CHECK POINT

CheckPoint FireWall-1™

Technical White Paper

info@CheckPoint.COM

Executive Summary

Setting up a "firewall" system that controls access from the Internet to a private network, stopping break-in attempts, is the single most important security measure to be taken when connecting to the Internet. This document describes the architecture and unique characteristics of CheckPoint's FireWall-1 Internet gateway security system. It outlines the major technology characteristics that enable CheckPoint FireWall-1 to establish full, transparent and true Internet Connectivity using the entire range of Internet protocols while ensuring network security.

Two mainstream methods are currently used to establish Internet firewalls:

- Application gateways: They are Secure but Inefficient. They are either Non-transparent to users and applications or Hard to set-up and Manage. Only a limited set of applications are supported and special tailoring is needed for each one.
- Packet Filtering: This is Insecure yet more Efficient. It is Transparent and Comprehensive to many protocols and applications, yet is Stateless. Traditional packet filters have only a Low-level protocol understanding and are Difficult to set up and verify. Lack of auditing mechanisms is also a major drawback.

CheckPoint FireWall-1 combines both methods to create an Efficient, Generic and Secure packet filtering engine. It is capable of Application level security, Unified support and handling of all protocols, Auditing and Alerting, and Transparent operation to users and system setup.

In addition to the filtering technology, CheckPoint FireWall-1 includes an object oriented Graphical User Interface that enables Simple and Flexible Management and Configuration.

Internet Firewalls Technology

When connecting a network to the Internet or to other networks, the most important security measure is to control access from the other networks to the private one. Securing the Internet link is done by putting a "firewall" system between the secured network and the Internet. The firewall's role is to ensure that all the communication between an organization's network and the Internet conforms to the organization's security policy. Additional means such as authentication and privacy enhancements may follow and complement firewalls, but stopping the "fire" from spreading into the private network is the first thing to do.

Two major techniques apply when building an Internet firewall:

- Application level and circuit gateways
- Packet filtering gateways

The major difference between the two techniques (which are commonly used in conjunction) lies in the communication flow. A packet filter gateway acts as a router between the two networks; packets flow from their source to destination, and the gateway either forwards or blocks the packets. When using application and circuit gateways, all packets are addressed to a user level application on the gateway that links between the two communication points by relaying the packets. In most application gateway implementations, additional packet filter machines are required to control and screen the traffic between the gateway and the networks. A typical configuration includes two routers with a "bastion host" in the middle, that acts as the application gateway.

Application Level and Circuit Gateways

For each application relayed, application level gateways use a specific, special purpose code. Application gateways can provide a high level of security, though they suffer from a number of deficits: only a limited number (usually only a small basic subset) of the applications and services are supported. In order to use the application gateways, user have to log into the gateway machine or to install a specific client application that uses the application gateway for each application they intend to use. Each "gatewayed" application is a different proprietary software and requires its own set of management tools and permissions.

Circuit gateways provide a more general way to implement application gateways. They may support some TCP applications, yet not all of them and not other protocols. However, users are still forced to use and install different client applications or change their work habits. Installing client applications on each internal computer may be a cumbersome task since the internal network is typically heterogeneous with respect to platforms, operating systems, versions, etc.

Network performance is also affected by both application gateways and circuit gateways: each packet must be processed twice by all communication layers, requires user-level processing and context switching. It should also be noted that the application gateway computer itself ("bastion-host" or "dual-homed gateway") remains exposed to the network, and additional means should be implemented to protect it (packet filtering). This typically results in limiting the available service and also additional hardware.

Packet Filtering Gateways

Packet filtering technologies provide an efficient and general way to control any type of network traffic and applications, requiring no changes in client applications, no specific applications management nor installation, and no additional hardware. Using a single unified packet filtering engine, the entire network traffic is processed and forwarded or blocked from a single point of control.

