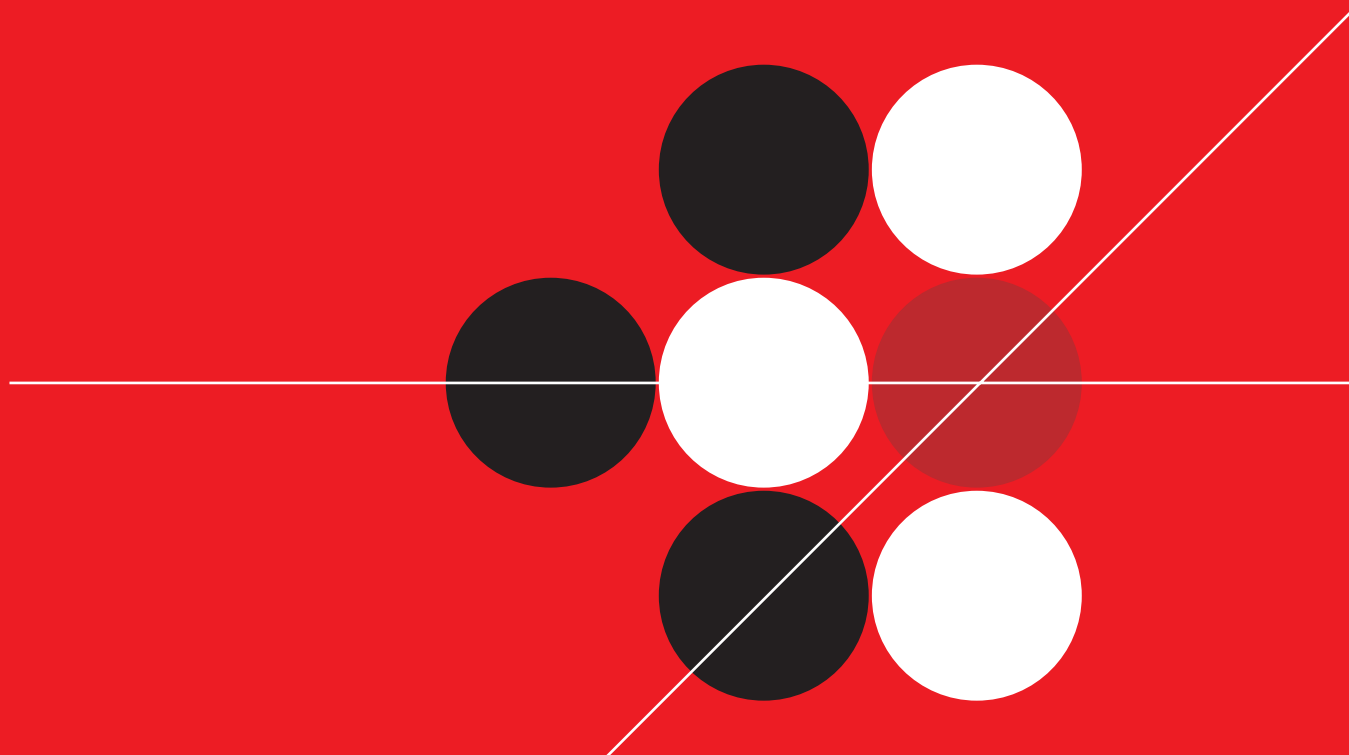
TREND MICRO™

Network VirusWall™ Enforcer 1200

Getting Started Guide



Document Part No. NVEM1267/60313

Release Date: January 2007

The user documentation for Trend Micro Network Virus Wall 1200 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

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

Contents

Preface

Network VirusWall Enforcer 1200 Documentation P-2
About This Getting Started Guide P-3
Audience P-4
Document Conventions P-4

Chapter 1: Getting Started

Package Contents 1-2
Network VirusWall Enforcer 1200 Front Panel 1-4
LED Indicators 1-4
Port Indicators 1-5
Network VirusWall Enforcer 1200 Back Panel 1-6
Dimensions and Weight 1-7
Power Requirements and Environmental Specifications 1-7

Chapter 2: Introducing Trend Micro™ Network VirusWall™ Enforcer 1200

Network VirusWall Enforcer 1200 2-2
Introducing Network VirusWall Enforcer 1200-specific Terms 2-3
Trend Micro Network VirusWall Enforcer 1200 Web Console 2-4
Understanding Network VirusWall Enforcer Ports 2-5
Deployment Overview 2-5

Chapter 3: Deploying Network VirusWall™ Enforcer 1200

Planning for Deployment 3-2
Deployment Overview 3-2
Phase 1: Plan the Deployment 3-3
Phase 2: Perform Preconfiguration 3-3
Phase 3: Manage Network VirusWall Enforcer 1200 Devices ... 3-3
Deployment Notes 3-4
Identifying What to Protect 3-5
Remote Access Endpoints 3-5
Guest Endpoints 3-9
Key Network Segments/Important Network Assets 3-9
Dual-switch VLAN Environment 3-11
Single-switch VLAN Environment 3-14
Planning for Network Traffic 3-15
Determining the Number of Devices to Deploy 3-15
Conducting a Pilot Deployment 3-16
Choosing a Pilot Site 3-16
Creating a Contingency Plan 3-16
Deploying and Evaluating your Pilot 3-16
Redefining Your Deployment Strategy 3-17
Deploying Network VirusWall Enforcer 1200 3-17
A Basic Deployment Scenario 3-18
Failopen Deployment 3-18

Chapter 4: Preparing for Preconfiguration

Preparing for Preconfiguration 4-2
Network VirusWall Enforcer 1200 Initial Tasks 4-2

Chapter 5: Preconfiguring Network VirusWall Enforcer 1200

Understanding Preconfiguration 5-2
Choosing the Preconfiguration Method 5-3
Using the Preconfiguration Console 5-3
Using the LCD Module 5-3
Performing Preconfiguration Using the Preconfiguration Console 5-5
Preparing the Preconfiguration Console 5-6
Logging on the Preconfiguration Console 5-7
Configuring Device Settings 5-11

Setting the Interface Speed and Duplex Mode 5-14
Logging off the Preconfiguration Console 5-15
Performing Preconfiguration Using the LCD Module 5-16
Connecting to the Network 5-18

Chapter 6: Configuring Network VirusWall Enforcer 1200

Configuring PEAgent Settings for Manual Deployment 6-2
Updating Components Manually 6-7

Chapter 7: Troubleshooting Preconfiguration

Device Issues 7-2
Contacting Technical Support 7-3

Index

Preface

Welcome to the Trend Micro™ Network VirusWall™ Enforcer 1200 Getting Started Guide. This book contains basic information about the tasks you need to perform to deploy the device. It is intended for novice and advanced users of Network VirusWall who want to plan, deploy, and preconfigure Network VirusWall Enforcer 1200.

This preface discusses the following topics:

- *Network VirusWall Enforcer 1200 Documentation* on page 2
- *About This Getting Started Guide* on page 3
- *Audience* on page 4
- *Document Conventions* on page 4

Network VirusWall Enforcer 1200 Documentation

The Network VirusWall Enforcer 1200 documentation consists of the following:

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

  The Online Help contains explanations about device components and features.

- Upgrade Guide (UG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site.

  The UG contains explanations about upgrading from previous Network VirusWall 1200 versions to Network VirusWall Enforcer 1200.

- Getting Started Guide (GSG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site

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

  If you are planning a large-scale deployment or have a complex network architecture and need more details about product architecture, refer to the *Network VirusWall Enforcer 1200 Administrator's Guide*.

- Administrator's Guide (AG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site

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

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

About This Getting Started Guide

The *Network VirusWall Enforcer 1200 Getting Started Guide* discusses the following topics:

- *Introducing Trend Micro™ Network VirusWall™ Enforcer 1200*—an overview of the device and its components
- *Getting Started*—details of the actual device and its specifications, including instructions for mounting and powering on the device
- *Deploying Network VirusWall™ Enforcer 1200*—recommendations to help you plan for the deployment of one or more devices
- *Preconfiguring Network VirusWall Enforcer 1200*—step-by-step instructions on how to install Trend Micro Control Manager and the necessary patches, including considerations and procedures on how to perform preconfiguration
- *Troubleshooting Preconfiguration*—troubleshooting tips for issues encountered during preconfiguration

Audience

The Network VirusWall Enforcer 1200 documentation assumes a basic knowledge of security systems, including:

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

Document Conventions

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

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

TABLE 1. Conventions used in the documentation

Chapter 1

Getting Started

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

This chapter contains the following topics:

- *Package Contents* on page 1-2

After completing the procedures in this chapter, proceed by:

- *Conducting a Pilot Deployment on page 3-16*
- *Deploying Network VirusWall Enforcer 1200* on page 3-17
- *Redefining Your Deployment Strategy* on page 3-17
- *Performing Preconfiguration Using the Preconfiguration Console* on page 5-5

Package Contents

Figure 1-1 illustrates the package contents.

FIGURE 1-1. The package contents

Tip: Refer to *Table 1-1* to check whether the package is complete. If any of the items are missing, please contact Trend Micro support (*See Contacting Technical Support on page 7-3*).

