Implementing Secure Network Design

MNU-2025

Dr. Ahmed Samy

Lecture 04

Module Contents

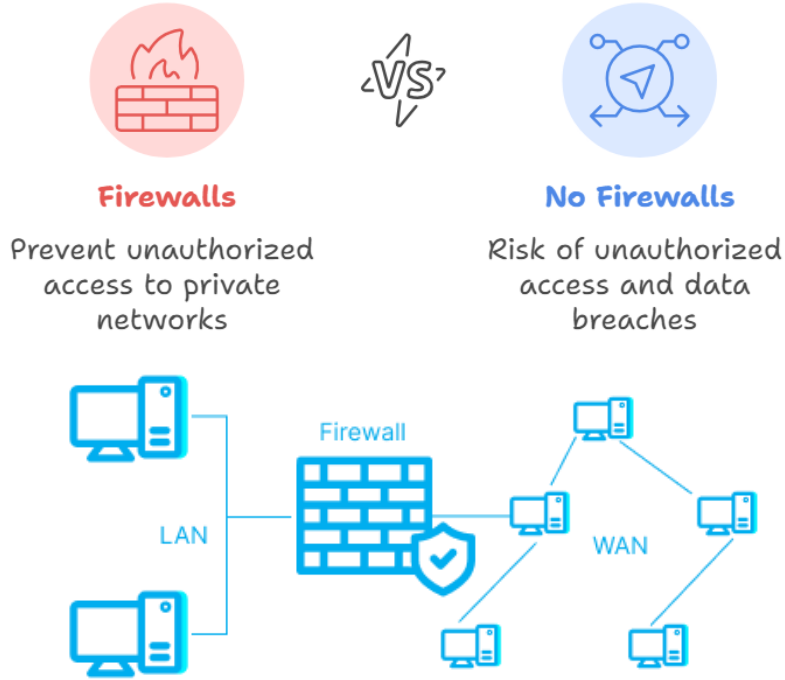
In this module, we will cover the below topics:

- TCP/IP and OSI Protocol Suites
- Network Devices
- Layer2 Attacks and Mitigation
- Layer3 Attacks and Mitigation
- Layer4 Attacks and Mitigation
- Firewall Technologies, IPS, and IDS

Firewall Technologies

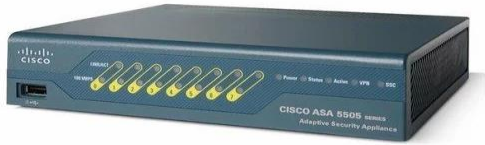
What is Firewall?

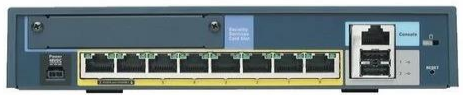
- Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on preconfigured security rules.
- Firewalls are often used to make sure internet users without access are not able to interface with private networks, or intranets, connected to the internet.
- Firewall is positioned between a network or a computer and a different network, like the internet.

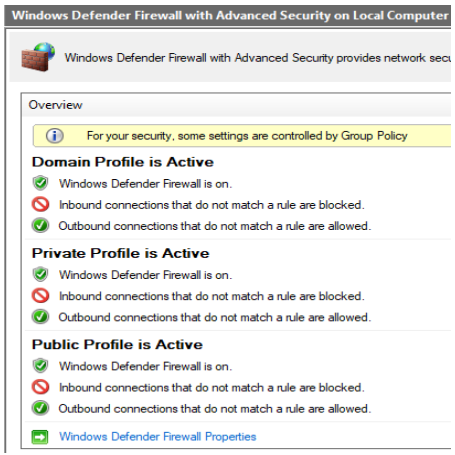


What is Firewall?

- Firewalls come in both hardware and software forms.
- A hardware firewall is a standalone physical device that sits between your network and the internet like CISCO, Fortinet, and PaloAlto firewalls.
- A software firewall is a program installed on individual devices (e.g., computers, smartphones, or servers) like Windows Defender Firewall and Norton Firewall.
- The hardware firewall protects the entire network where the software firewall protects only the device on which it is installed.

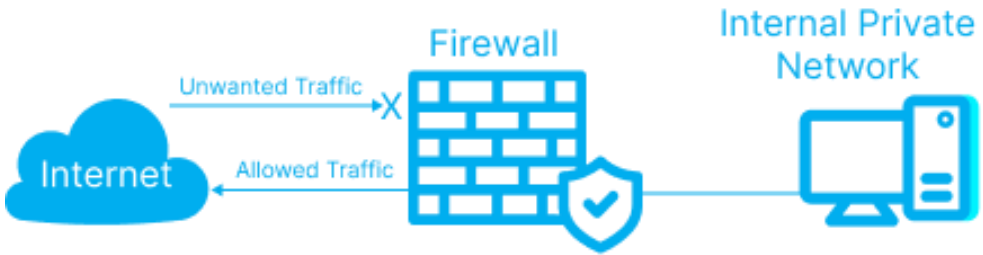






How do Firewalls work?

- A firewall system examines network traffic in accordance with predefined rules. It then filters the traffic and prevents it from coming from untrustworthy or suspicious sources.
- It only accepts incoming traffic that has been configured to accept it



How do Firewalls work?

1. **Identification of the Data Packets:** when a data packet is sent or received on a network, the firewall examines the packet to determine its source, destination, protocol, port, and other information.

2. **Comparison with Predefined Rules:** the firewall compares it against a set of predefined rules. These rules can be based on the type of traffic, the source of the traffic, the destination of the traffic, or the content of the traffic.

