

Guardian

Internet Security System

User's Guide

N e t  u a r d

Trademarks and Registered Names

All specifications are subject to change without notice.

NetGuard is a pending trademark of NetGuard Ltd. IBM and LAN Manager are registered trademarks of International Business Machines Corp. Netware[®] and Novell[®] are registered trademarks of Novell Corporation. Microsoft[®] and MS-DOS[®] are registered trademarks of Microsoft Corporation. Paradox is a trademark of Borland International. Cisco and Cisco Systems are registered trademarks of Cisco Systems, Inc. Brand and product names are trademarks or registered trademarks of their respective holders.

This user's guide refers to Guardian v2.2.

Publication Number: 27-7585-05

Proprietary Notice

This manual contains information proprietary to NetGuard and may not be reproduced in any form without prior written consent from NetGuard Ltd.



NetGuard Inc.

2445 Midway Road
Building 2
Carrollton, Texas 75006
U.S.A.
Tel: 1-972-738-6900/1-800-533-8439
Fax: 1-972-738-6999

NetGuard (UK) Ltd.

Thamesbourne Lodge,
Station Road, Bourne End,
Buckinghamshire SL8 5QH
United Kingdom
Tel: +44-1628-533-433
Fax: +441628-532-252

NetGuard Ltd.

LanOptics Building
Ramat Gabriel Industrial Park
P.O. Box 184
Migdal Ha-Emek 10551, Israel
Tel: +972-6-449-944
Fax: +972-6-540-124

LanOptics Nordic

Malmö Slagthus
Carlsгатan 12A
S-211 20 Malmö
Sweden
Tel: +46-40-10-8195
Fax: +46-40-10-8197

Contents

Using this Manual.....	v
How to Use this Manual	v
How this Manual is Organized	vi
Conventions Used in this Manual	vii
Typographical Conventions	vii
About Guardian.....	1-1
What is Guardian?	1-1
Features	1-2
Guardian Components	1-3
Guardian Products	1-4
Firewall.....	1-4
Network Address Translation (NAT)	1-4
Remote User Authentication	1-4
Virtual Private Network (VPN).....	1-4
Installation and Configuration	2-1
Introduction	2-1
Designing the Network Configuration	2-2
Preparing the Agent Station.....	2-5
Hardware Requirements.....	2-5
System Software Installation.....	2-6
Verifying the Configuration.....	2-7
Assigning Static Routes.....	2-9
Installing the Agent	2-10
Tuning the ARP Processor.....	2-12
Verifying the Agent Installation.....	2-13
Installing Guardian Manager	2-15
Hardware Requirements.....	2-15
Software Requirements.....	2-15
Installing the Guardian Manager	2-16
Ordering Your Guardian Agents.....	2-17
Entering the Permanent Key	2-18
Getting Started.....	3-1
Running Guardian	3-1
Communicating with the Guardian Agent	3-1

Inserting the IP Address and Data Encryption Key	3-3
Establishing Initial Communications with the Agent	3-5
Changing the Default Encryption Key	3-6
Guardian Main Screen.....	3-7
Menu Bar	3-7
Toolbar	3-8
Alerts and Logs Window	3-10
Basic Windows Skills.....	3-11
Exiting Guardian.....	3-11

Performing Common Tasks4-1

Introduction	4-1
Monitoring Agents	4-2
Monitoring User Activity.....	4-3
Monitoring Real-time Sessions.....	4-3
Monitoring Individual Sessions	4-8
Reviewing Alerts and Logs	4-9
Limiting the Amount of Data Per User.....	4-13
Defining Network Objects	4-14
Defining a New Network Object	4-14
Modifying an Object's Definition.....	4-16
Deleting an Object's Definition.....	4-17
Defining Internet Services.....	4-18
Defining a New Service.....	4-18
Modifying a Service's Definition.....	4-20
Deleting a Service's Definition	4-20
Defining a New Protocol	4-21
Modifying and Deleting a Protocol's Definition.....	4-22
Creating a Firewall Strategy.....	4-23
Creating a NAT Strategy	4-23
Creating a Virtual Private Network (VPN).....	4-23
Viewing Statistics	4-24
Creating Temporary Rules.....	4-25
Suspending All Internet Communications.....	4-27

Planning Your Company's Firewall.....5-1

What is a Firewall?	5-1
Security Types	5-1
Installing a Firewall Strategy.....	5-6
Creating and Editing a Firewall Strategy	5-8

Network Address Translation	6-1
What is NAT?	6-1
Features	6-3
Implementing NAT	6-5
Creating and Modifying a NAT Strategy.....	6-7
Making Static Assignments.....	6-9
Making Dynamic Assignments.....	6-11
Assigning a Single Address.....	6-14
Saving the Address Assignment Table.....	6-14
Installing the NAT Strategy.....	6-15
User Authentication.....	7-1
What is User Authentication?.....	7-1
One-time Password Authentication.....	7-2
Authentication Process.....	7-3
Initializing the Authentication Process.....	7-3
Running the Authentication Program.....	7-4
Implementing Guardian Authentication	7-5
Preparing the Network for User Authentication.....	7-6
Modifying the Firewall Strategy	7-7
Performing User Authentication	7-9
Virtual Private Networks.....	8-1
What is Encryption?.....	8-1
Symmetric Key Scheme.....	8-1
Public/Private Key Scheme.....	8-2
Guardian Encryption Scheme or Virtual Private Network.....	8-2
Encryption Key Example	8-3
Implementing Encryption for the LA Branch.....	8-4
Verifying	8-9
Encryption Properties for the LA Branch.....	8-9
Implementing Encryption for the Boston Branch	8-10
Implementing Encryption for the London Branch.....	8-12
Appendix A.....	A-1
Installing the Agent on the LAN Segment.....	A-1
Setting up the Guardian Gateway	A-3
Reconfiguring the Router	A-4

Using this Manual

How to Use this Manual

This manual contains the concepts and step-by-step instructions you need to know when using the Guardian System. We recommend that you read through the manual thoroughly.

If you are looking for a particular topic, use the Table of Contents at the beginning of the manual.

- Chapters 1-3 provide an overview of the system and guides you through installation and configuration.
- Chapter 4 provides instructions for performing frequently used tasks.
- Chapters 5-8 provide a description of the various products which are supplied with the Guardian.
- Appendix A provides instructions for installing a Guardian agent on the same segment as the network.

This manual assumes that you are familiar with the basic concepts of using Microsoft Windows NT. For information about using Windows NT, refer to your *Microsoft Windows NT User's Guide*.

How this Manual is Organized

This manual is divided into eight chapters. The following is a brief description of each chapter.

	Chapter	Content
1	About the Guardian System	Provides an introduction to the Guardian System. What is the Guardian System? What are its main features and advantages?
2	Getting Started	Presents an overview of the system, the user interface and the main screens.
3	Installation and Configuration	Demonstrates the Guardian System installation and describes the system's requirements.
4	Performing Common Tasks	Provides step-by-step instructions for performing tasks using the Guardian manager.
5	Planning Your Company's Firewall	Describes designing a firewall strategy, filtering, and monitoring.
6	Network Address Translation	Describes installing and implementing NAT.
7	User Authentication	Provides instructions for installing and performing user authentication.
8	Virtual Private Networks	Provides instructions for encrypting data for secure communication.

Conventions Used in this Manual

Typographical Conventions

The following typographical conventions are used in this manual:

- Keyboard commands are enclosed in square brackets, for example:

Press [Enter]

Press the enter key on the

keyboard.

- The regular sans serif font refers to a menu or sub-menu item.

This format – Main menu option → Sub-menu option – indicates a menu selection, where the first option is the main menu item and the second option indicates the sub-menu item to select, for example:

File → Exit

Choose the File menu and then select the Exit command.

- The **bold sans serif** font is used to refer to a button in a dialog box. For example:

Click the **Execute** button.

- Words that appear in *italics* indicate:

Cross references to other sections in the manual.

Example: See *Chapter 4: Performing Common Tasks*.

-or-

New terms and words used for emphasis.

- The following bullets and numbering formats are used to indicate different types of lists:

- | | |
|------------|---|
| 1, 2 ... n | Represents a step-by-step list of procedures |
| ◆ | Diamond bullets represent a single command procedure. |
| • | Round bullets represent a list of points or features. |

About Guardian

What is Guardian?

The Guardian is a distributed Internet access security system. The Guardian uses a MAC layer stateful inspection mechanism with additional features to increase security, improve network efficiency and create a user-friendly interface for configuration and management.

The Guardian provides centralized network management functions for the protection of your network. Not only does Guardian prevent unauthorized access, but it also serves as a tool for network administration. The network administrator can monitor real-time usage of the network, limit user access to the network, restrict network access to specific days and hours, and restrict the use of heavy programs to reduce expenses.

The user authentication feature provides a mobile user with access to a predefined source in your protected network. Access is allowed on a temporary basis and to certain services only. For example, a mobile user can connect to the company's mail server to check for mail.

As companies access the Internet more and more, the vulnerability of their private networks increases. The global race to connect to the information superhighway leaves enterprise networks without protection against espionage, sabotage, hacking and other Internet-based dangers. This problem becomes even more acute in corporations with several sites interconnected via the Internet. An infiltrator needs only to access the private

network at one site to compromise the company's entire enterprise network.

The Guardian is the solution for securing your private network.

Features

The Guardian security system provides the following features:

- Enterprise network security system and safeguard.
- Powerful notification and logging mechanism.
- Completely transparent to client applications without duplicating log on requests.
- Adaptable to network expansion and restructuring.
- Built-in system for LAN management.
- Monitoring of suspicious events by enabling the network administrator to monitor events pre-defined as suspicious in real time, instead of waiting for a log, whereby the violator may have already logged out.
- Real-time session monitoring, which keeps track of all Internet higher protocols and services and enforces your network's pre-defined security policy.
- Traffic control feature, allowing individual traffic limitations for each host on the LAN.
- Supports all Internet services and allows for the definition of new services.
- Activity log for review by the network administrator.

- Proprietary protocol for communications between agent and manager. Each frame between the manager and agent is encrypted.
- Does not require the user to have extensive knowledge of Internet protocols.

Guardian Components

Guardian consists of two software modules: *Guardian manager* and *Guardian agent*.

- The Guardian manager is the main user interface to the agent and operates under Microsoft Windows 95 and Windows NT. The manager can be installed anywhere on the network reachable by TCP/IP protocol.
- The Guardian agent operates under Windows NT. The Guardian agent is installed at every site between the Internet and the local network. The Guardian agent can be installed directly on the router/gateway to the Internet or on a dedicated machine between the router and the local network.

The agent inspects every packet passing through the Guardian gateway and decides each packet's fate according to your filtering specifications.

For added security, all communications between the Guardian agent and Guardian manager are encrypted. The encryption differs for each agent.

Guardian Products

The following products are available in the Guardian system:

Firewall

A *firewall* is a software product located between the company's internal LAN and the Internet to provide security to a company's private LAN. Guardian assists you in building a *firewall strategy* based on your corporate security considerations. For example, you may decide to filter your company's communications for security reasons and for traffic control purposes. You determine which communications will be prohibited and the actions to be taken.

Network Address Translation (NAT)

Network Address Translation (NAT) is a Guardian application that provides flexible and secure IP addressing for your local network. NAT enables you to maximize your assignment of network addresses by dynamically mapping official IP addresses to local addresses.

Remote User Authentication

Remote user authentication allows a remote user to access a predefined source in a protected network for certain services on a temporary basis.

Virtual Private Network (VPN)

With the growth of international networks, public and private e-mail systems, a greater need to secure private

communication has arisen. One method for ensuring privacy is *encryption*. The encryption process transforms data into a form unreadable by anyone that might be monitoring the line. This transforms an insecure channel of information, such as the Internet, into a *Virtual Private Network (VPN)*.

Installation and Configuration

Introduction

This section provides instructions for preparing the agent station and installing the agent. The agent station is prepared without disturbing the network. When the installation is complete, the network connection is cut for a very short period, to position the agent.

The Guardian installation consists of the following steps:

- Designing the network configuration
- Preparing the agent station
- Installing the agent
- Tuning the ARP Processor
- Verifying the agent installation

A sample configuration assists you in the installation process.

Designing the Network Configuration

The example below is a sample configuration which can be used as a base for any configuration. In most cases, the configuration you choose will probably be easier than the example. If you choose to connect only one LAN segment to the Internet using a single router, follow the instructions which follow for LAN1 and router R1 only.

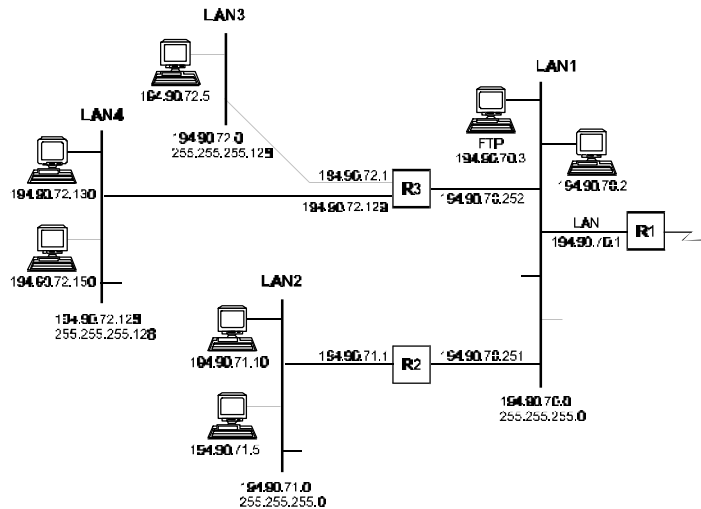


Figure 2-1 Sample Configuration

As illustrated in the sample configuration, the company has four LAN segments, LAN1 - LAN4, connected to the Internet. The LAN 3 (sub-net 194.90.72.0 netmask 255.255.255.128) and LAN4 (sub-net 194.90.72.128 netmask 255.255.255.128) segments are connected through router R3 to the LAN1 segment (net 194.90.70.0 netmask 255.255.255.0).

Segment LAN2 (net 194.90.71.0 netmask 255.255.255.0) is connected through the router R2 to a segment LAN1 (net 194.90.70.0 netmask 255.255.255.0). Finally, segment

LAN1 (net 194.90.70.0 netmask 255.255.255.0) is connected to the Internet Service Provider (ISP) through router R1.

The company has one publicly accessed FTP server connected to the LAN1 segment with an IP address of 194.90.70.2.

The IP traffic within the company is regulated by a series of static route assignments configured on the company's routers R1, R2 and R3.

For each host connected to its LAN segment, the respective router is defined as the default gateway. This means that all the IP packets issued by those hosts and destined for the Internet, will be sent to the nearest router for processing.

The default gateway of routers R2 and R3 is router R1. The default gateway for router R1 is the ISP router's IP address. R1 has the following static route assignments:

- LAN3 and LAN4 can be accessed via R3
- LAN2 can be accessed via R2.

The correct position for the agent is between LAN1 and the router R1. In this way it protects, monitors and controls the TCP/IP traffic to/from the Internet for the entire company. Even though the IP address of the external adapter seems irregular, this is the appropriate configuration for the example network. The final configuration we want to achieve is displayed in Figure 2-2.

Note:

All the considerations in Figure 2-2 are based on the fact that the company may create a LAN segment which physically separates the agent workstation and router R1. The separate segment must be separated from the rest of the network. If this is not possible, refer to Appendix A for instructions on installing the agent on the same segment.

The company chose to position the publicly accessed FTP server 194.90.70.2 on the unprotected part of the network i.e., between the agent and router R1.

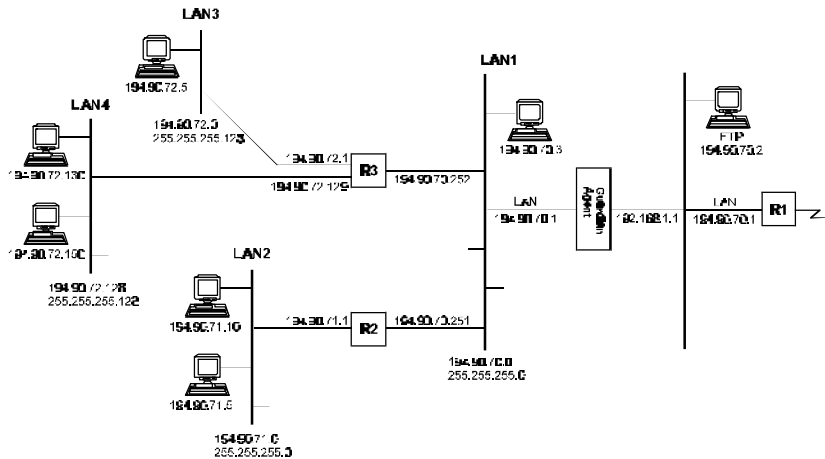


Figure 2-2 Final Configuration

Preparing the Agent Station

It is important to note that when you disconnect router R1 from the rest of the network, all the communication to/from the Internet stops. Thus, it is important to keep the disconnection time to a minimum. To achieve this, prepare the agent station before inserting it into the network.

Hardware Requirements

We recommend that you install the Guardian agent on an Intel P5 120Mhz computer with the following features:

- 32 Mbytes of RAM
- 160 Mbytes hard disk
- CD-ROM
- Minimum of 2 network adapters
- VGA monitor
- Keyboard
- Mouse

In keeping with our sample configuration, let's suppose that we have prepared a PC that matches the above requirements and has two LAN "Intel 82557 based 10/100 Ethernet PCI Adapters."

Note:

If one of the LAN adapters is a Token Ring adapter, it must be attached to the Token Ring network (using any type of MAU); otherwise the configuration will not be possible. We recommend that you connect the Token Ring adapter(s) to a separate dedicated network for the installation period.

System Software Installation

Follow the instructions below to install the system software on the agent workstation and check the configuration.

