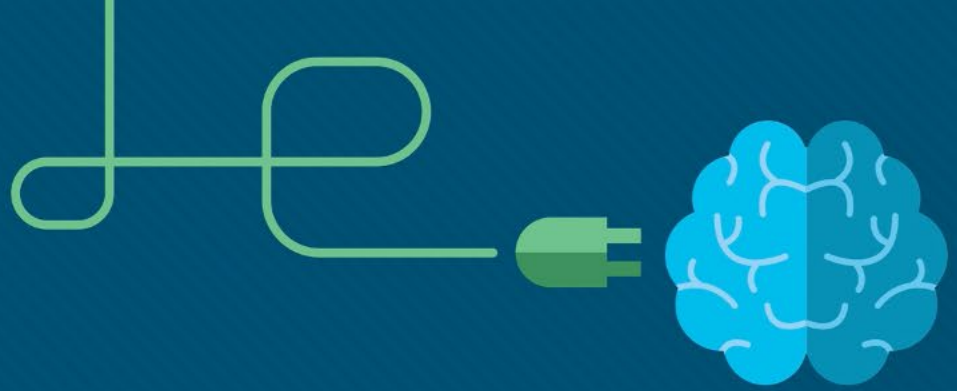


Module 15: Firewall Technologies

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Firewall Technologies

Module Objective: Explain how firewalls are implemented to provide network security.

Topic Title	Topic Objective
Secure Networks with Firewalls	Explain how firewalls are used to help secure networks.
Firewalls in Network Design	Explain design considerations for implementing firewall technologies

15.1 Secure Networks with Firewalls

Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Firewall features include:

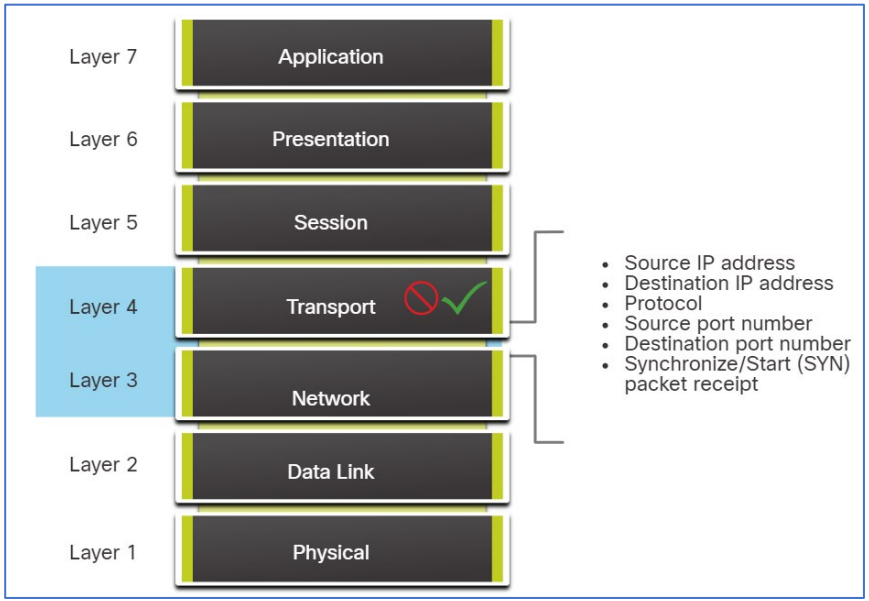
Firewall Features	Description
Common Firewall Properties	• Firewalls are resistant to network attacks. • Firewalls are the only transit point between internal corporate networks and external networks. • Firewalls enforce the access control policy.
Firewall Benefits	• They prevent the exposure of sensitive hosts, resources, and applications to untrusted users. • They sanitize protocol flow, which prevents the exploitation of protocol flaws. • They block malicious data from servers and clients. • They reduce security management complexity by off-loading most network access control to a few firewalls in the network.
Firewall Limitations	• A misconfigured firewall can have serious consequences for the network. • The data from many applications cannot be passed over firewalls securely. • Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attacks. • Network performance can slow down. • Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

Types of Firewalls

Common firewall types include packet filtering, stateful, application gateway, and next generation firewalls.

Packet Filtering (Stateless) Firewall

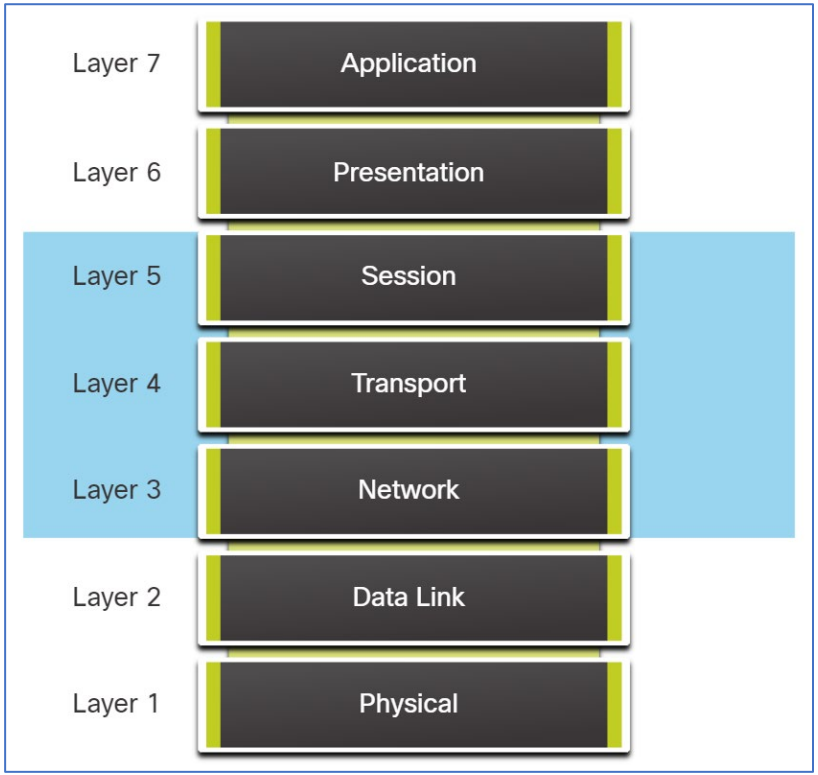
- Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



Types of Firewalls (Cont.)

Stateful Firewall

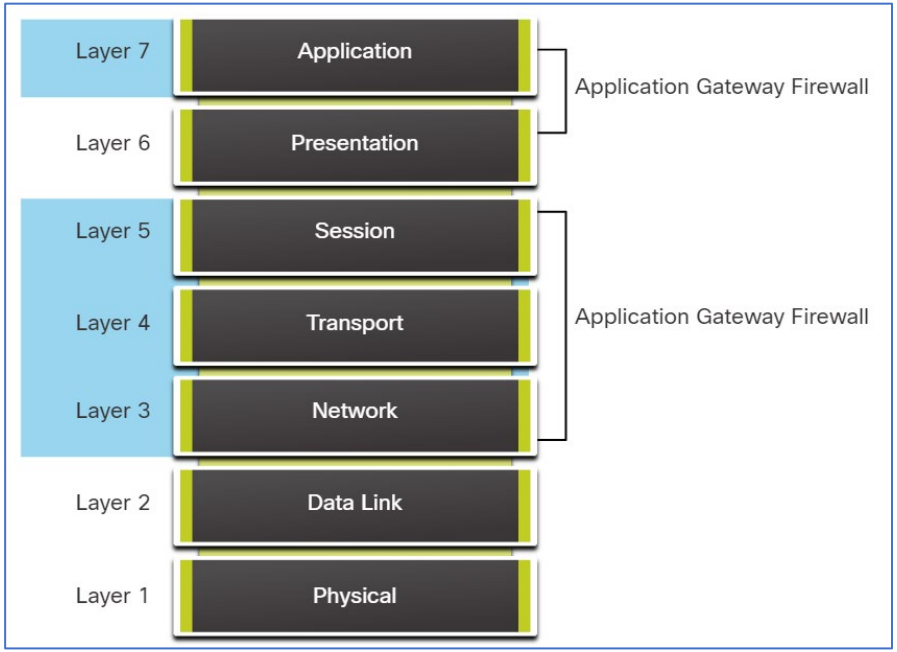
- Stateful firewalls are the most versatile and the most common firewall technologies in use.
- Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table.
- Stateful filtering is a firewall architecture that is classified at the network layer.
- It also analyzes traffic at OSI Layer 4 and Layer 5.



Types of Firewalls (Cont.)

Application Gateway Firewall

- An application gateway firewall (proxy firewall) filters information at Layers 3, 4, 5, and 7 of the OSI reference model.
- Most of the firewall control and filtering is done in software.
- When a client needs to access a remote server, it connects to a proxy server.
- The proxy server connects to the remote server on behalf of the client.
- Therefore, the server only sees a connection from the proxy server.



Types of Firewalls (Cont.)

Next Generation Firewall

Next-generation firewalls (NGFW) go beyond stateful firewalls by providing:

- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

Other methods of implementing firewalls include:

- **Host-based (server and personal) firewall** - A PC or server with firewall software running on it.
- **Transparent firewall** - Filters IP traffic between a pair of bridged interfaces.
- **Hybrid firewall** - A combination of the various firewall types. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall.

Packet Filtering Firewall Benefits and Limitations

Advantages and disadvantages of a packet filtering firewall include:

Packet Filtering Firewall	Description
Advantages of a packet filtering firewall	• Packet filters implement simple permit or deny rule sets. • Packet filters have a low impact on network performance. • Packet filters are easy to implement and are supported by most routers. • Packet filters provide an initial degree of security at the network layer. • Packet filters perform almost all the tasks of a high-end firewall at a much lower cost.
Disadvantages of a packet filtering firewall	• Packet filters are susceptible to IP spoofing. Threat actors can send arbitrary packets that meet ACL criteria and pass through the filter. • Packet filters do not reliably filter fragmented packets. Because fragmented IP packets carry the TCP header in the first fragment and packet filters filter on TCP header information, all fragments after the first fragment are passed unconditionally. Decisions to use packet filters assume that the filter of the first fragment accurately enforces the policy. • Packet filters use complex ACLs, which can be difficult to implement and maintain. • Packet filters cannot dynamically filter certain services. For example, sessions that use dynamic port negotiations are difficult to filter without opening access to a whole range of ports.

Stateful Firewall Benefits and Limitations

Some benefits and limitations to using a stateful firewall include:

Stateful Firewall	Description
Benefits	• Stateful firewalls are often used as a primary means of defense by filtering unwanted, unnecessary, or undesirable traffic. • Stateful firewalls strengthen packet filtering by providing more stringent control over security. • Stateful firewalls improve performance over packet filters or proxy servers. • Stateful firewalls defend against spoofing and DoS attacks by determining whether packets belong to an existing connection or are from an unauthorized source. • Stateful firewalls provide more log information than a packet filtering firewall.
Limitations	• Stateful firewalls cannot prevent application layer attacks because they do not examine the actual contents of the HTTP connection. • Not all protocols are stateful. For example, UDP and ICMP do not generate connection information for a state table, and, therefore, do not garner as much support for filtering. • It is difficult to track connections that use dynamic port negotiation. Some applications open multiple connections. This requires a whole new range of ports that must be opened to allow this second connection. • Stateful firewalls do not support user authentication.

15.2 Firewalls in Network Design

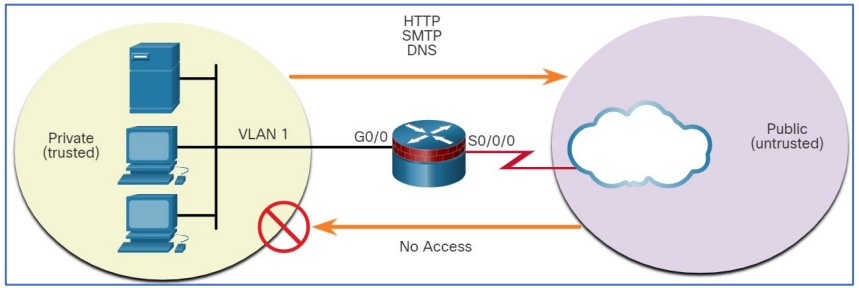
Common Security Architectures

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. Three common firewall designs are:

Private and Public

The public network (or outside network) is untrusted, and the private network (or inside network) is trusted. Typically, a firewall with two interfaces is configured as follows:

- Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
- Traffic originating from the public network and traveling to the private network is generally blocked.

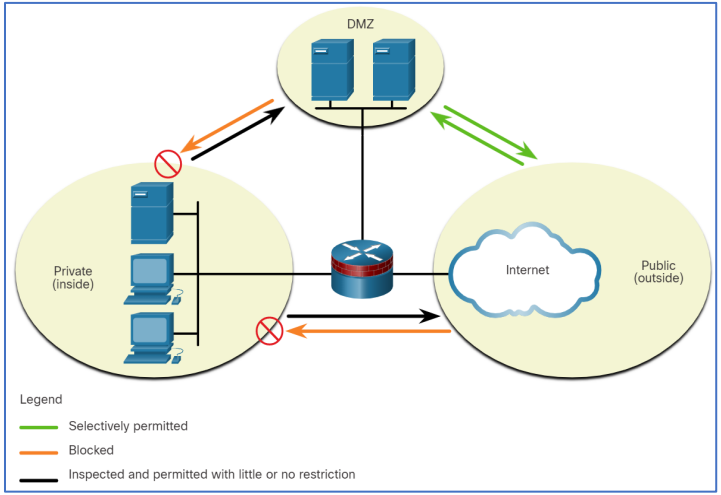


Common Security Architectures (Cont.)

Demilitarized Zone (DMZ)

A firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface.

