Check Point Getting Started Guide

NG FP3

For additional technical information about Check Point products, consult Check Point's SecureKnowledge at

http://support.checkpoint.com/kb/

Part No.: 700510
September 2002
# Table Of Contents

## Chapter 1  Check Point Enterprise Suite Overview
- Overview 13
- Securing the Internet 13
- Internet Firewall Technologies 14
- Firewall Requirements 14
- VPN-1/FireWall-1 Basic Concepts 15
- Stateful Inspection Technology 15
- VPN-1/FireWall-1 Architecture 16
- Check Point SmartDashboard 17
- SmartCenter Server 18
- VPN/FireWall Module 18
- Distributed Client/Server Deployment 19
- Enterprise Security Management 20
  - Defining a Security Policy — Check Point SmartDashboard 20
  - SmartView Tracker — Visual Tracking and Accounting 25
  - Real-time Status Monitoring — SmartView Status 26
  - Security and Network Management 27
- Enterprise Traffic Management 36
  - Provider-1 37
  - Reporting Module 37

## Chapter 2  Check Point Software Installation
- Check Point Software Installation Overview 39
- Starting the Installation — Windows 40
- Installing SMART Clients—Windows 44
- Starting the installation — Unix 45

## Chapter 3  Before Installing VPN-1/FireWal1-1
- Overview 51
- Preparing the VPN-1/FireWall-1 Machine 51
  - Protecting the VPN-1/FireWall-1 Machine 52
  - Routing 52
  - IP Forwarding 52
  - DNS 52
  - IP Addresses 53
  - VPN-1/FireWal1-1 Component Configuration 53
  - Installation 53
- Installation Overview for a New Installation 54
- Upgrading to a New Version of VPN-1/FireWall-1 55
  - Upgrade Sequence: SmartCenter Server and Module 55
  - Managing Previous Versions 55

List of Figures 3
Chapter 4 Installing and Configuring VPN-1/FireWall-1

Installing VPN-1/FireWall-1 (Windows) 61
Installing VPN-1/FireWall-1 (UNIX) 66
After Installing VPN-1/FireWall-1 70
  Reinstalling the Security Policy After Upgrading 70
  Obtaining Licenses 70
  Installing Licenses 71
Uninstalling VPN-1/FireWall-1 (Windows) 73
  Backing out to a previous version 73
Uninstalling VPN-1/FireWall-1 (UNIX) 73
  Backing out to a previous version 73
Configuring Check Point Products 73
  Licenses 74
  The Trial Period 76
  Administrators 78
  SMART Clients 84
  PKCS#11 Token 86
  Key Hit Session/Random Pool 87
  Certificate Authority 88
  Secure Internal Communication 89
  Fingerprint 93
  High Availability 94
  Interfaces 95
  VPN-1 Accelerator Driver 95
  SNMP Extension (Unix only) 95
  Automatic Start of Check Point Modules (Unix only) 95
Secure Internal Communications for Distributed Configurations 95
  Communicating Components 95
  Security Benefits 96
  Administrative Benefits 96
  SIC Certificates 96
  Communications between the SmartCenter Server(s) and Modules 97
  Communications Between the SmartCenter Server and the SMART Client 98
  Enabling Communication between Modules 99
  Resetting the Trust State of the Module 104
SIC Automatic Renewal 106
Frequently Asked Questions—Installing, Upgrading, Configuring 106

Chapter 5 VPN-1/FireWall-1 Tutorial

Introduction 113
Building a Security Policy 114

4 Check Point Getting Started Guide • September 2002
Preface

Check Point Product Overview
The interconnectivity of millions of computing devices — personal computers, servers, personal digital assistants, cellular phones, etc. — lies at the heart of modern commercial and governmental activity. It enables people and computers to exchange information and transactions at the speed of light, overcoming barriers of distance and language. It expands relationships beyond the limits of national borders and time zones, disintermediates the unproductive and enhances the value added by the productive. It brings producers and consumers closer together in worldwide communities.

The openness and interoperability that have made this vast network possible are at the core of its vulnerability. A door that opens to allow anyone to pass through can indeed allow anyone, vandals as easily as valued partners, to pass through. Communications that pass through public networks are exposed to interception, eavesdropping, and tampering. Resources — hardware, databases, confidential information, valuable relationships — are vulnerable to attack.

Check Point Enterprise Suite CD-ROM NG FP3 is a suite of integrated products that work together to provide security, quality of service and network management tools for enterprise environments.

Check Point Enterprise CD-ROM
This book provides an overview of the products available on the Check Point Enterprise Suite CD-ROM. An installation chapter provides step by step instructions on how to install and configure VPN-1/FireWall-1. Installation instructions for the other products are given in their respective User Guides.

Your Check Point license determines the Check Point products you can install from the CD and configure. The features enabled for each product also depend on your Check Point license.
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, “Check Point Enterprise Suite Overview” describes Check Point’s Secure Virtual Network technology and shows how VPN-1/FireWall-1’s architecture and features are used to enforce an enterprise-wide Security Policy.

Chapter 3, “Check Point Software Installation” describes the installation procedure for Check Point software products.

Chapter 2, “Before Installing VPN-1/FireWall-1” describes how a system must be prepared before installing VPN-1/FireWall-1.

Chapter 4, “Installing and Configuring VPN-1/FireWall-1” describes how to install VPN-1/FireWall-1.

Chapter 5, “VPN-1/FireWall-1 Tutorial” is a short tutorial presenting the major VPN-1/FireWall-1 features.

Chapter 6, “Introduction to Virtual Private Networks” describes how VPN-1/FireWall-1’s encryption features enable an enterprise to implement a Virtual Private Network.

Chapter 7, “” is a step-by-step tutorial for implementing a Virtual Private Network.

Check Point Documentation

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

The following User Guides are available for Check Point Enterprise Suite products.

1) Check Point Getting Started Guide — This book is an introduction to Check Point products.
2) Check Point SmartCenter Guide — This book describes the Check Point Management GUI, which is used to manage VPN-1/FireWall-1 and other Check Point products.


4) Check Point Virtual Private Networks Guide — This book describes the Check Point VPN-1/FireWall-1 encryption features.


6) Check Point FloodGate-1 Guide — This book describes Check Point FloodGate-1, which enables administrators to manage the quality of service on their networks.

7) Check Point SmartView Monitor User Guide — This book describes the Check Point Real Time Monitor, which enables administrators to monitor quality of service on their network links, as well as Service Level Agreement compliance.

8) Check Point Provider-1/SiteManager-1 Guide — This book describes Check Point Provider-1/SiteManager-1, which enables service providers and managers of large networks to provide Check Point products-based services to large numbers of subscribers.

9) Check Point SmartView Reporter Guide — This book describes the Check Point Reporting Module, which enables administrators to manage databases of Check Point log-based information.

10) Check Point UserAuthority User Guide — This book describes Check Point UserAuthority, which enables third-party and Web applications to leverage Check Point's sophisticated authentication and authorization technologies.


Note - For additional technical information about Check Point products, consult Check Point's SecureKnowledge database at [http://support.checkpoint.com/kb/](http://support.checkpoint.com/kb/)
# What Typographic Changes Mean

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

<table>
<thead>
<tr>
<th>Typeface or Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories; on-screen computer output</td>
<td>Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% You have mail.</code></td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, when contrasted with on-screen computer output</td>
<td><code>machine_name% su</code></td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Command-line placeholder: replace with a real name or value</td>
<td>To delete a file, type <code>rm filename</code>.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new words or terms, or words to be emphasized</td>
<td>Read Chapter 6 in User's Guide. These are called class options. You must be root to do this.</td>
</tr>
<tr>
<td>Save</td>
<td>Text that appears on an object in a window</td>
<td>Click the Save button.</td>
</tr>
</tbody>
</table>
TABLE P-2  Command-line Usage Conventions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[]</td>
<td>Optional variable</td>
<td><code>fw ver [-k] [-f filename]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use either or both of the <code>-k</code> and the <code>-f filename</code> options.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Compulsory variable</td>
<td><code>fw converthosts &lt;input_file&gt; [output_file]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>input_file</code> is compulsory. <code>output_file</code> is optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use one of the alternatives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use either the <code>Module IP</code> or the <code>object name</code> option</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Shell</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>C shell prompt</td>
<td><code>machine_name%</code></td>
</tr>
<tr>
<td>C shell superuser prompt</td>
<td><code>machine_name#</code></td>
</tr>
<tr>
<td>Bourne shell and Korn shell prompt</td>
<td><code>$</code></td>
</tr>
<tr>
<td>Bourne shell and Korn shell superuser prompt</td>
<td><code>+</code></td>
</tr>
<tr>
<td>DOS</td>
<td><code>current-directory&gt;</code></td>
</tr>
</tbody>
</table>

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

Check Point Enterprise Suite Overview

In This Chapter

- Overview .................................................. page 13
- VPN-1/FireWall-1 Basic Concepts .............. page 15
- VPN-1/FireWall-1 Architecture .................... page 16
- Enterprise Security Management ................. page 20

Overview

Securing the Internet

Internet technology is driving a worldwide business revolution. The reach of the Internet extends deep within the enterprise network, blurring the line between private and public networks. With critical communications travelling over heterogeneous networks, security deployments must protect enterprise networks against intrusion and ensure the privacy and integrity of communications. This requires a complete enterprise-wide security solution that protects networks, applications, and users — all the elements of the enterprise network. Check Point's Secure Virtual Network (SVN) architecture uniquely delivers end-to-end network security, enabling enterprises to protect business-critical Internet, intranet and extranet traffic.

VPN-1/FireWall-1 is a key component of SVN architecture and enables network security to be managed with a single enterprise-wide Security Policy. VPN-1/FireWall-1 is a comprehensive security platform that provides:

- SmartDefense — a product unique to Check Point that protects organizations from known and unknown network attacks.
Enterprise security can be extended with Check Point's Open Platform for Enterprise Security (OPSEC), providing central integration and management of complementary third-party security applications, services and platforms.

**Internet Firewall Technologies**

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, hosts, 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.
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.

**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:
- SMART Client (GUI)
- SmartCenter Server (also called Management Server)
- VPN/FireWall Module

**Check Point SmartDashboard**

The Check Point SmartDashboard (FIGURE 1-2), an intuitive graphical user interface, enables the administrator to define policies in terms of network objects (for example, hosts, networks, gateways, etc.) and rules.

Six kinds of policies can be defined:
- Security Policy
  A Security Policy specifies the types of communications allowed to enter and leave the network, and how connections will be authenticated and encrypted.
- Network Address Translation Policy
  A Network Address Translation Policy specifies how invalid internal IP addresses will be translated to valid IP addresses, enabling efficient use of the enterprise IP address space.
- Quality of Service (QoS) Policy
  A Quality of Service Policy specifies the allocation of bandwidth resources among connections, maximizing throughput.
- Desktop Security Policy
  A Desktop Security Policy enables the administrator to control access to desktops, both those within the local network and those connecting remotely.
- WebAccess Policy
  A WebAccess Policy enables the administrator to manage authorization requirements for Web applications.
- VPN Manager Policy
  A VPN Manager Policy enables the administrator to manage VPN communities.
FIGURE 1-2 Check Point "Security Dashboard" (SmartDashboard window)

**SmartCenter Server**

Policies are defined using the SmartDashboard GUI and saved on the SmartCenter Server. The SmartCenter Server maintains the Check Point databases, including network object definitions, user definitions, policies and log files for any number of enforcement points.

The SmartDashboard GUI and the SmartCenter Server can be deployed on the same machine or in a Client/Server configuration.

**VPN/FireWall Module**

The VPN/FireWall Module is deployed on Internet gateways and other network access points. The Security Policy is compiled on the SmartCenter Server and loaded to the VPN/FireWall Module, which enforces the policies. The VPN/FireWall Module can be installed on a broad range of platforms.
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. FIGURE 1-3 shows a distributed Client/Server configuration.

In this configuration the administrator configures and monitors network activity for several sites from a single desktop machine. The Security Policy is defined on the SMART Client, while the Check Point database is maintained on the SmartCenter Server (also called Management Server). The Security Policy is downloaded to three VPN/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 VPN/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 SmartDashboard

The Check Point SmartDashboard 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 1-4 SmartDashboard window with Security Policy Rule Base

The tabs displayed in the Check Point SmartDashboard 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 29.) If FloodGate-1 is licensed, then the SmartDashboard displays the QoS Policy tab. For information on FloodGate-1, see Check Point FloodGate-1 Guide.
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.

Network Objects

The SmartDashboard enables 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.
The Network Object Manager allows you to define the entities that are part of the Security Policy. Only those objects that are explicitly referenced in a Policy must be defined. These include:

**TABLE 1-1  Network Objects that can be explicitly referenced**

- Check Points (gateways, servers and hosts)
  - networks and sub-networks
  - Internet domains
  - OSE devices (routers)
  - embedded devices (for example, switches)
- logical servers (among which a processing load can be distributed automatically)
  - IP address ranges (logical entities)
  - gateway clusters (for High Availability)
  - dynamic objects
  - groups of the above objects
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.

Users can be defined either internally in the Check Point internal database, or they can be defined in an LDAP-compliant database using either a standard LDAP client or the Check Point LDAP-compatible SMART Client.

FIGURE 1-7 User Properties window - Check Point internal user and LDAP user
Services

The Service Window (FIGURE 1-8) 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 1-8 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.
SmartView Tracker — Visual Tracking and Accounting

VPN-1/FireWall-1's graphical SmartView Tracker provides visual tracking, monitoring and accounting information for all connections logged by Check Point Modules. Online viewing features enable real-time monitoring of network activity. The SmartView Tracker provides control over the log file display, providing quick access to information. Administrators can customize the SmartView Tracker 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 1-9 SmartView Tracker

The SmartView Tracker also allows administrators to identify suspicious connections and terminate active and future connections from a specific IP address.
FIGURE 1-10 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 Status Monitoring — SmartView Status

The SmartView Status window displays a snapshot of all the FireWalled and FloodGated systems throughout the enterprise, enabling real-time status and alerting. The SmartView 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,
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.
Multiple Authentication Schemes

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

- **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 VPN/FireWall Module machine 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 VPN/FireWall Module, 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.
Network Address Translation

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

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

- NAT Rule Base
- Automatic Configuration

Graphical NAT Rule Base

VPN-1/FireWall-1’s graphical user interface simplifies NAT definition and implementation. A flexible NAT 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.

FIGURE 1-13 Address Translation Rule Base

<table>
<thead>
<tr>
<th>NO.</th>
<th>SOURCE</th>
<th>ORIGINAL PACKET</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>SOURCE</th>
<th>ORIGINAL PACKET</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Local_Net</td>
<td>Local_Net</td>
<td>Any</td>
<td>Original</td>
<td>Local_Net</td>
<td>Local_Net</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Local_Net</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
<td>Local_Net</td>
<td>Local_Net</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>Remote_Net</td>
<td>Remote_Net</td>
<td>Any</td>
<td>Original</td>
<td>Remote_Net</td>
<td>Remote_Net</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>Remote_Net</td>
<td>Any</td>
<td>Any</td>
<td>Remote_Net</td>
<td>Remote_Net</td>
<td>Remote_Net</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
</tr>
</tbody>
</table>

Automatic Configuration

NAT properties are defined for specific network objects, such as gateways or networks. NAT rules are then automatically generated from these properties.
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 deployments can provide access to remote users when used with Check Point's VPN-1 SecuR emote Client software.
Check Point’s VPN-1 products support industry-standard algorithms and protocols, such as AES, DES, 3DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments. For more information, see Chapter 7, “Introduction to Virtual Private Networks”.

Security Servers

Authentication

Check Point 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 27.

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.

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.
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 1-15 URI Resource Definition tabs

Resources can be used in a Rule Base in the same way as a service (see FIGURE 1-16 on page 32). 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 1-16 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.

User Authority

Check Point VPN-1/FireWall-1 brings all enterprise applications into one centrally managed security framework by leveraging Check Point's proven networking, encryption and authentication technologies. VPN-1/FireWall-1 transparently integrates "best of breed" authentication mechanisms into enterprise applications, enabling intelligent authorization decisions based on a connection's security context: user identity and profile information, encryption and authentication parameters, networking information and desktop security parameters. VPN-1/FireWall-1 is the "security glue" that binds applications to network users, Check Point VPN-1/FireWall-1, and OPSEC applications to create an enterprise-wide Secure Virtual Network (SVN).

