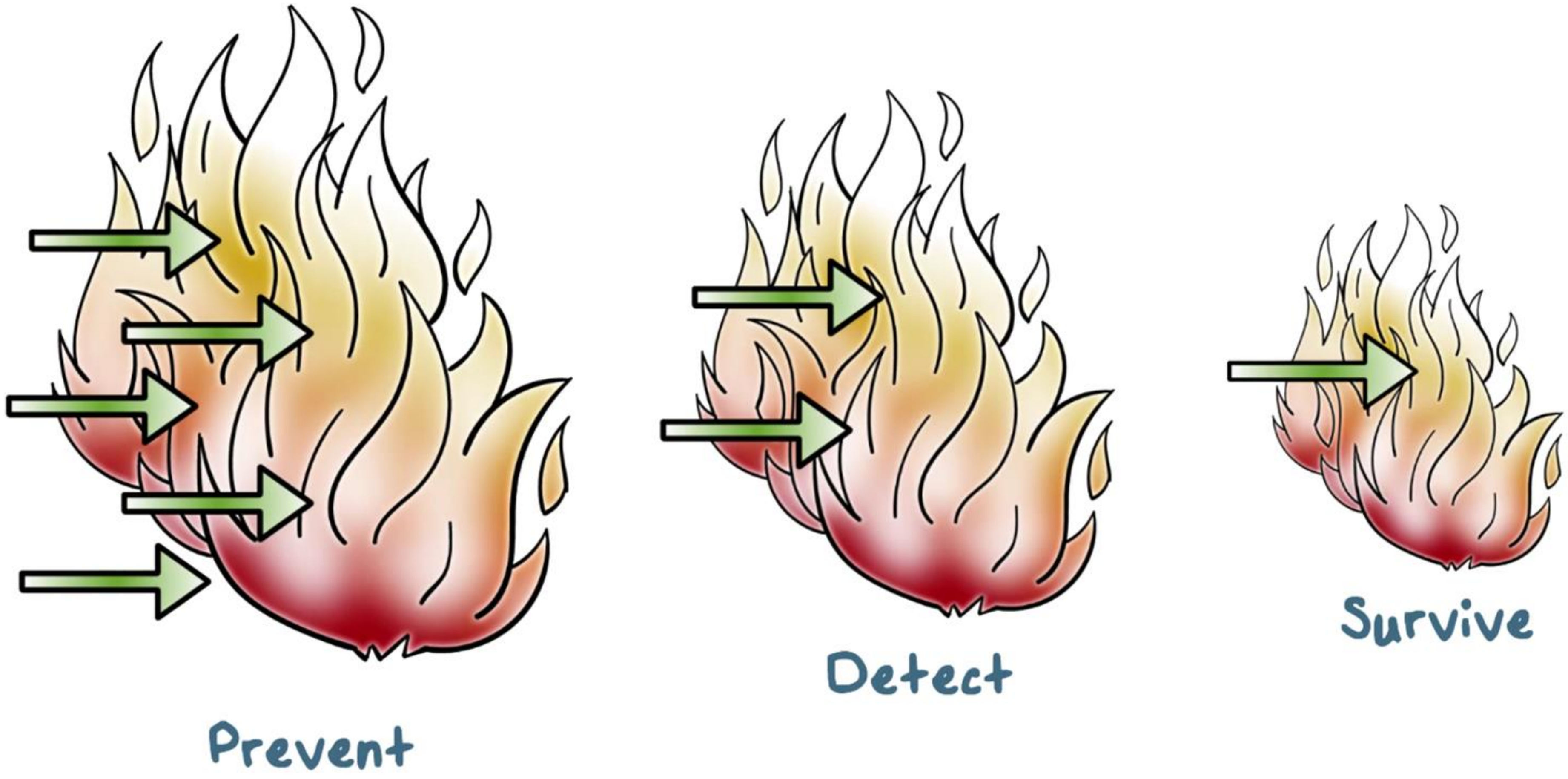
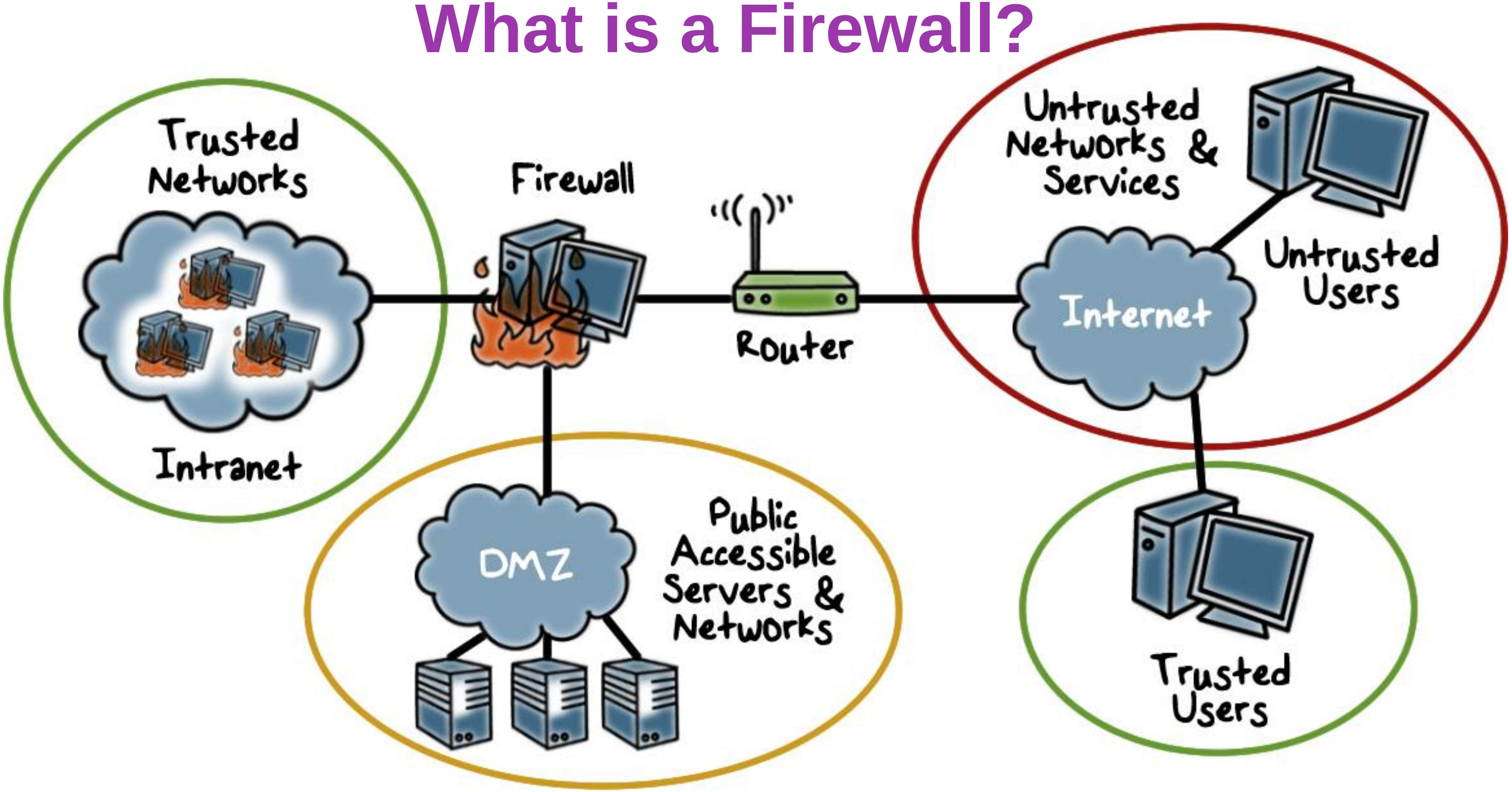
Firewalls
Lesson Introduction

