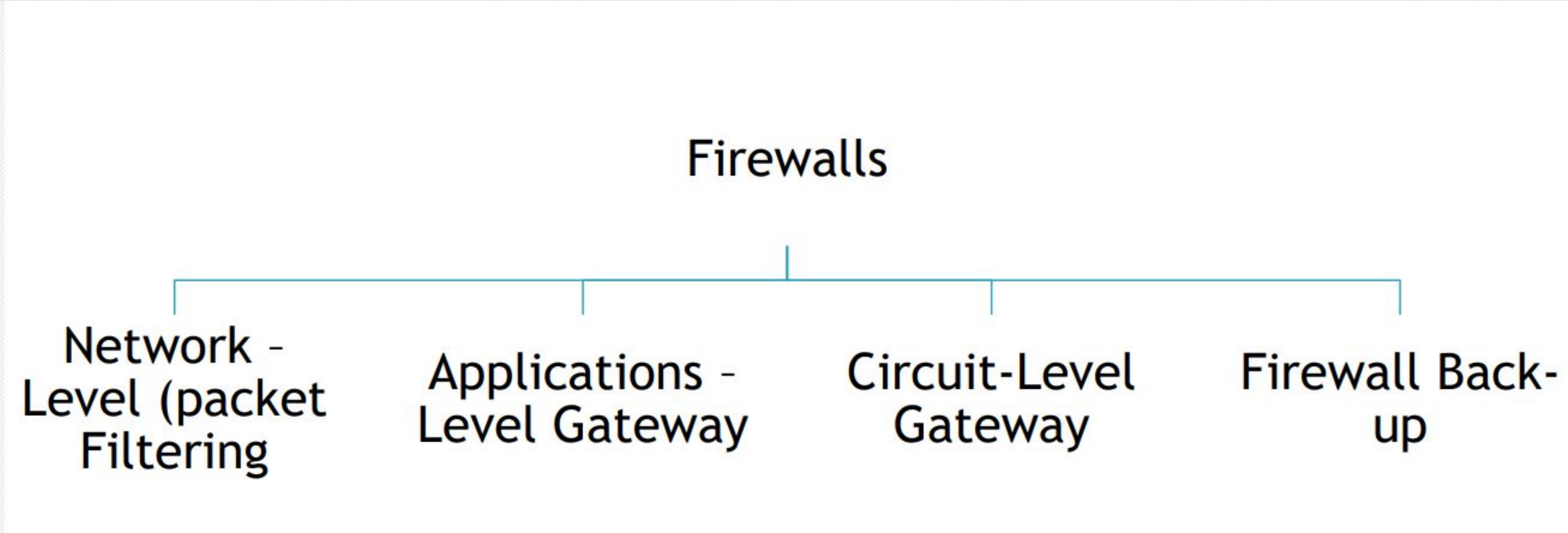
WEEK 5

FIREWALL



Firewalls

Network – Level (packet Filtering

Applications – Level Gateway

Circuit-Level Gateway

Firewall Back-up

DEFINITION

- A network security device that monitors traffic between two or more networks and allows or blocks traffic when necessary based on pre-defined set of security rules.
- Protects a network from a less secure network

DEFINITION(CONTINUED)

- ❑ Blocks undesirable incoming traffic, the same traffic could be allowed when outgoing. E.g. block incoming pings, but allow outgoing ones
- ❑ Generic configuration would include:
  - o Private network: to be secured (home, work, etc.)
  - o Public network: unsecure and threatening (Internet)

DEFINITION(CONTINUED)

❑ A check-point of control and monitoring for network traffic

❑ Interconnects networks with differing trust (internal, demilitarised zone and Internet).

❑ Imposes restrictions on network services

- only authorized traffic is allowed

DEFINITION(CONTINUED)

- ❑ Auditing and controlling access
  - ▪ can implement alarms for abnormal behavior (when a certain threshold of activity is exceeded, an alarm is triggered).
- ❑ Provides perimeter defence

WHY FIREWALLS

- Prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections
- Prevent illegal access/modification to internal data
  - E.g., cracker accesses /modifies a local database
- Allow only authorized access inside network (set of authenticated users/hosts)

FIREWALL FEATURES

- Port control
- Network address translation
- Application monitoring
- Packet filtering
- Data encryption
- Hiding presence 6
- Reporting/logging
- Email virus protection
- Pop ad blocking
- Cookie digestion
- Spyware protection
- etc

CLASSIFICATION OF FIREWALL

Characterized by protocol level it controls in

- ❑ Packet filtering (stateless and stateful)
- ❑ Application-level gateways
- ❑ Circuit-level gateways

- Combination of the above is dynamic packet filter

CLASSIFICATION OF FIREWALL (CONTINUED)

Firewalls may be implemented as a stand-alone hardware device or in the form of software running a client computer or proxy server.

CLASSIFICATION OF FIREWALL (CONTINUED)

Thus, can be classified also as:

❑ Hardware firewall

- A software firewall running on a dedicated piece of hardware or a specialized device

❑ Software firewall In practice, a computer may be protected by both hardware and software firewalls.

