Designing the network architecture, zones, and locations for firewalls:

- External DMZ: Public servers
- Public Servers include Web Server, DNS Server, Mail Server
- The External DMZ is a dedicated space for servers that face the public, which enhances security by keeping them isolated from the internal network.

- Internal DMZ: Internal Web Server
- The Internal DMZ is a secure area that houses the internal web server, safeguarding the internal applications and data from the External DMZ.

- Trusted Zone: Database Server
- The Trusted Zone Firewall supervises traffic in between the Internal DMZ and DB
- Make sure that sensitive information can only be accessed by the web servers.

- Engineering Zone: Engineering Department
- Accounting Zone: Accounting Department and Application Server (port 3030)
- The Department Zone consists of two departments, allowing for customized security policies based on the specific requirements of each department.

Security Controls:

- Place stateful firewalls at the perimeter of the network and between segments to enforce traffic rules
- Configure the firewalls to allow the necessary traffic between segments and the Internet while denying all other traffic

External DMZ:

- Public Web Server
- DNS Server
- Mail Server
- This makes it so it is available to both internal and Internet users. The external DMZ Firewall controls access to these servers.

Internal DMZ:

- Internal Web Server, hosts internal Web app running on port 8080. This server can be accessed through the Departmental Firewall
- Database Server

Engineering Department:

- Engineering Department machines

Accounting Department:

- Accounting Department machines
- The Accounting Department application server is running on port 3030 inside the Accounting Department
- The Accounting Firewall will control access to this server
- Users inside the accounting department can only access this

Trusted Zone:

- Database Server, only accessible by public and internal web servers
- DMZ Firewall and Departmental Firewall control access to DB Server

Border Firewall:

- Between the Internet and External DMZ
- Both the Border Firewall and Department Firewalls allow users in both departments to browse ports 80 and 443. These are the Internet Ports.
- Prevents incoming connections to client machines

Internal DMZ Firewall:

- Between the External DMZ and Internal DMZ

Engineering Firewall:

- Between Internal DMZ and Engineering Zone
- Has its own dedicated firewall

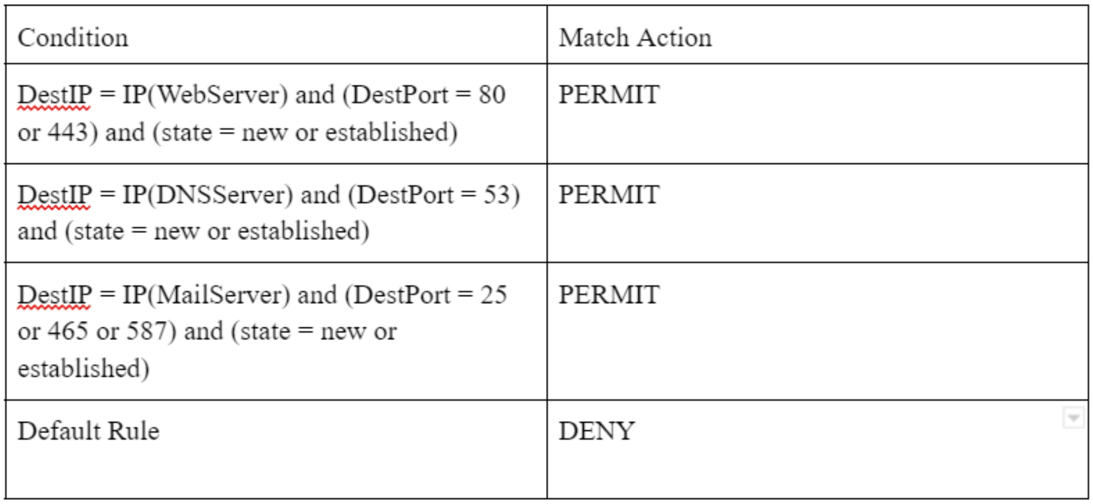
Accounting Firewall:

- Between Internal DMZ and Accounting Zone
- Has its own dedicated firewall

Firewall Rules

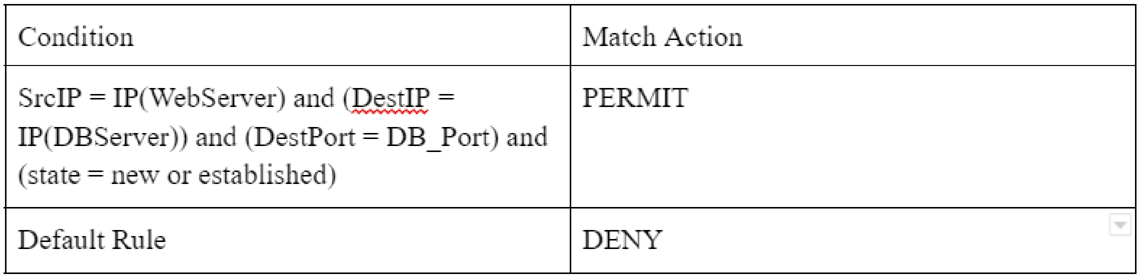
Border Firewall:

Firewall Name: Border Firewall; Interface Name: Ingress



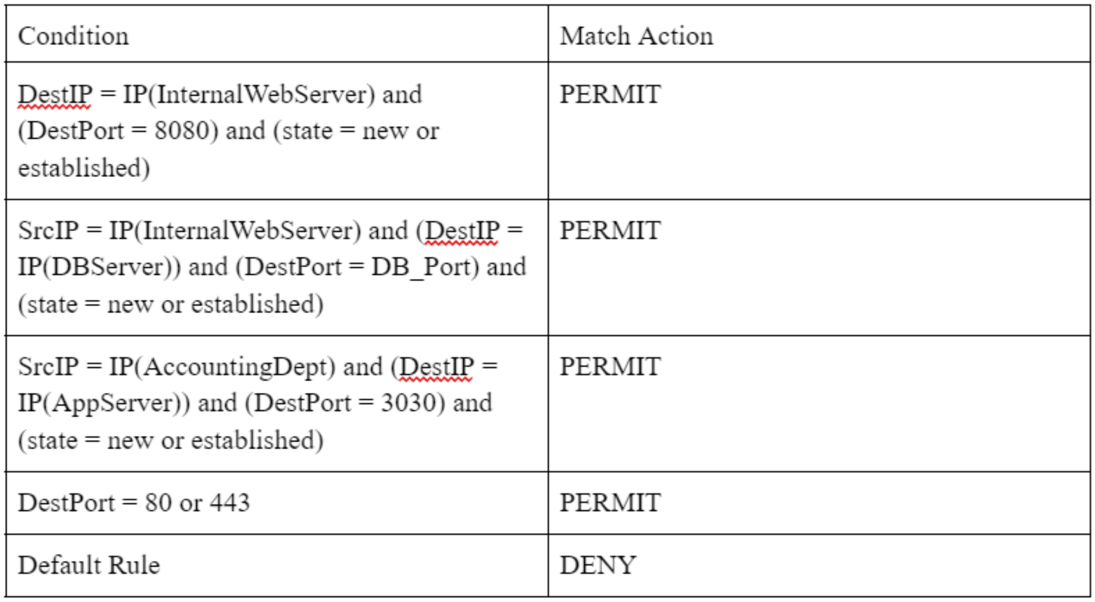
Condition	Match Action
DestIP = IP(WebServer) and (DestPort = 80 or 443) and (state = new or established)	PERMIT
DestIP = IP(DNSServer) and (DestPort = 53) and (state = new or established)	PERMIT
DestIP = IP(MailServer) and (DestPort = 25 or 465 or 587) and (state = new or established)	PERMIT
Default Rule	DENY

Firewall Name: Border Firewall; Interface Name: DMZ-egress



Condition	Match Action
SrcIP = IP(WebServer) and (DestIP = IP(DBServer)) and (DestPort = DB_Port) and (state = new or established)	PERMIT
Default Rule	DENY

Firewall Name: Border Firewall; Interface Name: Internal-egress



Condition	Match Action
DestIP = IP(InternalWebServer) and (DestPort = 8080) and (state = new or established)	PERMIT
SrcIP = IP(InternalWebServer) and (DestIP = IP(DBServer)) and (DestPort = DB_Port) and (state = new or established)	PERMIT
SrcIP = IP(AccountingDept) and (DestIP = IP(AppServer)) and (DestPort = 3030) and (state = new or established)	PERMIT
DestPort = 80 or 443	PERMIT
Default Rule	DENY

Ingress Rules:

1. Permit TCP from ANY to IP (Public Web Server) with destination port WWW or 443 [A, E]
2. Permit TCP to ANY to IP (DNS Server) with destination port DOMAIN [A,I}
3. Permit TCP from ANY to IP(Mail Server) with destination ports IMAP, SMTP, or POP3[A]
4. Deny ALL [M]

