COM port) on a computer.
2. Ensure that the computer has terminal communications software, such as HyperTerminal.

   Configure the properties as follows:

   - **Bits per second:** 115200
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop bits:** 1
   - **Flow control:** None
3. Power on the device to the on position and wait for a welcome message to appear on the LCD module.
4. Press **Enter** when the terminal interface displays "`Network VirusWall 1200 preconfiguration, Press <ENTER> to continue...`"
5. After connection, the terminal screen appears blank. Press **Enter**. The **User Name** login prompt displays.
6. Type one of the following user names and its corresponding password:

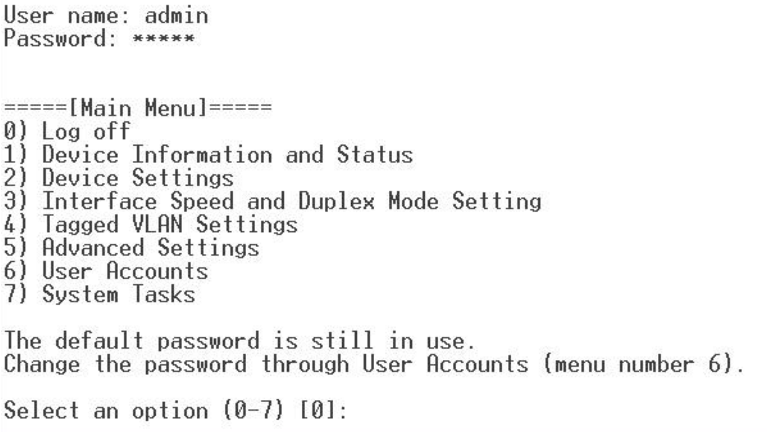
   a. **user name**: admin; **password**: admin

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

   b. **user name**: monitor; **password**: monitor

      This account permits only the following tasks:

      - change the password for the monitor login
      - view—but not modify—device settings, such as the device’s IP address
      - view system logs
7. After a successful logon, the **Main Menu** appears as shown in Figure 3-2.



```
User name: admin
Password: *****


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

The default password is still in use.
Change the password through User Accounts (menu number 6).

Select an option (0-7) [0]:
```

FIGURE 3-2. Terminal Interface main menu

Changing the User Password

Trend Micro highly recommends changing the default passwords for both the **admin** and **monitor** accounts.

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

To change the default password for the *admin* account:

1. On the Network VirusWall console session **Main Menu**, type `1` to select **User Accounts**. The user name and its corresponding permissions appears.
2. Type `1` to select **Change Password**.
3. Type the number corresponding to the user password to change.
4. Type both the current and new passwords. Passwords must be 5–12 alphanumeric characters (no spaces allowed).

To change the default password for the *monitor* account:

1. On the Network VirusWall console session **Main Menu**, type `1` to select **User Accounts**. The user name and its corresponding permissions appears.
2. Type `1` to select **Change Password**.
3. Type the number corresponding to the user password to change.
4. At the **New Password** prompt, type new password and press `<ENTER>`. If the entered password is valid, a **Retype New password** prompt appears. Passwords must be 5–12 alphanumeric characters (no spaces allowed).
5. Retype the new password and press `<ENTER>`. If the two typed passwords match, Network VirusWall accepts the new password and a **Press ENTER to continue...** prompt appears. If they don’t match, Network VirusWall prompts you to retype the new password.

Using Network VirusWall in a Network with a NAT Device

Network VirusWall supports networks that use a Network Address Translation (NAT) device. The following NAT deployments are possible:

- **Scenario 1:** A Network VirusWall device using an IP address belonging to the internal network and a Control Manager server using an IP address belonging to the external (public) network
- **Scenario 2:** A Control Manager server using an IP address belonging to the internal network and a Network VirusWall device using an IP address belonging to the external (public) network

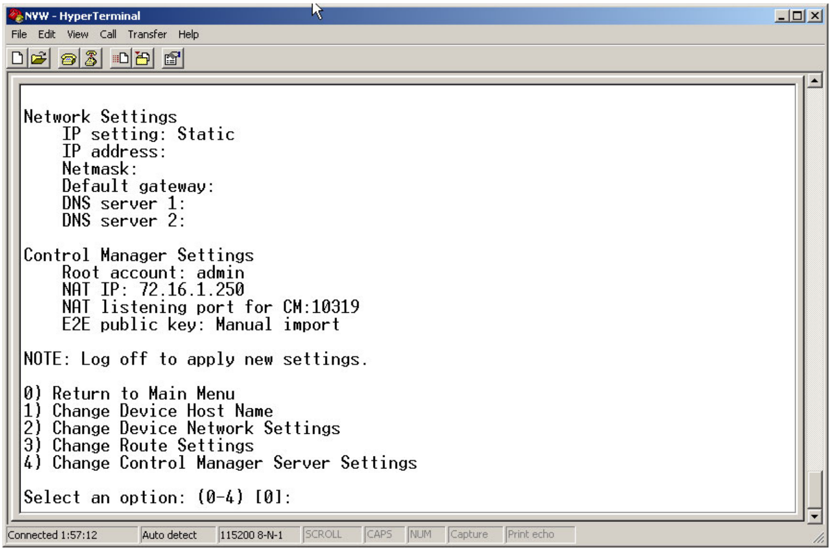
Follow the instructions below for your network topology.

Scenario 1: NVW Device in Internal Network, Control Manager in Public Network

In order to use Network VirusWall (NVW) with a NAT device when NVW is in the internal network, specify the NAT device's IP address and port information in the NVW Preconfiguration console and then enable IP port forwarding on the NAT device to register Network VirusWall to a Control Manager server that is located in the public network.

To enable NAT mode for Control Manager:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type `2` and press **Enter** to select the **Device Settings** menu.
3. Type `4` and press **Enter** to select the **Change Control Manager Server Settings** menu.
4. At the **Import the E2E public key manually?** prompt, type `y` and press Enter. The **Root account =>** prompt appears.
5. Type the name of the root account and press **Enter.** The **NAT IP=>** prompt appears.
6. Type the IP address of your NAT device and press **Enter.** The **NAT listening port for CM** prompt appears.
7. Type the NAT listening port for your Trend Micro Control Manager and press **Enter.** The **Copy and paste the contents of the Public Encryption Key (E2EPublic.dat):** prompt appears.
8. Copy and paste the contents of the Public Encryption Key and press **Enter** and then **CTRL-D.** The console displays your Public Encryption Key for verification, along with the prompt, **Do you want to save? (y/n) [y] .**
9. Type `y` and press **Enter** or just press **Enter** to accept the default choice (yes). NVW imports your Public Encryption Key and displays the network settings and Control Manager settings that you have entered.



```
Network Settings
    IP setting: Static
    IP address:
    Netmask:
    Default gateway:
    DNS server 1:
    DNS server 2:

Control Manager Settings
    Root account: admin
    NAT IP: 72.16.1.250
    NAT listening port for CM:10319
    E2E public key: Manual import

NOTE: Log off to apply new settings.

0) Return to Main Menu
1) Change Device Host Name
2) Change Device Network Settings
3) Change Route Settings
4) Change Control Manager Server Settings

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

FIGURE 3-3. NVW terminal interface showing NVW network settings and Control Manager settings

10. Log off the Preconfiguration console to save your changes.

Note: NVW does not save your changes until you log off from the Preconfiguration Console.

To enable IP port forwarding on the NAT device:

1. Follow the instructions in your NAT device documentation to enable port forwarding.
2. Set **Network VirusWall TCP** to **10319.**

Scenario 2: Control Manager in Internal Network, NVW Device in Public Network

In order to use Network VirusWall (NVW) with a NAT device when NVW is in the public network, enable NAT mode on the Control Manager server and then enable IP port forwarding on the NAT device to register Network VirusWall to a Control Manager server that is located behind a NAT device.

To enable NAT mode on the Control Manager server:

1. Install Control Manager server. (See *Control Manager Getting Started Guide* for details.)
2. When the **Specify Message Routing Path** window appears, click **IP Port forwarding** under **Source of incoming messages.**
3. Type the public IP address used by the NAT device in the first text box.
4. Type `10319` (the Control Manager TCP port) in the second text box.

To enable IP port forwarding on the NAT device:

1. Follow the instructions in your NAT device documentation to apply the following port settings.
2. Set **Time server UDP** to **123.**
3. Set **Control Manager server UDP** to **10319.**
4. Set **Control Manager Web server port** to **80** (This is the default value. You can modify this port number on the Trend Micro Control Manager **System Settings** screen. See *Configuring System Settings* on page 4-6 for more information).
5. Set **Control Manager server TCP** to **10319.**

Adding or Modifying Device Settings

The **Device Settings** menu allows you to modify the following:

- **The Network VirusWall host name** – type a name that represents the Network VirusWall device and appears on the Control Manager management console
- **The Network VirusWall network settings** – configure device IP address, netmask, gateway address and DNS server addresses
- **The Control Manager settings** – specify the Control Manager server End-to-End (E2E) public key used for secure data communications between the Control Manager agent on Network VirusWall and the Control Manager server

  For more information on the Control Manager server E2E public key and secure communications, see the *Control Manager Getting Started Guide* and the Control Manager management console online help.

Adding or Modifying the Network VirusWall Host Name

To add or modify the Network VirusWall host name:

1. Type `2` in the **Main Menu** to select **Device Settings**. The default Network VirusWall settings and Control Manager settings appear, followed by four menu choices.
2. Type `1` to change the Network VirusWall host name.
3. Type a new host name up to 63 alphanumeric characters (spaces are not allowed).

Note: Each Network VirusWall device on your network must have a unique host name to register to the Control Manager server.

To verify that your new host name has been accepted, return to the **Main Menu** and type `2` to reselect **Device Settings**. The new host name now displays next to **Host name** under "Device Settings Summary."

Adding or Modifying Network VirusWall Network Settings

To add or modify the Network VirusWall network settings:

1. Type `2` in the **Main Menu** to select **Device Settings**. The Network VirusWall settings and Control Manager settings appear.
2. Type `2`, **Change Device Network Settings,** to change the Network VirusWall network settings. A prompt displays asking you if you want to use a dynamic IP setting.
3. Type `y` to have a DHCP server on your network determine the Network VirusWall IP address, netmask, gateway address, and DNS server addresses.

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

Tip: Trend Micro recommends assigning 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.

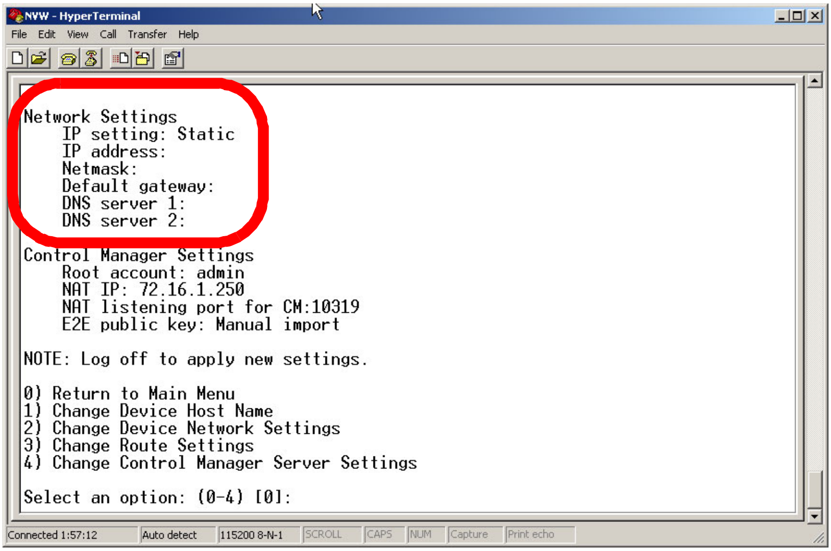
Adding and Modifying Static Routes

You can use the terminal interface to add, delete, or modify static routes via your router IP address.

Note: Before attempting to add a static route via your router IP address, be sure to add NVW network settings. You must add your NVW network settings before you can add static routes.

To add route settings from within the terminal interface:

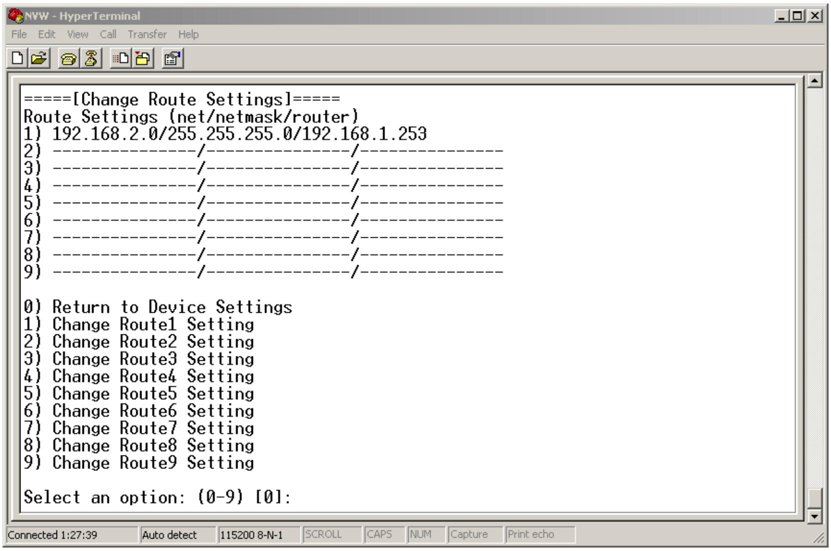
1. Log on to Network VirusWall 1200 terminal interface using the admin account.
2. Select **2**, **Device Settings.** The terminal interface displays the network settings for the Network VirusWall device and the Control Manager settings.
3. Verify that the network settings for the Network VirusWall device have already been set. If necessary, set them now, before proceeding. (See *Adding or Modifying Network VirusWall Network Settings* on page 3-10.)



```
Network Settings
    IP setting: Static
    IP address:
    Netmask:
    Default gateway:
    DNS server 1:
    DNS server 2:

Control Manager Settings
    Root account: admin
    NAT IP: 72.16.1.250
    NAT listening port for CM:10319
    E2E public key: Manual import

NOTE: Log off to apply new settings.