Table 1-1 specifies each item:

QUANTITY	ITEM	DESCRIPTION
1 unit	Network VirusWall Enforcer 1200	The device.
1 piece	Power cord	Supplies power to the device (length is 79 in/200 cm).
1 piece	Ethernet cable (RJ-45 crossover cable)	Connects a device to a computer used during Rescue Mode (length is 39 in/100 cm).
1 piece	Console cable (RS-232)	Connects the device to the computer used during preconfiguration (length is 79 in/200 cm).
1 set	Rack Ears	Mounts a Network VirusWall Enforcer 1200 to a standard 19 in rack cabinet.
1 CD	Trend Micro Solutions CD for Network VirusWall Enforcer 1200	Contains patches, hot fix installers, tools, and documentation. The PDF documentation includes: • *Trend Micro Network VirusWall Enforcer 1200 Upgrade Guide* • *Trend Micro Network VirusWall Enforcer 1200Getting Started Guide* • *Trend Micro Network VirusWall Enforcer 1200 Administrator's Guide* **Note:** Refer to *Troubleshooting* in the *Administrator's Guide* for instructions on how to use these tools.
2 books 1 sheet	*Trend Micro Network VirusWall Enforcer 1200 Upgrade Guide* *Trend Network VirusWall Enforcer 1200 Getting Started Guide* Trend Micro Network VirusWall Enforcer 1200 Safety Sheet	Printed *Trend Micro Network VirusWall Enforcer 1200 Upgrade Guide, Trend Micro Network VirusWall Enforcer 1200 Getting Started Guide,* and Safety Sheet.

TABLE 1-1. Network VirusWall Enforcer 1200 package contents

Network VirusWall Enforcer 1200 Front Panel

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

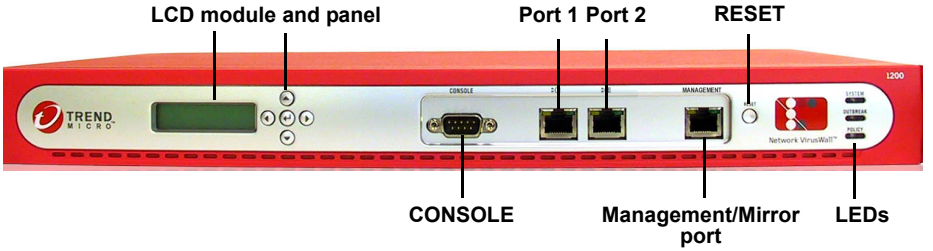


FIGURE 1-2. Network VirusWall Enforcer 1200 front panel

The following table describes each front panel element:

ELEMENT	DESCRIPTION
Liquid Crystal Display (LCD)	A 2.6 in x 0.6 in (65 mm x 16 mm) dot display LCD that is capable of displaying messages in 2 rows of 16 characters each.
Panel	5-button control panel that provides LCD navigation.
RESET Button	Resets the device.
Ports 1, 2	The Network VirusWall Enforcer 1200 documentation refers to each port by its number (for example, port 1 or 2).
Management Port	Connect to this port to access the Network VirusWall Enforcer Preconfiguration console. This port can also be used as a mirror port.

TABLE 1-2. Front panel description

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

LED Indicators

Network VirusWall Enforcer 1200 has three **l**ight-**e**mitting **d**iodes (LEDs) that indicate the **SYSTEM**, **POLICY**, and **OUTBREAK** status.

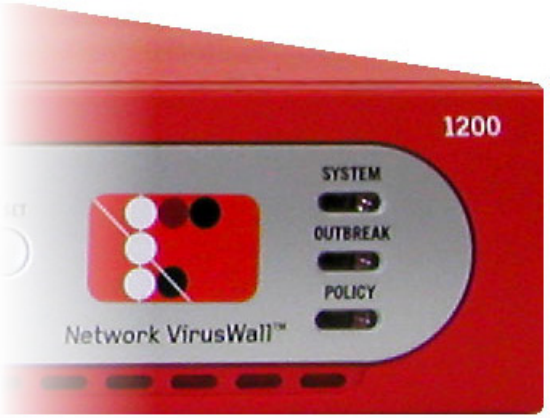


FIGURE 1-3. SYSTEM, POLICY, and OUTBREAK LED indicators

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

LED	STATE	DESCRIPTION
SYSTEM	Red– flashing	Device is booting.
	Red– steady	Power-On Self-Test (POST) error.
	Green– steady	Network VirusWall Enforcer 1200 program file (firmware) is ready.
POLICY	Green– flashing	Network Scan, or Policy Enforcement is enabled
	Off (no color)	No multiple policy scan.
OUTBREAK	Green– steady	Outbreak Prevention Services (OPS) is disabled when Control Manager manages Network VirusWall Enforcer 1200.
	Red– flashing	OPS is enabled.

TABLE 1-3. Network VirusWall Enforcer 1200 LED indicators

Port Indicators

Network VirusWall Enforcer 1200 has two user-configurable copper-based Ethernet ports. Each Ethernet port has an indicator that allows you to determine the port's current state. *Figure 1-4* illustrates the indicators of a port.

FIGURE 1-4. Port indicators 1 and 2

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

INDICATOR NUMBER	NAME	STATE	DESCRIPTION
1	ACT / BYPASS Status LED	No LED status	LAN Bypass LED
2	10 Mbps / 100 Mbps LINK Status LED	Green– steady	10 Mbps LED
			100 Mbps LED

TABLE 1-4. Port indicator description

Table 1-5 shows the possible states for each Network VirusWall Enforcer 1200 port based on the speed and duplex mode settings.

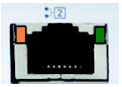
PORT	STATE	DESCRIPTION
Link 	Indicator 1– orange, flashing	Network packet transmission/receiving active.
	Indicator 2– green, steady	Port speed is 10 Mbps or 100 Mbps.

TABLE 1-5. Network VirusWall Enforcer 1200 port indicators

Network VirusWall Enforcer 1200 Back Panel

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

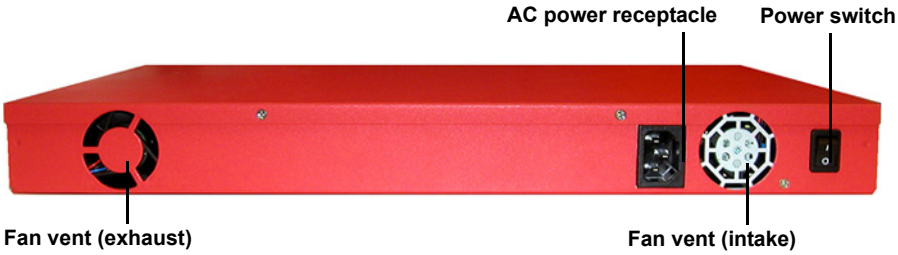


FIGURE 1-5. Network VirusWall Enforcer 1200 back panel

The following table describes each back panel element:

ELEMENT	DESCRIPTION
AC Power Receptacle	Connects to the power outlet and the device using the power cord (included in the package, see *Package Contents* on page 1-2).
Power Switch	Powers the device on and off.
Fan Vent (Intake)	Intake cooling vent for the device.
Fan Vent (Exhaust)	Exhaust cooling vent for the device.

TABLE 1-6. Back panel description

Dimensions and Weight

The following specifications apply to Network VirusWall Enforcer 1200:

Power Requirements and Environmental Specifications

The following settings apply to Network VirusWall Enforcer 1200:

ELEMENT	SPECIFICATION
AC input voltage	90 to 264 VAC (115/230 nominal)
AC input current (90 VAC)	4.0 A
AC input current (180 VAC)	2.0 A

TABLE 1-7. Network VirusWall Enforcer 1200 power requirements and environmental specifications

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

TABLE 1-7. Network VirusWall Enforcer 1200 power requirements and environmental specifications

Chapter 2

Introducing Trend Micro™ Network VirusWall™ Enforcer 1200

This chapter introduces Trend Micro Network VirusWall Enforcer 1200 and provides an overview of its components and deployment.

The topics discussed in this chapter include:

- *Network VirusWall Enforcer 1200* on page 2-2
- *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3
- *Trend Micro Network VirusWall Enforcer 1200 Web Console* on page 2-4
- *Understanding Network VirusWall Enforcer Ports* on page 2-5
- *Deployment Overview* on page 2-5

Network VirusWall Enforcer 1200

Network VirusWall Enforcer 1200 is an outbreak prevention appliance that helps organizations stop network viruses (Internet worms), block high-threat vulnerabilities during outbreaks, and quarantine and clean up infection sources. Network VirusWall Enforcer 1200, deployed at the network layer, uses threat-specific knowledge from Trend Micro to protect against threats as they enter the network. The device scans all the traffic on a specific network segment and applies one policy to an endpoint based on a first-match rule.