VPN/FireWall Module High Availability

VPN/FireWall Modules maintain information on authorized connections in dynamic state tables. When multiple VPN/FireWall Modules are deployed throughout the enterprise network, the connection information from each VPN/FireWall Module can be shared by all other modules. Sharing state information provides each VPN/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 VPN/FireWall Module fails, either due to a hardware or software problem, another VPN/FireWall Module can take over all the communications of the failed module without dropping any connections.
Utilizing multiple VPN/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 VPN/FireWall Module may not recognize a packet that is part of an authorized session and will drop or reject that packet.

Management High Availability

Two or more SmartCenter Servers can be configured in High Availability mode. If one is down, the administrator log on to another. Information on the SmartCenter Servers can be synchronized automatically or manually.

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 Security Policy like any other network object. For example, when a user connects to the local network through the VPN/FireWall Module, the VPN/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 1-17 External User Group (LDAP) window

Account Management is fully integrated in the VPN-1/FireWall-1 GUI.
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 many products from Cisco, Nortel (formerly Bay) Networks and 3Com.

FIGURE 1-18 Router Setup options for different brands of routers

The Security Policy is defined using the VPN-1/FireWall-1 Security SmartDashboard. 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 SmartView Tracker, 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.
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 Check Point FloodGate-1 Guide.

**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 1-19 Logical Server Properties window**

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.

**Provider-1**

Check Point Provider-1 enables MSPs and large enterprises to centrally create and manage the network Security Policies of multiple corporate sites, while maintaining secure isolation between individual customer databases.

For information about Check Point Provider-1, see *Check Point Provider-1 Guide*.

**Reporting Module**

The optional SmartView Reporter provides powerful log consolidation and reporting, and includes approximately 20 pre-defined reports. SmartView Reporter enables users to create custom reports for security audits, activity trending and accounting. Reports can be formatted as tables or graphs and can be printed, sent by email, or published to a Web site.

For information about Check Point SmartView Reporter, see *Check Point SmartView Reporter Guide*. 
CHAPTER 2

Before Installing VPN-1/FireWall-1

In This Chapter

Overview ................................. page 39
Preparing the VPN-1/FireWall-1 Machine .................. page 39
Installation Overview for a New Installation ............... page 42
Upgrading to a New Version of VPN-1/FireWall-1 .......... page 43
Which Components to Install ....................... page 46

Overview

This chapter describes how to prepare your system before you install VPN-1/FireWall-1.

Note - If you are not installing VPN-1/FireWall-1, then proceed to Chapter 3, “Check Point Software Installation.”

Preparing the VPN-1/FireWall-1 Machine

Before installing VPN-1/FireWall-1, you must first ensure that a number of preconditions exist (for example, that routing and DNS are correctly configured). Perform the procedure below before you begin the installation process.
Protecting the VPN-1/FireWall-1 Machine

1. Review the services running on the VPN-1/FireWall-1 machine and remove any service that is not required.
   Examples of services that are not required and might be considered a security risk are: NetBEUI, FTP and HTTP servers, etc.

Routing

2. 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.


   On Solaris2 and HP-UX, disable IP Forwarding in the kernel.
   For more information, see “IP Forwarding” on page 579 of Check Point SmartCenter Guide.

   When you install VPN-1/FireWall-1 on the Solaris2, HP-UX, and Windows NT platforms, VPN-1/FireWall-1 will control IP Forwarding by default, that is, 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.

DNS

4. 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**

5. 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.
- **Solaris** — Use the `ifconfig -a` command to display information about all the interfaces.
- **IBM AIX** — The `ifconfig` command is available, but it is best to use `smit` or `smitty` instead.
- **HP-UX** — The `ifconfig` command is available, but it is best to use `lanscan` instead.

6. Confirm that gateway’s name, as given in the `hosts` (Unix) and `hosts` (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 Gateway 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**

7. Familiarize yourself with the concepts of SmartCenter Server, Module and Management (GUI) Client by reading Chapter 1, “Check Point Enterprise Suite Overview”.

8. Determine which VPN-1/FireWall-1 component is to be installed on each computer. You must decide which computer(s) will host your SmartCenter Server(s), Module(s), and SMART Clients.

Note - If you are installing one of the Single Gateway Products, then the SmartCenter Server, Master and FireWalled Module must all be on the same machine, but you can still deploy the SMART Clients on a different machine.

**Installation**

9. In order to protect the computers on which you are installing VPN-1/FireWall-1 components, isolate them from the network so that they are not accessible from other computers.
Install the VPN-1/FireWall-1 components on the isolated computers. You should connect the computers to the network, and your local network to the Internet through the VPN/FireWall Module, only after VPN-1/FireWall-1 has been installed.

**Warning** - Do not open your network to the outside world before VPN-1/FireWall-1 has been installed and is protecting your network.

10 Verify that you have the correct version of the software for your OS and platform for all the VPN-1/FireWall-1 components.

11 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. Give the group a descriptive name, such as *fwadmin*.

12 If VPN-1/FireWall-1 is running, stop it, including the SMART Clients.

**Installation Overview for a New Installation**

To install VPN-1/FireWall-1 for the first time, proceed as follows:

1 Isolate the SmartCenter Server computer and the VPN/FireWall Module computer from the network so that they are not accessible from other computers.

2 Install and start VPN-1/FireWall-1 on the SmartCenter Server computer.

3 Install the VPN/FireWall Module on each of the managed (FireWalled) hosts.

**Note** - The VPN-1/FireWall-1 NG FP3 Boot Security feature may prevent the machine from completing the reboot following installation. If that is the case, see the instructions in the *Check Point FireWall Guide*.

4 Install the SMART Clients.

5 Connect the computers to the network and confirm connectivity between them.

6 Start the SMART Clients and connect to the SmartCenter Server.

7 Build a Security Policy and install it on the VPN/FireWall Modules.

VPN-1/FireWall-1 will then begin to enforce your Security Policy.
Upgrading to a New Version of VPN-1/FireWall-1

Supported Upgrade Paths

See the latest release notes.

Upgrading the OS to Solaris 8

The following procedure allow VPN-1/FireWall-1 to be used at all stages of an upgrade from Solaris 2.6 to Solaris 8. Proceed as follows:

1. Upgrade to VPN-1/FireWall-1 4.1 SP4.
2. Reboot the machine.
3. Upgrade the OS from Solaris 2.6 to Solaris 8.
4. Reboot the machine.
5. Upgrade to VPN-1/FireWall-1 NG.
6. Reboot the machine.

Note - Do not attempt to run VPN-1/FireWall-1 4.1 SP3 on Solaris 8. Upgrade VPN-1/FireWall-1 immediately after upgrading the OS.

Upgrade Sequence: SmartCenter Server and Module

1. First upgrade the SmartCenter Server and SMART Clients(s).
   When you upgrade the SmartCenter Server, its version in the SmartDashboard is set to NG FP3.
2. Then upgrade the VPN/FireWall Modules.
   After you upgrade each Module, you must manually change its version in the SmartDashboard to NG FP2 (in the General page of its Check Point Gateway or Node window).

Managing Previous Versions

During the installation process, you are asked whether to maintain backward compatibility. If you choose to do so, you will be able to manage Version 4.1 VPN/FireWall Modules from an NG FP3 SmartCenter Server.
Note the following compatibility issues:

- A Version NG FP3 SmartCenter Server can manage Version 4.1 VPN/FireWall Modules (only if Backward Compatibility is selected), but some Version NG FP3 features cannot be implemented on earlier VPN/FireWall Modules.
- A Version NG FP1 SmartCenter Server can manage Version 4.0 and 4.1 VPN/FireWall Modules (only if Backward Compatibility is selected), but some Version NG FP1 features cannot be implemented on earlier VPN/FireWall Modules.

What is Changed by the Upgrade?

FWDIR directory

VPN-1/FireWall-1 NG FP3 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 is changed to point to the 5.0 directory. If you uninstall NG FP3, the previous version is restored (that is, $FWDIR$ is set to point to the previous version).

VPN-1/FireWall-1 Database

When you upgrade to a new version of VPN-1/FireWall-1, the installation procedure carries the following elements 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 currently defined services are merged with the services defined in the new version of VPN-1/FireWall-1. In the case of a name conflict, the old objects (the ones you defined) will be kept.

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.

OPSEC Configuration information

In VPN-1/FireWall-1 NG, there is no longer a $fwopsec.conf$ file. The OPSEC configuration information on Modules is upgraded automatically (that is, copied from the existing $fwopsec.conf$ file to the database) when the Module is upgraded. To copy the configuration information from the Module to the upgraded SmartCenter Server, use the upgrade_fwopsec command.
The `upgrade-fwopsec` command upgrades OPSEC configuration information on the SmartCenter Server from pre-NG to NG format, based on the upgraded Module information.

For information on how to use this command, see “upgrade-fwopsec” on page 688 of the Check Point SmartCenter Guide.

**Minimizing Downtime During Upgrades**

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 SmartCenter Servers, because a SmartCenter Server cannot receive logs or alerts while it is being upgraded.

**Remote Upgrade using SmartUpdate**

SmartUpdate enables remote upgrade of the following:

- SVN Foundation
- VPN-1/FireWall-1
- FloodGate-1
- SecureClient Policy Server
- SmartView Monitor
- OPSEC products

For further information, see Chapter 2, “SmartUpdate” of the Check Point SmartCenter Guide.
After Upgrading

After upgrading, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy on all VPN/FireWall Modules, even if there has been no change in the Security Policy.

Which Components to Install

The following diagram (FIGURE 2-1) depicts a distributed VPN-1/FireWall-1 configuration.

FIGURE 2-1 Distributed VPN-1/FireWall-1 Configuration

NOTE: The Management Server can manage Access Lists on routers as well as VPN/FireWall Modules.
TABLE 2-1 lists the VPN-1/FireWall-1 components that must be installed on each computer.

**TABLE 2-1  Components to Install on Each Computer**

<table>
<thead>
<tr>
<th>on this computer</th>
<th>install this component</th>
<th>see also</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigBen</td>
<td>VPN-1/FireWall-1 SmartCenter Server (Enterprise Primary Management)</td>
<td>“Installing VPN-1/FireWall-1 (Windows)” on page 61, or “Installing VPN-1/FireWall-1 (UNIX)” on page 66</td>
</tr>
<tr>
<td>Tower</td>
<td>Windows Management (GUI) Client</td>
<td>“Installing SMART Clients—Windows” on page 54</td>
</tr>
<tr>
<td>FireWalled Gateway</td>
<td>VPN/FireWall Module (Called an Enforcement Module in the installation program)</td>
<td>“Installing VPN-1/FireWall-1 (UNIX)” on page 66</td>
</tr>
<tr>
<td>(London) (Solaris)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireWalled Gateway</td>
<td>VPN/FireWall Module (Enforcement Module)</td>
<td>“Installing VPN-1/FireWall-1 (Windows)” on page 61</td>
</tr>
<tr>
<td>(Paris) (NT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireWalled Gateway</td>
<td>VPN/FireWall Module (Enforcement Module)</td>
<td>“Installing VPN-1/FireWall-1 (UNIX)” on page 66</td>
</tr>
<tr>
<td>(Linux)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can also install VPN-1/FireWall-1 in a standalone configuration, in which the VPN/FireWall (Enforcement Module) and the SmartCenter Server (Enterprise Primary Management or Enterprise Secondary Management) are on the same machine.
Check Point Software Installation

In This Chapter

Check Point Software Installation Overview page 49
Starting the Installation — Windows page 50
Installing SMART Clients—Windows page 54
Starting the installation — Unix page 55

Check Point Software Installation Overview

This chapter describes how to install Check Point software.

All Check Point software can be installed from the Check Point Enterprise Suite CD. This chapter describes the installation “wrapper” that is common to all Check Point products. The detailed installation options of each individual product are described in each product's User Guide.

Before installing a Check Point software product, you should verify that the hardware and software platforms are appropriate to the software product. The minimum installation requirements requirements for all products on the Check Point CD, including VPN-1/FireWall-1, are given in the latest Release Notes.

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).
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.

The installation process has three stages:

1. **The Wrapper** — Selection of the products to be installed, with information about each product.
   See “Starting the Installation — Windows” on page 50 or “Starting the installation — Unix” on page 55.

2. **The Installer** — Installation of each product. For Windows, the Installer displays the installation status window.
   For VPN-1/FireWall-1, see “Installing VPN-1/FireWall-1 (Windows)” on page 61 or “Installing VPN-1/FireWall-1 (UNIX)” on page 66.

3. **Configuration** — Configuration of the installed products. The Configuration program is part of the SVN Foundation.
   See “Configuring Check Point Products” on page 73.

### Starting the Installation — Windows

1. Insert the VPN-1/FireWall-1 CD-ROM in the drive. The CD-ROM starts the Check Point installation program automatically. If for some reason it does not start automatically, run `setup.exe` file which is located under `\wrappers\windows`.
   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.

2. The **Welcome** window is displayed.
Note - At any point in the installation procedure, click on:
- **Next** to navigate to the next window, or
- **Back** to return to the previous window, or
- **Exit** to exit the installation procedure.

3 Click:
- **About Evaluation** to display the **Evaluation** window and proceed to step 4 on page 52, or
- **About Purchased Products** to display the **Purchased Products** window and proceed to step 4 on page 52, or
- **About the contents of this CD** to open a page on the Check Point Support website, or
- **Next** to display the **License Agreement** window and proceed to step 5 on page 52.
4 Click Next.

5 The License Agreement window is displayed.
FIGURE 3-4 License Agreement window

6 You must accept all the terms of the license agreement (by clicking 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.

7 Click Yes.

8 The Product Menu window is displayed.

FIGURE 3-5 Product Menu window

Select one of the following:

- Upgrade Installed products and install new products
**Installing SMART Clients—Windows**

SMART clients are installed from the Check Point Product CD. They can be installed together with other products or on their own.

1. In the **Server/Gateway Components** window (FIGURE 3-6), select **SMART Clients**.

**FIGURE 3-6 SMART Clients window**

2. Click **Next**.

- **Upgrade installed products**

  The following explanations relate to the **Upgrade Installed products and install new products** option.

9. Click **Next**.

10. Select the Check Point products you wish to install. For an explanation of each product, run the mouse over the checkboxes near each option.

11. Click **Next**.

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 “Installing and Configuring VPN-1/FireWall-1” on page 61.
- For information about installing other Check Point products, see the User Guides for those products.
When SMART clients are installed with other products, they are installed after the other products. Select the SMART clients (“GUIs”) you wish to install (FIGURE 3-7).

**FIGURE 3-7 Check Point SMART Clients installation window**

The following SMART clients are available:

<table>
<thead>
<tr>
<th>SmartMap</th>
<th>SmartView Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartView Tracker</td>
<td>SmartUpdate</td>
</tr>
<tr>
<td>SmartView Status</td>
<td>SmartView Reporter</td>
</tr>
<tr>
<td></td>
<td>VPN-1 SecureClient Packaging Tool</td>
</tr>
</tbody>
</table>

**Starting the installation — Unix**

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.

*Note*  • For a list of the OS versions supported by VPN-1/FireWall-1, see the Release Notes

To start the Check Point software installation procedure, proceed as follows:

1. Login as superuser.
2. Insert the CD in the drive.
Starting the installation — Unix

3 Mount the CD.

4 Change to the root directory on the CD.

5 Enter the following command to begin the installation process for Check Point Server and Gateway components:

`hostname# ./UnixInstallScript`

To install the Supplemental Components (VPN-1 Accelerator Card, VPN-1 Accelerator card II, and VPN-1 Accelerator Driver), see the instructions in Check Point Virtual Private Networks Guide.

The following window is displayed.

![Check Point Welcome screen (UNIX)](image)

Note: To move between windows, use the hot keys. The available hot keys appear on the highlighted last line of each installation window.
Press:

V (for evaluation product) to display the Evaluation Products window and proceed to step 6 on page 58, or

U (for purchased product) to display the Purchased Products window and proceed to step 6 on page 58, or

N (for next) to display the License Agreement window and proceed to step on page 58.

FIGURE 3-9 Evaluation Products screen (UNIX)

FIGURE 3-10 Purchased Products screen (UNIX)
6 Click N (for next) to proceed.
   The license agreement is displayed.

FIGURE 3-11 License Agreement screen (UNIX)

7 Press Space to read through the agreement, or Esc to get to the confirmation message. If you Accept the terms of the License Agreement, choose y.

8 Click N (for next) to proceed to the next window.
   The Check Point SVN Foundation is now installed (unless it is already installed). The Check Point SVN Foundation is used by all Check Point NG FP3 products, and is required for all Check Point NG products other than SMART Clients.

