



User Guide

3Com Firewall PC Card with 10/100 LAN

Models 3CRFW102 and 3CRFW103

<http://www.3com.com/>
<http://www.3com.com/productreg>

Published August 2002
User guide version 2.0

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145 ■ U.S.A.

Copyright © 2002 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this user guide.

Portions of this documentation are reproduced in whole or in part with permission from (as appropriate).

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, DynamicAccess, EtherCD, EtherLink and EtherLink II are registered trademarks and the 3Com logo is a trademark of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

All other company and product names may be trademarks of the respective companies with which they are associated.

CONTENTS

CONTENTS

INSTALLING THE PC CARD AND DRIVERS

3Com Firewall PC Card Installation CD Contents	1
3Com Firewall PC Card Models	1
Connecting to the Network	2
Setup for Windows XP, 2000, or 98SE	3
Setup for Windows NT4.0	4
PC Card LEDs	8
Uninstalling the Card--All Operating Systems	8

INSTALLING THE FIREWALL CLIENT

Architecture of Embedded Firewalls	11
Firewall PC Card	12

ADDITIONAL PC CARD FEATURES

Firewall Filtering	15
Advanced Security Processor	15
Data Encryption	15
Windows 2000 and Windows XP Offload Features	15
Hot Swapping	16
Offline Diagnostics	16

ADDITIONAL 3COM SOFTWARE

3Com Mobile Connection Manager	17
3Com Diagnostics	17
3Com Connection Assistant	21
3Com Launcher	22

DATA ENCRYPTION OFFLOAD

About Data Encryption	23
-----------------------	----

TECHNICAL SUPPORT

Online Technical Services	25
Support from Your Network Supplier	26
Support from 3Com	27
Returning Products for Repair	27

CONFIGURING IPSEC

Configuring IPsec in Windows 2000 and Windows XP	29
Example: Creating a Security Policy	29

REGULATORY INFORMATION

1

INSTALLING THE PC CARD AND DRIVERS

3Com Firewall PC Card Installation CD Contents

The Installation CD contains instructions for installing the 3Com Firewall PC Card with 10/100 LAN. It also contains options for:

- Viewing or installing the user guide.
- Viewing the readme.txt file.
- Creating installation diskettes from the CD.
- Exploring the contents of the CD.
- Installing additional software such as the 3Com Mobile Connection Manager and the 3Com Connection Assistant.

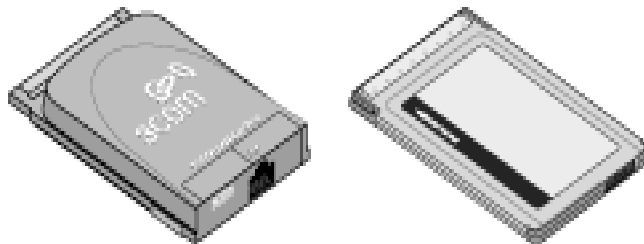


NOTE: *During installation of the 3Com Connection Assistant you will be prompted for contact information. Please complete this personal profile so that if you choose to report an issue, a support engineer can contact you if necessary. If you have an Internet connection, the 3Com Connection Assistant will ensure that your computer always has the updated files and the latest information for your PC card.*

3Com Firewall PC Card Models

The 3Com Firewall PC Card with 10/100 LAN (models 3CRFW102 and 3CRFW103) is part of a unique solution that provides distributed embedded firewall protection. This unique solution consists of the 3Com Embedded Firewall Policy Server and Management Console, and a Firewall Client which resides on the 3Com Firewall PC Card. In addition to providing firewall protection, the 3Com Firewall PC Card with 10/100 LAN connects a notebook computer securely to an Ethernet or Fast Ethernet network.

The 3Com Firewall PC Card models are shown below.



The 3CRFW103 Type III and the 3CRFW102 Type II

Connecting to the Network

The 3Com Firewall PC Card with 10/100 LAN model 3CRFW102 is a Type II PC card and the 3Com Firewall PC Card with 10/100 LAN model 3CRFW103 is a Type III PC card. Follow the instructions for your card to connect it to the network.



NOTE: *Your computer must have a CardBus PC Card slot for you to use the 3Com Firewall PC Card.*

3CRFW103 Type III PC Card

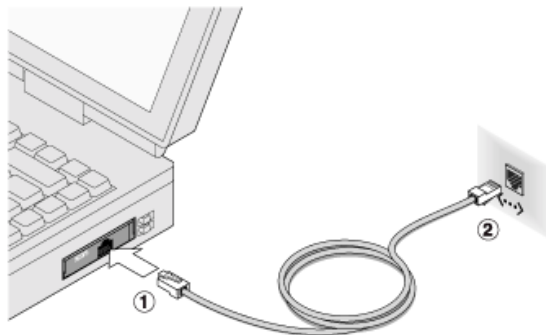
Follow these steps to connect your 3CRFW103 Firewall PC Card.

- 1 Insert the PC Card into the PC Card slot. Slide it in until it is firmly seated.



Do not force the PC Card into the slot or you may bend the pins inside the slot.

- 2 Connect the network cable to the 3CRFW103 PC Card (1).
- 3 Connect the network cable to the network port (2).



3CRFW102 Type II PC Card

Follow these steps to connect your 3CRFW102 Firewall PC Card.

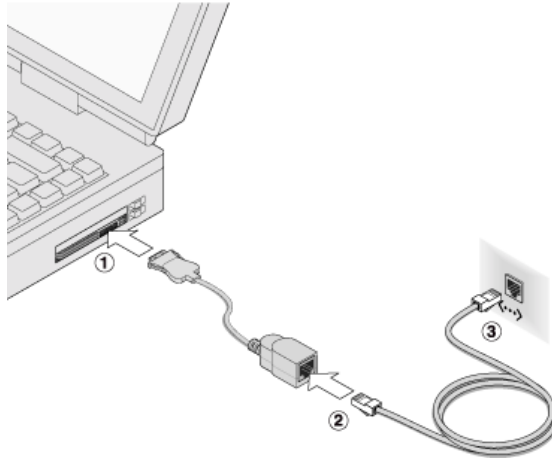
- 1 Insert the PC Card into the PC Card slot. Slide it in until it is firmly seated.



Do not force the PC Card into the slot or you may bend the pins inside the slot.

- 2 Connect the PC Card cable to the 3CRFW102 PC Card (1).
- 3 Connect the PC Card cable to the network cable (2).

- 4 Connect the network cable to the network port (3).