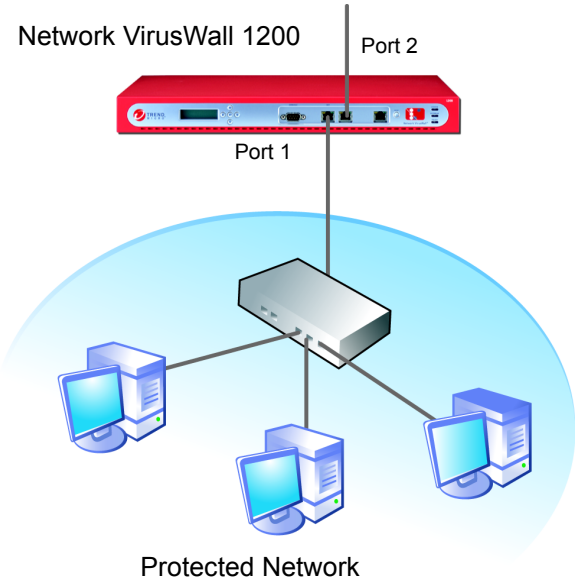


FIGURE 2-1. Network VirusWall Enforcer 1200 in a typical network deployment

Refer to *Understanding Network VirusWall Enforcer 1200* in the *Administrator's Guide* for product function, architecture, and other details.

Introducing Network VirusWall Enforcer 1200-specific Terms

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

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

The documentation sometimes refers to *Copper Gigabit Ethernet ports* as *ports* or *interfaces* (see *Understanding Network VirusWall Enforcer Ports* on page 2-5). You can specify the following port types for each physical port:

Failopen—a fault-tolerance solution, also known as LAN bypass, that allows the Network VirusWall Enforcer 1200 device to continue to pass traffic if a software or hardware failure occurs within the device.

Note: For more information on, see *Failopen Deployment* on page 3-18.

Trend Micro Network VirusWall Enforcer 1200 Web Console

The Network VirusWall Enforcer 1200 Web console provides central management for Network VirusWall Enforcer 1200 devices on your network. The Web console gives you the tools to configure and enforce security policies for an entire organization. This enables you to react quickly to network virus emergencies from nearly anywhere using the Web console.

After preconfiguration, the Web console enables you to perform the following Network VirusWall Enforcer 1200 administrative tasks:

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

For guidance on administering devices from the Web console, see the *Network VirusWall Enforcer 1200 Administrator's Guide.*

Understanding Network VirusWall Enforcer Ports

Network VirusWall Enforcer 1200 supports two ports—2 copper Ethernet ports.

Deployment Overview

Network VirusWall Enforcer 1200 deployment consists of the following steps:

1. Deciding on the deployment strategy

   Deploying Network VirusWall™ Enforcer 1200 provides the basic deployment and strategies. This chapter aims to help you determine the strategy you will take to deploy Network VirusWall Enforcer 1200.

2. Preparing for preconfiguration

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

3. Preconfiguring Network VirusWall Enforcer 1200

   Preconfiguring Network VirusWall Enforcer 1200 provides instructions to guide you during device preconfiguration.

4. Configuring Network VirusWall Enforcer 1200

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

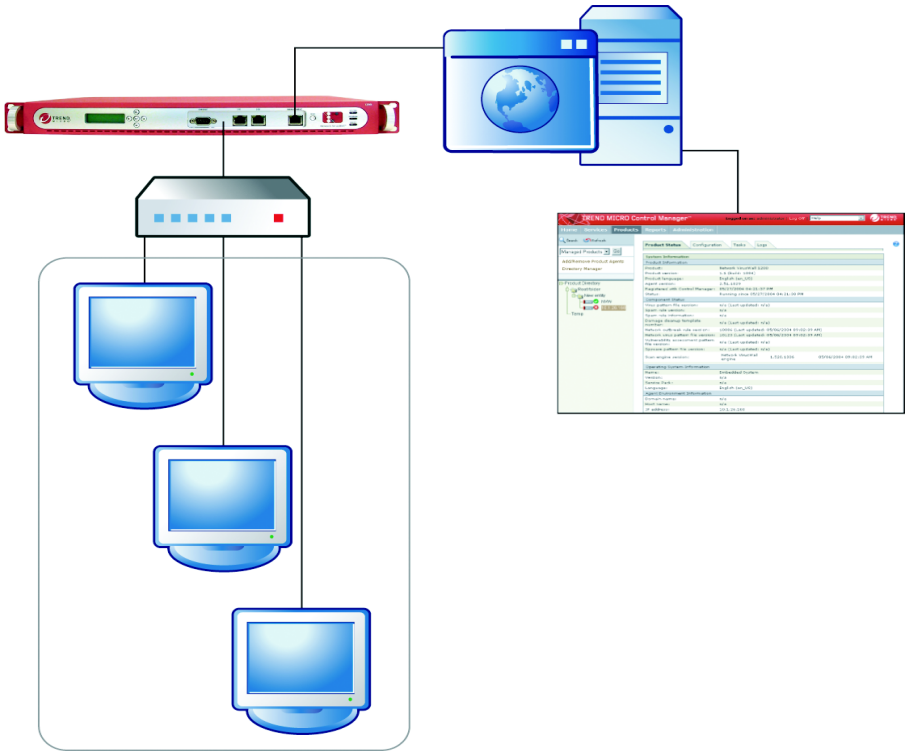


FIGURE 2-2. Network VirusWall Enforcer 1200 after deployment

Understanding Network VirusWall Enforcer 1200 of the *Administrator's Guide* provides details about the following concepts:

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

After checking the package contents and device's physical specifications in *Getting Started*, proceed to *Deploying Network VirusWall™ Enforcer 1200* for deployment considerations and sample deployment strategies.

Chapter 3

Deploying Network VirusWall™ Enforcer 1200

Before beginning to configure a Network VirusWall Enforcer 1200 device, plan how to integrate the device into your network. Determine which topology it will support.

This chapter explains how to plan for the deployment of Network VirusWall Enforcer 1200 devices. It also provides application and deployment scenarios to facilitate understanding of the various ways the device can help protect and secure your network.

This chapter contains the following topics:

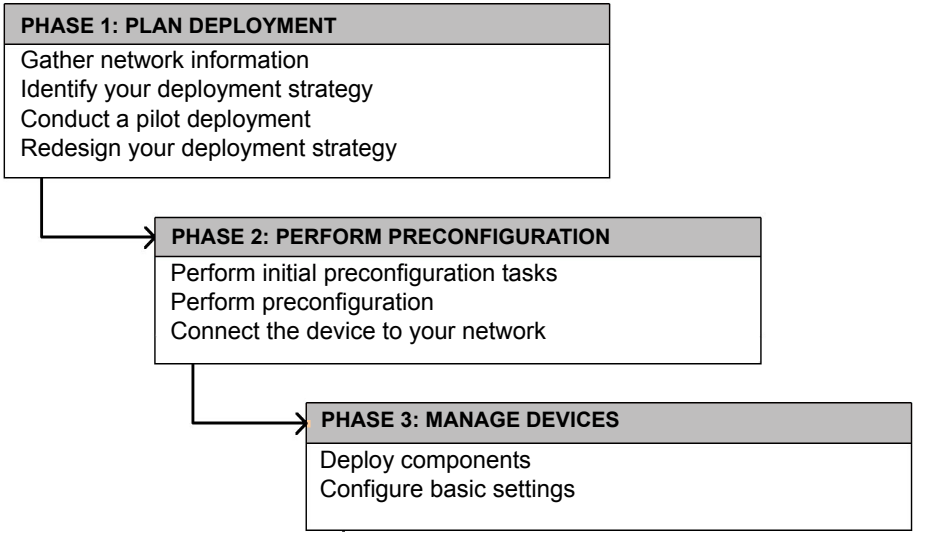
- *Planning for Deployment* on page 3-2
- *Identifying What to Protect* on page 3-5
- *Planning for Network Traffic* on page 3-15
- *Conducting a Pilot Deployment* on page 3-16
- *Redefining Your Deployment Strategy* on page 3-17
- *Deploying Network VirusWall Enforcer 1200* on page 3-17
- *Failopen Deployment* on page 3-18

Planning for Deployment

To take advantage of the benefits Network VirusWall Enforcer 1200 can bring to your organization, you will need an understanding of the possible ways to deploy one or more devices. This section provides deployment overview and considerations.

Deployment Overview

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



Phase 1: Plan the Deployment

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

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

Phase 2: Perform Preconfiguration

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

- Perform the initial preconfiguration tasks (See *Network VirusWall Enforcer 1200 Initial Tasks* on page 4-2)
- Perform preconfiguration on the device(s) (See *Performing Preconfiguration Using the Preconfiguration Console* on page 5-5)
- Connect the device(s) to your network (See *Connecting to the Network* on page 5-18)

Phase 3: Manage Network VirusWall Enforcer 1200 Devices

During phase 3, manage Network VirusWall Enforcer 1200 devices from the Web console. You can perform the following tasks:

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

Tip: This *Getting Started Guide* discusses phases 1 and 2. Refer to *Network VirusWall Enforcer 1200 Administrator's Guide* for instructions relating to phase 3.

