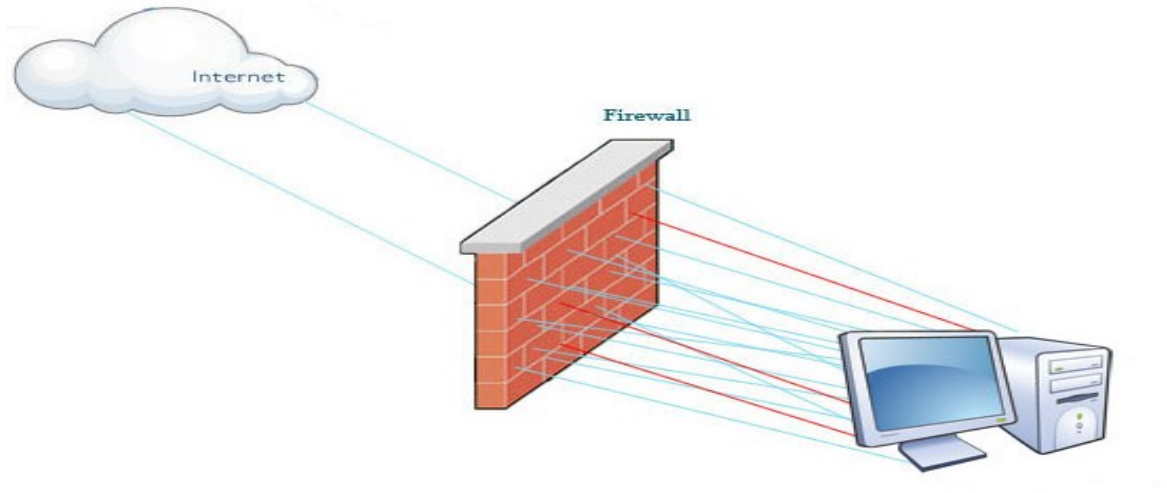
All about Firewalls

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and 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.



In non-computer industries, a firewall is a specially designed wall that controls the spreading of a fire. In networking, a firewall could be described as a specially designed device that controls the spreading of a network threat. The most commonly talked about source of network threats is the Internet. The Internet is the home of many unknown people that we cannot trust. There are hackers on the Internet that may want to do our networks harm. We can use a firewall to impede an untrusted person from doing damage to our networks. A more textbook definition of a computer firewall is that it is a method or device that regulates the level of trust between two or more networks. A firewall can consist of software, hardware or a combination of both. A firewall can protect your network from the Internet as well as regulate the traffic between networks within the same company. For instance, a firewall can allow the legal department's network to have access to the marketing file server but the marketing department can be refused access to legal. In this example the firewall is positioned between the marketing and legal networks so that all communication must pass through the firewall.

The firewall is then able to ensure that only authorized packets are allowed.

There are several types of firewall techniques:

- ***Packet filtering***: Looks at each packet entering or leaving the network and accepts orrejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- ***Application gateway***: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- ***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.
- ***Stateful Inspection Firewall*** : A stateful inspection firewall combines aspects of a packet-filtering firewall, a circuit-level gateway, and an application-level gateway. Like a packet-filtering firewall, a stateful inspection firewall operates at the network layer of the OSI model, filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Key Functions of a Firewall

Technically a firewall should have these basic functions:

- Manage and control network traffic
- Authentic access
- Protect resources
- Record and report on events
- Act as an intermediary
- Record and report on events

Packet-filtering

A packet-filtering firewall is a router or computer running software that has been configured to screen incoming and outgoing packets. A packet-filtering firewall accepts or denies packets based on information contained in the packets' TCP and IP headers. For example, most packet-filtering firewalls can accept or deny a packet based on the packet's full association, which consists of the following:

- Source address
- Destination address
- Application or protocol
- Source port number
- Destination port number

All routers (even those that are not configured to filter packets) routinely check the full association to determine where to send the packets they receive. However, a packet-filtering firewall goes one step further: Before forwarding a packet, the firewall compares the full association against a table containing rules that dictate whether the firewall should deny or permit packets to pass.

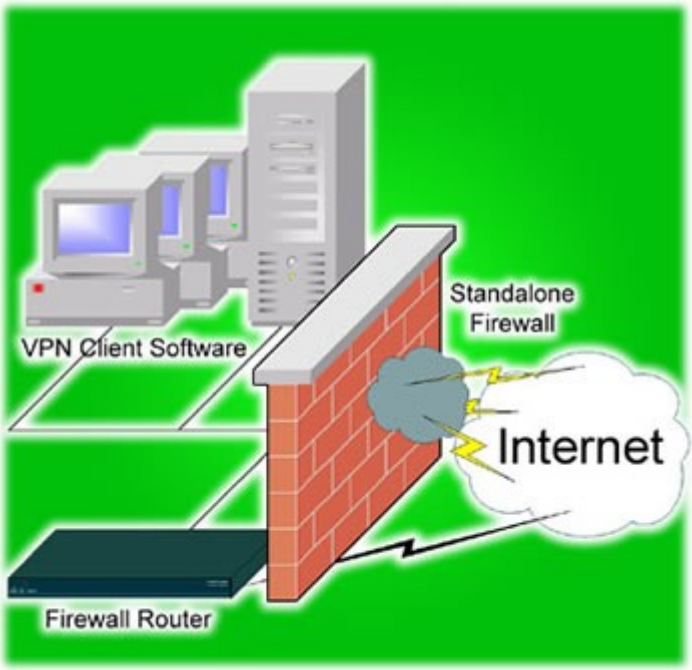
A packet-filtering firewall scans these rules until it finds one that agrees with the information in a packet's full association. If the firewall encounters a packet that does not meet one of the rules, the firewall will apply the default rule. A default rule should be explicitly defined in the firewall's table and, for strict security, should instruct thefirewall to drop a packet that meets none of the other rules.

Rules to Live By. You can define packet-filtering rules that indicate which packets should be accepted and which packets should be denied. For example, you could configure rules that instructed the firewall to drop packets from specific untrusted servers (generally called hosts on the Internet), which you would identify in the table by their IP addresses. You could also create a rule that permitted only incoming e-mail messages traveling to your mail server and another rule that blocked incoming e-mail messages from an untrusted host that had flooded your network with several gigabytes of data in the past.