0) Return to Main Menu
1) Change Device Host Name
2) Change Device Network Settings
3) Change Route Settings
4) Change Control Manager Server Settings

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

FIGURE 3-4. NVW Network settings must be set before you can add or modify static routes

4. Select **3, Change Route Settings.** A list of route settings displays showing any settings that have already been added. If no settings have been added, the list shows only empty lines, as shown in items 2 through 9 in **Figure 3-5 on page 3-13.**
5. Select **1, Change Route1 Setting.** A **net=>** prompt appears.
6. At the **net=>** prompt, type the new IP address of the net and press **Enter.**
7. At the **netmask=>** prompt, type the IP address of your netmask and press **Enter.**
8. At the **router=>** prompt, type the router IP address and press **Enter.**
9. Log off Network VirusWall 1200 terminal interface to save your changes.



```
=====[Change Route Settings]=====
Route Settings (net/netmask/router)
1) 192.168.2.0/255.255.255.0/192.168.1.253
2) ---------------/---------------/---------------
3) ---------------/---------------/---------------
4) ---------------/---------------/---------------
5) ---------------/---------------/---------------
6) ---------------/---------------/---------------
7) ---------------/---------------/---------------
8) ---------------/---------------/---------------
9) ---------------/---------------/---------------

0) Return to Device Settings
1) Change Route1 Setting
2) Change Route2 Setting
3) Change Route3 Setting
4) Change Route4 Setting
5) Change Route5 Setting
6) Change Route6 Setting
7) Change Route7 Setting
8) Change Route8 Setting
9) Change Route9 Setting

Select an option: (0-9) [0]:
```

FIGURE 3-5. You can use the Change Route Settings menu of NVW1200 to add a static route via the IP of your router.

To modify or delete route settings:

1. Log on to Network VirusWall 1200 terminal interface using the admin account.
2. Select **2**, **Device Settings.** The terminal interface displays the network settings for the Network VirusWall device and the Control Manager settings.
3. Select **3, Change Route Settings.** A list of existing route settings appears.
4. Select the number of the route setting that you wish to delete or modify. (You can enter up to nine route settings). The **net=>** prompt appears, showing the current net IP for your route setting.
5. Use the backspace key to delete any incorrect digits and type the correct digits to replace them.
6. Press **Enter.** The **netmask=>** prompt appears, showing the current netmask IP for your route setting.
7. Repeat the above steps for the netmask and router IP settings.
8. Log off of from the terminal interface in order to save your settings.

Adding or Modifying Control Manager Server Settings

There are two ways to modify Control Manager Server settings:

- Allow Network VirusWall to get the key from Control Manager
- Manually input the E2E public key

To allow Network VirusWall to get the key from the specified Control Manager server:

1. Type `2` in the **Main Menu** to select **Device Settings**. The current Network VirusWall settings and Control Manager settings appear.
2. Type `4` to change the Control Manager settings.
3. Type `n` or press `<ENTER>` when prompted to manually import the key.
4. Type the Control Manager IP address or host name and press **Enter.**
5. At the **Root account =>** prompt, type the TMCM power user name, which is set during Control Manager installation.
6. If your NVW device is in the internal network and there is a NAT device between it and Control Manager, enter the NAT IP at the **NAT IP =>** prompt. Otherwise, disregard this prompt and press **Enter.**

You can download the E2E public key from the Control Manager console by following these steps:

To obtain the E2E public key for manual input:

1. From within Control Manager, click the **Products** tab. The **Managed Products** screen appears.
2. Click the **Add/Remove Product Agents** link in the left-side panel. The **Add/Remove Product Agents** screen appears.
3. Click the **Public encryption key** link at the bottom of the **Add/Remove Product Agents** screen. The file containing the E2E public key downloads to your computer.

To manually input the E2E public key:

1. Type `2` in the **Main Menu** to select **Device Settings**. The current Network VirusWall settings and Control Manager settings appear.
2. Type `4` to change the Control Manager settings.

3. Type `y` when prompted to manually import the key.
4. Type the Control Manager power user name and type the key when prompted.
5. When prompted to keep the settings, type `y` to save or `n` to cancel.

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

Setting the Interface Speed and Duplex Mode

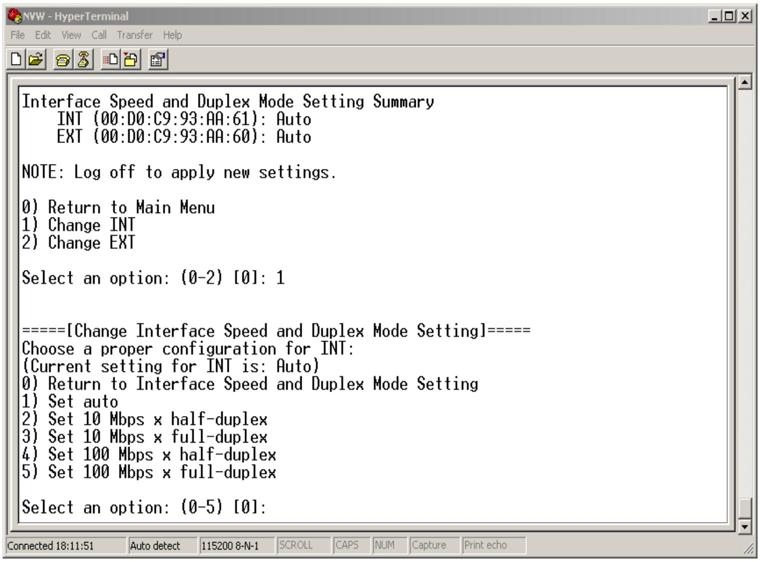
Use the terminal interface to configure the interface speed and duplex mode.

Note: Both the connected L2/L3 and Network VirusWall devices should have the same interface setting and duplex mode. Otherwise, the half-duplex mode setting will take effect.

To help guarantee the correct interface setting and duplex mode implementation, modify both the L2/L3 and Network VirusWall devices to have the same setting. Apply **100Mbps x full-duplex** for both the switch and Network VirusWall device.

To set the interface speed and duplex mode:

1. On the **Main Menu** of the Preconfiguration console, type `3` to select **Interface Speed and Duplex Mode Setting**. The Port Configuration menu appears, displaying the current port configuration summary.



```
Interface Speed and Duplex Mode Setting Summary
    INT (00:D0:C9:93:AA:61): Auto
    EXT (00:D0:C9:93:AA:60): Auto

NOTE: Log off to apply new settings.

0) Return to Main Menu
1) Change INT
2) Change EXT

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


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

Select an option: (0-5) [0]:
```

FIGURE 3-6. The Port Configuration (Interface Speed and Duplex Mode) menu

2. On the **Interface Speed and Duplex Mode Setting** screen, select the port you want to configure and type the menu number. For example, to configure the interface speed and duplex mode of port 1, type `1`.
3. Select from the available interface speed and duplex mode, and then type the menu number.
4. Log off the terminal interface for changes to take effect (see *Using the Terminal Interface* on page 3-3).

Configuring VLAN Settings

Create and edit Virtual Local Area Network (VLAN) tags that conform to the existing VLAN rules on your network. (See *About VLANs* on page 8-7 for more information on VLANs). Network VirusWall supports 50 tagged VLANs and 1 non-tagged VLAN.

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

To add a new VLAN ID:

1. Type `4` in the **Main Menu** to select **Tagged VLAN Settings**.
2. Type `1` in the **Tagged VLAN Settings** menu to select **Add VLAN**.
3. At the **New VLAN ID** prompt, type an ID number from 1 to 4094.
4. If the entry is valid, the **New VLAN name** prompt displays a default name.
5. If you want to bind the Network VirusWall IP address to the current VLAN, type `y` at the **Bind the current device IP address to this VLAN?** prompt.

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

To remove an existing VLAN:

1. Type `4` in the **Main Menu** to select **Tagged VLAN Settings**.
2. Type `2` in the **VLAN Setting** menu to select **Remove VLAN**.
3. At the prompt, type the ID number of the VLAN to delete.

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

To rename an existing VLAN:

1. Type `4` in the **Main Menu** to select **Tagged VLAN Settings**.
2. Type `3` in the **Tagged VLAN Settings** menu to select **Rename VLAN**.
3. At the prompt, type the ID number of the VLAN to rename.
4. Type the new name.

To modify the IP binding selection of a VLAN:

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

Changing the LCD Module Configuration

LCD Module (LCM) configuration controls whether the touch panel on Network VirusWall is locked or unlocked. If the touch panel is locked, preconfiguration is possible only by using the terminal interface.

To change the LCM Configuration:

1. Type `5` in the **Main Menu** to select **Advanced Settings**. The **Advanced Settings** menu appears.
2. Type `3` at the **Select an Option** prompt to select **Change LCD Module Configuration**. The **Allow configuration via the LCD module?** prompt appears.
3. Press `<ENTER>` or type `y` at the allow configuration via the LCD module.

Viewing System Logs

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.

To view system logs:

1. Type `7` in the **Main Menu** to select **System Tasks**. The **System Tasks** menu appears.
2. Type `1` to select **View System Logs**. System logs appear showing the following:
   - Date and time of log entry
   - Log entry
3. Press **Enter** to stop the log report.
4. At the prompt, type `y` or press `<ENTER>` to return to the **System Tasks** menu.

Configuring Advanced Settings

Network VirusWall advanced settings allow you to block or pass client traffic under the following conditions:

- After Vulnerability Assessment times out – if Network VirusWall is unable to retrieve Vulnerability Assessment information from the Control Manager server and reaches the default timeout value (See the *Control Manager Getting Started Guide* for detailed information on Vulnerability Assessment)
- During antivirus information retrieval – while Network VirusWall acquires the status of client antivirus installations and related components (see *Configuring Enforcement Policies* on page 5-8 for more information on configuring enforcement policies based on client antivirus status)

To block/pass traffic if Vulnerability Assessment times out:

1. Type `5` in the **Main Menu** to select **Advanced Settings**. The **Advanced Settings** menu appears.
2. Type `1` in the **Advanced Settings** menu to select **Change Blocking Policy for VA Timeout**. The **Block/pass all clients if Vulnerability Assessment times out** prompt appears.
3. To pass all client traffic, type `n` or press `<ENTER>`.
   To block all client traffic, type `y`.

To block/pass traffic during antivirus information retrieval:

1. Type `5` in the **Main Menu** to select **Advanced Settings**. The **Advanced Settings** menu appears.
2. Type `2` in the **Advanced Settings** menu. **The Block pending clients** prompt appears.
3. To pass all client traffic, type `n` or press **Enter.**
   To block all client traffic, type **`y`.**

You can enable LinkState Failover for Network VirusWall 1200.

To enable LinkState Failover:

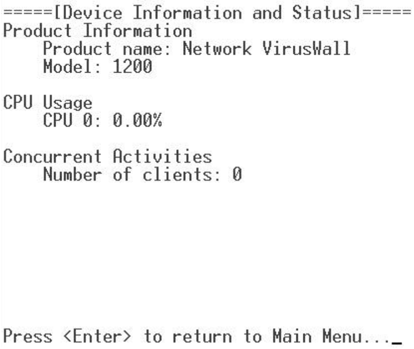
1. Log on to the Network VirusWall 1200 preconfiguration console.
2. Select **5, Advanced Settings.** The Advanced Settings list appears.
3. Select **5, Change LinkState Failover Setting.**
4. Type `y` to enable LinkState Failover.
5. Log off the Network VirusWall 1200 preconfiguration console in order to save your changes.

Viewing Device Information and Status

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

To view device information and status:

1. Access the terminal interface (see *Using the Terminal Interface* on page 3-3).
2. Type `1` in the **Main Menu** to view the system information. The **Device Information and Status** screen appears.



```
=====[Device Information and Status]=====
Product Information
    Product name: Network VirusWall
    Model: 1200

CPU Usage
    CPU 0: 0.00%

Concurrent Activities
    Number of clients: 0





Press <Enter> to return to Main Menu..._
```

FIGURE 3-7. Viewing system information

Setting Blocking Policy for VA

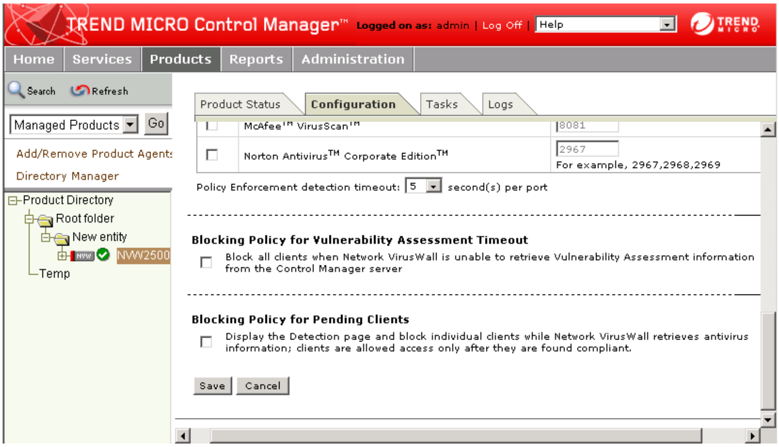
Network VirusWall advanced settings allows you to block clients when Network VirusWall is unable to retrieve Vulnerability Assessment information from the Control Manager server.

Set blocking policy for VA through the:

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

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

1. Access a managed Network VirusWall product (see the *Network VirusWall 1200 Getting Started Guide*).
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**. See *Setting blocking policy for VA timeout via TMCM* on page 3-22.



□ McAfee™ VirusScan™ 8081

□ Norton Antivirus™ Corporate Edition™ 2967
For example, 2967,2968,2969

Policy Enforcement detection timeout: 5 second(s) per port

Blocking Policy for Vulnerability Assessment Timeout

□ Block all clients when Network VirusWall is unable to retrieve Vulnerability Assessment information from the Control Manager server

Blocking Policy for Pending Clients

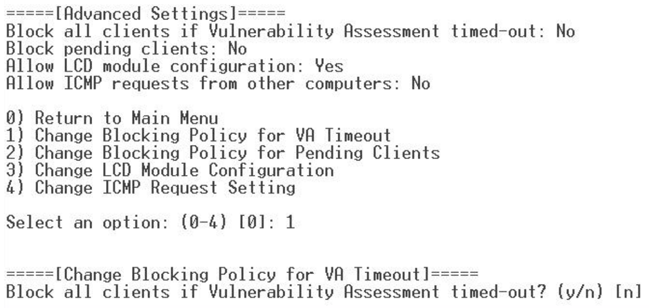
□ Display the Detection page and block individual clients while Network VirusWall retrieves antivirus information; clients are allowed access only after they are found compliant.