Deployment Notes

Consider the following when planning for a deployment:

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

  To protect an organization from network threats, position the device to key places on your network. The device should be able to scan all network traffic to prevent, detect, or contain threats.
- Each of the interfaces supports the following port speed and duplex mode settings:
  - 10Mbps x half-duplex
  - 10Mbps x full-duplex
  - 100Mbps x half-duplex
  - 100Mbps x full-duplex
- Both the connected L2/L3 and Network VirusWall Enforcer 1200 devices should have the same interface setting and duplex mode. Otherwise, the half-duplex mode setting will take effect. To help guarantee the correct interface setting and duplex mode implementation, modify both the L2/L3 and Network VirusWall Enforcer 1200 devices to have the same setting.The device supports IP addresses belonging to any classes (that is, class A, B, or C)

  Tip: Although each range is in a different class, you are not required to use any particular range for your internal network. It is a good practice, though, because it greatly diminishes the chance of an IP address conflict.
- Policy Enforcement support various actions for non-compliant or infected endpoints

Identifying What to Protect

Position Network VirusWall Enforcer 1200 between layer 2 (L2) or layer 3 (L3) devices.

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

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

Remote Access Endpoints

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

There are two types of remote endpoints:

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

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

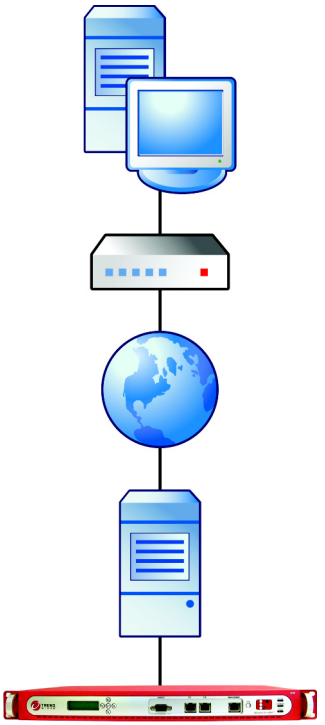


FIGURE 3-1 Dial-up service deployment scenario

Figure 3-1 illustrates a dialup connection between a home user and an organization's internal network. A RAS server, the point where the dialup connection terminates, is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3 for information about different types of ports). This means that all packets going between the RAS server and the LAN pass through the device. Once the home user establishes a connection with the RAS server, it essentially becomes part of the internal network as illustrated in the basic deployment scenario (See *A Basic Deployment Scenario* on page 3-18). The home user accesses both network resources and the Internet in the same way internal endpoints do.

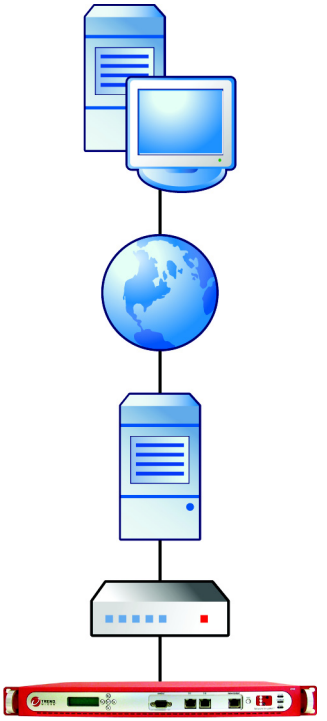


FIGURE 3-2 Endpoint to site VPN deployment scenario

Figure 3-2 illustrates a connection between a home user and an organization's internal network, only though a VPN server, which is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3 for information about different types of ports). In this configuration, the home user's VPN connection is considered to be part of the internal network.

Note: Network VirusWall Enforcer 1200 must be behind the VPN server, which encrypts and decrypts VPN traffic.

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

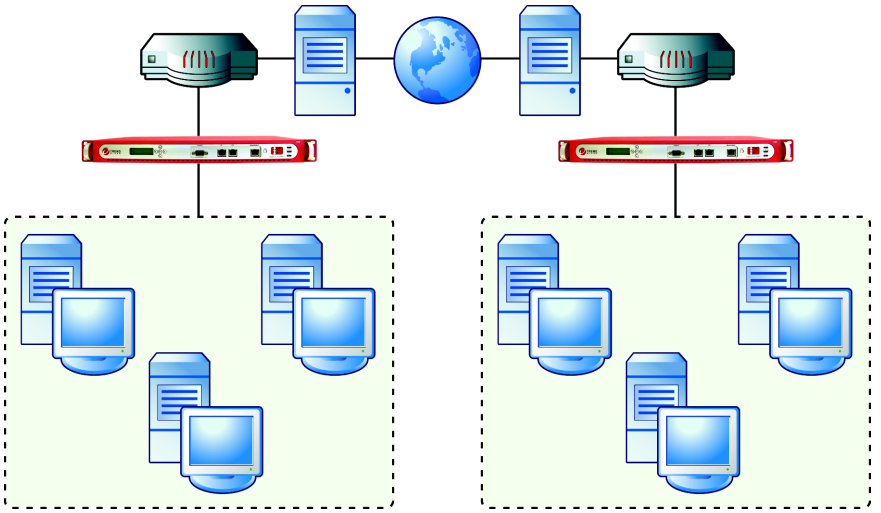


FIGURE 3-3. Site to site VPN deployment scenario

Figure 3-3 illustrates a VPN connection between two business units. As in the home user scenario, a VPN server is connected to a **REGULAR** port on each device (See *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3 for information about different types of ports).

Guest Endpoints

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

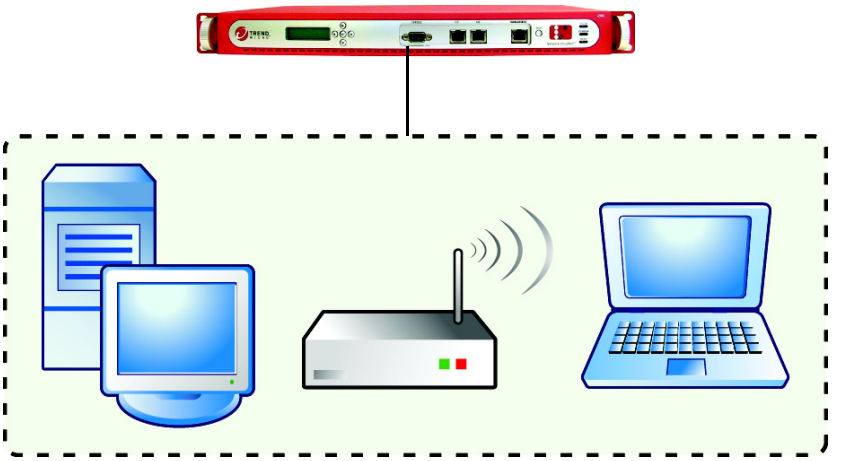


FIGURE 3-4. Guest network deployment scenario

Figure 3-4 illustrates a segment of an internal network especially for guest endpoints. A wireless access point, switch, or hub is connected to the **REGULAR** port (See *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3 for information about different types of ports). This type of topology ensures that the device scans all traffic before it leaves the guest network segment and makes isolation of the guest segment possible in the event of a virus outbreak.

Key Network Segments/Important Network Assets

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

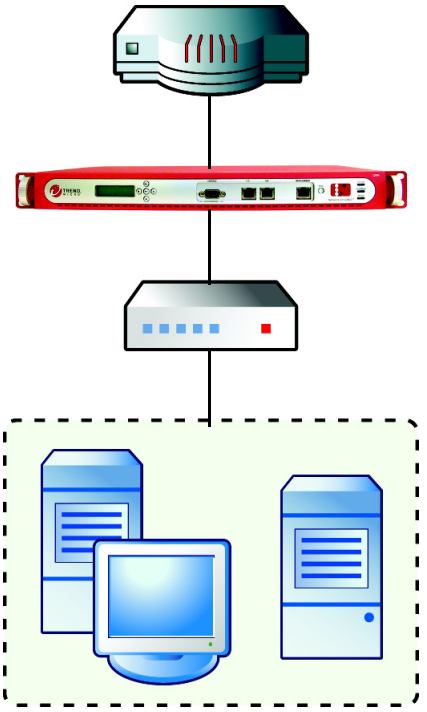


FIGURE 3-5. Key network segments scenario

Key Network Segments/Important Network Assets on page 3-9 illustrates a segment of an internal network containing email and Web servers, including endpoints. An internal switch or hub is connected to a **REGULAR** port (See *Introducing Network VirusWall Enforcer 1200-specific Terms* on page 2-3 for information about different types of ports), creating a segment where all packets going in and out of the segment can be scanned. Installing the device in this position adds the benefits of virus scanning and segment isolation in the event of a virus outbreak.

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

Dual-switch VLAN Environment

Network VirusWall Enforcer 1200 must be placed in line on the physical network to be able to provide security. In most situations, this means between an upstream switch and one or more downstream switches.

