Network Security (contd)

Exercise

- Using what we learned previously, determine the following:
  - What is the IP address of caslab.case.edu?
  - What ports are open on caslab.case.edu?
  - What versions of software *may* be running on caslab.case.edu?
    - If nmap does not work, can you do something else?
  - Do a search on the following: "xz utils vulnerability"
    - Click on the ars technica article that appears at the top
    - Read about the vulnerability and what services it affects (one service you installed)
      - Run the following: apt-cache policy xz-utils
      - Is your VM vulnerable to this particular vulnerability?

Recap

- OSI Model
- Packets
- Internet / Network Layer
  - IP address
- Transport Layer
  - Reliable / Unreliable communication with TCP or UDP
- Systems can be attacked using network protocols
  - TCP SYN flood
  - Spoof IP
- Systems can be scanned for open ports and vulnerabilities
  - Tools such as nmap

Domain Network Services (DNS)

- Exist within Application Layer, but plays critical role in Internet Layer
- Both a Protocol and a System
- Listens on Port 53
- System is made of hierarchy of DNS servers
- Hierarchy is based on authority
- Request are made over UDP
- Server has records
- Name → IP and IP → Name
- Why DNS? Do you know the IP to case.edu?

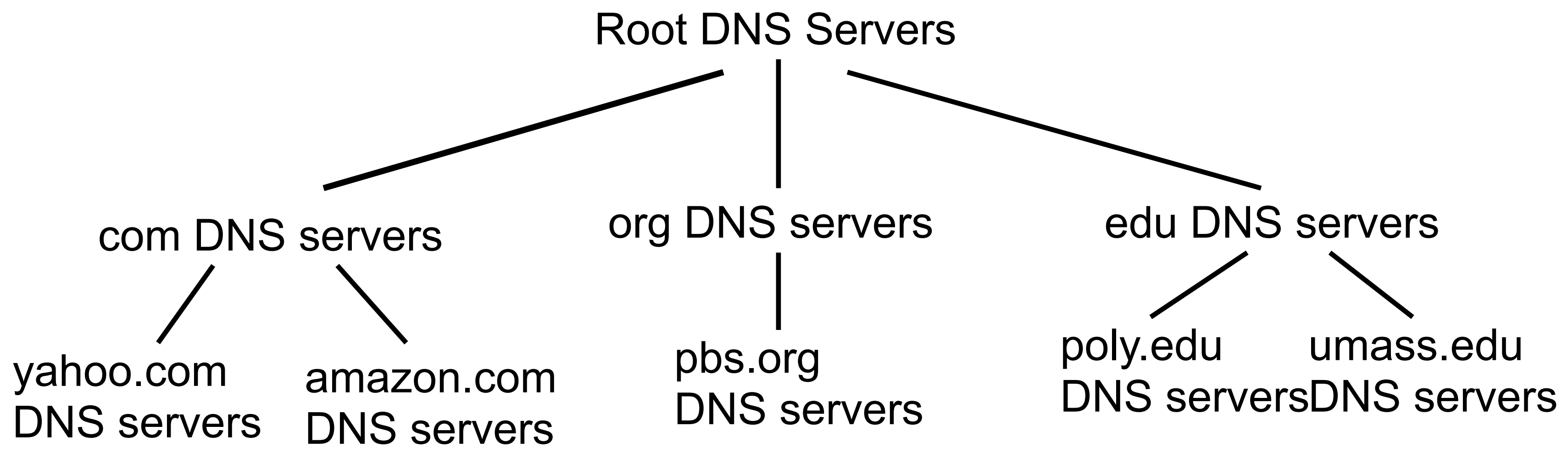
DNS Exercise

- host google.com
- dig google.com

- Get IP for google.com and put in browser, what do you see?

