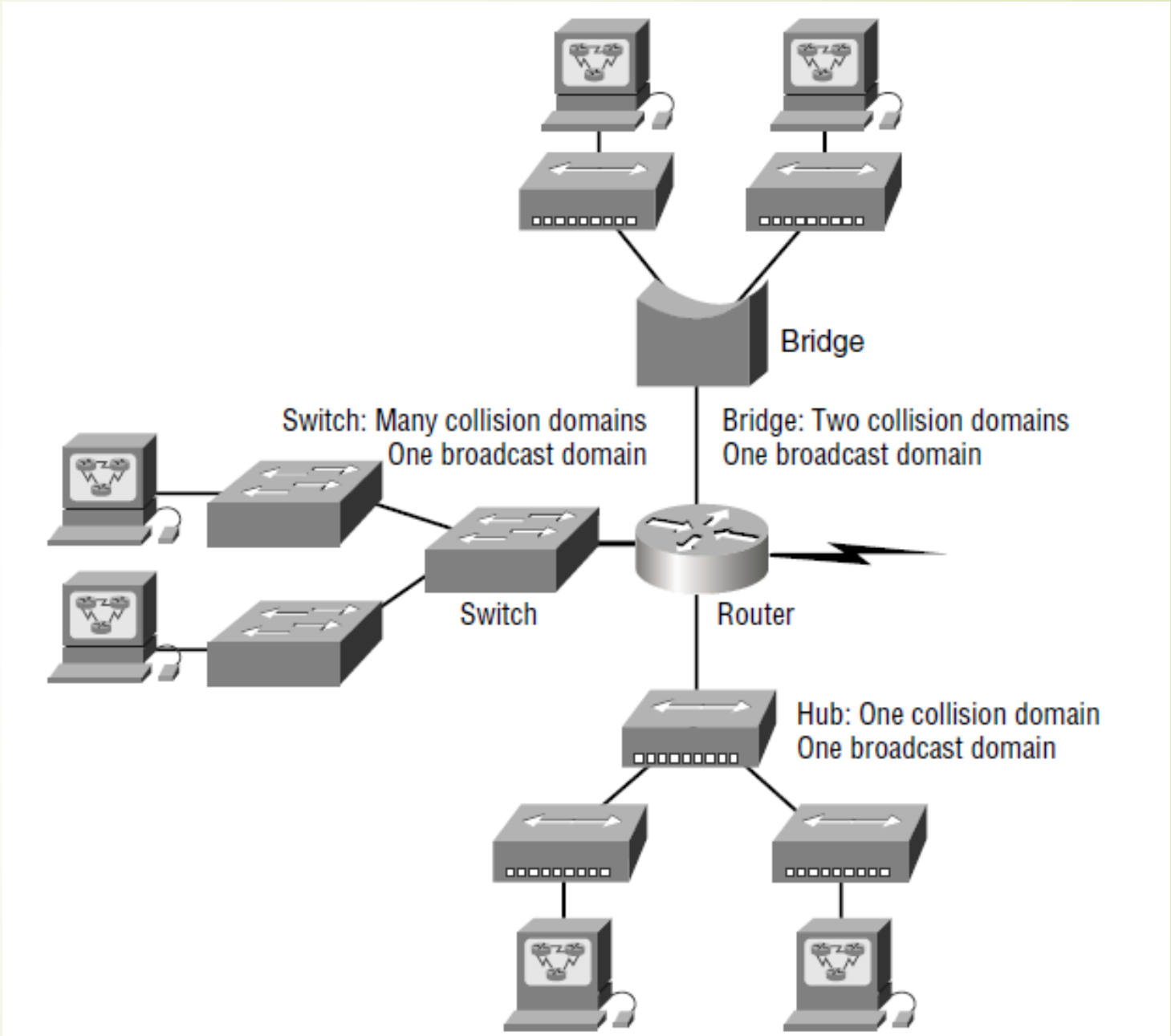
WAN Network Devices

Lecture 8

Agenda…

- WAN devices:
  1. Router
  2. Modem
  3. Firewall
  4. proxy
  5. Content filtering
  6. Packet shaper
  7. HIDS
  8. VPN concentrator

Networking Devices



Routing vs. Routed Protocols

- **Routed protocols**: Routed protocols (such as IP and IPX) are **used to transmit user data** through an internetwork.