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

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

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

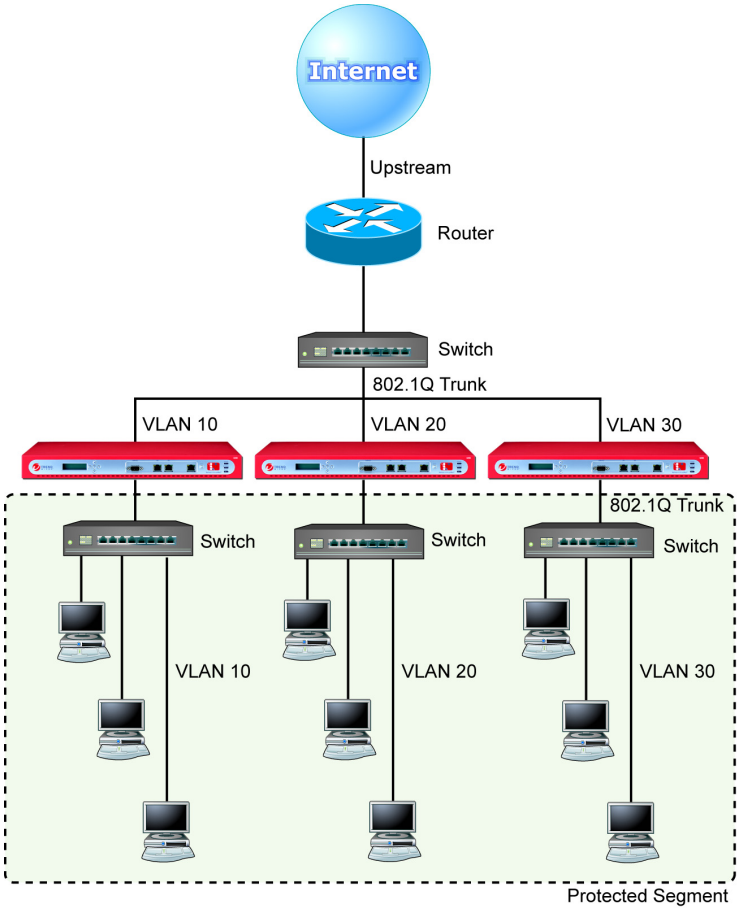


FIGURE 3-6. Multiple VLAN segments with each device protecting one segment

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

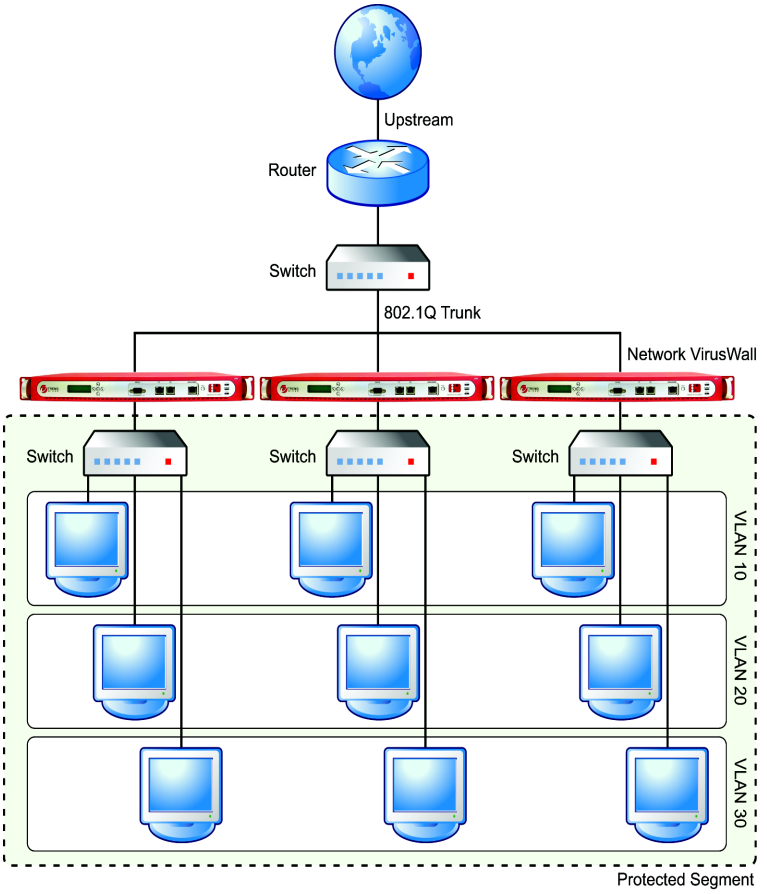


FIGURE 3-7. Multiple VLAN segments with each device protecting all segments

Single-switch VLAN Environment

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

- Is only possible when using a switch that can be configured to carry individual VLAN traffic on specific physical ports
- VLAN 20 is assigned to ports 1 and 2 on the switch
- The upstream network is connected to port 2 on the switch
- The **REGULAR** port on Network VirusWall Enforcer 1200 is connected to port 1 on the switch

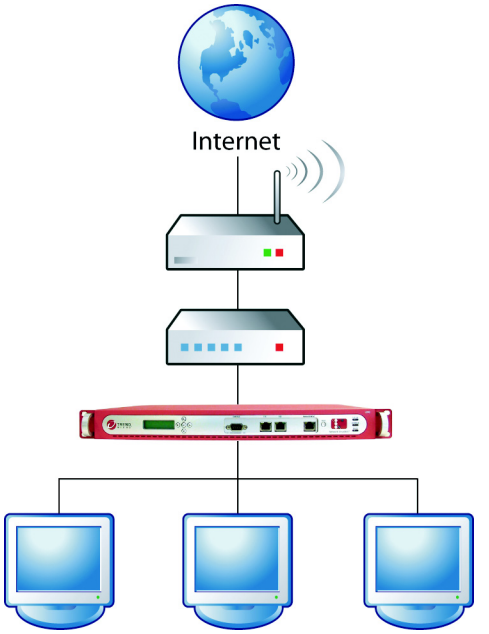


FIGURE 3-8. Single-switch VLAN environment

Planning for Network Traffic

The scenario presented in *Key Network Segments/Important Network Assets* on page 3-9 is also a good example of how to plan for network traffic. There is a strategic advantage to positioning the device in front of resources that endpoints access regularly, such as an email or Web server. Because many viruses make their way onto networks through email attachments and Web browsers, forcing traffic to pass through the device significantly reduces the risk of virus infection. Identify other places on your network through which large amounts of traffic pass and consider positioning the device at points where it can scan the most amount of traffic.

Determining the Number of Devices to Deploy

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

- **Existing Network topology**– based on your network topology, identify the segments you want the device to protect (see *Identifying What to Protect* on page 3-5)
- **Existing network device interfaces**– because the device handles 10/100Mbps or 1Gbps Fast Ethernet traffic, identify the network device interfaces that handle the same type of traffic and can therefore connect to Network VirusWall Enforcer 1200 devices
- **Desired effectiveness of protection**– to lower the risk of a virus outbreak spreading, segment several sections of your network with Network VirusWall Enforcer 1200 devices
- **Desired degree of performance**– consider the number of endpoints and the amount of traffic the device can handle

Conducting a Pilot Deployment

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

Perform the following tasks to conduct a pilot deployment:

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

Choosing a Pilot Site

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

Creating a Contingency Plan

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

Deploying and Evaluating your Pilot

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

Redefining Your Deployment Strategy

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

Deploying Network VirusWall Enforcer 1200

This section provides an example of a few basic deployment scenarios (see *page 3-18*) and deployment strategies:

Tip: See *Network VirusWall Enforcer 1200 Initial Tasks* on page 4-2 for checklists on how to prepare a device for deployment.

A Basic Deployment Scenario

The device can be installed on a network that contains Ethernet devices such as hubs, switches, and routers. Deploy Network VirusWall Enforcer 1200 between a switch that leads to the public network and a switch that protects a segment of the Local Area Network (LAN). It can also be installed between an edge switch and a hub. *Figure 3-9* illustrates a basic deployment scenario.

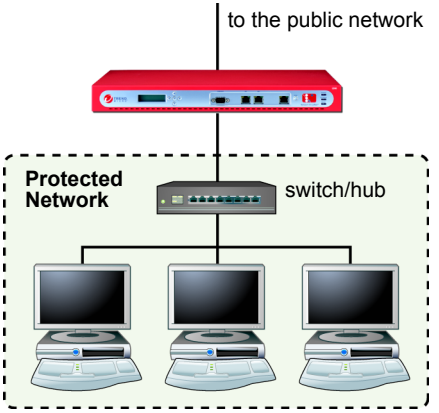


FIGURE 3-9. Basic deployment

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

Network VirusWall Enforcer 1200 protects your network as follows:

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

Failopen Deployment

Failopen deployment with Network VirusWall Enforcer 1200 has changed from previous versions of Network VirusWall.

To successfully deploy Network VirusWall Enforcer 1200 for failopen:

1. Deploy Network VirusWall Enforcer 1200 between two switches.

2. Trend Micro recommends connecting Network VirusWall Enforcer 1200 to the switches using straight-through cables.
3. Trend Micro recommends configuring the switches to use Rapid Spanning Tree Protocol (RSTP 802.1w) to lower the impact on the network when failopen occurs (under five seconds).

   When using the standard Spanning Tree Protocol (STP 802.1D) the network has a longer convergence time when failopen occurs (about 30 to 50 seconds).

Chapter 4

Preparing for Preconfiguration

Preconfiguring the device requires that you are connected to Network VirusWall Enforcer 1200.

This chapter contains the following topics:

- *Preparing for Preconfiguration* on page 4-2
- *Network VirusWall Enforcer 1200 Initial Tasks* on page 4-2

Preconfiguring Network VirusWall Enforcer 1200 requires the completion of related tasks.

