



# Network VirusWall™ Enforcer 1500i (CR100 Series)

Network Security for Enterprise and Medium Business

## Installation and Deployment Guide



Network Security

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 product, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro website at:

<http://www.trendmicro.com/download>

Trend Micro, the Trend Micro t-ball logo, ActiveUpdate, OfficeScan, Control Manager, and Network VirusWall are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2003-2010. Trend Micro Incorporated. All rights reserved.

Document part no. NVEM34453/100419

Release date: December 18, 2010

Product name: Trend Micro™ Network VirusWall™ Enforcer 1500i

Software version: 3.1

Protected by US patent no. 5,623,600

The user documentation for Network VirusWall Enforcer is intended to introduce the main features of the product and installation instructions for your production environment. Read through it prior to installing or using the product.

Detailed information about how to use specific features within the product are available in the Online Help and the Knowledge Base at the Trend Micro website.

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

About this Installation and Deployment Guide .....	viii
Content Overview .....	viii
Document Set .....	ix
Documentation and Software Updates .....	ix
Audience .....	x
Device and Software Version .....	x
Document Conventions .....	x

## Chapter 1: Introducing Network VirusWall Enforcer

Network VirusWall Enforcer Overview .....	1-2
Key Concepts .....	1-3
Technical Specifications .....	1-4

## Chapter 2: Getting Started

Package Contents .....	2-2
Front Panel .....	2-4
Installing the Bezel .....	2-7
Back Panel .....	2-9

Device Ports .....	2-10
Port Functions .....	2-11
Data Port Adapter .....	2-12
Network Port Indicators .....	2-12
Indicators on Onboard Ports .....	2-12
Indicators on the Copper Expansion Cards .....	2-13
Installing the Device .....	2-13

## **Chapter 3: Deploying Network VirusWall Enforcer**

Planning for Deployment .....	3-2
Deployment Overview .....	3-2
Phase 1: Plan the Deployment .....	3-2
Phase 2: Perform Preconfiguration .....	3-3
Phase 3: Manage Devices .....	3-3
Deployment Notes .....	3-3
Identifying What to Protect .....	3-4
Remote Access Endpoints .....	3-5
Guest Endpoints .....	3-8
Key Segments and Critical Assets .....	3-9
Dual-Switch VLAN Environment .....	3-10
Single-Switch VLAN Environment .....	3-12
Networks with IPv6 Addresses .....	3-13
IPv6 Limitations .....	3-13
Pure IPv6 Environments .....	3-14
Dual-Stack and Mixed Environments .....	3-14
Planning for Network Traffic .....	3-15
Determining the Number of Devices to Deploy .....	3-15
Fault Tolerance .....	3-15
Failopen .....	3-16
Failopen Considerations .....	3-16

Conducting a Pilot Deployment .....	3-17
Choosing a Pilot Site .....	3-17
Creating a Contingency Plan .....	3-18
Deploying and Evaluating your Pilot .....	3-18
Redefining Your Deployment Strategy .....	3-18
Basic Deployment Scenario .....	3-18

## **Chapter 4: Preconfiguring Network VirusWall Enforcer**

Before Preconfiguration .....	4-2
Verifying Network Support .....	4-2
Preparing for Preconfiguration .....	4-2
Understanding Preconfiguration .....	4-3
The Preconfiguration Console .....	4-3
Performing Preconfiguration .....	4-3
Logging on the Preconfiguration Console .....	4-4
Configuring Device Settings .....	4-6
Enabling Ports and Selecting Port Functions .....	4-7
Setting the Interface Speed and Duplex Mode .....	4-9
Connecting to the Network .....	4-10
Configuring Network VirusWall Enforcer .....	4-10

## **Chapter 5: Troubleshooting and Technical Support**

Device Issues .....	5-2
Getting Technical Support .....	5-3
Before Contacting Technical Support .....	5-3
Contacting Technical Support .....	5-3

## **Index**





# Preface

## Preface

Welcome to the Trend Micro™ Network VirusWall™ Enforcer 1500i *Installation and Deployment 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 who want to plan, deploy, and preconfigure Network VirusWall Enforcer.

This preface discusses the following topics:

- *About this Installation and Deployment Guide* on page viii
- *Document Set* on page ix
- *Audience* on page x
- *Document Conventions* on page x



# About this Installation and Deployment Guide

This document contains detailed information about getting started with Network VirusWall Enforcer. It provides an overview of the device and how to install it. It also covers initial configuration and deployment to help you prepare the device for use in protecting your network.

## Content Overview

The *Installation and Deployment Guide* provides the following information.

**TABLE P-1. Document contents**

<i>Introducing Network VirusWall Enforcer</i> on page 1-1	An overview of the device, its components, and its technical specifications
<i>Getting Started</i> on page 2-1	Details of the actual device and its specifications, including instructions for mounting and powering on the device
<i>Deploying Network VirusWall Enforcer</i> on page 3-1	Recommendations to help you plan for the deployment of one or more devices
<i>Preconfiguring Network VirusWall Enforcer</i> on page 4-1	Considerations and procedures on how to perform initial configuration (or preconfiguration)
<i>Troubleshooting and Technical Support</i> on page 5-1	Troubleshooting tips for issues encountered during preconfiguration

## Document Set

The following documents are provided with your product.

**TABLE P-2. Product documentation**

DOCUMENT	FORMAT	LOCATION	COVERAGE
Installation and Deployment Guide	PDF	<ul style="list-style-type: none"> <li>• USB flash drive</li> <li>• Trend Micro Download Center</li> </ul>	Guides you through device installation, deployment, and initial configuration
Administrator's Guide	PDF	<ul style="list-style-type: none"> <li>• USB flash drive</li> <li>• Trend Micro Download Center</li> </ul>	Explains features and guides you through managing policies, administrative tasks, and troubleshooting
Quick Start Guide	PDF and print	<ul style="list-style-type: none"> <li>• USB flash drive</li> <li>• Trend Micro Download Center</li> <li>• Product package</li> </ul>	Provides an overview of the device and initial tasks
Online Help	Web pages	<ul style="list-style-type: none"> <li>• Web console</li> </ul>	Explains options on the web console and relevant tasks
Readme	Text	<ul style="list-style-type: none"> <li>• USB flash drive</li> <li>• Trend Micro Download Center</li> </ul>	Provides late-breaking news and software build information

## Documentation and Software Updates

For the latest documentation and software updates, visit the Trend Micro Download Center at:

<http://downloadcenter.trendmicro.com/>

## Audience

This *Installation and Deployment Guide* is targeted at network administrators who will deploy the device. Network VirusWall Enforcer documentation assumes that readers have networking knowledge and understand antivirus and content security concepts.

## Device and Software Version

This *Installation and Deployment Guide* is released for administrators that are using the following device and software version.

**TABLE P-3. Target device and software**

PRODUCT INFORMATION	TARGET
Device	Network VirusWall Enforcer 1500i
Hardware series	CR100 Series
Software version	3.1

## Document Conventions

Network VirusWall Enforcer documentation uses the following conventions.

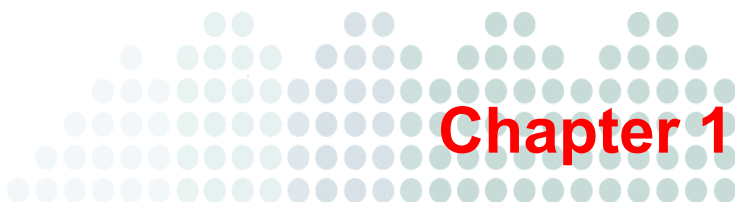
**TABLE P-4. Conventions used in the documentation**

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	References to user interface items, including menus, buttons, tabs, and other labels
<i>Italics</i>	References to other documentation

**TABLE P-4. Conventions used in the documentation (Continued)**

CONVENTION	DESCRIPTION
Monospace	Actual text, typed commands, file names, and program output
<b>Note:</b>	Important information
<b>Tip:</b>	Recommendations
<b>WARNING!</b>	Critical information





# Introducing Network VirusWall Enforcer

This chapter introduces Trend Micro™ Network VirusWall™ Enforcer 1500i and provides an overview of important concepts and features.

This chapter discusses the following topics:

- *Network VirusWall Enforcer Overview* on page 1-2
- *Key Concepts* on page 1-3
- *Technical Specifications* on page 1-4

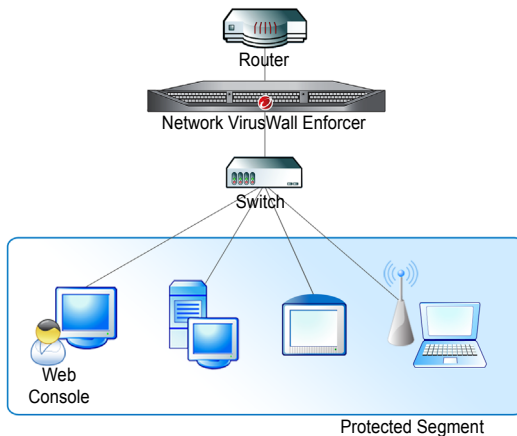
## Network VirusWall Enforcer Overview

Trend Micro™ Network VirusWall™ Enforcer 1500i is an outbreak prevention appliance that allows organizations to enforce security policies at the network layer. Network VirusWall Enforcer scans network traffic to help ensure that it is free of fast-spreading network viruses. It helps reduce the chance of severe security compromise by preventing ARP spoofing attacks.

