4.2 FIREWALL TECHNOLOGIES

BY AFFENDY ILYAS, AHMAD SHA, AIMAN SYAFIQ, FATIN ZULAIKHA, HAARIHARAN, ARIF, FIRDAUS, IMRAN, IZHAM, NASUHA, AFIQAH, AIMI

4.2.1 Securing Networks with Firewall

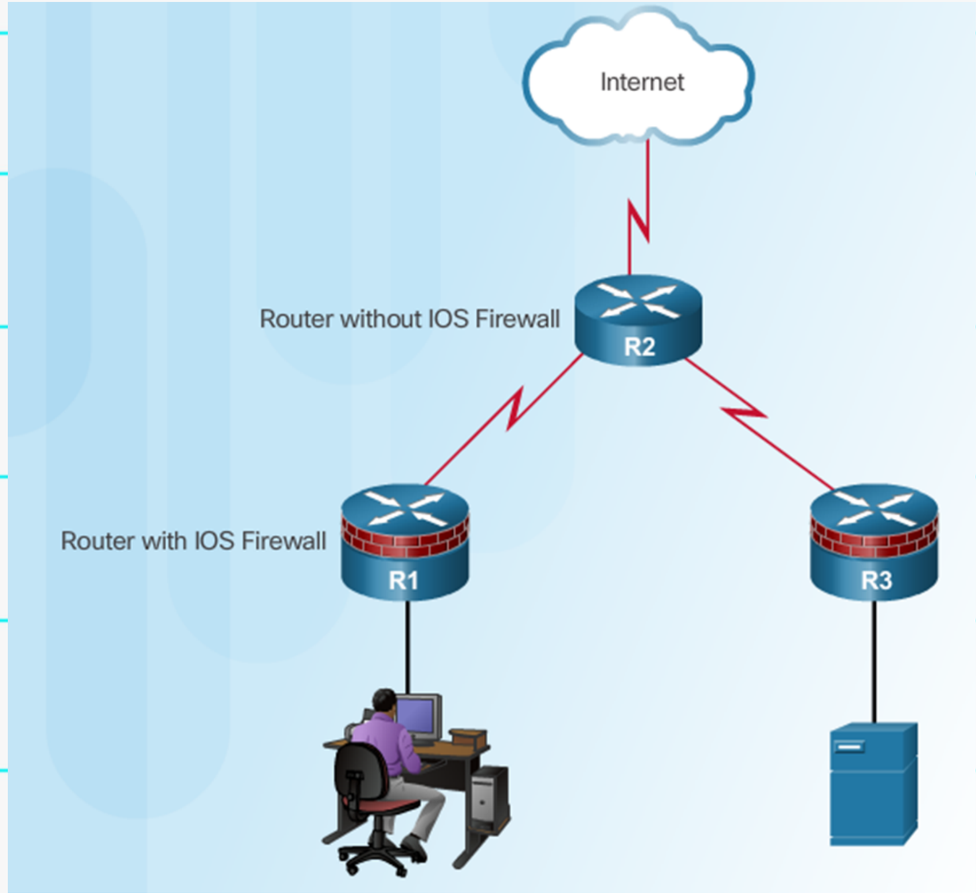
4.2.1.1 DEFINING FIREWALLS

01 Term firewall originally referred to a fireproof wall that prevented flames from spreading to connected structures.

02 Term in computer networks: a firewall prevents undesirable traffic from entering prescribed areas within a network.

All firewalls share some common properties:

- Firewalls are resistant to attacks.
- Firewalls are the only transit point between networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.



4.2.1.2 Benefits and Limitations of Firewalls

Benefits of Firewalls

- Prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
- Sanitize protocol flow, which prevents the exploitation of protocol flaws.
- Block malicious data from servers and clients.
- Reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

Limitations of Firewalls

1. A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.

2. The data from many applications cannot be passed over firewalls securely.

3. Network performance can slow down.

4. Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

5. Users might proactively search for ways around the firewall to receive blocked material

FIREWALL OPERATION

ALLOW OPERATION	DENY OPERATION
• Allow traffic from any external address to the web server • Allow traffic to FTP server • Allow traffic to SMTP server • Allow traffic to internal IMAP server	• Deny all inbound traffic with network addresses matching internal-registered IP address • Deny all inbound traffic to server • Deny all inbound ICMP echo • Deny all inbound MS Active Directory • Deny all inbound traffic to MS SQL queries • Deny all MS Domain Local Broadcasts

4.2.2 Types of Firewalls

4.2.2.1 Firewall Type Description

4.2.2.2 Packet Filtering Firewall Benefits and Limitations

4.2.2.3 Stateful Firewalls

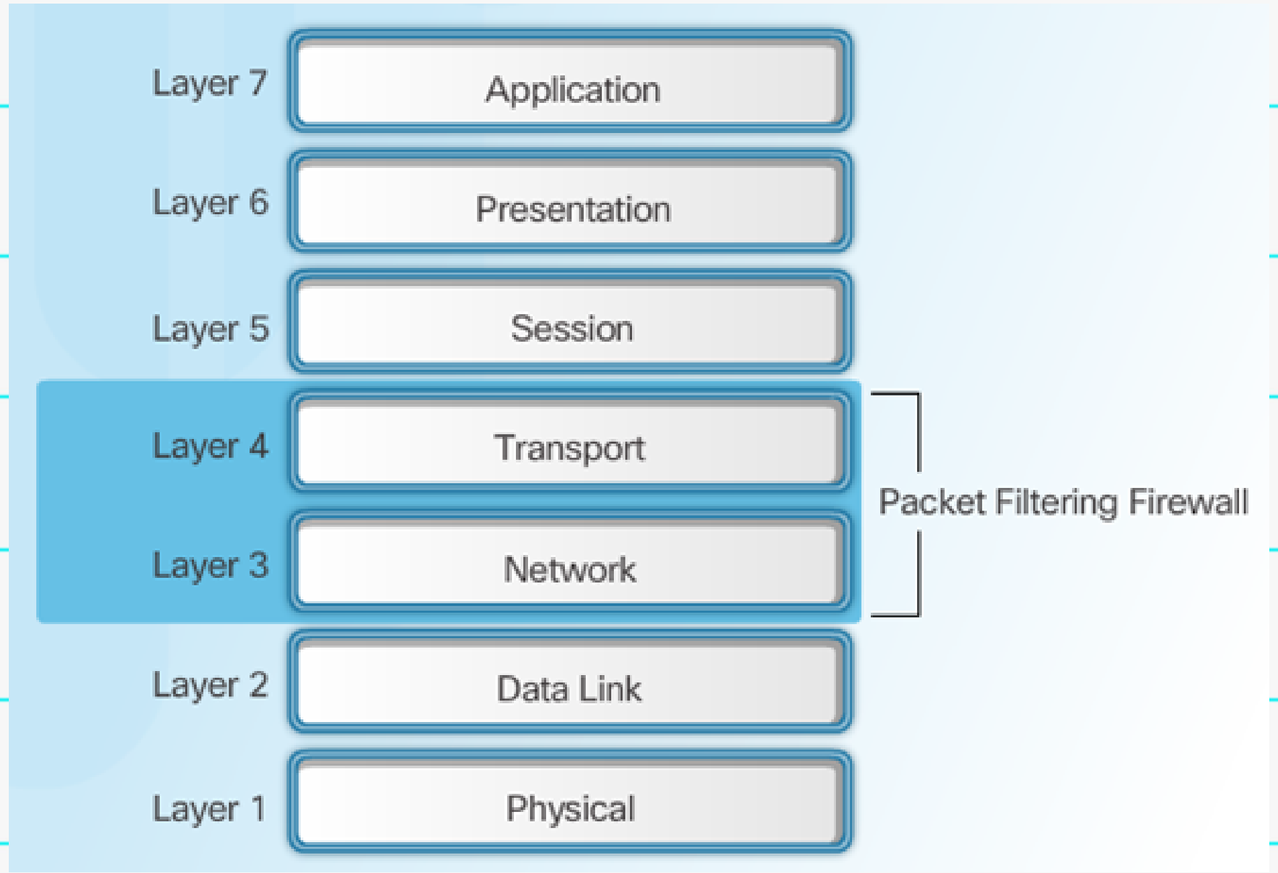
4.2.2.4 Stateful Firewall Benefits and Limitations

