JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

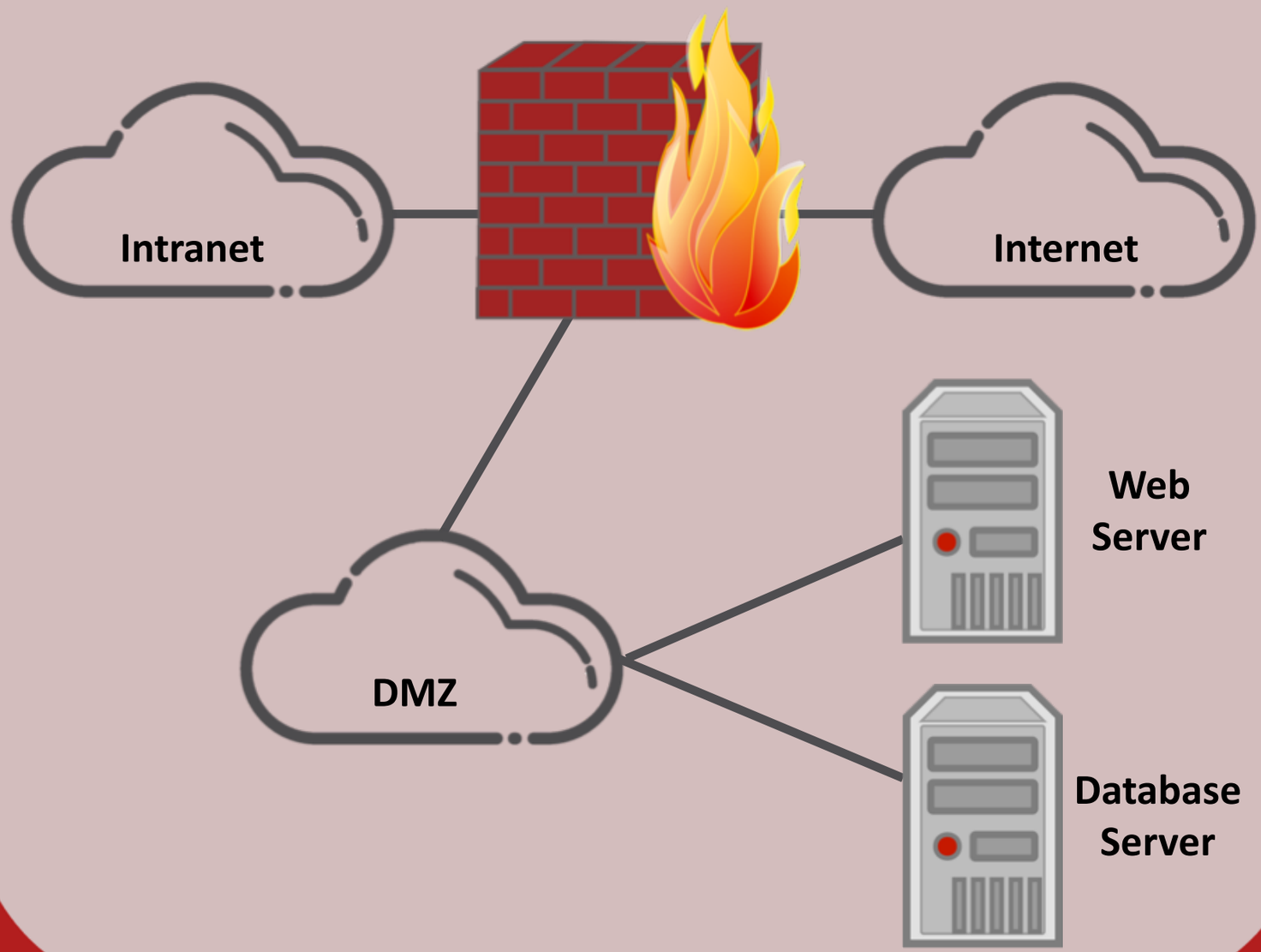
Network Perimeter Security

THREAT MANAGEMENT

Firewalls

- Most common network perimeter security
- Firewalls are at network boundaries
- Generally setup as triple-homed devices
  - Internet, DMZ, and intranet

