TREND MICRO™
Network VirusWall™ Enforcer 1200 Quick Start Guide

Trend Micro™ Network VirusWall™ Enforcer 1200 (NVWE) controls access to the corporate network to ensure that all devices-managed or unmanaged, local or remote-comply with corporate security policies before they connect. It prevents security risks from entering the network by scanning devices for the most up-to-date security software and critical Microsoft patches.

Use this *Quick Start Guide* to get Network VirusWall Enforcer 1200 up and running on your network. To obtain more information on product features and configure more advanced settings, see the following documentation:

• Getting Started Guide — Helps you plan for deployment and perform initial tasks.

• Administrator's Guide — Helps you configure all product features.

• Online help — Helps you configure all features and is accessible from the Web console. To access the online help, open the Web console and click the help icon ❓.

• Readme — Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

Note: Trend Micro recommends checking the corresponding link from the Update Center (http://www.trendmicro.com/download) for updates to the *Upgrade Guide, Quick Start Guide, Getting Started Guide, Administrator's Guide, Readme, and program file.*

① Open and inspect the Network VirusWall Enforcer 1200 carton

Please verify that the carton contains each of the following items:

| Network VirusWall 1200 | Power Cord | Ethernet Cable (RJ-45 Crossover) |
| Console Cable (RS-232) | Rack Ears | Document Set |

Contact Information
• Local offices: http://www.trendmicro.com/en/about/contact/us.htm
• Phone: + 1 (800) 228-5651 or + 1 (408) 257-1500
• Address: Trend Micro, 10101 N. De Anza Blvd, Cupertino, CA - 95014, USA

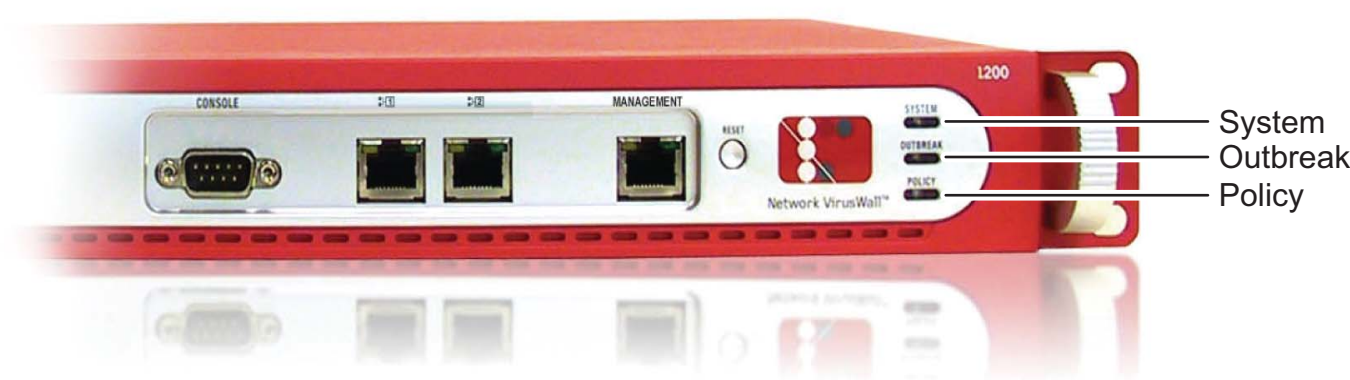### ② Understand Network VirusWall Enforcer 1200

Network VirusWall Enforcer 1200 scans all inbound and outbound traffic.