DNS Hierarchy

- Every publicly facing site must provide an authoritative DNS server
- This server provides names/IPs for systems within domain
- Also provides what the mail server is for email
- ISPs have their own DNS server
- DNS also provides load balancing and caching
- How to get answer?
  - Iterative
  - Client makes request to a DNS server
  - If that DNS server doesn’t have answer, it returns to the client next server to ask
  - Client asks next server and repeats this process until it gets answer

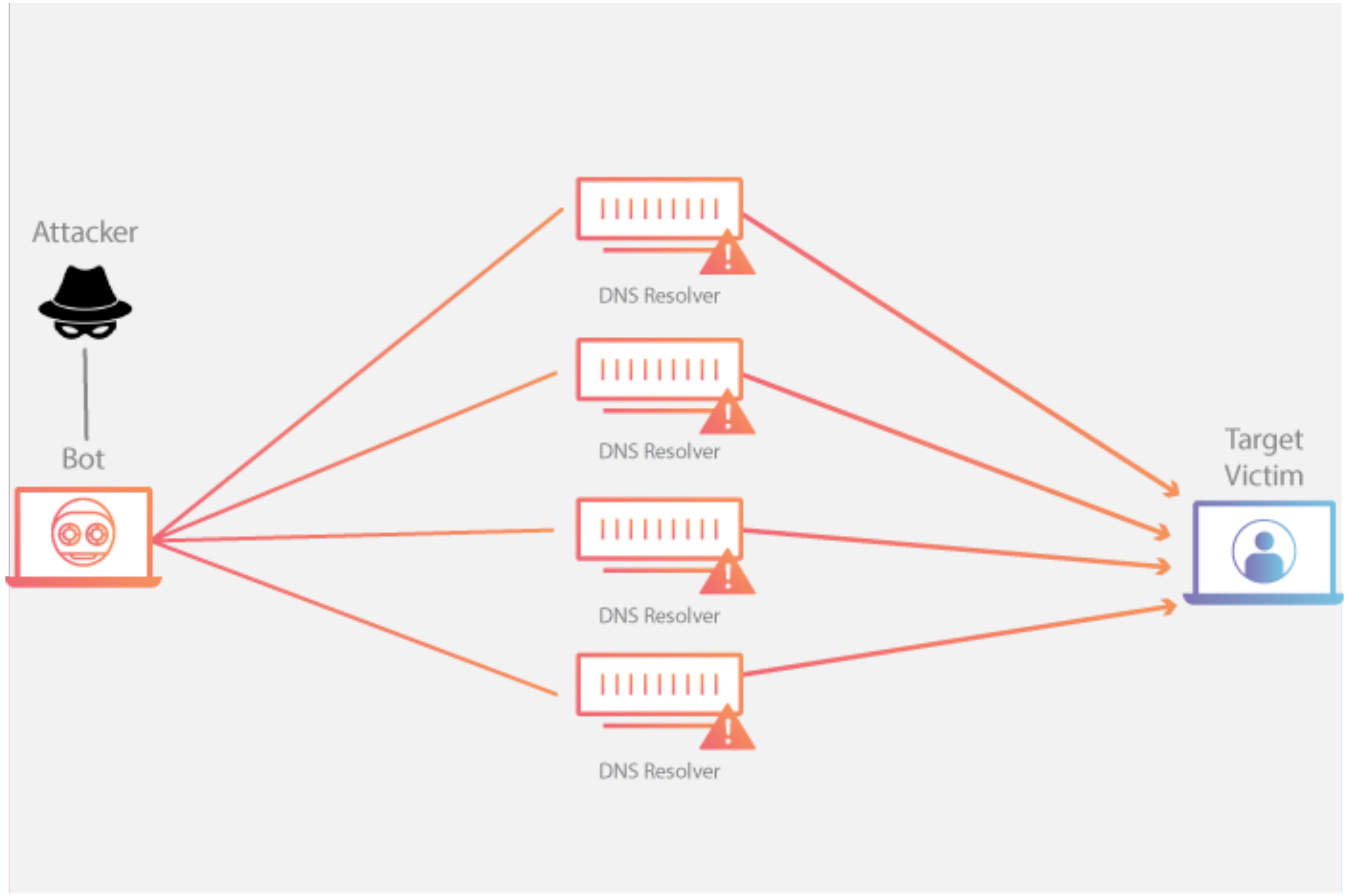


DNSSEC

- Cryptographic signatures added to DNS records
- Can verify domain name comes from authoritative server
  - Prevent response form a rogue server
- Keys used to generate digital signature, public and private key pair
  - Public key is published
- To work, it needs to have widespread adoption
  - Has received criticism
- https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