- **Routing protocols**: Any protocol that defines algorithms to be used for **updating routing tables** between routers. Examples include IGRP, RIP, and OSPF. They **determine the path** of a packet through an internetwork.

Routing table

- A **data table** stored in a router that **lists the routes** to particular **network destinations**, and in some cases, **metrics** (distances) associated with those routes.
- Network destinations might be **directly** connected and **remote** networks is stored in the **RAM** of the router (volatile).

Routing type

1. **Static routing** : the network administrator manually adds routes in each router's routing table
2. **Dynamic routing**: when routing protocols are used to find and update routing tables on routers.
3. **Default routing**: used to send packets with a remote destination network not in the routing table to the next-hop router.

Static routing….con'd

Advantages:

- No overhead on the router CPU
- No bandwidth usage between routers
- Security (because the administrator only allows routing to certain networks)

Disadvantages:

- The administrator must really understand the internetwork and how each router is connected to configure the routes correctly.
- If one network is added to the internetwork, the administrator must add a route to it on all routers.
- It's not feasible in large networks because it would be a full-time job.

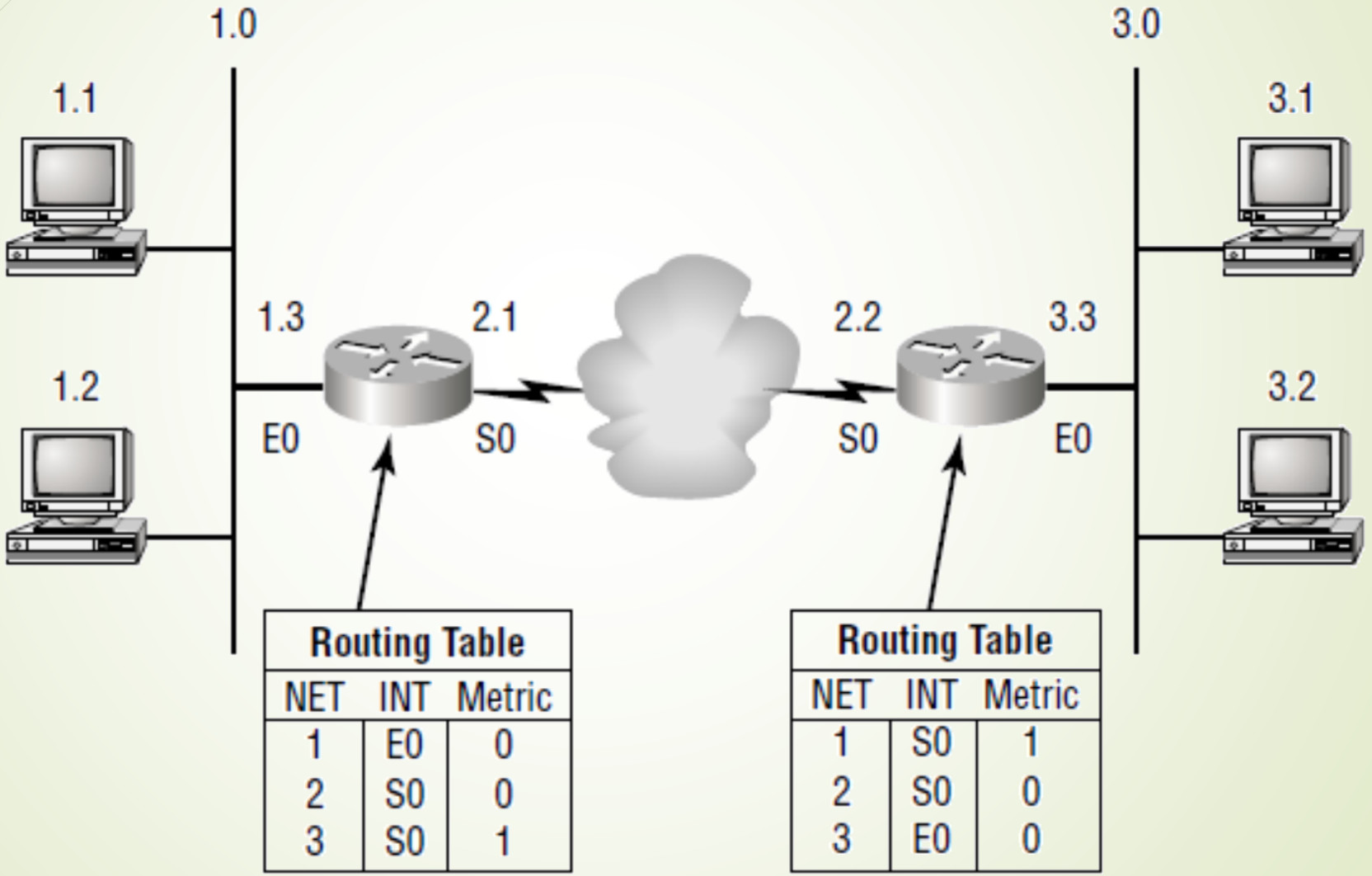
Routing protocols…1

- **Routing Information Protocol (RIP):**
  - It sends the **complete routing table** out to all active interfaces every 30 seconds.
  - only **uses hop count** to determine the best way to a remote network.
  - has a maximum allowable hop count of **15 by default**, meaning that 16 is deemed unreachable.
  - Works well in small networks, but it is inefficient on large networks.

Routing protocols…2

- **Open Shortest Path First(OSPF):**
  - Used to **find the best path** for packets as they pass through a set of connected networks
  - **link-state** routing protocol
  - **BW** of each link is used to calculate the **best cost** to a remote network.
  - When a **change** to a routing table occurs, the router immediately **multicasts** the information to **all other OSPF hosts** in the network so they will all have the same routing table information.

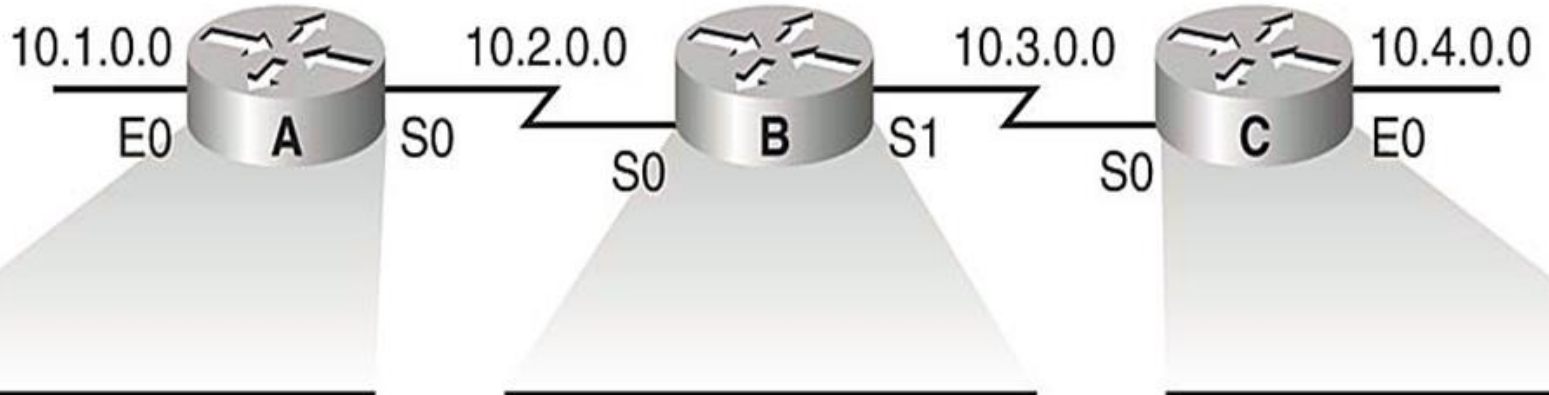
Routing tables



Routing Table		
NET	INT	Metric
1	E0	0
2	S0	0
3	S0	1

Routing Table		
NET	INT	Metric
1	S0	1
2	S0	0
3	E0	0

Another example:



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

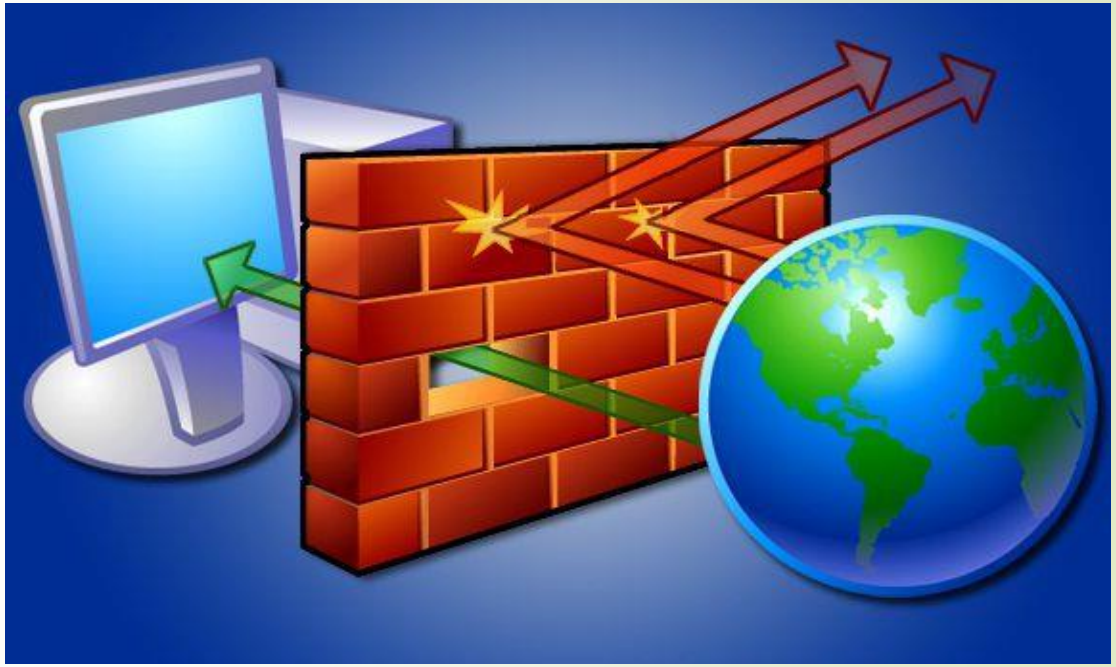
Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Things to keep in mind about routers

- Routers, by default, **will not** forward any broadcast or multicast packets.
- Routers use the **logical address** in a Network layer header to determine the next hop router to forward the packet to.
- Routers can use **access lists**, created by an administrator, to **control security** on the types of packets that are allowed to enter or exit an interface.
- Routers can provide **layer-2 bridging** functions **if needed** and can simultaneously route through the same interface.
- Provide **connections between (VLANs**) virtual LANs.
- Routers can provide quality of service (**QoS**) for specific types of network traffic.

Firewall

- 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** internal network and **untrusted** external network, such as the Internet.



