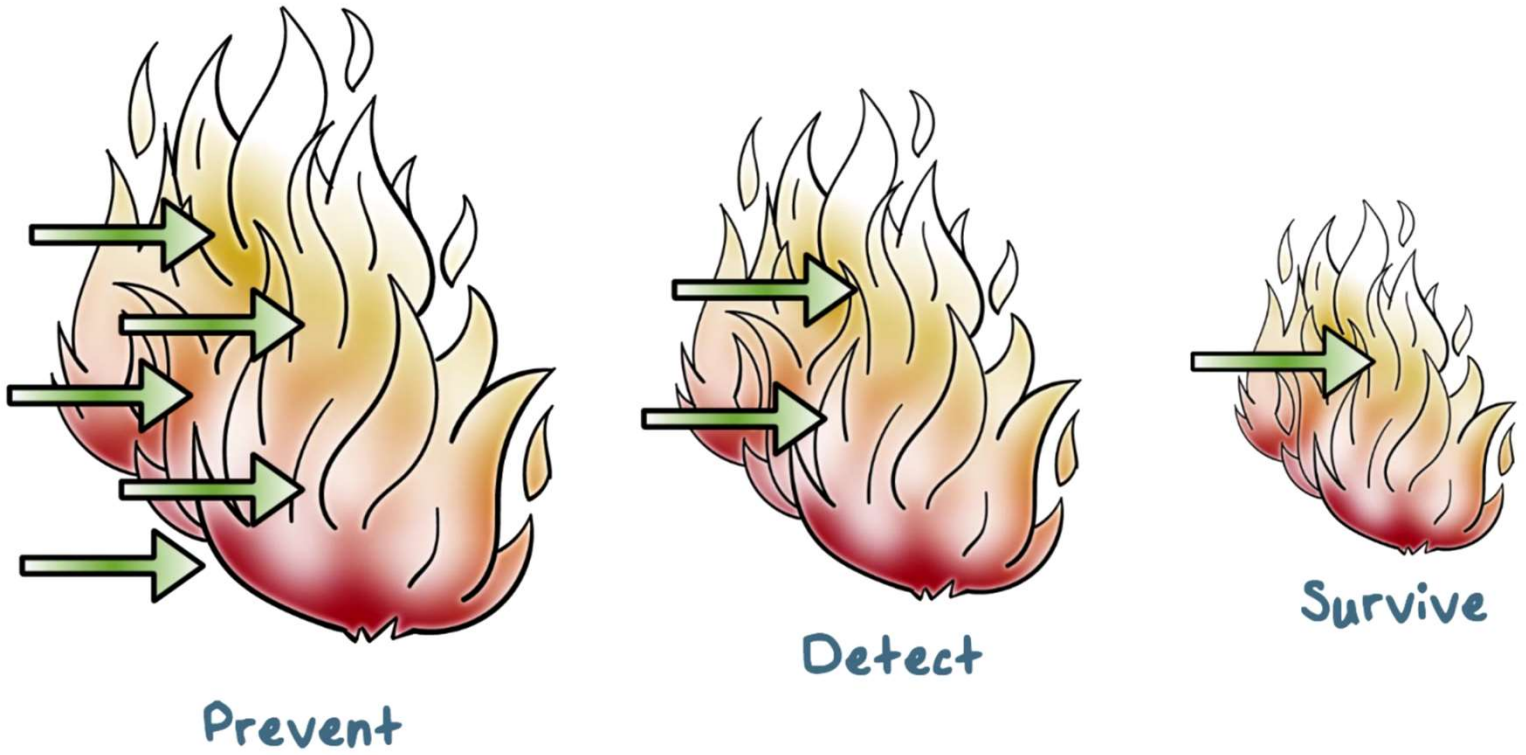
Firewalls
Lesson Introduction

- Part of network defense-in-depth
- Types of firewall filtering
- Deployment strategies