Attacking DNS

- Similar to UDP and TCP Attacks
- Ask DNS server for ANY result
- DNS resolver essentially attacks victim with response
- https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/



Cloudflare

IP Troubleshooting and Discovery

- Various tools to troubleshoot network
  - ping hostname|ip
- Can find route on network:
  - tcptraceroute hostname|ip
- Can find out who owns network:
  - whois.com
- Can connect to service
  - nc host port

Exercise - Using whois and dig

- Using whois.com ...
  - Who owns case.edu?
  - When does the domain expire?
  - Who is the admin contact?
  - How could this information help an attacker?
  - What is one of the DNS servers listed?
  - Try to query one of those DNS servers directly using dig:
    - dig @someserver sis.case.edu
    - Add ANY to the end of your query, what do you see?

Exercise - Using netcat (nc) and ping

- Run the following: nc www.case.edu 80
  - Then type in the following two lines, and then hit enter twice very quickly:
    - GET / HTTP/1.1
    - Host: www.case.edu
  - What do you see?
- Run the following:
  - ping ns.cwru.edu - What do you get?
  - ping ns4.oar.net - What do you get?

Routers vs Switches

- Routers make up Internet core
  - Determine where to send packets based on routing information
  - Various algorithms to determine best route (OSPF, Djikstra’s)
  - Use IP Address and traffic data
- Switches used for local network
  - Determine where to send with locally connected computers
  - No algorithm needed, computer has direct connection
  - Use Mac Address

Datalink Layer

- Focuses on transmitting packets within network
- Use a different address: MAC Address
    - Each address unique to network card
    - Address can be "cloned"

Exercise - Datalink

- Run the following:
  - ip addr
    - What is your MAC address? What encoding does it use?
    - Take note of it
  - arp -a
    - Try on the VM and your laptop
    - Do you see anything interesting on your VM?
    - What about your laptop?

Ethernet

- Protocol responsible for transmitting on a network
- Network used to use shared line
- Had to "listen" for communication before sending
- After sending, had to wait to hear if collision
- Do we used a shared line today in networking?

Ethernet Attacks - MAC Flooding

- Main idea:
  - Send fake data packets to a switch
  - Flood the switch so table fills
  - Goal is that every packet coming in gets sent to all devices in "fail-open mode"
  - https://nordvpn.com/blog/mac-flooding/

Recap

- Many different protocols and layers allow Internet and Networks to function
- Some ensure packet gets to a destination
- Some ensure packets arrive in order
- Some ensure systems can get an IP address
- Some ensure that we don’t have to remember IP address
- Important to divide components into layers, responsibilities are clear
- Many protocols and services can be attacked though
- Routers, switches, hosts need to be able to detect and respond to these attacks

Network Security Devices

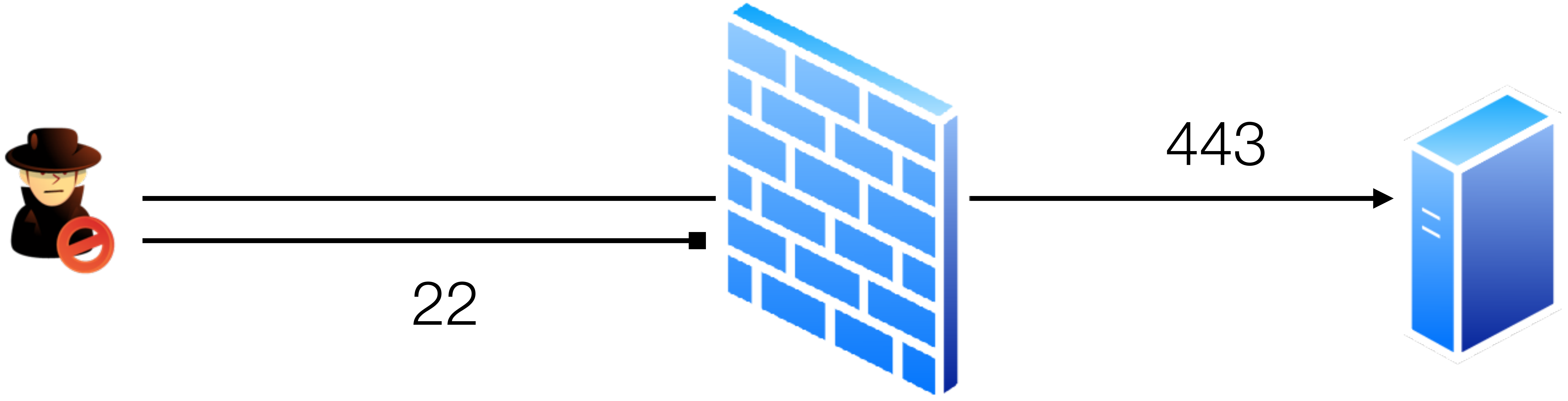
- Several devices that can help secure a network
- Some of these are software based as well
- Follow principle of defense in depth

