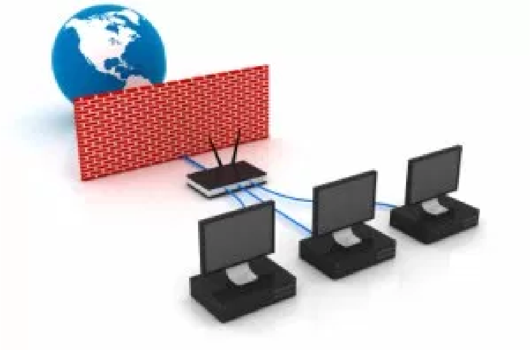
eBrahma

Firewall – Basic concepts

By Dinesh Sharma | April 13, 2015 1 Comment



Firewall – Basic concepts

A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

1. **Packet filter**: Packet filtering inspects each packet passing through the network and accepts or rejects it based on user-defined rules. Although difficult to configure, it is fairly effective and mostly transparent to its users. It is susceptible to IP spoofing.
2. **Application gateway**: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
3. **Circuit level gateway**: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

4. **Proxy server**: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Function

A **firewall** is a dedicated appliance, or software running on a computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

It is normally placed between a protected network and an unprotected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in.

A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone (DMZ).

A firewall's function within a network is similar to physical firewalls with fire doors in building construction. In the former case, it is used to prevent network intrusion to the private network. In the latter case, it is intended to contain and delay structural fire from spreading to adjacent structures.

Packet Filters

The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (**DEC**) developed filter systems known as**packet filter** firewalls. This fairly basic system was the first generation of what became a highly evolved and technical internet security feature. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based upon their original first generation architecture.

Packet filters act by inspecting the "packets" which represent the basic unit of data transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).

This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (it stores no information on connection "state"). Instead, it filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).

TCP and UDP protocols comprise most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between, and thus control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.

Packet filtering firewalls work on the first three layers of OSI reference model which means all the work done between the network and physical layers. When a packet originates from the sender and filters through a firewall the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through firewall it filters the packet on a protocol/port number basis(GSS). For example if a rule in the firewall exists to block telnet access then the firewall will block IP protocol for port number 23.

Application firewall

An **application firewall** is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. The application firewall is typically built to monitor one or more specific applications or services (such as a web or database service), unlike a stateful network firewall which can provide some access controls for nearly any kind of network traffic. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls

A network-based application layer firewall is a computer networking firewall operating at the application layer of a protocol stack, and are also known as a proxy-based or reverse-proxy firewall. Application firewalls specific to a particular kind of network traffic may be titled with the service name, such as a web application firewall. They may be implemented through software running on a host or a stand-alone piece of network hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it on to the client or server. Because it acts on the application layer, it may inspect the contents of the traffic, blocking specified content, such as certain websites, viruses, attempts to exploit known logical flaws in client software.

Network-based application-layer firewalls work on the application level of the network stack (for example, all web browser, telnet, or ftp traffic), and may intercept all packets traveling to or from an application. In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

Modern application firewalls may also offload encryption from servers, block application input/output from detected intrusions or malformed communication, manage or consolidate authentication, or block content which violates policies.

Circuit-Level Gateway

Circuit level gateways work at the session layer of the OSI model, or as a "shim-layer" between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.

Proxy Server

In computer networks, a **proxy server** is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

A proxy server has many potential purposes, including:

- To keep machines behind it anonymous (mainly for security).
- To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To bypass security/ parental controls.
- To scan transmitted content for Malware before delivery.
- To scan outbound content, e.g., for data leak protection.
- To circumvent regional restrictions.

A proxy server that passes requests and replies unmodified is usually called a gateway or sometimes tunneling proxy.

A proxy server can be placed in the user's local computer or at various points between the user and the destination servers on the Internet.

A **reverse proxy** is (usually) an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.

We will Discuss about Reverse Proxy in further articles…!!!

Hope you will like my post.Firewall – Basic concepts.Please share with others & friends.

Share this:

More

Related

Introduction to Network Firewalls Technologies

Introduction to Cisco ASA Firewall

Firewall Technologies – ACLs

Introduction to Network Firewalls Technologies
In "How To"

Introduction to Cisco ASA Firewall
In "How To"

Firewall Technologies – ACLs
In "Network"

Category: Network Security Tags: attacks, Firewall, Firewall – Basic concepts, how to, latest, network security, Proxy, Security, techonology

Iconic One Theme | Powered by Wordpress