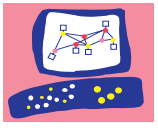
Check Point
Getting Started Guide

Check Point 2000

Part No.: 700001
January 2000

CHECK POINT™
Software Technologies Ltd.



We Secure the Internet.

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com

U.S. Headquarters:
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

http://www.checkpoint.com

February 2, 2000

Please direct all comments regarding this publication to **techwriters@checkpoint.com.**

Contents

Figures

Tables

Preface

Scope

This book provides an overview of the products available on the Check Point Enterprise CD-ROM. An installation chapter provides step by step instructions on how to install and configure each product.

Check Point Enterprise CD-ROM

The following products are available on the Check Point Enterprise CD-ROM:

- FireWall-1/VPN-1
- FloodGate-1
- SecuRemote
- SecureClient
- Reporting Module
- Meta IP

Your Check Point license determines the products you can install and configure. The features enabled for each product also depend on your Check Point license.

Note – The Check Point Account Management Client is not on this CD, but it can be obtained separately from your reseller.

VPN-1/FireWall-1

VPN-1/FireWall-1 is deployed on your Internet gateway and other network access points, and inspects every packet passing through key locations in your network according to an enterprise Security Policy. In addition to highly granular access control,

VPN-1/FireWall-1 includes security and network management features that are fully integrated into the enterprise-wide Security Policy and managed through an intuitive graphical user interface.

Open Security Extension (VPN-1/FireWall-1 Feature)

Open Security Extension feature enables VPN-1/FireWall-1 to manage third-party routers and other networking devices. The Security Policy is defined using the VPN-1/FireWall-1 Rule Base Editor. VPN-1/FireWall-1 then generates Access Control Lists (ACLs) and downloads them to selected routers and devices. There is no need to configure separate ACLs for each device. Open Security Externsion manages the following third-party devices:

- Bay Networks Routers — Version 7.x - 12.x
- Cisco Routers — IOS Version 9,10,11
- Cisco PIX Firewall — Version 3.0, 4.0, 4.1
- 3Com NetBuilder — Version 9.x
- Microsoft Routing and Remote Access Service (RRAS) for Windows NT Server 4.0 (Windows NT platforms only)

Access lists can be imported from PIX units, 3Com, Cisco and Microsoft RRAS, enabling the integration of existing filter configurations through the Check Point Policy Editor.

FloodGate-1

FloodGate-1 manages finite bandwidth resources to ensure reliable network performance for business-critical applications over wide area networks (VPNs, frame relay, satellite, and leased lines). FloodGate-1 precisely controls the traffic mix and allocation of available bandwidth by application, source, destination, user, etc. With FloodGate-1's weighted prioritization of network traffic, predictable performance for important applications is guaranteed and bandwidth is optimally utilized.

SecuRemote and SecureClient

Check Point SecuRemote enables mobile and remote Microsoft Windows 9x and Windows NT (Intel only) users to connect to their enterprise networks via dial-up Internet connections — either directly to the server or through Internet Service Providers — and communicate sensitive corporate data safely and securely. Check Point SecuRemote extends the Virtual Private Network (VPN) to the desktop and laptop.

Other uses for SecuRemote are:

- Specific employees can be granted encrypted access to sensitive corporate data.
- A server can be set up to provide encrypted information to paying customers only. Because the communication is encrypted, eavesdropping is impossible.
- Users at a remote office can conduct encrypted communications with the FireWalled enterprise network without installing VPN-1/FireWall-1 at the remote office.

Check Point SecureClient extends security to the desktop by enabling administrators to enforce a Security Policy on desktops — both inside the LAN and connecting from the Internet — and prevent authorized connections from being hijacked.

Check Point SecureClient consists of:

- SecuRemote Client software with the Desktop Security feature installed
- A Policy Server from which the SecuRemote Client obtains its Desktop Security Policy

Reporting Module

The Reporting Module allows you to monitor and audit all transactions in your FireWalled networks. You can generate detailed or summarized reports for all connections logged by your FireWall Modules. Reports can be used to analyze traffic between the enterprise network and the Internet as well as transactions within the enterprise.

Meta IP

Meta IP provides an automated solution for managing IP addressing and naming. Meta IP ensures control and reliability of address allocation while improving TCP/IP management efficiency. A modular, replicated architecture enables multi-level fault tolerance, cross-platform compatibility and distributed administration. Through a unique User-to-Address-Mapping (UAM) technology, IP addresses are associated with user login names for comprehensive auditing and improved troubleshooting. The combination of UAM with VPN-1/FireWall-1 enables you to automatically enforce security policies by the user in a dynamic addressing environment.

Who Should Use this User Guide

This User Guide is written for system administrators who are responsible for maintaining network security. It assumes you have a basic understanding and a working knowledge of:

- system administration
- the Unix or Windows operating system
- the Windows GUI
- Internet protocols (IP, TCP, UDP *etc*.)

Summary of Contents

Chapter 1, “What’s New in Check Point 2000?” describes the new features in Check Point 2000.

Chapter 2, “VPN-1/FireWall-1 Overview” describes Check Point’s Stateful Inspection technology and shows how VPN-1/FireWall-1’s architecture and features are used to enforce an enterprise-wide Security Policy.

Chapter 3, “Virtual Private Networks” describes how VPN-1/FireWall-1’s encryption features enable an enterprise to implement a Virtual Private Network.

Chapter 4, “VPN-1 SecureClient” describes how VPN-1/FireWall-1 implements LAN security.

Chapter 5, “Introduction to FloodGate-1” describes FloodGate-1 technology, architecture and features.

Chapter 6, “Open Security Extension” describes VPN-1/FireWall-1’s optional Open Security Extension feature.

Chapter 7, “Reporting Module” describes the Check Point Reporting Module components and their interaction with VPN-1/FireWall-1.

Chapter 8, “Meta IP” describes Meta IP architecture and features.

Chapter 9, “Before Installing VPN-1/FireWall-1” describes how a system must be prepared before installing VPN-1/FireWall-1.

Chapter 10, “Check Point Software Installation” describes the installation procedure for Check Point software products.

Chapter 11, “Installing VPN-1/FireWall-1” describes how to install VPN-1/FireWall-1.

Chapter 12, “VPN-1/FireWall-1 Tutorial” is a short tutorial presenting the major VPN-1/FireWall-1 features.

Additional Documentation

User Guides are available for each product in Portable Document Format (PDF) on the Check Point Enterprise CD-ROM. The Adobe Acrobat Reader is required to view PDF files and is also available on the Check Point Enterprise CD-ROM. You can also download the Acrobat Reader from the Adobe Web site (http://www.adobe.com).

VPN-1/FireWall-1

The VPN-1/FireWall-1 documentation set consists of the following books:

VPN-1/FireWall-1 Administration Guide

This book is the technical reference to VPN-1/FireWall-1 features, including authentication and address translation. In addition, chapters on troubleshooting and Frequently Asked Questions (FAQ) are included.

Check Point Virtual Private Networking

This book describes how to establish a Virtual Private Network using FireWall-1.

VPN-1/FireWall-1 Reference Guide

This book describes INSPECT, the command line interface and other reference subjects, and includes a glossary.

FloodGate-1

The FloodGate-1 documentation set consists of the following books:

Getting Started with Check Point FloodGate-1

This book describes how to install FloodGate-1.

Check Point FloodGate-1 Administration Guide

This book describes how to configure and manage a FloodGate-1 Bandwidth Policy.

Reporting Module

The Reporting Module documentation set consists of the following books:

Getting Started with the Check Point Reporting Module

This book describes how to install and configure the Reporting Module components. A tutorial provides step by step instructions for working with predefined settings immediately after installation.

Check Point Reporting Module Administration Guide

This book describes how to define reports and manage Reporting Module components.

Meta IP

Check Point Meta IP User Guide

This book describes how to install and manage Meta IP.

What Typographic Changes Mean

The following table describes the typographic changes used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen computer output	`machine_name% su` `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type `rm` *filename*.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide*. These are called *class* options. You *must* be root to do this.
Save	Text that appears on an object in a window	Click on the **Save** button.

Note – This note draws the reader's attention to important information.

Warning – This warning cautions the reader about an important point.

Tip – This is a helpful suggestion.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, Korn shell and DOS.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	*machine_name*%
C shell superuser prompt	*machine_name*#
Bourne shell and Korn shell prompt	$
Bourne shell and Korn shell superuser prompt	#
DOS	*current-directory*>

Network Topology Examples

Network topology examples usually show a gateway's name as a city name (for example, Paris or London) and the names of hosts behind each gateway as names of popular sites in those cities (for example, Eiffel and BigBen).

CHAPTER 1

What's New in Check Point 2000?

In This Chapter

Note – This chapter describes new features in Check Point 2000, and is intended for readers already familiar with VPN-1/FireWall-1. These new features are also described in the VPN-1/FireWall-1 User Guides.

Overview of New Features

This version of VPN-1/FireWall-1 includes the following new features:

- **High Availability —** Two or more VPN/FireWall Modules can be configured so that each one acts as a backup to the others. Additionally, the VPN/FireWall Modules can be synchronized so that connections will not be lost when a VPN/FireWall Module fails. See "High Availability" on page 3 for more information.

- **Desktop Policy Verification** — Policy Servers now maintain open connections with SecureClients and are immediately notified when a SecureClient is re-configured. Both Session Authentication and Client Encrypt rules can be applied only when a SecureClient is properly configured. For more information, see "Desktop Policy Verification" on page 98.
- **SecuRemote**
  - The Secure Domain Logon feature enables Windows NT SecuRemote users to securely log on to a domain controller using both LAN and dial-up connections. For more information, see "Secure Domain Logon" on page 162 of *Check Point Virtual Private Networks*.
  - SecuRemote Clients can be configured to automatically update a site's topology either when starting SecuRemote or just before the key exchange with that site. For more information, see "Automatic Topology Update" on page 165 of *Check Point Virtual Private Networks*.
  - SecuRemote Clients can be configured to automatically check the availability of a newer version of SecuRemote Client software before connecting to a site. For more information, see "Automatic Version Update" on page 167 of *Check Point Virtual Private Networks*.
  - SecuRemote Clients can be pre-configured with a partial site topology to reduce exposure of sensitive network information. The first time the SecuRemote Client connects to a site, the user will be given the opportunity to download the complete topology over the authenticated connection. For more information, see "Partial Topology" on page 168 of *Check Point Virtual Private Networks*.
  - A smaller SecuRemote Client installation file set (without the certificate functionality) is available. For more information, see "Thin Client" on page 169 of *Check Point Virtual Private Networks*.
- **Hybrid Mode** — VPN-1/FireWall-1 Hybrid Mode authentication extends IKE, enabling it to use any authentication method supported by VPN-1/FireWall-1. See "Hybrid Mode (Additional Authentication Schemes for IKE)" on page 20 for more information.
- **Intel RNG** — VPN-1/FireWall-1 and SecuRemote support the Intel RNG (pseudo random number generator) hardware for Windows NT 4.0, Windows 98, Windows 95 (OSR2 or later or Windows 95 with IE 3.02 or later). See "Intel RNG" on page 24 for more information.
- **Remote Licensing Management** — This feature enables the system administrator to manage VPN-1/FireWall-1 licenses on remote VPN/FireWall Modules from the Management Station. For more information, see "Remote Licensing Management" on page 54 of *VPN-1/FireWall-1 Reference Guide*.
- **Malicious Activity Detection** — VPN-1/FireWall-1's Malicious Activity Detection (MAD) feature provides a mechanism for detecting intrusion attempts or other suspicious events and notifying the system administrator by an alert or email message. See "Malicious Activity Detection (MAD)" on page 25 for more information.

- **CVP Manager —** The CVP Manager application enables a Resource to invoke any number of CVP Servers. This capability is useful when each of the CVP Servers performs a different function. See “CVP Manager” on page 31 for more information.
- **CVP/UFP Load Sharing —** Identical CVP Servers or identical UFP Servers can be configured to share the work load among themselves, increasing the availability of the CVP Servers or UFP Servers. See “CVP/UFP Load Sharing” on page 37 for more information.

High Availability

Overview

VPN-1/FireWall-1 enables two or more VPN/FireWall Modules machines to be configured so that each one acts as a backup for the others. If one of the VPN/FireWall Module machines fails for any reason, another VPN/FireWall Module takes its place in a manner that minimizes the number of lost connections.

Note – The VPN-1/FireWall-1 High Availability feature provides the mechanism for detecting failures and changing routing accordingly. The VPN-1/FireWall-1 synchronization feature provides the mechanism for synchronizing the states of the VPN/FireWall Modules. High Availability is described in this section. High Availability for encrypted connections is described in Chapter 12, “High Availability for Encrypted Connections” of *Check Point Virtual Private Networks*.

One of the machines is designated as the primary machine, and this machine serves as the gateway in normal circumstances. If the primary machine fails, control is passed to the first secondary machine. If that machine fails, control is passed to the next secondary machine, and so on.

Note – The High Availability feature is currently available for Windows NT and Solaris.

FIGURE 1-1 shows one possible network configuration for implementing the High Availability feature.

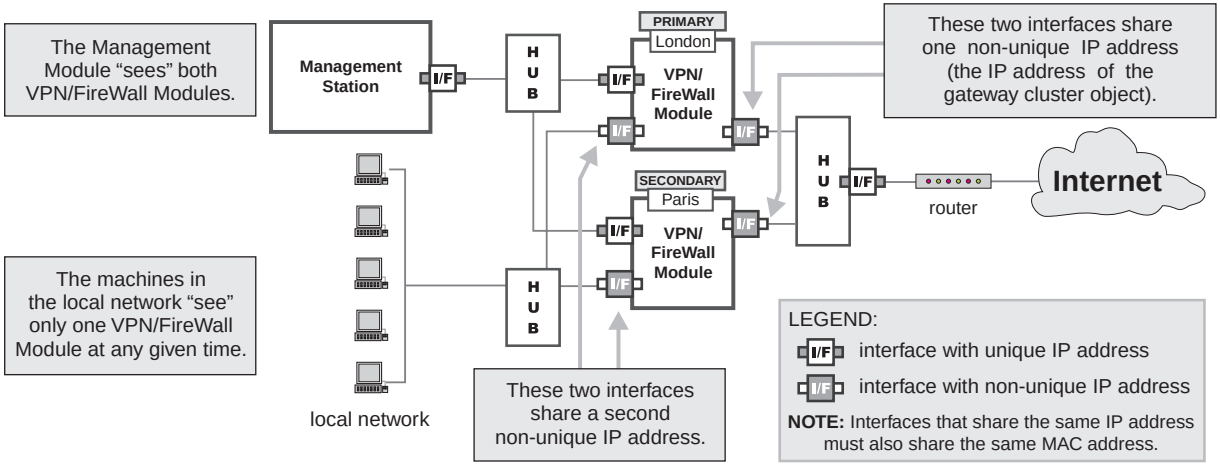


FIGURE 1-1 High Availability configuration

In this configuration, there are two VPN/FireWall Modules: London (the primary) and Paris (the secondary) each with three interfaces, as follows:

- an interface with a unique IP address, facing the Management Station

  These are the interfaces the Management Station sees. Because the Management Station must be able to download a Security Policy to both VPN/FireWall Modules, each VPN/FireWall Module must have its own unique IP address so that the Management Station can "see" them both at any given time. The machines also require unique IP addresses for system maintenance purposes.

  The network configuration in FIGURE 1-1 shows the Management Station connected to the same hub as the VPN/FireWall Modules, but this is one of many possible configurations. The only requirement is that there be a route from the Management Station to the unique IP addresses of each of the VPN/FireWall Modules, so that the Management Station can "see" all the VPN/FireWall Modules at any given time. The advantage of connecting through a hub is that the connection between the Management Station and the VPN/FireWall Module is then secured (see "Secured Interfaces" on page 6).

- a second interface with a non-unique IP address, facing the Internet through a hub

  This is the interface that the outside world sees. Because there are two interfaces (one on each VPN/FireWall Module) with the same IP (and MAC) address, only one of them can be active (that is, the outside world can see only one of them) at any given time. This is also the IP address defined for the gateway cluster object (see "Network Configuration" on page 234 of *Check Point Virtual Private Networks*) that includes these gateways.

- a third interface with a different non-unique IP address, facing the local network through a hub

  This is the interface that the local network sees. Because there are two interfaces (one on each VPN/FireWall Module) with the same IP address, only one of them can be active (that is, the local network can see only one of them) at any given time.

There can be any number of local networks, each of which is connected to both VPN/FireWall Modules on interfaces that share the same non-unique IP address (but each local network shares a different non-unique IP address).

Note –

- You will need at least three machines to implement High Availability: a Management Station and two VPN/FireWall Modules.
- Interfaces that share the same IP address must also share the same MAC address. For information on how to configure MAC addresses, see "Configure Shared Interfaces Window" on page 9 for Windows platforms or "MAC Addresses" on page 11 for Solaris platforms.
- Both the unique and non-unique IP addresses may be illegal.
- If the High Availability machines are synchronized, there must be a control channel between all the machines. For more information, see "Synchronization" on page 12.

When Does a VPN/FireWall Module Become Active?

A VPN/FireWall Module becomes active in place of another VPN/FireWall Module if the active VPN/FireWall Module fails, that is, if one of the following occurs on the active VPN/FireWall Module:

- The FireWall daemon (`fwd`) or any other process specified with the `cphaprob` command (see "cphaprob" on page 15) terminates.
- The `cphaprob` command reports a problem in the FireWall daemon (`fwd`) or any other specified process.

  By default, a VPN/FireWall Module reports a problem (using the `cphaprob` command — see "cphaprob" on page 15) when the Security Policy is uninstalled.
- An interface or cable fails.
- The machine crashes.
- The Security Policy is uninstalled.

When a VPN/FireWall Module goes down, another VPN/FireWall Module becomes active and (if the VPN/FireWall Modules are synchronized) also "takes over" the connections of the failed VPN/FireWall Module (see "Synchronization" on page 12 for more information on synchronization).

Before Configuring High Availability

Before you configure the High Availability feature, define the same IP address for each machine participating in the High Availability configuration.

To avoid network conflicts, proceed as follows:

1. Disconnect the machines participating in the High Availability configuration from the hub.
2. Define the IP addresses.

   You must define the IP addresses before configuring the High Availability feature, because the export and import of shared MAC addresses requires that the shared IP addresses be already configured.
3. Install VPN-1/FireWall-1.

   At the end of the installation you are prompted to reboot the computer.
4. Reconnect the machines participating in the High Availability configuration from the hub before or during the reboot.

Secured Interfaces

An interface is considered secured if a connection through that interface can be trusted (for example, if the interfaces that share the same IP and MAC addresses are connected with a cross cable or dedicated hub). If a Management Station and a VPN/FireWall Module are connected through secured interfaces, then the connection between the machines can be trusted because there is no way for an intruder to send packets on that connection. In addition, a secured interface can be safely used to transmit synchronization and High Availability information.

In a High Availability configuration, each machine should have at least one secured interface. Additional secured interfaces are recommended for backup purposes.

If there secured interfaces are configured, a VPN/FireWall Module will accept state change commands only on those interfaces. If there are no secured interfaces, a VPN/FireWall Module will accept state change commands on any interface.

Sharing IP and MAC Addresses

The recommended procedure is as follows:

1. On the primary machine, define the MAC addresses and other parameters for each interface.

   In most cases, you can use the default definitions.
2. Export the default MAC addresses from the primary machine to a file.
3. On each of the other (secondary) machines, import the file.

Note –

- MAC addresses can be freely exported and imported between Windows NT and Solaris machines.
- If you uninstall VPN-1/FireWall-1, then the original MAC addresses will be restored on Solaris machines but will not be restored on Windows NT machines.

Installation

The High Availability feature is part of the standard VPN-1/FireWall-1 installation. It should be installed only in a distributed configuration, that is, only when the Management Station and the VPN/FireWall Modules are installed on different machines.

Warning – Make sure the same version of VPN-1/FireWall-1 (including the build number) is installed on the Management Station and each VPN/FireWall Module.

When installing VPN-1/FireWall-1 for the first time, the Check Point configuration application is run automatically and you can configure the High Availability parameters at that time. Otherwise, you should reboot the machine after upgrading VPN-1/FireWall-1 and then configure the High Availability parameters.

You must configure the High Availability parameters separately on each VPN/FireWall Module machine. It is recommended that you configure the primary machine first and then configure each of the secondary machines in turn.

Note – Make sure you have obtained a license to use the High Availability feature.

Windows NT

Configuration

High Availability parameters are specified in the **High Availability** tab (FIGURE 1-2).

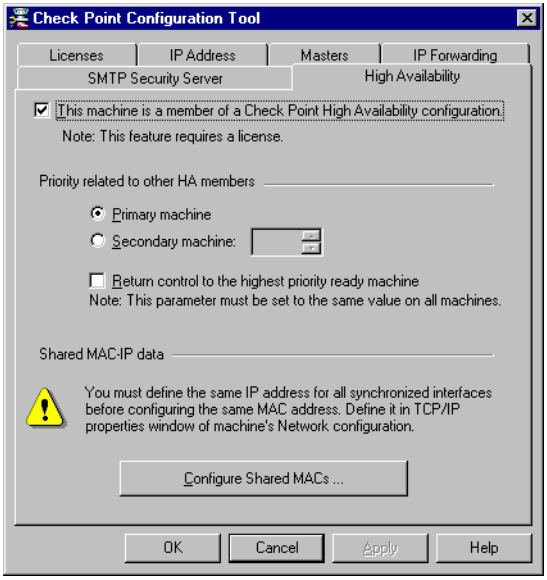


FIGURE 1-2 VPN-1/FireWall-1 Configuration - High Availability tab

This machine is a member of a Check Point High Availability configuration — Check this box to indicate that this machine participates in a High Availability configuration.

Priority related to other HA members — Select one of:

Primary machine — Check this box if this machine is the primary machine in the HA hierarchy.

Secondary machine — If this machine is one of the secondary machines in the HA hierarchy, specify its priority sequence number.

The primary machine's priority sequence number is 1, and control is passed to the secondary machines according to their priority sequence numbers. In other words, if the primary machine fails, control is passed to the secondary machine with sequence number 2. If that machine fails, control is passed to the secondary machine with sequence number 3, and so on.

If secondary machine 3 has control and secondary machine 2 is restored, then control will be returned to secondary machine 2 if **Return control to a higher priority machine when it is restored** is checked (see below).

Warning – This property must be set consistently on all the machines that participate in the High Availability configuration. Only one machine should be specified as the primary machine, and no two machines should have the same priority numbers.

Return control to a higher priority machine when it is restored — This option is useful when a secondary VPN/FireWall Module machine is less powerful than the primary VPN/FireWall Module machine. If this machine has control because all the machines with higher priorities have failed, control returns to the higher priority machine when it is restored.

If this option is not checked, then control will be returned to the higher priority standby machine only when the machine that has control fails (or is rebooted).

Warning – This property must be set to the same value on all the machines that participate in the High Availability configuration.

Configure Shared MACs — Click on this button to display the **Configure Shared Interfaces** window (FIGURE 1-3).

See FIGURE 1-1 on page 4 and the accompanying text for an explanation of shared IP and MAC addresses.

Sharing IP and MAC Addresses

The shared MAC addresses of interfaces on the High Availability machines are defined in the **Configure Shared Interfaces** window (FIGURE 1-3).

Configure Shared Interfaces Window

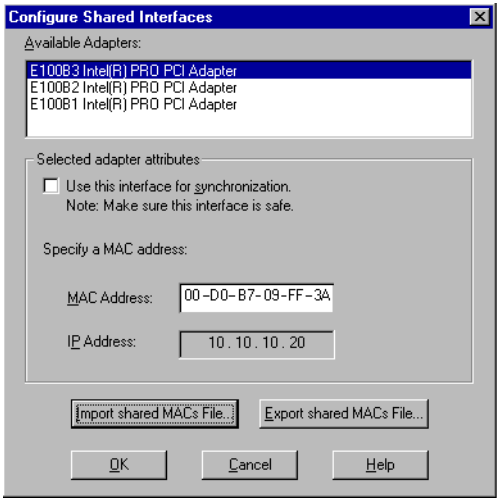


FIGURE 1-3 Configure Shared Interfaces window

Available Adapters — Select the adapter from the list.

Note – You should carefully scroll through all the adapters to confirm that the correct information is exported and imported.

Use this interface for synchronization — Check this box if this interface is secure (for example, if the interfaces that share the same IP and MAC addresses are connected with a cross cable) and can be safely used to transmit synchronization and High Availability information.

- See “Secured Interfaces” on page 6 for more information on secured interfaces.
- See “Synchronization” on page 12 for more information on synchronization.

MAC Address — This is the MAC address.

There is usually no reason to edit this field directly. Use the original MAC addresses from the primary machine.

IP Address — This is the IP address, and cannot be edited.

Import shared MACs file — Import the information about this machine’s interfaces from a file.

A window will be displayed in which you will be asked to specify the file’s location. It is recommended that you export on the primary machine and then import on the secondary machines.

Export shared MACs file — Export the information about this machine’s interfaces to a file.

A window will be displayed in which you will be asked to specify the file’s location. It is recommended that you export on the primary machine and then import on the secondary machines.

Solaris

Configuration

To configure the High Availability parameters, run the `cpconfig` program and select the `Enable High Availability` option (see “cpconfig” on page 4 of *VPN-1/FireWall-1 Reference Guide*).

```
Configuration Options:
----------------------
(1)  Licenses
(2)  Masters
(3)  SMTP Server
(4)  SNMP Extension
(5)  Groups
(6)  IP Forwarding
(7)  Default Filter
(8)  Enable High Availability

(9) Exit
```

You will be asked to configure:

- secured interfaces
- MAC Addresses
- High Availability parameters

Secured Interfaces

See “Secured Interfaces” on page 6 for more information on secured interfaces.

See “Synchronization” on page 12 for more information on synchronization.

```
Configuring High Availability Secured Interfaces...
===================================================
The following interfaces are configured on your machine
hme0 hme1 hme2
Secured interfaces are interfaces on which sensitive High Availability
information can be exchanged securely with other members of this
cluster.

Do you want to add secured interfaces (y/n) [y] ? y
Please enter the list of interfaces that will be secured interfaces.
Enter one interface per line, terminating with CTRL-D or your EOF
character.
hme0
Is this correct (y/n) [y] ? y
```

MAC Addresses

Note – It is highly recommended that you use the original MAC addresses from the primary machine by importing the file.

```
Configuring High Availability MAC Addresses...
==============================================

Do you wish to import MAC addresses configurations file (y/n) [n] ? y
Please enter the file name [/tmp/cphamacs] ? /tmp/cpha1
Following are the MAC addresses in the cphamacs file:
hme0: 8:0:20:b5:7c:12

NOTE: You can export this configuration to any other High Availability
machine
by launching cpha_export.
Would you like to modify the above configuration (y/n) [y] ? n
```

You will be asked to specify the location of the file to import. This file is created by the `cpha_export` command (see “cpha_export (Solaris only)” on page 18).

High Availability Parameters

Configure the High Availability parameters.

```
Configuring High Availability Priorities...
===========================================
You must configure the priority and the mode:
   Priority = 1 for the primary machine; 2,3,4... for the standby
machines.
   Mode = active-up or primary-up.
Following is the current configuration:
Priority: 1
mode: active-up
Would you like to modify the above configuration (y/n) [y] ? y
Priority (1..n) [1]:2
mode (active-up/primary-up) [active-up]:primary-up

Is this correct (y/n) [y] ? y

You have changed the High Availability configuration.
Would you like to restart VPN-1/FireWall-1 now
so that your changes will take effect? (y/n) [y] ? y
```

`priority` is 1 for the primary machine and greater than 1 for secondary machines.

`primary-up` corresponds to checking **Return control to a higher priority machine when it is restored** in the **High Availability** tab (FIGURE 1-2 on page 8).

Synchronization

It is not necessary for the High Availability machines to be synchronized. The advantage of synchronization is that connections will not be lost when a machine takes control from a machine that has gone down (but there are exceptions — see "Restrictions" on page 561 of *VPN-1/FireWall-1 Administration Guide* for more information). The disadvantage is the cost of synchronizing internal tables on all machines.

If you do not require synchronization, you must still configure the High Availability machines with synchronization set to `no sync` in the `$FWDIR/conf/sync.conf` file (see TABLE 1-1 on page 13).

If the High Availability machines are synchronized, there must be a control channel between all the machines (see "fw putkey" on page 12 of *VPN-1/FireWall-1 Reference Guide* for more information). Synchronization information is transmitted on TCP port 256 on the unique IP addresses.

There are three possible synchronization modes:

1. no synchronization
2. "old style" synchronization (compatible with previous versions of VPN-1/FireWall-1)
3. "new style" synchronization on UDP port 8116 (compatible with the High Availability feature described in this section) — this option should be used with caution.

Synchronization is defined in the `$FWDIR/conf/sync.conf` file (see "VPN-1/FireWall-1 State Synchronization" on page 557 of *VPN-1/FireWall-1 Administration Guide*).

The type of synchronization is specified by the `SyncMode` parameter, as follows:

```
SyncMode=mode
```

where *mode* is one of the following values:

TABLE 1-1 SyncMode values

value	meaning
`no sync`	There is no synchronization. This is the default setting, so there is no need to change existing configurations.
`CPHAP`	"new style" synchronization on UDP port 8116. All other lines in the file are ignored. This option should be used with caution.
`TCP sync`	"old style" synchronization (default value). Other lines in the file specify VPN/FireWall Modules with which to synchronize.

If any other value is specified for *mode*, then there is no synchronization and control will not pass to this machine.

Warning – Synchronization must be configured in the same way on all the machines that participate in the High Availability configuration.

If you do not wish to use synchronization, define `no sync` in the `$FWDIR/conf/sync.conf` file and restart VPN-1/FireWall-1.

Using High Availability in Virtual Private Networks

When implementing High Availability, the VPN/FireWall Modules should be defined as members of a gateway cluster in order to:

- synchronize connections and other important information required for VPN Single Entry Point implementation between the VPN/FireWall Modules, and
- ensure that the same Security Policy is installed on all the VPN/FireWall Modules.

For information about configuring the VPN/FireWall Modules as members of a cluster, see "VPN-1/FireWall-1 Configuration (SEP)" on page 235 of *Check Point Virtual Private Networks*.

In a Check Point High Availability configuration, the gateway cluster's IP address (defined in the **General** tab of the **Gateway Cluster Properties** window) should be the non-unique IP address facing the Internet that the gateways share (see FIGURE 1-1 on page 4). The IP address of each of the gateways in the cluster should be defined as the unique address facing the Management Station.

Log Viewer

Every change of a VPN-1/FireWall-1 Module status is recorded as an entry of the Log File and can be viewed with the Log Viewer. See "Log Viewer" on page 389 of *VPN-1/FireWall-1 Administration Guide* for more information

System Status

The status of High Availability modules can be viewed with the System Status Viewer. See "System Status Viewer" on page 369 of *VPN-1/FireWall-1 Administration Guide* for more information.

Commands

The following commands can be used with the High Availability feature:

- `cphastart`
- `cphastop`
- `cphaprob`
- `cpha_export`
- `cpha_import`
- `fw hastat`

cphastart

`cphastart` enables the High Availabilty feature on the machine. In NT, this is done when the VPN/FireWall Module is started. In Solaris, the `cphastart` command is part of the `fwstart` script.

Syntax

```
cphastart
```

cphastop

`cphastop` disables the High Availability feature on the machine.

Syntax

```
cphastop
```

cphaprob

cphaprob defines “critical” processes. When a critical process fails, the machine is considered to have failed.

Syntax

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> register
cphaprob -f <file> register
cphaprob -d <device> unregister
cphaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

Options

parameter	meaning
-d <device>	Add <device> to the list of devices that must be running for the VPN/FireWall Module to be considered active (in other words, if <device> fails, then the VPN/FireWall Module is considered to have failed)
-s	The status to be reported — one of: ■ “ok” — <device> is alive ■ “init” — <device> is initializing (the machine is down) ■ “problem” — <device> has failed
-t <timeout>	If <device> fails to contact the VPN/FireWall Module in <timeout> seconds, <device> will be considered to have failed. To disable this parameter, enter <0> as the timeout value.
-f <file> register	
register	Register <device> as a critical process.
unregister	Unregister <device> as a critical process.
state	Display the state of this VPN/FireWall Module and all the other VPN/FireWall Modules in the High Availability configuration.
-i[a] -e list	Display the state of devices.
report	Report the status of High Availability VPN/FireWall Modules and their status.
if	Display the state of interfaces.

A process specified by <device> should run cphaprob with the "-s ok" parameter to notify the High Availability module that the process is alive. If this notification is not received in <timeout> seconds, the process (and the machine) will be considered to have failed.

Example

This example illustrates how to manually cause a machine to fail and another machine to take over.

1 Verify that the primary machine is currently active with the following command:

```
#cphaprob state
```

Information similar to the following should be displayed:

```
1 (local) <IP-address> active
2         <IP-address> stand-by
```

2 Register a device that initializes with a problem report:

```
#cphaprob -d failDevice -s problem report
```

The machine will immediately fail, and the secondary machine will take over. failDevice is the name of a non-existent device in this case.

3 To reactivate the machine, enter the following command:

```
#cphaprob -d failDevice -s ok report
```

The machine will become active if **Return control to a higher priority machine when it is restored** in the **High Availability** tab (FIGURE 1-2 on page 8) (or the Solaris equivqalent) is checked.

Example

These examples illustrate various uses of the chaprob command.

```
[root@tuti]/opt/CPfw1-41/bin>cphaprob if

hme0       UP
hme1       UP
hme2       UP
```

```
[root@tuti]/opt/CPfw1-41/bin>cphaprob -a if

Required interfaces: 3
Required secured interfaces: 2

hme0       UP
hme1       UP                              (secured)
hme2       UP                              (secured)
```

```
[root@tuti]/opt/CPfw1-41/bin>cphaprob -i list

Built-in Devices:

Device Name: Interface Active Check
Current state: OK

Device Name: HA Initialization
Current state: OK

Registered Devices:

Device Name: sync & filter
Registration number: 0
Timeout: none
Current state: problem
Time since last report: 383.5 sec

Device Name: fwd
Registration number: 1
Timeout: 2 sec
Current state: OK
Time since last report: 0.2 sec
```

```
[root@tuti]/opt/CPfw1-41/bin>cphaprob -i -e list

Registered Devices:

Device Name: sync & filter
Registration number: 0
Timeout: none
Current state: problem
Time since last report: 569.9 sec

Device Name: fwd
Registration number: 1
Timeout: 2 sec
Current state: OK
Time since last report: 0.6 sec
```

cpha_export (Solaris only)

`cpha_export` (usually run on the primary machine) writes MAC address information to `stdout`. If the output is redirected to a file, it can be input (`stdin`) to `cpha_import` on another machine.

Syntax

```
cpha_export
```

cpha_import (Solaris only)

`cpha_import` (usually run on the secondary machines) imports MAC address information from `stdin` and updates the machine's MAC addresses accordingly. The normal procedure is to redirect `stdin` to read a file created by `cpha_export` on the primary machine.

Syntax

```
cpha_import
```

fw hastat

The `fw hastat` command displays information about High Availability machines and their states.

Syntax

```
fw hastat [<target>]
```

Options

parameter	meaning
<target>	A list of machines whose status will be displayed. If target is not specified, the status of the local machine will be displayed.

Additional Configuration Parameters

Cluster ID

If multiple High Availability clusters are defined, and machines from different clusters are connected to the same hub, then you must define, on each machine, the cluster to which it belongs.

To configure this parameter, proceed as follows:

Setting the Cluster ID (NT)

1. Run `regedt32`.
2. Select the **HKEY_LOCAL_MACHINE** window.
3. Browse to the following path:

   HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/CPHA

   This path exists only when the High Availability feature is installed.
4. Make sure “CPHA” key is selected.
5. From the menu, choose **Edit➤Add value**.
6. In the **Add Value** window, enter “ClusterID”.
7. Under **Data Type**, select “REG_DWORD”.
8. Click on **OK**.
9. When asked to enter the value (of the new registry value), enter an integer (default should be 0) that is unique to all the members of that cluster (High Availability configuration).
10. Stop the High Availability Module with the `cphastop` command.
11. Restart the High Availability Module with the `cphastart` command.

Setting the Cluster ID (Solaris)

1. Edit the file `$FWDIR/conf/cpha.conf`.
2. Insert a line:

```
ClusterID X
```

3. Replace `X` with an integer value for this cluster, usually one digit.
4. Save the file.
5. Stop the High Availability Module with the `$FWDIR/bin/cphastop` command.
6. Restart the High Availability Module with the `$FWDIR/bin/cphastart` command.

Setting the Number of Required Interfaces

You can optionally specify the number of interfaces that must be active in order for a machine to be considered available. There is usually no need to do this, because the High Availability feature configures this automatically.

To configure this parameter, proceed as follows:

Setting the Number of Required Interfaces (NT)

Add a "RequiredInterfaces" value to the registry. The procedure is identical to the one given in "Setting the Cluster ID (NT)" on page 19, except that the value is "RequiredInterfaces" instead of "ClusterID".

Setting the Number of Required Interfaces (Solaris)

Add a `RequiredInterfaces` line to `$FWDIR/conf/cpha.conf`. The procedure is identical to the one given in "Setting the Cluster ID (Solaris)" on page 19, except that the value is "RequiredInterfaces" instead of "ClusterID".

Hybrid Mode (Additional Authentication Schemes for IKE)

Overview

IKE supports authentication schemes using pre-shared secrets and certificates. Other authentication schemes (for example, RADIUS, Secure ID Defender, TACACS) are not supported by IKE. The VPN-1/FireWall-1 Hybrid authentication feature extends IKE by enabling it to use any authentication method supported by VPN-1/FireWall-1.

Modifications in the IKE Encryption Scheme

Hybrid mode extends the IKE Encryption protocol, as follows:

During Phase One, the SecuRemote Server unidirectionally authenticates itself to the user using a certificate issued by an Internal CA (see "Internal CA" below). The SecuRemote Server then challenges the user to provide credentials for all authentication schemes supported by the SecuRemote Server. The user provides the requested credentials. If the submitted credentials are valid, the peers initiate Phase Two of the IKE encryption scheme.

Internal CA

An Internal CA issues certificates for SecuRemote Servers. These certificates are used in the Hybrid authentication scheme to authenticate the server to a user.

To create an Internal CA on the Management Station and issue a certificate to a SecuRemote Server, use the `fw internalca` command line.

Note – The internal CA must be created before using IKE.

fw internalca

The `fw internalca` command is run on the Management Station. Before running the `fw internalca` command, stop the Management Server and any VPN/FireWall Module running on the machine. You can restart them after running the `fw internalca` command.

fw internalca create

`fw internalca create` creates (or recreates) an Internal CA, that is:

- initializes the Internal CA database
- generates public and private keys for the Internal CA
- issues a certificate for the Internal CA, and
- saves the certificate

Syntax

```
fw internalca create -dn <CA dn> [-force]
```

Options

parameter	meaning
`-dn <CA dn>`	The Distinguished Name of the Internal CA. The Distinguished Name must include at least the following attributes: organization name and country name.
`-force`	Delete the previously created Internal CA.

Example

```
fw internalca create -dn “o=Intersoft, c=us”
```

fw internalca certify

`fw internalca certify` issues a certificate for a VPN/FireWall Module.

Syntax

```
fw internalca certify -o <object name> [-force]
```

parameter	meaning
-o	a network object name
-force	erases the certificates previously issued for the VPN/FireWall Module

Example

The command:

```
fw internalca certify -o london
```

issues an Internal CA certificate for the VPN/FireWall module “London”.

Forcing IKE Pre-Shared Secret

To authenticate a user in Hybrid Mode, a SecuRemote Server checks the authentication scheme defined for the user. If no other authentication scheme is defined, IKE Pre-Shared Secret will be used by default. In certain cases it may be convenient to force the SecuRemote Server to use IKE Pre-Shared Secret only.

Consider the following scenario: a SecuRemote user is upgraded to IKE but the previous authentication scheme is not disabled. As a result, the SecuRemote Server will prompt the SecuRemote user for an obsolete password.

In another scenario, a VPN-1 administrator may want to define a new authentication scheme for all the users and force IKE Pre-Shared Secret before the task is completed.

To force IKE Pre-Shared Secret as an authentication method, add the `ike_hybrid_force_preshared` parameter to the file `objects.C`. This parameter determines which authentication method the SecuRemote Server will apply in order to establish communication with a SecuRemote Client. In this case, there are two possibilities:

- `ike_hybrid_force_preshared` is `false`. This is the default value for Check Point 2000. If `ike_hybrid_force_preshared` is `false`, the server will challenge the SecuRemote user for any authentication method defined for the user and supported by the SecuRemote Server. If no authentication method is defined, the SecuRemote Server will use IKE Pre-Shared Secret by default.
- `ike_hybrid_force_preshared` is `true`. In this case, the server will use IKE Pre-Shared Secret disregarding any other authentication method configured for the SecuRemote user.

You can force IKE key exchange for a specific SecuRemote user by setting Authentication Scheme to **Undefined** in the **Authentication** tab of the user’s **User Properties** window (FIGURE 1-4 on page 23).

Defining Timeout for User Authentication

The time allocated for user authentication is determined by the `ike_hybrid_user_timeout` parameter in the file `objects.C`.

The `ike_hybrid_user_timeout` parameter specifies the time period within which the client must submit his or her credentials in response to the server's challenge. The desired value between 1 and 300 seconds is entered in parentheses following the parameter, for example:

```
:ike_hybrid_user_timeout(100)
```

The default value is 90 seconds.

Note – The actual timeout period is as much as 36 seconds longer than the time specified by `ike_hybrid_user_timeout` parameter due to retransmissions. For example, if you specify `ike_hybrid_user_timeout (100)`, the actual time allocated for user authentication may be as long as 136 seconds.

Enabling Hybrid Mode

To enable Hybrid mode, proceed as follows:

1 Define an authentication method in the **Authentication** tab of the **User Properties** window (FIGURE 1-4).

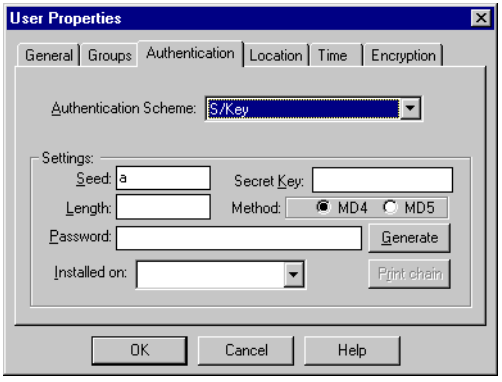


FIGURE 1-4 User Properties windows - Authentication tab showing S/Key authentication

2 In the **VPN** tab of the **Workstation Properties** window, define **IKE** as the encryption method and click on **Edit**.

The **IKE Properties** window is displayed (FIGURE 1-5).

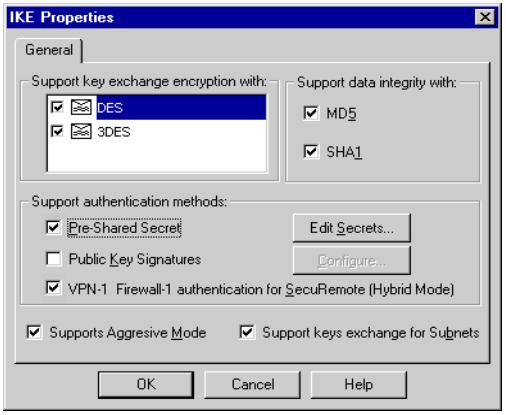


FIGURE 1-5 IKE Properties window

3. Under **Support authentication methods**, check **VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)**.

4. Create an Internal CA on the Management Server (see "Internal CA" on page 21).

5. Issue a certificate for each VPN/FireWall Module.

6. Update the topology on each SecuRemote Client (see "Updating a Site" on page 192 of *Check Point Virtual Private Networks*).

7. To use IKE Pre-Shared Secret, do one of the following:
   - Set the user's authentication method to **Undefined**.
   - Set the `ike_hybrid_force_preshared` property in the `objects.C` file (see "Forcing IKE Pre-Shared Secret" on page 22).

Intel RNG

VPN-1/FireWall-1 and SecuRemote use the Intel RNG (random number generator) hardware (when installed) as a seed for generating cryptographic random numbers.

A special Intel hardware component must be present on the motherboard. Supported Operating Systems are: Windows NT 4.0, Windows 98, Windows 95 (OSR2 or later or Windows 95 with IE 3.02 or later). Please refer to Intel's web site for more details.

To determine whether the Intel RNG is active, use the `fw intelrng` command (on the VPN/FireWall Module) or see **Help➤About** in SecuRemote.

You should install Intel's Security driver from the VPN-1/FireWall-1 installation CD (under 3rd party) or from Intel's web site. If the Security driver installation is taken from Intel's web site, only the full installation — which installs both the driver and the CAPI (Microsoft Cryptographic API) CSP (Cryptographic Service Provider) — should be used.

fw intelrng

`fw intelrng` displays the status of the Intel RNG. This command is a Windows NT only command.