3. **Allow or Block Decision:** the firewall decides whether to allow or block the data packet. If the data packet matches the rule, it is allowed to pass, and if it does not match the rule, it is blocked. All firewalls have an implicit deny policy which block all traffic that not match with any rule.

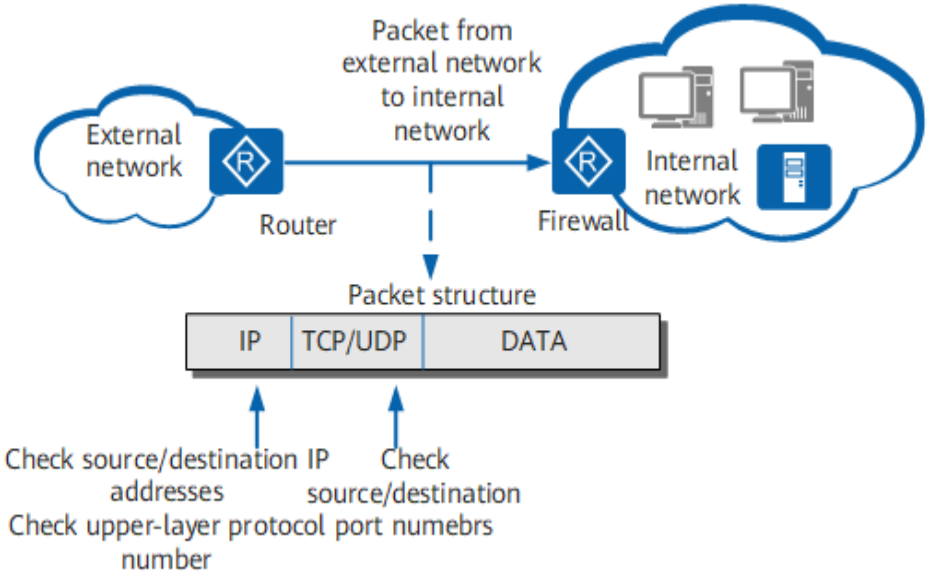
4. **Logging and Alerting:** If a data packet is blocked by the firewall, the firewall can log the event and alert the network administrator to investigate the event and take appropriate action.

Types of Network Firewall

1. **Packet-Filtering Firewalls (Traditional)**

- They operate at the network layer (Layer 3) of the OSI model, examining each incoming or outgoing packet and comparing it to a set of predefined rules. These rules can specify the IP address, port number, protocol, or other attributes of the packet.

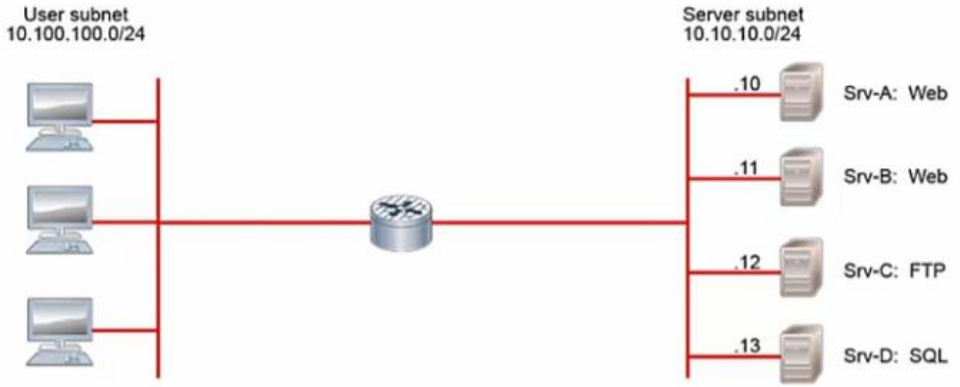
- They are simple and efficient but they can be vulnerable to attacks like IP spoofing attacks.



Types of Network Firewall

1. **Packet-Filtering Firewalls (Traditional)**

- What is the firewall action if source IP 10.100.100.100 is trying to connect to 10.10.10.11 on port 22?
- Traffic will be dropped.
- What is the firewall action if source IP 10.100.100.100 is trying to connect to 10.10.10.10 on port 80?
- Traffic will be allowed.




```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
access-list 100 deny ip any any log
```

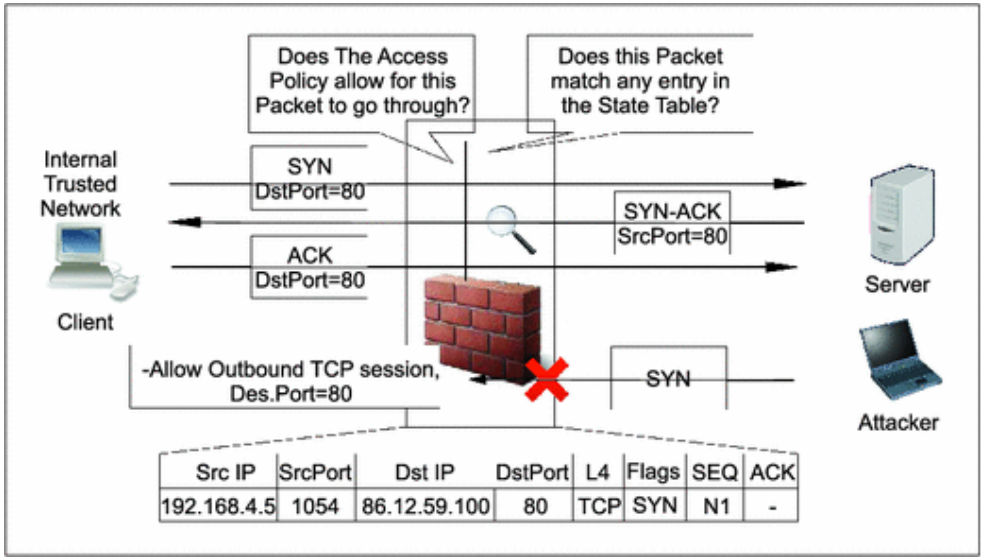
Types of Network Firewall

2. Stateful Inspection Firewalls

- Stateful firewalls maintain a state table that records information about ongoing network connections. When a packet arrives at the firewall, it is checked against the state table to determine if it belongs to an established connection.

- The state table stores details about each connection including:

  1. Source and destination IP addresses
  2. Port numbers
  3. Sequence numbers
  4. Relevant information

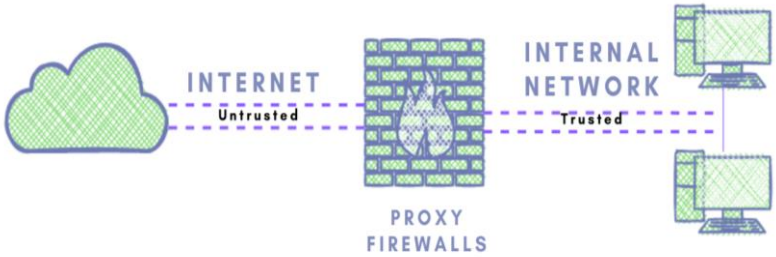


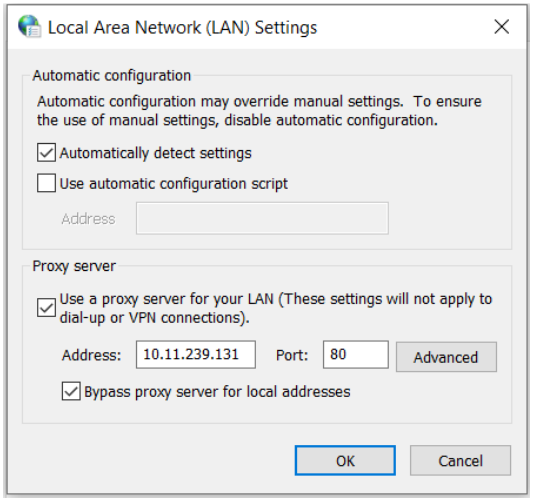
Types of Network Firewall

3. Proxy Firewall

- Operate at the application layer (Layer 7) of the OSI model, acting as intermediaries between clients and servers. They intercept all traffic between the client and server, examining it and filtering out any malicious or unauthorized traffic.

- If internal network devices want to access the internet, they must first interact with the proxy gateway. It hides IP addresses of all internal network.

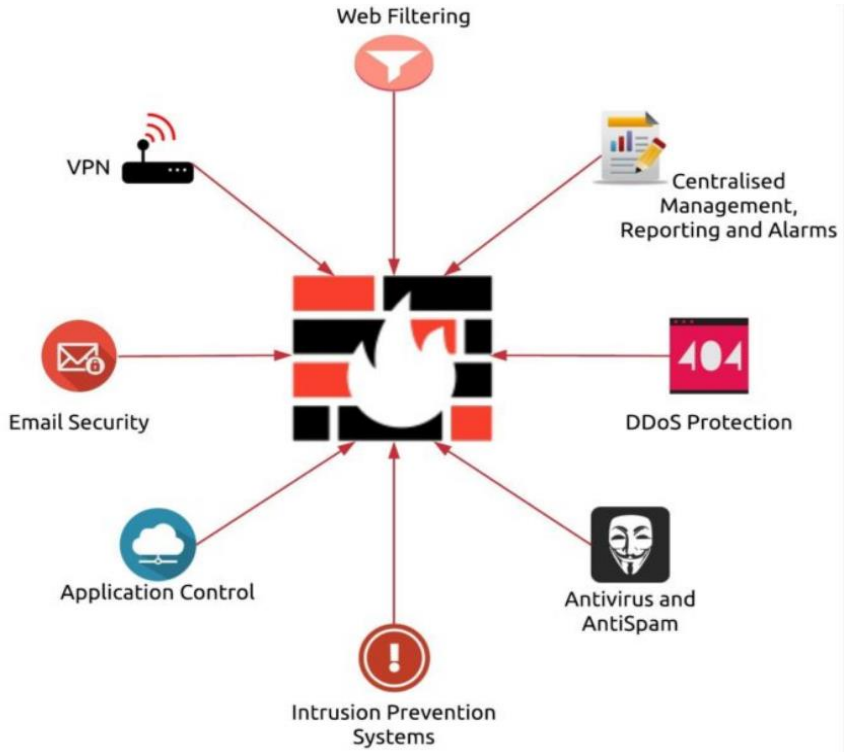




Types of Network Firewall

4. Next-Generation Firewalls (NGFW)

- NGFWs are enhanced versions of standard firewalls that include features such as in-line deep packet inspection, intrusion detection, application control, URL filtering, and more.
- They not only identify but also completely block malicious packets before they enter your network.



Firewalls and Security Zones

- Security zones are logical or physical segments of a network or interfaces that group devices and resources based on their security requirements.