To perform preconfiguration:

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

Deploying Network VirusWall™ Enforcer 1200 on page 3-1 discusses step 1, the succeeding sections discuss step 2, and *Preconfiguring Network VirusWall Enforcer 1200* on page 5-1 provides instructions for step 3.

Preparing for Preconfiguration

Complete the following tasks before preconfiguring the device:

- If you are upgrading from a previous version of Network VirusWall refer to the *Network VirusWall Enforcer 1200 Upgrade Guide* before continuing.
- Network VirusWall Enforcer 1200 initial tasks (See *Network VirusWall Enforcer 1200 Initial Tasks* on page 4-2).

Network VirusWall Enforcer 1200 Initial Tasks

Complete the following tasks before you preconfigure Network VirusWall Enforcer 1200:

- Determine the `admin` account password

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

- Prepare a computer that has terminal communications software, such as HyperTerminal for Windows (See *Preparing the Preconfiguration Console* on page 5-6).

Chapter 5

Preconfiguring Network VirusWall Enforcer 1200

This chapter contains the following topics:

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

Preconfiguring a Network VirusWall Enforcer 1200 device requires the completion of the following tasks:

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

Understanding Preconfiguration

As stated in *Preparing for Preconfiguration* starting on page 4-1, preconfiguring the device requires the completion of Network VirusWall Enforcer 1200-related tasks.

To perform preconfiguration:

1. Plan and determine the deployment strategy (see *Deploying Network VirusWall™ Enforcer 1200* on page 3-1).
2. Perform preconfiguration (see instructions starting on *Using the Preconfiguration Console* on page 5-3).
3. Perform configuration tasks (see *Configuring Policy Enforcement and Device Settings* in the *Administrator's Guide*).

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

After the preconfiguration procedure of the device is complete, you can then administer Network VirusWall Enforcer 1200 using the Web console. Refer to *Configuring Policy Enforcement and Device Settings* of the *Administrator's Guide*.

Choosing the Preconfiguration Method

Preconfigure the device through the:

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

Using the Preconfiguration Console

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

- Interface settings
- Network settings
- System logs

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

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

Using the LCD Module

Use the LCD and control panel on the front of the device to configure only Network VirusWall Enforcer 1200 network settings, such as the IP address. See *Performing Preconfiguration Using the LCD Module* on page 5-16 for details on how to use the LCD module.

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

WHAT YOU CAN DO	PRECONFIGURATION CONSOLE	LCD MODULE
Set the Network VirusWall Enforcer 1200 IP address, netmask, Gateway address, and DNS addresses	•	•
Lock/unlock LCD module panel controls	•	
View system logs	•	
Initialize the device to default settings	•	
Reset the device	•	•
Restore default settings (factory settings)	•	
Configure the interface speed and duplex mode	•	
View device settings	•	
Enable/disable SSH access	•	
Pattern/Engine rollback	•	
Allow changes to take effect immediately	(Need to log off)	•
Register to Control Manager	•	

TABLE 5-1. Comparison of available consoles for preconfiguration

Performing Preconfiguration Using the Preconfiguration Console

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

Tip: Check whether you have completed the *Network VirusWall Enforcer 1200 Initial Tasks* on page 4-2 before starting with the following steps.

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

Preparing the Preconfiguration Console

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

To prepare the Preconfiguration console:

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

      HyperTerminal prompts you for location information.

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

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

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

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

   e. Click the **Settings** tab.

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

Logging on the Preconfiguration Console

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

To access the Preconfiguration console:

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

   To power-on a device:

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

   b. Connect the power cord to an electrical outlet.

   Tip: See *Power Requirements and Environmental Specifications* on page 1-7 for device power requirements and environmental specifications.

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

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

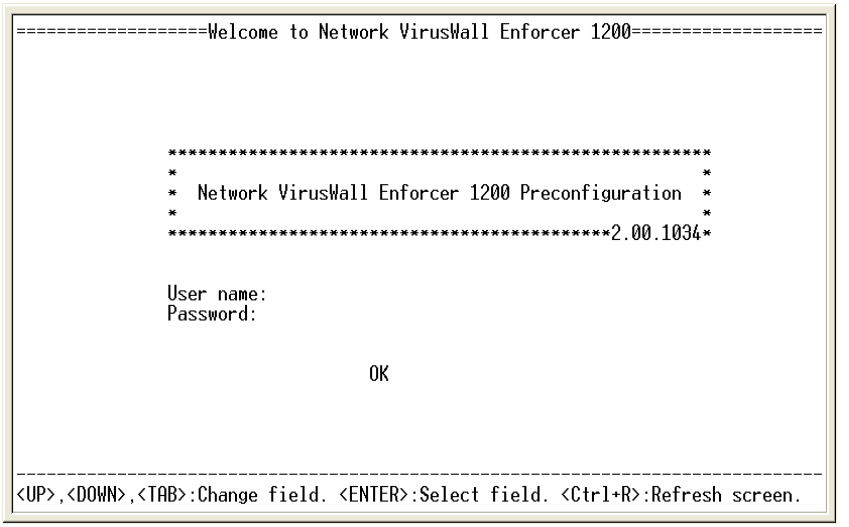


FIGURE 5-1. The Preconfiguration console logon prompt

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

   User name: `admin`

   Password: `admin`

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

   Use this login for full access to all preconfiguration features.

   Tip: See *admin password misplaced or forgotten* on page 7-2 for tips on how to troubleshoot a missing or forgotten password.

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

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

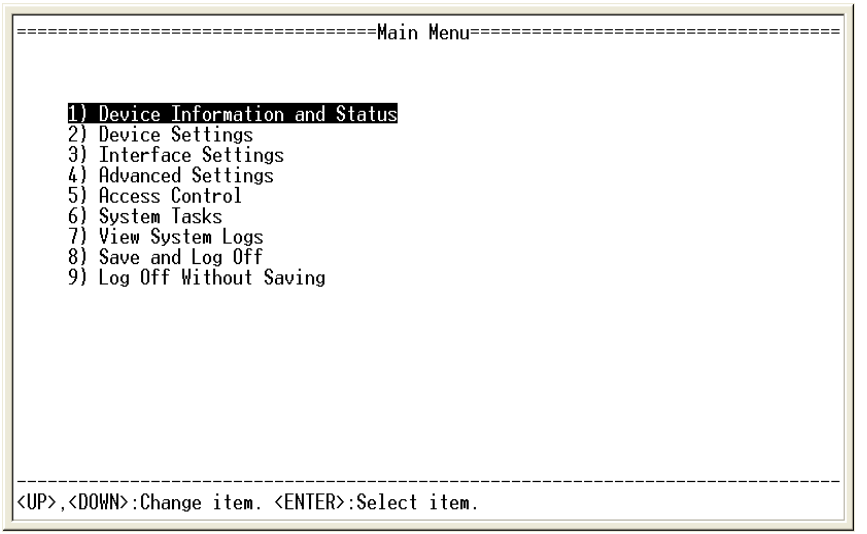


FIGURE 5-2. The Preconfiguration console Main menu

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

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

Configuring Device Settings

Immediately after logging onto the Preconfiguration console for the first time, change the default password to a secure password from the Web console. After changing the password, use the **Device Settings** menu to configure the Network VirusWall Enforcer 1200 host name that appears on the Web console and the Network VirusWall Enforcer 1200 network settings.

To configure the device settings:

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

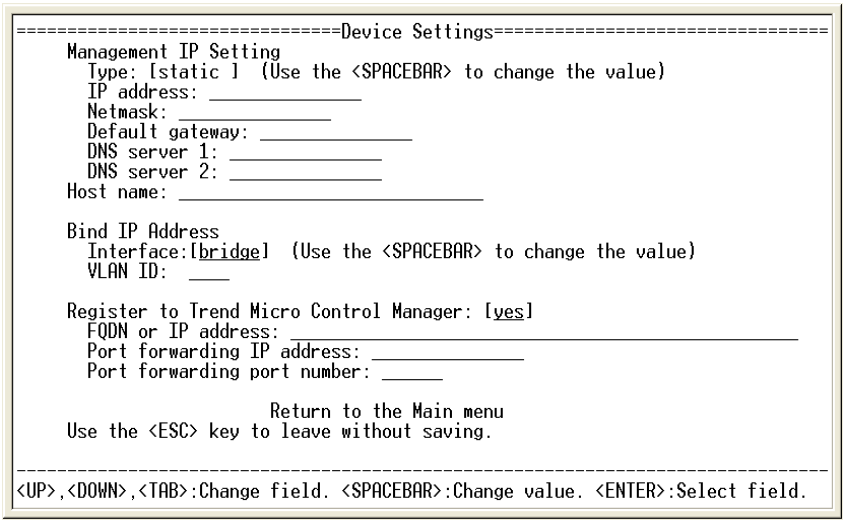


FIGURE 5-3. Network VirusWall Enforcer Device Settings

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

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

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

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

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

   Host names may be up to 30 alphanumeric characters (spaces not allowed). Trend Micro recommends a unique descriptive host name to represent and identify the device (through the front panel LCD module) or remotely (through the management console).