Syntax

```
fw intelrng
```

Examples

```
#fw intelrng
Using Intel(R) Security Driver.
```

```
#fw intelrng
Intel(R) Security Driver not detected.
```

Malicious Activity Detection (MAD)

Overview

VPN-1/FireWall-1's Malicious Activity Detection (MAD) feature provides a mechanism for detecting malicious or suspicious events and notifying the system administrator. This feature is available on the Windows NT and Solaris platforms and is implemented by reading the VPN-1/FireWall-1 Log File and matching Log entries to attack profiles. The VPN-1/FireWall-1 administrator can modify attack detection parameters, turn detection on or off for specific attacks, or disable the MAD feature entirely.

Attacks

TABLE 1-2 lists the attacks for which the Malicious Event Detection feature scans the Log File.

TABLE 1-2 Attack Names and Descriptions

attack name	description
successive_alerts	An excessive number of VPN-1/FireWall-1 alerts have been generated.
port_scanning	An excessive number of attempts to connect to ports on a specific destination IP address from the same source IP address have been detected. This attack is a superset of "blocked_connection_port_scanning" below.
blocked_connection_port_scanning	This attack is similar to the port_scanning attack, but deals only with connections that have been dropped or rejected. The assumption is that if a connection has been accepted then it can be ignored. Activating this attack requires less memory than detecting the port_scanning attack, but some attacks may be missed. There is no reason to activate both the port_scanning and blocked_connection_port_scanning attacks. This attack is a subset of "port_scanning" above.
login_failure	An excessive number of failed attempts to login to a specific destination IP address have been detected from the same source IP address. **Authentication Failure track** in the **Authentication** tab of the **Properties Setup** window should be set to "alert".
successive_multiple_connections	An excessive number of connections opened to a specific destination IP address and port number from the same source IP address have been detected.
land_attack	This is the well-known "land attack".
Additional Attacks — The defenses are pre-defined in VPN-1/FireWall-1, and other parameters defined in the MAD configuration file. Each individual attack is listed as an individual log entry by VPN-1/FireWall-1; MAD enables you to identify successive attacks.	
syn_attack	**Method** in the **SYNDefender** tab of the **Properties Setup** window must be set to either **SYN Gateway** or **Passive SYN Gateway**. For information about this attack, see "What is the TCP SYN Flooding Attack?" on page 617 of *VPN-1/FireWall-1 Administration Guide*.
anti_spoofing	The anti-spoofing properties must be set to alert in the **Security** tab of the interface's **Interface Properties** window (see "Interface Properties Window" on page 105 of *VPN-1/FireWall-1 Administration Guide*).

The meaning of "excessive number" for each attack is defined by the attack-specific parameters (see TABLE 1-4 on page 28).

MAD Configuration File

The configuration is specified in the file `$FWDIR/conf/cpmad_config.conf` on a VPN-1/FireWall-1 Management Station. There are two kinds of parameters:

- global (described in TABLE 1-3)
- attack-specific (described in TABLE 1-4)

A line beginning with # is considered a comment.

Note – The VPN/FireWall Module must be restarted in order for any changes to the configuration file to take effect.

Global Parameters

TABLE 1-3 lists the global parameters that apply to all attacks.

TABLE 1-3 Global Parameters

parameter	meaning
`MAD_system_mode`	Specifies whether VPN-1/FireWall-1 should scan for attacks. The value may be “on” or “off”.
`MAD_memory`	An integer specifying the memory allocated to MAD (in Kbytes). If MAD needs more memory than it has been allocated, it will exit. Memory requirements can be reduced by reducing the number of attacks, increasing the values of the resolution (`MAD_`*`attack_name`*`_resolution`) or decreasing `MAD_clean_interval`.
`MAD_clean_interval`	“Old” events (see `MAD_`*`attack_name`*`_time_interval` below) will be deleted from internal MAD tables every `MAD_clean_interval` seconds. High values reduce CPU usage but increase memory requirements.
`MAD_number_of_connection_attempts`	If the ELA or LEA Server terminates, MAD will try `MAD_number_of_connection_attempts` times to reconnect before exiting.
`MAD_interval_between_connection_attempts`	Specifies the time interval between each reconnection attempt (see “MAD_number_of_connection_attempts” above)

Attack-Specific Parameters

TABLE 1-4 lists the optional attack-specific parameters that can be specified for each attack.

Note – In TABLE 1-4, *attack_name* is a variable that stands for the name of a specific attack. The supported attacks are listed in TABLE 1-2 on page 26.

TABLE 1-4 Attack-Specific Parameters

parameter	meaning
MAD_*attack_name*_mode	Specifies whether VPN-1/FireWall-1 should scan for this attack. The value may be “on” or “off”.
MAD_*attack_name*_time_interval	The interval (in seconds) after which information about an attack will be deleted from the internal tables.
MAD_*attack_name*_repetitions	The number of times an event must occur in MAD_*attack_name*_time_interval seconds in order for MAD_*attack_name*_action to be taken. For example, the successive_alerts attack defense counts the number of alert log entries in the last MAD_successive_alerts_time_interval seconds. If this number is greater than MAD_successive_alerts_repetitions, then MAD_successive_alerts_action is taken.
MAD_*attack_name*_resolution	This parameter is similar to the **Excessive Log Grace Period** parameter in the **Log and Alert** tab of the **Properties Setup** window, and specifies the interval (in seconds) during which identical log entries are considered to have occured at the same time. A large value reduces memory usage but increases the probability that attacks will not be recognized. A value for MAD_*attack_name*_resolution that is greater than MAD_*attack_name*_time_interval has no meaning. For example, if MAD_*attack_name*_resolution is set to 5 seconds, then all identical log entries arriving within 5 seconds of the first one are combined into a single log entry. A log entry arriving 7 seconds after the first one is not combined, but any log entry arriving withing 5 seconds of that log entry is combined with it. Note that the log entries are always individually counted, but they can be combined into a single log entry by this parameter.
MAD_*attack_name*_action	The value may be any of the values “alert”, “mail”, “snmptrap”, “spoofalert”, “useralert” or “userauthalert”, corresponding to the values that can be specified in the **Log and Alert** tab of the **Properties Setup** window.

Example

Following is an an example of a fragment of the `$FWDIR/conf/cpmad_config.conf` file. Note that the attack's name is specified in a comment line (one that begins with the # character).

```
MAD_system_mode = on

# successive_alerts

MAD_successive_alerts_mode = on
MAD_successive_alerts_resolution = 60
MAD_successive_alerts_time_interval = 600
MAD_successive_alerts_repetitions = 100
MAD_successive_alerts_action = alert
```

Installation

The Malicious Event Detection feature is installed on the Management Station as part of the VPN-1/FireWall-1 installation.

Enabling and Disabling MAD

The MAD feature can be enabled or disabled by appropriately modifying the `$FWDIR/conf/cpmad_config.conf` file (that is, by setting `MAD_system_mode` to "on" or "off") and restarting VPN-1/FireWall-1. If for some reason MAD terminates (see "Troubleshooting" on page 30), it can be restarted only by restarting VPN-1/FireWall-1.

ELA Proxy

When the Management Module is started, the ELA proxy is started by default, but it can be stopped without affecting the Management Module. However, the ELA proxy must be running on the machine running MAD.

Troubleshooting

The more common MAD exit error messages (logged to `$FWDIR/log/cpmad.err`) are listed in TABLE 1-5.

TABLE 1-5 MAD Exit Error Messages

message	meaning
attack_name active value is invalid; must be on or off	
`parameter_name` does not exist in configuration file	The specified required parameter is missing from the configuration file (see "MAD Configuration File" on page 27).
`parameter_name` has no value in configuration file	The value of the parameter is not specified in the configuration file (see "MAD Configuration File" on page 27).
`parameter_name` is set to a non-postive value in configuration file	
configuration line `line_num` exceeds maximum allowed length	
configuration line `line_num` does not begin with # or `MAD_`	
ELA failure	Confirm that the ELA proxy is running.
failed to initialize LEA Client	The MAD Module is a LEA Client. Confirm that: ■ VPN-1/FireWall-1 is running. ■ The configuration file (`$FWDIR/conf/cpmad_opsec.conf`) is correct. ■ Port 18184 is not blocked.
failed to initialize LEA Server	Because the MAD Module is a LEA Client, it must be able to communicate with a LEA Server (usually, the Management Station). Confirm that: ■ VPN-1/FireWall-1 is running. ■ The configuration file (`$FWDIR/conf/cpmad_opsec.conf`) is correct. ■ Port 18184 is not blocked.
failed to read `fw.log`	
failed to set environment check `file_location`	This error message usually indicates that the `FWDIR` environment variable has not been set.
Global parameters not set	
Memory overflow - memory usage cannot exceed `max_memory` KBytes.	MAD has run out of memory. See "MAD_memory" on page 27 for more information.

Exit Without an Error Message

If MAD exits without writing an error message, confirm that:

1. The `fwd` process (the FireWall daemon) is running.
2. The `FWDIR` environment variable is correctly set.

CVP Manager

Overview

The CVP Manager application enables a Resource to invoke any number of CVP Servers. This capability is useful when each of the CVP Servers performs a different function.

In addition, identical CVP Servers can be configured to share the load among themselves.

The CVP Manager is defined on the VPN/FireWall Module as a CVP Server (see FIGURE 1-8 on page 32). The CVP Manager's configuration file (see "CVP Manager Configuration File" on page 33) specifies the sequence in which the CVP Servers are invoked, as well as other parameters.

Different Functionality

In the configuration shown in FIGURE 1-6, the CVP Manager invokes the CVP Servers on bigben, tower and bridge, one after the other.

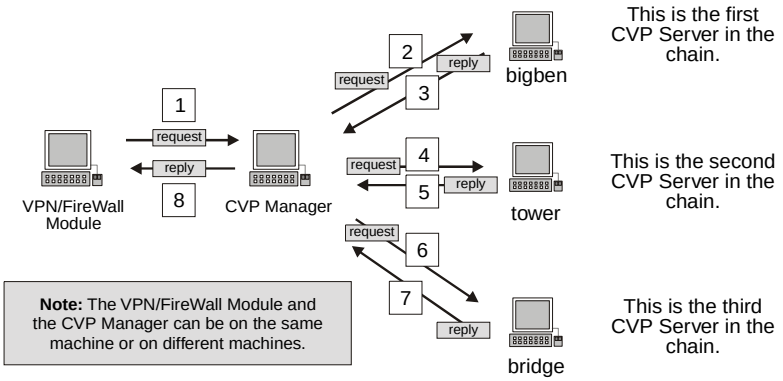


FIGURE 1-6 Three CVP Servers invoked one after the other

The configuration in FIGURE 1-6 is specified in the configuration file in FIGURE 1-9 on page 34.

Load Sharing

In the configuration shown in FIGURE 1-7, the CVP Manager invokes the CVP Server on bigben and then invokes either the CVP Server on tower1 or the CVP Server on tower2.

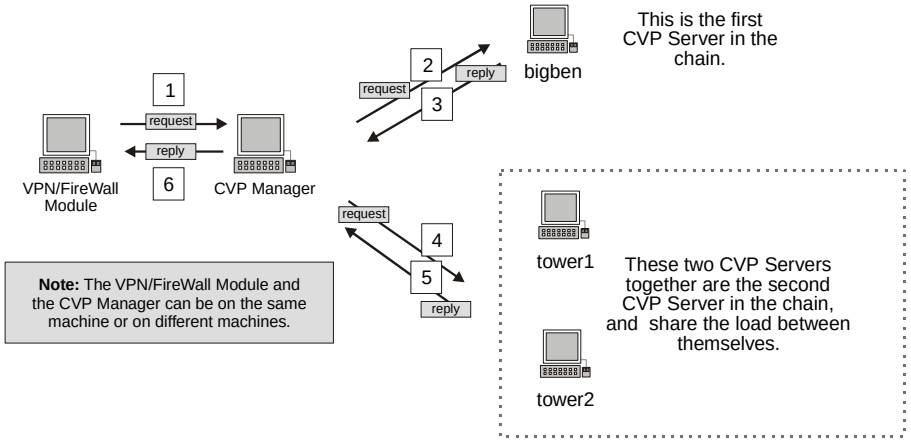


FIGURE 1-7 Three CVP Servers with load sharing

The configuration in FIGURE 1-7 is specified in the configuration file in FIGURE 1-10 on page 35.

Configuration

To configure multiple CVP Servers using the CVP Manager, proceed as follows:

1 Install the CVP Manager, either on the same machine as a VPN/FireWall Module that will be invoking it or on a different machine.

2 On the VPN-1/FireWall-1 Management Station, define the CVP Manager as a CVP Server in the **CVP Server Properties** window (FIGURE 1-8).

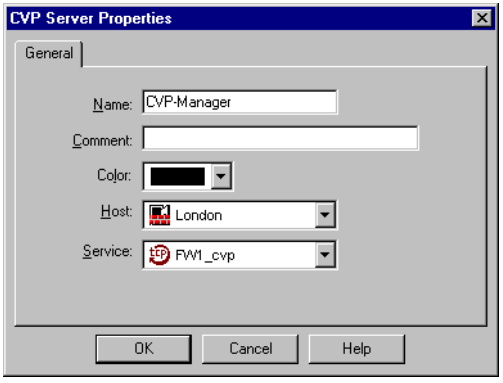


FIGURE 1-8 CVP Server Properties window

3. Configure the chained CVP Servers and specify the sequence in which they are invoked and other parameters.

   The chained CVP Servers are configured in the `cvpm.conf` file on the machine on which the CVP Manager is installed (see "CVP Manager Configuration File" on page 33).

4. Define a Resource that specifies the CVP Manager as the CVP Server.

5. Use the Resource in a rule.

6. Install the Security Policy.

Installation

The CVP Manager is an executable file and is available for the Windows NT and Solaris platforms. The CVP Manager can be installed when VPN-1/FireWall-1 is installed or at a later time.

CVP Manager Configuration File

The configuration is specified in the file `cvpm.conf`, in the directory in which the CVP Manager is installed.

If there are syntax errors in the configuration file, then whenever the CVP Manager is invoked, an error message ("Request could not be handled on Content Security Server") will be displayed on the CVP Manager machine and the user application (Web browser, FTP Client etc.). In addition, the error will be logged to the VPN-1/FireWall-1 Log.

Example

The following configuration file describes the configurations shown in FIGURE 1-6 on page 31 and in FIGURE 1-7 on page 32.

Note – Words in **`bold`** are keywords. In some cases, a number is appended at the end of a keyword (for example, **`chained_server`**_1). The numbers must be consecutive.

The following configuration file describes the configuration shown in FIGURE 1-6 on page 31 (no load sharing).

```
# CVPM Configuration file
# The port for FW-1-to-CVP-M communications
cvpm port 18181

############## Chain configuration
################################################
# 0=continue processing after server replies “unsafe”, 1=stop (drop)
drop_on_unsafe 1

# Recovery time in minutes for load sharing
recovery_time 1

# Number of servers on the chain
num_of_servers 3

chained_server_1 cvp_on_bigben
chained_server_2 tower_cvp_server
chained_server_3 cvp_srv_bridge

############## Server definitions
################################################
cvp_on_bigben port 18181
cvp_on_bigben ip 195.024.205.243

tower_cvp_server port 18181
tower_cvp_server ip 195.024.205.154

cvp_srv_bridge port 18181
cvp_srv_bridge ip 195.024.205.157
```

FIGURE 1-9 CVP Mannager Configuration - No Load Sharing Example

The following configuration file describes the configuration shown in FIGURE 1-7 on page 32 (with load sharing).

```
#  CVPM  Configuration  file

#  The port for FW-1-to-CVP-M communications
cvpm  port  18181

############## Chain configuration
#############################################
#  Number of servers in the chain
num_of_servers  2
chained_server_1    cvp_on_bigben
chained_server_2    tower_servers

#  0=continue processing after server replies “unsafe”, 1=stop (drop)
drop_on_unsafe  1
#  Recovery  time  in  minutes for load sharing
recovery_time    1

##############  Server definitions
#############################################

cvp_on_bigben    port    18181
cvp_on_bigben  ip  195.024.205.243


#  Number  of  servers  of  Load-Sharing
tower_servers  num_of_servers    2

#  The  method  can  be  random  /  round_robin
tower_servers  method round_robin
tower_servers server1 av_on_tower1
tower_servers server2 av_on_tower2

av_on_tower1 port  18303
av_on_tower1 ip  195.024.205.154

av_on_tower2 port  18304
av_on_tower2 ip  195.024.205.154
```

FIGURE 1-10 CVP Manager Configuration - Load Sharing Example

Authenticated Communications (Control Channel)

You can establish a non-SSL authenticated communication (control) channel between the VPN/FireWall Module, the CVP Manager and the CVP Servers by using the `cvpm_putkey` command.

Syntax

```
cvpm_putkey [-port port_number | fw | none] [-p password] <target>
```

Options

parameter	meaning
port	One of the following (see the example for details): ■ port_number — the port number on the CVP Manager (for the connection between the CVP Server and the CVP Manager) ■ fw — for the connection between the CVP Manager and the VPN/FireWall Module ■ none — for the connection between the CVP Manager and a CVP Server
-p password	The key (password). You will be prompted for this field if you do not enter it in the command line.
target	The IP address of the other machine (with which the control channel will be established)

Example

In the configuration shown in FIGURE 1-6 on page 31, if you wish to establish authenticated control channels between the machines, proceed as follows:

1 On the VPN/FireWall Module, enter the following command:

```
fw putkey -p <password> <IP address of CVP Manager>
```

This command, together with the first cvpm_putkey command in step 2, establishes the authenticated control channel between the VPN/FireWall Module and the CVP Manager.

2 On the CVP Manager, enter the following commands:

```
cvpm_putkey -port fw -p <password> <IP address of VPN/FireWall Module>
cvpm_putkey -port none -p <password> <IP address of bigben>
cvpm_putkey -port none -p <password> <IP address of tower>
cvpm_putkey -port none -p <password> <IP address of bridge>
```

The last three cvpm_putkey commands, together with the individual cvpm_putkey commands in step 3 through step 5, establish the authenticated control channels between the CVP Manager and each of the CVP Servers.

3 On bigben, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

4 On tower, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

5 On bridge, enter the following command:

```
cvpm_putkey -port 18181 -p <password> <IP address of CVP Manager>
```

6 In the configuration files on all the machines (see FIGURE 1-9 on page 34, for example) use the `auth_port` parameter instead of the `port` parameter.

Installation

To install the CVP Manager, proceed as follows:

- **NT** — Run `setup.exe` in the `windows\CPcvpm-41` directory on the CD.
- **Solaris** — Run `pkgadd` to install the `CPcvpm-41` package.

After the installation is complete, edit the `cvpm.conf file` (see "CVP Manager Configuration File" on page 33).

To start the CVP Manager, proceed as follows:

- **NT** — Start the CVP Manager Service using the Services Manager in the Control Panel.
- **Solaris** — Run the script `S99cvpm_d` in the `/etc/rc3.d` directory.

Alternatively, reboot the machine.

To remove CVP Manager, proceed as follows:

- **NT** — Use Add/Remove programs in the Control Panel.
- **Solaris** — Run `pkgrm CPcvpm-41`.

  The target directory is not removed by this command.

CVP/UFP Load Sharing

Identical CVP Servers or identical UFP Servers can be configured to share the work load among themselves. The major benefit of load-sharing is that it increases the availability of the CVP Servers or UFP Servers. If one Server fails, other Servers are available to continue working.

Load-sharing can be done using one of two load-sharing schemes:

- round-robin: tasks are assigned to each CVP or UFP Server in turn.

- random: tasks are randomly assigned to the CVP or UFP Servers.

To configure CVP or UFP load-sharing, proceed as follows:

1. Define the CVP Server or UFP Server using the VPN-1/FireWall-1 GUI.
2. Define Resource objects that specify CVP or UFP checking.
3. Define rules in the Rule Base that specify the action taken on connections that invoke each Resource.
4. Install the Security Policy.
5. Substitute multiple Servers to share the work intended for the Server defined in the GUI. To do this, add the following lines to `$FWDIR/conf/fwopsec.conf`. Keywords are in bold typeface.

   a. Enable load-sharing:

   ```
   use_load_share   yes
   ```

   Any value other than `yes` disables load-sharing.

   b. Designate recovery time (in minutes):

   ```
   recovery_time  <min>
   ```

   If VPN-1/FireWall-1 is unable to connect with the Server, it will not attempt to reconnect for `<min>` number of minutes. `<min>` is a positive integer.

   c. Specify the configuration of the Server defined using the VPN-1/FireWall-1 GUI:

   ```
   server        <ip addr>      <port>   opsec
   load_share    <ip addr>      <port>   <configured server>
   ```

   The parameters are explained in the table below:

parameter	meaning
`<configured server>`	The name of the Server defined using the VPN-1/FireWall-1 GUI. This is the Server for which multiple Servers will be substituted.
`<ip addr>`	The Server's IP address in dot format.
`<port>`	The Server's port number.

d Specify the number of Servers that will be used for load-sharing:

```
<configured server>   num_of_servers   <num>
```

<num> number of servers will be sharing the load intended for <configured server>. <configured server> is the same as in step c. <num> is a positive integer.

Warning – If the specified num_of_servers is greater than the actual number of Servers that were defined (see step f), VPN-1/FireWall-1 will fail.

e Select the method to be used for load-sharing:

```
<configured server>   method      random
```

or

```
<configured server>   method      round_robin
```

<configured server> is the same as in step c.

f Specify the name and configuration of each Server doing the load-sharing:

```
<configured server>  servern   <name of server n>

<name of server n>   port       <port for server n>
<name of server n>   ip         <ip addr for server n>
```

The parameters are explained in the table below:

parameter	meaning
<configured server>	The name of the Server defined using the VPN-1/FireWall-1 GUI. This is the same as in step c.
<name of server *n*>	The name of the *n*th Server.
<port of server *n*>	The port number of the *n*th Server.
<ip addr of server *n*>	The IP address of the *n*th Server, in dot format.
server*n*	This is **server1**, **server2**, **server3**... etc. See the warning in step d.

It is strongly recommended that one of the Servers specified in this step be identical to the Server defined using the VPN-1/FireWall-1 GUI (although it should be given two different names). This way, if the load-sharing fails, VPN-1/FireWall-1 will default to this Server.

To establish authenticated connections with these Servers, substitute the keyword `auth_port` for port. Note however that an authenticated connection cannot be established with the default Server.

6 Restart VPN-1/FireWall-1.

Example

Below is an example of `fwopsec.conf`. Note that `cvp_on_bigben` is identical to `my_server`, and therefore functions as the default Server.

```
use_load_share   yes

recovery_time    1

server        199.203.73.6      18181    opsec
load_share    199.203.73.6      18181    my_server

my_server     num_of_servers    2

my_server     method      round_robin

my_server     server1     cvp_on_bigben
my_server     server2     cvp_on_tower

cvp_on_bigben    port    18181
cvp_on_bigben    ip      199.203.72.6

cvp_on_tower     port    18181
cvp_on_tower     ip      192.115.205.154
```

CHAPTER 2

VPN-1/FireWall-1 Overview

In This Chapter

Overview

Internet Firewall Technologies

When you connect your network to the Internet, securing your network against intrusion is of critical importance. The most effective way to secure the Internet link is to put a firewall system between the local network and the Internet. The firewall ensures that all communication between an enterprise's network and the Internet conforms to the enterprise's Security Policy.

In order to effectively provide real security, a firewall must track and control the flow of communication passing through it. To reach control decisions for TCP/IP based services (for example, whether to pass, reject, encrypt or log communication attempts), a firewall must obtain, store, retrieve and manipulate information derived from all communication layers and from other applications.

It is not sufficient to examine packets in isolation. State information — derived from past communications and other applications — is an essential factor in making the control decision for new communication attempts. Both the communication state (derived from past communications) and the application state (derived from other applications) may be considered when making control decisions.

Firewall Requirements

Control decisions require that a firewall be capable of accessing, analyzing and utilizing the following:

1. **communication information** — information from all seven layers in the packet
2. **communication–derived state** — the state derived from previous communications

   For example, the outgoing PORT command of an FTP session could be saved so that an incoming FTP data connection can be verified against it.
3. **application–derived state** — the state information derived from other applications

   For example, a previously authenticated user would be allowed access through the firewall for authorized services only.
4. **information manipulation** — the evaluation of flexible expressions based on all the above factors

VPN-1/FireWall-1 Basic Concepts

Stateful Inspection Technology

Check Point's innovative Stateful Inspection technology implements all the necessary firewall capabilities at the network level. A powerful Inspection Module examines every packet passing through key locations in your network (Internet gateway, servers, workstations, routers or switches), promptly blocking all unwanted communication attempts. Packets do not enter the network unless they comply with the enterprise Security Policy. A powerful auditing mechanism centralizes logs and alerts from the entire system at the system manager's workstation.

VPN-1/FireWall-1 is completely transparent to both users and applications, and coexists with other security tools.

VPN-1/FireWall-1 Inspection Module

The VPN-1/FireWall-1 Inspection Module is inside the operating system kernel, between the Data Link and the Network layers (layers 2 and 3). Since the data link is the actual network interface card (NIC) and the network link is the first layer of the protocol stack (for example, IP), VPN-1/FireWall-1 is positioned at the lowest software layer.

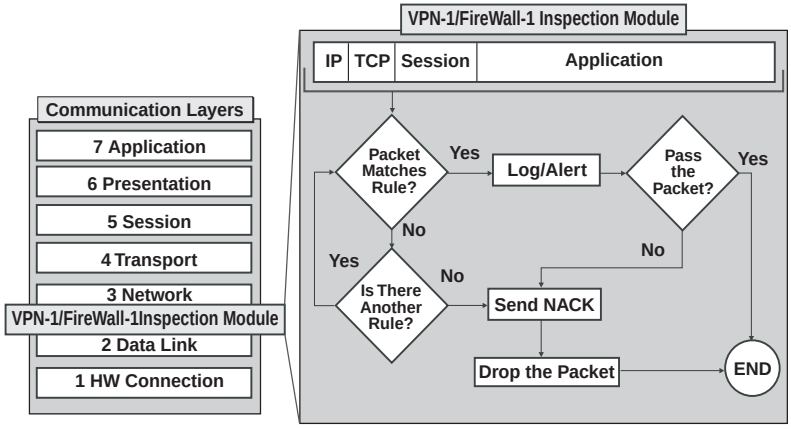


FIGURE 2-1 VPN-1/FireWall-1 Inspection Module

Inspecting at this layer ensures that VPN-1/FireWall-1 Inspection Module intercepts and inspects all inbound and outbound packets on the gateway. Packets are not processed by the higher protocol stack layers unless the Inspection Module verifies that they comply with the Security Policy. VPN-1/FireWall-1 examines IP addresses, port numbers, and any other information required in order to determine whether packets should be accepted, in accordance with the Security Policy.

VPN-1/FireWall-1 accesses and analyzes data derived from all communication layers. This “state” and “context” data is stored and updated dynamically, providing virtual session information for tracking connectionless protocols (for example, RPC and UDP-based applications). Cumulative data from the communication and application states, network configuration and security rules, are used to generate an appropriate action, either accepting, rejecting or encrypting the communication. Any traffic not explicitly allowed by the security rules is dropped by default and real-time security alerts are generated, providing the system manager with complete network status.

VPN-1/FireWall-1 understands the internal structures of the IP protocol family and the applications built on top of them, and is able to extract data from the packet’s application content and store it to provide context in those cases where the application does not provide it. VPN-1/FireWall-1 stores and updates state and context information in dynamic tables. These tables are continually updated, providing cumulative data against which VPN-1/FireWall-1 inspects subsequent communications.

INSPECT Language

Using Check Point's INSPECT language, VPN-1/FireWall-1 incorporates security rules, application, state and communication information into a powerful security system.

INSPECT is an object-oriented, high-level script language that provides the Inspection Module with the enterprise security rules. The Security Policy is defined using VPN-1/FireWall-1's graphical user interface. From the Security Policy, VPN-1/FireWall-1 generates an Inspection Script, written in INSPECT. Inspection Code is compiled from the script and loaded to the Inspection Module on the network's FireWalled enforcement points. Inspection Scripts are ASCII files and can be edited to meet specialized security requirements, though in practice, this capability is rarely needed.

VPN-1/FireWall-1 Architecture

VPN-1/FireWall-1's scalable, modular architecture enables an organization to define and implement a single, centrally managed Security Policy. The enterprise Security Policy is defined at a central management console and downloaded to multiple enforcement points throughout the network.

VPN-1/FireWall-1 consists of the following components:

- Graphical User Interface (GUI)
- Management Server
- FireWall Module

Graphical User Interface (GUI)

An enterprise-wide Security Policy is defined and managed using an intuitive graphical user interface. The Check Point Policy Editor allows you to define a Security Policy in terms of network objects (for example, hosts, networks, gateways, *etc.*) and security rules. The VPN-1/FireWall-1 GUI also includes a Log Viewer and System Status Viewer.

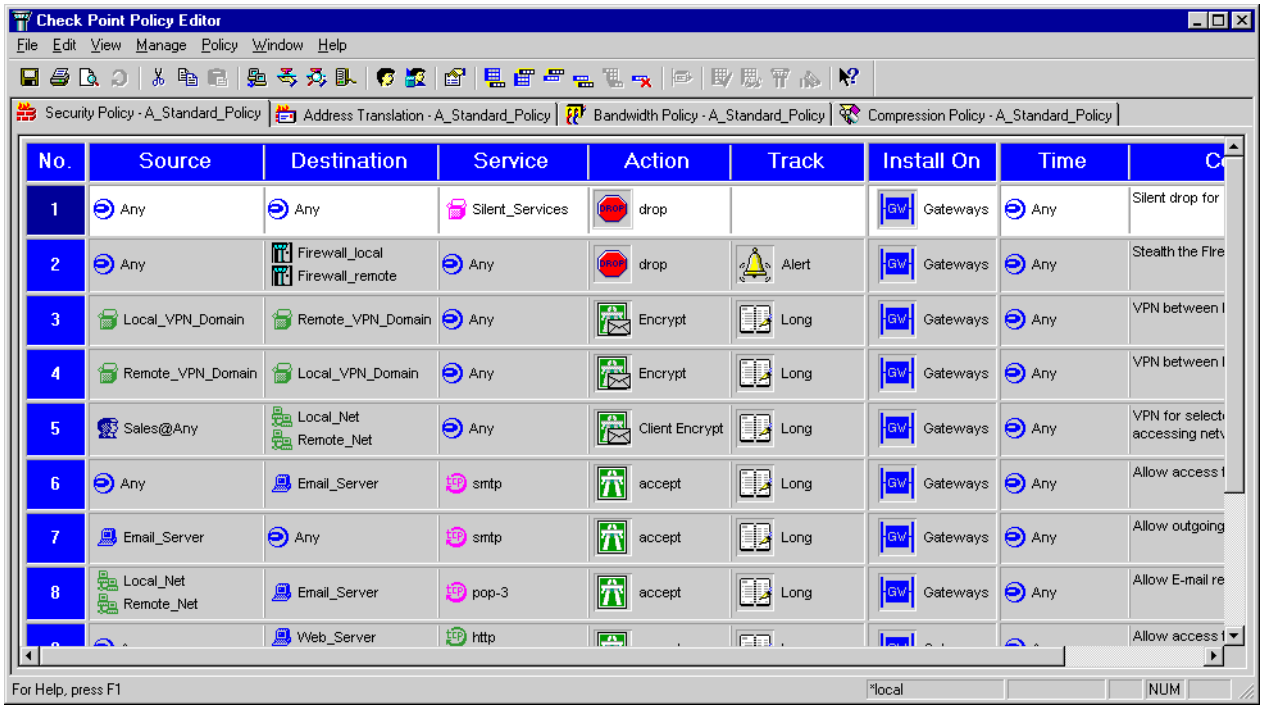


FIGURE 2-2 VPN-1/FireWall-1 Graphical User Interface — Check Point Policy Editor

Management Server

The Security Policy is defined using the GUI and saved on the Management Server. The Management Server maintains the VPN-1/FireWall-1 databases, including network object definitions, user definitions, the Security Policy and log files for any number of FireWalled enforcement points.

The GUI and the Management Server can be deployed on the same machine or in a Client/Server configuration. For a list of supported platforms for the GUI and the Management Server, see “VPN-1/FireWall-1 Platform Summary” on page 66.

FireWall Module

The FireWall Module is deployed on Internet gateways and other network access points. The Security Policy is defined using the GUI and saved to the Management Server. An Inspection Script, written in INSPECT, is generated from the Security Policy. Inspection Code is compiled from the script and loaded to the FireWall Module, which protects the network. The FireWall Module can be installed on a broad range of platforms. For more information, see “VPN-1/FireWall-1 Platform Summary” on page 66.

The FireWall Module includes the Inspection Module and the VPN-1/FireWall-1 Security Servers. The Inspection Module examines all communications according to an enterprise Security Policy. The Security Servers provide Authentication and Content Security features at the application level. A host is considered a FireWalled enforcement point if a FireWall Module or an Inspection Module is installed on that host.

Security Servers

Authentication

The Security Servers provide authentication for users of FTP, HTTP, TELNET and RLOGIN. If the Security Policy specifies user authentication for any of these services, the Inspection Module diverts the connection to the appropriate Security Server. The Security Server challenges the user for a user name and password. If authentication is successful, the Security Server opens a second connection to the target server. For more information on VPN-1/FireWall-1 authentication features, see “Authentication” on page 57.

Content Security

Content Security is available for HTTP, FTP and SMTP.

- **HTTP**

  The HTTP Security Server provides Content Security based on schemes (HTTP, FTP, GOPHER, etc.), methods (GET, POST, etc.), hosts (for example, “*.com”), paths, and queries. A file can be specified that contains a list of IP addresses and paths to which access will be denied or allowed.

- **FTP**

  The FTP Security Server provides Content Security based on FTP commands (PUT/GET), file name restrictions, and anti-virus checking for files transferred.

- **SMTP**

  The SMTP Security Server provides Content Security based on “From” and “To” fields in the mail envelope and header and attachment types. In addition, it provides a secure SMTP application that prevents direct online connection attacks. The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the “From” field, while maintaining connectivity by restoring the correct addresses in the response.

For more information on the above features, see “Content Security” on page 60.

Distributed Client/Server Deployment

VPN-1/FireWall-1 manages the enterprise Security Policy through a distributed Client/Server architecture that ensures high performance, scalability and centralized control. VPN-1/FireWall-1 components can be deployed on the same machine or in flexible

Client/Server configurations across a broad range of platforms (see “VPN-1/FireWall-1 Platform Summary” on page 66). FIGURE 2-3 shows a distributed Client/Server configuration.

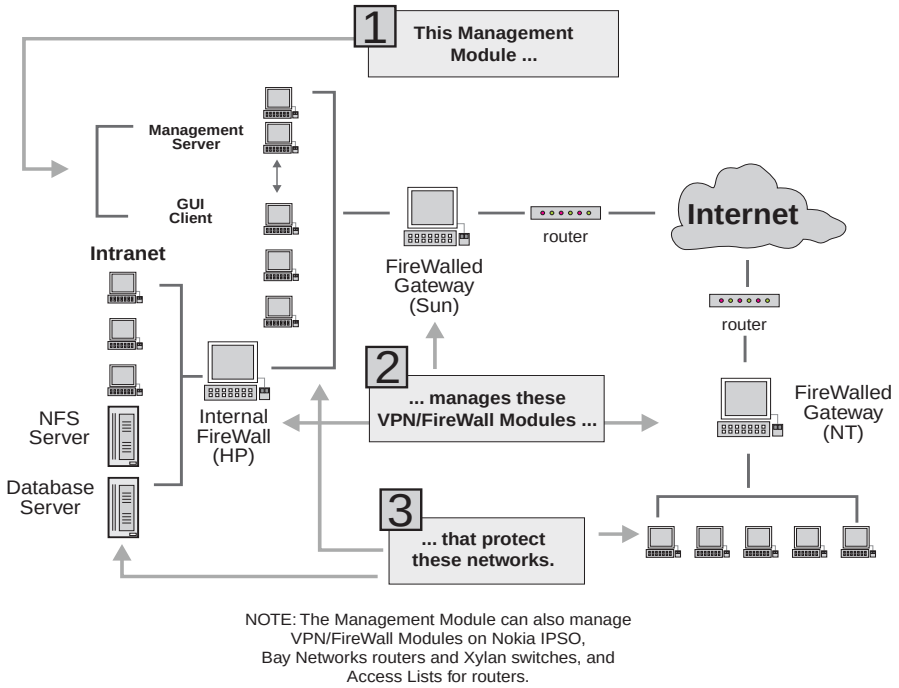


FIGURE 2-3 Distributed Client/Server Configuration

In this configuration the Security Administrator configures and monitors network activity for several sites from a single desktop machine. The Security Policy is defined on the GUI Client, while the FireWall database is maintained on the Management Server. The Security Policy is downloaded to three FireWall Modules (each on a different platform), which in turn protect three networks. The connections between the client, server and multiple enforcement points are secured, enabling true remote management.

Although VPN-1/FireWall-1 is deployed in a distributed configuration, Security Policy enforcement is completely integrated. Any number of FireWall Modules can be configured, monitored and controlled from a single workstation, but there is still only one enterprise-wide Security Policy that is defined and updated from a centralized management interface.

Enterprise Security Management

Defining a Security Policy — Check Point Policy Editor

The Check Point Policy Editor enables an enterprise to easily define a comprehensive Security Policy. A VPN-1/FireWall-1 Security Policy is defined in terms of a Rule Base and Properties.

Rule Base

A Rule Base is an ordered set of rules against which each communication is checked. Each rule specifies the source, destination, service and action to be taken for each communication — for example, whether it is permitted or denied. A rule also specifies how a communication is tracked — for example, a specific event can be logged and then trigger an alert message.

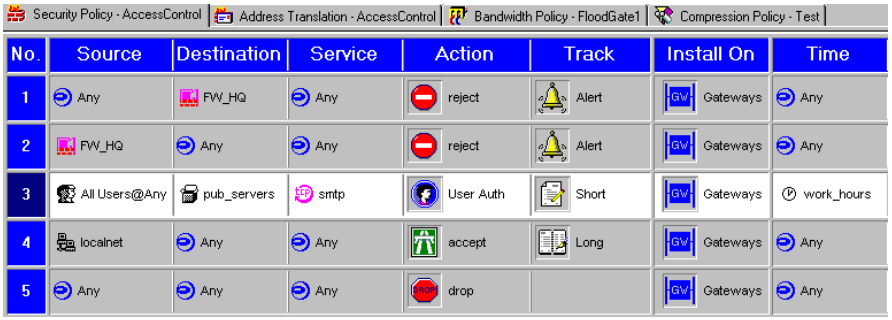


FIGURE 2-4 Rule Base — Security Rules

The tabs displayed in the Check Point Policy Editor depend on the products licensed. For example, if only VPN-1/FireWall-1 is licensed, then only the Security Policy Rule Base and Address Translation Rule Base tabs are displayed. (For more information on the Address Translation Rule Base, see “Network Address Translation” on page 58.) If FloodGate-1 is enabled, then the Policy Editor displays the Bandwidth Rules tab. For information on Bandwidth Rules, see Chapter 5, “Introduction to FloodGate-1.”

Properties

Properties specify general aspects of communication inspection, such as authentication session timeout periods, or how VPN-1/FireWall-1 handles established TCP connections. Properties are applied to all rules, so there is no need to specify repetitive details in the Security Policy.

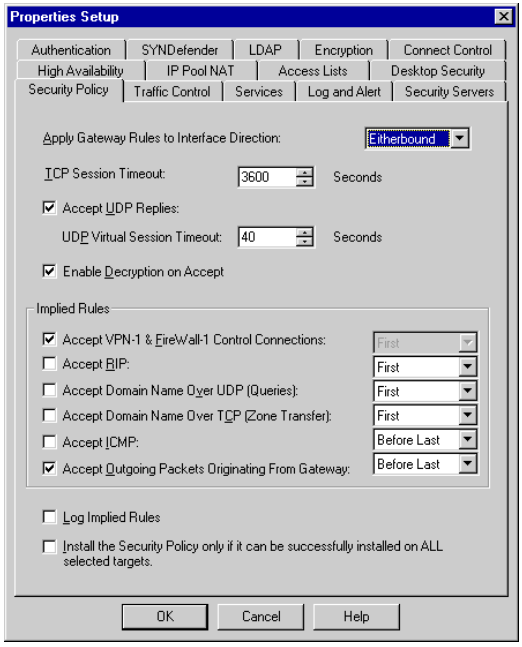


FIGURE 2-5 Properties Setup Window

Network Objects

The Rule Base Editor allows administrators to define network resources in terms of simple objects (for example, gateways, networks, routers or services) and their properties. Each object has a set of attributes, such as name or IP address. Network objects are easily defined and then used in the Rule Base.

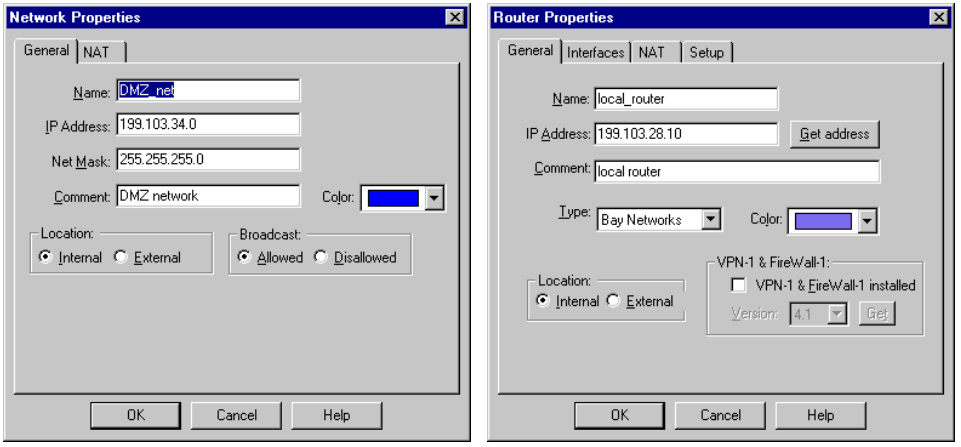


FIGURE 2-6 Network and Router Object Definitions

The Network Object Manager allows you to define the entities that are part of the Security Policy. Only those objects that are part of the Security Policy must be defined by the user. These include:

- networks and sub-networks
- hosts and gateways
- servers
- routers
- switches
- Internet domains
- logical servers (among which a processing load can be distributed automatically)
- Integrated FireWalls
- groups of the above

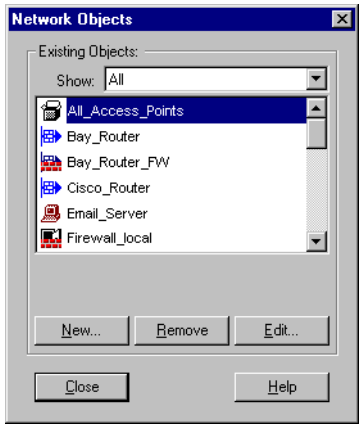


FIGURE 2-7 Network Object Manager window

Users

VPN-1/FireWall-1 enables access privileges to be defined for users on an individual or group basis. User groups can be created, and access privileges, including allowed sources and destinations as well as user authentication schemes, can be defined.

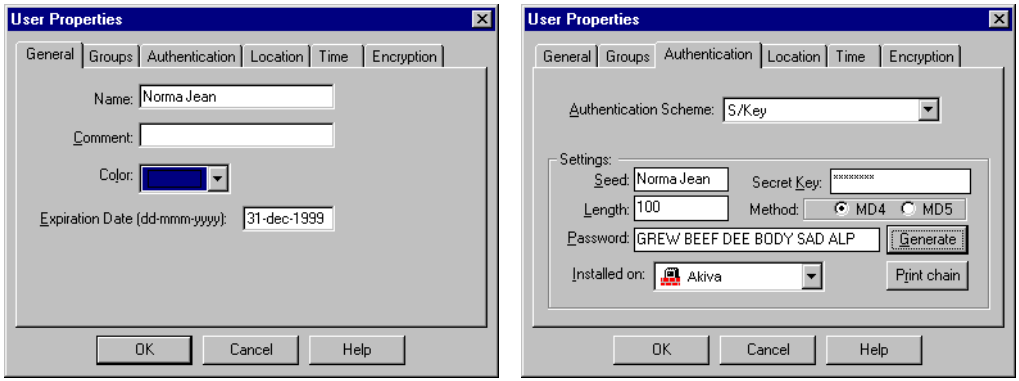


FIGURE 2-8 User Properties window

Services

The Service Manager (FIGURE 2-9) defines the services known to the system and used in the Security Policy. All network services are screened and controlled, even those that are not defined. VPN-1/FireWall-1 includes a comprehensive set of predefined TCP/IP and Internet services, including the following:

- Standard arpa-services: Telnet, FTP, SMTP, etc.
- Berkeley r-services: rlogin, rsh, etc.
- SunRPC services: NIS/yellow pages, NFS, etc.

- Advanced Internet protocols such as HTTP, Gopher, Archie and many others
- IP services: Internet Control Message Protocol (ICMP), Routing Internet Protocol (RIP), SNMP, etc.