FIGURE 3-12 SVN Foundation Installation (UNIX)
The Product Menu window is displayed. The available products depend on the Operating System of the machine.

**FIGURE 3-13 Product Menu (UNIX)**

![Product Menu (UNIX)](image)

**Note:**
- Select a menu item by typing the relevant number.
  - In a check box menu item you can select more than one item from the list. To deselect the item, type the number again.
  - In a radio box menu item you can select only one item from the list.

**10** Select the Check Point components you wish to install by typing their number. Click **N** (for next) to start the installation.

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 “Installing VPN-1/FireWall-1 (UNIX)” on page 66.”
- For information about installing other Check Point products, see the User Guides for those products.
Installing and Configuring VPN-1/FireWall-1

In This Chapter

Installing VPN-1/FireWall-1 (Windows) .......................................................... page 61
Installing VPN-1/FireWall-1 (UNIX) .............................................................. page 66
After Installing VPN-1/FireWall-1 ................................................................. page 70
Uninstalling VPN-1/FireWall-1 (Windows) ..................................................... page 73
Uninstalling VPN-1/FireWall-1 (UNIX) ......................................................... page 73
Configuring Check Point Products ................................................................. page 73
Secure Internal Communications for Distributed Configurations ....................... page 95
Frequently Asked Questions—Installing, Upgrading, Configuring ....................... page 106

Installing VPN-1/FireWall-1 (Windows)

This section applies both to new installations and to upgrades from a previous version.

1 First, complete the initial choices on the Check Point installation CD (see "Starting the Installation — Windows" on page 50 of the Check Point Getting Started Guide). In the Server/Gateway Components Window (FIGURE 4-1) select VPN-1/FireWall-1.
Installing VPN-1/FireWall-1 (Windows)

FIGURE 4-1 VPN-1/FireWall-1 selected in the Server/Gateway Components window

After completing the initial choices on the Check Point installation CD, the Selected Products window (FIGURE 4-2) summarizes the products selected for installation, including VPN-1/FireWall-1.

FIGURE 4-2 Selected Products window.

Note:
- SmartUpdate Server component is automatically installed as part of the VPN-1/FireWall-1 SmartCenter Server.
- SmartUpdate Client is installed together with the other SMART Clients (see “Installing SMART Clients—Windows” on page 54).

2 After completing the initial choices on the Check Point installation CD, the Selected Products window (FIGURE 4-2) summarizes the products selected for installation, including VPN-1/FireWall-1.
If the list of products is different from what you intended, click **Cancel** and make the initial choices again.

3 Click **Next**.

An **Installation Status** window shows the progress throughout the installation of all selected products.

4 The installation program checks whether the Check Point SVN Foundation is installed. If not, it is now installed.

The Check Point SVN Foundation is used by all Check Point NG FP3 products, and is required for all Check Point NG FP3 products other than SMART Clients.

The installation of VPN-1/FireWall-1 files now begins.

**FIGURE 4-3** Installation Progress message

5 In the VPN-1/FireWall-1 Enterprise Product window, select the product type to install on this machine:

**FIGURE 4-4** Enterprise Product window

To decide what product to install on this machine, you may find it useful to refer to **FIGURE 2-1** on page 46.

- Choosing **Enforcement Module** will install a VPN/FireWall Module on this machine.
• Choosing **Management Server (including Log Server)** will install a SmartCenter Server and a Log Server on this machine.

• Choosing **Log Server** will install a Log Server on this machine.

6 Specify whether you wish to install a Primary management or Secondary management. For more information about using Enterprise management Servers, see the Check Point SmartCenter Guide.

**FIGURE 4-5** Enterprise Primary or Secondary Management

![Image of Enterprise Primary or Secondary Management window]

7 The **Backward Compatibility** window (FIGURE 4-6, for SmartCenter Server only) allows you to maintain backward compatibility with previous versions. VPN-1/FireWall-1 NG FP3 provides backward with VPN/FireWall Modules of version 4.1.

If you need to manage version 4.1 VPN/FireWall Modules, choose **Install with backward compatibility**.
FIGURE 4-6 Backward Compatibility window

8 Click Next. In the Choose Destination window you can choose a different directory from the one suggested in the Destination Folder by clicking Browse. The installation now proceeds, and various progress messages are displayed.

9 Select the Smart Clients to be installed. You can add or remove Smart clients at a later time. See “Installing SMART Clients—Windows” on page 54.

10 Click Next. The installation now proceeds, and various progress messages are displayed.

11 Following the product installations, the configuration of VPN-1/FireWall-1 begins (see “Configuring Check Point Products” on page 73). The Check Point Configuration program (cpconfig) configures VPN-1/FireWall-1 by asking a series of questions.

12 A “Thank You” message (FIGURE 4-7) appears when all the installations have been completed.

FIGURE 4-7 Installation complete window

13 After installing and configuring, restart your computer in order to activate VPN-1/FireWall-1 (FIGURE 4-8).
Installing VPN-1/FireWall-1 (UNIX)

If VPN-1/FireWall-1 is running on the machine on which you installed VPN-1/FireWall-1, it will be stopped.

14 If you upgraded your VPN-1/FireWall-1 installation, install your Security Policy.

Installing VPN-1/FireWall-1 (UNIX)

This section applies both to new installations and to upgrades from a previous version.

1 First, complete the initial choices on the Check Point installation CD (see “Starting the installation — Unix” on page 55 of the Check Point Getting Started Guide).

2 From the Product Menu window, select VPN-1/FireWall-1 by typing the appropriate number.
Chapter 4 Installing and Configuring VPN-1/FireWall-1

FIGURE 4-9 Product Menu (UNIX)

To decide what product to install on this machine, you may find it useful to refer to FIGURE 2-1 on page 46.

- Choosing **Primary Management and Enforcement Module** will install both a SmartCenter Server and a VPN/FireWall Module on this machine.

Note: SmartUpdate is automatically installed as part of the VPN-1/FireWall-1 SmartCenter Server.

3 Press **N** (for next). The **Installation Type** window appears.

FIGURE 4-10 Installation Type (UNIX)

To decide what product to install on this machine, you may find it useful to refer to FIGURE 2-1 on page 46.

- Choosing **Primary Management and Enforcement Module** will install both a SmartCenter Server and a VPN/FireWall Module on this machine.
• Choosing **Enforcement Module** will install a VPN/FireWall Module on this machine.
• Choosing **Enterprise Primary Management** or **Enterprise Secondary Management** installs a SmartCenter Server on this machine.

For more information about using Enterprise Secondary Management, see “Management High Availability” on page 539 of the Check Point SmartCenter Guide.

• **Enterprise Log Server.** For information, refer to the Check Point SmartView Reporter Guide.

Choose an option. If you choose the **Enterprise Log Server** or any of the options which include a SmartCenter Server:

• **Enterprise Primary Management**
• **Enterprise Secondary Management**
• **Enforcement Module and Primary Management**

Proceed to step 4. To install only a VPN/FireWall Module on this machine, choose **Enforcement Module** and proceed to step 5.

**Note** - All the options which include a SmartCenter Server will allow you to manage other VPN/FireWall Modules from this machine.

4 Press **N** (for next). The **Installation Type** window appears.

The Backward Compatibility window (FIGURE 4-11, for SmartCenter Server only) allows you to maintain backward compatibility with previous versions. VPN-1/FireWall-1 NG provides backward with VPN/FireWall Modules of version 4.1. If you need to manage version 4.1 VPN/FireWall Modules, choose **Yes**.
A validation message showing the selected products appears (FIGURE 4-12).

Press **N** (for next) to continue the installation of:

- **VPN-1/FireWall-1**
- backward compatibility (if selected) options
- All other selected products
Following the product installations, the configuration of VPN-1/FireWall-1 begins (see “Configuring Check Point Products” on page 73). cpconfig configures VPN-1/FireWall-1 by asking a series of questions.

After configuring VPN-1/FireWall-1 you are required to reboot.

**After Installing VPN-1/FireWall-1**

**Reinstalling the Security Policy After Upgrading**

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 Check Point products require a license to enable their operation. Licenses are not required on SMART Clients. Both Permanent and Evaluation licenses can be obtained from the User Center:


Licenses can be either Central or Local. To work with SmartUpdate central license management, Central licenses are required. Management of licenses for all installed products is greatly simplified by using Central Licenses and SmartUpdate. Local licenses are also supported, and these can be imported into SmartUpdate. For more information about Central and Local Licenses, see Chapter 2, “SmartUpdate” in the Check Point SmartCenter Guide.
Evaluation Licenses
If you have a Certificate Key for your Check Point product, 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 Check Point product, then you can obtain an evaluation license from your Check Point reseller.

Permanent Licenses
To obtain a permanent license, proceed as follows:

1. Find the Certificate Key on the CD cover of the Check Point CD.
2. Obtain a permanent license that can be used with SmartUpdate:
   a. Login to the User Center http://www.checkpoint.com/usercenter
   b. In the My Products tab, select the product(s) to be licensed and click New or Modify License(s).
   c. Choose Use Central Licenses scheme or Use Local Licenses, and click Continue to Confirmation.

Installing Licenses
You must have a license to use Check Point products. If you did not enter your license(s) during the configuration immediately following installation, use the following procedures for installing your license(s) now.

Licenses are installed on the SmartCenter Server and on the Modules. For embedded systems, the license must be installed on the SmartCenter Server.

When you install a permanent license, it is best to delete any expired evaluation licenses. To remove old licenses use the cpconfig configuration application or use the cplic del command (see “cplic db_rm” on page 642 of Check Point SmartCenter Guide), or use the SmartUpdate GUI (see "Deleting a License from the License Repository" on page 114 of the Check Point SmartCenter Guide).

Installing Licenses Using SmartUpdate
Central and NG Local licenses can be remotely installed using SmartUpdate. See “Attaching a License to a Check Point Node” on page 107 of the Check Point SmartCenter Guide.
Installing Local Licenses Using Cpconfig

You can install a Local license when you configure the Check Point product, immediately after installing it, or at a later time by running the Check Point Configuration application `cpconfig`. See “Licenses” on page 74.

Installing Licenses Using the Command-line

1. The license email received from the User Center contains the license string and an attached license file. The license can be installed either remotely (from a SmartCenter Server), or locally:
   - Copy the license string to the clipboard. Copy the string that starts with `cplic put...` and ends with the last SKU/Feature, then paste the license at a root prompt, or
   - At a root prompt type the following commands:

     To install the license locally:

     ```
     hostname# cplic put <host expiration-date signature SKU/feature>
     ```

     For information on this command, see “cplic put...” on page 626” of the Check Point SmartCenter Guide.

     To install the license remotely from the SmartCenter Server:

     ```
     hostname# cplic put <object-name><host expiration-date signature SKU/features
     ```

     For information on this command, see “cplic <object-name> ...” on page 633” of the Check Point SmartCenter Guide.

2. When you enter your license, you will get a response similar to the following:

<table>
<thead>
<tr>
<th>Host</th>
<th>Expiration</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>215.157.142.120</td>
<td>26Mar2002</td>
<td>CPSUITE-EVAL-3DES-v50 CK0123456789ab</td>
</tr>
</tbody>
</table>

   License file updated

   In this example:
   - The license expires on March 26, 2001.
   - The license SKU is “CPSUITE-EVAL-3DES-v50”.
   - The Certificate Key is “CK0123456789ab”.

72 Check Point Getting Started Guide • September 2002
3 Confirm that you are using the correct licenses by printing the license. The last part of the response (the part beginning with “CK”) is the Certificate Key.

Use the `cplic print` command for a local License (see “cplic print” on page 630” of the Check Point SmartCenter Guide), and `cplic db_print` command for a remote License (see “cplic db_print” on page 643 of the Check Point SmartCenter Guide).

Uninstalling VPN-1/FireWall-1 (Windows)

To uninstall VPN-1/FireWall-1, use the Add/Remove Programs applet in the Windows Control Panel.

Backing out to a previous version

If you have a previous version installation, then uninstalling VPN-1/FireWall-1 will reactivates the previous version.

Uninstalling VPN-1/FireWall-1 (UNIX)

To uninstall VPN-1/FireWall-1 on

Solaris 2—Use `pkgrm`.

Linux—Use `rpm -e`.

If the Primary SmartCenter Server is uninstalled, you will need to uninstall all other Check Point Products on the computer and reinstall them from scratch.

Backing out to a previous version

If you have a previous installation, then uninstalling VPN-1/FireWall-1 will reactivates the previous version.

Configuring Check Point Products

- **Configuring a New or Upgrade Installation**—The configuration starts automatically after the Check Point product is installed or upgraded. The configuration options appear consecutively. Configure each option and then proceed to the next window.

  After configuration, you must reboot.

- **Configuring Installed Products**—Check Point products are configured by running the Check Point configuration application (`cpconfig`). When you do so, the different configuration options can be chosen from a menu (on UNIX platforms) or appear as individual tabs in the Configuration window (on Windows). To run the configuration application:
• Type `cpconfig` at the command prompt, or
• Windows platforms—go to `Start>Programs>Check Point SMART Clients>Check Point Configuration NG`

The Configuration program is part of the SVN Foundation.

The windows or menus displayed depend on the components installed on the machine. You will not necessarily see all the windows or menu items described here during your configuration process.

The following configuration options are available:

- Licenses
- The Trial Period
- Administrators
- SMART Clients
- PKCS#11 Token
- Key Hit Session/Random Pool
- Certificate Authority
- Secure Internal Communication
- Fingerprint
- High Availability
- Interfaces
- VPN-1 Accelerator Driver
- SNMP Extension (Unix only)
- Automatic Start of Check Point Modules (Unix only)
- Automatic Start of Check Point Modules (Unix only)

**Licenses**

Use this option to:
- view license details
- add required licenses for the host
- delete licenses from the host (Windows only). On Unix, to delete or overwrite a license use the `cplic del` command (see “cplic del” on page 820).

You do not need a license to run the SMART Client.
Use the `cpconfig` Licenses option to manage Local licenses only. Central licenses are managed via SmartUpdate. For details about the differences between Local and Central Licenses, and for information about centrally managing licenses on remote hosts, see Chapter 2 “Smart Update” on page 67 of the Check Point SmartCenter Guide.

**Note** - For a DAIP Module, do not use `cpconfig` to installing a license. A DAIP Modules can use only a Central license, which must be installed using the `cplic put` command.

**FIGURE 4-14** Licenses window (Windows)

Understanding License Details

The Licenses window shows the following information for each license:

- **IP Address** — the IP address of the machine for which the license is intended
- **Expiration Date** — the license expiration date
- **SKU/Features** — a string composed of four groups of 9 nine characters listing the features included in the license

**Obtaining Licenses**

If you have not yet obtained your license(s), see “Obtaining Licenses” on page 127 of the Check Point Getting Started Guide. You can add licenses after completing the other `cpconfig` configuration options.
The Trial Period

All purchased Check Point products have a 15 day trial period. During this period the software is fully functional and all features are available without a license. After that period, a permanent license must be installed in order to continue using the software. Alternatively, an evaluation license must be obtained.

The 15 day trial period on an Enforcement Module starts when Secure Internal Communication is initialized with the SmartCenter Server. On a SmartCenter Server, the trial period starts when the Certificate Authority is initialized during cpconfig configuration.

If a license is installed during the 15 day trial period, the effective license will be the installed license.

If all installed licenses are removed during the 15 day trial periods, the product will regain full functionality until the end of trial period.

If no licenses are installed, the remaining trial period is displayed when starting SmartUpdate and any of the other Check Point SMART Clients.

To see the remaining trial period, perform the Get Check Point Node Licenses operation in SmartUpdate, or open the Licenses tab on the Enforcement Module, or run the command cplic print locally on the Enforcement Module.

To Fetch One or More Licenses from a File

After installing the license, you should import the licenses to the SmartUpdate License Repository. On Windows platforms, to import one or more licenses from a license file, proceed as follows:

1  Click on Fetch from File.

FIGURE 4-15 Open License File window
2 Browse to the license file, select it, and click **Open**.

The license(s) that belong to this host are added. After installing the license, you should import the licenses to the Smart Update License Repository (see “Adding a License to the License Repository” on page 114).

**To Add a License Manually**

On Unix platforms, type the details of the license. The license email received from the User Center contains the license string and an attached license file. On Windows, proceed as follows:

1. Click on **Add** to add a license.

   The **Add License** window is displayed.

   ![Add License window](image)

2. The User Center results page and the license email received from the User Center contains the license installation instructions. To enter the license data, either:
   - Copy the license string to the clipboard. Copy the string that starts with `cplic` and ends with the last SKU/Feature, then click **Paste License**, or
   - Type in the information.