In addition, you can configure a packet-filtering firewall to screen packets based on TCP and User Datagram Protocol (UDP) port numbers. Configuring a firewall in this way enables you to implement a rule that tells the firewall to permit particular types of connections (such as Telnet and FTP connections) only if they are traveling to appropriate trusted servers (such as the Telnet and FTP server, respectively). However, the success of such a rule depends on a TCP/IP network convention: Servers (and clients) generally run particular TCP/IP applications over particular ports (often referred to as well-known ports), but servers are not required to use these ports.

Low Cost for Relatively Low Protection? The primary advantage of using a packet-filtering firewall is that it provides some measure of protection for relatively low cost and causes little to no delay in network performance. If you already have an IP router with packet-filtering capabilities, setting up a packet-filtering firewall will cost no more than the time it takes to

create packet-filtering rules. Most IP routers, including those manufactured by Novell, Cisco Systems, and Bay Networks, can filter incoming and outgoing packets.



Although the cost of a packet-filtering firewall is attractive, this firewall alone is often not secure enough to keep out hackers with more than a passing interest in your network. Configuring packet-filtering rules can be difficult, and even if you manage to create effective rules, a packet-filtering firewall has inherent limitations. For example, suppose you created a rule that instructed the firewall to drop incoming packets with unknown source addresses. This rule would make it more difficult but not impossible for a hacker to access at least some trusted servers with IP addresses: The hacker could simply substitute the actual source address on a malicious packet with the source address of a trusted client
Layer Upon Layer. In addition, a packet-filtering firewall primarily operates only at the network layer of the Open Systems Interconnection (OSI) model. The OSI model, which was developed by the International Standards Organization (ISO), identifies the seven layers at which computers communicate, ranging from the physical media over which they communicate to the applications they use to communicate.

All firewalls rely on information generated by protocols that function at various layers of the OSI model. Knowing the OSI layer at which a firewall operates is one of the keys to understanding different types of firewalls. Generally speaking, the higher the OSI layer at which a firewall filters packets, the greater the level of protection the firewall provides.

Because a packet-filtering firewall generally checks information only in IP packet headers, sneaking packets through this type of firewall is relatively easy: A hacker simply creates packet headers that satisfy the firewall's rules for permitting packets. Beyond that, a packet-filtering firewall cannot detect the contents of a packet.

Advantages of packet filtering firewall :

- They can process packet at very fast.
- They can easily match on most filed in layer -3 and layer -4 segment header providing lots of flexibility in implementing security policies.
- Cost effective with lower resource usage
- Low impact on network performance
- Most suitable for smaller networks

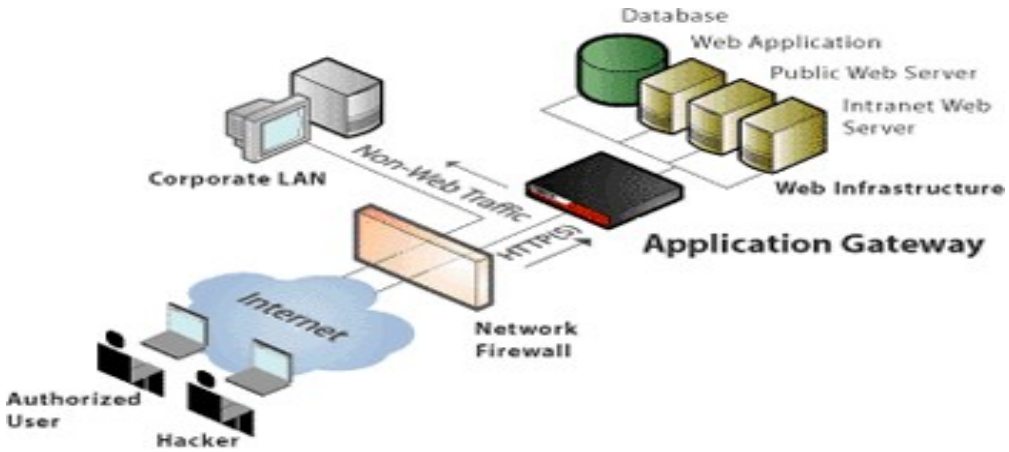
Disadvantages of packet filtering firewall

- They can be complex to configure.
- They can not prevent application layer attacks .
- They do not support user authentication connection.
- They have limited logging capabilities.

Application level Gateway Firewall (procxy firewall)

Like a circuit-level gateway, an application-level gateway intercepts incoming and outgoing packets, runs proxies that copy and forward information across the gateway, and functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. However, the proxies that an application-level gateway runs differ in two important ways from the pipe proxies that a circuit-level gateway uses:

The proxies are application specific.
The proxies can filter packets at the application layer of the OSI model.



Application -specific Proxies. Unlike pipe proxies, application-specific proxies accept only packets generated by services they are designed to copy, forward, and filter. For example, only a Telnet proxy can copy, forward, and filter Telnet traffic. If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services for which there is not a proxy. For example, if an application-level gateway ran FTP and Telnet proxies, only packets generated by these services could pass through the firewall. All other services would be blocked.

Application-level Filtering. Unlike a circuit-level gateway, an application-level gateway runs proxies that examine and filter individual packets, rather than simply copying them and blindly forwarding them across the gateway. Application-specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer (which is the highest layer) of the OSI model. These proxies can filter particular kinds of commands or information in the application protocols the proxies are designed to copy, forward, and filter.

Application gateways can also restrict specific actions from being performed. For example, the gateway could be configured to prevent users from performing the FTP put command. This command lets users write to the FTP server. Prohibiting this action can prevent serious damage of the information stored on the server.

Transparency--Ah, There's the Rub! An application-level gateway is one of the most secure firewalls available, but some vendors (usually those that market stateful inspection firewalls) and users claim that the security an application-level gateway offers has a drawback--lack of transparency. Ideally, an application-level gateway would be as transparent as it is secure. Users on the trusted network would not notice that they were accessing Internet services through a firewall. In reality, however, users often experience delays or must perform multiple logins before they are connected to the Internet or an intranet via an application-level gateway.

Although most vendors claim that application-level gateways are transparent, many vendors recommend that you configure the gateway to require user authentication before users access an untrusted network, a process that foils true transparency.

Some firewall vendors that market products as application-level gateways have tried to overcome the transparency problem. For example, one particular application gateway uses a version of the SOCKS protocol (rather than application-specific proxies) to route TCP/IP services. SOCKS is a proposed Internet Engineering Task Force (IETF)
standard that provides transparent authentication services for clients requesting
connections to devices through firewalls. However, a SOCKS server is not transparent to network administrators: You must modify the applications running on each client that will use the firewall.