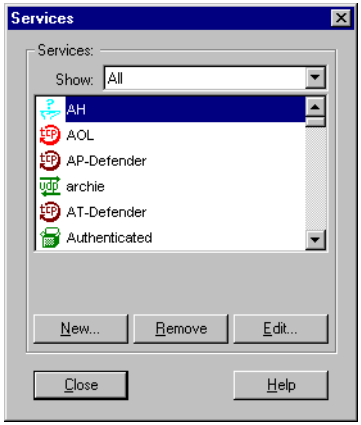


FIGURE 2-9 Services window

New services can be defined by selecting the service type and setting the service's attributes. Services can be grouped in families and hierarchies to facilitate management. VPN-1/FireWall-1 includes the following service types:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Remote Procedure Call (RPC)
- Internet Control Message Protocol (ICMP)
- Others — enables definition of services and protocols that do not conform to the standard set of attributes. Services are defined using simple expressions and macros.

Log Viewer: Visual Tracking and Accounting

VPN-1/FireWall-1's graphical Log Viewer provides visual tracking, monitoring and accounting information for all connections logged by the FireWalled gateways. On-line viewing features enable real-time monitoring of network activity. The Log Viewer provides control over the log file display, providing quick access to information.

Administrators can customize the Log Viewer to display or hide specific fields or events. Logs and log records can be filtered and searched to quickly locate and track events of interest.

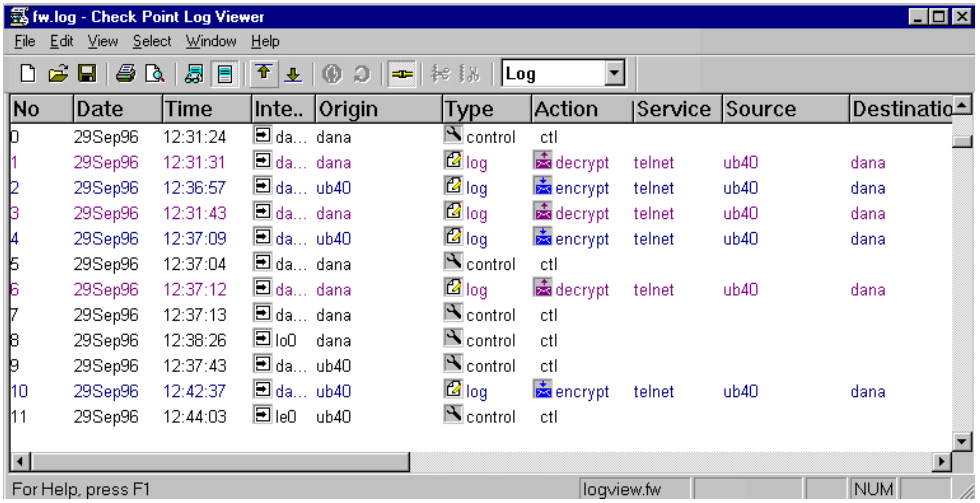


FIGURE 2-10 Log Viewer

The Log Viewer also allows administrators to identify suspicious connections and terminate active and future connections from a specific IP address.

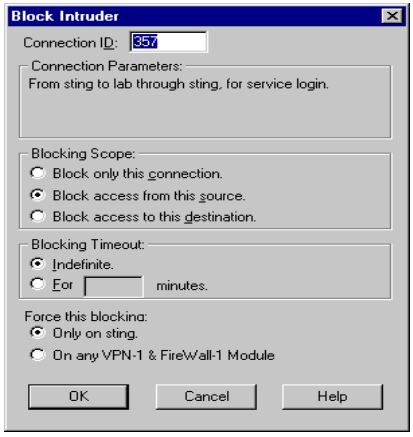


FIGURE 2-11 Blocking Suspicious Connections

The Check Point OPSEC framework provides the Log Export Application (LEA) API for exporting VPN-1/FireWall-1 Log data to other applications (for example, spreadsheets or databases). Reporting and event-analysis applications are available from multiple OPSEC partners.

Real-time Monitoring: System Status Viewer

The System Status Viewer window displays a snapshot of all the FireWalled and FloodGated systems throughout the enterprise, enabling real-time status and alerting. The System Status window also provides traffic statistics — the number of packets inspected, logged or rejected — for each host. Administrators can also specify an action to be taken if the status of a FireWalled host changes. For example, VPN-1/ FireWall-1 can issue an alert notifying system managers of any suspicious activity.

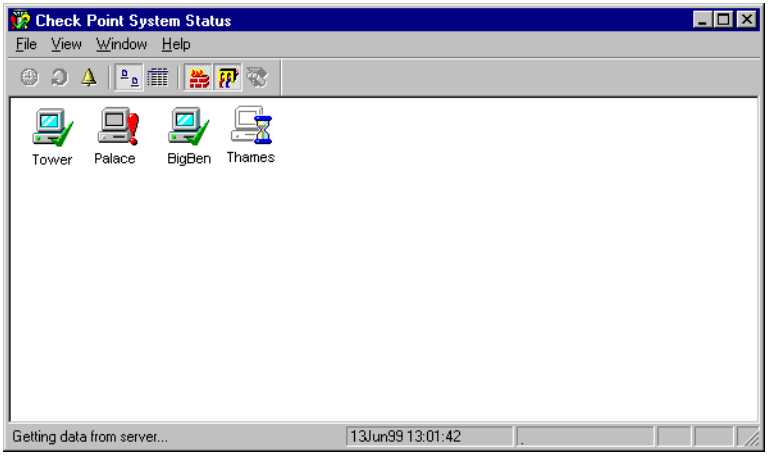


FIGURE 2-12 System Status Window

Security and Network Management

In addition to highly granular access control, VPN-1/FireWall-1 includes security and network management features that are fully integrated into the enterprise-wide Security Policy and managed through the graphical user interface. The VPN-1/ FireWall-1 Security Suite includes the following capabilities:

- Authentication
- Network Address Translation
- Virtual Private Networks
- Content Security
- ConnectControl (Server Load Balancing)
- LDAP Account Management
- Open Security Extension (Third-party Device Management)
- High Availability

Authentication

VPN-1/FireWall-1 provides local and remote users secure, authenticated access to network resources. Flexible authentication methods provide access for users of any IP application or service. Administrators can determine how each individual is authenticated, which servers and applications are accessible and the times during which the user is granted access.

FIGURE 2-13 User Authentication Rule

Multiple Authentication Schemes

VPN-1/FireWall-1 supports the following authentication schemes:

- VPN-1/FireWall-1 Password
- OS Password
- S/Key
- SecurID tokens
- RADIUS
- Axent Pathways Defender
- TACACS/TACACS+
- Digital Certificates

Authentication Methods

VPN-1/FireWall-1 provides the following authentication methods:

- **User Authentication**

  User Authentication provides access privileges on a per user basis for FTP, TELNET, HTTP, and RLOGIN, regardless of the user's IP address. If a local user is temporarily away from the office and logging in on a different host, the administrator can define a rule that allows that user to work on the local network without extending access to all users on the same host. User Authentication is transparent — the user does not have to explicitly connect to the FireWalled gateway but can initiate a connection directly to the target server.

- **Client Authentication**

  Client Authentication allows access from a specific IP address. The user working on a client performs the authentication by successfully meeting an authentication challenge, but it is the client machine that is granted access. Client Authentication is available for any service. Flexible sign-on methods allow users transparent or non-transparent access, depending on the properties of the Client Authentication rule.

- **Session Authentication**

  Session Authentication can be used to transparently authenticate any service on a per-session basis. After the user initiates a connection to a server behind the FireWalled gateway, VPN-1/FireWall-1 opens a connection with a Session Authentication Agent. The Agent challenges the user for a proper authentication

response before VPN-1/FireWall-1 allows the connection to continue to the requested server. The Session Authentication Agent is installed on the authenticating client or on another machine in the network.

Transparent User-to-Address Mapping (UAM) Service

VPN-1/FireWall-1 integrates with Check Point's IP address management solution — Meta IP — to deliver transparent single sign-on for network access. The UAM service of Meta IP captures both Windows NT login information and dynamically assigned IP addresses. This mapping of user identity and IP address is made available to VPN-1/FireWall-1 to enforce user-level security policies. With full authentication information from the UAM server, VPN-1/FireWall-1 does not have to challenge users each time they request a connection through the FireWall.

For more information on Meta IP, see Chapter 8, "Meta IP" in this book.

Network Address Translation

VPN-1/FireWall-1's flexible Network Address Translation features provide complete Internet access for internal hosts with invalid or private IP addresses. VPN-1/FireWall-1's dynamic address translation hides invalid internal addresses behind a single IP address, while static address translation maps each invalid internal address to a corresponding valid address.

VPN-1/FireWall-1 provides the following methods for configuring Address Translation:

- Graphical Address Translation Rule Base
- Automatic Configuraton

Graphical Address Translation Rule Base

VPN-1/FireWall-1's graphical user interface simplifies the definition and implementation of Address Translation. A flexible Address Translation Rule Base allows administrators to specify objects by name rather than by IP address. Administrators can apply rules to specific destination IP addresses, source IP addresses or services.

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	MyNetwork	Any	Any	nat	= Original	= Original	Gateways
2	IllegalAddresses	Any	Any	LegalAddresses	= Original	= Original	Gateways
3	Any	LegalAddresses	Any	= Original	IllegalAddresses	= Original	Gateways
4	Any	DMZ-Servers	StandardPorts	= Original	= Original	NonStandardPorts	Gateways

FIGURE 2-14 Address Translation Rule Base

Automatic Configuration

Address Translation properties are defined for specific network objects, such as workstations or networks. Address Translation rules are then automatically generated from these properties.

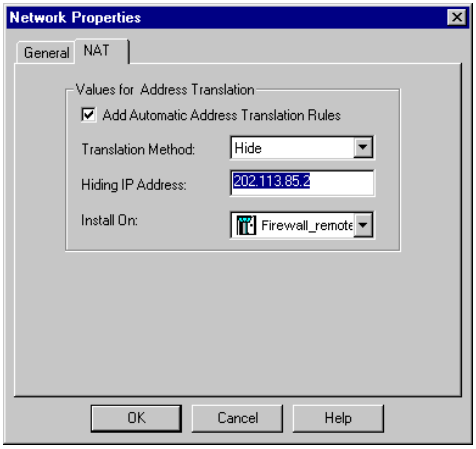


FIGURE 2-15 Automatically Generating Address Translation for a Network

Virtual Private Networks

Preventing break-ins is only one of the goals of an enterprise's network Security Policy. Along the dynamic, constantly changing path linking a communication's source and its destination, there are many opportunities for unscrupulous individuals to eavesdrop on communications or even to tamper with them. An enterprise wishing to protect the confidentiality and integrity of its data must add another layer of protection to its Security Policy: encryption and authentication.

Privacy is an issue not only for communications on public networks but also on private networks, since many private networks also use public carriers for some segments.

VPN-1/FireWall-1's optional VPN (Virtual Private Network) module protects communications on the Internet and enables an enterprise to build its own easy-to-maintain Virtual Private Network (VPN) using private and public network segments.

VPN-1/FireWall-1 provides the ideal platform for enterprise VPN deployments, encrypting communications to guarantee data privacy and security. In addition to site-to-site VPN capability, VPN-1 Gateway deployments can provide access to remote users when used with Check Point's VPN-1 SecuRemote Client software. For more information on the SecuRemote Client, see *Check Point Virtual Private Networks*.

Check Point's VPN-1 Gateway product supports industry-standard algorithms and protocols, such as DES, Triple DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments. VPN-1 Gateway is one component in a group of VPN products. For more information, see *Check Point Virtual Private Networks*.

Content Security

VPN-1/FireWall-1 provides powerful Content Security for HTTP, SMTP and FTP connections, including anti-virus checking for transferred files, access control for specific network resources (for example, URLs, files *etc*.) and SMTP commands. Content Security is defined using Resource objects and implemented by the Security Servers. Check Point's OPSEC framework also provides open APIs for integrating third-party content screening applications.

Resources

A Resource object defines a group of entities accessed by a specific protocol. Resource definitions are based on HTTP, FTP and SMTP. For example, a URI (Uniform Resource Identifier — based on HTTP) Resource may specify a group of Web sites accessed through HTTP or FTP.

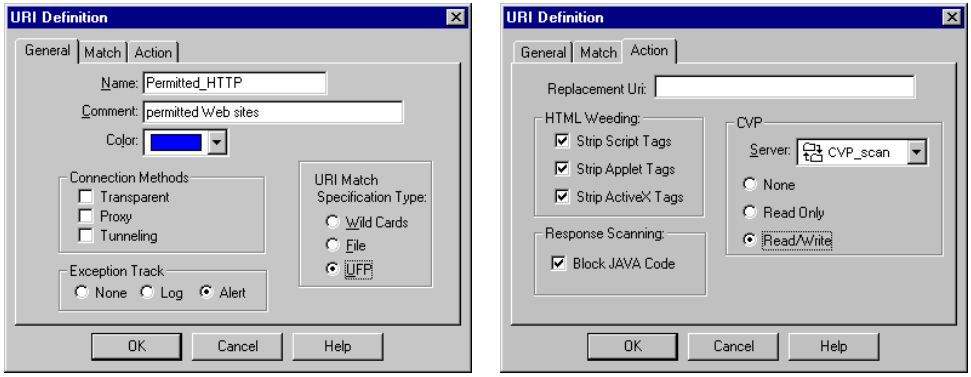


FIGURE 2-16 URI Resource Definition tabs

Resources can be used in a Rule Base in the same way as a service (see FIGURE 2-17 on page 60). When a connection matches a rule with a Resource, the VPN-1/FireWall-1 Inspection Module diverts the connection to the appropriate Security Server. The Security Server can then query a third-party server, such as a URL filtering server, which performs the required content inspection. VPN-1/FireWall-1 processes the original connection depending on the reply from the server and the action in the rule.

FIGURE 2-17 URI Resource Rule

Anti-virus Inspection

Anti-virus inspection is vital to enterprise security. VPN-1/FireWall-1 integrates third-party anti-virus applications through the Content Vectoring Protocol (CVP) API. For example, if an FTP Resource definition specifies anti-virus checking, VPN-1/FireWall-1 intercepts FTP attempts and sends the transferred files to a CVP server, which examines the files. VPN-1/FireWall-1 processes the original connection depending on the results.

URL Screening

URL screening provides precise control over Web access, allowing administrators to control access to undesirable or inappropriate Web pages. VPN-1/FireWall-1 checks Web connection attempts using third-party URL Filtering Protocol (UFP) servers. The UFP API is used to integrate UFP servers that maintain lists of URLs and their categories
(for example, alcohol, gambling, etc.). URL databases can be updated to provide current lists of unacceptable sites.

Java and ActiveX Stripping

VPN-1/FireWall-1's extensive screening capabilities effectively protect enterprise networks from Java and ActiveX attacks. VPN-1/FireWall-1's flexible Resource definition allows administrators to:

- strip Java applets and script from HTML pages
- strip ActiveX tags from HTML pages
- block Java code from incoming HTTP

VPN-1/FireWall-1 also integrates Java screening capabilities of third-party applications.

High Availability

FireWall Modules maintain information on authorized connections in dynamic state tables. When multiple FireWall Modules are deployed throughout the enterprise network, the connection information from each FireWall Module can be shared by all other modules. Sharing state information provides each FireWall Module with full awareness of all enterprise communications.

VPN-1/FireWall-1's High Availability feature leverages the sharing of state information to provide fault tolerance. If a FireWall Module fails, either due to a hardware or software problem, another FireWall Module can take over all the communications of the failed module without dropping any connections.

Utilizing multiple FireWall Modules with state table synchronization has the additional benefit of providing asymmetric routing support. The synchronization of state information is necessary when packets that are part of the same session travel via different routes and pass through different gateways. Without accurate state information on all communications, a FireWall Module may not recognize a packet that is part of an authorized session and will drop or reject that packet.

LDAP Account Management

Check Point's Account Management module integrates user information maintained in LDAP (Lightweight Directory Access Protocol) directories into the VPN-1/FireWall-1 framework. With the Account Management module, VPN-1/FireWall-1 applies user-level security data retrieved from an LDAP-compliant server to enforce the Security Policy.

LDAP users and servers can be defined and used in the Rule Base like any other network object. For example, when a user connects to the local network through the FireWalled gateway, the FireWall Module queries the LDAP database to obtain user data. In this way, VPN-1/FireWall-1 uses information from LDAP servers without the need to import large user databases.

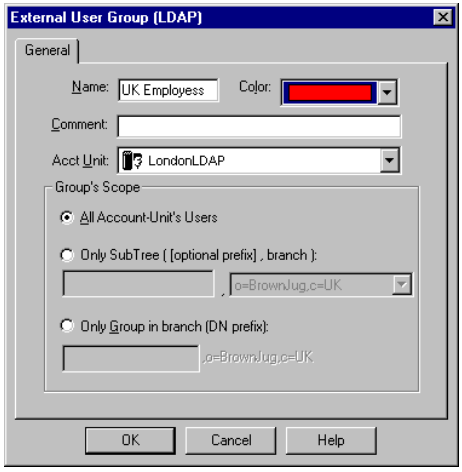


FIGURE 2-18 External User Group (LDAP) window

The Account Management system includes a Java-based graphical user interface for managing LDAP users. The Account Management Client can be launched from the VPN-1/FireWall-1 GUI or as a standalone application. Administrators can use the Account Management Client to define "live templates" that can be used to apply common configuration properties to multiple users. Changes to the template are

automatically applied to all users associated with the template. All communication between VPN-1/FireWall-1, the Account Management Client and LDAP servers is secured through SSL.

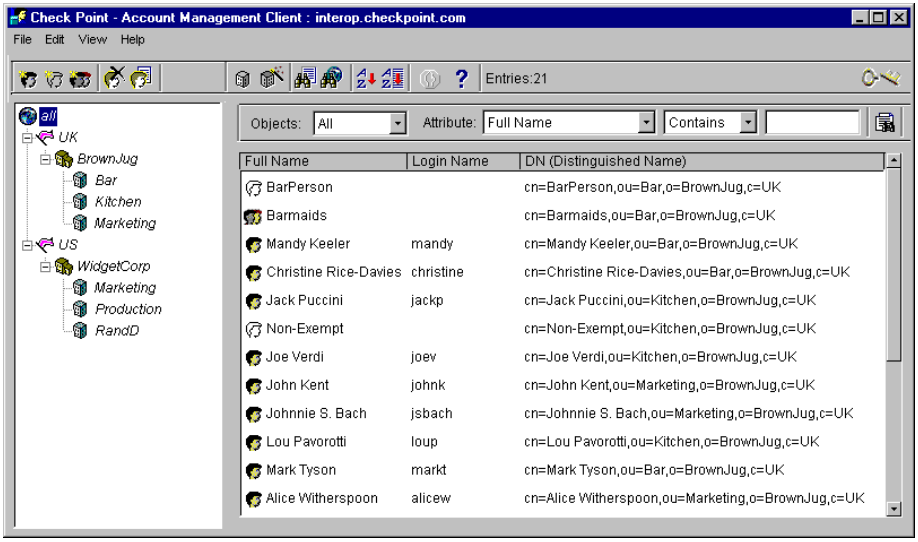


FIGURE 2-19 Account Management Client

Open Security Extension

Check Point's Open Security Extension is an optional module that enables VPN-1/FireWall-1 to manage an enterprise-wide Security Policy for a variety of third-party network security devices, including products from Cisco, Nortel (Bay Networks), 3Com and Microsoft. The Security Policy is defined using the VPN-1/FireWall-1 Rule Base Editor. VPN-1/FireWall-1 then generates Access Control Lists (ACLs) and downloads them to selected routers and devices. There is no need to configure separate ACLs for each device.

With Open Security Extension, VPN-1/FireWall-1 also imports existing Access Lists and compiles them into object-oriented security policies for simpler management. In addition, VPN-1/FireWall-1 displays syslog messages from third-party security devices in the graphical Log Viewer, delivering centralized logging and reporting capability. With Open Security Extension, devices from multiple vendors are seamlessly integrated into the network and managed through the Security Policy.

FIGURE 2-20 Router Access List Import Options

Enterprise Traffic Management

FloodGate-1

Check Point FloodGate-1 is a policy-based enterprise bandwidth management solution for VPN, Private WAN, and Internet links. It ensures reliable network performance for business critical traffic such as VPN, ERP, e-commerce, and telephony by prioritizing them over discretionary traffic. Bandwidth is precisely controlled based on an intuitive combination of weighted priorities, guarantees, and limits. With FloodGate-1, organizations can realize the cost savings of shared links, without sacrificing the performance for critical traffic. FloodGate-1 integrates with Check Point's network security solutions.

For information on FloodGate-1, see Chapter 5, “Introduction to FloodGate-1.”

ConnectControl — Server Load Balancing

VPN-1/FireWall-1’s optional ConnectControl module enhances network connectivity through advanced server load balancing. VPN-1/FireWall-1 implements load balancing using a Logical Server object, which is a group of servers providing the same service.

Administrators can define a rule directing connections of a particular service to the appropriate Logical Server. Although a Logical Server may consist of several servers, the client is aware of only one server.

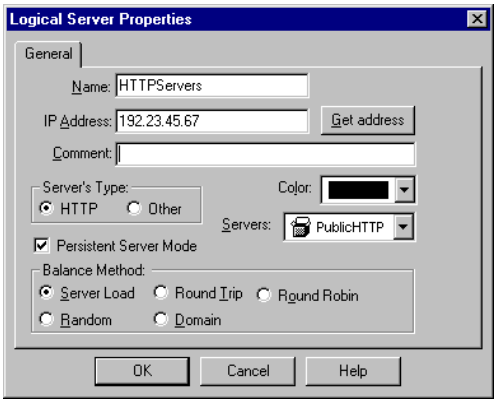


FIGURE 2-21 Logical Server Properties Definition

The Logical Server handles the connection attempt using one of the following load balancing algorithms:

- **server load** — VPN-1/FireWall-1 queries the servers to determine which is best able to handle the new connection. There must be a load measuring agent on the server.
- **round trip** — VPN-1/FireWall-1 uses PING to determine the round-trip times between the FireWall and each of the servers and chooses the server with the shortest round trip time.
- **round robin** — VPN-1/FireWall-1 simply assigns the next server in the list.
- **random** — VPN-1/FireWall-1 assigns a server at random.
- **domain** — VPN-1/FireWall-1 assigns the “closest” server, based on domain names.

VPN-1/FireWall-1 Platform Summary

TABLE 2-1 lists the OS platforms on which VPN-1/FireWall-1 is supported.

TABLE 2-1 Platform Summary

Component	Platforms
GUI Client	■ Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ X/Motif (Solaris, HP-UX 10.20, IBM AIX)
Management Module, VPN/FireWall Module, SecureServer	■ Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ Solaris 2.6, Solaris Operating Environment 7 (formerly known as Solaris 2.7) in 32 bit installation mode only — SPARC and x86 ■ HP-UX 10.20, 11.0 ■ IBM AIX 4.2.1, 4.3.2 ■ Red Hat Linux 6.1 with kernel version 2.2.x
SecureClient, SecuRemote	Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only

Conclusion

To summarize, VPN-1/FireWall-1's sophisticated technology includes a number of unique features:

Stateful Inspection Technology

By firewalling at the lowest software layer, VPN-1/FireWall-1 ensures that the Firewall Module intercepts and inspects all inbound and outbound packets on all FireWalled hosts. The Firewall Module can inspect all the information in the message, and understands the internal structures of the IP protocol family and applications built on top of them. VPN-1/FireWall-1 is able to extract data from the packet's application content and store it to provide context in those cases where the application does not provide it. VPN-1/FireWall-1 can perform any logical or arithmetic operation required to implement the Security Policy.

Transparency and Efficiency

The generic and flexible underlying FireWall Module is capable of learning and understanding any protocol, as well as adapting to newly defined protocols and applications. This capability is achieved by using high-level definitions, and requires no code changes.

VPN-1/FireWall-1 is transparent to applications and users.

In addition, VPN-1/FireWall-1 provides a sophisticated anti-spoofing feature which detects spoofed packets by ensuring that the interface on which a packet arrives corresponds to its IP address.

Authentication

VPN-1/FireWall-1 implements strong User, Client and Session Authentication using different authentication schemes. All components of the Security Policy are fully integrated with the Rule Base, the object-oriented GUI and the Log Viewer.

Simplicity

VPN-1/FireWall-1 provides two compatible user interfaces — graphic and command-line — for user interaction and OS integration. In-band and out-of-band secure management is supported.

VPN-1/FireWall-1's rule–based design enables users to define a Security Policy in terms of simple objects and relationships between them. Only the network objects used in the Rule Base need be defined by the user, and a comprehensive list of pre-defined services is available.

The FireWall Module is implemented as an independent compact code module, and resides inside the operating system kernel as a loadable kernel level module. Because it is inside the operating system kernel, the FireWall Module is efficient and introduces no additional memory requirements or context switch overhead.

Manageability

Enterprise-wide security (between different departments in the same enterprise), server security and inter-network security can be managed by VPN-1/FireWall-1 with equal facility. Secure distributed management is seamlessly integrated into VPN-1/FireWall-1. Though different parts of the Security Policy are implemented at different layers and even on different computers, there is still only one integrated Security Policy, one Rule Base and one centralized logging and alerting mechanism.

INSPECT Language

VPN-1/FireWall-1 provides an object-oriented, high level script language to facilitate debugging and enables administrators to tailor Inspection Scripts to their specialized requirements.

Security rules, application knowledge, context information, and packet data are combined into a powerful, integrated system that can implement any Security Policy based on any combination of parameters and logical expressions. Network and services objects are grouped together and stored in hash-based access lists (static and dynamic), providing high-level definitions, efficient management and processing, and adaptive and intelligent inspection. For additional information about INSPECT, see Chapter 3, "The INSPECT Language," of *VPN-1/FireWall-1 Reference Guide*.

Additional Documentation

For information on configuring and managing VPN-1/FireWall-1, consult the following books:

- *VPN-1/FireWall-1 Administration Guide*

  This book is the technical reference to VPN-1/FireWall-1 features, including authentication and address translation. In addition, chapters on troubleshooting and Frequently Asked Questions (FAQ) are included.

- *Check Point Virtual Private Networking*

  This book describes how to establish a Virtual Private Network using VPN-1/FireWall-1.

- *VPN-1/FireWall-1 Reference Guide*

  This book describes INSPECT, the command line interface and other reference subjects, and includes a glossary.

- *Account Management Client*

  This book describes how to install and use the Check Point Account Management Client.

The above books are available as PDF (Portable Document Format) files on the VPN-1/FireWall-1 CD-ROM. The Adobe Acrobat Reader is required to view these files and is also available on the Check Point CD-ROM.

Additional Reading

Books

Building Internet Firewalls

D. Brent Chapman and Elizabeth D. Zwicky , O'Reilly, 1995 (ISBN: 1565921240)

An excellent book, containing much useful information about “hardening” the firewall machine itself.

Actually Useful Internet Security Techniques

Larry Hughes, New Riders Publishing, 1995

The author describes his experiences managing Unix servers and workstations in a hostile environment. Although not a firewall-specific book, the technology and information nicely complements other reference material.

Essential System Administration

Aeleen Frisch. O’Reilly Edition: 1991; ISBN: 0-937175-80-3

Recommended for serious UNIX users and system administrators. “It provides a compact, manageable treatment of the tasks and issues that everyone responsible for a UNIX system faces.”

Firewalls and Internet Security

William Cheswick and Steven Bellovin, Addison-Wesley,1994

The authors describe their experiences building and managing firewalls for AT&T.

Internet Firewalls and Network Security

Karanjit Siyan, Ph.D. and Chris Hare. New Riders Publishing: 1995;
ISBN: 1-56205-437-6

Presents a hands-on approach to data security and describes a number of commercially available products, including FireWall-1.

Internetworking with TCP/IP, Vols. I, II and III

Douglas Comer and David Stevens. Prentice-Hall: Editions: 1991/2,
ISBN: 0-13-468505-9 (I), 0-13-472242-6 (II), 0-13-474222-2 (III)

A detailed discussion on the architecture and implementation of the Internet and its protocols. Vol. I (on principles, protocols and architecture) is suitable for the general reader; Vol. 2 (on design, implementation and internals) and Vol. 3 (on client-server computing) are fairly technical.

Mastering Windows NT Server 4 - Third Edition

Mark Minasi, Christa Adersen, Elizabeth Creegan. Network Press - SYBEX:1996
ISBN 0-7821-1920-4

A guide to managing NT Server as a stand-alone network or as part of a corporate enterprise network.

Practical UNIX Security

Simson Garfinkel & Gene Spafford. 1st Edition June 1991. 512 pages,
ISBN: 0-937175-72-2

Guides system administrators in making their UNIX system — either System V or BSD — as secure as possible without trusted system technology. The book describes UNIX concepts and how they enforce security, how to defend against and handle security breaches, and explains network security (including UUCP, NFS, Kerberos, and firewall systems) in detail.

Router Products Configuration and Reference, Vol. I, II, III. Cisco Systems, Inc.: Release 9.0

TCP/IP Illustrated, Vols. I, II and III

Gary R. Wright and Richard Stevens, Addison Wesley Professional Computing Series: 1st Edition August, 1995, 3 volumes; ISBN: 0-201-63354-X

This is an ongoing series covering many facets of TCP/IP, and brings a highly effective visual approach to learning about the TCP networking protocol suite.

TCP/IP Network Administration

Craig Hunt. O'Reilly: 1st Edition August, 1992. 502 pages, ISBN: 0-937175-82-X

A complete guide to setting up and running a TCP/IP network for administrators of networks of systems or stand-alone systems that access the Internet. It starts with the fundamentals: what the protocols do and how they work, how to request a network address and a name (the forms needed are included in an appendix), and how to set up your network. Beyond basic setup, the book discusses how to configure important network applications, including `sendmail`, the `r*` commands, and some simple setups for NIS and NFS. There are also chapters on troubleshooting and security. In addition, this book covers several important packages that are available from the Net (such as gated). Covers BSD and System V TCP/IP implementations.

The Internet Complete Reference

Harley Hahn and Rick Stout. Osborne McGraw-Hill Edition: 1994; ISBN: 0-07-881980-6

A complete, illuminating, useful, exciting, and quite readable book on the Internet covering most of the commonly used services. Includes a catalog of Internet resources (over 140 pages).

Unix System Administration Handbook

Evi Nemeth, Garth Snyder, and Scott. Seebass Publisher, Prentice-Hall Edition: 1989; ISBN: 0-13-933441-6

A classic "attempt to condense everything that a system administrator should know about UNIX into a single, easy-to-use volume." Source codes for programs listed are available on the Internet.

Unix System Security

David A. Curry. Addison Wesley Professional Computing Series; ISBN 0-201-56327-4.

A compact and readable guide for users and system administrators.

On-Line Documents

Anonymous ftp on ftp.greatcircle.com under pub/firewalls.

Contains papers, archives of firewall discussions, and subscription information for the mailing list.

VPN-1/FireWall-1 Mailing List

To subscribe to the VPN-1/FireWall-1 mailing list, send a message to
majordomo@lists.us.checkpoint.com
with "subscribe fw-1-mailinglist *email-address*" in the message text, where *email-address* is your email address.

Check Point Home Page

The Check Point home page is at http://www.checkpoint.com.

CHAPTER 3

Virtual Private Networks

In This Chapter

Overview

The Problem

When Bob sends Alice a message over a public network such as the Internet, the message passes through many computers, routers, switches and similar equipment before it arrives at Alice's computer. Charlie has many opportunities to intercept the message along the way and even to alter it, so that the message that Alice receives may be quite different from the one that Bob sent. In fact, Charlie might even send Alice a false message, disguised to appear as though it was sent by Bob.

Alice and Bob want to ensure:

- **Privacy** — that no one can listen to their communication.

  Bob wants to be sure that only Alice can read the message he sends her. Privacy can be achieved by using encryption.

- **Integrity** — that no one is tampering with their communication.

  Bob wants to be sure that the message that Alice will receive is exactly the same message that he sent, that is, that message was not tampered with in transit. Integrity can be achieved through the use of hashing.

- **Authenticity** — that no one is sending false messages.

  Alice wants to be sure that the message she received from Bob really did come from Bob, and not from someone else. Authenticity can be achieved through the use of digital signatures.

The Check Point VPN-1/FireWall-1 Solution

VPN-1/FireWall-1's optional VPN (Virtual Private Network) module protects communications on the Internet and enables an enterprise to build its own easy-to-maintain Virtual Private Network (VPN) using private and public network segments.

VPN-1/FireWall-1 provides the ideal platform for enterprise VPN deployments, enabling encrypted communications and guaranteeing data privacy, integrity and authenticity. In addition to site-to-site VPN capability, VPN-1/FireWall-1 Gateway deployments provide access to remote users when used with Check Point's VPN-1 SecuRemote Client software. For more information on the SecuRemote Client, see "SecuRemote" on page 83.

Check Point's VPN-1 products support industry-standard algorithms and protocols, such as DES, 3DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments.

Some Definitions

Encryption

Encrypting a message modifies ("encrypts") its text ("plaintext" or "cleartext") so that the encrypted text ("ciphertext") can only be read ("decrypted") with the aid of some additional information ("key") known only to the sender and the intended recipient.

Encryption Algorithm

The detailed sequence of mathematical operations by which the cleartext and key are combined to produce the encrypted text. Examples of encryption algorithms are DES (Data Encryption Standard) and CAST.

Key Strength

A measure of the difficulty of decrypting text when the encryption algorithm is known and only the key is unknown. The key strength is usually a function of the key length.

Hashing

A hash is a computation performed on a message whose result can be used to uniquely identify the message, because (a) even a small change in the message leads to a vastly different hash result, and (b) it is computationally unfeasible to compute a message that yields a given hash result.

Digital Signature

A digital signature is some text that can only have been created by someone who knows a specified secret. Encrypting an agreed-upon text can serve as a digital signature (because decryption produces the agreed-upon text) provided that only the "signer" knows the encryption key.

Secrecy

Secret Key Encryption

The simplest way to encrypt a message is by using a secret key, known only to the sender and recipient. Because a secret key is used to both encrypt and decrypt a message, it is also known as a symmetric key. Ensuring the key's secrecy is critical, since anyone who knows the key can decrypt and read the message.

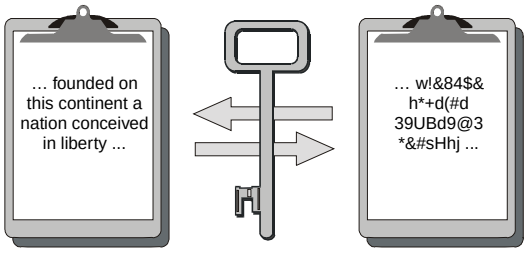


FIGURE 3-1 Encrypting and then decrypting with a secret key

Sharing a Secret Key

Secret key encryption is simple and fast, but it has two disadvantages:

- A secure channel is required by which the correspondents can agree on a key before their first encrypted communication.

  This is a serious drawback, because if such a channel existed, there might be no need for encryption. Agreeing on a secret key by direct face-to-face negotiation may be impractical or unfeasible, and the correspondents may have to agree on a key by mail or telephone or some other relatively insecure means.

- The number of keys required can quickly become unmanageable, since there must be a different key for each pair of possible correspondents.

  For example, the number of keys that must be managed for 10,000 entities (people or computing devices) is about 50 million!

Public Key Encryption

Public key systems, where each correspondent has a pair of keys, can solve both these problems.

A key-pair is composed of two mathematically related keys: a public key known to everyone, and a private key known only to its owner. A message encrypted with one of the keys in a key-pair can only be decrypted with the other key in the pair.[1] Because different keys are used for encryption and decryption, they are known as asymmetric keys.

1. This section describes the RSA public key scheme, where the public and private keys are used to encrypt and decrypt messages. In contrast, the Diffie-Hellman public key scheme is used to exchange secret keys without communicating secret information. VPN-1/FireWall-1 uses both RSA and Diffie-Hellman keys.

If Bob wants to send Alice a message, he encrypts the message with Alice's public key before sending it to her. Because the message was encrypted with Alice's public key, it can only be decrypted with Alice's private key. The only person who knows Alice's private key is Alice herself, so only Alice can read the message. If Charlie were to somehow intercept the message, he would be unable to read it because he doesn't know Alice's private key.

Integrity

Bob wants to be sure that the message that Alice receives is the same message that he sent, in other words, that no one tampers with the message while it is in transit on the network. To ensure the message's integrity, Bob computes a hash of the message.

A hash is a mathematical computation ("hash function") performed on the text of the message. The hash function is designed so that changing even one bit in the message results in a completely different hash result, and there is no practical way to reverse the computation, that is, to compute a message from a given hash result. So the hash result uniquely identifies the message.

When Alice receives the message, she decrypts it, applies the same hash function and compares her hash result to Bob's hash result.

If they are the same, then Alice can be sure that the message was not tampered with, because the hash she calculated is the same one that Bob calculated.

Authenticity

Bob also wants Alice to be able to verify that the message actually came from him and not from an impostor, so Bob attaches his digital signature to the message. A digital signature acts as proof of the sender's identity and the message's integrity.

One widely-used technique for creating digital signatures is for Bob to encrypt some pre-agreed text (for example, the hash result) with his private key (which only he knows). Alice can then decrypt the digital signature with Bob's public key and compare it to the hash result she calculated. If they are the same, she knows that the message can only have come from Bob.

Summary

To summarize, here is a step-by-step description of one way that Bob can send Alice a message so that they can both be sure that only Alice can read the message, and Alice can be sure that the message she receives was sent by Bob and was not tampered with:

1. First, Bob computes a hash of the message.
2. Bob encrypts the hash with his own private key — this is the digital signature.

   Only Bob can do this, because only he knows his private key.
3. Bob encrypts the message with Alice's public key.
4. He then sends Alice both the encrypted hash and the encrypted message.

When she receives the message, Alice can confirm that it was sent by Bob and also that it was not tampered with, as follows:

5 First, she decrypts the message using her private key.

Only Alice can do this, because only she knows her private key.

6 Next, she decrypts the digital signature using Bob's public key.

7 Alice calculates the hash value of the unencrypted message (this is the same calculation that Bob performed) and compares it to the hash value received from Bob.

If they are the same, then Alice can be sure that:

- The message was sent by Bob, because Bob is the only person who knows Bob's private key and thus the only person who could have encrypted the hash value.
- The message was not tampered with, because the hash value Alice calculated is the same one that Bob calculated.

Note – In this scenario, the hash value serves two purposes: it confirms the message's integrity and is also the pre-agreed text of the digital signature. It is possible to use some other pre-agreed text, but the hash value is convenient because it is different for each message and doesn't actually have to be agreed on in advance.

Public Key vs. Private Key Technology

Public key encryption requires significantly more computation effort than private key encryption, and so is much slower. In practice, encrypted communication sessions are often divided into two phases:

- a preliminary, relatively short key negotiation (exchange) phase, secured by inefficient public key encryption, in which a private key is negotiated (exchanged) for encrypting the actual message (communication)

  IKE (Internet Key Exchange, formerly known as ISAKMP/OAKLEY) and SKIP (Simple Key-Management for Internet Protocols) are examples of commonly-used key exchange mechanisms.
- the message encryption phase, in which the message is encrypted using the efficient private key negotiated in the first phase

  DES (Data Encryption Standard) and CAST are examples of commonly-used encryption algorithms.

Certificates

Verifying Public Keys

Trusting a Public Key

Since public keys are the basis for secure encryption, there needs to be a reliable way of obtaining public keys. For example, if Bob and Alice obtain each others' public keys over an insecure channel such as the Internet, they must be certain that the keys are genuine. Alice cannot simply ask Bob for his public key, because there is the danger that Charlie might intercept Alice's request and send Alice his own key instead. Charlie would then be able to read all of Alice's encrypted messages to Bob (and Bob would not be able to read them).

What is a Certificate Authority?

A Certificate Authority (CA) is a trusted third party from whom public keys (and possibly other information) can be reliably obtained, even over an insecure channel.

What is a Certificate?

A certificate is issued by a trusted Certificate Authority and identifies the bearer (which may be a person or computer) and contains some information about the bearer. For example, a CA might send Bob's certificate to Alice. If Alice trusts the CA, then she by implication trusts the information in the certificate. This information might be:

- Bob's unique identifier (for example, his LDAP Distinguished Name)
- Bob's public key
- the CA's unique identifier, so that anyone examining a certificate can know who issued it
- a digital signature, signed with the CA's private key

Alternatively, Bob can send Alice his certificate directly. In either case, Alice can verify the certificate (this is equivalent to verifying Bob's public key) by the procedure described earlier. To do this, she needs the CA's public key, which must be reliably available from an out-of-band source, such as a printed directory.

To prove his identity to Alice, Bob sends her a message consisting of:

- a digital signature, encrypted with his private key
- his certificate (if Alice doesn't already have it) which includes his unique identifier (for example, his LDAP Distinguished Name and IP address)

Alice verifies the digital signature using Bob's public key (from the certificate), proving that the message could only have been encrypted by Bob and that the information it contains (specifically, Bob's unique identifier, which is in both the certificate and the message) is genuine. In this way, Bob can prove who he is and what his IP address is, and Alice can be confident that she is communicating with Bob and not with someone else who is pretending to be Bob.

After Alice and Bob prove their identities in this way, they can use each other's public keys with confidence, because they are certified by certificates from a trusted CA. Usually, the public keys are used to negotiate a secret key for encrypting the actual message.

Note – In a Virtual Private Network, certificates are also used by encrypting entities (for example, gateways) to identify themselves and supply their public keys to their peers.

To summarize, a certificate is like a passport. It identifies the bearer and contains some important information about him or her.

Passports

A passport is issued by a government, and presented by the bearer to anyone who needs to verify the bearer's identity.

A passport consists of the following elements:

1. Proof that the passport belongs to the bearer: the bearer's photograph.
2. Some important information about the bearer: for example, the bearer's name.
3. An expiration date.
4. Proof that the passport is genuine and that it has not been tampered with: the issuer's seal and the special paper on which the passport is printed are intact.

For example, Alice Smith might present her US passport to Donna, an airport immigration official, to prove her identity. Donna believes that Alice is who she claims to be (that is, that she is a US citizen named Alice Smith) because:

1. The passport belongs to Alice and not to someone else (the picture is Alice's picture).
2. Donna can see that Alice's passport has not been tampered with.
3. Donna trusts the issuer (that is, she trusts the US State Department to issue passports in a reliable way).
4. Alice's passport has not yet expired (the expiration date printed in the passport has not passed)

If Bob tries to use Alice's passport, he will be found out because Alice's photograph doesn't match his face. If Bob tries to replace Alice's photograph with his own, the tampering will be immediately noticeable.

Certificates

A certificate is issued by a trusted Certificate Authority and identifies the bearer (which may be a person or computer). A certificate is often embedded in a token, which is either an encrypted disk file or a hardware device, such as a smart card. The token has a password, or PIN. Only someone who physically has the token (the file or device) in his or her possession and knows its PIN can use the token.

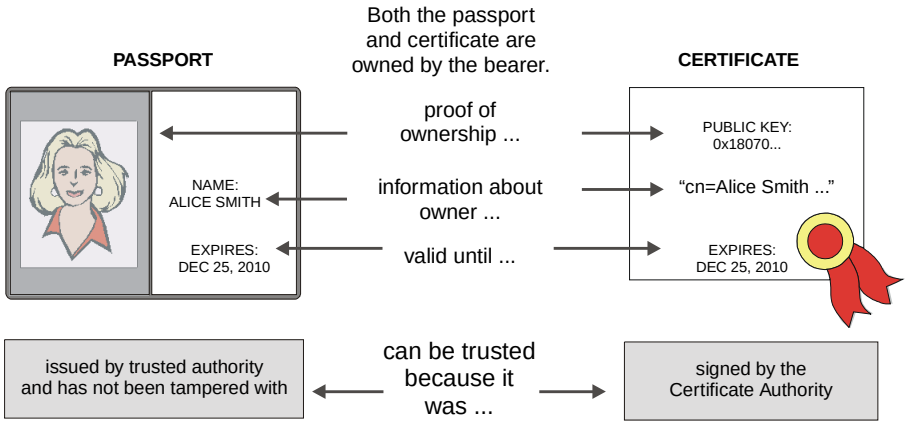


FIGURE 3-2 Passports and Certificates

Note – In one popular model, the information in the token is called a profile. In addition to the certificate, the profile includes the Certificate Authority's public and private keys (used for validating information signed by the Certificate Authority, such as a CRL). The profile is kept either on a hardware device or is saved as a file on a diskette, limiting physical access and minimizing the possibilities of misuse.

The certificate contains some important information about the bearer.

1. Proof that the certificate belongs to the bearer: for example, the bearer's public key.

   The public key is considered proof, because the signature can be verified with it.

2. Some important information about the bearer: for example, the bearer's DN (Distinguished Name).

3. An expiration date.

4. Proof that the certificate is genuine and has not been tampered with: a digital signature.

   The entire certificate, including its hash, is signed by the Certificate Authority, proving that the certificate could only have been created by the Certificate Authority.

Bob cannot use Alice's certificate for two reasons:

1. Bob doesn't have Alice's private key.

   The private key is on a hardware token (a physical device) which is in Alice's possession, and which she carefully guards. With some physical devices, the private key is physically protected and cannot be read out.

2. Even if Bob had the certificate (for example, if he has stolen the hardware token), he still doesn't know the access password (PIN).

   Only Alice knows the access password. Without the password, the certificate cannot be used.

The certificate's security is based on these factors:

- the difficulty of obtaining (and reading) the physical device on which the certificate is stored
- the secrecy of the access password (PIN).