LCD module and panel — Management/Mirror port

CONSOLE — Port 1 — Port 2 — Reset button — LEDs
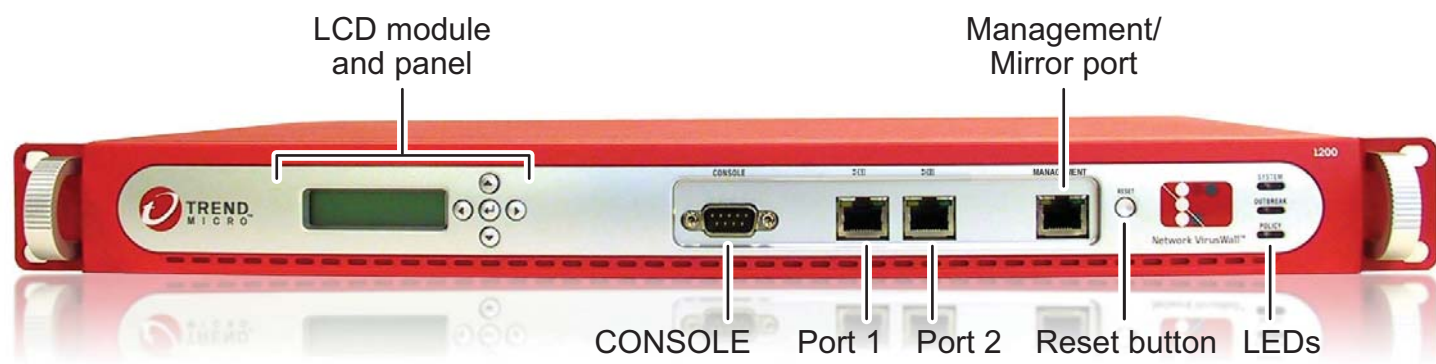
Explanation of front panel items

The front panel of Network VirusWall Enforcer 1200 contains a Liquid Crystal Display (LCD), panel, ports, and LEDs. The following table describes each front panel element.
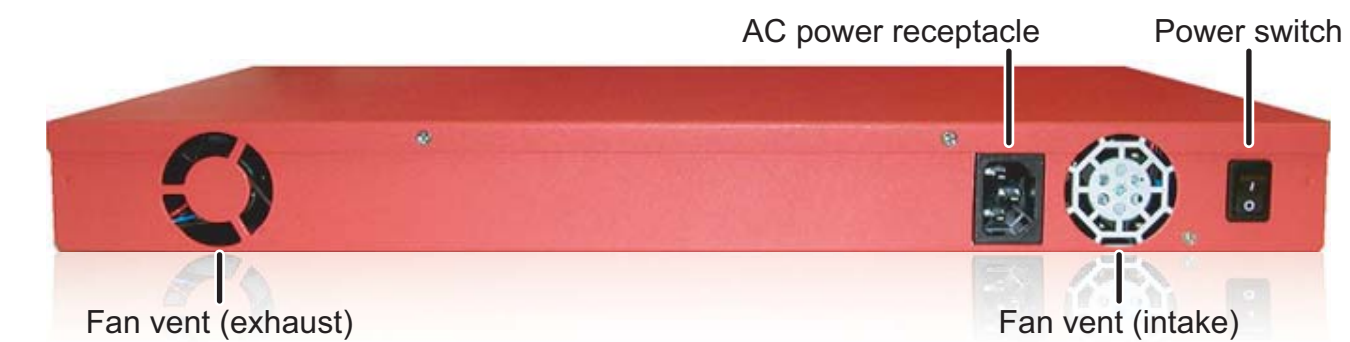
Element	Description
Liquid Crystal Display (LCD)	A 2.6 in x 0.6 in (65mm x 16mm) dot display LCD that is capable of displaying messages in 2 rows of 16 characters each.
Panel	5-button control panel that provides LCD navigation.
RESET Button	Resets the device.
Ports 1,2	The Network VirusWall Enforcer 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 1200 Web console. This port can also be used as a mirror port.
CONSOLE	Connect to this port to access the Network VirusWall Enforcer Preconfiguration console.

System
Outbreak
Policy

Explanation of LED indicators

Network VirusWall Enforcer 1200 has three light emitting diodes (LEDs) that indicate SYSTEM, POLICY, and OUTBREAK status. The following table shows the possible behavior for each LED.

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.
Outbreak	Green - steady	Registered to Control Manager.
	Red - flashing	OPS is enabled.
Policy	Green - flashing	Network Scan, or Policy Enforcement is enabled.
	Off (no color)	No multiple policy scan.

AC power receptacle   Power switch

Fan vent (exhaust)   Fan vent (intake)

Network VirusWall Enforcer 1200 back

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

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.

③ Decide the network configuration

Before proceeding with the Network VirusWall Enforcer 1200 setup, decide how to integrate the device into your network and determine which topology it will support. Position Network VirusWall Enforcer 1200 between layer 2 (L2) or layer 3 (L3) devices to scan all packets entering and leaving that section of the network.