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

Defense-in-Depth



What is a Firewall?



Firewalls Quiz

Mark the box next to all those items that firewalls **can stop**:

□ Hackers breaking into your system

□ Internet traffic that appears to be from a legitimate source

□ Viruses and worms that spread through the internet

□ Spyware being put on your system

□ Viruses and worms that are spread through email

□

Firewall Design Goals

- Enforcement of security policies
  - All traffic from internal network to the Internet, and vice versa, must pass through the firewall
  - Only traffic authorized by policy is allowed to pass
- Dependable
  - The firewall itself is immune to subversion

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**

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

Firewalls Features Quiz

Mark all the answers that apply:

Malware can disable:

□ Software firewalls

□ Hardware firewalls

□ Antivirus checkers

Firewalls can stop/control:

□ Pings

□ Packet Sniffing

□ Outbound network traffic

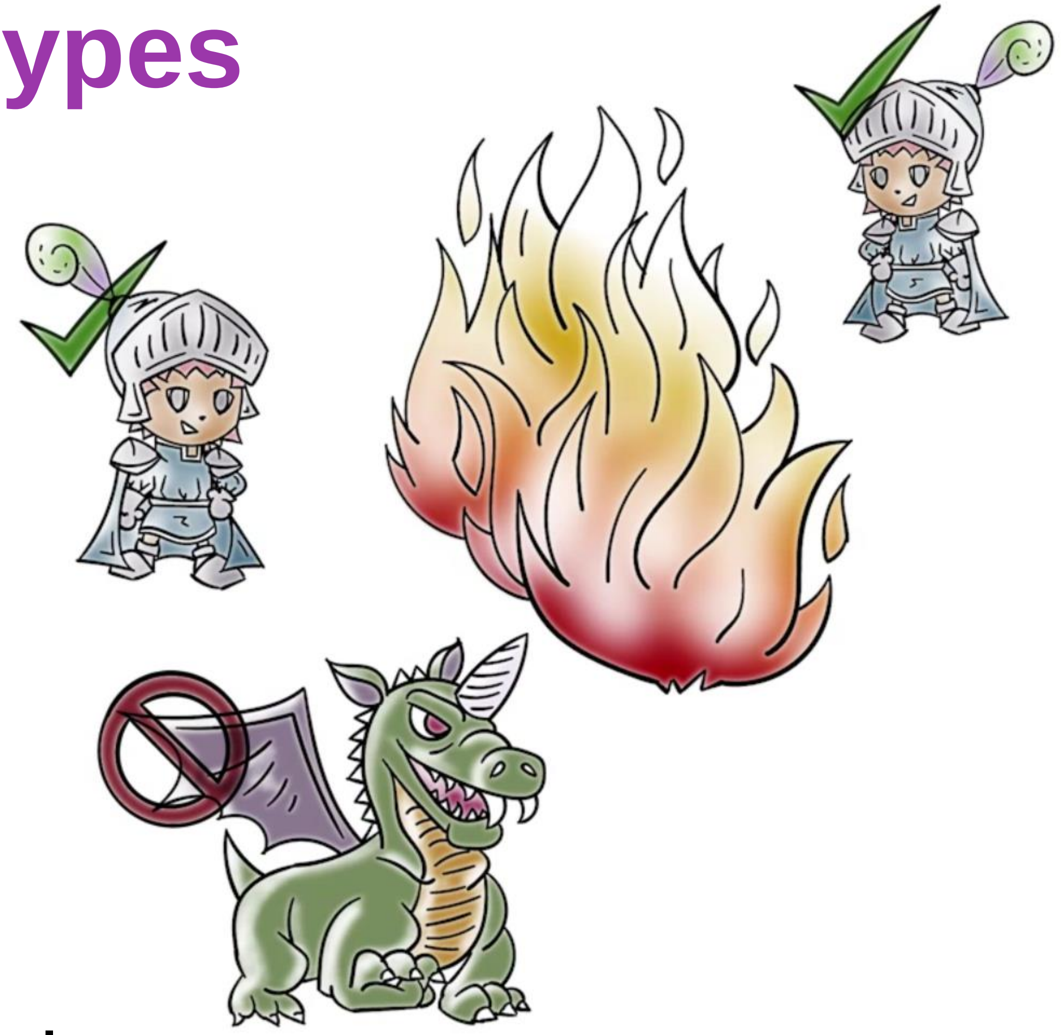
Firewalls and Filtering

- Packets **checked then passed**

- **Inbound & outbound** affect when policy is checked

Filtering Types

- **Packet filtering**
  - Access Control Lists
- **Session filtering**
  - Dynamic Packet Filtering
  - Stateful Inspection
  - Context Based Access Control



