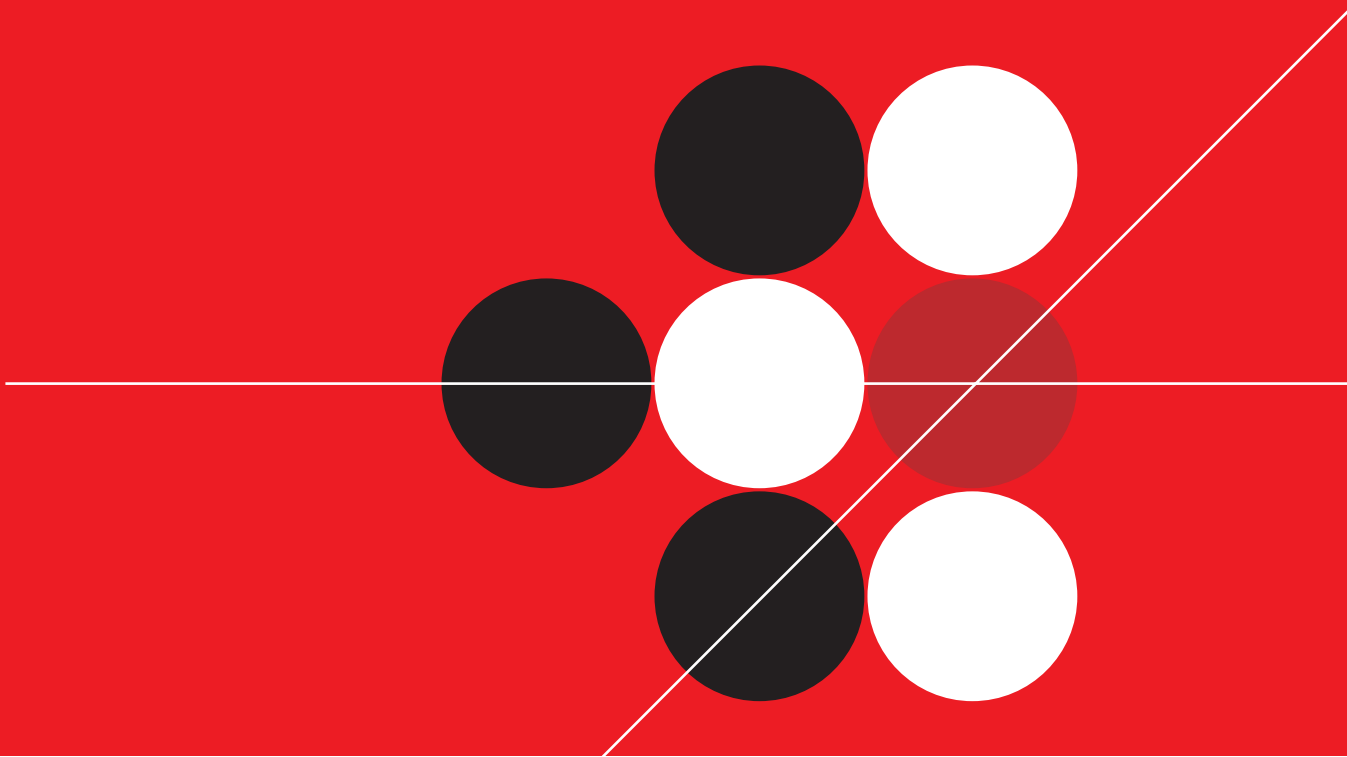
TREND MICRO™
Network VirusWall™ 1200

Getting Started Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

www.trendmicro.com/download

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. NVEM12103/41110

Release Date: November 2004

The Getting Started Guide for Trend Micro Network VirusWall™ 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.

For technical support, please refer to Contacting Technical Support starting on page 5-1 for contact details. Detailed information about how to use specific features within Trend Micro Control Manager are available in the online help file and online Knowledge Base at Trend Micro's Web site. For more detailed installation and configuration instructions, refer to the *Control Manager Getting Started Guide* and the *Network VirusWall User's Guide* located in PDF form on the *Trend Micro Solutions CD for Network VirusWall*.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 1

Introduction

Welcome to the Getting Started Guide for the Trend Micro™ Network VirusWall™ 1200. This book contains basic information about how to install Network VirusWall 1200. This book is intended for first-time users of Trend Micro Control Manager™ and Network VirusWall who want to quickly deploy and configure the product.