3. Click **Calculate**, and make sure the result matches the validation code received from the User Center.

4. Click **OK**.
To Delete a License

1. In the Licenses window, select the license to be deleted.
2. Click Delete, or press the Delete key on the keyboard.

Administrators

FIGURE 4-17 Administrators window

Use this option to:
- add administrators who are permitted on the SMART Client side, that is, the administrators who will be allowed to use a SMART Client to connect to the SmartCenter Server installed on this machine
- modify Administrator permissions
- delete Administrators

The availability of permissions depends on the installed products.

Whenever an administrator logs in, all actions are recorded on the SmartCenter Server in a file called $FWDIR/log/fw.adtlog which is viewed using the Log Viewer. Administrator actions are also logged to a text file called $FWDIR/log/cpmi_audit.txt.
Administrators

Chapter 4 Installing and Configuring VPN-1/FireWall-1

In This Section

To Add an Administrator...

You must define at least one administrator, otherwise no one will be able to use the SmartCenter Server you have just installed.

The administrator password should be at least four characters long, with no spaces.

1. Click Add to specify an administrator. The Add Administrator window is displayed.

**FIGURE 4-18 Add Administrator window**

2. Enter the Administrator Name.

To Add an Administrator

You must define at least one administrator, otherwise no one will be able to use the SmartCenter Server you have just installed.

The administrator password should be at least four characters long, with no spaces.

1. Click Add to specify an administrator. The Add Administrator window is displayed.

**FIGURE 4-18 Add Administrator window**

2. Enter the Administrator Name.
3 Enter the **Password**.  
The password should be at least four characters long, with no spaces.  
You must enter the password twice in order to confirm it.

4 Specify the Administrator’s **Permissions**. The following table shows the available administrator permissions options.

<table>
<thead>
<tr>
<th>TABLE 4-1 Add and Edit Administrator Permission Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selecting this option...</strong></td>
</tr>
<tr>
<td>Read/Write All</td>
</tr>
<tr>
<td>Read Only All</td>
</tr>
<tr>
<td>Customized</td>
</tr>
<tr>
<td>Smart Update</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Objects Database</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Check Point Users Database</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Selecting this option…</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
</tbody>
</table>
| **LDAP Users Database** | • Read/Write permission allows the administrator to define, remove and modify LDAP users and groups.  
• Read Only permission allows the administrator to view LDAP users and groups but not modify them.  

For more information on LDAP Users database administrators, see “LDAP Administrators” on page 21 of Check Point User Management. |
| **Security Policy** | • Read/Write allows the administrator to manage Security Policies and rules within the Policies. The administrator can install and uninstall Security Policies.  
• Read Only allows the administrator to open and view Security Policies but not to modify them. |
| **QoS Policy** | • Read/Write allows the administrator to manage QoS policies and rules within the policies. The administrators can install and uninstall QoS Policies.  
• Read Only allows the administrator to open and view QoS Policies but not to modify them. |
| **Log Consolidator Policy** | • Read/Write allows the administrator to manage Log Consolidator policies and rules within the policies. The administrator can install and uninstall Log Consolidator Policies.  
• Read Only allows opening and viewing Log Consolidator policies but not to modifying them. |
| **Reporting Tool** | • Read/Write allows the administrator to create and manage report definitions.  
• Read Only permission allows the administrator to process reports and change Runtime parameters, but not to create or modify report definitions. |
| **Monitoring** | • Read/Write permission allows the administrator full access to the Log Viewer, System Status and Traffic Monitoring.  
• Read Only permission prevents the administrator from interrupting connections. |
To Modify Administrator Permissions

1. Select the Administrator to be edited.
2. Click on Edit in the Administrators window.

   The Edit Administrator window will open (very similar to “Add Administrator window, FIGURE 21-5 on page 24).
3. Specify the Administrator’s Permissions. TABLE 21-1 on page 25 explains the available administrator permissions options.

To Delete an Administrator

1. Select the Administrator to be deleted.
2. Click Delete in the Administrators window.

Concurrent Sessions

In order to prevent more than one administrator from modifying a Security Policy at the same time, VPN-1/FireWall-1 implements a locking mechanism.

Any number of administrators can view a Security Policy at the same time, but only one of them can have write permission at any given moment. Upon opening a Security Policy, an administrator is granted write permission only if both of the following conditions are true:

- The administrator has been assigned Read/Write or User Edit privileges.
- No other administrator currently has write permission for the Security Policy at this time.

For example, suppose Bob and Alice are both administrators. Bob has Read/Write privileges and Alice has User Edit privileges. Suppose no one has the Security SmartDashboard open. If Alice opens the Security SmartDashboard, she will be granted User Edit permission. If Bob opens the same Security Policy before Alice closes it on her workstation, then Bob will not be granted Read/Write permission. Instead, he will be asked whether he wishes to quit or to open the Security Policy with Read Only permission.
Read Only Sessions

An administrator with Read/Write or User Edit privileges can open a Read Only session by checking the Read Only checkbox in the Check Point SmartDashboard Login window.

![Login window]

During the Read Only session, another administrator with Read/Write privileges can log in and be granted write permission.

Authenticating VPN-1/FireWall-1 Administrators

You may wish to authenticate VPN-1/FireWall-1 administrators, even if they are defined as administrators and connecting from authorized SMART Clients.

Note: VPN-1/FireWall-1 administrators are always authenticated. This section describes how to implement additional authentication mechanisms.

To authenticate VPN-1/FireWall-1 administrators, proceed as follows:

1. Configure your SmartCenter Server so that it is protected by a VPN/FireWall Module.
   - The VPN/FireWall Module can be on the same machine as the SmartCenter Server or on a different machine.

3 Add a rule to the Rule Base specifying Client Authentication or Client Encryption as the Action, for example, the rule shown below:

**TABLE 4-2 Rule Base Example**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW1Admin@Any</td>
<td>MgmtStation</td>
<td>FW1_mgmt</td>
<td>Client Encryption</td>
<td>Log</td>
<td>the VPN/Firewall Module that protects the SmartCenter Server</td>
</tr>
</tbody>
</table>

The FW1_mgmt service is a TCP service on port 258.

4 Add rules to the Rule Base that allow the other control connections you need, (since you disabled them in step 2).

**SMART Clients**

**FIGURE 4-20** SMART Clients window

Specify the SMART Clients, that is, the remote computers from which administrators will be allowed to connect to the SmartCenter Server.
There is no need to define a SMART clients that is on the same machine as the SmartCenter Server. If no SMART clients are defined, you will be able to manage the SmartCenter Server you have just installed only from a SMART clients running on the same machine.

**To Add a SMART clients**

Enter the SMART clients's name and click on Add to add it to the list of allowed SMART clients. You can add SMART clients using any of the following formats:
- IP address (For example 1.2.3.4).
- Machine name (For example Alice, or Alice.checkpoint.com).
- Any (Any IP without restriction).
- IP1-IP2 (A range of addresses. For example 1.2.3.4-1.2.3.40).
- Wild cards (For example 192.140.150.* or *.checkpoint.com).

**Note:** When specifying SMART clients using any formats OTHER THAN the IP address, you must add an explicit rule in the Rule Base allowing the SMART clients to connect to the SmartCenter Server. For example:
- Source—Network Address Range, Destination—SmartCenter Server, Service—CPMI, Action—Accept.
- If specifying a SMART clients using a single IP address or machine name, an explicit rule is not required.

The connection between the SMART clients and the SmartCenter Server is enabled in SmartCenter by checking the Accept VPN-1 & FireWall-1 control connections property in the FireWall-1 Implied Rules page of the Global Properties window.

If the connection between the SMART clients and the SmartCenter Server passes through a VPN/FireWall Module, then the Security Policy must be re-installed on the VPN/FireWall Module so that the newly added SMART clients can connect to the SmartCenter Server.

**To Remove a SMART clients**

To remove a SMART clients from the allowed list, select it and click on Remove.
PKCS#11 Token

FIGURE 4-21: PKCS#11 Token window

Use this window to register a cryptographic token for use by VPN-1/FireWall-1, to see details of the token, and to test its functionality.

For configuration details, see the “PKCS#11 Token” on page 58 of Check Point Virtual Private Networks.
You are asked to enter random keystrokes. The random data collected in this session is used in various cryptographic operations.

Enter random characters containing at least six different characters. Do not type the same character twice in succession, and try to vary the delay between the characters. Keystrokes that are too fast or too similar to preceding keystrokes are ignored.

Keep typing until you hear a beep and the bar is full.
Certificate Authority

This option allows you to create an Internal Certificate Authority (ICA) on SmartCenter Server, and create a Secure Internal Communication (SIC) certificate for the SmartCenter Server.

SIC certificates are used to authenticate communication between Check Point communicating components, or between Check Point communicating components and OPSEC Applications.

Management FQDN

cpconfig tries to resolve the FQDN (fully qualified domain name) of the SmartCenter Server and supplies this as a default. If this is not the correct FQDN, change the contents of the Management FQDN field. This may be useful if there is a problem resolving the FQDN of the SmartCenter Server.

Specifying the correct FQDN ensures that the Certificate Revocation List (CRL) can be reliably retrieved by a communicating component, so that it can properly authenticate a certificate.

A fully qualified domain name consists of a host name and a domain name. For example, www.checkpoint.com is a fully qualified domain name.
The ICA needs the FQDN in order to insert the CRL Distribution Point correctly in every certificate it issues. Communicating components retrieve the CRL by reading the certificate and looking for the CRL Distribution Point. The location of the CRL distribution point is an HTTP address in the form http://FQDN/<CRL_filename>.

To see the location of the CRL applicable for a certificate, in SmartDashboard, edit the SmartCenter Server object, and in the VPN page, select the certificate and click Edit > View. The CRL Distribution Point is one of the fields in the certificate.

Secure Internal Communication

FIGURE 4-24 Secure Internal Communication window

The Secure Internal Communication window is used to establish trust between this machine and the Primary SmartCenter Server. Once trust is established this machine can communicate with other Check Point communicating components. Trust is established by creating a certificate on the SmartCenter Server and delivering it to this machine.

Where this is a machine with a dynamically assigned IP address (DAIP Module), the SmartCenter Server can push a certificate to the DAIP Module if the current IP address of the DAIP module is known when initializing SIC (in SmartDashboard, in the Communications window of the DAIP object).
For information about communications in a distributed environment, see “Secure Internal Communications for Distributed Configurations” on page 160 of the Check Point Getting Started Guide or page 48 of the Check Point SmartCenter Guide.

**To Initialize a Module for Communication**

1. To enable communication, enter here the same Activation Key as in SmartDashboard, in the **Check Point Gateway - General** page of the Module.
   Confirm this Activation Key in the **Confirm Password** field.

2. At a SMART Client, connect to the SmartCenter Server and open SmartDashboard. (In a Management High Availability configuration, connect to the Primary SmartCenter Server).

3. In SmartDashboard, create an object for the Module, and give it a name and an IP address.

   **Note**: If the Module has dynamic IP address, see “Defining a Module with a Dynamic IP Address” on page 482 of the Check Point SmartCenter Guide.

   The following explanation matches the Classic Mode of creating an object:
   a. Choose **Network Objects** from the **Manage** menu, and click on **New > Check Point Gateway**…
   b. In the **Check Point Gateway — General Properties** page fill in the Module name and IP address.
   c. Check the appropriate product.

4. Initialize the Module:
   a. In the **Check Point Gateway — General Properties** page, click **Communication…**
In the **Communication** window, enter the Activation Key — the SAME Activation Key as you entered when configuring the Module.

Confirm this Activation Key in the **Confirm Activation Key** field.

**Note** · For the next step to work, the SVN Foundation and the VPN-1/FireWall-1 services must be running on the Module, and there must be IP connectivity from the Management Server to the Module.

**C** Click **Initialize** to start the Module initialization process.

At this point a certificate is issued to the Module. It is signed, and securely transferred to the Module.

The Module status is reported in the **Trust State** field.

**Trust state**—Trust is established only after a certificate has been issued by the Internal Certificate Authority on the SmartCenter Server, and delivered to the Module.

If a Module is Initialized or Reset, the Trust state of the Module as reported in `cpconfig` may be different than the Trust state reported at the SmartDashboard.

**Note** the difference between the **Trust state** and the output of the **Test SIC Status** button in the SmartDashboard **Communication** window of the Module: The **Trust state** reflects the situation after Module initialization, that is, when an activation key is exchanged and certificate is sent to the Module. In contrast, **Test SIC Status** reflects the SIC status after the Module has the certificate.

The Trust State as reported in `cpconfig` in the **Secure Internal Communication** and in the SmartDashboard in the **Communication** window can be in one of three states:
- **Uninitialized** — The Module is not initialized and therefore cannot communicate because it has not received a certificate from the Internal Certificate Authority on the SmartCenter Server.

- **Initialized but trust not established** —
  
  At the Module, in `cpconfig`, in the **Secure Internal Communication** window, this means that a one-time password has been typed in but the Module has not yet received a certificate from the Internal Certificate Authority on the SmartCenter Server.

  In the SmartDashboard in the **Communication** window, this means that a certificate has been issued to this Module but has not been delivered, so trust (secure communication) cannot yet be established.

- **Trust established** — The trust between the Module and the SmartCenter Server has been established. The Module can communicate securely.

  Trust will be established and the Module will be able to communicate when the certificate is successfully delivered to the Module, the **Trust State is Trust established**, and the SIC name (or DN) of the Module is reported in the **General** page of the **Workstation Properties** window.

  **Note** - The setting up of SIC communication can be tracked by viewing the `$CPDIR\log\cpd.elg` log file on the Module.


Upon successful initialization the newly defined Module can securely communicate with any other certificate owner Module.

**To Reset the Trust State of a Module**

1. In the **Secure Internal Communication** window/menu, click or select **Reset**.

2. For the other half of this procedure, see “How to Reset the Trust State of the Module” on page 169.
The **Fingerprint** window shows the fingerprint of the SmartCenter Server. The fingerprint is a text string derived from the certificate of the SmartCenter Server. It is used to verify the identity of the SmartCenter Server being accessed via the SMART clients. You should compare this fingerprint to the fingerprint displayed in SmartCenter the first time a SMART client connects to this SmartCenter Server.

**Note** - In a Management High Availability configuration, you can view and save the Fingerprint. For the...
- primary SmartCenter Server — in the **Fingerprint** window once the ICA Initialization has succeeded (see FIGURE 21-13).
- secondary SmartCenter Server — in the **Secure Internal Communication** tab, if the Trust Status is **Trust Established**.

**How to Use the Fingerprint to Confirm the Identity of the SmartCenter Server**

1. In the **Fingerprint** window, click **Export to file** and save the file.
2. Take the file over to the SMART clients via some non-network means such as a diskette, or confirm the fingerprint of the SmartCenter Server by fax or telephone.
3. From a SMART client, make a first time connection to SmartCenter Server. The Fingerprint of a SmartCenter Server is displayed (see **FIGURE 21-14**).
FIGURE 4-27 Fingerprint of a SmartCenter Server as displayed at the SMART clients

4 Make sure the fingerprint of the SmartCenter Server is identical to the fingerprint displayed in the SMART clients.

Note - You should not make a first-time connection to a SmartCenter Server from a SMART clients, unless you have the SmartCenter Server fingerprint to hand, and are able to confirm it is the same as the fingerprint displayed in the SMART clients.

High Availability

FIGURE 4-28 High Availability window

Turn on the State Synchronization and the ClusterXL High Availability and Load sharing capability.
See Chapter 3, “ClusterXL in the Check Point FireWall-1 Guide” for information on how to configure a High Availability environment.

Interfaces

A ROBO Gateway is an object which inherits most of its properties and its policy from the Profile object to which it is mapped. Each ROBO gateway represents a large number of gateways, which subsequently inherit the properties stipulated by the Profile object.

Select the IP addresses that represent the interfaces defined for each object from the drop down list.

VPN-1 Accelerator Driver

This option turns on the VPN-1 Accelerator Driver. The VPN-1 Accelerator Driver is available on multiple CPU machines.

Changes to this setting only take effect after booting the machine.

SNMP Extension (Unix only)

Use this option to configure the SNMP daemon. The SNMP daemon enables the VPN/FireWall Module to export its status to external network management tools.

Automatic Start of Check Point Modules (Unix only)

Specify whether the VPN/FireWall Module will start automatically at boot time.

Secure Internal Communications for Distributed Configurations

Communicating Components

In a distributed configuration, communicating components such as the SmartCenter Server and the Modules are deployed on different computers.