Packet Filtering

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

- 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

Packet Filtering Firewall

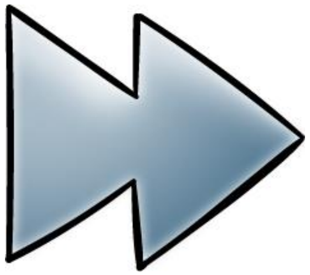
Filtering rules are based on information contained in a network packet:

- 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

Firewall Filtering Quiz

Rank each policy based on **user convenience and security.**

Use number **1 for best, 2, 3 for worst**

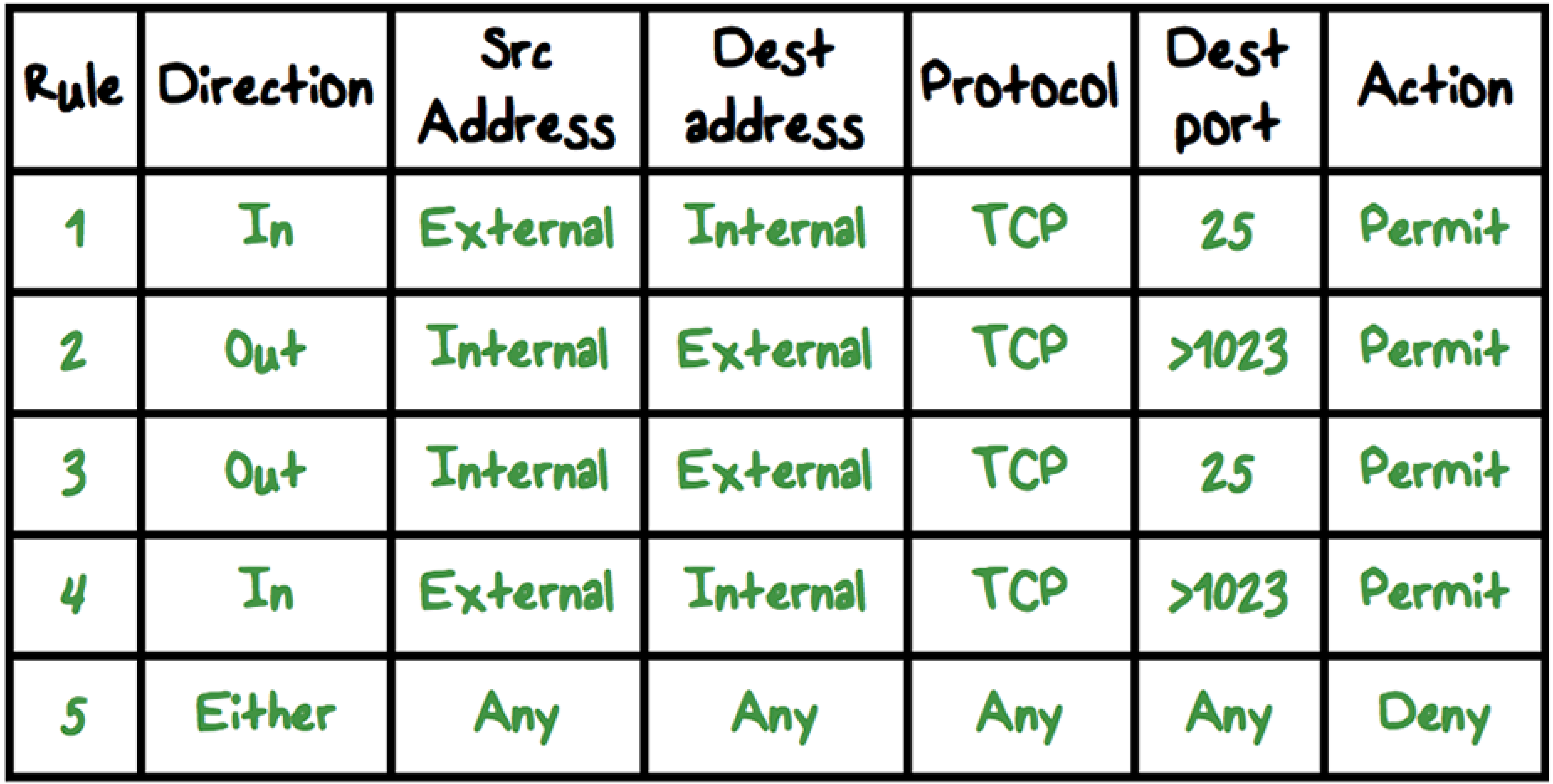
Policy	**Ease of Use**	**Security**
Accepts only packets it knows are safe		
Drops packets it knows are unsafe		
Queries user about questionable packet		

Typical Firewall Configuration

- If **dynamic protocols** are in use, ***entire ranges of ports must be allowed*** for the protocol to work.