Setup for Windows XP, 2000, or 98 SE

Follow these steps to setup your Firewall PC Card for Windows XP, 2000, and 98 SE.

- 1 With the computer on and Windows running, insert the *Installation CD* into the CD-ROM drive. The auto-start feature starts the installation.
If auto-start is disabled on your computer, or if auto-start is enabled and nothing happens within five seconds, click *Start>Run* and type *d:\setup.exe* (where d: is your CD-ROM drive).
- 2 Select *Install PC Card Software* from the menu.
- 3 Make sure the Firewall PC Card is inserted into the PC Card slot. You are prompted to "Add new Hardware." Respond to the prompts to add the new hardware.
- 4 You may be prompted for the location of drivers on the *Installation CD*. If so, use D:\, where D:\ is your CD-ROM drive.
- 5 During the installation process, you may receive prompts for your Windows operating system installation CD. Insert the operating system installation CD and indicate the correct path.
- 6 Your computer goes through a brief installation process during which it displays several windows indicating what is currently installing. *This takes several minutes.*

Confirming Installation for Windows XP, 2000, or 98 SE

Follow these steps to confirm installation for your Firewall PC Card for Windows XP, 2000, and 98 SE.

- 1 Right-click the *My Computer* icon, and then click *Properties*.
- 2 Select the Hardware tab (Windows 2000), and click *Device Manager*.
- 3 Double-click *Network Adapters* and make sure *3Com 3CRFW10_ PC Card with 10/100 LAN* appears.

If a red X or a yellow exclamation point (!) appears by the name of the network card, the installation was not successful. See "Troubleshooting Windows XP, 2000, and 98 SE Installations" for troubleshooting help.

Troubleshooting Windows XP, 2000, and 98 SE Installations

Symptom	Solution
Basic troubleshooting, applicable for all problem situations.	<p>Inspect all cables and connections.</p> <p>Check whether your PC Card is fully inserted into the slot.</p> <p>Verify you have the latest BIOS for your system. If not, check the Web site for your computer and follow the BIOS upgrade instructions.</p> <p>Check for multiple installations of the PC Card.</p> <p>Check whether your system's CardBus Controller is installed and running properly: go to <i>My Computer/Control Panel/System/Hardware/Device Manager/PCMCIA</i>. Verify the controller is present and shows no errors.</p> <p>If you see a red X, enable the PC Card by checking the appropriate box under Properties.</p> <p>If you see a yellow exclamation mark, click the icon to determine the conflict. Verify system resources are adequate. Free system resources (i.e. disable the infrared port), remove and reinstall the PC card.</p>
The LAN device is not functional. LED on the connector or PC Card is off or mismatches the real network speed.	<p>Use <i>My Computer/Control Panel/System/Hardware/Device Manager/Network Adapters</i> to inspect the status of your PC Card.</p> <p>If you see a red X, enable the PC Card by checking the appropriate box under Properties.</p> <p>If you see a yellow exclamation mark, click the icon to see what the conflict is. Verify there are adequate system resources. Free system resources (for example, disable the infrared port), remove and reinstall the PC Card.</p>
Losing network connection after disconnecting or changing the media speed.	Use specific frame types such as 802.2 or 802.3 (permanent solution). Restart after disconnecting and reconnecting the cable in NetWare networks (temporary solution). This situation can occur when using NetWare servers and IPX/SPX protocol. It happens when the frame type is selected automatically.
At installation, Update Device Driver window does not appear.	<p>The PC Card may have already been installed.</p> <p>The PC Card may have been installed as "Other Devices" because of a previous faulty installation. Uninstall and reinstall the network card.</p> <p>PCMCIA may not be enabled on your system. Refer to your Windows operating system's help for instructions for enabling PCMCIA.</p>
Other connection issues.	Run the 3Com Connection Assistant <i>Start/Programs/3Com NIC Utilities/3Com Connection Assistant</i> to check any other issues. Choose <i>Options</i> from "Self Service" or "Assisted Service".

Setup for Windows NT 4.0

Before You Begin Installation, the Windows NT setup procedure you use depends on whether networking has already been installed on your notebook.



Note: Installing the Firewall PC Card in Windows NT requires either Softex version 2.79 or later or SystemSoft version 5.20.03 or later.

Before setting up the PC Card, you need to know:

- Your network file server name, network account user name, and password.

- The protocol used in the Microsoft Windows network (NWLink IPX/SPX compatible transport, TCP/IP protocol, NetBEUI protocol).
- The name of the NT server domain or workgroup to which you belong.
- Your IP address (unless you are using DHCP).

Setup with No Networking Installed

If no networking is installed, follow these steps:

- 1 Turn your notebook computer on.
- 2 Install your Card and Socket Services (i.e. Softex or SystemSoft).
- 3 Copy i386 directory from Windows NT CD to your hard drive.
- 4 In **SystemSoft** you will be prompted to configure the PC card when it is inserted. Click *Correct*.

In **Softex** you will be prompted to configure the PC card when it is inserted. Select "Manually install the driver for this card".
When the Select OEM Driver window opens, select "Network Adapter" and click *OK*.
- 5 When the system prompts: "Windows NT Networking is not installed. Do you want to install it now?", click *Yes*. This opens the *Network Setup Wizard*.

If this message does not appear, go to "Windows NT With Networking Installed," and follow the instructions.
- 6 Check *Wired to the network* and click *Next*.
- 7 When the system prompts to have setup start searching for a network adapter, click *Select from List*.
- 8 Click *Have Disk*.
- 9 Insert the *3Com Firewall PC Card with 10/100 LAN Installation CD* in the CD-ROM drive. Type the path to drivers (where D:\ is your CD-ROM drive).
For **SystemSoft**: D:\drivers\syssoft
For **Softex**: D:\drivers\softex
Then click *OK*.
- 10 When the Select OEM Option window opens, select *3Com Firewall PC Card with 10/100 LAN* and click *OK*.

The Network Setup Wizard window appears.
- 11 Click *Next*.
- 12 In the Network Protocols list, place a check mark next to each network protocol required for your site and click *Next*.
- 13 In the Network Services window, place a check mark in the box next to each desired service. Select the default settings.
- 14 Click *Next* to install the selected components.

The message "Windows NT is ready to install networking" appears.
- 15 Click *Next*.

The Windows NT Setup windows asks for the location of the Windows NT installation files.