Secure Internal Communication (SIC) secures communication between

- Check Point SVN components (such as SmartCenter Servers, SMART clients, VPN/FireWall Modules, Customer Log Modules, SecureConnect Modules, Policy Servers), and between
- Check Point SVN components and OPSEC applications.
Security Benefits

Securing communication allows you to be absolutely sure that
- a SMART Client is connecting to a SmartCenter Server to which it is authorized to connect,
- the Security Policy loaded on a VPN/FireWall Module came from the SmartCenter Server, rather than a machine pretending to be the SmartCenter Server.
- data privacy and integrity have been maintained

Administrative Benefits

As well as enhancing security, SIC substantially eases the administration of large installations by reducing the number of configuration actions. It is no longer necessary to perform `fw putkey` operations between pairs of communicating components. Instead, it is simply a matter of performing a simple initialization procedure for each component from the SmartDashboard.

SIC Certificates

Secure Internal Communication for Check Point SVN components uses:
- Certificates for authentication, and
- Standards-based SSL for encryption.

SIC certificates uniquely identify Check Point-enabled machines or OPSEC applications across the VPN-1/FireWall-1 system. For example, a computer may have one certificate for Check Point products and a certificate for each OPSEC application. Certificates are created by the Internal Certificate Authority (ICA) on the SmartCenter Server for communicating components managed by the SmartCenter Server.

For information about certificates and their benefits, see “Certificates” on page 23 of Check Point Virtual Private Networks.

Note - VPN certificates (those used for IKE for example), and SIC certificates are used for different purposes and are managed differently.
- VPN certificates are managed from the VPN page of the VPN-1 installed object (see “Workstation Encryption Properties” on page 94 of Check Point Virtual Private Networks)
- SIC certificates are managed from the Communication window on the General page of any Check Point installed object (see “Enabling Communication between Modules” on page 22).

Consider the distributed VPN-1/FireWall-1 configuration depicted in FIGURE 0-1.
Communications between the SmartCenter Server(s) and Modules

The ICA creates a certificate for the SmartCenter Server machine during the SmartCenter Server installation. The ICA itself is created automatically during the installation procedure (see “Installing VPN-1/FireWall-1 (Windows)” on page 115 or “Installing VPN-1/FireWall-1 (UNIX)” on page 123 of the Check Point Getting Started Guide).

Certificates for the VPN/FireWall Modules and any other communicating component are created via a simple initialization from the SmartDashboard (see “Enabling Communication between Modules” on page 22). Upon initialization, the ICA creates, signs, and delivers a certificate to the communicating component. Every Module can verify the certificate for authenticity.

Communications between the SmartCenter Server(s) and Modules

Communications between a SmartCenter Server and its Modules are authenticated using their certificates, and according to a policy specified in a policy file on each machine. Communication using certificates will take place provided that the communicating components

- are of the appropriate version
- agree on the authentication method
- agree on the encryption method
The SmartCenter Server and the Modules are identified by their SIC name (also known as the DN).

Full backward compatibility allows a SmartCenter Server to communicate with a VPN/FireWall Module of version 4.1 or earlier using the legacy shared secret (fw putkey) method. The two communicating components use the password to create a shared key which they exchange and use to set up an encrypted secure link between them.

Communications Between the SmartCenter Server and the SMART Client

On the SmartCenter Server, the SMART client must be defined as being authorized to connect to the SmartCenter Server.

For information on how to do this, see “Administrators” on page 136 (for Windows) or “Administrators” on page 154 (for Unix) of the Check Point Getting Started Guide.

When invoking the SmartDashboard on the SMART client, the VPN-1/FireWall-1 administrator is asked to identify himself and to specify the IP address of the SmartCenter Server.

The SMART client initiates an SSL based connection with the SmartCenter Server. The SmartCenter Server verifies that the Client’s IP address belongs to an authorized SMART client, and sends back its certificate.

Upon authenticating the SmartCenter Server's certificate, the administrator is asked to verify that the right SmartCenter Server is connected. Verification is done using the SmartCenter Server fingerprint (see the Check Point Getting Started Guide “How to Use the Fingerprint to Confirm the Identity of the SmartCenter Server” on page 151). The fingerprint is a text string that represents a certain hash value computed from the SmartCenter Server certificate.

Once the administrator approves the identity of the SmartCenter Server, the administrator’s name and password are securely sent to the SmartCenter Server.

The administrator’s name and password are used to authenticate the user as a Policy Management authorized user.
Enabling Communication between Modules

**Note**: Where a reference is made to a Module, it applies equally to all communicating components (see "Communicating Components" on page 19), including VPN/FireWall Modules and OPSEC applications.

### Enabling Communication — New Module Registration

After installing a new Module, proceed as follows:

1. **At the Module machine**, use `cpconfig` to initialize the Module:
   
   In the Secure Internal Communication tab (for Windows, see FIGURE 0-2) or option (for Unix) of the `cpconfig` configuration utility of the Module, enter and confirm the one-time password.

   ![Secure Internal Communication window (for Windows)](image)

2. **At a SMART Client**, connect to the SmartCenter Server and open SmartDashboard. (In a Management High Availability configuration, connect to the Primary SmartCenter Server).

---

Chapter 4  Installing and Configuring VPN-1/FireWall-1  99
3 In SmartDashboard, create an object for the Module, and give it a name and an IP address.

Note - If the Module has dynamic IP address, see “Defining a Module with a Dynamic IP Address” on page 482 of the Check Point SmartCenter Guide.

The following explanation matches the Classic Mode of creating an object:

a Choose Network Objects from the Manage menu, and click on New > Check Point Gateway...

b In the Check Point Gateway — General Properties page fill in the Module name and IP address.

c Check the appropriate product.

4 Initialize the Module:

a In the Check Point Gateway — General Properties page, click Communication...

FIGURE 4-31 Communication Window

b In the Communication window, enter the Activation Key — the SAME Activation Key as you entered when configuring the Module.

Confirm this Activation Key in the Confirm Activation Key field.

Note - For the next step to work, the SVN Foundation and the VPN-1/FireWall-1 services must be running on the Module, and there must be IP connectivity from the Management Server to the Module.
Click **Initialize** to start the Module initialization process. At this point a certificate is issued to the Module. It is signed, and securely transferred to the Module.

The Module status is reported in the **Trust State** field.

**Trust state**—Trust is established only after a certificate has been issued by the Internal Certificate Authority on the SmartCenter Server, and delivered to the Module.

If a Module is Initialized or Reset, the Trust state of the Module as reported in `cpconfig` may be different than the Trust state reported at the SmartDashboard.

Note the difference between the **Trust state** and the output of the **Test SIC Status** button in the SmartDashboard *Communication* window of the Module: The **Trust state** reflects the situation after Module initialization, that is, when an activation key is exchanged and certificate is sent to the Module. In contrast, **Test SIC Status** reflects the SIC status after the Module has the certificate.

The Trust State as reported in `cpconfig` in the *Secure Internal Communication* and in the SmartDashboard in the *Communication* window can be in one of three states:

- **Uninitialized** — The Module is not initialized and therefore cannot communicate because it has not received a certificate from the Internal Certificate Authority on the SmartCenter Server.

- **Initialized but trust not established** —
  
  At the Module, in `cpconfig`, in the *Secure Internal Communication* window, this means that a one-time password has been typed in but the Module has not yet received a certificate from the Internal Certificate Authority on the SmartCenter Server.

  In the SmartDashboard in the *Communication* window, this means that a certificate has been issued to this Module but has not been delivered, so trust (secure communication) cannot yet be established.

- **Trust established** — The trust between the Module and the SmartCenter Server has been established. The Module can communicate securely.

Trust will be established and the Module will be able to communicate when the certificate is successfully delivered to the Module, the **Trust State is Trust established**, and the SIC name (or DN) of the Module is reported in the *General* page of the *Workstation Properties* window.

**Note** - The setting up of SIC communication can be tracked by viewing the `\%CPDIR\%log\cpd.elg` log file on the Module.
5 Install the Security Policy on the Module.
Upon successful initialization the newly defined Module can securely communicate with any other certificate owner Module

Enabling Communication — Upgrading 4.1 Modules

Start or continue from Step 1 or Step 2, as appropriate:

Note -
- You can upgrade to NG only from version 4.1 and higher.
- The version of the SmartCenter Server must always be at least the version of the VPN/FireWall Module with the highest version.
- The trust relationship between the management and module is maintained at all stages of the upgrade. The old trust relationship, based on a shared secret is converted to one based on proving identity using certificates.

1 SmartCenter Server Version: 4.1 to NG
Module Version: 4.1
Upgrade the SmartCenter Server version to NG. For details, see “Installing VPN-1/FireWall-1 (Windows)” on page 115 or “Installing VPN-1/FireWall-1 (UNIX)” on page 123 of the Check Point Getting Started Guide.
The SmartCenter Server can manage version 4.1 Modules. At this point the trust relationship between the Management and Modules is based on the shared secret generated prior to the SmartCenter Server upgrade.

2 SmartCenter Server Version: NG
Module Version: Upgrade from 4.1 to NG
Upgrade the Module version to NG. For details, see “Installing VPN-1/FireWall-1 (Windows)” on page 115 or “Installing VPN-1/FireWall-1 (UNIX)” on page 123 of the Check Point Getting Started Guide.
It is perfectly possible for a SmartCenter Server to manage both version 4.1 and NG Modules. The Modules can be upgraded whenever convenient.

3 From the SmartDashboard, open the General page of the Check Point Gateway window of the Module (FIGURE 0-4) and change the Version to NG.
At this point a certificate is issued to the Module. It is signed, and securely transferred to the Module. The Module status is reported in the Trust State field.

**Trust state**—Trust is established only after a certificate has been issued by the Internal Certificate Authority on the SmartCenter Server, and delivered to the Module.

If a Module is Initialized or Reset, the Trust state of the Module as reported in `cpconfig` may be different than the Trust state reported at the SmartDashboard.

Note the difference between the Trust state and the output of the Test SIC Status button in the SmartDashboard Communication window of the Module: The Trust state reflects the situation after Module initialization, that is, when an activation key is exchanged and certificate is sent to the Module. In contrast, Test SIC Status reflects the SIC status after the Module has the certificate.

The Trust State as reported in `cpconfig` in the Secure Internal Communication and in the SmartDashboard in the Communication window can be in one of three states:
- **Uninitialized** — The Module is not initialized and therefore cannot communicate because it has not received a certificate from the Internal Certificate Authority on the SmartCenter Server.

- **Initialized but trust not established** —
  At the Module, in `cpconfig`, in the Secure Internal Communication window, this means that a one-time password has been typed in but the Module has not yet received a certificate from the Internal Certificate Authority on the SmartCenter Server.

  In the SmartDashboard in the Communication window, this means that a certificate has been issued to this Module but has not been delivered, so trust (secure communication) cannot yet be established.

- **Trust established** — The trust between the Module and the SmartCenter Server has been established. The Module can communicate securely.

  The Module will be able to communicate when the Trust State is Trust Established. The Module name (or DN) of the Module is reported in the General page of the Check Point Gateway window.

  This sends the certificate to the Module, and completes the SIC configuration of the Module.


### Resetting the Trust State of the Module

During the operational lifetime of VPN-1/FireWall-1, it may be required to revoke a Module's certificate by resetting the Module trust state. This is needed when the security of the Module has been breached, and it is suspected that its private key has been stolen. It is also needed when a decision has been taken to cease the operation of a Module. Whatever the reason, in such a case all other Modules must be notified that the Module's certificate is no longer valid.

Modules are informed of Modules with invalid certificates through a certificate revocation list (CRL) that is issued and signed by the Internal Certificate Authority (ICA) on the SmartCenter Server. A CRL is a file containing the serial numbers of all revoked certificates. Every Module caches a CRL so that it can deny connection from an imposter if the latter uses an old certificate already listed in its CRL.

As a result of the revocation, the ICA issues a new CRL with the serial number of the revoked Module's certificate added. The new CRL bears a new date and time of issue. The SIC protocol ensures fast propagation to all Modules. Part of the protocol
negotiation between any two Modules is CRL checking. If one side of the connecting parties holds a newer CRL, then the other side replaces its own CRL with the newer one.

To allow a Module that has been reset to communicate, the Module must be re-initialized.

**How to Reset the Trust State of the Module**

To reset the trust state of a Module, proceed as follows:

**Warning**
- For the reset operation to be complete, you must reset the trust state of a Module both in the SmartDashboard and in the Module's `cpconfig` configuration utility.
- Modules other than the SmartCenter Server will receive the new CRL the next time a SIC connection is made (such as when the Security Policy is installed on the Modules).

1. **Reset the Trust State in the SmartDashboard:**
   - a. At a SMART client, connect to the SmartCenter Server and open the SmartDashboard.
   - b. In the SmartDashboard, open the Module's **Gateway Properties** page, and click **Communication**...
   - c. In the **Communication** window, click **Reset**.

   You can also reset a Module by deleting the Module object from the SmartDashboard. Proceed as follows:
   - a. In the SmartDashboard, choose **Network Objects** from the **Manage** menu.
   - b. Select the Module object, and click **Remove**.

2. **Reset the Trust State at the Module machine:**
   - a. At the Module machine, open the `cpconfig` configuration utility of the Module.
   - b. In the **Secure Internal Communication** tab click **Reset**.

3. **Install the Security Policy on all Modules.** This also deploys the new CRL to all Modules.
How to Re-establish Trust for the Module

1. Reset the Module (see How to Reset the Trust State of the Module). If you deleted the Module object from the SmartDashboard:
   - At a SMART client, connect to the SmartCenter Server and open SmartDashboard. (In a Management High Availability configuration, connect to the Active SmartCenter Server.)
2. Continue from “Enabling Communication — New Module Registration, step a on page 23

SIC Automatic Renewal

SIC certificates are issued by default for five years from the date of issue. Prior to NG FP3, when SIC certificate expired, SIC for the Module had to be manually reset. As of NG FP3, SIC certificates are renewed automatically after 75% of the life of the certificate.

When the cpd process on the Module starts, it schedules a time when the certificate is to be renewed. When this time arrives, cpd requests a new certificate from the Internal Certificate Authority (ICA). When the new certificate is received, the Module moves the current SIC certificate to $CPDIR/conf/old_sic_cert.p12, renames the new certificate as $CPDIR/conf/sic_cert.p12, and resets SIC on the Module.

When the ICA gets a request to renew a SIC certificate, it issues the certificate and then schedules an event to revoke the old SIC certificate after seven days. This is done in case the Module did not successfully complete the renew operation, and gives the Module seven days to complete the operation.

Frequently Asked Questions—Installing, Upgrading, Configuring

Question: How do I move VPN-1/FireWall-1 to another machine?

First of all, you must ensure that you have a valid license for the new machine. Once the license issue is resolved, the simplest procedure is as follows:

1. Install VPN-1/FireWall-1 on the new machine.

If your SmartCenter Server manages VPN/FireWall Modules on other machines, you must repeat the fwm putkey procedure for all the machines (see “Secure Internal Communications for Distributed Configurations).
2 Make a copy of the Security Policy files from the old machine.

For information on which files to backup, see “How do I back up my Security Policy?” on page 107.

3 Restore the Security Policy backup files (see step 2 above) to the new machine.

4 Start the GUI on the new machine to confirm that the Security Policy was successfully transferred.

5 If the new machine is the FireWalled gateway, then define the new machine as a gateway.

   In the new machine’s **Workstation Properties** window, check the **Gateway** flag.

6 Delete the old machine from the Network Object Manager.

   Alternatively, you can leave the old machine, but uncheck the **VPN-1 & FireWall-1 Installed** flag in its **Workstation Properties** window.

7 Install the Security Policy.

   The above procedure describes the simplest case: where the SmartCenter Server and VPN/FireWall Modules are on one machine, and the Security Policy is installed on gateways. If your configuration is more complicated, you will have to modify the procedure accordingly.

**Question: How do I back up my Security Policy?**

To back up your Security Policy, make copies of the following files:

**TABLE 4-3 Backing Up a Security Policy**

<table>
<thead>
<tr>
<th>to back up</th>
<th>make a copy of these files</th>
</tr>
</thead>
<tbody>
<tr>
<td>network objects</td>
<td>$FWDIR/conf/objects_5_0.C (on the SmartCenter Server)</td>
</tr>
<tr>
<td>Rule Base</td>
<td>• $FWDIR/conf/*.W</td>
</tr>
<tr>
<td></td>
<td>• $FWDIR/conf/rulebases.fws</td>
</tr>
<tr>
<td>user database</td>
<td>$FWDIR/database/fwauth.NDB*</td>
</tr>
</tbody>
</table>

**Question: What Objects are Carried Over from the Previous Version?**

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 (users and network objects)
- Key database
- R ule 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.