Protocol	IP Source	Port Source	IP Destination	Port Destination	Action
TCP	ANY	ANY	IP(Public Webserver)	WWW	Permit
TCP	ANY	ANY	IP(DNS Server)	DNS	Permit
TCP	ANY	ANY	IP(Mail Server)	SMTP	Permit
ICMP	ANY	N/A	ANY	N/A	Deny
ANY	ANY	ANY	ANY	ANY	Deny

Egress Rules:

1. Permit ICMP from IP(Internal DMZ) to ANY with ICMP ping requests[H]
2. Deny ALL [M]

Protocol	IP Source	Port Source	IP Destination	Port Destination	Action
ICMP	ANY	N/A	ANY	N/A	Permit
ANY	ANY	ANY	ANY	ANY	Deny

Internal DMZ Firewall:

Ingress rules:

1. Permit TCP from IP(External DMZ) to IP(Internal Web Server) with destination port 8080 [C]
2. Permit TCP from IP(Engineering Zone) to IP(Internal Web Server) with destination port 8080 [C]
3. Permit TCP from IP(Accounting Zone) to IP(Internal Web Server) with destination port 8080 [C]
4. Permit TCP from IP(Public Web Server) to IP(Database Server) with destination port DB_PORT [D]
5. Permit TCP from IP(Internal Web Server) to IP(Database Server) with destination port DB_PORT [D]
6. Deny ALL [M]

Protocol	IP Source	Port Source	IP Destination	Port Destination	Action
TCP	IP(Engineering)	ANY	IP(Internal Webserver)	8080	Permit
TCP	IP(Accounting)	ANY	IP(Internal Webserver)	8080	Permit
ANY	ANY	ANY	ANY	ANY	Deny

Egress rules:

1. Permit ICMP from IP(Internal DMZ) to ANY with ICMP ping requests [H]
2. Deny ALL [M]

Protocol	IP Source	Port Source	IP Destination	Port Destination	Action
TCP	IP(Internal Webserver)	ANY	IP(DB Server)	DB_PORT	Permit
ANY	ANY	ANY	ANY	ANY	Deny

Engineering Firewall:
Ingress rules:

1. Permit TCP from IP(Internal DMZ) to IP(Engineering Zone) with destination port WWW or 443 [E]
2. Deny ALL [M]

Egress rules:

1. Permit ICMP from IP(Engineering Zone) to ANY with ICMP ping requests [H]
2. Deny ALL [M]
3. Accounting Firewall

Accounting Firewall:
Ingress rules:

1. Permit TCP from IP(Internal DMZ) to IP(Accounting Zone) with destination port WWW or 443 [E]
2. Permit TCP from IP(Accounting Zone) to IP(Application Server) with destination port 3030 [G]
3. Deny ALL [M]

Egress rules:

1. Permit ICMP from IP(Accounting Zone) to ANY with ICMP ping requests [H]
2. Deny ALL [M]

External DMZ:

Ingress Rules:

- Permit TCP from IP(Internet) to IP(Public Web Server) with destination port WWW or 443 [E]
- Permit TCP from IP(Internet) to IP(DNS Server) with destination port 53 [E]
- Permit TCP from IP(Internet) to IP(Mail Server) with destination port 25, 110, 143, 465, 587, 993, 995 [E]
- Permit TCP from IP(Internet) to IP(External DMZ Firewall) with destination port 80, 443, 53, 25, 110, 143, 465, 587, 993, 995 [E]
- Deny ALL [M]

Egress Rules:

- Permit TCP from IP(Public Web Server) to IP(Internet) with destination port WWW or 443 [E]
- Permit TCP from IP(DNS Server) to IP(Internet) with destination port 53 [E]
- Permit TCP from IP(Mail Server) to IP(Internet) with destination port 25, 110, 143, 465, 587, 993, 995 [E]
- Permit TCP from IP(External DMZ Firewall) to IP(Internet) with destination port 80, 443, 53, 25, 110, 143, 465, 587, 993, 995 [E]
- Deny ALL [M]