Historically, packet filtering technologies did not address all the security requirements. Only basic and insufficient information was available for filtering (e.g. only source and destination address and port numbers), the number of rules was limited and high performance penalty was paid when using many rule instances. Lack of context or state information has eliminated the possibility of using packet filters for datagram based protocols like UDP and RPC. Auditing and alerting mechanisms were also missing in most cases. Previous packet filtering technologies also suffered from poor management interfaces. Implementing them requires high level of understanding of the communication internals, writing low-level bit and bytes code, making it very hard to change and adopt and easy to err. Some packet filters are implemented inside routers' hardware, thus having limited computing power and filtering capabilities. Others are implemented as software packages commonly processing the packets in user-level process requiring multiple data copies, expensive delays and context switches, and delivering lower throughput.

Most existing Internet firewalls use a combination of packet filter screening computer or hardware-router (for controlling the lower layers of communication), with application gateways (for the enabled applications). This setup provides only limited non-transparent and non-flexible connectivity, yet requires a high level of price in setup time, management, and expertise.

CheckPoint FireWall-1

CheckPoint FireWall-1 combines the efficiency of implementing a general purpose solution for all network protocols, with application level savvy. As part of the interface a comprehensive installation procedure and logging and alerting mechanisms are included. On top of this unique protocol independent technology, a simple, intuitive, object-oriented user interface enables easy, flexible and uniform way of implementing the organization's global security policy. Following sections detail the functions of FireWall-1.

FireWall-1 Overview

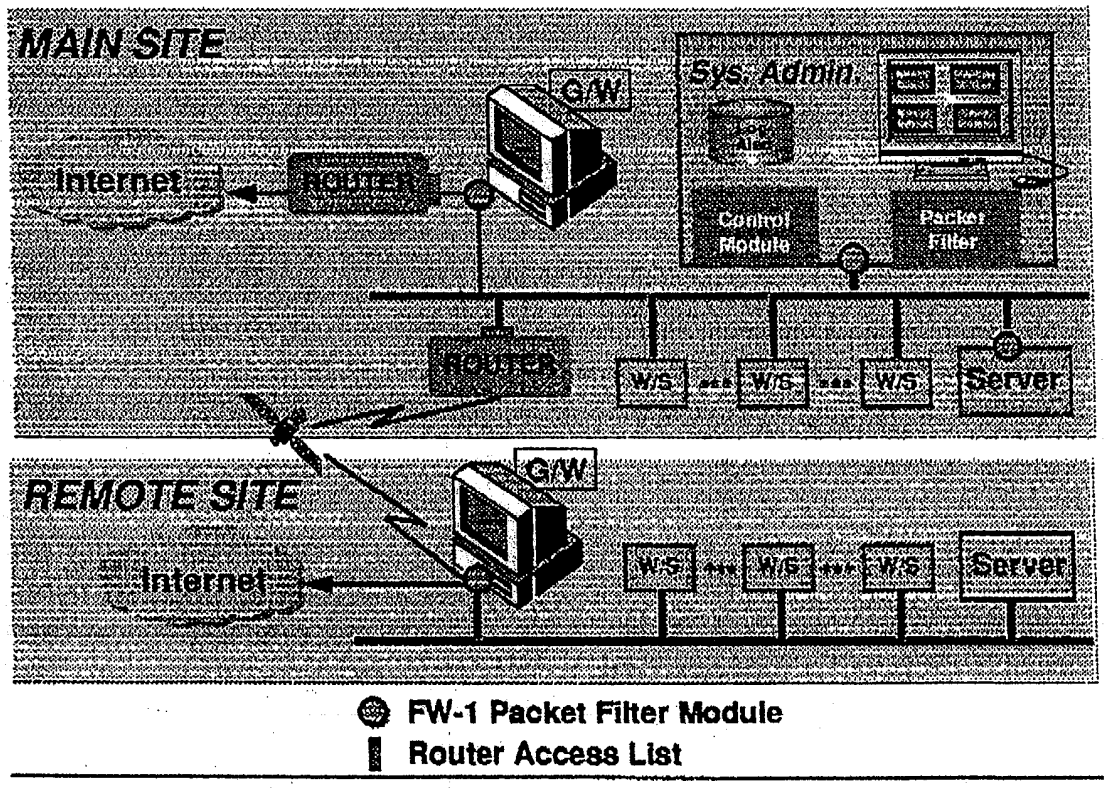
The CheckPoint FireWall-1 Internet Gateway acts as a router between the organization's internal networks and the Internet. All the network traffic between the organization's internal network, Internet sites, and the application gateways between them is routed through the gateway. This ensures full security coverage of the entire spectrum of Internet protocols and services and that each and every packet is screened and verified to comply with the organization's security policy. ensuring full security coverage of the entire spectrum of Internet protocols and services.