Defense-in-Depth

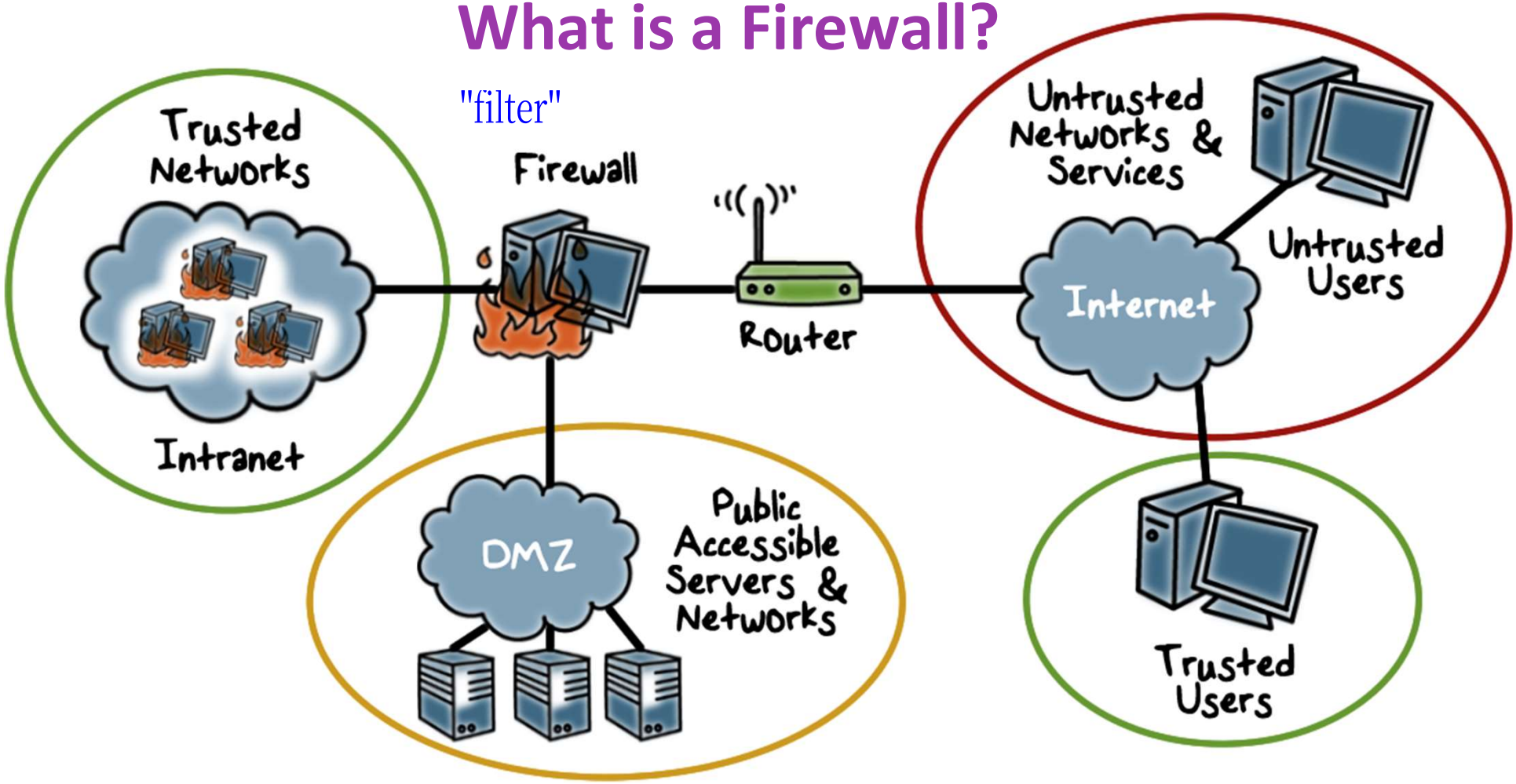


Detection: Looking for indicators that something is going on.

Prevent malicious activity from actually penetrating

What is a Firewall?

"filter"



Manage traffic, reduce the possibility that an attacker make an intrude

Firewall on PC usually prevents outbound activity: if malware reaches your PC, it will try to send information back to inform its "landing" and send back collected data.

Firewall Design Goals

- **Enforcement of security policies**
  - All traffic from internal network to the Internet, and vice versa, must pass through the firewall Any traffic going though needs to be checked
  - Only traffic authorized by policy is allowed to pass you need to establish what is authorized, no ground rule
- **Dependable**
  - The firewall itself is immune to subversion

Taking down a firewall makes it much easier for an attacker to intrude. Firewall itself needs to be protected!