► **To install the software**

- 1 On the agent workstation, install the MS Windows NT Workstation/Server 4.0.
- 2 During setup, select the TCP/IP protocol to be installed. The other network protocols (IPX, NetBIOS etc.) are optional.
- 3 Assign the IP address of router R1 (194.90.70.1 with netmask 255.255.255.0) to the LAN adapter that will be connected to LAN1.
- 4 Assign IP address 192.168.1.1 (with netmask 255.255.255.0 and default gateway 192.168.1.2) to the LAN adapter that will be connected to a separate LAN segment via router R1.

Note:

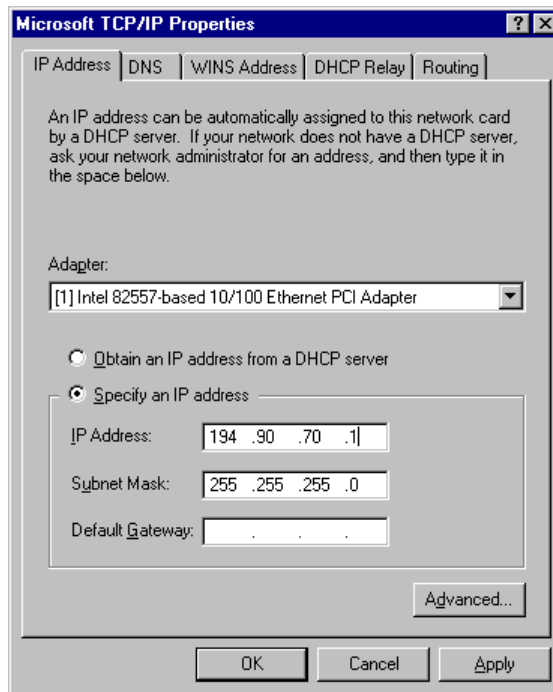
If you are not familiar with the Guardian installation process, we strongly recommend assigning the mentioned IP address.

Verifying the Configuration

Follow the instruction below to verify the configuration.

► **To verify or change the configuration**

- 1 In the Control Panel, double-click the **Network** icon.
- 2 From the list of network components, double-click **TCP/IP** protocol. The Microsoft TCP/IP Properties dialog box appears.

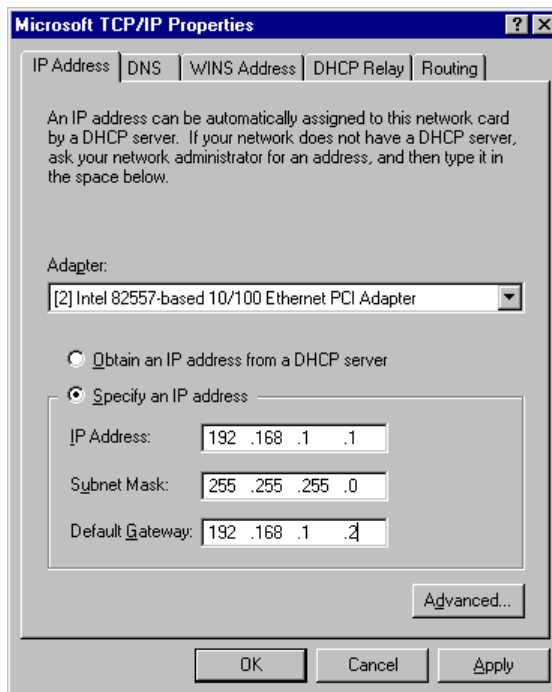


- 3 From the drop-down list, choose the first LAN adapter (connected to LAN1). Check that the IP address is 194.90.70.1 and that the network mask is 255.255.255.0.

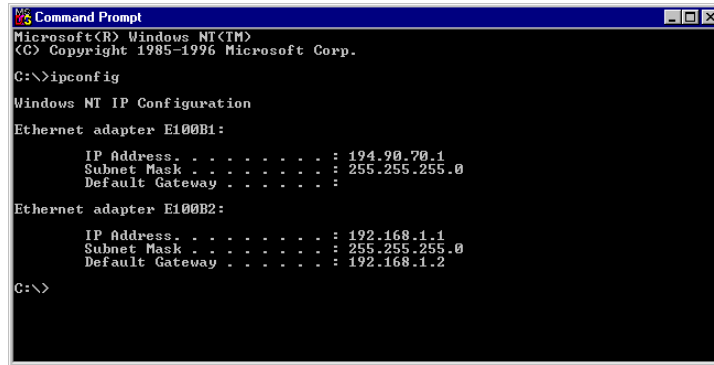
Note:

There should not be a default gateway defined for this LAN adapter.

- 4 Choose the second LAN adapter (connected to a separate LAN segment with router R1) and check that the IP address is 192.168.1.1, the network mask is 255.255.255.0 and the default gateway is 192.168.1.2.



You can also use the IPCONFIG command in the Windows NT Command Prompt window to check the TCP/IP configuration. This command, however, only allows you to review the TCP/IP configuration and does not allow modifications. An example of the IPCONFIG screen follows.



```
Microsoft Windows [Version 4.0.9506]
Copyright (c) 1996 Microsoft Corporation

C:\>ipconfig

Windows NT IP Configuration

Ethernet adapter E100B1:

    IP Address. . . . . : 194.90.70.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter E100B2:

    IP Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.2

C:\>
```

Assigning Static Routes

After installing and verifying the software, you must assign static routes to the agent station for routing the incoming TCP/IP traffic destined for LAN2, LAN3 and LAN4, via routers R2 and R3.

► To setup the static route assignments

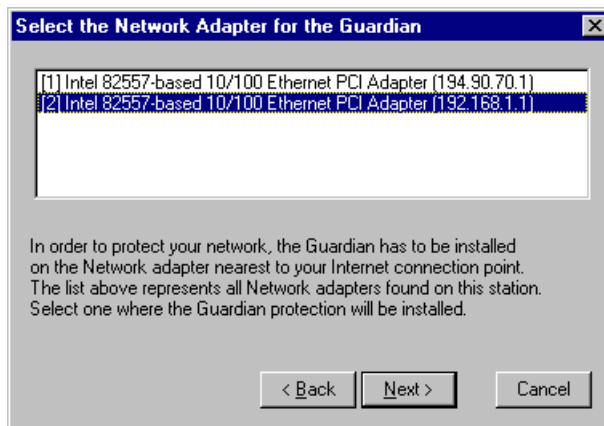
- 1 In the Windows NT command prompt window, type the following commands:
Route add -p 194.90.71.0 mask 255.255.255.0
194.90.70.251
Route add -p 194.90.72.0 mask 255.255.255.0
194.90.70.252
- 2 Restart the computer. The workstation is ready for the agent installation.

Installing the Agent

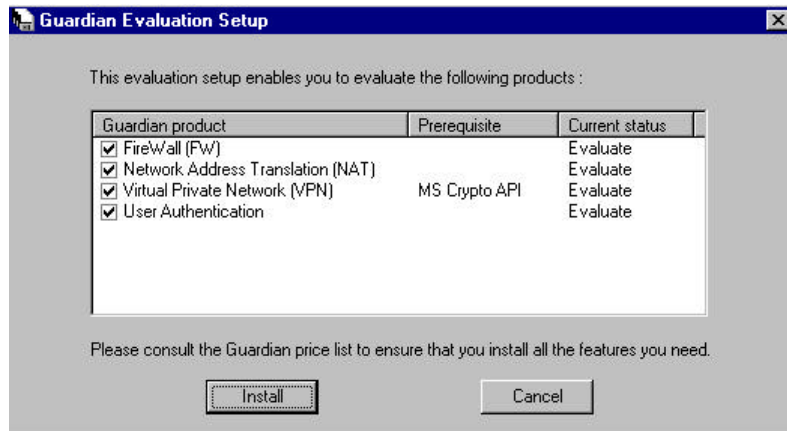
The Guardian agent installation is performed by running the agent installation from the compact disc or by downloading the self- extracting file from our web site. After installing the agent, you can verify the installation using the IPCONFIG command and also check that the agent is active.

► **To install the agent**

- 1 Download and run the executable agent file from our web site. Details of our web site appear in the introductory pages of this manual.



- 2 In the Select the Network Adapter dialog box, choose the adapter for connection to the Internet closest to the router. In keeping with our sample configuration, this is adapter 2.
- 3 Click **Next**. The Guardian Evaluation Setup dialog box appears.



- 4 In the Guardian Evaluation Setup dialog box, select the products you wish to evaluate. We recommend that you evaluate all the products. Click **Install**.

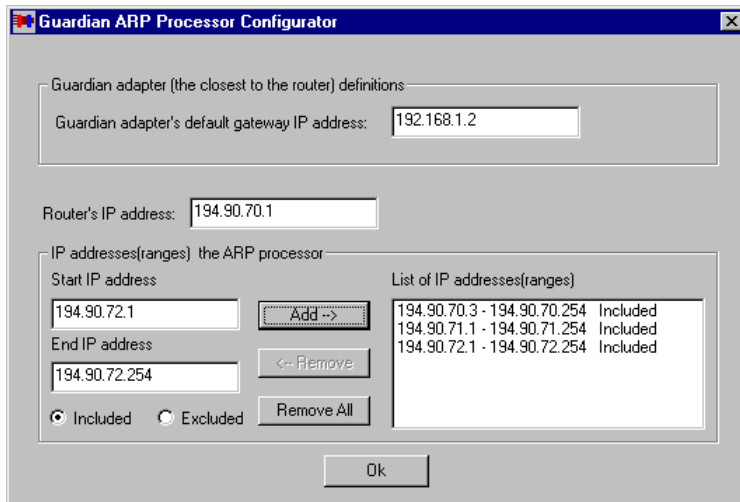
This concludes the installation process. You must now tune the ARP processor to complete the configuration.

Tuning the ARP Processor

After installing the Guardian Agent, you need to run the ARP Processor program to complete the network configuration. During this process, the network recognizes the agent.

► **To run the ARP Processor program**

- 1 In the Guardian folder, double-click the **ARP Processor** icon. The ARP Processor Configurator dialog box appears.



- 2 In the Guardian Adapter's Default Gateway IP Address field, type 192.168.1.2. This is the default gateway's IP address specified for the LAN adapter connected to a separate network with router R1, as per our sample configuration.
- 3 In the Router's IP Address field, type 194.90.70.1. This is the IP address of router R1.

- 4 In the Start IP Address and End IP Address fields, type the range of IP addresses for the IP networks behind the agent workstation i.e. LAN1, LAN2, LAN3 and LAN4.

Note:

Exclude those workstations which are connected to the separate network between the agent and router R1 from the ranges. Thus, in the ARP Processor Configurator dialog box, you will see that the first range for LAN1 starts with IP address 194.90.70.3. The FTP server connected to the separate LAN segment between the agent and router R1 has an address of 194.90.70.2.

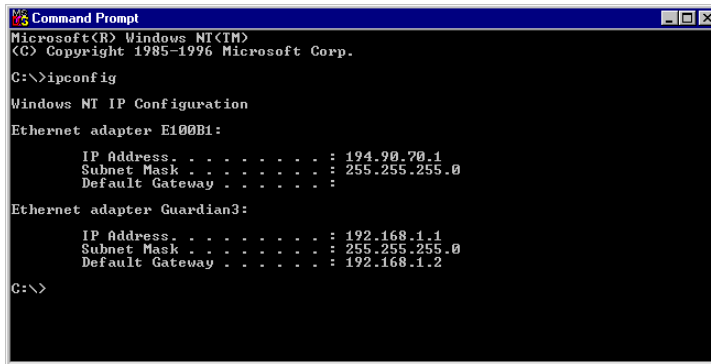
- 5 Restart and physically insert the agent workstation into the network.

Verifying the Agent Installation

After restarting the agent workstation, check the configuration using the IPCONFIG command.

► **To verify the agent installation**

- ◆ At the Windows NT command prompt, type IPCONFIG and press <Enter>. The Command Prompt screen appears.



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ipconfig

Windows NT IP Configuration

Ethernet adapter E100B1:

    IP Address. . . . . : 194.98.70.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Guardian3:

    IP Address. . . . . : 192.168.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.2