FIGURE 3-8. Setting blocking policy for VA timeout via TMCM

5. Click **Save**.

To set blocking policy for VA through the terminal interface:

1. Type `5` 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. See *Setting blocking policy for VA timeout via the terminal interface* on page 3-23.



```
=====[Advanced Settings]=====
Block all clients if Vulnerability Assessment timed-out: No
Block pending clients: No
Allow LCD module configuration: Yes
Allow ICMP requests from other computers: No

0) Return to Main Menu
1) Change Blocking Policy for VA Timeout
2) Change Blocking Policy for Pending Clients
3) Change LCD Module Configuration
4) Change ICMP Request Setting

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


=====[Change Blocking Policy for VA Timeout]=====
Block all clients if Vulnerability Assessment timed-out? (y/n) [n]
```

FIGURE 3-9. Setting blocking policy for VA timeout via the terminal interface

3. At the confirmation prompt, type `y` to block all clients if VA times out. Otherwise, type `n` to allow clients even if VA has timed out.

The Advanced Settings summary displays the new setting.

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

Setting Blocking Policy for Pending Clients

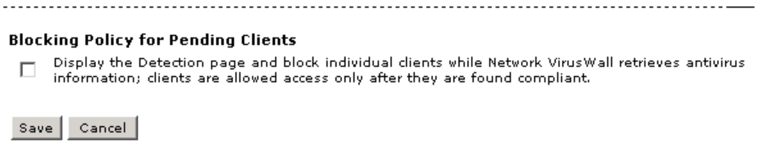
Network VirusWall advanced settings allows you to block clients when Network VirusWall has not yet retrieved Vulnerability Assessment information from the Control Manager server.

Set blocking policy for pending clients through the:

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

To set blocking policy for Pending Clients through the TMCM management console:

1. Access a managed Network VirusWall product (see the *Network VirusWall 1200 Getting Started Guide*).
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 Pending Clients** section, select **Display the Detection page and block individual clients while Network VirusWall retrieves antivirus information; clients are allowed access only after they are found compliant**. See *Setting blocking policy for Pending Clients via TMCM* on page 3-24.



Blocking Policy for Pending Clients

□ Display the Detection page and block individual clients while Network VirusWall retrieves antivirus information; clients are allowed access only after they are found compliant.

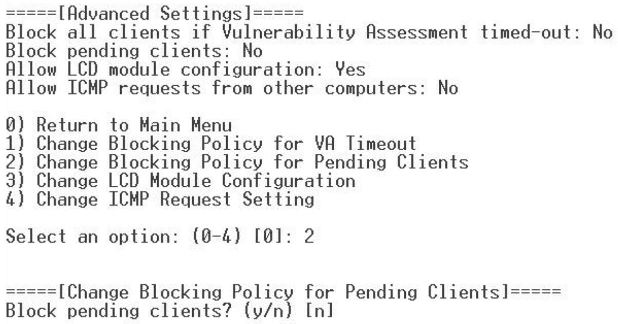
.

FIGURE 3-10. Setting blocking policy for Pending Clients via TMCM

5. Click **Save**.

To set blocking policy for VA through the terminal interface:

1. Type `5` 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 `2` to change the blocking policy for pending clients setting. See *Setting blocking policy for Pending Clients via the terminal interface* on page 3-25.



```
=====[Advanced Settings]=====
Block all clients if Vulnerability Assessment timed-out: No
Block pending clients: No
Allow LCD module configuration: Yes
Allow ICMP requests from other computers: No

0) Return to Main Menu
1) Change Blocking Policy for VA Timeout
2) Change Blocking Policy for Pending Clients
3) Change LCD Module Configuration
4) Change ICMP Request Setting

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


=====[Change Blocking Policy for Pending Clients]=====
Block pending clients? (y/n) [n]
```

FIGURE 3-11. Setting blocking policy for Pending Clients via the terminal interface

3. At the **Block pending clients?** prompt, type `y` to block all clients while VA is pending. Otherwise, type `n` to allow clients even if VA has not yet finished.

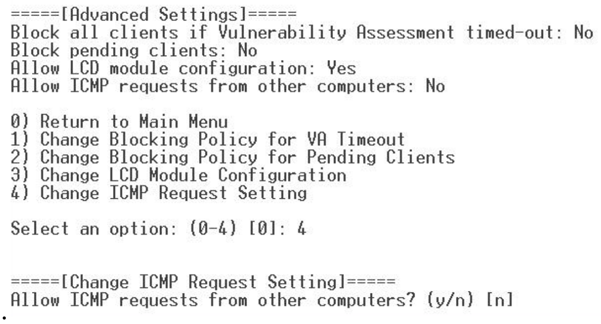
The Advanced Settings summary displays the new setting.

Allowing ICMP Requests

Network VirusWall 1200 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 terminal interface.

To allow ICMP requests to reach a Network VirusWall device:

1. Access the terminal interface (see *Network VirusWall 1200 Getting Started Guide*).
2. Type `5` to open the Advanced Settings menu. The Advanced Settings Summary screen displays. See*Allowing ICMP requests* on page 3-26 for a screen shot.



```
=====[Advanced Settings]=====
Block all clients if Vulnerability Assessment timed-out: No
Block pending clients: No
Allow LCD module configuration: Yes
Allow ICMP requests from other computers: No

0) Return to Main Menu
1) Change Blocking Policy for VA Timeout
2) Change Blocking Policy for Pending Clients
3) Change LCD Module Configuration
4) Change ICMP Request Setting

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


=====[Change ICMP Request Setting]=====
Allow ICMP requests from other computers? (y/n) [n]
.
```

FIGURE 3-12. Allowing ICMP requests

3. Type `4` to toggle the ICMP request setting
4. Type `y` to allow ICMP requests to reach a Network VirusWall device. Otherwise, type `n`.
5. The Advanced Settings Summary screen refreshes and displays the current ICMP request setting.

Importing and Exporting the Configuration File

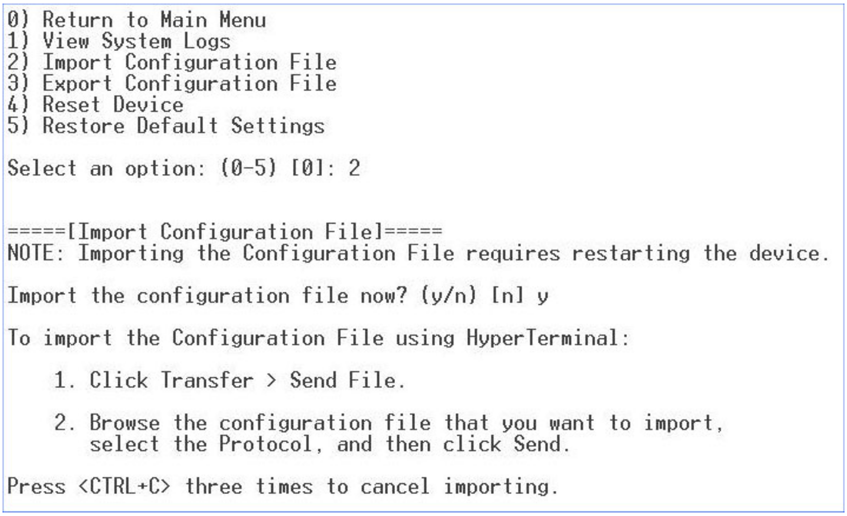
Use the terminal interface to import and export the Network VirusWall configuration. This allows easy replication of existing Network VirusWall settings from one Network VirusWall 1200 to other devices of the same model and locale settings.

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 1200 terminal interface (see *Using the Terminal Interface* on page 3-3).
2. Type `7` in the main menu to select **System Tasks**. The **System Tasks** menu appears.
3. Type `2` to import the configuration file. A confirmation prompt appears.

4. Type `y` to continue. The **Import configuration file now?** prompt appears.



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

Select an option: (0-5) [0]: 2


=====[Import Configuration File]=====
NOTE: Importing the Configuration File requires restarting the device.

Import the configuration file now? (y/n) [n] y

To import the Configuration File using HyperTerminal:

    1. Click Transfer > Send File.

    2. Browse the configuration file that you want to import,
       select the Protocol, and then click Send.

Press <CTRL+C> three times to cancel importing.
```

.

FIGURE 3-13. Importing the Network VirusWall configuration file

5. Type `y` to import the configuration file. The terminal interface displays instructions on how to transfer the file using your terminal software.

6. In your terminal emulator, set your transfer protocol to **Kermit**.

7. Follow your terminal emulator's instructions on sending files. If you are using HyperTerminal, follow these procedures.

To import the configuration file using HyperTerminal:

1. Click **Transfer/Send File**.

2. Type or browse to the folder where the configuration file will be saved.

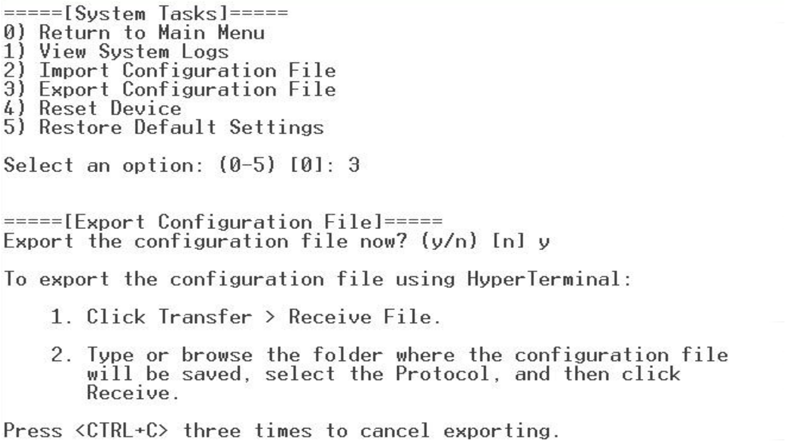
3. For your transfer, select **Kermit** protocol.

4. Click **Send**.

Note: Refer to *Using the Terminal Interface* on page 3-3 for detailed information on using the preconfiguration menu through the terminal interface.

To export the configuration file:

1. Access the Network VirusWall 1200 terminal interface (see *Using the Terminal Interface* on page 3-3).
2. Type 7 in the main menu to select the **System Tasks** menu.
3. Type 3 to export the configuration file. A confirmation prompt appears.



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

Select an option: (0-5) [0]: 3


=====[Export Configuration File]=====
Export the configuration file now? (y/n) [n] y

To export the configuration file using HyperTerminal:

    1. Click Transfer > Receive File.

    2. Type or browse the folder where the configuration file
       will be saved, select the Protocol, and then click
       Receive.

Press <CTRL+C> three times to cancel exporting.
```

FIGURE 3-14. Exporting the Network VirusWall configuration file

4. Type y to continue. The terminal interface displays instructions on how to transfer the file using your terminal software.
5. In your terminal emulator, set your transfer protocol to **Kermit**.
6. Follow your terminal emulator’s instructions on receiving files. If you are using HyperTerminal, follow these procedures.

To save the configuration file using HyperTerminal:

1. Click **Transfer/Receive File**.
2. Type or browse to the folder containing the configuration file.
3. For your transfer, select **Kermit** protocol.
4. Click **Receive**.

Note: Refer to *Using the Terminal Interface* on page 3-3 for detailed information on using the preconfiguration menu through the terminal interface.

Restoring Default Settings

If you experience any problems during preconfiguration, you have the option of restoring the default settings by initializing Network VirusWall.

To restore default settings:

1. Type `7` in the **Main Menu** to select **System Tasks**. The **System Tasks** menu appears.
2. Type `5` to select **Restore Default Settings**. A confirmation prompt appears.
3. Type `y` to continue. The Network VirusWall device resets and restores the factory defaults.

WARNING! *Restoring default settings loses all preconfigured settings that are different from the factory defaults. If you wish to preserve settings for later use, Adding or Modifying Device Settings on page 3-9.*

Network VirusWall reverts to the following factory default settings when initialized:

Setting	Default Value
Network VirusWall host name	none
IP address type	Static
IP address	none
Netmask	none
Default gateway	none
DNS server 1	none
DNS server 2	none

TABLE 3-2. Default factory settings

Resetting Network VirusWall

Reset Network VirusWall if you experience any problems or if you are prompted to do so when using the Control Manager management console. There are two methods of resetting Network VirusWall:

- Press the **RESET** button on the front of the device.
- Use the terminal interface to reset Network VirusWall.VirusWall

To reset Network VirusWall via the terminal interface:

1. Type `7` in the **Main Menu** to select **System Tasks**. The **System Tasks** menu appears.
2. Type `4` to select **Reset Device**. A confirmation message appears.
3. Type `y` to continue.

Note: When Network VirusWall resets, it preserves all changes to preconfiguration settings.

Entering Rescue Mode

If problems arise that prohibit the normal functioning of Network VirusWall, you may need to upload the program file or boot loader. See *Entering Rescue Mode* on page 7-4 and *Understanding the Program and Boot Loader Files* on page 7-6 for more information.

Logging Off the Terminal Interface

Log off the terminal interface after finishing preconfiguration.

To log off:

1. Type `0` in the **Main Menu** to select **Log off**. A confirmation message appears.
2. Type `y` to log off.

Note: Network VirusWall saves all preconfiguration changes when you log off.

Using the LCD Module Panel

With the front panel LCD module, you can configure only the Network VirusWall device's IP address. Use the terminal interface for access to all other preconfiguration options (see *Comparison of preconfiguration methods* on page 3-2).

There are five buttons on the LCD module panel:

- ▲ **Up arrow** – cycle forward through the alphanumeric characters displayed on the panel
- ▼ **Down arrow** – cycle backward through the alphanumeric characters displayed on the panel
- ◀ **Left arrow** – move the focus or cursor to the left
- ▶ **Right arrow** – move the focus or cursor to the right
- ↵ **Enter** – confirm selection or input

Note: The LCD module and the terminal interface cannot be used simultaneously. In order to use the LCD module panel, log out of the terminal interface first.

To configure the Network VirusWall IP address through the LCD module:

1. Press **Enter**. A prompt displays asking if you want to change settings.
2. To continue, ensure the * is next to `Yes`; otherwise, move it next to `No`.
3. Press **Enter**.
4. If you selected `Yes`, a prompt displays asking to have the Network VirusWall IP address dynamically assigned.

   To use a dynamic IP address, do the following:

   a. Ensure the * is next to `Yes` and press **Enter**.

   b. Enter the Control Manager server IP address.

   c. Enter the Control Manager power user name.

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

   a. Ensure the * is next to `No` and press **Enter**.

   b. Enter the new Network VirusWall IP address, netmask, Gateway address, and DNS server addresses.

   c. Enter the Control Manager server IP address.

   d. Enter the Control Manager power user name.