- Traffic originating from the private network is inspected as it travels toward the public or DMZ network. Inspected traffic returning from the DMZ or public network to the private network is permitted.
- Traffic originating from the DMZ network and traveling to the private network is usually blocked.
- Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
- Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected.



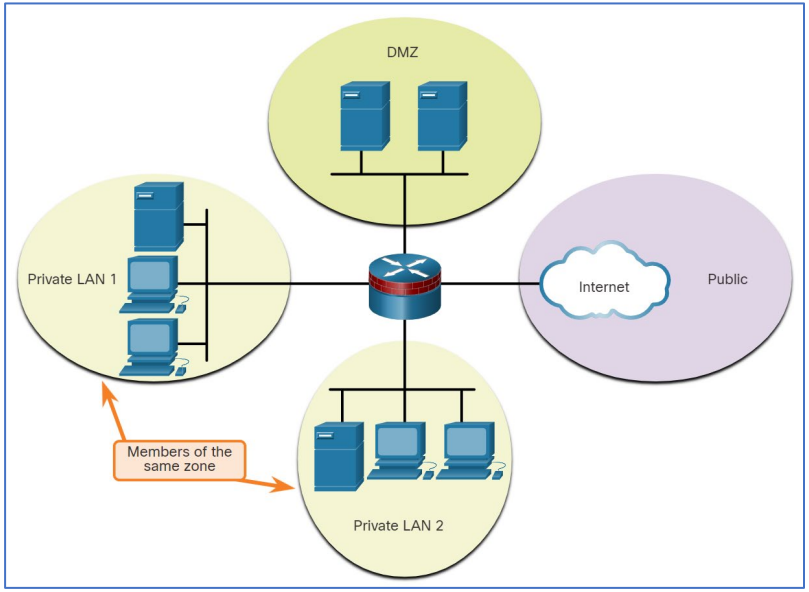
- Traffic originating from the public network and traveling to the private network is blocked.

Common Security Architectures (Cont.)

Zone-Based Policy Firewalls (ZPFs)

ZPFs use zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. Zones specify where a Cisco IOS firewall rule or policy should be applied.

- Security policies for LAN 1 and LAN 2 are similar and can be grouped into a zone for the firewall.
- By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely.
- All zone-to-zone traffic is blocked. Configure a policy allowing or inspecting traffic To permit traffic between zones.
- The only exception to this default **denying any** policy is the router's self-zone.



Layered Defense

A layered defense uses different types of firewalls combined in layers to add depth to an organization's security. For example:

- **Network core security** -Protects against malicious software and traffic anomalies, enforces network policies, and ensures survivability.
- **Perimeter security** -Secures boundaries between zones.
- **Communications security** -Provides information assurance.
- **Endpoint security** -Provides identity and device security policy compliance.

Policies can be enforced between layers and inside the layers. These policy enforcement points determine whether traffic is forwarded or discarded.

If the policy allows, the traffic goes to the screened firewall or bastion host system that applies more rules to the traffic and discards suspect packets.

Layered Defense (Cont.)

A layered defense approach is optional to ensure a secure internal network. A network administrator must consider many factors when building a complete in-depth defense:

- Firewalls typically do not stop intrusions from hosts within a network or zone.
- Firewalls do not protect against rogue access point installations.
- Firewalls do not replace backup and disaster recovery mechanisms resulting from attack or hardware failure.
- Firewalls are no substitute for informed administrators and users.

This partial list of best practices can serve as a starting point for a firewall security policy.

- Position firewalls at security boundaries.
- Deny all traffic by default and permit only services that are needed.
- Ensure controlled physical access to the firewall.
- Regularly monitor firewall logs.
- Practice change management for firewall configuration changes.
- Remember that firewalls primarily protect from technical attacks originating from the outside.

15.3 Firewall Technologies Summary

What Did I Learn in this Module?

- Packet filtering (stateless) firewalls provide Layer 3 and sometimes Layer 4 filtering.
- A stateful inspection firewall allows or blocks traffic based on state, port, and protocol.
- Application gateway firewalls (proxy firewall) filter information at Layers 3, 4, 5, and 7.
- Next-generation firewalls provide services beyond application gateways, such as integrated intrusion prevention, application awareness, control to see and block risky apps, access to future information feeds, and techniques to address evolving security threats.
- Common security architectures define the boundaries of traffic entering and leaving the network.
- Some designs are as simple as designating an outside network and an inside network determined by two firewall interfaces.
- Networks that require public can access to services will often include a DMZ that the public can access, while strictly blocking access to the inside network.
- ZPFs use the concept of zones to provide additional flexibility.
- A layered security approach uses firewalls and other security measures to provide security at different functional layers of the network.