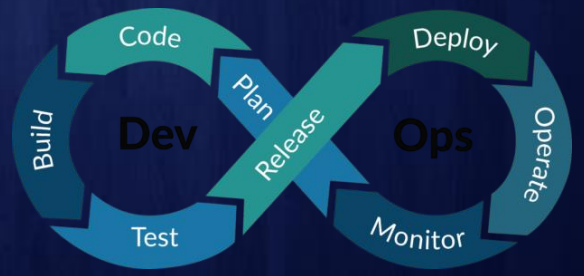
AWS SAA + SysOps + Developer + DevOps Course #Day-18

We will start at 8 AM,
Stay tuned



RAKESH TANINKI
LEARN TO UNLEARN

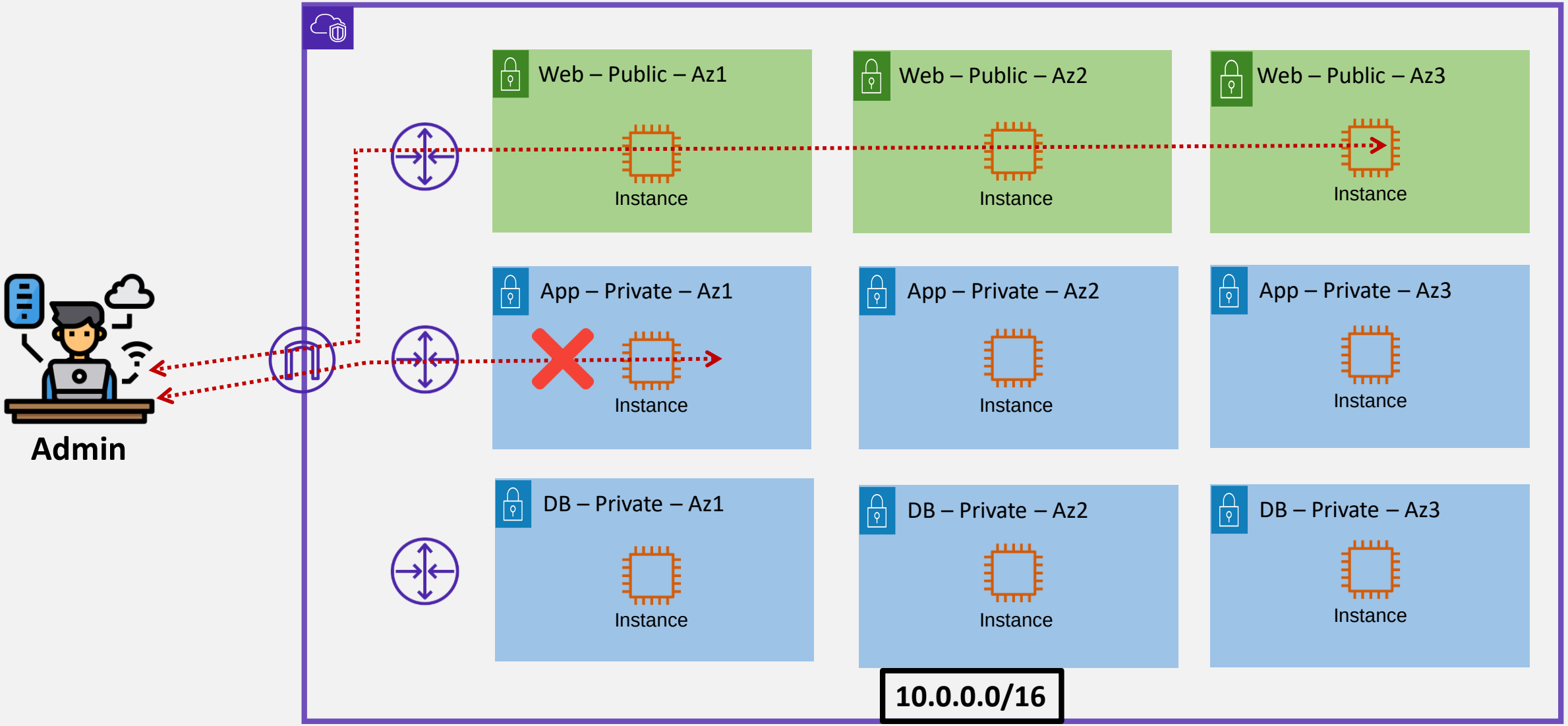
Recap:

- VPC Advanced
  - VPC Sizing
  - Subnet Sizing
  - Internet Gateway
  - Route Tables
  - Custom VPC Demo
  - Security Group Rules Demo
  - Route Tables Demo

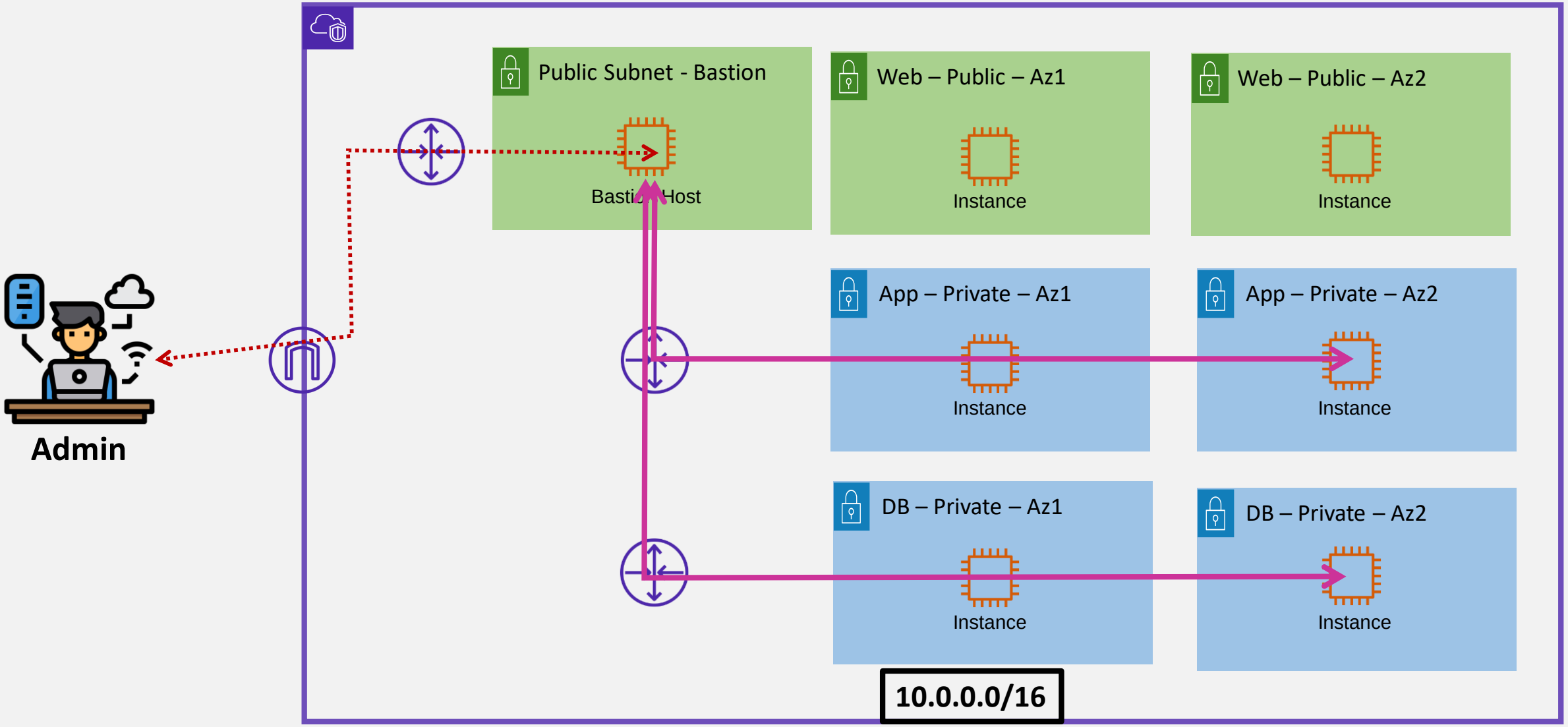
Today's topics:

- VPC Advanced
  - Bastion host / Jump box
  - Stateful vs stateless firewalls
  - Security Groups
  - Network Access Control Lists (NACL's)
  - NAT Gateway
  - NAT Gateway vs NAT Instance
- Demo
  - Jump box
  - NAT Gateway
  - NACLs
  - SGs

Bastion Host / Jump box



Bastion Host / Jump box



Entry point to connect with VPC Servers

Stateful and Stateless firewall

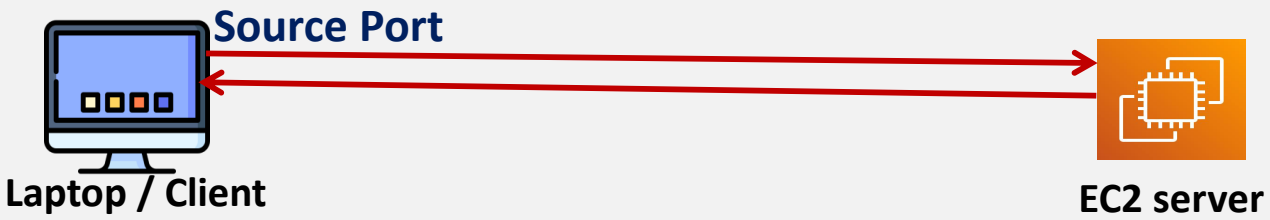
Every service is mapped with an IP and a port

3.1.5.8:80 Or 3.1.5.8:443 → http://domain.com Or https://domain.com

Stateful and Stateless firewall

Request → Destination IP + Port

Response → Destination IP + Port → Ephermal ports → 1024 - 65535



Stateless firewall

2 firewall rules are needed for inbound and outbound

Response are always comes from ephermal ports

Stateful firewall

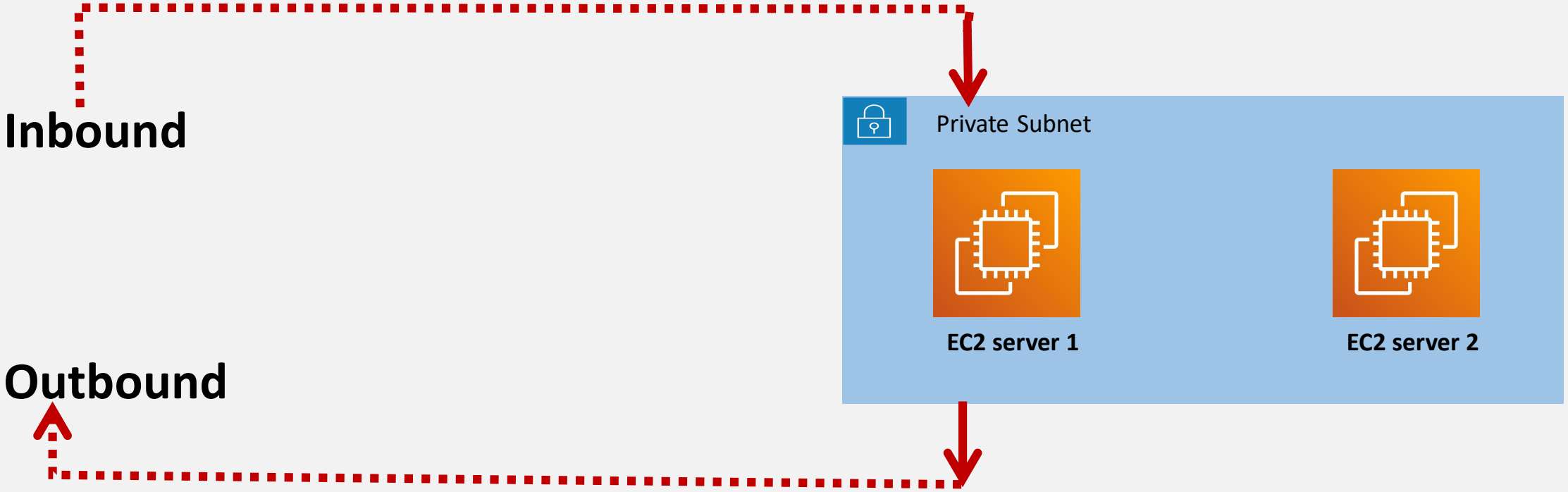
Stateful firewalls are intelligent enough to identify the request and response