**Question: What files are modified during re-configuration?**

The following files are created modified during reconfiguration:

- control.map
- masters
- fwauth.keys
- fwaughtd.conf
- cp.license
- external.if (for VPN-1/FireWall-1/25, VPN-1/FireWall-1/50, etc.)

You must create and modify the loggers file manually.

**Question: Must I re-install the Security Policy after upgrading?**

After upgrading, VPN-1/FireWall-1 loses its state, so you must start the GUI and install the Security Policy.

**Question: If I change the IP address of a network object, when does the change take effect?**

You must re-install the Security Policy for the change to take effect.

When you re-install a Security Policy, VPN-1/FireWall-1 internal state tables are cleared, so there is the possibility that some connections may be lost, as follows:

- **FTP data connections**
  
  If you have an open FTP connection and the Security Policy is re-installed before the FTP server attempts to open the back connection, then the back connection will be rejected.

- **UDP connections**

- **TCP connections, in very rare circumstances**
  
  An open encrypted session will be dropped if the newly installed Security Policy allows the session to be unencrypted.

If you are concerned about losing these connections, then you should take care to re-install your Security Policy during off-peak hours.

**Question: If I have an NG management and a 4.1 or 4.0 Module, how do I re-establish communication between them?**

Version 4.0 and 4.1 VPN/FireWall Modules on hosts and gateways managed by an NG SmartCenter Server, validate communication between them using an authentication password that is used to set up a secure link.
For this to work, you must have installed the SmartCenter Server with backward compatibility.

If you have a NG management and a 4.1 or 4.0 Module, and you need to re-establish communication between them (e.g. after installing a new 4.1 Module or adding a log server to a Module) you need to use the `fwm putkey` authentication password (the “old way”). This is done using either

- the `cpconfig` configuration utility and SmartDashboard, or
- the command line

**Using cpconfig and SmartDashboard**

1. In the `cpconfig` configuration utility of the Version 4.x VPN/FireWall Module, go to the Masters Configuration tab and specify an authentication password.

2. Stop (`fwstop`) and start (`fwstart`) the Module.

3. In SmartDashboard, define the 4.x Module object and enter the same password in the Communication window of the Module object.

**Using fwm putkey from the command line**

For the configuration depicted in FIGURE 2-1 on page 46 of the Check Point Getting Started Guide in which BigBen is an NG SmartCenter Server, and Chelsea London and Paris are 4.0 or 4.1 hosts, you must provide the authentication passwords for three control links by performing `fwm putkey` as follows:

**TABLE 4-4 VPN-1/FireWall-1 distributed configuration - fwm putkey**

<table>
<thead>
<tr>
<th>from</th>
<th>to</th>
<th>and conversely, from</th>
<th>to</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigBen</td>
<td>Chelsea</td>
<td>Chelsea</td>
<td>BigBen</td>
</tr>
<tr>
<td>BigBen</td>
<td>London</td>
<td>London</td>
<td>BigBen</td>
</tr>
<tr>
<td>BigBen</td>
<td>Paris</td>
<td>Paris</td>
<td>BigBen</td>
</tr>
</tbody>
</table>

To do this (using the same password for all hosts), proceed as follows:

1. Login to BigBen (the SmartCenter Server) and enter the following command:

   ```bash
   fwm putkey -p <password> Chelsea London Paris
   ```
If you do not enter the password in the command line (using the `-p <password>` syntax), you will be prompted for the password twice, as follows:

```
fwm putkey Chelsea London Paris
Enter secret key: <password>
Again secret key: <password>
```

2 Login to Chelsea and enter the following command:

```
fwm putkey -p <password> BigBen
```

3 Stop (`fwstop`) and start (`fwstart`) the Module.

4 Login to London and enter the following command:

```
fwm putkey -p <password> BigBen
```

5 Stop (`fwstop`) and start (`fwstart`) the Module.

6 Login to Paris and enter the following command:

```
fwm putkey -p <password> BigBen
```

7 Stop (`fwstop`) and start (`fwstart`) the Module.

Alternatively, you can use a different password for every host pair, as follows:

1 Login to BigBen and enter the following commands:

```
fwm putkey -p <password1> Chelsea
fwm putkey -p <password2> London
fwm putkey -p <password3> Paris
```

2 Login to Chelsea and enter the following command:

```
fwm putkey -p <password1> BigBen
```

3 Stop (`fwstop`) and start (`fwstart`) the Module.

4 Login to London and enter the following command:

```
fwm putkey -p <password2> BigBen
```

5 Stop (`fwstop`) and start (`fwstart`) the Module.

6 Login to Paris and enter the following command:

```
fwm putkey -p <password3> BigBen
```

7 Stop (`fwstop`) and start (`fwstart`) the Module.
Only after you have done this will the four machines be able to communicate on the secure links.

**Note:** If you specify names (rather than IP addresses), all machines must have the same name resolution for the other side. In this example, all machines must resolve BigBen in the same way (to the same interface). You can use the \-n parameter for the fwm putkey command on the SmartCenter Server to ensure this. Alternatively, instead of a machine's name, you can specify its IP address (or a comma-separated list of the IP addresses of its different interfaces).

**Question:** Is SIC tolerant of Network Address Translation (NAT)? If there is a NAT device between the SmartCenter Server and the Module, will communication be affected?

SIC is completely tolerant of NAT because the SIC protocol is based on certificates and “SIC Names” and not on IP addresses. A NAT device between the SmartCenter Server and the Module will not have any effect on their ability to communicate using SIC.

**Question:** How do I prevent the fingerprint of a SmartCenter Server appearing the first time a SMART client connects to it?

1. On the SMART client machine, open the Registry Editor (on Windows machines, use Regedit).
2. Go to the Registry entry; HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Connection\5.0\Known Servers
3. Add a new DWORD Value with Name NewServerOK and the Value 1.

**Question:** How do I prevent the SMART client recognizing a SmartCenter Server to which it has already connected?

1. On the SMART client machine, open the Registry Editor (on Windows machines, use Regedit).
2. Go to the Registry entry; HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Connection\5.0\Known Servers
   This entry contains the Names and fingerprints of SmartCenter Servers that the SMART client recognizes.
3. Select the Name of the SmartCenter Server that the SMART client should no longer recognize.
4. Click Delete.

**Question:**
CHAPTER 5

VPN-1/FireWall-1 Tutorial

In This Chapter

Introduction ........................................ page 113
Building a Security Policy ....................... page 114
Network Address Translation ..................... page 142
Monitoring the Security Policy ................. page 144

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 5-1.

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 Check Point modules on each machine, as needed (see TABLE 5-1).

2. Define the network objects.
   The network objects are listed in TABLE 5-2 on page 115.
You do not have to define the individual hosts in localnet, because they will not be explicitly used in the Rule Base.

**TABLE 5-2** Network Objects

<table>
<thead>
<tr>
<th>object name</th>
<th>description</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>FWall</td>
<td>the VPN/FireWall Module (the gateway), which enforces the Security Policy and protects the network</td>
<td>(3 interfaces) le0 (to Internet) - 192.32.32.32 le1 (to DMZ) - 192.32.42.32 le2 (to localnet) - 199.199.199.32</td>
</tr>
<tr>
<td>localnet</td>
<td>the internal network</td>
<td>199.199.199.0</td>
</tr>
<tr>
<td>DMZ</td>
<td>the DeMilitarized Zone — where the public servers are located</td>
<td>192.32.42.0</td>
</tr>
<tr>
<td>MailServer</td>
<td>provides mail services</td>
<td>192.32.42.102</td>
</tr>
<tr>
<td>FTPServer</td>
<td>provides FTP services</td>
<td>192.32.42.103</td>
</tr>
<tr>
<td>HTTPServer</td>
<td>provides HTTP (Web) services</td>
<td>192.32.42.104</td>
</tr>
</tbody>
</table>

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 136).

4 Define a Rule Base.

5 Install the Rule Base (Security Policy) on the VPN/FireWall Module machine, which will enforce the Security Policy.
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

The configuration is shown in FIGURE 5-1 on page 114. Installation instructions are given in Chapter 4, “Installing and Configuring VPN-1/FireWall-1.”

Install VPN-1/FireWall-1 in the following sequence:

1. Install the VPN/FireWall Module on FWall.

   When you configure FWall immediately after the installation, define Hatter as FWall’s Master.

2. Install the SMART Clients on Queen.

3. Install the SmartCenter Server on Hatter.

   When you configure Hatter immediately after the installation, define FWall as Hatter’s remote VPN/FireWall Module.

4. On Hatter, define Queen as a SMART Clients.

5. On Hatter, define the administrators who will be allowed to manage the Security Policy.

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 SMART Clients

Start the Check Point SMART Client GUI (from Start > Programs > Check Point Smart Clients > SmartDashboard). The Welcome to Check Point SmartDashboard window (FIGURE 5-2) is displayed.

FIGURE 5-2 Welcome to Check Point SmartDashboard window

Enter your user name, password and the name of the server to which to connect. Then click OK.

The Check Point SmartDashboard window is opened, showing an empty Security Policy Rule Base (FIGURE 5-3).
FIGURE 5-3 VPN-1/FireWall-1 SmartDashboard window (Security Dashboard)

The SmartDashboard window’s title shows the name of the Policy currently displayed. Depending on your license (the VPN-1/FireWall-1 features your SmartCenter Server is licensed to implement), you will see some or all of the following tabs in the SmartDashboard window:

- **Security Policy**
  

- **Address Translation**

  The Address Translation Rule Base is described in Chapter 2, “Network Address Translation (NAT)” of Check Point FireWall-1.
The Address Translation Rule Base is described in Chapter 2, “Network Address Translation (NAT)” of Check Point FireWall-1.

- **VPN Manager**
  The VPN Manager tab is described in the book Check Point Virtual Private Networks.

- **Desktop Security Policy**
  The SecureClient Policy is described in the book Check Point SecureClient User Guide.

- **WebAccess**
  The Web Access tab is described in the book Check Point UserAuthority.

### Defining the Network Objects

**Network Objects**

The network objects in the example configuration are listed in TABLE 5-2 on page 115.

**Note** - There is no need to define the Primary SmartCenter Server (Hatter in this example) as an network object in the Check Point database, unless you wish to explicitly refer to it in the Security Policy.

Usually, there is no need to refer to the SmartCenter Server in the Security Policy. Secure communication is automatically established between the SmartCenter Server and all the Check Point Modules (VPN/FireWall Module, FloodGate Module, etc.) defined in its database.

In contrast, you must explicitly define all the Check Point Module machines.
**Gateway — FWa11**

1. Open the **Gateway Properties** window (FIGURE 5-7).

   TABLE 5-3 lists several ways to open the **Gateway Properties** window:

### TABLE 5-3 Creating a new gateway

<table>
<thead>
<tr>
<th>from the ...</th>
<th>... proceed as follows to open the Gateway Properties window (FIGURE 5-7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage menu</td>
<td>• From the Manage menu, choose Network Objects.</td>
</tr>
<tr>
<td></td>
<td>• In the Network Objects window, click New and select Check Point &gt; Gateway from the menu.</td>
</tr>
<tr>
<td>objects toolbar</td>
<td>If the objects toolbar is not visible, choose View &gt;</td>
</tr>
<tr>
<td></td>
<td>Toolbars &gt; Objects from the menu.</td>
</tr>
<tr>
<td></td>
<td>• Select ▼ from the toolbar.</td>
</tr>
<tr>
<td></td>
<td>• In the Network Objects window click New and select Check Point &gt; Gateway from the menu.</td>
</tr>
<tr>
<td>Network Objects tree</td>
<td>• Click ▽ in the object tree tabs to display the Network Objects tree.</td>
</tr>
<tr>
<td></td>
<td>• Right-click Network Objects in the Network Objects tree and select Check Point &gt; New &gt; Gateway, or</td>
</tr>
<tr>
<td></td>
<td>• Right-click Check Point in the Network Objects tree and select New &gt; Gateway</td>
</tr>
</tbody>
</table>

**Note** - See TABLE 5-4 on page 183 of *Check Point SmartCenter Guide* for an explanation of the different network object types (including Check Point objects).

The first time you create a gateway, you will be asked whether you want to create it using the wizard or the classical method.
2 Select **Simple mode (wizard)**.

3 Check **Don't show this dialog again**.

4 In the first wizard window (FIGURE 5-5) fill in the gateway's name and IP address according to TABLE 5-4.

FIGURE 5-5 FWall — first gateway creation wizard window
In the next wizard window (FIGURE 5-6), check **Edit gateway’s properties**.

**FIGURE 5-6** FWall — last gateway creation wizard window

---

**TABLE 5-4** FWall — FWall’s properties window — first wizard window

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>FWall</td>
<td>This is the name by which the object is known on the network; the response to the <em>hostname</em> command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.32.32</td>
<td>This is the interface associated with the host name in the DNS — get this by clicking <em>Get Address</em>. For gateways, this should always be the IP address of the external interface.</td>
</tr>
<tr>
<td>Check Point products installed</td>
<td>Select <em>VPN-1 Pro</em> and <em>FireWall-1</em></td>
<td></td>
</tr>
</tbody>
</table>

5. In the next wizard window (FIGURE 5-6), check **Edit gateway’s properties**.

**FIGURE 5-6** FWall — last gateway creation wizard window

---

6. Click **Finish**.

The **General** page of FWall’s **Gateway Properties** window (FIGURE 5-7) is displayed.
7 Fill in the data in FWall’s **General** page as shown in **TABLE 5-5**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Optional.</td>
<td>This is the text that is displayed at the bottom of the <strong>Network Objects</strong> window when this object is selected</td>
</tr>
<tr>
<td>Dynamic Address</td>
<td>Not checked.</td>
<td>This field is checked only for Modules whose IP addresses are dynamically assigned, for example, by DHCP.</td>
</tr>
<tr>
<td>Secure Internal</td>
<td>See step 8 below.</td>
<td>The procedure outlined in step 8 in below establishes a secure communication channel between Check Point Modules.</td>
</tr>
</tbody>
</table>

8 Click **Communication**.

The **Communication** window (FIGURE 5-8) is displayed.
In the **Communication** window, enter the one-time password that will be used to secure the first communication between the SmartCenter Server (Hatter) and FWall. Enter the password twice, in **Activation Key** and then again in **Confirm Activation Key**.

The password must be the same password you entered for FWall when you configured FWall directly after installing the VPN/FireWall Module on it, in the **Secure Internal Communication** tab.

**10 Click **Initialize**.**

At this point, the SmartCenter Server issues a certificate for FWall, signs it, and securely transfers it to FWall. This process is known as establishing a trust relationship between the SmartCenter Server and the Module.

If **Trust State** is **Trust Established**, then the operation was successful and Hatter and FWall can securely communicate. If **Trust State** is any other value, then trust was not successfully established and Hatter and FWall cannot communicate securely.

For more information, including what to do if trust is not successfully established, see “Secure Internal Communications for Distributed Configurations” on page 19.

**11 Click **Close.**

**Add Interfaces**

**12 Click **Topology** (in the tree on the left side of the **Gateway Properties** window) to display the **Topology** page (FIGURE 5-9).**
FIGURE 5.9 Gateway Properties window - Topology page

![Gateway Properties window](image)

No interfaces are shown, since you have not yet defined any.

13 Click **Get Topology**.

VPN-1/FireWall-1 automatically calculates Fwall’s topology based on its routing tables and displays the results in the **Get Topology Results** window (FIGURE 5-10).
14 Confirm that the information displayed in the **Get Topology Results** window is correct and if it is, click **Accept**.

For information on the **Get Topology Results** window, and on how to define interfaces manually, see “Automatic Topology Discovery and Definition” on page 188 of *Check Point SmartCenter Guide*.

15 After you have defined all three interfaces, you can see them in the **Topology** page of the **Gateway Properties** window (FIGURE 5-11).
Authentication Methods

16 Open the Authentication page of the Gateway Properties window (FIGURE 5-12) by clicking Authentication in the tree in the left pane.
In the Authentication tab of the Gateway Properties window, select the Authentication methods that FWa11 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 5-6.