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

---

5. Save the settings when prompted on the display.

Chapter 4

Getting Started with Network VirusWall 1200

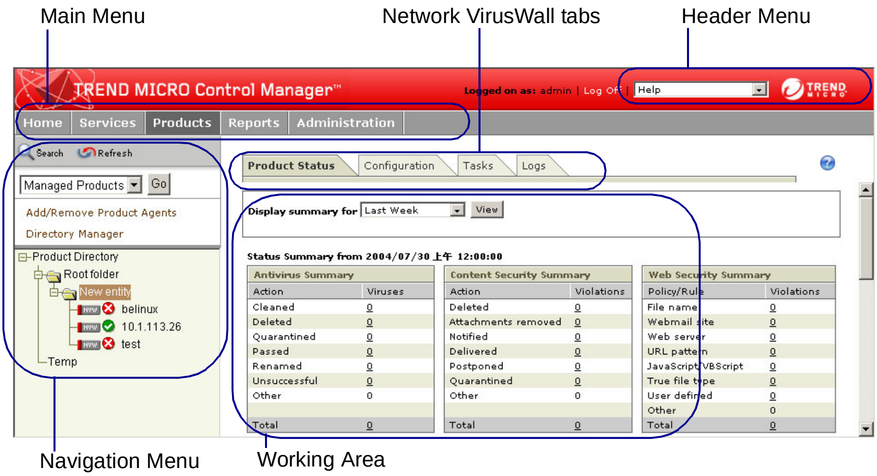
This chapter describes how to access Network VirusWall devices from the Control Manager management console, view system information, deploy Network VirusWall components, and modify device settings.

The topics discussed in this chapter include:

- *Accessing Network VirusWall Devices* on page 4-2
- *Viewing Network VirusWall System Information* on page 4-4
- *Deploying Network VirusWall Components* on page 4-5
- *Configuring System Settings* on page 4-6

Accessing Network VirusWall Devices

The 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.Figure 4-1 illustrates the main components of the Control Manager management console.



Display summary for Last Week

Status Summary from 2004/07/30 上午 12:00:00

Antivirus Summary	
Action	Viruses
Cleaned	0
Deleted	0
Quarantined	0
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	0

Content Security Summary	
Action	Violations
Deleted	0
Attachments removed	0
Notified	0
Delivered	0
Postponed	0
Quarantined	0
Other	0
Total	0

Web Security Summary	
Policy/Rule	Violations
File name	0
Webmail site	0
Web server	0
URL pattern	0
JavaScript/VBScript	0
True file type	0
User defined	0
Other	0
Total	0

FIGURE 4-1. The Control Manager management console displays configuration, status, and tasks for all registered Network VirusWall devices.

Note: See the *Control Manager Getting Started Guide* and 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, a directory of managed products appears. The host name of each registered Network VirusWall device appears next to the NVW ✓ icon.
3. Click the Network VirusWall host name to manage. The **System Information** screen displays.

Control Manager and 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:

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

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 is directly related to Network VirusWall 1200. 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 4-2).
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.

Deploying Network VirusWall Components

Deploy the following components to Network VirusWall 1200 after performing preconfiguration and after a virus outbreak:

- **Network scan engine:** scans traffic passing through Network VirusWall at the packet level. The network scan engine is specifically designed to find network viruses.
- **Network virus pattern files:** contains a regularly updated database of packet-level network virus patterns. Trend Micro updates the network virus pattern file daily to ensure Network VirusWall can identify any new network viruses.
- **Network outbreak rule:** contains a regularly updated collection of behavior-based network threat rules.
- **Program file:** consists of an image of the operating system, system programs, and all components necessary to get Network VirusWall functioning properly

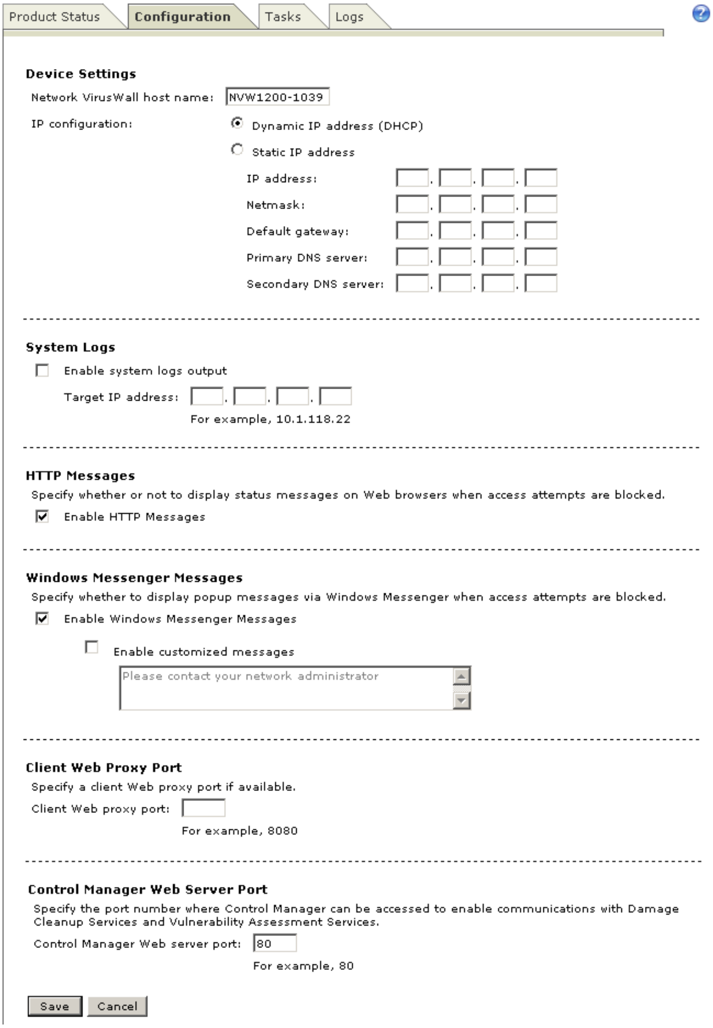
To deploy components to Network VirusWall:

1. Access Network VirusWall 1200 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 1200 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 ensure your network has the most up-to-date antivirus protection. Ensure that you first perform a Manual Download on the Control Manager server (see the *Control Manager Getting Started Guide* for more information.)

Configuring System Settings

Network VirusWall 1200 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.



Device Settings

Network VirusWall host name: NVW1200-1039

IP configuration: ● Dynamic IP address (DHCP)

○ Static IP address

IP address: ___ . ___ . ___ . ___

Netmask: ___ . ___ . ___ . ___

Default gateway: ___ . ___ . ___ . ___

Primary DNS server: ___ . ___ . ___ . ___

Secondary DNS server: ___ . ___ . ___ . ___

System Logs

□ Enable system logs output

Target IP address: ___ . ___ . ___ . ___

For example, 10.1.118.22

HTTP Messages

Specify whether or not to display status messages on Web browsers when access attempts are blocked.

☑ Enable HTTP Messages

Windows Messenger Messages

Specify whether to display popup messages via Windows Messenger when access attempts are blocked.

☑ Enable Windows Messenger Messages

□ Enable customized messages

Please contact your network administrator

Client Web Proxy Port

Specify a client Web proxy port if available.

Client Web proxy port: ___

For example, 8080

Control Manager Web Server Port

Specify the port number where Control Manager can be accessed to enable communications with Damage Cleanup Services and Vulnerability Assessment Services.

Control Manager Web server port: 80

For example, 80

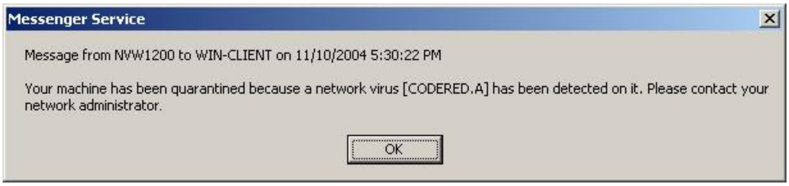
FIGURE 4-2. The Control Manager System Settings screen

To modify system settings:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **System Settings.** The **System Settings** screen appears.
4. Click **Next.** The **System Settings** screen displays the following options.
   - **Device Settings:** configure Network VirusWall 1200 host name and network settings, including IP address, netmask, gateway address, and DNS server addresses (see *To modify device settings:* on page 4-10)
   - **System Logs:** specify which computer to send the system log to (see *To enable a system log:* on page 4-10)
   - **HTTP Messages**: select **Enable HTTP messages** (selected by default) to enable Web browser messages to display on client machines when access attempts are blocked (because a client is either quarantined or blocked)

Note: Trend Micro recommends keeping the default selection **Enable HTTP messages**. This setting ensures that users know why their machines are blocked when attempting to access the Internet. Client host names do not appear on the status messages unless you configure existing DNS server(s) on your network.

- **Windows Messenger Messages**: select **Enable Windows Messenger Messages** to display a pop-up message via the Windows Messenger when access attempts are blocked.

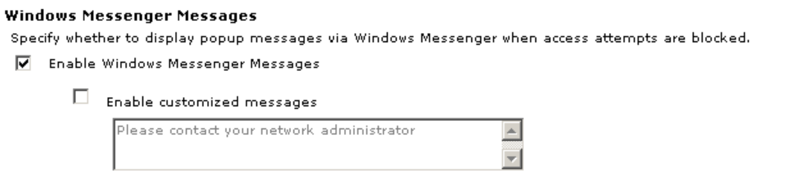


Message from NVW1200 to WIN-CLIENT on 11/10/2004 5:30:22 PM

Your machine has been quarantined because a network virus [CODERED.A] has been detected on it. Please contact your network administrator.

FIGURE 4-3. Sample Windows Messenger Service notification

You can provide detailed instructions to your users by customizing this message. After selecting **Enable Windows Messenger Messages**, select **Enable customized messages** and type your message in the field provided. The default content is "Please contact your network administrator." Network VirusWall saves your message when you click Save at the bottom of the screen.



Windows Messenger Messages

Specify whether to display popup messages via Windows Messenger when access attempts are blocked.

☑ Enable Windows Messenger Messages

□ Enable customized messages

Please contact your network administrator

FIGURE 4-4. Use the *Enable customized messages* field under Windows Messenger Messages in the Systems Settings screen to customize these notifications

- **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 match the Web server port number entered during Control Manager installation. See the *Control Manager Getting Started Guide* for more information.)

Note: There are many configuration fields on the **System Settings** screen. Control Mangager will apply changes only after you have clicked **Save** at the very bottom of the screen.

To modify device settings:

1. Type a new host name in the **Network VirusWall host name** field.
2. Next to **IP configuration**, select the type of IP address for Network VirusWall 1200. If there is a DHCP server on your network and you want it to dynamically assign an IP address to Network VirusWall 1200, select **Dynamic IP address (DHCP)**. Otherwise, select **Static IP address** and type the **IP address**, **netmask**, **default gateway** address, and **Primary** and **Secondary DNS server addresses**.

To enable a system log:

1. Select the **Enable System Logs output** check box.
2. Type the IP address of the machine that will receive a system log.

Tip: Use the Network VirusWall 1200 System Log Viewer, a user-friendly, Windows-based application, to view logs. See *Using the Log Viewer* on page 6-7 for more information.

Chapter 5

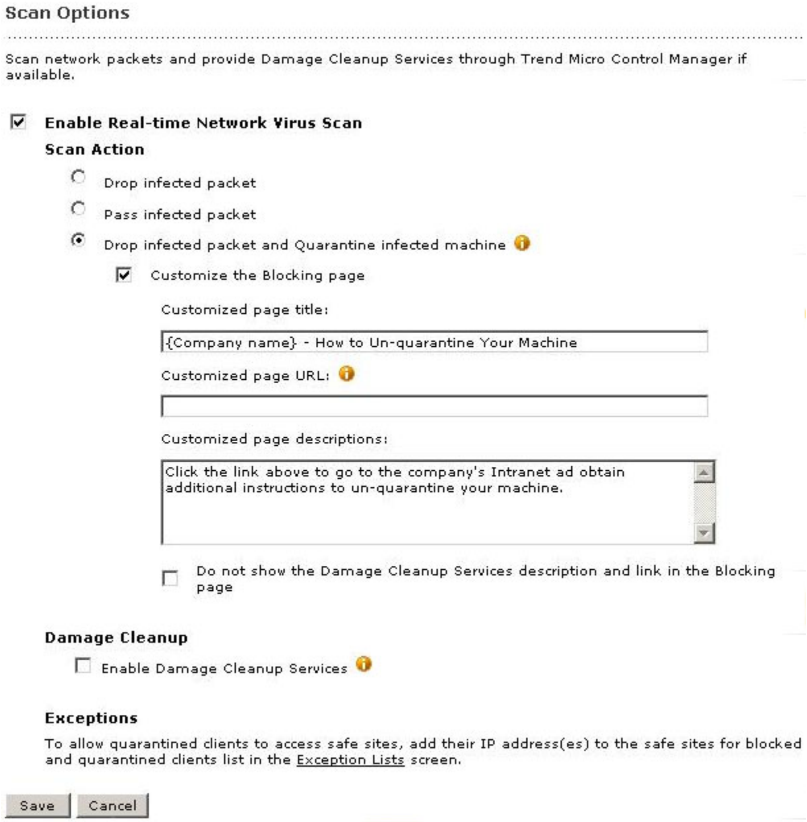
Configuring Basic Settings

This chapter introduces the settings you need to configure to take advantage of Network VirusWall 1200 virus-scanning capabilities. After Network VirusWall is installed on your network and has the most up-to-date components, enable and configure a wide range of settings, which include scan options, Network Outbreak Monitor, enforcement policies, component updates, and exception lists.

The topics discussed in this chapter include:

Configuring Scan Options

The **Scan Options** screen, as shown in Figure 5-1 on page 5-2, allows you to enable real-time scanning of network traffic, to select an action to take on infected packets and clients, and to enable Damage Cleanup Services. See the *Control Manager Getting Started Guide* for more information on Damage Cleanup Services.



Scan Options

Scan network packets and provide Damage Cleanup Services through Trend Micro Control Manager if available.

☑ **Enable Real-time Network Virus Scan**

Scan Action

○ Drop infected packet

○ Pass infected packet

● Drop infected packet and Quarantine infected machine

☑ Customize the Blocking page

Customized page title:

{Company name} - How to Un-quarantine Your Machine

Customized page URL:

Customized page descriptions:

Click the link above to go to the company's Intranet ad obtain additional instructions to un-quarantine your machine.

□ Do not show the Damage Cleanup Services description and link in the Blocking page

Damage Cleanup

□ Enable Damage Cleanup Services

Exceptions

To allow quarantined clients to access safe sites, add their IP address(es) to the safe sites for blocked and quarantined clients list in the Exception Lists screen.

FIGURE 5-1. The *Scan Options* screen

Through this screen an administrator can customize the content of the Web-based notification page that displays when a user’s computer is quarantined.

