Firewall

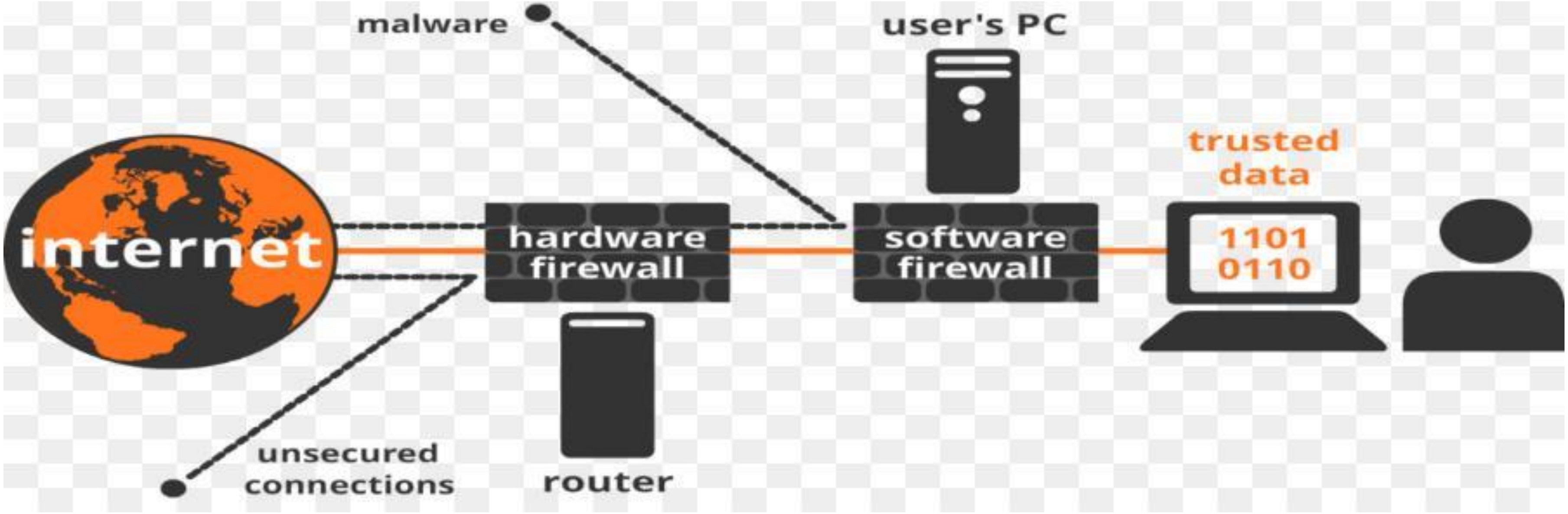
Cyber Security Foundation Course

AGENDA

- Definition
- Firewall types
- Software Firewall
- Packet-Filter Firewall (ACL)
- Stateful firewall
- Firewall zones
- Firewall topology

Firewall Definition

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.(Wikipedia)



Firewall Types

- **Software Firewall** (will be Covered today)
- **Packet-filtering** firewalls (will be Covered today)
- **Stateful inspection** firewalls. (will be Covered today)
- **Application-level** gateways (a.k.a. **proxy, WAF**) (will Cover Later)
- **Next-gen firewalls**. (will Cover Later)

Software Firewall

A **Software Firewall** is a piece of software that is installed on the personal computer's systems in order to protect it from unauthorized access, monitors and controls incoming and outgoing network traffic.

Examples: Windows Firewall

Packet-filtering firewalls (1)

Also Known as Access Control List (ACL), is a layer 3 firewall System used to control network access by monitoring and controlling outgoing and incoming packets and allowing them to pass or Deny based on the source and destination IP addresses, protocols and ports.

Examples: Rules deployed on routers

```
ACTION-REJECT FROM-9.117.249.0/24 PORT-21
```

```
permit 0.0.0.0 in via rip from 198.41.11.1
```

Packet-filtering firewalls (2)

Advantages:

- **Very Fast to process.**
- **Low process.**
- **Easy Syntax.**

Limitations:

- **Hard to configure.**
- **Access decisions are based only on IP address and port numbers.**
- **Doesn’t track the sessions.**

Stateful firewall

is a layers 3 and 4 firewall System that individually tracks sessions of network connections to control network access by monitoring and controlling outgoing and incoming packets

How Stateful Firewall Works ?