Firewall Access Policy

Lists the types of traffic authorized to pass through the firewall

- **Includes**: address ranges, protocols, applications and content types

Firewall Access Policy

Developed from the organization's information security **risk assessment and policy**, and a broad specification of **which traffic types** the organization needs **to support**

- Refined to detail the filter elements that can be **implemented within an appropriate firewall topology**

A firewall with inappropriate design is worse than having no firewall at all. Because you assume that your security is ensured with that "misbehaving" firewall.

Firewall Limitations

Firewalls cannot protect...

- Traffic that does not cross it
  - Routing around
  - Internal traffic
- When misconfigured

Additional, Convenient Firewall Features

- Gives insight into traffic

  mix via **logging**

- **Network Address Translation**

- Encryption

External cannot reach the internal address. All they see is a firewall, it is the only address that is visible from the outside.

You can put encryptor and decrytors on the firewall, but the drawback is that it is going to slow everything down.

Firewalls and Filtering

- Packets **checked then passed**
- **Inbound & outbound** affect when policy is checked

Filtering Types

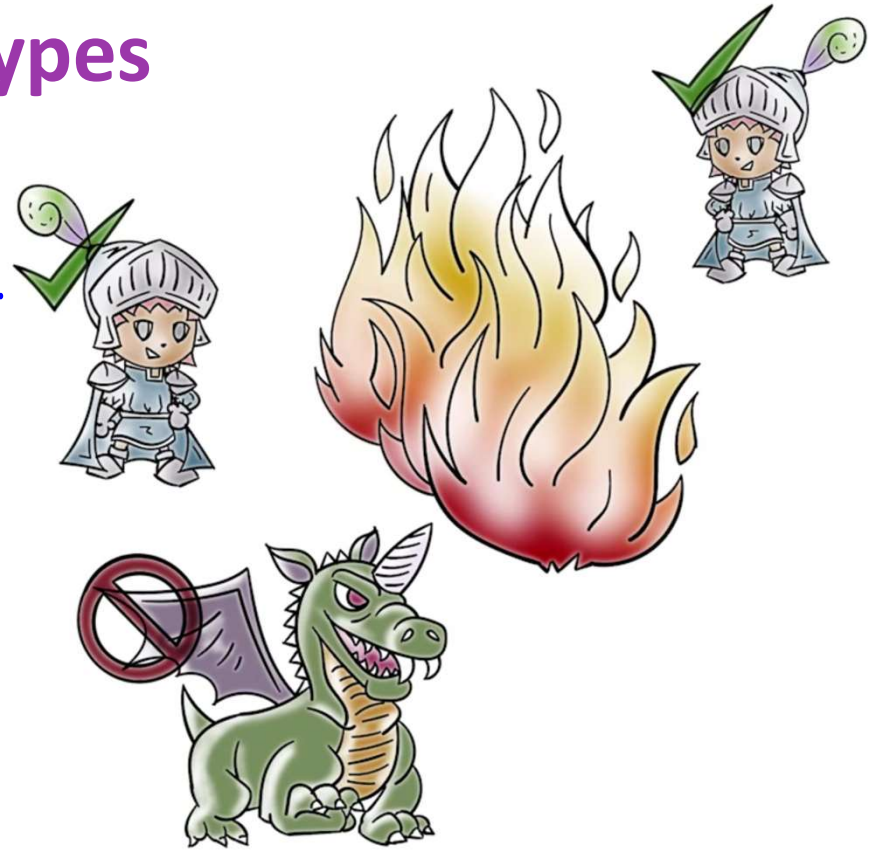
- **Packet filtering**

Anything not on the approved list will be blocked.

  - Access Control Lists

- **Session filtering**

  - Dynamic Packet Filtering
  - Stateful Inspection
  - Context Based Access Control



Packet Filtering

- Decisions made on a **per-packet**

  basis Look at every packet header that come across

- No state information saved

Packet Filtering Firewall

- **Applies rules to each incoming and outgoing IP packet**
  - Typically a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match

If someone pretends that his packet is come from somewhere else, packet filtering will fail.