Creating Certificates

A user's certificate is created by a Certificate Authority. There are several different ways in which the user acquires the certificate, depending on the PKI vendor:

1. A file (sometimes called a "profile") is created, either by the user or by the Certificate Authority.
   - One method is for the user to create the profile on his or her own computer, using special client software (for example, the Check Point SecuRemote Client). The user can then store the profile file on a diskette or on a hardware token, minimizing the possibility of its unauthorized copying and misuse. Some hardware tokens can generate the key pairs on the device, providing enhanced security for the user's private key. The profile file is further protected by the access password, known only to the user.
   - A second method is for the Certificate Authority to create the profile file (preferably on a hardware token) and then give it to the user. This method centralizes the creation of profile files, but may be impractical in a geographically dispersed organization.
2. The user registers to the Certificate Authority using a Web browser, and can then export the certificate and private key for the use of other applications.
3. The user creates a certificate registration request in a file, and transfers the file (via mail, ftp, *etc*.) to the Certificate Authority. The Certificate Authority approves the request and generates the certificate on a file, which is transferred back to the user (again using mail, ftp, etc).

Certificate Revocation Lists

When a user leaves an organization, or when a key is compromised (for example, when a token is stolen), the user's certificate must be revoked. The Certificate Authority does this by issuing and distributing a Certificate Revocation List (CRL), a list of certificates that are no longer valid.

Certificate Revocation Lists are issued periodically, at fixed intervals, by a Certificate Authority, but they can be issued at any time if required. Before accepting a certificate, the CRL should be examined to confirm that the certificate has not been revoked. The CRL's distribution point — the address from which an up-to-date CRL can be obtained — usually an LDAP or HTTP-based Web Server — is usually specified in the certificate.

Certificate Authorities

IKE

In the IKE encryption scheme, an encrypting gateway's CA is specified in the **Certificates** tab of the **Workstation Properties** window. The CA itself is defined in the **CA Properties** window. See also Chapter 3, "Certificate Authorities" of *Check Point Virtual Private Networks* for more information.

FWZ and SKIP

In the FWZ and SKIP encryption schemes, FireWalled Management Modules function as Certificate Authorities for the encrypting gateways.

VPN-1 Accelerator Card

In addition to the standard software implementation, Check Point VPN-1 IKE encryption can be implemented in a hardware accelerator card, significantly increasing the throughput and reducing CPU utilization.

VPN-1 Accelerator Card is installed on the encrypting gateway. Its installation is completely transparent, and no changes to the Rule Base or configuration files are required.

Note – The VPN-1 Accelerator Card supports IKE encryption only.

SecuRemote

Overview

Check Point VPN-1 SecuRemote enables PC users to securely communicate sensitive and private information to networks and individual servers. Check Point VPN-1 SecuRemote extends the VPN to Windows 9x and Windows NT workstations and desktops, using both dial-up and LAN connections.

Typical uses for SecuRemote are:

- Specific employees can be granted encrypted access to sensitive corporate data.
- A server can be set up to provide encrypted information to paying customers only. Because the communication is encrypted, eavesdropping is impossible.
- Users at a remote office can conduct encrypted communications with the FireWalled enterprise network without installing VPN-1/FireWall-1 at the remote office.
- General network access (email, intranet Web, *etc*.) can be provided for remote employees such as telecommuters and business travelers.
- A group of workers dealing with sensitive information can create private workgroups over internal, shared-access networks such as Ethernets by using VPN-1 SecuRemote and encryption-enabled application servers.

VPN-1 SecuRemote is based on a technology called Client Encryption. Because SecuRemote encrypts data before it leaves the laptop, it offers a completely secure solution for remote connections.

VPN-1 SecuRemote can transparently encrypt any TCP/IP communication. There is no need to change any of the existing network applications on the user's PC. SecuRemote can interface with any existing adapter and TCP/IP stack. A PC on which SecuRemote is running can be connected to several different VPN-1/FireWall-1 sites.

A VPN-1/FireWall-1 security manager can enable access for SecuRemote users with the standard VPN-1/FireWall-1 Rule Base editor. After a SecuRemote user is authenticated, a completely transparent secured connection is established and the user is treated just as any user in the Virtual Private Network. The network administrator can enforce VPN-1/FireWall-1 security features, including authentication servers, logging and alerts, on SecuRemote connections (just as with any other connection).

The configuration below depicts a Virtual Private Network with a nomadic SecuRemote user securely connected to the Enterprise network through the Internet.

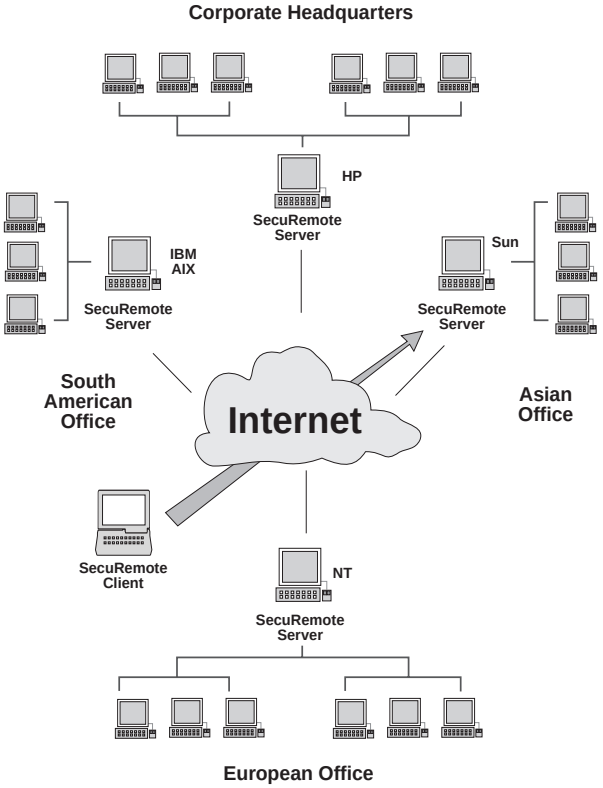


FIGURE 3-3 Virtual Private Network with a nomadic SecuRemote Client

SecuRemote includes support for dynamic IP addressing, which is necessary for dial-up communication. SecuRemote can also be used from stationary PC's with fixed IP addresses.

SecuRemote supports IKE key exchange, as well as the proprietary FWZ protocol. Strong user authentication is supported by means of Entrust certificates, as well as a number of other authentication schemes (RADIUS, S/Key, password *etc*). Encryption schemes include (in accordance with export restrictions):

- IKE using DES, triple DES or 40 bit encryption
- FWZ (a Check Point proprietary scheme) using DES or FWZ1

Additional Information

For information about configuring the SecuRemote Server (VPN/FireWall Module), see Chapter 9, “SecuRemote Server” of *Check Point Virtual Private Networks*.

For information about the SecuRemote Client software, see Chapter 10, “SecuRemote Client” of *Check Point Virtual Private Networks*.

CHAPTER 4

VPN-1 SecureClient

In This Chapter

Overview

What is Check Point VPN-1 SecureClient?

Check Point VPN-1 SecureClient extends security to the desktop by enabling administrators to enforce a Security Policy on desktops — both inside the LAN and connecting from the Internet — and prevent unauthorized users from taking control of authorized connections ("hijacking" them). In addition, the configuration of SecureClient machines can be verified and access denied to misconfigured SecureClient machines.

Check Point VPN-1 SecureClient consists of:

- VPN-1 SecuRemote Client software with the Desktop Security feature installed
- A Policy Server from which the VPN-1 SecuRemote Client obtains its Desktop Policy

Examples

FIGURE 4-1 on page 88 shows how an intruder can take advantage of an existing valid SecuRemote connection to penetrate the internal enterprise network. This kind of attack can be prevented by enforcing — on the VPN-1 SecuRemote Client — a Desktop Policy that does not allow incoming connections to the VPN-1 SecuRemote Client.

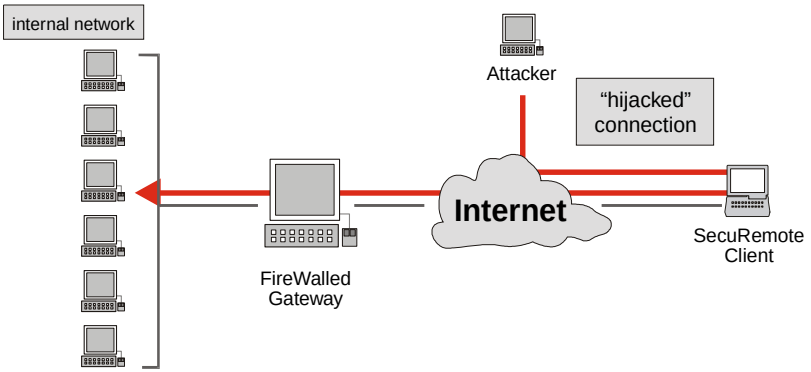


FIGURE 4-1 Taking unauthorized control of ("hijacking") a SecuRemote connection

In FIGURE 4-2, the servers in FinanceNet are protected by an internal VPN/FireWall Module on Tower. The Security Policy allows Bob on BigBen to connect to FinanceNet, but users on Tate are not allowed to do so.

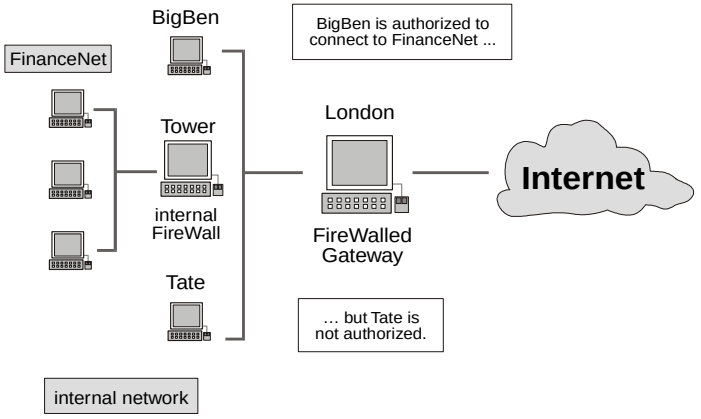


FIGURE 4-2 Securing an internal subnetwork

By installing SecureClient on BigBen, this high degree of security can be enhanced to:

- Prevent Tate (and anyone else) from taking control of the connection between BigBen and FinanceNet.

  This is configured by installing a Desktop Policy on BigBen in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-4 on page 93).

- Encrypt connections between BigBen and FinanceNet.

  This is configured (in the **VPN** tab of Tower's **Workstation Properties** window) by:

  - defining FinanceNet to be in Tower's encryption domain
  - checking **Exportable to SecuRemote**

- Verify that BigBen is properly configured.

  The proper configuration is defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-4 on page 93). The configuration is verified by defining a Client Encrypt rule for the connection and checking **Apply Rule only if Desktop Configuration Options are Verified** in the rule's **User Encryption Action Properties** window (FIGURE 4-5 on page 95).

Example Configuration

Network Configuration

FIGURE 4-3 depicts a configuration in which SecureClient provides security both inside and outside the LAN.

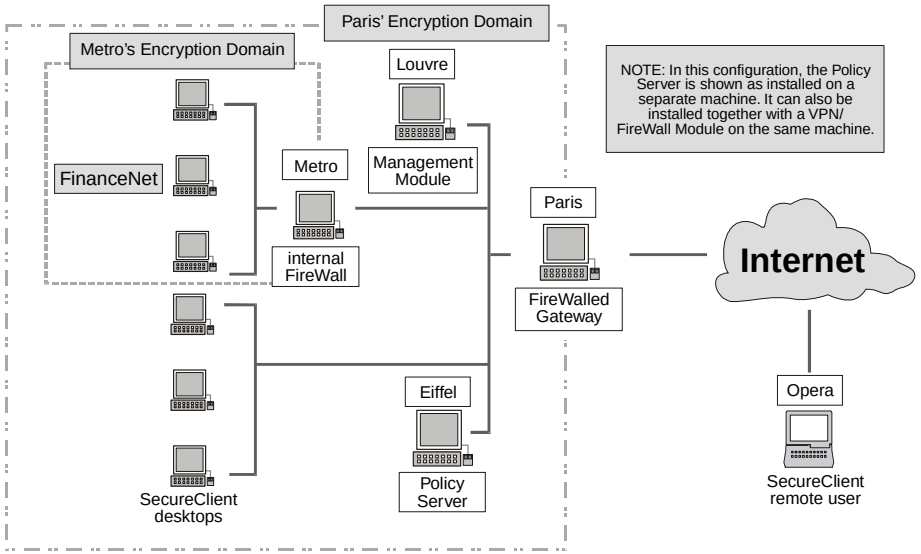


FIGURE 4-3 Securing a LAN with VPN-1 SecureClient

The configuration consists of:

- a Management Module (Louvre), on which the Security Policy is defined
- a FireWalled gateway (Paris), which enforces the Security Policy
- a Policy Server (Eiffel), from which the Desktop Policy is downloaded to the SecureClients
- an internal VPN/FireWall Module (Metro), which protects the Finance subnet by encrypting connections

An internal VPN/FireWall Module is required to protect a network (as in this configuration), but if only the host itself must be protected, then a VPN-1 SecureServer Module is adequate.

- a number of internal SecureClient desktops
- a remote SecureClient (Opera)

Note – The Policy Server can be installed either on a separate machine, or together with a VPN/FireWall Module on the same machine. So for example, in FIGURE 4-3, the Policy Server can be either on Eiffel or on Paris.

Installed Software Modules

TABLE 4-1 lists the VPN-1/FireWall-1 software installed on each of the machines in FIGURE 4-3.

TABLE 4-1 Installed Software Modules

machine	installed VPN-1/FireWall-1 software module
Louvre	Management Module
Paris	VPN/FireWall Module
Eiffel	VPN/FireWall Module with SecureClient license
Metro	VPN/FireWall Module
desktops	SecureClient (SecuRemote with Desktop Security enabled)
Opera	SecureClient (SecuRemote with Desktop Security enabled)

Desktop Security can be enabled in the VPN-1 SecuRemote Client when it is installed.

Configuring SecureClient

To configure SecureClient (referring to the example configuration in FIGURE 4-3), proceed as follows:

1 Install the appropriate VPN-1/FireWall-1 software and licenses on each machine (see TABLE 4-1).

2 Define the network objects (see Chapter 4, “Network Objects” of *VPN-1/FireWall-1 Administration Guide* for information) and configure them as described in TABLE 4-4.

TABLE 4-2 Network Objects Configuration

network object	configuration
Louvre	In the **General** tab of Louvre’s **Workstation Properties** window, check **Management Station**.
Paris	In Paris’ **Workstation Properties** window: ■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**. ■ In the **VPN** tab, specify Paris’ encryption domain. ■ In the **VPN** tab, check **Exportable to SecuRemote**.
Eiffel	In Eiffel’s **Workstation Properties** window: ■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**. ■ In the **VPN** tab, check **Exportable to SecuRemote**. ■ In the **Policy Server Properties** window (FIGURE 4-7), define Eiffel as a Policy Server.
Metro	In Metro’s **Workstation Properties** window: ■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**. ■ In the **VPN** tab, specify Metro’s encryption domain. ■ In the **VPN** tab, check **Exportable to SecuRemote**.

3 Configure the SecuRemote and Desktop Security options in the **Desktop Security** tab of the **Properties Setup** window (see FIGURE 4-4 on page 93).

4 Define the users and user groups who will be allowed access to the protected networks (see Chapter 5, “Managing Users” of *VPN-1/FireWall-1 Administration Guide* for information).

5 Define the Policy Server and assign a user group (see FIGURE 4-7 on page 97).

6 Define the appropriate rules to allow authorized users to access the protected networks (see Chapter 8, “Security Policy Rule Base” of *VPN-1/FireWall-1 Administration Guide* for information).

In the example, the required rule is similar to:

Source	Destination	Services	Action	Track	Install On
FinanceUser@Any	FinanceNet	Any	Client Encrypt	None	Gateways

7. If the configuration includes overlapping encryption domains (as in FIGURE 4-3 on page 89), then define a rule allowing access through the "outer" VPN/FireWall Module as described in "Overlapping Encryption Domains" on page 98.

8. Define a rule on the Policy Server that allows the (pre-defined) FW1_pslogon service between the SecureClient and the Policy Server.

9. If there is a VPN/FireWall Module between the Policy Server and the SecureClient, you must allow the fw1_encapsulation and RDP services for FWZ and the IPSec service for IKE.

10. Install the Security Policy.

    This will also download the Desktop Policy to the Policy Server.

11. SecureClient users then download the Desktop Policy.

    To download a Desktop Policy, the SecureClient user should do one of the following:

    - Choose **Policy➤Login to Policy Server** select a Policy Server, *or*
    - Right-click on the SecureClient icon in the taskbar and choose **Login**, *or*
    - Click on  in the toolbar.

    The user then is challenged to authenticate himself or herself. If the user is not a member of the group specified in the **Policy Server Properties** window (FIGURE 4-7 on page 97), the Desktop Policy is not downloaded.

The SecuRemote Client's taskbar icon changes when a Desktop Policy has been successfully downloaded.

-  indicates that a Desktop Policy is being enforced.

  The lock is either green (packet allowed) or red (packet dropped).

-  indicates that a Desktop Policy is being enforced, and that the SecureClient's configuration has been verified by the Policy Server.

  The lock is either green (packet allowed) or red (packet dropped).

-  indicates that no Desktop Policy is being enforced.

Properties Setup — Desktop Security Tab

The Desktop Policy is defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-4 on page 93) and is downloaded from the Management Module (Louvre) to the Policy Server (Eiffel) when the Security Policy is installed.

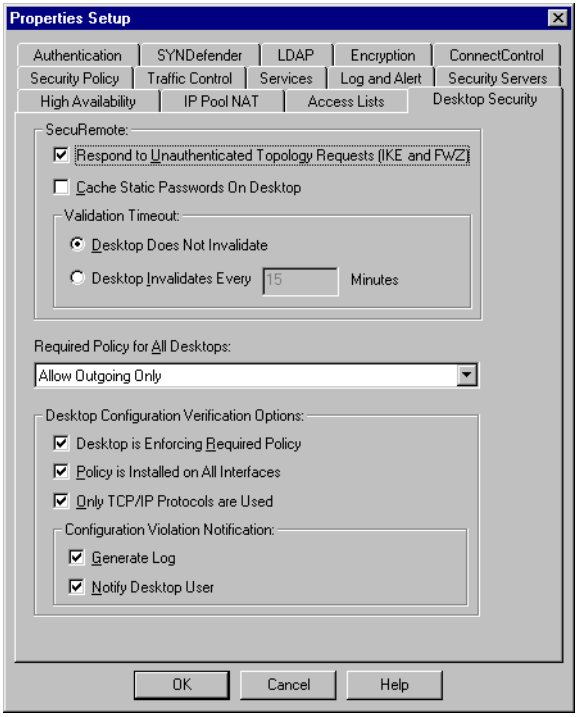


FIGURE 4-4 Properties Setup — Desktop Security tab

Required Policy for All Desktops specifies the Desktop Policy that will be downloaded to all Policy Servers (and from there to SecureClients). These Desktop Security Policies are described in TABLE 4-3:

TABLE 4-3 Desktop Policy options

Desktop Policy	meaning (inbound and outbound refer to the desktop)
Allow All	No Desktop Policy is installed on the SecureClient. This option is equivalent to the standard VPN-1 SecuRemote Client.
Allow Outgoing Only	Only outbound connections (from the SecureClient) are allowed, except for the following (which are also allowed): ■ ICMP return packets ■ Session Authentication Agent protocol (port 261)
Allow Encrypted Only	Only VPN (encrypted) connections are allowed (inbound and outbound)
Allow Outgoing and Encrypted	Connections allowed by **Allow Outgoing Only** and **Allow Encrypted Only** are allowed.

Desktop Configuration Verification

Desktop Configuration Verification Options specifies the components of the desktop configuration that the Policy Server verifies when an encrypted connection is negotiated (during the key exchange procedure). If the Desktop Policy does not conform, the action specified under **Configuration Violation Notification** is taken.

TABLE 4-4 Configuration Verification options

Option	means that the Policy Server verifies that ...
Desktop is Enforcing Required Policy	... the desktop is enforcing the Security Policy defined for it in **Required Policy for All Desktops**.
Policy is Installed on all Interfaces	... the Desktop Policy is installed on all of the desktop's interfaces.
Only TCP/IP Protocols are Used	... only TCP/IP is enabled on the desktop (and not, for example, IPX).

After the Desktop Policy has been downloaded, the Policy Server maintains an open connection to the SecureClient. If Policy Server is notified whenever the SecureClient's Desktop Policy is modified.

You can verify that the SecureClient is properly configured before applying a rule whose action is either Client Encrypt or Session Authentication. A misconfigured SecureClient is denied access under the rule. The configuration components verified are the components checked in the **Desktop Security** tab of the **Properties Setup** window.

The result of a configuration verification is cached for the time period (in seconds) specified by the `timeout` parameter in the `$FWDIR/database/fwdtmquery.C` file.

```
(
    :cache_params (
           :timeout (15)
    )
)
```

If this file does not exist, the timeout period defaults to 15 seconds. If `timeout` is set to zero, there is no caching and the configuration is verified for each connection.

Client Encrypt

In the Client Encrypt rule's **User Encryption Action Properties** window (FIGURE 4-5), check **Apply Rule Only if Desktop Configuration Options are Verified**.

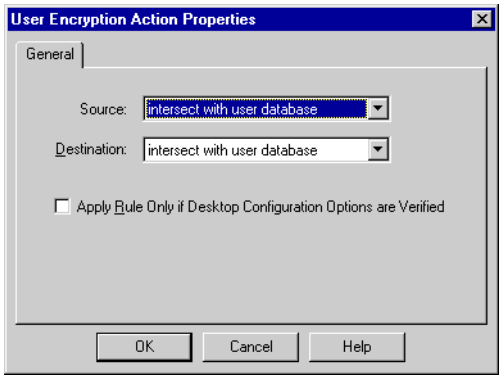


FIGURE 4-5 User Encryption Action Properties window

Getting Here – To display the **User Encryption Action Properties** window, double-click on the Client Encrypt action in the rule.

Session Authentication

In the Session Authentication rule's **Session Authentication Action Properties** window (FIGURE 4-6), check **Verify secure configuration with Policy Server** and select a Policy Server from the drop-down list.

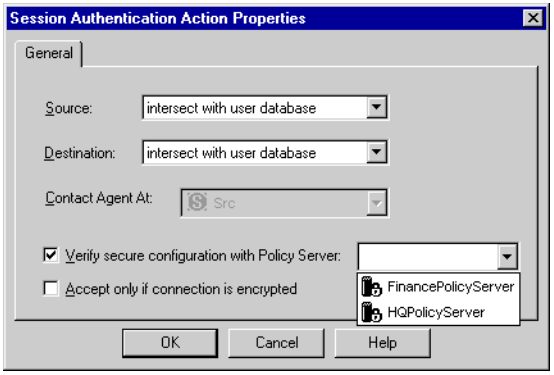


FIGURE 4-6 Session Authentication Action Properties window

Getting Here – To display the **Session Authentication Action Properties** window, double-click on the Session Authentication action in the rule.

The VPN/FireWall Module enforcing the rule will confirm with the specified Policy Server that the SecureClient is properly configured.

Note – The first time you install a Security Policy that includes a Session Authentication rule with **Verify secure configuration with Policy Server** checked, you must stop and restart the VPN/FireWall Module before the setting takes effect.

Policy Server Properties Window

Policy Servers are defined in the **Policy Server Properties** window (FIGURE 4-7).

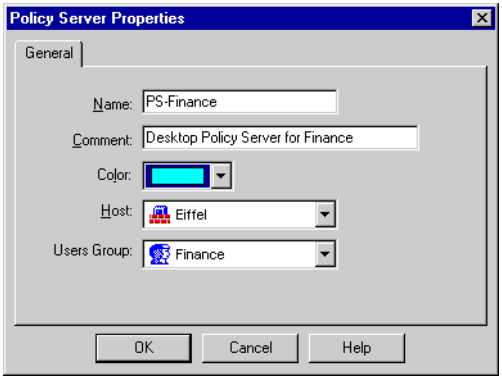


FIGURE 4-7 Policy Server Properties window

Getting Here – To display this window, choose **Manage➤Servers** in the menu, and in the **Server Objects** window (FIGURE 10-1 on page 319 of *VPN-1/FireWall-1 Administration Guide*):

- To define a new Policy Server, click on **New** and then on **Policy Server**.
- To edit the properties of an existing Policy Server, select the Policy Server and click on **Edit**.

Host must be a workstation for which:

- **VPN-1 & FireWall-1** is checked and Version set to **4.1** or higher in **Modules Installed** in the **General** tab of its **Workstation Properties** window
- **Exportable to SecuRemote** is checked in the **VPN** tab of its **Workstation Properties** window

Users Group specifies the users who will be downloading their Desktop Security Policies from the Policy Server. The user group can be a FireWall-1 group or a group defined on an LDAP Server. The Policy Server counts the users to verify that the software license is not violated.

When a Security Policy is installed, the Desktop Policy defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-4 on page 93) is downloaded to all the Policy Servers.

Overlapping Encryption Domains

When the remote SecureClient (Opera in the example configuration depicted in FIGURE 4-3 on page 89) connects to a host in the Finance subnet, it encrypts with Metro. The site's topology information specifies that Metro's encryption domain is contained in Paris' encryption domain, so there must be a rule that allows encrypted communications to pass through Paris without being decrypted, as follows:

Source	Destination	Services	Action	Track	Install On
Any	FinanceNet	Encrypted_Services	Accept	None	Paris

"Encrypted_Services" is a pre-defined service. There must also be an appropriate Client Encrypt rule on Metro to decrypt the connection (see step 6 on page 91 for an example).

Warning – FWZ encryption without encapsulation is not supported for overlapping encryption domains.

Installing Desktop Policies

When the Security Policy is installed on the VPN/FireWall Modules, the Policy Servers receive the Desktop Policy that they will later install on the SecureClients. The Policy Servers install the Desktop Policy on the SecureClients when the users login to the Policy Server, explicitly or implicitly (see "Downloading a Desktop Policy" on page 101).

Specifying the Desktop Policy

The Desktop Policy to be downloaded to SecureClients is specified in **Required Policy for All Desktops** in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-8 on page 99). See TABLE 4-3 on page 94 for an explanation of the available options.

Desktop Policy Verification

In the **Desktop Security** tab of the **Properties Setup** window (FIGURE 4-8 on page 99), the system administrator can specify that the Desktop configuration be verified, and the action to take if the configuration is incorrect. See TABLE 4-3 on page 94 for an explanation of the available options.

The Desktop configuration is verified when the SecureClient user downloads a Desktop Policy from the Policy Server, and whenever the desktop performs a key exchange with a Version 4.1 or higher VPN/FireWall Module.

If the configuration is incorrect, the action specified in **Configuration Violation Notification** is taken. The options are:

Generate Log — Generate a log entry to the VPN-1/FireWall-1 Log.

The log entry's action is "Deauthorize" and the reason is the text given in TABLE 4-5 on page 100.

Notify Desktop User — Display an error message window (for example, FIGURE 4-10 on page 102) on the SecureClient machine.

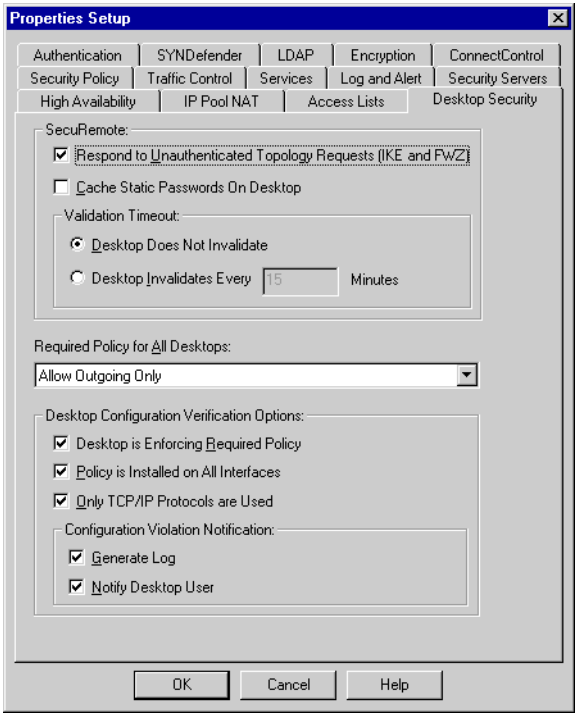


FIGURE 4-8 Properties Setup — Desktop Security tab

TABLE 4-5 lists the error messages displayed in the VPN-1/FireWall-1 log or on the desktop when the desktop is incorrectly configured.

TABLE 4-5 Desktop Configuration Errors

Log text	Desktop error message text	meaning
“Old SecuRemote”	There is no message on the desktop.	An obsolete version of SecuRemote, which does not support Desktop Security, is installed on the desktop.
“Lost policy”	“You are not authorized to have a policy!”	The user has been removed from the group of users authorized to receive a Desktop Policy from the Policy Server. This error occurs only if the desktop tries to download a policy from the same Policy Server from which it last downloaded a policy.
“No policy”	“The security policy on your computer has been removed.”	The desktop has no Desktop Policy.
“Wrong Policy”	“You are using an inappropriate policy. Load a new policy from your Policy Server.”	The Desktop Policy on the desktop is different from the Desktop Policy specified in **Required Policy for All Desktops**.
“Not all network adapters are protected and you are using non-IP protocol which is not protected.”	“Not all network adapters are protected and you are using a non-IP protocol which is not protected.”	The SecuRemote Client is not bound to all the network adapters, and is using a non-IP protocol.
“Not all network adapters are protected.”	“Not all network adapters are protected.”	The SecuRemote Client is not bound to all the network adapters.
“non-IP protocol in use.”	“You are using NetBEUI or another non-IP network protocol which is not protected.”	The SecuRemote Client is using a non-IP protocol.

Enforcing the Desktop Policy

There are several ways in which the system administrator can restrict access to SecureClients.

- Rule Base

  Define a rule with Client Encrypt as the **Action**.

- **Client Encryption Properties** window (FIGURE 4-5 on page 95)

  Select **Apply Rule only if Desktop Configuration Options are Verified**. This feature has no effect on pre-Version 4.1 VPN/FireWall Modules.

In addition, the system administrator can deny a user access by removing the user from the user group.

SecureClient on the Desktop

Downloading a Desktop Policy

A Desktop Policy is downloaded to the SecureClient when the SecureClient logs in to the Policy Server, either explicitly or implicitly.

Explicit Login

The SecureClient user is asked whether to download a Desktop Policy whenever the user adds or updates a site.

Adding or Updating Sites

When a user adds or updates a site, the **Download Policy** window (FIGURE 4-9) is displayed.

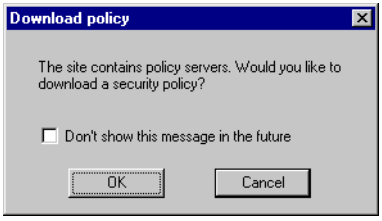


FIGURE 4-9 Download Policy window

The window is also displayed when the SecuRemote Client is restarted.

Click on **OK** to download a Desktop Policy. The user will be asked to authenticate himself or herself. If the authentication is successful and the user is authorized to download a policy from the Policy Server (that is, the user is a member of the user group specified in the **Policy Server Properties** window — see “Policy Server Properties window” on page 97), a Desktop Policy will be downloaded. If the newly-downloaded Desktop Policy is different from the one currently installed, a message will be displayed (FIGURE 4-10).

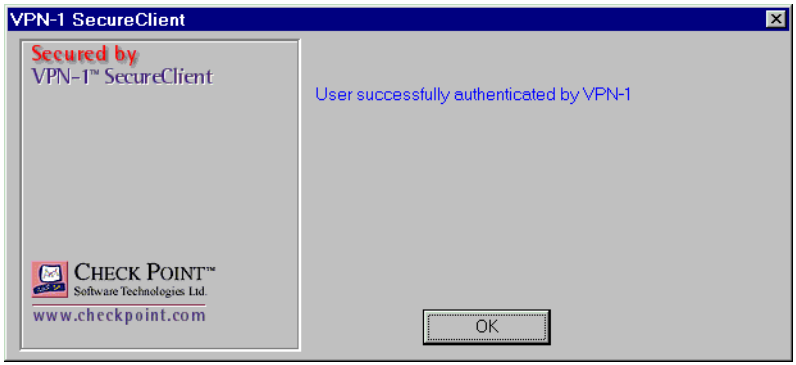


FIGURE 4-10 SecureClient message

Possible messages (displayed in red) are:

- "The security policy on your computer has been removed."
- "The security policy on your computer has changed."
- "You are not authorized to have a policy."

Logging in to a Policy Server

When a user selects **Login to Policy Server** from the **Policy** menu, a sub-menu is displayed from which a Policy Server must be selected. The Policy Servers listed (in the format *site*:*PolicyServer*) are those defined for the current site. You cannot login to a Policy Server if its site is disabled in the SecuRemote Client.

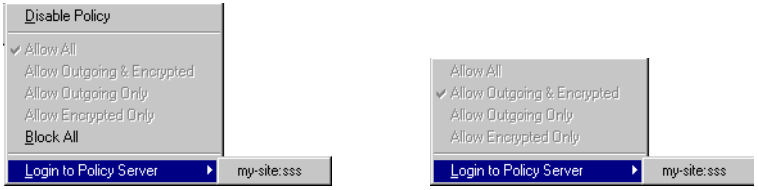


FIGURE 4-11 Policy menus

The Desktop Policy currently being enforced is marked by a check (✔).

Note – Alternatively, right-click on the SecuRemote icon in the Windows system tray and select **Login**, or double-click on the SecuRemote icon.

Choose one of the following from the **Policy** menu:

Note – The Desktop Policy currently being enforced is marked by a check (✔).

- **Disable Policy**

  Disable the Desktop Policy, or if it is already disabled, enable it. You will be asked to confirm your action.

FIGURE 4-12 Warning when you choose Disable Policy

If you choose **Disable Policy** while there are active encrypted connections, the connections will continue and the change will take effect only after you restart SecuRemote.

If you later download a Desktop Policy from a Policy Server, the newly-downloaded policy is enabled.

- **Allow All**

  No Desktop Policy is installed on the SecureClient. This option is equivalent to the standard VPN-1 SecuRemote Client.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Outgoing Only**

  Only outbound connections (from the SecureClient) are allowed, except for the following (which are also allowed):

  - ICMP return packets
  - Session Authentication Agent protocol (port 261)

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Encrypted Only**

  Only VPN (encrypted) connections are allowed (inbound and outbound).

  If the SecureClient is inside an encryption domain, it is limited to communication with peers inside an internal encryption domain. For example, in FIGURE 4-2 on page 88, BigBen would be able to communicate with FinanceNet but not with Tate.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Outgoing & Encrypted**

  Connections allowed by **Allow Outgoing Only** and **Allow Encrypted Only** are allowed.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Block All**

  Block all connections to the SecuRemote Client machine.

  The Policy Server never installs this policy on the SecuRemote Client machine. You will be asked to confirm your action.

- **Login to Policy Server**

  Select the Policy Server from the sub-menu.

  Select the Policy Server from the list, which includes all the Policy Servers defined for the selected site.

  The policy that you receive or change will remain in effect even if you reboot your computer.

Note – A Desktop Policy is installed only on those interfaces on which SecuRemote is also installed and only affects the TCP/IP protocol. Your system administrator may decide to configure the VPN/FireWall Modules to warn you and to limit your access if you have unprotected interfaces and/or protocols.

Implicit Login

A Desktop Policy is installed automatically when the SecureClient initiates a connection to a site and the user is asked to authenticate himself or herself to a VPN/FireWall Module which is also a Policy Server.

Boot Policy

When a SecureClient machine on which a Desktop Policy is being enforced boots up, a boot policy allowing only outgoing connections is enforced until the SecureClient Desktop Policy is loaded.

Logging

SecureClient logs, if any are generated, are written to a text file named `c:\SR.log`, if one exists. The contents of `c:\SR.log` are erased each time the SecuRemote Client is started. You can create an empty `SR.log` file using a text editor.

IP Forwarding

When the user logs in to the OS, SecureClient checks if IP Forwarding is enabled. If it is enabled, a warning is displayed and SecureClient-specific features are disabled, that is, the SecureClient functions as a SecuRemote Client.

SecuRemote Icons

TABLE 4-6 shows the SecuRemote icons displayed in the system tray.

TABLE 4-6 SecureClient System Tray Icons

Icon	meaning
	standard SecuRemote icon
	Allow out-going and/or encrypted communication. The lock is green.
	**Block All** policy is in effect, but no packet has been dropped recently.
	A packet was dropped while non-trivial policy (**Allow Encrypted Only**, **Allow Out-going Only**, and **Allow Outgoing & Encrypted Only**) is in effect. Information about dropped packets is logged to the local log file (see "Logging" on page 104). The lock is red for about half a second.
	A Desktop Policy is being enforced, and the security of the SecureClient's configuration has been verified by the Policy Server.
	A packet was dropped while in **Block All** policy is in effect. The lock is red for about half a second.

userc.c File

userc.c parameters

The `userc.c` file (located on the Secure Client) contains information about the Secure Client configuration, including site topology. The parameters listed in TABLE 4-7 are defined in the `options` section.

Warning – The SecuRemote Client performs minimal syntax checking for the `userc.c` file. If a parameter is entered incorrectly, the site to which it belongs is deleted. No error messages are displayed.

TABLE 4-7 userc.c parameters

parameter (default value in parentheses)	meaning
`default_ps`	If specified, the IP address (in dot format) of a Policy Server to which the SecureClient will automatically logon upon launch.

CHAPTER 5

Introduction to FloodGate-1

In This Chapter

Internet Bandwidth Management Technologies

Overview

When you connect your network to the Internet, it is vitally important to make the most efficient use of the available bandwidth. An effective bandwidth management policy ensures that even at times of network congestion, bandwidth is allocated in accordance with enterprise priorities.

In the past, network bandwidth problems have been addressed either by adding more bandwidth (an expensive and usually short term "solution") or by router queuing.

Routers are capable of queuing traffic according to pre-defined parameters, but their effectiveness as bandwidth managers is limited by their inability to "understand" network traffic at any useful level. For example, a router cannot distinguish between PointCast and HTTP, match an FTP data connection to its control connection, or guarantee bandwidth to an application. Moreover, router queuing often results in chunky traffic which downgrades performance even more. In short, router queuing is an ineffective solution for complex modern Internet protocols.

FloodGate Requirements

In order to provide effective bandwidth management, a bandwidth management tool, or "floodgate," must track and control the flow of communication passing through it, based on information derived from all communication layers and from other applications.

An effective floodgate must address all of the following issues:

- Flexible Prioritization

  It is not sufficient to simply prioritize communications, for example, to specify a higher priority for HTTP than for SMTP. The result may well be that all bandwidth resources are allocated to one service and none to another. A floodgate must be able to divide the available resources so that more important services are allocated more bandwidth, but all services are allocated some bandwidth.

- Minimum Bandwidth

  A floodgate must be able to guarantee a service's minimum required bandwidth. A floodgate that allocates, for example, 0.5KBps to an audio streaming service is effectively wasting those 0.5KBps. A floodgate must also be able to allocate bandwidth preferentially, for example, to move a company's CEO to the "head of the line" when he or she browses the Web.

- Classification

  A floodgate must be able to accurately classify communications and distinguish between similar services, for example, between PointCast and HTTP[1], but simply examining a packet in isolation does not provide all the information needed to make an informed decision. State information — derived from past communications and other applications — is also required. A packet's contents, the communication state and the application state (derived from other applications) must all be considered when making control decisions.

- Monitoring

  A floodgate must provide a clear picture of what is actually happening, so that a network administrator can monitor network performance in real time.

FloodGate-1's Innovative Technology

FloodGate-1 is a bandwidth management solution for Internet and Intranet gateways that enables network administrators to set bandwidth policies to alleviate the bandwidth congestion at network access points. The overall mix of traffic is dynamically controlled by managing bandwidth usage for entire classes of traffic, not just individual connections. FloodGate-1 controls both inbound and outbound traffic

1. This is an important distinction, because PointCast sessions are initiated automatically, without an explicit action by the user, who is often unaware of the extent to which PointCast consumes valuable resources. Moreover, since PointCast uses HTTP, distinguishing PointCast from HTTP is non-trivial.

flows at data rates up to 10 Mbps. FloodGate-1 also includes traffic analysis tools which can be used by the administrator to diagnose the nature of traffic congestion and define the appropriate Bandwidth Policy.

FloodGate-1 enables the administrator to direct bandwidth to applications in the "right" ratio: in accordance with the enterprise Bandwidth Policy. Using Check Point's sophisticated RDED (Retransmission Detection Early Drop) mechanism, FloodGate-1 smooths connections and drastically reduces retransmit counts, greatly improving the efficiency of the enterprise's existing lines. The increased bandwidth that FloodGate-1 makes available to important applications comes at the expense of less important (or completely unimportant) applications. Purchasing more bandwidth can be significantly delayed.

In addition, FloodGate-1 controls connection latency in the outbound direction. Latency is often more perceptible than bandwidth for interactive applications, and latency growth is noticeable long before a transmission line is full. The full benefits of FloodGate-1's latency control are realized when FloodGate-1 is installed at both ends of a connection and effectively controls latency in both directions.

Network traffic can be classified by Internet service, source or destination IP address, Internet resource (for example, specific URL designators), and traffic direction (inbound or outbound). A FloodGate-1 Bandwidth Policy consists of rules which specify the weights, limits, and guarantees that are applied to the different classifications of traffic.

A rule can have multiple sub-rules, enabling an administrator to define highly granular Bandwidth Policies. FloodGate-1 incorporates Check Point's patented Stateful Inspection technology to derive complete state and context information for all network traffic. This traffic information is used by FloodGate-1's Intelligent Queuing Engine (IQ Engine™) to accurately classify traffic and place it in the proper transmission queue. The network traffic is then scheduled for transmission based on the Bandwidth Policy. The IQ Engine includes an enhanced, hierarchical Weighted Fair Queuing (WFQ) algorithm to precisely control the allocation of available bandwidth and ensure efficient line utilization.

Technology Overview

FloodGate-1 implements three innovative technologies to provide all the necessary floodgate capabilities:

- Intelligent Queuing Engine — for allocating bandwidth
- Stateful Inspection — for classifying communications
- RDED (Retransmission Detection Early Drop) — for reducing the number of retransmits and retransmit storms

Intelligent Queuing Engine

FloodGate-1 uses an enhanced Weighted Fair Queuing algorithm to manage bandwidth allocation. A FloodGate-1 packet scheduler is installed on each network interface and moves packets through a dynamically changing scheduling tree at different rates in

accordance with the Bandwidth Policy. High priority packets move through the scheduling tree and emerge on the other side of the interface more quickly than low priority packets.

The IQ Engine leverages TCP's throttling mechanism to automatically adjust bandwidth consumption by individual connections or classes of traffic. Traffic bursts are delayed and smoothed by FloodGate-1's packet scheduler, pushing back on the traffic and forcing the application to fit the traffic to the Bandwidth Policy. By intelligently delaying traffic, the IQ Engine effectively controls the bandwidth of all IP traffic.

The preemptive IQ Engine responds immediately to changing traffic conditions and guarantees that high priority traffic always takes precedence over low priority traffic. Accurate bandwidth allocation is achieved even when there are large differences in the weighted priorities (for example 50:1). In addition, since packets are always available for immediate transmission, the IQ Engine provides precise bandwidth control for both inbound and outbound traffic and ensures 100% bandwidth utilization during periods of congestion.

Stateful Inspection

Employing Stateful Inspection technology, FloodGate-1 accesses and analyzes data derived from all communication layers. This state and context data are stored and updated dynamically, providing virtual session information for tracking both connection-oriented and connectionless protocols (for example, UDP-based applications). Cumulative data from the communication and application states, network configuration and bandwidth allocation rules are used to classify communications.

Stateful Inspection enables FloodGate-1 to parse URLs and set priority levels based on file types. For example, FloodGate-1 can identify HTTP file downloads with *.exe or *.zip extensions and allocates bandwidth accordingly.

RDED (Retransmit Detect Early Drop)

TCP exhibits extreme inefficiency under certain bandwidth and latency conditions. RDED prevents these inefficiencies by detecting retransmits in TCP streams and preventing the transmission of redundant packets when multiple copies of a packet are concurrently queued on the same flow. The result is a dramatic reduction of retransmit counts and positive feedback retransmit loops. Implementing RDED requires the combination of intelligent queuing and full reconstruction of TCP streams, capabilities that exist together only in FloodGate-1.

FloodGate-1 Rule Base

A FloodGate-1 Rule Base consists of any number of rules, each of which classifies connections and indicates how to allocate bandwidth for them:

Connection Classification

A connection is classified according to three criteria:

- source — a set of network objects, including specific computers, entire networks or domains
- destination — a set of network objects, including specific computers, entire networks or domains
- service — a set of IP services, sub-services or URLs

Bandwidth Allocation

A rule can specify three factors to be applied to bandwidth allocation:

1. weights

   Available bandwidth at any given moment is divided among the connections according to weights. For example, suppose outgoing Web traffic is deemed to be three times as important as incoming FTP traffic, and these services are assigned weights of 30 and 10 respectively. Then when lines are congested, FloodGate-1 will always accurately maintain the ratio of bandwidth allocated to outgoing Web traffic and incoming FTP traffic at 3:1.