4.2.2.5 Next Generation Firewalls

4.2.2.1 Firewall Type Description

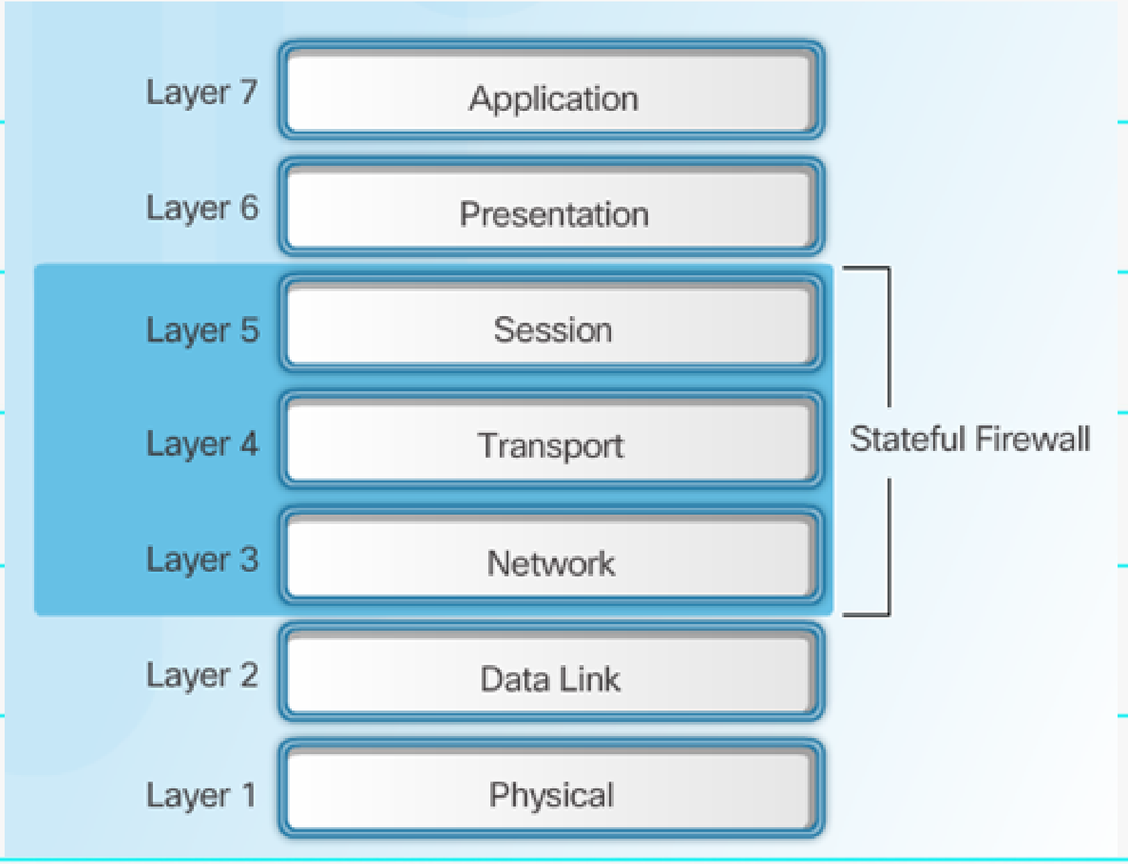
1. Packet Filtering Firewall

Typically a router with the capability to filter some packet content, such as Layer 3 and sometimes Layer 4 information



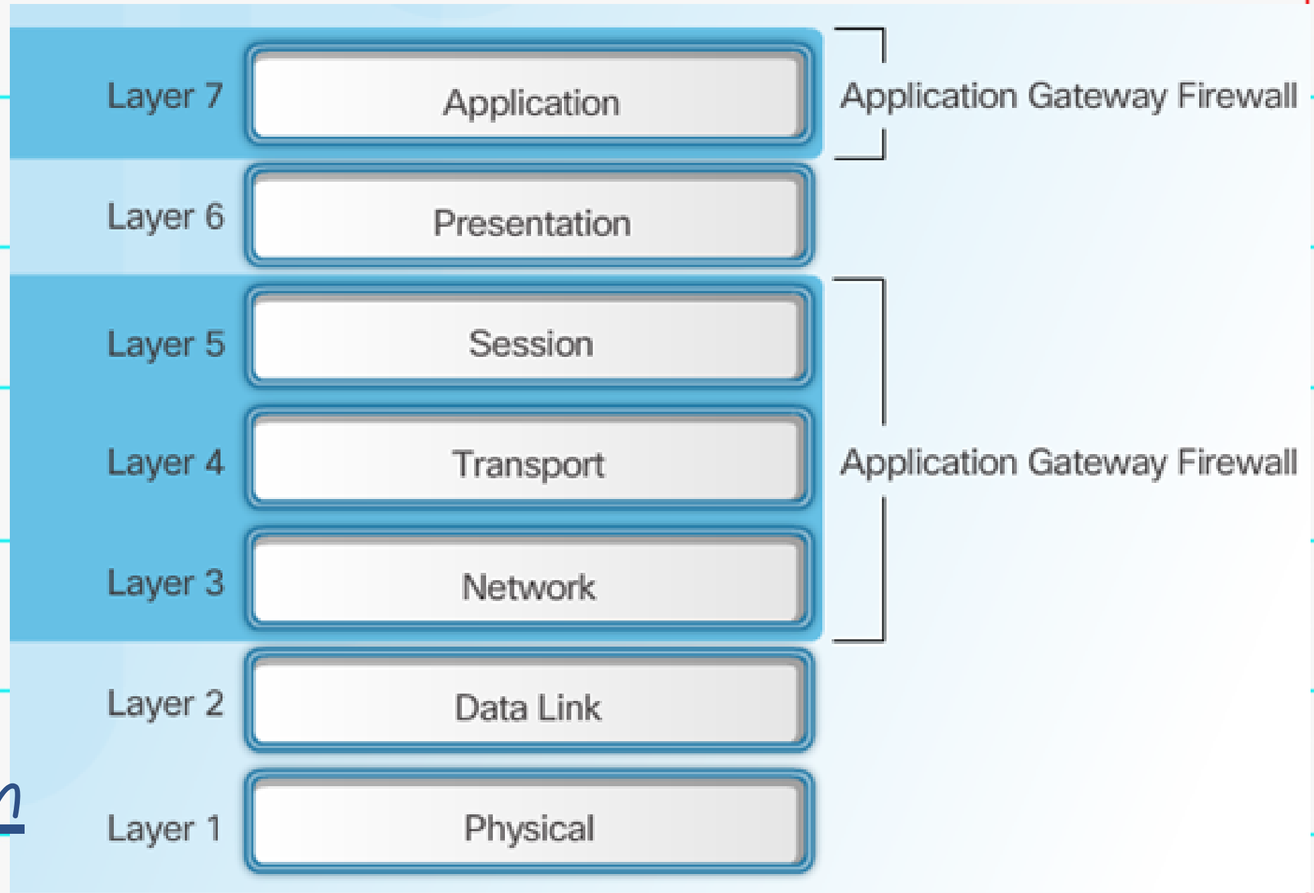
2. Stateful Firewall

Monitors the state of connections, whether the connection is in an initiation, data transfer, or termination state



3. 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. The proxy server connects to the remote server on behalf of the client.



4.2.2.2 Packet Filtering Firewall Benefits and Limitations

Packet filters implement simple permit or deny rule sets.

Packet filters are easy to implement, and are supported by most routers.

Packet filters have a low impact on network performance.

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.

LIMITATIONS USING A PACKET FILTERING FIREWALL

1. Packet filters are susceptible to IP spoofing. Hackers can send arbitrary packets that meet ACL criteria and pass through the filter.