Packet Filtering Firewall

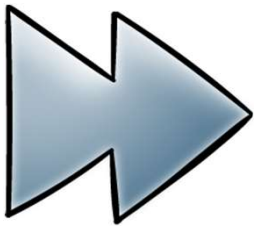
Filtering rules are based on information contained in a network packet:

- Source IP address
- Destination IP address
- Source and destination transport-level address:
- IP protocol field
- Interface

Packet Filtering Firewall

- **Two default policies:**

- **Discard -** prohibit unless expressly permitted
  - –More conservative, controlled, visible to users
- **Forward -** permit unless expressly prohibited
  - –Easier to manage and use but less secure



Packet Filtering Examples

Rule	Direction	Src Address	Dest address	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Anything that does not conform to the rule will be denied (default: discard)

Packet Filtering Advantages

- **Advantages:**
  - Simplicity
  - Typically transparent to users and are very fast

Packet Filtering Weaknesses

- Cannot prevent attacks that **employ application specific vulnerabilities or functions**
- Limited **logging** functionality
- Vulnerable to attacks and exploits that **take advantage of TCP/IP**
- Packet filter firewalls are susceptible to **security breaches caused by improper configurations**

Packet Filtering Firewall Countermeasures

- **IP Address spoofing Countermeasure:** Discard packets with an inside source address if the packet arrives on an external interface.
- **Source Routing Attacks Countermeasure:** Discard all packets in which the source destination specifies the route.
- **Tiny Fragment Attack Countermeasure:** Enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header

A packet with incomplete header. If break up a packet: separate the header information into multiple parts, the firewall won't recognize it as bad address. If it doesn't see a bad address, the default rule may let it pass through.

Stateful Inspection Firewall

Tightens rules for TCP traffic by creating a directory of TCP connections

- There is an entry for each currently established connection
- Packet filter will allows incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number,

Inspects data for protocols like FTP, IM, and SIPS commands

Connection State Table

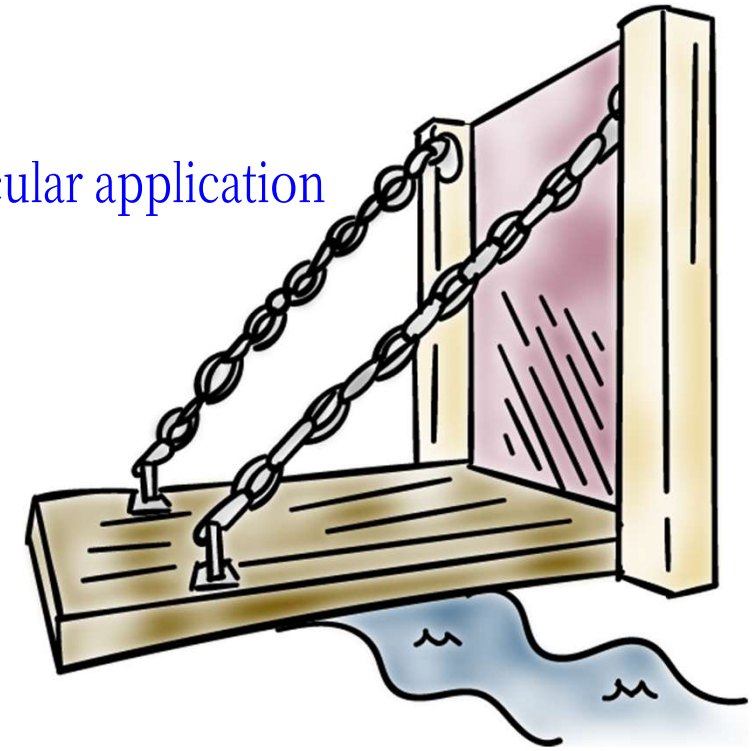
Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.23132.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an **application proxy**

Not a generic firewall, it is tuned and tailored for a particular application

- Acts as a **relay** of application-level traffic (basically a man or system in the middle)