Network VirusWall Enforcer can identify infected computers and deliver cleanup services to these endpoints. Because it works at the network layer, it can effectively quarantine and isolate actual and potential infection sources. It can address infected endpoints, endpoints with software vulnerabilities or those without adequate malware protection, and endpoints that violate network usage policies.

Network VirusWall Enforcer helps organizations take precise action on security policy violations to proactively detect, contain, and even eliminate malware outbreaks. With Network VirusWall Enforcer in the network, organizations can significantly reduce network downtime due to rapidly spreading malware and reduce the cost of dealing with the malware at individual endpoints.

*Figure 1-1* depicts a how Network VirusWall Enforcer can be deployed to protect a network.



**FIGURE 1-1. Basic Deployment**

## Key Concepts

Before proceeding to the succeeding sections of this document, take note of the following concepts.

**TABLE 1-1. Key Concepts in this Document**

CONCEPT	DESCRIPTION
Management port	Dedicated for management purposes. You can specify only one management port.
Mirror port	Sends all traffic passing the device to a computer to capture all data. The data can then be used for debugging purposes. You can specify one mirror port. Using this port type can impact performance.
Regular ports	Carries analyzed traffic to and from segments. You can specify multiple regular ports. Regular ports are also referred to as "bridge" ports.
Failopen	A fault-tolerance solution also known as "LAN bypass" that allows the Network VirusWall Enforcer device to continue to pass traffic even if a software or hardware failure occurs within the device.
Preconfiguration console	The console used to preconfigure a Network VirusWall Enforcer device. The preconfiguration process involves port configuration and setup of the management IP address to enable access to the web console.
Web console	The browser-based administrative console for defining policies and managing the device.



# Technical Specifications

The following table lists the technical specifications of Network VirusWall Enforcer:

**TABLE 1-2.      Technical specifications**

SPECIFICATION	DETAILS
Base unit	Dell™ OEM CR100 Rack Mount Server
Processor	Intel™ Core™ 2 Duo E2160 Processor, 2GHz
Memory	1GB ECC
Onboard NIC	Two RJ-45 10/100/1000 Mbps Ethernet
Network adapter (expansion slot)	Silicom™ PEG2BPi-SD-RoHS (Dual Port Copper Gigabit Ethernet PCI Express Bypass Server Adapter)
Power supply	345W



## Chapter 2

# Getting Started

This chapter guides you through setting up and powering on a Trend Micro™ Network VirusWall™ Enforcer 1500i device.

This chapter discusses the following topics:

- *Package Contents* on page 2-2
- *Front Panel* on page 2-4
- *Back Panel* on page 2-9
- *Device Ports* on page 2-10
- *Installing the Device* on page 2-13

## Package Contents

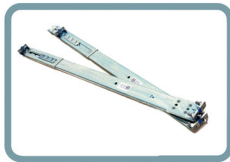
*Figure 2-1* illustrates the package contents.



Device with bezel



Power cord



Rack kit



Documents  
and USB drive

**FIGURE 2-1.** Package contents

---

**Note:** The actual items in your package may appear slightly different from those shown in this document.

---

Refer to *Table 2-1* to check whether the package is complete. If any of the items is missing, please contact Trend Micro support (see *Getting Technical Support on page 5-3*).

**TABLE 2-1. Network VirusWall Enforcer package contents**

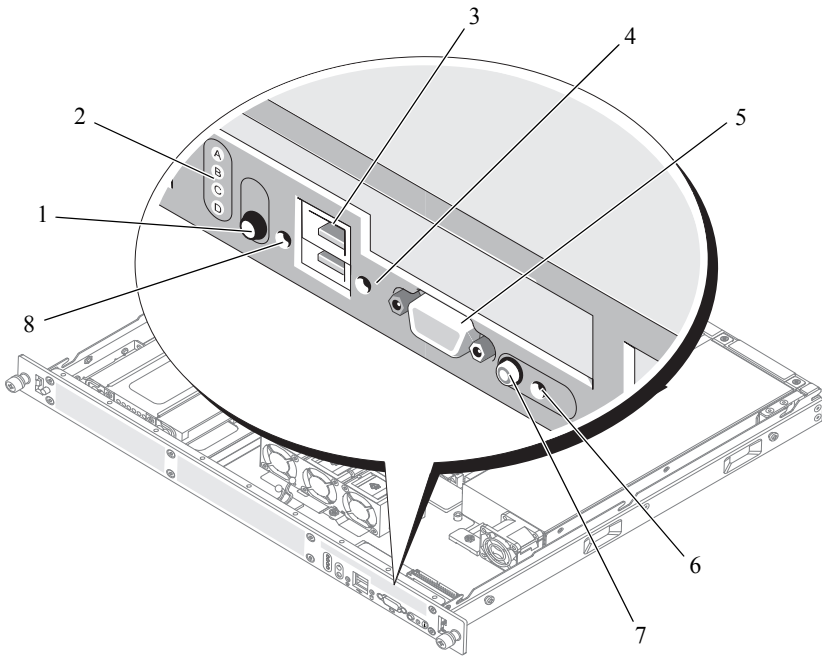
QUANTITY	ITEM	DESCRIPTION
1 unit	Network VirusWall Enforcer device	The device and the lockable bezel
1 piece	Power cord	Supplies power to the device
1 set	Rack kit	Mounts the device to a standard 19-inch rack cabinet
1 unit	Network VirusWall Enforcer USB flash drive	<p>Bootable USB flash drive that can be used to restore the device operating system and software. This flash drive also includes tools and device documentation, specifically:</p> <ul style="list-style-type: none"> <li>• Image file for the Network VirusWall Enforcer operating system</li> <li>• Security Appliance License Agreement</li> <li>• Third-party License Attributions</li> <li>• Administrator's Guide</li> <li>• Installation and Deployment Guide</li> <li>• Quick Start Guide</li> <li>• Readme</li> <li>• Trend Micro™ Control Manager™ patches</li> <li>• Syslog and TFTP tools</li> </ul> <hr/> <p><b>Note:</b> Refer to the troubleshooting section in the <i>Administrator's Guide</i> for instructions on how to use the provided tools.</p> <hr/>

**TABLE 2-1. Network VirusWall Enforcer package contents (Continued)**

QUANTITY	ITEM	DESCRIPTION
3 printed documents	<ul style="list-style-type: none"><li>• Security Appliance License Agreement</li><li>• Quick Start Guide</li><li>• Dell™ Product Information Guide</li></ul>	Printed documents that provide safety, licensing, and getting started information. Consult these documents before using Network VirusWall Enforcer.


## Front Panel

*Figure 2-2* shows the controls, indicators, connectors, and features on the front panel, behind the removable bezel. *Table 2-2* provides component descriptions.






**FIGURE 2-2. Front panel**

**TABLE 2-2. Front panel features**

ITEM	COMPONENT	ICON	DESCRIPTION
1	Power-on indicator, power button		The power button turns the device on and off. The indicator lights up when the device is on.
2	Diagnostic indicators (4)		The diagnostic indicators aid in troubleshooting hardware-related issues with technical support.

**TABLE 2-2. Front panel features (Continued)**

ITEM	COMPONENT	ICON	DESCRIPTION
3	USB connectors (2)		The connectors accept USB 2.0-compliant devices. Use these connectors to attach a keyboard and configure the device.
4	Hard drive activity indicator		The green hard drive activity indicator flashes when the hard drive is in use.
5	Video connector		Connects to a monitor; can be used to locally access and configure the device.
6	Device status indicator		<p>The blue device status indicator lights up during normal device operation.</p> <p>The amber device status indicator flashes when the device needs attention due to a hardware problem.</p>
7	Device identification button		You can use the device identification buttons on the front and back panels to locate a particular device within a rack. When one of these buttons is pushed, the blue device status indicators on the front and back panels blink until one of the buttons is pushed again.
8	NMI button		The nonmaskable interrupt (NMI) button is used to troubleshoot software and device driver errors. This button can be pressed using the end of a paper clip. Use this button only if directed to do so by qualified support personnel.

A photo of the Network VirusWall Enforcer front panel appears below.



**FIGURE 2-3.** Network VirusWall Enforcer front panel

## Installing the Bezel

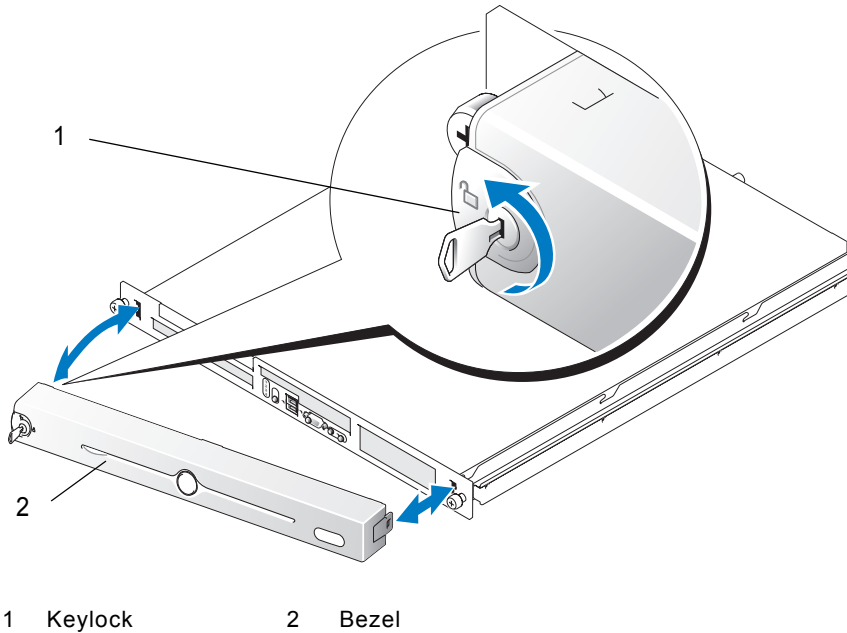
The device is supplied with a removable bezel as shown in [Figure 2-4](#).