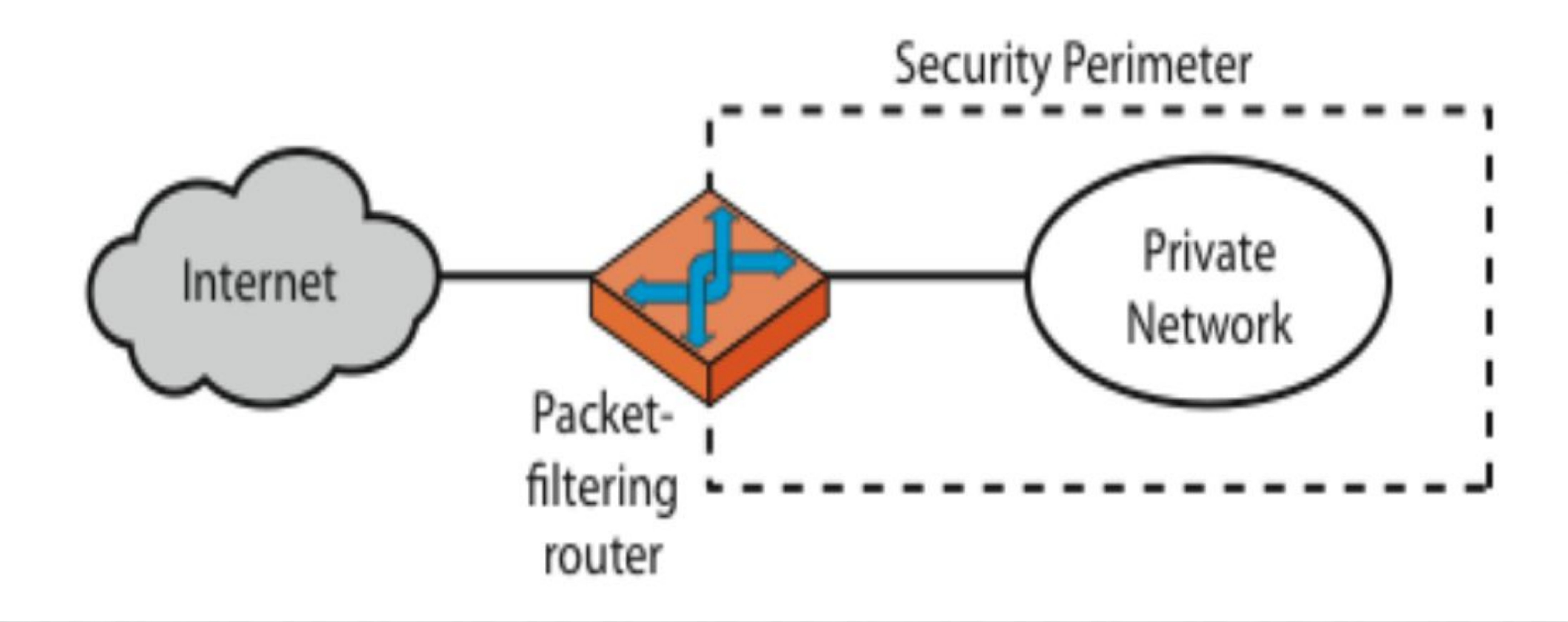
FIREWALLS: HARDWARE AND SOFTWARE

Hardware

- CISCO PIX Firewall.
- Checkpoint.
- Sun's iForce VPN/Firewall.
- Fortinet.
- Watchguard. ▪ Sophos. ▪ Forcepoint. ▪ Juniper SRX.

- Software
  - Linux Iptables
  - Windows firewall
  - Pfsense (Unix Distribution)
  - IPFire
  - Kaspersky ▪ Zone alarm

FIREWALLS – PACKET FILTERS



(a) Packet Filtering Router

FIREWALLS – PACKET FILTERS

❑ Uses transport -layer information only

  - IP Source Address and Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP (Internet Control Message Protocol) message type

- Examples
  - DNS uses port 53
  - No incoming port 53 packets except known trusted servers

FIREWALLS – PACKET FILTERS (CONTINUED)

- ACK (Acknowledgment): The ACK flag is used to acknowledge receipt of data or to confirm the successful establishment of a connection (handshake).
- FIN (Finish): The FIN flag is used to initiate the graceful termination of an established TCP connection.
- RST (Reset): The RST flag is used to abruptly terminate a TCP connection or to indicate an error condition.
- PSH (Push): The PSH flag is used to instruct the receiving device to deliver received data to the application layer immediately, without waiting for the TCP buffer to fill up or for the receiving device to perform further processing