The **Scan Options** screen allows you to configure the following:

- **Real-time Network Virus Scan**: enable this option to scan network packets (enabled by default) See *Enabling Real-time Network Virus Scan* on page 5-4 for more information.
- **Scan Action**: select an action to take on infected packets and infected computers (see *To customize the blocking Web page:* on page 5-5
- **Damage Cleanup Services**: enable this option to run Damage Cleanup Services (DCS) on infected computers (see the *Control Manager Getting Started Guide* for more information on DCS)
- **Exceptions**: add IP addresses of blocked and quarantined computers to allow them to access safe sites

Understanding Quarantined and Blocked Clients

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

- **Quarantine** – blocks traffic from clients that are infected. If Network VirusWall detects an infected packet, it can isolate the client, thus helping to ensure that no traffic from that client leaves the Protected Network.

  Configure Network VirusWall to quarantine clients on the **Scan Options** screen.

  Quarantined clients appear on the **Virus Infections Summary** screen and can be un-quarantined (see *Viewing Client Summary Information* on page 6-2 for more information).

  Browsers on quarantined clients can be redirected only to a blocking page located on Network VirusWall. If you enable HTTP messages to appear on quarantined and blocked clients, the blocking page displayed on quarantined client browsers can redirect users to the Damage Cleanup Services (DCS) manual cleanup tool (see *Configuring System Settings* on page 4-6 for information on enabling HTTP messages, and see the Control Manager Getting Started Guide for information on DCS).

Note: Network VirusWall quarantines a maximum of 2048 computers and drops all network traffic from additional computers (over 2048) whose packets are infected.

- **Block** – blocks only specified types of traffic from clients that violate Network VirusWall Policy Enforcement settings.

  Configure Network VirusWall to block clients on the **Network VirusWall Policy Enforcement** screen (see *Configuring Enforcement Policies* on page 5-8 for more information).

  Blocked clients appear on two screens: **Network VirusWall Policy Violations Summary** and **Outbreak Prevention Violations Summary** (see *Viewing Client Summary Information* on page 6-2 for more information).

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 Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Scan Options**. The **Scan Options** screen appears.
4. Click **Next**.
5. Ensure that **Enable Real-time Network Virus Scan** is selected (the default setting) to have Network VirusWall 1200 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 1200 from forwarding any packets it finds containing malicious code
   - **Pass infected packet:** click to allow Network VirusWall 1200 to forward all packets, even if they contain malicious code

- **Drop infected packet and Quarantine infected machine** (the default setting)**:** click to prevent Network VirusWall 1200 from forwarding any packets, and quarantine the computer that originated the infected packet. Network VirusWall 1200 disallows all traffic to and from a quarantined computer. Network VirusWall allows you to customize the blocking page displayed on a quarantined computer. See*To customize the blocking Web page:* on page 5-5 for more information.

Tip: For maximum security, select **Drop infected packet and Quarantine infected machine**. Using this setting reduces the chances of spreading a network virus and allows you to immediately isolate and treat any infected computers.

7. Click **Save**.

To customize the blocking Web page:

1. Ensure that **Enable Real-time Network Virus Scan** is selected, so that the options below are active.
2. Ensure that **Drop infected packet and Quarantine infected machine** is selected (the default setting), so that the **Customize the Blocking page** options are active.
3. Ensure that **Customize the Blocking page** is selected (the default setting), so that the options below are active.
4. Type the **Customized page title** (255 characters maximum).

Tip: Trend Micro suggests including your company name and a brief description, such as, "How To Remove Your Computer from Quarantine."

5. In the **Customized page URL** field (255 characters maximum) type the URL of the blocking page. (For example, the URL can be your company's Intranet antivirus page that provides the latest security patches and other antivirus-related information.)

Note: The **Customized page URL** must begin with `http://` or `https://`

6. In the **Customized page description** field (512 characters maximum), type the content for the notification page to display when the blocking page appears. Helpful information here might include instructions on what users can do to remove a computer from quarantine.

Note: If you do not wish to display the Damage Cleanup Services description and a link to it in the blocking page, select **Do not show the Damage Cleanup Services description and link in the Blocking page** under the **Customized page description** field.

To enable Damage Cleanup Services:

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

Note: Damage Cleanup Services must be activated on your Control Manager server before you can use it. 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 *Creating Exception Lists* on page 5-17 for more information.

Automating the Removal of Infected Clients from Quarantine

Network VirusWall can automatically remove infected clients from quarantine. In order for DCS to log in to the infected computer to clean it, DCS must be able to find the client in the **Account Manager Tool**. To 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).

Enabling Network Outbreak Monitor

A high number of simultaneous network sessions or connections on certain client ports is often a signal of an attack or virus infection. Use Network Outbreak Monitor to trigger an outbreak alert notification message when this occurs. If Network Outbreak Monitor triggers an alert, it sends a configurable message to specified recipients.

To enable and configure Network Outbreak Monitor:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Network Outbreak Monitor**.
4. Click **Next**.
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 how tolerant you would like Network VirusWall 1200 to be towards simultaneous network connections. The following options are available:
   - **High:** click to enable the most sensitive setting. Network VirusWall 1200 checks the network most often and does not tolerate many simultaneous network connections
   - **Medium:** click to enable a moderately sensitive setting. Network VirusWall 1200 only tolerates some simultaneous network connections
   - **Low:** click to enable the least sensitive setting. Network VirusWall 1200 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 5-17 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 Enforcement Policies

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.

Note: Network VirusWall Policy Enforcement is not enabled by default.

To enable and configure Network VirusWall Policy Enforcement:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Policy Enforcement**.
4. Click **Next**.
5. Select the **Enable Network VirusWall Policy Enforcement** check box.
6. Under **Policy Details**, select actions to take when Network VirusWall 1200 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™ 7.0 with Orchestrator agent**

    - **Norton Antivirus™ Corporate Edition™**
- **Windows clients with no identifiable antivirus products**
- **All un-identifiable 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 Policy Enforcement Services To Block* on page 5-10 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 1200 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 a vulnerability:

- **Block:** block specified traffic (to specify which types of traffic to block, select ports associated with TCP and UDP services. See *Configuring Policy Enforcement Services To Block* on page 5-10 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 1200 is not in outbreak prevention mode (normal mode) and when it is in outbreak prevention mode.

Note: 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 5-17 for more information.

8. Click **Save**.

   To block ports associated with certain services, click **Services to Block**. See *Configuring Policy Enforcement Services To Block* on page 5-10 for more information.

   To configure advanced settings, including client assessment frequency, policy tolerance, and details for identifiable antivirus software, click **Advanced Settings**. See *Configuring Advanced Settings* on page 5-13 for more information.

Configuring Policy Enforcement 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 1200 can block TCP and UDP traffic destined for ports that you specify. See *The "TCP services to block" section of the Block TCP and UDP Services screen* on page 5-11and *The "UDP services to block" section of the Block TCP and UDP services screen* on page 5-12.

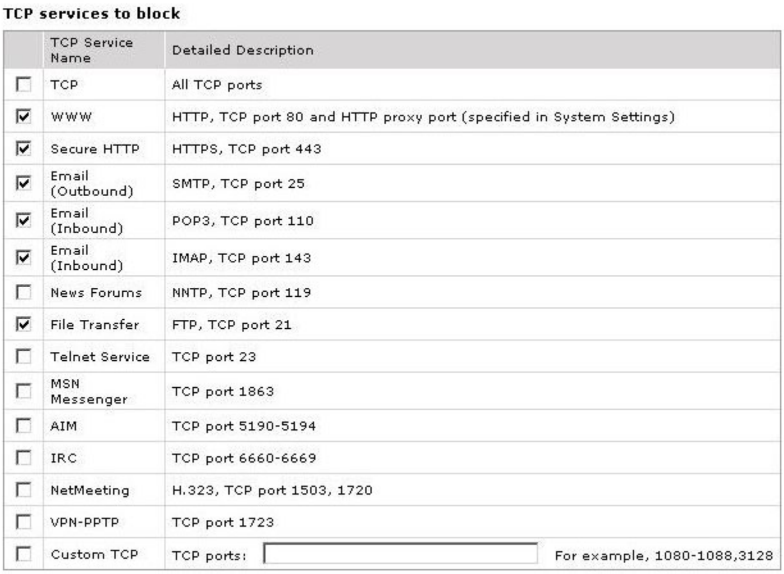
To block TCP services:

1. Access Network VirusWall 1200 from the Control Manager management console.
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 **Enable Network VirusWall Policy Enforcement** check box is selected and click **Services to Block**. The **Block TCP and UDP Services** screen displays.
6. In the **TCP services to block** section, select ports to block that are associated with TCP.

As shown in Figure 5-2 on page 5-11, these TCP 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



TCP services to block

	TCP Service Name	Detailed Description
□	TCP	All TCP ports
☑	WWW	HTTP, TCP port 80 and HTTP proxy port (specified in System Settings)
☑	Secure HTTP	HTTPS, TCP port 443
☑	Email (Outbound)	SMTP, TCP port 25
☑	Email (Inbound)	POP3, TCP port 110
☑	Email (Inbound)	IMAP, TCP port 143
□	News Forums	NNTP, TCP port 119
☑	File Transfer	FTP, TCP port 21
□	Telnet Service	TCP port 23
□	MSN Messenger	TCP port 1863
□	AIM	TCP port 5190-5194
□	IRC	TCP port 6660-6669
□	NetMeeting	H.323, TCP port 1503, 1720
□	VPN-PPTP	TCP port 1723
□	Custom TCP	TCP ports: ______ For example, 1080-1088,3128

FIGURE 5-2. The "TCP services to block" section of the *Block TCP and UDP Services* screen

---

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

---

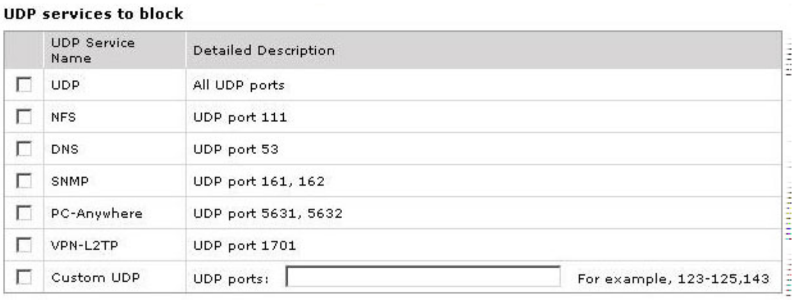
7. Click **Save**. The **Network VirusWall Policy Enforcement** screen appears again.

Note: Network VirusWall now allows you to set custom TCP ports. To do so, select **Custom TCP** and type the port numbers in the **TCP ports** field.

To block UDP services:

1. Access Network VirusWall 1200 from the Control Manager management console.
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 **Enable Network VirusWall Policy Enforcement** check box is selected and click **Services to Block**. The **Block TCP and UDP Services** screen displays.

In the **UDP services to block** section, select ports to block that are associated with UDP.



UDP services to block

	UDP Service Name	Detailed Description
□	UDP	All UDP ports
□	NFS	UDP port 111
□	DNS	UDP port 53
□	SNMP	UDP port 161, 162
□	PC-Anywhere	UDP port 5631, 5632
□	VPN-L2TP	UDP port 1701
□	Custom UDP	UDP ports: ▭ For example, 123-125,143

FIGURE 5-3. The "UDP services to block" section of the *Block TCP and UDP services* screen

---

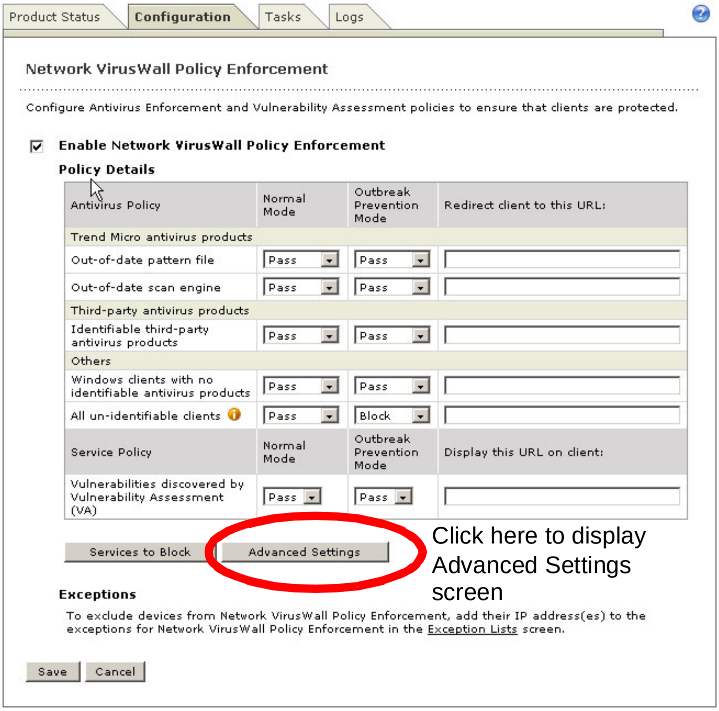
Note: Network VirusWall now allows you to set custom UDP ports. To do so, select **Custom UDP** and type the port numbers in the **UDP ports** field.

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 page 5-8).
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Policy Enforcement**.
4. Click **Next>>**. The **Network VirusWall Policy Enforcement** screen appears. See *The Network VirusWall Policy Enforcement screen* on page 5-13.



Network VirusWall Policy Enforcement

Configure Antivirus Enforcement and Vulnerability Assessment policies to ensure that clients are protected.