Triple-Homed Firewalls

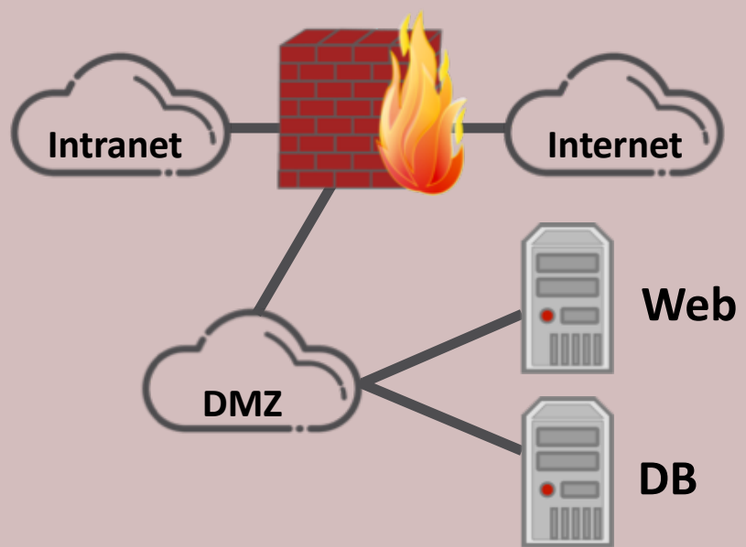


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Demilitarized Zone (DMZ)

- Special network zone hosting servers that gets traffic from the internet

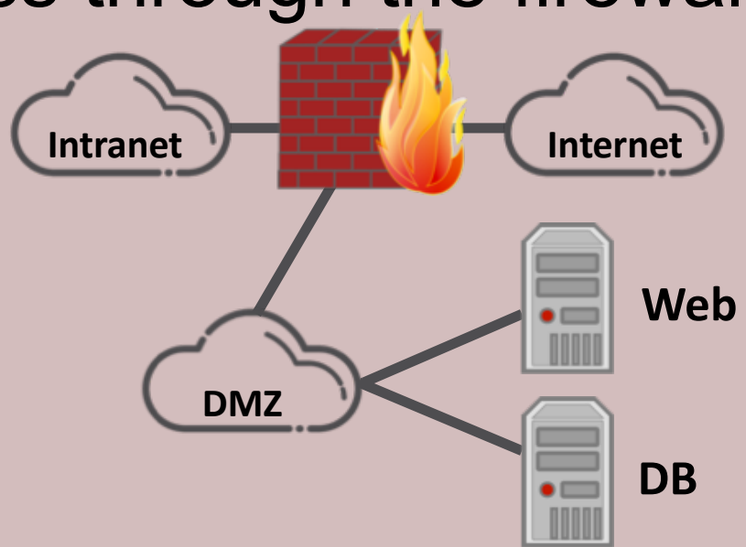
- Acts as an semi-trusted zone



Access Control List (ACL)

- All traffic passing through the firewall is checked against the ACL

- ACL contains rules to define what traffic can pass through the firewall



Access Control List (ACL)

- Firewall should be deny by default
  - If no rule says allowed, traffic is denied

Rule	SourceIP	Source port	DestIP	Dest port	Action
1	any	any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	any	any	any	Deny
3	any	any	192.168.120.1	any	Deny
4	192.168.120.0	any	any	any	Allow
5	any	any	192.168.120.2	25	Allow
6	any	any	192.168.120.3	80	Allow
7	any	any	any	any	deny

Firewall Types

- Packet Filtering
  - Check each packet against rules for IP and port
- Stateful Inspection
  - Maintains information about the state of each connection (basic firewalls sold today)
- Next-Generation (NGFWs)
  - Uses contextual information about users, apps, and processes to make decisions
- Web Application (WAFs)
  - Protects against web application attacks like SQL injection and Cross-site Scripting (SQL/XSS)

Common TCP Ports

Port	Service
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP3
123	NTP

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Common TCP Ports

Port	Service
143	IMAP
161	SNMP
389	LDAP
443	HTTPS
1433	SQL Server
1521	Oracle
1720	H.323
1723	PPTP
3389	RDP

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE