

## Firewall Basics

by: Manu Arian, 07/27/2004

<http://www.securitydocs.com/library/2413>

### What is a firewall?

A firewall is a gateway that restricts and controls the flow of traffic between networks, typically between an internal corporate network and the Internet. Firewalls may also provide secure gateway services between internal networks. For example, a military installation may have two networks, one for non-classified general communications and another network that is connected to strategic defense systems. A very secure firewall must be in place to ensure that only authorized users access the defense network. In some cases, no connection may be the most secure policy.

Castles and castle defenses are often used as an analogy in describing firewalls. A castle is designed to protect the people on the inside from the storming hoards on the outside. There is a perimeter defense system that keeps attackers as far away as possible (outer walls, moats, and so on). The castle gate is the “choke point” through which people and supplies must pass to enter or exit the castle. It is the most heavily defended part of the castle.

A firewall is a “choke point” for internal networks that actively inspects and controls the flow of traffic between networks. In the case of a proxy firewall, traffic never flows directly between the networks. Instead, the proxy “repackages” request and responses. No internal host is directly accessible from the external network and no external host is directly accessible by an internal host. Think about the people in the castle. During times of tension, they may prefer to stay inside the castle and use proxy agents to take care of their business on the outside.

Part of the design of a secure Internet-connected network is to create what is called a “demilitarized zone” or DMZ, which is a network that exists between the protected and the unprotected network. The DMZ is protected by a perimeter defense system, much like the outer walls and moats of a castle. Picture the market yard of a castle. In medieval times, local townspeople and traders were usually allowed to enter the yard with relative ease so they could deliver or pick up goods. At night, the gates were closed and goods were brought into the castle—usually after close inspection. Guards were posted at the gates during the day to scrutinize all the people coming into the market yard. If known hooligans tried to enter, they were immediately pointed in the other direction and given the boot.

The DMZ between the protected and unprotected network follows this analogy. Internet users can freely enter the DMZ to access public Web servers, but screening routers exist at the access point to filter out unwanted traffic, such as floods of packets from hackers who are trying to disrupt operations. At the same time, the internal private network is protected by highly secure firewalls. Within the castle walls was the keep, a heavily fortified structure that provided the last defense against attackers.

Interestingly, the castle proved quite capable of withstanding attacks until the cannon came along. In the 16th century, Essex and Cromwell overran many castles in Ireland with little force. They simply blew the parapets off the top of castle walls to make them indefensible, and then scaled the walls. What similar weapons will our network defenses face? Firewalls have become quite sophisticated over the years, but they are not an all-in-one security solution. Firewalls are just one tool in the arsenal of security tools available to security administrators. Note the following:

- A firewall may consist of several pieces of equipment, including a router, a gateway server, and an authentication server.
- Firewalls monitor incoming and outgoing traffic and filter, redirect, repackage, and/or discard

packets. Packets may be filtered based on their source and destination IP address, source and destination TCP port numbers, setting of bits in the TCP header, and so on.

- In the case of a proxy firewall, the firewall is the endpoint of the incoming and outgoing connection. It can perform extensive security and validation scans on the packets it processes. The proxy runs safe, uncorrupted, and bug-free versions of protocols and software.
- Firewalls can enforce an organization's security policies by filtering the outgoing traffic of internal users to ensure that it complies with usage policies.
- Sophisticated logging, auditing, and intrusion detection tools are now part of most commercial firewalls.
- RFC 2979, "Behavior of and Requirements for Internet Firewalls," (October 2000) describes other firewall characteristics.

Hackers and attackers just keep getting smarter, more aggressive, and more numerous. In 2000, China announced that it could not keep up with the United States militarily, and threatened to wage an information war on the United States. Computer systems at U.S. military installations are under constant attack by both sophisticated and unsophisticated attackers. How many undetected intruders are in those systems?

For example, an attacker may set up an attack well in advance by using e-mail virus techniques to plant so-called "zombie" programs on hundreds or thousands of computers owned by innocent Internet users, many within your own network. The programs are set to wake up at specific times and begin launching attacks against other systems. The real attacker cannot be identified because the attacks are coming from innocent users all over the Internet. The entire Internet can become a weapon aimed at your private network.

Because of these threats, firewalls are now needed in nearly every Internet connected computer, especially those that are connected to "always-on" services, such as DSL and cable (CATV) connections. A typical home setup is to network the parent's and the kid's computers together, and share a single DSL or cable connection to the Internet. Since the connection is always on, it has a continuous IP address that is posted like a flag on the Internet. Hackers will eventually find the IP address and keep coming back to examine and disrupt systems. Firewalls are designed to protect these systems while minimizing complex setup procedures.

### **Firewall Terminology**

A standard firewall terminology helps remove the confusion surrounding firewall technology. RFC 2647, "Benchmarking Terminology for Firewall Performance," (August 1999) is one document that attempts to establish such terminology. The most important terms it describes are outlined next. Refer to the RFC for a more complete description. The following list has been reordered for clarity and reworded for conciseness.

