
# 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:**

# Copyrights and Trademarks



## 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.

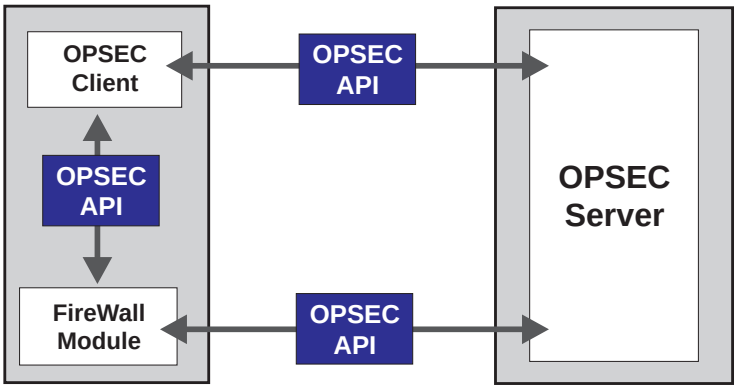


Figure 1 OPSEC Client/Server Communication

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.

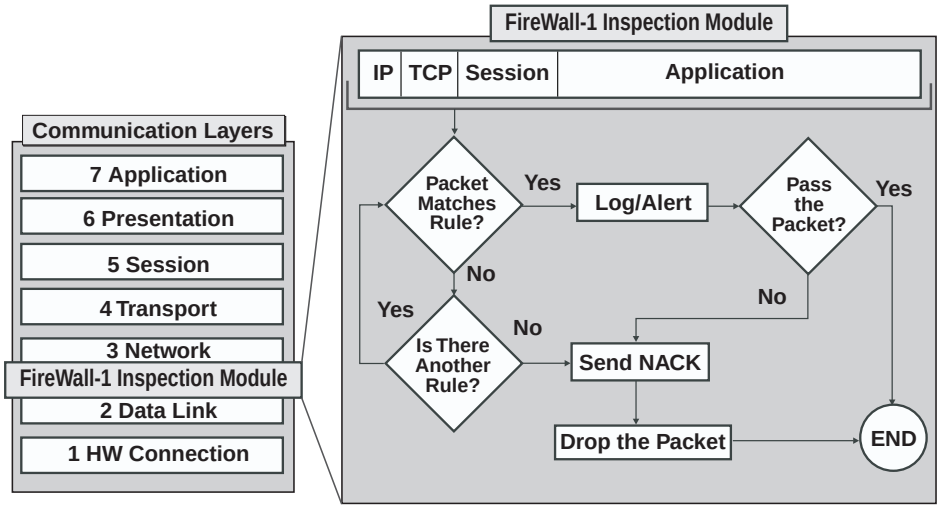


Figure 2 FireWall-1 Inspection Module

## 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

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.