- 16 Enter the path to the Windows NT installation files (this is the location on the hard drive where the I386 directory was copied from the NT CD) and click *Continue*.
The Setup window appears again.
- 17 In the 3Com Network Interface dialog box, accept the default settings and click *OK*.
The default settings work in most instances. However, you may specify network link settings, auto polarity, and IRQ and I/O values.
- 18 When prompted whether you are using DHCP, click *Yes*, if you are using DHCP, or *No*, if you are not using it.
- 19 When the Protocol window for enabling or disabling protocols opens, click *Next*.
- 20 When Windows NT is ready to start the network, click *Next* to copy the network files.
- 21 Enter your notebook name and workgroup or domain name when prompted.
- 22 When the system displays "Networking has been installed on your notebook," click *Finish*.
- 23 When prompted to restart the notebook, remove the *3Com Firewall PC Card with 10/100 LAN Installation CD* from the CD-ROM drive and click *Yes*.

If you had a Windows service pack installed prior to setting up the PC Card, reinstall it now.



SystemSoft Note: After installation, the card will not be hot-swappable until a Hot-Swap test is performed. Open the CardWizard and select the 3Com Firewall PC Card. Click Wizard. The Wizard information window appears. Click Test to perform the Hot-Swap test and follow the prompts.

Confirming Installation To confirm installation:

- 1 Double-click *My Computer*, double-click *Control Panel*, and then double-click *Network*.
- 2 Select the Adapters tab.
3Com Firewall PC Card with 10/100 LAN appears on the list.

Windows NT with Networking Installed

Follow these steps if networking is installed:

- 1 Make sure Card and Socket Services are installed (i.e. Softex or SystemSoft).
- 2 Turn the notebook on.
- 3 Insert your PC card.
- 4 In **SystemSoft** you will be prompted to configure the PC card when it is inserted. Click *Correct*.

In **Softex** you will be prompted to configure the PC card when it is inserted. Select "Manually install the driver for this card".
When the Select OEM Driver window opens, select "Network Adapter" and click *OK*.

- 5 In the Control Panel, double-click *Network*.
- 6 Open the Adapter tab and click *Add*.
The Select network Adapter window appears.
- 7 If the message "networking not installed" appears, go to "Setup With No Networking Installed" for instructions.
- 8 Click *Have Disk*.
- 9 Insert the *3Com Firewall PC Card with 10/100 LAN Installation CD* in the CD-ROM drive. Type the path to drivers (where D:\ is your CD-ROM drive).
For **SystemSoft**: D:\drivers\syssoft
For **Softex**: D:\drivers\softex
Then click *OK*.
- 10 When the Select OEM Option window opens, select *3Com Firewall PC Card with 10/100 LAN* and click *OK*.
- 11 Wait while the files are copied to your notebook.
- 12 In the Network Settings window, accept the default settings and click *Continue*.
The default settings work in most instances. However, you may specify network link settings, auto polarity, and IRQ and I/O values.
- 13 Click *OK* to save.
- 14 If prompted, enter IP information and click *OK*.
- 15 When prompted whether you are using DHCP, click *Yes*, if you are using DHCP, or *No*, if you are not using it.
- 16 When prompted to restart the notebook, remove the *3Com Firewall PC Card with 10/100 LAN Installation CD* from the CD-ROM drive and click *Yes*.



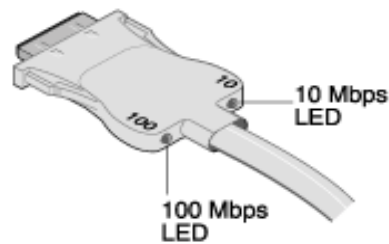
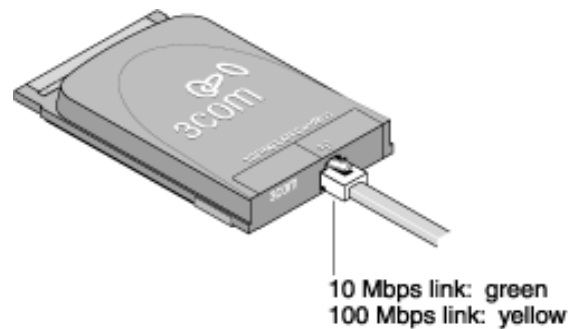
SystemSoft Note: After installation, the card will not be hot-swappable until a Hot-Swap test is performed. Open the CardWizard and select the 3Com Firewall PC Card. Click Wizard. The Wizard information window appears. Click Test to perform the Hot-Swap test and follow the prompts.

Troubleshooting Windows NT 4.0 Installations

Symptom	Solution
Basic troubleshooting, applicable for all problem situations.	<p>Inspect all cables and connections.</p> <p>Check whether your PC Card is fully inserted into the slot.</p> <p>Verify whether you have the latest BIOS for your system. If not, check the Web site for your notebook and follow the BIOS upgrade instructions.</p> <p>The event log lists any problems found during system operation. To check the event log for errors, select <i>Programs/Admin Tools/Event Viewer</i> from the Start menu.</p>
Failure after Suspend/Resume.	<p>This problem usually indicates a power-management problem. Since Windows NT 4.0 does not support power management, we recommend you disable power management in the BIOS. Make sure you have the latest BIOS for your notebook or upgrade your software from Microsoft.</p>
Card not functioning.	<p>Open Windows NT Diagnostics. From the Start menu, select <i>Programs/Admin Tools/Windows NT Diagnostics</i>.</p> <p>Check for resource conflicts and make sure the settings for the PC Card are valid.</p>
Need to force speed and duplex settings.	<p>In most cases, the automatic settings work fine. To force speed and duplex settings to match those of an attached device:</p> <ol style="list-style-type: none"> 1. Open <i>Control Panel/Network</i>. 2. Click the <i>Adapters</i> tab. 3. Select Link Settings and specify the desired values.
Slow or dropped connection on a 10/100 switch.	<p>The switch may be forced to 10Mbps. Open <i>Control Panel/Network</i>. Click the <i>Adapters</i> tab, select <i>Properties</i>, and disable Auto Polarity.</p>
Other connection issues.	<p>Run the 3Com Connection Assistant <i>Start/Programs/3Com NIC Utilities/3Com Connection Assistant</i> to check any other issues. Choose <i>Options</i> from "Self Service" or "Assisted Service".</p>

PC Card LEDs

Before the PC Card and cable LEDs (shown here) can be used for troubleshooting, the PC Card must be connected to the network and the driver must be installed.



LED	On	Off	Flashing
10 Mbps	Good 10BASE-T connection between PC Card and hub	No connection. (Off when 100 LNK LED is on.)	There may be a problem with your physical connection. Check that all cables are connected securely.
100 Mbps	Good 100BASE-TX connection between PC Card and hub	No connection. (Off when 10 LNK LED is on.)	