Also, although SOCKS includes other security features (such as private-key and public-key encryption), it does not filter individual packets. Therefore, the products that rely on SOCKS might fall justifiably into the realm of circuit-level gateways rather than application-level gateways.

Advantages of application gateway firewall

- They authenticate individual not device.
- Hackers can have herder time with spoofing and implementing DOS attacks
- They can monitor and filter application data.
- They can provide detailed logging.
- Work only on configured protocols
- Can prevent diverse kinds of attacks

Disadvantages of application gateway firewall

- They process packets in software.
- They support small number of application .
- They sometimes require special client software.

Circuit-level Gateway

A circuit-level gateway monitors TCP handshaking between packets from trusted clients or servers to untrusted hosts and vice versa to determine whether a requested session is legitimate. To filter packets in this way, a circuit-level gateway relies on data contained in the packet headers for the Internet's TCP session-layer protocol. Because a circuit-level gateway filters packets at the session layer of the OSI model, this gateway operates two layers higher than a packet-filtering firewall does.

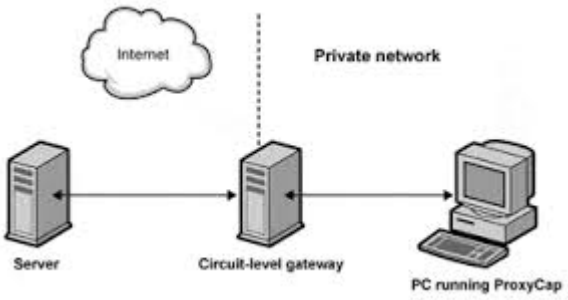


Figure .1

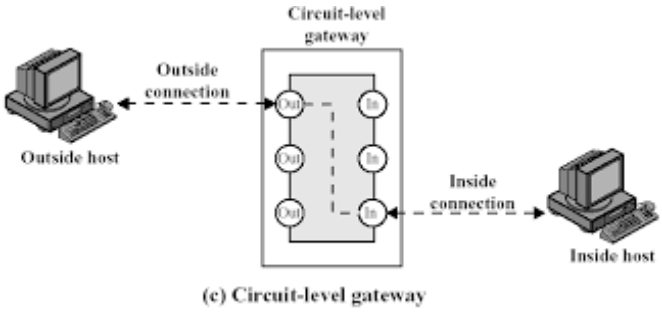


Figure .2

Monitoring Handshaking--Circuitously. To determine whether a requested session is legitimate, a circuit-level gateway uses a process similar to the following: A trusted client requests a service, and the gateway accepts this request, assuming that the client meets basic filtering criteria (such as whether DNS can locate the client's IP address and associated name).

Next, acting on behalf of the client, the gateway opens a connection to the requested untrusted host and then closely monitors the TCP handshaking that follows. This handshaking involves an exchange of TCP packets that are flagged SYN (synchronize) or ACK (acknowledge). These packet types are legitimate only at certain points during the session. See the SYNDefender white paper for a more detailed description of the SYN/ACK process.

A circuit-level gateway determines that a requested session is legitimate only if the SYN flags, ACK flags, and sequence numbers involved in the TCP handshaking between the trusted client and the untrusted host are logical.

Pipe Proxies. After a circuit-level gateway determines that the trusted client and the untrusted host are authorized to participate in a TCP session and verifies the legitimacy of this session, the gateway establishes a connection. From this point on, the circuit- level gateway simply copies and forwards packets back and forth without further filtering them.

The gateway maintains a table of established connections, allowing data to pass when session information matches an entry in the table. When the session is completed, the gateway removes the associated entry in the table and closes the circuit this session used.

A circuit-level gateway relies on special applications to perform copy and forward services. These applications are sometimes called pipe (or generic) proxies becausethey establish a virtual circuit, or pipe, between two networks and then allow packets (generated by one or more types of TCP/IP applications) to pass through this pipe.

Seldom Standalone. Because pipe proxies generally support several TCP/IP services, a circuit-level gateway can extend the number of services supported by an application- level gateway, which relies on application-specific proxies. In fact, most circuit-level gateways are not stand-alone products but instead are packaged with application-level gateways.

Proxy Server Protection. A circuit-level gateway provides one other important security function: It is a proxy server. Although the term proxy server suggests a server that runs proxies (which is true of a circuit-level gateway), the term actually means something different. A proxy server is a firewall that uses a process called address translation to map all of your internal IP addresses to one "safe" IP address. This address is associated with the firewall from which all outgoing packets originate.

Advantage of circuit level gateway

Circuit level gateway firewalls offer one of the quickest ways for identifying malicious content. They are deployed at the session layer of the OSI model and monitor sessions to determine the legitimacy of the connection request. According to technical experts, this firewall creates a stealth cover for a private network. Some associated benefits include:

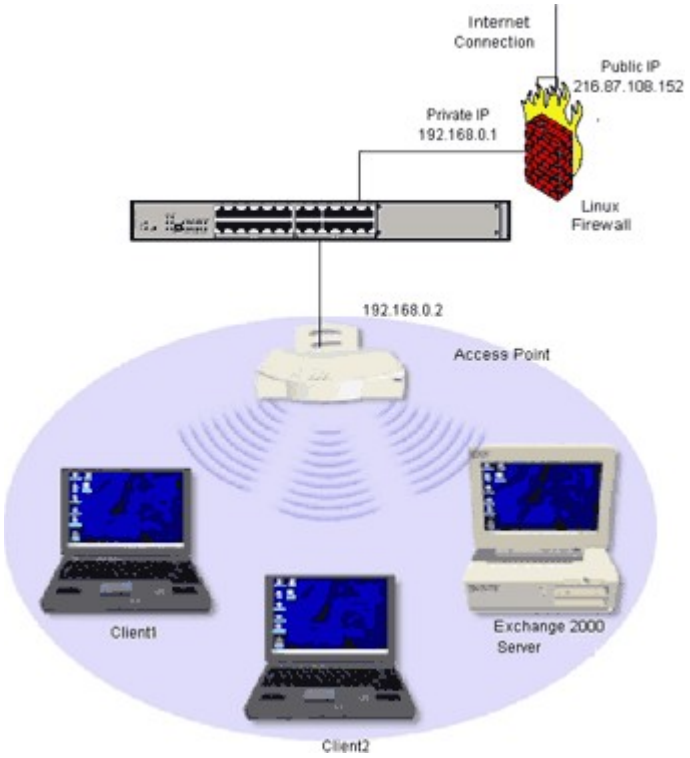
- Comparatively inexpensive than other firewalls.
- Provide anonymity to the private network.
- Monitor Transmission Control Protocol's (TCP) three way handshake .
- Private network data hiding.
- Avoidance of filtering individual packets.
- Don't need a separate proxy server for each application.

Disdvantage of circuit level gateway

- Active content can not be scanned or disallowed commands.
- Can only handle TCP connections – new extensions proposed for UDP.
- TCP/IP stacks are mandatorily be modified by vendor for using CL Gateways.

Stateful Inspection Firewall

A stateful inspection firewall combines aspects of a packet-filtering firewall, a circuit- level gateway, and an application-level gateway. Like a packet-filtering firewall, a stateful inspection firewall operates at the network layer of the OSI model, filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers.



A stateful inspection firewall also functions as a circuit-level gateway, determining whether the packets in a session are appropriate. For example, a stateful inspection firewall verifies that SYN and ACK flags and sequence numbers are logical.
Finally, a stateful inspection firewall mimics an application-level gateway: The firewall evaluates the contents of each packet up through the application layer and ensures that these contents match the rules in your company's network security policy.

Better Performance, Same Level of Security? Like an application-level gateway, a stateful inspection firewall can be configured to drop packets that contain specific commands. For example, you could configure a stateful inspection firewall to drop FTP packets containing a Put or Get command.

Unlike an application-level gateway, however, a stateful inspection firewall does not break the client-server model to analyze application-layer data. An application-level gateway requires two connections: one connection between the trusted client and the gateway and another connection between the gateway and the untrusted host. The gateway then relays information between the two connections. Although some people insist that this configuration ensures the highest degree of security, other people argue that this configuration slows performance unnecessarily.

A stateful inspection firewall, on the other hand, does not require two connections, allowing a direct connection between a trusted client and an untrusted host. To provide a secure connection, a stateful inspection firewall intercepts and examines each packet up through the application layer of the OSI model.
Rather than relying on application-specific proxies (and thus limiting users to the services for which you are running a proxy), a stateful inspection firewall relies on algorithms to recognize and process application-layer data. These algorithms compare packets against known bit patterns of authorized packets and are theoretically able to filter packets more efficiently than application-specific proxies.

Because a stateful inspection firewall allows a direct connection between a trusted client and an untrusted host, some people believe this firewall is less secure than an application-level gateway. However, other people argue that using a direct connection makes a stateful inspection firewall perform better than an application-level gateway at no cost to security.

A stateful inspection firewall is a popular solution for securing Internet and intranetconnections because this firewall is transparent to users, scrutinizes data at the highest OSI layer, and does not require you to modify clients or run a separate proxy for each service that runs over the firewall

Advantages of stateful inspection firewall
As you learned in the previous explanation, stateful firewalls have advantages over packet-filtering firewalls:

- Stateful firewalls are aware of the state of a connection.
- Stateful firewalls do not have to open up a large range of ports to allow communication.
- Stateful firewalls prevent more kinds of DoS attacks than packet-filtering firewalls and have more rebust logging .
- stateful firewalls are aware of a connection's state: Stateful firewalls typically build a state table and use this table to allow only returning traffic from connections currently listed in the state table. After a connection is removed from the state table, no traffic from the external device of this connection is permitted. Therefore, these types of connections are more difficult to spoof.
- Allows direct connection between client and server
- Makes connections and data transfer more secure

Disadvantages stateful inspection firewalls:

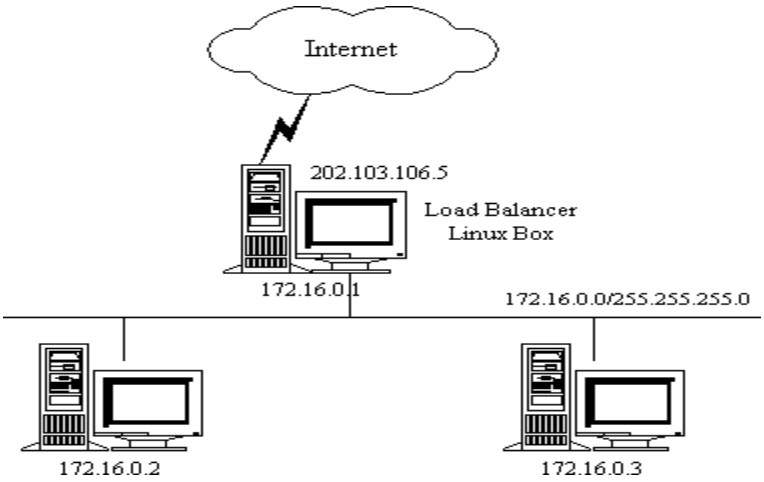
- They can be complex to configure.
- They cannot prevent application-layer attacks.
- They do not support user authentication of connections.
- Not all protocols contain state information.
- Some applications open multiple connections, some of which use dynamic port numbers for the additional connections.
- Additional overhead is involved in maintaining a state table.

Network Address Translation (NAT)

Short for Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

NAT serves three main purposes:

- Provides a type of firewall by hiding internal IP addresses
- Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
- Allows a company to combine multiple ISDN connections into a single Internet connection.



Dynamic NAT

Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address.
Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.

Dynamic NAT helps to secure a network as it masks the internal configuration of a private network and makes it difficult for someone outside the network to monitor individual usage patterns. Another advantage of dynamic NAT is that it allows private network to use private IP addresses that are invalid on the Internet but useful as internal addresses.

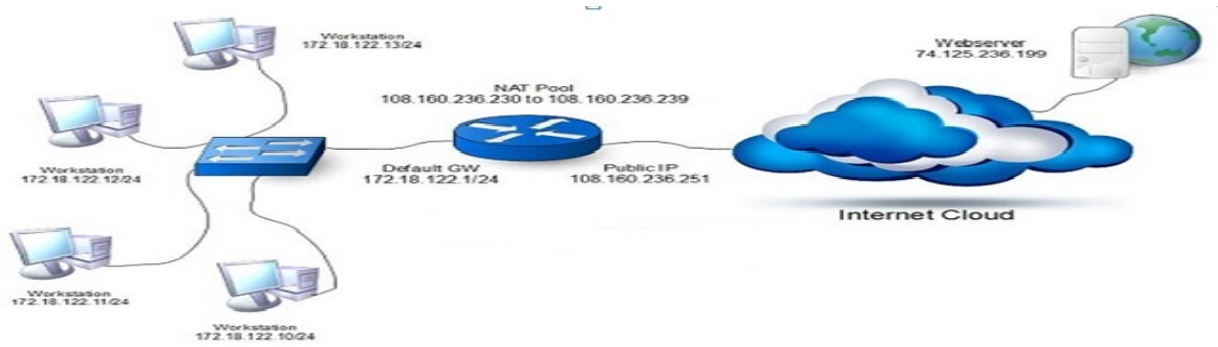


Figure .Dynaic NAT

Static NAT :

Static NAT (Network Address Translation) - Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet.

A type of NAT in which a private IP address is mapped to a public IP address, where the public address is always the same IP address (i.e., it has a static address). This allows an internal host, such as a Web server, to have an unregistered (private) IP address and still be reachable over the Internet.

Static NAT maps network traffic from a static external IP address to an internal IP address or network. It creates a static translation of real addresses to mapped addresses.

Static NAT provides internet connectivity to networking devices through a private LAN with an unregistered private IP address.

- Static NAT also supports the following types of translation:
- To map multiple IP addresses and specified ranges of ports to a same IP address and different range of ports
- To map a specific IP address and port to a different IP address and port

Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address while the mapped-to address is the real host IP address.

Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size. For each private address, a public address must be allocated. No address pools are necessary.

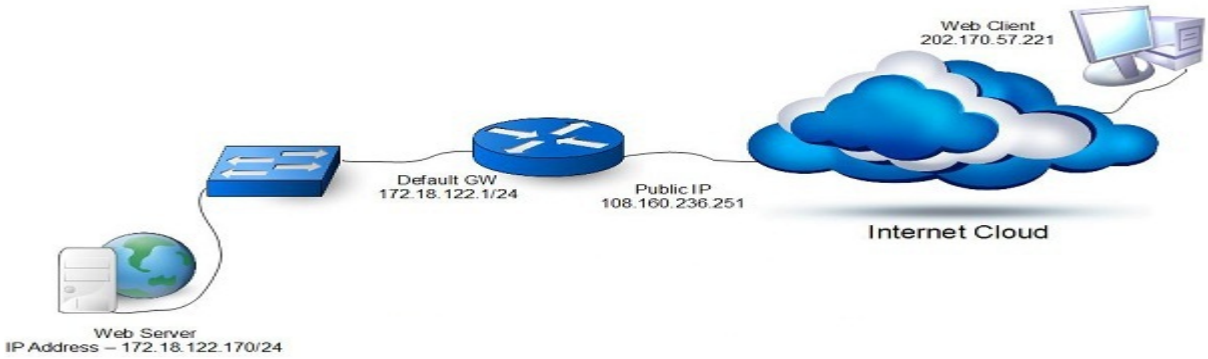


Figure .Static NAT

Advantages of NAT

- NAT hides the internal network's IP addresses.
- It simplifies routing. Internal hosts are assigned IP addresses from the internal network, so other internal systems can access them without special routes or routers. The same hosts are accessed from the public network through globally routable IP addresses translated by NAT.
- NAT is transparent to the client so it allows you to support a wider range of clients.
- NAT supports a wide range of services with a few exceptions. Any application that carries and uses the IP address inside the application does not work through NAT.
- NAT consumes fewer computer resources and is more efficient than using SOCKS and application proxy servers.
- The Universal Connection can flow through NAT.

Disadvantages of NAT

- NAT provides minimum logging services.
- You must enable IP forwarding before you can use NAT to make an Internet connection.
- NAT is not as adept as either the SOCKS or application proxy servers in detecting attacks.
- NAT can break certain applications, or make these applications more difficult to run.

Port Forwarding

port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

Types of Port Forward

1. Local port forwarding
2. Remote port forwarding
3. Dynamic port forwarding

1. **Local port forwarding:** Local port forwarding is the most common type of port forwarding. It is used to let a user connect from the local computer to another server, i.e. forward data securely from another client application running on the same computer as a Secure Shell (SSH) client. By using local port forwarding, firewalls that block certain web pages are able to be bypassed

Some uses of local port forwarding:

- Using local port forwarding to Receive Mail.
- Connect from a laptop to a website using an SSH tunnel.

2. **Remote port forwarding:** This form of port forwarding enables applications on the server side of a Secure Shell (SSH) connection to access services residing on the SSH's client side.[8] In addition to SSH, there are proprietary tunnelling schemes that utilize remote port forwarding for the same general purpose.[9] In other words, remote port forwarding lets users connect from the server side of a tunnel, SSH or another, to a remote network service located at the tunnel's client side.

   To use remote port forwarding, the address of the destination server (on the tunnel's client side) and two port numbers must be known. The port numbers chosen depend on which application is to be used.

   Remote port forwarding allows other computers to access applications hosted on remote servers. Two examples:

- An employee of a company hosts an FTP server at their own home and wants to give access to the FTP service to employees using computers in the workplace. In order to do this, an employee can set up remote port forwarding through SSH on the company's internal computers by including their FTP server's address and using the correct port numbers for FTP (standard FTP port is TCP/21)
- Opening remote desktop sessions is a common use of remote port forwarding. Through SSH, this can be accomplished by opening the virtual network computing port (5900) and including the destination computer's address.

3. **Dynamic port forwarding :** Dynamic port forwarding (DPF) is an on-demand method of traversing a firewall or NAT through the use of firewall pinholes. The goal is to enable clients to connect securely to a trusted server that acts as an intermediary for the purpose of

sending/receiving data to one or many destination servers.

DPF can be implemented by setting up a local application, such as SSH, as a SOCKS proxy server, which can be used to process data transmissions through the network or over the Internet. Programs, such as web browsers.

DPF is a powerful tool with many uses; for example, a user connected to the Internet through a coffee shop, hotel, or otherwise minimally secure network may wish to use DPF as a way of protecting data. DPF can also be used to bypass firewalls that restrict access to outside websites, such as in corporate networks.

INTRUTION DETECTION SYSTEM

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

1. Network intrusion detection systems (NIDS)
2. Host-based intrusion detection systems (HIDS)
3. Wireless intrusion prevention system (WIPS)

IDS Detection Types

There is a wide array of IDS, ranging from antivirus software to tiered monitoring systems that follow the traffic of an entire network. The most common classifications are:

1. Network intrusion detection systems (NIDS): A system that analyzes incoming network traffic.
2. Host-based intrusion detection systems (HIDS): A system that monitors important operating system files.
3. Wireless intrusion prevention system (WIPS): Analyzes network protocol activity across the entire wireless network, looking for any untrustworthy traffic.

There is also subset of IDS types. The most common variants are based on signature detection and anomaly detection.

- **Signature-based**: Signature-based IDS detects possible threats by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from antivirus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.
- **Anomaly-based**: a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion of malware. This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behavior against this trust model. While this approach enables the detection of previously unknown attacks, it can suffer from false positives: previously unknown legitimate activity can accidentally be classified as malicious.

Why Intrusion Detection Systems are Important

Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations. An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats.

Packet characteristic to filter

- A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. If the packet passes the test, it's allowed to pass. If the packet doesn't pass, it's rejected.
- Packet filters are the least expensive type of firewall. As a result, packet-filtering firewalls are very common However, packet filtering has a number of flaws that knowledgeable hackers can exploit. As a result, packet filtering by itself doesn't make for a fully effective firewall.
- **Packet filters are very efficient.** They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports are determined, the packet filter quickly applies its rules and either sends the packet along or rejects it. In contrast, other firewall techniques have a more noticeable performance overhead.
- **Packet filters are almost completely transparent to users.** The only time a user will be aware that a packet filter firewall is being used is when the firewall rejects packets. Other firewall techniques require that clients and/or servers be specially configured to work with the firewall.
- **Packet filters are inexpensive.** Most routers include built-in packet filtering.

Firewalls

- A firewall is a computer connected to both a private (protected) network and a public (unprotected) network, which receives and resubmits specific kinds of network requests on behalf of network clients on either the private or public network.
- Firewalls involve proxies. A proxy acts as a middle-man in a network transaction. Rather than allowing a client to speak directly to a server, the proxy server receives the request from the client, and then resubmits the request, on behalf of the client, to the target server. Each protocol or type of network transaction typically requires its own proxy program, and an administrator enables or installs specific proxies to determine what kinds of services will be allowed between the two networks.
- Firewalls are not routers or address translators. Never does a firewall copy or forward a packet from the internal network to the external network, or vice versa. The internal network uses private address space. Neither side of the firewall knows about the address space on the other side of the firewall, and does not know how to route data to the other side of the firewall.

Packet Filters

- A packet filter is a set of rules, applied to a stream of data packets, which is used to decide whether to permit or deny the forwarding of each packet. These rules are usually on a router or in the routing layer of a computer's network protocol stack. Using a packet filter, an administrator can dictate what types of packets are allowed into or out of a network or computer.
- Some devices, such as the Cisco PIX, combine address translation with packet filtering. Like a firewall, this prevents the outside network from having knowledge of the address space on the protected network. However, aside from translating the addresses of the internal network, packets are forwarded as received through the unit, and no proxies are involved. This certainly improves security, but, strictly speaking, this is not a firewall.
- It is worth noting that any good firewall will also employ packet filtering. This is done to protect the firewall Itself from intrusion and to isolate intruders from the internal network should an attacker gain control of the firewall.

What is stateful Firewall?

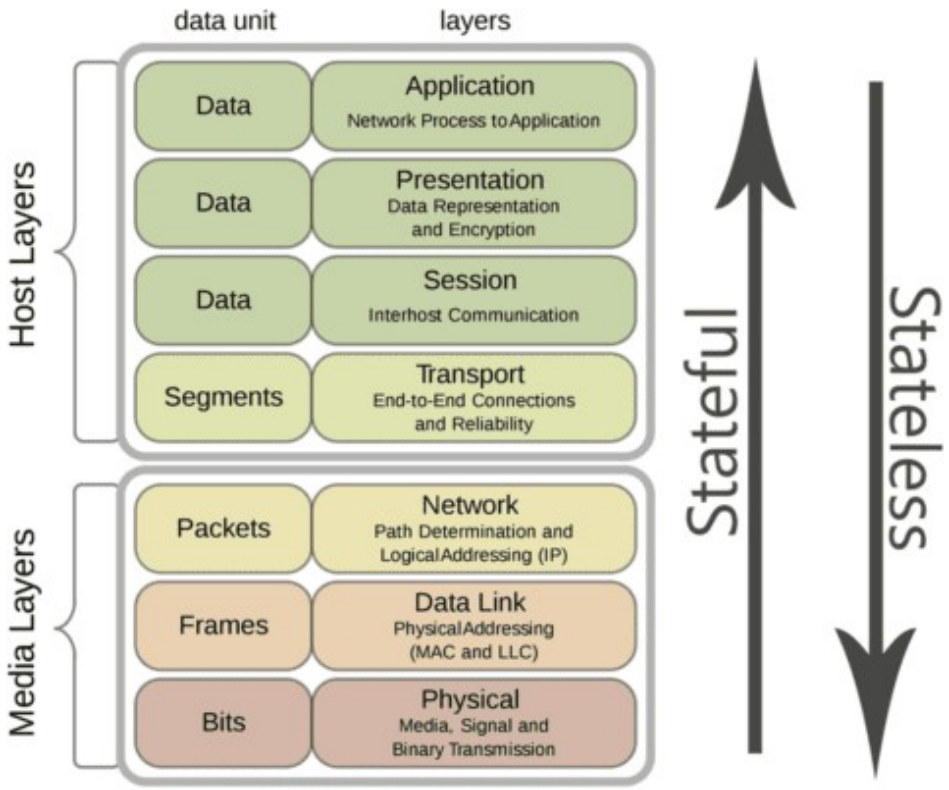
Stateful firewalls monitor all aspects of the traffic streams, their characteristics and communication channels. These firewalls can integrate encryption or tunnels, identify TCP connection stages, packet state and other key status updates

What is stateless Firewall?

Stateless firewalls use clues from the destination address, source and other key values to assess whether threats are present, then block or restrict those deemed untrusted. Preset rules enforce whether traffic is permitted or denied, but the system is typically unable to determine the difference between truly desired communications and sophisticated attempts to disguise unauthorized communications as trusted ones.

As one of the earlier iterations of firewalls, stateless firewalls don't look beyond the header of packet contents to determine if traffic is authorized.

Stateful Vs Stateless – What's the dfference?