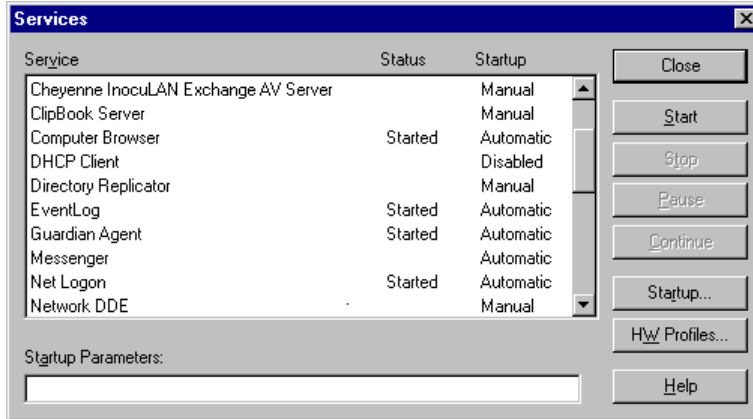
C:\>
```

Note:

The Guardian is installed on the second adapter.

➤ **To check that the Guardian agent is active**

- 1 In the Control Panel, double-click the **Services** icon. The Services dialog box appears.



- 2 Check that the Guardian agent appears in the list of services.
- 3 Click **Close** to exit this dialog box.

Installing Guardian Manager

Hardware Requirements

We recommend that you install the Guardian manager on an Intel P5 120Mhz computer with the following features:

- 32 Mbytes of RAM
- 160 Mbytes hard disk
- CD-ROM
- Minimum of 1 network adapter
- VGA monitor
- Keyboard
- Mouse

Software Requirements

- Microsoft Windows NT
- Microsoft Windows 95

Installing the Guardian Manager

Follow the instructions below to install the Guardian Manager.

► **To install the manager**

- 1 Insert the Guardian compact disk into the CD-ROM drive.
- 2 Follow the instructions displayed on the screen.
- 3 When the Choose Destination Location screen appears, select the drive and directory in which the Guardian manager will be installed.
- 4 Follow the instructions displayed on the screen.
- 5 When the folder selection screen appears, select the folder in Program Manager in which the Guardian manager icon will be installed. The default folder name is Guardian Manager.
- 6 A notification message will be displayed when the Guardian Manager installation has been completed successfully.

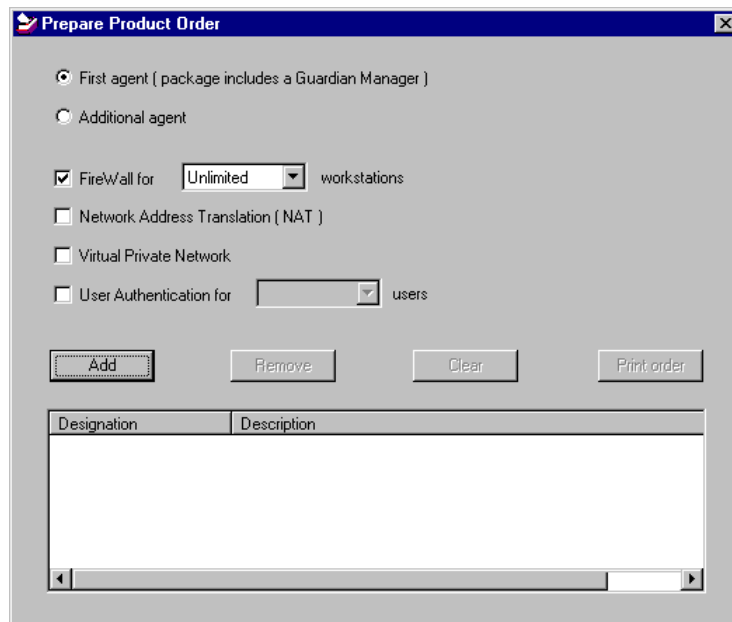
The Guardian Manager group will contain the Guardian Manager icon(eye), Database viewer icon and Guardian Help icon.

Ordering Your Guardian Agents

The Guardian evaluation copy will operate for a limited period of 30 days. Within this time period, you must order the permanent products. The procedures for ordering the Guardian products are described below.

► **To prepare a product order**

- 1 In the Guardian program folder, choose **Prepare a Product Order**. The Prepare Product Order dialog box appears.



- 2 Select the type of agent you are ordering: First agent or Additional. Choose First agent if this is the first time you are ordering a Guardian agent. Or, choose Additional Agent if you have previously ordered an agent.

- 3 Choose the products you want to order.

When you order a Firewall, choose the number of workstations in your network from the drop-down list. Similarly, when you choose User Authentication, choose the number of users.

- 4 Click Add to include the selected products in the order. The products you ordered appear in the bottom part of the screen.
- 5 Choose Print Order to see a printout of the products you ordered.
- 6 Send the product order to Netguard or a registered distributor.

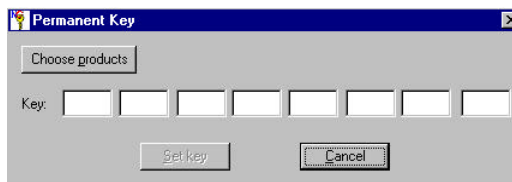
When the software package arrives, register the Guardian and request the permanent key.

Entering the Permanent Key

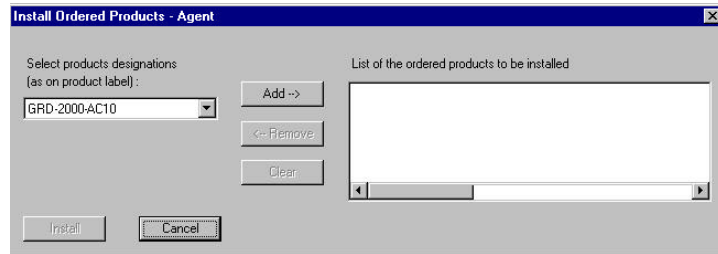
The permanent key is a group of eight hexadecimal numbers that are bound to your hard disk's serial number. By entering the permanent key, you complete the registration process and convert the time-limited installation into a permanent one.

► To enter the permanent key

- 1 From the Guardian Program Folder, choose Guardian Permanent Installation. The Permanent Key screen appears.



2. Type in the number sequences of the permanent Key supplied by Netguard, in the spaces provided.
3. Click **Choose Products**. The Install Ordered Products Agents dialog box appears.



4. From the drop-down list, select the product destination as it appears on the product label.
5. Click **Add** to include the product in the list of products to install.
6. Click **Install**. The products are now permanent.

Getting Started

Running Guardian

There are two ways to start your Guardian application:

- In the Programs list under Start, click **Guardian Manager**.

-or-

- If you created a shortcut on your desktop, then double-click the Guardian Manager icon in the Guardian program group.

The Guardian main screen appears.

Communicating with the Guardian Agent

You can choose whether to install the Guardian manager on the same station as the Guardian agent or on a remote station.

If you install the Guardian manager on the same station as the Guardian agent, communication is established automatically with an agent named *Local Agent*. If you do *not* install the Guardian manager on the same station as the Guardian agent, you must insert the agent's IP address and encryption code to establish communications.

The manager fills one of two functions, according to the corresponding agent:

- controlling manager
- observing manager

The controlling manager *performs* all the functions of establishing temporary rules, suspending communications etc. The observing manager can only *observe* functions.

Only one person can have controlling privileges at a time using a special password. Others can function as observing managers only. This method avoids conflict in the company by keeping the number of users with controlling privileges to a minimum.

Note:

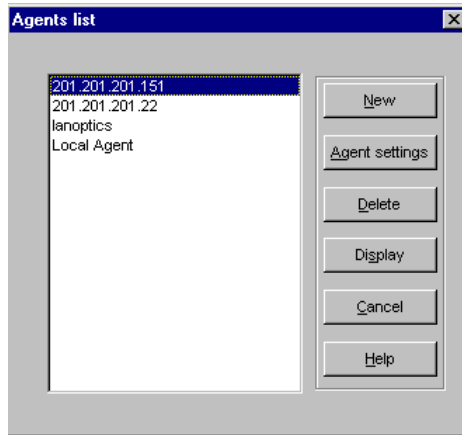
When there is no communications link with the Guardian agent, the Guardian logo appears in the Agent dialog box instead of the graph.

Inserting the IP Address and Data Encryption Key

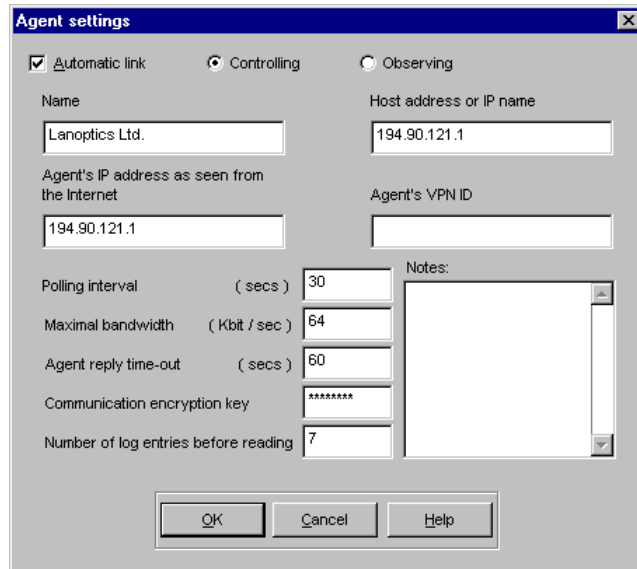
For first time installation of the agent, you will be prompted to change the encryption key. Insert any eight character key at the prompt.

► To insert the IP address

- 1 From the Main menu, choose the **Agents** option. The Agents List dialog box displays a list of the agents.



- 2 To view or edit an existing agent's settings, select the agent and click **Agent Settings**. To define a new agent, click **New**. The Agent Settings dialog box displays.



- 3 Select the Automatic Link box and then the Controlling or Observing option.
- 4 If the agent is new, insert its name.
- 5 Insert the agent's IP address in the Host Address or IP Name field.
- 6 Insert the IP address as seen from the Internet.
- 7 If you want to implement VPN, insert the agent's VPN ID number.
- 8 Click **OK** to save the information and close the dialog box.

Note:

When the manager establishes communications with a newly installed agent, it uses the default encryption key code. We strongly recommend that you change the default code after initial communications have been established.

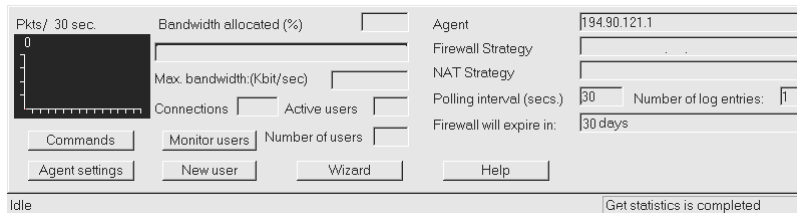
Establishing Initial Communications with the Agent

After you insert the agent's IP address and encryption code, you enter the Agent dialog box to establish initial communications with the agent.

► To display agent activity

- 1 In the Agents List dialog box, select the agent and click **Display**.

The Agent dialog box appears.



- 2 In the Agent dialog box, the Guardian logo will be replaced by a graph of the agent's activity. However, the graph remains black or displays red (indicating that all traffic is rejected) until a firewall strategy has been installed on the Guardian agent.

You now need to create a firewall strategy and install it on the Guardian agent. To simplify the process, we recommend that you use the wizard. Refer to *Chapter 5, Installing a Firewall Strategy and Creating and Editing a Firewall Strategy*.

Note:

If *Invalid key* appears on the status line, then an incorrect key was entered. Without the correct encryption key, the Guardian agents cannot decipher encrypted communications from the Guardian manager.

Warning:

No traffic will be able to pass the Guardian gateway until a firewall strategy is installed.

Changing the Default Encryption Key

To ensure maximum security, change the agent default encryption key code as soon as possible.

► **To change the default encryption code**

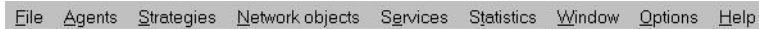
- 1 From the Main menu, choose **Agents**→**Agents list**. A list of agents appear.
- 2 Select the appropriate agent; click **Display**. The Local Agent dialog box appears.
- 3 Click **Commands**; the Commands dialog box appears.
- 4 In the Mode box, choose **Firewall**. The list of commands in the box change.
- 5 In the Commands box, choose **Set Encryption Key**.
- 6 Enter a new key code of up to 8 alphanumeric characters in the encryption key box. Verify it by retyping the key code.
The key code is case sensitive.
- 7 Click **Execute** to save the information and close the dialog box.

Guardian Main Screen

The Guardian main screen is composed of the following elements:

- Main menu bar
- Toolbar
- Alerts and Logs windows

Menu Bar



A brief description of the menu bar options follows:





Menu bar option	Action
File	Provides the Exit option to exit Guardian.
View	Controls the display of the real-time session monitoring window.
Agents	Defines new Guardian agents and edits the description of existing agents.
Strategies	Creates and edits firewall and NAT strategies, when appropriate.
Network Objects	Defines network objects that you use in the source and destination cells in your firewall strategy.
Services	Defines TCP, UDP or other Internet protocols and services.











Statistics	Displays statistics on network sessions.
Window	Performs tasks on the windows currently open (resizes, organizes etc.).
Options	Allows you to alter the display of the Guardian application.
Help	Provides online Help for the Guardian program, including keyword search and contents for easy access.





Toolbar



The toolbar contains buttons for quick access to frequently-used menu items. The following table lists and briefly describes the buttons.

Toolbar Button	Name	Action
	Agents list	Create, edit, open and delete agents.
	Firewall strategies	Create, edit and delete firewall strategies.
	NAT Strategies	Create, edit and delete NAT strategies.
	Network Objects	Create, edit and delete network objects.

Toolbar Button	Name	Action
	Services	Create, edit and delete services.
	Show statistics	Display or print statistics.
	Large icons	Create large icons for the agents in the Real-time Monitor window.
	Small icons	Create small icons for the agents in the Real-time Monitor window.
	List	Create list of users in the Real-time Monitor window.
	Details	Create detailed list of users in the Real-time Monitor window.
	Cascade window	Arrange windows so they overlap.
	Tile windows	Arrange windows as non-overlapping tiles.
	Arrange icons	Arrange icons at the bottom of the window.
	Arrange agents	Arrange the agents around the screen.

Toolbar Button	Name	Action
	Arrange agents with more information	Arrange agents around the screen with more information.
	Show alerts window	Display alerts window.
	Show Logs window	Display log window.
	About	Display program information.

Alerts and Logs Window

The Alerts window and Logs window are minimized on the bottom of the main screen.



A brief explanation of the Alerts and Logs windows follows.

Window	Does this
Alerts Window	Provides detailed information about possible unauthorized attempts to access the system.
Log Entries Window	Provides detailed information about Guardian's log entries and system users.

Basic Windows Skills

This manual assumes that you are familiar with the basic concepts of using Microsoft Windows NT. For information about using Windows NT, refer to your *Microsoft Windows NT User's Guide*.

Exiting Guardian

At the end of a session, exit Guardian as described below.

► **To exit Guardian**

- 1 From the Main menu, choose **File**→**Exit**.
- 2 Click **Yes** at the prompt in order to save modifications made during your session.

Performing Common Tasks

Introduction

This chapter is designed to provide step-by-step instructions for performing some of the more common tasks with the Guardian Manager. For more detailed descriptions of the dialog boxes, use Guardian's Online Help.

This chapter describes the following procedures:

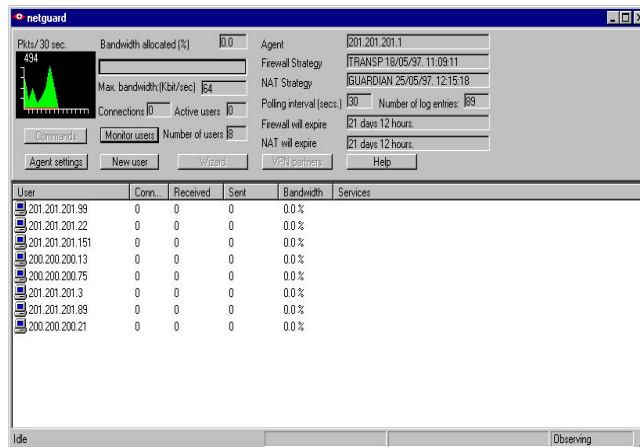
- Defining network objects
- Defining Internet services
- Creating, editing and installing a firewall strategy
- Creating, editing and installing a NAT strategy
- Viewing statistics
- Performing user authentication
- Creating a Virtual Private Network
- Monitoring user activity
- Limiting the amount of data per user
- Creating temporary rules

Monitoring Agents

When you install the firewall strategy, the Guardian automatically updates the contents of the Agent dialog box.

► **To display Guardian agent information**

- 1 In the Main menu, choose **Agents**. The Agents List dialog box displays.
- 2 Select the agent and click on **Display**. The Agent dialog box displays.



The graph in the upper left corner shows the action taken on the packets that passed through the Guardian gateway over a period of time. Green indicates packets that were passed through the gateway. Red indicates packets that were rejected or ignored. The total number of packets (passed, rejected and ignored) is shown in blue.

This graph is updated online at the agent's polling interval. The scale of the y-axis is adjusted automatically to accommodate the number of packets. The scale of the x-

axis represents the time in minutes with a maximum of approximately 10 minutes.

The Agent dialog box also displays the percentage of bandwidth utilization of the entire system and each monitored user. The calculation is based on the maximum bandwidth specified in the Agent Settings dialog box.

Monitoring User Activity

You can monitor the sessions in real time and view detailed information about a specific session.

Monitoring Real-time Sessions

You can monitor any of the network sessions in real time from the Agent dialog box.

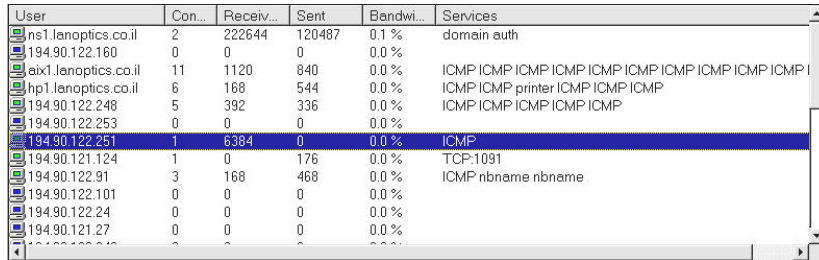
Note:

If you did not create the firewall strategy with the wizard, you must enter the networks you want to monitor in the Properties dialog box (accessed from the firewall strategy dialog box). See *Chapter 5, Creating or Editing Properties*.

► **To monitor a network session**

- 1 From the Main menu, choose **Agents**. The Agents List dialog box appears.
- 2 Select the agent that will be used for monitoring and click **Display**. Close the Agents List dialog box. The Agent dialog box displays.
- 3 In the Agent dialog box, click **Monitor Users/Hide Users** to toggle between viewing or hiding the real-time sessions.

The lower portion of the dialog box shows the real-time sessions for the monitored users.



User	Con...	Receiv...	Sent	Bandwi...	Services
ns1.lenoptics.co.il	2	222644	120487	0.1 %	domain auth
194.90.122.160	0	0	0	0.0 %	
eix1.lenoptics.co.il	11	1120	840	0.0 %	ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP I
hp1.lenoptics.co.il	6	168	544	0.0 %	ICMP ICMP printer ICMP ICMP ICMP
194.90.122.248	5	392	336	0.0 %	ICMP ICMP ICMP ICMP ICMP
194.90.122.253	0	0	0	0.0 %	
194.90.122.251	1	6384	0	0.0 %	ICMP
194.90.121.124	1	0	176	0.0 %	TCP:1091
194.90.122.91	3	168	468	0.0 %	ICMP nbname nbname
194.90.122.101	0	0	0	0.0 %	
194.90.122.24	0	0	0	0.0 %	
194.90.121.27	0	0	0	0.0 %	

In the real-time monitoring window, you can view the IP address or name, number of connections, bytes received, bytes sent (transmitted), percentage of the total bandwidth and services used for each of the monitored users.

If information is hidden in a column, increase the column's width by pointing at the column title and dragging when the cursor changes to a double-headed arrow.

Color Coding of Icons

The icons are color coded to indicate the status of the station. Green indicates that the station is active and blue indicates that it is inactive.

Manipulating the Real-time Monitoring Window

Toggle between **Hide Users** and **Monitor Users** to hide or display the Real-time Monitoring window in the Agents dialog box.

Use the options in the View menu, or icons in the toolbar, to alter the appearance of the user information. You can view either large icons, small icons, a list of the users or a detailed list of users.

To increase the width of a column, drag the column title.

Sorting the Monitored Users

You can sort the monitored users in the list by their name, number of connections, bytes received, bytes sent or percentage of the bandwidth being utilized.

Click on the title of the column that you would like to sort by. For example, to sort by the number of bytes received, click **Received** in the column title-bar.

Specifying Monitored Users

Networks are specified as monitored in the properties for a firewall strategy. All the users in this network will then appear in the monitored list of users in the real-time monitoring window. For further details, refer to *Chapter 5, Planning your Company's Firewall*.

Note:

After modifying the firewall strategy, it must be installed on the Guardian agent for the changes to take affect.

Adding New Monitored Users

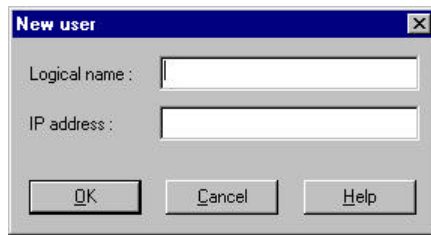
You can add individual users for monitoring purposes.

► **To add an individual user to the list**

- 1 In the Agent dialog box, click **New User**.

-or-