**FIGURE 2-4.** Network VirusWall Enforcer with the bezel

To prevent users from inadvertently powering off the device, attach the bezel.





**FIGURE 2-5. Installing and removing the bezel**

**To install the bezel:**

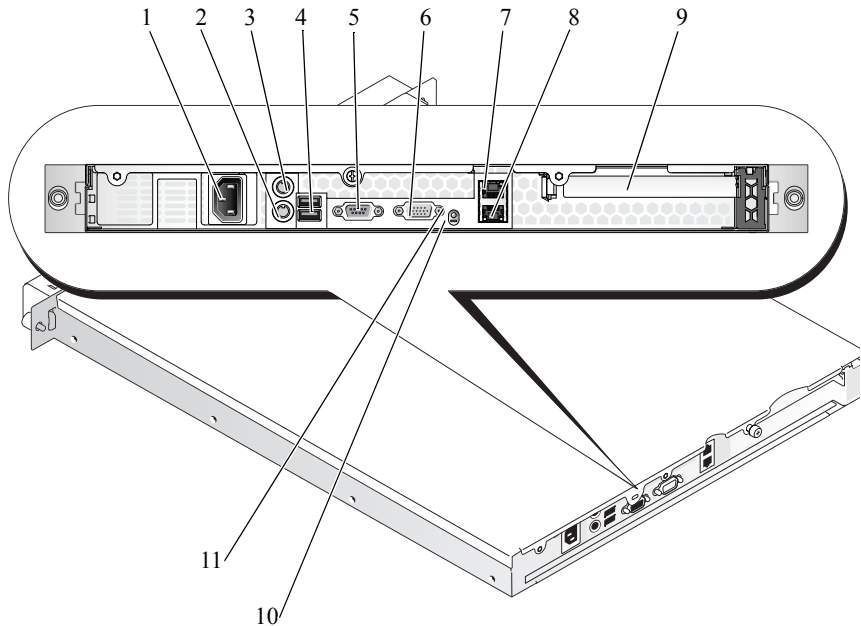
1. Hook the right end of the bezel into the bezel slot on the right side of the device front plate
2. Rotate the other end of the bezel toward the front panel and press the bezel onto the panel to engage the latch.
3. Lock the bezel.

**To remove the bezel:**

1. Unlock the bezel.
2. Unlatch the left end of the bezel and rotate it away from the front panel.
3. Unhook the right end of the bezel and pull the bezel away from the device.

## Back Panel

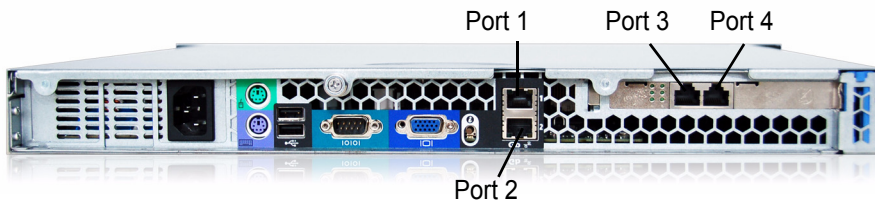
*Figure 2-6* shows the controls, indicators, and connectors located on the back panel.



1	Power supply connector	2	Keyboard connector	3	Mouse connector
4	USB connectors (2)	5	Serial connector	6	Video connector
7	Network port 1	8	Network port 2	9	NIC expansion slot
10	Device status indicator	11	Device identification button		

**FIGURE 2-6. Back panel**

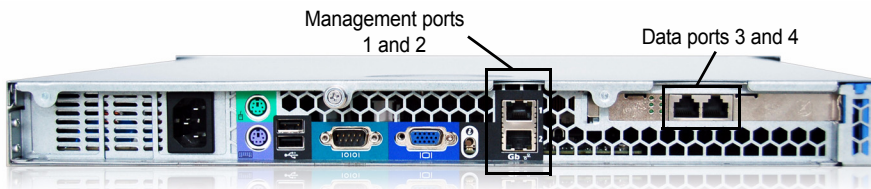
A dual port server adapter occupies the expansion slot. The two ports in this card correspond to ports 3 and 4, as shown in the image below, for a total of four network ports.



**FIGURE 2-7. Standard four-port configuration**

## Device Ports

Network VirusWall Enforcer supports four network ports, with the first two ports (port 1 and 2) providing management functionality. More specifically, these ports can be configured as management (MGMT) or mirror (MIRR) ports. Ports 3 and 4 are regular data ports that connect to the network and provide security functionality. The device applies its protection features to packets that pass through these data ports.



**FIGURE 2-8. Network VirusWall Enforcer ports**

## Port Functions

Network VirusWall Enforcer ports can be classified based on their function. As described earlier, there are regular data ports and management ports. Management ports can be assigned different functions as shown in the table below.

**TABLE 2-3. Port types**

<b>TYPE (INTERFACE TYPE; PORT NUMBER)</b>	<b>FUNCTION (CODE)</b>	<b>DEFAULT STATE</b>	<b>DESCRIPTION</b>
Data (Copper or Fiber; ports 3 onwards)	Regular (REG)	Enabled	These are the standard ports used for policy enforcement. Network VirusWall Enforcer can assess endpoints connected to this port through L2 or L3 switches.
Management (Copper; ports 1 to 2)	Management (MGMT)	Disabled	You can access the web console through all regular ports, but you can also dedicate a single port for accessing the web console and managing the device.
	Mirror (MIRR)		Assign this function to send all traffic through this port. You can use this port to capture all scanning data, which can be used for debugging. Note that having a mirror port can impact performance.

While the management ports are onboard ports, Network VirusWall Enforcer data ports are provided using Silicom PEG2BPi-SD-RoHS (Dual port Copper Gigabit Ethernet PCI Express Bypass Server Adapter). This server adapter provides maximum network uptime with copper bypass circuitry.

By using bypass server adapters, Network VirusWall Enforcer data ports provide a fault-tolerance solution known as "failopen" or "LAN bypass". This solution allows the Network VirusWall Enforcer to continue passing network traffic even if other device components fail or when the device loses power.

---

**Note:** Management ports do not support failopen.

---

## Data Port Adapter

While the management ports are onboard ports, Network VirusWall Enforcer data ports are provided using Silicom PEG2BPi-SD-RoHS (Dual port Copper Gigabit Ethernet PCI Express Bypass Server Adapter). This server adapter provides maximum network uptime with copper bypass circuitry.

By using bypass server adapters, Network VirusWall Enforcer data ports provide a fault-tolerance solution known as "failopen" or "LAN bypass". This solution allows Network VirusWall Enforcer to continue passing network traffic even when other device components fail or when the device loses power.

---

**Note:** Ports in the management interface do not support failopen.

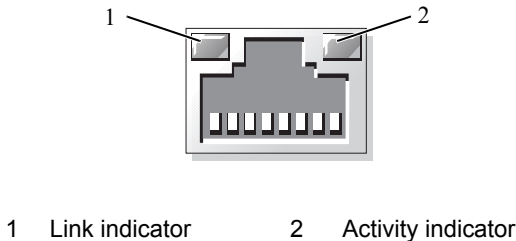
---

## Network Port Indicators

Each Network VirusWall Enforcer port has an indicator that allows you to determine the port's current state.

### Indicators on Onboard Ports

Each onboard port (ports 1-2) on the back panel has an indicator that provides information on network activity and link status. The following figures and tables describe the indicators on the onboard ports.



**FIGURE 2-9. Onboard port indicators**

**TABLE 2-4. Indicator codes for onboard ports**

INDICATOR CODE	STATUS
Link and activity indicators are off.	The port is not connected to the network.
Link indicator is green.	The port is connected to a valid link partner on the network.
Activity indicator is blinking yellow.	Network data is being sent or received.

**Indicators on the Copper Expansion Cards**

Network VirusWall Enforcer has a two-port gigabit server adapter in its expansion slot. Each port in the card corresponds to three LED indicators that provide the following information:

- Link/Activity (top LED, green)—lit at any speed and blinks with activity
- 100 (middle LED, green)—lit when connected at 100Mbit/s
- 1000 (middle LED, green)—lit when connected at 1000Mbit/s

**Installing the Device**

To use Network VirusWall Enforcer:

- Mounted to a standard 19-inch four-post rack cabinet  
The device requires 1 rack unit (RU) of vertical space in the rack.

---

**Tip:** If mounting more than one device, position and mount the devices in close proximity. Doing so allows you to easily maintain the devices.

---

- On any stable surface as a freestanding device  
For freestanding installation, ensure that the device has at least 2in (5.08 cm) of clearance on each side to allow for adequate airflow and cooling.

---

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

---

Installing the device involves performing the following tasks.

---

**WARNING!** Before performing the following tasks, review the safety instructions in the Product Information Guide that came with the device.

---

### Step 1: Unpack the device

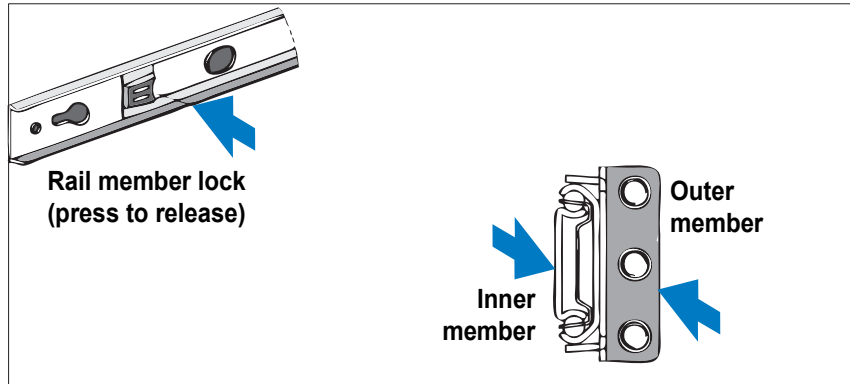
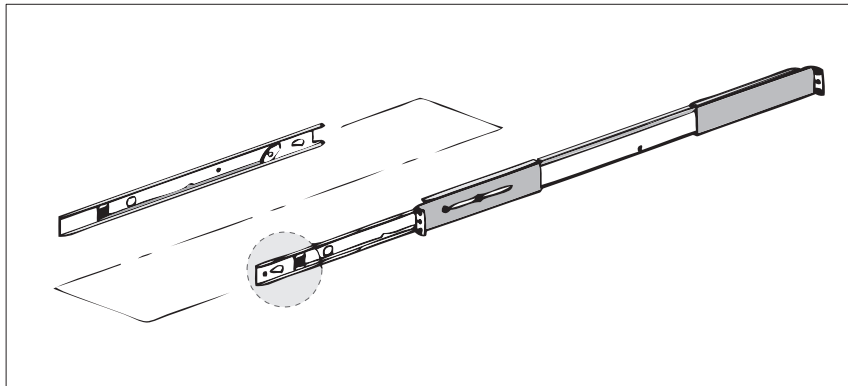
Unpack your device. The Network VirusWall Enforcer rack kit is very simple to use but will require a #2 Phillips-head screwdriver. The kit contains two rail assemblies as well as screws and brackets for attaching the device.

### Step 2: Install the rails and device in a rack

Assemble the rails and install the device in the rack.

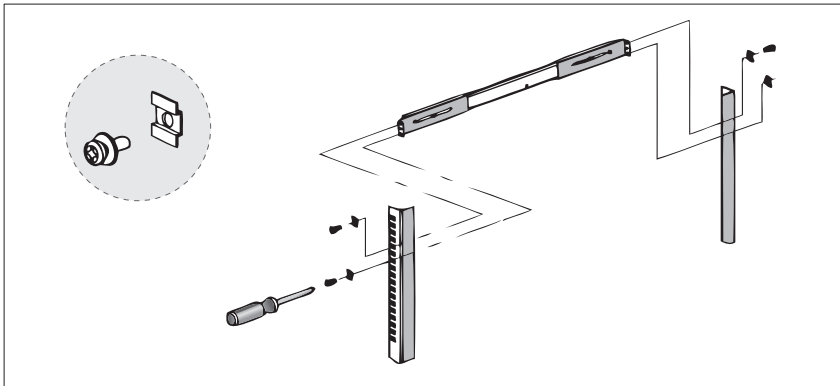
**To assemble the rack kit:**

1. Release and detach the inner member from each of the rails.

**FIGURE 2-10. Releasing the inner member****FIGURE 2-11. Sliding the inner member out to detach it**

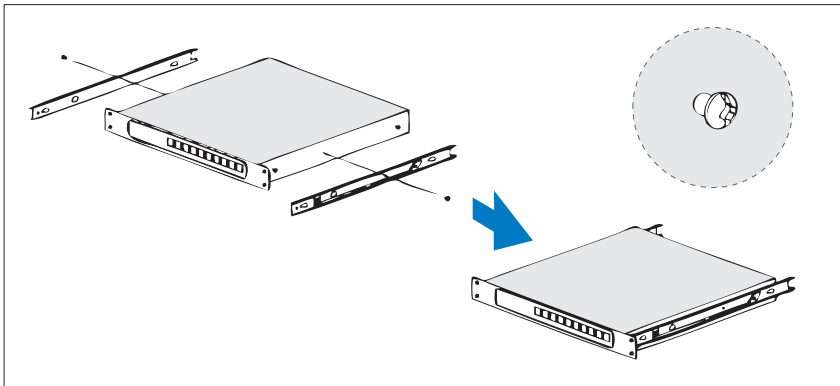
2. Using the provided screws, attach the outer member to the rack frame.





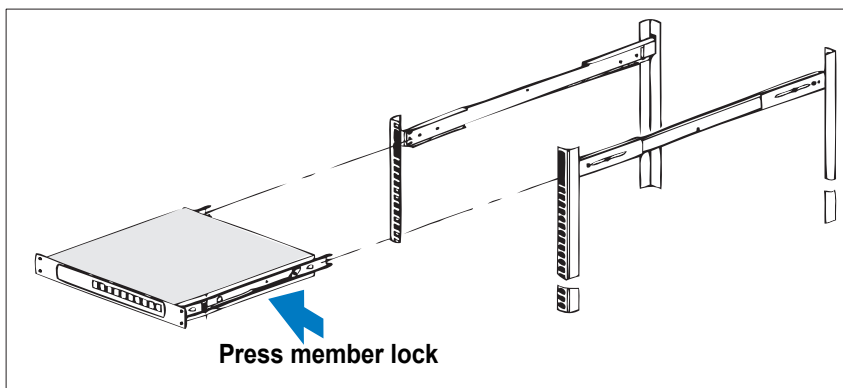
**FIGURE 2-12. Attaching the outer member to the rack frame**

3. Using another set of provided screws, attach the inner member to the Network VirusWall Enforcer device.



**FIGURE 2-13. Attaching the inner member to the device.**

4. Mount the device onto the rack.



**FIGURE 2-14. Mounting the device**

### **Step 3: Connect the keyboard and monitor (optional)**

Connect the keyboard and monitor. The connectors on the back of your device have icons indicating which cable to plug into each connector. Be sure to tighten the screws (if any) on the monitor's cable connector.

### **Step 4: Connect the power cables**

Connect the power cable(s) to the device and, if using a monitor, connect the monitor's power cable to the monitor.

### **Step 5: Turn on the device**

Press the power button on the device and on the monitor (optional). The power indicators should light up.

### **Step 6: Install the bezel (optional)**

Install the bezel. For detailed information, see [Installing the Bezel](#) on page 2-7.





## Chapter 3

# Deploying Network VirusWall Enforcer

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

This chapter explains how to plan for the deployment. It also provides deployment scenarios to help you understand the various ways the device can protect your network.

This chapter discusses the following topics:

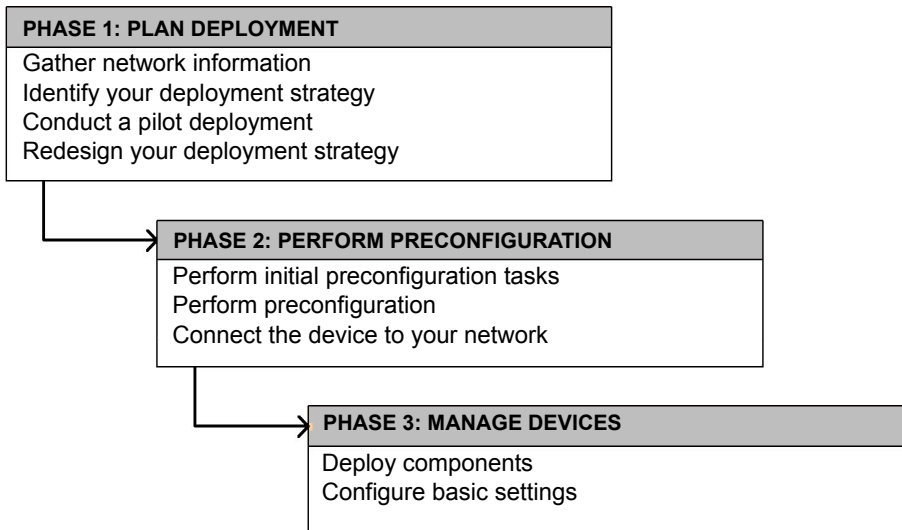
- *Planning for Deployment* on page 3-2
- *Identifying What to Protect* on page 3-4
- *Planning for Network Traffic* on page 3-15
- *Fault Tolerance* on page 3-15
- *Conducting a Pilot Deployment* on page 3-17
- *Redefining Your Deployment Strategy* on page 3-18
- *Basic Deployment Scenario* on page 3-18

# Planning for Deployment

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

## Deployment Overview

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



---

**Tip:** This *Installation and Deployment Guide* discusses phases 1 and 2. Refer to the *Administrator's Guide* for information related to phase 3.

---

## Phase 1: Plan the Deployment

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

- Identify the segments of your network that are in the greatest need of protection.

- Plan for network traffic, considering the location of critical computers, such as email, web, and application servers.
- Determine 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

In phase 2, begin implementing the plan you created in phase 1 by performing the following tasks:

- Perform the initial preconfiguration tasks (see [Before Preconfiguration](#) on page 4-2).
- Perform preconfiguration on the device(s) (see [Performing Preconfiguration](#) on page 4-3).
- Connect the device(s) to your network (see [Connecting to the Network](#) on page 4-10).

## Phase 3: Manage Devices

During phase 3, manage Network VirusWall Enforcer devices from the web console. For this phase, consult the following sections of the Administrator's Guide:

- *Understanding Network VirusWall Enforcer* provides details about relevant concepts, including management options, endpoints, security risks, policy enforcement, device ports, fault tolerance, updatable components, SNMP support, and VLAN support.
- *Preparing for Policy Enforcement* discusses the tasks you need to perform before creating policies and deploying them to your network.
- *Policy Creation and Deployment* covers actual policy creation, providing sample scenarios and instructions.

## Deployment Notes

Consider the following when planning for a deployment:

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

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

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

---

**Note:** Both the connected L2/L3 and Network VirusWall Enforcer devices should have the same port speed and duplex mode. Otherwise, the Network VirusWall Enforcer port will operate in half-duplex mode. To simplify configuration, you can set Network VirusWall Enforcer to auto-select the optimum port speed and duplex mode. Likewise, allow your switch to auto-select the port speed and duplex mode.

---

- For IPv4 addresses, the device supports addresses belonging to any class (class A, B, or C). For IPv6 addresses, it supports global unicast and link-local addresses.

---

**Tip:** Although each range is in a different class, you are not required to use any particular range for your internal network. However, selecting a fixed range greatly diminishes the chance of IP addressing conflicts.

---

- Policy enforcement and network virus scan support various actions for noncompliant or infected endpoints.

## Identifying What to Protect

Position Network VirusWall Enforcer between layer 2 (L2) or layer 3 (L3) devices. This way, the device can apply its protection to packets coming in or out of your network.

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

- 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, or application servers

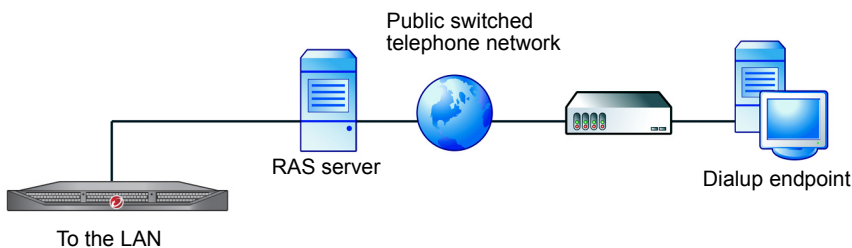
## Remote Access Endpoints

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.

You can consider two types of remote endpoints:

- **Dialup/VPN users**—telecommuters who typically dial up or use VPN to connect to your network
- **External business units**—offices located outside the main network site that need access to resources on the main network

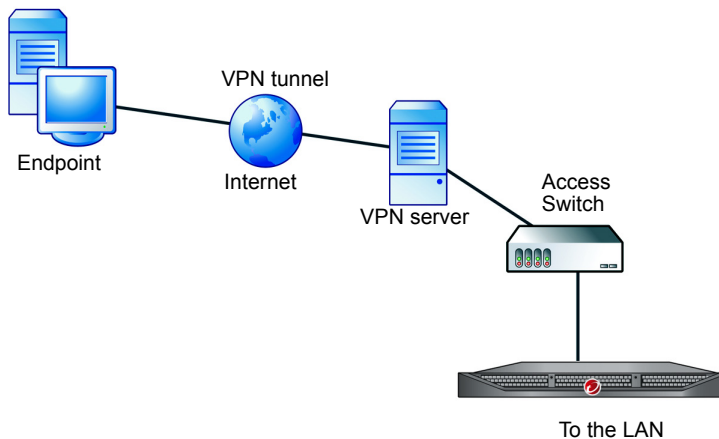
A home user could establish a dialup connection or a VPN connection to access a company's internal network resources. Most likely, business units would establish a VPN connection.



**FIGURE 3-1.** Dialup 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 *Key Concepts* on page 1-3 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 *Basic Deployment Scenario* on page 3-18). The home user accesses both network resources and the Internet in the same way that internal endpoints access them.



**FIGURE 3-2. Endpoint-to-site VPN deployment scenario**

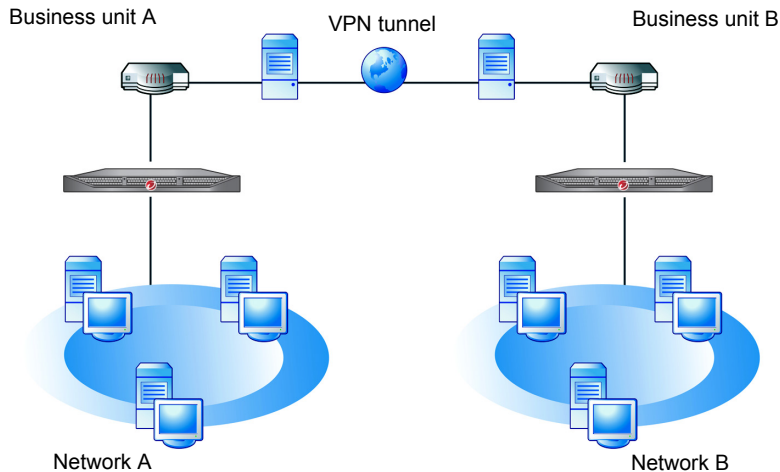
*Figure 3-2* illustrates a connection between a home user and an organization's internal network through a VPN server connected to a regular port (see *Key Concepts* on page 1-3 for information about different types of ports). In this configuration, the home user's VPN connection is considered part of the internal network.

---

**Note:** Network VirusWall Enforcer 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 dialup user scenario (see [Figure 3-1](#)).

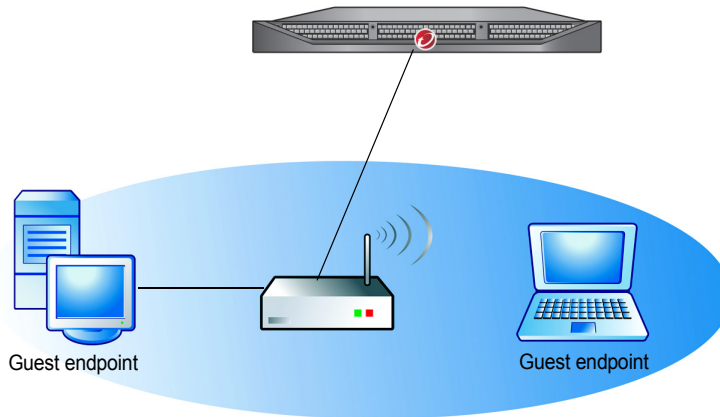


**FIGURE 3-3. Site-to-site VPN deployment scenario**

[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 [Key Concepts](#) on page 1-3 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 a major risk because they are typically outside the scope of the network security infrastructure. These endpoints are more likely to violate antivirus policies and introduce security risks to the network.

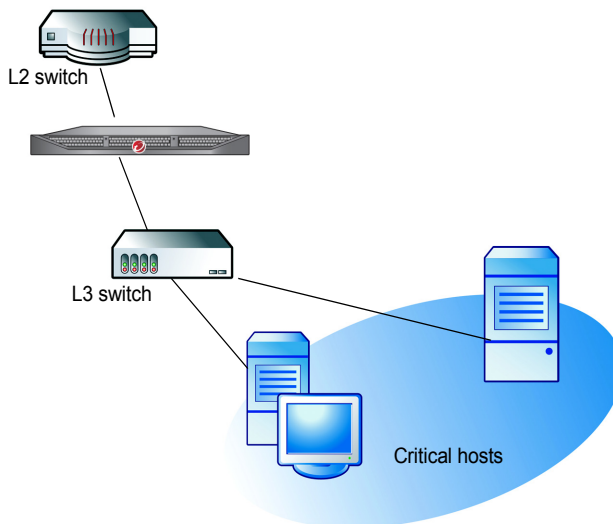


**FIGURE 3-4. Guest network deployment scenario**

*Figure 3-4* illustrates a segment of an internal network for guest endpoints. A wireless access point, switch, or hub is connected to the regular port (see [Key Concepts](#) on page 1-3 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 Segments and Critical Assets

Key network segments need to be protected from network-based threats. This may include a group of endpoint computers or network resources critical to your organization, such as email, web, or application servers.



**FIGURE 3-5. Key network segments scenario**

The diagram above 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 [Key Concepts](#) on page 1-3 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.

The device can also guard against attacks that not only originate on the Internet, but also attacks that may originate from within your network. Since traffic first passes through the device before reaching 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 must be placed in line on the physical network to provide security. In most situations, this means placing it between an upstream switch and one or more downstream switches.