**TABLE 5-6 Other Network Objects**

<table>
<thead>
<tr>
<th>object name</th>
<th>type</th>
<th>IP address</th>
<th>Net Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>localnet</td>
<td>network</td>
<td>199.199.199.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DMZ (External Services Network)</td>
<td>network</td>
<td>192.32.42.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>MailServer</td>
<td>host</td>
<td>192.32.32.102</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>FTPServer</td>
<td>host</td>
<td>192.32.32.103</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>HTTPServer</td>
<td>host</td>
<td>192.32.32.104</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**Networks**

To create a network, open the Network Properties window (FIGURE 5-13).

**TABLE 5-7 Creating a new network**

<table>
<thead>
<tr>
<th>from the ...</th>
<th>... proceed as follows to open the Network Properties window (FIGURE 5-13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage menu</td>
<td>· From the Manage menu, choose Network Objects.</td>
</tr>
<tr>
<td></td>
<td>· In the Network Objects window, click New and choose Network from the menu.</td>
</tr>
<tr>
<td>objects toolbar</td>
<td>If the objects toolbar is not visible, choose View &gt; Toolbars &gt; Objects from the menu.</td>
</tr>
<tr>
<td></td>
<td>· Select Network from the toolbar.</td>
</tr>
<tr>
<td></td>
<td>· In the Network Objects window, click New and choose Network from the menu.</td>
</tr>
<tr>
<td>Network Objects tree</td>
<td>· Click in the object tree tabs to display the Network Objects tree.</td>
</tr>
<tr>
<td></td>
<td>· Right-click Network Objects in the Network Objects tree and choose New &gt; Network, or</td>
</tr>
<tr>
<td></td>
<td>· Right-click Networks in the Network Objects tree and choose New Network.</td>
</tr>
</tbody>
</table>
localnet

FIGURE 5-13 shows the **Network Properties** window after entering the data for localnet.

![Network Properties window - localnet](image)

TABLE 5-8  localnet — Network Properties window — General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>localnet</td>
<td>This is the network’s name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>199.199.199.0</td>
<td></td>
</tr>
<tr>
<td>Net Mask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>internal localnet</td>
<td>This is the text that is displayed at the bottom of the <strong>Network Objects</strong> window when this object is selected.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Included</td>
<td>Consider the network’s broadcast IP address as being part of the network.</td>
</tr>
</tbody>
</table>

DMZ

FIGURE 5-14 shows the **Network Properties** window after entering the data for the **External Services Network, DMZ**.
Defining the Network Objects

FIGURE 5-14 Network Properties window - DMZ

Network Properties window - DMZ

TABLE 5-9 DMZ — Network Properties window — General tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>DMZ</td>
<td>This is the network’s name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.42.0</td>
<td></td>
</tr>
<tr>
<td>Net Mask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>DMZ</td>
<td>This is the text that is displayed at the bottom of the Network Objects window when this object is selected.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Included</td>
<td>Consider the network’s broadcast IP address as being in the network.</td>
</tr>
</tbody>
</table>

Hosts (Servers)

19 To define a host object, click New and choose Check Point > Host from the menu.

The General page of the Gateway Properties window is displayed.

Mail Server

FIGURE 5-15 shows the General page of the Gateway Properties window for the Mail Server.
Define FTP Server and HTTP Server in the same way.

TABLE 5-10 Mail Server — Gateway Properties window — General page

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>MailServer</td>
<td>This is the name by which the object is known on the network; the response to the hostname command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.42.102</td>
<td>Get this by clicking Get Address.</td>
</tr>
<tr>
<td>Comment</td>
<td>Mail Server</td>
<td>This is the text that is displayed at the bottom of the Network Objects window when this object is selected.</td>
</tr>
<tr>
<td>Dynamic Address</td>
<td>Do not check this field.</td>
<td>This field is checked only for Modules whose IP addresses are dynamically assigned, for example, by DHCP.</td>
</tr>
<tr>
<td>Check Point products</td>
<td>Do not check this field.</td>
<td>No Check Point products are installed on this machine.</td>
</tr>
</tbody>
</table>

20 Define FTP Server and HTTP Server in the same way.
FTP Server

FIGURE 5-16 shows the General page of the Gateway Properties window for the FTP Server.

FIGURE 5-16: Host Properties window — FTP Server
TABLE 5-11 FTP Server — Gateway Properties window — General page

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>FTPServer</td>
<td>This is the name by which the object is known on the network; the response to the <code>hostname</code> command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.42.103</td>
<td>Get this by clicking <code>Get Address</code>.</td>
</tr>
<tr>
<td>Comment</td>
<td>FTP Server</td>
<td>This is the text that is displayed at the bottom of the <code>Network Objects</code> window when this object is selected.</td>
</tr>
<tr>
<td>Dynamic Address</td>
<td>Do not check this field.</td>
<td>This field is checked only for Modules whose IP addresses are dynamically assigned, for example, by DHCP.</td>
</tr>
<tr>
<td>Check Point products</td>
<td>Do not check this field.</td>
<td>No Check Point products are installed on this machine.</td>
</tr>
</tbody>
</table>

HTTP Server

FIGURE 5-17 shows the General page of the Gateway Properties window for the HTTP Server.
FIGURE 5-17 Host Properties window — HTTP Server

TABLE 5-12 HTTP Server — Gateway Properties window — General page

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>HTTPServer</td>
<td>This is the name by which the object is known on the network; the response to the hostname command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.42.104</td>
<td>Get this by clicking Get Address.</td>
</tr>
<tr>
<td>Comment</td>
<td>HTTP Server</td>
<td>This is the text that is displayed at the bottom of the Network Objects window when this object is selected.</td>
</tr>
<tr>
<td>Dynamic Address</td>
<td>Do not check this field.</td>
<td>This field is checked only for Modules whose IP addresses are dynamically assigned, for example, by DHCP.</td>
</tr>
<tr>
<td>Check Point Products</td>
<td>Do not check this field.</td>
<td>No Check Point products are installed on this machine.</td>
</tr>
</tbody>
</table>
Creating Users

21 To create users, display the Users window by choosing Users and Administrators from the Manage menu.

FIGURE 5-18 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

22 To create a new user, click New and choose User by Template > Standard User from the menu (FIGURE 5-19).

FIGURE 5-19 New User Object Menu

23 In the User Properties window (FIGURE 5-20), enter the data for the new user Bob.
Define Bob’s Authentication Method as **OS Password**.

This means that Bob must have an OS account on each machine on which he is authenticated.

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 5-21). This means that Alice does not need to have an OS account on a machine on which she is authenticated.
26 In Alice’s Authentication tab, click Change Password.

27 In the Change Password window, enter the password twice: once in Password and a second time in Confirm Password.

Create a New Group

28 To create a new group, click New and choose Group from the menu (FIGURE 5-19 on page 136).

The Group Properties window (FIGURE 5-23) is displayed.
FIGURE 5-23 Group Properties window

29 Enter the name of the group (Managers) and a comment (optional).

30 Next, select Alice and Bob and click 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
After defining your network objects and your users, you are now ready to define a Rule Base.

31 Click in the Toolbar to add a new rule to your currently empty Rule Base. A default “drop” rule (FIGURE 5-24) is displayed, which you must modify.
Add the rules, one after the other, until your Security Policy Rule Base looks like this:

**FIGURE 5-25 Complete Rule Base**

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>None</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>localnet</td>
<td>FIPServer</td>
<td>Any</td>
<td>accept</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>localnet</td>
<td>FIPServer</td>
<td>smtp</td>
<td>accept</td>
<td>None</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>MailServer</td>
<td>smtp</td>
<td>accept</td>
<td>None</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td>HTTPServer</td>
<td>HTTP</td>
<td>accept</td>
<td>None</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>6</td>
<td>Managed@Any</td>
<td>FIPServer</td>
<td>label</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>7</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Reject</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Tip** - When selecting an object from the long list in the **Add Object** window (FIGURE 5-26), you can speed up the selection by typing the first few letters of the object's name to position the list near the object.

**FIGURE 5-26 Add Object window — before and after typing “htt”**
Installing a Security Policy

To install the Security Policy on the gateway (FWall), choose Install from the Policy menu.

TABLE 5-13 Explanation of Rule Base

<table>
<thead>
<tr>
<th>Rule No.</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>This rule prevents anyone from accessing the gateway itself (&quot;stealth rule&quot; — hides the gateway).</td>
</tr>
<tr>
<td>2</td>
<td>This rule allows all internal hosts to go anywhere except FTPServer (note the negation of FTPServer in Destination).</td>
</tr>
<tr>
<td>3</td>
<td>This rule allows all internal hosts to FTP to FTPServer.</td>
</tr>
<tr>
<td>4</td>
<td>This rule allows unrestricted access to MailServer on DMZ.</td>
</tr>
<tr>
<td>5</td>
<td>This rule allows unrestricted access to HTTPServer on DMZ.</td>
</tr>
<tr>
<td>6</td>
<td>This rule specifies User Authentication for Managers group members on incoming TELNET to FTPServer.</td>
</tr>
<tr>
<td>7</td>
<td>This rule is the “none of the above” or “cleanup” rule; it rejects and logs all other communications.</td>
</tr>
</tbody>
</table>
Network Address Translation

In the following figure, another network (HRnet) has been added to the configuration.

FIGURE 5-27 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 5.28 HRnet Network Properties - General tab.

2 Click the **NAT** tab.

3 Check **Add Automatic Address Translation Rules**.

**Hide NAT**

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**.

**Static NAT**

To statically translate HRnet’s invalid addresses, select **Static** from the Translation Method drop down list and enter (in **First Valid IP Address**) the first IP address of the valid network addresses you have acquired.
Monitoring the Security Policy

Monitoring System Status

The **SmartView Status** window (FIGURE 5-30) presents a high-level view of operation and flow statistics for all FireWalled objects.

To display the **SmartView Status** window, double-click its icon on the desktop.
Viewing the Log

The SmartView Tracker 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 when a Security Policy is installed or uninstalled), are also logged.

The format of a log entries is determined by the log type specified in the rule's track field.
Introduction to Virtual Private Networks

In This Chapter

Overview

Overview

Certificates

VPN-1 Accelerator Card

VPN-1 SecuRemote

VPN-1 SecureClient

page 147

page 153

page 158

page 159

page 161

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 and read 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 the 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 SecuR emote Client and SecureClient software. For more information on the SecuR emote Client and SecureClient, see “VPN-1 SecuR emote” on page 159 and “VPN-1 SecureClient” on page 161 of Check Point Desktop Security Guide.

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.
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 6-1 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. Because different keys are used for encryption and decryption, they are known as asymmetric keys.

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

Alice wants to be sure that the message that Bob receives is the same message that she 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, Alice 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 Bob receives the message, he decrypts it, applies the same hash function and compares his hash result to Alice's hash result.

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

Authenticity

If Bob sends Alice a message, he 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 a 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) is an example of a commonly-used key exchange mechanism.

- the message encryption phase, in which the message is encrypted using the efficient private key negotiated in the first phase

  DES (Data Encryption Standard), AES (Advanced 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 must 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.

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 Public Key Infrastructure (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 SecuR emote 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

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” for more information.

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. On Windows NT, its installation is completely transparent, and no changes to the Security Policy or configuration files are required.

To install a VPN-1 Accelerator Card II on Windows 2000, proceed as follows:

1. Turn off your PC.
2. Physically install the card.
3. Turn off the PC.
   - Windows 2000 will automatically attempt to install a new hardware device.
4. In the Add/Remove Hardware Wizard window, click Close.
5. Install the CPacc package.
6. Reboot.
7. From the Windows Control Panel, select Add/Remove Hardware.
   - The Add/Remove Hardware Wizard appears.
Choose the Broadcom coprocessor as the device to install.

When prompted for the .inf file, browse for the cryptonet.inf file in the $FWDIR/conf directory.

When prompted for the .sys file, browse for the cryptonet.sys file in the %root/system32/drivers directory.

Reboot.

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

VPN-1 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, Windows NT, and Windows 2000 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.

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.

FIGURE 6-5 Virtual Private Network with a nomadic SecuRemote Client
SecuRemote supports IKE key exchange. Strong user authentication is supported by means of certificates, as well as a number of other authentication schemes (RADIUS, S/Key, password etc). Encryption schemes include (in accordance with export restrictions) triple DES or AES.

Additional Information
For information about configuring the SecuRemote Server (VPN/FireWall Module), see Chapter 1, “VPN-1 SecuRemote Server” of Check Point Desktop Client Guide.
For information about the SecuRemote Client software, see Chapter 2, “VPN-1 SecuRemote Client” of Check Point Desktop Client Guide.

VPN-1 SecureClient

Overview
Check Point VPN-1 SecureClient extends security to the desktop by enabling administrators to enforce a Security Policy on desktops — both inside and outside the LAN — and prevent unauthorized users from taking control of SecureClient or SecuRemote machine and penetrating the enterprise network via SecuRemote encrypted connections. In addition, the configuration of SecureClient machines can be verified and access denied to misconfigured SecureClient machines.

User-granular policies allow the administrator to exercise full access control over a desktop by creating a rule base and enforcing it on the client machine.

Check Point VPN-1 SecureClient consists of:
- VPN-1 SecureClient software with the Desktop Security feature installed
- a Policy Server from which the VPN-1 SecureClient obtains its Desktop Policies

Figure 6-6 shows how an intruder can take advantage of a SecuRemote machine to penetrate the internal enterprise network using a SecuRemote encrypted connection. This kind of attack can be prevented by enforcing Desktop Policies on the SecureClient and by performing Secure Configuration Verification (SCV) on the FireWalled gateway.
FIGURE 6-6 Taking unauthorized control of a SecuRemote machine

In FIGURE 6-7, 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. The FireWall on Tower both checks the identity of the user on BigBen and verifies that BigBen is securely configured.

FIGURE 6-7 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 page of the Global Properties window (FIGURE 1-1 on page 32 of Check Point Desktop Security Guide) (for SecureClients Version 4.1), or
• installing a Desktop Security Policy on Bridge.

• Encrypt connections between BigBen and FinanceNet.

This is configured by:

• defining FinanceNet to be in Tower’s encryption domain in the VPN page of Tower’s Workstation Properties window
• checking Exportable to SecuRemote in the Topology page of Tower’s Workstation Properties window (FIGURE 4-3 on page 68).

• Verify that BigBen is securely configured (SCV).

The proper configuration is defined in the Desktop Security page of the Global Properties window (FIGURE 1-1 on page 32 of Check Point Desktop Security Guide). The SCV policy can be extended through external SCV checks by editing the local.scv file in the $FWDIR\conf directory on the Management Server. The Client machine’s secure configuration is enforced 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 1-13 on page 28).

Example SecureClient Configuration

Network Configuration

FIGURE 6-8 depicts a configuration in which SecureClient provides security both inside and outside the LAN.
The configuration consists of:

- a Management Module (Louvre), on which the Desktop Security Policy is defined
- a FireWalled gateway (Paris), which enforces the Security Policy
- a Policy Server (Eiffel) from which Desktop Policies are 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 Secure Server is adequate.

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

**Note** - Network objects participating in the example configuration reflect the functional needs and do not necessarily represent actual machines. In reality, such components as Policy Server, VPN/FireWall Module and/or Management Station can reside on the same machine.
Installed Software Modules

TABLE 6-1 lists the VPN-1/FireWall-1 software installed on each of the machines in FIGURE 6-8.

<table>
<thead>
<tr>
<th>machine</th>
<th>installed VPN-1/FireWall-1 software module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Louvre</td>
<td>Management Module with a SecureClient user license</td>
</tr>
<tr>
<td>Paris</td>
<td>VPN/FireWall Module</td>
</tr>
<tr>
<td>Eiffel</td>
<td>VPN/FireWall Module and Policy Server with a Policy Server license</td>
</tr>
<tr>
<td>Metro</td>
<td>VPN/FireWall Module</td>
</tr>
<tr>
<td>desktops</td>
<td>SecureClient (SecuRemote with Desktop Security enabled)</td>
</tr>
<tr>
<td>Opera</td>
<td>SecureClient (SecuRemote with Desktop Security enabled)</td>
</tr>
</tbody>
</table>

Desktop Security can be enabled in the VPN-1 SecureClient when it is chosen during the installation.

Licensing

SecureClient needs two separate licenses:
- User license — general user license, installed on VPN-1/FireWall-1 Management Servers.
  The user license contains a maximum user count.
- Policy Server license, installed on each Policy Server’s VPN/FireWall Module.

For more licensing information, please contact the User Center at: http://www.checkpoint.com/usercenter
Virtual Private Network Tutorial

In This Chapter

Overview page 167
VPN Site and VPN Community page 168
Topology of a VPN Community page 168
Setting up Communities page 169
IKE/IPSec Properties page 175
Security Policy Conversion page 178
Integrating VPN and Access Control page 178
Configuration page 179

Overview

VPN configuration is considered to be a complicated task facing a system administrator while setting up a security system. Check Point VPN-1/FireWall-1's powerful, innovative and user-friendly management tools provide a simplified VPN setup mode that reduces the VPN configuration process to essentials, making it straightforward and simple.

The new approach involves understanding of a few basic terms (namely, VPN site and VPN community) which are discussed in detail below.
VPN Site and VPN Community

The management model enables the system administrator to directly define a VPN on a group of gateways. Each gateway and all or part of its protected domain constitute a new entity referred to as a VPN site (not to be confused with a site defined for SecuRemote/SecureClient). By grouping an unlimited number of VPN sites, the system administrator creates a VPN Community whose pre-defined properties are automatically applied to each Community member.

A VPN Community is a collection of VPN sites and the enabled VPN tunnels among them. The structure of a VPN Community is automatically translated into establishment of encrypted connections between its members. The administrator is relieved of the necessity to design and define encryption rules.

By defining a VPN Community, the administrator completes the VPN configuration. To create an all-encompassing security system, he or she will be merely required to define access control. Because the new management model totally separates VPN as a secure connectivity platform from access control, no access control related decision will affect the VPN Community, and vice versa.

This chapter presents a step-by-step description of how to define HQ and London as VPN Sites and incorporate them into a VPN Community.

Topology of a VPN Community

The topology of a VPN community is the collection of VPN links enabled by the VPN community. For instance in a star topology all the VPN connections from the satellites to the center of the community are enabled. Likewise, in a mesh topology every VPN link between any pair of community members is enabled. It is important to note that the VPN topology has no effect on clear connections between community members. For instance, if enabled by access control policy, a clear connection between two satellites of a star topology in a VPN community will be allowed.

There are two topologies available for VPN Communities:

- **mesh** — every VPN connection between any pair of members (VPN-1 gateways) is enabled in the community, and

- **star** — any VPN connection between satellite gateways and central gateways in the community is enabled. Star topology can have two flavors:
  - meshed center
  - not meshed center: no VPN connection is enabled among the central gateways in the Community.

The following principles are applied to VPN Communities:
1) A network object can participate in multiple communities.

2) A VPN link between any pair of VPN-1 gateways can be defined only once, thus it can be defined in a single VPN community.

3) In star topology, encrypted connection between two satellites cannot be established even if explicitly allowed by a rule. To create a VPN connection between these network objects, do one of the following:
   - add them to another star-configured VPN Community: one as central, the other as a satellite, or
   - add them to a mesh-configured VPN Community.

**Setting up Communities**

**Setting up a Mesh-Configured VPN Community**

To create a mesh-configured VPN Community, proceed as follows on the SmartCenter Server:

1. Make sure that NG Feature Pack 2 is installed on every gateway you wish to add to the Community.

2. Make sure that the gateways’ VPN Domains are properly defined on the Topology page of the Workstation Properties window.

3. Select \( \text{} \) from the toolbar. Alternatively, you can display the VPN Communities window by selecting VPN Communities from the Manage menu.

4. Right-click Intranet and select New>Meshed from the menu. The Meshed Community Properties window is displayed.

5. On the General page of the Meshed Community Properties window, enter Name and optionally Comment.

6. Click Participant Gateways. The Participant Gateways window is displayed.

7. Click Add to display the Participant Gateways window (FIGURE 7-3). The window contains the list of all the available NG FP 2 VPN-1 modules/sites.
Setting up Communities

Select the appropriate VPN-1 modules/sites (multiple selection is available) and click **OK**.

**Note**: The IKE/IPSec default properties defined per community will apply to all the community members. These properties can be modified, if necessary. For more information, see “IKE/IPSec Properties” on page 175.

**Setting up a Star-Configured VPN Community**

To create a star-configured VPN Community, proceed as follows on the SmartCenter Server:

1. Make sure that NG Feature Pack 2 is installed on every gateway you wish to add to the Community.

2. Make sure that the gateways’ VPN Domains are properly defined on the **Topology** page of the **Workstation Properties** window.

3. Select ![Intranet.png](image) from the toolbar. Alternatively, you can display the VPN Communities window by selecting **VPN Communities** from the **Manage** menu.

4. Right-click **Intranet** and select **New>Star** from the menu.

The **Star Community Properties** window is displayed (FIGURE 7-1):
5 On the General page of the **VPN Community Properties** window, enter **Name** and optionally **Comment**.

6 Define the Community traffic Security Policy by enabling or disabling **Accept all encrypted traffic**. The informative field below displays the tracking option for the encrypted traffic selected under **Community Default Rule** in the Log and Alert page of the **Global Properties** window (Figure 6-2 on page 92).

7 Click **Central Gateways**. The **Central Gateways** window is displayed.
Click **Add** to display the **Add Central Gateways** window (FIGURE 7-3). The window contains the list of all the gateways that can be added to the center of a star-configured Community, namely:

- all VPN-1 FP2 internal (internally managed) gateways (clusters, gateways with dynamic IP address)
- all external (externally managed) VPN gateways
- Check Point VPN-1 gateways (any version)
- interoperable devices

**Note** - When defining a SecuRemote Community, only internal gateways appear in the **Add Central Gateways** window.
Select the appropriate VPN-1 modules/sites (multiple selection is available) and click **OK**.

The selected VPN-1 modules/sites will appear in the **Participant Gateways** field of the **Central Gateways** page (FIGURE 7-3). To enable encrypted connection among the central gateways, select **Mesh center gateways**.

10 Click **Satellite Gateways**.

The **Satellite Gateways** window is displayed.

11 Click **Add** to display the **Add Satellite Gateways** window. The window contains the list of all the available NG FP 2 VPN-1 modules/sites.

12 Select the appropriate VPN-1 modules/sites (multiple selection is available) and click **OK**.

The selected VPN-1 modules/sites will appear in the **Participant Gateways** field on the **General** page of the **Star Community Properties** window (FIGURE 7-1).

13 Click **Do not encrypt** to select the services that will not be encrypted. To edit a selected service:

- double-click it or
- highlight it and press **Edit**.

The services passing in clear will not constitute part of the encryption domain. If a domain is selected in the **IF VIA** column of a rule, there will be no match by the unencrypted services.
14 Click **OK** to create a new star-configured Intranet community.

**Note** - The IKE/IPSec default properties defined per community will apply to all the community members. These properties can be modified, if necessary. For more information, see “IKE/IPSec Properties” on page 175.

**Remote Access Community**

The Remote Access Community allows defining gateways available to SecuRemote/SecureClient users and globally setting the SecuRemote/SecureClient users’ encryption properties.

The Remote Access Community is created by default. To edit it, proceed as follows:

1. In the VPN Communities list, double-click on Remote_Access_Community to display the **Remote Access Community Properties** window (FIGURE 7-4).

**FIGURE 7-4 Remote Access Community Properties window**

2. Edit the list of gateways on the **Participant Gateways** page. External gateways or interoperable devices cannot participate in the Remote Access Community.

3. Edit the list of user groups on the **Participant Users Group** page.
Remote Access VPN

The VPN properties for all the users of the Remote Access Community are globally defined in the VPN page of the Global Properties window. For detailed information, see Chapter 8, “Remote Access with VPN Clients.”

IKE/IPSec Properties

Some community-wide encryption properties (that apply to all VPN-1 modules/sites participating in this Community) are defined in the VPN Properties, Advanced Properties and Shared Secret pages of the Community Properties window.

VPN Properties

This page defines community-wide IKE and IPSec properties.

Perform key exchange encryption with — Specifies the encryption algorithm.

Perform data integrity with — Specifies the cryptographic checksum method to be used for ensuring data integrity.
Advanced Properties

This page defines advanced Community-wide VPN properties.

FIGURE 7-6 Advanced Properties page

IKE (Phase 1)

Use Diffie-Hellman group — This feature allows you to enhance security by selecting a longer Diffie-Hellman group.

Renegotiate IKE security associations every... minutes — The number of minutes after which IKE Security Associations expire.

For more information about IKE Properties, see Chapter 6, “VPN Properties”.

Perform key exchange encryption with — Specifies the encryption algorithm.

Perform data integrity with — Specifies the cryptographic checksum method to be used for ensuring data integrity.

IPSec (Phase 2)

Use Perfect Forward Secrecy — This feature ensures that an eavesdropper who uncovers a long-term encryption key will be unable to use it to decrypt traffic sent in the past.
Use Diffie-Hellman group — Select one of the groups. For more information, see “Diffie-Hellman Parameters Flexibility” on page 37.

Renegotiate IPSec security associations every... minutes — The number of minutes after which IPSec Security Associations expire.

Support Site to Site IP Compression — Enables stateless and reversible compression of IP packets.

Reset all VPN properties — Pressing this button will restore the default VPN properties, including those which do not appear in the Policy Editor.

NAT —

Disable NAT inside the VPN community — Enable this property to cancel the Network Address Translation (NAT) among the VPN Community participants.

**Shared Secret**

This page allows defining the IKE pre-shared secret for the external VPN modules. The internal VPN modules will continue using Internal CA certificates to negotiate VPN tunnels.

**FIGURE 7-7 Shared Secret page**
Select **Use only shared secret for all external members** and use the **Edit** button to define a shared secret for each external VPN module participating in the community.

**Security Policy Conversion**

The conversion tool from traditional mode to VPN communities is designed to modify a traditional Security Policy into a Simplified VPN Policy and vice versa while maintaining the Policy's integrity.

To run the converter, from the **Policy** menu select **Convert to** and choose either of the two options: **Simplified VPN** or **Traditional QoS**. A wizard opens which will guide you through the conversion process.

Note that if an installation target does not meet all the requirements for Communities participation (e.g. version or product), then this Module will not appear as a candidate in the list of Modules in the wizard's **VPN Policy configuration** page. That means that the VPN Policy may be false and installation may fail. In that case, it is highly important to specify the exact requirements for each community to allow the user checking why a module does not meet the requirement.

The converter is unable to convert the Auth+Encryption rules and drops the Encryption part, thereby deviding the rule of its original meaning.

**Integrating VPN and Access Control**

Being completely separated from the access control, the VPN Configuration can nevertheless be used for a significantly simpler and better tuned access control configuration.

When the access control configuration is based on VPN Communities:

- the **Encrypt** option is not available in any rule's **Action** or **ClientEncrypt** menu
- no VPN property is configurable in the **Rule Base** as opposed to Traditional mode where the encryption properties can be configured per rule
- the VPN Community can be added to the **Rule Base** in the IF VIA column. This column is an additional matching criteria in the Rule Base. When a community is added to the IF VIA column of a rule, a packet will match this rule only if it matches the rules of the community specified (passing through a VPN tunnel enabled by the community). For instance, this allows the administrator to create a rule similar to **FIGURE 7-8**.

**FIGURE 7-8 VPN Community-based access control rule**

| Any | Any | User_internet | Total | Accept |
Such a rule means that only encrypted traffic which passed via one of the VPN connections enabled by the defined community will be accepted. Traffic that matches the Source, Destination and Service of this rule, but not IF VIA will not match this rule rather than be dropped by this rule.

If *Any is selected in the IF VIA column (no Community is defined), the matching for this rule will rely only on the Source, Destination and Service, like in Traditional mode.

The IF VIA column allows multiple choice as well. When a log is required for a rule that includes a community in the IF VIA column, the log for matching traffic will state Encrypted.

**Configuration**

The following VPN configuration modes are available on the VPN-Pro page of the Global Properties window (FIGURE 7-9):
• **Simplified mode to all new Security Policies** — separates the VPN policy from the FireWall policies, as described in this chapter.

• **Traditional Mode to all new Security Policies** — disables VPN Communities and allows to use Regular mode only.

• **Traditional or Simplified mode per new Security Policy** — allows creating a regular Rule Base in addition to the Simplified VPN Rule Base.

If you selected **Simplified mode to all new Security Policies** or **Traditional or Simplified mode per new Security Policy** mode, you can check **Use VPN communities as a matching factor**.... If this option is enabled, the **If Via** column will be added to each newly created Rule Base. This column introduces an additional matching parameter by allowing you to define not only the source and destination of a connection, but also the VPN Community it passes through.
Index

Symbols

$FWDIR/log/cpmi_audit.txt file 78
$FWDIR/log/fw.adtlog file 78

Numerics

3Com 35
3DES 31

A

Accept VPN-1/FireWall-1 control connections property 83
access control logging 78
Administrator
   for SmartUpdate 80
   authenticating 83
AES 31, 149
asymmetric keys 150
authentication passwords synchronizing 108, 109

B

backup
   backing up a Security Policy 107
backward compatibility 43
Bay Networks 35
before installing VPN-1/FireWall-1 73

C

certificate
   security based on 157
cisco 35
cleanup rule 141
connections
   lost when Security Policy re-installed 108
control connection encrypting 97
control.map file modified during VPN-1/
   FireWall-1 reconfiguration 108

CP:license file modified during VPN-1/
   FireWall-1 reconfiguration 108
cpshared, see SVN Foundation

crl 156
description of 158
distribution point 158

desktop security
   enabling 165
diffie-hellman 150
digital certificates 31
digital signature 151
   displaying
SmartView Status Window 145
distributed configuration diagram 46
downtime
   minimizing while upgrading 45
dynamic NAT 29

E

embedded systems
   where to install license 71
encryption
   hardware acceleration 158
   hash, of message 151, 152

F

FireWalled, defined 31
FloodGate-1 36
FTP
   back connection 108
data connection 108
   PORT command 108
fw putkey 109
FW1_mgmt 84
fwauth.keys file
   modified during VPN-1/
   FireWall-1 reconfiguration 108
fwauthd.conf file
   modified during VPN-1/
   FireWall-1 reconfiguration 108

G

groups
   creating 42

H

hardware acceleration 158
HP-UX 181
disabling IP Forwarding 40

I

ICA 97
IKE
specifying the encrypting gateway’s IP address 41
supported by SecuR emote 161
supported by VPN-1
Accelerator Card 158
Inspection Module
defined 31
installation
overview 42
preparing the machine 39
installing
what to do before 39
installing a VPN-1/FireWall-1 license 71
Internal Certificate Authority, see ICA
IP addresses
when does changing take effect 108
IP Forwarding
disabling in the Solaris2 and HP-UX kernels 40
ISA KM P/OAKLEY 153

L

license
confirming that you are using correct licenses 73
installing 71, 72
obtaining 70
obtaining an evaluation license 71
removing old licenses 71
where to install 71
where to install for embedded systems 71
lmhosts file 41
logging
Access Control 78

M

Management Station
protecting 83
masters file
modified during VPN-1/FireWall-1 reconfiguration 108
mesh topology 168
mesh-configured VPN community setup 169
message hash 151, 152
monitoring system status 144
moving VPN-1/FireWall-1 to another machine 106

N

network object
creating 136, 138
none of the above rule 141
Nortel Networks 35

O

objects_5_0.C file 107

P

passport
comparison of certificate to 155
password
limitation on length in Windows 80
PK1 31
Provider-1 37
public key 150
trusting 153

R

re-configuration
files modified during 108
RSA 150

S

secret key
sharing 149
Secure Virtual Network 13
SecureClient
licensing 165
Security Policy
backing up 107
SIC
administrative benefits 96
certificates 96
configuring for a new Module 99
configuring for upgraded Modules 102
ICA 97
overview 95
security benefits 96
simplified VPN configuration 167
smart card
certificate stored on 156
SmartDefense 13
SmartUpdate
adding an administrator 80
Administrator permissions 80
SmartView Status window 144
SmartView Tracker 145
Solaris2
disabling IP Forwarding 40
star topology 168
star-configured VPN community setup 170
state tables
cleared when Security Policy re-installed 108
static NAT 29
stealth rule 141
SVN 13
SVN Foundation 45
symmetric key 149
system status
monitoring 144

topology 125
topology of VPN Communities 168
upgrading 43
changes during 44
managing previous versions 43
minimizing downtime
during 45
objects carried over from
previous version 44, 107
OS to Solaris 8 43
reinstalling Security Policy
after 108
VPN-1/FireWall-1 loses its state
after 46
UserAuthority 33

VPN Community
IKE/IPSEC properties 175
setup 168
VPN community 168
IKE/IPSEC properties 179
VPN configuration modes 179
VPN-1 Accelerator card
IKE 158
installing on Windows
2000 158
VPN-1 SecureServer 164
VPN-1/FireWall-1
uninstalling 73
VPN-1/FireWall-1
moving to another
machine 106
uninstalling (NT) 73
uninstalling (Unix) 73