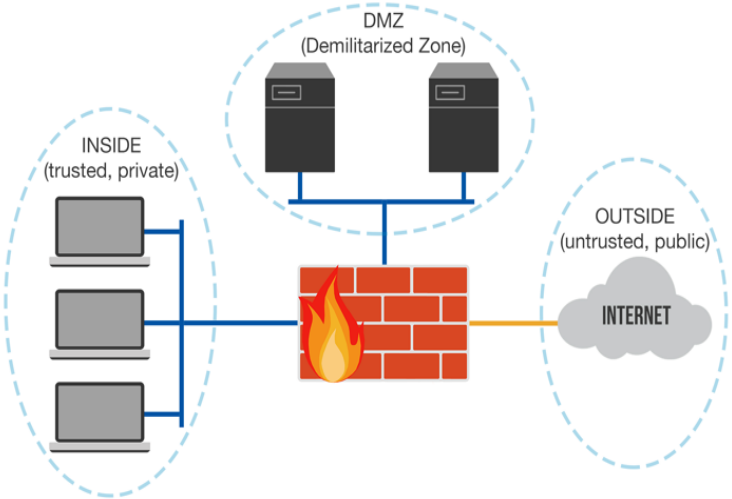
- **Common Security Zones**

➢ **Untrusted Zone (External Zone):** considered highly risky; all traffic from this zone is treated as potentially malicious.

➢ **DMZ (Demilitarized Zone):** a semi-trusted zone that hosts publicly accessible services like web servers, email servers, or DNS servers.

➢ **Trusted Zone (Internal Zone):** Includes internal networks, traffic within this zone is considered safe.

➢ **Guest Zone**: Provides limited access to external users (e.g., visitors or contractors).



Firewall Policy

- A firewall policy is a set of rules that control network traffic, determining which traffic is allowed or blocked.
- **Key Components:**

1. Source and Destination IP
2. Source and Destination Interfaces or Zones
3. Services/Protocols
4. Action (Allow/Deny)
5. Schedule
6. Logging
7. NAT
8. Security Profile Inspection

From 1-5 are mandatory, and from 6-8 are optional.

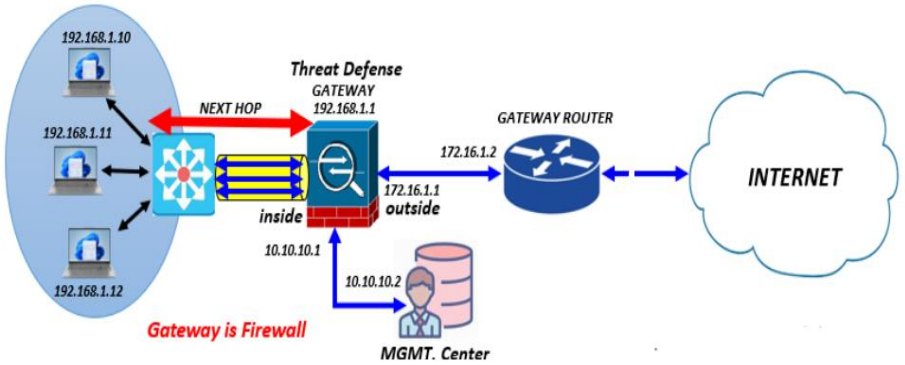
```
config firewall policy
    edit 1  # Policy ID (unique identifier)
        set name "Allow Web Traffic"
        set srcintf "port1"  # Source interface (e.g., internal network)
        set dstintf "wan1"  # Destination interface (e.g., internet)
        set srcaddr "internal_subnet" # Source address object
        set dstaddr "all" # Destination address object
        set action accept
        set schedule "always"
        set service "HTTP" "HTTPS"  # Allowed services
        set logtraffic all # log all traffic matching this rule
        set nat enable # Enable NAT
    next
```

```
config firewall address
    edit "internal_subnet"
        set subnet 192.168.1.0 255.255.255.0
    next
    edit "server_IP"
        set ipmask 203.0.113.1 255.255.255.255
    next
end
```

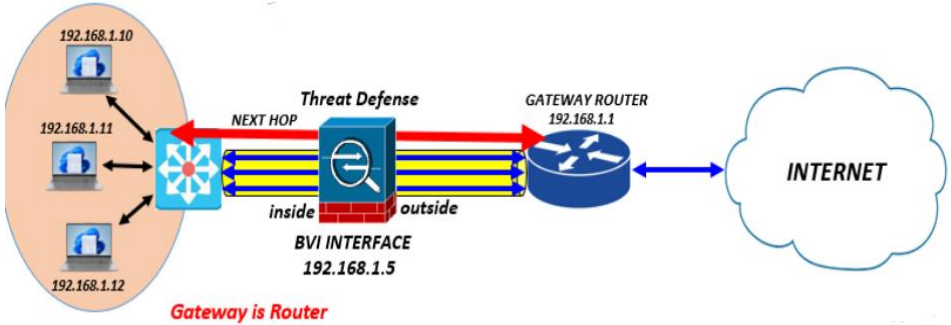
```
set security policies from-zone trust to-zone untrust policy allow-web match source-address any
set security policies from-zone trust to-zone untrust policy allow-web match destination-address any
set security policies from-zone trust to-zone untrust policy allow-web match application junos-http junos-https
set security policies from-zone trust to-zone untrust policy allow-web then permit
```