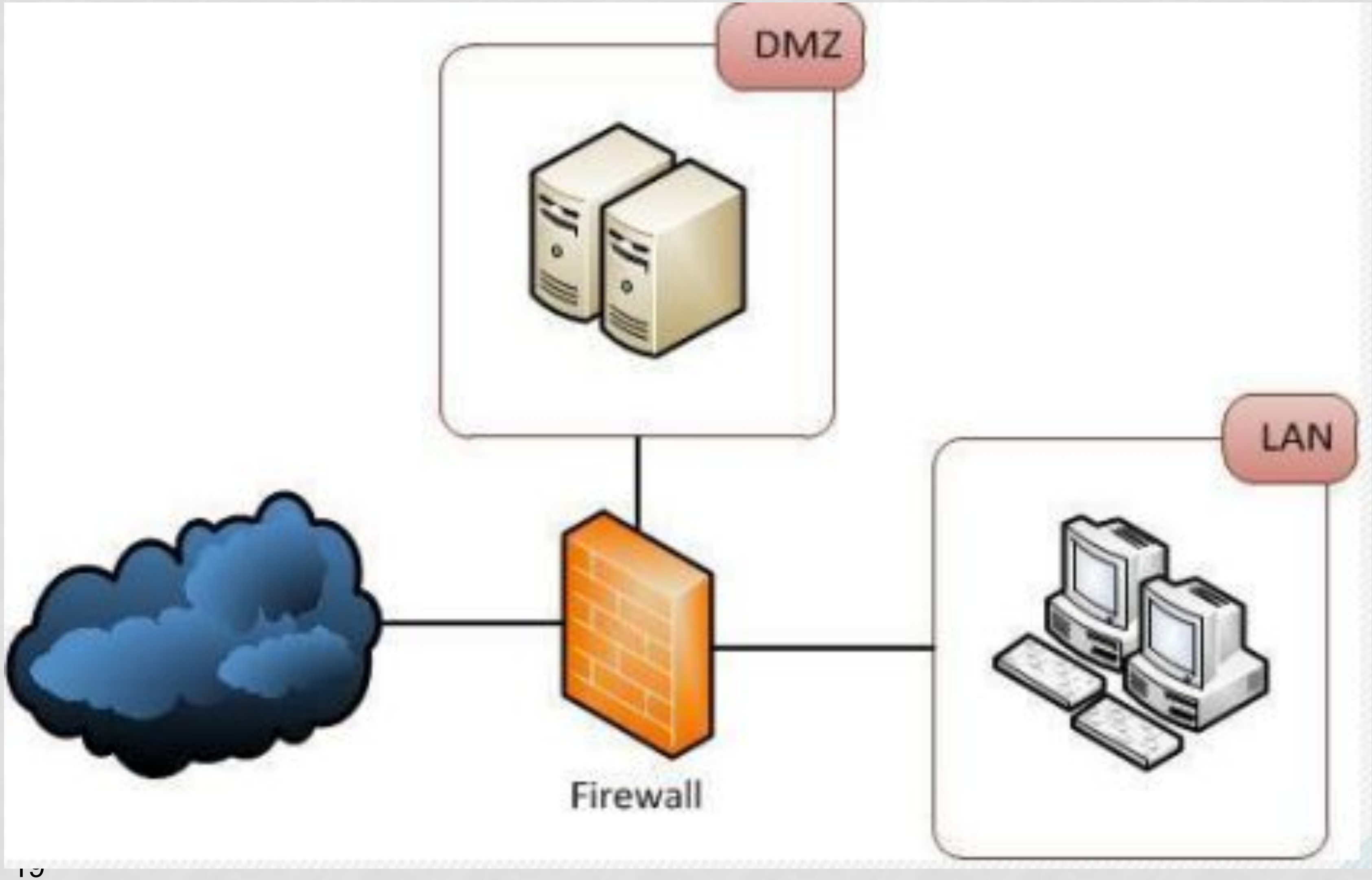
USE OF PACKET FILTERS

- ❑ Filtering with incoming or outgoing interfaces
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems
    - Ingress – incoming traffic (data)
    - Egress – outgoing traffic (data)

PACKET FILTERS CONFIGURATION

- ❑ Start with a security policy
- ❑ Specify allowable packets in terms of logical expressions on packet fields
- ❑ Rewrite expressions in syntax supported by your vendor (e.g CISCO, HUAWEI, etc)
- ❑ General rules - least privilege
  - All that is not expressly permitted is prohibited
  - If you do not need it, eliminate it

FIREWALLS COMMON CONFIGURATIONS



FIREWALLS COMMON CONFIGURATIONS (CONTINUED)

- If three networks (with varying trust): e.g. internal, Demilitarized zone, and Internet
- The DMZ would contain servers that can be accessed from outside the company, e.g. Web servers, Email servers, DNS, etc.
- Allow:
    - Internet to DMZ,
    - DMZ to Internet,
    - Internal to Internet
- Block:
- Internet to Internal, DMZ to Internal

FIREWALLS COMMON CONFIGURATIONS – CONT’D

❑ If only two networks: e.g. home and Internet

❑ Allow

- Almost any traffic from home to Internet

❑ Block

- Almost any traffic from Internet to home