Uninstalling the Card--All Operating Systems

Sometimes previous or unfinished installations leave problems that affect PC Card operation. If the PC Card installation is unsuccessful for any reason, your best course may be to remove the PC Card and its software and repeat the installation procedures with a fresh installation of the operating system. Possible problems may be indicated if:

- The PC Card is not working.
- Windows NT is not detecting the PC Card.
- The system issues a warning tone at startup.

If you are having any of these problems:

- 1 From the *Control Panel>Network>Adapters*, select *3Com Firewall PC Card with 10/100 LAN* and click *Remove*.
- 2 Remove the PC Card from the PC Card slot.
- 3 Restart the computer and reinstall the PC Card.

This procedure removes the PC Card only.

2

INSTALLING THE FIREWALL CLIENT

The 3Com Firewall PC Card with 10/100 LAN provides secure, trusted connections inside and outside your network. The 3Com Firewall PC Card with 10/100 LAN is part of a unique solution that provides distributed hardware level protection. This solution consists of the 3Com Embedded Firewall Policy Server and Management Console, and a Firewall Card. Together they complement and enhance enterprise perimeter firewalls, antivirus programs and host-based applications. The 3Com Firewall PC Card with 10/100 LAN is hardware-based and is installed at individual computers. The firewall security rules are executed independent of the host operating system, protecting each individual computer. Performing these security processes in the hardware makes this solution extremely tamper resistant.

To protect today's business network, your security system should incorporate the following:

- Comprehensive protection that extends to the end system regardless of how the LAN topology changes.
- Tamper-resistant security that operates independent of the host OS and other security programs.
- Manageable enforcement that allows you to define security through user policies.

Software-based security, such as personal firewalls, interact with and protect a PC's operating system. This dependency on the host makes them inherently susceptible to malicious code and "security holes" found in many well-known operating systems. Once the OS has been compromised, it is easy to disable the host-based security. This compromised host can then be used as a covert launching pad for attacks on other systems across your network.

In contrast, with the 3Com Embedded Firewall Solution, enforcement is handled by the Firewall Client Device, keeping it separate from the host and making it very tamper resistant. Even if a hacker manages to invade a secured host, the Firewall Client Device continues to block attempts to further infiltrate your network.

For more information on the 3Com Embedded Firewall solution, go to www.3com.com/security.

Architecture of Embedded Firewalls

The 3Com Embedded Firewall is a centrally managed solution. Being centrally managed prohibits end users or malicious code from modifying security policies. There are two components required to achieve this level of security and capability: a Policy Server and a Firewall Client Device located in the computer being protected.

The 3Com Embedded Firewall Policy Server and Management Console (sold separately) is used by the security administrator to define and control the security policies that are executed by the server, desktop, and notebook firewalls. This central management console also provides security logging capabilities, giving administrators the ability to view logs and perform troubleshooting.

The 3Com Embedded Firewall Client Devices (available in desktop and server PCI, as well as laptop-based Cardbus) receive security policies from the policy server. This security processor on each of these firewalls examines the traffic passing through the device and blocks traffic that falls outside of the security policy.

Firewall PC Card

The 3Com Embedded Firewall solution applies security policy enforcement capabilities to all traffic transmitted from and received by an individual laptop, desktop, or server.

The Firewall Client Device provides transparent packet filtering in accordance with the rules that are setup by a security administrator. The rules are defined through a centralized management console and are communicated to the firewall client devices via the policy server.

Like traditional perimeter firewalls, the 3Com Embedded Firewall solution is capable of classifying and acting upon packets based on the following criteria:

- Source IP Address
- Source IP Mask
- Source Port
- Destination IP Address
- Destination IP Mask
- Destination Port
- IP Protocol (TCP, UDP, etc.)
- Direction (Inbound, Outbound, both)

Once the traffic has been classified, actions that may be taken on the packet are:

- Allow
- Allow and Audit
- Deny
- Deny and Audit

Optional Control Headers

The 3Com Firewall PC Card includes optional controls for the following:

No Sniffing--Prevents the Firewall Client Device from sniffing traffic addressed to other devices on your network.

No Spoofing--Prevents the Firewall Client Device from sending packets on the network with forged source IP addresses.

Non-IP Traffic--Denies Non-IP Traffic such as IPX or NetBEUI.

Fragmented Packets--Denies fragmented packets.

IP Options--Denies packets with IP options. These packets are usually used for network testing and debugging.

In addition to these features, the Firewall PC Card products are also “location aware”. This allows a security administrator to provide varying levels of security depending on where the notebook computer is located. A strict policy can be implemented while the notebook computer is outside of the perimeter firewall, and a less restrictive one can be in place while the notebook is inside the perimeter.

Enabling the Firewall

Until you enable the firewall functionality of the 3Com Firewall PC Card with 10/100LAN, it will emulate the functions of a standard network interface card. Enabling the firewall functionality requires the 3Com Embedded Firewall Policy Server.

The 3Com Embedded Firewall Policy Server allows you to create a cryptographic binding between the Firewall Client Devices and the Policy Server. This prevents someone from installing a central management console and taking control of your Firewall Client Devices.

When you create a customized installation package, the following cryptographic functions are preformed:

- 1** When the Policy Server is installed, it generates an RSA 1024 Public/Private keypair. The public key is written to the Firewall Client Device flash memory.
- 2** When the Firewall Client Device boots up, it generates a random 3DES session key, encrypts that key with the policy server’s public key, and then sends that information to the policy server.
- 3** The policy server decrypts the message using its private key, and then implements the random 3DES session key as communicated by the Firewall Client Device.
- 4** This cryptographic binding adds to the tamper resistance of the 3Com Embedded Firewall solution. It encrypts the policy distribution traffic between your Policy Server and the Firewall Client Devices. It also locks down your Firewall Client devices so they only accept policies from your specific Policy Server (because of the public/private keypair).

Please see the 3Com Embedded Firewall Policy Server Administration Guide for more information on creating a customized installation package that will enable the firewall functionality on your Firewall PC Card and cryptographically bind the card to your Policy Server.

Important Notes

The 3Com Firewall Client provides state-of-the-art network security and is designed to be tamper resistant. Follow these simple procedures to avoid inadvertently triggering the tamper-resistance feature. Doing so will prevent a time-consuming recovery process.

Procedure 1

Create and retain a policy server recovery diskette.