Modes of Deployment

1. Routed Mode

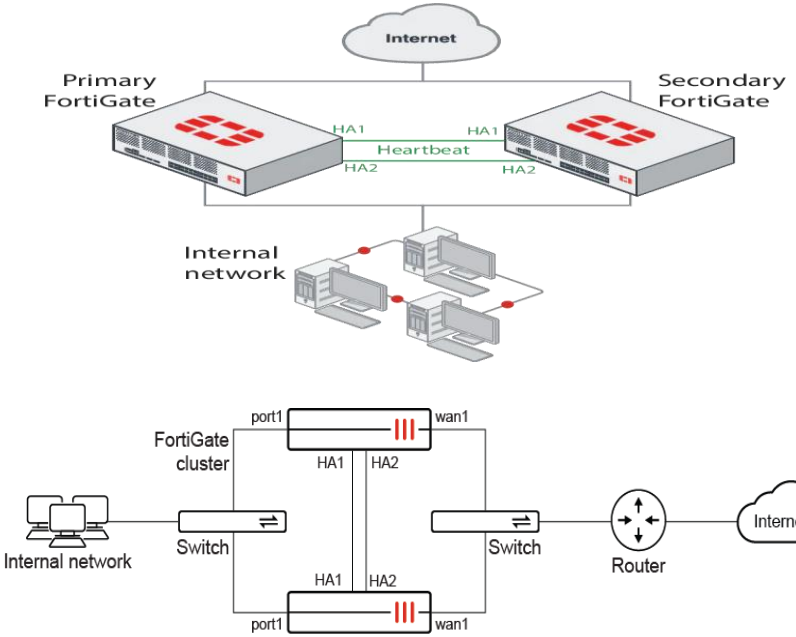


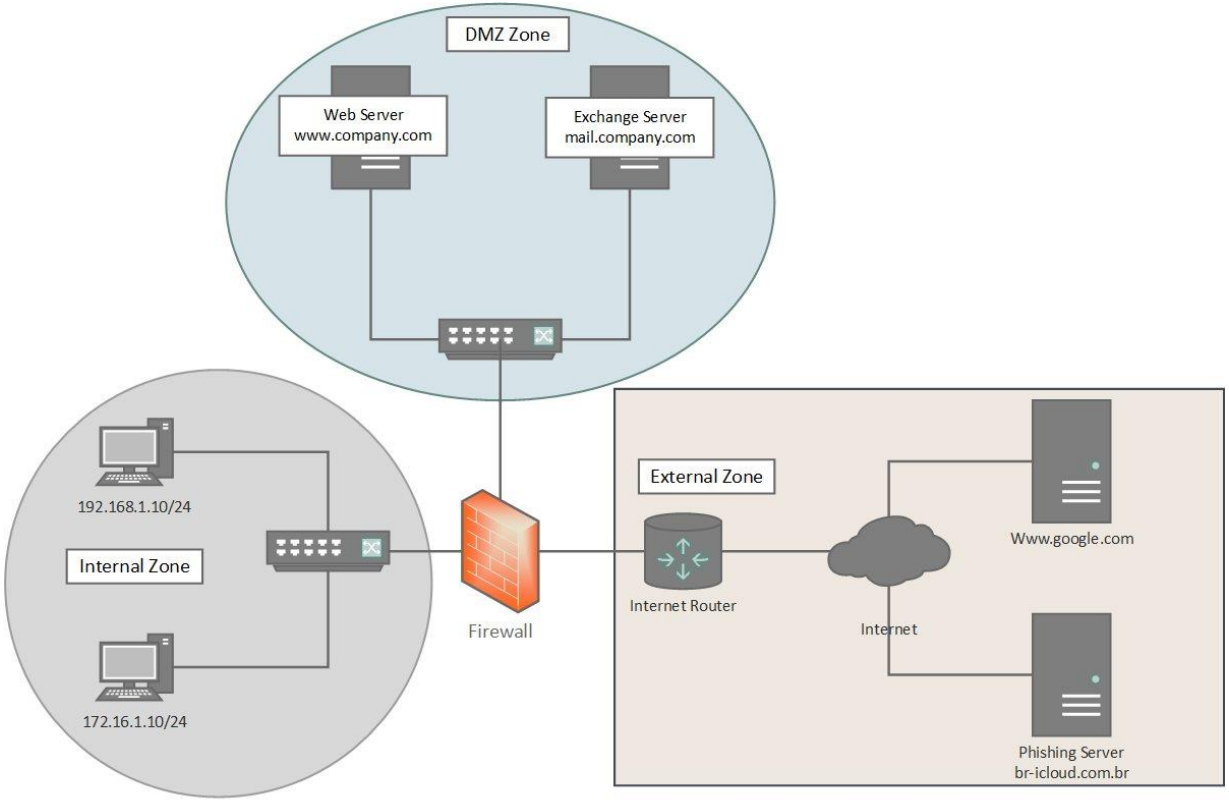
2. Transparent Mode

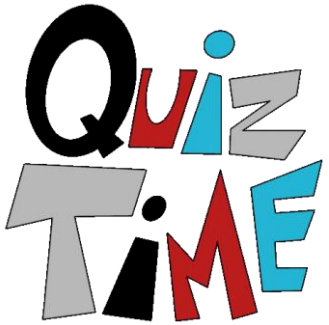


High Availability

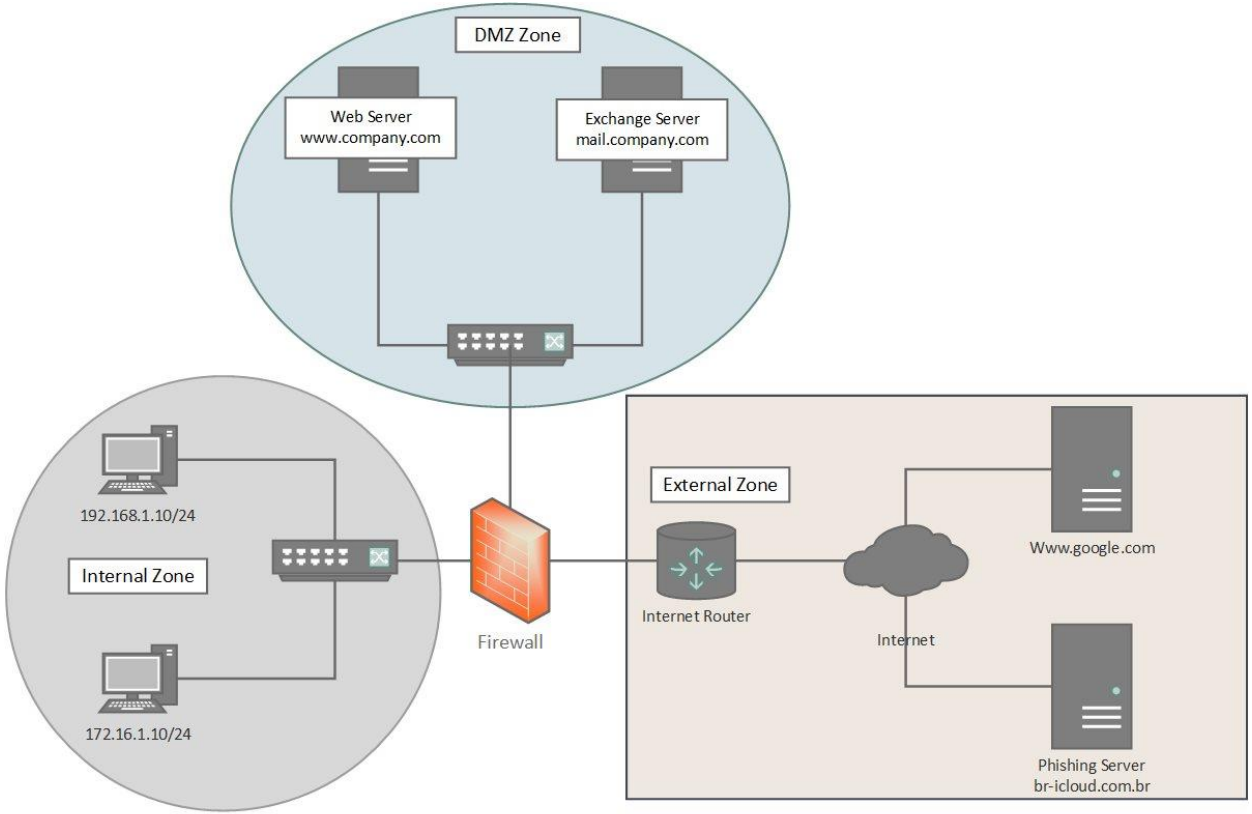
- High Availability (HA) refers to a setup where two or more firewalls work together to ensure uninterrupted network security.
- HA configurations are designed to provide redundancy and failover capabilities, ensuring that if one firewall fails, another can take over seamlessly.
- **Active-Passive Mode:** The primary firewall handles all traffic, while the secondary firewall remains on standby. If the primary fails, the secondary takes over.
- **Active-Active Mode:** Both firewalls actively handle traffic, sharing the load. If one fails, the other takes over the full load.

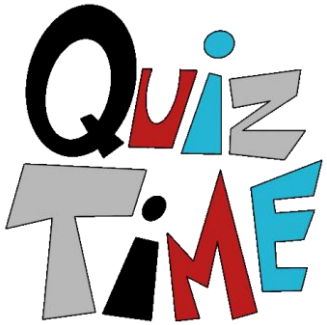