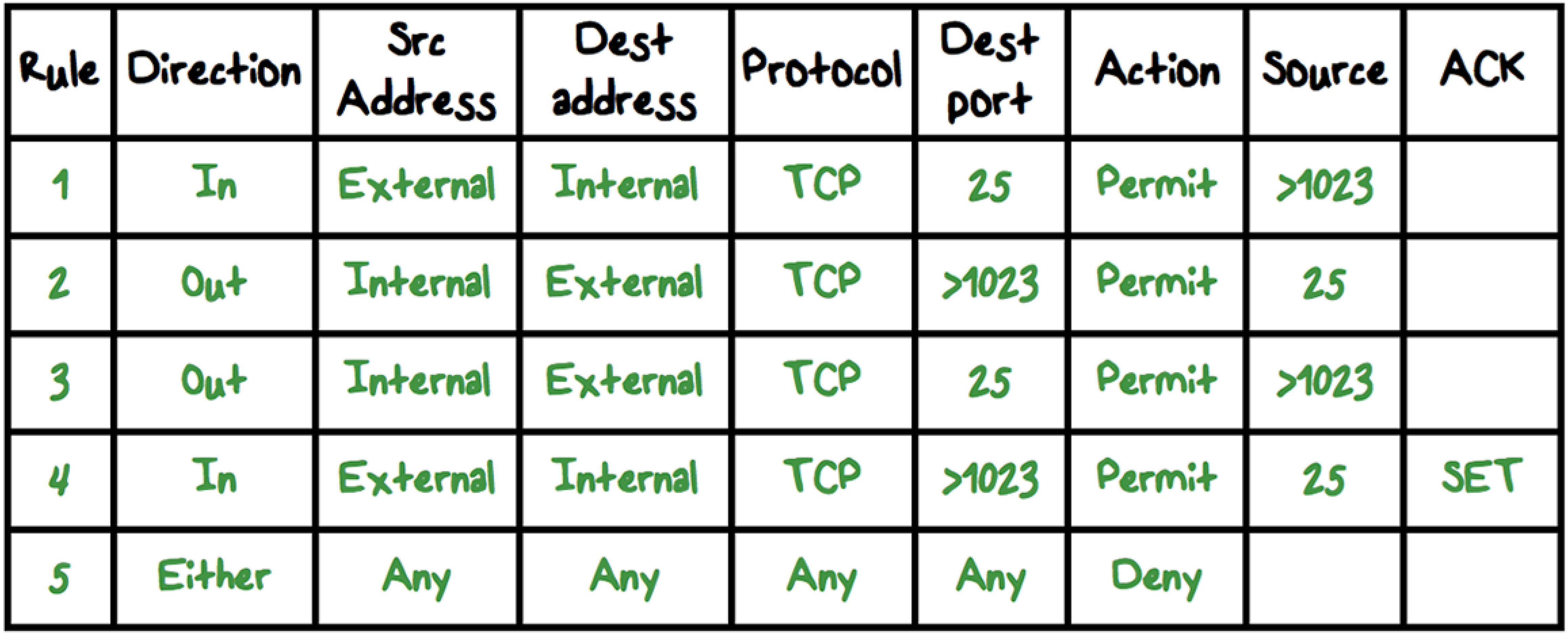
- **Ports > 1024 left open**

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

Modifying the Rules on Source Ports



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

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

Packet Filtering Quiz

In order for a fragmented packet to be successfully reassembled at the destination each fragment must obey the following rules. Mark all answers that are true:

□ Must not share a common fragment identification number.

□ Each fragment must say what its place or offset is in the original unfragmented packet.

□ Each fragment must tell the length of the data carried in the fragment.

□ Finally the fragment does not need to know whether more fragments follow this one.

Stateful Inspection Firewall

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

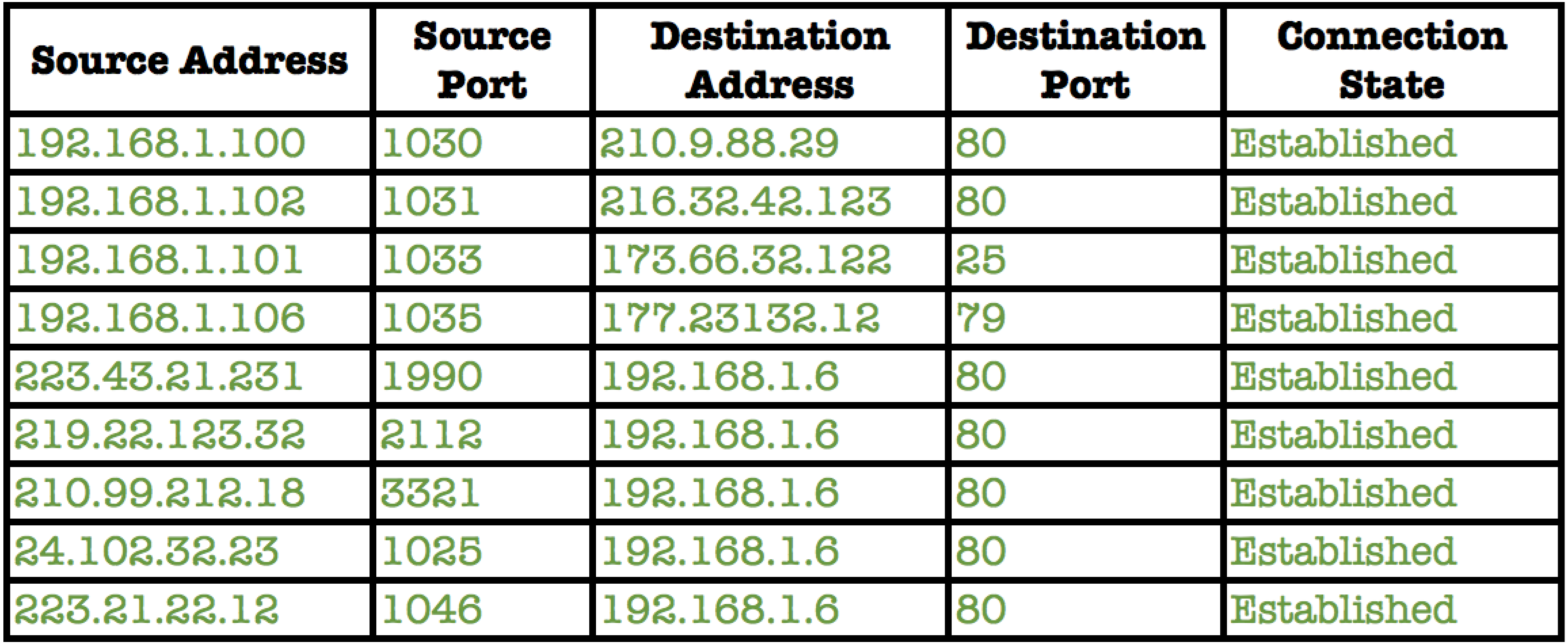
- There is an entry for each currently established connection
- Packet filter will allows incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory

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

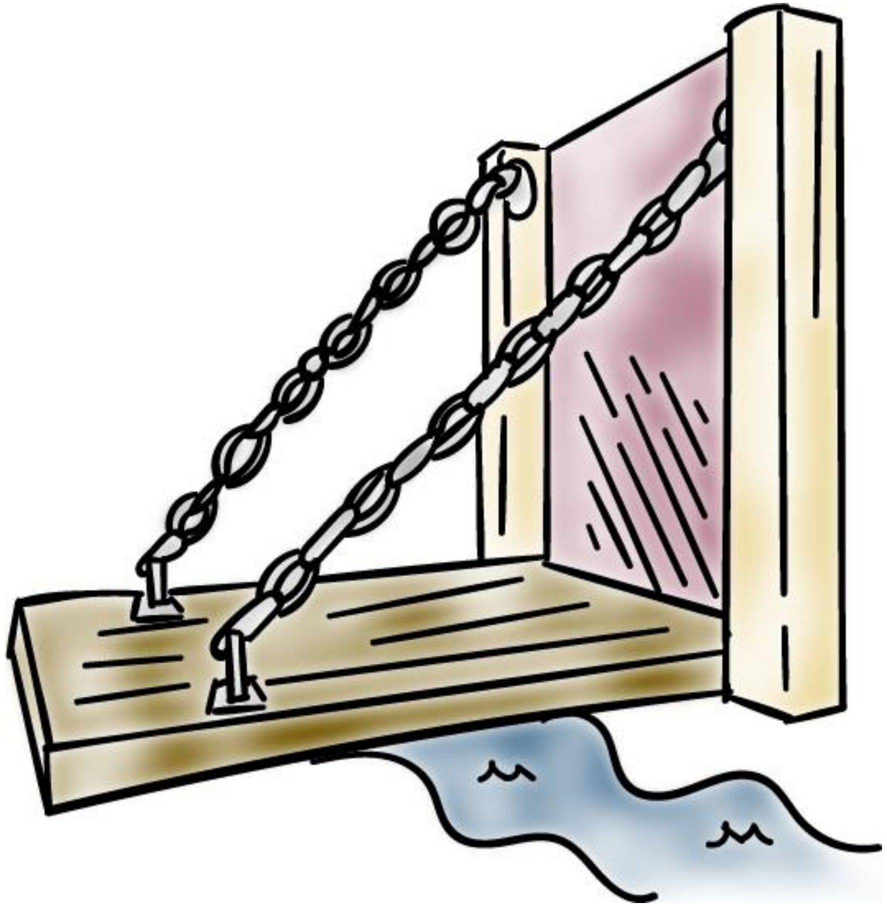


Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.23132.12	79	Established
223.43.21.231	1990	192.168.1.6	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