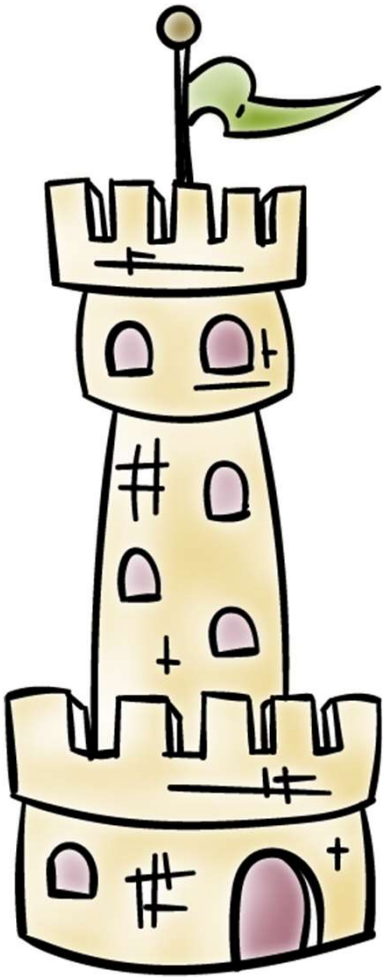
Application-Level Gateway

communication has to go through an intermediary.

- **Must have proxy code for each application**
  - May restrict application features supported
  - Tend to be more secure than packet filters

Disadvantage

- Additional processing overhead on each connection

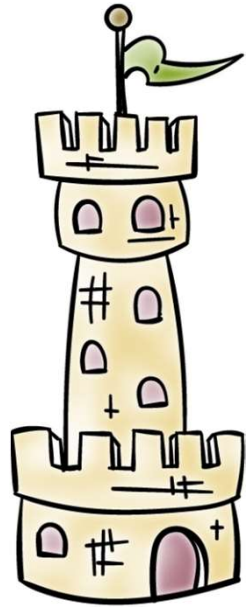


Bastion Hosts

- Serves as a **platform** for an application-level gateway

- System identified as a **critical strong point** in the network's security

Bastion Hosts

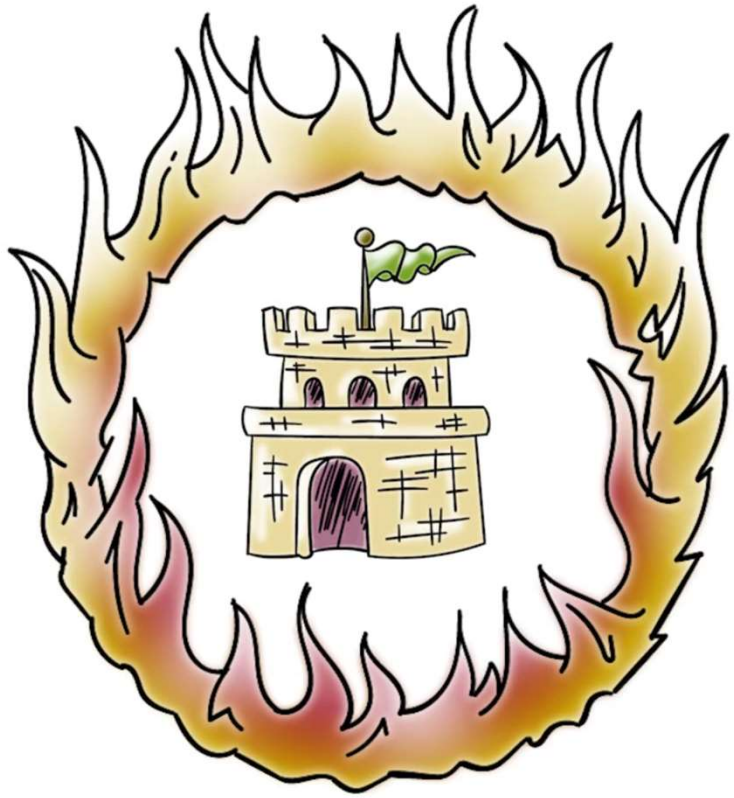


Common characteristics:

- Runs secure O/S, only essential services
- May require user authentication to access proxy or host
- Each proxy can restrict features, hosts accessed
- Each proxy is small, simple, checked for security
- Limited disk use, hence read-only code
- Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.