```
set security policies from-zone Internal to-zone External policy allow-web match source-address 192.168.1.0/24
set security policies from-zone Internal to-zone External policy allow-web match destination-address any
set security policies from-zone Internal to-zone External policy allow-web match application https
set security policies from-zone Internal to-zone External policy allow-web then permit
```



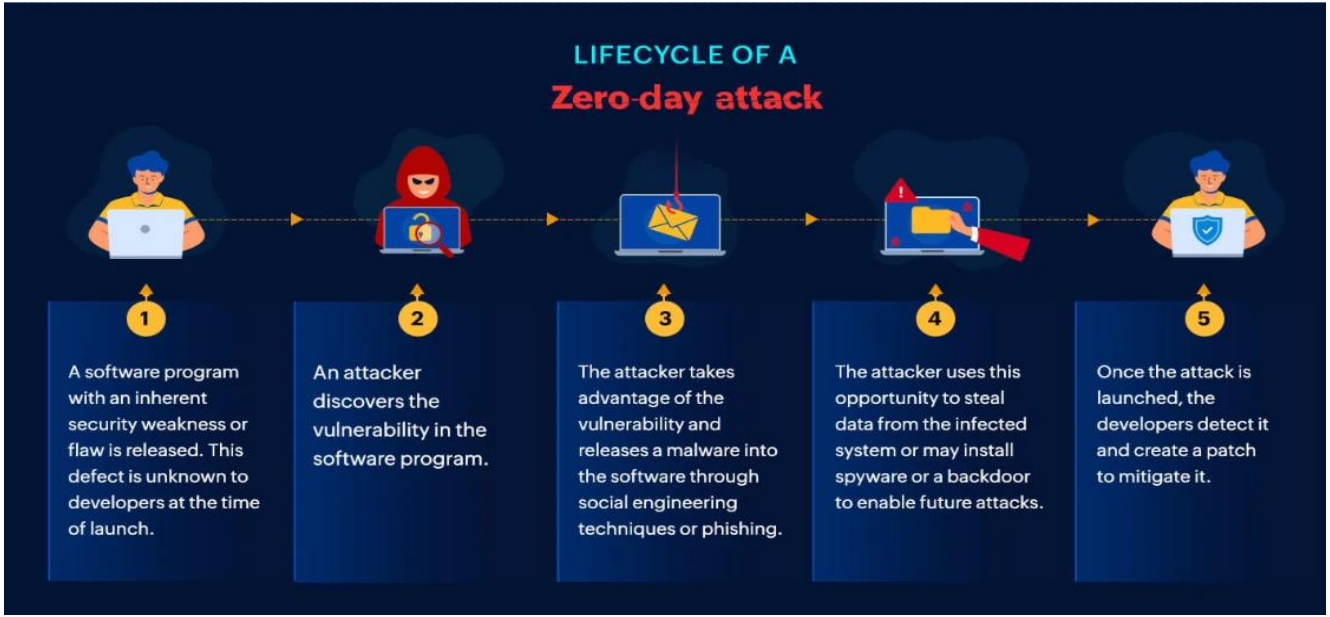



```
set security policies from-zone Internal to-zone External policy allow-web match source-address 172.16.1.0/24
set security policies from-zone Internal to-zone External policy allow-web match destination-address any
set security policies from-zone Internal to-zone External policy allow-web match application smtp
set security policies from-zone Internal to-zone External policy allow-web then permit
```