From the list of agents in the Agent dialog box, select a user and click the right mouse button. From the options that appear, choose **New User**. The New User dialog box appears.



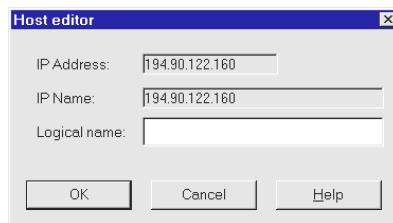
- 2 Type the username (optional) and the IP address.
- 3 Click **OK** to add the user.

Naming a Monitored User

You may replace the IP address of a monitored user with a name of your choice.

► **To rename the monitored user**

- 1 From the list of agents in the Agent dialog box, select a monitored user.
- 2 Click the right mouse button and choose **Edit User**. The Host Editor dialog box appears.



- 3 Type the new name and click **OK**.

Temporarily Deleting Inactive Users from the List

You can delete inactive users from the list in the Agents dialog box. At the next poll, the inactive users reappear.

► To delete inactive users from the list

- 1 From the list in the Agents dialog box, select a monitored user.
- 2 Click on the right mouse button and choose **Delete User** or **Delete All Users** from the options that appear.

If the deleted user(s) is inactive, it does not appear in the list. However, once the user(s) becomes active, it will reappear after the next polling of the Guardian agent.

All the users on the monitored networks appear in the list each time the dialog box is closed and reopened.

Monitoring Individual Sessions

You can view detailed information about an individual user's connections.

► **To view a specific user's sessions**

- ◆ From the list in the Agents dialog box, select a user and double click. A dialog box with the user's current sessions displays.

Host	Service	Sent	Received	Elapsed time	Bandwidth
dns.NetVision.net.il(...)	domain	1805416	2601672	146:17:02	0.8 %
nvsgj1.NetVision.net...	smtp	19501	262240	46:58:14	0.0 %
solomon.pacific.net...	domain	257	122	00:03:44	0.0 %
192.52.60.129	ICMP	0	504	00:03:37	0.0 %
ii.intel.com(143.185...	smtp	440	0	00:03:38	0.0 %
aurora.intel.com(143...	smtp	3019	848	00:02:38	0.0 %
194.90.1.52	smtp	1531	824	00:02:17	0.0 %
dns.NetVision.net.il(...)	domain	126	206	00:01:47	0.0 %
149.174.177.134	domain	342	245	00:01:44	0.0 %
128.139.6.1	domain	144	144	00:01:40	0.0 %
149.174.177.134	smtp	9476	51732	00:01:10	0.1 %
149.174.206.134	smtp	1874	14452	00:00:24	8.0 %

Suspending a Session

You can suspend a session via the dialog box above. This feature is useful, for example, when a session utilizes a large percentage of the bandwidth.

► **To suspend a real-time session**

- 1 Display a user's current session (see instructions above).
- 2 From the list of sessions, choose the session to suspend.

3 Click **Suspend Connection**.

-or-

Select an agent, click the right mouse button, and choose the Suspend option from the drop-down menu.

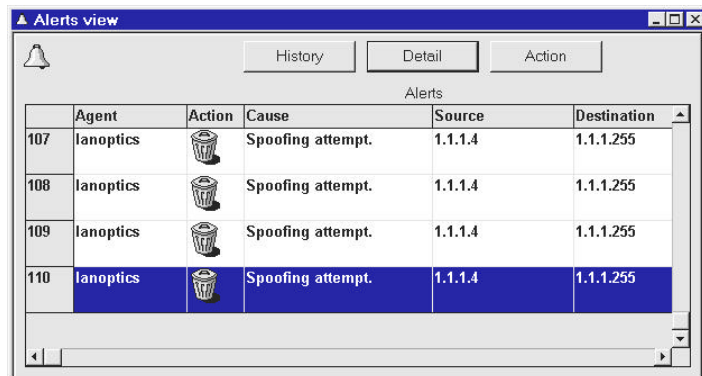
Reviewing Alerts and Logs

You can view alert and log entries online in the Alert window and Log window, respectively. These windows display all the alert/log entries for the current manager session. Previous entries are logged in the History until you delete them.

The Alert window and Log window are both minimized at the bottom of the screen upon entering the Guardian manager. To display the window, either click on the maximize button or use the Window menu.

► To display additional information about an entry

- 1 Maximize the alert or log window.
- 2 Double-click the entry, or select the entry and click **Detail**. The Alerts view dialog box displays.

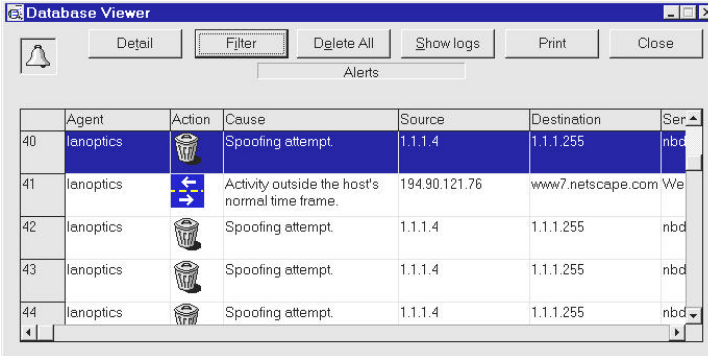


Reviewing the Alert and Log Histories

Alerts and log entries from previous manager sessions are saved until you delete them.

► To review the history

- 1 Maximize the alert or log window.
- 2 In the alert or log window, select a session.
- 3 Click **History**. The Database Viewer displays.



The screenshot shows a window titled "Database Viewer" with a menu bar containing "Detail", "Filter", "Delete All", "Show logs", "Print", and "Close". Below the menu bar is a "Alerts" label. The main area contains a table with the following data:

	Agent	Action	Cause	Source	Destination	Ser
40	lanoptics		Spoofing attempt.	1.1.1.4	1.1.1.255	nbd
41	lanoptics		Activity outside the host's normal time frame.	194.90.121.76	www7.netscape.com	We
42	lanoptics		Spoofing attempt.	1.1.1.4	1.1.1.255	nbd
43	lanoptics		Spoofing attempt.	1.1.1.4	1.1.1.255	nbd
44	lanoptics		Spoofing attempt.	1.1.1.4	1.1.1.255	nbd

- 4 From the Database Viewer you can delete entries, view details and print the history.

Filtering Alerts and Log Entries

You can filter the entries that are displayed in the main screen and History dialog box. This only affects the display of the alerts. All alerts will be logged in the database file regardless of the filter settings.

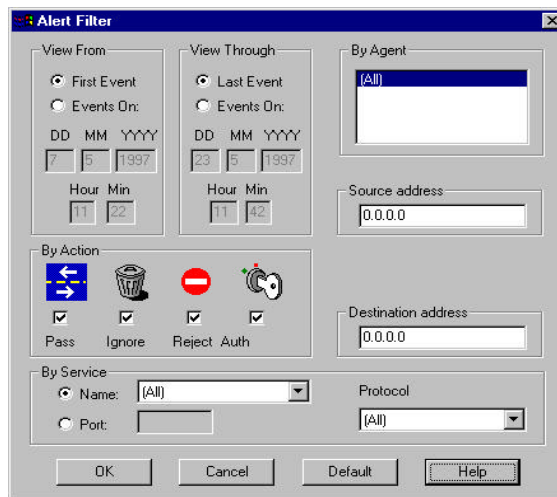
Alerts and log entries may be filtered by several criteria. You may use any combination of these. Filter entries according to:

- The date and time that they occurred.

- Type of action taken on the packet that generated the alert or the reason that the log entry was generated.
- The Guardian agent that reported the entry.
- The source and destination address of the packet that generated the entry.

➤ **To filter the entries displayed**

- 1 In the Alert window or Log window, click **History**. The Database Viewer dialog box appears.
- 2 In the Database Viewer dialog box, click **Filter**. The Alert Filter or Log Filter dialog box displays.



A description of the filtering options in the Alert Filter dialog box follows.

Filtering by Time

You can filter the alerts according to the date and time they occurred.

► **To filter by time**

- 1 In the View From section of the Alert Filter dialog box, click **Events On**.
- 2 Type the start date and time.
- 3 In the View Through section of the dialog box, click **Events On**.
- 4 Type the end date and time.

Filtering Alerts by Action

Use the check boxes to select which of the actions will be displayed in the Alert window.

Filtering Log Entries by Their Type

Use the check boxes to select which of the log types will be displayed in the Log window.

Filtering by Internet Service

Select the Protocol of the service and either the name or port number by which to filter the display.

Filtering by Agent

Enter the name of the reporting agents by which to filter the display.

Filtering by Address

Enter the address of either the source object and/or destination object by which to filter the display.

Limiting the Amount of Data Per User

You can limit the amount of data that can be sent by a user.

► **To limit the amount of data**

- 1 From the Main menu, choose **Network objects**. The Network objects dialog box appears.
- 2 In the Network objects dialog box, click **Edit**. The Host dialog box appears.
- 3 Click **Enable traffic control**. Specify the amount of data allowed per user in Kbytes in the appropriate box.
- 4 Decide the Action to be taken when the traffic limit is exceeded: Pass with Alert, or Pass with Log, or Suspend.

If you choose Suspend, you must also enter:

- Time in minutes to suspend communications for the user,

-or-

- Suspend with Alert, or
- Suspend with Log.

- 5 Click **OK** to implement the limitation.

Defining Network Objects

By defining network objects, you can greatly reduce the number of rules in your firewall strategy. You need to define both network objects, such as hosts, gateways, routers and networks, as well as network services.

Defining a New Network Object

If you used the wizard to create a firewall, then it has already created some network objects for you. Follow the instructions below to define additional network objects.

► **To define a new network object**

- 1 From the Main menu, choose **Network Objects**. The Network Objects dialog box displays.

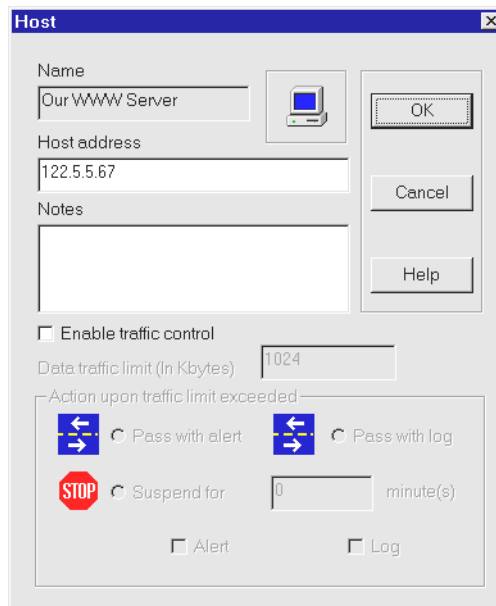


- 2 Click **New**. The New Object dialog box appears at the bottom of the Network Objects dialog box.

The New Object dialog box displays the types of network objects you can add.

- 3 Click the type of network object you want to define. The relevant dialog box displays.

For example, if you selected host, the Host dialog box displays.



- 4 Insert the name and host address that you want to assign to the host object.
- 5 Click **OK**.
- 6 Repeat the steps to define all the network objects that you need to create a firewall strategy.

The table below provides a description of the network objects.

Network Object	Type	Usage
Host	H	Define one IP address.
Range	R	Define a consecutive range of IP addresses.
Network	N	Define an entire network.
User	USE R	Define a remote user.
Group	G	Define a selection of several unrelated network objects (except users).
User Group	G	Define a group of objects.

Modifying an Object's Definition

You can modify an object's definition to update information. Depending on the type of object, you can change the object name, IP address, etc.

► To modify an object's definition

- 1 In the menu bar, choose **Network Objects**. The Network Objects dialog box displays.
- 2 Select the object you want to modify and click **Edit**. (The types of network objects displayed are determined by the check boxes selected.)
- 3 Modify the information and click **OK**.

Deleting an Object's Definition

Follow the instructions below to delete an object's definition from the database.

► **To delete an object's definition**

- 1 From the menu bar, choose **Network Objects**. The Network Objects dialog box displays.
- 2 Select an object and click **Delete**. (The types of network objects displayed is determined by the check boxes selected.)

Defining Internet Services

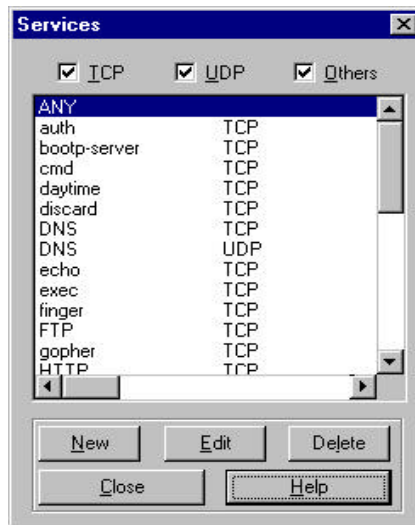
Guardian allows you to control access to and from the Internet, not only based in the source and destination of each session, but also according to the service requested. Guardian comes with numerous services already defined. You can either edit these existing services or add new ones.

Defining a New Service

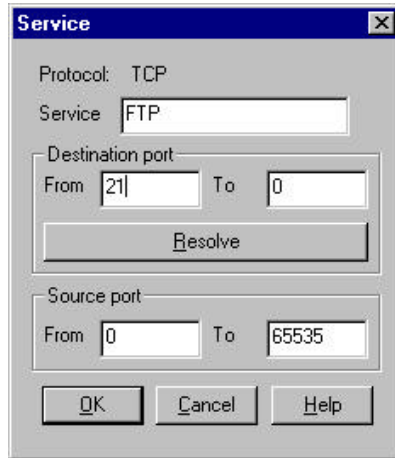
You can add new services to the list as they are introduced to the Internet.

► **To define a new service**

- 1 From the Main menu, choose **Services**. The Services dialog box displays.



- 2 Click **New**. A dialog box appears with two types of network services - TCP and UDP. The third option, Others, allows you to add a new *protocol*.
- 3 Click on the service that you want to define. The Service dialog box displays.



- 4 Enter the service name, for example, FTP.
- 5 Click **Resolve**. If a service by this name is already defined in the services file in the system directory, its details will be inserted into the fields that follow.

If a service by this name is not already defined, insert the name that you want to allocate to the service, its destination port address and its source port address range.

If you would like to group multiple services, you can define them as a range. Or, you can limit the source port in the range.

- 6 Repeat the steps to define all the services required by your corporate security policy.

Modifying a Service's Definition

The Guardian manager is supplied with a list of most Internet services. You can modify a service's name, destination port and source port.

► **To modify a service's definition**

- 1 From the Main menu, choose **Services**. The Services dialog box displays.
- 2 Select the service and click **Edit**. (Check boxes allow you to filter the types of services to display: TCP or UDP.)
- 3 Edit the service's destination port address range and its source port address range. You can limit these ranges as required.
- 4 Click on **OK**.

Deleting a Service's Definition

Follow the instructions below to delete a service's definition.

► **To delete a definition**

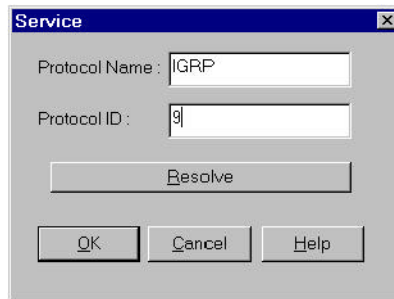
- 1 From the Main menu, choose **Services**. The Network Services dialog box displays.
- 2 Select a service and click **Delete**. A prompt appears.
- 3 Choose **Yes** to delete the service definition.

Defining a New Protocol

You can add a new protocol, or edit existing protocols.

► **To define a new protocol**

- 1 In the Services dialog box, click **New**. The Add Service dialog box displays.
- 2 In the Add Services dialog box, click **Others**. The Service dialog box appears.



- 3 In the Protocol Name field, assign a name which identifies the user.
- 4 In the Protocol ID field, assign the number of the protocol. This number can be assigned manually, or by clicking **Resolve** to examine the Protocol file for an existing protocol with the same name as the new protocol. If a protocol is found, its identification number is inserted in the Protocol ID field.

Modifying and Deleting a Protocol's Definition

Follow the instructions below to modify a protocol's definition.

➤ **To modify a protocol's definition**

- 1 From the Main menu, choose **Services**. The Services dialog box displays.
- 2 Select the protocol and click **Edit**.
- 3 Edit the protocol name and ID.
- 4 Click **OK** to save the new definition.

➤ **To delete a protocol's definition**

- ◆ Follow the instructions for deleting a service's definition. Instead of selecting a service, select a protocol.

Creating a Firewall Strategy

Guardian assists you to create your own firewall strategy (filter) or modify the one supplied. For detailed instructions on creating and modifying a firewall strategy, refer to *Chapter 5, Planning your Company's Firewall*.

Creating a NAT Strategy

Guardian assists you to create your own NAT strategy. All the static and dynamic address assignment are combined create a NAT strategy. The network administrator can modify the NAT strategy, by creating new assignments or editing existing ones. For detailed instructions on creating a NAT strategy, refer to *Chapter 6, Network Address Translation*.

Creating a Virtual Private Network (VPN)

The inflexibility and cost of dedicated point-to-point connections between networks, has led to the use of Virtual Private Networks. VPNs utilize some public segments for communication. This system enables a company to communicate via the Internet, a process which simplifies and speeds up connection to any destination around the world.

The main disadvantage of VPNs, is that the public segments are often insecure. This could result in unauthorized access to, and monitoring of, the private network.

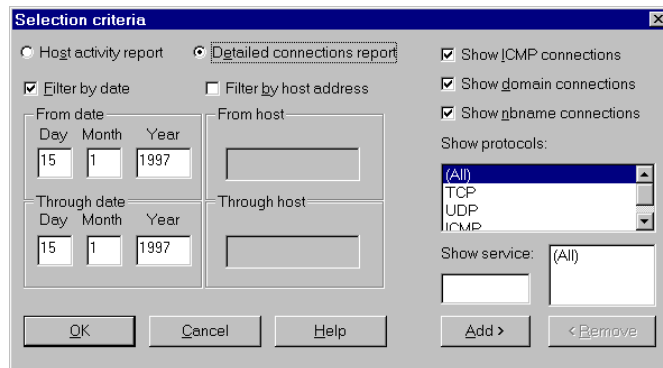
Guardian provides a solution to this problem by encrypting data for it's passage through the network. The method of encryption, and instructions on how to encrypt the data, are described in more detail in *Chapter 8, Virtual Private Networks*.

Viewing Statistics

You can view two reports via the Statistics menu: the host activity report which displays details of sessions for all hosts, and the connections report which displays connections for a specified time period.

► **To view statistics**

- 1 From the Statistics menu, choose **Show Statistics**. You can also click the graph button in the toolbar. The Selection Criteria dialog box appears.



- 2 Click the report you want to view: host activity or detailed connections report.
- 3 Fill in the parameters available for the specific report. Choose **OK** to generate the report.

Creating Temporary Rules

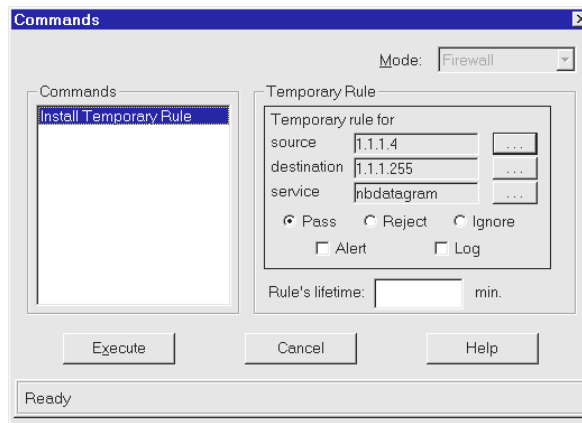
The procedures described in this section are usually not required in the daily operation of Guardian. However, they may be useful in emergency situations.

You can create a temporary rule immediately without having to enter and edit your filter. For example, a temporary rule can stop unwanted packets from passing the gateway or grant someone temporary access to the Internet.

From the Alert or Log window in the main screen, choose the event that most closely corresponds with the temporary action that you are going to create. For instance, if you wish to stop packets from passing between a certain source and your local network, click on the event notifying you of their passage, if there is one.

► To create a temporary rule

- 1 In the Alert or Log window, select an event from the list.
- 2 Click the **Action** button. The Commands dialog box appears.



- 3 In the Commands dialog box, change the Source, Destination and/or Service by clicking on the box to the right.
- 4 Select the action to be taken: pass, reject or ignore.
- 5 Select the notification type: alert or log.
- 6 Insert the time in minutes that the temporary rule will be active. After this time, it is automatically deleted.
- 7 Click **Execute**. Verify that the operation was successful in the status line, at the bottom of the dialog box.

Suspending All Internet Communications

You can suspend all Internet communications.

Caution:

Reserve using this command for emergency situations.

► **To suspend all communications**

- 1 In the Agent dialog box, click **Commands**. The Commands dialog box displays.
- 2 From the Commands dialog box, choose Suspend Operations.
- 3 Click **Execute**.
- 4 Verify that the operation was successful in the status line.