After installing your first policy server, it is critical to make a copy of the files named "public.key" and "server.keystore" from your installation. Save this data indefinitely in a safe, secure location.

In the unlikely event of a disaster, such as a disk crash on all your policy server machines and a simultaneous loss of all disk backups for these machines, this recovery diskette allows you to "clone" your policy server and regain management control of your network interface cards. A clean installation of the policy server cannot communicate with your Firewall Client network interface cards (which is the intended design, for security reasons).

If you do not create a recovery diskette and you lose all policy server installation data, you will not be able to recover your network interface cards. They will continue to enforce the fallback mode specified in their last EFW policy, indefinitely. These network interface cards must be replaced in order to obtain a different policy.

Procedure 2

If diagnostics are desired, install them before the Firewall Client.

If diagnostics are desired for a network interface card installation, install them first from the 3Com EtherCD before installing the 3Com Firewall Client. Installing them over the Firewall Client may make the card inoperable.

Procedure 3

Do not attempt installation of non-firewall firmware over an Firewall PC Card.

Instruct users and administrators that after installation of the Firewall Client on a card, installing any non-firewall firmware over this Firewall Client installation may render the card inoperable. If you wish to install non-firewall firmware on an Firewall Client network interface card, you must first successfully delete the card from its Firewall Client domain using the Management console, as noted below.

Procedure 4

Use the correct procedure for removing a card from the Firewall Client system.

Always delete a network interface card from the 3Com Firewall Client via the Management Console first, if you intend to remove it from the system and wish to "uninstall" the firewall client on the card. If this step is not taken, moving a Firewall Client card to a non-firewall host, or attempting to install non-firewall firmware over an Firewall Client card, may render it inoperable. The principle here is that only the firewall administrator may make the decision that a network interface card should no longer have an embedded firewall; the end user cannot effectively remove a firewall.

3

ADDITIONAL PC CARD FEATURES

Firewall Filtering

The 3Com Firewall PC Card with 10/100 LAN includes a Firewall Client license. The Firewall Client filters inbound and outbound data according to the policy specified by your security administrator to protect you from network attacks wherever you go.

Advanced Security Processor

The 3Com Firewall PC Card with 10/100 LAN has an on-board security processor that offloads key networking and security tasks from the notebook's central processing unit to the security processor even when running bandwidth-intensive applications such as voice, video, imaging, and Internet and intranet applications.

Data Encryption

The 3Com Firewall PC Card with 10/100 LAN can provide data encryption standard 56-bit (DES) encryption and triple DES 168-bit (3DES) encryption. Encryption processing is handled entirely by the security processor and the encryption chip that resides on the PC Card.

The on-board encryption chip enables true end-to-end network security (IPSec) (see "Configuring IPSec in Windows 2000 and Windows XP") at the data capacity of the connected network cable (wire speed), without sacrificing performance. Until encryption is enabled, the 3Com Firewall PC Card with 10/100 LAN functions as a standard 10/100 CardBus LAN card.

Windows 2000 and Windows XP Offload Features

The 3Com Firewall PC Card with 10/100 LAN supports Windows 2000 and Windows XP IPSec offload features in an IP environment. The offload features are designed to enhance the operating system capabilities by offloading key TCP/IP networking and security tasks from the Windows 2000 operating system:

- IPSec Offload—reduces CPU utilization by allowing the security processor and a crypto chip on the LAN card to perform data encryption operations.
- TCP Segmentation Offload—reduces CPU utilization by allowing the security processor on the LAN card to perform segmentation of TCP packets.



NOTE: *Windows 2000 and Windows XP do not allow IPSec offloads and TCP Segmentation offloads for the same session. Though all offload types may be enabled, TCP Segmentation offloading will not occur during an IPSec session.*

- IP and TCP Checksum Offload—reduces CPU utilization by allowing the security processor on the LAN card to perform the checksum calculation of TCP/IP and UDP/IP packets.
- 802.1P Packet Priority Offload—reduces CPU utilization by allowing the security processor on the LAN card to perform the insertion of the 802.1Q tag header into the packet.

Refer to “Offloading Encryption Processing” for more information about Windows 2000 and Windows XP offloading features.

Hot Swapping

If your computer supports hot swapping, you can add a new 3Com LAN PC Card or remove and replace a 3Com LAN PC Card without turning off power to the computer. Hot swapping lets you expand connections without taking the computer out of service. It makes troubleshooting faster and easier because you do not need to wait for the computer to restart.

Offline Diagnostics

The 3Com Firewall PC Card includes offline diagnostics programs for configuring, testing, and troubleshooting PC Cards. The configuration program within the DOS diagnostics program is used for a notebook running DOS or NetWare. The LAN diagnostics program (3Com NIC Doctor) is a windows-based program used for a PC running Windows XP, Windows 2000, Windows NT 4.0, or Windows 98. This program may also be used to flash upgrade the PC card.

4

ADDITIONAL 3COM SOFTWARE

3Com Mobile Connection Manager

3Com Mobile Connection Manager (MCM) stores the information you need for a connection from different locations, saving you the time and trouble of setting up a new connection each time you move to a new location or dial in to a new location. A mobile configuration contains the correct system settings to reach a specific computer network or dial-up location from your current location. These preferred settings are categorized by and stored in MCM profiles and configurations.

When you want to connect to a specific network, run MCM to examine the list of existing mobile configurations. The name of the last-used configuration is shown in bold. If a mobile configuration has already been created for this location, select it and click *Activate* or *Connect* to start the connection process. If no mobile configuration has been created, MCM lets you create a new one by importing configurations developed by your system administrator, or creating a new configuration.

3Com Diagnostics

The 3Com Firewall PC Card with 10/100 LAN uses two types of network card diagnostics programs: a Windows-based diagnostics program and a DOS-based diagnostics program.



NOTE: *If diagnostics are desired for a network interface card installation, install them first from the 3Com EtherCD before installing the 3Com Firewall Client. Installing them over the Firewall Client may make the card inoperable.*

Before starting any diagnostics program, close all running applications.

Use the Windows-based 3Com Network Interface Card Diagnostics program if you are running any of the following operating systems:

- Windows XP
- Windows 2000
- Windows 98 SE
- Windows NT 4.0

Use the 3Com DOS Diagnostics program if you are running any of the following operating systems:

- DOS
- NetWare

Running the Network Card Diagnostics Tests

The 3Com Network Interface Card Diagnostics program for Windows contains tests that can check the status of the following items:

- Network
- Network PC Card

To run the network card test or network test:

- 1 Make sure that the network card, the network driver, and the 3Com Network Interface Card Diagnostics program are installed.
- 2 Open the Windows *Start* menu.
- 3 Select Programs, and then 3Com NIC Utilities.
- 4 Click *3Com NIC Doctor*.

