EXHIBIT B



Check Point FireWall-1™ White Paper

Version 3.0 — June 1997
P/N 400-3000

http://www.checkpoint.com

Executive Summary

Expanding Internet technologies have redefined corporate approaches to internetworking and security. As the Internet becomes the forum for corporate communications and international commerce, enterprises require an innovative, comprehensive security solution.

Check Point Software Technologies Ltd. meets these growing connectivity needs with FireWall-1, the leading network security solution. FireWall-1 enables enterprises to define and enforce a single, comprehensive security policy while providing full, transparent connectivity. Utilizing Check Point's patented Stateful Inspection Technology and Open Platform for Secure Enterprise Connectivity (OPSEC), FireWall-1 integrates and centrally manages all aspects of network security.

This document describes the unique features of Check Point FireWall-1's Security Suite, and also presents OPSEC, an innovative framework that provides integrated management for FireWall-1 and third-party security applications. In addition, simple step-by-step procedures demonstrate how to build a FireWall-1 Rule Base to implement a security policy for both a simple and more detailed network configuration. Finally, performance data illustrates how FireWall-1's high levels of speed, transparency and efficiency deliver unmatched network security.

In This Document:

The Check Point FireWall-1 Security Suite	*page 3*
Configuring FireWall-1	*page 24*
Performance	*page 31*
Conclusion	*page 32*

Copyrights and Trademarks

© 1994–1997 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

FireWall-1, SecuRemote, Stateful Inspection, INSPECT, Check Point and the Check Point logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. Sun, SPARC, Solaris and SunOS are trademarks of Sun Microsystems, Inc. UNIX and OPEN LOOK are registered trademarks of UNIX System Laboratories, Inc. Cisco is a registered trademark of Cisco Systems, Inc. Bay Networks is a registered trademark of Bay Networks, Inc. Security Dynamics and SecurID are registered trademarks and ACE/Server is a trademark of Security Dynamics Technologies, Inc. HP is a registered trademark of Hewlett-Packard Company. Windows is a trademark and Microsoft is a registered trademark of Microsoft Corporation. Telnet is a registered trademark of SoftSwitch, Inc. Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

All other products or services mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky
Ramat Gan 52520, Israel
Tel: 972-3-613 1833
Fax: 972-3-575 9256

e-mail: info@checkpoint.com

U.S. Headquarters:
400 Seaport Court, Suite 105
Redwood City, CA 94063
Tel: 800-429-4391
415-562-0400
Fax: 415-562-0410

HTTP://www.checkpoint.com

The Check Point FireWall-1 Security Suite

Check Point FireWall-1's comprehensive Security Suite delivers an enterprise-wide security solution that goes far beyond the capabilities of previous firewall solutions. FireWall-1's unique and innovative Security Suite includes:

- Open Platform for Secure Enterprise Connectivity (OPSEC)
- Stateful Inspection Technology
- Enterprise-wide Security Management
- Distributed Client/Server Architecture
- Authentication
- Network Address Translation
- Encryption
- Content Security
- Connection Control
- Router Management

OPSEC

Check Point's OPSEC introduces a new standard in enterprise security that integrates all aspects of network security through a single, extensible management framework.

OPSEC allows enterprises to take full advantage of the FireWall-1 Security Suite and other security applications. The OPSEC framework provides central configuration and management for FireWall-1, while integrating third party security applications. Enterprises can choose the security components, from Check Point and other vendors, that best meet their requirements. OPSEC is both open and extensible, incorporating a variety of security applications in a single, centrally managed security system. Enterprises can take full advantage of the latest security technologies and can upgrade individual components without having to reconfigure an entire security system.

Enterprises can plug into Check Point's OPSEC framework in the following ways:

- **OEM/Bundling**
  The FireWall-1 Inspection Module runs directly on third-party security equipment.
- **Published APIs**
  Check Point provides Application Programming Interfaces for open protocols.
- **Network Security Applications**
  FireWall-1 supports third-party applications securely out-of-the-box.

The OPSEC Model

In the OPSEC framework, the enterprise security system is composed of several components, each of which is provided by different a different vendor and installed on a different machine. FireWall-1 distributes security tasks to the OPSEC components. Transactions between FireWall-1 and OPSEC security components take place using open, industry standard protocols.

Example OPSEC components are:

- a CVP (Content Vectoring Protocol) server that examines files for viruses
- a UFP (URL Filtering Protocol) server that categorizes URLs

Published APIs

OPSEC provides C language APIs for configuring transactions between FireWall-1 and OPSEC components. The OPSEC API is a powerful and easy to use environment that defines an asynchronous interface suitable for developing:

- servers that implement one or more OPSEC security tasks
- clients that use an OPSEC server

OPSEC Client/Server Interaction

In a common OPSEC model, FireWall-1 acts as a client sending requests to an OPSEC server. FireWall-1 intercepts a connection and generates a request to the OPSEC server. The server processes the request and sends a reply to FireWall-1. FireWall-1 processes the original connection based on the reply.

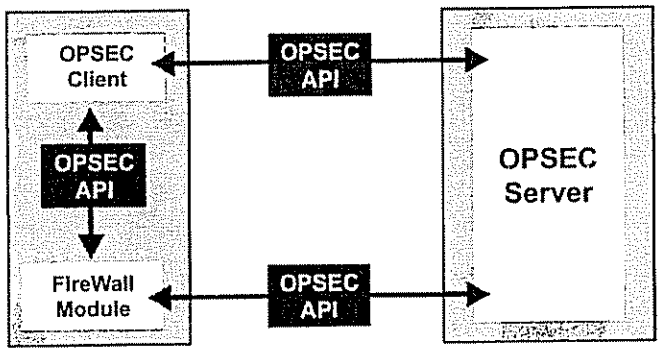

Figure 1 OPSEC Client/Server Communication

For example, FireWall-1 intercepts a connection request from an internal host to a specific URL. FireWall-1 passes the request to a UFP server, which checks a list of permitted and denied URLs. The UFP server sends FireWall-1 a reply stating that the requested URL is a denied Web site. FireWall-1 denies the original connection.

In the "standard" framework, FireWall-1 is the OPSEC client, but other scenarios are also possible:

- An OPSEC client (not a FireWall) communicates directly with an OPSEC server without the intervention of a FireWall Module.
- A FireWall Module acts as the OPSEC server

Stateful Inspection Technology

FireWall-1's patented Stateful Inspection Technology delivers full firewall capabilities, assuring the highest level of network security. FireWall-1's powerful Inspection Module analyzes all packet communication layers and extracts the relevant communication and application state information. The Inspection

Module understands and can learn any protocol and application. By employing this flexible, extensible technology, FireWall-1 meets the dynamic security requirements of today's enterprise.

FireWall-1 Inspection Module

The FireWall-1 Inspection Module resides in the operating system kernel, below the Network layer, at the lowest software level. By inspecting communications at this level, FireWall-1 can intercept and analyze all packets before they reach the operating systems. No packet is processed by any of the higher protocol layers unless FireWall-1 verifies that it complies with the enterprise security policy.

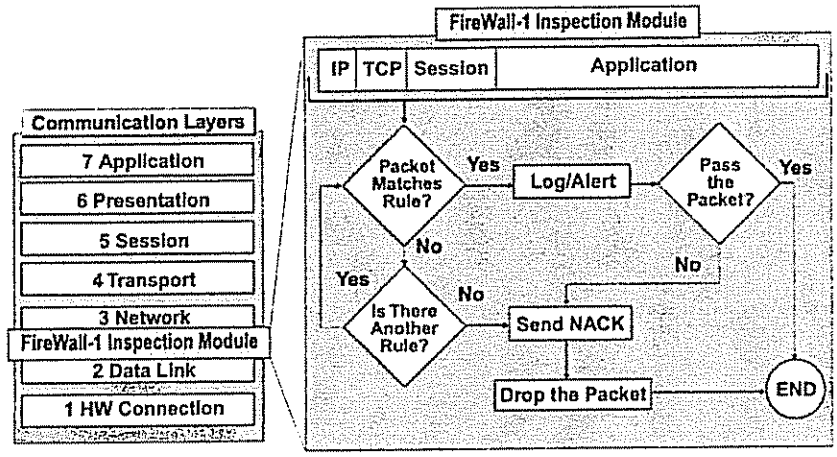

Figure 2 FireWall-1 Inspection Module

Full State Awareness

The Inspection Module has access to the "raw message," and can examine data from all packet layers. In addition, FireWall-1 analyzes state information from previous communications and other applications. The Inspection Module examines IP addresses, port numbers, and any other information required in order to determine whether packets comply with the enterprise security policy.

The Inspection Module stores and updates state and context information in dynamic connections tables. These tables are continually updated, providing cumulative data against which FireWall-1 checks subsequent communications.

FireWall-1 follows the security principle of "All communications are denied unless expressly permitted." By default, FireWall-1 drops traffic that is not explicitly allowed by the security policy and generates real-time security alerts, providing the system manager with complete network status.

Securing "Stateless" Protocols

The FireWall-1 Inspection Module understands the internal structures of the IP protocol family and applications built on top of them. For stateless protocols such as UDP and RPC, the Inspection Module extracts data from a packet's application content and stores it in the state connections tables, providing

context in cases where the application does not provide it. In addition, the Inspection Module can dynamically allow or disallow connections as necessary. These capabilities provide the highest level of security for complex protocols

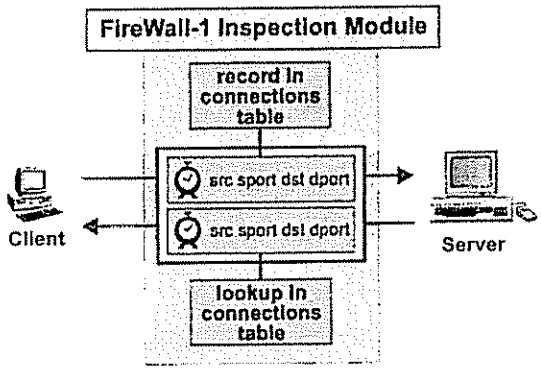

Figure 3 FireWall-1 Inspecting a UDP Session

INSPECT Language

Using Check Point's INSPECT language, FireWall-1 incorporates security rules, application knowledge, context information, and communication data into a powerful security system.

INSPECT is an object-oriented, high-level script language that provides the Inspection Module with the enterprise security rules. In most cases, the security policy is defined using FireWall-1's graphical interface. From the security policy, FireWall-1 generates an Inspection Script, written in INSPECT. Inspection Code is compiled from the script and loaded on to the FireWalled enforcement points, where the Inspection Module resides. Inspection Scripts are ASCII files, and can be edited to facilitate debugging or meet specialized security requirements.

INSPECT provides system extensibility, allowing enterprises to incorporate new applications, services, and protocols simply by modifying one of FireWall-1's built-in script templates using the graphical user interface.

Enterprise-Wide Security Management

Centralized Security Policy

FireWall-1 allows an enterprise to define and implement a single, centrally managed security policy. A FireWall-1 security policy is expressed in terms of a Rule Base and Properties.

The Rule Base is an ordered set of rules against which each communication is tested, while Properties define overall standards of communication inspection. FireWall-1 rules specify the source, destination, service and action taken for each communication. The security rules also specify which communication events are logged and the information included in each log entry.

The security policy is managed and updated from a single, centralized workstation. All communications between this workstation and FireWalled enforcement points are authenticated and transmitted on secure channels.

Graphical User Interface

FireWall-1's intuitive graphical user interface offers a powerful set of tools for the centralized management and implementation of an enterprise security policy.

Object-Oriented Management

Rule Base Editor

FireWall-1's object-oriented Rule Base enables an enterprise to easily define and implement a comprehensive security policy. Administrators can specify enterprise networks, users, and servers, and the relationships between them. This centrally managed solution makes it easy to modify network object parameters and update the security policy.

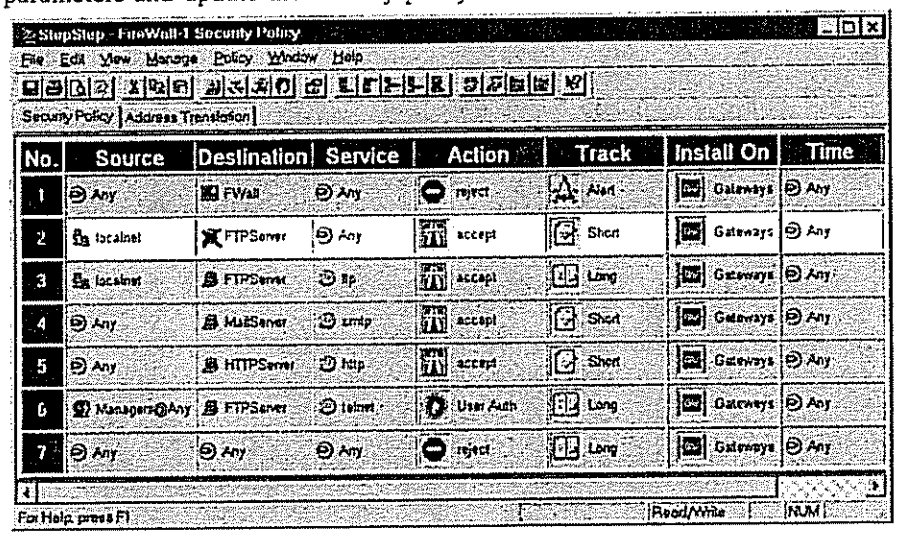

Figure 4 FireWall-1 Rule Base Editor

A FireWall-1 Rule Base specifies the actions taken on communication attempts — whether they are allowed, disallowed, logged, etc.

Properties Setup

A security policy is defined not only by the Rule Base, but also by the parameters in the Properties Setup window. Properties define the overall aspects of communication inspection without the need to specify repetitive details in the Rule Base.

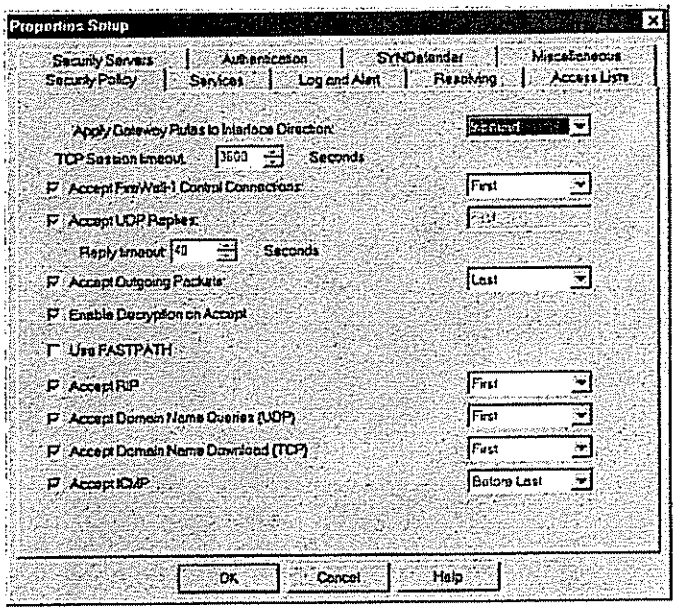

Figure 5 Properties Setup window - Security Policy tab

Object Managers

Object Managers make it easy to define all the network's elements in terms of object classes and their properties. Objects can be grouped in families or organized in hierarchies for more efficient control. Object properties can be centrally managed and updated.

Every object has a set of attributes, such as network address, subnet-mask, etc. The user specifies some of these attributes, while others are extracted by FireWall-1 from the network databases, like the `hosts` and `networks` files,

Network Information Services (NIS/Yellow Pages), and the Internet domain service. SNMP agents are used for extracting additional information, including the interfaces and network configuration of hosts, routers and gateways.

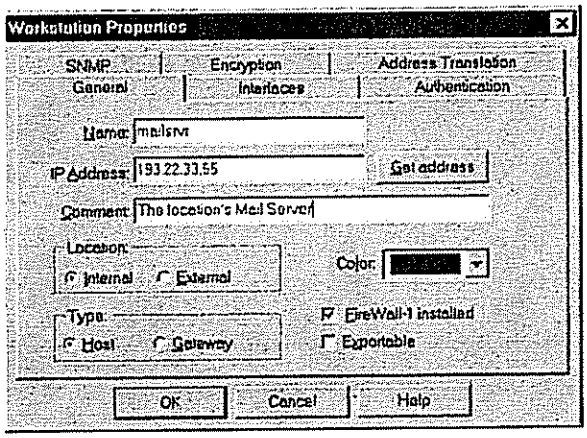

Figure 6 Workstation Properties window - General tab

FireWall-1's graphical user interface allows Administrators to define the following object classes:

- **Network Objects** — networks and sub-networks, hosts, gateways and servers (FireWalled or not), routers, Internet domains, and logical servers
- **Users** — individuals and groups accessing the network

  Administrators can define user access privileges, including allowed sources and destinations as well as user authentication schemes.
- **Services** — services known to the system and used in the security policy

  FireWall-1 includes a comprehensive set of over 100 TCP/IP and Internet services. New services can be added easily.
- **Resources** — sets of entities which can be accessed by a specific protocol

  FireWall-1 Resources can be defined based on HTTP, FTP and SMTP.
- **Time Objects** — time periods during which rules are in effect
- **Servers** — content screening and authentication servers
- **Keys** — encryption keys for interoperability with third party encryption devices that do not support automated key management

Visual Tracking and Accounting: Log Viewer

FireWall-1's graphical Log Viewer provides visual tracking, monitoring and accounting information for all connections passing through FireWalled gateways. On-line viewing features enable real-time monitoring of communication activities and alerts. The Log Viewer also displays significant network events, such as security policy installations or system shutdowns.

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

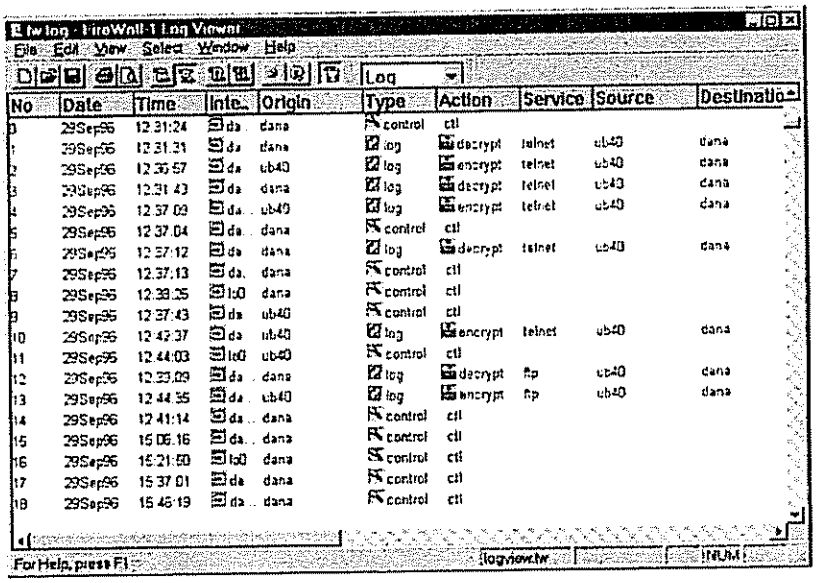

Figure 7 Log Viewer

Reports are easily generated by applying selection criteria to chosen fields, providing both detailed and comprehensive views. Reports can be printed or exported to third party applications, such as spreadsheets or trouble-ticketing systems. Exported log information is authenticated and transmitted on secure channels to protect sensitive auditing information.

Real-time Alerting: System Status Viewer

FireWall-1 provides real-time status, auditing, and alerting capabilities. The System Status window displays a snapshot of all the FireWalled systems throughout the enterprise. The status of each FireWalled host is available at a glance. The System Status window also provides packet statistics — the number of packets accepted, logged or rejected — for each FireWalled host.

Administrators can also specify an action taken if the status of a FireWalled host changes. For example, FireWall-1 can issue an alert notifying system managers of any suspicious activity.

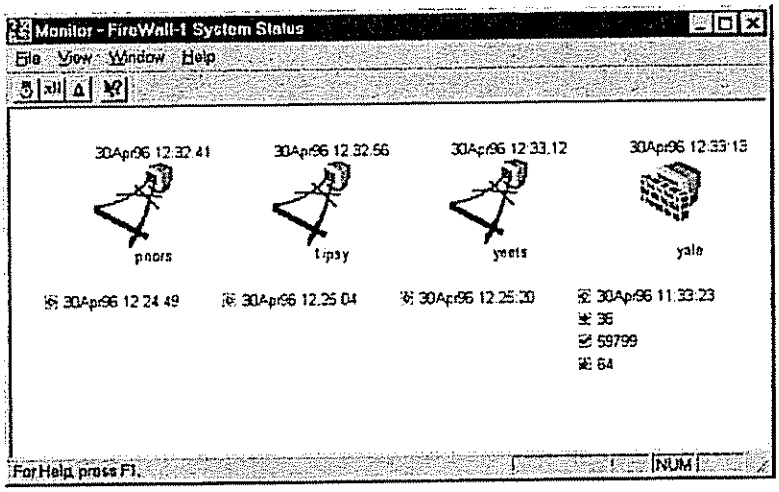

Figure 8 System Status Window

Anti-Spoofing

FireWall-1 detects spoofed packets by checking that the source IP address of a packet entering a FireWalled gateway corresponds to the appropriate gateway interface. FireWall-1's object-oriented interface allows Security Administrators to define anti-spoofing for all gateway interfaces and generate alerts.

The Interface Properties window specifies anti-spoofing detection. Figure 9 depicts the anti-spoofing properties for a gateway's external interface — le0. By specifying "Others" under Valid Addresses, the Security Administrator assures that only packets that whose source IP address does not belong to the networks behind this gateway will be allowed to pass.

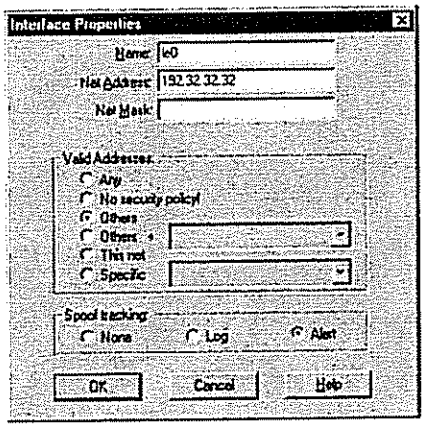

Figure 9 Interface Properties window with anti-spoofing defined

Distributed Client/Server Architecture

FireWall-1 manages the enterprise security policy through a distributed Client/Server architecture that ensures high performance, scalability and centralized control.

FireWall-1 consists of two primary modules — the Management Module and the FireWall Module. These modules can be deployed in a number of flexible Client/Server configurations across a broad range of platforms (see "Platform Summary" on page 34).

FireWall-1's Client/Server architecture is completely integrated. There is only one security policy and one Rule Base, defined and maintained at a single management point, which controls multiple FireWalled enforcement points.

Management Module

The Management Module includes the GUI and the management database functionalities — the Rule Base, network objects, services, users etc. The security policy is defined on the GUI. The components of the Management Module can reside on the same machine or be deployed in a Client/Server configuration (see Figure 10 on page 13).

FireWall Module

The FireWall Module includes the Inspection Module and Security Servers.

The FireWall Module implements the security policy, logs events, and communicates with the Management Module using the FireWall daemons. A machine on which the FireWall-1 Inspection Module is installed is known as a "FireWalled system."

The FireWall Module can be installed on a broad range of platforms (see "Platform Summary" on page 34). It usually resides on a dual-homed host (a gateway) but can also be installed on a server.

A FireWall-1 security policy is defined using the GUI on the Management Module. Inspection Code is then generated and installed on the FireWall Modules that will enforce the security policy.

The Management Module GUI client, the Management Module server and the FireWall Module can be installed on the same computer if its platform supports all three components, or on three different computers. In either case, the System Administrator defines and maintains the security policy on the Management Module, while the FireWalled Gateways (where the FireWall Module is installed) enforce the security policy.

Distributed Configurations

Figure 10 depicts a distributed configuration, on which a Management Module (in the Client/Server implementation) controls three FireWall Modules, each of which is on a different platform, which in turn protect three heterogeneous networks.

In this configuration the Security Administrator can configure and monitor network activity for several sites from a single desktop machine. The security policy is defined on the GUI Client, while the FireWall database is maintained on the Management Server. The connections between the client, server and multiple enforcement points are secured, enabling true remote management.

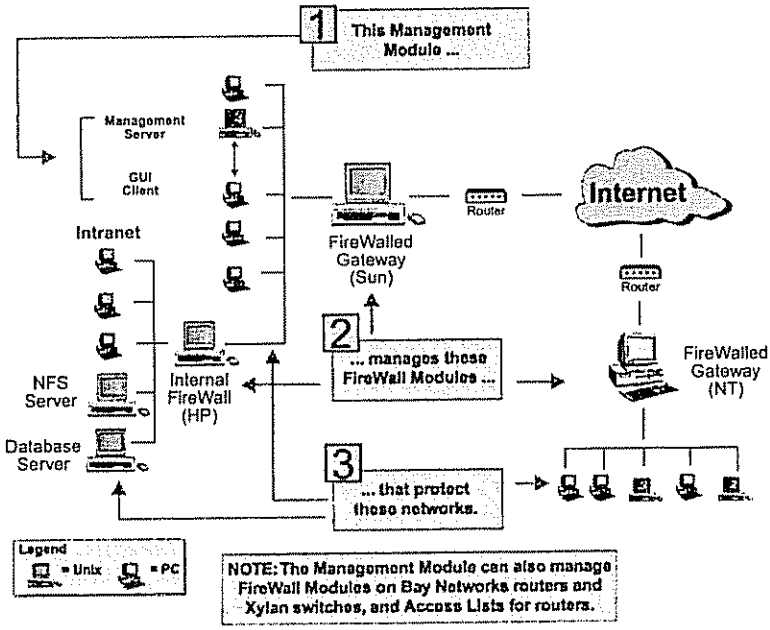

Figure 10 Distributed FireWall-1 Configuration

Although FireWall-1 is deployed in a distributed configuration, security policy enforcement is completely integrated. Any number of FireWall Modules can be set-up, monitored and controlled from a single workstation, but there is still only one enterprise-wide security policy maintained by a single rule base and log file. Authorized management clients can access security control information from anywhere on the network.

Authentication

FireWall-1 provides remote users and telecommuters secure, authenticated access to enterprise resources using multiple authentication schemes. FireWall-1 authentication services securely validate users or clients that try to access the internal network. Modifications to local servers or client applications are not required. Authentication services are fully integrated into the enterprise-wide security policy and can be centrally managed through FireWall-1's graphical user interface. All authentication sessions can be monitored and tracked through the Log Viewer.

Authentication Methods

FireWall-1 provides three authentication methods:

1. **User Authentication**
2. **Client Authentication**
3. **Session Authentication**

User Authentication

FireWall-1's transparent 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 Security Administrator may define a rule that allows that user to work on the local network without extending access to all users on the same host.

The FireWall-1 Security Servers implement user authentication on the gateway. FireWall-1 intercepts a user's attempt to start an authenticated session on the requested server and directs the connection to the appropriate Security Server. After the user is authenticated, the FireWall-1 Security Server opens a second connection to the host. All subsequent packets of the session are intercepted and inspected by FireWall-1 on the gateway.

Client Authentication

Client Authentication enables an administrator to grant access privileges to a specific user at a specific IP address. In contrast to User Authentication, Client Authentication is not restricted to specific services, but provides a mechanism for authenticating any application, standard or custom. FireWall-1 Client Authentication is not transparent, but it does not require any additional software or modifications on either the client or server. The administrator can determine how each individual is authenticated, which servers and applications are accessible, at what times and days, and how many sessions are permitted.

Session Authentication

Session Authentication can be used to authenticate any service on a per-session basis. After the user initiates a connection to the server, FireWall-1 opens a connection with a Session Authentication Agent The Agent performs the required authentication, after which FireWall-1 allows the connection to continue to the requested server.

Authentication Schemes

FireWall-1 supports the following authentication schemes:

1. **S/Key** — The user is challenged to enter the value of requested S/Key iteration.
2. **SecurID** — The user is challenged to enter the number displayed on the Security Dynamics SecurID card.
3. **OS Password** — The user is challenged to enter his or her OS password.
4. **Internal** — The user is challenged to enter his or her internal FireWall-1 password on the gateway.
5. **RADIUS** — The user is challenged for a response, as defined by the RADIUS server.

6. **Axent** — The user is challenged for the response, as defined by the Axent server.

Network Address Translation

FireWall-1's Network Address Translation features provide complete Internet access for internal hosts with invalid or secret IP addresses. Internal hosts can be accessible from the Internet, even though their internal IP addresses are invalid Internet addresses. FireWall-1 supports both IP address hiding and static Address Translation, providing full Internet connectivity for internal clients. At the same time, FireWall-1 completely integrates Address Translation rules in the security policy, maintaining full network security.

Configuring Address Translation

FireWall-1 Address Translation rules can be simply generated and integrated into the enterprise security policy. FireWall-1 provides three methods for configuring Address Translation:

1. Automatic Configuration
2. Address Translation Rule Base (Windows and X/Motif only)
3. Command Line Interface

Automatic Configuration

Address Translation properties can be defined for particular objects, such as workstations or networks. Address Translation rules are then automatically generated, and the object's properties are applied whenever it is used in the security policy.

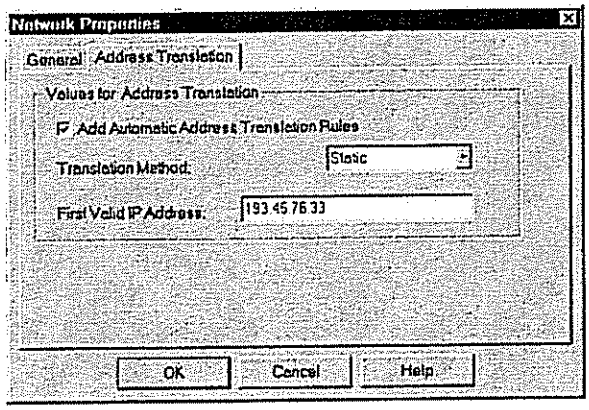

Figure 11 Automatically Generating Address Translation for a network

Graphical Address Translation Rule Base

FireWall-1's graphical user interface simplifies the definition and implementation of Address Translation rules. This flexible Address Translation Rule Base allows administrators to:

- specify objects by name rather than by IP address

- restrict rules to specified destination IP addresses, as well as to the specified source IP Addresses
- translate both source and destination IP addresses in the same packet
- restrict rules to specified services (ports)
- translate ports

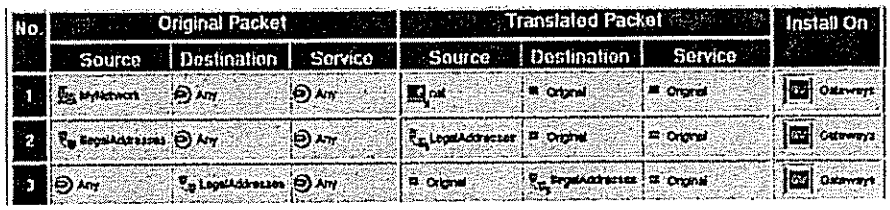

Figure 12 Address Translation Graphical User Interface

Command-Line Interface

Address Translation rules can be defined using a command line interface application (`fwxlconf`). It is also possible to directly edit the text file `$FWDIR/conf/xlate.conf`.

Translation Modes

FireWall-1 supports two kinds of Address Translation modes to protect internal addressing schemes while providing full Internet access:

- **Dynamic**

  FireWall-1 translates many invalid addresses to a single valid address and dynamically assigns port numbers to distinguish between the invalid address. Dynamic address translation is called "Hide Mode," because the invalid address are hidden behind the valid address.
- **Static**

  FireWall-1 translates each invalid address to a corresponding valid address.

Virtual Private Networks

Long-distance communications between enterprises, partners, branch offices and mobile users have become essential to business relations. Enterprises are increasingly using public networks, such as the Internet, as a flexible, cost-effective connection between their private networks. However, public networks expose corporations to the following dangers:

- break-ins — unauthorized Internet access to internal networks
- eavesdropping — enterprise communications can be monitored and tampered with as they travel over the Internet

Check Point FireWall-1 allows enterprises to take full advantage of Virtual Private Networks. FireWall-1's encryption services establish secure communication channels over the Internet, assuring full privacy, authenticity and data integrity in corporate internetworking.

FireWall-1 Encryption

FireWall-1 provides transparent, selective encryption for a wide range of services, allowing organizations to make full use of the Internet for all business and connectivity needs. Multiple encryption schemes, key management and an internal Certificate Authority are fully integrated with other FireWall-1 features. FireWall-1's intuitive graphical interface makes it simple to define and manage encryption in an enterprise security policy.

Secure VPNs

FireWalled gateways encrypt data communications traveling over the Internet between private networks, creating secure, Virtual Private Networks. FireWall-1 implements encryption for corporate internetworks without the need to install and configure encryption software on every host in the networks involved. A FireWalled gateway performs encryption on behalf of its encryption domain —the local area network (LAN) or group of networks that it protects. Behind the gateway, in the internal networks, packets are not encrypted. Only packets traveling over public segment of the connection are encrypted.

Selective Encryption

FireWall-1's selective encryption feature allows the transmission of both clear and encrypted data between the same workstations and networks. Instead of encrypting all communications between corporate networks, FireWall-1 allows administrators to define the specific services that require encryption.

Multiple Encryption Schemes

FireWall-1 supports three encryption schemes:

1. FWZ, a proprietary FireWall-1 encryption scheme
2. Manual IPSec, an encryption and authentication scheme that uses fixed keys
3. SKIP (Simple Key-Management for Internet Protocols), developed by Sun Microsystems, that adds improved keys and key management to IPSec

The relationship between the components of the encryption schemes, as implemented in FireWall-1, is illustrated in Table 1.

Table 1 Comparison of Encryption Schemes

feature	FWZ	Manual IPSec	SKIP
portability	Check Point proprietary	standard	standard supported by Sun and other vendors
key management	yes	no	yes
Session Keys	each TCP or UDP session has a new key	fixed	keys change over time or as amount of data encrypted exceeds threshold
number of keys required is proportional to the ...	number of correspondents	square of the number of correspondents	number of correspondents
packet size	unchanged	increased	increased
gateway can encrypt/decrypt on behalf of other hosts	yes	yes (in Tunnel Mode)	yes (in Tunnel Mode)

DES, FWZ1 and RC4 are all encryption algorithms used to encrypt the data portion of a packet.

High Efficiency and Performance

FireWall-1 encryption does not alter communication length, maintains MTU validity and eliminates packet fragmentation, thus achieving the highest performance available over the network. FireWall-1 supports encryption speeds greater than 10 Mb/sec through a standard desktop workstation. In addition, routing priorities and policies are preserved.

FireWall-1 SecuRemote

FireWall-1 SecuRemote extends the Virtual Private Network to the desktop and laptop. Mobile and remote Microsoft Windows 95 and NT users can connect to their enterprise networks via dial-up Internet connections — either directly to the server or through Internet Service Providers — and transfer sensitive corporate data as safely and securely as from behind the corporate Internet FireWall.

FireWall-1 SecuRemote is based on a technology called Client Encryption. Because FireWall-1 SecuRemote encrypts data before it leaves the laptop, it offers a completely secure solution for remote access user-to-FireWall connections. FireWall-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. FireWall-1 SecuRemote can interface with any existing adapter and TCP/IP stack. A PC on which FireWall-1 SecuRemote is running can be connected to several different sites that use VPNs.

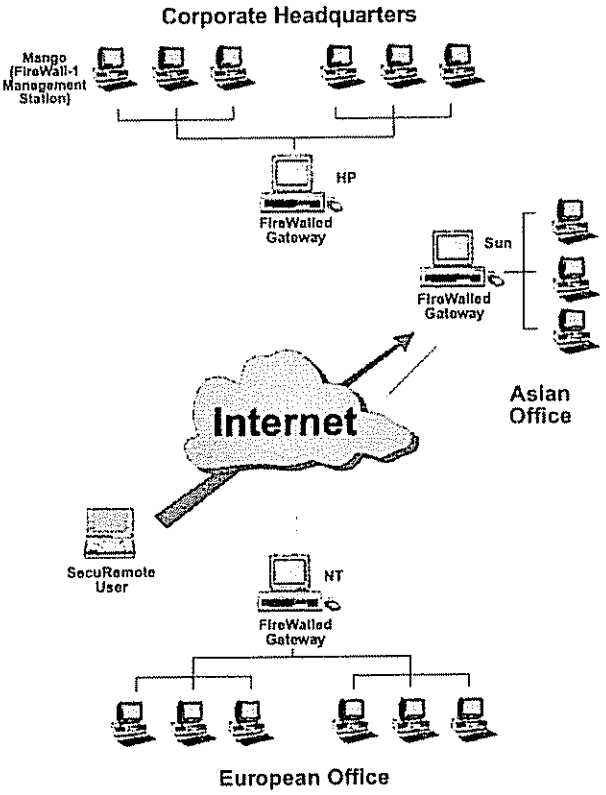

Figure 13 Virtual Private Network with Nomadic Users

SecuRemote is completely integrated with all FireWall-1 features, including authentication, logging, and alerting. After a FireWall-1 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.

FireWall-1 SecuRemote includes the following features:

- support for dynamic IP addressing, which is necessary for dial-up communication
- strong user authentication using Diffie-Hellman and RSA algorithms
- strong encryption using FWZ1 or DES

Content Security

FireWall-1's extensive content security capabilities protect networks from various threats, including viruses and suspicious Java and ActiveX code, while providing fine-tuned access control to the Internet. FireWall-1 content security is defined through Resource objects, and implemented by a suite of Security Servers at the

application level. Content Security is fully integrated with other FireWall-1 features, and is centrally managed through the intuitive graphical interface. In addition, Check Point's OPSEC framework provides open APIs for integrating third-party content screening applications.

Resources

FireWall-1 Resource objects enable content security by providing precise control over Internet access. A Resource object defines a group of entities that can be accessed by a specific protocol as well as content screening properties. FireWall-1 Resources are based on HTTP, FTP and SMTP. A URI resource, for example, may include a list of permitted URLs accessed through HTTP and FTP.

FireWall-1 Resources incorporate Content Security into the enterprise security policy. Resources can be used in a Rule Base in exactly the same way as a service. The standard logging and alerting methods are available to monitor Resource use.

Security Servers

FireWall-1 includes Security Servers for HTTP, FTP and SMTP. When a rule specifies a Resource in the Service field, the Inspection Module diverts all the packets in the connection to the appropriate Security Server, which performs the content screening included in the Resource definition.

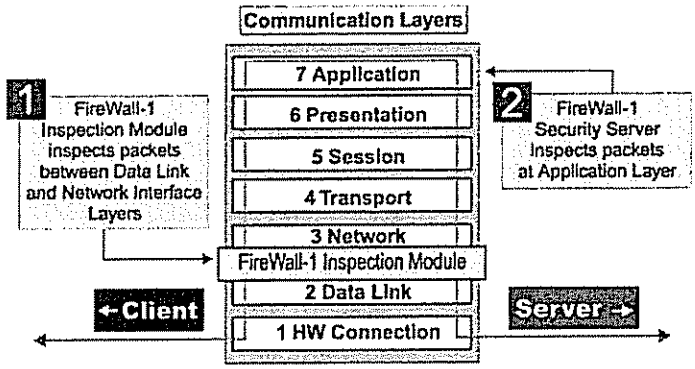

Figure 14 A connection mediated by a FireWall-1 Security Server

For each connection established through the Security Servers, administrators can control Internet access according to the fields that belong to a specific service: URLs, file names, FTP PUT/GET commands, request types and more.

HTTP Server

URI resources can define schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, "*.com"), paths and queries. Alternatively, a file containing a list of IP addresses and servers can be specified.

FTP Server

The FTP Security Server provides authentication services and content security based on FTP commands (PUT/GET), file name restrictions, and Anti-Virus checking for files.

SMTP Server

The FireWall-1 SMTP server provides precise control over SMTP connections, assuring maximum connectivity and security. SMTP resource definitions allow administrators to hide internal IP addresses from outgoing e-mail, strip specific attachment types, drop messages above a given size and more

Anti-virus Inspection

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

Check Point's OPSEC management provides an open API for defining transactions between FireWall-1 and third-party CVP servers.

URL Screening

URL screening provides precise control over Web access, allowing administrators to define undesirable or inappropriate Web pages. FireWall-1 checks Web connection attempts using third-party URL Filtering Protocol (UFP) servers. UFP servers contain lists of URLs and their appropriate categories (i.e. permitted or denied). URL databases can be updated to provide a current list of blocked sites. OPSEC includes an API for integrating third-party URL screening applications.

Java and ActiveX Stripping

FireWall-1's extensive screening capabilities effectively protect enterprise networks from Java and ActiveX attacks. Using FireWall-1's flexible Resource definition, administrators can control incoming Java and ActiveX code according to specific conditions, such as host, URL or authenticated user name.

FireWall-1's Java and ActiveX screening includes the following capabilities:

- stripping Java applet tags from HTML pages
- stripping Java applets from all server-to-client replies, even if the reply is a compressed or archived file
- blocking Java attacks by blocking suspicious back connections
- stripping ActiveX tags from HTML pages

Connection Control

Load Balancing

FireWall-1 extends network connectivity by distributing a processing load among several servers. FireWall-1 implements load balancing using a network object known as a Logical Server, a group of servers providing the same service. In the Rule Base, Administrators can define a rule directing connections of a particular service to the appropriate Logical Server. The Logical Server handles the connection attempt using one of five pre-defined load balancing algorithms:

1. **server load**

   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.

2. **round trip**

   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.

3. **round robin**

   FireWall-1 simply assigns the next server in the list.

4. **random**

   FireWall-1 assigns a server at random.

5. **domain**

   FireWall-1 assigns the "closest" server, based on domain names.

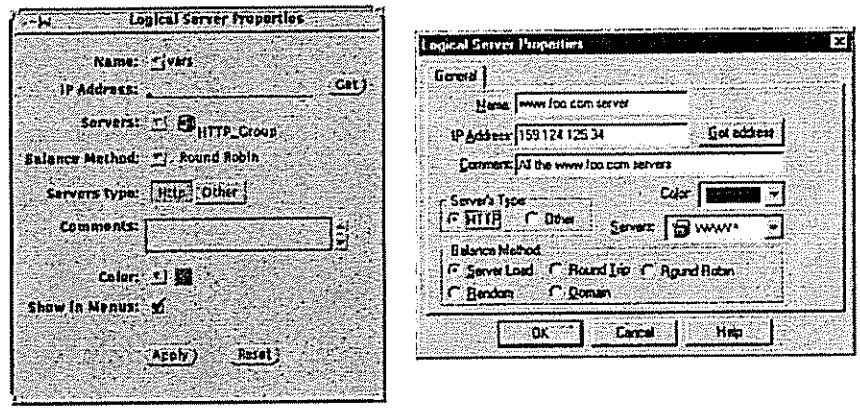

Figure 15 Logical Server properties definition

Although a Logical Server may consist of several servers, the client is aware of only one server. When the service request reaches the FireWall, FireWall-1 determines which of the servers in the group will fulfill the request, based on the load balancing algorithm assigned to the logical server.

Synchronization of FireWall Modules

FireWall Modules running on different machines can automatically share information from state connection tables and mutually update each other.

State table synchronization enables FireWall-1 to support high availability systems If one of the FireWalled gateways stops functioning and another one takes its place, the second FireWalled gateway has the most recent state information from the first gateway and can seamlessly take over network connections.

Shared state information also provides support for asymmetric routing configurations — different routes for different segments of a connection. The IP protocol supports a network configuration in which all packets sent from host A to host B are routed through one gateway, but all packets sent from host B to host A are routed through a second gateway.

Router Management

FireWall-1 provides centralized network and security management for routers throughout the enterprise. The enterprise security policy is defined and maintained from a single management station, while routers operate as security enforcement points.

FireWall-1 manages routers in two ways:

- **Access Lists**

  FireWall-1 downloads Access Lists derived from the security policy to selected routers.
- **Stateful Inspection**

  The FireWall-1 Inspection Module runs directly on specific routers and network devices. The standard FireWall-1 features, with the exception of encryption, address translation, and client and session authentication are supported.

FireWall-1 supports the following routers and network devices:

- Bay Networks routers

  Bay Networks routers support both Access Lists and Stateful Inspection.
- CISCO routers
- 3COM routers
- Xylan switches

Configuring FireWall-1

This section describes two possible network configurations with FireWall-1 and shows how to define and implement an enterprise security policy for these configurations. The first example discusses a simple configuration for a small, fictitious enterprise. A more complex configuration reflects the growing security requirements of the same organization.

Note – These configurations are examples for the purposes of this document only.

A Simple Configuration

Web Write Productions is a small multimedia and web design company with 20 employees, a small internal network and a mail server. Employees use the Internet for e-mail, FTP and HTTP services to communicate with customers and access the Web. While Web Write employees require complete Internet access, the company wants to protect the internal network. At the same time, Web Write employees need to receive mail from customers located outside of the corporate network.

In This example, FireWall-1 is installed on a gateway computer (named "Wolfman" in the rules that follow).

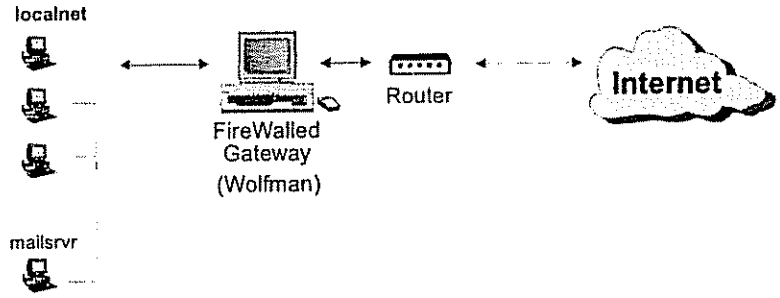

Figure 16 Example Simple Network Configuration

A Typical Security Policy

For above configuration a typical security policy might be this:

- external networks may access the local network only to send mail to local computers
- local computers may access the entire network: localnet and Internet

This policy protects the private network from non-local networks, but puts no restrictions on local computers.

The next section describes how this security policy can be implemented using FireWall-1. Next, you will see how this security policy is "tightened up" so that the potential loopholes are blocked.

Implementing a Security Policy

In order to implement a security policy, you must:

1. Using the Object Managers, define the network objects used in the Rule Base.

   You do not have to define the entire network to FireWall-1 — only the objects that are used in the Rule Base. For the configuration described here, you must define the gateway (Wolfman), the mail server (mailsrvr) and the local network (localnet).

2. Define services used in your security policy (optional).

   You do not have to define the commonly used services. These are already defined for you in FireWall-1. You should define only those uncommon services that are part of your security policy.

   Defining network objects and services is very straightforward. In most cases, you need only specify a name, because FireWall-1 can obtain the object's properties from the appropriate system databases (DNS, `hosts`, etc.).

3. Define the Rule Base — the rules for accepting, rejecting and logging packets
4. Install the Rule Base — install the Inspection Code on the gateways.

Defining the Rule Base

After you define network objects, users and services, the next step in implementing a security policy is to define the relationships between them using the Rule Base editor.

In this simple example, there are only two rules, corresponding to the policy given above.

The first rule (non-local networks may only send mail to the mail server) can be expressed in the Rule Base editor as follows:

Source	Destination	Services	Action	Track	Install On
Any	mailsrvr	smtp	Accept	Short Log	Gateways

The second rule (local computers may access the entire network: localnet and Internet) can be expressed in the Rule Base editor as follows:

Source	Destination	Services	Action	Track	Install On
localnet	Any	Any	Accept	Short Log	Gateways

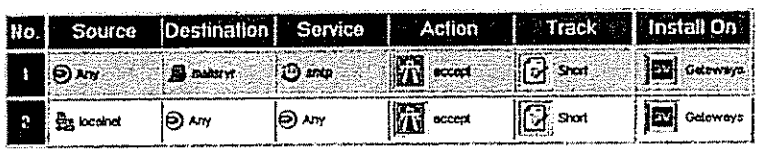

Figure 17 Rule Base editor window showing first two rules

Fine Tuning the Security Policy

Implicit Drop

FireWall-1 follows the principle "Communications that are not explicitly permitted are denied." To enforce this principle, FireWall-1 implicitly adds a rule at the end of the Rule Base that drops all communication attempts not described by the other rules.

Since the rules are examined sequentially for each packet, only packets not described by the first two rules are examined by the implicit rule. However, if you rely on the implicit rule to drop these packets, they will not be logged, because only packets which are described by a rule can be logged by the Rule Base. To log these packets, you must explicitly define a "none of the above" rule, as follows:

Source	Destination	Services	Action	Track	Install On
Any	Any	Any	Reject	Long Log	Gateways

If you do not explicitly define such a rule, FireWall-1 will implicitly define one for you, and the packets will be dropped. In no case will FireWall-1 allow these packets to pass.

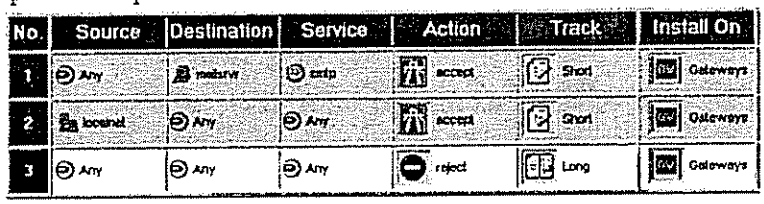

Figure 18 Rule Base including first three rules

"Stealthing" the Gateway

The Rule Base described above has a shortcoming — it enables localnet computers to get on the gateway (assuming that they have Unix accounts and passwords). In the given configuration, this is usually not desirable. To prevent any computers (not just local computers) from getting on the gateway, you must add a rule (before the other rules) as follows:

Source	Destination	Services	Action	Track	Install On
Any	Wolfman	Any	Reject	Long Log	Gateways

Protecting the gateway in this manner makes it inaccessible to other users and applications (except for FireWall-1 management purposes). The gateway becomes an invisible network object that, from the point of view of the network, does not even exist.

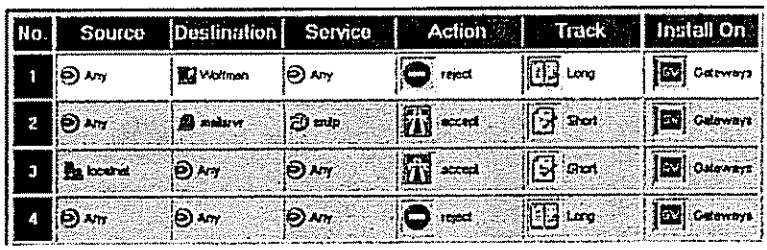

Figure 19 Rule Base editor with rule protecting the gateway

You may wish to confirm that the gateway is indeed inaccessible by performing the following experiment (after you have installed the Rule Base). TELNET out through the gateway and then try to TELNET back to the gateway. The second TELNET will fail. [1]

Note – The icons representing network objects convey information about the objects. Gateways look like gates, and a brick wall inside a host or gateway icon indicates that the object is FireWalled.

This rule does not prevent users from sitting at the gateway keyboard and going out of the network. To further protect the gateway, you may wish to add a rule that rejects any packet which originates on the gateway and issue an alert, as follows:

Source	Destination	Services	Action	Track	Install On
Wolfman	Any	Any	Reject	Alert	Source

The reason that Install On is specified as Source in this rule is that by default, gateways enforce rules on inbound traffic only. The rule is enforced on Wolfman, but because Wolfman is specified as Source, the rule is enforced only in the outbound direction (that is, it applies only to packets leaving Wolfman which also originate on Wolfman). If Install On were specified as Gateways, then the rule would apply only to packets entering Wolfman which also originate on Wolfman, in other words, to no packets at all.

1 You should be aware that if you ping the gateway (rather than TELNET back) from the outside, you will succeed, because the Accept ICMP property is specified by default as the first rule in the Properties Setup window.

A More Detailed Configuration

Within a year, Web Write wants to add a public server (DMZ — Demilitarized Zone) to provide HTTP and FTP services to customers and employees outside the enterprise network.

The new network configuration depicted in Figure 20 is similar to the first one, except that a public server (DMZ — Demilitarized Zone) and an external client have been added. DMZ provides HTTP, FTP and other services to non-local networks, but does not initiate any traffic. DMZ is actually a third interface attached to the gateway, and might be a network, a sub-network or a host

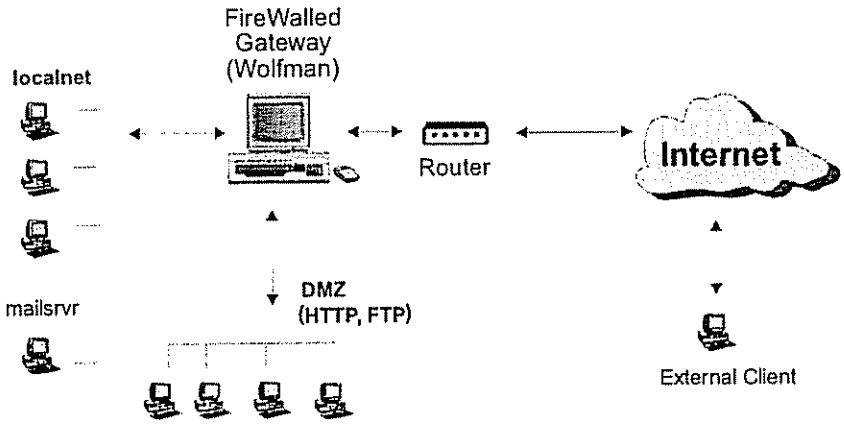

Figure 20 Detailed Network Configuration

The first two rules in the security policy for this configuration are the same as the security policy for the previous example, with the following additional rule allowing external networks access to the DMZ using HTTP and FTP:

Source	Destination	Services	Action	Track	Install On
Any	DMZ	HTTP, FTP	Accept	Short Log	Gateways

Additional Considerations

External Users

In the above configuration, it is possible to add a rule allowing external users, managers Bob and Alice, to TELNET to an FTP server on the DMZ for administrative purposes, no matter from which IP address they connect

FireWall-1's graphical user interface makes it easy to define and integrate this rule into the security policy. To implement this rule, you must:

1. Define two users, Alice and Bob, and specify their respective General and Authentication properties. Figure 21 depicts the Authentication properties for one of these users.

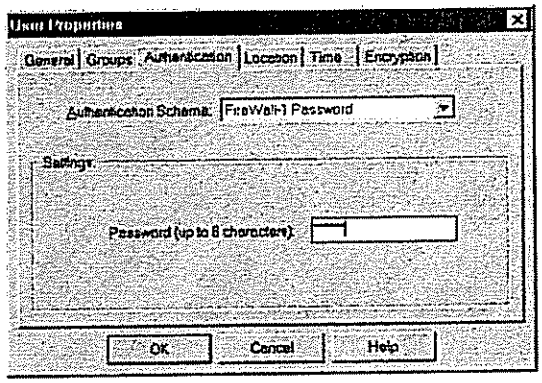

Figure 21 User Properties Window - Authentication Tab

2. Define a User Group called Managers, composed of Alice and Bob.

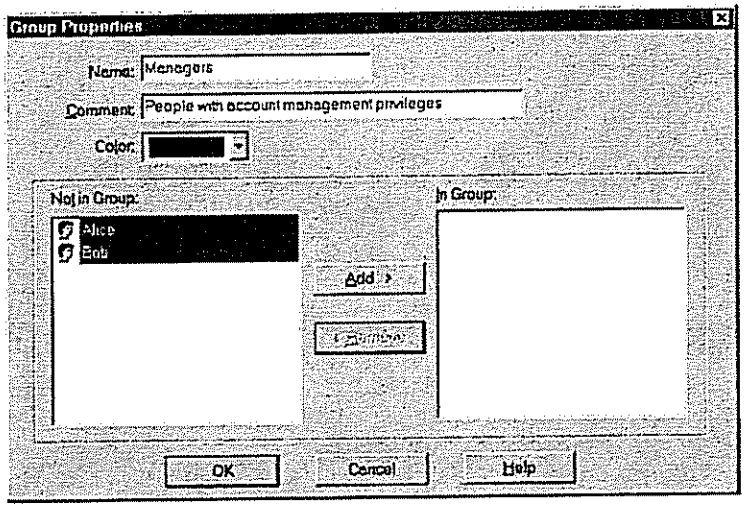

Figure 22 Group Properties Window

3. Add the following rule to the Rule Base:

Source	Destination	Services	Action	Track	Install On
Managers@Any	FTP Server	TELNET	User Auth	Short Log	Gateways

A Complete Rule Base

Figure 23 shows the complete rule base for the configuration depicted in Figure 20 on page 28.

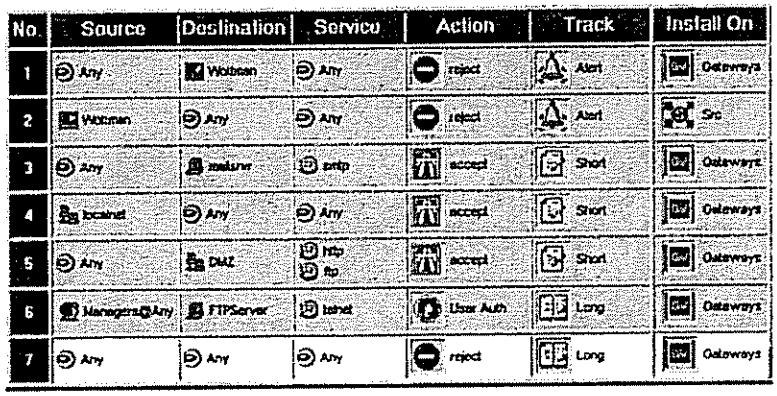

Figure 23 Complete Rule Base

Table 2 explains each rule in the Rule Base:

Table 2 Explanation of Rule Base Fields

Rule No.	Explanation
1	prevents anyone from getting on the gateway
2	prevents communications originating on the gateway
3	non-local host can only send mail to the Mail Server
4	local computers may access the entire network: localnet and Internet
5	allows access to the DMZ using FTP and HTTP
6	specifies User Authentication for Managers group members to TELNET to the FTP server, regardless of their IP address.
7	Implicit drop - rejects and logs all other communications

Installing a Rule Base

When you install a Rule Base on the FireWall Modules which are to enforce it, FireWall-1 verifies that the Rule Base is logical and consistent, and then generates and downloads the Inspection Code to the specified FireWall Modules. If the specified network object is a router, FireWall-1 generates and downloads the appropriate router access list rather than the Inspection Code.

Performance

The Inspection Module's simple and effective design achieves optimum performance through the following techniques:

- Running inside the operating-system kernel imposes negligible overhead in processing. No context switching is required, and low-latency operation is achieved.
- Advanced memory management techniques, such as caching and hash tables, are used to unify multiple object instances and to efficiently access data.
- Generic and simple inspection mechanisms are combined with a packet inspection optimizer to ensure optimal utilization of modern CPU and OS designs

In tests, network performance degradation was too small to be measured when operating at full LAN speed (10Mb/sec) on the lowest-end SPARCstation machine; the measurement included communication latency and network bandwidth. FireWall-1 can run even at 100Mb/sec on standard workstations.

Performance impact on the inspecting gateway host was also negligible. These results indicate that there is almost no performance penalty for current Internet speeds (56kb or T1 - 1.5Mb/sec speeds and up to full 10Mb/sec speed) on standard desktop workstations. Independent testing has shown consistently similar results.

FireWall-1's exceptional performance enables efficient, fully transparent outbound traffic — for example, to the Internet — while strictly enforcing powerful authentication procedures on inbound connections. FireWall-1 provides fully integrated security with no discernible performance penalty.

Conclusion

Check Point FireWall-1 meets the extensive security demands of today's enterprise. A sophisticated, comprehensive Security Suite establishes FireWall-1 as the complete network security solution.

OPSEC

Check Point's innovative OPSEC framework provides central configuration and management for FireWall-1 and external security applications. This open, extensible framework allows enterprises to utilize the full potential of FireWall-1, while at the same time incorporating the third-party security tools that best meet their needs.

Stateful Inspection Technology

Using Stateful Inspection Technology, FireWall-1 assures complete, transparent network security. Positioned at the lowest software layer, the FireWall Inspection Module intercepts and inspects all inbound and outbound packets before they reach the upper protocol layers of the FireWalled host. The Inspection Module analyzes state and context information from all packet layers and verifies whether it complies with the enterprise security policy. In addition, FireWall-1 provides complete security for stateless protocols.

FireWall-1 Stateful Inspection Technology meets evolving connectivity needs, allowing enterprises to take advantage of the latest security technologies. The flexible Inspection Module can learn and understand new protocols.

Enterprise-wide Security Management

FireWall-1 maintains and enforces a single, centrally managed enterprise security policy. An intuitive graphical user interface allows users to simply define a Rule Base and implement a security policy. FireWall-1's powerful set of graphical tools also provides real-time logging, auditing, accounting and alerting capabilities for all connections passing through FireWalled enforcement points.

Distributed Client/Server Architecture

FireWall-1's distributed Client/Server architecture enables centralized control and extensibility. FireWall-1 can be deployed in a number of flexible configurations across a broad range of platforms. A single, comprehensive security policy is defined and maintained from one management point, while multiple FireWalled enforcement points protect the network.

Content Security

FireWall-1's advanced content security features provides precise control over Web, FTP, HTTP, and SMTP connections. This new level of security is fully integrated with other FireWall-1 features and can be defined and centrally managed through the graphical Rule Base.

Connection Control

FireWall-1's connection control features extend network connectivity while assuring high performance levels. FireWall-1 can distribute a processing load over a number of servers. In addition, FireWall Modules running on different machines can mutually update each other and take over connections if one goes down.

Authentication

FireWall-1 authentication services provide remote users and telecommuters secure access to enterprise resources. FireWall-1 provides client, session and transparent user authentication, and supports multiple authentication schemes.

Network Address Translation

Network Address Translation features provide complete Internet access for internal hosts with invalid or secret IP addresses. FireWall-1 supports both IP address hiding and static Address Translation. Address Translation rules can be defined through the graphical user interface or generated automatically.

Encryption

FireWall-1's transparent, selective encryption establishes secure Virtual Private Networks. Multiple encryption schemes, key management and an internal Certificate Authority are fully integrated with other FireWall-1 features. In addition, FireWall-1 SecuRemote provides remote users secure access to their corporate networks.

Anti-Spoofing

A sophisticated anti-spoofing feature detects spoofed packets by checking that a packet's physical origin corresponds to its IP address.

Router Management

FireWall-1 provides centralized security and network management for routers. Access Lists are generated from the security policy and downloaded routers throughout the network. In addition, the Inspection Module runs directly on Bay Networks routers and Xylan switches. This feature extends Stateful Inspection to the router and switch levels.

Check Point Software Technologies Ltd.

Platform Summary

component	available platforms
FireWall-1 client (Client/Server model)	Windows 95, Windows NT (Intel only), X/Motif
FireWall-1 server (Client/Server model)	Windows NT 3.51 and 4.0 (Intel only), SunOS 4.1.3 and higher, Solaris 2.3, 2.4 and 2.5, HP-UX 9 and 10
FireWall-1 Management Module (OpenLook GUI)	SunOS 4.1.3, Solaris 2.3, 2.4 and 2.5, HP-UX 9 and 10
FireWall-1 FireWalled host or gateway	Windows NT 3.51 and 4.0 (Intel only), SunOS 4.1.3 and higher, Solaris 2.3, 2.4 and 2.5, HP-UX 9 and 10, Bay Networks routers and Xylan switches (limited functionality)
Controlled Routers	Bay Networks, Cisco, 3Com
SecuRemote	Windows 95 and Windows NT

Contacting Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky
Ramat Gan 52520, Israel
Tel: 972-3-613 1833
Fax: 972-3-575 9256

e-mail: info@checkpoint.com

U.S. Headquarters:
400 Seaport Court, Suite 105
Redwood City, CA 94063
Tel: 800-429-4391
415-562-0400
Fax: 415- 562-0410

HTTP://www.checkpoint.com