Use the Resume Operations command to restore communications with the Internet. The graph for this agent, in the Agent dialog box, will be empty (black).

Planning Your Company's Firewall

What is a Firewall?

A firewall is a software product located between the router and the Internet which secures a company's private LAN. Guardian assists you in building a firewall strategy based on your corporate security considerations. For example, you may decide to filter your company's communications for security reasons and for traffic control purposes. To achieve this, you determine which communications will be prohibited and the actions to be taken. This comprises your firewall strategy.

Security Types

Instead of relying on a single type of system, as in many other firewall products, Guardian provides several levels of security. All of these combine to restrict unwanted entry into your network.

Application-level

Guardian features built-in security functions at the application and protocol levels. These provide for protection even for complex protocols such as FTP and RPC.

Guardian solves the following security problems:

- With Telnet protocol there is no built-in way to detect attempts to invade the system. This is due to the fact that most Telnet sessions are not broken after several unsuccessful attempts to enter a valid password. Guardian keeps track of all short Telnet sessions (port 23) and checks user data for one of the following words: Invalid, Incorrect, Bad, Sorry or Failed.
- With User Datagram Protocol (UDP), communications are connectionless and inherently difficult to protect. Since UDP communications are always query/response, each outbound packet should be accompanied by an inbound packet. By maintaining a UDP “connection”, Guardian filters any unexpected UDP packets. It is much easier to spoof UDP packets than TCP packets, since there are no handshakes or sequence numbers.

Real-time Monitoring

You can monitor all network sessions in real time. This includes details on the number of bytes sent, number of bytes received, percentage of the total bandwidth and services used. If necessary, you can even terminate a session online.

Monitoring of Suspicious Events

This is a built-in system which allows the run-time monitoring of suspicious events in the system. You can set the threshold for these events and determine the action to be taken.

Suspicious events include:

- Multiple short TCP sessions (possibly someone attempting access).

- Unusual log on times (does someone really need to log on at 3:00 am?).
- Multiple failed password attempts in FTP and Telnet (maybe he mistyped the password, but not 17 times!).

Statistical Files

Guardian produces extensive statistical data based on monitoring of the gateway.

Log Files

All actions taken, based on all the security levels, are logged according to your specifications. Log entries can then be filtered to enable further precision. Not only does the log provide a history of the actions taken, but it can also be reviewed to search for anything amiss.

Security Considerations

Each corporation must develop a security policy based on its own specific needs. This section attempts to highlight some of the more common security considerations.

- Decide what is and what is not permitted. The business and structural need of the organization might restrict the personal use of corporate computers.
- Do you want to restrict *outgoing* traffic to guard against employees exporting valuable data? There are technological considerations such as whether a specific protocol be barred from use because it poses a security risk.
- If unauthorized access from the outside concerns you, you can monitor *incoming* requests.

To reduce risks, Guardian is designed to prohibit all communications that you have not explicitly made allowable.

How Filtering Works

Each firewall strategy (filter) is composed of a series of sequential rules starting with #1. Each packet is screened according to these rules beginning with rule 1, followed by rule 2, rule 3, etc. If the packet meets one of the rules, then Guardian deals with the packet as the rule stipulates. If none of the rules in the firewall strategy are met, then Guardian ignores the packet. The sequential order of rules is very important when creating a firewall strategy. Only the first rule that matches the packet will act upon it.

If none of the rules are met, the packet is ignored.

Considerations for Firewall Design

The construction of your firewall strategy depends upon your company's security policy. However, it is important to keep the following principles in mind:

Remember that all communications that are not expressly allowed are prohibited.

- **Limit your rules to those that are necessary.** Since every frame is checked against every rule, limiting the number of rules will greatly improve filter performance.
- **Place the rules that will be used most frequently at the top of the firewall strategy.** This will improve filter performance by reducing the number of rules that the frames are checked against.

- **Limit services to those that are necessary.** If you only need e-mail, then make sure that it's the only service allowed.

- **Limit the destinations.** If you have a mail server, allow access to the mail server only and not to every address on your network.
- **Limit access to the hosts in your network.** If you're using the Internet as a corporate backbone, only allow your other sites to access your host using FTP.
- **Limit access to your host to standard days and times.** Take into account holidays and time zones. Should you really allow access at 3:30 A.M. Sunday mornings? Maybe yes, if you have offices in the Far East; probably not, if you have no dealings outside your time zone.
- **Control traffic.** Not everyone in your network needs to send 50M over the Internet.

Installing a Firewall Strategy

The wizard enables you to create a basic firewall strategy for the servers on your network. The wizard automatically defines network objects for your servers based on the IP addresses that you supply and inserts these network objects into rules.

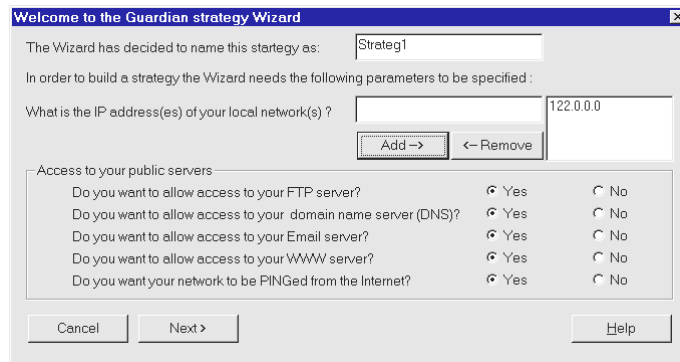
► **To create a firewall strategy using the wizard**

- 1 In an open Agent dialog box, click **Wizard**.

-or-

From the Menu bar, click **Agent**; the Agents List dialog box appears. Select the agent on which you want to install the wizard's firewall strategy; click **Display**. The Agent dialog box appears. Click **Wizard**.

The first Firewall Wizard dialog box appears.



The wizard automatically assigns a name to the strategy. You may edit the name.

- 2 Use the **Add** and **Remove** buttons to insert the IP address(es) of your local network(s).

- 3 Select the public servers that are installed on your network and click **Next**; the next Firewall Wizard dialog box appears.

Public server(s)

IP address(es) of your network(s): 122.0.0.0

Please specify the IP address(es) of your public server(s):

	IP Address	Object Name
Your FTP server is	<input type="text"/>	Our FTP Server
Your DNS server is	<input type="text"/>	Our DNS Server
Your Email server is	<input type="text"/>	Our Email Server
Your WWW server is	<input type="text"/>	Our WWW Server

< Back Next > Cancel Help

- 4 Insert the IP addresses for the servers on your network. You may modify the name that Guardian automatically assigns to each of these network objects.
- 5 Click **Next**; the next Wizard dialog box displays.

Complete the strategy Wizard

The Guardian Wizard has built the following strategy for you:
All hosts in your network will always be able to access any host in the Internet for any services.

You FTP server (122.0.0.1)
You DNS server (122.0.0.2)
You EMAIL server (122.0.0.3)
You WWW server (122.0.0.4)

Your network will be accessible by the ICMP protocol from the Internet.
Please remember: The Wizard has built a basic strategy which may satisfy the most common security requirements. In order to build more sophisticated strategy please use the Strategy Editor.

Press to review/edit the strategy built by Wizard.

< Back Finish Cancel Help

- 6 Click **Finish** to create the basic firewall or **Edit** to modify the information you entered.

- 7 At the prompt, click **Yes** to install the firewall strategy on the Guardian agent. A message appears notifying you that the installation was successful.

The name of the firewall strategy appears in the Firewall Strategy field in the Agent dialog box.

Warning:

The firewall strategy will not come into effect until it is installed on the Guardian gateway.

Creating and Editing a Firewall Strategy

Guardian assists you in making your own firewall strategy (filter) or modifying the one supplied. This section provides instructions for *generating* rules and filters. For hints and conceptual considerations on *designing* rules and filters, refer to the section *Considerations for Firewall Design* earlier in this chapter.

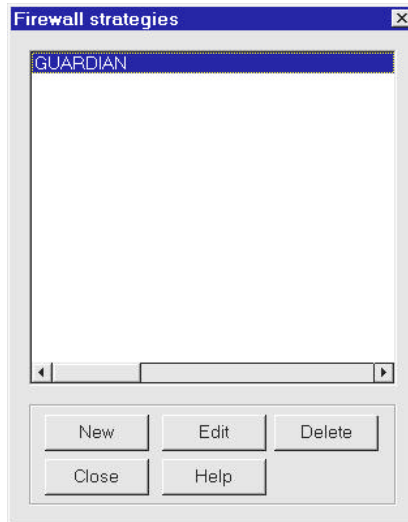
The rules are all shown in a clear table format. Each line is a rule. The rules are numbered sequentially beginning with rule 1. Each rule is divided into the following cells: Source, Destination, Service, Apply at, Action and Comments.

Creating a Rule

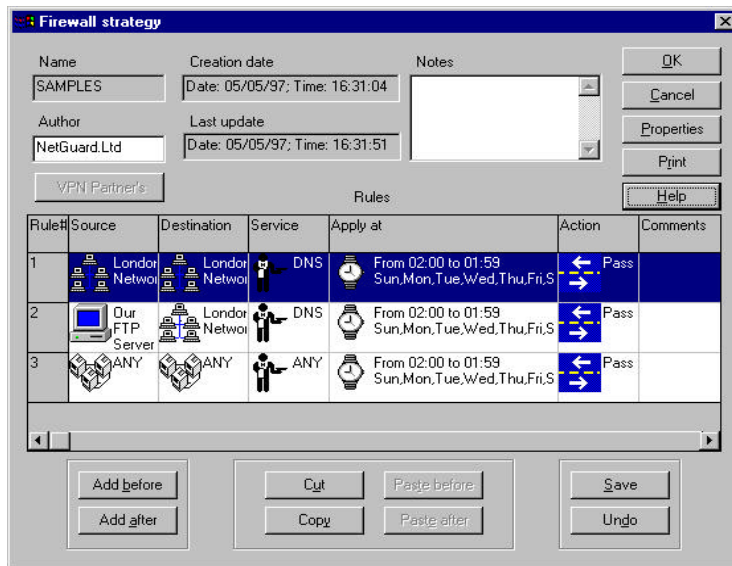
All the rules are combined to create the firewall strategy (filter). The administrator can modify the firewall strategy, by creating new rules or editing existing ones.

► **To create a rule**

- 1 In the menu bar, choose **Strategies** → **Firewall Strategies**. The Firewall Strategies dialog box appears.



- 2 In the Firewall Strategies dialog box, click **New**. A firewall strategy list appears.
- 3 From the list, select a firewall strategy and click **Edit**. Alternatively, double-click the strategy on the list. The Firewall Strategy dialog box appears.



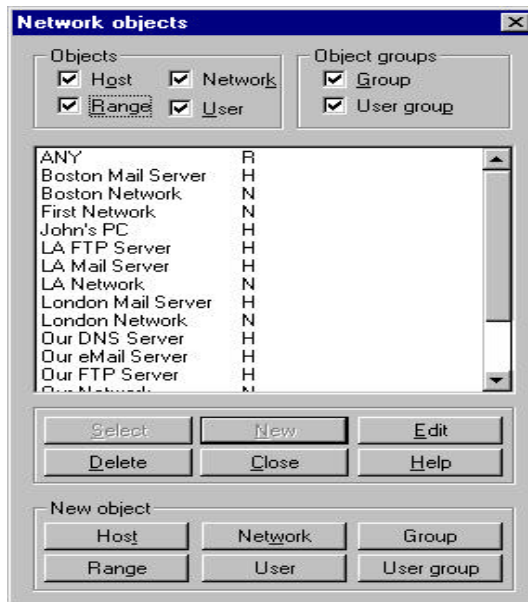
- 4 Assign a name for the new firewall strategy. You may insert your name as the firewall strategy's author and add notes.

Inserting a Source and Destination

You determine the source and destination of the communication packets in the Firewall Strategy dialog box.

► To insert a source and destination in the cells

- 1 Double click the Source cell in Rule #1. The Network Objects dialog box displays a list of the network objects that you have defined. (The types of network objects displayed is determined by the check boxes selected.) You also define a new network object or edit an existing definition from here.



- 2 In the Network Objects dialog box, double-click a network object to insert it into the Source cell. Alternatively, select an object and click **Select**. The Network Objects dialog box closes.

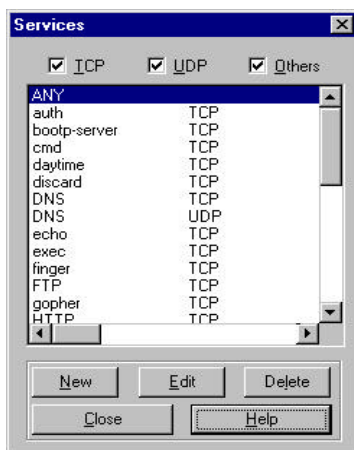
- 3 Double-click the Destination cell in Rule #1. The Network Objects dialog box displays a list of the network objects that you have defined. (The types of network objects displayed is determined by the check boxes selected.) You can also define a new network object or edit an existing definition from here.
- 4 In the Network Objects dialog box, double-click a network object to insert it into the Destination cell. Alternatively, select an object and click **Select**. The Network Objects dialog box closes.

Inserting a Service

You insert new services or edit existing services such as TCP or UDP from the Firewall Strategy dialog box.

► **To insert a service in the cell**

- 1 Double-click the Service cell in Rule #1 in the Firewall Strategy dialog box. The Services dialog box displays a list of the network objects that you have defined. (The services displayed is determined by the check boxes selected.) You can also define a new service object or edit an existing definition from here.



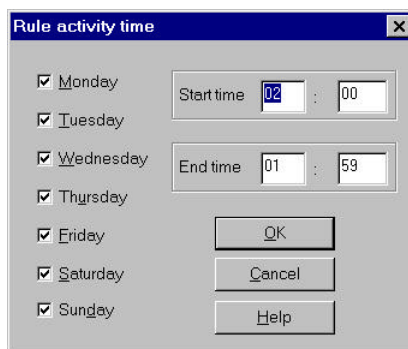
- 2 Double-click a service to insert it into the Service cell or choose a service and then click **Select**. The Services dialog box closes.

Changing the Default Time Frame

The default settings in the Apply At cell make the rule active all the time.

► To change the time frame

- 1 Double-click the Apply At cell in Rule #1. The Rule Activity Time dialog box appears.



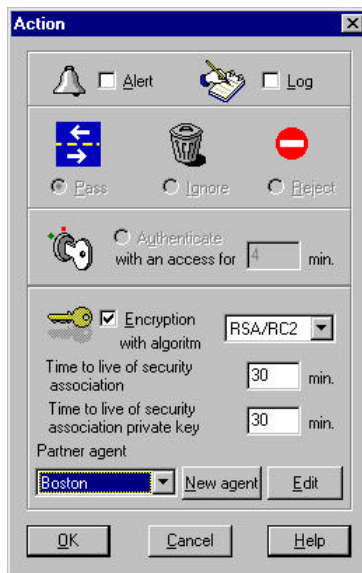
- 2 Enter the time and day when this rule will be active. Click **OK** to save the information and close the dialog box.

Changing the Action to be Taken and Notification

When a rule is applied to a packet, the rule determines whether the packet will be passed, ignored or rejected. The notification method can be alert, log or both. By default, all frames meeting the rule will be passed without notification (Pass).

► **To change the action and notification**

- 1 Double click the Action cell in Rule #1. The Action dialog box appears.



- 2 Choose the action that will be taken on every packet that meets this rule.
- 3 Choose the notification method.
- 4 Click **OK** to save the new parameters.

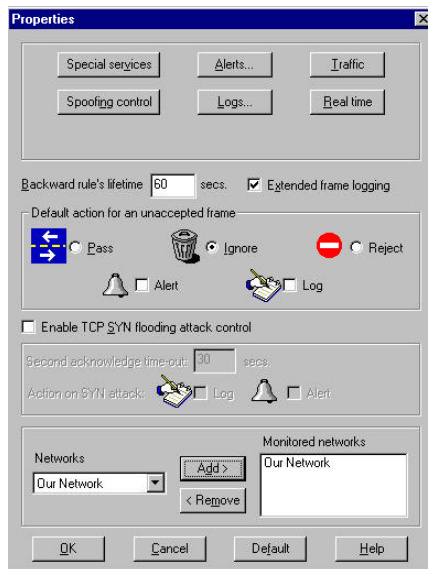
Creating or Editing Properties

Properties affect aspects of the agent such as the alert mechanism, the activation of built-in security mechanisms, traffic limitations and networks to be monitored.

Properties are downloaded with the filter to each agent.

► To create or edit properties

- 1 In the Firewall Strategy dialog box, click **Properties**. The Properties dialog box appears.



- 2 In the Networks box, select the Network objects you want to include or delete from the monitored networks. Click **Add** or **Remove**.

Monitor real-time sessions of all the network via the real-time monitoring window in the Agent dialog box.

- 3 Click **OK** to save the information and close the dialog box.

Inserting Additional Rules

You can insert additional rules in any order in the dialog box. Remember that the sequential order of rules in the firewall strategy is important. Only the first rule that matches the packet is carried out.

➤ **To insert additional rules in the firewall strategy**

- 1 In the Firewall Strategy dialog box, click **Add After** to insert a line for the next rule (Rule #2) or click **Add Before** to insert a line for a new rule above Rule #1.
- 2 Continue to create all the rules in the firewall strategy.

Cutting, Pasting and Copying Rules

Rules can be cut, copied and pasted.

➤ **To cut a rule**

- ◆ Select the rule and click **Cut**.

➤ **To paste a rule**

- 1 Select the rule which will precede or follow the rule you want to paste.
- 2 Click **Paste before** or **Paste after**.

➤ **To copy a rule**

- 1 Select the rule and click **Copy**.
- 2 Paste the rule in its new position.

Saving the Firewall Strategy

Click on **Save** to save the information and close the dialog box.

Modifying an Existing Rule

You can modify the cell entries in rules by double-clicking the cell.

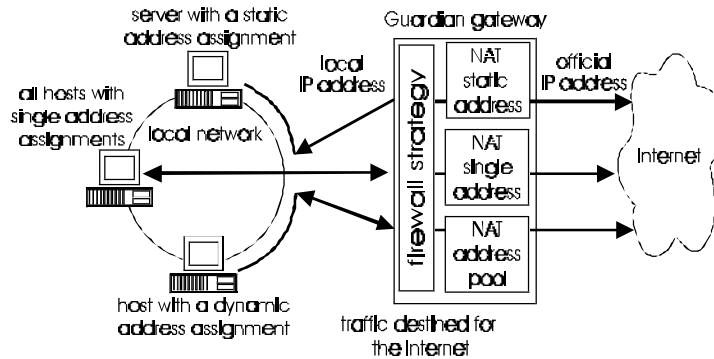
Network Address Translation

What is NAT?

Network Address Translation (NAT) is an optional Guardian application that provides flexible and secure IP addressing for your local network. NAT enables you to maximize your assignment of network addresses by dynamically mapping official IP addresses to local addresses. Since a vast majority of stations in an organization, except servers, only require access to the Internet on a temporary basis, they do not all require official IP addresses and can use a local IP addressing system. NAT provides all of these stations with an official address from a pool of official addresses as required. The operation of NAT is completely transparent to the Internet, the stations and all applications.

You can assign each TCP/IP host in your network with either a static address (a permanent IP address) or assign a group of hosts dynamic addresses (shared official addresses from a pool) depending upon your own requirements. Alternatively, you can assign all your hosts a single official IP address.

You can also assign differing priority levels to hosts. Should all your hosts attempt to access the Internet simultaneously, there would be insufficient official addresses to go around. Although this situation is unlikely with the 256 addresses in a Class C network, access would then be distributed to hosts with the highest priority levels.



The figure above displays three examples of network traffic. For traffic on the internal network only, local IP addresses are used. For traffic from a TCP/IP host on the local network to a device on the Internet:

- Packets from hosts with static address assignments are routed via their permanent official IP addresses for all communications. This could represent their Web server, mail server or any dedicated workstation.
- Packets from hosts with dynamic address assignments are routed via the NAT agent on the Guardian gateway. The NAT agent modifies the packet to replace the local IP address with an official Class C address from the pool.

All the hosts in a company with a single address assignment will appear to the outside as a single address.

