Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall can be hardware, software, or both.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines. Firewalls have been the first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

# History

The term firewall originally referred to a wall intended to confine a fire within a building. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment. The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s.

## First Generation

The first reported type of network firewall is called a packet filter. Packet filters act by inspecting packets transferred between computers. When a packet does not match the packet filter's set of filtering rules, the packet filter either drops (silently discards) the packet, or rejects the packet (discards it and generate an Internet Control Message Protocol notification for the sender) else it is allowed to pass. Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers.

The bulk of Internet communication in 20th and early 21st century used either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) in conjunction with well-known ports, enabling firewalls of that era to distinguish between, and thus control, specific types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter used the same non-standard ports.

## Second Generation

From 1989–1990, three colleagues from AT&T Bell Laboratories, Dave Presotto, Janardan Sharma, and Kshitij Nigam, developed the second generation of firewalls, calling them circuit-level gateways.

Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model. This is achieved by retaining packets until enough information is available to make a judgment about its state. A risk to be aware are denial-of-service attacks that bombard the firewall with thousands (or more) of fake connections in an attempt to overwhelm the firewall by filling its connection state memory.

## Third Generation

Marcus Ranum, Wei Xu, and Peter Churchyard developed an application firewall known as Firewall Toolkit (FWTK). In June 1994, Wei Xu extended the FWTK with the kernel enhancement of IP filter and socket transparent. This was known as the first transparent application firewall, released as a commercial product of the Gauntlet firewall at Trusted Information Systems. Gauntlet firewall was rated one of the top firewalls during 1995–1998.

The key benefit of application layer filtering is that it can "understand" certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port or detect if a protocol is being abused in any harmful way.

As of 2012, the so-called next-generation firewall (NGFW) is nothing more than the "wider" or "deeper" inspection at the application layer. For example, the existing deep packet inspection functionality of modern firewalls can be extended to include:

* Intrusion prevention systems (IPS)
* User identity management integration (by binding user IDs to IP or MAC addresses for "reputation")
* Web application firewall (WAF). WAF attacks may be implemented in the tool "WAF Fingerprinting utilizing timing side channels" (WAFFle)

# Types of Firewalls

Firewalls are generally categorized as network-based or host-based. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. They are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network. Firewalls also vary in type depending on where the communication originates, where it is intercepted, and the state of communication being traced.

## Packet Filters or Network Layer Firewalls

When a packet passes through a packet-filtering firewall, its source and destination address, protocol and destination port number are checked. The packet is dropped if it does not comply with the firewall's rule set and is not forwarded to its destination. For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for Transmission Control Protocol (TCP) port number 23, the port where a Telnet server application would be listening.

Packet-filtering firewalls work mainly on the network layer of the OSI reference model, although the transport layer is used to obtain the source and destination port numbers. They examine each packet independently and do not know whether any given packet is part of an existing stream of traffic. Packet-filtering firewalls are effective, but because they process each packet in isolation, they can be vulnerable to IP spoofing attacks and have largely been replaced by stateful inspection firewalls.

## 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. Circuit-level firewall applications represent the technology of next to the first generation.

Firewall technology supervises TCP handshaking among packets to confirm a session is genuine. Firewall traffic is cleaned based on particular session rules and may be controlled to acknowledged computers only. Circuit-level firewalls conceal the detail s of the protected network from the external traffic, which is helpful for interdicting access to impostors. But circuit-level firewalls do not clean entity packets. 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.

## Proxies

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

Proxies make tampering with an internal system from the external network more difficult, so that misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While the use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

## Web Application Firewall

A Web application firewall (WAF) is a firewall that monitors, filters or blocks data packets as they travel to and from a Web application. A WAF can be either network-based, host-based or cloud-based and is often deployed through a proxy and placed in front of one or more Web applications. Running as a network appliance, server plug-in or cloud service, the WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic.

Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers. Through customized inspections, a WAF is also able to prevent cross-site scripting (XSS) attacks, SQL injection attacks, session hijacking and buffer overflows, which traditional network firewalls and other intrusion detection systems may not be capable of doing. WAFs are especially useful to companies that provide products or services over the Internet. There are 3 types of Web application firewall:

1. Network-based Web application firewall
2. Host-based Web application firewall
3. Cloud-hosted Web application firewall

# Advantages of Firewalls

1. Protects the network and the workstation from malware and spyware attacks.
2. Firewall software is easy to install and has less impact on network performance.
3. Allows monitoring of the network’s and computer’s security and generates an alert when some unusual activity is detected.
4. The network protected by a firewall can only be accessed by authorized users.
5. Allows filtering of websites i.e., defining websites which can/cannot be accessed by a particular user.

# Disadvantages of Firewalls

1. A dedicated hardware firewall costs more than a software firewall. It is difficult to install, and upgrade, takes up physical space, and involves complex wiring.
2. The hardware firewalls tend to be more expensive than the software firewalls.
3. The software firewalls take up system resources and it is difficult to remove or uninstall the firewall.
4. Configuring and maintaining the firewall can be a difficult task.
5. The firewalls can be difficult to use correctly especially for the new users. They may block the users from performing certain actions on the Internet until the firewall is configured correctly.