Firewall Technologies

by Sophia

WHAT'S COVERED

In this lesson, you will learn about various firewall technologies and some prominent features of firewalls. This includes discussion about network-based firewalls, host-based firewalls, packet-filter firewalls, and access control lists. You will also learn about scanning services and other firewall features including content filtering, signature identification, context awareness, and security zones.

Specifically, this lesson will cover

1. Defining Firewalls

Firewalls are usually a combination of hardware and software. The hardware part is usually a router, but it can also be a computer or a dedicated piece of hardware called a black box that has two network interface cards (NICs) in it. One of the NICs connects to the public side, and the other one connects to the private side. Its software is configured to scrutinize each incoming and outgoing packet and reject any suspicious ones.

Firewalls generally allow only packets that pass specific security restrictions to get through; they can also permit, deny, encrypt, decrypt, and proxy all traffic that flows through, either between the public and private parts of a network or between different security domains, or zones, on a private network. The system

administrator decides on and sets up the rules a firewall follows when deciding to forward data packets or reject them.

Firewalls can be placed on top of an existing operating system or be self-contained. A version of a firewall, black-box systems are typically proprietary and have external controls that aren't controlled by the operating system itself. Another option is to use a Unix or Windows, general-purpose server operating system to run your firewall. These both support third-party firewall products.

DID YOU KNOW

If your firewalls are not configured properly, they are not going to effectively protect network assets. Most firewalls are configured as default-deny, meaning that the only network connections allowed are the ones explicitly permitted. A system administrator has to configure this, and with the multitude of applications and ports involved in internal-external network communication, firewall configuration can be complex. Some firewall administrators may resort to the default-allow option, where all traffic is allowed to pass through unless it has been specifically blocked. But doing this is not best practice because it may permit inadvertent or undesirable network connections and make security breaches much more likely to happen. Even though the default-allow option is easier to configure, this method is best to be avoided.

TERM TO KNOW

Firewall

Software and/or hardware that monitors traffic in and out of a private network or a personal computer and allows or blocks such traffic depending on its perceived threat.

1a. Network-Based Firewalls

A **network-based firewall** is what companies use to protect their private network from public networks. The defining characteristic of this type of firewall is that it is designed to protect an entire network of computers instead of just one system. It is usually a combination of hardware and software.

HINT

Protecting an entire network of computers from malicious attacks is quite the challenge. Most of the firewall features that we are going to cover in this lesson are designed with this goal in mind, although the technology is certainly applicable to host-based firewalls too.

TERM TO KNOW

Network-based firewall

A type of firewall that is designed to protect an entire network.

1b. Host-Based Firewalls

In contrast to a network-based firewall, a **host-based firewall** is implemented on a single machine, so it protects only that one machine. This type of firewall is usually a software implementation because you do not need any additional hardware in your personal computer to run it. All current Windows client operating systems come with the Windows Defender Firewall, which is a great example of a host-based solution.

DID YOU KNOW

Host-based software solutions are typically not as secure as a separate hardware-based solution. This is because if you are running a dedicated black-box firewall, and someone manages to hack in and disable it, your best-case scenario may be just a ruined firewall. Believe it or not, even if that happens, all the data on your internal network may still be safe if the attacker was not able to get past the black-box. But if an attacker were able to penetrate your internal network and make it through the software firewall running on your local computer, they could not only view or steal your files, but also vandalize your entire system.

TERM TO KNOW

Host-based firewall

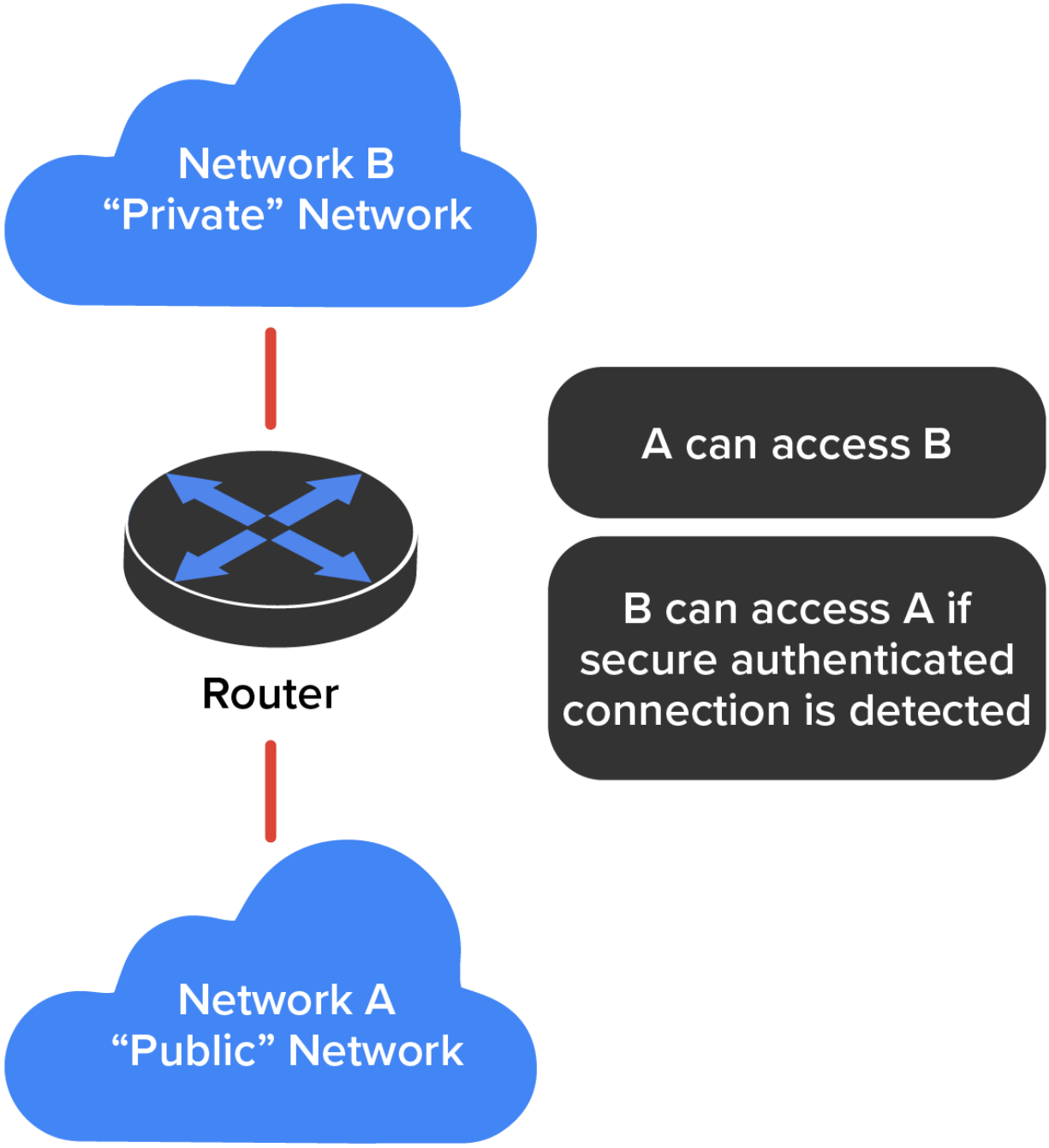
A type of firewall that is implemented locally on a single machine to protect only that one machine.

2. Firewall Technologies

There are many types of firewall technologies, and they all differ in the way that they restrict information flow. Things like access control lists and dynamic packet filtering are often used as firewalls in their own right, or they can be implemented along with proxies, DMZs, and other firewall technologies to build a serious, formidable system of protection.

2a. Access Control Lists

The first line of defense for any network that is connected to the Internet is an **access control list** (ACL). ACLs reside on your routers and determine by IP addresses which machines are allowed to use those routers and in what direction. The diagram below gives you a great demonstration of how ACLs can work to prevent users on Network B from accessing Network A. However, hosts from Network B can access Network A if a secure authenticated connection is used.



TERM TO KNOW

Access control list

A security scheme for network-level security.

2b. Firewalls at the Application Layer Versus the Network Layer

By now, you know all about the OSI model and that Layer 7 (Application layer) is at the top of the model and the Network layer is third up from the bottom. And as a rule of thumb, the higher you get in the OSI model, the more complex the firewall actions become.

DID YOU KNOW

The first firewalls that were developed functioned solely at the Network layer, and the earliest of these were known as **packet-filter firewalls**, which means that the firewall looks at an incoming packet and applies it against the set of rules in the ACL(s). If the packet passes, it gets sent on. If not, the packet is dropped. This type of filtering is very basic because all the firewall considers is the individual packet. All that matters are the source and destination addresses, protocol, and port number. The firewall does not care whether that packet is stand-alone or part of another data stream. This process works fairly well for common protocols such as TCP and User Datagram Protocol (UDP), which communicate on predefined port numbers.

TERM TO KNOW

Packet-filter firewall

A type of firewall that looks at an incoming packet and applies it against the set of rules in an ACL.

2c. Stateful Versus Stateless Network Layer Firewalls

A basic packet filter does not care about whether the packet it is examining is stand-alone or part of a bigger message stream. That type of packet filter is said to be a **stateless firewall**, in that it does not monitor the status of the connections passing through it. These types of firewalls tend to be susceptible to various DoS attacks and IP spoofing. The one big advantage that a stateless firewall has over its stateful counterparts is that it uses less memory. Today, stateless firewalls are best used on an internal network where security threats are lower and there are few restrictions.

In contrast to a stateless firewall, a **stateful firewall** is one that keeps track of the various data streams passing through it. If a packet that is a part of an established connection hits the firewall, it is passed through. New packets are subjected to the rules as specified in the ACL. These types of firewalls are better at preventing network attacks that look to exploit existing connections, or DoS attacks.

A stateful firewall works at Layer 4 of the OSI Model (Transport layer) by using the TCP three-way handshake. First, the client sends a packet with the SYN bit set to the firewall. The firewall interprets this as a new connection and passes the request to the appropriate service provider on the internal network. Next, the service provider responds with a packet that has both the SYN and ACK bits set. Finally, the client responds with a packet with only the ACK bit set. At that point, the connection is considered established and the firewall will only allow packets that have the same connection identification. The established connection is logged in a state table.

If there is activity on the connection for a specified period of time, the connection will time out in the state table. Any new communication will need to be reestablished based on the ACL rules.

HINT

Stateful firewalls tend to be a bit slower at establishing connections than stateless ones because there is more processing to do. After the connection is established, though, stateful firewalls are usually faster because they just have to check the state table for the connection instead of comparing the packet against all the relevant ACLs. This is done via stateful packet inspection. Most stateful firewalls can also keep track of connections using connectionless protocols such as UDP.

TERMS TO KNOW

Stateless firewall

A firewall that does not monitor the status of the connections passing through it.

Stateful firewall

A firewall that monitors the status of the connections passing through it.

2d. Scanning Services

Most firewalls are capable of performing **scanning services**, which means that they scan different types of incoming traffic in an effort to detect problems. For example, firewalls can scan incoming HTTP traffic to look for viruses or spyware, or they can scan email looking for spam. You can often set scanning rules that will prevent users from downloading files over a certain size. Two categories of content are typically scanned: mail and web.

EXAMPLE The table below shows some examples of typical scanning functions you might configure, depending on your network's needs.

Category	Protocol	Function
Mail	SMTP and POP3	Scans all scannable files in an email
Mail	SMTP and POP3	Rejects all messages larger than 15 MB
Mail	SMTP	Rejects messages addressed to more than 100 recipients
Mail	SMTP	Cleans emails or attachments containing malware, and attaches a notification that the malware was deleted
Web	HTTP	Scans all file downloads
Web	HTTP	Scans webmail sites for AOL, MSN, Google, and Yahoo!
Web	FTP	Scans all file transfers
Web	HTTP and FTP	Skips scanning of files larger than 50 MB; can also enable deferred scanning
Web	HTTP and FTP	Cleans files in which malware is detected; deletes files that cannot be cleaned

You can adjust scanning configurations to address certain needs.

EXAMPLE If you are concerned about bandwidth, you can limit the size of files transferred via FTP or HTTP. If mail storage is an issue, then you can set the firewall to reject mail larger than 10 MB. Keep in mind that by changing firewall settings you may be increasing your security risk.

Content filtering is very closely related to scanning services. Specifically, **content filtering** means blocking data based on the content rather than the source of the data. Most commonly, this is used to filter email and website access.

The reason for using content filtering is to enforce organizational policies. For example, most companies have a zero-tolerance policy against hate speech or pornography. If a user on a company network uses that network to spread hate mail or pornography, the company could be liable for damages in a lawsuit if they did not take measures to prevent such actions. It is not only a moral issue, but a legal issue.

IN CONTEXT

Content filtering is also important in places like schools. Parents do not want their kids to be able to stumble upon an adult site in the school library while researching a school project. Content filtering can block sites from being accessed. You can also find several parental-control software packages for home use that employ content filtering.

There are several ways to filter content; here are some of the more common categories used:

- Attachment (blocking attachments of a certain type, such as EXE files)
- Content-encoding
- Email headers
- Language
- Phrases
- Proximity of words to each other
- URLs

Nearly all filtering methods use a combination of filters to protect users from improper content.

TERMS TO KNOW

Scanning services
Processes that scan different types of incoming traffic in an effort to detect problems.

Content filtering
Processes that block data based on the content of the application data rather than the source of the data.

2e. Signature Identification

Firewalls can also stop attacks and problems through a process called **signature identification**. Viruses that are known will have a signature, which is a particular pattern of data, within them. Firewalls (and antivirus programs)

can use signatures to identify a virus and remove it. The same holds true for other types of malware, such as worms and spyware.

Numerous network attacks have signatures as well.

> EXAMPLE If your router starts getting hit by large numbers of SYN requests, you may be at the beginning of a SYN flood attack. The inundation of SYN traffic is a signature of a SYN flood.

TERM TO KNOW

Signature identification

Processes that detect virus or attack signatures that contain a particular pattern of data.

2f. Context Awareness

A firewall that is 'context aware' is one that can take into consideration the context in which traffic is arriving at the firewall. It can detect different applications, users, and devices in addition to IP addresses. Because of this more sophisticated approach, context-aware firewalls let administrators track how applications are used across a range of devices. For example, they may track or prevent the posting or sharing of videos on Facebook using an iPhone, PC, or other device. Context-aware firewalls also enable companies to enforce policies, like not allowing a specific group of employees to access games on iPads.

2g. Zones

A **zone** is an individual area of the network that has been configured with a specific trust level. Firewalls are ideal devices to regulate the flow of traffic between zones. The diagram below provides a good example of how zone levels could work.

The Internet would be a zone with no trust or a low level of trust. The DMZ, located between the Internet and the internal network, could have a medium level of trust. The computers on the intranet would all be within a high trust zone. The higher the trust level, the less scrutiny you place on data coming from a computer in that zone.

TERM TO KNOW

Zone

An area of the network that has been configured with a specific trust level.

SUMMARY

In this lesson, you learned about various **firewall technologies**, as well as some prominent features of **firewalls**. Specifically, this lesson covered **network-based firewalls**, **host-based firewalls**, packet-filter firewalls, and **access control lists**. These technologies included **firewalls at the application layer versus the network layer** and **stateful versus stateless network-layer firewalls**. Finally, you learned about **scanning services** and other firewall features including content filtering, **signature identification**, **context awareness**, and security **zones**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Access Control List
A security scheme for network-level security.

Content Filtering
Processes that block data based on the content of the application data rather than the source of the data.

Firewall
Software and/or hardware that monitors traffic in and out of a private network or a personal computer and allows or blocks such traffic depending on its perceived threat.

Host-Based Firewall
A type of firewall that is implemented locally on a single machine to protect only that one machine.

Network-Based Firewall
A type of firewall that is designed to protect an entire network.

Packet-Filter Firewall
A type of firewall that looks at an incoming packet and applies it against the set of rules in an ACL.

Scanning Services
Processes that scan different types of incoming traffic in an effort to detect problems.

Signature Identification
Processes that detect virus or attack signatures that contain a particular pattern of data.

Stateful Firewall
A firewall that monitors the status of the connections passing through it.

Stateless Firewall
A firewall that does not monitor the status of the connections passing through it.

Zone

An area of the network that has been configured with a specific trust level.