The NAT agent also enables return communications from the Internet. Addresses are returned to the pool at the end of each Internet session, as well as periodically for increased security.

Features

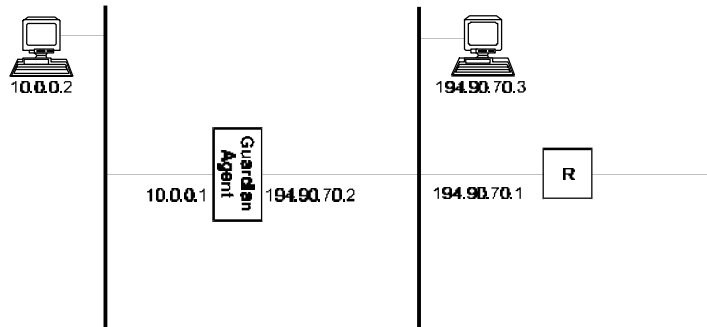
Use of the Guardian NAT agent provides many benefits. The list below contains some NAT agent features:

- Maximizes the use of your official IP addresses. Stations that do not have continuous communications with the Internet are automatically given an official IP address from the pool as required.
- Pools official IP addresses and distributes them on a priority basis. You can define the priority for each station or group of stations. If necessary, a high priority station will disconnect a lower priority one to access the Internet.
- Servers used for mail, FTP and Web can all be given a static (permanent) official IP address. Outsiders are only given easy access to the servers they need.
- Uses a local addressing system which renders your internal network invisible to the public. Outsiders will have no way of obtaining a list of your internal IP addresses.
- Increases network security.
- Allows you to reconfigure the network without having to change your TCP/IP addressing.
- Enables you to change your official IP addresses without having to reconfigure an existing TCP/IP network station by station.
- Saves both the expense and time involved in obtaining additional official IP addresses. Service providers can supply a client with single address assignment, instead of a Class C Internet.

- Ensures smooth enterprise growth by facilitating network expansion without acquiring new IP addresses or reconfiguring your network.
- Automatically reassigns addresses after a lapse in the transmission or receipt of frames without interrupting an open session. This is a further security measure which prevents outsiders from learning your internal addresses.
- Enables reply frames within a specified time period. NAT manipulates the source and destination addresses in the headers to assure that frames reach the station with the assigned address.
- Enables stations with internal IP addresses to automatically access the Internet with an official IP address without any system reconfiguration.
- Enables the assignment of priorities with dynamic NAT assignments. Thus, if you have a limited number of official IP addresses, you may determine which hosts are given priority assignments.

Implementing NAT

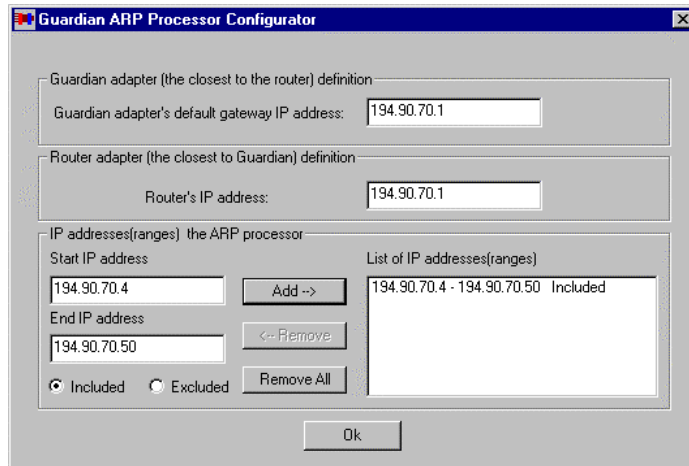
This section provides a sample of how NAT may be implemented in a network.



In the example, the company has an internal network 10.0.0.0, a range of official IP addresses from 194.90.70.4 to 194.90.70.50 and a computer outside the firewall with address 194.90.70.3 which can access the Internet. As part of the installation, you create a separate network between the router and the Guardian Agent. Then, after installing the agent, you run the ARP processor.

► **To run the ARP processor**

- 1 In the Guardian folder, double-click the ARP Processor icon. The Guardian ARP Processor Configurator dialog box appears.



- 2 In the Guardian Adapter's Default Gateway IP Address field, type the default gateway's IP address for the LAN adapter, connected with router R to the separate network 194.90.70.1.
- 3 In the Router's IP Address field, type the IP address of router R: 194.90.70.1.
- 4 Click **OK** to implement NAT.

Creating and Modifying a NAT Strategy

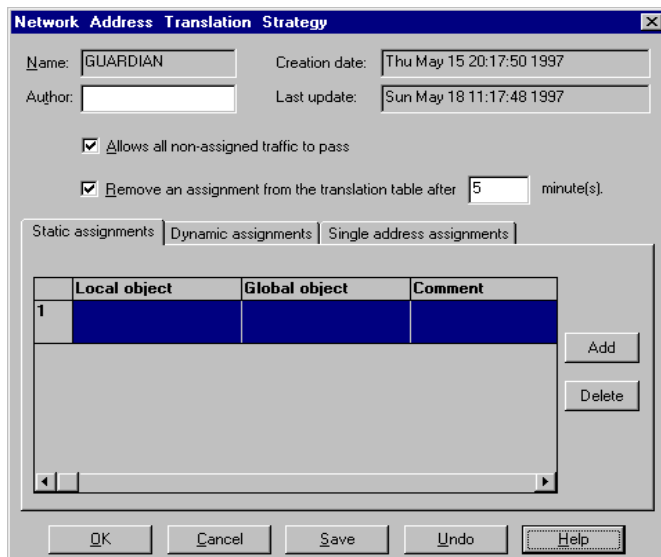
Guardian assists you in making your own NAT strategy. All the static and dynamic address assignments are combined to create a NAT strategy. The network administrator can modify the NAT strategy, by creating new assignments or editing existing ones.

► **To create a NAT strategy**

- 1 In the menu bar, choose **Strategies**→**NAT Strategies**. The NAT Strategies dialog box displays.



- 2 In the NAT Strategies dialog box, click **New**. A list of NAT strategies appears.
- 3 From the list, choose a NAT strategy and click **Edit**. Or, double-click a strategy. The NAT Strategy dialog box displays.



- 4 Type a name for the NAT strategy you are creating. You may insert your name as the author.
- 5 Type the IP address of your official Class C network (global network). You may now assign any or all of the 256 IP addresses.

Making Static Assignments

The Static Assignment area of the NAT Strategy dialog box is used to create a list of static address assignments for host objects. Examples of host objects are an FTP server, Web server and Domain Name Server, that permanently require an official IP address. Each host object (local IP address) should be linked to a single global object (official IP address). Static address assignments will always take priority over dynamic address assignment.

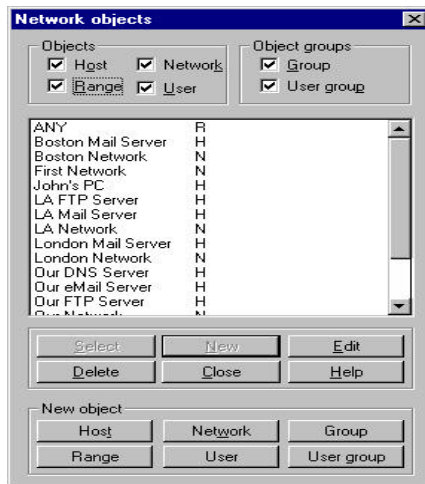
To define static address assignments, verify that the Static Assignment radio button is selected.

Inserting a Local Object and Global Object

A local object is a host object defined with a local (or internal) IP network address. A global object is a host object defined with an official IP network address. Global objects must have an address in the official IP network specified in the IP Address field.

► To insert local and global object in the cells

- 1 In the NAT Strategy dialog box, double-click the **Local Object** cell. The Network Objects dialog box displays with a list of the host objects that you have defined.



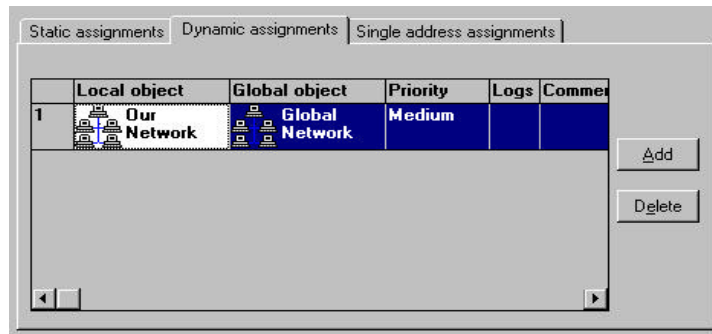
You can also define a new host object or edit an existing definition from here.

- 2 In the Network Objects dialog box, double-click a host object or, select an object and click **Select** to insert it into the Local Object cell. The Network Objects dialog box closes.
- 3 Double-click the Global Object cell. The Network Objects dialog box displays a list of the host objects that you have defined with an IP address in the official network. You can also define a new host object or edit an existing definition from here.
- 4 Double-click a network object in the Network Objects dialog box, or select an object and click **Select** to insert it into the Global Object cell. The Network Objects dialog box closes.

Making Dynamic Assignments

Use this table to create a list of dynamic address assignments for objects that do not require an official IP address on a permanent basis. Instead, these objects are assigned an address from a pool of official addresses. Assignment is performed as required on a priority basis. Each local host, range or network object (multiple local IP addresses) should be assigned a global host, range or network object (multiple official IP addresses).

To define dynamic address assignments, verify that the Dynamic Assignment radio button is selected. The table in the dialog box changes.



Inserting a Local Object and Global Object

A local object is a network object defined with a local (or internal) IP network address or several local addresses. A global object is a network object defined with an official IP network address or several official addresses. Global objects must have an address in the official (global) IP network specified in the IP Address field.

► **To insert local and global objects in the cells**

- 1 In the Dynamic Assignment screen, double-click the **Local Object** cell. The Network Objects dialog box displays a list of the network objects you have defined. (The types of network objects displayed are determined by the check boxes selected.)
You can also define a new network object or edit an existing definition from here.
- 2 In the Network Objects dialog box, double-click a network object, or select an object and click **Select** to insert it into the Local Object cell. The Network Objects dialog box closes.

Note:

Group objects cannot be used for defining dynamic address assignment.

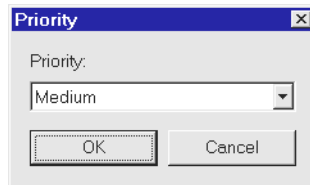
- 3 Double-click the **Global Object** cell. The Network Objects dialog box displays with a list of the network objects that you have defined with an IP address in the official network. (The types of network objects displayed is determined by the check boxes selected.)
You can also define a new network object or edit an existing definition from here.
- 4 In the Network Objects dialog box, double-click a network object, or select an object and click **Select** to insert it into the Global Object cell. The Network Objects dialog box closes.

Changing the Priority Level

By default all objects are assigned medium priority. If necessary, objects specified with a higher priority may replace lower priority objects to access the Internet.

► To change an object's priority level

- 1 In the Dynamic Assignment screen, double-click the Priority cell. The Priority dialog box displays.



- 2 From the drop-down list, choose the appropriate priority level for users assigned with this address. Click **OK**.

Enabling Log Notification

By default errors in address assignments are not logged. To enable log notification, double-click the Log cell. An icon representing a note-pad appears in the cell.

Removing an Address Assignment

You are able to remove an address assignment from the list of dynamic assignments.

► To remove an address assignment from the list

- If the assignments have not yet been saved, click **Undo**.
- If the assignments have already been saved, choose an assignment and click **Delete**.

Inserting Additional Assignments

- ◆ To insert another address assignment, click **Add** to insert a new line at the bottom of the table.

Modifying an Existing Assignment

You can modify the cell entries in an address assignment by double-clicking the cell.

Assigning a Single Address

You can create a list of single assignments for multiple objects that do not require an official IP address on a permanent basis by assigning them a single IP address.

Verify that the Single Address Assignment radio button is selected. To define single address assignments, follow the steps for static address assignments earlier.

Saving the Address Assignment Table

After modifying the address assignment table, we advise you to save the new parameters. The instructions below are to save both the static and dynamic address assignments.

► To save the address assignments

- 1 In the NAT Strategy dialog box, click **Save**.
- 2 Click **OK** to close the dialog box.

Installing the NAT Strategy

A NAT strategy must be installed (downloaded) on a Guardian agent for it to be operational.

► **To install the NAT strategy**

- 1 In the main menu bar, click **Agents**. Choose the name of the agent on which the NAT strategy will be installed and click **Display**. The Agent dialog box displays.
- 2 In the Agent dialog box, click on **Commands**. The Commands dialog box displays.
- 3 In the Mode drop down list, choose NAT.
- 4 From the list of available commands, choose **Install NAT Strategy**.
- 5 Use the arrow key to select the name of the NAT strategy to be installed.
- 6 Click **Execute** and check the status line to verify that the installation is successful.
- 7 Click **Cancel** to close the dialog box.

User Authentication

What is User Authentication?

User authentication provides a process which enables a mobile or remote user to access a predefined source in a protected network for certain services on a temporary basis.

For a more detailed explanation of user authentication, study the example below.

Example

A mobile user connects to the company's mail server to check for mail. If the mail server is located in the secured network behind a firewall, the mobile user needs a special rule that allows him to access the mail server. The rule in this situation may be: User's source IP address to Mail server allow POP3 and SMTP services.

The problem with this rule is that the user's IP address is unknown when the strategy is created. Moreover, the user's IP address is changed each time the mobile user connects to the Internet service provider. The solution to this problem, usually, is to allow access to the mail server for ANY source, therefore opening potential security "gaps" in the corporate firewall.

Another solution to the problem is to find a process that checks the user's identity. If the check is successful, the corporate firewall automatically opens a short-time channel to a predefined server, for a specific service.

An example of an authentication process is challenge/password based authentication. When the user tries to access the protected resource, the firewall requests a password. In the same query, the firewall sends a pre-agreed phrase (challenge) to the user. The challenge identifies the firewall which sent the request as “friendly”. The user enters the password, which is sent to the firewall for verification.

If the password is correct, according to the strategy, the firewall creates a temporary rule which allows the user to access the internal network.

One-time Password Authentication

The challenge/password authentication method has one significant weakness— each time the user is asked for a password, the same password is sent to the firewall. This means that anyone who is able to intercept the password may use it. The solution to this problem is a one-time password (OTP).

The OTP is valid only for the current session and will not be accepted the next time someone tries to gain access to the protected server. The next password cannot be predicted or calculated from the current password or even from the entire sequence of previous passwords.

To use OTP authentication, synchronized processes must be created on the firewall and on the mobile user’s computer. Synchronization is necessary to ensure that each time the legal user produces a new password, it will match the password expected by the firewall.

There are several products, incorporating special hardware, which produce a sequence of OTPs. The Guardian uses the OTP authentication method which evolved from the RFC 1938 (May 1996 by N. Haller

Bellcore and C.Metz Kaman Sciences Corporation). It is based on the fact that there is an irreversible hash function. In other words, a $P(i+1)$ password can always be produced from the $P(i)$ by applying the hash function to the $P(i)$; i.e. $P(i+1) = \text{HashFunction}(P(i))$.

However, there is no way to reverse the hash function. For example, the following is impossible:

$P(i) = \text{SomeFunction}(P(i+1))$. NetGuard uses the Message-Digest 5 (MD5) Algorithm as a hash function.

Authentication Process

Initializing the Authentication Process

The authentication process is as follows:

- Two sides participate in the authentication process—the client which runs on the mobile user’s computer, and the authentication server which is part of the firewall software.
- The user and the administrator generate the first password $P(0)$ together. The administrator creates a new user (see the section on Guardian Authentication) and chooses a challenge, a text phrase seen by the user each time authentication is initiated.
- The user chooses a secret phrase which he types each time authentication is required. The administrator doesn’t know this phrase. As an alternative, the administrator can supply the user with the secret phrase. The administrator’s challenge and the user’s secret phrase are combined to produce a 64-bit word which becomes the $P(0)$.

- The administrator enters the number (N) of times that the hash function will be sequentially applied to the P(0). This may be a large number, since it defines the number of the successful authentication acts that this specific user is allowed.
- The user initialization program then moves the P(0) through the hash function N times. The result, P(N), is stored on the firewall machine along with the user name, number N, challenge and prototype of the temporary rule for the user.

This concludes the initialization process.

Running the Authentication Program

Each time the mobile user wants to access an internal protected resource, he/she runs a client authentication program which works as follows:

- The program calls the authentication server which initiates the authentication process for this user (defined by the user name).
- The authentication server searches its user database for a definition of the user. If it finds a definition, it sends a challenge to the authentication client, along with the last number (K).
- The mobile user sees the challenge on the screen, checks it and if it is correct, enters the secret phrase. The secret phrase is combined with the challenge and a 64-bit initial password P(0) is produced.
- The initial password is moved through the hash function K-1 times and the result P(K-1) is sent back to the firewall.

- The firewall receives the P(K-1) and moves it through the hash function once. The result **MUST** be identical to the P(K) password stored for this user.

If the passwords are identical, the authentication is successful and the following process occurs:

- The latest correct password P(K-1) is stored in the database along with its number K-1. These values are used in the next authentication. An access confirmation message is sent to the client.
- A rule template is taken from the user database. The firewall fills an empty source IP address field in the rule with the current user's IP address and installs that temporary rule in the strategy.

The user is now able to contact the required server.

- When the temporary rule expires, the authentication process is repeated. If an incorrect password or no password is specified, the connection is closed.

Implementing Guardian Authentication

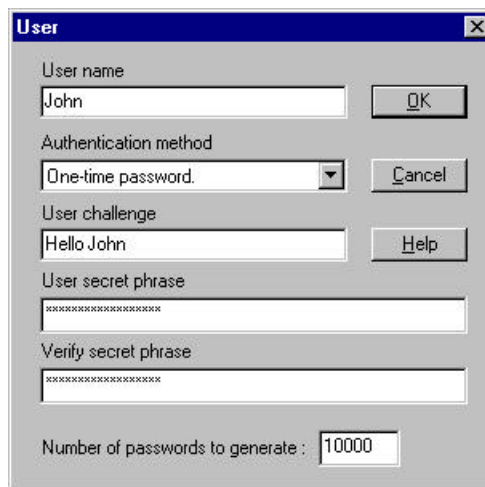
Authentication enables a mobile user access to certain services in the company's protected network (e.g. mail server) for a specified period of time. Two sides participate in the authentication process: the client which runs on the mobile user's computer, and the authentication server in the firewall software. To enable mobile user authentication, the administrator adds the mobile user to the network objects and firewall strategy in the protected network, and chooses an action for the packets.

Preparing the Network for User Authentication

The first step in authentication is to add the remote user to the existing network objects.

► **To add a new user to the network objects**

- 1 From the Main menu, select **Network Objects**. The Network Objects dialog box appears.
- 2 In the Network Objects dialog box, click **New**.
- 3 In the New Object dialog box, click **User**. The User dialog box appears.



The screenshot shows a dialog box titled "User" with the following fields and controls:

- User name:** A text box containing "John" and an "OK" button.
- Authentication method:** A dropdown menu set to "One-time password." and a "Cancel" button.
- User challenge:** A text box containing "Hello John" and a "Help" button.
- User secret phrase:** A masked text box (asterisks).
- Verify secret phrase:** A masked text box (asterisks).
- Number of passwords to generate:** A text box containing "10000".

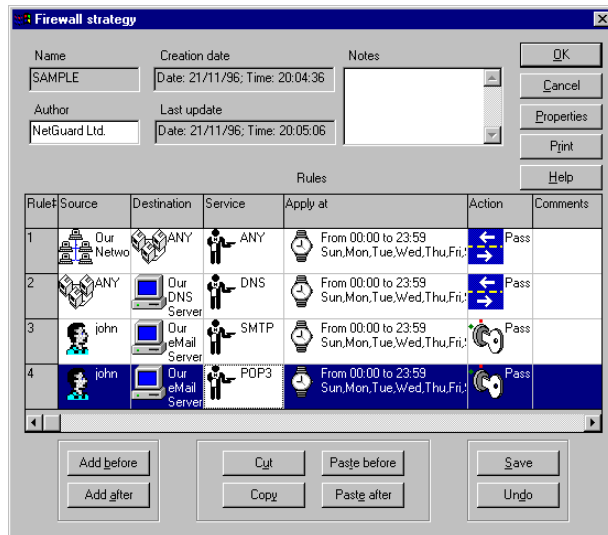
- 4 Type the required information. Click **OK**.

Modifying the Firewall Strategy

Create a rule for the remote user in the firewall strategy.

► **To modify the firewall strategy**

- 1 From the Strategies menu, choose **Firewall Strategies**. The Firewall Strategy screen appears.
- 2 Choose a strategy and click **New**. The following dialog box appears.



Note:

In rules 3 and 4 the user, John, is allowed to access the company's mail server via SMTP and POP3. The action is authenticated.

- 3 Double click **Action** in the related rule to change the action for a packet when this rule is met. The Action dialog box appears.



- 4 Choose the notification type: Alert or Log.
- 5 Choose Authenticate.
- 6 Type the amount of access time. Click **OK**.

In the above example, access is allowed for 30 minutes. After 30 minutes, the firewall initiates the authentication process again. If it fails, the rule will be removed.

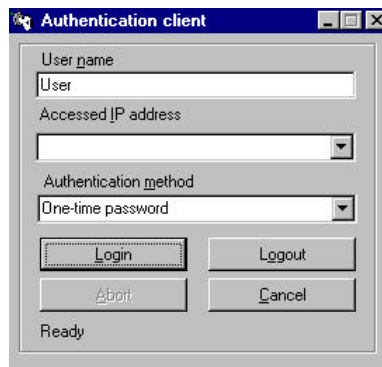
After loading the strategy, the agent is ready to accept the authentication requests.

Performing User Authentication

The instructions below guide the mobile user through the authentication process.

► **To perform mobile user authentication**

- 1 Run the authentication client program. The Authentication Client dialog box appears.



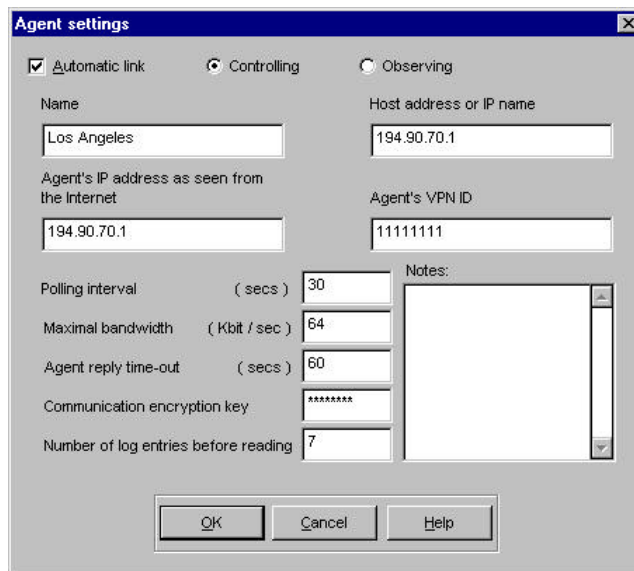
- 2 Enter the required information.
- 3 Click **Authenticate**. The client contacts the server.
- 4 At the prompt, type the secret phrase. If the phrase is correct, the firewall displays the Access granted message.

In the Client Authentication dialog box, the Accessed IP address is the IP address of the server that the user intends to contact, not the firewall itself.

Note:

To enable authentication, the firewall computer must be accessible to the client from the Internet. Therefore, if using the NAT, ensure that the firewall computer is defined as a static assignment in the NAT strategy.

Please note that a new entry appears in the manager's Agent Settings dialog box (below).



The new field is the Agent's IP address, as seen from the Internet. In this field, specify the "real" IP address that the client requires to access the firewall computer via the Internet.

The mobile user can now contact the permitted services in the network, for example, the mail server.

Virtual Private Networks

What is Encryption?

With the growth of international networks, public and private e-mail systems, a greater need to secure private communication has arisen. One method of ensuring privacy is encryption. There are two types of encryption schemes: symmetric or private, and public/private key schemes. The Guardian encryption method uses *both* schemes.

Symmetric Key Scheme

In the symmetric key system, the receiver and the sender of the message hold the same private key which uses the same algorithm. The encryption process transforms data into a form unreadable by anyone that might be monitoring the line. The recipient uses his private key to decipher the message. Thus, even if the channel is insecure, communication is secure. The symmetric, or private key scheme has the advantage of being relatively fast and easy to use, even though it has some drawbacks.

The symmetric key system is based on the theory that the sender and receiver of a message know and use the same secret key to decipher the message. There are many ways to send the secret key: via telephone, courier etc. However, these methods are not reliable. The challenge was to find a way for the sender and receiver to agree on the secret key without anyone finding out. This led to the creation of the public/private key scheme.

Public/Private Key Scheme

In the public/private key scheme, each side receives a pair of keys: a public key and a private key. The public key is published, whereas the private key is kept secret, eliminating the need for transferring secret information. Anyone can send a confidential message using public information only, but the message can only be decrypted with a private key. The recipient is the sole owner of the key.

Guardian Encryption Scheme or Virtual Private Network

The Guardian encryption method employs both the symmetrical and the public/private key methods. The public/private key is used only at the beginning of each session in the form of a relatively short encrypted code. This code is used to exchange keys, which establishes the identity of the sender and recipient. Then, the body of the message is encrypted with a symmetric key which is exchanged at each session. Therefore, most of the communication is done through the symmetric or session key, which speeds up transfer of information and avoids lengthening the communication packets.

An example of how Guardian's virtual private network works, follows.

EncryptionKey Example

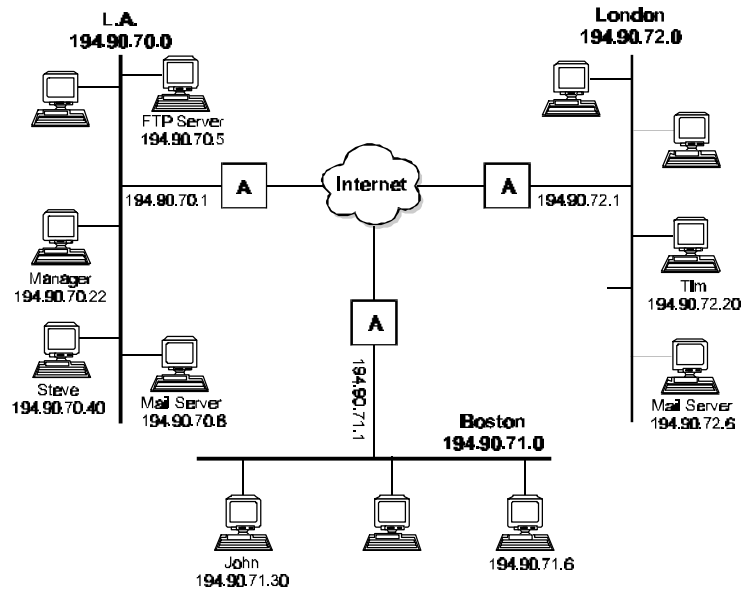


Figure 8-1 Example of Encryption

Company X has three major branches that send confidential materials over the Internet. Steve is the branch manager in Los Angeles, Tim is the manager in London and John is the manager in Boston. All three need to send confidential material to each other through their e-mail. In addition, the Boston branch needs to transmit confidential material using FTP to the Los Angeles branch only. Finally, John has a sister, Mary, in New York to whom he sends unencrypted messages.

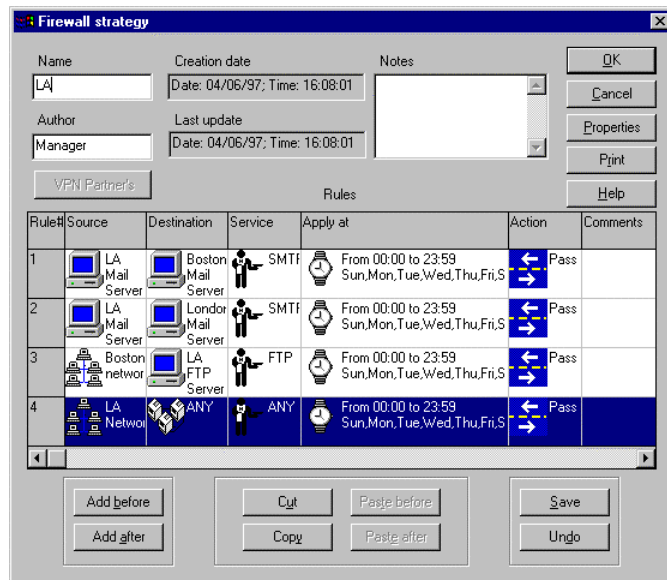
How will their firewall strategy be configured? The process is described in the sections that follow.

Implementing Encryption for the LA Branch

Once you have installed the encryption feature, you need to create a firewall strategy. The following example designs the strategy for the branch in Los Angeles in the example above.

Note:

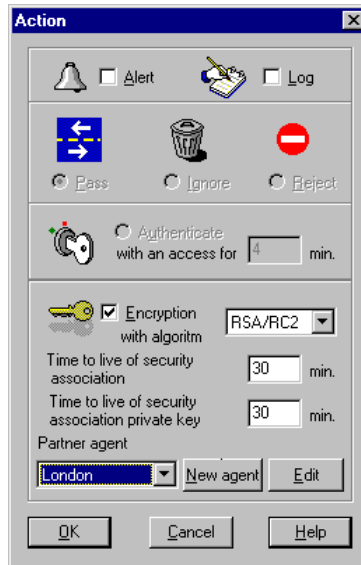
The same encryption should be installed on each agent.



This example shows the firewall strategy before implementing encryption. Source, Destination and Service are defined, and 'Pass' is the default Action.

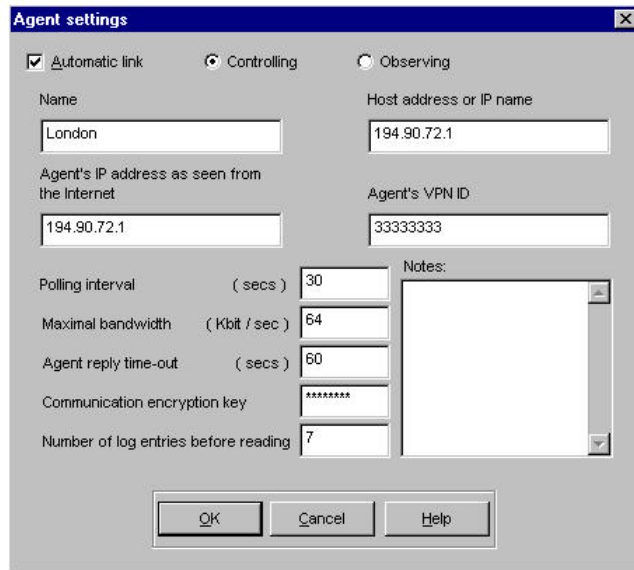
► **To encrypt data**

- 1 Create a new, or edit an existing firewall strategy.
- 2 In the Firewall Strategy screen, double click **Action**. The Action dialog box appears, as seen from the LA agent.



- 3 In the Action dialog box, enable Encryption.
- 4 From the drop-down list, choose an algorithm. The local agent and the partner agent must use the same algorithm.
- 5 In the Time to live of security association box, enter the time that the session key is active.
- 6 In the Time to live of security association private key box, enter the time that the private key is active.

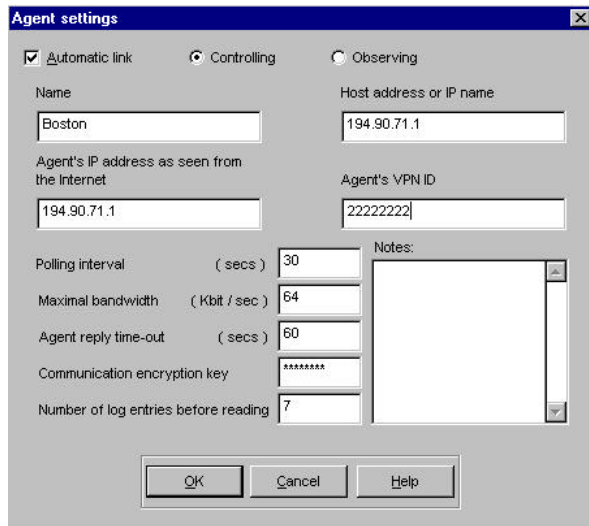
- 7 From the drop-down list, choose a partner agent. In our example above, Steve would choose either John or Tim.
- 8 Click **New Agent** to add a new agent or **Edit** to modify an existing agent's settings. The Agent Settings dialog box appears.



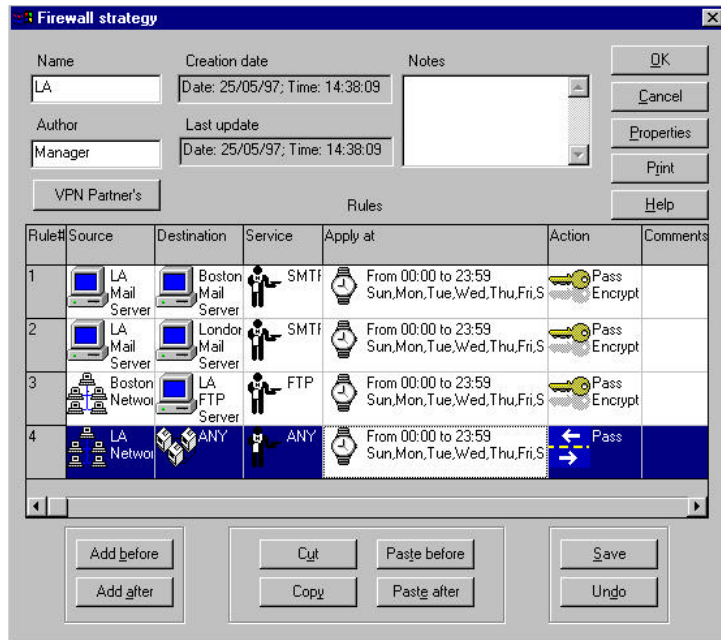
- 9 Click **OK** to update the agent settings. The Agent Settings dialog box closes.
- 10 In the Action dialog box, click **OK** to enable encryption. The Action dialog box closes, and the Action rule in the Firewall Strategy dialog box is updated.
- 11 Follow the preceding instructions to add Boston as a partner agent. The Action dialog box appears as follows.



To add or edit the agent settings for the Boston partner agent, click **Add** or **Edit** in the Action dialog box. The Agent Settings dialog box appears:



The action rule in the Firewall Strategy dialog box is updated as follows:

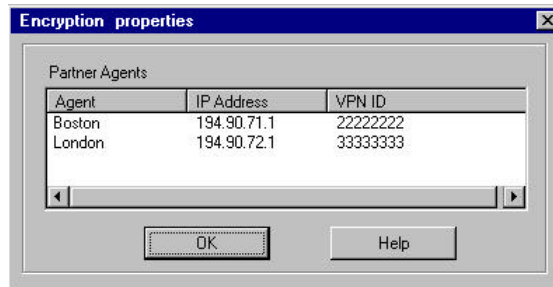


Verifying Encryption Properties for the LA Branch

Follow the instructions below to ensure that the LA agent has the correct VPN partners.

► **To verify encryption properties**

- ◆ In the Firewall Strategy dialog box, click **VPN Partners**. The Encryption Properties dialog box appears. Verify that the information that appears is correct.



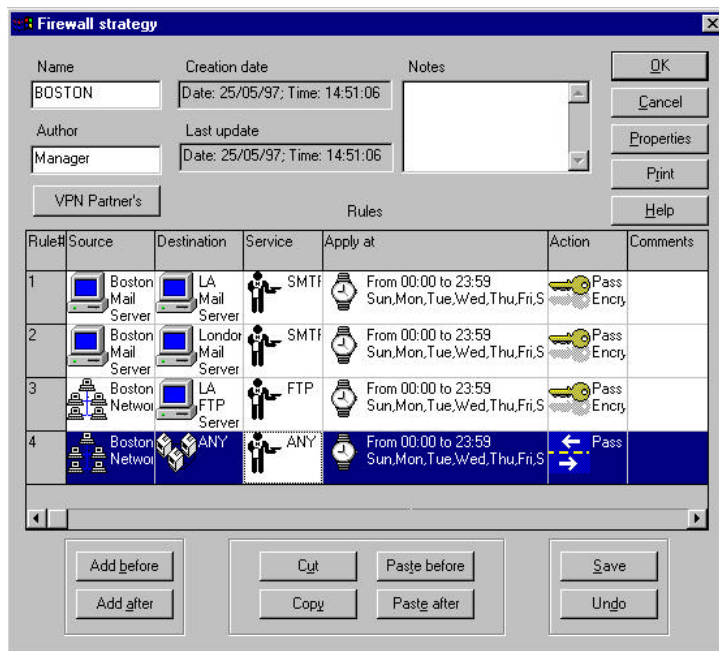
You have completed the encryption installation at the LA Branch. Now you follow similar procedures to implement encryption at the other two branches.

Implementing Encryption for the Boston Branch

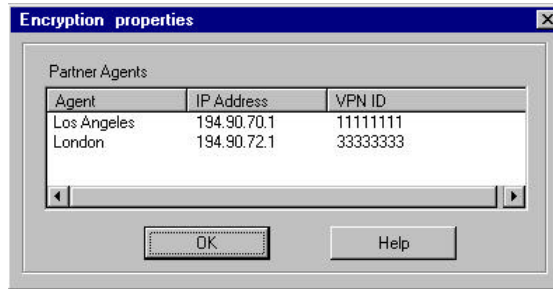
Now you need to design the firewall strategy for the Boston branch in the example.

► **To implement encryption for the Boston branch**

- 1 Follow the instructions for implementing encryption and verifying the encryption properties for the LA branch. The Firewall Strategy dialog box appears as follows:



- 2 Verify the encryption properties for the Boston branch, in the same way you did the LA branch. The Encryption properties dialog box appears as follows.



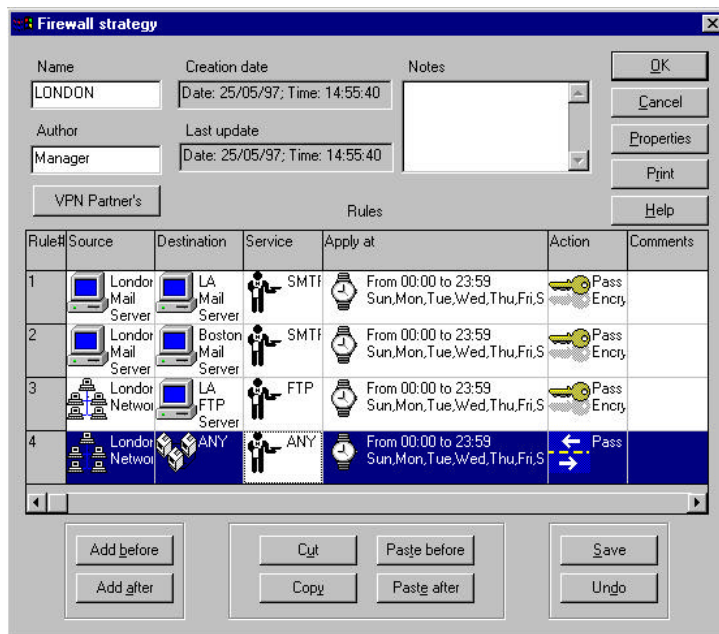
You have finished implementing encryption for the Boston Branch.

Implementing Encryption for the London Branch

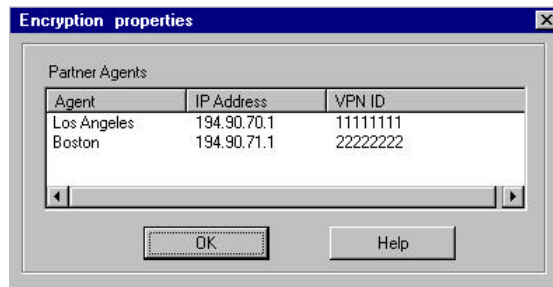
Now you need to design the firewall strategy for the London branch.

► **To implement encryption for the London branch**

- 1 Follow the instructions for implementing encryption and verifying the encryption properties for the LA branch. The Firewall Strategy dialog box appears as follows:



- 2 Verify the encryption properties for the Boston branch, in the same way you did the LA branch. The Encryption properties dialog box appears as follows.



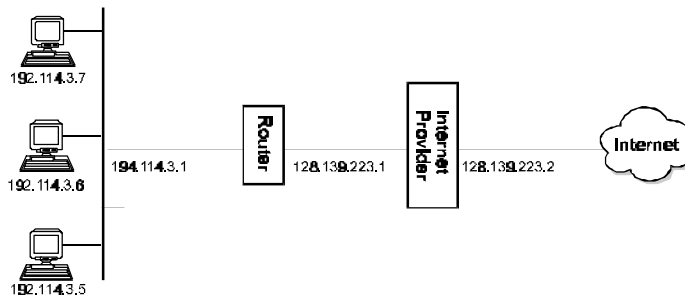
You have finished implementing encryption for the three branches and can now send data safely across the Internet.

Appendix A

Installing the Agent on the LAN Segment

When it is impossible to separate the networks physically, we create an additional Auxiliary network between the router and Guardian agent. The IP network address of the Auxiliary network does not matter, since only two adapters are connected there and they are not supposed to communicate with a host outside the Auxiliary network. The following network address may not be used for the Auxiliary network since it has been reserved by the Internet community for internal/test usage – 192.168.36.0.

Consider an example of a network which has been assigned an address 192.114.3.0 by the Internet authorities. It is a Class C network which allows 254 hosts belonging to the network to communicate with other hosts over the Internet. The following figure shows the network configuration without Guardian.



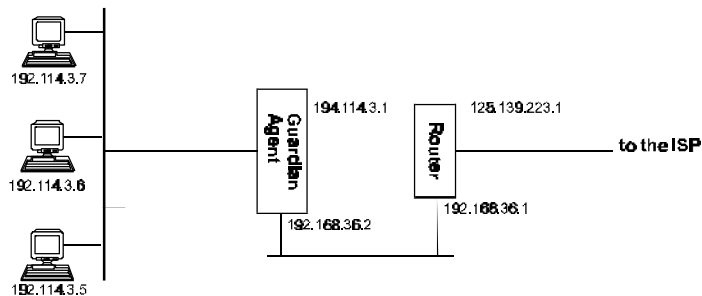
In the configuration, we connected our private network 192.114.3.0 to the Internet using a router. The router has one connection to our network with the address

192.114.3.1. The other side of the router (128.139.223.1) is connected to our Internet provider (probably via modem and phone line). Our Internet provider has assigned our router an address of 128.139.223.1 on the leg nearest to the Internet provider. The Internet provider's side of the connection has address 128.139.223.2. So, as we can see, the router connects two different networks 192.114.3.0 and 128.139.223.0.

All the workstations in the network are configured with addresses in the range of 192.114.3.1 through 192.114.3.254. Each workstation has the address of the router (192.114.3.1) as the address of its default gateway. This means that all the IP traffic designated to the network addresses other than 192.114.3.x will be transferred to the router which knows how to handle them (actually transfers traffic to the nearest router which is located at the Internet provider).

As we mentioned before, the correct site to install the Guardian agent is between the router and our network. Since the Guardian agent acts as a gateway and you will not change the configuration on each of your hosts, the best solution is to install the Guardian agent in such a manner that it will look like a router to all hosts in our network. Since the Guardian agent will have the same address as the router (192.114.3.1), you will not have to change your hosts' configuration.

The following figure illustrates the final configuration.



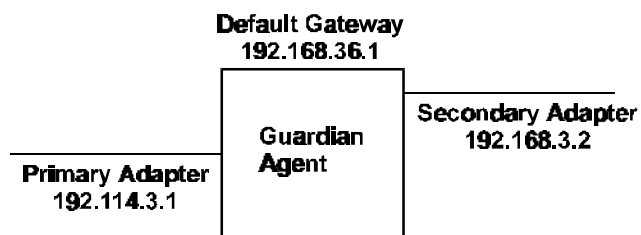
Setting up the Guardian Gateway

To minimize network disruption, you can set up and configure the IP addresses for the gateway before actually connecting it to the network. For the required hardware and software, refer to the relevant sections earlier in this manual.

Configuring the Guardian Gateway

At this stage, we configure the IP addresses for the Guardian gateway. The Guardian gateway is basically a computer with two network adapters. One adapter connects to the Secured network, while the second adapter, along with the router's adapter, constitutes the auxiliary network 192.168.36.0.

The following figure shows the configuration of the Guardian gateway.



We configure the Guardian agent in such way that:

- The primary adapter which will be connected to our Secured network has IP address 192.114.3.1 (which is currently used by the router). This does not create any potential problem, since the Guardian agent is not yet connected to the network.
- The computer's secondary network adapter has IP address 192.168.36.2. It will connect to the Auxiliary network.
- The IP address of the router (192.168.36.1) is defined as an address of the default gateway for the Guardian agent. Thus, all frames received by the Guardian agent and designated to the Internet, will be transferred to the router from where they are routed further.

Reconfiguring the Router

Now, we access the router and change its configuration so that all TCP/IP traffic will be routed via the Guardian gateway.

The following explanations are based on the assumption that the router we use to connect to the Internet provider is a Cisco router. The required changes in configuration are minor and are almost irrespective of the model. We assume also that we are dealing with the working router's configuration, i.e. at this stage of the installation process the private network is able to communicate with the Internet.

There are two parameters that we are going to change:

- IP address of the network adapter which is connected to the network where our hosts are connected.

- Static routing table entry which defines the route for the frames designated to our private network (192.114.3.0) to be sent to the Guardian agent.

After accessing the router, type SHOW CONF at the router's command prompt. This command shows the current router's configuration. Search for the line that begins with and states the name of the adapter. In this case, INTERFACE is the name of the adapter. Usually, an Ethernet adapter appears as Ethernet0, while TokenRing0 represents the Token Ring adapter. The next line in the dialog resembles the line that follows:

IP address 192.114.3.1 255.255.255.0, where the network adapter is assigned an IP address of 192.114.3.1 with a net mask of 255.255.255.0 (Class C network).

The following is a fragment of the configuration that is going to be changed.