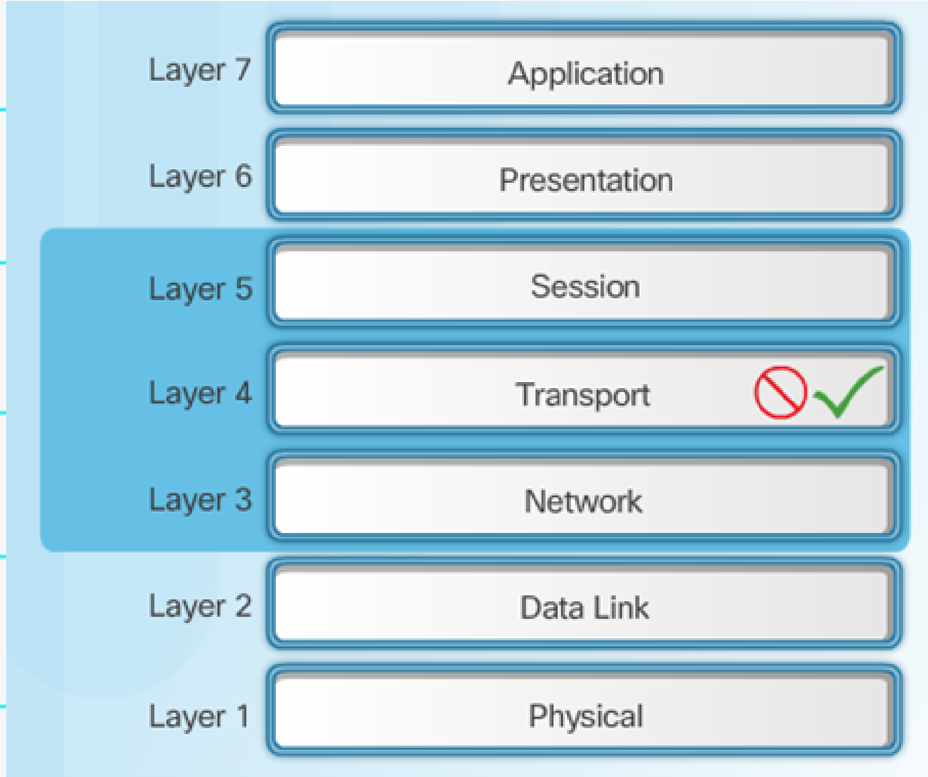
2. Packet filters use complex ACLs, which can be difficult to implement and maintain.

3. Packet filters are stateless. They examine each packet individually rather than in the context of the state of a connection.

4. Packet filters cannot dynamically filter certain services and packet filters do not reliably filter fragmented packets.

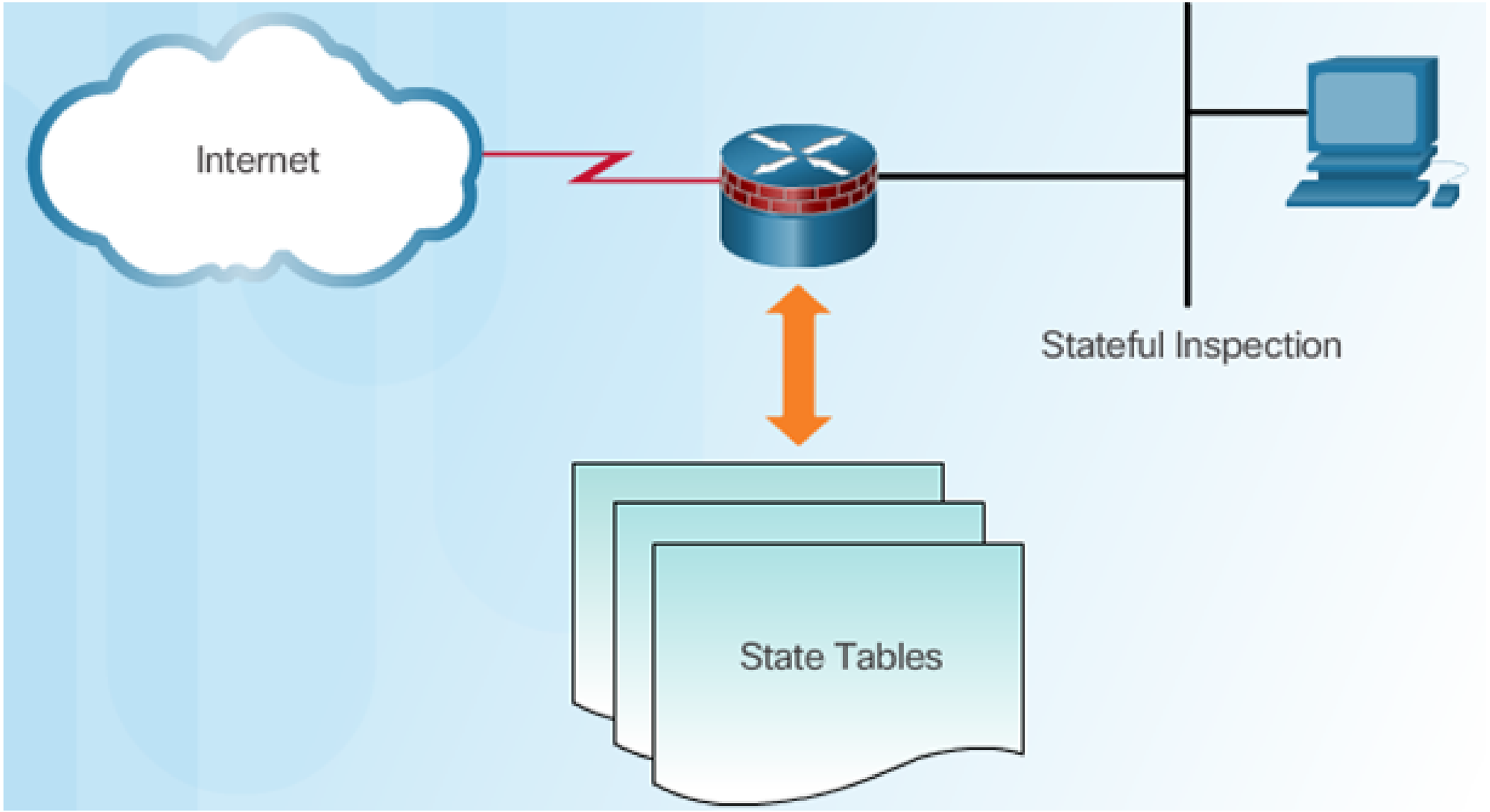
4.2.2.3 Stateful Firewalls

1. Stateful Firewalls and OSI Model

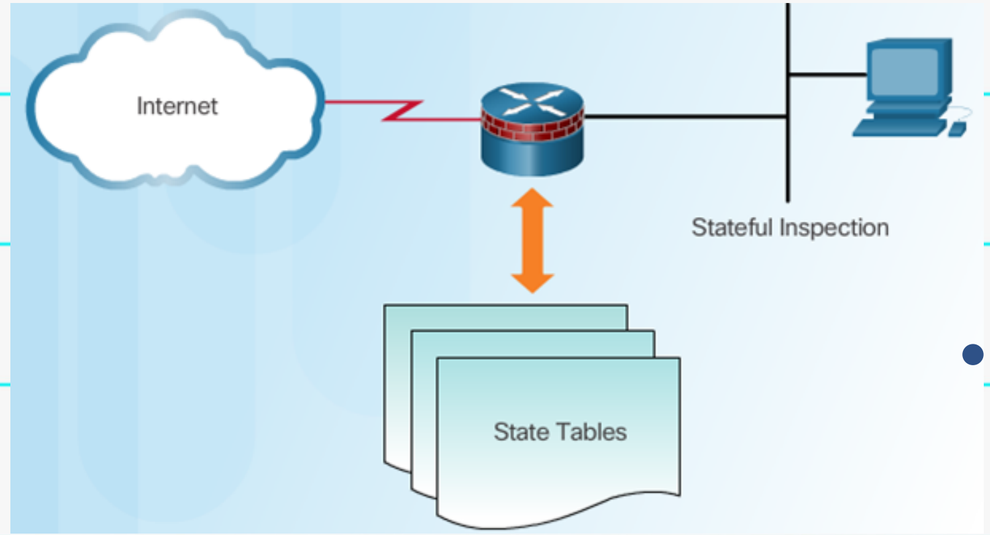


- Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table.
- Stateful filtering is a firewall architecture that is classified at the network layer.
- It tracks each connection traversing all interfaces of the firewall and confirms that they are valid.
- The firewall examines information in the headers of Layer 3 packets and Layer 4 segments.

Figure 2. State Tables



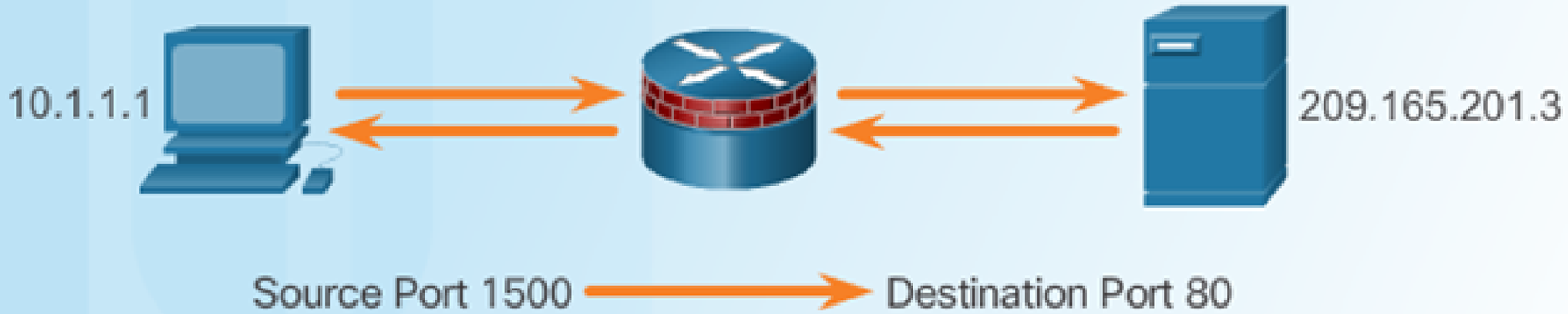
2. State Tables



- Stateful firewalls use a state table to keep track of the actual communication process, as shown in this Figure.