   If only two connections are active: the first has a weight of 30 and the second has a weight of 10. Then as long as they are competing, the first receives 75% (that is, 30 /40) of the remaining bandwidth and the second receives 25% (10 /40) of the remaining bandwidth. If the first closes, the second will receive 100% of the bandwidth.

   Allocating bandwidth according to weights instead of absolute priorities (such as those used in router queuing) ensures that all connections always receive at least some of the available bandwidth.

2. guarantees

   A guarantee allocates a minimum bandwidth to all the connections described by the rule, or alternatively, to each connection under the rule.

3 limits

A limit specifies the maximum bandwidth that will be assigned to all the guaranteed connections together. A limit defines a point beyond which connections under a rule will not be allocated bandwidth, even if there is unused bandwidth available. Because the use of limits can result in wasted bandwidth, FloodGate-1 provides a more flexible allocation factor: weights (see above).

Note – Bandwidth allocation is not fixed. As connections are opened and closed, FloodGate-1 continuously changes the bandwidth allocation to accommodate competing connections, in accordance with the Bandwidth Policy.

FloodGate-1 Architecture

Basic Concepts

FloodGate-1's efficient, protocol-independent Intelligent Queuing and Stateful Inspection technology provides a single integrated network bandwidth management solution. An intuitive, object oriented user interface enables easy, flexible, and uniform implementation of an organization's global Bandwidth Policy.

FloodGate-1 inspects and schedules every packet passing through key locations in an IP network. When lines are not congested, FloodGate-1's packet inspection and bandwidth allocation introduce an insignificant delay (less than 2 milliseconds).

It is when the network lines become congested that FloodGate-1 provides its real benefits. Instead of allowing all traffic to flow equally, FloodGate-1 ensures that important traffic takes precedence over less important traffic so that the enterprise can continue to function with minimum disruption possible, despite network congestion. FloodGate-1 ensures that an enterprise can make the most efficient use of a congested network.

By dynamically controlling the mix of traffic at an aggregate level (not just on a per-connection) basis, FloodGate-1 delivers total bandwidth management. For the first time, an enterprise can intelligently allocate limited bandwidth among multiple classes of traffic, including critical Internet applications or important groups of users.

FloodGate-1 is completely transparent to both users and applications. FloodGate-1 coexists with other software.

A line is said to be "FloodGated" if a FloodGate Module controls the bandwidth on that line. The FloodGate Module is inside the operating system kernel, between the Data Link and the Network layers (layers 2 and 3). Since the data link is the actual network interface card (NIC) and the network link is the first layer of the protocol stack (for example, IP), FloodGate-1 is positioned at the lowest software layer.

The FloodGate-1 Management Server is used to configure the enterprise-wide Bandwidth Policy, control the FloodGate Modules, and monitor performance. A set of command line utilities enable operation from a standard terminal.

FloodGate-1 works independently of the network interface, and therefore supports all network interfaces that are supported by the underlying operating system.

FloodGate Modules

FloodGate-1 consist of three components:

1. FloodGate-1 GUI Management Client

   The Bandwidth Policy Rule Base editor is used to create and modify the Bandwidth Policy and define the network objects. If both VPN-1/FireWall-1 and FloodGate-1 are licensed, then Bandwidth Rules are displayed as an additional tab in the Check Point Policy Editor.

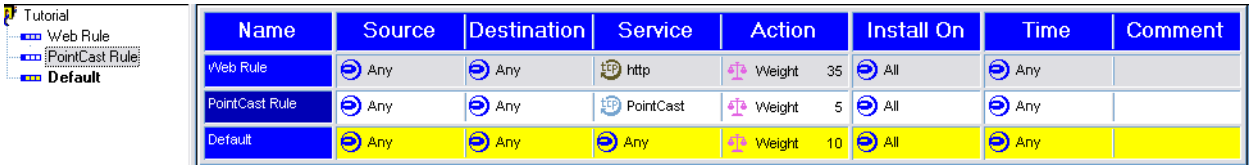


FIGURE 5-1 Bandwidth Rules in the GUI

2. Management Server

   The Management Server controls and distributes the Bandwidth Policy to all FloodGate Modules.

3. FloodGate Module

   The FloodGate Module implements the Bandwidth Policy at network access points and controls the flow of inbound and outbound traffic.

Management Server

The Management Server includes the GUI and the Management Server.

FloodGate Module

The FloodGate Module enforces the Bandwidth Policy defined in the Management Server.

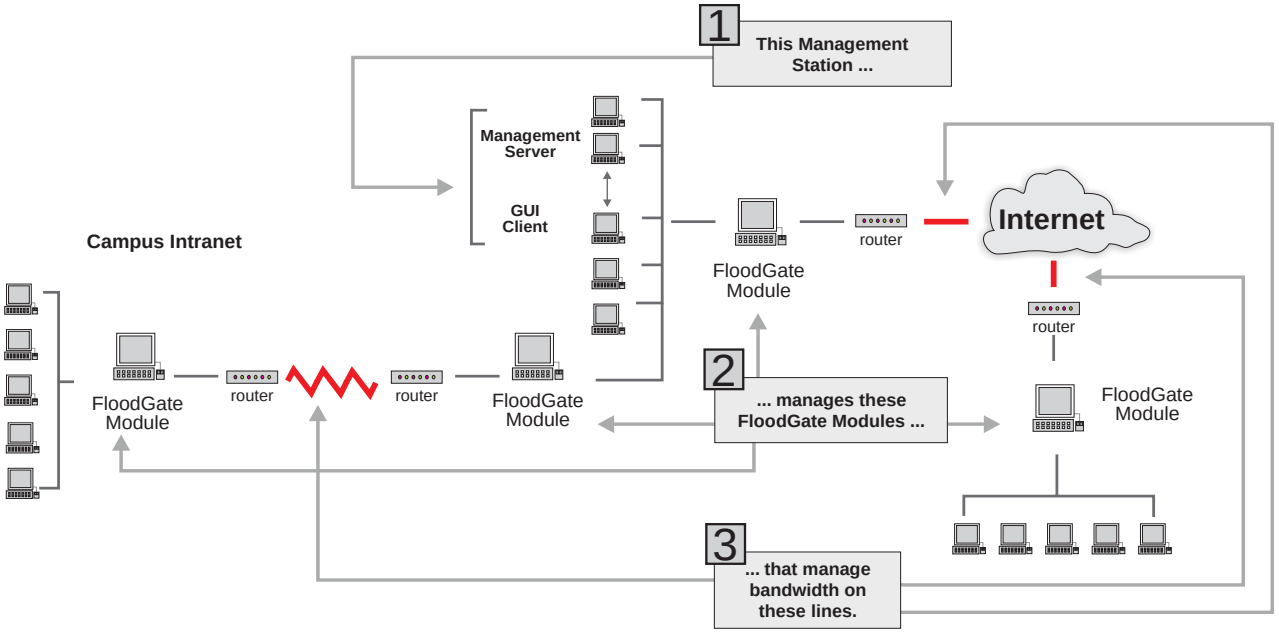


FIGURE 5-2 Distributed FloodGate-1 Configuration

FIGURE 5-2 shows a distributed configuration, on which one Management Station (consisting of a Management Server and a GUI Client) controls four FloodGate Modules, which in turn manage bandwidth allocation on three FloodGated lines.

Bandwidth Policy

A FloodGate-1 Bandwidth Policy is defined in terms of FloodGate Modules, interfaces, services, resources and the rules that govern the interactions between them. Once these have been specified, the Bandwidth Policy is installed on the FloodGate Modules that will enforce it on their network interfaces.

A single Management Server can control and monitor multiple FloodGate Modules. The FloodGate Module operates independently of the Management Server. FloodGate Modules can operate on additional Internet gateways and interdepartmental gateways.

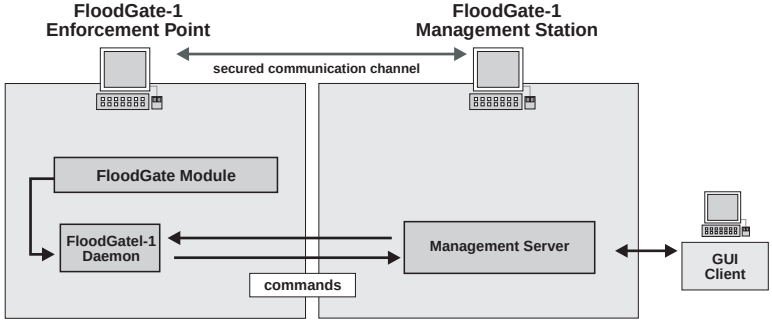


FIGURE 5-3 FloodGate-1 Components

FIGURE 5-3 depicts a configuration where the FloodGate Module and the Management Server are installed on different machines. They can also be installed on the same machine.

Bandwidth Rule Base

A Rule Base is a set of rules that defines a specific Bandwidth Policy. A rule classifies a communication in terms of its source, destination and service, and specifies the bandwidth to be allocated to connections to which the rule applies. If both VPN-1/ FireWall-1 and FloodGate-1 are enabled by your license, Bandwidth Rules are defined using the Check Point Policy Editor.

The Rule Base and the properties of the objects (networks, hosts and services) used in the Rule Base are compiled and transmitted on a secured control channel from the FloodGate-1 Management Station — the computer on which the Bandwidth Policy was defined — to the FloodGate Modules that will enforce the policy. The FloodGate-1 daemon loads the compiled code into the OS kernel, which enforces the Bandwidth Policy. Communication between the FloodGate Module hosts and the Management Server is secured (see FIGURE 5-3).

Performance

The FloodGate Module's simple and effective design achieves optimum performance by these techniques:

- Running inside the operating-system kernel imposes negligible overhead in processing. No context switching is required, and low-latency operation is achieved.
- Advanced memory management techniques, such as caching and hash tables, are used to unify multiple object instances and to efficiently access data.

- Generic and simple inspection mechanisms are combined with a packet inspection optimizer to ensure optimal utilization of modern CPU and OS designs.
- The preemptive Packet Scheduler ensures that high priority traffic is always given precedence over lower priority traffic. In addition to bandwidth limits and guarantees, FloodGate-1 prioritizes traffic based on weighted priorities to ensure that even low priority traffic receives some bandwidth on a consistent basis.

Technology Comparison

TABLE 5-1 summarizes the differences between FloodGate-1 and other, less sophisticated methods of bandwidth management.

FloodGate-1 uses Multi-Path Queuing, which provides an unlimited number of queues and grows or shrinks dynamically with no fixed limits. In this sense, Multi-Path Queuing is a better form of TCP Rate Control.

TABLE 5-1 TCP Rate Control technology Comparison

Efficiency Criteria	Basic/Classic Queuing (Class Based Queuing) typical in routers	TCP Window Control (or Sizing)	Check Point Multi-Path Queuing
Response Time	As single or limited queues fill up, response times increase quickly.	As the number of connections increases, the response time also increases because of the round trip acknowledgment requirements of TCP Window Control. The longer the round trip time, the longer the response time due to delays in implementing window control changes.	Response time is immediate since there is no round trip acknowledgment required and there are unlimited queues that are dynamically allocated as requirements change.
Line Utilization	Line utilization is inefficient because only what is in the queue can be controlled.	As the number of connections increases (over 200), line utilization falls because the window sizing decisions do not occur quickly enough.	Line utilization can attain 100% because changes are instantaneous and are unaffected by the number of connections.
Latency	Latency control is poor because there is only a single queue (or a limited number of queues).	Latency is unpredictable as the number of connections grows. Window sizing decisions are based upon incorrect information that results from delayed acknowledgments.	Predictable and controllable, even as the number of connections grows.

TABLE 5-1 TCP Rate Control technology Comparison (continued)

Efficiency Criteria	Basic/Classic Queuing (Class Based Queuing) typical in routers	TCP Window Control (or Sizing)	Check Point Multi-Path Queuing
Number of Connections	Limited by the queue size.	Limited by the rate at which changes to the Window Control connection can be made and the time it takes for them to actually occur.	Unlimited, based upon the dynamic preemptive nature of Multi-Path Queuing.
Congestion	Will already have occurred due to the rigid, limited number of queues.	Is prevented as long as the Window Control changes are instantaneous. Congestion is created if window sizing changes are not instantaneous.	No congestion is caused because changes and adjustments to increased traffic are instantaneous due to the dynamic nature of Multi-Path Queuing.
Accuracy	Limited by the rigid, limited number of queues.	Accuracy is limited by the rate at which changes to the Window Control connection can be made and the time it takes for them to actually occur. As the number of connections grows, accuracy suffers.	Accuracy is 100%, even as the number of connections grows.
Queues are too deep or too shallow, resulting in packet loss	Applies.	Does not apply; there are no queues.	Does not apply since the number of queues is unlimited and dynamic within Multi-Path Queuing.
Inbound Traffic Control	No inbound control capabilities.	No inbound shaping because the decision making process for window control criteria is located too far from the sender.	Achieved through a preemptive scheduling process proprietary to Check Point.
Non TCP Application protocol support. (UDP, ICMP, multimedia applications)	Will support non TCP applications and protocols.	TCP Window Control cannot control non-TCP applications and protocols because they are connectionless. Connectionless protocols do not require acknowledgment. Therefore, there is no window to size and the only way to control non-TCP applications is through a form of queuing.	Full support for all TCP/IP applications, protocols and services, including many of the most popular multimedia applications available today.

Conclusion

To summarize, FloodGate-1's sophisticated technology includes a number of unique features:

Intelligent Queuing Engine

FloodGate-1's Intelligent Queuing Engine (IQ Engine™) accurately classifies traffic and places it in the proper transmission queue. The IQ Engine includes an enhanced, hierarchical Weighted Fair Queuing (WFQ) algorithm to precisely control the allocation of available bandwidth and ensure efficient line utilization, and moves packets through a dynamically changing scheduling tree at different rates, in accordance with the Bandwidth Policy.

Stateful Inspection

The FloodGate Module inspects and schedules all inbound and outbound packets on all FloodGated lines. The FloodGate Module can examine and evaluate all the information in the message, and understands the internal structures of the IP protocol family and applications built on top of them. FloodGate-1 is able to extract data from the packet's application content and use it to provide context for effective classification.

Simplicity

FloodGate-1's rule-based design enables users to define a Bandwidth Policy in terms of simple objects and relationships between them. Only the network objects used in the Rule Base need be defined by the user, and a comprehensive list of predefined services is available.

The FloodGate Module is implemented as an independent, compact code module, and resides inside the operating system kernel as a loadable kernel-level module.

FloodGate-1 is transparent to applications and users and requires no special configuration or setup other than on the machines on which it is installed.

Manageability

Enterprise-wide bandwidth management and inter-network bandwidth management can be managed by FloodGate-1 with equal facility.

Supporting data rates of up to 45 Mbps, FloodGate-1 improves quality of service by eliminating the burst-and-delay effect inherent in most Internet traffic. Comprehensive monitoring capabilities provide detailed information to show the allocation of bandwidth by user, application and connection.

CHAPTER 6

Open Security Extension

In This Chapter

Security Device Management

Expanding Internet technologies have redefined corporate approaches to internetworking and security. As the Internet becomes the forum for business communications, an integrated framework for network security and management is essential.

Enterprises currently deploy a variety of networking technologies at critical network access points — either between segments of the local network or at the Internet link. Hardware routers and software packet filters examine packets based on complex filtering rules. Other hardware devices combine packet filtering with security features such as address translation, authentication, and encryption.

These diverse technologies are difficult to configure and manage within a single network for the following reasons:

Complex Configuration Methods

Filtering rules are complex and manually configured for each device. Filtering rules are either defined on the command-line interface of each device or in a text file that is installed via separate TELNET or SNMP sessions. This requires a detailed knowledge of complex filtering syntax, the IP addresses of specific hosts and networks, and the ways in which different devices apply filtering rules.

Limited Manageability

Multiple networking and security devices also divide the network into separate management systems. Each device protects a different segment of the network. Filtering rules are configured and updated for each device and downloaded through separate TELNET or SNMP sessions. Administrators must devise separate management strategies and security configurations for each network segment.

Restricted Network Growth

It is difficult to update and expand the enterprise network. The incorporation of additional network objects or security devices requires a new set of filtering rules for each device. As a result, network administrators are often restricted to single-vendor networking solutions.

Inconsistency

The security administrator defines filtering rules for each network segment without an overall view of the entire configuration, making it nearly impossible to enforce an enterprise-wide Security Policy. Separate configuration strategies often generate errors and unexpected interactions between filtering rules, thereby exposing the entire network.

Open Security Extension

In contrast, Check Point's optional Open Security Extension module integrates diverse networking technologies into the VPN-1/FireWall-1 management framework. An enterprise-wide Security Policy is defined using the Check Point Policy Editor. VPN-1/FireWall-1 then generates filter rules, or Access Lists, from the Security Policy and distributes them to routers and security devices throughout the network.

The Check Point Policy Editor simplifies security configuration and management. Administrators can define routers, security devices and other network resources in terms of simple network objects and their properties. The enterprise Security Policy is defined using the Policy Editor. Access rules are defined in terms of network objects, services and connections. Both object properties and access rules are easily modified and automatically updated using the Policy Editor. This object oriented method is both simple and efficient, freeing network administrators from time-consuming configuration tasks.

Security management is consistent and integrated. Access Lists for all devices are automatically examined for inconsistencies or unexpected interactions between rules. Each device enforces the relevant security rules. Although multiple devices protect the network, there is only one Security Policy, which is maintained by the VPN-1/ FireWall-1 Management Server.

Open Security Extension provides an open framework for network management. Access Lists are managed for any number of the following third-party routers and devices:

- Bay Networks Routers — Version 7.x -12.x
- Cisco Routers — IOS Version 9,10,11
- Cisco PIX Firewall — Version 3.0, 4.0, 4.1
- 3Com NetBuilder — Version 9.x
- Microsoft Routing and Remote Access Service (RRAS) for Windows NT Server 4.0 (Windows NT platforms only)

Open Security Extension enables VPN-1/FireWall-1 administrators to import Access Lists for PIX, 3Com, Cisco and Microsoft RRAS, enabling the integration of existing filter configurations through the Check Point Policy Editor.

Integration with VPN-1/FireWall-1

Router and device management is fully integrated into VPN-1/FireWall-1 architecture and centrally managed through the Check Point Policy Editor.

Check Point GUI Client

The Check Point GUI Client is used to define and modify the Security Policy. The Security Policy is defined in terms of network objects, devices, services, and access rules.

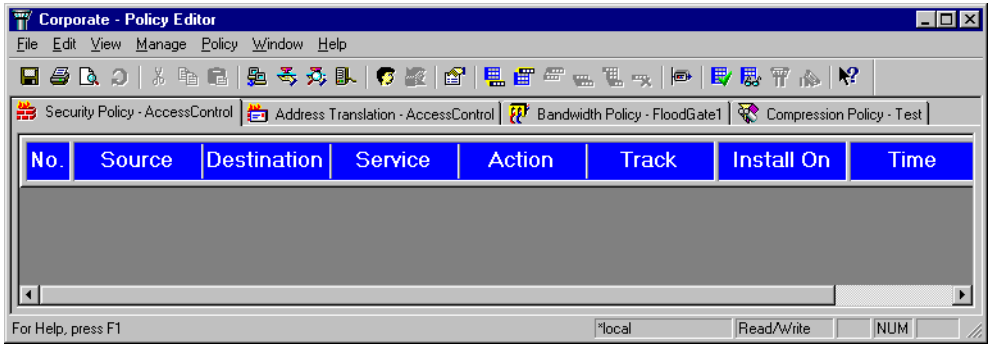


FIGURE 6-1 Check Point Policy Editor

The GUI Client also includes a graphical Log Viewer that shows all connections logged by the `syslog` facility of managed routers and security devices. For more information see “Log Viewer” on page 127.

Check Point Management Server

The Security Policy is defined using the Policy Editor and saved on the Management Server. The Management Server maintains the Security Policy and the VPN-1/FireWall-1 databases, including the Rule Base, router and integrated firewall objects, and services. Access Lists are generated from the Security Policy and distributes them to designated routers and security devices.

Distributed Configurations

The Check Point GUI Client and the Management Server can be deployed on the same machine or in a Client/Server configuration to enable remote management. In a Client/Server deployment, a GUI client is the front end to the Management Server. The Security Policy is defined using the GUI client and maintained on the Management Server. The Management Server generates Access Lists from the Security Policy. Access Lists are downloaded to network routers and devices, which protect the network. Both the GUI Client and the Management Server can be installed on any supported platform.

FIGURE 6-2 on page 123 shows a Client/Server configuration in which the Management Server controls two different security devices, each of which protects an internal heterogeneous network.

In this configuration, the Security Administrator configures and monitors different network segments from a single desktop machine. The Security Policy is defined using the Policy Editor on the Check Point GUI Client, while the database is maintained on the Management Server. The connections between the Client, Management Server and multiple enforcement points are secured, enabling true remote management.

Although VPN-1/FireWall-1 components can be deployed in a distributed configurations, Security Policy enforcement is completely integrated. Any number of routers and security devices can be configured, monitored and controlled from a single management console, but there is only one Security Policy. Only authorized managers can access and update the Security Policy from anywhere on the network.

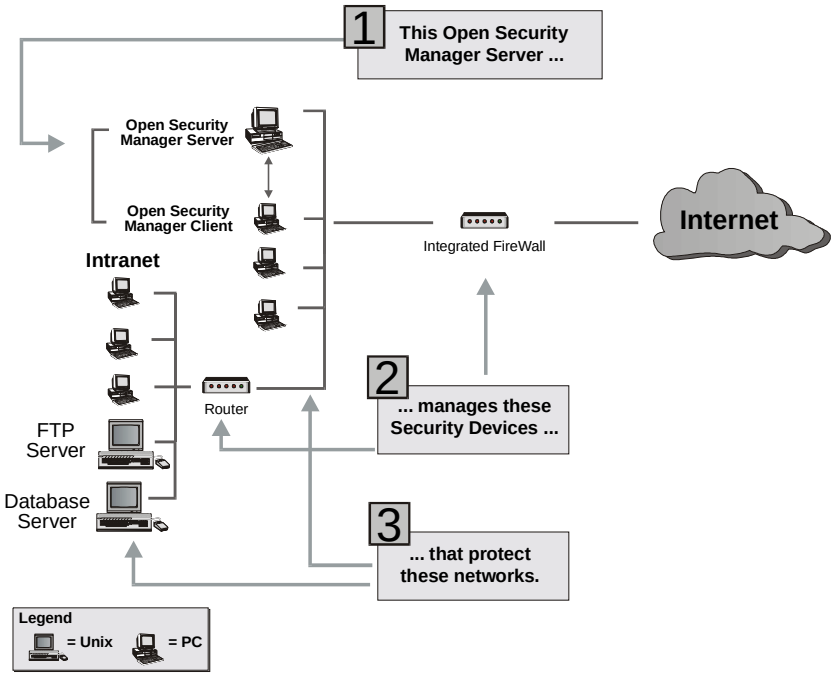


FIGURE 6-2 Distributed Configuration

Check Point Policy Editor

Defining Managed Devices

The VPN-1/FireWall-1 Network Object Manager makes it easy to define all the network's resources in terms of object classes and their properties. Objects can be grouped in families or organized in hierarchies for more efficient control. Object properties can be centrally managed and updated.

Every object has a set of attributes, such as network address, subnet-mask, etc. The user specifies some of these attributes, while the Management Server retrieves other properties from the network databases. SNMP agents extract additional information, including the interfaces and network configuration of hosts, routers and other devices.

The Network Object Manager (FIGURE 6-3) is used to define the routers and devices that are managed by the Security Policy.

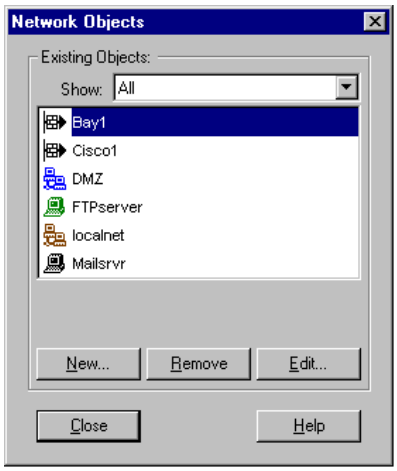


FIGURE 6-3 Network Object Manager

Open Security Extension enables VPN-1/FireWall-1 administrators to define and manage the following objects:

- routers

  Router objects include hardware and application packet filters. Bay, Cisco, 3Com and Microsoft Steelhead routers are managed as router objects.

- integrated firewalls

  An integrated firewall is a hardware device providing packet filtering and additional security features, such as authentication. Cisco PIX Firewall is managed as an integrated firewall.

- groups of the above

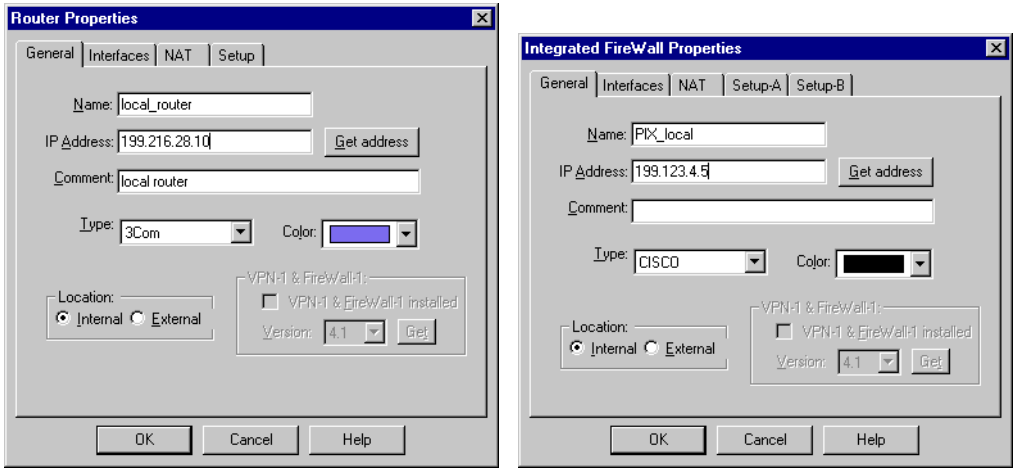


FIGURE 6-4 3Com router and PIX integrated firewall objects

Rule Base

Routers and integrated firewall objects can be defined and used in the Rule Base. A Rule Base is an ordered set of rules that defines a specific Security Policy. A rule describes a communication in terms of its source, destination and service, and specifies whether the communication should be accepted or rejected. A rule also specifies whether a communication is to be logged by the `syslog` facility of the router or integrated firewall enforcing the rule.

Rules also specify the host, interface and direction to which a rule applies. Packets can be inspected in any of three directions: inbound, outbound or eitherbound, depending on the objects on which the rule is installed and therefore enforced.

The Rule Base and the properties of the objects (networks, services, and hosts) used in the Rule Base are converted into Access Lists, which are installed on the targeted routers and integrated firewalls.

Open Security Manager follows the security principle of “All communications are denied unless expressly permitted.” Open Security Manager drops traffic that is not explicitly allowed by the enterprise Security Policy.

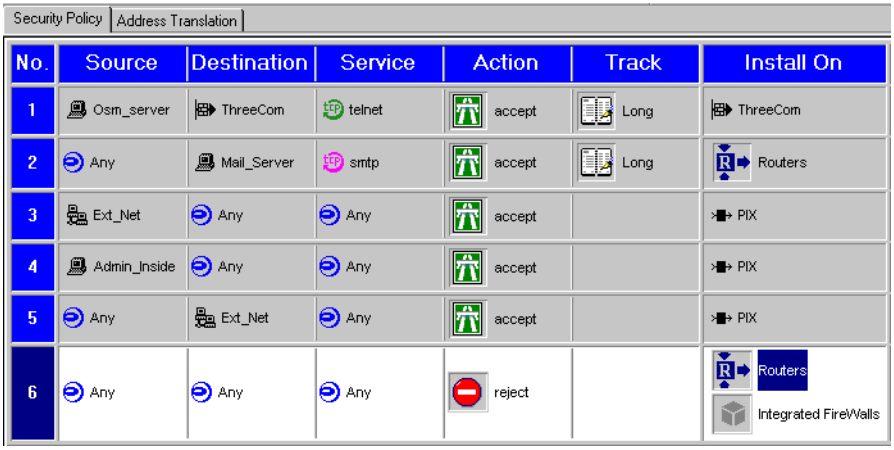


FIGURE 6-5 Example Rule Base

Properties

A Security Policy is defined not only by the Rule Base, but also by the parameters in the **Access Lists** tab of the **Properties Setup** window (FIGURE 6-6 on page 127). Properties define the overall aspects of inspection without the need to specify repetitive details in the Rule Base. Properties are global to all Rule Bases. Properties are not applied to an imported Rule Base.

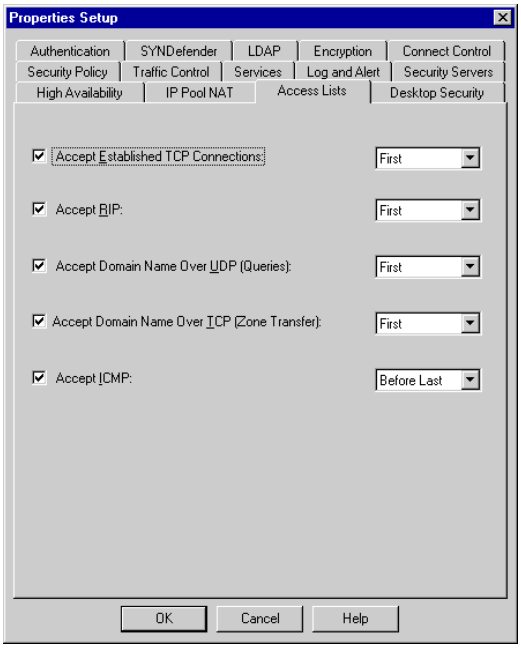


FIGURE 6-6 Properties Setup Window - Access Lists tab

Address Translation Rule Base

The VPN-1/FireWall-1 Address Translation Rule Base simplifies PIX address translation management. The Address Translation Rule Base allows administrators to specify objects by name rather than by IP address. Administrators can define simple, graphical rules that dynamically or statically map the local network addresses to PIX Global Addresses.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	InsideAddresses	Any	Any	GlobalAddresses	= Original	= Original	PIX1	
2	AdminInside	Any	Any	AdminGlobal	= Original	= Original	PIX1	

FIGURE 6-7 Address Translation Rule Base editor

Log Viewer

A graphical Log Viewer enables visual tracking and monitoring for all connections passing through managed routers and security devices. On-line viewing features enable real-time monitoring of network activity. The Log Viewer also displays significant events, such as Security Policy installations.

The Log Viewer also provides precise control over the log file display, providing quick access to relevant information. Administrators can customize the Log Viewer to display or hide specific fields. Logs and log records can be filtered and searched to quickly locate and track events of interest. Colors and icons attached to events and fields also facilitate tracking.

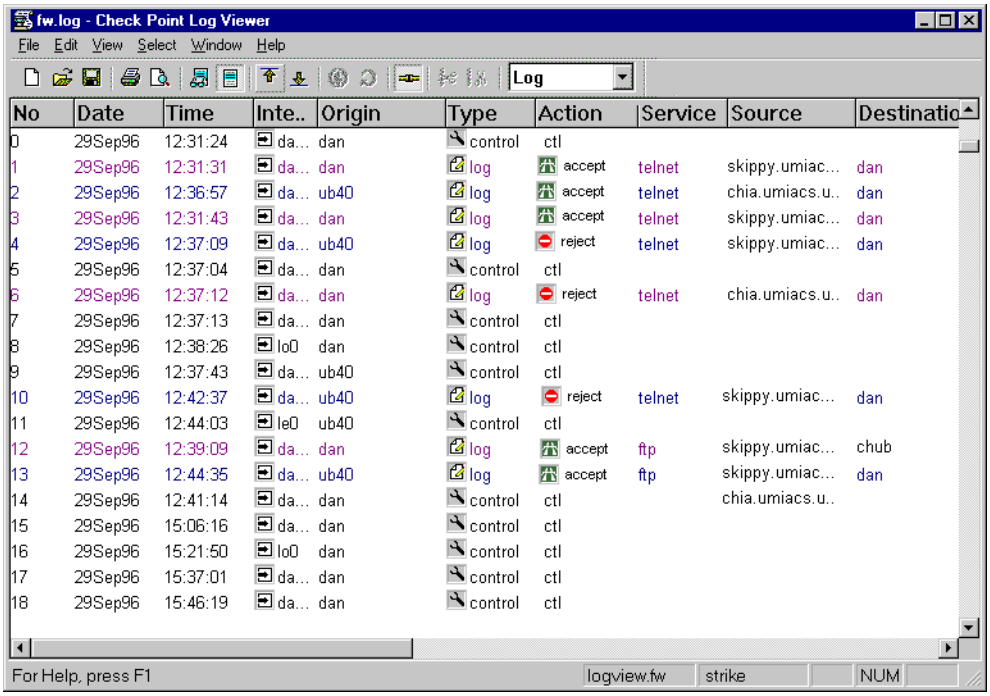


FIGURE 6-8 Log Viewer

Conclusion

Open Security Extension enables VPN-1/FireWall-1 Administrators to manage multiple security devices across the enterprise network within a single framework.

Centralized Management

Administrators can configure and monitor an enterprise Security Policy from a single management console. The Security Policy is defined using the Check Point Policy Editor and maintained on the Management Server. Access Lists are generated from the Security Policy and installed on the targeted routers and integrated firewalls. A flexible Client/Server structure enables remote configuration and management. Designated administrators can access and configure the Security Policy from anywhere on the network. Security management is completely integrated — there is only one Security Policy, maintained on the Management Server.

Simple Configuration

An intuitive, object-oriented interface allows administrators to simply define a Rule Base and implement a Security Policy. Administrators no longer need to manually configure complex filter rules. Instead, routers and devices are defined in terms of simple objects and their properties. Object properties can be automatically retrieved using SNMP agents. Network objects can be centrally managed and updated. The graphical Check Point Policy Editor provides a comprehensive view of the enterprise's security configuration.

Consistency

VPN-1/FireWall-1 checks the Rule Base for redundant and inconsistent rules, eliminating configuration errors and unexpected interactions between rules.

Open Management Framework

Open Security Extension enforces a single enterprise Security Policy across multiple vendor routing and security devices. Network administrators are no longer restricted to single-vendor networking solutions. In addition, new network objects and devices can be integrated into the network without the need to configure separate filter rules for each network segment.

CHAPTER 7

Reporting Module

In This Chapter

Overview

The Check Point Reporting Module delivers a comprehensive solution for monitoring and auditing traffic in a FireWalled network. You can generate fully detailed or summarized reports for all connections intercepted and logged by the FireWall Module. Reports can be used to track and analyze traffic between your enterprise network and the Internet as well as transactions within your enterprise.

Network Traffic Monitoring

The Reporting Module provides in-depth details on network traffic and activity. Network Administrators can generate reports in order to:

- Analyze the network load.

  Network load reports can help administrators determine which services require the most network resources. Reports can further identify the departments and users that generate the most traffic and times of peak activity.

- Detect and monitor suspicious activity.

  Network administrators can produce reports documenting blocked traffic, alerts, rejected connections, or failed authentication attempts in order to identify possible intrusions.

- Audit and estimate costs of network use.

  The Reporting Module provides information on how the use of network resources is divided among corporate users and departments. Reports summarizing customer use of services, bandwidth and time can provide a basis for estimating cost per user or department.

Detailed Reporting

The Reporting Module system provides fine-tuned control over the collection and processing of VPN-1/FireWall-1 Log data. VPN-1/FireWall-1 Log entries are consolidated into connection records which are then loaded into a central database. Administrators configure all consolidation parameters and select the connection attributes that make up the database.

Administrators can define reports based on detailed customer and connection data. Flexible report parameters specify how connection data is processed and displayed. The Reporting Module includes different report types to display network trends and events of interest. Reports can be generated as tables, pie charts or graphs.

A selection of predefined reports provide essential information network transactions. These reports may serve as the basis for more customized reports to fit the specific requirements of the enterprise.

Report Distribution

The Reporting Module centrally manages report distribution. Reports are produced in ASCII, HTML, OS command formats and distributed to specific network objects. The Reporting Module also includes a proprietary format for report results. For example, an ASCII file can be sent as email attachment, a report results file can be sent to a printer, and an HTML file can be sent to a local HTTP server.

Centralized Management

A modular architecture enables centralized data collection and report management. A powerful Log Consolidator collects and consolidates VPN-1/FireWall-1 Log data from the VPN-1/FireWall-1 Management Server. Consolidated records are loaded into a Database that is the central data store for the Reporting Module system. All report and distribution parameters are configured from a graphical user interface. While multiple GUI clients may configure report parameters, all data collection and retrieval processes run on a single machine.

Reporting Module Architecture

Report generation consists of two basic processes:

1. VPN-1/FireWall-1 Log consolidation

   Reports are based on VPN-1/FireWall-1 Log data. The Reporting Module aggregates multiple VPN-1/FireWall-1 Log entries into detailed connection records. Details from these records are then exported to a Database. This Database maintains all the information available for report generation.

   Log consolidation enables you to integrate multiple Log entries into a single entry in the Database. Connection data is maintained in a format that both enables efficient retrieval and saves disk space.

2. Data retrieval

   Connection information is retrieved from the Database in order to generate reports.

The Reporting Module includes the following components to implement Log consolidation and data retrieval:

- Reporting Client

  Log consolidation and data retrieval parameters are defined using the Reporting Client.

- Reporting Server

  The Reporting Server uploads VPN-1/FireWall-1 Log data and generates reports according to parameters defined using the Reporting Client.

Reporting Client

The Reporting Client is supported on Windows 9x and Windows NT platforms. This section describes the Reporting Client components.

The Reporting Client includes two Graphical User Interface components:

- Log Consolidator
- Reporting Tool

Log Consolidator

VPN-1/FireWall-1 logs are processed and stored according to a Consolidation Policy. The Consolidation Policy is defined using the Log Consolidator.

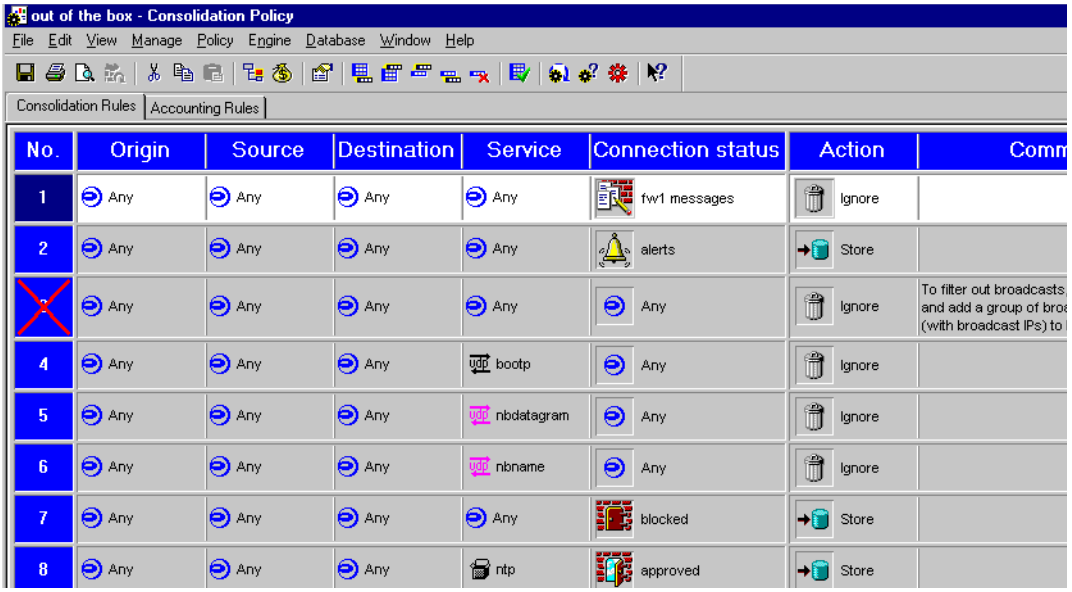


FIGURE 7-1 Log Consolidator — Consolidation Policy

A Consolidation Policy consists of consolidation rules and accounting rules. Consolidation rules define which logged connections are stored in the Database, and how they are consolidated. Accounting rules assign customer names and accounting units (for example, the cost for use of a specific service) to consolidated records. In this way connections can be attributed to specific departments or users within the organization for accounting purposes.

Reporting Tool

The Reporting Tool enables you to define report attributes and generation parameters and view report results. Report display formats, output formats, and distribution parameters are also defined using the Reporting Tool.

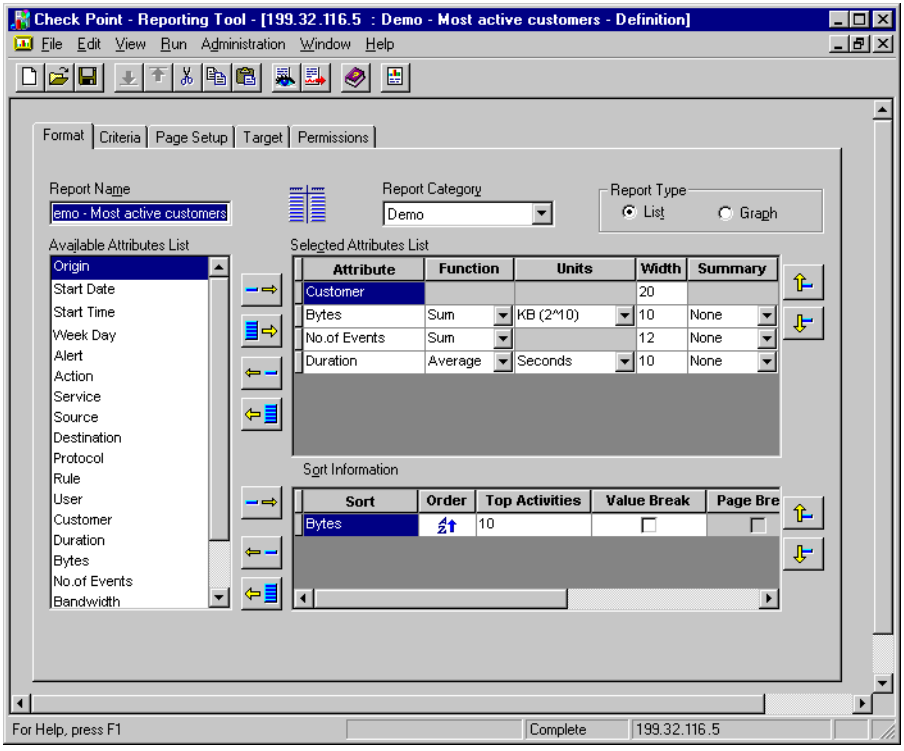


FIGURE 7-2 Reporting Tool Graphical User Interface

Reporting Server

Log consolidation and data retrieval parameters are defined using the Reporting Client (the Log Consolidator and the Reporting Tool) and downloaded to the Reporting Server. The Reporting Server uploads VPN-1/FireWall-1 Log data and generates reports according to parameters defined on the Reporting Client. The Reporting Server consists of the following components:

- Log Consolidator Engine
- Database
- Report Server

The Reporting Server is supported on the Windows NT and Solaris platforms. This section describes the Reporting Server components.

Log Consolidator Engine

The Log Consolidator Engine collects Logs from the VPN-1/FireWall-1 Management Server and integrates multiple Log entries into detailed connection records. Specific information from the consolidated records is then stored in the Database.

The Log Consolidator Engine processes Logs according to the Consolidation Policy. The Consolidation Policy is defined using the Log Consolidator (see FIGURE 7-1 on page 134).

Database

The Log Consolidator Engine populates the Database with connection records. The Database maintains detailed information on network transactions derived from VPN-1/FireWall-1 Log files. The Report Server retrieves and processes information from the Database.

Report Server

Report generation and distribution parameters are defined on the Reporting Tool and downloaded to the Report Server. The Report Server retrieves the required information from the Database. The Report Server sends results to the Reporting Client and other specified targets in the requested formats. For example, a generated report can be sent as an HTML file to a local HTTP server.

Interaction Between Components

The Reporting Server (Report Server, Log Consolidator Engine, and Database) is installed on the same machine as the active VPN-1/FireWall-1 Management Server. Both the Reporting Server and the VPN-1/FireWall-1 Management Server must be installed on a Windows NT platform.

Note – This version of the Reporting Module is compatible with VPN-1/FireWall-1 version 4.0 SP-2 or higher.

Note – The Reporting Server can also be installed on a standalone Windows NT machine, and the active Management Server is installed on another machine, on any platform. This configuration requires a second VPN-1/FireWall-1 Management Server, version 4.0 SP-2 or higher.

The Reporting Client (including the Log Consolidator and the Reporting Tool) can be installed on the same machine as the Reporting Server or on a separate Windows 95 or Windows NT machine to enable remote management.