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

Understanding the Protected Network

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

Network VirusWall creates a Protected Network to accomplish these tasks:

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

What is Trend Micro Control Manager?

Trend Micro™ Control Manager™ is a central management console that manages Trend Micro products and services, antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager provides central management for one or more Network VirusWall devices on your network and gives you the tools to configure and enforce antivirus policies for an entire organization. This enables you to react quickly to network virus emergencies from nearly anywhere using the management console.

The Control Manager management console enables you to perform the following administrative tasks on Network VirusWall:

- Analyze your network's protection against viruses
- Update your protection
- Enforce antivirus policies
- Monitor the network for suspicious activity
- Monitor Network VirusWall devices via SNMP
- Utilize Control Manager services

Deployment Overview

Network VirusWall deployment consists of the following steps:

1. Installing Trend Micro Control Manager on a server on the **network**. A brief overview of Control Manager installation and system requirements appears in Chapter 2, *Installing Trend Micro Control Manager*.
2. Preconfiguring Network VirusWall using a **console connection**. Preconfiguration configures Network VirusWall for your network and allows Network VirusWall to establish communication with Control Manager upon connection to the network, and is described in Chapter 3, *Preconfiguring Network VirusWall*.
3. Connecting Network VirusWall to the **network**. When you connect Network VirusWall to the network, it establishes communication with the Control Manager server. Instructions on how to connect Network VirusWall and view

Network VirusWall devices in the Control Manager management console appear in Chapter 4, *Deploying Network VirusWall 1200*.

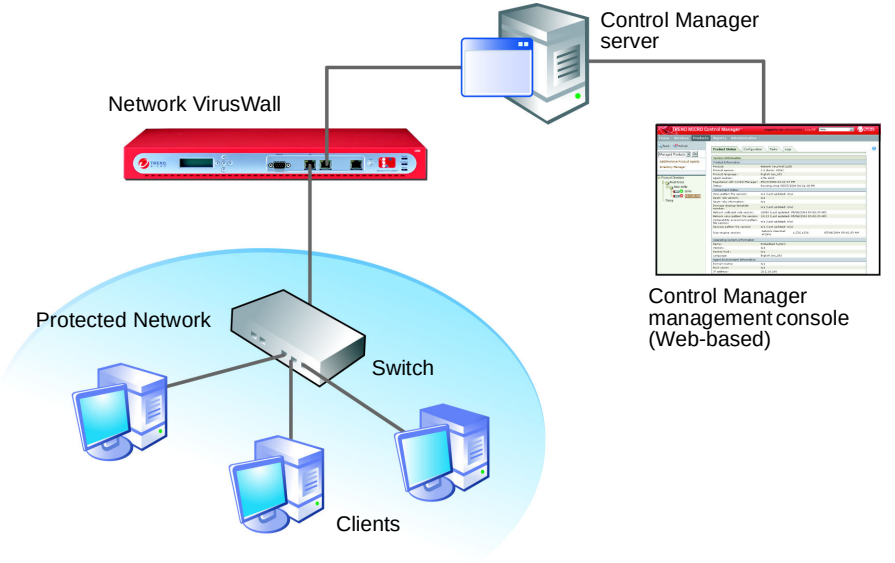


FIGURE 1-1. Network VirusWall and Control Manager after deployment

Package Contents

The Network VirusWall 1200 package includes the following items:

- Network VirusWall 1200 device
- Power cord
- Ethernet Cable (RJ-45 crossover cable)
- Console Cable (RS-232)
- Rack Ears
- Document set, including the following items:
  - This *Trend Micro Network VirusWall 1200 Getting Started Guide*

- The *Trend Micro Solutions CD for Network VirusWall 1200*
- Safety sheet
- Warranty card

FIGURE 1-2. The Network VirusWall package contents

Chapter 2

Installing Trend Micro Control Manager

This chapter guides you through installing the Control Manager server. In addition to listing the system requirements for the Control Manager server, it also contains instructions on how to register and activate your software.

This chapter contains the following topics:

System Requirements

The following table lists the minimum system requirements for a Control Manager server.