IPS and IDS

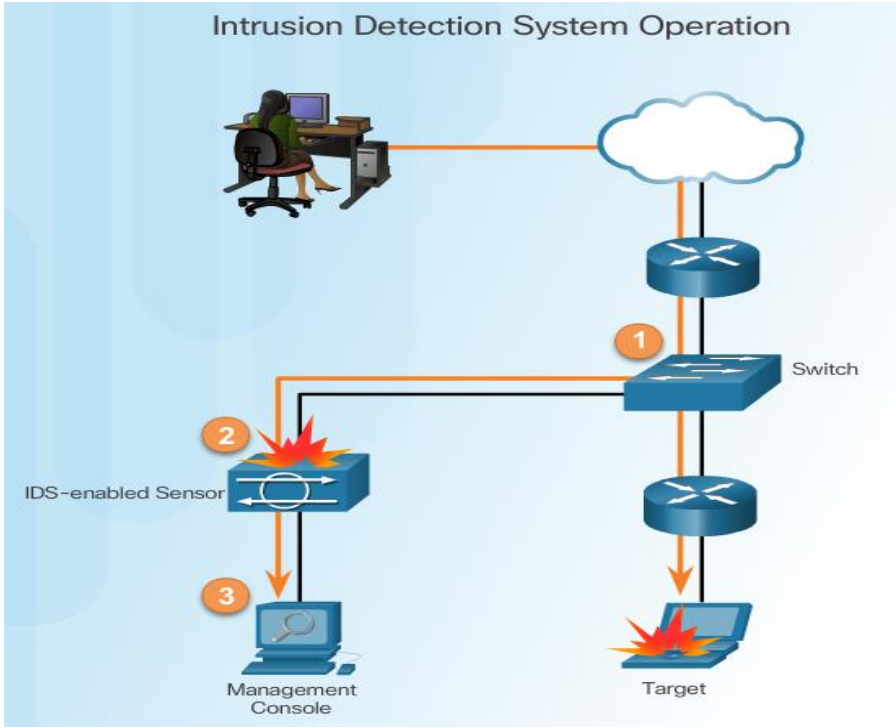
Zero Day Exploits

- The term "Zero Day" refers to the fact that developers have zero days to fix the flaw before attackers can take advantage of it. These exploits are particularly dangerous because they occur before security patches or updates are available, leaving systems exposed to potential breaches.



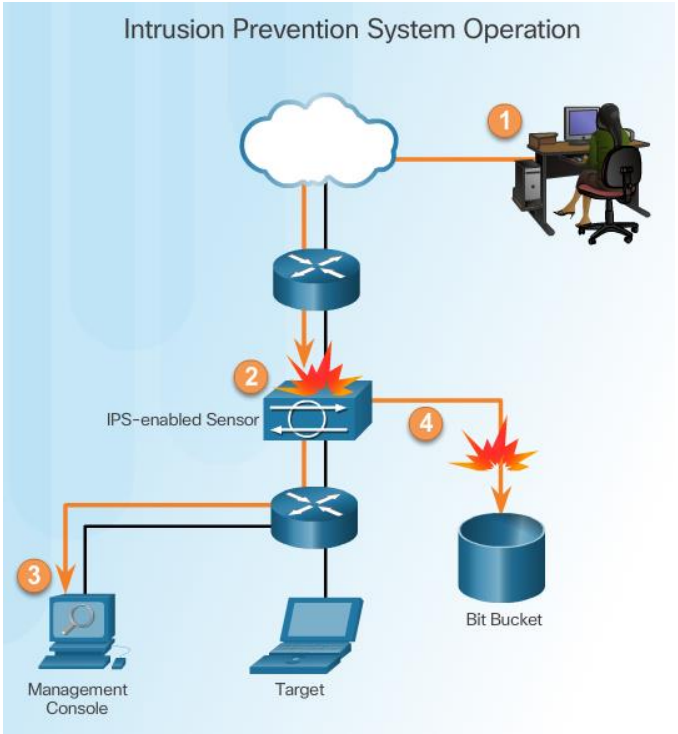
Monitor for Attacks

- Advantages of an Intrusion Detection System (IDS):
  - Works passively
  - Requires traffic to be mirrored in order to reach it
  - Network traffic does not pass through the IDS unless it is mirrored

