Firewalls explained

04 February 2024 12:17

IPS, IDS and Firewall — Three major "NETSEC" components. (Chapter 9 of the book)

What is IPS? — Net. Security

Firewall — What is a firewall — controls the incoming and outgoing traffic

Inbound — Into the network — What is the use of —

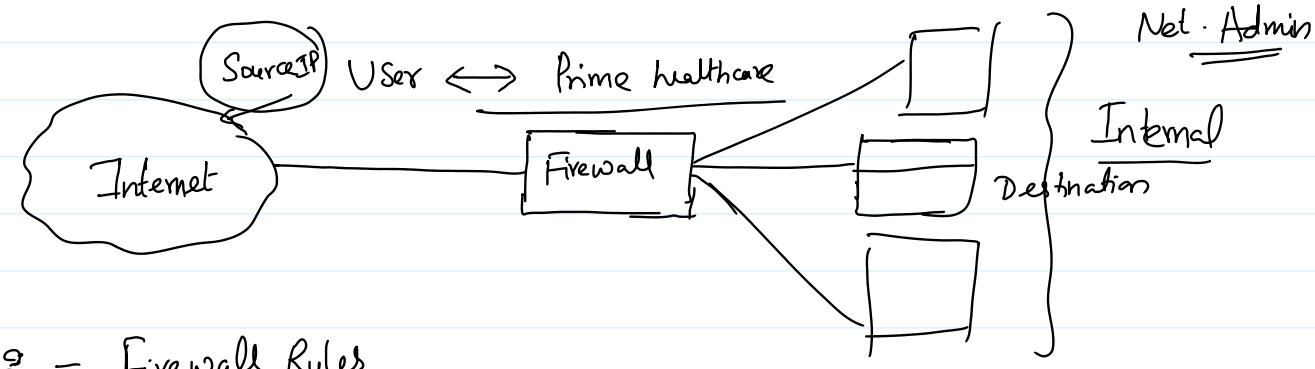
outbound — outside the network — Firewall ⟹ Prevent unauthorized packets from entering or exiting the network

The rules are called "Firewall Rules" = which packets to allow = to block

1) IP address ← Source and destination IP address
2) Port Number
3) Protocol ⟹ Connected / Related

Firewall decides ⟷

Firewall Rules — Conf by Net. Admin



Packet? — Firewall Rules

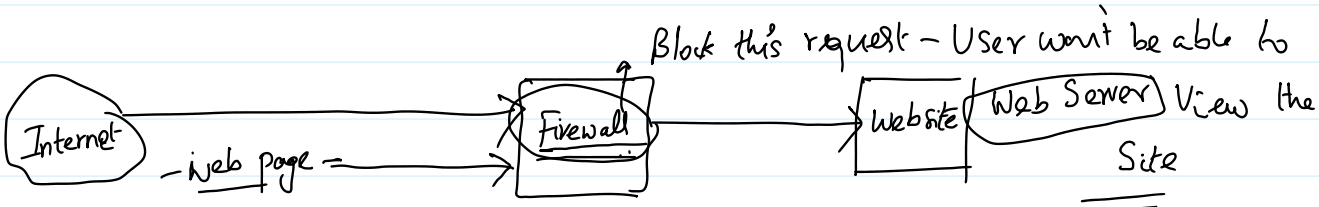
	Source IP	Destination IP	Port	Protocol	Action
1)	25.25.25.25 External	192.168.1.5 Internal	2533	TCP ⟷	Allow / Deny?
2)	25.25.25.25 External	192.168.0.8 Internal	25	SMTP Mail	Allow / Deny?

Action — Allow / Deny ⟺ Block

Default action — {Allow all / Block all}

Rules - Firewall Rules — Which packets to allow and packets to block

No rules configured — Default Rule — To block all traffic



{ Protocol : HTTP
Port : 80 } Allow all traffic from the internet
protocol : HTTP port : 80

Relaxation

Source IP	Destination IP	Protocol	Port	Action
Any External IP	IP of Web Server	HTTP	80 (X)	Allow
Any External IP	IP of Web Server	HTTPS	443 (X)	Allow

HTTP : 80

25.25.25.25 ⟷ 192.168.0.8 : 80 — Allow
Web Site

— Port doesn't match —

25.25.25.25 — 192.168.0.8 : 8080 — { Deny access }

	Source	Destination	Port	Protocol	Action
1	Any	Any	>1024	TCP	Deny
2	Any	Any	<1024	TCP	Allow

25.25.25.25 — 192.168.0.8 : 8080 — Deny
192.168.0.8 : 80 — Allow

Source — Destination

192.168.0.8 — 25.25.25.25 : 8080 — Denied | Blocked.