- Each time a TCP or UDP connection is established for inbound or outbound connections, a stateful firewall logs the information in a state table for that specific flow.

Figure 3. Stateful Firewall Operation



Inside ACL (Outgoing Traffic)	Outside ACL (Incoming Traffic)
`permit ip 10.0.0.0.0.0.0.255 any`	`Dynamic: permit tcp host 209.165.201.3 eq 80 host 10.1.1.1 eq 1500`

3. Explaining Stateful Firewall Operation

- Figure 3 shows host 10.1.1.1 is requesting a web page from the server at 209.165.201.3.
- During the request, the stateful packet filter firewall retains certain details by saving the state of the request in the state table.
- After that router dynamically added an access control entry for return traffic sourced from server 209.165.201.3, on port 80, and destined to host 10.1.1.1 on port 1500.

4.2.2.4 Stateful Firewall Benefits and Limitations

Benefits	Limitations
• Primary means of defense • Strong packet filtering • Improved performance over packet filters • Defends against spoofing and DoS attacks • Richer data log	• No application layer inspection • Limited tracking of stateless protocols • Difficult to defends against dynamic port negotiation • No authentication support port negotiation

4.2.2.5 Next Generation Firewalls

Granular identification, visibility, and control of behaviors within applications.

Proactive protection against Internet threats.

Performance of NAT, VPN, and SPI.

Restricting web and web application use based on the reputation of the site.

Enforcement of policies based on the user, device, role, application type, and threat profile.

Use of an IPS (Intrusion Prevention System)

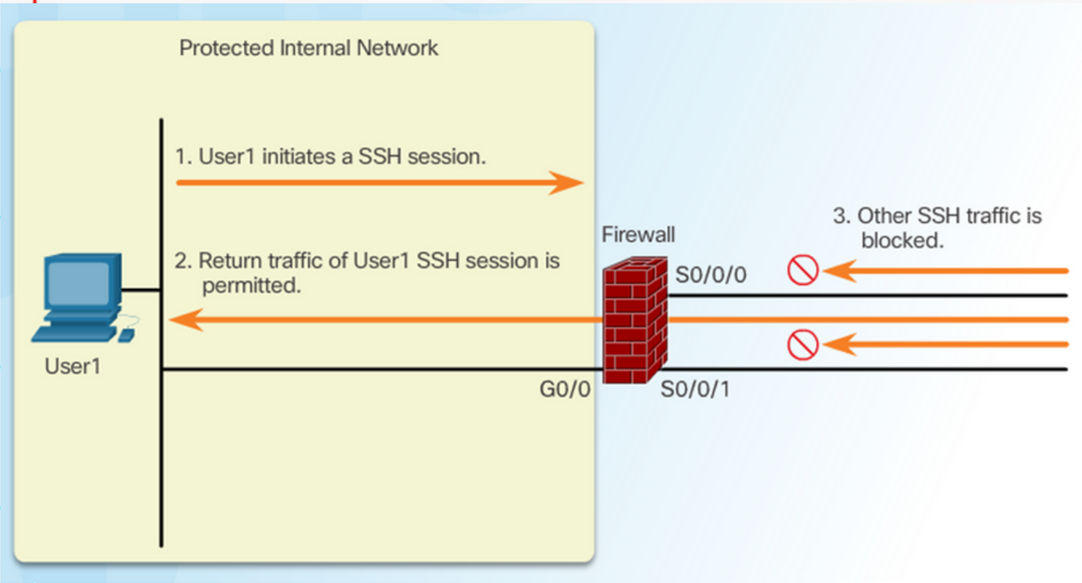
4.2.3 Classic Firewall

4.2.3.1 Introducing Classic Firewall

4.2.3.2 Classic Firewall Operation

4.2.3.3 Classic Firewall Configuration

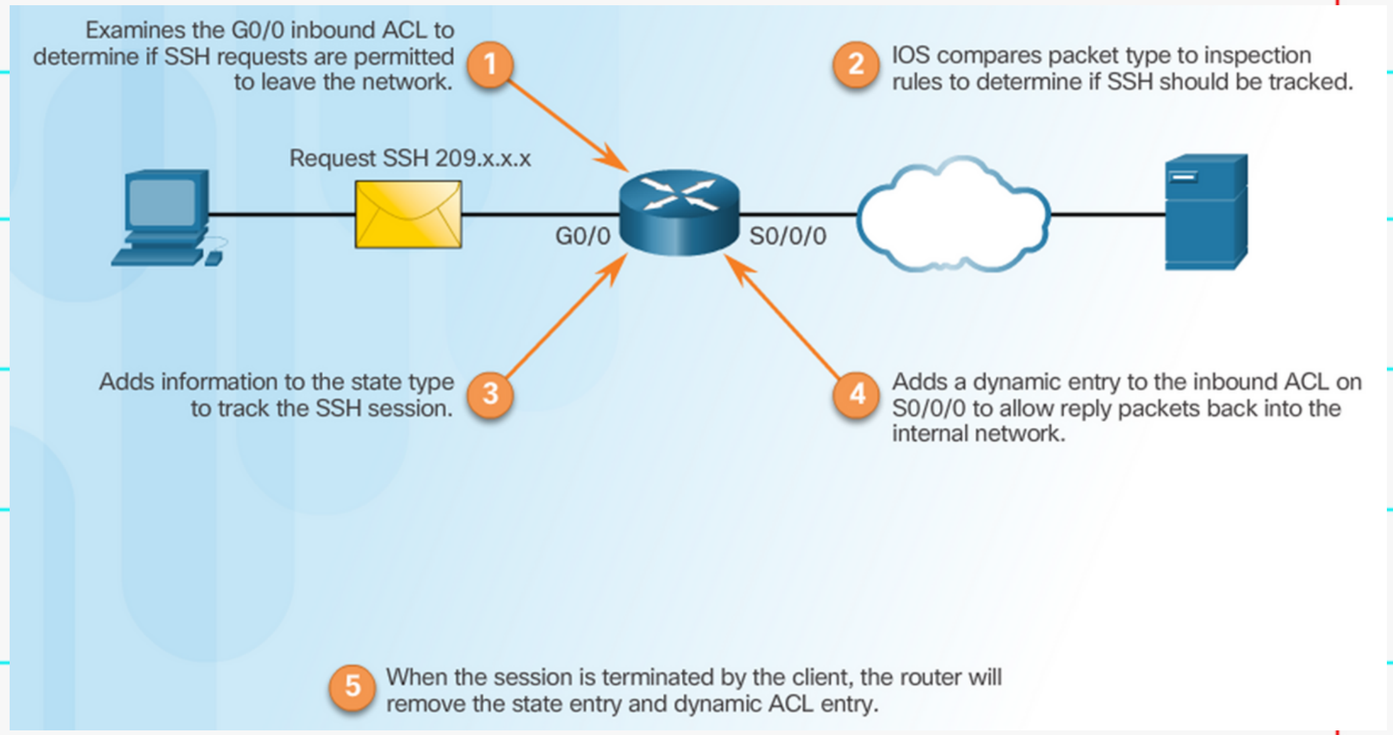
4.2.3.1 Introducing Classic Firewall



- Cisco IOS Classic Firewall, formerly known as context-based access control (CBAC), is a stateful firewall feature added to the Cisco IOS prior.
- Classic Firewall provides four main functions: traffic filtering, traffic inspection, intrusion detection, and generation of audits and alerts also examine supported connections for embedded NAT and Port Address Translation (PAT) information and perform the necessary address translations.
- Additionally, Classic Firewall only detects and protects against attacks that travel through the firewall.
- Cisco IOS Software Classic Firewall will continue to be maintained for the future.
- The strategic development direction for Cisco IOS Software's will be carried by the Zone-Based Policy Firewall (ZPF).