☑ **Enable Network VirusWall Policy Enforcement**

Policy Details

Antivirus Policy	Normal Mode	Outbreak Prevention Mode	Redirect client to this URL:
Trend Micro antivirus products			
Out-of-date pattern file	Pass	Pass	
Out-of-date scan engine	Pass	Pass	
Third-party antivirus products			
Identifiable third-party antivirus products	Pass	Pass	
Others			
Windows clients with no identifiable antivirus products	Pass	Pass	
All un-identifiable clients	Pass	Block	
Service Policy	Normal Mode	Outbreak Prevention Mode	Display this URL on client:
Vulnerabilities discovered by Vulnerability Assessment (VA)	Pass	Pass	

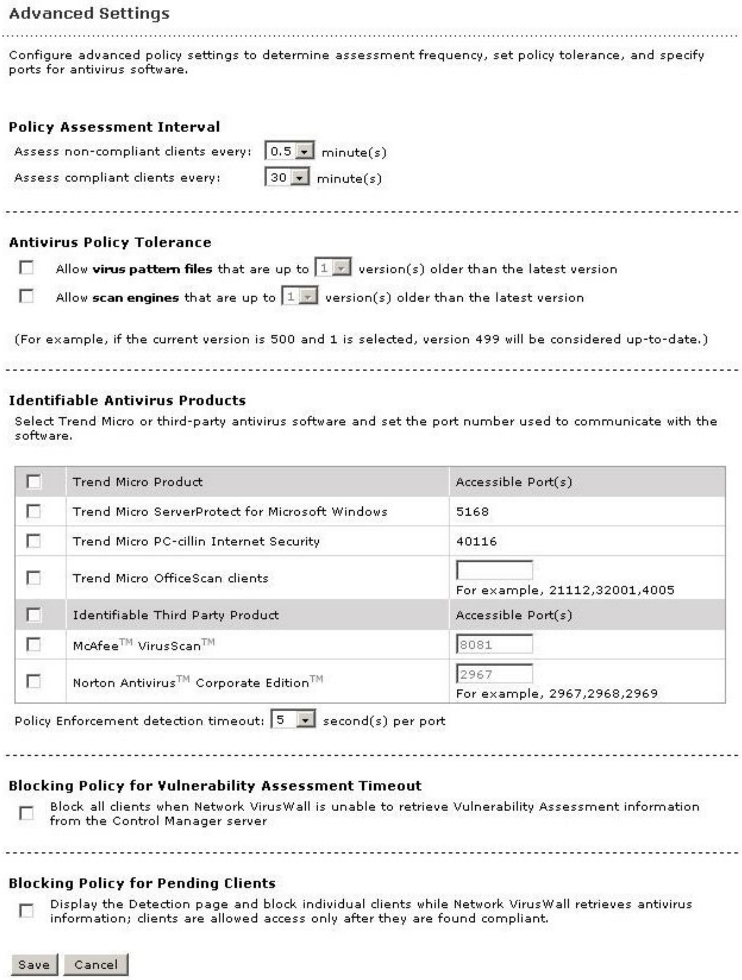
Click here to display Advanced Settings screen

Exceptions

To exclude devices from Network VirusWall Policy Enforcement, add their IP address(es) to the exceptions for Network VirusWall Policy Enforcement in the Exception Lists screen.

FIGURE 5-4. The *Network VirusWall Policy Enforcement* screen

5. Ensure the **Network VirusWall Policy Enforcement** check box is enabled, and then click **Advanced settings**. The **Advanced Settings** screen appears (see *The Advanced Settings screen* on page 5-14).



Advanced Settings

Configure advanced policy settings to determine assessment frequency, set policy tolerance, and specify ports for antivirus software.

Policy Assessment Interval

Assess non-compliant clients every: 0.5 minute(s)

Assess compliant clients every: 30 minute(s)

Antivirus Policy Tolerance

□ Allow **virus pattern files** that are up to 1 version(s) older than the latest version

□ Allow **scan engines** that are up to 1 version(s) older than the latest version

(For example, if the current version is 500 and 1 is selected, version 499 will be considered up-to-date.)

Identifiable Antivirus Products

Select Trend Micro or third-party antivirus software and set the port number used to communicate with the software.

□	Trend Micro Product	Accessible Port(s)
□	Trend Micro ServerProtect for Microsoft Windows	5168
□	Trend Micro PC-cillin Internet Security	40116
□	Trend Micro OfficeScan clients	For example, 21112,32001,4005
□	Identifiable Third Party Product	Accessible Port(s)
□	McAfee™ VirusScan™	8081
□	Norton Antivirus™ Corporate Edition™	2967 For example, 2967,2968,2969

Policy Enforcement detection timeout: 5 second(s) per port

Blocking Policy for Vulnerability Assessment Timeout

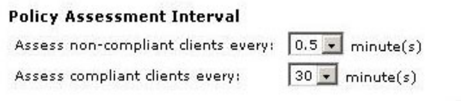
□ Block all clients when Network VirusWall is unable to retrieve Vulnerability Assessment information from the Control Manager server

Blocking Policy for Pending Clients

□ Display the Detection page and block individual clients while Network VirusWall retrieves antivirus information; clients are allowed access only after they are found compliant.

FIGURE 5-5. The *Advanced Settings* screen

6. Under the **Policy Assessment Interval** section, select a frequency to assess both clients that are compliant and non-compliant with the policy. Network VirusWall 1200 determines each client's compliance every time it performs a policy assessment. The first time Network VirusWall 1200 performs an assessment, all clients are considered compliant. See *The "Policy Assessment Interval" section of the Advanced Settings screen* on page 5-15.



Policy Assessment Interval

Assess non-compliant clients every: 0.5 minute(s)

Assess compliant clients every: 30 minute(s)

FIGURE 5-6. The "Policy Assessment Interval" section of the *Advanced Settings* screen

---

Tip: Trend Micro recommends the default settings of **0.5** minutes for **non-compliant clients** and **30** minutes for **compliant clients**. These settings help ensure that Network VirusWall checks non-compliant 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 1200 has 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 that are allowable.

Note: Network VirusWall recognizes a total of four scan engine versions and eight virus pattern file versions. After a scan engine update, Network VirusWall treats a new scan engine as the up-to-date version. The version it replaced is treated as one version out-of-date, and so on. However, after a virus pattern file update, the eight out-of-date versions are replaced with the most recent eight versions, and the most recent version is treated as the up-to-date version. See *Deploying Network VirusWall Components* on page 4-5 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 1200 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 1200 can identify the following antivirus installations:

   - Trend Micro™ ServerProtect™ for Microsoft™ Windows™
   - Trend Micro OfficeScan clients
   - Trend Micro PC-cillin Internet Security (version 11.35 and above)
   - McAfee™ VirusScan™ with Orchestrator agent
   - Norton Antivirus™ Corporate Edition™

   WARNING! *Network VirusWall cannot detect antivirus installations other than those listed above. Network VirusWall does not enforce policies 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 1200 stops 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. See *The Network VirusWall Policy Enforcement screen* on page 5-13

12. Click **Save**.

Note: Network VirusWall reverifies a blocked computer’s compliance status 30 seconds after the computer is blocked. If the blocked computer becomes compliant before policy violation is resolved within this interval, the computer remains blocked. However, during this 30-second interval, the computer can still connect to other computers within the Protected Network.

Windows/Office Update for Blocked Clients

One reason that a vulnerability policy may have blocked 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 5-13.)
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: If a client that is blocked by Vulnerability Assessment (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 4-6).

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).

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 Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, select **Exception 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 Enforcement Policies* on page 5-8 for more information)
    - **Enable safe sites for blocked and quarantined clients:** configure the safe site list that quarantined and blocked clients can access

    Note: For security reasons there is no exception setting to enable safe sites for Outbreak Prevention Policy violations.

    - **Enable Exceptions for Network Outbreak Monitor:** configure a list of computers exempted from Network Outbreak Monitor (see *Enabling Network Outbreak Monitor* on page 5-7 for more information)
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**.
8. To remove addresses from the list, click them in the list and click **Remove**. Use the `CTRL` or `SHIFT` keys to make multiple selections.
9. Click **Save**.

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

- Server components of Trend Micro products (for example, OfficeScan)
- Proxy servers that clients use to access the Internet
- DNS servers

- Computers 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.

Updating Components

To help ensure that all Network VirusWall 1200 devices help protect your network from the latest virus threats, regularly update their components. The following components can be updated:

- **Network scan engine:** scans traffic passing through Network VirusWall at the packet level. The network scan engine is specifically designed to find network viruses.
- **Network virus pattern file:** contains a regularly updated database of packet-level network virus patterns. Trend Micro often updates the network virus pattern file to ensure Network VirusWall can identify any new network viruses.
- **Network outbreak rule:** contains a regularly updated collection of behavior-based network threat rules. Trend Micro often updates the network outbreak rule to ensure Network VirusWall can identify potential network attacks which try to exploit the systems.
- **Program file:** the Network VirusWall 1200 program, also referred to as the image, which includes the operating system, system programs, and all components necessary to get Network VirusWall functioning properly
- **Damage cleanup template:** contains a regularly updated database of malware for use with Damage Cleanup Services

Configuring Update Settings

Use the Update Settings screen to configure an update source, including proxy settings if your network has a proxy server to connect to the Internet. Also configure an update schedule to deploy Network VirusWall 1200 components automatically.

To configure an update source:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **Update Settings**.
4. Click **Next**.
5. Under **Update Source**, choose whether to receive updates from the Trend Micro ActiveUpdate server or from another source and type the source URL.

Note: **Trend Micro ActiveUpdate server** is selected by default.

6. Click **Save**.

To configure proxy settings:

1. If you use a proxy server to connect to the Internet, select the **Use a proxy server to download update components from the Internet** check box.
2. Type the host name of the proxy server and its port number.
3. Select the protocol the proxy server uses: **HTTP**, **Socks 4**, or **Socks 5**.

   If your proxy server requires a password, type your user name and password under **Authentication**.
4. Click **Save**.

To configure an update schedule:

1. Select the **Enable scheduled update** check box.
2. Under **Select update components**, select the components to update:
   - **Network scan engine**
   - **Network virus pattern file**
   - **Network outbreak rule**

Tip: Trend Micro recommends selecting **Network virus pattern file** and **Network outbreak rule** as these components are often updated.

3. Under **Configure an update schedule**, specify a schedule to perform the updates:
    - **By minute:** click to update every { } minutes. Select a number of minutes from the list.
    - **Hourly, every:** click to update every { } hours. Select a number of hours from the list.
    - **Daily, every:** click to update every { } days. Select a number of days from the list.
    - **Weekly, every:** click to update every { } weeks. Select a day from the list.

    Regardless of the selection, specify when to perform the scheduled update in the **Start time** lists.
4. Click **Save**.

Performing Manual Update

Perform a Manual Update anytime to check for updated Network VirusWall components. Components that can be updated include the network virus pattern file, network scan engine, network outbreak rule, and program file. Network VirusWall 1200 takes the components from the update source that you specify in the **Update Settings** screen.

Tip: Trend Micro recommends updating components immediately after deploying Network VirusWall 1200 and whenever there is a virus outbreak.

To perform a Manual Update:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. In the main window, click the **Configuration** tab.
3. Under **Select configuration**, click **Manual Update**.
4. Click **Next**. The **Manual Update** screen displays showing a table of components to update, the version numbers of the components currently in use and the version number of the latest components available.

5. Select the components to update:
   - **Network scan engine**
   - **Network virus pattern file**
   - **Network outbreak rule**
   - **Program file**
6. Click **Update Now** to update the components.

Note: If the components are already up to date, the Manual Update does not execute.

Chapter 6

Viewing and Analyzing Antivirus Information

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 1200 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 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. Also un-quarantine infected clients and 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:
     - **NTKD** – for machines running Windows 95 (95, 98, and Me)
     - **VxD** – 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 5-13).

   The following icons represent client status:

   - ⊗ client is quarantined due to infection
   - ⛔ client is blocked due to a violation of Network VirusWall Policy Enforcement or Outbreak Prevention Policies (see *Configuring Enforcement Policies* on page 5-8 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 5-17 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 1200 to quarantine clients on the **Scan Options** screen (see *Configuring Scan Options* on page 5-2 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 the from the exception list for Network VirusWall Policy Enforcement by doing the following:
    - Select the client(s) to unblock and click **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 1200 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 1200-related information from the event logs:

- **Module updates:** updates to the Network VirusWall 1200 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 1200 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 event severity **Information** report Network VirusWall 1200-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 1200-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 time period. Log entries created during this time period display.

   To select a time 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 1200 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 1200. 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.

Viewing Security Logs

When Network VirusWall 1200 detects a virus or security violation, it creates a security log entry. Query and view the following types of Network VirusWall 1200-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 1200 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 a time period. Log entries created during this time period will display.

To select a time period 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 1200 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 1200. 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.

Using the Log Viewer

Network VirusWall 1200 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 System Settings* on page 4-6 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.
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 1200 generates them.

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

Chapter 7

Performing Administrative Tasks

This chapter explains how to perform important administrative tasks.

The topics discussed in this chapter include:

Replicating Configuration Settings

If you have more than one Network VirusWall 1200 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 1200 devices.

To replicate Network VirusWall 1200 settings:

1. Access Network VirusWall 1200 from the management console.
2. Click the **Tasks** tab.
3. Under **Select task**, select **Configuration Replication**.
4. Click **Network VirusWall 1200** under **Supported products**.

Note: The Control Manager server on your network may be managing products other than Network VirusWall 1200.

5. Click **Next**.
6. In the product directory, select the Network VirusWall device to receive the configuration settings.
7. Click **Replication**.

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 perform a reset.

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 Network VirusWall 1200 from the Control Manager management console.
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.
6. Click **Apply Now**.

Note: When Network VirusWall is physically turned off, all traffic is unblocked.

Resetting Network VirusWall

Reset Network VirusWall 1200 if you experience any problems or if the Control Manager management console prompts you to perform a reset.

Use the following methods to reset Network VirusWall 1200:

- The preconfiguration menu
- The **RESET** button on the front panel of the device
- The Control Manager management console

To reset Network VirusWall 1200 through the preconfiguration menu:

1. Log on the Network VirusWall 1200 terminal interface.
2. Type `7` in the main menu to select **System Tasks**. The **System Tasks** menu appears.
3. Type `4` to select **Reset Device**. A confirmation screen appears.
4. Type `y` and press `<ENTER>` to continue.

Note: See *Performing Preconfiguration* on page 3-1 for detailed information on using the preconfiguration menu through the terminal interface.

To reset Network VirusWall 1200 with the Reset button:

Press the Reset button on the front panel of the device. Network VirusWall 1200 resets (see *Hardware and Connections* on page 1-7).

To reset Network VirusWall 1200 through the Control Manager management console:

1. Access Network VirusWall 1200 from the management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **System Tasks**.
4. Click **Next**.
5. Click **Reset Now**.
6. Confirm the reset when prompted.

Note: While Network VirusWall is resetting, it will pass all traffic to and from the Protected Network.

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 7-1 for a summary of rescue mode settings.

WARNING! *Rescue mode is intended for troubleshooting only. Under normal circumstances you do not need to enter rescue mode. See Troubleshooting on page 9-4 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 7-1. Rescue mode settings

Enter rescue mode through the LCD module panel or the terminal interface.

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 terminal interface:

1. Reset Network VirusWall while logged on the terminal interface. See *Logging On to the Terminal Interface* on page 3-3 for information.
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.