Specifications	Minimum Requirements
CPU	Intel Pentium™ III Processor 450MHz or higher
Memory	256MB RAM
Disk space	300MB for Control Manager Standard Version 300MB for MSDE 2000 (Optional)
Operating system	Microsoft™ Windows™ Server 2003 Standard / Enterprise Edition, Microsoft Windows 2000 Server / Advanced Server with Service Pack 3, Microsoft Windows NT 4 with Service Pack 6a
Web server	Microsoft Internet Information Server (IIS) 4.0 or higher
Database	Microsoft SQL Server Desktop Engine (MSDE) 1.0 / 2000 (2000 + SP3 is recommended) Microsoft SQL Server 7.0 Microsoft SQL Server 2000 (2000 + SP3 is recommended)
Others	SQL ODBC driver 3.7 or higher Windows Installer (included in Control Manager package)
Management console	Browser- Microsoft Internet Explorer 5.5 with SP2 or higher Java VM- Microsoft Version 5.0.0.3805 or higher

TABLE 2-1. Control Manager server hardware and software system requirements

Note: For recommended system requirements and sizing recommendations, refer to the *Trend Micro Control Manager Getting Started Guide*, available in Portable Document Format (PDF) on the *Trend Micro Solutions CD for Network VirusWall 1200* included in the Network VirusWall package.

Installing a Control Manager Server

You need the following information for the installation:

- Target server address and port information
- Control Manager registration key

To install a Control Manager server:

Step 1: Register and activate the product and services

1. Insert the *Trend Micro Solutions CD for Network VirusWall 1200*. The setup program starts.
2. Click **Trend Micro Control Manager** and click **Install**. The Control Manager installer starts.
3. Follow the on-screen instructions to obtain an activation code from the Trend Micro Registration Web site and activate purchased services.

Step 2: Specify Control Manager server file location and communications settings

1. From the **Product Activation (Step 2)** screen, click **Next**. Specify a location for Control Manager files. The default location is `C:\Program Files\Trend Micro`.
2. Click **Next**. Select a security level and network address - this is the network address you use during Network VirusWall preconfiguration.

Note: If you use the host name or FQDN to identify your server, make sure that this name can be resolved on Network VirusWall 1200, otherwise Network VirusWall 1200 cannot communicate with the Control Manager server.

---

3. Click **Next**. The **Choose Destination Location** screen appears.
4. Specify the location of the Control Manager backup and authentication files. Click **Browse** to specify an alternate location.
5. Click **Next**. The **Specify Web Server Information** screen appears.
6. From the **IP address** list, select the IP address or FQDN/host name you want to use for the Control Manager management console.

Step 3: Choose and configure database information

1. Click **Next**. The **Setup Control Manager Database** screen appears.

2. Select a database to use with Control Manager.
   - **Install Microsoft Data Engine (MSDE)**

   Note: The Microsoft SQL Server Desktop Engine (MSDE) is suitable only for a small number of connections. An SQL server is preferable for large Control Manager networks.

   - **SQL Server** - the setup program automatically selects this option if an SQL server is detected on your server. Provide the following information:
     - **SQL Server (\Instance)**
     - **SQL Server Authentication**

WARNING! *For security reasons, do not use an SQL database that is not password protected.*

3. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is "db_ControlManager".
4. Click **Next** to create the required database.

Step 4: ASet up root account and configure proxy server

1. Click **Next**. The **Create Root Account** screen appears:

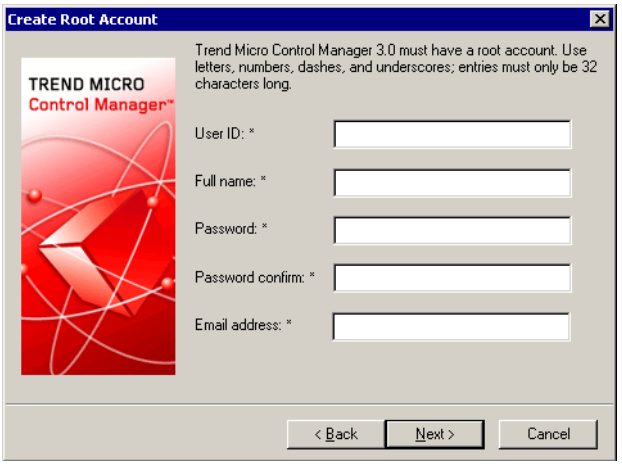


FIGURE 2-1. The Control Manager Create Root Account screen.