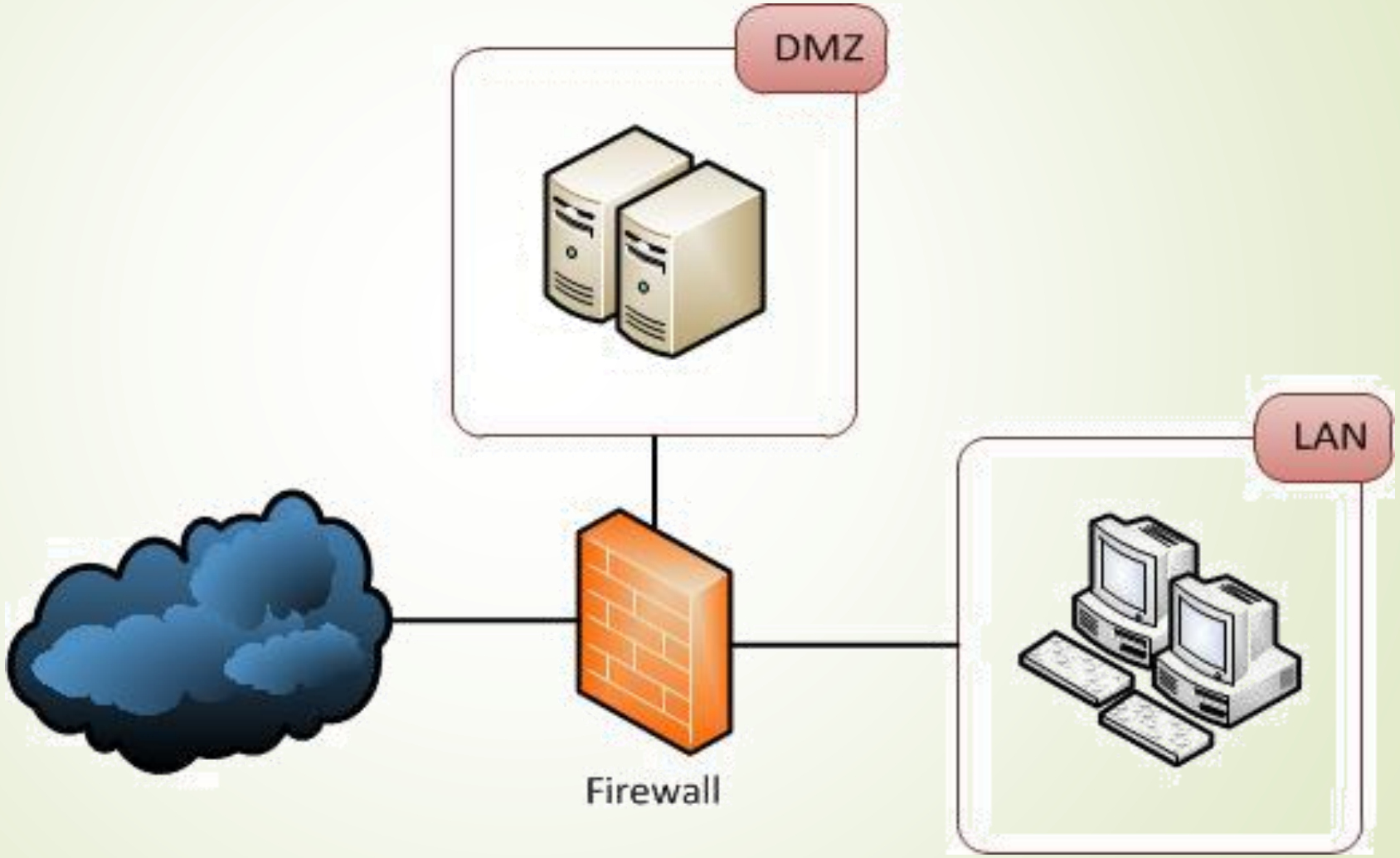
Firewall

- is a hardware or software system that **prevents unauthorized access** to or from a network
- Typical functions of traditional firewalls:
  - packet filtering
  - network- and port-address translation (NAT)
  - stateful inspection (keeps track of the state of network connections).
  - virtual private network (VPN) support

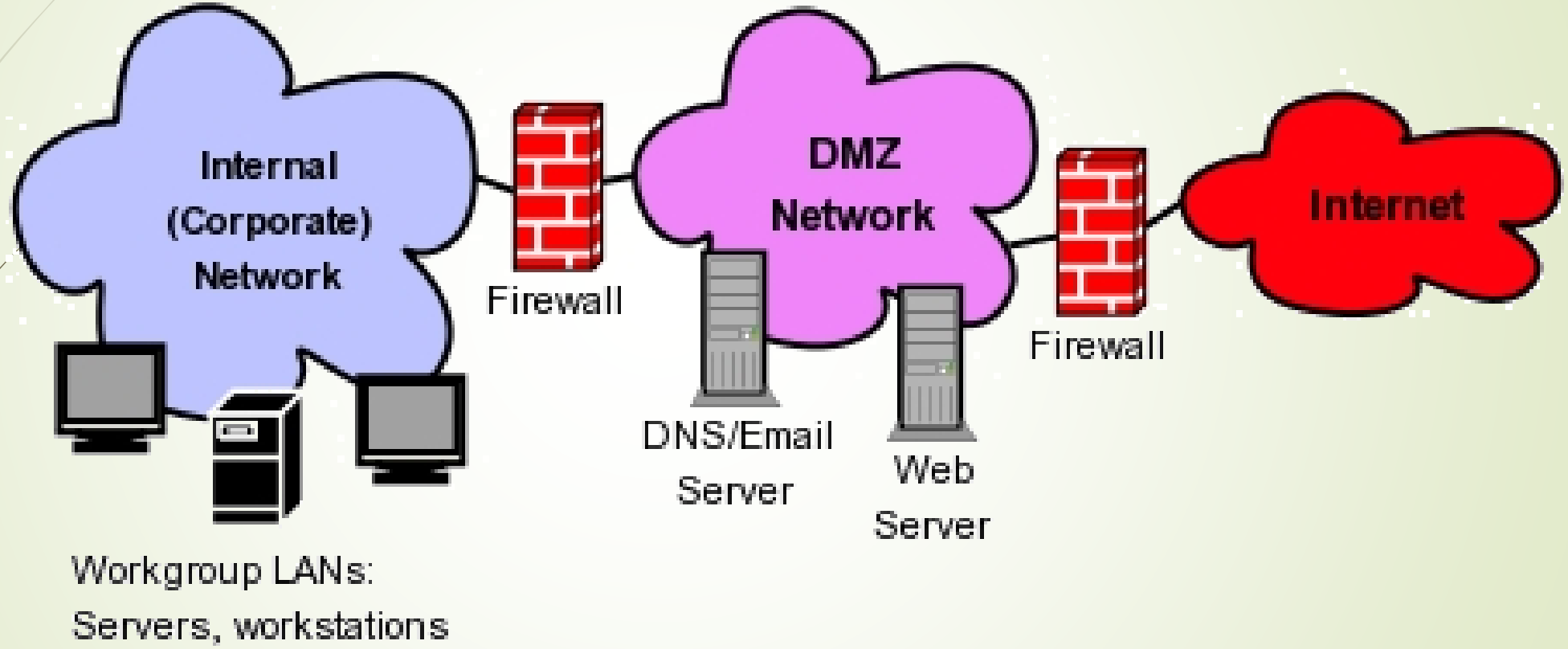
DMZ

- **De-Militarized Zone** (sometimes referred to as a **perimeter network**) is a physical or logical subnetwork that contains and exposes an organization's **external-facing services to an untrusted network**, usually a larger network such as the Internet. The **purpose** of a DMZ is to add an **additional layer of security** to an organization's local area network (LAN)
- The DMZ functions as a **small, isolated network** positioned between the Internet and the private network and, if its design is effective, allows the organization extra time to detect and address breaches before they would further penetrate into the internal networks.

Firewall deployment



Another FW deployment.



Next Generation Firewalls (NGF)

- The goal of next-generation firewalls is to :
  - include more layers of the OSI model,
  - improving filtering of network traffic that is dependent on the packet contents.
- NGFWs come with comprehensive management and reporting, policy enforcement for applications and user control, intrusion prevention, deep packet inspection, sandboxing, and incorporate threat intelligence feeds.

Some famous FW vendors

- Juniper
- Palo Alto
- Cisco
- Fortinet
- Sophos
- ForcePoint
- SonicWall