Understanding the Program and Boot Loader Files

The Network VirusWall program file 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. The program file name is as follows:

```
NVW_Rescue_1242.R
```

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

```
NVW_Rescue_1242.B
```

You can obtain these files from two locations:

- **Trend Micro download Website** – contains the most up-to-date versions (www.trendmicro.com/download)
- **Trend Micro Solutions CD for Network VirusWall 1200** – the included CD contains the program file with factory defaults (see *Restoring Default Settings* on page 3-29) 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\
  ```

Uploading the Program File and Boot Loader

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
- **Network VirusWall 1200 Rescue Utility** – utilize a user-friendly Windows-based utility

Uploading via 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 1200*.
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 7-4).
4. Connect one end of the included cross-over Ethernet cable that came with the device to your computer's LAN port and the other end to either the **INT** port 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 *Understanding the Program and Boot Loader Files* on page 7-6 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 page 3-1 for more information).

Uploading with the Network VirusWall 1200 Rescue Utility

Uploading with the Network VirusWall 1200 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 1200 Rescue Utility can only be run on 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 via the Command Line* on page 7-6).

The utility is included on the *Trend Micro Solutions CD for Network VirusWall 1200*. 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 1200 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 1200 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 1200*.
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 7-4).
4. Connect one end of the included cross-over Ethernet cable to your computer's LAN port and the other end to the **INT** port 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 or reset the device or modify any device settings.If you uploaded the program file, wait for the device to finish the automatic reset.*

Chapter 8

SNMP and VLAN

This chapter provides information on two important Network VirusWall-supported technologies: Simple Network Management Protocol (SNMP) and IEEE 802.1Q Virtual Local Area Networks (VLANs). Network VirusWall can send traps to specific network management stations. It also recognizes tagged and non-tagged IEEE 802.1Q VLANs and preserves the existing VLAN settings on your network. Network VirusWall supports SNMP version 2c for SNMP traps and SNMP versions 1 and 2c for the SNMP agent.

The topics discussed in this chapter include:

About Simple Network Management Protocol

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.

SNMP Architecture

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.

SNMP Agent Management Information Base

On the agents, information is organized 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. The objects are grouped into 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.

SNMP 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 an SNMP agent shutdown or an authentication error.

SNMP Communications

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 more specific functions.

SNMP 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 NMSs 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.

Network VirusWall 1200 and SNMP

Network VirusWall 1200 supports SNMP with the following specifications:

Network VirusWall 1200 SNMP Agent

- **Versions:** 1 and 2c
- **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:** communities have the following characteristics:
  - **Default community name:** public
  - **Access privileges:** READ ONLY (the **get** command)
  - **Maximum number of community names:** 5 community names
  - **Community name character limitations:** 1 ~ 33 alphanumeric characters (including underscore: "_")

- **Trusted Network Management Stations (NMS):** allows up to 255 specific network management station IP addresses to access the agent (by default, any all NMSs are allowed)

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. Click the **NVW SNMPv2 MIB file** link. to download the `nvw_mib2.zip` file.
5. Unzip the file.

Network VirusWall 1200 SNMP Traps

See Table 8-1 for a list of traps Network VirusWall can send to Network Management Stations.

Trap Name	Trap Description: (when Network VirusWall 1200 sends the trap)
Coldstart	enable SNMP agent
Linkdown	network connection broken
Linkup	network connection established
Authentication failure	wrong user name or password when logging in the terminal interface
NotifyShutdown	SNMP agent disabled

TABLE 8-1. Supported SNMP traps

SNMP Trap Limitations

The following SNMP trap limitations exist:

- **Version supported:** 2c
- **Community Names:**
    - Limited to one community name
    - 1–33 alphanumeric characters (including underscore: "_")
- **Destination Network Management Station (NMS) IP addresses:** Limited to one NMS IP address

SNMP Agent Limitations

The following SNMP agent limitations exist:

- **Version supported:** 2c
- **System location and System contact:** 0–254 characters (ASCII 32–126, excluding "&")
- **Community Names**:
    - Limited to 5 community names
    - 1–33 alphanumeric characters (including underscore: "_")
- **Destination Network Management Station (NMS) IP addresses:** Limited to 255 NMS IP addresses

Configuring SNMP Notifications

Configure Simple Network Management Protocol (SNMP) notification settings to allow a network management station to receive traps from Network VirusWall. Also enable the SNMP agent, which adds security to SNMP communications. See *About Simple Network Management Protocol* on page 8-2 for more information on SNMP.

Tip: Trend Micro recommends enabling all SNMP agent community options for added security. This ensures only specific network management stations are able to access Network VirusWall 1200 after authenticating to the device.

To enable SNMP traps:

1. Access Network VirusWall 1200 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 1200 will send traps.
7. Click **Save**.

To enable SNMP agent:

1. Access Network VirusWall 1200 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 1200 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 1200 (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 1200 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**.

About VLANs

A Virtual Local Area Network (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 are. They are connected 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). Generally speaking, 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 1200 and VLANs

Network VirusWall 1200 will recognize both tagged and non-tagged IEEE 802.1 Q VLAN frames, thereby preserving the VLAN structure on your network. Using the existing VLAN membership settings on your network, configure Network VirusWall 1200 to recognize up to 50 VLAN IDs within a valid ID range of 1 to 4094. VLAN configuration can only be done while performing preconfiguration (see *Configuring VLAN Settings* on page 3-17 for more information).

Note: If the Control Manager server on your network belongs to a VLAN, bind the Network VirusWall IP address to the same IEEE 802.1Q VLAN (tagged or non-tagged). This will help ensure effective communication between the Control Manager server and Network VirusWall 1200.

VLAN IP Binding Example

If you are deploying Network VirusWall in a multiple VLAN environment, bind the Network VirusWall IP address to the VLAN ID that corresponds to the network segment on which the device is located. Trend Micro also recommends placing the Control Manager server on the same segment. The following is an example:

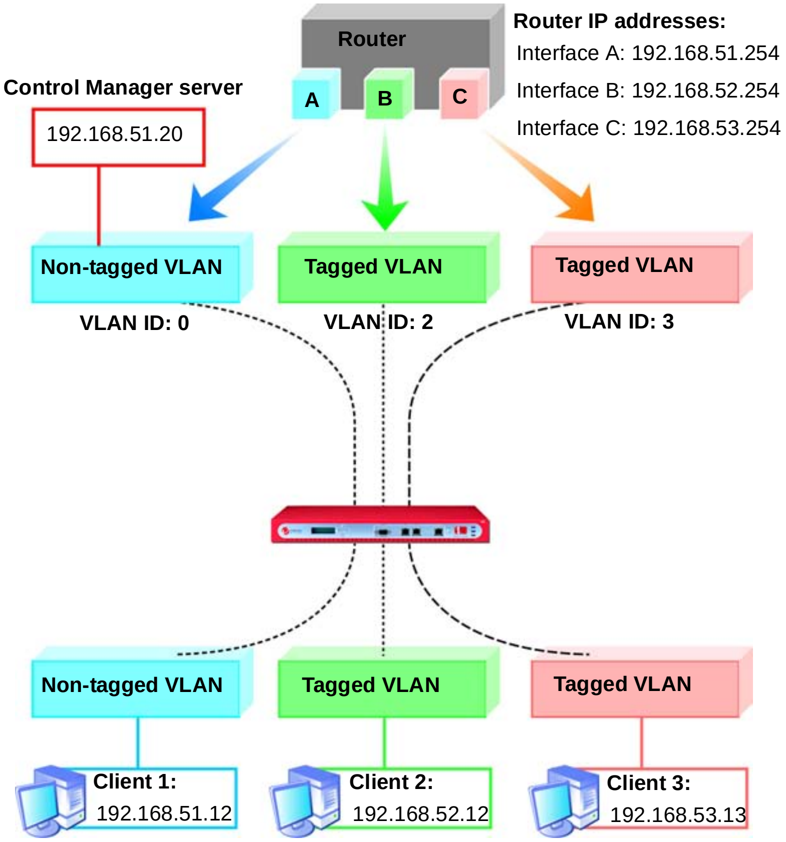


FIGURE 8-1. VLAN IP binding example

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

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

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

Table 8-2 illustrates where you should bind the Network VirusWall IP address if you change it:.

Network VirusWall IP address	Bind to this VLAN ID
192.168.51.11	VLAN ID 0
192.168.52.11	VLAN ID 2
192.168.53.11	VLAN ID 3

TABLE 8-2. VLAN IP binding example

Note: The only way to change VLAN settings is to perform preconfiguration. See *Performing Preconfiguration* on page 3-1 for more information.

Dual-switch VLAN configurations

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

Most VLAN configurations will utilize two switches. Single-switch VLAN configurations are possible; for more information refer to *Single-switch Configurations* on page 8-13. The figures in this section illustrate multiple downstream switches in a flat topology, however, a single in line configuration is also possible.

In Figure 8-1 on page 8-9, Network VirusWall devices are installed between an upstream switch and downstream switches. This configuration is appropriate when multiple VLANs carry moderate network traffic, and the upstream switch carries high-bandwidth traffic. The upstream switch carries traffic on VLANs 10, 20, and 30, and the downstream switches carry traffic for individual VLANs.

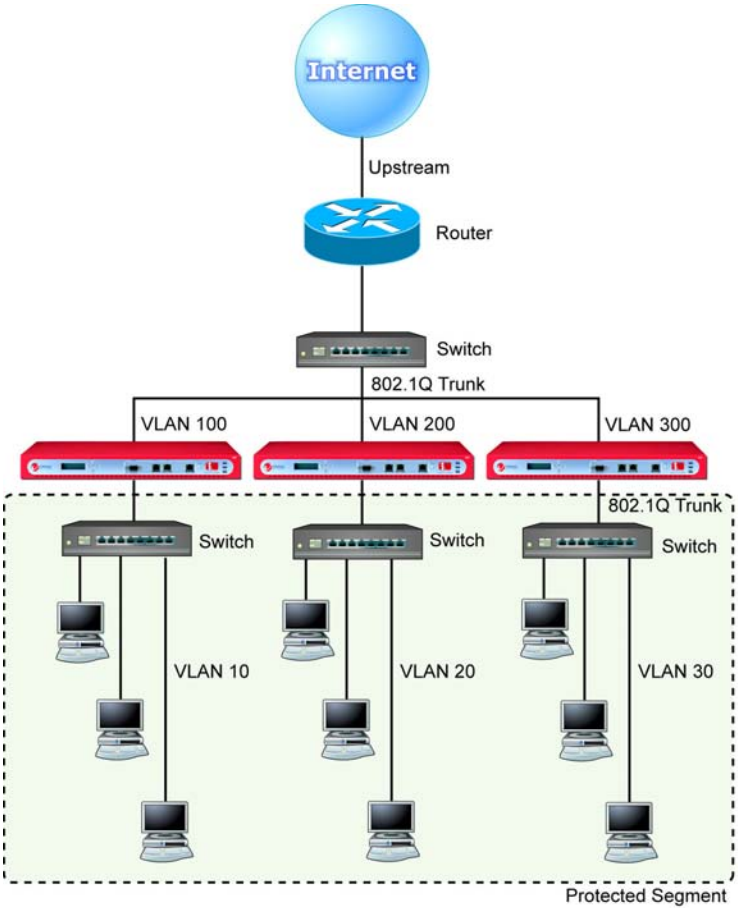


FIGURE 8-2. Multiple VLAN segments with each Network VirusWall protecting one segment

In Figure 8-3 on page 8-12, Network VirusWall devices are installed on a 802.1Q trunk line between two switches. The upstream switch is configured to handle high-bandwidth traffic on VLANs 10, 20, and 30. Downstream switches handle lower bandwidth traffic on VLANs 10, 20, and 30. This configuration is appropriate when VLANs span multiple physical local area networks, or are defined logically for the purpose of separating user groups.

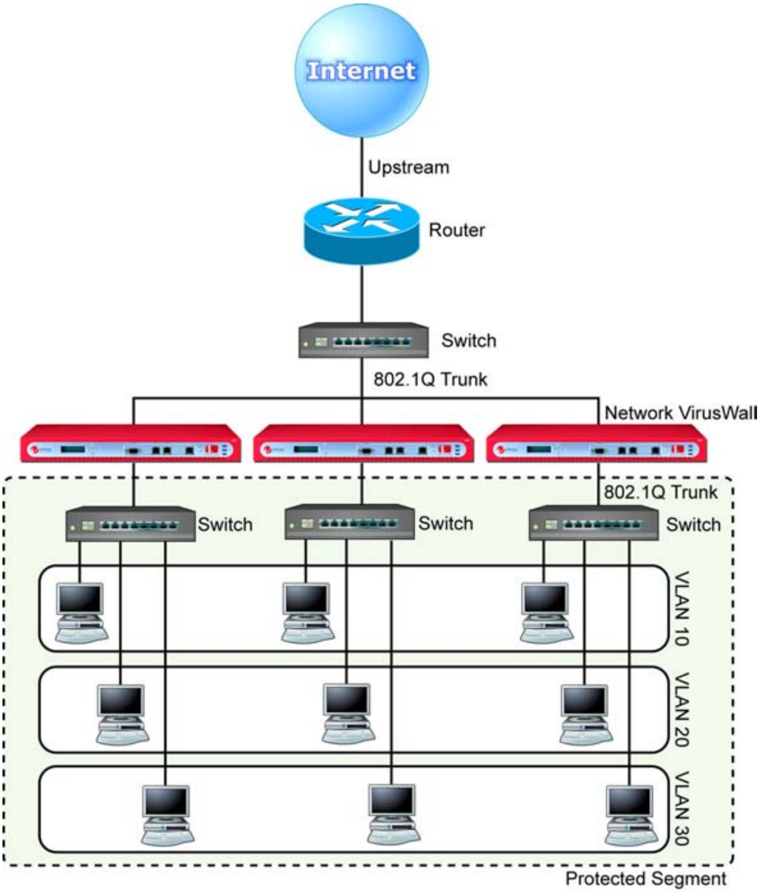


FIGURE 8-3. Multiple VLAN segments with each Network VirusWall protecting all segments

Single-switch Configurations

The single-switch configuration that appears in Figure 8-4 on page 8-13 is only possible when using a switch that can be configured to carry individual VLAN traffic on specific physical ports. In Figure 8-4 on page 8-13, VLAN 20 is assigned to ports 1 and 2, and VLAN 200 is assigned to ports 3 and 4. The upstream network is connected to port 4, the **Ext** port on Network VirusWall connected to port 3, The **Int** port on Network VirusWall is connected to port 2, and the downstream network connected to port 1.

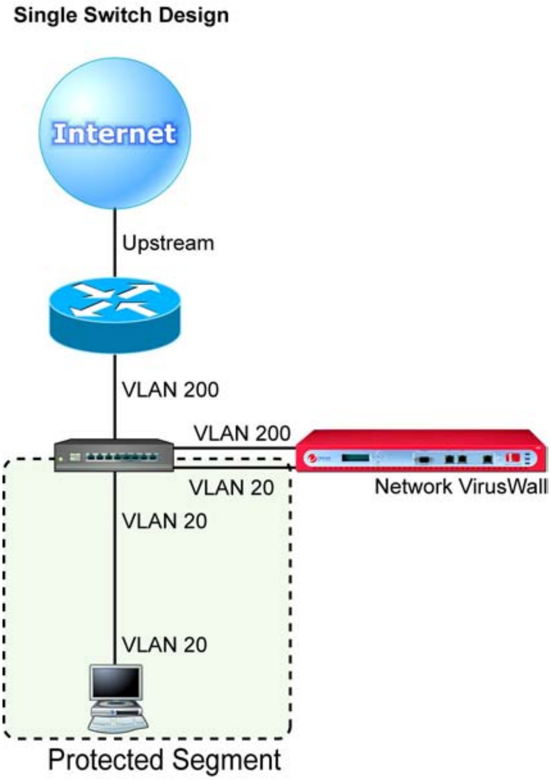


FIGURE 8-4. Single-switch configuration

The configuration shown in Figure 8-5 on page 8-14 is only possible using a switch that has ports that can be individually assigned to VLANs and that support load-balancing between multiple ports. This configuration is well suited for use in high-bandwidth networks where one Network VirusWall device placed in line would create a bottleneck.

In Figure 8-5 on page 8-14, VLAN 20 is assigned to ports 1 and 2, and VLAN 200 is assigned to ports 3 and 4. The upstream network is connected to port 4, the **Ext** port on Network VirusWall connected to port 3, The **Int** port on Network VirusWall is connected to port 2, and the downstream network connected to port 1.

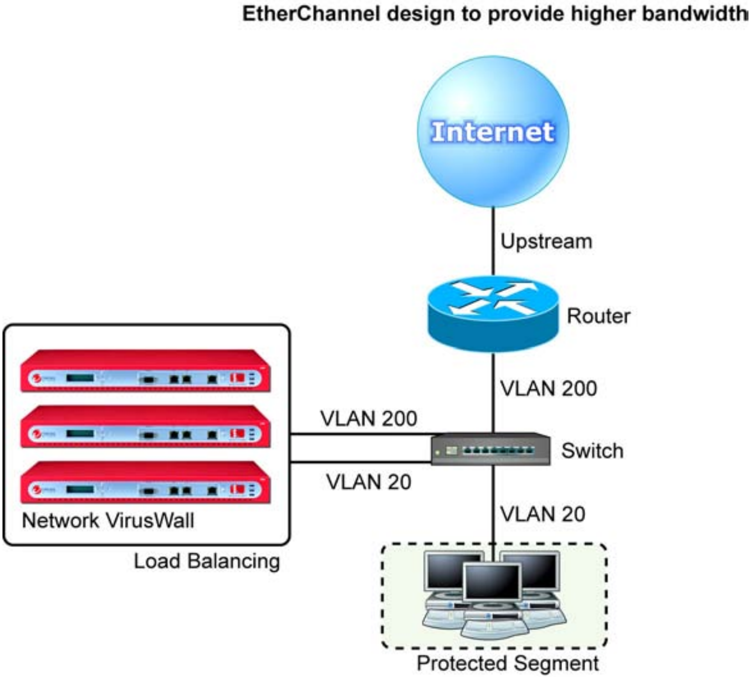


FIGURE 8-5. Single-switch configuration with multiple Network VirusWall devices using load balancing

Viewing VLAN Settings

View information for tagged and non-tagged Virtual Local Area Networks (VLANs) configured during preconfiguration. See *About VLANs* on page 8-7 for more information on VLAN.

To view VLAN information:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Configuration** tab.
3. Under **Select configuration**, click **VLAN Information**.
4. Click **Next**. The read-only **VLAN Information** screen shows the following:
    - **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)

Note: The only way to change VLAN settings is to perform preconfiguration. See *Performing Preconfiguration* on page 3-1 for more information.

Chapter 9

Technical Support, Troubleshooting and FAQs

This chapter provides technical support information, addresses troubleshooting issues that may arise, and answers frequently asked questions.

The topics discussed in this chapter include:

Contacting Technical Support

A license to Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year, after which you must purchase renewal maintenance on an annual basis to continue receiving these services.

You can contact Trend Micro via fax, phone, and email, or visit us at www.trendmicro.com. Evaluation copies of all Trend Micro products can be downloaded from our Web site.

Trend Micro Incorporated
10101 N. De Anza Blvd.
Cupertino, CA 95014-9985

Tel: +1-408-257-1500
Fax: +1-408-257-2003