FIGURE 7-3 depicts the interaction between the Reporting Module components:

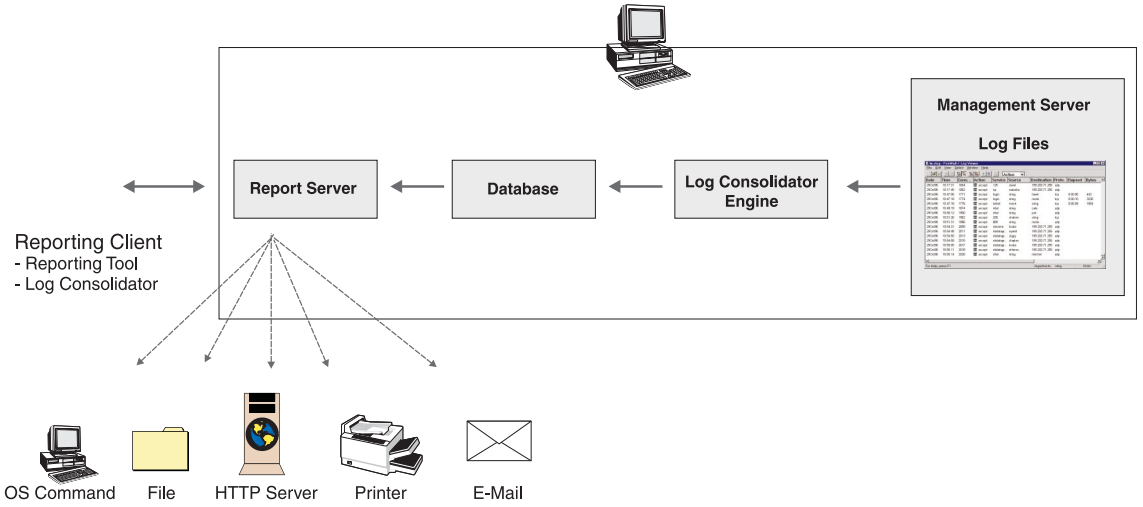


FIGURE 7-3 Reporting Module Components

Data Flow

1. The Log Consolidator Engine collects Log entries from the Management Server and integrates multiple entries according to the Consolidation Policy.

   Consolidation and accounting rules are defined using the Log Consolidator.

2. The Log Consolidator Engine stores specific details from the consolidated records in the Database.

3. The Report Server retrieves connection data according to report generation and distribution parameters defined with the Reporting Tool.

4. The Report Server sends report results to the Reporting Client. Report results are displayed on the Reporting Tool GUI.

   Reports can be generated in different formats — ASCII files, HTML, or FWR (proprietary format) files. The Report Server distributes report results to specified network targets in the requested format.

FIGURE 7-4 depicts the Reporting Module components within the FireWalled network.

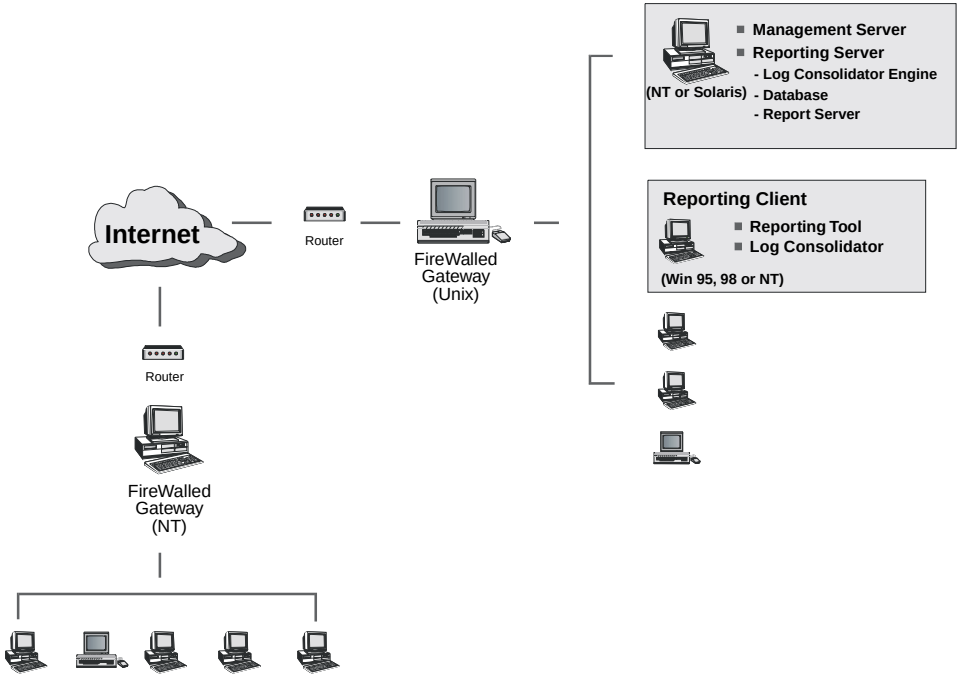


FIGURE 7-4 Example Configuration

In the above configuration, all FireWalled gateways send logs and alerts to the VPN-1/FireWall-1 Management Server. The Reporting Server components and the Management Server are installed on a single Windows NT machine. Report generation and distribution information is defined using the Reporting Tool GUI. Reports can be configured and activated using the Reporting Tool GUI.

Security

Data collection and distribution is centralized and secure. All communication between the system components is encrypted. Although multiple GUI clients can configure system parameters, all data collection and retrieval processes run on a single machine. Only designated Administrators may modify system parameters.

All Reporting Module users are the VPN-1/FireWall-1 Administrators. There are two user levels: Administrator and Standard User. Administrators are VPN-1/FireWall-1 Administrators with Read/Write permissions. Administrators can define and modify reports, and specify the other users that have access to the report definition. Standard Users are VPN-1/FireWall-1 Administrators with Read Only permissions. Standard Users may display and activate defined reports. In this way, only relevant users may access specific information.

CHAPTER 8

Meta IP

Overview

Managing and controlling the rapidly growing IP infrastructure of modern corporate networks is the major concern of today's enterprise-wide network managers. With exponential network growth and increasing demands on the IP infrastructures, network managers need a system that can help them quickly and reliably manage all IP services.

Why Meta IP?

The Meta IP 4.1 IP Management System

Meta IP 4.1 is a modular IP Management System that provides centralized control and distributed management of enterprise-scale IP networks. It consists of a suite of tightly integrated IP network services (DHCP, DNS, and RADIUS). Meta IP provides flexible and easy-to-use enterprise management, auditing and reporting tools, and a distributed LDAP architecture data repository. These components provide fault-tolerant IP services to every user and device connected to the network. They also let you control IP Addresses, services, and network devices, as well as protecting your infrastructure from catastrophic failure.

Administration can be accomplished from any console on the network. Should a problem arise or a configuration question be raised while you are not physically present at the server, there is no need to move to the server to interact with it. There is always the built-in ability to access the Meta IP/DNS, Meta IP/DHCP, and Meta IP/RADIUS servers from most any PC, Mac, SUN, HP or UNIX-based workstation on the network, while still retaining the full security of encrypted command transmission. This is made possible via the *Meta IP/Admin Console* – an easy to use, intuitive graphical interface that includes cross-platform capability. Any machine with a Java interpreter can run the *Meta IP/Admin Console*.

You can view and process reports in HTML format for simple, easy-to-view presentations. You can email, print, and save reports or address/user tracking information as simple text documents. You can then import the documents into a favorite spreadsheet for more detailed graphing and usage tracking that can help you make important network decisions easily.

System Architecture

The modular and distributed nature of the Meta IP System architecture allows the incremental deployment of IP management into both new and existing networks. Its DEN-ready[1] technology provides a fully distributed, enterprise-capable IP management solution by integrating information systems and essential IP network services. Each of the Meta IP system's services can be distributed throughout the network and monitored and managed centrally.

In addition, Meta IP's LDAP-compliant data store distributes and replicates network data. Replication and distribution of critical network data assures a highly fault tolerant level for daily operations.

Component Services

DHCP (Dynamic Host Configuration Protocol) Service

The Meta IP System incorporates the leading standards-based DHCP server for the automation of IP Address allocation. The Meta IP/DHCP server supports true Dynamic DNS for the dynamic registration of client lease information, SNMP publication of lease activity and operational state information, automatic service fail-over and recovery, and support for Token Ring networks.

Meta IP/DHCP complies to the following Requests for Comments (RFCs):

- RFC 0951 Bootstrap Protocol (BOOTP)
- RFC 1497 BOOTP Vendor Information Extensions
- RFC 1534 Interoperation Between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 2132 DHCP Options and BOOTP Vendor Extensions

DNS (Domain Name System) Service

Meta IP/DNS is the industry leading commercial Domain Name System service for Windows NT. Based on the latest BIND (Berkeley Internet Name Domain) 8.1.2 version, Meta IP/DNS automates the translation of computer host names to IP Addresses.

With Meta IP/DNS, network managers can consolidate DNS management of both UNIX and Windows NT-based DNS servers on the network. In addition, Meta IP/DNS is one of the only DNS services on the market today that offers an intelligent load balancing add-on solution.

1. DEN: Directories Enabled Networks.

Meta IP/DNS complies to the following Requests for Comments (RFCs):

- RFC 0974 Mail Routing and the Domain System
- RFC 1034 Domain names – concepts and facilities
- RFC 1035 Domain names – implementation and specification
- RFC 1183 New DNS RR Definitions
- RFC 1884 IP Version 6 Addressing Architecture
- RFC 1886 DNS Extensions to support IP version 6
- RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- RFC 2052 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2065 Domain Name System Security Extensions
- RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 2137 Secure Domain Name System Dynamic Update

RADIUS (Remote Authentication Dial-in User Service) Service

Since remote computing has become more common and necessary, the Meta IP System includes a standards-based implementation of the Remote Authentication Dial-In User Service (RADIUS). The RADIUS service supports the configuration and authentication of dial-in users via client communications servers. It easily integrates into network authentication services for configuration on a per user basis.

Meta IP/RADIUS complies to the following Requests for Comments (RFCs):

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)

UAM (User-to-Address Mapper ™) Service

The Meta IP/UAM Service matches user names to IP Addresses and other related information to allow system-wide auditing and policy-based networking. The UAM tracks the usage of IP Address leases by recording data sent to it by the UAT, DHCP and RADIUS services for later study.

Meta IP 4.1 Key Features

Search Utility

The Meta IP/Admin Console's context sensitive Search feature lets you conveniently search through a large database of network objects for specific elements that match your search criteria.

RADIUS User Interface Improvements

Meta IP 4.1 supports configurable RADIUS Realms, an easy method of controlling user and client configuration. Realms are user-configured RADIUS authorization methods that are accessible to users. They let you incorporate whatever degree of login flexibility you need for your RADIUS clients and users.

Print view to HTML formatted files

Meta IP 4.1 can export detailed network configuration details to HTML format files. These are then displayed in your web browser, but can be saved for later study.

Enhanced Auditing and Reporting Functions

Meta IP 4.1 incorporates enhanced auditing and reporting capabilities to help you improve network management and security by providing more timely information. Network managers can now obtain detailed reports on specific IP Addresses[1], network services and lease pool information.

LDAP (Lightweight Directory Access Protocol) data storage

Meta IP 4.1 uses an integrated LDAP data store that is compliant with the LDAP database format and can be accessed by any LDAP engine, including Netscape's *Directory Server*.

SNMP (Simple Network Management Protocol) Support

SNMP support exists within all Meta IP Network Service modules. This allows for integration with SNMP consoles and SNMP-based reporting tools such as *HP OpenView* and *Tivoli NetView*. This lets you access detailed network status information and configure the system to alert you when certain events occur.

PNG (Political, Network, and Geographical) Multiview Java Manager

PNG Multiview lets you manage your organization from the Political, Network, and Geographical perspectives. In addition, cross-platform remote management features allow easy access to the data from any console on any platform within the network.

Multi-platform Support

Meta IP 4.1 now includes multi-platform support. This lets Meta IP integrate and manage DNS services on various UNIX based platforms in addition to Microsoft Windows NT platforms. The *Meta IP/Admin Console* service can manage most of the popular UNIX-based DNS services via the *Meta IP/SMC* (Service Manager Client) service.

1. IP Address reporting requires Meta IP/UAM.

Meta IP 4.1 is available in three packages: Meta IP 4.1 Enterprise, Meta IP 4.1 Standard, and Meta DNS.

TABLE 8-1 Meta IP packages

Meta IP System Feature	Meta IP 4.1 Enterprise	Meta IP 4.1 Standard	Meta DNS
Meta IP/Admin Console Server	✔	✔	✔
Meta IP LDAP	✔	✔	✔
Meta IP/DNS	✔	✔	✔
Meta IP/DHCP	✔	✔	
Meta IP UAT and UAM	✔	✔	
Meta IP/RADIUS	✔		
Meta IP LDAP Replicator	✔		

CHAPTER 9

Before Installing VPN-1/FireWall-1

In This Chapter

Before Installing VPN-1/FireWall-1

Before installing VPN-1/FireWall-1, you must first ensure that a number of pre-conditions exist (for example, that routing and DNS are correctly configured). Perform the procedure below *before* you begin the installation process.

Note – The software in this version is an upgrade to Check Point VPN-1/FireWall-1 Version 4.1. If you have an earlier version of VPN-1/FireWall-1 installed, it will be upgraded. If you do not have an earlier version installed, a full version of VPN-1/FireWall-1 will be installed.

Protecting the VPN-1/FireWall-1 Machine

1. If you are installing VPN-1/FireWall-1 on a Windows NT machine, disable the NetBEUI protocol on that machine.

   If you do not disable NetBEUI, it will be possible to access the NT machine from within the LAN using the NetBEUI protocol. This access will not be intercepted by VPN-1/FireWall-1, since NetBEUI is not an IP protocol.

2 Review the services running on the VPN-1/FireWall-1 machine and remove any service that is not required.

Routing

3 Confirm that routing is correctly configured on the gateway, as follows:

a Send an ICMP packet (PING) from a host inside your (trusted) network through the gateway to your router on the other (untrusted) side.

b TELNET from a host inside your (trusted) network through the gateway to a host on the Internet, to confirm that you can reach that host.

c TELNET from a host on the Internet to a host inside your (trusted) network.

If any of these tests fail, then find out why and solve the problem before continuing.

IP Forwarding

If IP Forwarding is enabled, the gateway will route packets to other IP addresses.

4 On NT, enable the **Enable IP Forwarding** option in the **Protocols➤TCP/IP Protocol Properties➤Routing** tab (accessible from the Network applet in the Control Panel).

On Solaris2 and HP-UX, disable IP Forwarding in the kernel.

When you install VPN-1/FireWall-1 on the Solaris2, HP-UX and Windows NT platforms, you can specify that VPN-1/FireWall-1 controls IP Forwarding, that is, that IP Forwarding will be enabled only when VPN-1/FireWall-1 is running. This ensures that whenever the gateway is forwarding packets, VPN-1/FireWall-1 is protecting the network.

For more information, see “IP Forwarding” on page 22 of *VPN-1/FireWall-1 Reference Guide*.

DNS

5 Confirm that DNS is working properly.

The easiest way to do this is to start a Web browser on a host inside the internal network and try to view Web pages on some well-known sites. If you can’t connect, solve the problem before continuing.

IP Addresses

6 Make a note of the names and IP addresses of all the gateway’s interfaces.

You will need this information later when you define your Security Policy. Also, if you are installing a Single Gateway product, you must know the name of the external interface (the interface connected to the Internet).

NT — Use the `ipconfig /all` command to display information about all the interfaces. Note that NT uses the hyphen (“`-`”) rather than the colon (“`:`”) to separate the fields in the MAC address.

Solaris — Use the `ifconfig -a` command to display information about all the interfaces.

IBM AIX — The `ifconfig` command is available, but it’s best to use `smit` or `smitty` instead.

HP-UX — The `ifconfig` command is available, but it’s best to use `lanscan` instead.

7 Confirm that gateway’s name, as given in the `hosts` (Unix) and `lmhosts` (Windows) files, corresponds to the IP address of the gateway’s *external* interface.

This ensures that when you define the gateway as a network object and click on **Get Address** in the **Workstation Properties** window to retrieve its IP address, the **IP Address** field will specify the gateway’s external interface. If you fail to do so, IKE encryption (among other features) will not work properly.

VPN-1/FireWall-1 Component Configuration

8 Familiarize yourself with the concepts of Management Module, Master and FireWalled host by reading Chapter 1, “Pre-Installation Configuration” of *VPN-1/FireWall-1 Administration Guide*.

To summarize, the Management Module (also known as the Management Server) is the computer on which the Security Policy is maintained. The Master is the computer to which logs and alerts are sent. A FireWalled host is a computer on which a VPN/FireWall Module has been installed and which enforces some part of the security policy.

9 Determine which VPN-1/FireWall-1 component is to be installed on each computer.

You must decide which computer(s) will host your Management Module(s), which will host your Master(s) and which will host your FireWalled host(s).

In addition, if you are installing a Client/Server configuration, then you must decide which computer will host your GUI Client and which will host your Management Module.

Note – If you are installing one of the Single Gateway Products, then the Management Module, Master and FireWalled Module must all be on the same machine, but you can still deploy the Management Module in the Client/Server configuration.

Connectivity

10 Confirm that there is connectivity between all the hosts (including GUI Clients) on which VPN-1/FireWall-1 components will be installed, in other words, that they can all talk to each other.

If you don't verify this before you install VPN-1/FireWall-1, then if you encounter connectivity problems later on, you will not know the source of the problem. You may end up spending a great deal of time in "debugging" VPN-1/FireWall-1 only to discover that the problem is elsewhere.

To verify that there is connectivity between all the machines, try pinging them from each other. If the pings are not successful, then determine what the problem is (using the standard network debugging tools) and fix it. Continue only after you have verified that the machines can all talk to each other.

11 Verify that you have the correct version of the software for your OS and platform for all the VPN-1/FireWall-1 components.

12 If a number of people will be administering the VPN-1/FireWall-1 system, create a Unix group before you install VPN-1/FireWall-1.

13 If VPN-1/FireWall-1 is running, stop it, including the GUI Client.

Installation Procedure for a New Installation

To install VPN-1/FireWall-1 for the first time, proceed as follows:

1 Install and start VPN-1/FireWall-1 on the Management Module computer.

At this point, the Management Module will log only itself. Since there are no rules, then by default everything will be allowed to pass.

You can change this behavior by disabling IP Forwarding. For more information about IP Forwarding, see "IP Forwarding" on page 22 of *VPN-1/FireWall-1 Reference Guide*.

2 Install and start the VPN/FireWall Module on each of the managed (FireWalled) hosts.

Since there are no rules, then by default everything will be allowed to pass.

3 Return to the Management Module and start the VPN-1/FireWall-1 Graphic User Interface.

4 Build a Rule Base and install the Security Policy on the managed (FireWalled) hosts.

VPN-1/FireWall-1 will then begin to enforce your Security Policy.

Upgrading to a New Version of VPN-1/FireWall-1

Upgrading From a Version Before Version 4.0

You can upgrade to Version Check Point 2000 only from Version 3.0 and higher. If you are running a version prior to 3.0, then proceed as follows:

1. Upgrade from that version to Version 3.0.
2. Upgrade from Version 3.0 to Version Check Point 2000.

Backward Compatibility

VPN-1/FireWall-1 Version Check Point 2000 is installed in its own directory and does not overwrite previous versions of VPN-1/FireWall-1. After a successful installation, the `FWDIR` environment variable should be changed to point to Version Check Point 2000. If you uninstall Version Check Point 2000, the previous version is restored (that is, `FWDIR` is set to point to the previous version).

During the installation process, you will be asked whether to maintain backward compatibility with Version 4.0. If you choose to do so, you will be able to manage Version 4.0 and Version 3.0 VPN/FireWall Modules from a Version Check Point 2000 Management Station.

Note the following compatibility issues:

- A Version Check Point 2000 Management Module cannot manage a Version 2.1 (or earlier) VPN/FireWall Module.
- A Version Check Point 2000 Management Module can manage Version 4.0 and Version 3.0 VPN/FireWall Modules (only if Backward Compatibility is selected — see above), but some Version Check Point 2000 features (for example, multiple CAs) cannot be implemented on earlier VPN/FireWall Modules.

When upgrading to Version Check Point 2000 from Version 4.0, you must first upgrade the Management Module (including the GUI) and then upgrade the VPN/FireWall Modules. When you upgrade the Management Module, its version is set to Check Point 2000 if it is also a VPN/FireWall Module. After you upgrade each VPN/FireWall Module to VPN-1/FireWall-1 Version Check Point 2000, you must then manually change its version to Check Point 2000 (in the **General** tab of its **Workstation Properties** window).

VPN-1/FireWall-1 Database

When you upgrade to a new version of VPN-1/FireWall-1, the installation procedure carries the following elements over to the new version:

- VPN-1/FireWall-1 database
- Key database
- Rule Base
- Properties
- Encryption Parameters

VPN-1/FireWall-1 attempts to merge your database with its own new database. For example, you will have the benefit of services defined in the new version and you will retain the services you defined in the previous version. In the case of a name conflict, the old objects (the ones you defined) will be retained.

The files containing these elements are not simply copied. The files are converted to the format of the new version of VPN-1/FireWall-1. This means that you *cannot* copy these files from a previous version to the new version.

Minimizing Downtime During Upgrades

If you would like to upgrade to the new version while minimizing downtime, proceed as follows:

1. Prepare another computer (the "new machine") with the same IP address as the machine on which the previous version of VPN-1/FireWall-1 is installed (the "old machine"), but *do not connect the new machine to the network*.
2. Copy the entire disk from the old machine to the new machine.

   The new machine is now an exact duplicate of the old machine.
3. Upgrade to the new version of VPN-1/FireWall-1 on the new machine.
4. Physically disconnect the old machine from the network and connect the new machine (which now has the new version of VPN-1/FireWall-1 installed) in its place.

   Open connections through the old machine will be dropped.

This procedure is applicable to both VPN/FireWall Modules and Management Modules, because a Management Module cannot receive logs or alerts while it is being upgraded.

After Upgrading

After upgrading, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy on all FireWalls, even if there has been no change in the Security Policy.

CHAPTER 10

Check Point Software Installation

In This Chapter

Overview

This chapter describes the Check Point software installation procedure.

All Check Point software can be installed from the Check Point CD.

Note – The software in this version is an upgrade to Check Point Management Suite 4.1. If you have an earlier versions of the software components installed, they will be upgraded. If you do not have earlier versions installed, a full version will be installed.

Before Installing

Before installing a Check Point software product, you should verify that the hardware and software platforms are appropriate to the software product.

- The pre-requisite requirements for VPN-1/FireWall-1 are given in Chapter 9, “Before Installing VPN-1/FireWall-1”.

- The pre-requisite requirements for other Check Point software products are given in the installation chapters of their User Guides.

Note – Complete documentation for all Check Point software products (including User Guides) is provided on the CD in PDF Adobe Acrobat Portable Document Format (PDF). Acrobat reader software for most supported platforms are also provided on the CD. Alternatively, readers can also be downloaded from Adobe (www.adobe.com). The CD does not contain an Acrobat reader for Solaris2-x86.

In addition, for some products (such as VPN-1/FireWall-1, Floodgate-1, Reporting Tool and others) you must plan which components will be installed on which machines. For additional information, see the respective User Guides of each product.

Starting the Installation

In This Section

Windows

To start the Check Point software installation procedure, proceed as follows:

1. Insert the CD in the drive.
2. The Check Point **Welcome** screen (FIGURE 10-1) is displayed.

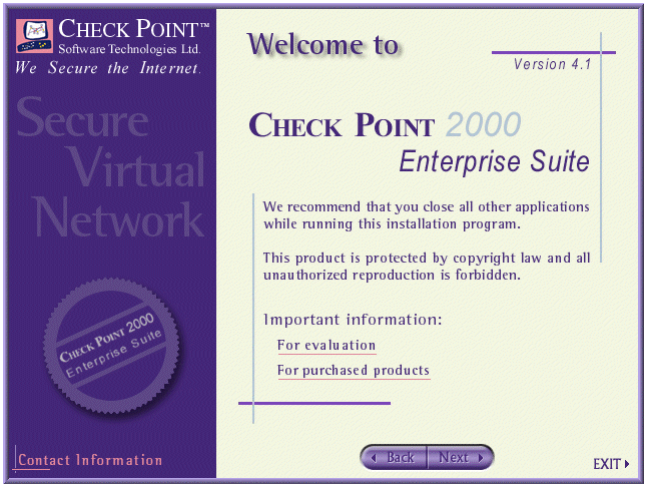


FIGURE 10-1 Check Point welcome screen

Note – At any point in the installation procedure, click on:

- **Next** to navigate to the next screen. *or*
- **Back** to return to the previous screen, *or*
- **Exit** to exit the installation procedure.

3 Click on:

- **Evaluation** to display the **Evaluation** screen (FIGURE 10-2) and proceed to step 4 on page 154, *or*
- **Purchased Products** to display the **Purchased Products** screen (FIGURE 10-3) and proceed to step 5 on page 154, *or*
- **Next** to display the **License Agreement** screen (FIGURE 10-4) and proceed to step 7 on page 155.

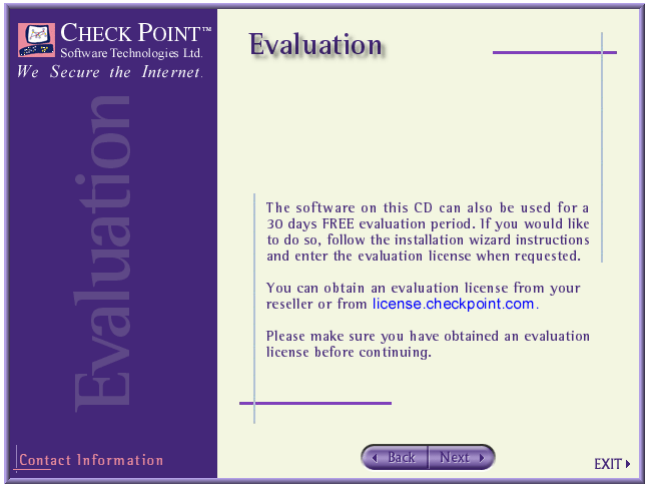


FIGURE 10-2 Evaluation screen

4 Click on **Next** to display the **License Agreement** screen (FIGURE 10-4) and proceed to step 7 on page 155.

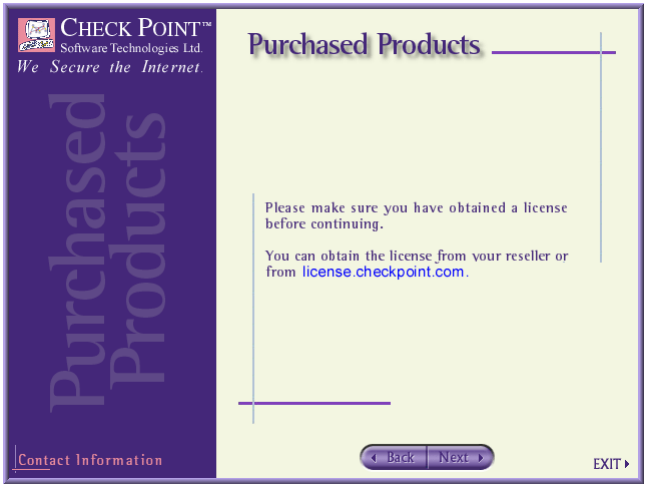


FIGURE 10-3 Purchased screen

5 Click on **Next** to display the **License Agreement** screen (FIGURE 10-4) and proceed to step 7 on page 155.

6 Click on **Next** to display the **License Agreement** screen (FIGURE 10-4).

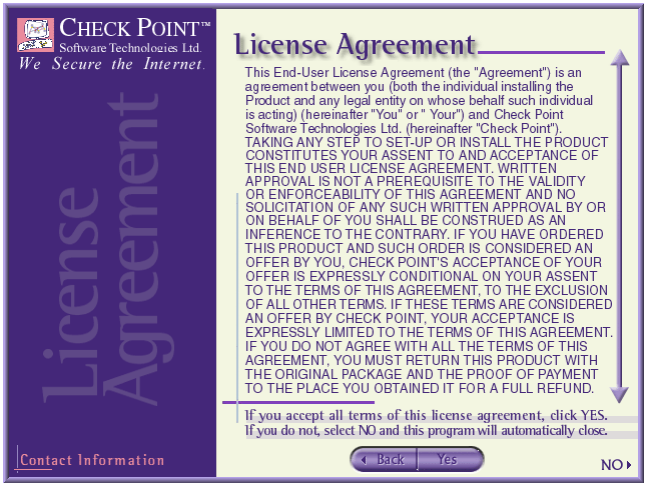


FIGURE 10-4 License Agreement screen

7 You must accept all the terms of the license agreement (by clicking on **Yes**) before continuing.

You can view the text of the license agreement by scrolling through it. If you choose not to accept all these terms, click on **No** and the installation procedure will terminate without installing any Check Point software products.

8 Click on **Yes** to display the **Product Menu** screen (FIGURE 10-6).

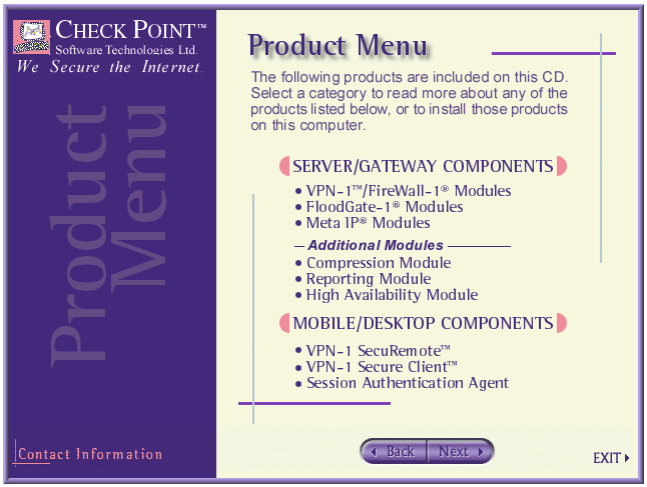


FIGURE 10-5 Product menu screen

9 Select the products you wish to install.

10 Click on **Next** to display the **Setup Type** screen (FIGURE 10-6).

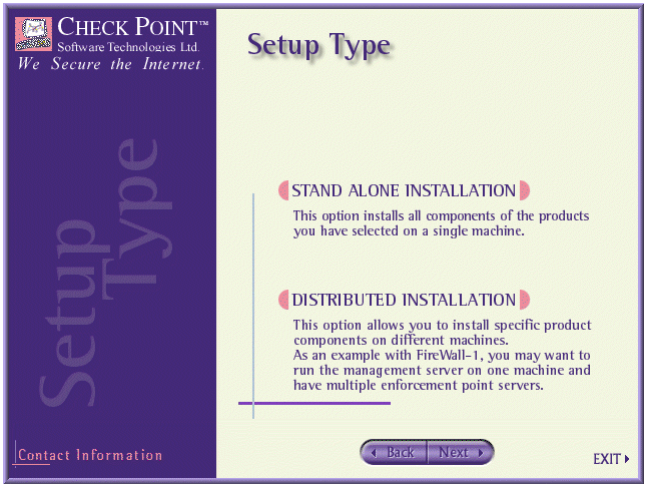


FIGURE 10-6 Setup Type screen

11 Select one of the following and click on **Next**.

Quick Installation — to install all the components of all the selected products on this machine

If you select **Quick Installation**, then proceed to step 14.

Customize Installation — to install the components of all the selected products on different machines

12 The **Distributed Installation** screen is displayed.

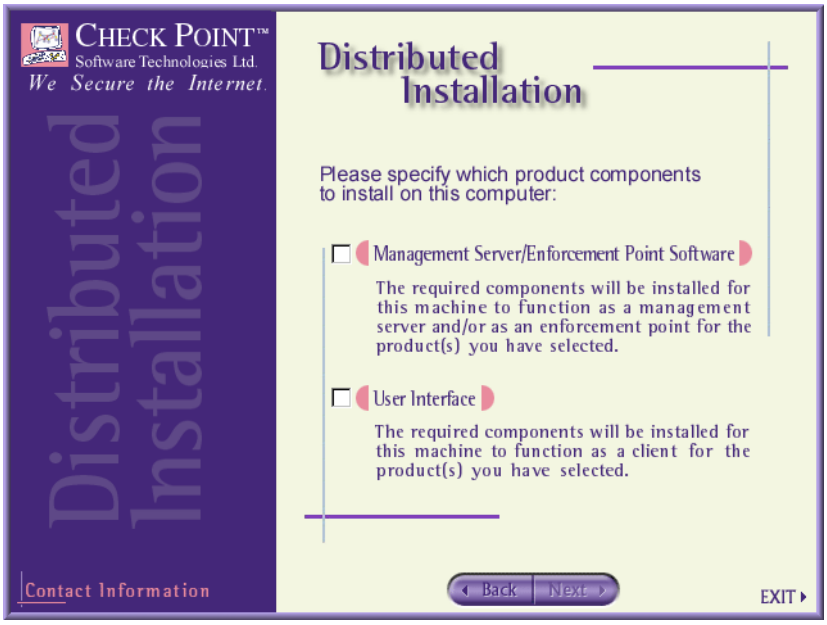


FIGURE 10-7 Distributed Installation screen

13 Select the products you wish to install and click on **Next**.

Management Server/Enforcement Point — to install a Management Server, a VPN/FireWall Module or a SecureServer on this machine

User Interface — to install a User Interface product on this machine.

Note – SecureServer is an internal VPN/FireWall Module that encrypts with SecureClients.

14 At this point, the installation procedure invokes the individual installation procedures of the products you have chosen to install.

- For information about installing VPN-1/FireWall-1, see Chapter 11, “Installing VPN-1/FireWall-1.”

- For information about installing other Check Point products, see the User Guides for those products.

Unix

To start the Check Point software installation procedure, proceed as follows:

1. Login as superuser.
2. Insert the CD in the drive.
3. Mount the CD.
4. Change to the root directory on the CD.
5. Enter the following command to begin the installation process:

```
hostname# InstallU
```

The following screen is displayed:

```
+-------------------------------------------------------------------+
|                           Welcome                                 |
+-------------------------------------------------------------------+
| Welcome to Check Point 2000 Enterprise Suite!                |
| We recommend that you close all other applications while running    |
| this installation program.                                        |
|                                                                   |
| This product is protected by copyright law and all unauthorized re- |
| production is forbidden.                                          |
|                                                                   |
+-------------------------------------------------------------------+
| Important information:                                            |
| 1. For evaluation                                                 |
| 2. For purchased products                                         |
+-------------------------------------------------------------------+
                      +------------------------+
                      |        ACTIONS         |
                      +------------------------|
                      | N. Next                |
                      | E. EXIT                |
                      +------------------------+
 Please select one of 1 or 2 for more information or type N to continue.
```

6 The next screen displays a list of the products to install:

```
+-----------------------------------------------+
|               PRODUCT MENU                    |
+-----------------------------------------------+
| [ ] 1. VPN-1 / FireWall-1 Modules             |
| [ ] 2. FloodGate-1 Modules                    |
| [ ] 3. (Compression Module - not available)   |
| [ ] 4. Meta IP Modules                        |
+-----------------------------------------------+

          +------------------------+
          |       ACTIONS          |
          +------------------------|
          | C. Contact Information |
          | R. Review of products  |
          | H. Help                |
          | N. Next                |
          | E. EXIT                |
          +------------------------+

Please select one or more products, then select N to continue.
```

Select or unselect one or more of the products by entering the numbers (separated by commas or spaces) and then enter `N` to continue to the next screen. For example, if you type:

```
1 4 N
```

then you will select products `1` and `4` (VPN-1/FireWall-1 Modules and MetaIP Modules) and the installation procedure will continue to the next step.

7 Next, you are asked whether to install all the product components on this machine (stand alone configuration) or on different machines (distributed configuration):

```
+-------------------------------------------------------------------------+
|                            SETUP TYPE                                   |
+-------------------------------------------------------------------------+
| [*] 1. STAND ALONE INSTALLATION                                         |
|       This option installs all components of the products               |
|       you have selected on a single machine.                            |
| [ ] 2. DISTRIBUTED INSTALLATION                                         |
|       This option allows you to install individual product components   |
|       on different machines.                                           |
|       As an example with FireWall-1, you may want to run the management |
|       server on one machine and have multiple enforcement point servers.|
+-------------------------------------------------------------------------
                       +------------------------+
                       |        ACTIONS         |
                       +------------------------|
                       | C. Contact Information |
                       | N. Next                |
                       | B. Back                |
                       | E. EXIT                |
                       +------------------------+

Please specify the setup type, then select N to continue.
```

- If you are installing all the components of the selected products on this machine, choose `STAND ALONE INSTALLATION`.
- If you are installing the components of the selected products on different machines, choose `DISTRIBUTED INSTALLATION`.

8 Next, you are asked to confirm your choices.

9 Next, the installation procedure invokes the individual installation procedures of the products you have chosen to install.

- For information about installing VPN-1/FireWall-1, see Chapter 11, “Installing VPN-1/FireWall-1.”
- For information about installing other Check Point products, see the User Guides for those products.

CHAPTER 11

Installing VPN-1/ FireWall-1

In This Chapter

This chapter explains how to install VPN-1/FireWall-1 and obtain and install your license(s). The procedure given here can be used to install VPN-1/FireWall-1 for the first time, to reconfigure an existing installation, or to upgrade to a newer version of VPN-1/FireWall-1.

Before installing VPN-1/FireWall-1, carefully review Chapter 9, “Before Installing VPN-1/FireWall-1”.

For information about installing other Check Point products, see the User Guides for those products.

Note – The software in this version is an upgrade to Check Point VPN-1/FireWall-1 Version 4.1. If you have an earlier version of VPN-1/FireWall-1 installed, it will be upgraded. If you do not have an earlier version installed, a full version of VPN-1/ FireWall-1 will be installed.

Which Components to Install

FIGURE 11-1 depicts a distributed VPN-1/FireWall-1 configuration.

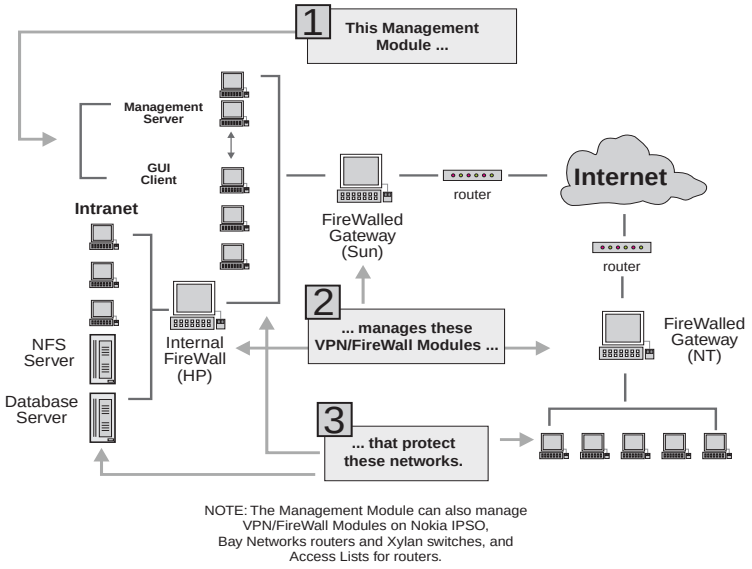


FIGURE 11-1 Distributed VPN-1/FireWall-1 Configuration

TABLE 11-1 lists the VPN-1/FireWall-1 components that must be installed on each computer.

TABLE 11-1 Components to Install on Each Computer

on this computer	install this component	see also
Management Server	Management Server	"Installing on Windows Platforms" on page 163, *or* "Installing on Unix Platforms" on page 184
GUI Client	Windows or X/Motif GUI Client	"Installing on Windows Platforms" on page 163, *or* "Installing the X/Motif GUI Client" on page 198
FireWalled Gateway (Solaris)	VPN/FireWall Module	"Solaris" on page 185
FireWalled Gateway (HP)	Inspection Module	"HP-UX" on page 186
FireWalled Gateway (NT)	VPN/FireWall Module	"IBM AIX" on page 188

For an explanation of the differences between an Inspection Module and a VPN/FireWall Module, see “VPN/FireWall Module” on page 4 of *VPN-1/FireWall-1 Administration Guide*.

Note – For information about installing Inspection Modules on embedded systems, consult the hardware vendor’s documentation. Also, see Chapter 17, “Routers and Embedded Systems” of *VPN-1/FireWall-1 Administration Guide*.

Installing on Windows Platforms

Minimum Installation Requirements

TABLE 11-2 lists the minimum hardware and operating system required for installing the VPN-1/FireWall-1 GUI Client.

TABLE 11-2 Minimum Requirements (GUI Client)

Platforms	Windows 9x, Windows NT 4.0[1] SP4, SP5 and SP6
Disk space	40 Mbytes
Memory	32 Mbytes
Network Interface	All interfaces supported by the operating systems.

1. An X/Motif GUI, functionally equivalent to the Windows GUI, is also available. For information on how to install the X/Motif GUI, see “Installing the X/Motif GUI Client” on page 198.

TABLE 11-3 lists the minimum hardware and operating system required for installing a VPN-1/FireWall-1 Management Module or VPN/FireWall Module.

TABLE 11-3 Minimum Requirements (Management or VPN/FireWall Module)

Operating System	Windows NT 4.0 SP4, SP5 and SP6
Processor	Intel Pentium II 300+ MHz or equivalent
Disk space	40 MBytes
Memory	64MB minimum, 128MB recommended
Network Interface	All interfaces supported by the operating systems.

Installing VPN-1/FireWall-1

Note – For information on installing the X/Motif GUI Client, see "Installing the X/Motif GUI Client" on page 198.

If you are installing VPN-1/FireWall-1 using the Single CD installation procedure (described in Chapter 10, "Check Point Software Installation" of *Getting Started Guide*), then proceed to step 5 on page 165.

Otherwise, insert the VPN-1/FireWall-1 CD-ROM in the drive and proceed as follows:

1. Open the **File** menu and choose **Run**.
2. Run the `SETUP` application in the `Windows` directory.

Installation

3. The **Welcome** window is displayed.

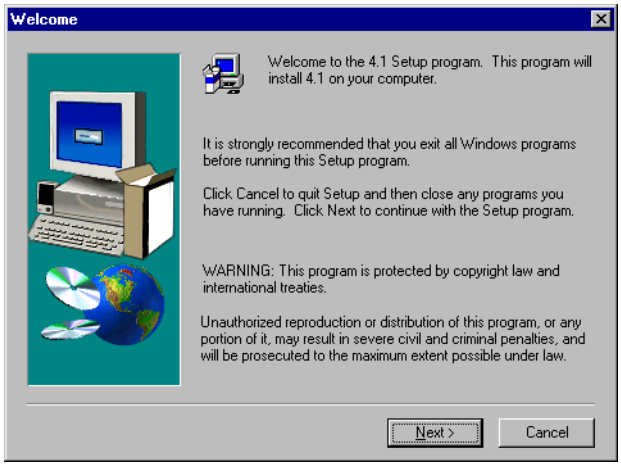


FIGURE 11-2 Welcome window

4. Click on **Next** to proceed to the next window.

5 If this is not the first time you have installed VPN-1/FireWall-1 on this computer, you will be asked whether to upgrade the existing configuration or replace it.

If this is the first time you are installing VPN-1/FireWall-1 on this computer, then proceed to step 8 on page 167.

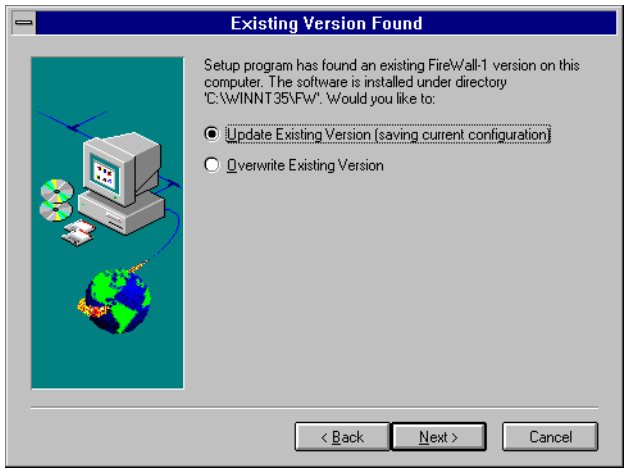


FIGURE 11-3 Existing Version Found window

Note – If a previous version of VPN-1/FireWall-1 is installed on this machine, then a new VPN-1/FireWall-1 version of the current configuration will now be installed. If you wish to install a new version of a different configuration, then you must first uninstall the previous version of VPN-1/FireWall-1.

During the installation, temporary files and directories will be created in the directory specified by the `temp` environment variable.

If VPN-1/FireWall-1 is running on the machine on which you are installing VPN-1/FireWall-1, it will be stopped. After the installation is complete, you will have to restart VPN-1/FireWall-1 and install your Security Policy.

- If you are updating an existing VPN-1/FireWall-1 configuration, your objects and Security Policy will be retained.
- If you overwrite an existing VPN-1/FireWall-1 configuration, your previous objects and Security Policy will be erased.

6 Click on **Next** to proceed to the next window.

7 Next you are asked whether to maintain backward compatibility with previous version of VPN-1/FireWall-1 (Management Stations only).