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

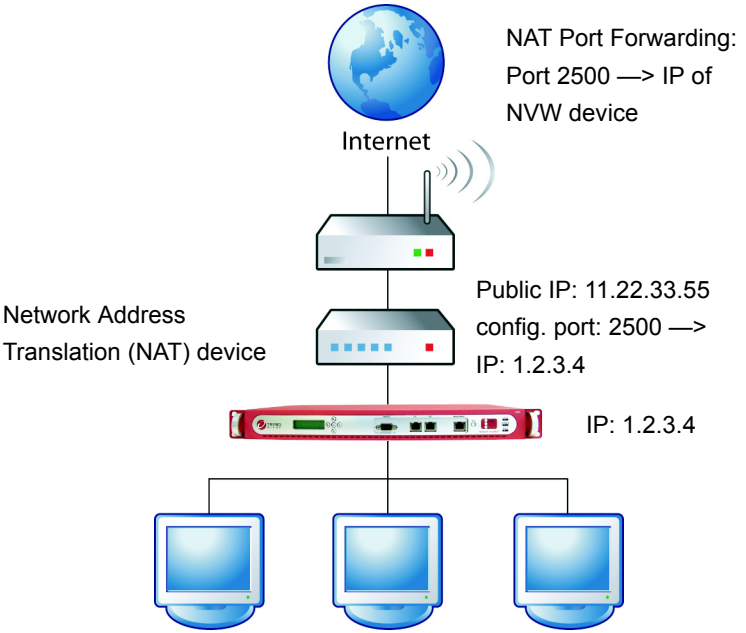


FIGURE 5-4. Network VirusWall Enforcer 1200 deployment in a network environment using a NAT device (with sample IP address and port)

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

---

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

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

Setting the Interface Speed and Duplex Mode

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

Note: Both the connected L2/L3 and Network VirusWall Enforcer 1200 devices should have the same interface setting and duplex mode. Otherwise, the half-duplex mode setting will take effect. Apply **100Mbps x full-duplex** for both the switch and Network VirusWall Enforcer 1200 device.

To set the interface speed and duplex mode:

1. On the **Main Menu** of the Preconfiguration console, type 3 to select **Interface Settings**. The Interface Settings Screen appears.

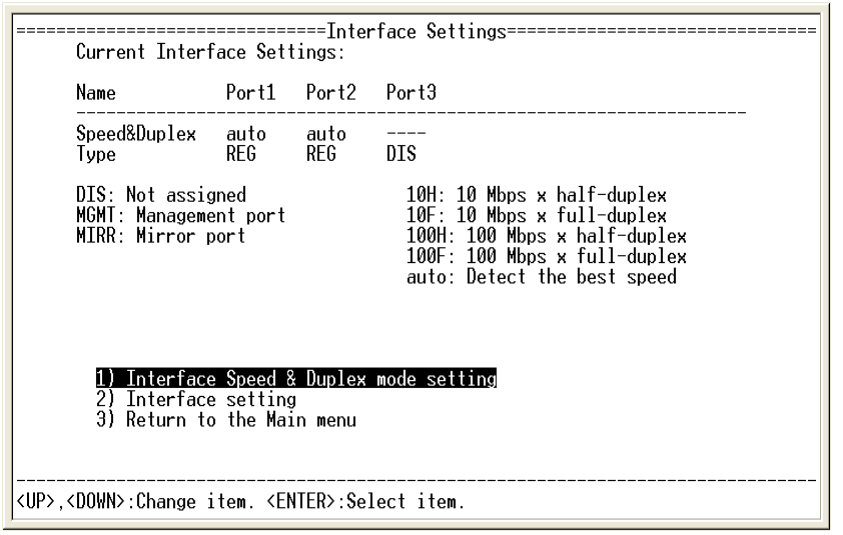


FIGURE 5-5. Network VirusWall Enforcer Interface Settings

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

   The **Interface speed & duplex mode setting** screen displays the current interface speed and duplex setting for all ports.

3. Select the port by using the up and down arrows.

4. Select the speed by using the space bar to scroll through the speed options.
5. Select **Return to the previous menu**. The **Interface Settings** screen displays.
6. Type 2 to select **Interface setting**.
7. Use the down arrow to go to Port 3.
8. Use the spacebar to select MGMT.
9. Type 3 to select **Return to Main menu**. The **Main Menu** displays.
10. Select **Save and Log Off** for changes to take effect.

Logging off the Preconfiguration Console

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

To log off the Preconfiguration console:

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

Note: In order to apply new settings, you must log off Network VirusWall Enforcer 1200.

Performing Preconfiguration Using the LCD Module

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

There are five buttons on the LCD console:

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

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

- **ENTER** – confirm selection or input

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

To configure the IP address through the LCD module:

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

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

---

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

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

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

   To use a dynamic IP address, do the following:

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

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

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

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

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

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

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

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

6. Press **ENTER** ( ). The console requests the Control Manager IP address.
7. Type the Control Manager IP address.

   If you do not want to register to Control Manager continue to step 8.
8. Press **ENTER** ( ) to save the settings when prompted.

Connecting to the Network

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

To connect the device to your network:

1. Connect one end of a 10/100Mbps Ethernet cable to a **REGULAR** port and the other to a segment of your network
2. Power on the device (see *page 5-7*).

Note: Network VirusWall Enforcer 1200 can handle various interface speed and duplex mode network traffic. See *Setting the Interface Speed and Duplex Mode* on page 5-14.

Chapter 6

Configuring Network VirusWall Enforcer 1200

After preconfiguring Network VirusWall Enforcer 1200, you are ready to configure the device and commence network protection.

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

- *Configuring PEAgent Settings for Manual Deployment* on page 6-2
- *Updating Components Manually* on page 6-7
- Change the user password
- Configure Policy Enforcement

Refer to the following documentation for instructions relating to changing your password and configuring policy enforcement:

- *Network VirusWall Enforcer 1200 Administrator's Guide*– includes instructions on how to configure and administer the device from the applicable management tools

  See *Getting Started with Network VirusWall Enforcer 1200* in the *Administrator's Guide* for instructions.
- *Network VirusWall Enforcer 1200 Online Help*– provides instructions on how to configure Network VirusWall Enforcer 1200 devices Web console

See *Preface* on page 1 for a complete description of Network VirusWall Enforcer 1200 documentation.

Configuring PEAgent Settings for Manual Deployment

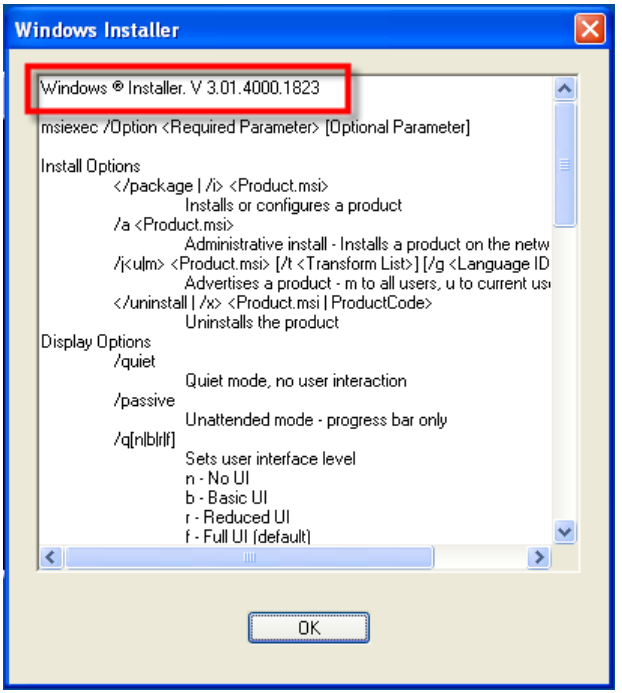
You can configure Network VirusWall Enforcer 1200 to use agentless or persistent agent mode. In persistent agent mode the PEAgent, which installs on the end-users' client computer, communicates with Network VirusWall Enforcer 1200. You can configure the Network VirusWall Enforcer 1200 port which communicates with the PEAgents.

End-users install the PEAgent as they attempt to access the Internet or Intranet. If remote deployment is unsuccessful, the Web browser they use to access the Internet is configured to prevent ActiveX from running, or if their Web browser does not support ActiveX (Firefox), the user needs to install the PEAgent manually.

Installing the PEAgent component requires Windows Installer engine 2.0 on the client computer, that is included in the Windows XP platform. However, for previous Windows versions (Windows 98/ME/2000), the client computer will need to download or update the Windows Installer engine.

To check the Windows Installer version:

1. Click **Start > Run...**. The Run dialog box appears.
2. Type `cmd` in the **Open** field. The Command Line Interface appears.
3. Type `msiexec` at the command prompt and press `Enter`. The Windows Installer dialog box appears.
4. Verify the Windows Installer engine version on the client computer is greater than 2.0.



Manually installing the PEAgent requires the following from the administrator:

1. A location for the PEAgent installation program
2. Configure the communication port for PEAgent and Network VirusWall Enforcer 1200 (optional)
3. Customize the **Performing Endpoint Assessment** endpoint notification.