If request is allowed response automatically allowed

1 firewall rule is enough for request

→ Ephermal ports are not needed to open as response is always allowed irrespective of the rules

NACL – Stateless firewall



- NACL – Network Access Control List operates at Subnet level
- Inbound and Outbound, both need to allowed
- Allow and Deny – based on the rules set
- Rules are processed by Rule Id, smaller has more priority
- Implicit deny if nothing matches

NACL – Stateless firewall (default)

Inbound rules (2)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound rules (2)

Edit outbound rules

Filter outbound rules

1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

NACL – Stateless firewall (custom)

Inbound rules (1)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound rules (1)

Edit outbound rules

Filter outbound rules

1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

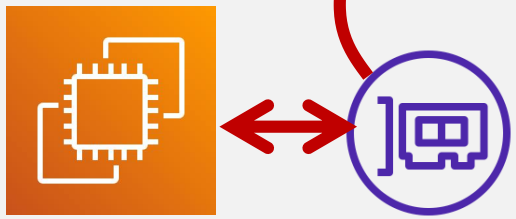
NACL – Key Points

- NACL is stateless
- Subnet level firewall
- No logical resources are allowed
- Each subnet can have only one NACL
- Use to block bad Ips / location IPs

Security Groups – Stateful firewall

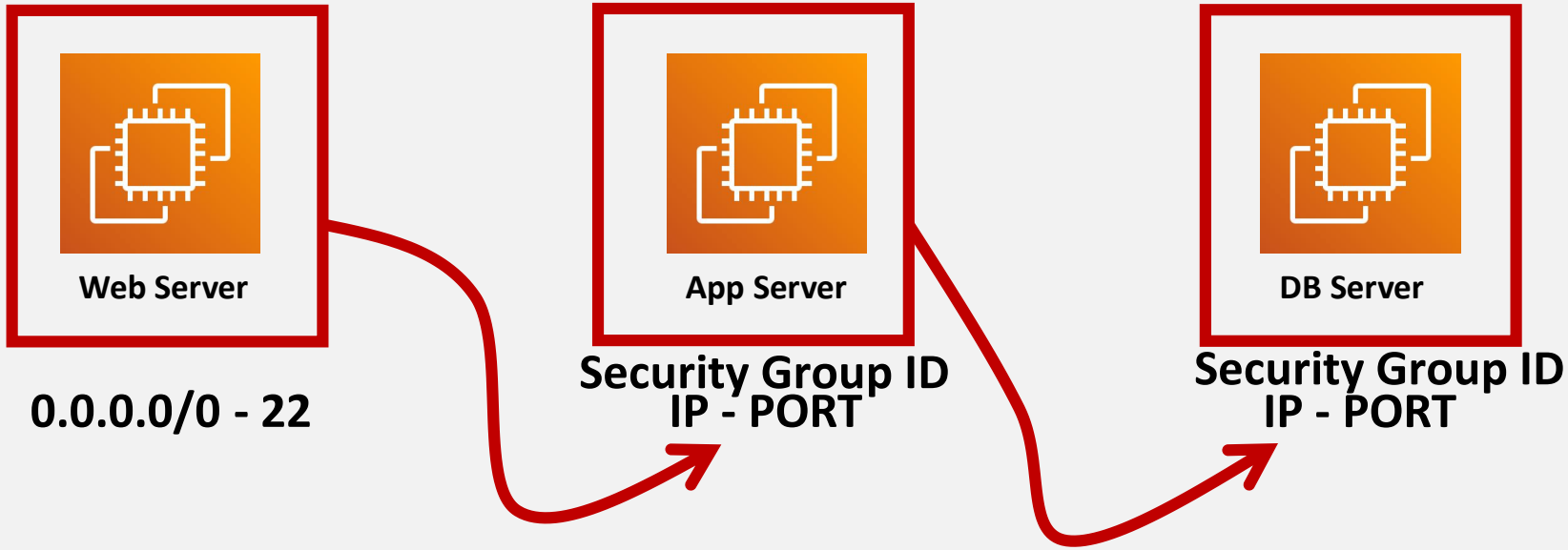
- Firewall at instance level
- Stateful – detect the response automatically
- If request is allowed – response allowed automatically
- No explicit deny
- Cannot block IP or bad acctions
- Supports AWS logical resources / IP / CIDRs
- Attached to ENI not EC2

