Firewalls

Firewalls have been one of the most popular and important tools used to secure networks since the early days of interconnected computers. The basic function of a firewall is to screen network traffic for the purposes of preventing unauthorized access between computer networks. Firewalls are the first line of defense between the internal network and untrusted networks like the Internet.

Applications that want to bypass firewalls may encrypt their traffic. This makes the firewall's job more difficult by rendering most of the communication unreadable. Blocking all encrypted traffic isn't really feasible except in highly restricted environments where security is more important than application functionality, and a "permit by exception" policy blocks all encrypted application traffic except for that on a whitelist of allowed, known applications. And broad-spectrum decryption capability isn't within the reach of most consumers and enterprises, despite Moore's law's predicted wholesale advances in computing power. However, controlling application communications can still be done even if the traffic is encrypted, by some of the more advanced firewalls.

Applications that encrypt their network traffic can be controlled by fourth-generation firewalls, although it's easier to permit or deny the entire application than it is to control the specific functions within it. Today's fourth-generation firewalls have extensive lists of known applications based on extensive research and analysis ready to drag-and-drop into a policy configuration.

Mandatory Firewall Features

- **Application Awareness**: The firewall must be able to process and interpret traffic at least from OSI layers three through seven. At layer three, it should be able to filter by IP address; at layer four by port; at layer five by network sessions; at layer six by data type, and, most significantly, at layer seven to properly manage the communications between applications.
- **Accurate Application Fingerprinting**: The firewall should be able to correctly identify applications, not just based on their outward appearance, but by the internal contents of their network communications as well. Correct application identification is necessary to ensure that all applications are properly covered by the firewall policy configuration.
- **Granular Application Control**: In addition to allowing or denying the communication among applications, the firewall also needs to be able to identify and characterize the features of applications so they can be managed appropriately. File transfer, desktop sharing are examples of features that the firewall should be able to control.

- **Bandwidth Management**: The Quality of Service of preferred applications can be managed through the firewall based on real-time network bandwidth availability. If a sporting event is broadcast live via streaming video on a popular web site, your firewall should be able to proactively limit or block access so all those people who want to watch it don't bring down your network. The firewall should integrate with other network devices to ensure the highest possible availability for the most critical services.

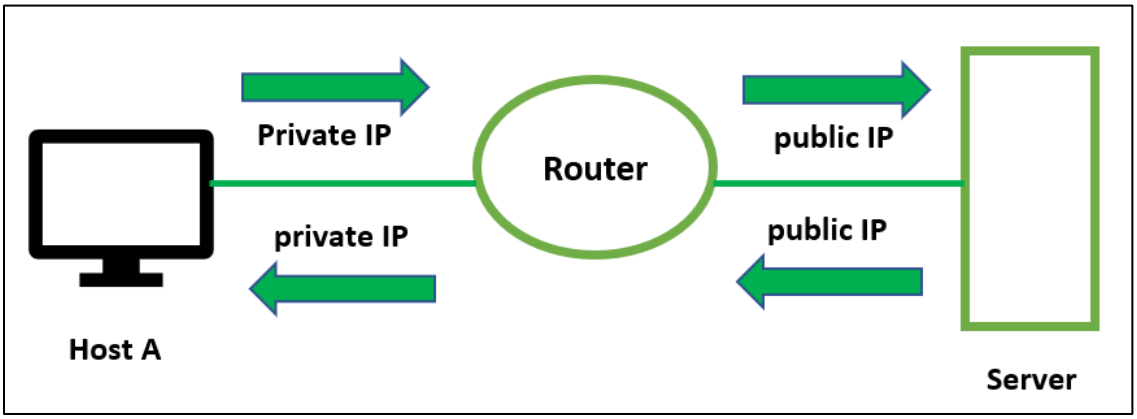
Core Firewall Functions

Due to the placement within the network infrastructure, firewalls are ideally situated for performing certain functions in addition to controlling application communication.

- **Network Address Translation (NAT):** The primary version of TCP/IP used on the Internet is version 4 (IPv4). Version 4 of TCP/IP was created with an address space of 32 bits divided into four octets, mathematically providing approximately four billion addresses. Strangely enough, this is not sufficient. A newer version of IP, called IPv6, has been developed to overcome this address-space limitation, but it is not yet in widespread deployment.