The 3Com Network Interface Card Diagnostics screen appears.



NOTE: Click *Help* to obtain general information about the function of a screen. To obtain specific information about any topic on a screen, click the question mark (?) in the upper right corner of the screen, move it over a topic, and click once.

The following tabs are available for viewing network card data:

Tab	Description
General	Select the General tab to display the node address, I/O address, and device ID for the installed network card.
Configuration	Select the Configuration tab to view and modify configuration settings for the installed network card.
Statistics	Select the Statistics tab to view network traffic statistics about the installed network card.
Diagnostics	Select the Diagnostics tab to access diagnostics tests that you can run on the installed network card.
Support	Select the Support tab to access various 3Com customer support resources.
Utilities	Select the Utilities tab to update firmware for the installed network card.

- 5 Select the Diagnostics tab.

The Diagnostics screen appears.

Running the Network Test

Run the Network Test to check the network card connectivity to the network.

To successfully pass the Network Connectivity test, at least one of the following conditions must be met:

- A Windows client running on the same network. This client must have a successfully installed Windows diagnostics program that is currently not running.
- A NetWare server running on the same network.
- A DHCP server running on the same network.

A DNS server running on the same network with TCP/IP properties configured for the DNS server.

To run the Network test:

- 1 On the Diagnostics screen, click *Run Network Test*.
The Network Connectivity Test screen appears.
- 2 Click *Start*.
- 3 If the test passes, the network card connection to the network is functioning correctly.
- 4 Click *Close*.
- 5 If the test fails:
 - Make sure that the network card is properly connected to the network cable.
 - Make sure that the hub or switch to which the network card is connected is powered on.
 - Make sure that the cable complies with the proper length and specifications for your network.

Running the Network Interface Card Test

Run the Network Interface Card Test to check the physical components, connectors, and circuitry on the network card.

- 1 On the Diagnostics screen, click *Run NIC Test*.
The NIC Test screen appears.
- 2 Click *Perform NIC Test*.
While the test is running, a progress bar indicates test progress.
If the test passes, the network card is functioning correctly.
If the test fails, a message indicates the error type. Click *Help* in the error message screen to obtain more information.
- 3 Click *Close*.

Running the 3Com DOS Diagnostics Program

- 1 Reboot the computer using a DOS-bootable disk.



CAUTION: *If you are running Japanese DOS, you must switch to U.S. mode DOS before running the 3Com DOS diagnostics program.*

- 2 Insert the *3Com Firewall PC Card with 10/100 LAN Installation CD* in the CD-ROM drive.
- 3 At the DOS prompt, enter the following command:

d:\3c99xcfg.exe

where d:\ indicates the drive location of the *3Com Firewall PC Card with 10/100 LAN Installation CD*.

Viewing the Network Card LEDs in the Diagnostics Program

To view the LEDs in the 3Com Network Interface Card Diagnostics program:

- 1 Make sure the network card, the network driver, and the 3Com Network Interface Card Diagnostics program are installed.
- 2 Open the Windows *Start* menu.
- 3 Select *Programs*, and then *3Com NIC Utilities*.
- 4 Click *3Com NIC Doctor*.

The 3Com Network Interface Card Diagnostics General screen appears and displays following LEDs:

Link—lights if there is a valid connection between the network card and the network.

Transmit—lights if the network card is transmitting information.

Receive—lights if the network card is receiving information.

Viewing Network Statistics

To view Network Statistics:

- 1 Make sure that the network card, the network driver, and the 3Com network card Diagnostics program are installed.
- 2 Open the Windows *Start* menu.
- 3 Select *Programs*, and then *3Com NIC Utilities*.
- 4 Click *3Com NIC Doctor*.

The 3Com network card Diagnostics General screen appears.

- 5 Click the *Statistics* tab.

The Statistics screen appears.

The information is updated by the card driver every 5 seconds.

For a description of each statistic, click the question mark (?) in the upper right corner of the screen, drag it over a statistic and click once. A pop-up box appears, displaying information about the statistic.

- 6 Click *OK* to exit the diagnostics program. To go to another diagnostics screen, click the associated tab.

Using the 3Com Icon in the Windows System Tray

The 3Com icon, which can be enabled to appear in the Windows system tray, allows you to start the 3Com Network Interface Card Diagnostics program. It also allows you to view the network card's link speed and number of frames sent and received.

Enabling the Icon

- 1 Make sure that the network card, the network driver, and the 3Com Network Interface Card Diagnostics program are installed.
- 2 Open the Windows *Start* menu.
- 3 Select *Programs*, and then *3Com NIC Utilities*.
- 4 Click *3Com NIC Doctor*.

The 3Com Network Interface Card Diagnostics General screen appears.

- 5 On the General screen, select the check box next to *Show Icon in System Tray*.
- 6 Close the *3Com Network Interface Card Diagnostic* program.

The network card icon appears in the Windows system tray.

When you double-click the icon, the 3Com Network Interface Card Diagnostics program starts.

Displaying Network Statistics

When you drag the mouse pointer over the icon (but do not double-click the icon) a network statistics box appears, displaying the following information:

Frames Sent and Received—A count of the number of frames (packets) sent and received through the network card since the last time statistics were reset.

Link Speed—The speed (10 Mbps or 100 Mbps) at which the network card is connected to the network.

The information is updated each time you move your mouse pointer over the 3Com icon.

Removing the 3Com Network Interface Card Diagnostics Program

The 3Com Network Interface Card Diagnostics Program can be removed using the Add/Remove Programs Wizard in Windows.

For instructions on using the Add/Remove Programs Wizard in Windows, see your Windows documentation.

3Com Connection Assistant

The 3Com Connection Assistant is interactive software that gives you an easy to use diagnostic and repair tool. Using this tool makes troubleshooting easier and helps you quickly resolve problems. Go to *Start/Programs/3Com NIC Utilities/3Com Connection Assistant* to find this utility.

Using the Connection Assistant you can:

- Automatically check your computer and repair problems
- Search for solutions for specific hardware or software problems
- Find answers to your questions about business processes, tasks, and applications
- Connect, via the Internet, to technical support when you need assistance with your computer hardware and software
- Get assistance even if you are not connected to the Internet

Connection Assistant Toolbar

The toolbar at the top of the Connection Assistant Home Page includes these options:

- Connection Assistant Home--Clicking this link will always return you to the Connection Assistant Home Page.
- Assisted Service--Click this link to send a request for assistance to a technical support engineer if you need help fixing a Network Interface Card problem.