2. Provide the following account information:
   - User ID - **This is the Power User ID you use during Network VirusWall preconfiguration** (see the procedure *To configure Network VirusWall device settings:* on page 3-5.)
   - Full Name
   - Password
   - Password confirmation
   - Email address
3. Click **Next**.

   If you use a proxy server connect to the Internet, select the **Enable proxy server** check box, and then set the following:
   - Proxy server- type the FQDN, IP address, or NetBIOS name of the server
   - Port- type the proxy port number
   - Proxy type- click the appropriate proxy type: HTTP or SOCKS
   - User name
   - Password

4. Click **Next**. The system verifies the proxy settings you entered. The proxy configuration screen for Trend VCS agents appears. If you are using legacy versions of Control Manager, refer to the *Trend Micro Control Manager Getting Started Guide* located on the *Trend Micro Solutions CD for Network VirusWall*.

Step 5: Configure notification settings

1. Click **Next**. The **Notification Settings** screen appears.
2. Configure the settings used for the Control Manager notification functions.
3. Click **Next**. The **Specify Message Routing Path** screen appears.
4. Define the routes for incoming and outgoing messages or requests. These settings allow you to adapt Control Manager to your company's existing security systems. Select the appropriate route.

Note: Message routing settings are only set during installation. Proxy configurations made here are not related to the proxy settings used for Internet connectivity–though the same proxy settings are used by default.

Source of incoming messages:

- **Direct from registered agents**- Control Manager can directly receive incoming messages.
- **Proxy server**- use a proxy server when receiving messages.
- **IP port forwarding**- this feature configures Control Manager to work with the IP port forwarding function of your company's firewall. Provide the firewall server's FQDN, IP address or NetBIOS name, and then type the port number that Control Manager opened for communication.

Route for outgoing messages

- **Direct to registered agents** - Control Manager sends outgoing messages directly to Network VirusWall.
- **Proxy server** - Control Manager sends outgoing messages via a proxy server.

5. Click **Next**. Specify the Start menu program folder that will contain the Control Manager shortcut. The default is **Trend Micro Control Manager**. Click **Next**.
6. Click **Finish** to complete the installation.

Register and Activate Control Manager

After you have successfully installed Control Manager, please check the license status and expiration date on the management console, click **Administration** > **Registration** > **License Information**. If the status is not "Activated" or is expired, obtain an Activation Code and activate your software (on the Web console, click **Administration** > **Registration** > **License Information** > **Activate the product**). If you experience issues with your Activation Code, please contact technical support (see *Contacting Technical Support* on page 5-1 for more information).

Download the Latest Components

After installation, download the latest components (Pattern files, Cleanup templates, Engine updates) from the Trend Micro ActiveUpdate server to help maintain the highest security protection (on the management console, click **Administration** > **Update Manager > Manual Download)**. If a proxy server exists between a Control Manager server and the Internet, configure the proxy server settings (on the management console, click **Administration** > **System Settings**).

Chapter 3

Preconfiguring Network VirusWall

This chapter explains how to perform preconfiguration, which is necessary before deploying Network VirusWall to the network. Preconfiguration allows you to modify basic Network VirusWall default settings and perform network configuration. Preconfiguration also commands the Network VirusWall device to register itself with the Control Manager server upon connecting to the network.

Hardware and Connections

This section explains the Network VirusWall front and back panel ports, connections, and LEDs. It also provides step-by-step information on connecting the device to your network.

Network VirusWall 1200 Front Panel

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

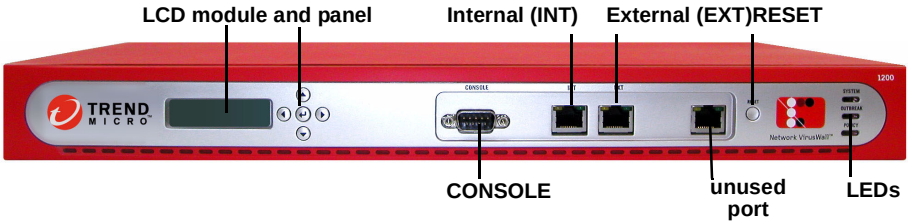


FIGURE 3-1. Front panel

Network VirusWall 1200 Back Panel

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

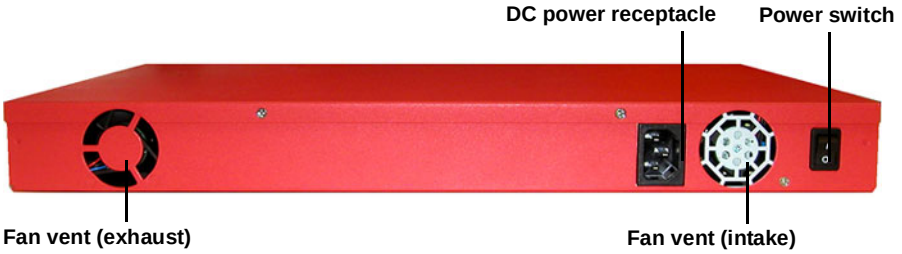


FIGURE 3-2. Back panel

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

Connecting the Hardware

Before you preconfigure Network VirusWall, designate a computer for preconfiguration. Network VirusWall requires the following connections for preconfiguration:

- A console connection to the computer you use for preconfiguration
- A network connection to the network running Control Manager

Note: Both connections may be made to the same computer.

Preconfiguring with the Terminal Interface

With the terminal interface, you can configure all Network VirusWall preconfiguration settings. If you do not have access to a computer with terminal communications software, use the Network VirusWall LCD module panel to perform preconfiguration (refer to the *Trend Micro Network VirusWall 1200 User's Guide* located on the *Trend Micro Solutions CD for Network VirusWall* for instructions on using the LCD module panel).

Note: Changes to Network VirusWall preconfiguration settings will not take effect until you log off the terminal interface.

Logging on to the Terminal Interface

Use HyperTerminal to access the terminal interface. To open HyperTerminal, click **Start > Programs > Accessories > Communications > HyperTerminal**.

HyperTerminal prompts you for location information. Click **Cancel** when prompted for dial-up location information. To enter information in the terminal interface, type the information and press **ENTER**.

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

To log on to the terminal interface:

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

   Configure the properties as follows:

   - **Bits per second:** 115200
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop bits:** 1
   - **Flow control:** None
3. Power on the device to the on position and wait for a welcome message to appear on the LCD module (typically 1-2 minutes).
4. Press **Enter** when the terminal interface displays "`Network VirusWall 1200 Preconfiguration, Press <ENTER> to continue...`"
5. After connection, the terminal screen appears blank. Press **Enter**. The **User Name** login prompt displays.
6. Type the default administrator user name and its corresponding password:

   user name: admin; **password**: admin

   Use this login for full access to all Network VirusWall preconfiguration features.
7. After logging on, the **Main Menu** appears.

Changing the User Password

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

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

1. On the Network VirusWall console session **Main Menu**, type `1` to select **User Accounts**. The user name and its corresponding permissions appears.
2. Type `1` to select **Change Password**.
3. Type the number corresponding to the user password to change.
4. Type both the current and new passwords. Passwords must be between 5 and 12 alphanumeric characters in length (spaces are not allowed).

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

1. On the Network VirusWall console session **Main Menu**, type `1` to select **User Accounts**. The user name and its corresponding permissions appears.
2. Type `1` to select **Change Password**.
3. Type the number corresponding to the user password to change.
4. At the **New Password** prompt, type new password and press `<ENTER>`. If the entered password is valid, a **Re-type new password** prompt appears. Passwords must be between 5 and 12 alphanumeric characters in length (spaces are not allowed).
5. Retype the new password and press `<ENTER>`. If the two typed passwords match, Network VirusWall accepts the new password and a **Press `ENTER` to continue...** prompt appears. If they don't match, Network VirusWall prompts you to retype the new password.

Configuring Device Settings

After changing the password, use the **Device Settings** menu to configure the Network VirusWall host name, Network VirusWall network settings, and Control Manager settings.

To configure Network VirusWall device settings:

1. On the Network VirusWall console session **Main Menu**, type `2` to select **Device Settings**. The default Network VirusWall settings and Control Manager settings appear.
2. Type `1` to change the Network VirusWall host name.

3. Type a host name that represents the Network VirusWall device on the network and on the Control Manager management console. Host names may be up to 63 alphanumeric characters (spaces not allowed).

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

---

4. Press **Enter**, the console returns to the **Device Settings** menu.
5. Type `2` to change the Network VirusWall network settings. A prompt displays asking you if you want to use a dynamic IP setting.
6. Type `Y` to have a DHCP server on your network determine the Network VirusWall IP address, netmask, gateway address, and DNS server addresses.