  In order to conserve IPv4 addresses, blocks of addresses have been specified that will never be used on the Internet. These network ranges are referred to as "private" networks.

  This allows organizations to use these blocks for their own corporate networks without worrying about conflicting with an Internet network. However, when these networks are connected to the Internet, they must translate their private IP network addresses into public IP addresses (NAT) in order to be routable. By doing this, a large number of hosts behind a firewall can take turns or share a few public addresses when accessing the Internet.



Network Address Translation

- **Port Address Translation (PAT):** With Port Address Translation (PAT), a single public IP address is used for all internal private IP addresses, but a different port is assigned to each private IP address. This type of NAT is also known as NAT Overload and is the typical form of NAT used in today's networks. It is even supported by most consumer-grade routers. PAT allows supporting many hosts with only few public IP addresses.

- **Auditing and Logging:** A firewall makes a great auditor. They have the ability to record any communication that flows through them if given enough disk space or remote logging capabilities. Attack attempts will leave traces in the logs, and if administrators are vigilantly monitoring the systems, attacks can be stopped before they succeed. Therefore, it is crucial to log and keep track of system activity. Firewalls should keep track of both successful and unsuccessful system events.

Additional Firewall Capabilities

- **Application and Website Malware Execution Blocking**: Previously, for a virus to run, a user had to click on a button or link that was disguised. These viruses wouldn't spread very far if the end users were wise enough to spot the virus creators' methods. Without the help of end users, modern malware may run and spread itself. By use of automatic, browser-based code execution, a virus can be activated by merely opening a web page. These "invisible" infection vectors should be able to be found and stopped by firewalls with advanced anti-malware capabilities. Once malware has successfully infected a victim system and is attempting to communicate "back home" to its controller for instructions, they ought to be able to block that transmission.
- **Antivirus**: Malware can and should be blocked on the network by firewalls that are sophisticated enough to detect it. To complement the organization's endpoint antivirus software, malware control solutions should be layered, and the firewall can play a key role in a network-based malware blocking capability.
- **Intrusion Detection and Intrusion Prevention**: Firewalls can provide IDS and IPS capabilities at the network perimeter, which can be a useful addition or substitution for standard purpose-built intrusion detection and prevention systems, especially in a layered strategy.
- **Web Content Filtering and Caching**: The firewall is optimally positioned on the network to filter access to web sites. One can choose to implement a separate URL filtering system or service, or can get a firewall that has the capability built-in. Modern firewalls demonstrate web content filtering capabilities that rival those of purpose-built systems.
- **Email (Spam) Filtering**: Modern firewalls can subtract the spam from the e-mail messages before they get delivered to the mail server. One can sign up for an external service or buy a purpose-built spam filter instead, but with a firewall that includes this capability, one can have another option.

- **Enhance Network Performance**: Firewalls need to be able to run at "wire speed"—fast enough to avoid bottlenecking application traffic. They should be able to perform all the functions that have been enabled without impacting performance. In addition, firewalls should be able to allocate network bandwidth to the most critical applications to ensure QoS, without sacrificing filtering functionality.

Firewall Design

Firewalls may be software based or, more commonly, purpose-built appliances. The specific features of the firewall platform and the design of the network where the firewall lives are key components of securing a network. To be effective, firewalls must be placed in the right locations on the network, and configured effectively. Best practices include

- All communications must pass through the firewall. The effectiveness of the firewall is greatly reduced if an alternative network routing path is available; unauthorized traffic can be sent through a different network path, bypassing the control of the firewall.
- The firewall permits only traffic that is authorized. If the firewall cannot be relied upon to differentiate between authorized and unauthorized traffic, or if it is configured to permit dangerous or unneeded communications, its usefulness is also diminished.
- In a failure or overload situation, a firewall must always fail into a "deny" or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.
- The firewall must be designed and configured to withstand attacks upon itself. Because the firewall is relied upon to stop attacks, and nothing else is deployed to protect the firewall itself against such attacks, it must be hardened and capable of withstanding attacks directly upon itself.