- Options--Set different security, message, and display options for your Connection Assistant pages.
- Help--Browse Help information for a variety of topics, links and features related to the 3Com Connection Assistant.

Connection Assistant Options

The Connection Assistant may also contain the following options:

- Diagnose My Network Interface Card--Click this link to get information about your system, network and network interface card. In addition to providing detailed information, it also supplies solutions if a problem is detected with your 3Com network interface card.
- List Solutions--Contains a list of relevant topics for you reference.
- Network Settings--Provides detailed information about your network.
- Search--Locate topics and solutions.

3Com Launcher

The 3Com Launcher is a utility that allows you to start 3Com applications from a single source on your screen. When the 3Com Launcher is installed and started, it appears as a small toolbar with icons of the various 3Com programs that can be started through the Launcher. Programs such as the 3Com Diagnostics, the 3Com Mobile Connection Manager, or the 3Com Connection Assistant can all be launched with a single click from the 3Com Launcher toolbar.



5

Data Encryption Offload

About Data Encryption

The 3Com Firewall PC Card with 10/100 LAN performs data encryption processing offloads in Windows 2000 and Windows XP, which means that the network card, the 3Com Firewall PC Card with 10/100 LAN, rather than the operating system does the encryption.

Encryption processing is handled entirely by the 3XP processor on the network card. The 3XP processor enables true end-to-end network security at the data capacity of the connected network cable without sacrificing performance.

The data encryption offload capability of the 3Com Firewall PC Card with 10/100 LAN is disabled when you first unpack it. U.S. law requires that users be certified to use certain data encryption products.

The 3Com Firewall PC Card with 10/100 LAN uses Internet Protocol Security (IPSec) encryption, which is a framework of open standards for ensuring secure private communications over IP networks. IPSec ensures confidentiality, integrity, access control, and authenticity of data communications across a public IP network.

Offloading Encryption Processing

You can configure two or more computers running Windows 2000 and Windows XP to perform IPSec encryption by changing the local security setting in the operating system. With most non-3Com Firewall PC Card with 10/100 LAN, all the IPSec processing is done by the host central processing unit (CPU), which significantly diminishes CPU performance. The 3Com Firewall PC Card with 10/100 LAN can offload all the encryption processing from the host CPU, thereby freeing the CPU to work on other tasks.

For two or more computers running non-Windows 2000 or Windows XP operating systems, IPSec encryption is provided by third-party applications. The 3Com Firewall PC Card with 10/100 LAN does not provide IPSec encryption offloading for those operating systems.

A

Technical Support

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

Register for support at *support.3com.com/registration/frontpg.pl*

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site
- 3Com Connection Assistant

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

`http://www.3com.com/`

This service provides access to online support information, such as technical documentation and a software library, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

The 3Com Knowledgebase is a database of technical information to help you install, upgrade, configure, or support 3Com products. The Knowledgebase is updated daily with technical information discovered by 3Com technical support engineers. This complimentary service, which is available 24 hours a day, 7 days a week to 3Com customers and partners, is located on the 3Com Corporation World Wide Web site at:

`http://knowledgebase.3com.com`

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **`ftp.3com.com`**
- Username: **`anonymous`**
- Password: **`<your Internet e-mail address>`**



NOTE: With Web browser software, such as Netscape Navigator and Internet Explorer, you do not need a user name and password.

3Com Connection Assistant

The 3Com Connection Assistant is interactive software that gives you an easy to use diagnostic and repair tool. Using this tool makes troubleshooting easier and helps you quickly resolve problems. Go to:

Start/Programs/3Com NIC Utilities/3Com Connection Assistant

to find the utility.

By using the Connection Assistant you can:

- Automatically check your computer and repair problems
- Search for solutions for specific hardware or software problems
- Find answers to your questions about business processes, tasks, and applications
- Connect, via the Internet, to technical support when you need assistance with your computer hardware and software
- Get assistance even if you are not connected to the Internet

For more information about 3Com Connection Assistant, contact your help desk directly or visit us at: www.3com.com/connectionassistant

Support from Your Network Supplier

If you require additional assistance, consult your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you consult your network supplier, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to consult your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, go to the Web site associated with your region of the world shown below.

Region	URL for Regional Web Site
Asia and the Pacific Rim	ap.3com.com/contacts/support-contacts.html
Africa, Europe, and the Middle East	emea.3com.com/support/supportnumbers.html
Latin America	lat.3com.com/lat/support/index.html
North America	csoweb4.3com.com/contactus/

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense. To obtain an authorization number, go to the Web site listed above for your region.

B

Configuring IPSec

Configuring IPSec in Windows 2000 and Windows XP

IPSec primarily consists of two parts:

encryption/decryption

authentication

To send or receive encrypted data in a PC running Windows 2000 or Windows XP with a 3Com Firewall PC Card with 10/100 LAN installed, you must first create a security policy, and then enable encryption on the network card.

The security policy establishes and defines how encrypted network traffic between your PC and a specified server occurs.

Authentication enables the receiver to verify the sender of a packet by adding key fields to a packet without altering the packet data content.

The following table shows the available levels of encryption:

Encryption Type	Encryption Level	Description
AH	Medium	Authentication only
ESP	High	Authentication and encryption
Custom	Varies	Provides encryption and an extra authentication that includes the IPheader. Custom allows you to select options for both AH and ESP, such as MD/SHA-1 and DES/3DES, and you can select the rate at which new keys are negotiated. Microsoft uses IKE key exchange to renew keys every x seconds or y bytes. You may want to set these values low and have frequent key updates, or higher for better performance. For more information, see the Microsoft documentation about creating IPSec flows.

Example: Creating a Security Policy

The process you use to create and enable a security policy depends on your network environment requirements. The following is an example of one approach to creating a security policy.



NOTE: You must complete all of the sequences in this example to establish and enable a security policy for transmitting and receiving encrypted data over the network.

Defining the Console

This sequence establishes the console and defines its parameters.

- 1 In the Windows task bar, click *Start>Programs>Accessories>CommandPromp*.
- 2 At the DOS prompt, enter
MMC
The Console1 screen appears
- 3 In the menu, click *Console*, then *Add/Remove Snap-in*.
The Add/Remove Snap-in screen appears.
- 4 Click *Add*.
The Add Standalone Snap-in screen appears.
- 5 Select *IP Security Policy Management* and click *Add*.
The Select which computer this Snap-in will manage screen appears.
- 6 Enable the *Local* computer option.
- 7 Click *Finish*, *Close*, and then *OK*.