Host Based Firewalls

- Used to secure an **individual host**
- Available in operating systems or can be provided as an add-on package
- **Filter and restrict** packet flows
- Common location is a server



Host Based Firewall Advantages

Advantages:

- Filtering rules can be **tailored** to the host environment
- Protection is provided **independent of topology**
- Provides an **additional layer** of protection

Personal Firewalls

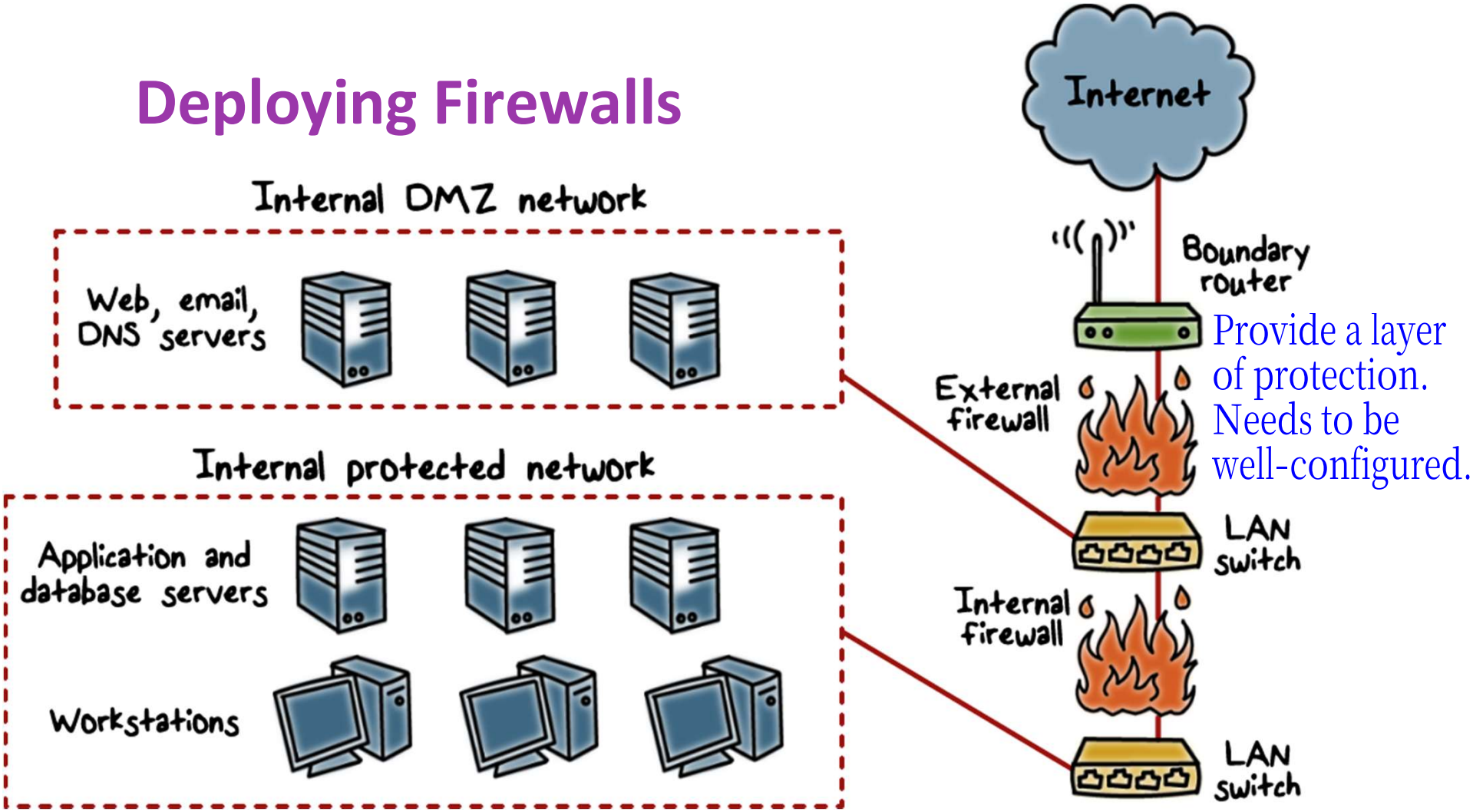
- **Controls traffic between a personal computer or workstation and the Internet or enterprise network**
- For both home or corporate use
- Typically is a software module on a personal computer

Commonly used for preventing malwares from reaching out.