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

Tip: Trend Micro recommends assigning a static IP address to Network VirusWall. If the IP address changes often, communication issues may arise between the Control Manager server and Network VirusWall depending on your network topology, architecture, VLAN settings, and so on.

---

7. After specifying the network settings, press **Enter**. The console returns to the **Device Settings** menu.
8. Type `3` to configure the Control Manager settings.
9. Type `N` when prompted to manually import the Control Manager public key. Network VirusWall automatically downloads the public key when it registers with Control Manager. The public key ensures secure communication between Network VirusWall and Control Manager.
10. Type the Control Manager IP address or host name and the power user name.

Note: Set the Control Manager IP address, host name, and power user name during Control Manager installation. Use a host name if the Control Manager server obtains an IP address from a DHCP server. Test the connection to the Control Manager server by using the command ping {hostname} from the command prompt, where {hostname} is the Control Manager server domain name.

---

11. Press `0` to return to the **Main Menu**, and press `0` again to log off Network VirusWall

---

Note: If your network is configured to use one or more VLANs, refer to the instructions on configuring VLAN settings in the *Trend Micro Network VirusWall 1200 User's Guide* located on the *Trend Micro Solutions CD for Network VirusWall.*

---

12. Log on to the Network VirusWall console again using the administrator name and password. Trend Micro recommends viewing system logs to see the progress of Control Manager registration.
13. Type 7 in the **Main Menu** to select **System Tasks**. The **System Tasks** menu appears.
14. Type 1 to select **View System Logs**. System logs appear showing the following information:
    - Date and time of log entry
    - Log entry

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

---

15. Press **Enter** to stop the log report.
16. At the prompt, type `Y` to return to the main menu.

You are now ready to install Network VirusWall on the network.

Restoring Default Settings

If problems arise during preconfiguration, use the **Restore Default Settings** option to re-initialize Network VirusWall, thus restoring settings to the factory defaults.

WARNING! *Restoring default settings loses all preconfigured settings that are different from the factory defaults. If you wish to preserve settings for later use, see Importing and Exporting Configuration Settings on page 3-8.*

To restore default settings:

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

Importing and Exporting Configuration Settings

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

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

To import the configuration file:

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

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

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

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


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

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

To import the Configuration File using HyperTerminal:

    1. Click Transfer > Send File.

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

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

FIGURE 3-3. Importing the Network VirusWall configuration file

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

To import the configuration file using HyperTerminal:

1. Click **Transfer/Send File**. The **Send File** window appears.
2. Click **Browse** to select the configuration file that you want to import.
3. Under **Protocol**, select **Kermit** protocol.
4. Click **Send** to start importing the configuration file.

To export the configuration file:

1. Access the Network VirusWall 1200 terminal interface (see *Preconfiguring with the Terminal Interface* on page 3-3).
2. Type 7 in the main menu to select the **System Tasks** menu.

3. Type 3 to export the configuration file. A confirmation message appears.

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

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


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

To export the configuration file using HyperTerminal:

    1. Click Transfer > Receive File.

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

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

FIGURE 3-4. Exporting the Network VirusWall configuration file

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

To save the configuration file using HyperTerminal:

1. Click **Transfer/Receive File**. The **Receive File** window appears
2. Click **Browse** to select the folder where the configuration file will be saved.
3. Under **Protocol**, select **Kermit** protocol.
4. Click **Receive** to start exporting the configuration file.

Resetting Network VirusWall

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

- Press the **RESET** button on the front of the device.
- Use the terminal interface

To reset Network VirusWall settings via the terminal inteface:

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

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

Logging off the Terminal Interface

Log off the terminal interface after finishing preconfiguration.

To log off:

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

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

3. Save the settings when prompted on the display.

Chapter 4

Deploying Network VirusWall 1200

After installing Control Manager and preconfiguring Network VirusWall, you are ready to deploy Network VirusWall to the network. After deployment, set a schedule for Network VirusWall to regularly update components.

Connecting to the Network

This section explains how to connect Network VirusWall to your network.

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

Be sure to connect Network VirusWall between the segment that you are protecting and the segment you want to protect. Refer to Figure 4-1 for an illustration of a typical deployment. Note that the Control Manager server may be within or outside of the protected network, as long as the host name or IP address can be resolved between the two.