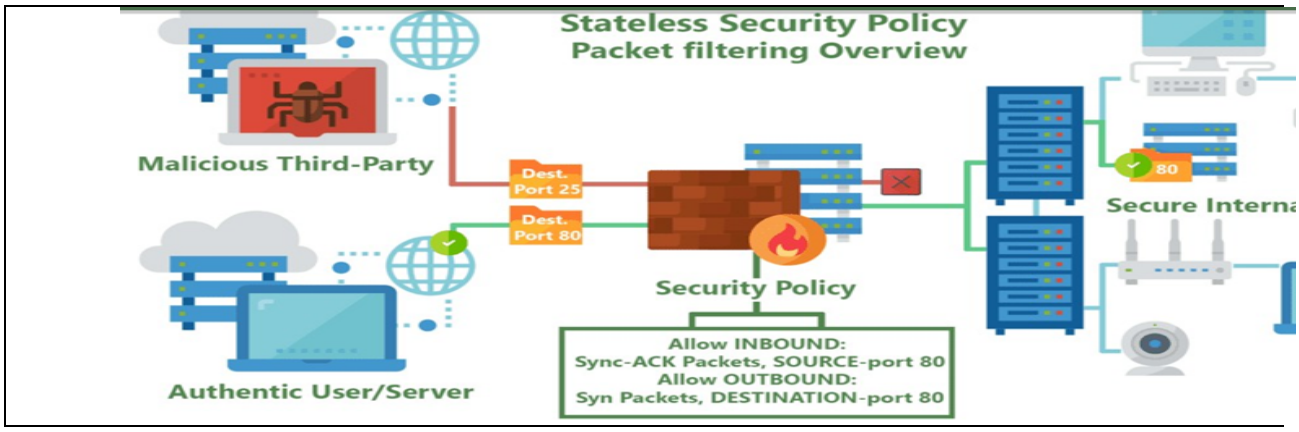


Inclination of Stateless vs Stateful firewalls in the 7 layers of the OSI model.

Stateless and stateful firewalls may sound pretty similar with being denoted with a single distinction, but they are in fact two very different approaches with diverging functions and capabilities. Packet filtering potential, is one of principle ways in which stateless and stateful firewalls differ from each other. While both firewall implementations perform packet filtering, the differences between them is in the methodology, depth and lengths they go to performing this function.

With these details in mind, well define the main distinctions between the two as this will help categorize and explain these implementations and the di"erences that exist between stateless and stateful firewalls. The main focus will be on how they compare to each other in terms of packet filtering performance, levels of security features o"ered and latent hardware requirements to run these functions. Let’s start o" by understanding what both stateless and stateful firewalls are, what they are meant to do, and finally how stateless/stateful firewalls implemented as a solution compare in the real world.

Stateless Firewalls



Stateless firewalls are some of the oldest firewalls on the market and have been around for almost as long as the web itself.

The purpose Of stateless firewalls is to protect computers and networks — specifically: routing engine processes and resources. They provide this security by filtering the packets of incoming tra c distinguishing between udp/tcp tra c and port numbers. The packets are either allowed entry onto the network or denied access based either their source or destination address or some other static information such as the tra c type (udp/tcp).These days completely stateless firewalls are far and few in-between.

Today they are most commonly seen in the form of CPE's (modems/router combos) given to customers by typical service providers. This equipment, usually given to residential internet consumers, provide simple firewalls using packet filtering and port forwarding functionality built on top of low-power CPE's. Providing very basic but powerful security restricting incoming and outgoing tra c useful to protect commonly abused ports often by self-propagating or DDOSing malware, such as ports 443, 53, 80 and 25. This blanket port filtering is mostly implemented using white-lists allowing only a few key ports for application-specific tra c such as VoIP, as 90% of all internet tra c traverses with the Hyper-Text Transfer Protocol (HTTP) through proxy requests to Domain Name Servers (DNS). In other cases, such as when hosting servers for: multiplayer video games, email/web services, or live-streaming video, users must manually configure these firewalls outside of their default security policy to allow different ports & applications through the filter.

One commonly known pitfall of stateless firewalls is that they are unable to view packets as part of wider tra c and will inspect them in isolation and are mostly unable to distinguish the myriad of application-level tra c types (such as HTTP, HTTPS, FTP, VoIP, SSH, etc). This can make them function more efficiently due to them only checking the header part of an inspected packet.

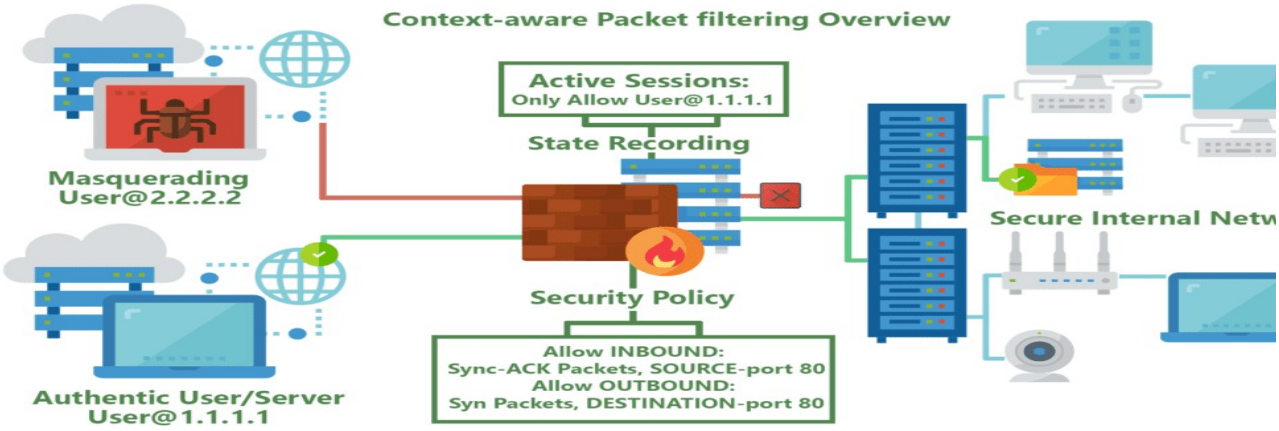
Pros of stateless firewall

- Stateless firewall deliver fast performance.
- Heavy traffic is no match for stateless firewall.
- Stateless firewall have historically been cheaper to purchase although these days stateful firewall have significantly comedown in price.

Cons of stateless firewall

- Stateless firewall do not inspect traffic.
- Stateless firewall does not examine an entire packets.
- Stateless firewall require some configuration to arrive at a suitable level of protection.

Stateful Firewall



Most firewalls today over at least some basic level of stateful monitoring. The main distinction between what can be very rudimentary stateful firewalls, and extremely robust packet-processing solutions, is in the level of protocol support. Greater support for differentiating between the diverse tra c and protocol types provides firewalls with the e cacy needed to analyze numerous application-level tra c, such as multimedia protocols, datagram protocols, file-transfer protocols, authentication/security protocols and so on.