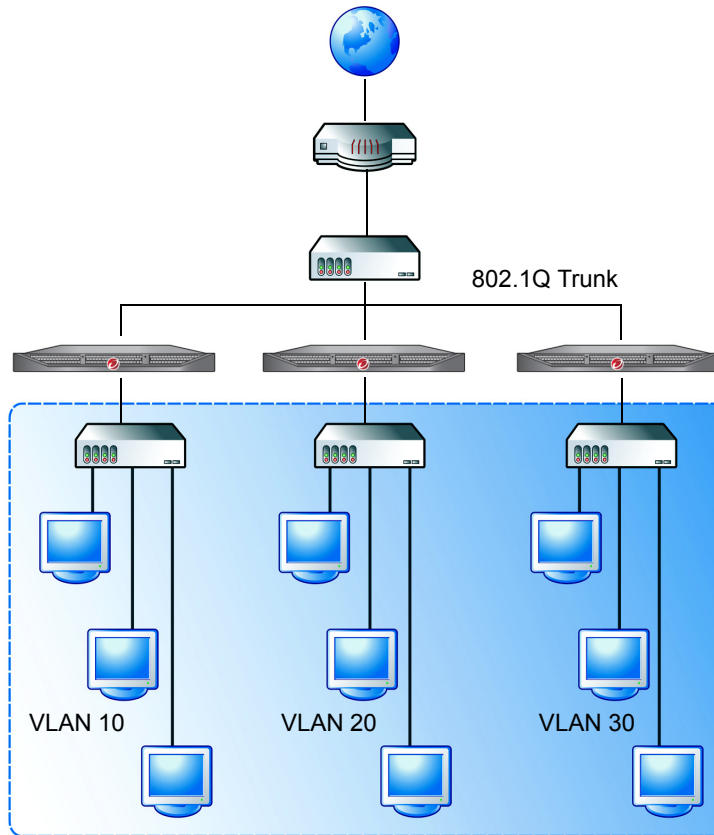
Most VLAN configurations will utilize two switches. Single-switch VLAN configurations are possible; for more information, refer to [\*Single-Switch VLAN Environment\*](#) on page 3-12. The figures in this section illustrate multiple downstream switches in a flat topology; however, a single in line configuration 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.

---

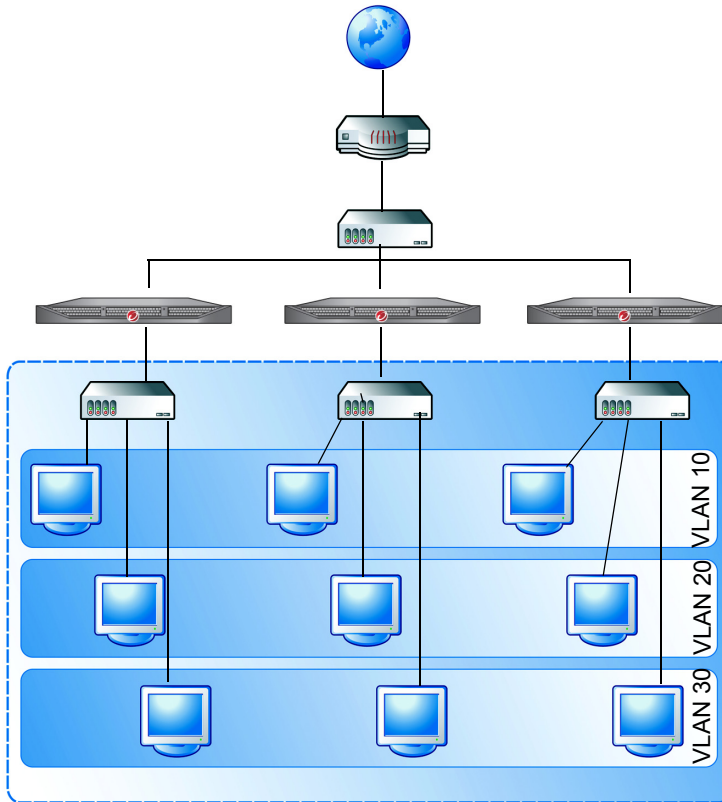
**Note:** Ensure that Spanning Tree Protocol (STP) is enabled. If STP is not enabled, packets may loop for an indefinite period.

---



**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.



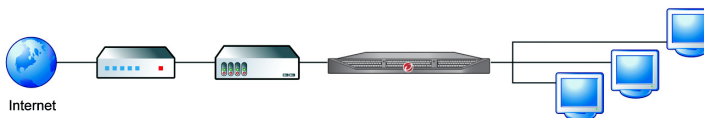
**FIGURE 3-7. Multiple VLAN segments with each device protecting all segments**

## Single-Switch VLAN Environment

A single-switch configuration may have the following properties:

- Possible only 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 is connected to port 1 on the switch.
- Endpoints are connected to other regular ports on Network VirusWall Enforcer.



**FIGURE 3-8. Single-switch VLAN environment**

## Networks with IPv6 Addresses

Administrators deploying Network VirusWall Enforcer in an environment with IPv6 addresses must plan carefully to ensure that the device can provide protection and does not interfere with network connectivity.

### IPv6 Limitations

The following features are not supported on IPv6 networks:

- Threat mitigation with Threat Discovery Appliance
- Policies that require user authentication using Kerberos
- Program rescue
- Enforcement of network application policies (port activity, instant messengers, file transfers, and Outbreak Prevention Policy)
- Remote detection of endpoint operating systems for policy enforcement
- ActiveUpdate through Network Address Translation/Protocol Translation (NAT-PT)
- Addressing:
  - Dynamic addressing from a Windows DHCPv6 server



- Limited Linux DHCPv6 support; the device can obtain an IP address, a prefix, and a DNS from a Linux DHCPv6 server, but it will not be able to obtain gateway settings.
- Specifying a link-local IP address as the update source

## Pure IPv6 Environments

In environments with purely IPv6 hosts, administrators do not need to perform special deployment tasks. As long as Network VirusWall Enforcer is supplied with a valid IPv6 address, it can function normally. Note, however, that certain device features are not available in pure IPv6 environments as described in [IPv6 Limitations](#) on page 3-13.

---

**Note:** Many resources on the Internet, including the Trend Micro™ ActiveUpdate™ and product registration servers, are accessible only through IPv4 traffic. When configured as an IPv6-only host, Network VirusWall Enforcer traffic to and from the Internet can be translated using a dual-stack proxy.

---

## Dual-Stack and Mixed Environments

Environments with dual-stack hosts or those with both IPv6 and IPv4 hosts require relatively complex deployment planning. Consider the following key points during planning:

- Ensure that you configure both an IPv4 and IPv6 address for Network VirusWall Enforcer if it will be processing both kinds of traffic.
- Network VirusWall Enforcer cannot perform traffic translation when in dual-stack mode. It will treat IPv6 and IPv4 traffic independently.
- Note the limitations of the device on IPv6 networks as discussed in [IPv6 Limitations](#) on page 3-13.

## Planning for Network Traffic

The scenario presented in *Key Segments and Critical Assets* on page 3-9 is 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 server or an Internet gateway. Because many viruses make their way into 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 placing the device where it can scan the most traffic.

## Determining the Number of Devices to Deploy

Determine how many devices would best meet your security requirements. Consider the following factors:

- **Existing network topology**—based on your network topology, identify the segments that you want the device to protect (see *Identifying What to Protect* on page 3-4)
- **Existing network device interfaces**—because a 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 devices
- **Desired effectiveness of protection**—to lower the risk of a virus outbreak spreading, segment several sections of your network with Network VirusWall Enforcer devices
- **Desired degree of performance**—consider the number of endpoints and the amount of traffic that a device can handle

## Fault Tolerance

Network VirusWall Enforcer provides fault tolerance with the failopen feature.

## Failopen

Failopen or LAN bypass involves one Network VirusWall Enforcer device. Failopen is a fault-tolerance solution that allows a Network VirusWall Enforcer to continue passing network traffic even when other device components fail or when the device loses power.

### Failopen Considerations

Consider the following important points about failopen:

- If the switches on your network do not support auto MDI/MDI-X, use a crossover and non-crossover cable combination to enable failopen. Invalid cable combinations prevent Network VirusWall Enforcer from using failopen and can result in network issues. Refer to device documentation to determine whether your L2 switches support auto MDI/MDI-X.
- All regular ports on the device support LAN bypass and will allow traffic bypass even when the device is powered off.
- To help ensure that failopen works, keep the total length of the network cable connecting regular ports to other devices within 100 meters (~328 feet).
- Resetting a Network VirusWall Enforcer device with failopen enabled temporarily blocks network connection for about 30 seconds.
- [Table 3-1](#) describes the connection status of ports when certain procedures are performed.

**TABLE 3-1. Port status**

TIME (SECONDS)	PROCEDURE	REGULAR PORTS WITH FAILOPEN
2	Restarting the device	Disconnected

TABLE 3-1. Port status

TIME (SECONDS)	PROCEDURE	REGULAR PORTS WITH FAILOPEN
38	Configuring memory	Connected
	Initializing	Connected
	Loading Grand Unified Bootloader (GRUB)	Connected
	Booting Network VirusWall Enforcer mini kernel	Connected
	Starting kernel	Connected
12	Disabling failopen and bridge learning	Disconnected
n/a	Preconfiguring the device	Connected

## Conducting a Pilot Deployment

Trend Micro recommends conducting a pilot deployment in a controlled environment to help you understand how the device features work. A pilot deployment also helps you determine how the device can be used to accomplish your security goals and the level of support you will likely need after a full deployment.

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. Look at other devices on your network, such as switches or firewalls, and other software installations, such as OfficeScan™ and Control Manager™. 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 or do not meet the expected results during 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 security installations on your network. This pilot evaluation can be rolled into the overall production and deployment plan.

---

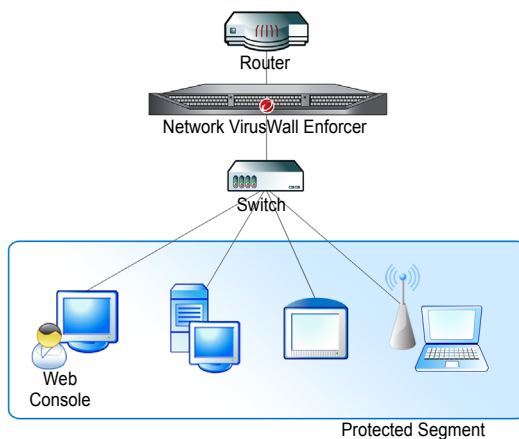
**Tip:** See [Performing Preconfiguration](#) on page 4-3 and [Verifying Network Support](#) on page 4-2 for checklists on how to prepare a device for deployment.