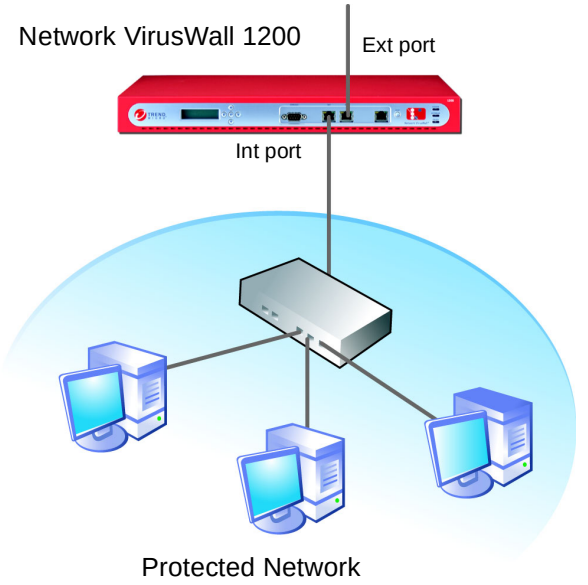


FIGURE 4-1. Network VirusWall typical network deployment

To connect Network VirusWall to your network:

1. Connect one end of a 10/100 Mbps Ethernet cable to the **INT** (Internal) port and the other to the segment of the network that Network VirusWall will protect (the Protected Network).
2. Connect one end of another 10/100 Mbps Ethernet cable to the **EXT** (External) port and the other end to the part of the network that leads to the public network.
3. Connect one end of the power adapter to the **PWR** port and the other end to an electrical outlet.
4. Push the power switch to the **On** position.

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

Accessing Network VirusWall Devices

Once you have connected Network VirusWall to your network, you can access Network VirusWall configuration settings, define product tasks (including scheduled software updates), and view Network VirusWall logs via the Control Manager management console.

The Control Manager management console provides a single console for managing Trend Micro products. See the *Control Manager Getting Started Guide* and online help for detailed information on using the Control Manager management console.

To access Network VirusWall devices:

1. Open the Control Manager management console.
2. In the main menu, click **Products**. On the navigation menu, a directory of managed products appears. The host name of each registered Network VirusWall device appears next to the 

icon.
3. Click the Network VirusWall host name to manage. The **System Information** screen displays.

Deploying Network VirusWall Components

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

To deploy components to Network VirusWall:

1. Access Network VirusWall 1200 from the Control Manager management console.
2. Click the **Tasks** tab.
3. Under **Select task**, select the component to deploy to the selected Network VirusWall 1200 device:
   - **Deploy engines:** deploy the network scan engine
   - **Deploy pattern files/cleanup templates:** deploy the network virus pattern file and network outbreak rule
   - **Deploy program files:** deploy the program file

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

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

Configuring Update Settings

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

To configure an update schedule:

1. Select the **Enable scheduled update** check box.
2. Under **Select update components**, select the components to update:

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

---

3. Under **Configure and update schedule**, specify a schedule to perform the updates:
4. Specify when to perform the scheduled update in the **Start time** lists.
5. Click **Save**.

Chapter 5

Technical Support and Troubleshooting

This chapter provides technical support information and addresses troubleshooting issues that may arise. Refer to the *Trend Micro Network VirusWall User's Guide* located on the *Trend Micro Solutions CD for Network VirusWall 1200* for additional FAQs and troubleshooting.

Contacting Technical Support

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

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

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

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

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

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

Email and Web Resources

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

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

Knowledge Base

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

Troubleshooting

The section covers hardware and configuration troubleshooting issues.

Hardware Issues

	Issue	Corrective Action
1	LEDs do not illuminate	Verify secure power cable and network cable connections. If the error persists, there may be a hardware issue. Contact your vendor.

	Issue	Corrective Action
2	Unable to access the terminal interface	Verify secure console port connections and terminal communications software settings.
3	Unable to change settings with the LCD module panel	To change settings with the LCD module panel, you must first press and hold down the return button  . If an issue with any LCD module buttons persist, the hardware may need to be repaired. Contact your vendor.
4	The **POLICY** LED is illuminated (red steady)	Antivirus policy enforcement and Vulnerability Assessment are not operational due to a memory shortage. Network VirusWall will drop all network packets. Reset Network VirusWall.