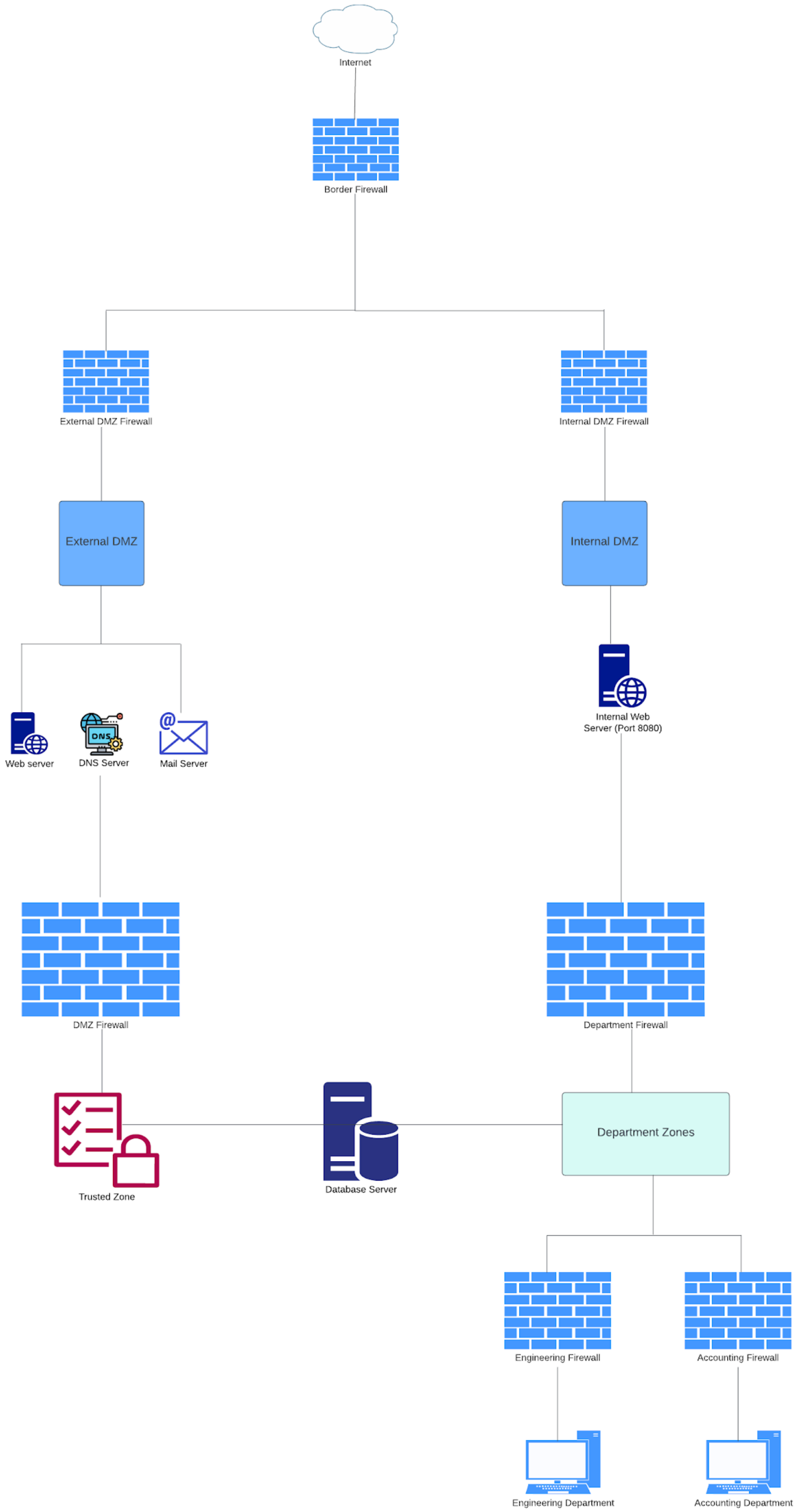
Analysis:

This network architecture and firewall rules cover the security policies (A to N). It includes separate zones for each department, an external DMZ for public servers, and an internal DMZ for the internal Web Server and Database Server. The firewall rules are designed to follow the least privilege principle and fail-safe default principle.

To ensure proper security, the network architecture includes a border firewall with three interfaces: Ingress, DMZ-egress, and Internal-egress. The Ingress interface is connected to the Internet, the DMZ-egress interface is connected to the external DMZ, and the Internal-egress interface is connected to the internal network. Each interface requires specific rules to control the flow of traffic and to ensure proper security

Down below is a schema of the network architecture visualized, drawn and designed in LucidChart.

Network Diagram


Internet
Border Firewall
External DMZ Firewall
Internal DMZ Firewall
External DMZ
Internal DMZ
Web server
DNS
DNS Server
@
Mail Server
Internal Web Server (Port 8080)
DMZ Firewall
Department Firewall
Trusted Zone
Database Server
Department Zones
Engineering Firewall
Accounting Firewall
Engineering Department
Accounting Department