Stateful firewalls are a more advanced, modern extension of stateless packet filtering firewalls in that they are continuously able to keep track of the state of the network and the active connections it has such as TCP streams or user datagram protocol (UDP) communication. The ability to acknowledging & utilize the context of incoming tra c and data packets is one of the principle advantages stateful firewalls have over their stateless cousins, allowing them to understand how to tell the difference between legitimate and malicious tra c or packets. This ultimately gives stateful firewalls one of the most powerful security tools in modern policies that protect their network connections through the implementation of additional security procedures for new or ongoing/active connections. In most cases, new connections will need to introduce

Stateful firewalls are not without their vulnerabilities, however. The special handshake involved in establishing new active connections requires a significant increase in software/network connection complexity & the computational power needed to implement them, leaving such firewalls vulnerable to cyber threats such as distributed denial of service (DDoS) attacks. This threat has been mitigated by many users of stateful firewalls by spreading out a network's tra c

across more firewall appliances, with many using third-party cloud-based service middle-men, in order to reduce the risk and necessary infrastructure

Pros of Stateful firewall

- Stateful firewall are highly skilled at detecting unauthorized attempts and forged messages (forged=fake).
- Stateful firewall do not need many port to open for proper connection.
- Statefull firewalls offers extensive logging capabilities and robust attack prevention (robust = strong, tough) .
- An intelligent system , stateful firewall base future filtering decision on the cumulative sum of past and present finding.

Cons of stateful firewall

- Vulnerabilities may allow a hackers to compromise and take control over a firewall that is not updated with the latest software releases.
- Some stateful firewall can be tricked to allow outside connection with an action as simple as viewing a WebPages.
- Man-in-the-middle attacks may pose grether vulnerabilities.

Which is better?

As is with most things, this varies on a case-by-case basis, with only the most basic residential users likely served well with their mostly stateless firewall given by their service providers. When it comes to power-users or business oriented networks, they are best served by the powerful stateful firewall implementations provided by dedicated systems running software such as PFSense, Endian Having said this, while next-gen stateful firewalls

Over all of the same security features present in stateless firewalls, they do not come without the need for cost-benefit analysis that should be done in regards to their feature-set and packet-

filtering depth. The as important trade-o"s and aspects of modern firewalls boil down to these requirements:

σ

- Security Level (How secure/sensitive the information & network is)
- Performance Requirements (packets per second, devices on network, application overhead)
- Software/Hardware Complexity, in terms of the integrations of upgradability, maintenance & support/EOL infrastructure, space

For simple home use, modern computers have more than enough power to run robust software-based firewalls on desktop PC's for example, but to easily secure the entire network using always-on purpose built low-power appliances like the NCA-1210 Edge Security Appliance is a more cost-effective solution. Much more stable as a whole, these dedicated appliances can be configured to consistently protect all home & handheld devices like smart thermostats/lights, IP cameras and smart phones from unwanted snooping/tampering by intruders – 24/7 while keeping maintenance, power, space and heat footprints to a minimum.

For more advanced usage such as small businesses, power users (online collaborators, home labs, tech enthusiasts, live-streamers) & larger entities, robust stateful firewalls are almost

certainly the most viable option to protect sensitive user data, connections and active services.Here the heavier upfront cost of powerful hardware like the FW-8894 NGFW is less significant

compared to the massive issues arising from the damages of lackluster security. Sub-par security can enable data breaches bringing issues such as: lawsuits, corporate/public image taint, service outages and contract/privacy breaches can all easily dwarf any upfront security investments.

Today businesses looking for the right security solution are best served by experts in the field of network security & hardware/software integration like Lanner. Capable of providing full services like validation, security module integration & quality assurance from the start – from the silicon & factory assembly all the way to the business premises.

Pros of Stateful Firewalls	Cons of Stateful Firewalls	Pros of Stateless Firewalls	Cons of Stateless Firewalls
+ Stateful firewalls are highly skilled at detecting unauthorized attempts or forged messaging.	- Vulnerabilities may allow a hacker to compromise and take control over a firewall that is not updated with the latest software releases.	+ Stateless firewalls deliver fast performance.	- Stateless firewalls do not inspect traffic.
+ The powerful memory retains key attributes of network connections.	- Some stateful firewalls can be tricked to allow or even attract outside connections with an action as simple as viewing a webpage.	+ Heavy traffic is no match for stateless firewalls, which perform well under pressure without getting caught up in the details.	- The stateless firewall also does not examine an entire packet, but instead decides whether the packet satisfies existing security rules.
+ These firewalls do not need many ports open for proper communication.	- Man-in-the-middle attacks may pose greater vulnerabilities.	+ Stateless firewalls have historically been cheaper to purchase, although these days stateful firewalls have significantly come down in price.	- These firewalls require some configuration to arrive at a suitable level of protection.
+ Stateful firewalls offer extensive logging capabilities and robust attack prevention.			
+ An intelligent system, stateful firewalls base future filtering decisions on the cumulative sum of past and present findings.			

Should you choose a stateless or stateful firewall?

Firewalls provide security for businesses of all sizes. Looking at the pros and cons of different types of firewalls can help to narrow down which is the best fit for your business.

Small Business Firewall Needs

A small business such as a sole proprietorship or single-member LLC will benefit from a firewall to keep internal documents and systems safe while keeping out the bad guys. Considering the typically higher cost of the stateful firewall, it's reasonable that a stateless firewall instead would be a suitable choice for small business needs. Tra□c volumes may be lower than a major enterprise, so incoming threats may also be fewer and farther between. The fast performance of a stateless firewall coupled with its ability to handle large loads make this firewall a possible choice for savvy small business owners.

Enterprise Firewall Needs

Also known as dynamic packet filtering, stateful firewalls tend to offer better security features for corporations than stateless firewalls. These firewalls are powerful workhorses prepared to detect threats and confront them head-on. Sophisticated memory capabilities allow the firewall system to grow smarter over time. Continual tra□c monitoring provides a thick layer of security that complements other protective measures for larger corporations. Robust attack prevention and logging capabilities empower network administrators to keep organizational assets intact.

Other Scenarios for Choosing Stateless Firewalls

Keep in mind that stateless firewall technology is somewhat outdated. That said, there are a few situations where this technology may be a viable option:

- A small office with few trusted people who are looking for routing capabilities could get by with a stateless firewall.
- Stateless firewalls may also be enough when used inside a network, residing between VLANs to add a bit more control but knowing that the external tra□c is already being handled by a stateful (and preferably “Next Gen” firewall).

DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
OSI	Open Systems Interconnection
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network