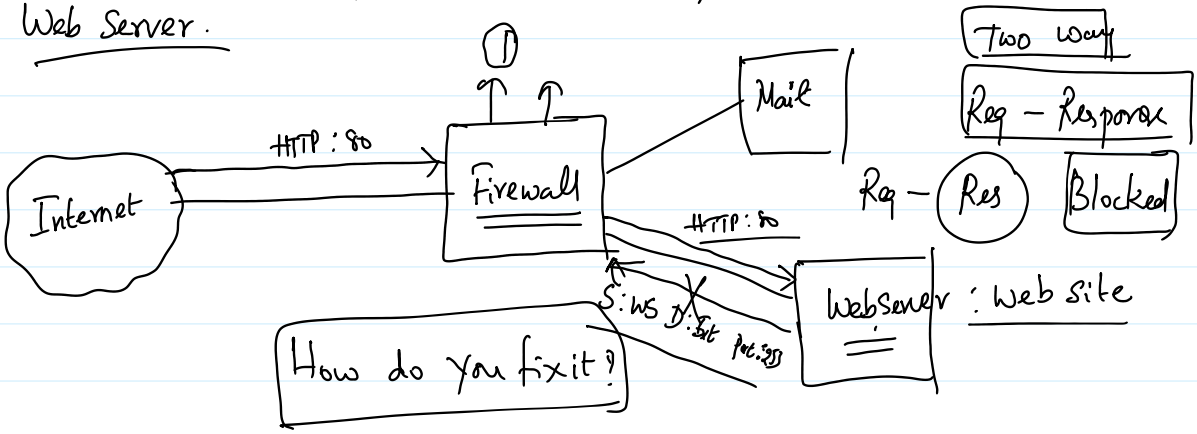
Source — Destination

192.168.0.8 — 25.25.25.25 : 8080 — Denied / Blocked.

Packet - filtering firewall - Filtering the net. packets based on IP, and ports Address

↑ Publicaccess -

Scenario: You want allow (People) to accen your mail Server and Web Server.



	Source	Destination	Port	Protocol	Action
1)	Any	IP of Email Server	25	SMTP	Allow
2)	Any	IP of Web Server	80	HTTP	Allow
3)	Any	IP of WS	443	HTTPS	Allow
4)	IP of email Server	Any	>1024	SMTP	Allow
5)	IP of WS	Any	>1024	HTTP, HTTPS	{ Allow }

Stateless Firewall - Doesn't keep track of any State information

Stateful Firewall - Keeps track of state of the packets

{ keep track of session information }

25.25.25.25 — 192.168.0.8 ; (443) ↔ Session - TLS

(HTTPS Server) (TLS handshake) Keep track

HTTPS (TLS handshake) Keep track

Server)

State of the packets

Inspect ↔ Keep track → Data inside the packets

TLS

Transport layer headers

Lower level headers (Transport, Data)

Software

Where is firewall implemented?

- Host (computer) → Host-based Firewall
- Router → Firewall function.

Network-Based Firewall → Routers / Switches.

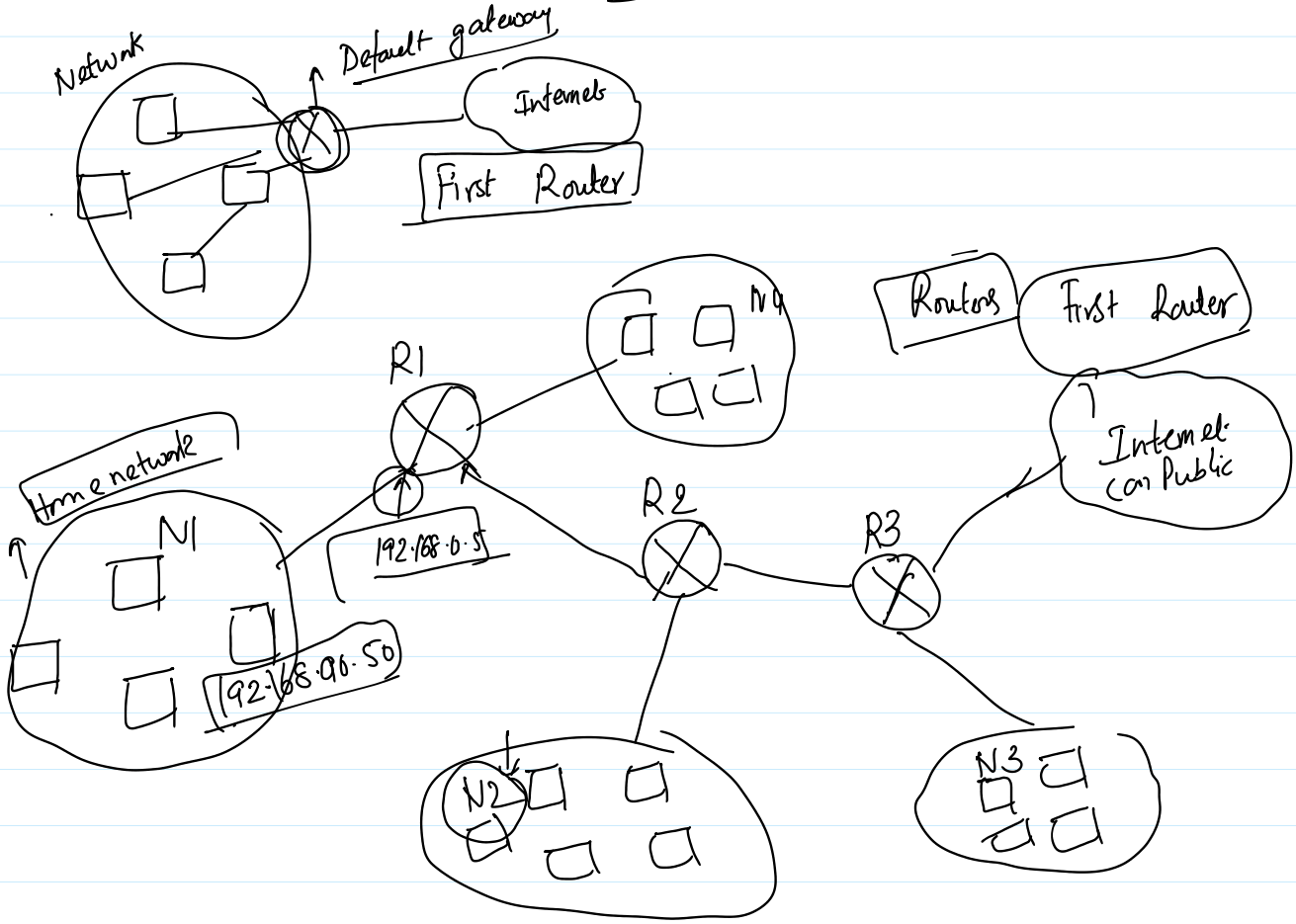
Firewall - Routers

Cisco Firewalls

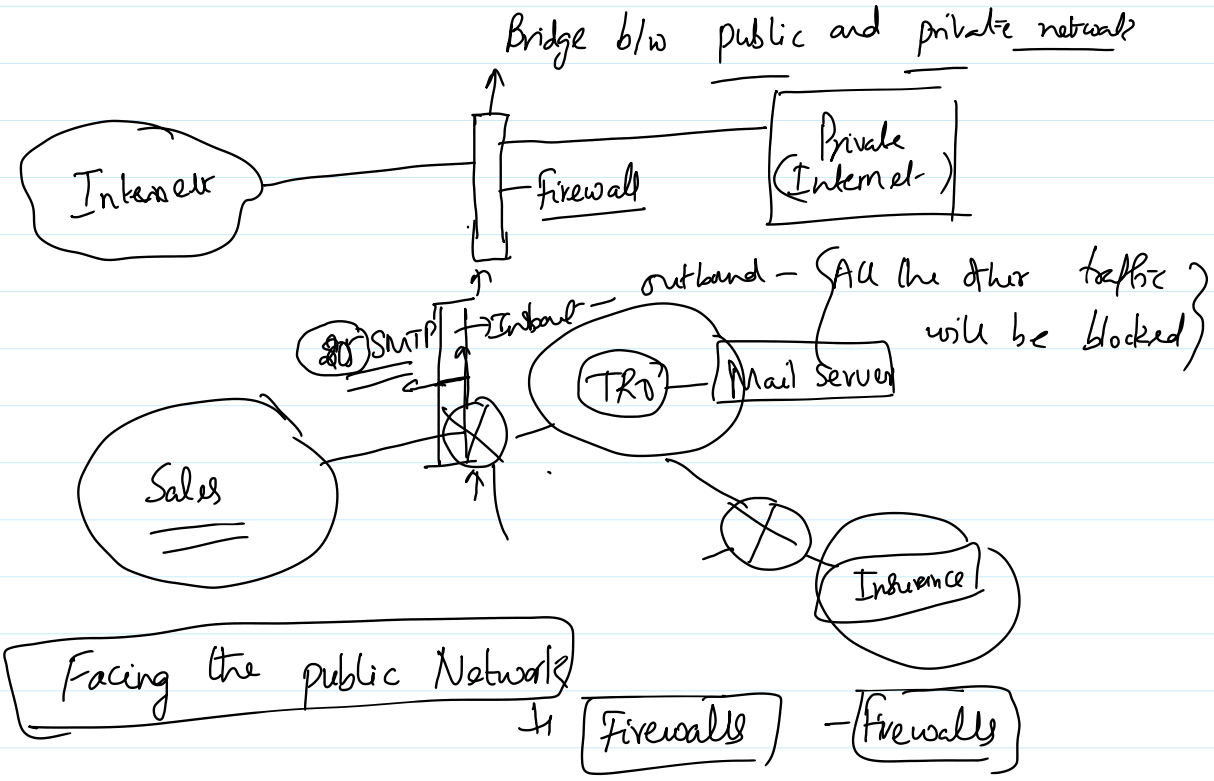
Cisco make Routers → firewalls

Default gateway - What is Def gateway?

- First exit point outside the



Where is a firewall placed within the network? (Placement of firewall)



Questions

1) What is a firewall? – A NetSec security – Monitors – Controls – Incoming and outgoing traffic

2) Purpose of a firewall – Prevention of unauthorized or malicious network activity.

3) What are firewall rules? – Rules on to be followed on which packets to allow or block.

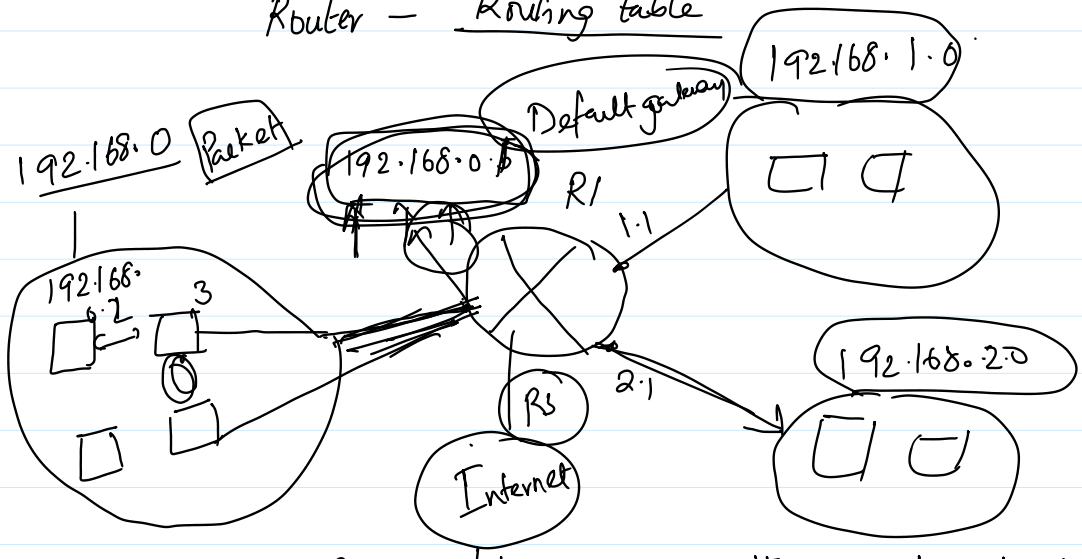
4) Types of firewalls – {Stateful, Stateless}
   - Stateful: {Inspection Firewall}

Based = Implemented – Host based (computer / Host PC)
– Network based (Routers & Switches)

5) Default gateway –

Router – Routing table

Router – Routing table



Routing table – where the packet should be routed

Route → Default gateway

Source	Destination	Route
192.168.0.2	192.168.2