Firewalls

- Placed at point where level of trust changes
- Block IPs and/or ports
- Network based and host-based firewalls
- Home router acts as a firewall
- Various types:
  - Packet Filter
  - Stateful Packet Inspection
  - Deep Packet Inspection

Packet Filter Firewall

- Simple solution
- Examines destination IP and port and protocol being used
- Examines one packet at a time
- More sophisticated attacks can spread an attack across multiple packets

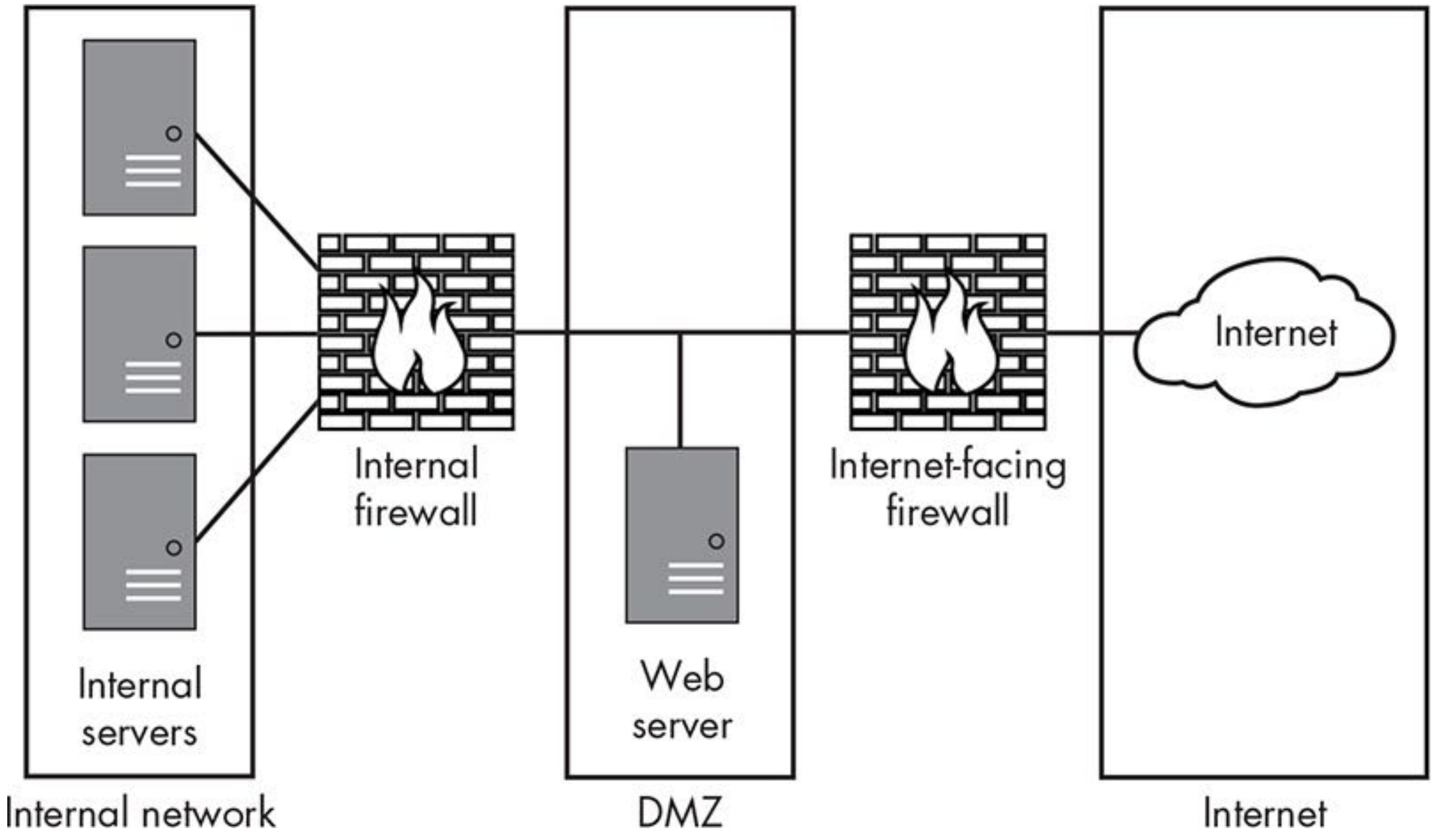


Stateful and Packet Inspection Firewall

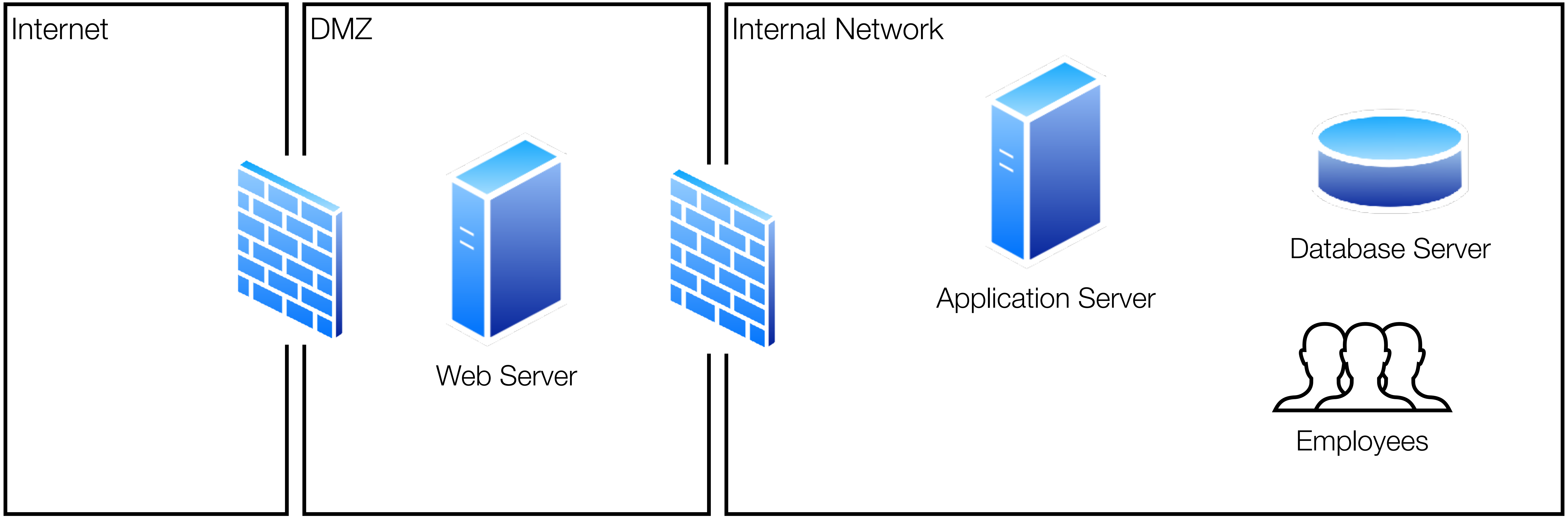
- Stateful Packet Inspection
  - Examines traffic from a connection (e.g. a TCP connection from a web browser to a web server)
    - Connection is the pairing of a source/destination IP and port combination
  - Uses a state table to keep track of connection
  - Once connection closes (TCP close) any additional traffic would need to establish a new connection using TCP
- Deep Packet Inspection
  - More complex, analyze content of traffic where others look at essentially the origin and destination
  - Privacy issues if content is opened
  - If encrypted traffic, such as TLS, not so much an issue unless proxied