Stateful Firewall depend on firewall's state table Concept to track the sessions, for TCP it will check the initial request for a connection (SYN) against its Rule, If permitted This will initiate an entry in the firewall's state table, If the destination host returns a packet (SYN-ACK) state table reflects this. For UDP it track state by only using the source and destination address and source and destination port numbers.

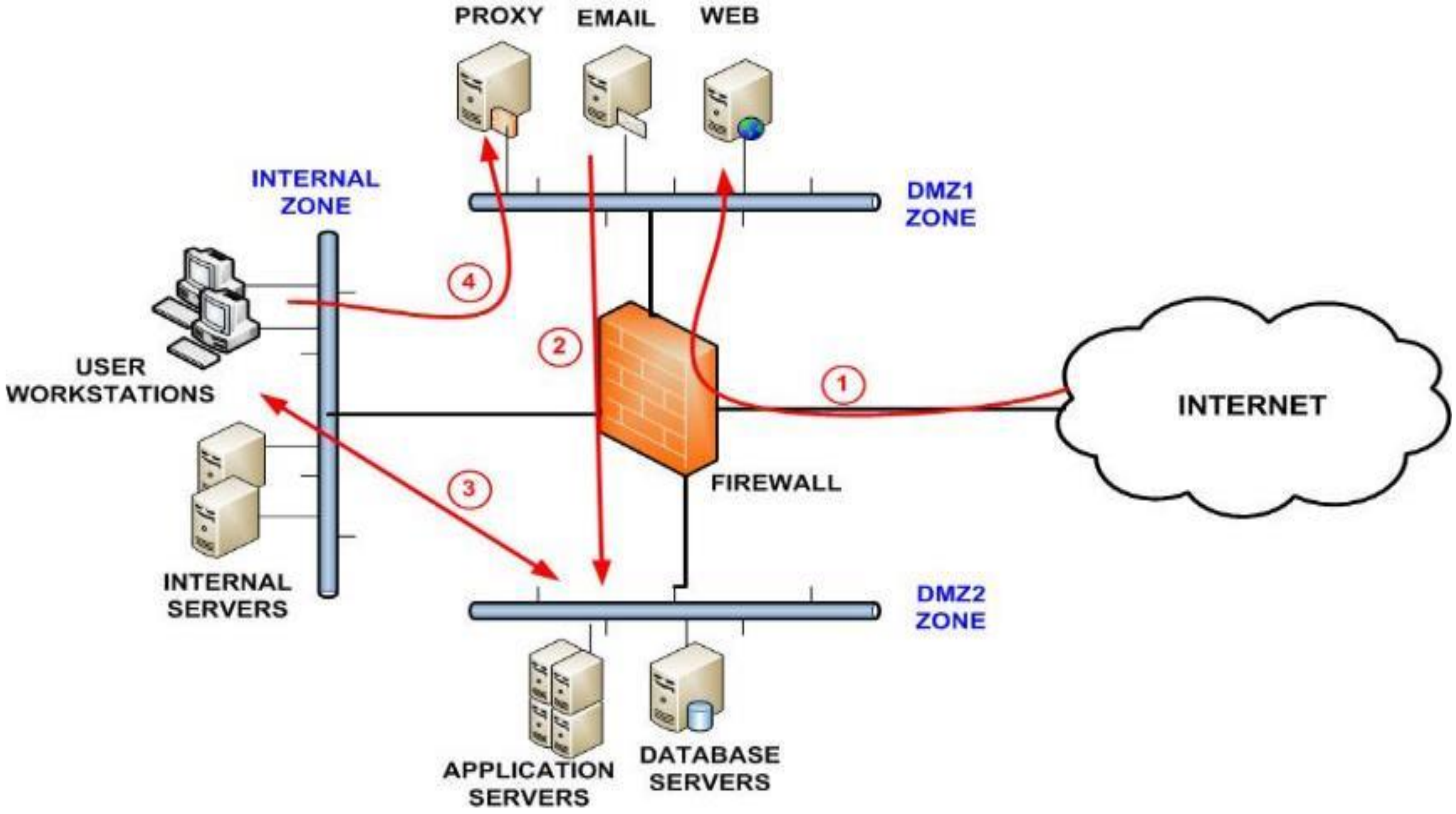
Firewall zones

Private (Internal) : trusted Zone that inside the Environment include Endpoint machines, internal servers

Public (Internet): Untrusted Zone include the Internet

Demilitarized Zone (DMZ): Zone that place Any service provided to users on the public internet. Some of the most common of these services include web servers ,email, and DNS

Firewall topology



Thanks!

Any questions?