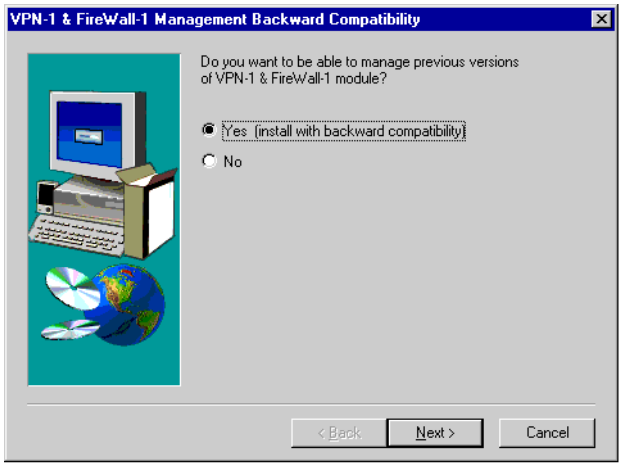


FIGURE 11-4 Backward Compatibility window

If a previous version of VPN-1/FireWall-1 is installed on this Management Station, then you may wish to preserve that version for backup (or backout) purposes. Even if no previous version is installed, then you still have the option of managing previous versions of remote VPN/FireWall Modules.

Note – If this is not the first time you have installed VPN-1/FireWall-1 on this computer, then at this point a new version of the current configuration of VPN-1/FireWall-1 will be installed, and the installation procedure will end.

8 In the **Selecting Setup Type** window, choose the VPN-1/FireWall-1 component you wish to install.

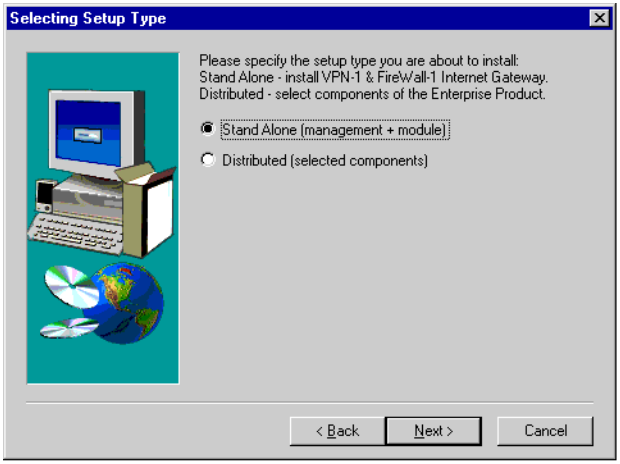


FIGURE 11-5 Selecting Setup Type window

- In a **Stand Alone** configuration, the Management Module and the VPN/FireWall Module are on the same computer.
- In a **Distributed** configuration, the Management Module and the VPN/FireWall Module are on different computers, and you will have to install each Module separately.

Note – The High Availability feature can be installed only in a distributed configuration.

In both cases, you can install the GUI Client on another computer.

9 Click on **Next** to proceed to the next window.

- If you have selected **Stand Alone**, proceed to step 11 on page 168.
- If you have selected **Distributed**, proceed to step 10 on page 168.

10 In the **VPN-1/FireWall-1 Enterprise Product** window, select the Module to install.

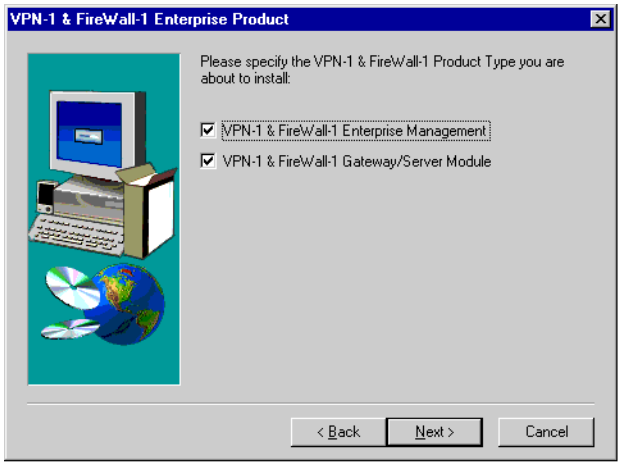


FIGURE 11-6 Enterprise Product window

If you select **VPN-1 & FireWall-1 Enterprise Management**, then proceed to step 12 on page 169.

If you select **VPN-1 & FireWall-1 Gateway/Server Module**, then proceed to the next step (step 11).

11 In the **VPN-1/FireWall-1 Gateway/Server Module** window, select the Module to install.

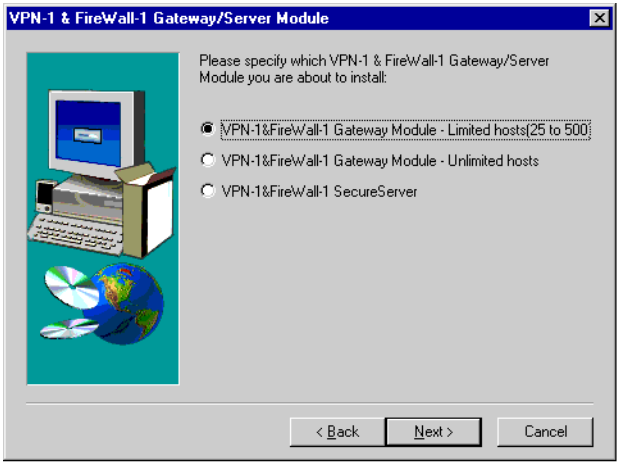


FIGURE 11-7 Gateway/Server Module window

Note – SecureServer is an internal VPN/FireWall Module that encrypts with SecureClients.

12 Specify the destination directory in the **Choose Destination Location** window.

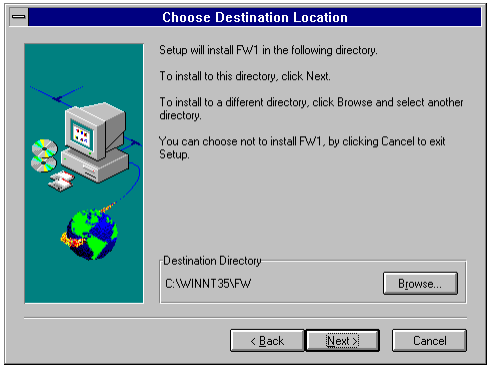


FIGURE 11-8 Destination Directory window

You can choose a different directory from the one suggested in the **Destination Directory** window by clicking on **Browse**.

If you install VPN-1/FireWall-1 in a directory different from the default directory specified in the **Choose Destination Location** window, then you must set the `FWDIR` environment variable to point to the directory in which you installed VPN-1/FireWall-1. Failure to do so will impair the functionality of the `fwinfo` debugging tool.

13 If you install a VPN-1/FireWall-1 Enterprise Product, you will be asked to specify the VPN-1/FireWall-1 Module to install (FIGURE 11-9).

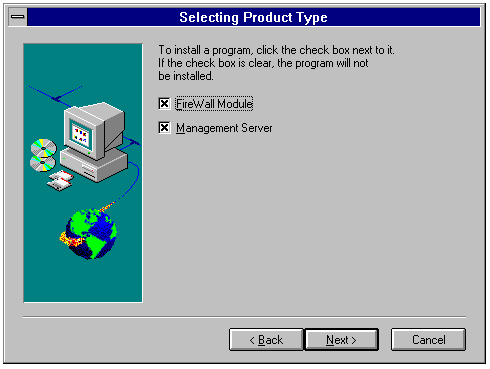


FIGURE 11-9 Selecting Product Type window

- To install the VPN/FireWall Module, choose **VPN/FireWall Module**.
- To install the Management Server, choose **Management Server**.

14 If you install a VPN-1/FireWall-1 VPN/FireWall Module Product, then you will be asked to specify the specific product (FIGURE 11-10).

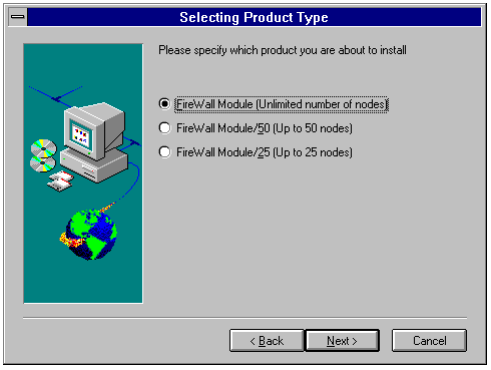


FIGURE 11-10 Selecting a VPN/FireWall Module Product

15 If you install a VPN-1/FireWall-1 Inspection Module Product, then you will be asked to specify the specific product (FIGURE 11-11).

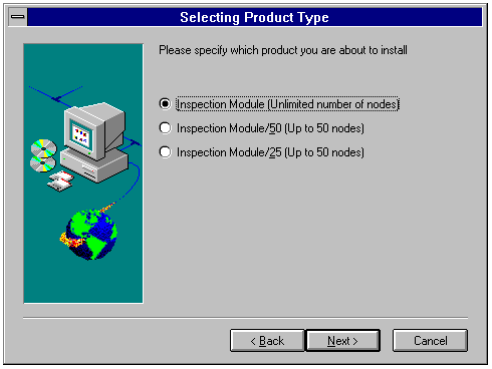


FIGURE 11-11 Selecting an Inspection Module Product

Configuration

The VPN-1/FireWall-1 software is then installed, and the VPN-1/FireWall-1 Configuration Wizard displays the configuration option windows one after the other.

Note – The options displayed depend on the VPN-1/FireWall-1 components you have installed on this host. You will not necessarily see all the windows described here during your configuration process.

Configure each option and then proceed to the next window by clicking on **Next**. If you wish to modify an option, you can return to a previous window by clicking on **Back**.

You can modify the configuration at any time by running the VPN-1/FireWall-1 Configuration application. When you do so, the different configuration options will be displayed as different tabs in the **Configuration** window.

Licenses

16 Add the required licenses for this host.

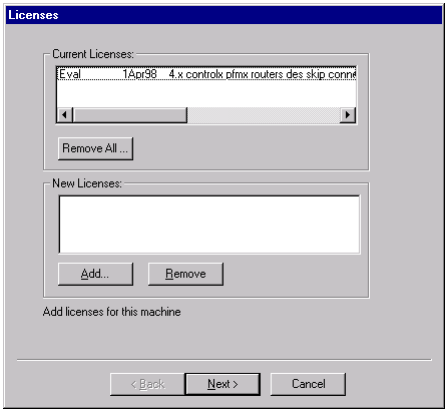


FIGURE 11-12 Licenses window

17 Click on **Add** to add a license.

The **Add License** window (FIGURE 11-13) is displayed.

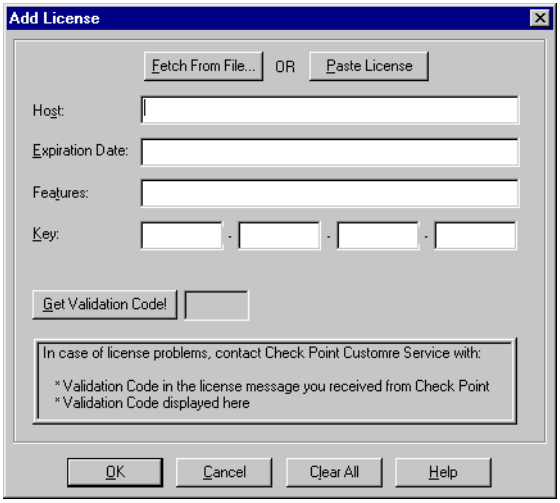


FIGURE 11-13 Add License window

18 Enter the license data and click on **OK.**

- TABLE 11-6 on page 200 lists the elements of the license string.
- You do not need a license to run the Windows GUI Client.
- If you have not yet obtained your license(s), see “Obtaining Licenses” on page 199.

19 Click on **Next** to proceed to the next window.

Administrators

20 Next, you are asked to specify Administrators.

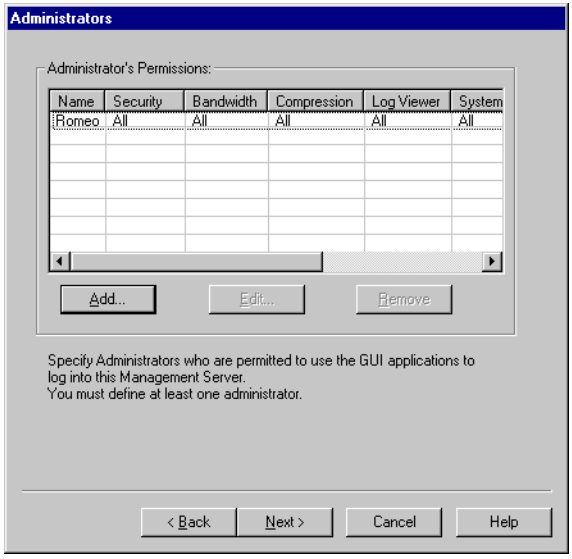


FIGURE 11-14 Administrators window

Specify the administrators who are permitted on the GUI Client side, that is, the administrators who will be allowed to use the GUI Client with the Management Server you have just installed.

You must define at least one administrator, otherwise no one will be able to use the Management Server you have just installed.

21 Click on **Add** to specify an administrator. The **Add Administrator** window is displayed.

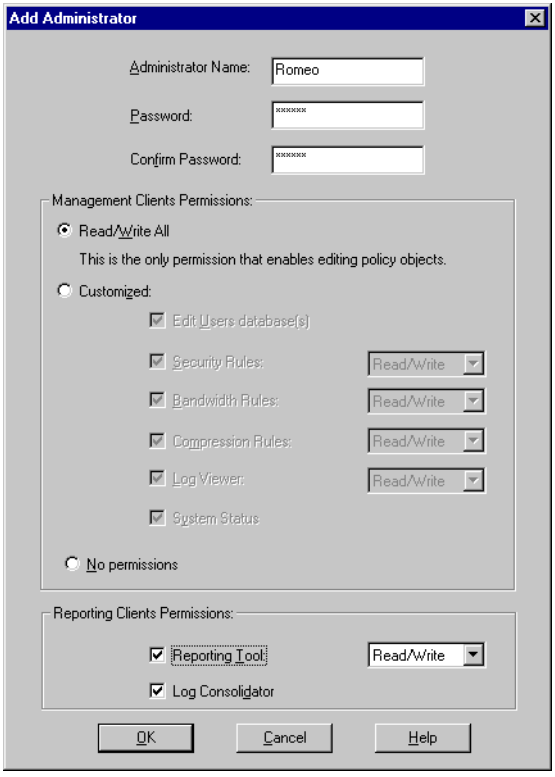


FIGURE 11-15 Add Administrator window

22 Enter the **Administrator Name.**

23 Enter the **Password**.

The password should be no more than 8 characters long and should contain both alphabetic and numeric characters.

You must enter the password twice in order to confirm it.

24 Specify the Administrator's **Permission**.

See "Access Control" on page 62 of *VPN-1/FireWall-1 Administration Guide* for information about administrator permissions.

To modify an administrator's details, click on **Edit** in the **Administrators** window (FIGURE 11-14 on page 173).

25 Click on **Next** to proceed to the next window.

26 Confirm that the machine's IP Address (as specified in the `hosts` file) is correct.

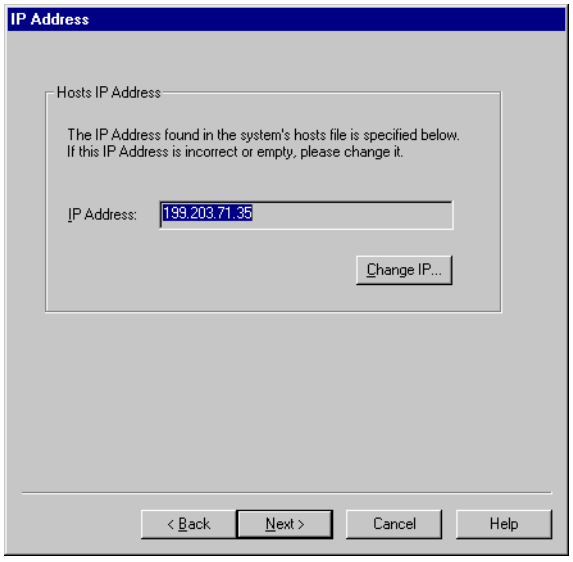


FIGURE 11-16 IP Address window

If **IP Address** is incorrect, click on **Change IP** to change it. The change will be made in the `hosts` file as well.

GUI Clients

27 Specify the GUI Clients, that is, the remote computers from which administrators will be allowed to use the GUI Client with the Management Server you have just installed.

If you do not define at least one GUI Client, you will be able to manage the Management Server you have just installed only from a GUI Client running on the same machine.

Enter the GUI Client's name and click on **Add** to add it to the list of allowed GUI Clients.

To remove a GUI Client from the allowed list, select it and click on **Remove**.

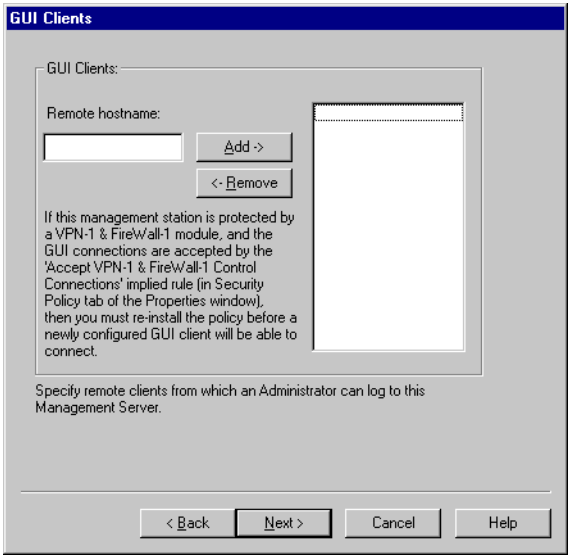


FIGURE 11-17 GUI Clients window

28 Click on **Next** to proceed to the next window.

Masters

If you have installed only a VPN/FireWall Module on this computer, you must specify the Master, that is, the computer to which logs and alerts will be sent, and from which the VPN/FireWall Module will obtain its Security Policy.

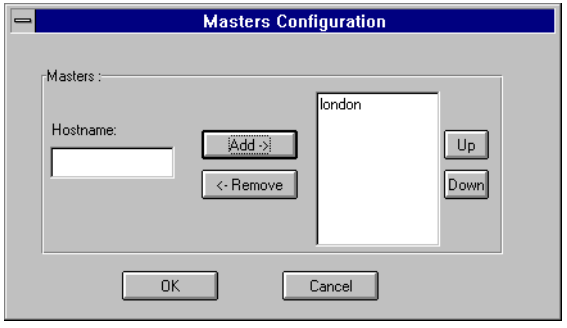


FIGURE 11-18 Masters Configuration window

29 Enter a host name and select **Add** to add the host to the list of Masters.

You may enter any number of Masters. The VPN/FireWall Module will use the first Master in the list with which it can establish contact, so the order of the names in the list is important. For additional information, see “Redirecting Logging to Another Master” on page 420 of *VPN-1/FireWall-1 Administration Guide*.

To move a Master up in the list, select it and then select **Up**. To move a Master down, select it and then select **Down**.

Password

When you add a Master, you must specify an authentication password that the Masters (Management Modules) and VPN/FireWall Modules use when communicating with each other. This is the same password you will use when you issue the `fw putkey` command on the Master. See “fw putkey” on page 12 of *VPN-1/FireWall-1 Reference Guide* for more information about `fw putkey`.

FIGURE 11-19 Add Master window

For additional information, see “Distributed Configurations” on page 69 of *VPN-1/FireWall-1 Administration Guide*.

30 Enter the password (limited to 8 characters in length) twice and then click on **OK**.

31 Click on **Next** to proceed to the next window.

Remote Enforcement Points

If you have installed a Management Module on this computer, you must specify the remote VPN/FireWall Modules for which this Management Module is defined as Master.

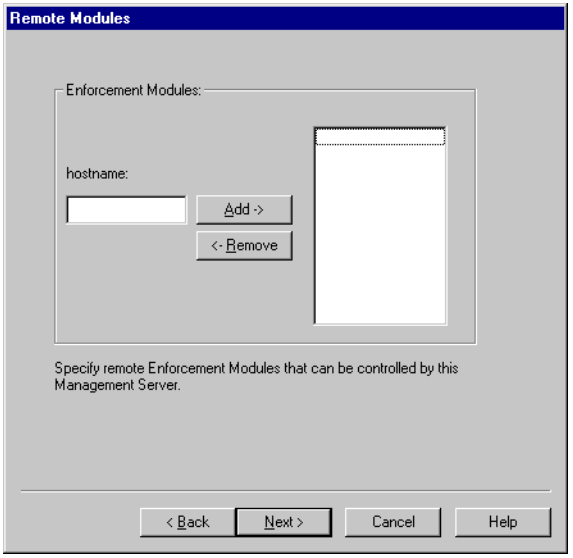


FIGURE 11-20 Remote Modules window

32 Enter a host name and click on **Add** to add the host to the list of remote VPN/FireWall Modules.

Click on **OK** when you have finished entering the list of host names.

33 When you add a remote VPN/FireWall Module, you must specify an authentication password that the Masters (Management Modules) and the remote VPN/FireWall Modules use when communicating with each other. This is the same password you will use when you issue the `fw putkey` command on the remote FireWalled host. See “fw putkey” on page 12 of *VPN-1/FireWall-1 Reference Guide* for more information about `fw putkey`.

For additional information, see “Distributed Configurations” on page 69 of *VPN-1/FireWall-1 Administration Guide*.

34 Click on **Next** to proceed to the next window.

External Interface (for the Single Gateway, VPN/FireWall Module/n and Inspection Module/n products only)

35 Specify the name of the external interface.

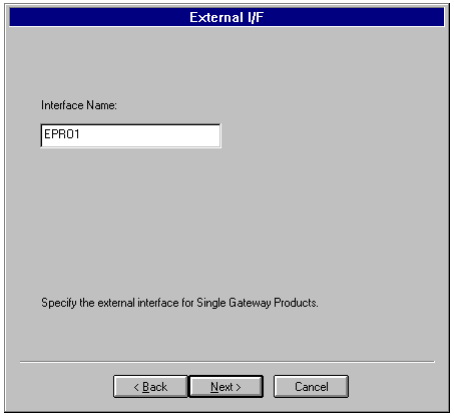


FIGURE 11-21 External IF window

Specify the name, for example "EPRO1," *not* the IP address.

To see a list of the interfaces attached to the computer, type `ipconfig` at the command prompt. The interface name is the one appearing in the first line describing the interface. For example, suppose the first line reads:

```
Ethernet Adapter E159x1
```

The interface name in this case is `E159x1`.

IP Forwarding

36 Specify whether you want VPN-1/FireWall-1 to control IP Forwarding on the gateway.

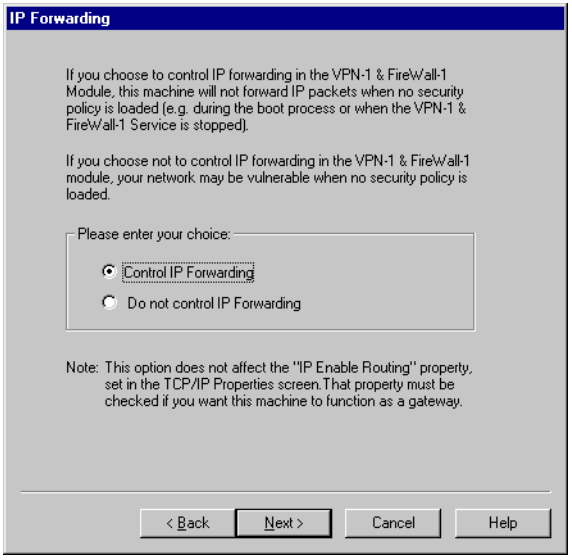


FIGURE 11-22 IP Forwarding window

If you do not allow VPN-1/FireWall-1 to control IP Forwarding, you are taking the risk that your system will be unprotected when no Security Policy is loaded, for example, when the system is being re-booted. For more information about IP Forwarding, see “IP Forwarding” on page 22 of *VPN-1/FireWall-1 Reference Guide*.

37 Click on **Next** to proceed to the next window.

SMTP Security Server

38 Specify the parameters of the SMTP Security Server.

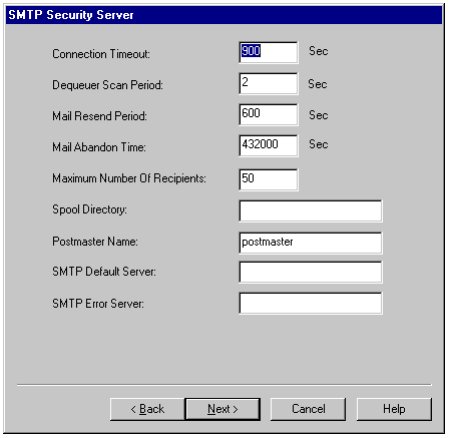


FIGURE 11-23 SMTP Security Server window

These parameters are described in “SMTP Security Server” on page 348 of *VPN-1/FireWall-1 Administration Guide*.

39 Click on **Next** to proceed to the next window.

High Availability

40 If you have installed only a VPN/FireWall Module on this computer, specify in the **High Availability** window (FIGURE 11-24) whether this gateway is a member of a High Availability configuration.

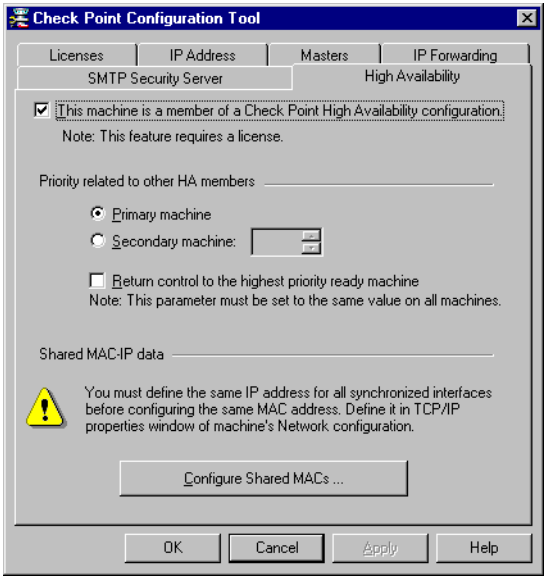


FIGURE 11-24 High Availability window

If you check **This machine is a member of a Check Point High Availability configuration**, then you must configure the machine's IP and MAC addresses accordingly. See "High Availability" on page 3 for information on how to configure a High Availability environment.

Random Key Generation

41 In order to generate seeds for random encryption keys, follow the instructions in the **Key Hit Session** window.

Enter the characters with a delay of a few seconds between them. Do not type the same character twice in succession, and try to vary the delay between the characters.

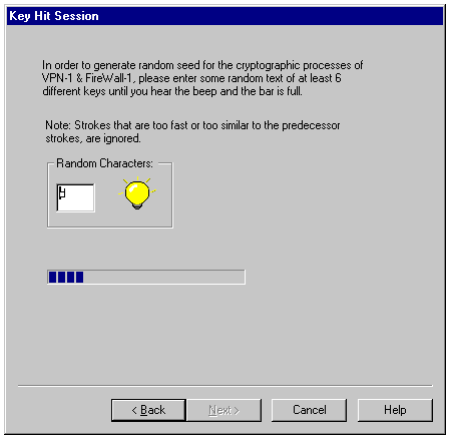


FIGURE 11-25 Key Hit Session window

42 Click on **Finish** to conclude the configuration process.

43 You have now reached the end of the installation procedure.

If you do not configure these options now, you can configure them at a later time by running the VPN-1/FireWall-1 Configuration application. When you do so, the different configuration options will be displayed as individual tabs in the **Configuration** window.

Uninstalling VPN-1/FireWall-1 (NT)

To uninstall VPN-1/FireWall-1, double-click on the **Uninstaller** icon in the VPN-1/FireWall-1 program group.

Stopping VPN-1/FireWall-1 (NT)

There are three ways to stop the VPN-1/FireWall-1 from inspecting communications:

- Uninstall the Security Policy

  This method leaves the Inspection Module in-place, but the Security Policy is empty. VPN-1/FireWall-1 still functions but the net result is that all packets are accepted and no logging occurs.

- Stop Inspection

  To stop inspecting under this method, proceed as follows:

  1 Select **Services** in the **Control Panel** program group.

  2 Select **VPN-1/FireWall-1 daemon**.

  3 Click on **Stop**.

When VPN-1/FireWall-1 is stopped in this way, packets still pass through VPN-1/FireWall-1, but it does nothing.

- Disabling VPN-1/FireWall-1

  This method disables VPN-1/FireWall-1. To stop inspecting under this method, proceed as follows:

  1. Select **Devices** in the **Control Panel** program group.
  2. Select **VPN-1/FireWall-1**.
  3. Click on **Startup**.
  4. Choose **Disabled**.
  5. Reboot the computer.

  After you reboot, VPN-1/FireWall-1 will no longer be in the stack.

Reconfiguring VPN-1/FireWall-1 (NT)

To reconfigure VPN-1/FireWall-1, run the VPN-1/FireWall-1 Configuration application (see "cpconfig" on page 4 of *VPN-1/FireWall-1 Reference Guide)*.

Installing on Unix Platforms

Minimum Installation Requirements

TABLE 11-4 lists the minimum hardware and operating system required for installing a VPN-1/FireWall-1 Management Module or VPN/FireWall Module.

TABLE 11-4 Minimum Requirements (Unix Platforms)

Operating System	■ Solaris 2.6, Solaris Operating Environment 7 (formerly known as Solaris 2.7) — SPARC and x86 ■ HP-UX 10.20, HP-UX 11.0 ■ IBM AIX 4.3.1 and 4.3.2
Disk space	40 Mbytes (software installation only)
Memory	64MB minimum, 128MB recommended
Network Interface	All interfaces supported by the operating systems.

Note – VPN-1/FireWall-1 is supported on the 32-bit versions of these operating systems only.

Installing VPN-1/FireWall-1

You can install VPN-1/FireWall-1 either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

Solaris

Note – See TABLE 11-4 for a list of the OS versions supported by VPN-1/FireWall-1.

You will use the command line utility `pkgadd (1m)` to install VPN-1/FireWall-1.

To install VPN-1/FireWall-1, proceed as follows:

1. Become superuser.
2. Before beginning the installation process, make sure that the environment variable `FW_BOOT_DIR` is not defined by entering the following command:

```
hostname# unset FW_BOOT_DIR
```

3. Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).
4. Start the installation process.

```
hostname# pkgadd -d .
```

   For information about the `pkgadd` command, refer to the Unix documentation.

5. `pkgadd` presents a lists of packages, and asks you to choose one to install.

Specify the package you wish to install by entering either its name or its number (see TABLE 11-5).

TABLE 11-5 VPN-1/FireWall-1 package names

name	component
CPfw1-41	VPN-1/FireWall-1
CPgui-41	VPN-1/FireWall-1 GUI
CPla-41	Load Agent

6 At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /opt/CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

7 Proceed to “Configuring VPN-1/FireWall-1” on page 191.

HP-UX

Note – See TABLE 11-4 for a list of the OS versions supported by VPN-1/FireWall-1.

Special Notes for HP-UX 10

Note – VPN-1/FireWall-1 on HP-UX 10 requires that the “transitional links” option be enabled. You can obtain the necessary OS patches from HP’s support site.

The first time you boot, VPN-1/FireWall-1 will fail, because there is no Security Policy at this point. After you have defined a Security Policy, subsequent re-boots will proceed normally.

HP-UX 10.20

This version of HP-UX already includes the PFS package. Please check the man page for the `pfs_mount` command for details on setting up an `/etc/pfs_fstab` file.

VPN-1/FireWall-1 requires that the aC++ library, `/usr/lib/libCsup.1`, is at level O7 or higher.

The VPN-1/FireWall-1 installation procedure checks that the library is at the required level. If not, the installation will stop and report the problem.

You can obtain the correct library version from your reseller or from the HPUX support site.

HP-UX 11

The X/Motif GUI is not supported in HP-UX 11.

Installation

Note – If you encounter a problem with the depth of the CD-ROM directories, use the files in `hpux/TarFiles`.

In HP-UX, VPN-1/FireWall-1 is installed using the `swinstall` application.

1. Insert the VPN-1/FireWall-1 CD-ROM in the drive.
2. Copy the installation files to the `/tmp` directory.
3. If the `/tmp` directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

   For information about the `swreg` command, refer to the HP-UX documentation.

4. Type the following command to install VPN-1/FireWall-1:

```
hostname# swinstall &
```

5. The **SD Install - Software Selection** window is displayed, and then the **Specify Source** window is displayed on top of it.
6. Click on **Source Depot Path**.
7. In the **Depot Path** window, select the CD-ROM.
8. Click on **OK** to close the **Depot Path** window.
9. Click on **OK** to close the **Specify Source** window.
10. In the **SD Install - Software Selection** window, select **VPN-1/FireWall-1**.

    If you double-click on **VPN-1/FireWall-1**, you will be able to select individual VPN-1/FireWall-1 components to install (see TABLE 11-5 on page 186).

11. From the **Actions** menu, select **Install (analysis)**.

12 When the analysis phase completes, click on **OK**.

13 When the installation phase completes, click on **Done**.

Note – VPN-1/FireWall-1 for HP-UX is always installed in the `/CPfw1-41` directory, so you cannot choose an arbitrary `$FWDIR`.

14 From the **File** menu, select **Exit**.

15 Read "Special Notes for HP-UX 10" on page 186 before proceeding to the next step.

16 At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

17 Proceed to "Configuring VPN-1/FireWall-1" on page 191.

IBM AIX

Note – See TABLE 11-4 for a list of the OS versions supported by VPN-1/FireWall-1.

Special Notes for IBM AIX

Please note the following issues:

1 By default, AIX does not enable IP Forwarding.

Warning – If you enable IP Forwarding while VPN-1/FireWall-1 is not running, you will be exposing your network. Make sure that it is not turned on in one of the `.rc` scripts during boot. Turn it on (with the `no -o ipforwarding=1` command) in the `fwstart` script after VPN-1/FireWall-1 starts enforcing a Security Policy, and turn it off (with the `no -o ipforwarding=0` command) in the `fwstop` script just before VPN-1/FireWall-1 stops.

Because of this AIX feature, it is not possible to control IP Forwarding from within VPN-1/FireWall-1, so you will not be asked to configure this feature during the installation process.

See "IP Forwarding" on page 22 of *VPN-1/FireWall-1 Reference Guide* for more information.

2. VPN-1/FireWall-1 Version 4.0 for AIX does not support the Default Security Policy feature, so you will not be asked to configure this feature during the installation process. This is not considered to be a security risk, because of the AIX boot sequence does not expose the computer.

   See “Default Security Policy” on page 305 of*VPN-1/FireWall-1 Administration Guide* for more information.

3. In order for the X/Motif GUI to function properly, the `LANG` environment variable must be defined.

4. SecurID authentication is not available.

5. When installing a VPN-1/FireWall-1 component, verify that there are no other VPN-1/FireWall-1 components running.

6. The FireWall X/Motif GUI uses the Release 5 X/Motif libraries. AIX 4.3 installs Release 6 X/Motif libraries by default, so the user must manually install the Release 5 libraries in order to use the VPN-1/FireWall-1 X/Motif GUI.

Installation

In IBM AIX, VPN-1/FireWall-1 is installed using the `smit` application.

If you have a version of VPN-1/FireWall-1 already installed and you want to overwrite it, you will not be able to do this using `smit`’s overwrite option. Instead, uninstall VPN-1/FireWall-1 and then install it.

It is recommended that you run `fwstop` before performing an upgrade or uninstalling VPN-1/FireWall-1.

1. Become superuser.

2. Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).

3. Enter the following command to install VPN-1/FireWall-1:

```
hostname# smit &
```

4. Click on **Software Installation and Maintenance**.

5. Click on **Install and Update Software**.

6. Click on **Install Software Products at Latest Level**.

7. Click on **New Software Products at Latest Level**.

8. In the **New Software Products at Latest Level** window, enter the input device or the name of the directory where the VPN-1/FireWall-1 installation files are located.

If you are installing from a CD-ROM, click on **List** and select the CD device in the dialog box.

Note – VPN-1/FireWall-1 for AIX is always installed in the `/usr/lpp/CPfw1-41` directory, so you cannot choose an arbitrary `$FWDIR`.

9 A dialog box is displayed in which you are asked to review the installation parameters and confirm them.

10 In **SOFTWARE to install**, click on **List**.

11 Select **VPN-1/FireWall-1**.

12 Click on **OK** to start the installation process.

13 When the installation completes, exit `smit`.

14 At the command prompt, enter the following commands.

```
hostname# setenv FWDIR /usr/lpp/CPfw1-41
hostname# set path=($FWDIR/bin $path)
```

15 Proceed to “Configuring VPN-1/FireWall-1” on page 191.

Configuring VPN-1/FireWall-1

The configuration process (the `cpconfig` application) starts automatically when you install VPN-1/FireWall-1.

Upgrade

If `cpconfig` detects a previous VPN-1/FireWall-1 installation, `cpconfig` displays the following screen (FIGURE 11-26) and you can configure whichever options you wish to, in any sequence.

```
Welcome to VPN-1/FireWall-1 Configuration Program.
==========================================
This program will let you re-configure your VPN-1/FireWall-1
configuration.

Configuration Options:
----------------------
(1)  Licenses
(2)  Administrators
(3)  GUI clients
(4)  Remote Modules
(5)  Security Servers
(6)  SMTP Server
(7)  SNMP Extension
(8)  Groups
(9)  IP Forwarding
(10) Default Filter
(11) Random Pool
(12) CA Keys
(13) Secured Interfaces
(14) High Availability MAC Addresses
(15) High Availability



(16) Exit

Enter your choice (1-16) :
Thank You...
```

FIGURE 11-26 cpconfig reconfiguration options

When you have finished, select the **Exit** option. For information about the configuration options, see “cpconfig” on page 4 of *VPN-1/FireWall-1 Reference Guide*.

The rest of this section describes the configuration process for a new installation of VPN-1/FireWall-1.

New Installation

Note – The questions you will be asked in the configuration process sometimes depend on your answers to earlier questions, so you may not be asked to answer all the questions listed here.

1. If `cpconfig` does not detect a previous VPN-1/FireWall-1 installation, `cpconfig` asks you to confirm your consent to the license agreement.

2. `cpconfig` then configures VPN-1/FireWall-1 by asking you a series of questions. First, the following screen is displayed:

```
Choosing Installation
---------------------
(1) VPN-1 & FireWall-1 Stand Alone Installation
(2) VPN-1 & FireWall-1 Distributed Installation

Option (1) will install VPN-1 & FireWall-1
Internet GateWay (Management Server and Enforcement Module)
on a single machine.
Option (2) will allow you to install specific
components of the VPN-1 & FireWall-1 Enterprise Products
on different machines.

Enter your selection (1-2/a):
```

- To install all the VPN-1/FireWall-1 components on this machine, choose `(1)` (`VPN-1 & FireWall-1 Stand Alone Installation`) and proceed to step 4 on page 193.

  In this case, the Management Server and Enforcement (VPN/FireWall) Module will both be installed on this machine, and the Management Module will be unable to manage Enforcement Modules on other machines. You can install the GUI Client on any machine.

- To install the VPN-1/FireWall-1 components on different machines, choose `(2) VPN-1 & FireWall-1 Distributed Installation` and proceed to the next step.

3 If you choose `(2) VPN-1 & FireWall-1 Distributed Installation`, the following screen is displayed:

```
Which of the following VPN-1 & FireWall-1 options do you wish to
install/configure ?
-------------------------------------------------------------------
(1) VPN-1 & FireWall-1 Enterprise Management
(2) VPN-1 & FireWall-1 Gateway/Server Module
(3) VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module
```

- If you choose `VPN-1 & FireWall-1 Enterprise Management`, then proceed to step 6 on page 193.
- If you choose `VPN-1 & FireWall-1 Gateway/Server Module` or `VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module`, then proceed to the next step (step 4).

4 Choose one of the following:

```
Which Module would you like to install ?
----------------------------------------
(1) VPN-1 & FireWall-1 Gateway Module - Limited hosts (25, 50, 100.,
       250 or 500)
(2) VPN-1 & FireWall-1 Gateway Module - Unlimited hosts
(3) VPN-1 & FireWall-1 SecureServer
```

Note – VPN-1/FireWall-1 SecureServer is an internal VPN/FireWall Module that encrypts with VPN-1 SecureClients.

5 If you choose the first option (`VPN-1 & FireWall-1 Gateway Module - Limited hosts`), you will be asked to specify the external interface (the one connected to the Internet), for example, le0.

6 Next, you are asked whether you wish to start VPN-1/FireWall-1 automatically at boot time.

```
Start VPN-1/FireWall-1 automatically from /etc/rc y/n [y]?
```

Type `y` if you want VPN-1/FireWall-1 to start automatically each time the system boots.

7 Next, you are asked to enter group names.

```
Please specify group name [<RET> for no group permissions]:
```

If you have created a VPN-1/FireWall-1 group, enter its name now. If you have not yet set up a VPN-1/FireWall-1 group, press <Return>. The script prompts for confirmation of your group name.

8 Next, you are asked if you have a VPN-1/FireWall-1 license:

If you have not yet obtained your license(s), see "Obtaining Licenses" on page 199.

If you have already obtained your license, enter y, and enter your license when prompted. If you have not yet obtained your license, then enter n. You may complete the installation process and add your license later.

9 Next, you are asked to enter a list of administrators, that is, people who are allowed to use the GUI clients (computers) to administer the VPN-1/FireWall-1 Security Policy on the Management Server.

```
You may now define administrators that are allowed to use the GUI
clients (i.e., the Windows GUI).
At any later time you can modify administrators and passwords by
running fwm -a
You must define at least one administrator in order to use the GUI
clients.
```

If you choose not to define any administrators now, you will not be able to use the VPN-1/FireWall-1 Client/Server configuration until you do so, using the `fwm` program (see "fwm" on page 27 of *VPN-1/FireWall-1 Reference Guide* for more information).

10 Next, you are asked to enter a list of trusted GUI clients.

```
You should now enter a list of trusted hosts that may be used
as GUI clients (i.e., on which you may run the Windows GUI).
At any later time you can add hosts to this list by modifying
$FWDIR/conf/gui-clients.
```

At least one GUI client must be defined if you wish to use the VPN-1/FireWall-1 Client/Server configuration. If you do not define one now, you can do so later by modifying the file `$FWDIR/conf/gui-clients`. This file consists of IP addresses or resolvable names, one per line.

11 If you have installed a Management Module on this computer, you must specify the remote VPN/FireWall Modules for which this Management Module is defined as Master.

Enter the IP addresses or resolvable names of all hosts this Management Module controls.

Enter a single IP address or resolvable name on each line then terminate the list with `Ctrl-D` or your EOF character.

A host name is the name returned by the `hostname` command.

12 The screen will show your entries and ask you for confirmation.

```
Is this correct y/n [y] ?
```

If the list of hosts on the screen is correct, press `<Return>`. If it is incorrect, type `n`, and make the necessary corrections.

13 Next, you are asked to configure the SMTP Security Server.

14 Next, you are asked to configure the SNMP daemon.

15 If you have installed only a Management Server (Module) on this computer, you must specify the name(s) of the machine(s) that will be this machine's Master(s).

Enter the IP addresses or resolvable names of all hosts allowed to perform control operations on this host.

Enter a single IP address or resolvable name on each line then terminate the list with `Ctrl-D` or your EOF character.

A host name is the name returned by the `hostname` command.

16 The screen will show your entries and ask you for confirmation.

```
Is this correct y/n [y] ?
```

If the list of hosts on the screen is correct, press `<Return>`. If it is incorrect, type `n`, and make the necessary corrections.

17 If you have installed only a VPN/FireWall Module on this computer, specify whether this gateway is a member of a High Availability configuration.

```
Would you like to install the High Availability product (y/n) [n] ? y
```

If you answer yes, you must configure the machine's IP and MAC addresses accordingly. See "High Availability" on page 3 for information on how to configure a High Availability environment.

18 Next, you are asked to type in random characters that will be used to generate a Certificate Authority key.

Enter the characters with a delay of a few seconds between them. Do not type the same character twice, and try to vary the delay between the characters.

19 If you are installing a Management Module or a VPN/FireWall Module, you are asked to specify an authentication password to be used by the Management and VPN/FireWall Modules to validate communication between them.

Enter the same authentication password for all hosts and gateways managed by the same Management Module. For additional information, see "Distributed Configurations" on page 69 of *VPN-1/FireWall-1 Administration Guide*.

20 **(All Platforms Except IBM AIX)** Next, you are asked whether to disable IP Forwarding in the kernel, and allow VPN-1/FireWall-1 to control IP Forwarding.

For more information about IP Forwarding, see "IP Forwarding" on page 22 of *VPN-1/FireWall-1 Reference Guide*.

21 **(All Platforms Except IBM AIX)** Next, you are asked whether to install a default Security Policy at boot time, to protect your network until VPN-1/FireWall-1 starts.

The default Security Policy provides basic protection until the VPN-1/FireWall-1 Security Policy is loaded. For information about the default Security Policy, see "IP Forwarding" on page 22 of *VPN-1/FireWall-1 Reference Guide*.