Personal Firewalls

- Can be housed in a **router that connects all of the home computers** to a DSL, cable modem, or other Internet interface
- Typically much **less complex** than server-based or stand-alone firewalls
- **Primary role is to deny unauthorized remote access**
- May also monitor outgoing traffic to detect and block worms and malware activity

Deploying Firewalls



Provide a layer of protection. Needs to be well-configured.

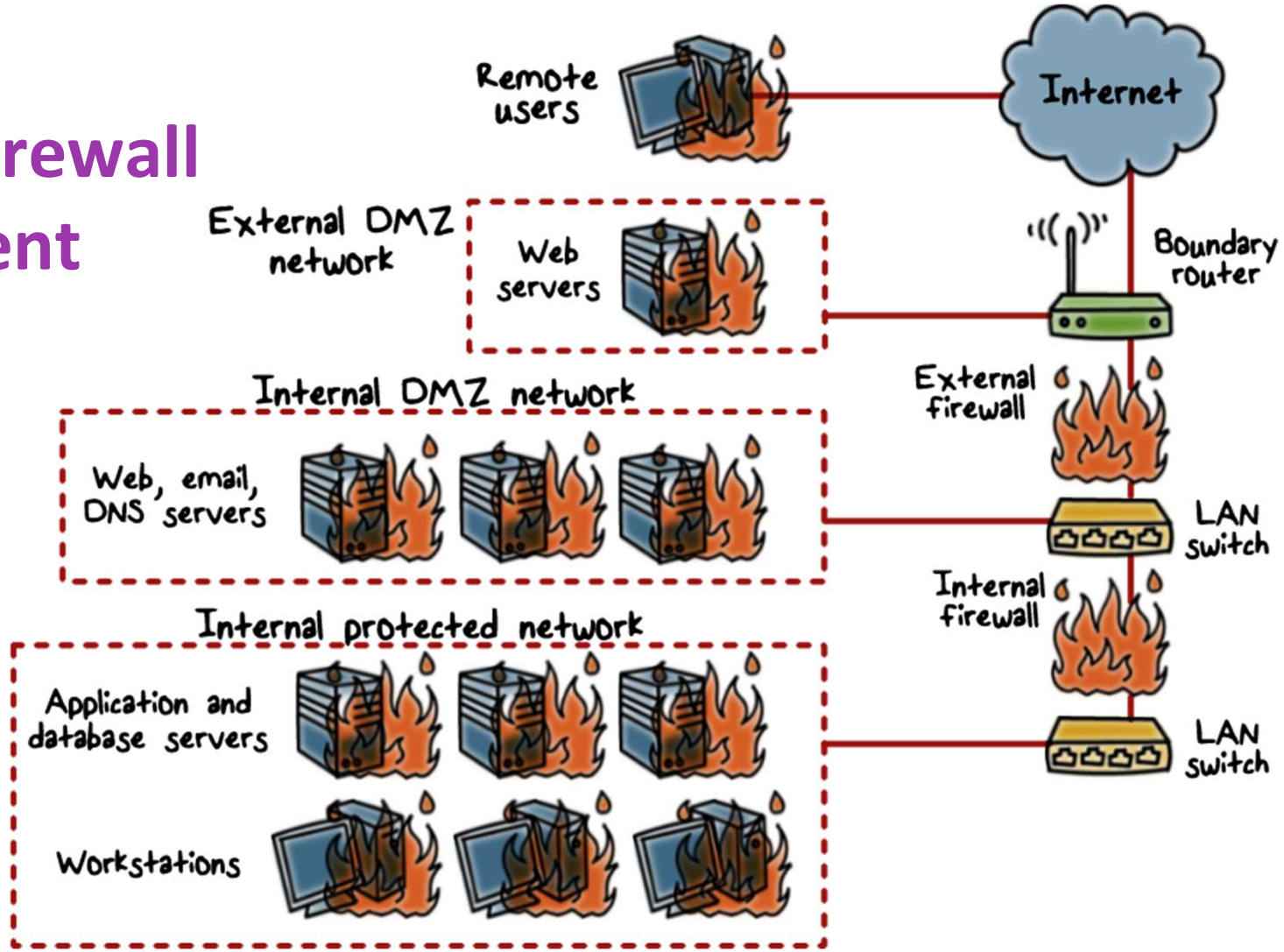
External: close to or facing untrusted environment.
Internal: face to the internal environment where there is important data.