Configuration Issues

	Issue	Corrective Action
Issues with Control Manager		
1	Network VirusWall is unable to register with the Control Manager server	Check all network connections and ensure the you have correctly performed preconfiguration. If you changed the Network VirusWall IP address, manually reset the device to allow it to register to the Control Manager server. If Control Manager 3.0 is installed on a server running Windows Server 2003, Network VirusWall may not be able to use the Control Manager time service to synchronize with the server, and will therefore be unable to register to the Control Manager service. **To remedy this issue, choose one of the following:** • Install Active Directory on the Windows Server 2003 server so Network VirusWall can synchronize with the Windows Server 2003 time service. • Disable the Windows Server 2003 time service and enable **Trend Micro Network Time Protocol** so Network VirusWall can synchronize with the Control Manager server time service.

	Issue	Corrective Action
2	Network VirusWall displays a **sync time** error and is unable to register to CM server	A sync time error is displayed when Network VirusWall is unable to synchronize with the Control Manager server. **To remedy this issue, do the following:** 1. On the computer acting as the Control Manager server, open **Services** under the Windows **Administrative Tools**. Click **Start** > **Programs** > **Administrative Tools** > **Services**. 2. Stop the **Windows Time** service. 3. Start the **Trend Micro Network Time Protocol** service. 4. Reset the Network VirusWall device. If the issue persists and Network VirusWall is in a multiple VLAN environment, ensure that the Network VirusWall IP address is bound to the correct VLAN ID.
3	Communication between the Network VirusWall agent and the Control Manager server is not taking place according to the Communicator Scheduler settings	Network VirusWall supports only GMT system time; it is not possible to configure other time settings. The schedule you configure on the Control Manager Communicator Scheduler must take into account any time difference between the time settings on the Control Manager server and GMT time (see the *Control Manager Getting Started Guide* and online help for more information on the Communicator scheduler).
4	The Network VirusWall icon on the Control Manager management console appears as active even when the device is offline	When Network VirusWall 1200 is turned off, or is disconnected from the network, the Control Manager agent for Network VirusWall is not given the opportunity to inform Control Manager that it is going offline. As a result, it relies on Control Manager's status verification mechanism to update its operating status. If the default heartbeat settings are used, Control Manager may require up to 180 minutes to update the status. The actual time would depend on when Network VirusWall sent its last heartbeat. See the *Control Manager Getting Started Guide* and online help for information on changing Heartbeat settings.

	Issue	Corrective Action
5	Network VirusWall is unable to communicate with Vulnerability Assessment (VA)	Ensure that VA is activated (see the *Control Manager Getting Started Guide*). Verify that the Control Manager Web server port is correct. This port was configured during Control Manager installation (see *Installing a Control Manager Server* on page 2-3).
6	Vulnerability Assessment (VA) settings are set to block, but Network VirusWall does not block vulnerable clients	To remedy this issue before performing a Vulnerability Assessment, do the following: 1. Access the Control Manager management console. 2. Click **Services** > **Vulnerability Assessment** > **Global Settings**. 3. Click the check boxes for the machines to block under **Auto Enforcement Settings**. 4. Under **Action Settings for Manual Vulnerability Assessment Tool**, click **Assess by all vulnerability names**. 5. Click **Enable enforcement on machines that are { }**, and select a vulnerability from the list. To remedy this issue after performing a Vulnerability Assessment, do the following: 1. Access the Control Manager management console. 2. Click **Services** > **Vulnerability Assessment** > **Security Summary**. 3. In the **Enforcement Summary** table, click the number of blocked clients under **Machine Count**. 4. Click **Block**.
7	The message "get key error" displays on the LCD module	The LCD module display shows "get key error" until you log on the terminal interface and press <ENTER> or until you press the enter button on the front panel.

	Issue	Corrective Action
8	Blocked clients are not able to access Damage Cleanup Services (DCS) to issue a cleanup request	Ensure that DCS is activated (see the *Control Manager Getting Started Guide*) and enabled.
9	The icon and user name for a Network VirusWall device that was removed from the network still appears on Control Manager	Access the product directory on the Control Manager management console. Remove the Network VirusWall device (see the *Control Manager Getting Started Guide* and online help for information on adding and removing products).

Index