```
...
interface Ethernet0
ip address 192.114.3.1 255.255.255.0
...
```

We want these lines to be:

```
...
interface Ethernet0
ip address 192.168.36.1 255.255.255.0
...
```

To do this, at the router's prompt type the CONF T command. The following shows a fragment of the dialog:

```
router# show conf
...
interface Ethernet0
    ip address 192.114.3.1 255.255.255.0
...
```

```
end
router#conf term
Enter configuration commands, one per
line. End with
CNTL/Z
router (config) #interface Ethernet0
router (config-if) #ip address
192.168.36.1
255.255.255.0
router (config-if) #^Z
router#write
```

Note:

After changing the router's IP address, communications will most likely be broken. If you used the Telnet session to configure the router, upon saving the router's configuration, the session will be closed. This is normal. To avoid this, you should configure the router via a console connected directly to the router, and not via a Telnet session.

After this dialogue we can issue the **SHOW CONF** command and ensure that the IP address for network adapter has been changed:

```
...
interface Ethernet0
ip address 192.168.36.1 255.255.255.0
...
```

- 1 We have to assign a static routing entry to the router in such a way that all the frames reaching the router and destined for network 192.114.3.0 are transferred to gateway 192.3.168.36.2, which is the Guardian agent.

In the same configuration list that we get by the **SHOW CONF** command, we have to add a static routing entry. All the routing table entries begin with

the word IP ROUTE. We have to add the following string to the configuration:

```
ip route 192.114.3.0 255.255.255.0
192.168.36.2
```

The string means that all the frames destined for network 192.114.3.0, i.e. with destinations in the range of 192.114.3.0 through 192.114.3.255, will be sent to the Guardian agent that has IP address of 192.168.36.2. To do this, the following dialog occurs:

```
router#conf term
Enter configuration commands, one per
line. End with CNTL/Z.
router (config) #ip route 192.114.3.0
255.255.255
192.168.36.2
router (config-if) #^Z
router#write
```

The following is an example of the Cisco's router configuration before and after the changes. The changed lines are printed in BOLD.

```
Using 778 out of 32762 bytes
!
version 10.3
!
hostname router
!
enable secret 5
$1$TuPt$u5KPJBneTwva2u5Wwb9ZA/
enable password guardian
!
dlsw disable
dlsw allroute_sna
dlsw allroute_netbios
!
```

```
interface Serial0
  no ip address
  encapsulation frame-relay
  keepalive 11
  frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
  description link to netvision
  ip address 194.90.4.233 255.255.255.252
  no cdp enable
  frame-relay interface-dlci 16
!
interface TokenRing0
  ip address 192.114.3.1 255.255.255.0
<will change>
  ring-speed 16
!
interface PCbus0
  no ip address
  shutdown
!
router igrp 1
  network 192.114.3.0
!
ip route 0.0.0.0 0.0.0.0 194.90.4.234
snmp-server community public RO
!
!
line con 0
line aux 0
line vty 0 4
  password guardian
  login
!
end
```


The following is a new configuration:

```
Using 778 out of 32762 bytes
!
version 10.3
!
hostname router
!
enable secret 5
$1$TuPt$u5KPJBneTwva2u5Wwb9ZA/
enable password guardian
!
dlsw disable
dlsw allroute_sna
dlsw allroute_netbios
!
interface Serial0
  no ip address
  encapsulation frame-relay
  keepalive 11
  frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
  description link to netvision
  ip address 194.90.4.233 255.255.255.252
  no cdp enable
  frame-relay interface-dlci 16
!
interface TokenRing0
  ip address 192.168.36.1 255.255.255.0
<changed>
  ring-speed 16
!
interface PCbus0
  no ip address
  shutdown
!
router igrp 1
  network 192.168.36.0
```

```
!  
ip route 0.0.0.0 0.0.0.0 194.90.4.234  
ip route 192.114.3.0 255.255.255.0  
192.168.36.2 <added>  
snmp-server community public RO  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
password guardian  
login  
!  
end
```

The router has now been configured.

2. Now we can disconnect the router from our private network. The following figure shows the final configuration.