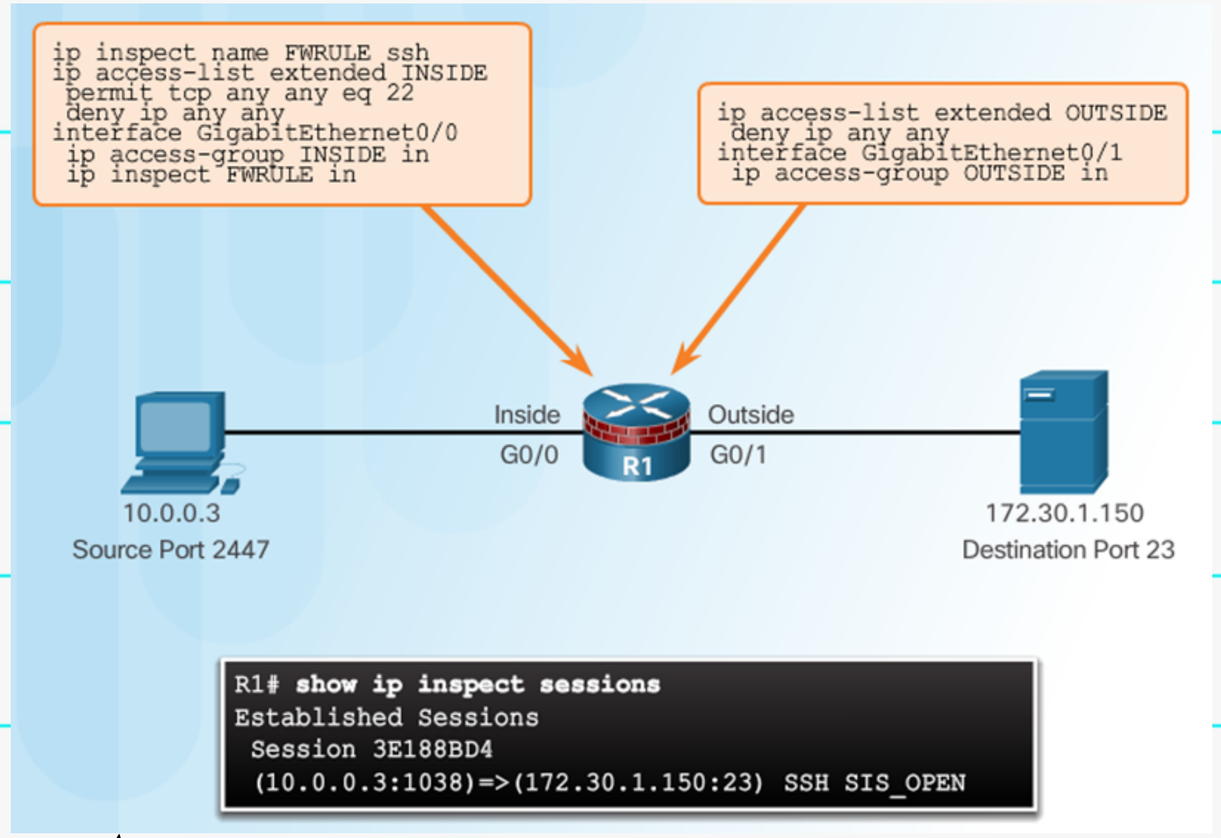
4.2.3.2 Classic Firewall Operation

Classic firewall creates temporary openings in the ACL to allow returning traffic and enabled to inspect SSH traffic.



1. If the ACL denies this type of connection, the packet is considered invalid and may be thrown away.
2. Based on the inspection rules for Classic Firewall, the Cisco IOS software might inspect the connection otherwise, the connection goes to the next step.
3. The connection information is compared to entries in the state table and if it does exist, the idle timer for the connection is reset.
4. If a new entry is added, a dynamic ACL entry is added to allow the returning SSH traffic that is part of the same SSH connection. These dynamic ACL entries are not saved to NVRAM.
5. When the session terminates, the dynamic information from the state table and the dynamic ACL entry are removed.

4.2.3.3 Classic Firewall Configuration



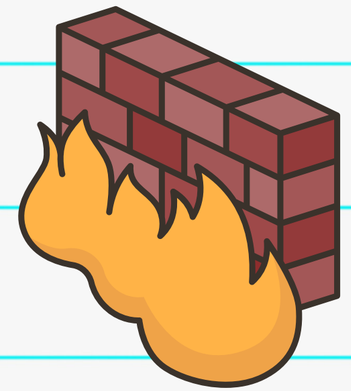
Steps to configure this policy using a Classic Firewall.

Step 1: Choose the internal and external interfaces.

Step 2: Configure ACLs for each interface.

Step 3: Define inspection rules.

Step 4: Apply an inspection rule to an interface.



The administrator wants to allow SSH sessions between the 10.0.0.0 and 172.30.0.0 networks. However, only hosts from the 10.0.0.0 network are allowed to initiate SSH sessions. All other access is denied.

4.2.4 Firewalls in Network Design

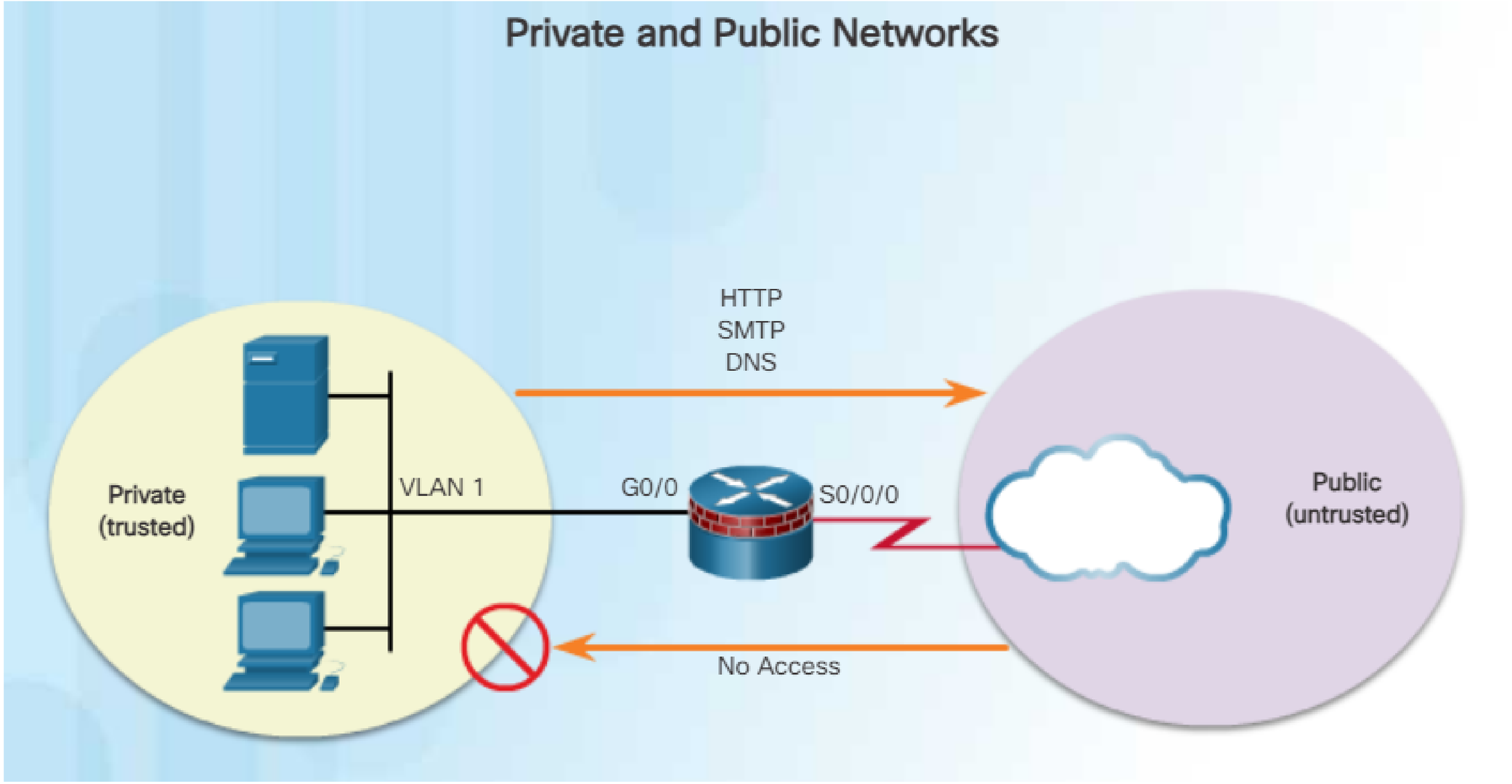
4.2.4.1 Inside and Outside Networks

4.2.4.2 Demilitarized Zones

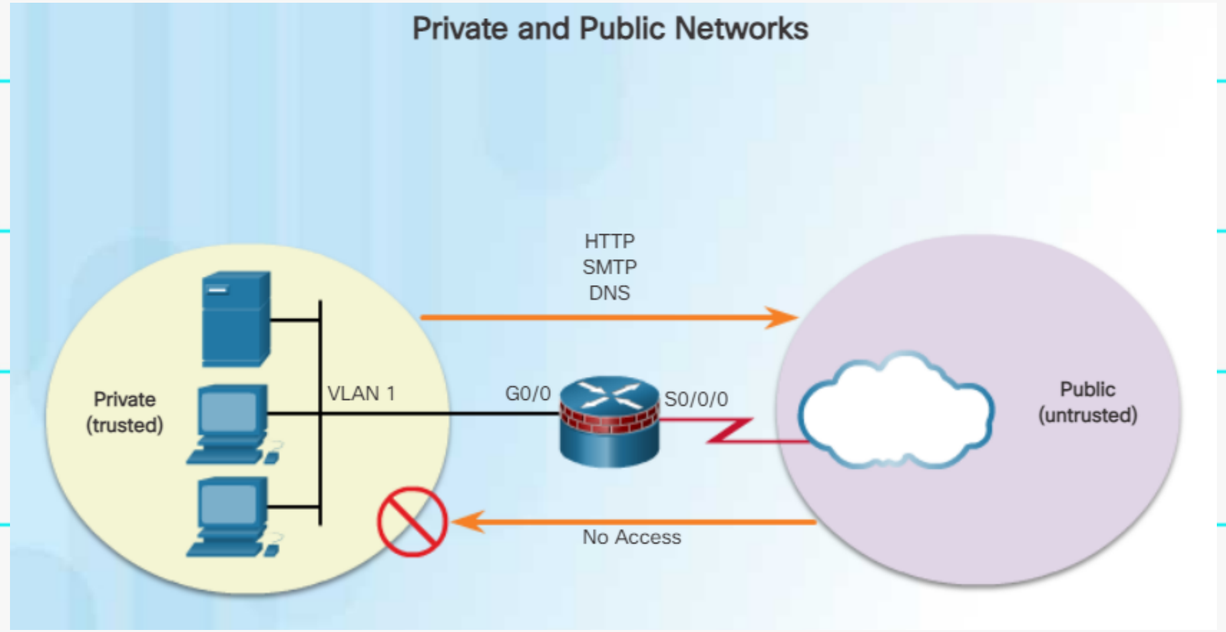
4.2.4.3 ZPFs

4.2.4.4 Layered Defense

4.2.4.1 Inside and Outside Networks



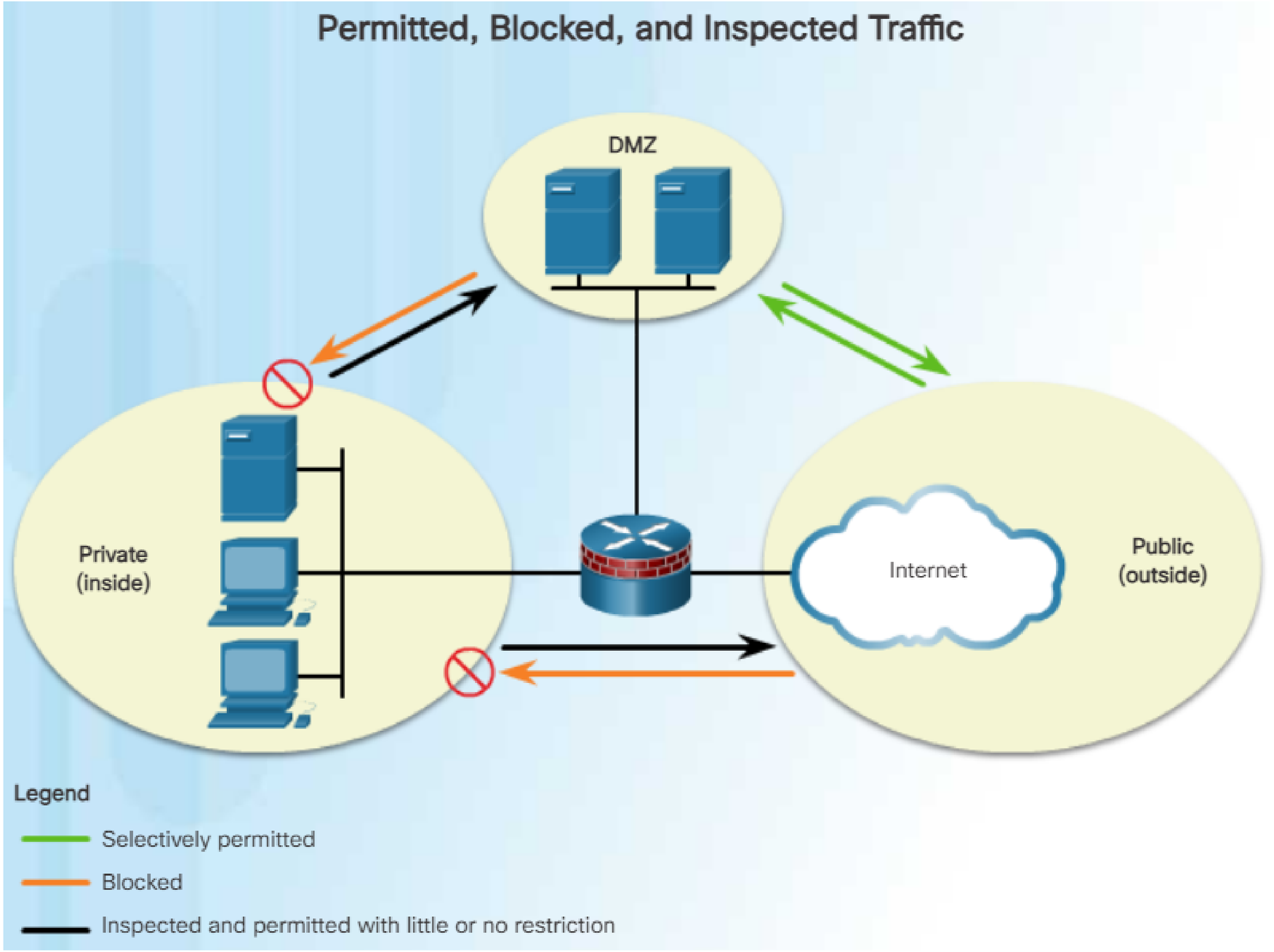
4.2.4.1 Inside and Outside Networks



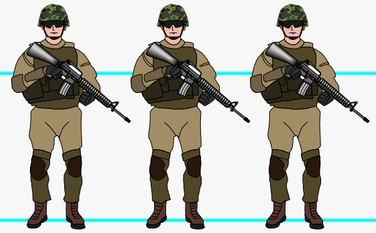
- Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.

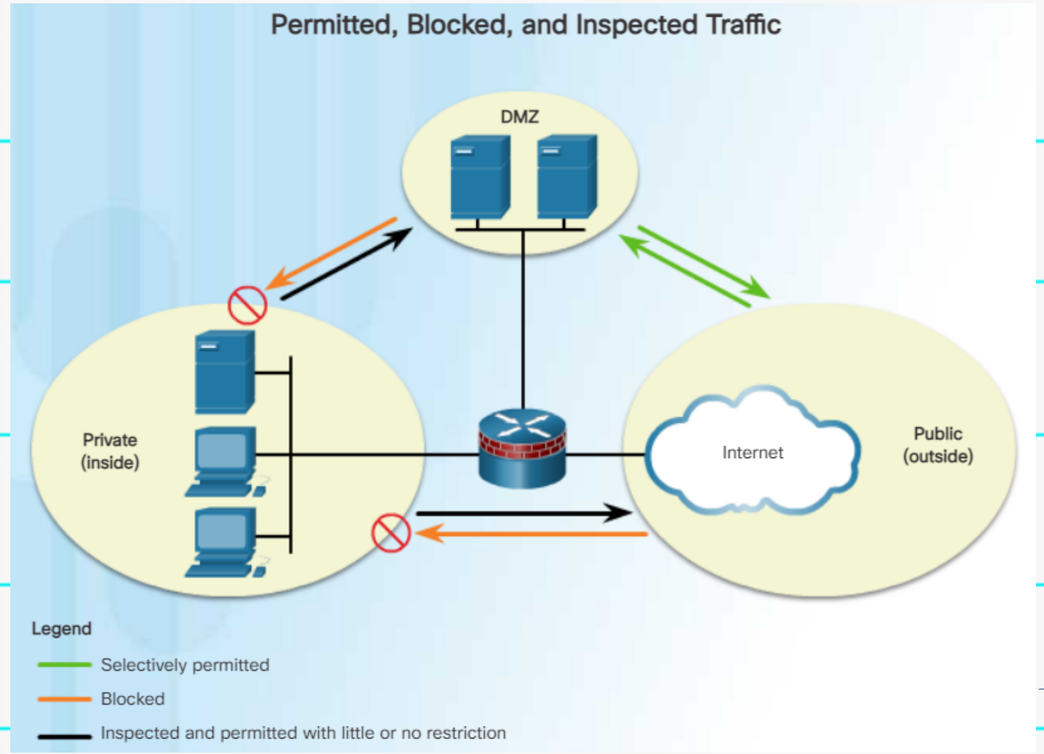
- Figure shown, the public network (or outside network) is untrusted, and the private network (or inside network) is trusted.

4.2.4.2 Demilitarized Zones



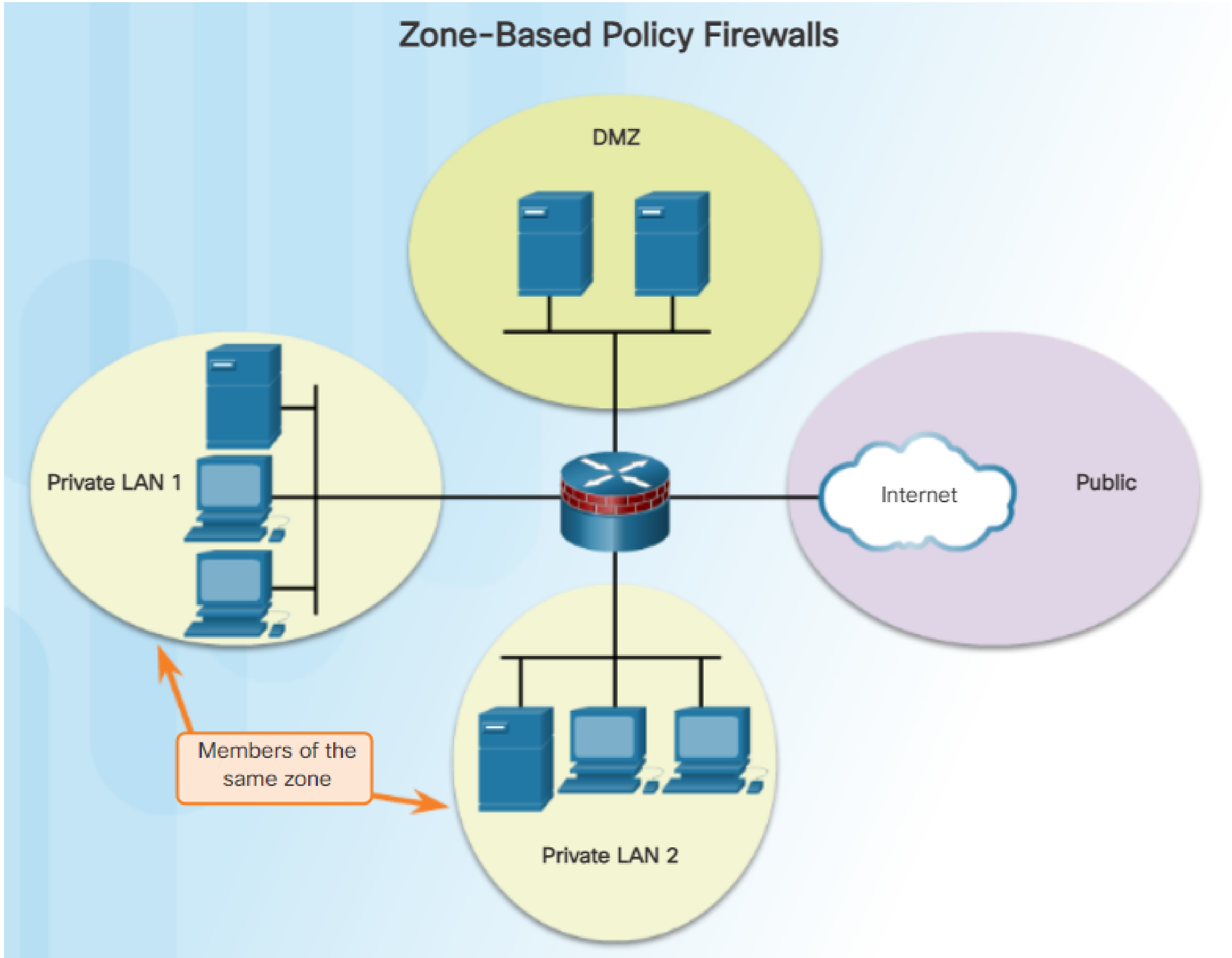
4.2.4.2 Demilitarized Zones



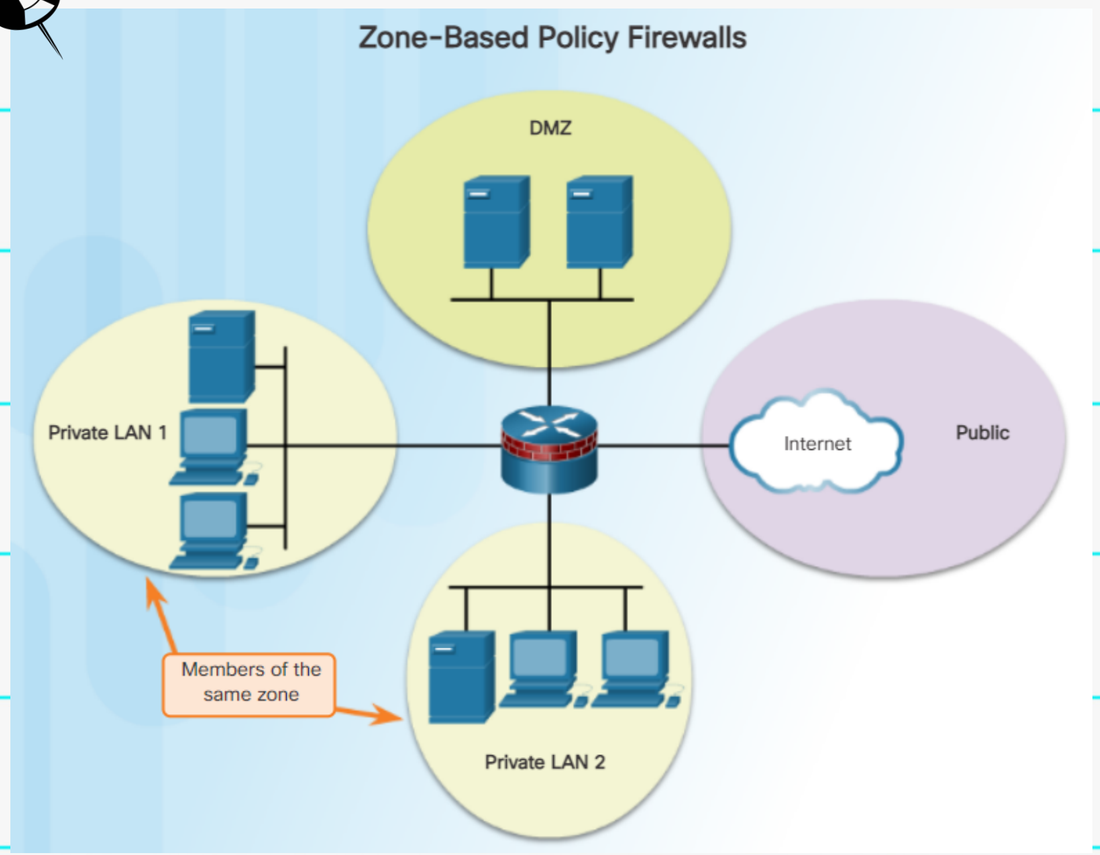


- Firewall designed where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface
- Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
- Type of traffic is typically email, DNS, HTTP, or HTTPS traffic. Return traffic from the DMZ to the public network is dynamically permitted.