Network Zoning

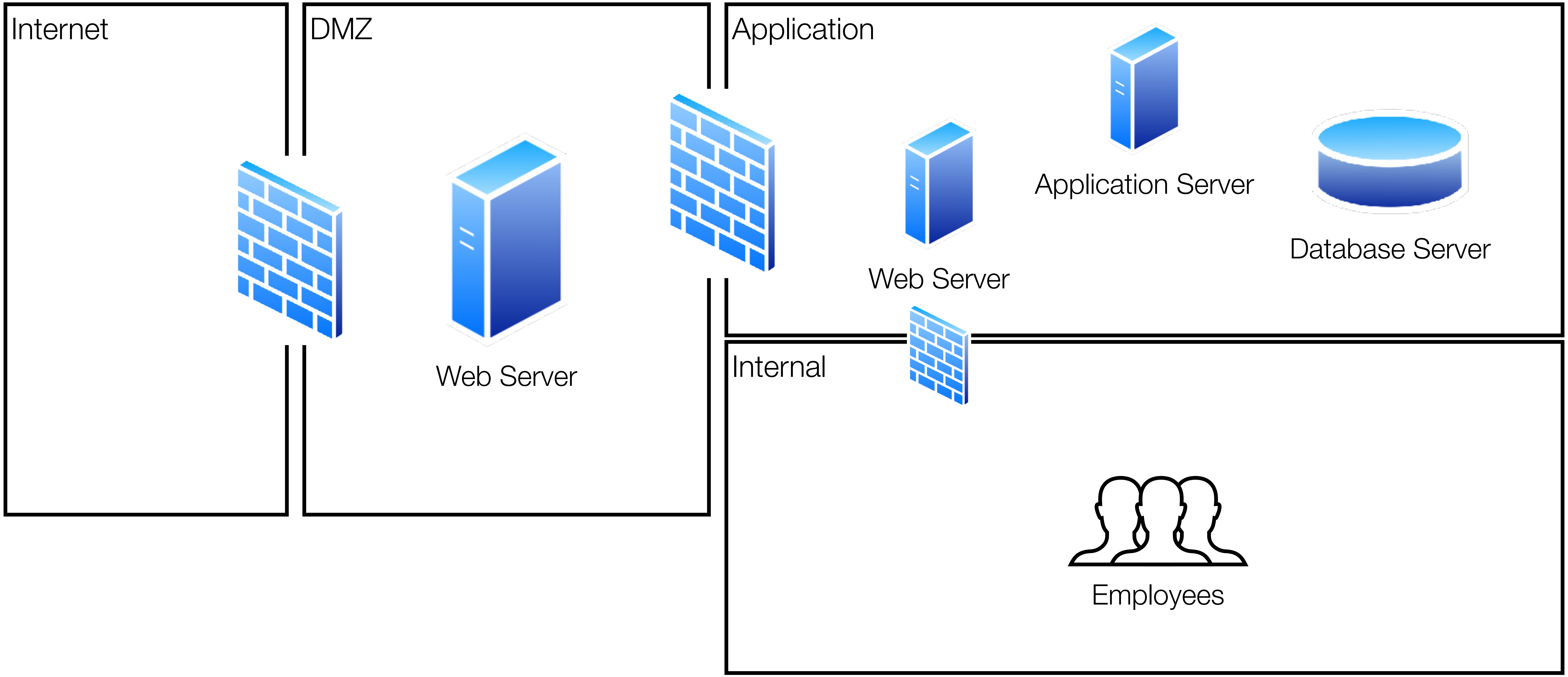
- Traffic passes through areas where trust changes
- Create network zones:
  - DMZ
  - Internal
  - Application
  - Data
  - and more ...
- Have redundancy within networks (load balancers)