Internal Firewalls

Internal Firewall Purposes:

- Add more **stringent filtering capability**
- Provide **two-way protection** with respect to the DMZ
- **Multiple firewalls** can be used to protect portions of the internal network from each other

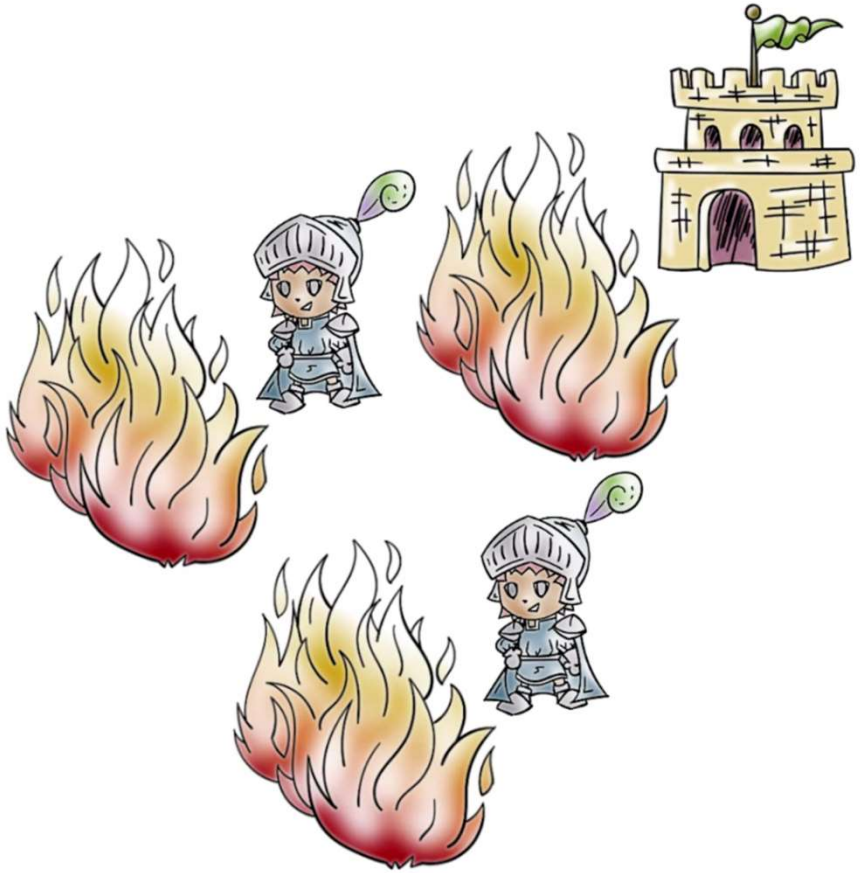
Distributed Firewall Deployment



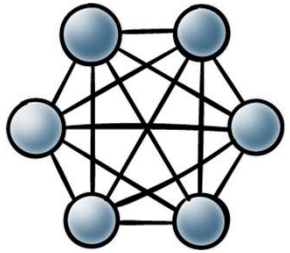
Distributed Firewall Deployment

An important aspect of distribute firewall configuration:

- **Security Monitoring**



Firewall Topologies



- **Host-resident firewall:** includes personal firewall software and firewall software on servers
- **Screening router:** single router between internal and external networks with stateless or full packet filtering
- **Single bastion inline:** single firewall device between an internal and external router
- **Single bastion T:** has a third network interface on bastion to a DMZ where externally visible servers are placed.
- **Double bastion inline:** DMZ is sandwiched between bastion firewalls.
- **Double bastion T:** DMZ is on a separate network interface on the bastion firewall
- **Distributed firewall configuration:** used by some large businesses and government organizations

Firewalls
Lesson Summary

- Enforce security policy to prevent attacks by way of traffic filtering; default deny
- Packet filtering and session filtering, application-level gateway
- Host-based firewalls, screen router, bastion hosts, and DMZ