4.2.4.3 Zone-based policy (ZPFs)



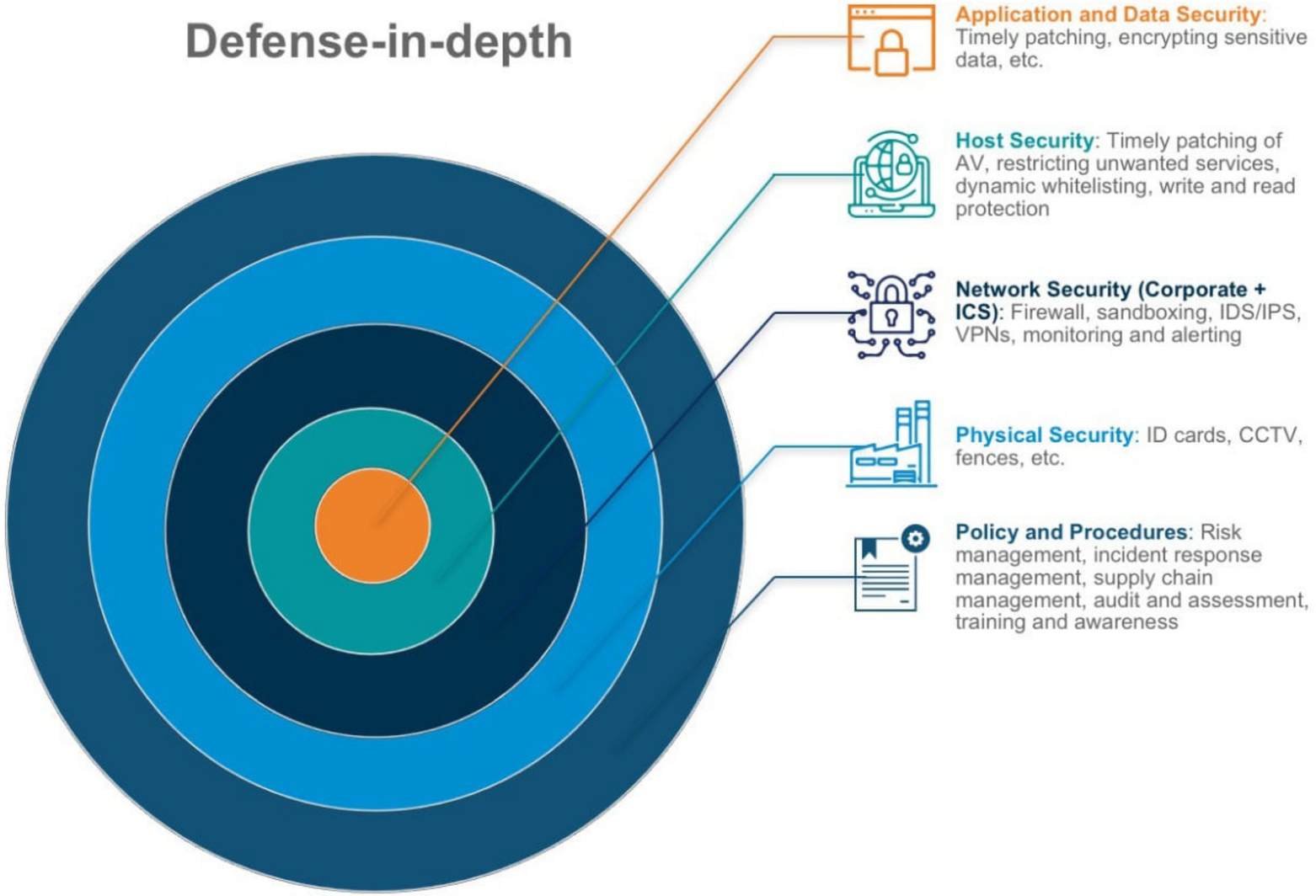
4.2.4.3 Zone-Based Policy (ZPFs)



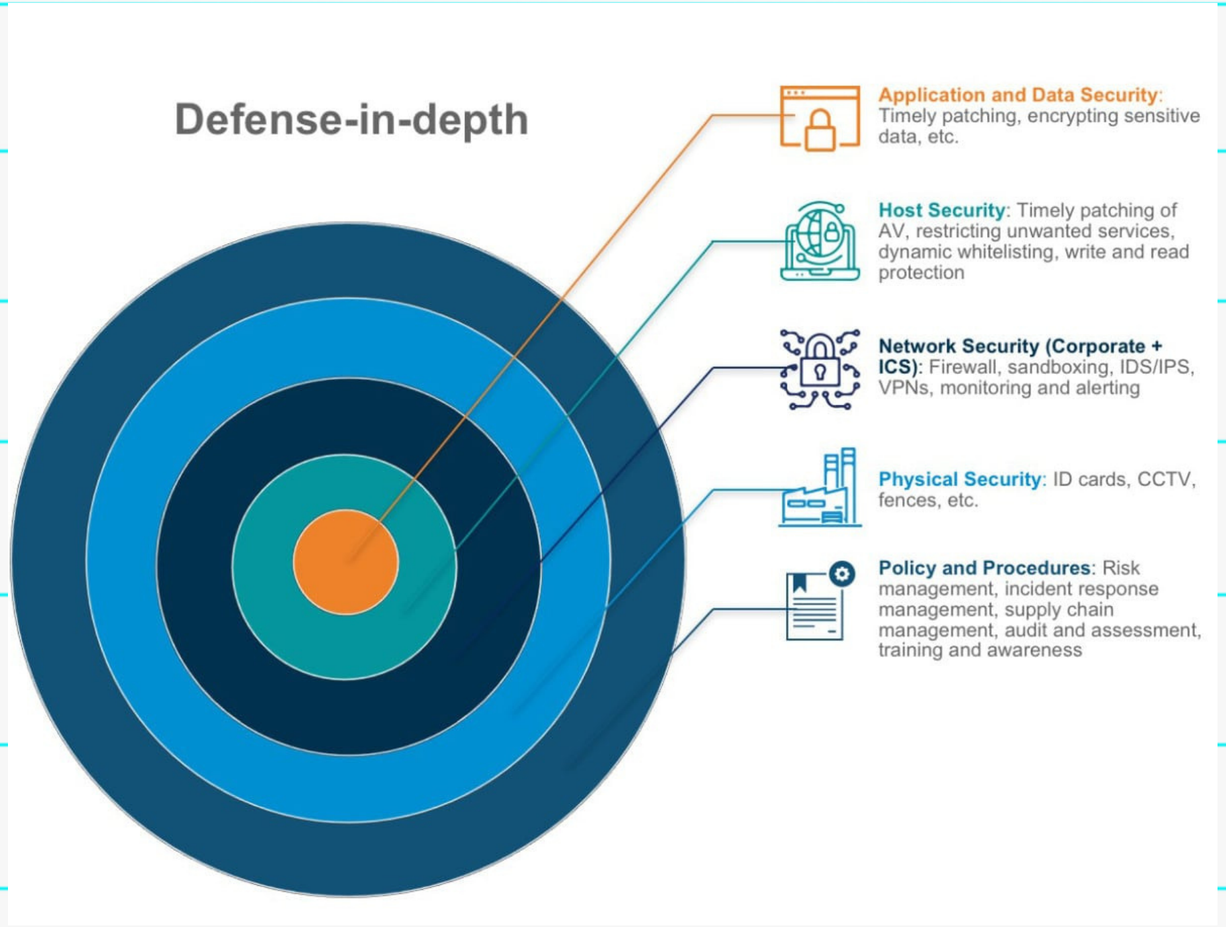
Use concept of zone.

- A group of one or more interfaces that have similar functions or features.
- By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. However, all zone-to-zone traffic is blocked.
- The only exception to this default deny any policy is the router self zone. The self zone is the router itself and includes all the router interface IP addresses.

4.2.4.4 LAYERED DEFENSE



4.2.4.4 LAYERED DEFENSE



- A layered defense uses different types of firewalls that are combined in layers to add depth to the security of an organization.

Factors when building a complete in-depth defense:

- Firewalls typically do not stop intrusions that come 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.

THANK YOU!

Get Ready For Quiz

Question 1

Which three layers of the OSI model include information that is commonly inspected by a stateful firewall?

Question 1 Answer

Layer 3, Layer 4, Layer 5

Question 2

Which type of firewall is supported by most routers and is the easiest to implement?

Question 2 Answer

Packet filtering firewall

Question 3

How does a firewall handle traffic that is originating from the DMZ network and traveling to a private network?

Question 3 Answer

Traffic is usually blocked when it is originating from the DMZ network and traveling to a private network.

Question 4

Packet filters are vulnerable to IP spoofing.

What do you think True or False?

Question 4 Answer

True because Hackers can send arbitrary packets that meet ACL criteria and pass through the filter.

THANK YOU!

From Group 6

Resource Page

Use these icons and illustrations in your Canva Presentation. Happy designing!