CheckPoint FireWall-1 is composed of two major components:

- Packet Filter Modules — a mainly packet filtering firewall
- Control Module

A single Control Module can control and monitor multiple Packet Filter Modules. The Packet Filter Module operates autonomously of the Control Module, providing an on-going, simple, powerful, and reliable packet filtering. Packet Filter Modules can operate on additional Internet gateways, as well as inter-departmental gateways and on critical servers, thus providing peripheral defense as well as in-depth security and compartmentalization.

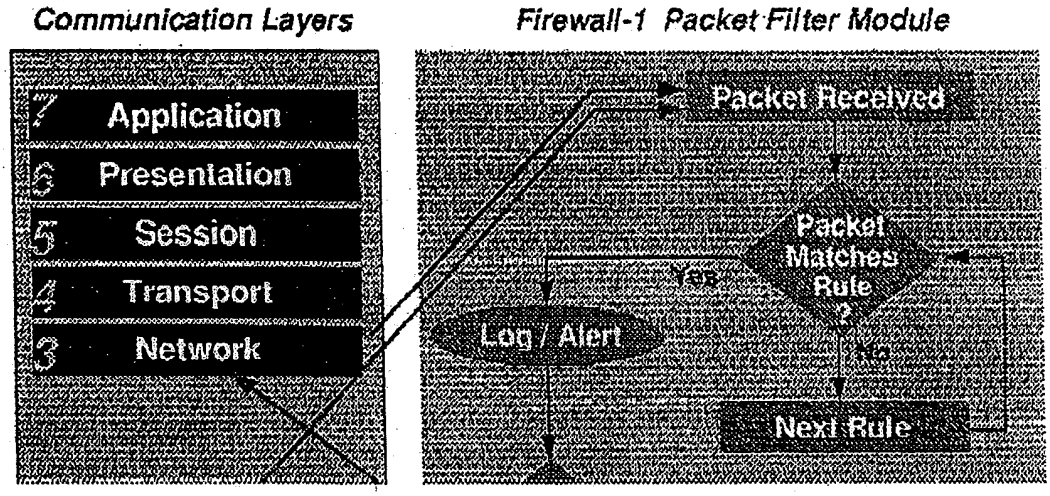
The control workstation and packet filter module can reside either on the same gateway machine, or on two different hosts. In the latter, communication between the two is authenticated, using a one-time-password authentication scheme.



CheckPoint's Packet Filter Module Architecture

CheckPoint FireWall-1 packet filter module resides on the gateway host, acting as a security router between the protected networks. The packet filter module is plugged between the Data Link and the Network layers (layers 2 and 3). The Data Link being the actual network interface card (NIC) and the Network Link is the first layer of the protocol stack (e.g. IP). Inbound and outbound packets on gateway are intercepted and subjected to the security rules defined and installed in the packet filter module. Filtering at this layer ensures that no packet is processed by the various protocol stack layers before being verified to comply with the security policy.

Packets that are not explicitly to be accepted by the security policy, are simply dropped ("That which is not expressly permitted is prohibited").



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.