Creating the Policy

This sequence creates and names the new security policy.

The Console1 and Console Root screen appears with IP Security Policies on Local Machine displayed in the list.

- 1 In the left pane, click *IP Security Policies on Local Machine*.
- 2 Right-click inside the right pane below the list items.
- 3 From the pop-up menu, select *Create IP Security Policy*.
The IP Security Policy Wizard starts.
- 4 Click *Next*.
The IP Security Policy Name screen appears.
- 5 Enter a name for the new security policy that you are creating and, if you wish, a description that identifies the policy.
- 6 Click *Next*.
The Requests for Secure Communication screen appears.
- 7 Clear the *Activate the default response rule* check box.
- 8 Click *Next* and then *Finish*.
- 9 Click *Add*.
The Security Rule Wizard starts.
- 10 Click *Next*.
The Tunnel Endpoint screen appears.
- 11 Enable the default option *This rule does not specify a tunnel*, and click *Next*.
The Network Type screen appears.
- 12 Enable the default option All network connections, and click *Next*.
The Authentication Methods screen appears.
- 13 Enable the *Use this string to protect the key exchange (preshared key)*: option, type the appropriate string text in the entry field, and then click *Next*.

Creating a Filter

This sequence creates a filter for the policy.

The IP Filter List screen appears.

- 1 Click *Add*.
A new IP Filter List screen appears.
- 2 Enter a name for the filter and click *Add*.
The IP Filter Wizard starts.
- 3 Click *Next*.
The IP Traffic Source screen appears.
- 4 Click *Next*.
The IP Traffic Destination screen appears.
- 5 Select *A Specific IP Address* in the pull-down list.
The IP Address entry box appears on the IP Traffic Destination screen.
- 6 Enter destination IP address, and then click *Next*.
The IP Protocol Type screen appears.
- 7 Accept the default and click *Next*.
- 8 Click *Finish* to close the IP Filter Wizard.
- 9 Click *Close* to close the IP Filter List screen.

Binding the Filter

This sequence attaches the new filter to the policy.

The IP Filter List screen appears.

- 1 Enable the option for the new filter name and make sure the new filter name is selected.
- 2 Click *Next*.

Creating the Filter Action

This sequence defines how the filter acts on the policy.

The Filter Action screen appears.

- 1 Click *Add*.
The Filter Action Wizard starts.
- 2 Click *Next*.
The Filter Action Name screen appears.
- 3 Enter a name (for example: 3DEW to the Server), and then click *Next*.
The Filter Action General Options screen appears.
- 4 Accept the default and click *Next*.
The screen *Communicating with computers that do not support IPSec* appears.
- 5 Accept the default value and click *Next*.
The IP Traffic Security screen appears.
- 6 Select *Custom*, and then click *Settings*.
The Custom Security Method Settings screen appears.
- 7 Enable the *Data integrity and encryption (ESP)* check box and make the appropriate selections in the Integrity and algorithms list boxes.

- 8 Click *OK*, *Next*, and then *Finish*.

Binding the Filter Action

This sequence attaches the new filter action to the filter and policy.

The Filter Action screen appears.

- 1 Enable the filter action option and make sure that the filter name is selected. (In this example, we used the filter name: *3DES to the Serve*.)
- 2 Click *Next*, *Finish*, and *Close*.
The newly created policy appears in the right pane of the Console Root\IP Security Policies on Local Machine screen.
- 3 Exit this screen and, when prompted, save the new policy information. Use a meaningful name for future reference.

You can modify this security policy by double-clicking the icon that is created when you save the policy in the previous step.

Enabling Encryption

An encryption policy must exist in the Console Root\IP Security Policies on the Local Machine screen before you can enable encryption on the 3Com Firewall PC Card with 10/100 LAN.

To enable encryption:

- 1 Right-click the desired policy icon in the right pane of the screen.
- 2 Select *Assign*.
- 3 A green plus (+) symbol appears on the policy icon to indicate that encryption is toggled on.

Disabling Encryption

An encryption policy must exist in the Console Root\IP Security Policies on the Local Machine screen before you can disable encryption on the 3Com Firewall PC Card with 10/100 LAN.

To disable encryption:

- 1 Right-click the desired policy icon in the right pane of the screen.
- 2 Select *Un-assign*.
The absence of a green plus (+) symbol on the policy icon indicates that encryption is toggled off.

REGULATORY INFORMATION



NOTE: *This product contains encryption. It is unlawful to export out of the U.S. without obtaining a U.S. Export License.*

FCC PART 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ✦ Reorient or relocate the receiving antenna.
- ✦ Increase the separation between the equipment and receiver.
- ✦ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ✦ Consult the dealer or an experienced radio/TV technician for help.

MANUFACTURER'S DECLARATION OF CONFORMITY

3Com Corporation
3930 W. Parkway Blvd.
West Valley City, UT 84120
(800) 527-8677

Declares that the Product:

Date: January 28, 2002

Name: 3Com

Model Number:

Equipment Type: 10/100 LAN PC Card

3CRFW102 and 3CRFW103

Tested To Comply With FCC Standards



FOR HOME OR OFFICE USE

Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this equipment may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

INDUSTRY CANADA (ICES-003)

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

AVIS DE CONFORMITÉ À LA RÉGLEMENTATION D'INDUSTRIE CANADA

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

SAFETY

This equipment has been tested and certified according to the following safety standards and is intended for use only in Information Technology Equipment which has been tested and certified to these or other equivalent standards:

- ✦ *UL Standard 1950 / CSA C22.2 No. 950*
- ✦ *IEC 60950*
- ✦ *EN 60950*

For superior network performance, 3Com recommends the use of Category 5 or Category 5e rated LAN cable.

CE NOTICE



This device complies with the requirements of European Directive **89/336/EEC** - EMC Directive.

EN55022: Limits and methods of measurement of radio interference characteristics of Information Technology Equipment (ITE), [Class B].

EN55024: Information technology equipment - Immunity characteristics - Limits and methods of measurement.

Council Directive 72/23/EEC - Low Voltage Directive
EN60950: Safety of Information Technology Equipment

VCCI CLASS B

This is a Class B product based on the standard of the Voluntary Control Council for Interference from information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置
家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受
と、受信障害を引き起こすことがあります。

従って正しい取り扱いをして下さい。

Manual version 2.0
August 15, 2002