---

## 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 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. A switch or a router is connected to a regular port.



**FIGURE 3-9. Basic Deployment**

Network VirusWall Enforcer protects your network as follows:

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

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





## Chapter 4

# Preconfiguring Network VirusWall Enforcer

This chapter discusses the following topics:

- *Before Preconfiguration* on page 4-2
- *Understanding Preconfiguration* on page 4-3
- *The Preconfiguration Console* on page 4-3
- *Performing Preconfiguration* on page 4-3
- *Connecting to the Network* on page 4-10
- *Configuring Network VirusWall Enforcer* on page 4-10



## Before Preconfiguration

Complete the following tasks before you preconfigure Network VirusWall Enforcer:

- Test the failopen functionality. Network traffic should still pass through the device after a hardware or system error or if the device loses power.
- Determine the password for the admin account.

---

**Tip:** There are two default accounts: Admin and PowerUser. These accounts use admin and poweruser, respectively, as their default passwords.

---

- Determine the host name for the device.

## Verifying Network Support

In a failopen deployment, the total length of the network cable connecting regular ports to other devices must not exceed 100 meters (~328 feet).

A cable longer than the maximum length will prevent failopen from working. See [Failopen Considerations](#) on page 3-16 for more information.

## Preparing for Preconfiguration

To prepare for preconfiguration, check if you have completed the instructions in [Before Preconfiguration](#) on page 4-2 before starting with the succeeding steps.

Also, ensure that you can access Network VirusWall Enforcer directly. Before powering on the device, attach the following peripherals:

- VGA monitor
- Keyboard

---

**Tip:** For instructions on how to connect peripherals and power on the device, see [Installing the Device](#) on page 2-13.

---

## Understanding Preconfiguration

Ensure that the tasks in [Preparing for Preconfiguration](#) on page 4-2 have been completed before starting preconfiguration.

### To perform preconfiguration:

1. Plan and determine the deployment strategy (see [Deploying Network VirusWall Enforcer](#) on page 3-1).
2. Perform preconfiguration (see instructions in [The Preconfiguration Console](#) on page 4-3).
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 4-2), use the Preconfiguration console to proceed.

## The Preconfiguration Console

The Preconfiguration console lets you configure basic device settings directly using a keyboard and a monitor. All initial configuration tasks, like specifying port functions and the device IP address must be done through the Preconfiguration console.

The Preconfiguration console can also be accessed using an SSH client such as PuTTY. However, before this can be done, you must configure the device IP address and ensure that the device can connect to the network. For more information on accessing the Preconfiguration console remotely, see the *Administrator's Guide*.

## Performing Preconfiguration

You must complete the following tasks to preconfigure the device:

1. [Logging on the Preconfiguration Console](#) on page 4-4
2. [Configuring Device Settings](#) on page 4-6
3. [Setting the Interface Speed and Duplex Mode](#) on page 4-9



### To log on to the Preconfiguration console

1. To get full access to the Preconfiguration console, type the default administrator user name and password:

**User name:** admin

**Password:** admin

---

**Note:** Only the administrator and power user accounts can be used to log on to the Preconfiguration console. Immediately after logging on to the web console, change the passwords to these accounts for increased security. For more information, see the *Administrator's Guide*.

---

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

---

**Note:** The Preconfiguration console has a timeout value of ten minutes. If the console is idle for ten minutes, it automatically logs off the account. Also, to help protect the console from unauthorized access, users must wait between each logon attempt after three unsuccessful attempts.

---

```
=====Main Menu=====
1) Device Information and Status
2) Device Settings
3) Register to Trend Micro Control Manager
4) Interface Settings
5) Advanced Settings
6) Access Control
7) System Tasks
8) View System Logs
9) Save and Log Off
A) Log Off Without Saving

<UP>,<DOWN>:Change item. <ENTER>:Select item.
```

FIGURE 4-2. The Preconfiguration console main menu

## Configuring Device Settings

Immediately after logging on to the Preconfiguration console for the first time, configure the device host name and network settings.

### To configure the device settings:

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

```
=====Device Settings=====
Host name: 0NNJNUW1P
Management IP Setting (IPv4)
  Type: lstatic 1 (Use the <SPACEBAR> to change the value)
  IP address: 10.64.1.241
  Netmask: 255.255.255.0
  Default gateway: 10.64.1.1
  DNS server 1: 10.64.1.54
  DNS server 2: 10.64.1.55
Management IP Setting (IPv6)
  Type: lstatic 1 (Use the <SPACEBAR> to change the value)
  IP address: fe80::1
  Subnet prefix length: 64
  Default gateway:
  DNS server 1:
  DNS server 2:
Bind IP Address
  Interface: lbridge1 (Use the <SPACEBAR> to change the value)
  VLAN ID: 2
                                Return to the Main menu
  Use the <ESC> key to leave without saving.

<UP>, <DOWN>, <TAB>: Change field. <SPACEBAR>: Change value. <ENTER>: Select field.
```

**FIGURE 4-3.** Device Settings screen

---

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

---

2. Type a host name that properly represents the device in the network.  
Each device on your network must have a unique host name. Control Manager™ uses this unique host name during registration and as the managed product name.

Host names may contain up to 30 alphanumeric characters without spaces. Trend Micro recommends a unique descriptive host name to represent and identify the device as seen through the management console. For example, designate `NVWE-NY-main` as the host name for a device protecting a New York main office.

3. Type or select the management IP address settings under Management IP settings. Specify either the IPv4 or the IPv6 settings as necessary. When using Network VirusWall Enforcer as a dual-stack host, provide both IPv4 and IPv6 settings.

---

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

---

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

## Enabling Ports and Selecting Port Functions

Depending on your desired deployment, you may need to enable certain ports and specify their function. By default, only the regular ports are enabled. So, if you need to use management or mirror port functionality, you need to enable the management ports, which are ports 1 and 2.

**To enable non-regular ports and modify their function:**

1. On the **Main Menu** of the Preconfiguration console, type **4** to open the Interface Settings screen.

```
=====Interface Settings=====
Current Interface Settings:

Name          Port1 Port2 Port3 Port4
-----
Speed&Duplex  ----  ----  auto  auto
Type          DIS   DIS   REG   REG

DIS: Not assigned
N/A: External card not installed
MGMT: Management port
MIRR: Mirror port

10H: 10 Mbps x half-duplex
10F: 10 Mbps x full-duplex
100H: 100 Mbps x half-duplex
100F: 100 Mbps x full-duplex
1000F: 1000 Mbps x full-duplex
auto: Detect the best speed

1) Interface Speed & Duplex mode setting
2) Interface setting
3) Return to the Main menu

<UP>,<DOWN>:Change item. <ENTER>:Select item.
```

**FIGURE 4-4. Interface Settings screen**

2. Type **2** to select **Interface setting**.  
The Interface Settings screen changes so that the function of each port can be selected and modified.
3. Select a port by using the up and down arrows. Each port number corresponds to the physical ports as shown below.

**FIGURE 4-5. Network VirusWall Enforcer ports**

4. To modify the function of the selected port depending on your deployment strategy, press the SPACEBAR. Disabled management interface (onboard) ports can be assigned the following functions:
  - **DIS**—the port is disabled; this is the default setting
  - **MGMT**—the port is specifically used to manage the device
  - **MIRR**—the port is used to mirror network traffic to another computer; this is typically used for debugging

---

**Tip:** For more information about different port functions, see [Port Functions](#) on page 2-11.

---

5. Select **Return to the previous menu** and press ENTER.

## Setting the Interface Speed and Duplex Mode

Both the connected L2/L3 and Network VirusWall Enforcer devices should have the same port speed and duplex mode. Otherwise, the Network VirusWall Enforcer port will operate in half-duplex mode. To simplify configuration, you can set Network VirusWall Enforcer to auto-select the optimum port speed and duplex mode. However, manual selection of the correct port speed and duplex mode can help ensure optimal network performance. Use the Preconfiguration console to configure the interface speed and duplex mode.

### To set the interface speed and duplex mode:

1. On the Interface Settings screen, type **1** to open the **Interface speed & duplex mode setting** screen, which displays the current interface speeds and duplex settings of all ports.
2. Select a port by using the up and down arrows.
3. Select the speed, using the SPACEBAR to scroll through the speed and duplex mode options. For more information on the supported speed and duplex modes, see [Deployment Notes](#) on page 3-3.
4. After configuring all port speeds and duplex modes, select **Return to the previous menu** to go back to the **Interface Settings** screen.



5. Type **3** to select **Return to Main menu**. The **Main Menu** displays.
6. Select **Save and Log Off** to make changes take effect.

---

**Note:** In order to apply the configuration changes made in the Preconfiguration console, you must save and log off.

---

## Connecting to the Network

Make sure you preconfigure the device before attempting to connect the device 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 the cable to a regular port and the other to a segment of your network.
2. Power on the device.

---

**Note:** Network VirusWall Enforcer can handle various interface speed and duplex mode network traffic. See [Setting the Interface Speed and Duplex Mode](#) on page 4-9.