22 If necessary, remove the files that were extracted to your `/tmp` directory, for example:

```
hostname# cd /tmp
hostname# rm fwtar.gz*
hostname# rm fwinstall
hostname# rm gunzip
```

23 You have now reached the end of the installation procedure.

If you have your license(s), but have not yet installed them, see "Installing Licenses" on page 199. If you have not yet obtained your license(s), see "Obtaining Licenses" on page 199.

Special Notes

Special Note for Management Servers

If you have installed the VPN-1/FireWall-1 Management Server, you must first define administrators (people who are allowed to manage the VPN-1/FireWall-1 Management Server using a Windows GUI Client) and GUI Clients (computers from which administrators will be allowed to manage the VPN-1/FireWall-1 Management Server).

Administrators

To define administrators, run the program `fwm` on the VPN-1/FireWall-1 Management Server, as follows:

To add an administrator, enter the following command at the system prompt:

```
hostname# fwm -a
```

You will be prompted to type the user's name, password and permissions. You will be asked to confirm the password by typing it a second time.

To delete an administrator, enter the following command at the system prompt:

```
hostname# fwm -r
```

You will prompted to type the user's name.

For additional information, see "fwm" on page 27 of *VPN-1/FireWall-1 Reference Guide*.

GUI Clients

To define GUI Clients, you must edit the file `$FWDIR/conf/gui-clients`. The file consists of IP addresses or resolvable names, one per line.

Upgrading

When upgrading, the currently defined services are merged with the services defined in the new version of VPN-1/FireWall-1. In case of conflict, the previous definition takes precedence over the one in the new version.

Installation Problems

1. If you receive a message that a file is missing, you are in the wrong directory.
2. You can safely ignore any tty warnings during the installation procedure.

Reconfiguring VPN-1/FireWall-1

You can modify your VPN-1/FireWall-1 configuration by running `cpconfig`. See “cpconfig” on page 4 of *VPN-1/FireWall-1 Reference Guide* for more information.

Uninstalling VPN-1/FireWall-1 (Unix)

Note – If you have a previous Version 4.0 installation, then uninstalling Version 4.1 will reactivate Version 4.0.

HP-UX and IBM AIX

To uninstall VPN-1/FireWall-1 on HP-UX and IBM AIX, use the same administration application you used to install it.

Solaris2

To uninstall VPN-1/FireWall-1 on Solaris2, use `pkgrm`.

When you uninstall VPN-1/FireWall-1, a message is displayed instructing you to reboot the computer using the `shutdown` command. Make sure you use the `shutdown` command in `/usr/sbin`, which recognizes the `-y` parameter.

Installing the X/Motif GUI Client

The VPN-1/FireWall-1 X/Motif GUI Client enables you to run the VPN-1/FireWall-1 GUI Client under X/Motif, which provides a Windows “look and feel” on a Unix machine.

Note – For instructions on installing the Windows GUI Client, see “Installing on Windows Platforms” on page 163.

The X/Motif GUI Client can be installed as part of the VPN-1/FireWall-1 installation process. See “Installing on Unix Platforms” on page 184 for more information.

The FireWall X/Motif GUI Client uses the Release 5 X/Motif libraries.

After Installing VPN-1/FireWall-1

Reinstalling the Security Policy

After upgrading to a new version, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy on all FireWalls, even if there has been no change in the Security Policy.

Obtaining Licenses

All VPN-1/FireWall-1 products require a license to enable their operation. Licenses are installed on the Management Station and FireWall and Inspection Modules. Licenses are not required on GUI Clients. For an embedded system, the license is installed on its Management Station.

Evaluation Licenses

If you have a Certificate Key for your copy of VPN-1/FireWall-1, then you can obtain an evaluation license by following the procedure for obtaining a permanent license.

If you do not have a Certificate Key for your copy of VPN-1/FireWall-1, then you can obtain an evaluation license from your VPN-1/FireWall-1 reseller.

Permanent Licenses

To obtain a permanent license, proceed as follows:

1. Obtain a Certificate Key from your VPN-1/FireWall-1 reseller.
2. Contact http://license.checkpoint.com/ to obtain a permanent license.

   When you install a permanent license, it is best to remove any expired evaluation licenses. See “fw dbload” on page 13 of *Check Point Reference Guide* for information on how to remove old licenses.

X/Motif Licenses

You need a special license to use the X/Motif GUI, which you can obtain from your VPN-1/FireWall-1 reseller. The X/Motif license must be installed on the Management Server.

Installing Licenses

You must have a license to use VPN-1/FireWall-1 products. If you did not enter your license(s) during installation, use the following procedures for installing your license(s) now, according to the platform(s) on which you installed each product.

For embedded systems, the license must be installed on the Management Server.

Windows Platforms

You can install your license when you install the VPN-1/FireWall-1 software, or at a later time by running the VPN-1/FireWall-1 Configuration application. This is the same application that you ran when you installed the Management Server (see “Installing on Windows Platforms” on page 163).

Unix Platforms

1 At a root prompt type the following command:

```
hostname# fw putlic hostid date licensekey features certificatekey
```

- `date`, `features`, and `certificatekey` are case insensitive.
- The variable information (the license string) represents the alphanumeric code you will receive from the License Distribution Center.

TABLE 11-6 fw putlic parameters

Element	Meaning
`hostid`	If the license is an evaluation license, enter `"eval"`. Otherwise, enter a string as follows:

platform	type
Solaris	the response to the `hostid` command (beginning with `0x`)
HP-UX	the response to the `uname -i` command (beginning with `0d`)
AIX	the response to the `uname -l` command (beginning with `0d`), *or* the response to the `uname -m` command (beginning and ending with `00`)
NT	IP address of the external interface (in dot notation); last part cannot be 0 or 255

`date`	The date format is `DDmonYYYY` for evaluation licenses and "never" for permanent licenses.
`licensekey`	This is the License Key string you received from the License Distribution Center, for example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m`
`features`	This is a string listing the features included in the license, for example: `CPSUITE-EVAL-3DES-v41`
`certificatekey`	This is the Certificate Key string, for example: `CK0123456789ab`

2 When you enter your license, you will get a response similar to the following example:

```
        Host            Expiration Features
Eval    199.213.71.172  21Jul1999 CPSUITE-EVAL-3DES-v41 CK0123456789ab
License file updated
```

In this example:

- The license is an evaluation license.
- The license expires on July 21, 1999.
- The features are “CPSUITE-EVAL-3DES-v41”.
- The Certificate Key is “CKO123456789ab”.

3. Confirm that you are using the correct licenses by the following procedure:

   a. Run `fwstop`.

   b. Run `fwstart`.

   c. Print the license using the `fw printlic` command.

   The last part of the response (the part beginning with “CK”) is the Certificate Key.

For information on these commands, see Chapter 1, “Command Line Interface” of *VPN-1/FireWall-1 Reference Guide*.

Enabling Logging for FloodGate-1 and Third Party Products

FloodGate-1 uses the OPSEC Event Logging API (ELA) Proxy Server to write log entries to the common VPN-1/FireWall-1 log database. Third party products, such as RealSecure, also use the ELA Proxy Server. Check your product’s documentation to verify whether the ELA Proxy is used. Start the ELA Proxy if your product requires it.

Windows NT

To start the service, enter the following command:

```
net start elaservice
```

Alternatively, select `elaservice` from the **Services** applet in the Windows **Control Panel** and click on **Start**.

To stop the service, enter the following command:

```
net stop elaservice
```

Alternatively, select `elaservice` from the **Services** applet in the Windows **Control Panel** and click on **Stop**.

Solaris 2.x

To run `ela_proxy`, enter the following command:

```
$FWDIR/bin/ela_proxy
```

The procedure for stopping the `ela_proxy` process is the same as for other Unix processes.

CHAPTER 12

VPN-1/FireWall-1 Tutorial

In This Chapter

Introduction

This chapter presents a detailed step by step guide to installing VPN-1/FireWall-1 and building and deploying a Security Policy. The configuration used is depicted in FIGURE 12-1.

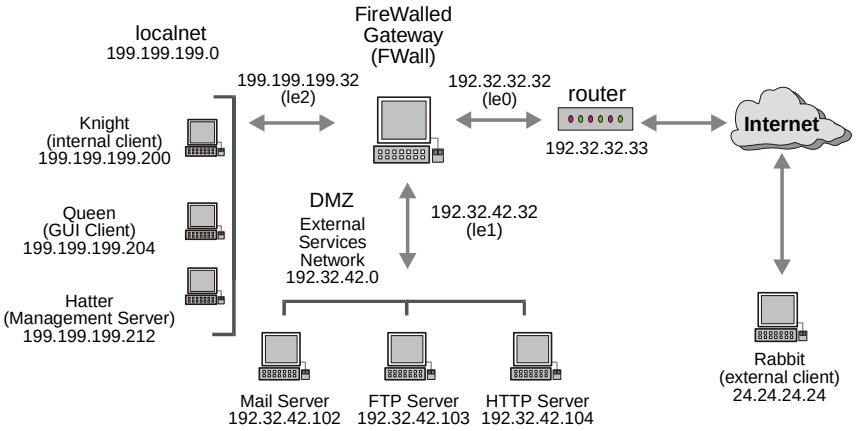


FIGURE 12-1 Network Configuration

The example configuration is relatively simple — though it contains many of the elements found in complex configurations — so if you work through the example, you will become familiar with many of the issues involved in setting up VPN-1/FireWall-1.

Building a Security Policy

To deploy a Security Policy, you must perform the following steps:

1 Install the appropriate VPN-1/FireWall-1 modules on each machine, as needed (see TABLE 12-1).

TABLE 12-1 VPN-1/FireWall-1 Modules to Install on Each Workstation

computer	function	VPN-1/FireWall-1 module
FWall	FireWalled Gateway	FireWall Module
Queen	GUI Client	Management Module - GUI
Hatter	Management Server	Management Module

2 Define the network objects.

The network objects are listed in TABLE 12-2 on page 205.

You don't have to define the individual hosts in localnet, because they will not be explicitly used in the Rule Base.

TABLE 12-2 Network Objects

object name	description	IP address
Hatter	the Management Station	199.199.199.212
FWall	the FireWalled gateway, the workstation that is protecting the network	(3 interfaces) **le0** (to Internet) - 192.32.32.32 **le1** (to DMZ) - 192.32.42.32 **le2** (to localnet) - 199.199.199.32
localnet	the internal network	199.199.199.0
DMZ (External Services Network)	the Demilitarized Zone - where the public servers are located	192.32.42.0
MailServer	provides mail services	192.32.42.102
FTPServer	provides FTP services	192.32.42.103
HTTPServer	provides HTTP (Web) services	192.32.42.104

The system hosts file for FWall is:

```
#
# Internet host table
#
127.0.0.1       localhost
192.32.32.32    FWall               loghost
192.32.42.32    FWall2
199.199.199.32  FWall3
192.32.42.102   mailserver
192.32.42.103   ftpserver
192.32.42.104   httpserver
192.32.32.33    router
```

3 Define the users.

Two users must be defined in this example: Alice and Bob (see "Creating Users" on page 221).

4 Define a Rule Base.

5 Install the Rule Base (Security Policy) on the FireWalled machine.

Before Installing VPN-1/FireWall-1

Before installing VPN-1/FireWall-1, confirm that your network is properly configured, especially in regard to routing. You must ensure that each of the internal networks (localnet and DMZ) and the gateway (FWall) can all “see” each other, in other words, that the routing tables are correctly defined.

You can do this by logging on to each of the hosts and pinging other hosts in the internal networks and on the Internet. It is essential that you verify that your routing is correctly configured before you install VPN-1/FireWall-1, otherwise you will be unable to isolate network problems and determine their cause.

Installation

VPN-1/FireWall-1 is configured in the Client/Server implementation, as shown in FIGURE 12-1 on page 204. To install VPN-1/FireWall-1, proceed as follows:

1. Install the FireWall Module on FWall.

   Define Hatter as FWall’s Master.

2. Install the GUI Client on Queen.

3. Install the Management Server on Hatter.

   Define FWall as Hatter’s remote FireWall Module.

4. On Hatter, define Queen as a GUI Client.

   For information on how to define GUI Clients to the Management Server, see “Access Control” on page 62 of *VPN-1/FireWall-1 Administration Guide*.

5. On Hatter, define the administrators who will be allowed to use the GUI Client to manage the Security Policy.

   For information on how to define administrators to the Management Server, see “Access Control” on page 62 of *VPN-1/FireWall-1 Administration Guide*.

Security Policy

The Security Policy for this configuration is as follows:

- External users can access only the DMZ network (a network that provides external services such as Mail, FTP and HTTP).
- Internal users can access the entire network, including localnet, DMZ and the Internet.
- Users Bob and Alice can TELNET to the FTP Server on the DMZ for administrative purposes, no matter from which IP addresses they connect.

Starting the GUI Client

Start the VPN-1/FireWall-1 Graphical User Interface by double-clicking on the VPN-1/FireWall-1 icon. The **Check Point Policy Editor Login** window (FIGURE 12-2) is then displayed.

FIGURE 12-2 Policy Editor Login window

Enter your user name, password and the name of the server to which to connect. Then click on **OK**.

After a brief delay, during which the VPN-1/FireWall-1 database is loaded, the VPN-1/FireWall-1 **Policy Editor** window (FIGURE 12-3) is displayed, showing an empty Rule Base.

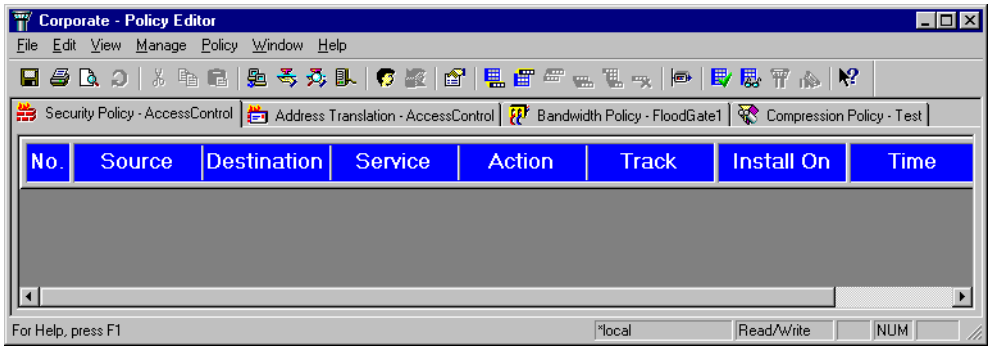


FIGURE 12-3 Policy Editor window with empty Rule Base

The name of the Security Policy currently displayed is shown in the **Policy Editor** window's title bar.

Defining the Network Objects

Network Objects

The network objects in the example configuration are listed in TABLE 12-2 on page 205.

1 Open the **Network Objects** window, by:

- selecting  from the toolbar, *or*
- choosing **Network Objects** from the **Manage** menu

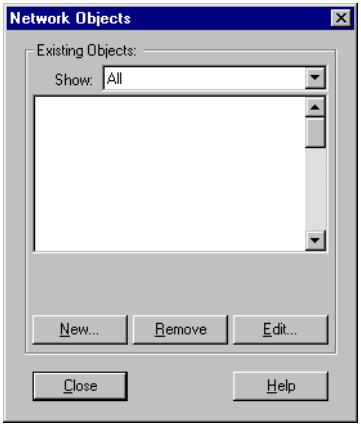


FIGURE 12-4 Network Objects window

Workstation

2 Create a new workstation.

To create a new workstation, click on **New**. A menu appears (FIGURE 12-5 on page 208) listing the types of objects you can create.

FIGURE 12-5 Network Objects menu

3 Choose **Workstation** from the menu.

The **General** tab of the **Workstation Properties** window is displayed.

4 Fill in the data in Hatter's **General** tab as shown in TABLE 12-4.

TABLE 12-3 Hatter — Workstation Properties window — General tab

Field	Value	Explanation
Name	Hatter	the name by which the object is known on the network - the response to the `hostname` command
IP Address	192.199.199.212	the interface associated with the host name in the DNS — get this by clicking on **Get Address**
Comment	Management Station	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	**Internal**	**External** only for network objects that are part of an external network and are not managed by this Management Module
Type	**Host**	
Management Station	Checked	

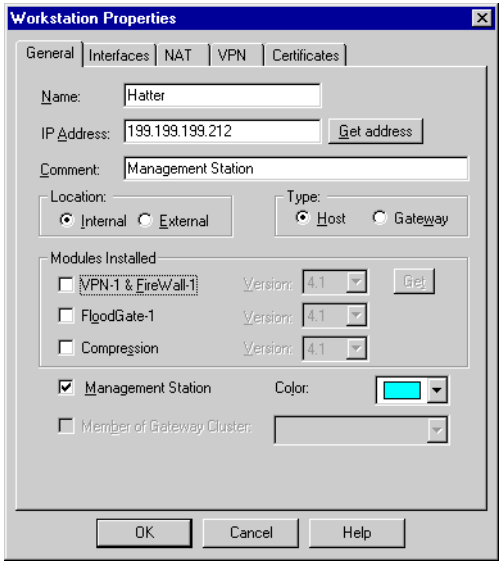


FIGURE 12-6 Hatter's Workstation Properties window - General tab

5 Click on **OK** to close Hatter's **Workstation Properties** window.

6 Create another workstation (FWall) by clicking on **New** in the **Network Objects** window (FIGURE 12-4 on page 208).

7 Fill in the data in FWall's **General** tab as shown in TABLE 12-4.

TABLE 12-4 FWall — FWall's Workstation Properties window — General tab

Field	Value	Explanation
Name	FWall	the name by which the object is known on the network - the response to the `hostname` command
IP Address	192.32.32.32	the interface associated with the host name in the DNS — get this by clicking on **Get Address** For gateways, this should always be the IP address of the external interface.
Comment	FireWalled gateway to Internet	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	**Internal**	**External** only for network objects that are part of an external network and are not managed by this Management Module
Type	**Gateway**	
Modules Installed	Check **VPN-1 & FireWall-1**	so that the Security Policy will be installed on FWall
Version	Check Point 2000	the VPN/FireWall Module version installed on this workstation

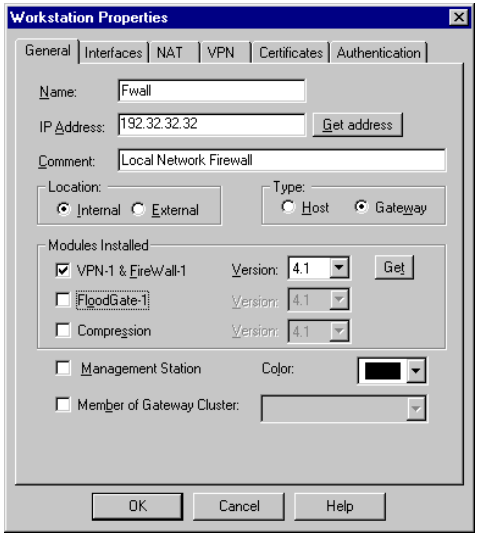


FIGURE 12-7 Workstation Properties window - General tab

Add Interfaces

8 Click on the **Interfaces** tab.

The **Workstation Properties** window - **Interfaces** tab (FIGURE 12-8) is displayed.

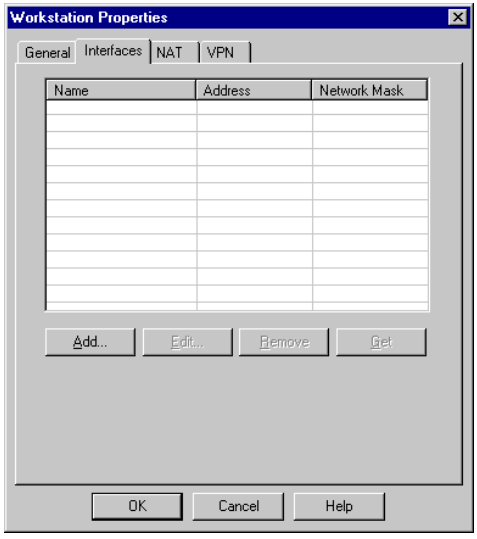


FIGURE 12-8 Workstation Properties window - Interfaces tab

No interfaces are shown, since you haven't defined any yet.

The easiest and most reliable way to define the interfaces is to click on **Get** and then proceed to "Authentication Methods" on page 214. Alternatively, you can define the interfaces manually by performing step 9 through step 10 for each interface.

9 To define an interface, click on **Add**.

The **Interface Properties** windows (FIGURE 12-9 on page 213) are displayed.

10 For each interface, fill in the data in the **Interface Properties** windows (FIGURE 12-9 on page 213) and click on **OK**, as follows:

TABLE 12-5 Field Values — Interface Properties window — le0

Field	Value	Explanation
General tab		
Name	le0	
Net Address	192.32.32.32	
Net Mask	255.255.255.0	
Security tab		
Valid Addresses	Others	Only packets whose source IP addresses belong to neither localnet nor DMZ are allowed to enter FWall through this interface; all other packets are spoofed.
Spoof Tracking	Alert	the action to take when spoofing is detected

TABLE 12-6 Field Values — Interface Properties window — le1 (FIGURE 12-9)

Field	Value	Explanation
General tab		
Name	le1	
Net Address	192.32.42.32	
Net Mask	255.255.255.0	
Security tab		
Valid Addresses	This Net	Only packets whose source IP addresses belong to DMZ are allowed to enter FWall through this interface; all other packets are spoofed.
Spoof Tracking	Alert	the action to take when spoofing is detected

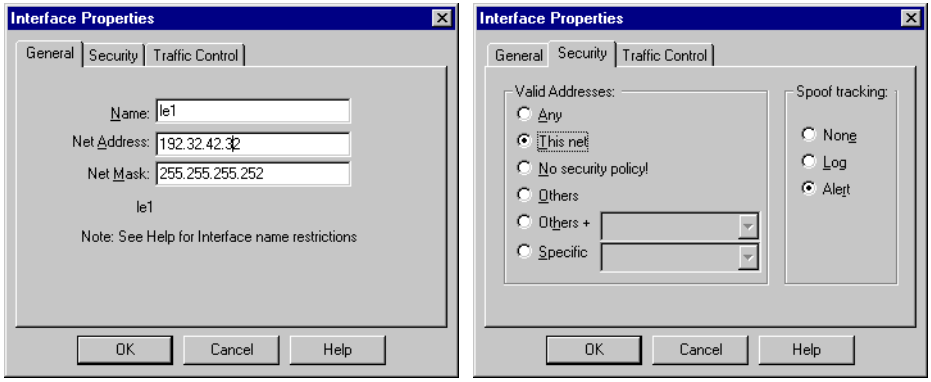


FIGURE 12-9 Interface Properties windows for le1

TABLE 12-7 Field Values — Interface Properties window — le2

Field	Value	Explanation
General tab		
Name	le2	
Net Address	199.199.199.32	
Net Mask	255.255.255.0	
Security tab		
Valid Addresses	This Net	Only packets whose source IP addresses belong to localnet are allowed to enter FWall through this interface; all other packets are spoofed.
Spoof Tracking	Alert	the action to take when spoofing is detected

11 After you have defined all three interfaces, you can see them in the **Interfaces** tab of the **Workstation Properties** window (FIGURE 12-10).

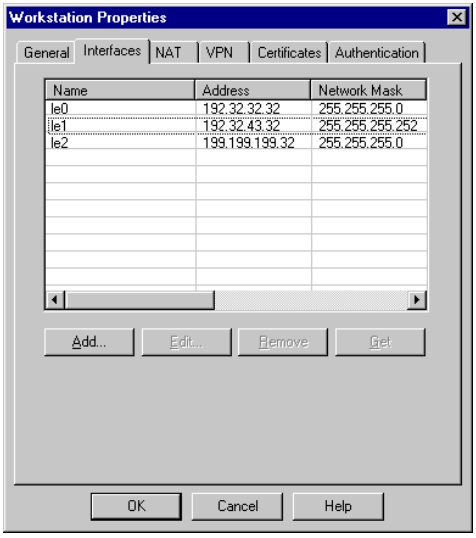


FIGURE 12-10 Interfaces tab showing all interfaces

Authentication Methods

12 Click on the **Authentication** tab of the **Workstation Properties** window.

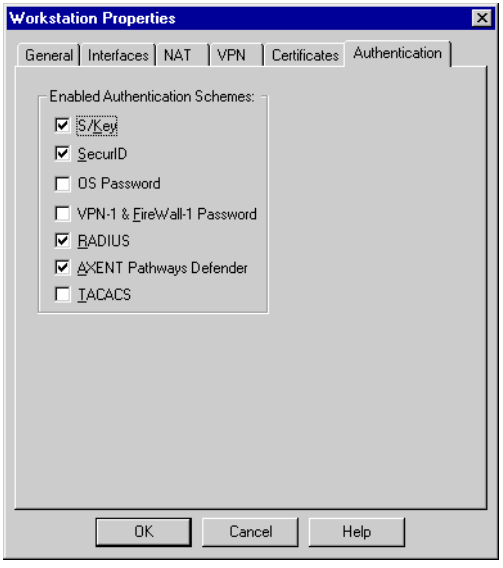


FIGURE 12-11 Workstation Properties window - Authentication tab

13 In the **Authentication** tab of the **Workstation Properties** window, select the Authentication methods that FWall will support for User, Client and Session Authentication.

In this example, these are:

- **OS Password**
- **VPN-1 & Firewall-1 Password**

Creating the Other Network Objects

The other network objects you must create are listed in TABLE 12-8.

TABLE 12-8 Other Network Objects

object name	type	IP address	Net Mask
Hatter	workstation	199.199.199.212	Not Applicable
localnet	network	199.199.199.0	255.255.255.0
DMZ (External Services Network)	network	192.32.42.0	255.255.255.0
MailServer	workstation	192.32.32.102	Not Applicable
FTPServer	workstation	192.32.32.103	Not Applicable
HTTPServer	workstation	192.32.32.104	Not Applicable

Networks

14 To define a network, click on **New** and choose **Network** from the menu. The **General** tab of the **Network Properties** window is displayed.

localnet

FIGURE 12-12 shows the **Network Properties** window after entering the data for localnet.

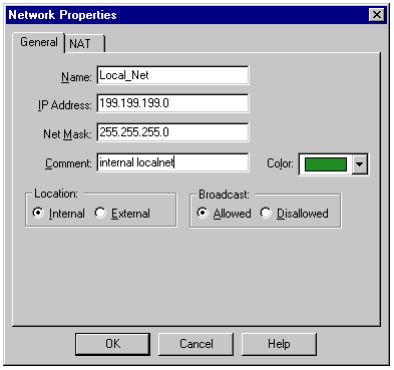


FIGURE 12-12 Network Properties window - localnet

TABLE 12-9 localnet — Network Properties window — General tab

Field	Value	Explanation
Name	localnet	the network's name
IP Address	199.199.199.0	
Net Mask	255.255.255.0	
Comment	internal localnet	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	Internal	**External** only for external networks
Broadcast	Allowed	consider the network's broadcast IP address as being part of the network

DMZ

FIGURE 12-13 shows the **Network Properties** window after entering the data for the External Services Network, DMZ.

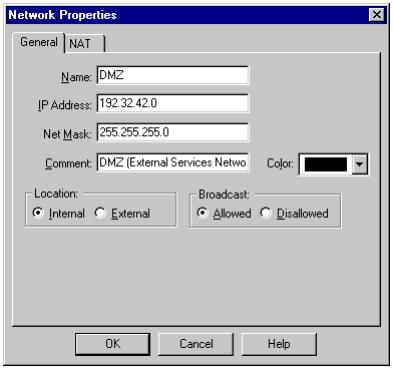


FIGURE 12-13 Network Properties window - DMZ

TABLE 12-10 DMZ — Network Properties window — General tab

Field	Value	Explanation
Name	DMZ	the network's name
IP Address	192.32.42.0	
Net Mask	255.255.255.0	
Comment	DMZ (External Services Network)	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	Internal	**External** only for external networks
Broadcast	Allowed	Consider the network's broadcast IP address as being in the network.

Hosts (Servers)

15 To define a host object, click on **New** and choose **Workstation** from the menu.

The **General** tab of the **Workstation Properties** window is displayed.

Mail Server

FIGURE 12-14 shows the **General** tab of the **Workstation Properties** window for the Mail Server.

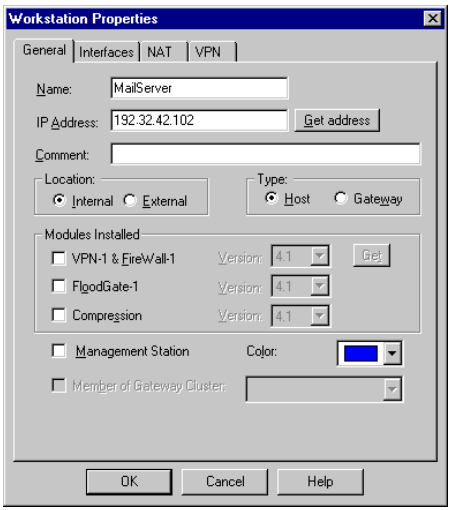


FIGURE 12-14 Host Properties window - Mail Server

TABLE 12-11 Mail Server — Workstation Properties window — General tab

Field	Value	Explanation
Name	MailServer	the name by which the object is known on the network - the response to the hostname command
IP Address	192.32.42.102	Get this by clicking on **Get Address.**
Comment	Mail Server	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	Internal	**External** only for network objects that are part of an external network — not managed by this FireWall Module
Type	Host	
Modules Installed	none checked	the Mail Server is not FireWalled

16 Define the FTP Server and the HTTP Server in the same way.

FTP Server

FIGURE 12-15 shows the **General** tab of the **Workstation Properties** window for the FTP Server.

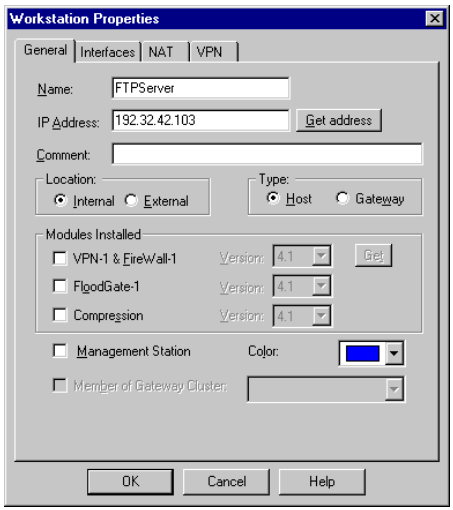


FIGURE 12-15 Host Properties window - FTP Server

TABLE 12-12 FTP Server — Workstation Properties window — General tab

Field	Value	Explanation
Name	FTPServer	the name by which the object is known on the network - the response to the hostname command
IP Address	192.32.42.103	get this by clicking on **Get Address**
Comment	FTP Server	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	Internal	External only for network objects that are part of an external network — not managed by this FireWall Module
Type	Host	
Modules Installed	none checked	the FTP Server is not FireWalled

HTTP Server

FIGURE 12-16 shows the **General** tab of the **Workstation Properties** window for the HTTP Server.

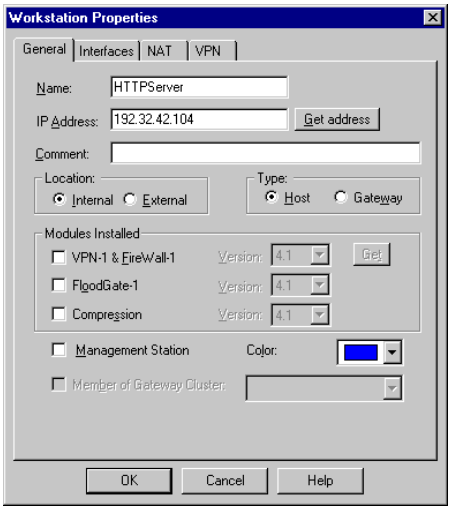


FIGURE 12-16 Host Properties window - HTTP Server

TABLE 12-13 HTTP Server — Workstation Properties window — General tab

Field	Value	Explanation
Name	HTTPServer	the name by which the object is known on the network - the response to the hostname command
IP Address	192.32.42.104	Get this by clicking on **Get Address.**
Comment	HTTP Server	the text that is displayed at the bottom of the **Network Objects** window when this object is selected
Location	Internal	External only for network objects that are part of an external network — not managed by this FireWall Module
Type	Host	
Modules Installed	none checked	the HTTP Server is not FireWalled

FIGURE 12-17 shows the **Network Objects** window after all the network objects have been defined.

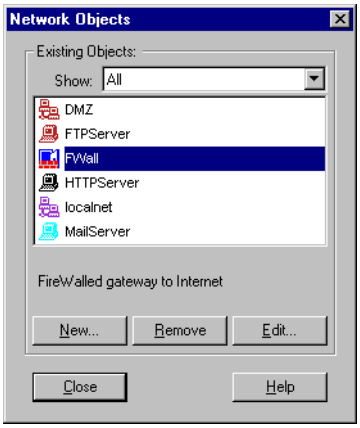


FIGURE 12-17 Network Objects window showing all defined objects

Creating Users

17 To create users, display the **Users** window by choosing **Users** from the **Manage** menu, or by clicking on  in the toolbar.

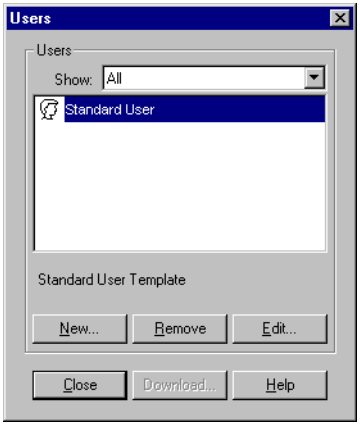


FIGURE 12-18 Users window showing no users defined

There are no users listed in the **Users** window, because you have not yet defined any. Only the **Standard User** user template is listed. Any users you define will be based on the **Standard User** user template, unless you define another template and base user definitions on that template.

Create a New User

18 To create a new user, click on **New** and choose **Standard User** from the menu (FIGURE 12-19).

FIGURE 12-19 New User Object Menu

19 In the **User Properties** window (FIGURE 12-21 and FIGURE 12-20), enter the data for the new user Bob.

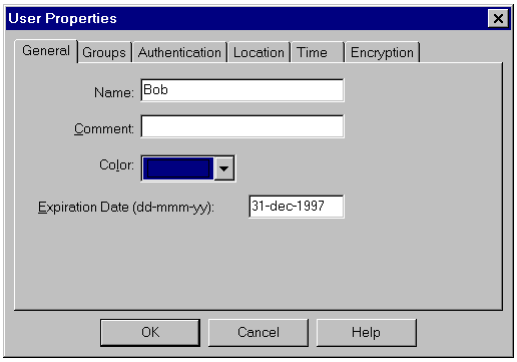


FIGURE 12-20 User Properties window — General Tab

20 Define Bob's Authentication Method as **OS Password**.

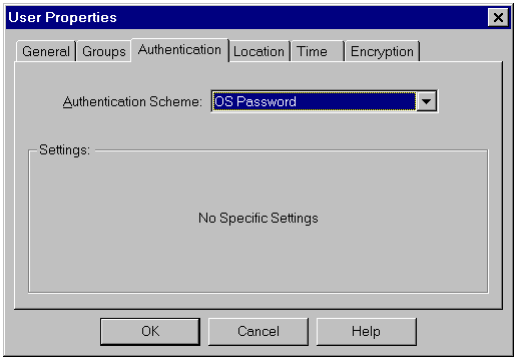


FIGURE 12-21 User Properties window — Authentication Tab (OS Password)

This means that Bob must have an OS account on each machine on which he is authenticated.

21 Next, define another user, Alice, also based on the **Standard User** user template.

However, define Alice's **Authentication Method** as **VPN-1 & FireWall-1 Password** (FIGURE 12-22). This means that Alice does not need to have an OS account on a machine on which she is authenticated.

22 Enter Alice's **VPN-1 & FireWall-1 Password**.

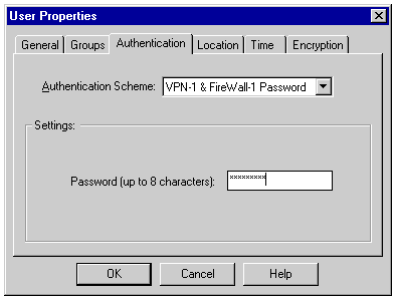


FIGURE 12-22 User Properties window — Method Tab (VPN-1 & FireWall-1 Password)

Note – OS Password and **VPN-1 & FireWall-1 Password** are the **Authentication Methods** defined in the **Authentication** tab of the **Workstation Properties** window for FWall (FIGURE 12-11 on page 214).

Create a New Group

23 To create a new group, click on **New** and choose **Group** from the menu (FIGURE 12-5 on page 208).

The **Group Properties** window (FIGURE 12-23) is displayed.

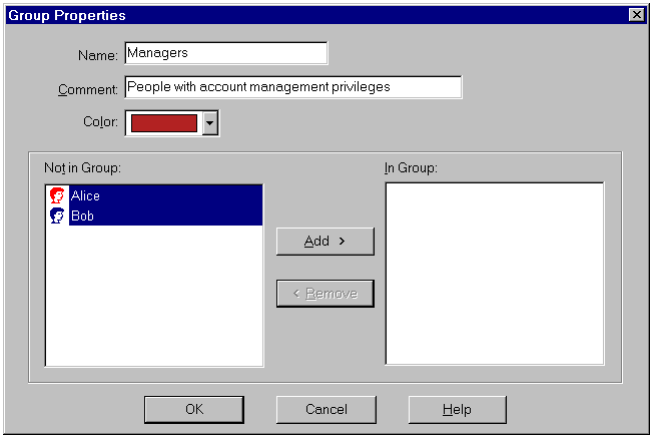


FIGURE 12-23 Group Properties window

24 Enter the name of the group (**Managers**) and a comment (optional).

25 Next, select **Alice** and **Bob** and click on **Add** to add them to the **Managers** group.

An Alternative Way

Another way to do this is as follows:

a. Define a group **Managers**.

b. Define a user template **TManager**.

c. In **TManager**'s **Groups** tab, specify **Managers**.

d. Define **Bob** and **Alice** based on the **TManager** template.

The new users are automatically members of **Managers**.

Defining a Rule Base

Having defined your network objects and your users, you are now ready to define a Rule Base.

26 Click on  in the Toolbar to add a new rule to your currently empty Rule Base.

A default "drop" rule (FIGURE 12-24) appears, which you must modify.

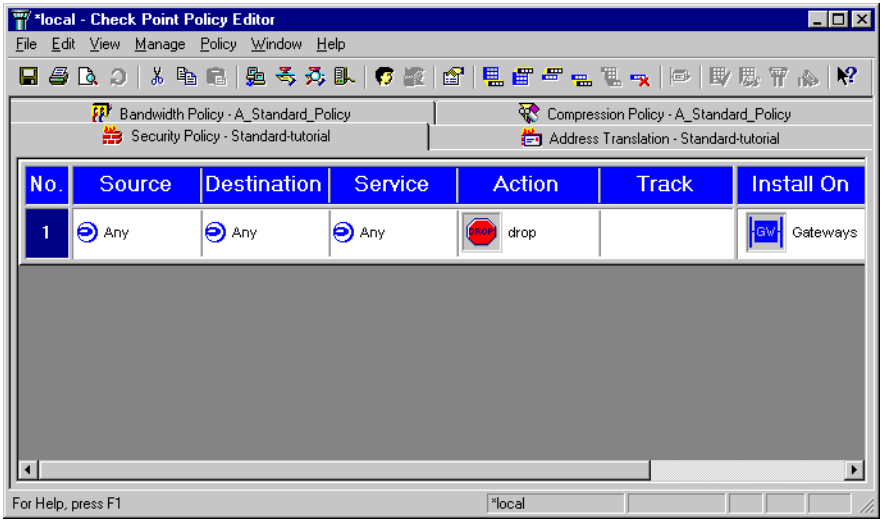


FIGURE 12-24 Default Drop Rule

27 Add the rules, one after the other, until your Rule Base looks like this:

Security Policy | Address Translation

No.	Source	Destination	Service	Action	Track	Install On
1	Any	FWall	Any	reject	Alert	Gateways
2	localnet	FTPServer	Any	accept	Short	Gateways
3	localnet	FTPServer	ftp	accept	Long	Gateways
4	Any	MailServer	smtp	accept	Short	Gateways
5	Any	HTTPServer	http	accept	Short	Gateways
6	Managers@Any	FTPServer	telnet	User Auth	Long	Gateways
7	Any	Any	Any	reject	Long	Gateways

FIGURE 12-25 Complete Rule Base

The Rule Base is explained in TABLE 12-14.

TABLE 12-14 Explanation of Rule Base

Rule No.	Explanation
1	prevents anyone from accessing the gateway itself
2	allows all internal hosts to go anywhere except FTPServer (note the negation of FTPServer in **Destination**)
3	allows all internal hosts to FTP to FTPServer
4	allows unrestricted access to MailServer on DMZ
5	allows unrestricted access to HTTPServer on DMZ
6	specifies User Authentication for Managers group members on incoming TELNET to FTPServer
7	rejects and logs all other communications

Installing a Security Policy

28 To install the Security Policy on the gateway (FWall), choose **Install** from the **Policy** menu.

Network Address Translation

In FIGURE 12-26, another network (HRnet) has been added to the configuration.

FIGURE 12-26 Network with invalid IP addresses

Suppose that HRnet's IP addresses are invalid. To enable the hosts in HRnet to communicate over the Internet, their addresses must be translated to valid addresses using VPN-1/FireWall-1's Network Address Translation feature.

There are two methods of translating IP addresses. One method (hiding) is to hide all the invalid addresses behind the gateway's valid address. This method has the advantage that it works with the valid address you already have, but its disadvantage is that it is impossible to initiate connections to the hosts in HRnet from the outside world.

The second method (static translation) is to acquire valid addresses and translate the invalid addresses to valid addresses on a one-to-one basis. This method enables outside hosts to initiate connections to the hosts in HRnet, but its disadvantage is that you will have to acquire valid addresses.

Translating Network Addresses

To translate HRnet's invalid addresses, proceed as follows:

1 Define HRnet.

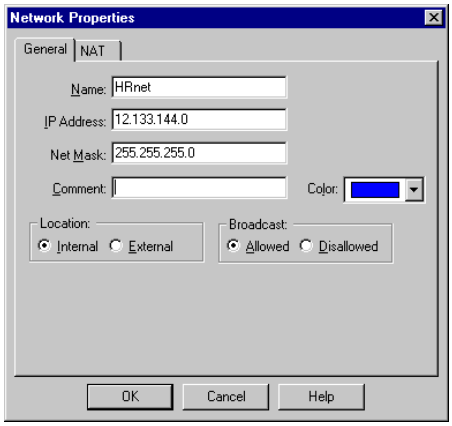


FIGURE 12-27 HRnet Network Properties - General tab

2 Click on the **NAT** tab.

3 Check **Add Automatic Address Translation Rules**.

Hide

To hide HRnet's invalid addresses behind the gateway's valid address (that of its external interface), select **Hide** from the **Translation Method** drop down list and enter the valid IP address of FWall's external interface (192.32.32.32) in **Hiding IP Address**.

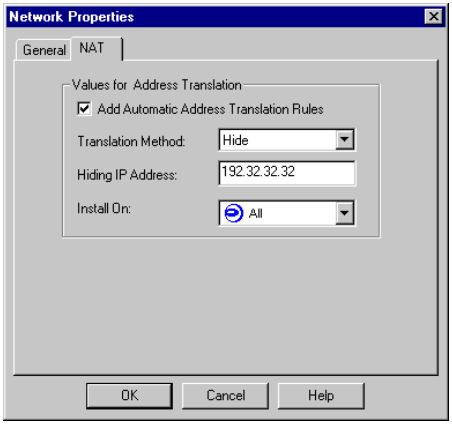


FIGURE 12-28 HRnet Network Properties - Hiding

Static Translation

To statically translate HRnet's invalid addresses, select **Static** from the **Translation Method** drop down list and enter the first IP address of the valid network addresses you have acquired in **First Valid IP Address**.

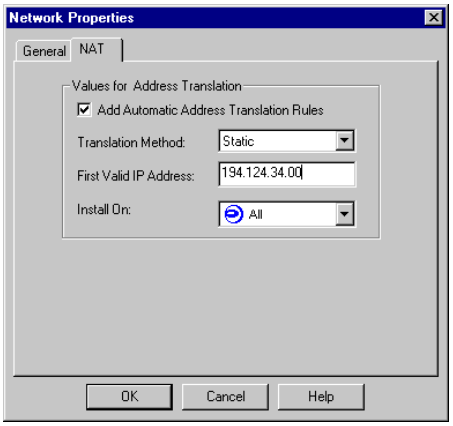


FIGURE 12-29 HRnet Network Properties - Static Translation

Monitoring the Security Policy

Monitoring System Status

The System Status View window presents a high-level view of operation and flow statistics for all FireWalled objects. To display the **System Status View** window, double-click on its icon on the desktop.

Viewing the Log

The Log Viewer allows you to view entries in the Log File. Each entry in the Log File is a record of an event that, according to the Rule Base or the Properties, is to be logged. In addition, every event which caused an alert, as well as certain important system events (such as security policies being installed or uninstalled on a host), are also logged. The format of log entries requested by a rule is determined by the log type specified in the relevant rule's **Track** field. To display the **Log Viewer** window, double-click on its icon on the desktop.

Index

N

O

P

Q

R

S

T

U

V

W

X