



Check Point FireWall-1®

Technical Overview

Version 4.0 — April 1999

P/N 3140000010

<http://www.checkpoint.com>

Executive Summary

Expanding Internet technologies have redefined corporate approaches to internetworking and network security. The Internet has become the new forum for business communications and international commerce. Organizations require an innovative solution that integrates all aspects of network security, connectivity, and management.

Check Point Software Technologies Ltd. meets this challenge with FireWall-1, the industry's 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. An integrated product suite extends FireWall-1's capabilities to all levels of security and management.

This document describes the unique features of Check Point FireWall-1. A simple step-by-step procedure demonstrates how to build a FireWall-1 Rule Base and install a Security Policy for a simple network configuration.

In This Document:

<i>FireWall-1 Technology and Architecture</i>	<i>page 2</i>
<i>Enterprise Security Management</i>	<i>page 7</i>
<i>Configuring FireWall-1</i>	<i>page 18</i>
<i>Complementary Check Point Products</i>	<i>page 21</i>
<i>FireWall-1 Platform Summary</i>	<i>page 24</i>

FireWall-1 Technology and Architecture

Stateful Inspection Technology

Check Point's patented Stateful Inspection Technology assures the highest level of network security and performance. A powerful Inspection Module examines every packet passing through key locations in your network (Internet gateway, servers, workstations, routers, or switches), promptly blocking all unwanted communication attempts. Packets do not enter the network unless they comply with the enterprise Security Policy.

FireWall-1 Inspection Module

The FireWall-1 Inspection Module is located in the operating system kernel, below the network layer, at the lowest software level. The Inspection Module analyzes all packets before they reach the gateway operating systems. Packets are not processed by any of the higher protocol layers unless FireWall-1 verifies that they comply with the enterprise Security Policy. The Inspection Module examines communications from any IP protocol or application, including "stateless" protocols, such as UDP and RPC.

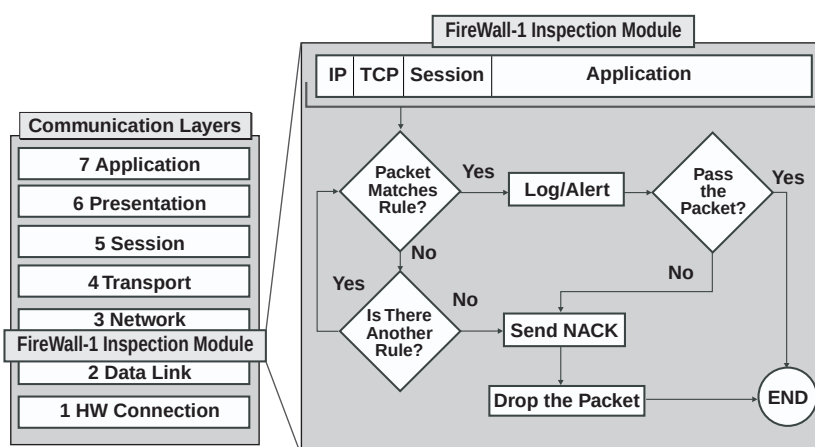


FIGURE 1 Inspecting Communications

Full State Awareness

FireWall-1 examines data from all seven communication layers and also analyzes state information from previous communications. The Inspection Module checks IP addresses, port numbers, and any other information required to determine whether packets are permitted by the enterprise Security Policy.

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. 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.

INSPECT Language

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

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

FireWall-1 Components

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.

FireWall-1 consists of the following components:

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

Graphical User Interface (GUI)

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



FIGURE 2 FireWall-1 Graphical User Interface

Management Server

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

The GUI and the Management Server can be deployed on the same machine or in a Client/Server configuration. For a list of supported platforms for the GUI and the Management Server, see “FireWall-1 Platform Summary” on page 24.

FireWall Module

The FireWall Module is deployed on Internet gateways and other network access points. The Management Server downloads the Security Policy to the FireWall Module, which protects the network. The FireWall Module can be installed on a broad range of platforms. For more information, see “FireWall-1 Platform Summary” on page 24.

The FireWall Module includes the Inspection Module and the FireWall-1 Security Servers. The Security Servers provide Authentication and Content Security features.

Authentication

The Security Servers provide authentication for users of FTP, HTTP, TELNET and RLOGIN. If the Security Policy specifies authentication for any of these services, the Inspection Module diverts the connection to the appropriate Security Server. The Security Server performs the required authentication. If the authentication is successful, the connection proceeds to the target server. For more information on FireWall-1 authentication features, see “Authentication” on page 10.

Content Security

Content Security is available for HTTP, FTP and SMTP.

■ HTTP

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

■ 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 sendmail application that prevents direct online connection attacks. The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the “From” field, while maintaining connectivity by restoring the correct addresses in the response.

For more information on the above features, see “Content Security” on page 13.

Distributed Client/Server Deployment

FireWall-1 manages the enterprise Security Policy through a distributed Client/Server architecture that ensures high performance, scalability and centralized control. FireWall-1 components can be deployed on the same machine or in flexible Client/Server configurations across a broad range of platforms (see “FireWall-1 Platform Summary” on page 24). FIGURE 3 shows a distributed Client/Server configuration.

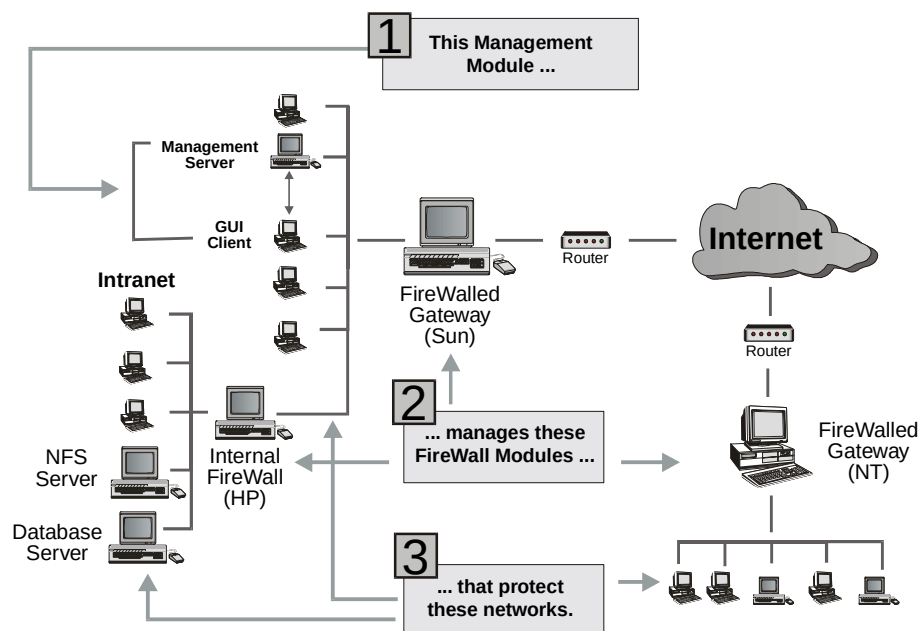


FIGURE 3 Distributed Client/Server Configuration

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

Although 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 that is defined and updated from a centralized management interface.

OPSEC

Check Point's OPSEC (Open Platform for Secure Enterprise Connectivity) integrates all aspects of network security within a single, extensible framework. The OPSEC framework provides central configuration and management for FireWall-1, while integrating third-party security applications. The enterprise security system is composed of several components, each of which may be provided by a different vendor

and installed on a different machine. FireWall-1 distributes security tasks to the OPSEC components. Organizations can choose the security components, from Check Point and other vendors, that best meet their requirements.

OPSEC Integration

OPSEC solutions allow enterprises to take full advantage of the FireWall-1 Security Suite and other security applications. Enterprises can plug into Check Point's OPSEC framework in the following ways:

OEM/Bundling

The FireWall Module or the Inspection Module runs directly on third-party security or networking devices. Example OEM or embedded devices include Alcatel (Xylan) switches or Nortel (Bay Networks) routers.

Check Point APIs

The Check Point OPSEC SDK provides Applications Programming Interfaces (APIs) for open protocols. Administrators can use the OPSEC APIs to configure transactions between FireWall-1 and OPSEC components, such as servers that implement security tasks (for example, anti-virus servers) or clients that use an OPSEC server. The OPSEC SDK includes the following APIs:

- CVP (Content Vectoring Protocol) used to implement content screening and anti-virus checking.
- UFP (URL Filtering Protocol) used to control access to external Web sites.
- SAMP (Suspicious Activity Monitoring Protocol) used to detect and block intrusion attempts.
- LEA (Log Export API) used to retrieve and export FireWall-1 Log data.
- OMI (Object Management Interface) used to develop a client that can query, modify and install a FireWall-1 Security Policy.

Open Industry-Standard Protocols

FireWall-1 supports industry-standard network security and management protocols to enable the integration of third-party security products and network management tools. Example standards include:

- RADIUS (Remote Authentication Dial-in User Service) used to authenticate dial-up users. RADIUS servers are available from third-party vendors such as Axent and Security Dynamics.
- LDAP (Lightweight Directory Access Protocol) used to integrate and manage user directories.

Integrated OPSEC solutions can be configured and managed using the FireWall-1 graphical user interface. Check Point tests and certifies all OPSEC solutions for interoperability.

Enterprise Security Management

Defining a Security Policy

The FireWall-1 GUI enables an enterprise to easily define a comprehensive Security Policy. A 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.

Security Policy Address Translation							
No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	FW_HQ	Any	reject	Alert	Gateways	Any
2	FW_HQ	Any	Any	reject	Alert	Gateways	Any
3	All Users@Any	pub_servers	smtp	User Auth	Short	Gateways	work_hours
4	localnet	Any	Any	accept	Long	Gateways	Any
5	Any	Any	Any	drop		Gateways	Any

FIGURE 4 Rule Base

Properties

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

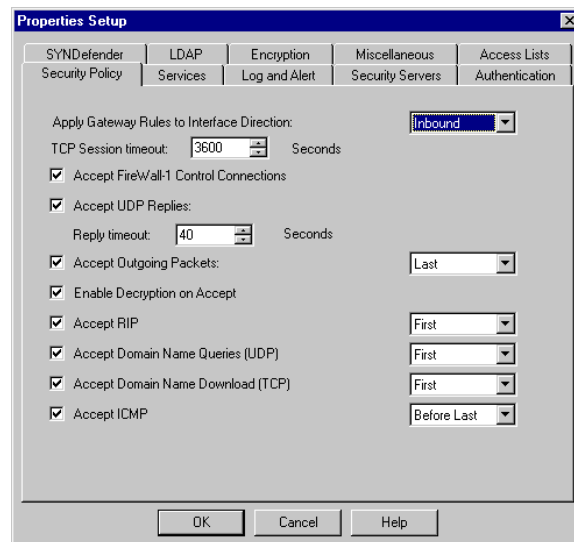


FIGURE 5 Properties Setup Window

Network Objects

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

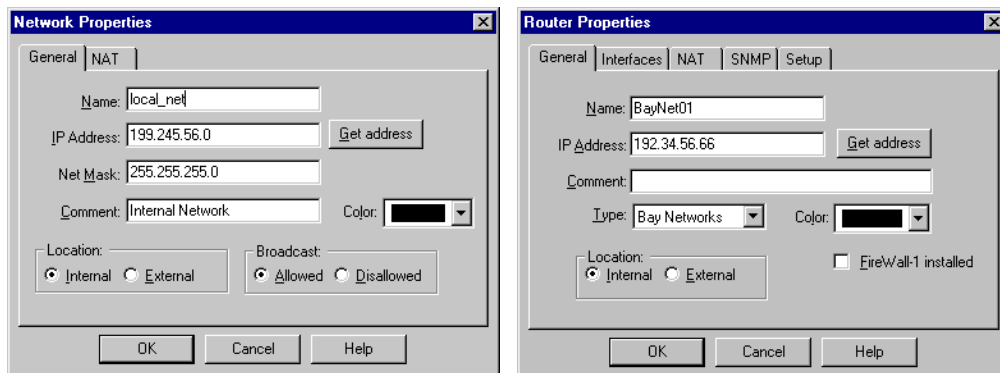


FIGURE 6 Network and Router Object Definitions

Log Viewer: Visual Tracking and Accounting

FireWall-1's graphical Log Viewer provides visual tracking, monitoring and accounting information for all connections logged by the FireWalled gateways. On-line viewing features enable real-time monitoring of network activity. The Log Viewer provides control over the log file display, providing quick access to information. Administrators can customize the Log Viewer to display or hide specific fields or events. Logs and log records can be filtered and searched to quickly locate and track events of interest.

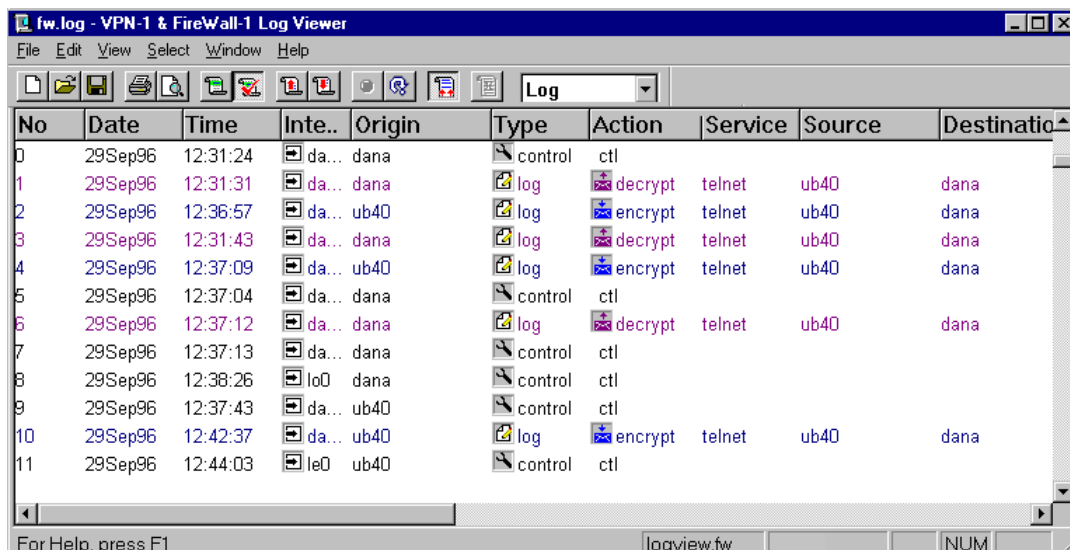


FIGURE 7 Log Viewer

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

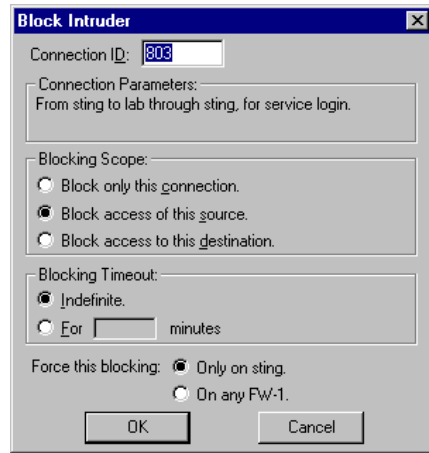


FIGURE 8 Blocking Suspicious Connections

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

Real-time Monitoring: System Status Viewer

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

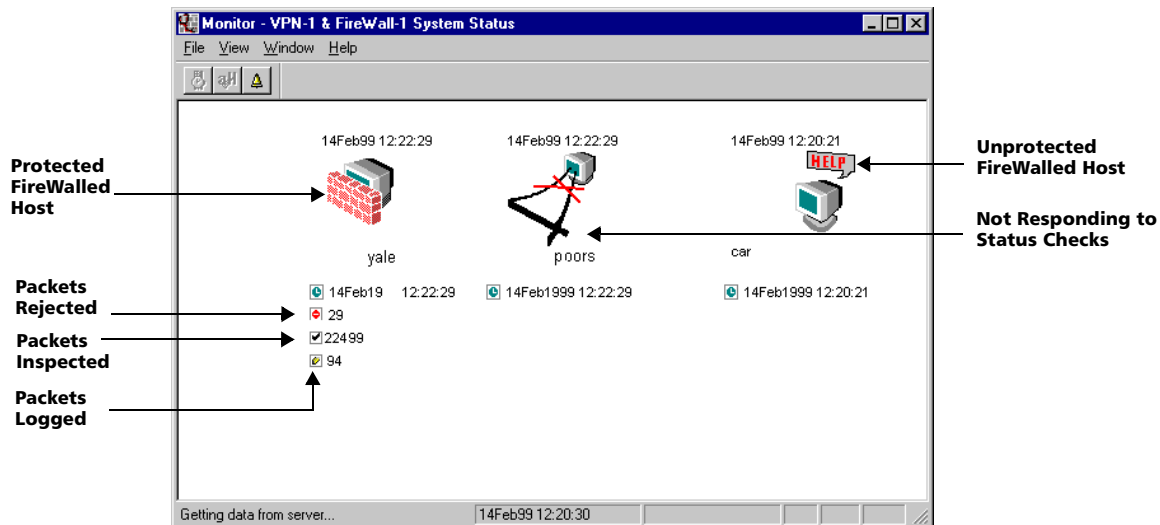


FIGURE 9 System Status Window

Security and Network Management

In addition to highly granular access control, 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 FireWall-1 Security Suite includes the following capabilities:

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

Authentication

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.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	 All Users@Any	 pub_servers	 smtp	 User Auth	 Short	 Gateways	 work_hours

FIGURE 10 User Authentication Rule

Multiple Authentication Schemes

FireWall-1 supports the following authentication schemes:

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

Authentication Methods

FireWall-1 provides the following authentication methods:

■ User Authentication

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

■ Client Authentication

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

■ Session Authentication

Session Authentication can be used to transparently authenticate any service on a per-session basis. After the user initiates a connection to a server behind the FireWalled gateway, FireWall-1 opens a connection with a Session Authentication Agent. The Agent challenges the user for a proper authentication response before FireWall-1 allows the connection to continue to the requested server. The Session Authentication Agent is installed on the authenticating client or on another machine in the network.

Transparent User-to-Address Mapping (UAM) Service

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

For more information on Meta IP, see "IP Address Management — Meta IP™" on page 23.

Network Address Translation

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

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

- Graphical Address Translation Rule Base
- Automatic Configuraton

Graphical Address Translation Rule Base

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

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

FIGURE 11 Address Translation Rule Base

Automatic Configuration

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

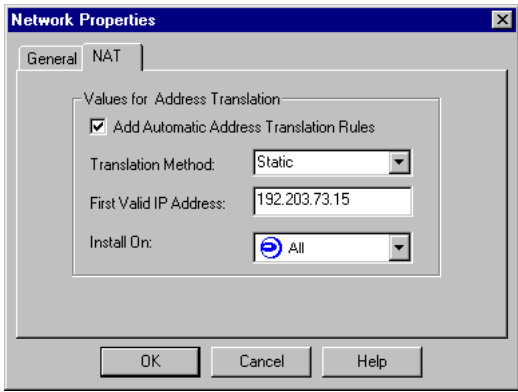


FIGURE 12 Automatically Generating Address Translation for a Network

Virtual Private Networks

When integrated with Check Point's optional VPN module, FireWall-1 provides the ideal platform for enterprise VPN deployments. This integration forms Check Point's VPN-1 Gateway solution and encrypts communications to guarantee data privacy and security. In addition to site-to-site VPN capability, VPN-1 Gateway deployments can provide access to remote users when used with Check Point's VPN-1 SecuRemote Client software.

Check Point's VPN-1 Gateway product supports industry-standard algorithms and protocols, such as DES, Triple DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments. VPN-1 Gateway is just one component of Check Point's VPN-1 product family. For more information, see "Complementary Check Point Products" on page 21.

Content Security

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

Resources

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

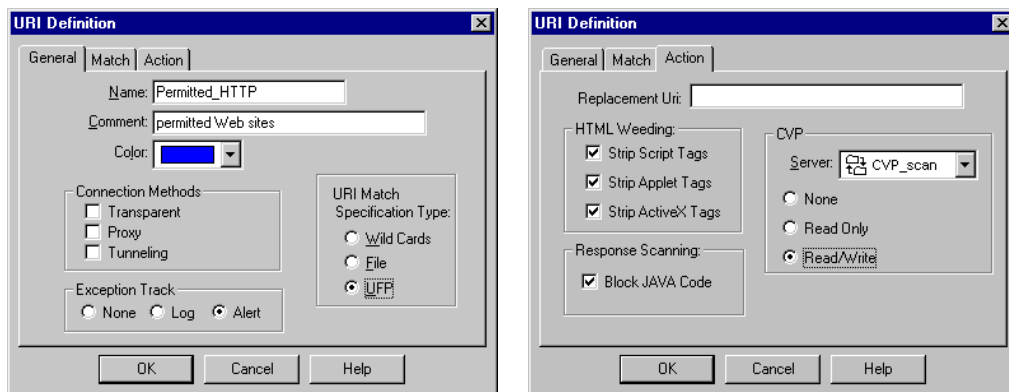


FIGURE 13 URI Resource Definition tabs

Resources can be used in a Rule Base in exactly the same way as a service (see FIGURE 14 on page 14). When a connection matches a rule with a Resource, the 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. FireWall-1 processes the original connection depending on the reply from the server and the action in the rule.

No.	Source	Destination	Service	Action	Track	Install On
1	 localnet	 Any	 http->Permitted_sites	 accept	 Long	 Gateways

FIGURE 14 URI Resource Rule

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) API. 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, which examines the files. 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. 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

FireWall-1's extensive screening capabilities effectively protect enterprise networks from Java and ActiveX attacks. 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

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

High Availability

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

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

Utilizing multiple FireWall Modules with state table synchronization has the additional benefit of providing asymmetric routing support. The synchronization of state information is necessary when packets that are part of the same session travel via

different routes and pass through different gateways. Without accurate state information on all communications, a FireWall Module may not recognize a packet that is part of an authorized session and will drop or reject that packet.

ConnectControl™ — Server Load Balancing

FireWall-1's optional ConnectControl module enhances network connectivity through advanced server load balancing. 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. The Logical Server handles the connection attempt using one of five possible pre-defined load balancing algorithms.

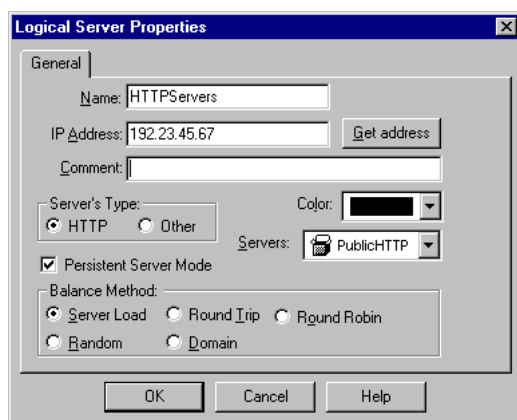


FIGURE 15 Logical Server Properties Definition

FireWall-1 includes the following load balancing algorithms:

- **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.
- **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.
- **round robin** — FireWall-1 simply assigns the next server in the list.
- **random** — FireWall-1 assigns a server at random.
- **domain** — FireWall-1 assigns the “closest” server, based on domain names.

LDAP Account Management

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

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

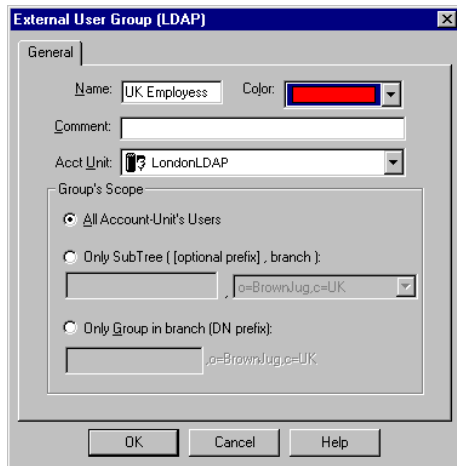


FIGURE 16 External User Group (LDAP) window

The Account Management system includes a Java-based graphical user interface for managing LDAP users. The Account Management Client can be launched from the FireWall-1 GUI or as a standalone application. Administrators can use the Account Management Client to define “live templates” that can be used to apply common configuration properties to multiple users. Changes to the template are automatically applied to all users associated with the template. All communication between FireWall-1, the Account Management Client and LDAP servers is secured through SSL.

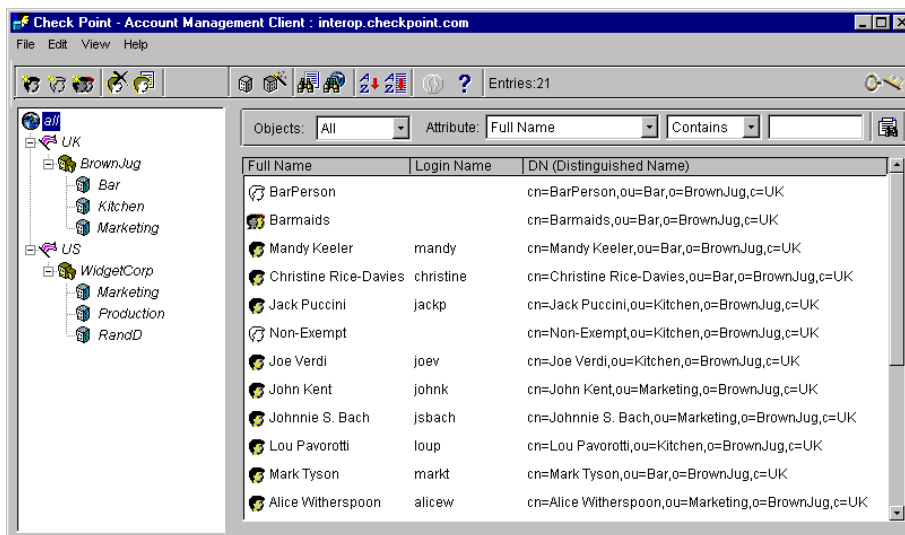


FIGURE 17 Account Management Client

Open Security Extension

Check Point's Open Security Extension is an optional module that enables FireWall-1 to manage an enterprise-wide Security Policy for a variety of third-party network security devices, including products from Cisco, Nortel (Bay Networks), 3Com and Microsoft. The Security Policy is defined using the FireWall-1 Rule Base Editor. 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, FireWall-1 also imports existing Access Lists and compiles them into object-oriented security policies for simpler management. In addition, FireWall-1 displays syslog messages from third-party security devices in the graphical Log Viewer, delivering centralized logging and reporting capability. With Open Security Extension, devices from multiple vendors are seamlessly integrated into the network and managed through the Security Policy.

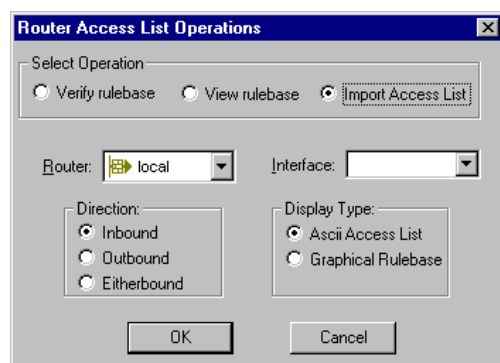


FIGURE 18 Router Access List Import Options

Configuring FireWall-1

A FireWall-1 Security Policy is simple to define and implement. This section shows how to define a Security Policy for a small enterprise with a simple network configuration.



Note – This configuration is an example for the purposes of this document only.

A Simple Configuration

A small multimedia and web design company has 20 employees, a small internal network and a DMZ network which includes a mail server. Employees use the Internet for e-mail, FTP and HTTP services to communicate with customers and access the Web. While employees require complete Internet access, the company wants to protect the internal network. At the same time, employees need to receive mail from customers located outside of the corporate network. In this configuration, FireWall-1 is installed on a gateway machine.

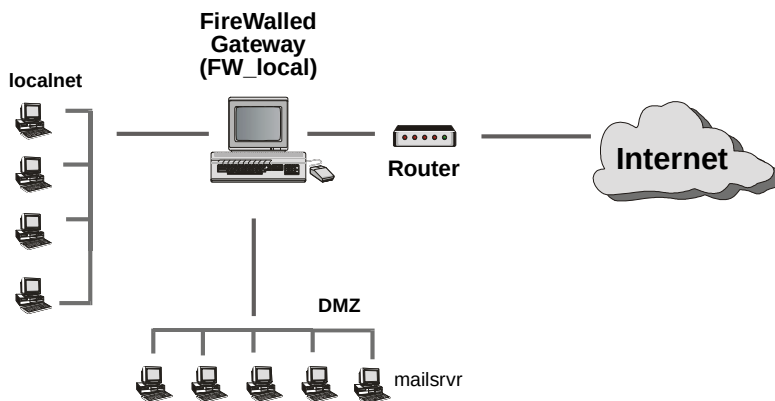


FIGURE 19 Simple Network Configuration

A Typical Security Policy

For the above configuration a typical Security Policy might consist of the following:

- external users may access the local network only to send mail to local computers
- internal users may access the entire network: localnet, the mail server on the DMZ, and the Internet

This policy protects the private network from untrusted external users but puts no restrictions on local users.

Defining and 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 — only the objects that are used in the Rule Base. For the configuration described here, you must define the gateway (FW_local), the mail server (mailsrvr) and the local network (localnet).

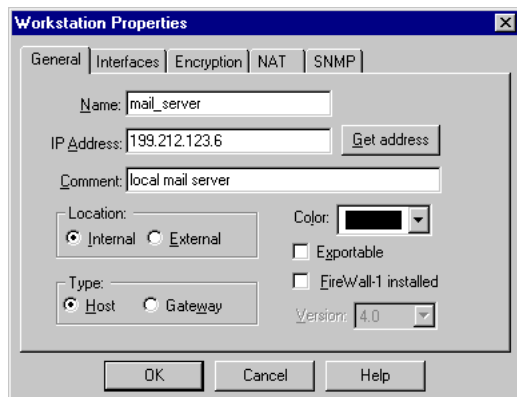


FIGURE 20 Workstation Properties Window — Mail Server Definition

- 2 Define services used in your Security Policy.
You do not have to define commonly used services, such as SMTP. FireWall-1 includes more than 150 pre-defined services to facilitate administration. You only have to define any custom services that are used in your network.
- 3 Define the Rule Base — the rules for accepting, rejecting and logging packets.

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

The first rule (external users may only send mail to the mail server) can be expressed in the Rule Base Editor as follows:

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

The second rule (internal users may access the entire network: localnet, the mail server on the DMZ, and the Internet) can be expressed in the Rule Base Editor as follows:

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

FireWall-1 drops all communications that are not explicitly permitted by the Security Policy. Rules are examined sequentially and the first rule that matches a connection is applied. An implicit rule at the end of the Rule Base drops all connections that do not match the previous rules. You can explicitly define a rule that logs these connections as follows:

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

Even if you do not define this rule, FireWall-1 will not allow these connections. The advantage of defining this rule is that you now have a record of communication attempts that are not permitted by the Security Policy.

FIGURE 21 shows the Rule Base Editor with the three rules defined.

Security Policy Address Translation						
No.	Source	Destination	Service	Action	Track	Install On
1	Any	mail_server	smtp	accept	Short	Gateways
2	localnet	Any	Any	accept	Short	Gateways
3	Any	Any	Any	reject	Long	Gateways

FIGURE 21 Rule Base Editor Showing All Rules

The above Rule Base shows that it is simple to define the required rules for a Security Policy. A simple Rule Base can be modified with additional rules to meet the specific requirements of any enterprise.

- 4 Install the Security Policy — load the Inspection Code to the gateways. You can also install the Security Policy on routers using the Open Security Extension module.

The Security Policy is installed using the Rule Base Editor. The Rule Base Editor allows you to specify the FireWalled machines and enforcement points that will implement the Security Policy.

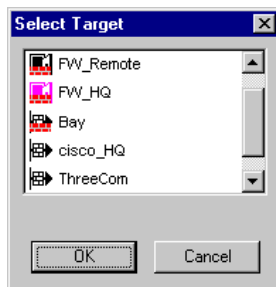


FIGURE 22 Selecting Enforcement Points

Complementary Check Point Products

Check Point offers a suite of security and network management products fully integrated with FireWall-1. These solutions extend FireWall-1's capabilities to provide secure enterprise connectivity.

Network Security

VPN-1 Products

Check Point VPN-1 products allow organizations to take full advantage of Virtual Private Networks. VPN-1 products create secure communication channels over the Internet, assuring full privacy, authenticity and data integrity in corporate internetworking. VPNs are centrally configured and managed as part of the enterprise Security Policy.

VPN-1 Products include the following:

- **VPN-1 Gateway™**
VPN-1 Gateway is a tightly integrated software solution comprised of Check Point's market-leading FireWall-1 enterprise security suite and advanced VPN-1 technology. With Check Point VPN-1 Gateway, network administrators can deploy and manage an integrated solution for network security and VPN capability. Check Point VPN-1 solutions support industry standard algorithms and protocols (IPSec, IKE, Triple DES, etc.) and are available for single gateway deployments as well as multi-site, enterprise-wide VPNs with centralized management.
- **VPN-1 RemoteLink™**
VPN-1 RemoteLink is a complete hardware and software security appliance solution providing secure Internet access for branch office deployments. VPN-1 RemoteLink includes complete enterprise security with FireWall-1, Virtual Private Networking with VPN-1, and integrated IP routing — all in a single appliance that can be quickly deployed and safely managed from a centralized management console.
- **VPN-1 SecuRemote™**
This client-side encryption software extends the enterprise VPN to desktop, remote, and mobile users. With VPN-1 SecuRemote, Windows 95, Windows 98, and Windows NT users can connect to the corporate network via dial-up Internet connections and establish secure VPN sessions. Unlimited SecuRemote clients can be deployed with VPN-1 Gateway and VPN-1 RemoteLink products at no additional cost.
- **VPN-1 Certificate Manager™**
VPN-1 Certificate Manager provides a complete turnkey public key infrastructure (PKI) solution for Check Point VPN-1 Gateway solutions. VPN-1 Certificate Manager integrates best-of-breed PKI-based certificate authority and LDAP directory server technologies with a unified installation procedure and centralized policy-based management interface. This streamlined solution supports strong authentication for both site-to-site and client-to-site VPNs, using X.509 digital certificates.

■ VPN-1 Accelerator Card™

This plug-and-play hardware PCI card for Sun Solaris and Windows NT platforms speeds VPN performance through acceleration of strong data encryption algorithms. The VPN-1 Accelerator Card improves performance up to 10 times greater than software-only solutions by accelerating both DES and Triple DES encryption in an IPSec IKE virtual private network. This product is ideal for demanding VPN environments where high data throughput rates (up to 45 mbps) must be supported.

Provider-1™

Check Point Provider-1 pairs network security capabilities with powerful policy-based management capabilities developed specifically for Managed Service Providers (MSPs). Provider-1 enables MSPs to centrally create and manage the network security policies of multiple corporate customers on a single hardware server, while maintaining complete and secure isolation between individual customer databases. Provider-1 enables MSPs to dramatically reduce the hardware and personnel costs associated with managed security services.