Web: http://www.trendmicro.com
Knowledge Base: http://kb.trendmicro.com/solutions/

You can download evaluation copies of all Trend Micro software from the Web site, `www.trendmicro.com`.

For contact information in your country or region, refer to:
`www.trendmicro.com/en/about/contact/overview.htm`

Online Resources

Email: info@trendmicro.com
sales@trendmicro.com

Security Information

Comprehensive security information is available at the Trend Micro Web site:
`www.trendmicro.com/vinfo/`

Use the Web site to learn about:

- Computer virus hoaxes
- A weekly virus alert, listing the viruses that will trigger during the current week
- How to determine if a virus detection is a false alarm

- Trend Micro™ Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- Trend Micro virus reading room, with dozens of articles about the latest issues in computer viruses, including the threat posed by Java applets and ActiveX controls
- Product details and white papers

Knowledge Base

Trend Micro provides Knowledge Base, an online database filled with answers to technical product questions. Use it, for example, if you are getting an error message and want to find out what to do to. Type the following URL in your browser's address bar:
`kb.trendmicro.com/solutions/`

New solutions are added daily. However, if you do not find the answer you seek, you can submit your question online, where a TrendLabs engineer will provide you with an answer or contact you for more information.

TrendLabs

TrendLabs is a global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.

TrendLabs makes up the backbone of the Trend Micro customer service infrastructure. It continuously monitors potential security threats around the world and conducts virus-related research aimed at identifying, detecting, and eliminating new viruses. These efforts result in frequent virus pattern file updates and scan engine refinements.

Staffed by a team of several hundred engineers and certified support personnel, TrendLabs also provides a wide range of product and technical support services to customers worldwide. Dedicated service centers are located in Lake Forest, CA, Tokyo, Manila, Taipei, Munich, and Paris to ensure the most rapid response to virus outbreak and urgent customer support matters.

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.

Troubleshooting

The section covers hardware and configuration troubleshooting issues.

Hardware Issues

#	ISSUE	CORRECTIVE ACTION
1	LEDs do not illuminate	Verify secure power cable and network cable connections (see *Hardware and Connections* on page 1-7 and the *Network VirusWall 1200 Quick Installation Guide* for more information). If the error persists, there may be a hardware problem. Contact your vendor.
2	Unable to access the terminal interface	Verify secure console port connections and terminal communications software settings (see *Using the Terminal Interface* on page 3-3 for more information).
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 return button ↵. If the return button does not respond, verify that no user is logged on to NVW's terminal interface. If a problem with any LCD module buttons persist, there may be a hardware problem. Contact your vendor.
4	The **POLICY** LED is illuminated (red steady)	Antivirus policy enforcement and Vulnerability Assessment are not operational due to a memory problem. Network VirusWall will drop all network packets. Reset Network VirusWall (see *Resetting Network VirusWall on page 7-3*).

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 the you have correctly performed preconfiguration (see *Hardware and Connections on page 1-7* and *Preconfiguration Overview on page 3-2* for more information). If you changed the Network VirusWall IP address, manually reset the device to allow it to register to the Control Manager server. If Control Manager 3.0 is installed on a server running Windows 2003 member server, 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 is displayed 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 (see *VLAN IP Binding Example on page 8-8* for more information.

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 1200 is turned off, or is disconnected from the network, the Control Manager agent for Network VirusWall is not given the opportunity to inform Control Manager that it is going offline. As a result, it relies on Control Manager’s status verification mechanism to update its operating status. If the default heartbeat settings are used, Control Manager may require up to 180 minutes to update the status. The actual time would depend on when Network VirusWall sent its last heartbeat. See the *Control Manager Getting Started Guide* and online help for information on changing Heartbeat settings.
5	Network VirusWall is unable to communicate with Vulnerability Assessment (VA)	Ensure that VA is activated (see the *Control Manager Getting Started Guide*). Verify that the Control Manager Web server port is correct. This port was configured during Control Manager installation (see *Configuring System Settings on page 4-6*).

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 Summary** table, click the number of blocked clients under **Machine Count**. 4. Click **Block**.
7	The message "get key error" displays on the LCD module	The LCD module display shows "get key error" until you log on the terminal interface and press <ENTER> or until you press the **ENTER** button on the front panel.
8	Blocked clients are not able to access Damage Cleanup Services (DCS) to issue a cleanup request	Ensure that DCS is activated (see the *Control Manager Getting Started Guide*) and enabled (see *Configuring Scan Options on page 5-2*).
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).
10	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 4-6*).

11	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.
12	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 quarantining and blocking clients		
13	Network VirusWall is not quarantining clients whose packets are infected.	Check your scan options settings (see *Configuring Scan Options on page 5-2*). Network VirusWall quarantines a maximum of 2048 clients and drops all network traffic from additional clients (over 2048) whose packets are infected. Reconsider your deployment plan to take into consideration the number of clients on the Protected Network.
14	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. Click **mail.** A screen shows that the Yahoo! ID is locked. Follow the directions on the screen to unlock the ID.
15	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 Policy Enforcement Services To Block on page 5-10* for more information).
16	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.
Issues with enforcing policies		
17	Network VirusWall Policy Enforcement does not 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 can not detect client information. Consider the design of your network configuration regarding subnetting and the placement of routing devices.

18	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).
19	Clients blocked due to being assessed as vulnerable by Vulnerability Assessment are unable to start a vulnerability re-assessment.	Same as above.
20	Some clients on the Network VirusWall Policy Violations Summary screen are unable to be removed from the exception list	If a client’s IP address is included in a range of IP addresses that has been added to the exception list for Network VirusWall Policy Enforcement, you can not 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 5-17* for more information).
21	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.
22	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.

23	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.
24	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 will actually send packets to the proxy using a proxy port; the proxy will be responsible for actual packet delivery. Unless the proxy itself is within the Protected Network, Network VirusWall will not block the client traffic.
25	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.**
Other issues		
26	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 *Configuring Update Settings on page 5-19*). 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 5-17*).
27	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 *Enabling Network Outbreak Monitor on page 5-7*).

28	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 that your network DHCP and DNS server settings are correct (see *Configuring System Settings on page 4-6*).
29	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.

Frequently Asked Questions

This section answers common questions you may have about Network VirusWall 1200.

Where are logs stored and how can they be accessed?

Network VirusWall 1200 only uses a 128MB compact flash card 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. On the other hand, system logs (which also include debug information) can be sent to any computer on the network. See *Configuring System Settings on page 4-6* for more information.

What is the third network port used for?

The Network VirusWall 1200 device comes with three network ports:

- **INT (Internal)** – connects to the segment of the network the Network VirusWall will protect
- **EXT (External)** – connects to the segment of the network that leads to the public network
- **unlabeled** – disabled in Network VirusWall 1200. This port will be used in future Network VirusWall models.

Can Network VirusWall 1200 devices be connected or stacked together to improve throughput?

Network VirusWall 1200 devices are designed for parallel connections, not serial connections and therefore cannot be connected together.

If a malfunction occurs that prevent Network VirusWall 1200 from operating, will the Protected Network traffic be blocked?

Network VirusWall 1200 has a built-in LAN bypass feature. This helps ensure that in the event of a hardware or software failure, all network traffic will pass freely through the device. Traffic from the Protected Network will not be blocked.

Can I PING Network VirusWall 1200 to see if it is on the network?

Yes. Network VirusWall 1200 now allows users to ping it to verify that it is on the network.

Can I enable SSL Web browser security with Damage Cleanup Services and Vulnerability Assessment?

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?

Yes, Network VirusWall 1200 can be used on a network that uses a Network Address Translation (NAT) device. To configure Network VirusWall to work with your NAT, you must enable IP port forwarding on the NAT device and enable NAT mode on the Control Manager server. See *Using Network VirusWall in a Network with a NAT Device on page 3-6* for detailed instructions.

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

Network VirusWall 1200 is unable to block Instant Messaging (IM) services if those services utilize a proxy server.

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.

Device Specifications

This appendix provides general system and hardware specifications for Network VirusWall 1200.

Physical	
Height	1.75" (44.4mm)
Depth	12.6" (320.5mm)
Width	16.8" (426mm)
Weight	9.9 lbs. (4.5Kg)
Processor system	
CPU	Intel Celeron 1.2 GHz, 256KB L2 cache
Chipset	Intel 815E
BIOS	Award 4 Mb Flash
Bus	
PCI	32-bit/33MHz
Memory	
Technology	PC-133 SDRAM
Max. Capacity	256 MB

Socket	144-pin SO-DIMM	
Ethernet		
Interface	10/100 Base-TX (3 ports)	
Controller	Intel 82562ETx1 i82559ERx2	
Connector	RJ-45 x3	
Fail-Over	Ethernet bypass support	
Cooling		
Blower	1 (3CFM), 1 (4 CFM)	
Management		
Serial connection	RS-232 x1	
Power Adaptor	**Input**	**Output**
	AT PS, AC voltage: 90 ~ 264V @ 47 ~ 63 Hz, full range	180 W
Environmental	**Operating condition**	**Non-operating**
Temperature	32 ~ 104°F (0° ~ 40°C)	-4 ~ 167°F (-20° ~ 75°C)
Humidity	5 ~ 85% @ 104°F (40°C)	5 ~ 95%
Performance		
Maximum throughput	180 Mbps	
Maximum concurrent connections	68,000 connections	

Appendix B

Box Contents

This appendix provides a list of the Network VirusWall 1200 box contents.

Quantity	Component	Details and specifications
1	Network VirusWall 1200 appliance	See *Device Specifications* on page A-1.
1	Power cable	
1	Ethernet cable	CAT-5 crossover cable with RJ 45 connectors used for entering rescue mode only (see *Using the LCD Module Panel* on page 3-31).
1	Serial cable	2 meter cable with R232 connectors for performing preconfiguration through the terminal interface (see *Using the Terminal Interface* on page 3-3)
2	Keep ears and screws	
1	Trend Micro Solutions CD for Network VirusWall 1200	Trend Micro Control Manager 3.0 Installation Wizard, rescue utility, program file and boot loader, and documentation (including *Network VirusWall 1200 Administrator's Guide*, readme files, and *Control Manager Getting Started Guide*)
1	Safety sheet	Safety recommendations and warnings
1	Warranty card	Trend Micro warranty policy

Index