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. Policies are applied based on the trigger criteria that the endpoint matches. Once an endpoint matches the trigger criteria of one policy, only that policy is applied to the endpoint.

Router or Switch
Network VirusWall Enforcer 1200
Router or Switch
Endpoints   Endpoints
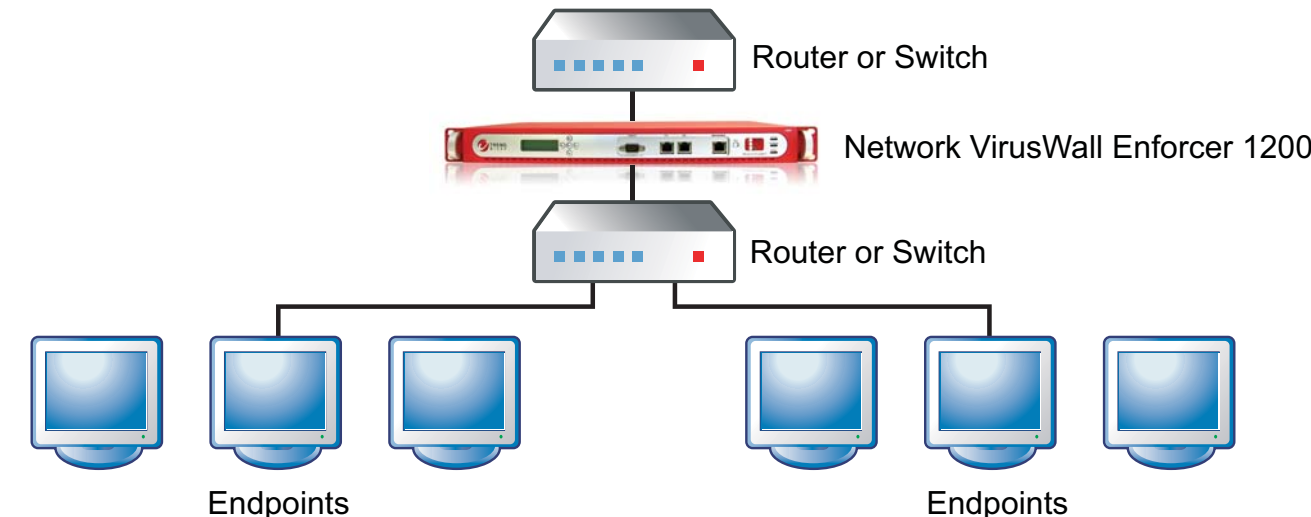
Hardware Setup

Use the chart below to prepare the network values for which Network VirusWall Enforcer 1200 will prompt you.

Value	Your Answer
IP address	
Netmask	
Default gateway	
DNS server 1	
DNS server 2	
VLAN	

To register Network VirusWall Enforcer 1200 to Trend Micro Control Manager, you need to prepare additional Control Manager specific information. Refer to Appendix B in the *Administrator's Guide* for more information about Control Manager and instructions on registering Network VirusWall Enforcer 1200 to Control Manager.

④ Mount the Network VirusWall Enforcer 1200 device

Mount the Network VirusWall Enforcer 1200 device in a standard, 19-inch four-post rack cabinet, or on any stable surface as a freestanding device. Instructions can be found in the *Getting Started Guide*, which is available in print, on the Network VirusWall Enforcer 1200 CD, and from the Trend Micro Update Center.

When mounting the device, be sure to allow at least two inches clearance in all directions for cooling.

⑤ Prepare the Preconfiguration console

The computer you choose for preconfiguration must have HyperTerminal.

To prepare the Preconfiguration console:

1. Connect one end of the included console cable to the CONSOLE port on the front panel of the device and the other end to the serial port (COM1, COM2, or other COM port) on a computer.

2. Open HyperTerminal:
   a. Click **Start > Programs > Accessories > Communications > HyperTerminal**. HyperTerminal prompts you for location information.
   b. Click **Cancel** when prompted for dial-up location information.
   c. Type the information and press **Enter** to enter information in the terminal interface.
   d. On the HyperTerminal window, click **File > Properties**.
   e. Click the **Settings** tab.
   f. Under Backspace key sends, select **Del**.