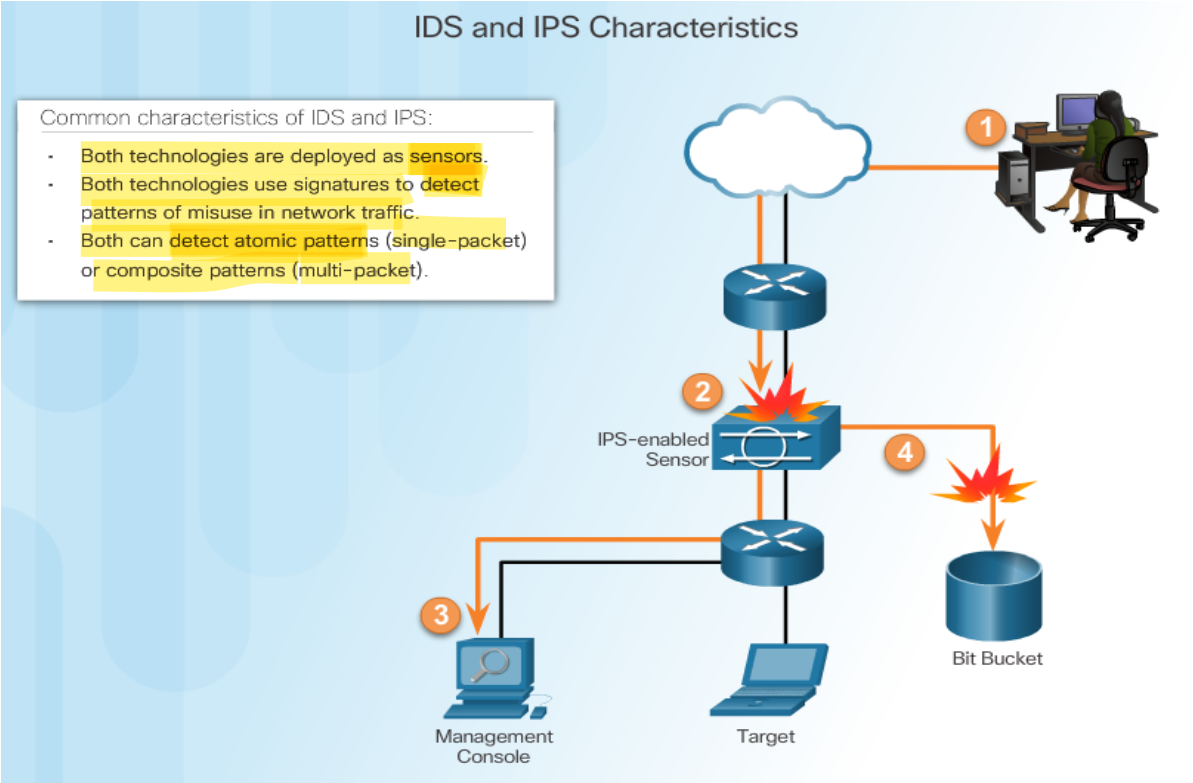


Detect and Stop Attacks

- Advantages of an Intrusion Prevention System (IPS):
  - Implemented in an inline mode
  - Monitors Layer 3 and Layer 4 traffic
  - Can stop single packet attacks from reaching target
  - Responds immediately, not allowing any malicious traffic to pass



Similarities Between IDS and IPS



Advantages and Disadvantages of IDS and IPS

- **Advantages**

IDS	IPS
Provides valuable insights into network traffic and potential security breaches.	Automatically blocks malicious traffic, preventing attacks from causing damage.
Because it doesn't actively block traffic, there's less risk of disrupting legitimate network activity due to false positives.	Reduces the need for manual intervention, enabling faster response times.
Logs and reports generated by IDS can be crucial for post-incident analysis.	Significantly enhances network security by stopping threats before they penetrate the network.

Advantages and Disadvantages of IDS and IPS

- **Disadvantages**

IDS	IPS
IDS only detects threats; it doesn't prevent them.	Analyzing and blocking traffic can introduce latency and impact network performance.
Can generate a high volume of alerts, some of which may be false positives	Incorrectly blocking legitimate traffic can disrupt critical business operations.
	Requires careful configuration and tuning to minimize false positives and maintain optimal performance

IPS Detection Methods

1. **Signature-Based Detection:**

- This method relies on a database of known attack patterns, or "signatures." The IPS compares network traffic against these signatures. If a match is found, the IPS takes action to block the traffic.
- Strengths: Highly effective for detecting known threats. Relatively low false positive rate.
- Weaknesses: Ineffective against new or unknown threats (zero-day attacks). Requires constant signature database updates.

2. **Anomaly-Based Detection:**

- This method establishes a baseline of "normal" network behavior. The IPS then monitors traffic for deviations from this baseline. Unusual activity is flagged as potentially malicious.
- Strengths: Can detect unknown threats and zero-day attacks. Adaptive to changing network conditions.
- Weaknesses: Higher false positive rate. Requires careful baseline configuration.

IPS Detection Methods

3. Policy-Based Detection:

- This method enforces security policies defined by network administrators. The IPS blocks any traffic that violates these policies
- Strengths: Highly customizable, enforces organizational security standards.
- Weaknesses: Requires significant upfront configuration, can be difficult to maintain.

4. Reputation-Based Detection:

- This method relies on databases that compile information about the trustworthiness of various network entities. These databases are often provided by threat intelligence vendors.
- These databases contain information about:
  1. Known malicious IP addresses (e.g., those associated with botnets or malware distribution).
  2. Domains known to host phishing websites or malware.
  3. Other indicators of compromise.

Thanks!

Do you have any questions?