Step 1: Provide a location for the PEAgent installation program

1. Insert the Network VirusWall Enforcer 1200 Solutions CD.
2. Locate the PEAgent installation file: `...\Programs\PEAgent\PEAgent.msi`.
3. Copy the `PEAgent.msi` file to a shared folder that everyone on your network can access.

Step 2: Configure the communication port for PEAgent and Network VirusWall Enforcer 1200

This step is optional. Proceed to step 3 if you do not need to change the port number for PEAgent-Network VirusWall Enforcer 1200 communication.

To configure the communication port for PEAgent:

1. Insert the Network VirusWall Enforcer 1200 Solutions CD.
2. Locate the PEAgent configuration tool file: `...\Programs\PEAgent\PEAgent_Config.exe`.
3. Copy the PEAgent configuration tool to the folder where the `PEAgent.msi` file is located.
4. Double-click the `PEAgent_Config.exe`. The PEAgent configuration tool dialog box appears.
5. Specify the location of the `PEAgent.msi` file in the **Location of PEAgent Installer** field.
6. Specify the port that the PEAgent uses to communicate with Network VirusWall Enforcer 1200 in the **Client port** field.
7. Click **OK**.

To configure the communication port for Network VirusWall Enforcer 1200:

1. In the Network VirusWall Enforcer 1200 Web console, click **Policy Enforcement > PEAgent Settings**. The PEAgent Settings screen appears.
2. Type a port number for PEAgent-Network VirusWall Enforcer 1200 communication in the **PEAgent port** field.

WARNING! *Changing this setting will stop communication with all PEAgents until the PEAgents update their listening port to the same port number as Network VirusWall Enforcer 1200.*

3. Click **Save**.

Step 3: Customize the Performing Endpoint Assessment endpoint notification

You should customize the **Performing Endpoint Assessment** endpoint notification so that users under the following situations can download and install the PEAgent manually:

- Remote deployment is unsuccessful
- Users use a Web browser other than Internet Explorer (Firefox, Mozilla)
- User does not allow ActiveX to run on their computers

To customize the Performing Endpoint Assessment endpoint notification:

1. In the Network VirusWall Enforcer 1200 Web console, click **Policy Enforcement > Endpoint notifications**. The Endpoint Notifications screen appears.
2. Click **Performing Endpoint Assessment** under Web Notifications. The Performing Endpoint Assessment Endpoint Notification screen appears.
3. Customize the notification text to include a link to the `PEAgent.msi` file. For example:

```
<!-- axp body begin -->

<br>

<table width="100%" border="0" cellpadding="0" cellspacing="0">

  <tr>

    <td>

    <table width="100%" border="0" cellpadding="0"
cellspacing="0">

    <tr><td class="header">

    <p>
```

```
    Please wait while <%=PRODUCT_NAME%> performs an assessment
of your computer. This may take a few minutes, depending on the
current network traffic.

    </p>

    <p>

    <ul style="list-style: disc;" type=disc>

     <li><font size="2" color=#E70009 face="Verdana, Arial,
Helvetica, sans-serif">

      If this page does not refresh in a few minutes, close and
re-open your browser. </font></li>

     <li>

      <font size="2" color=#E70009 face="Verdana, Arial,
Helvetica, sans-serif">

      If this screen continues reappearing and you are not able
to view the detection result, contact your network
administrator.</font> </li>

     <li>

      <font size="2" color=#E70009 face="Verdana, Arial,
Helvetica, sans-serif">

     Click Reassess, if you have already installed the PEAgent.
If you have not installed the PEAgent click <A href="<Location
of PEAgent.msi>" target="_blank">Download PEAgent </A> <font>
</li>

     </ul>

    </p>

    </td></tr>

    </table>

   </td>

  </tr>

</table>

<br>
```

```
<!-- axp body end -->
```

4. Click **Preview** to verify the notification is what you require.
5. Click **Save**.

Tip: When creating policies remember to add the IP address of the server which PEAgent.msi is located to the Policy URL Exception list (Step 6: Policy URL Exceptions of policy creation), so that blocked endpoints can access the PEAgent Installer.

Updating Components Manually

After preconfiguring Network VirusWall Enforcer 1200, download the latest components (Network Virus Pattern, Cleanup templates, Network Virus Engine) to help maintain the highest security protection.

To perform a manual update:

1. Click **Updates** in the side bar. The drop down menu displays.
2. Click **Manual**. The Manual Update screen displays.
3. Select the **Component** checkbox to update all components or select checkboxes to update individual components.
4. Click **Update**.

Use the **Summary** screen from the Network VirusWall Enforcer 1200 Web console to verify whether Network VirusWall Enforcer 1200 updates the selected components during manual update.

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

Chapter 7

Troubleshooting Preconfiguration

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

Tip: Refer to the *Network VirusWall Enforcer 1200 Administrator's Guide* in the *Trend Micro Solutions CD for Network VirusWall Enforcer 1200* for additional FAQs and troubleshooting.

This chapter contains the following topics:

- *Device Issues* on page 7-2
- *Contacting Technical Support* on page 7-3

Note: *Troubleshooting* in the *Administrator's Guide* has more details regarding Control Manager and Network VirusWall Enforcer 1200 integration troubleshooting.

Device Issues

#	Issue	Corrective Action/Explanation
1.	LEDs do not illuminate	Verify secure power cable and network cable connections. If the error persists, there may be a hardware issue. Contact your vendor. See *LED Indicators* on page 1-4 for details on the Network VirusWall Enforcer 1200 LED.
2.	Unable to access the Preconfiguration console	Verify secure console port connections and terminal communications software settings. See *Preparing the Preconfiguration Console* on page 5-6 for details on setting the terminal communications software settings.
3.	Unable to change settings with the LCD module panel	Verify whether the LCD module configuration is set to ON. Otherwise, the OFF LCD module configuration state will prevent you from configuring Network VirusWall Enforcer 1200 through the LCD module. In addition, to change settings with the LCD module panel, you must first press and hold down the return button  . **Tip:** Refer to *Changing the LCD Module Configuration* in the *Administrator's Guide* for instructions on how to toggle this setting. If an issue with any LCD module buttons persists, the hardware may need to be repaired. Contact your vendor.

Contacting Technical Support

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

Index

A

Administrator's Guide P-2
appliance 2-2
architecture 2-2
audience P-4

C

Cable
  console 1-3
cable
  Ethernet 1-3
components
  downloading 6-7
connections
  to the network 5-18
Connectors
  ports 1-7
Console
  cable 1-3
Contingency plan 3-16
Conventions P-4
  document P-4

D

deploying Network VirusWall
  overview 2-5
Deployment
  number of devices 3-15
  planning 3-2
  scenario 3-18
  strategy redesign 3-17
device 2-2
device settings
  configuring 5-11
Document
  conventions P-4
Document conventions P-4
Documentation P-2
Duplex mode 5-18

E

Ethernet cable 1-3
Evaluating your pilot 3-16

F

Failopen
  deployment 3-18
failopen 2-3

G

Getting Started Guide P-2
  about P-3
Glossary 2-3
GSG. See Getting Started Guide.
Guest clients 3-9

H

HyperTerminal 4-2

I

Interface speed 5-18
IP address
  static 5-12
Issues
  accessing Preconfiguration console 7-2
  LCD module configuration 7-2
  LED 7-2
  Preconfiguration console 7-2

N

Network VirusWall Enforcer
  about the appliance 2-2
  Administrator's Guide P-2
  components 2-2
  device settings 5-11
  documentation P-2
    audience P-4
    conventions P-4
  Getting Started Guide P-2
  how it works 2-2
  introduction 2-2
  online help P-2
  printed documentation P-3
  protection 2-2
Notes
  control panel 5-16
  deployment with VPN 3-7
  duplex mode 5-14, 5-18

interface speed 5-14, 5-18
LCD module 1-4, 5-16
LCM console 1-4, 5-16
panel 5-16
Preconfiguration console 5-10
saving configurations 5-15
system logs 5-13
timeout 5-10
Update Center P-2
using control panel 5-16
using LCD module 5-16
VPN 3-7

O

OLH P-2
Online help P-2

P

panel
back 1-7
front 1-4
password
default 5-9
PEAgent 6-2
manually installing 6-3
Pilot
choosing a site 3-16
conducting a pilot deployment 3-16
Preconfiguration Method 5-3
Preface P-1

R

Remote clients 3-5

S

setting interface speed and duplex mode 5-14
Solutions CD 1-3
Speed 5-18
Static IP address 5-12

T

Tips
about this GSG 3-3
addresses 3-4
admin 4-2
before preconfiguring Network VirusWall 5-5
checking package 1-2
control panel 5-16
documentation P-2
FAQs 7-1
glossary 2-3
host names length 5-12
HyperTerminal 5-6
LCD module timeout 5-17
monitor 4-2
Network VirusWall
accounts 4-2
host names 5-12
initial tasks 5-5
IP address 5-12
positioning Network VirusWall 3-5
powering on device 5-7
preconfiguring 5-10
reading LCD module 5-16
static IP address 5-12
timeout 5-17
troubleshooting 7-1
using HyperTerminal 5-6

U

unit 2-2
Update
manually updating components 6-7
Update Center P-2

W

Who should read this document
audience P-4