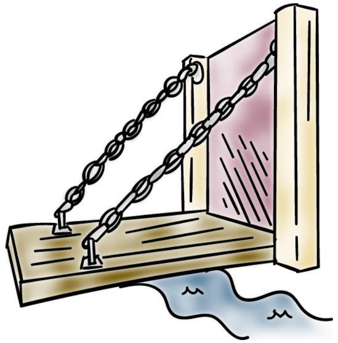
Application-Level Gateway

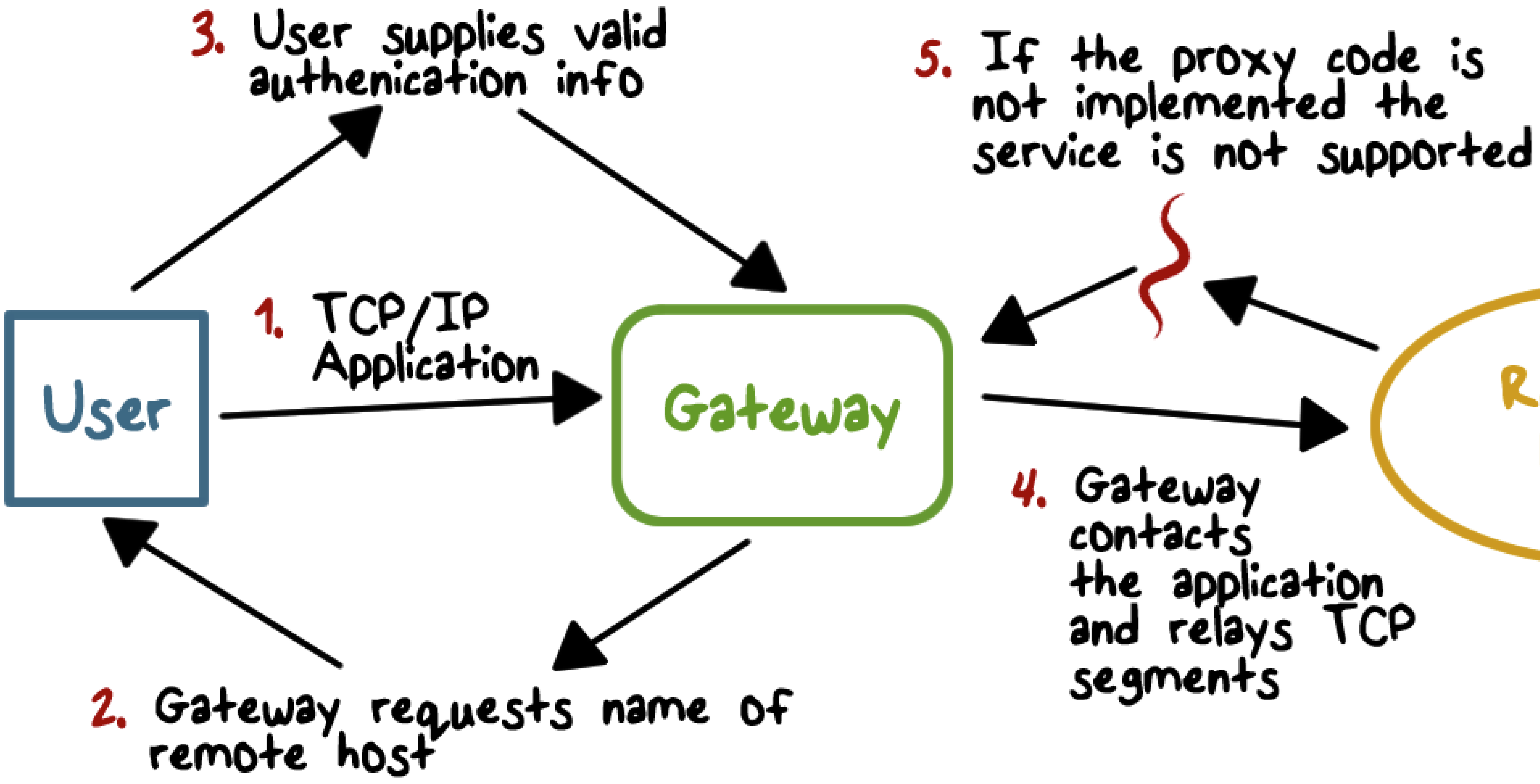
- Also called an **application proxy**

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



Application-Level Gateway





1. TCP/IP Application

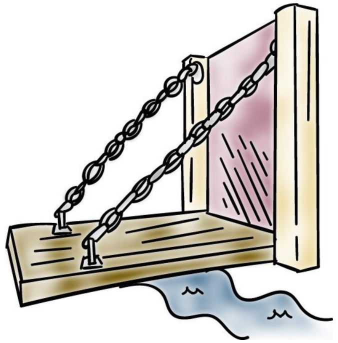
2. Gateway requests name of remote host

3. User supplies valid authenication info

4. Gateway contacts the application and relays TCP segments

5. If the proxy code is not implemented the service is not supported

Application-Level Gateway



- **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

Filtering Quiz

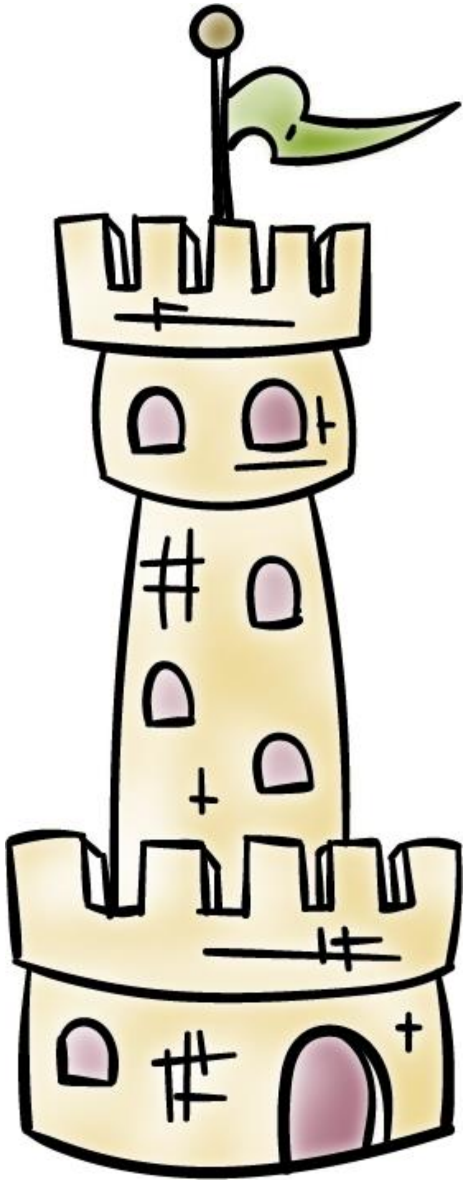
Mark each statement as either
T for True of **F for False**:

□ A packet filtering firewall is typically configured to filter packets going in both directions.

□ A prime disadvantage of an application-level gateway is the additional processing overhead on each connection.

□ A packet filtering firewall can decide if the current packet is allowed based on another packet that it has just examined.

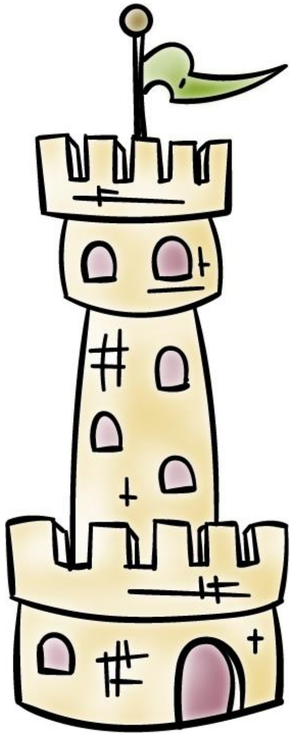
□ A stateful inspection firewall needs to keep track of information of an active connection in order to decide on the current packet.



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

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

Personal Firewalls - Common Services

- Personal file sharing (548, 427)
- Windows sharing (139)
- Personal Web sharing (80, 427)
- Remote login—SSH (22)
- FTP access (20-21, 1024-65535 from 20-21)
- Remote Apple events (3031)
- Printer sharing (631, 515)
- IChat Rendezvous (5297, 5298)
- ITunes Music Sharing (3869)
- CVS (2401)
- Gnutella/Limewire (6346)
- ICQ (4000)

IRC (194)
MSN Messenger (6891-6900)
Network Time (123)
Retrospect (497)
SMB (without netbios–445)
VNC (5900-5902)
WebSTAR Admin (1080, 1443)

Advanced Firewall Protection

- **Stealth Mode** hides the system from the internet by dropping unsolicited communication packets