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

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

6 Log on to the Preconfiguration console

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

To log on to 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 in the *Getting Started Guide* for 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'.

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

   User name: admin
   Password: admin
   Use this login for full access to all preconfiguration features.

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

7 Configure device settings

You can quickly assign Network VirusWall Enforcer 1200 a fixed IP address using the Preconfiguration console. You will need the information you prepared in step 3.

To configure device settings:

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

   ✏️ **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.

3. Type a host name that properly represents the device in the network. Trend Micro recommends a unique descriptive host name to represent and identify the device locally (through the front panel LCD module) or remotely (through the management console). Host names may be up to 30 alphanumeric characters ("A-Z, a-z, 0-9 and hyphens "-" can be used. Spaces are not allowed).

   > **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 device settings, select **Return to main menu** and press **Enter**.

5. Select **Save and log off**. A confirmation message displays.

6. Click **OK**.

You can register Network VirusWall Enforcer 1200 to Trend Micro Control Manager from the Device Settings screen. Refer to the *Administrator's Guide* for more information.

8 Connect Network VirusWall Enforcer 1200 to your test network

After preconfiguration, you must switch off the device before connecting it to the network.

To connect Network VirusWall Enforcer 1200 to your network:

1. Connect one end of a 10/100Mbps Ethernet cable to Port 1 or Port 2 and the other to a segment of your network.

2. Power on the device.

   ✏️ **Note:** Network VirusWall Enforcer 1200 can handle various interface speed (up to 100Mbps) and duplex mode network traffic. See the *Getting Started Guide* for more information.

Management/
Mirror port

Port 1   Port 2
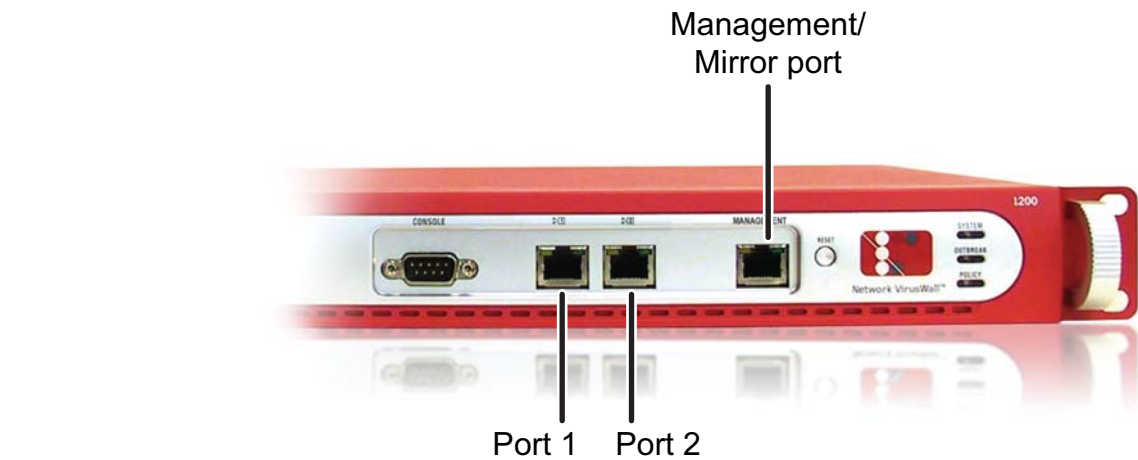
3. Hardware configuration is now complete. To test the hardware setup and complete the configuration, relocate to a computer with access to the device and open a Web browser. Type the IP address of the device to access the Web console.

9 Log on to the Web console and change the default passwords

Network VirusWall Enforcer 1200 ships with two default accounts - admin and poweruser. Both accounts use admin and poweruser, respectively, as their default password. Change the default passwords of these accounts to prevent unauthorized access.

Open the Web console from a desktop or laptop on the network that can access the device (and is running Internet Explorer version 6.0 or later).

To change default passwords:

1. Type the Network VirusWall Enforcer 1200 IP address in your Web browser's address field:

   `http://[IP Address]`
   where `[IP Address]` is the IP you just assigned.

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

   User name: admin
   Password: admin

   TREND MICRO™
   Network VirusWall™ Enforcer 1200
   Please type your user name and password to access the product console.
   Username:
   Password: [Log On]

3. From the main menu, click **Administration > Administrative Accounts**.

4. Click a **User ID**. The Edit Administrative Account screen displays.

5. Type a new password for the account next to **Password**. Repeat this step next to **Password confirm**.

6. Click **Save**.

Change the passwords for each of the two default accounts.

10 Default Policy

Network VirusWall Enforcer 1200 allows you to create multiple policies directed at different types of endpoints and traffic. Network VirusWall Enforcer 1200 follows a first-match rule. **This means that once Network VirusWall Enforcer 1200 matches a policy to an endpoint, the device will no longer search for further matches to the endpoint down the policy list**. So, the device only applies the first policy that matches the endpoint.

Once you have set up Network VirusWall Enforcer 1200, there is one active default sample policy that matches any source and any destination. Adding new policies pushes older policies to a lower priority. So to use the broad settings available in the default sample policy, you must move the default policy to a higher priority. Refer to the *Administrator's Guide* for more information about policy enforcement.

11 Test and finish setting up Network VirusWall Enforcer 1200

Trend Micro recommends that you update the pattern files and test your installation to confirm that it works. Instructions for these and other important tasks are described in the *Getting Started Guide* and *Administrator's Guide*.

---

12 Upgrading Network VirusWall Enforcer 1200

To perform the following procedure you will need the Trend Micro Network VirusWall Enforcer 1200 Solutions CD. To roll back the device after upgrading, perform this process using the `NVW_image_downgrade_2.0.1000.en.us.b` file in place of the boot image file (.B file) and the previous version of the program image in place of the program image (.R file).

To upgrade Network VirusWall Enforcer 1200:

1. Connect to the device using the Console port and Port 1.

2. Specify the IP address of your computer to the same segment as the Network VirusWall Enforcer 1200 device:

   a. Click **Start > Control Panel > Network and Internet Connections > Network Connections**. The **Network Connections** window appears.

   b. Right-click the network connection you will use to connect to the Network VirusWall 1200 device. A pop up menu appears.

   c. Select **Properties**. The **Connection Properties** dialog box appears.

   d. Select **Internet Protocol (TCP/IP)** from the **This connection uses the following items** list. Internet Protocol (TCP/IP) highlights in the list.

   e. Click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.

   f. Select **Use the following IP address** and match the first three octets of the IP address in the **IP address** field to the IP address of the Network VirusWall Enforcer 1200 device.

      For example: If the device IP address is 192.168.252.1, set the IP address for your computer to 192.168.252.XX (where XX represents a number you specify).

   g. Specify the following in the **Subnet mask** field: 255.255.255.0.

   h. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.

   i. Click **Close** to close the **Connection Properties** dialog box.

3. Perform 5 **Prepare the Preconfiguration console** to prepare the Hyper Terminal console to connect to the Network VirusWall Enforcer device

4. Reset the device by pressing the **Reset** button on the front panel of the device.

5. After the device reboots, type `r` in the HyperTerminal console before the Rescue Mode countdown completes.

6. Insert the *Trend Micro Network VirusWall Enforcer 1200 Solutions CD*.

7. Locate and execute the `nvwrescue.exe` file on the Solutions CD. The Trend Micro Network VirusWall Rescue Utility dialog box appears.

8. Click **Browse** and import the device boot image (.B file) from the Solutions CD.

9. Click **Update** in the Trend Micro Network VirusWall Rescue Utility dialog box. The device uploads the boot image and reboots automatically.

10. Click **Finish**. When the device reboots a message appears in the HyperTerminal console prompting you to enter rescue mode.

11. Type `r` in the HyperTerminal console before the Rescue Mode countdown completes.

12. Locate and execute the `nvwrescue.exe` file on the Solutions CD. The Trend Micro Network VirusWall Rescue Utility dialog box appears.

13. Click **Browse** and import the device program image (.R file) from the Solutions CD.

14. Click **Update** in the Trend Micro Network VirusWall Rescue Utility dialog box. The device uploads the program image and reboots automatically.

15. Click **Finish**. When the device reboots a message appears in the HyperTerminal console prompting you to enter rescue mode. The device has successfully been upgraded.

16. Do not enter rescue mode. Wait until the rescue mode countdown elapses. The Preconfiguration console Login screen appears.