Firewall -A device or group of devices that enforces an access control policy among networks. Firewalls connect protected and unprotected networks, or support tri-homing, which allows a DMZ network.

Protected network -A network segment or segments to which access is controlled. Protected networks are sometimes called "internal networks," but RFC 2647 states that the term is inappropriate because firewalls increasingly are deployed within an organization, where all segments are by definition internal.

Unprotected network -A network segment or segments to which access is not controlled by the firewall.

Demilitarized zone (DMZ) -A network segment or segments located between protected and unprotected networks. The DMZ may not be connected to the protected network in any way. The DMZ may also

include perimeter defense systems. For example, The DMZ can be made to look like it is part of the protected network, luring hackers into traps that log their activities and attempt to track the source of the activity.

Dual-homed firewall -A firewall with two interfaces, one attached to the protected network and one attached to the unprotected network.

Tri-homed firewall -A tri-homed firewalls connect three network segments with different network addresses. Typically, these would be protected, DMZ, and unprotected segments.

Proxy -A request for a connection made on behalf of a host. A proxy stands between the protected and unprotected network. Think of a quarantined area where people on the inside use a telephone to talk to people on the outside. All external connections leading into the proxy terminate at the proxy. This effectively eliminates IP routing between the networks. The proxy repackages the messages into new packets that are allowed into the internal network. The proxy also terminates internal traffic that is headed out to the Internet and repackages it in a new packet with the source IP address of the proxy, not the internal host. Most important, the proxy inspects and filters traffic. A predefined “rule set” is used to determine which traffic should be forwarded and which should be rejected. There are two types of proxies: application proxies and circuit proxies, as described shortly.

Network address translation (NAT) -A method of mapping one or more private, reserved IP addresses to one or more public IP addresses. NAT was defined to conserve IPv4 address space and refer to a specific block of IP addresses that are never recognized or routed on the Internet. It allows organizations to use their own internal IP addressing scheme. A NAT device translates between internal and external addresses, and is usually combined with proxy services. NAT devices are implemented in firewalls to support the private addressing scheme as defined in RFC 1918.

Application proxy -A proxy service that is set up and torn down in response to a client request, rather than existing on a static basis (as is the case with circuit proxies). The application proxy performs all of the services of a proxy, but for specific applications. In contrast, a basic proxy performs generic packet filtering. The application proxy only processes packets related to the applications that it supports. If code is not installed for an application, those incoming packets are dropped. Packets are only forwarded after a connection has been made, which is subject to authentication and authorization.

Circuit proxy - A proxy service that statically defines which traffic will be forwarded. The circuit proxy is a special function performed by application proxies, usually to support proxy connection between internal users and outside hosts. The packets are relayed without performing any extensive processing or filtering because the packets are from trusted internal users, and they are going outside. However, packets that return in response to these packets are fully examined by the application proxy services.

Policy - A document defining acceptable access to protected, DMZ, and unprotected networks. Security policies set general guidelines for what is and is not acceptable network access.

Rule set - The collection of access control rules that determines which packets are forwarded or dropped.

Allowed traffic - Packets forwarded as a result of the rule set.

Illegal traffic - Packets specified for rejection in the rule set.

Rejected traffic - Packets dropped as a result of the rule set.

Authentication - The process of verifying that a user requesting a network resource is who he, she, or it claims to be, and vice versa. The entity being authenticated might be the client machine or a user, so authentication may take the form of verifying IP addresses; TCP or UDP port numbers; passwords; and other advanced forms of identification, such as token cards and biometrics.

Security association - The set of security information related to a given network connection or set of connections. This definition covers the relationship between policy and connections. Associations may be set up during connection establishment, and they may be reiterated or revoked during a connection.

Packet filtering - The process of controlling access by examining packets based on the content of packet headers. Header information, such as IP address or TCP port number, is examined to determine whether a packet should be forwarded or rejected, based on a rule set.

Stateful packet filtering - The process of forwarding or rejecting traffic based on the contents of a state table maintained by a firewall. When stateful filtering is used, packets are only forwarded if they belong to a connection that has already been established and that is being tracked in a state table.

Logging - The recording of user requests made to the firewall. All requests are typically logged, including allowed, illegal, and rejected traffic.

An intrusion detection system actively monitors network access points to detect hackers and track attacks as they progress.

SOCKS is a circuit-level proxy firewall service that attempts to provide a secure channel between two TCP/IP hosts, typically a Web client on an internal corporate network that wants to access an outside Web server (on the Internet, on another company's network, or on another part of an intranet). SOCKS provides firewall services, as well as auditing, management, fault tolerance, and other features.

Most firewalls also perform authentication to verify the identity of the users or processes. RADIUS is often used as the authentication service. It is the same authentication service used for dial-up network access by both enterprise networks and Internet service providers. By authenticating users, the firewall has additional information it can work with to filter packets. For example, it can allow a specific user to access some services but not others. Modern firewalls also support VPNs, which provide secure tunnels between a firewall and a remote user across the Internet. The firewall authenticates the user, encrypts all data, and ensures data integrity by using digital signature technology.