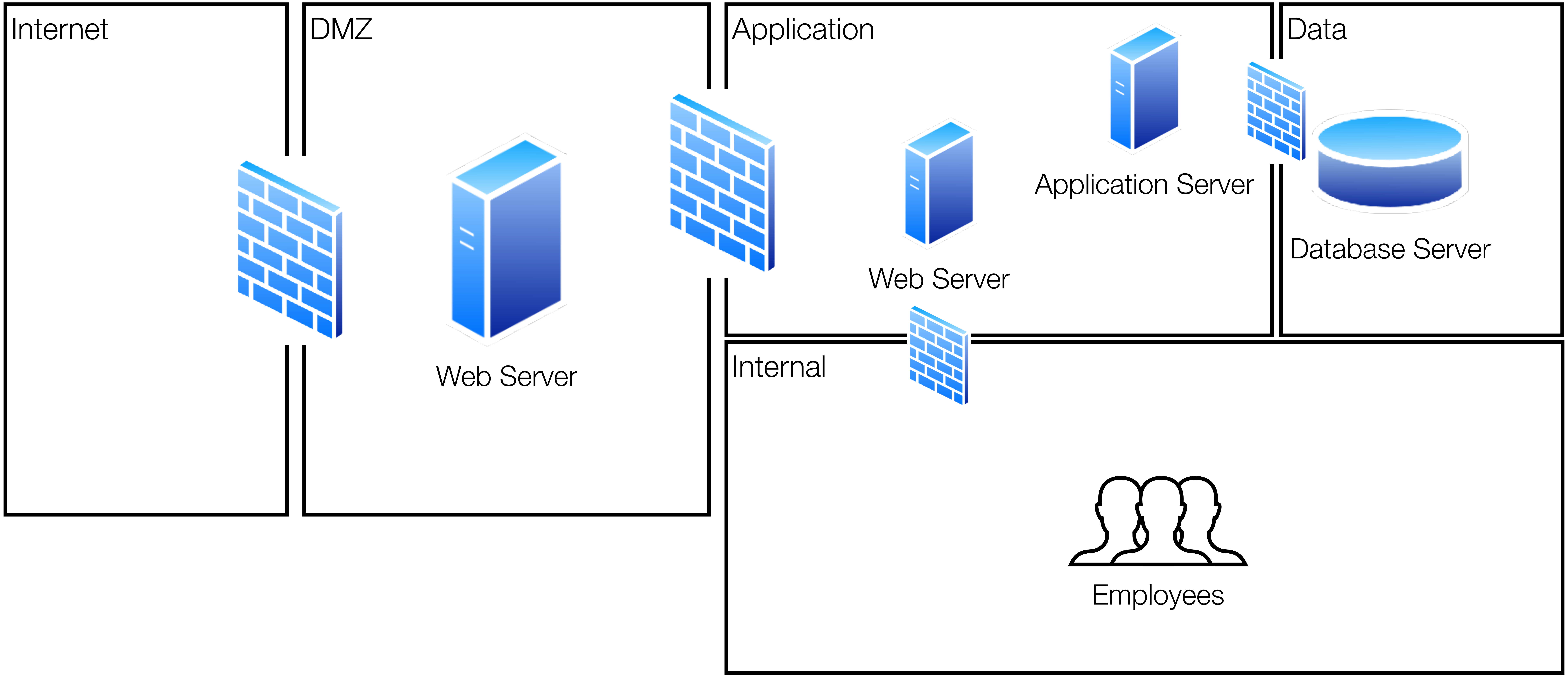
Network Zone Example - Simple



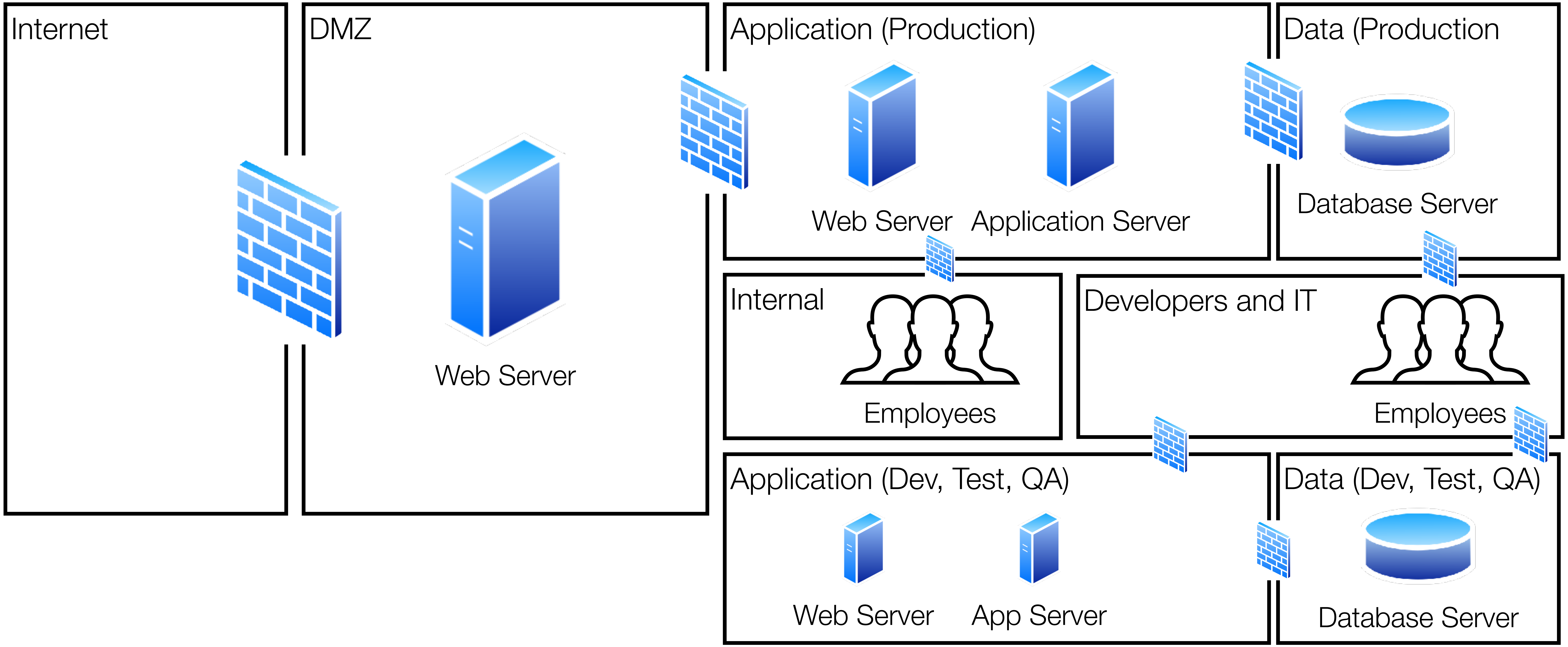
Network Zone Example - More Protection



Network Zone Example - Even More Protection



Network Zone Example - And More Protection



Proxy Server

- Used for application, example is a web proxy
- Can provide defense to application by being a reverse proxy
- Can configure in Apache web server as well
- Can be put in an external DMZ (were you have web servers in internal DMZ)

IDS

- Hardware or software
- Monitor network, hosts, applications, can determine if there is an attack based on a certain signature or anomaly
- Signature is like an antivirus
- Anomaly can be traffic or activity on the network or system
- IPS is a like an IDS, but actually prevents intrusion
  - https://www.snort.org/

Honeypot

- Attracts attackers to a system with the idea there is valuable data
- Larger group of honeypots is a honeynet
- Might implement countermeasures or traps for attackers

Network Access

- Wireless
  - Should use WPA2 or WPA3
  - Do not use WEP
  - Tools to attack wireless networks: Kismet, Aircrack-nG
- VPNs
  - Allow you to create a secure connection between two points
  - Typically used to access organization resources when offsite
  - Service used at Case is Fortinet
- Network Switches
  - Should authenticate clients connected to network
  - Do not allow anyone to access network by plugging into Ethernet
- Use Secure Protocols
  - SSH instead of Telnet
  - SFTP/SCP instead of FTP

SSH Into Server

- From terminal, run the following given your hostname:
    - ssh username@servername.local

Packet Capture - MITM

- Many popular tools out there
- Wireshark is one of the most
- Open wireshark from the terminal: sudo wireshark
    - Click on the wireshark button in the upper left
    - Type in http in the filter, open browser and type in http://caslab.case.edu
    - Type in icmp in the filter, open terminal and do a ping case.edu
- MITM - Man In The Middle
    - Capture traffic between two endpoints
    - Can modify traffic as well (we will see later with app pen testing)
    - SSH into server, you see an initial warning message

Network Security Recap

- Defense in depth - Hardware and software
- Network zones - Create areas of trust
- Authenticate nodes
- Protocols can be attacked
- IPs can be spoofed
- Close any doors that do not need to be open - Uninstall services not needed
- Use secure protocols when possible
- Important to have regular scanning of network

Quiz!

- Passcode is portscan