- **UDP packets** can be blocked

- Logging for **checking on unwanted activity**

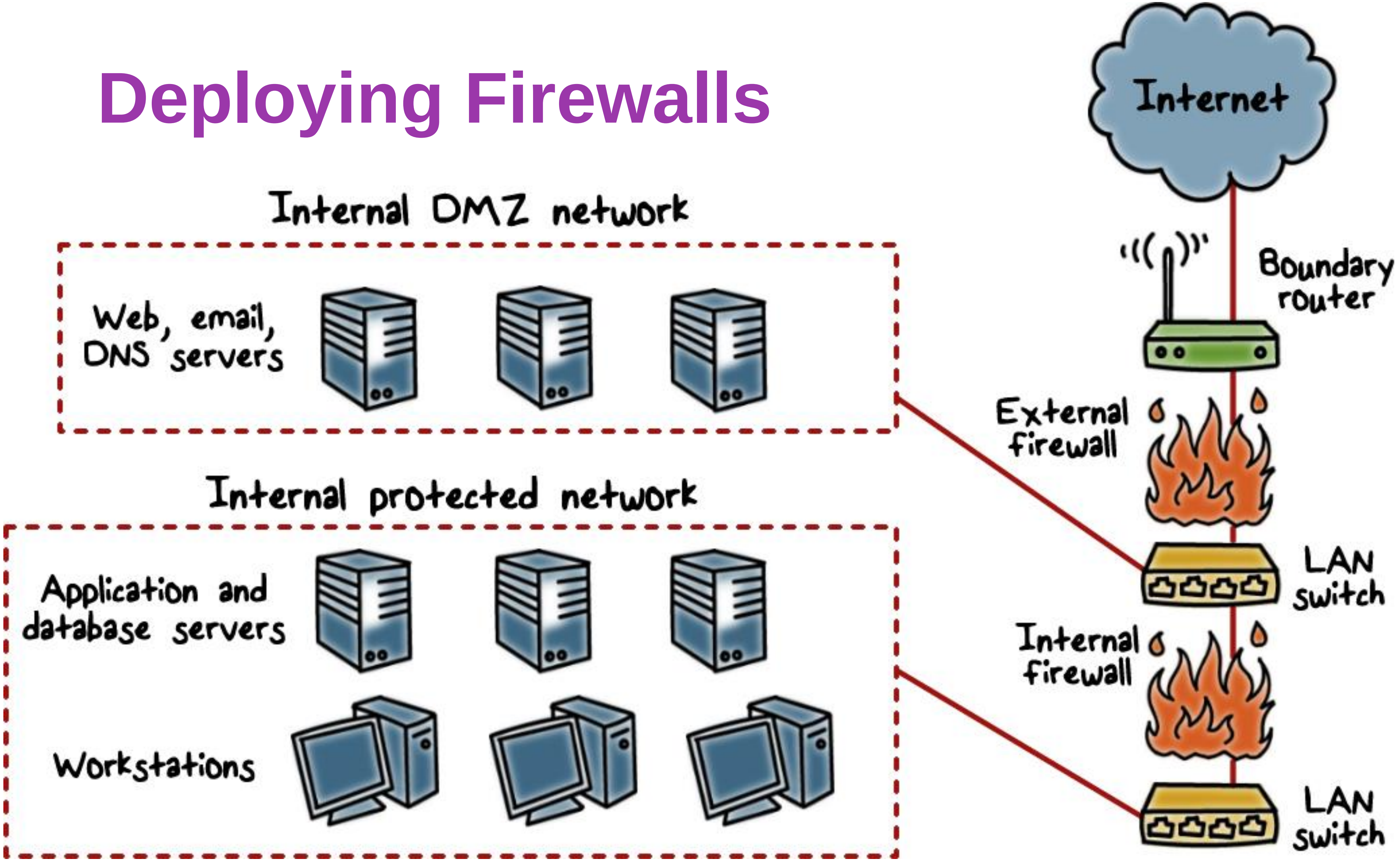
- Applications must have **authorization** to provide services

Personal Firewalls Quiz

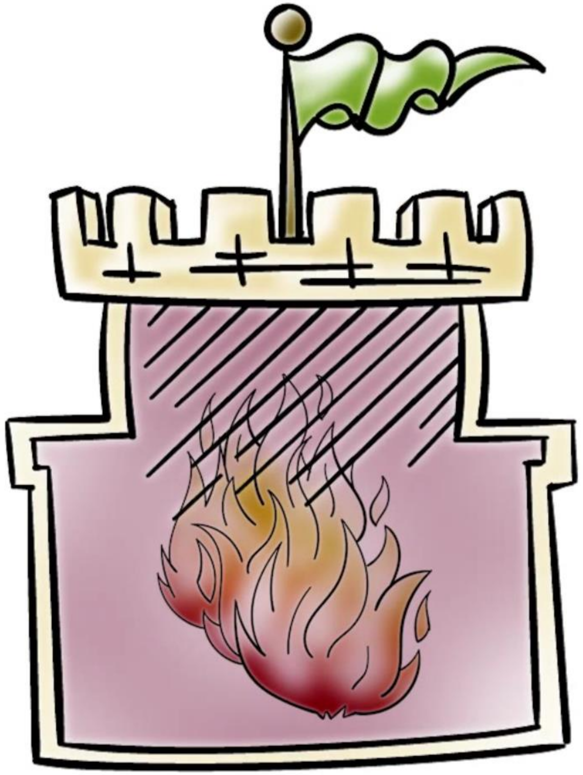
A company has a conventional firewall in place on its network. Which (if any) of these situations requires an additional personal firewall?

- □ An employee uses a laptop on the company network and at home.
- □ An employee uses a desktop on the company network to access websites worldwide
- □ A remote employee uses a desktop to create a VPN on the company’s secure network.
- □ None of the above, in each case the employee’s computer is protected by the company firewall.