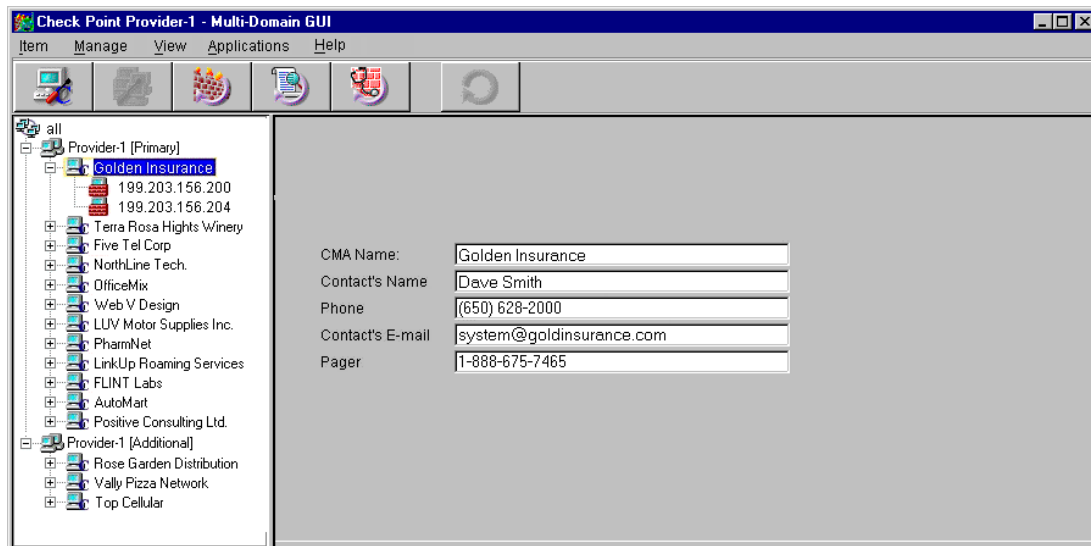
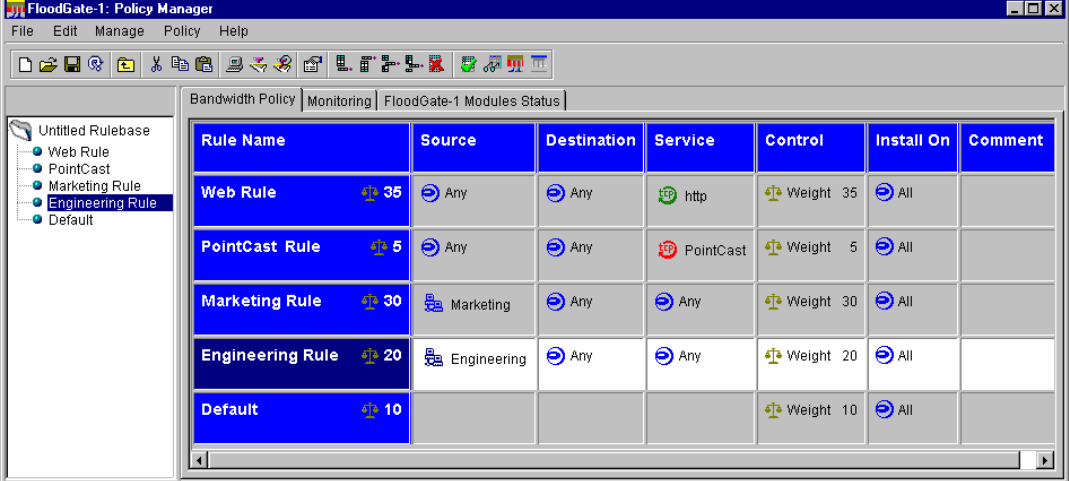


FIGURE 23 Provider-1 Multi Domain GUI

Enterprise Traffic Management — FloodGate-1™

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



The screenshot shows the 'FloodGate-1: Policy Manager' window. On the left is a tree view of the 'Untitled Rulebase' containing 'Web Rule', 'PointCast', 'Marketing Rule', 'Engineering Rule', and 'Default'. The main area displays a table for the 'Bandwidth Policy'.

Rule Name	Source	Destination	Service	Control	Install On	Comment
Web Rule	Any	Any	http	Weight 35	All	
PointCast Rule	Any	Any	PointCast	Weight 5	All	
Marketing Rule	Marketing	Any	Any	Weight 30	All	
Engineering Rule	Engineering	Any	Any	Weight 20	All	
Default				Weight 10	All	

FIGURE 24 FloodGate-1 Bandwidth Policy

IP Address Management — Meta IP™

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

FireWall-1 Platform Summary

Component	Platforms
FireWall-1 GUI Client (Client/Server configuration)	Windows 95, Windows 98, Windows NT (3.51 and 4.0 - Intel only) X/Motif (on Solaris 2.5 and 2.6, HP-UX 10.x, IBM AIX 4.2.1 and 4.3.0)
FireWall-1 Management Server (Client/Server configuration)	Windows NT (3.51 and 4.0, Intel only), Solaris 2.5 and higher, HP-UX 10.x, IBM AIX 4.2.1 and 4.3.0
FireWall-1 Management Module (OpenLook GUI)	Solaris 2.5 and higher
FireWall-1 FireWall Module	Windows NT (Intel only), Solaris 2.5 and higher, HP-UX 10.x, IBM AIX 4.2.1 and 4.3.0, Nokia IP Routing
FireWall-1 Inspection Module	Windows NT (Intel only), Solaris 2.5 and 2.6, HP-UX 10.x, IBM AIX 4.2.1 and 4.3.0, Bay Networks, Xylan (limited functionality)
SecuRemote	Windows 95, Windows 98, Windows NT (3.51 and 4.0, Intel only)

© 1999 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:

Check Point, the Check Point logo, FireWall-1, FloodGate-1, INSPECT, IQ Engine, Open Security Manager, Open Security Extension, OPSEC, Provider-1, VPN-1 Accelerator Card, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 RemoteLink, VPN-1 SecuRemote, and ConnectControl are trademarks or registered trademarks of Check Point Software Technologies Ltd. Meta IP and User-to-Address Mapping are trademarks of MetaInfo, Inc., a wholly-owned subsidiary of Check Point Software Technologies, Inc. RealSecure is a trademark of Internet Security Systems, Inc. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Check Point Software Technologies Ltd.

International Headquarters:

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

e-mail: info@Checkpoint.com

U.S. Headquarters:

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

<http://www.checkpoint.com>

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