---

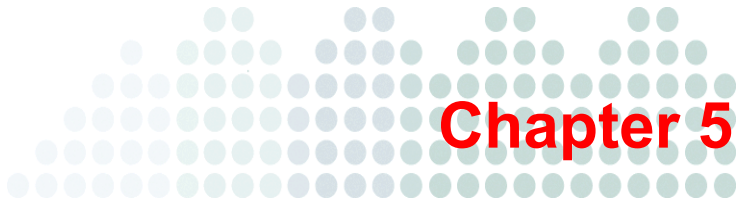
## Configuring Network VirusWall Enforcer

After preconfiguring Network VirusWall Enforcer, you can configure the device and start protecting your network.

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

- Change the password for the default accounts
- Activate the device
- Update components
- Configure policy enforcement

For more information, refer to the *Online Help* and the *Administrator's Guide*. See [Document Set](#) on page ix.



# Troubleshooting and Technical Support

This chapter provides troubleshooting information for issues that may arise during the preconfiguration.

---

**Tip:** Refer to the *Administrator's Guide* for answers to frequently asked questions and other troubleshooting tips.

---

This chapter discusses the following topics:

- [Device Issues](#) on page 5-2
- [Getting Technical Support on page 5-3](#)

## Device Issues

#	ISSUE	CORRECTIVE ACTION/EXPLANATION
1	admin password misplaced or forgotten	<p>You have two options:</p> <ol style="list-style-type: none"><li>1. If the device has registered to Control Manager, you can access the web console and change the password through the Control Manager console using a Control Manager account.</li><li>2. You can reload the device image from the provided USB flash drive. Note that this will remove any settings and policies stored on the device.</li></ol> <hr/> <p><b>Note:</b> Reloading the Network VirusWall Enforcer image will restore the default settings. You can only recover device settings if you exported them to a file earlier.</p> <hr/>
2	Unable to access the Pre-configuration console remotely	<p>Verify secure console port connections and SSH client software settings.</p> <p>See the <i>Administrator's Guide</i> for more information on accessing the Preconfiguration console remotely.</p>
3	Network packet delivery is too slow and seems to be blocked	<p>Network VirusWall Enforcer does not refresh its MAC address table if one of the links fails. The result is a temporary delay in packet delivery.</p>

## Getting Technical Support

Trend Micro is committed to providing service and support that exceeds your expectations. You must register your product to qualify for support.

### Before Contacting Technical Support

Before contacting technical support, see if these resources can help you address your problem:

- **Product documentation**—the *Administrator's Guide*, *Installation and Deployment Guide*, and *Online Help* provide comprehensive information about Network VirusWall Enforcer. Search these documents for helpful information.
- **Knowledge Base**—a key part of our technical support website, the Trend Micro Knowledge Base contains the latest information about Trend Micro products.

To search the Knowledge Base, visit:

<http://esupport.trendmicro.com>

### Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- Email support
- Online Help—configuring the product and parameter-specific tips
- Readme—late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base—technical information procedures provided by the Support team:

<http://esupport.trendmicro.com>

- Product updates and patches

<http://www.trendmicro.com/download/>

To locate the Trend Micro office nearest you, visit:

<http://www.trendmicro.com/en/about/contact/overview.htm>

Having the following information ready before you contact our support staff can help them resolve problems faster:

- Device model and image (firmware) version
- Deployment setup
- Interface speed and duplex mode settings
- Exact text of any error messages
- Steps to reproduce the problem

# Index

## A

- activation 4-10
- ActiveUpdate 3-13
- activity indicator 2-13
- Administrator's Guide ix, 2-3
- airflow and cooling 2-14
- application policy 3-13
- audience x
- auto MDI/MDI-X 3-16

## B

- back panel 2-9
- basic deployment 3-18
- bezel 2-3, 2-7—2-8, 2-17
  - installation 2-8
  - removal 2-8

## C

- cables 3-16
- concepts 1-3
- configuration 4-6, 4-10
- Control Manager 2-3, 5-2
- conventions x
- critical hosts 3-9
- crossover cables 3-16

## D

- data interface 2-11
- data ports 2-10
- delayed packets 5-2

- Dell OEM CR100 1-4
- deployment
  - identifying what to protect 3-4
  - number of devices 3-15
  - overview 3-2
  - planning 3-2
- deployment planning 3-2
- deployment scenarios
  - basic deployment 3-18
- deployment stages 3-2
- deployment strategy 3-18
- device identification button 2-6, 2-9
- device image 5-2
- device ports 2-10
- device settings 4-6
- device status indicator 2-6, 2-9
- diagnostic indicators 2-5
- dialup 3-5—3-6
- DIS 4-9
- document
  - conventions x
- document set ix
- documentation
  - audience x
- Dual 3-10
- dual-stack 4-7
- dual-switch VLAN 3-10
- duplex mode 4-9

## **E**

endpoint notifications 3-13  
expansion cards 2-12  
expansion slot 2-13

## **F**

failopen 1-3, 2-12, 3-16  
    and port status 3-16  
    cable length 3-16  
    considerations 3-16  
    effect of a reset 3-16  
    without power 3-16  
fault-tolerance 1-3, 2-12, 3-16  
file transfers 3-13  
freestanding installation 2-14  
frequently asked questions (FAQs) 5-1  
front panel 2-4, 2-7

## **G**

Grand Unified Bootloader 3-17  
GRUB 3-17  
guest endpoints 3-5, 3-8

## **H**

hard drive activity indicator 2-6  
host names 4-7

## **I**

image file 2-3  
installation 2-13  
    connecting the power cable 2-17  
    installing the bezel 2-17  
    keyboard and monitor 2-17  
    rack mounting 2-14  
    rail assembly 2-14  
    turning on the device 2-17  
Installation and Deployment Guide ix, 2-3  
instant messengers 3-13  
Intel Core 2 Duo 1-4

interface speed 4-9  
introduction 1-1  
IPv4 addresses 3-4  
IPv6 addresses 3-4  
IPv6 networks  
    dual-stack and mixed environments 3-14  
    limitations 3-13  
    pure environments 3-14  
issues 5-2

## **K**

Kerberos 3-13  
key network segments 3-9  
key network segments and assets 3-5, 3-9  
keyboard 4-2  
keylock 2-8

## **L**

LAN bypass 1-3, 2-12, 3-16  
LED indicators 2-13  
link indicator 2-13  
link-local 3-14  
Linux DHCPv6 3-14

## **M**

mail servers 3-9  
management interface 2-11, 4-8  
management IP address 4-7  
management port 2-10—2-11  
MDI/MDI-X 3-16  
memory 1-4  
MGMT 2-10—2-11, 4-9  
MIRR 2-10—2-11, 4-9  
mirror port 1-3, 2-10—2-11  
monitor 2-6, 4-2  
mounting the device 2-14

## **N**

NAT devices 4-7  
NAT-PT 3-13

- Network Address Translation/Protocol Translation 3-13
- network cables 4-2
- network port 2-9
- network traffic, planning for 3-15
- network virus scan 3-4
- NIC expansion slot 2-9
- nonmaskable interrupt (NMI) button 2-6
- non-regular ports 4-8
- notifications 3-13

## O

- onboard NIC 1-4
- Online Help ix
- Outbreak Prevention Policy 3-13
- overview 1-2

## P

- package contents 2-2—2-3
- packet delivery 5-2
- passwords 4-10
  - default 4-5
  - lost passwords 5-2
- pilot deployment 3-17
  - contingency plan 3-18
  - evaluation 3-18
  - site 3-17
- policy enforcement 3-4, 4-10
- port activity 3-13
- port functions 2-11, 4-7
- port indicators
  - copper expansion cards 2-13
  - onboard ports 2-12
- ports 2-10
  - default state 2-11
  - expansion card 2-12
- power button 2-5
- power cord 2-3
- power supply 1-4

- power-on indicator 2-5
- preconfiguration 4-1
  - network verification 4-2
  - performing 4-3
  - preparations 4-2
  - troubleshooting 5-1
  - understanding 4-3
- Preconfiguration console 1-3, 4-3
  - access issues 5-2
  - login 4-4
  - password 4-5
  - remote access 4-3, 5-2
  - saving changes 4-10
  - timeout 4-5
- preface vii
- printed documents 2-4
- processor 1-4
- Product Information Guide 2-4
- program rescue 3-13
- PuTTY 4-3

## Q

- Quick Start Guide ix, 2-3—2-4

## R

- rack cabinet 2-14
- rack kit 2-3, 2-14
- RAS server 3-6
- Readme ix, 2-3
- REG 2-11
- regular port 1-3, 2-11
- remote access service 3-5
- remote clients 3-5
- remote detection 3-13
- remote endpoints 3-5

## S

- safety instructions 2-14
- Security Appliance License Agreement 2-3—2-4



- serial connector 2-9
- server adapter 1-4, 2-11—2-13
- Silicom 1-4, 2-11—2-12
- single-switch VLAN 3-10, 3-12
- specifications 1-4
- SSH client 4-3
- standard configuration 2-10
- static IP address 4-7
- syslog 2-3

## **T**

- TFTP tool 2-3
- Third-party License Attributions 2-3
- threat mitigation 3-13
- troubleshooting 5-1

## **U**

- unpacking 2-14
- update source 3-14
- updates 4-10
- USB connectors 2-6, 2-9
- USB flash drive 2-3, 5-2
- user authentication 3-13

## **V**

- VGA 4-2
- video connector 2-6, 2-9
- VLAN 3-12
- VPN 3-5
- VPN tunnel 3-7

## **W**

- web console 1-3
- web servers 3-9
- Windows DHCPv6 3-13