Deploying Firewalls



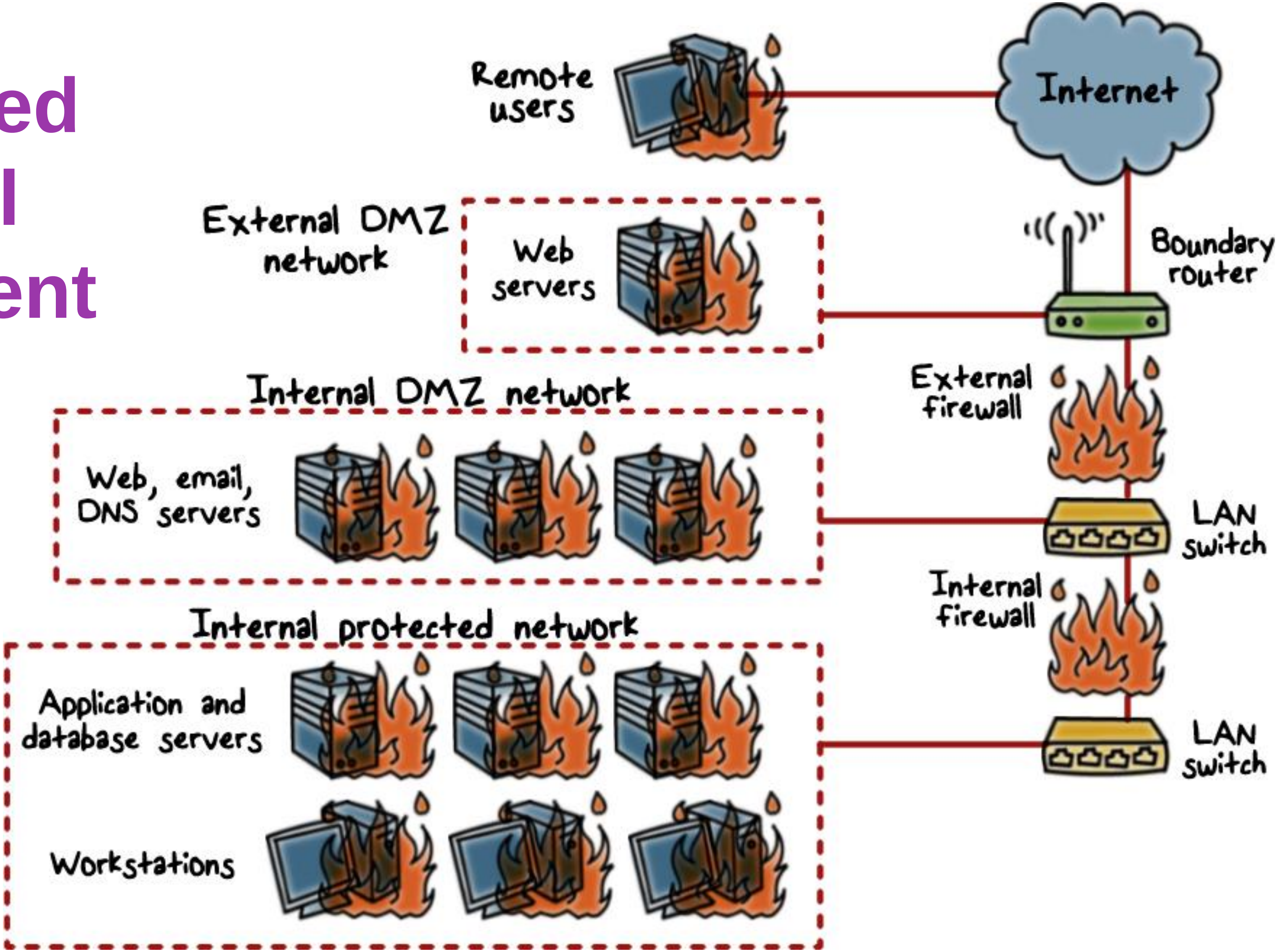
Internal Firewalls



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

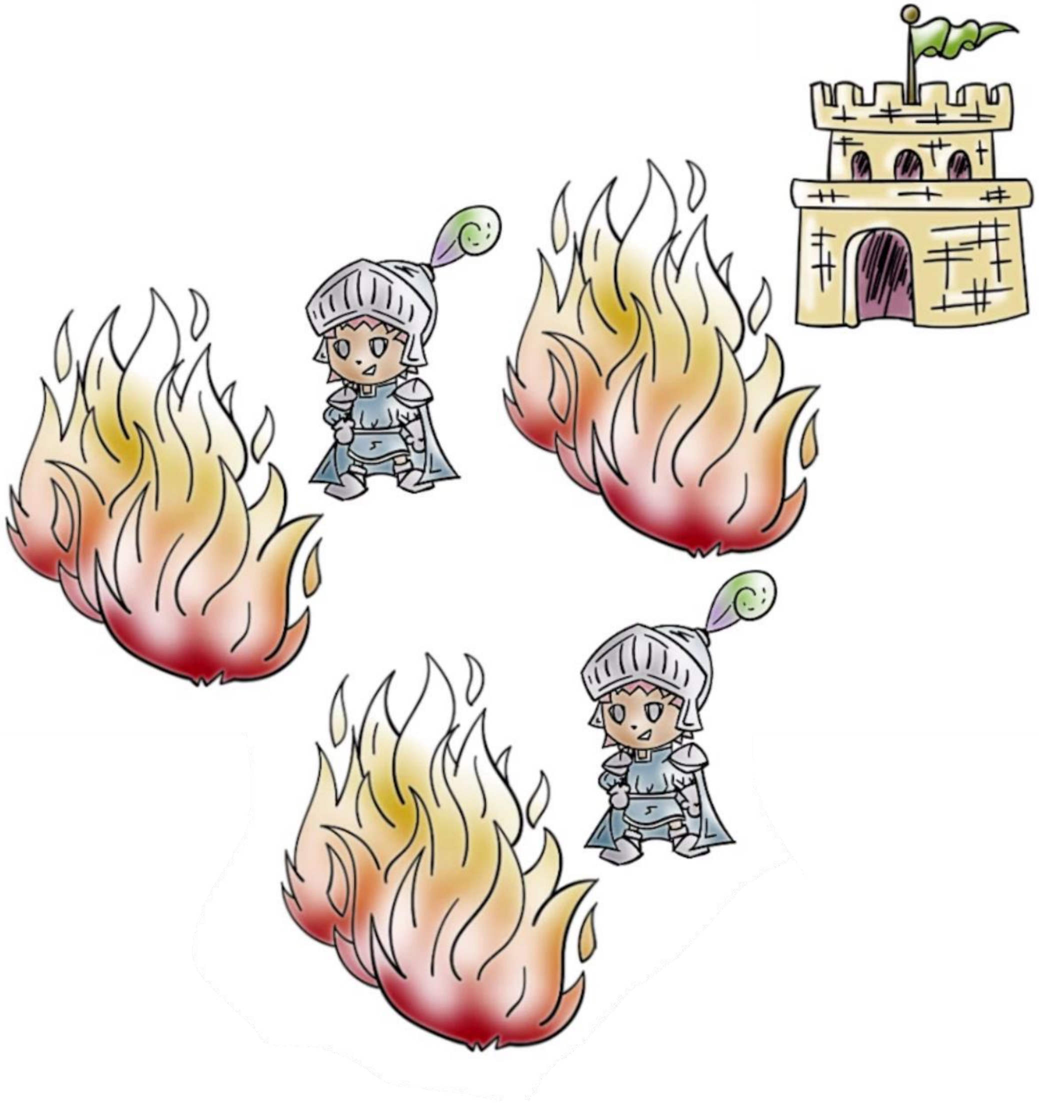


Distributed Firewall Deployment

An important aspect of distribu

firewall configuration:

- **Security Monitoring**



Firewall Deployment Quiz

Choose the most correct answer and enter the corresponding letter in the text box.

Typically the systems in the □ require or foster external connectivity such as a corporate Web site, an e-mail server, or a DNS server.

A. DMZ

B. IP protocol field

C. boundary firewall

D. VPN

Stand-alone Firewall Quiz

Choose the most correct answer and enter the corresponding letter in the text box.

A □ configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.

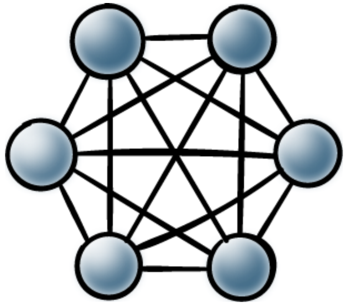
A. packet filtering firewall

B. distributed firewall

C. personal firewall

D. stateful inspection firewall

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