1. Private IP
2. Public IP
3. Elastic IP
4. SGs

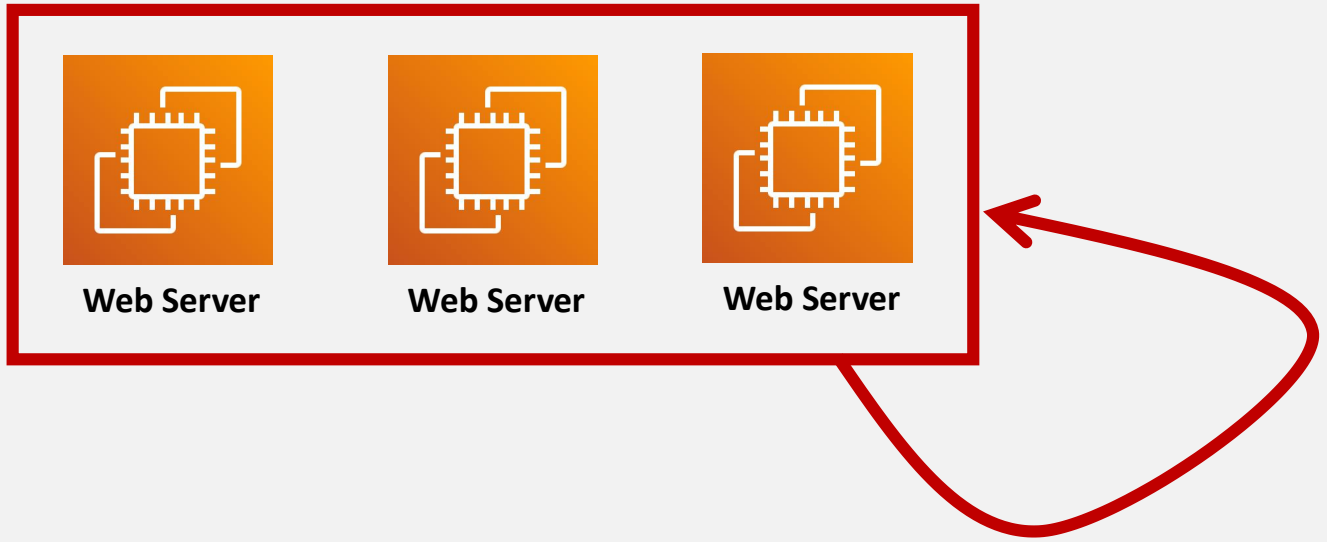


EC2 server 1

Security Groups – Logical references

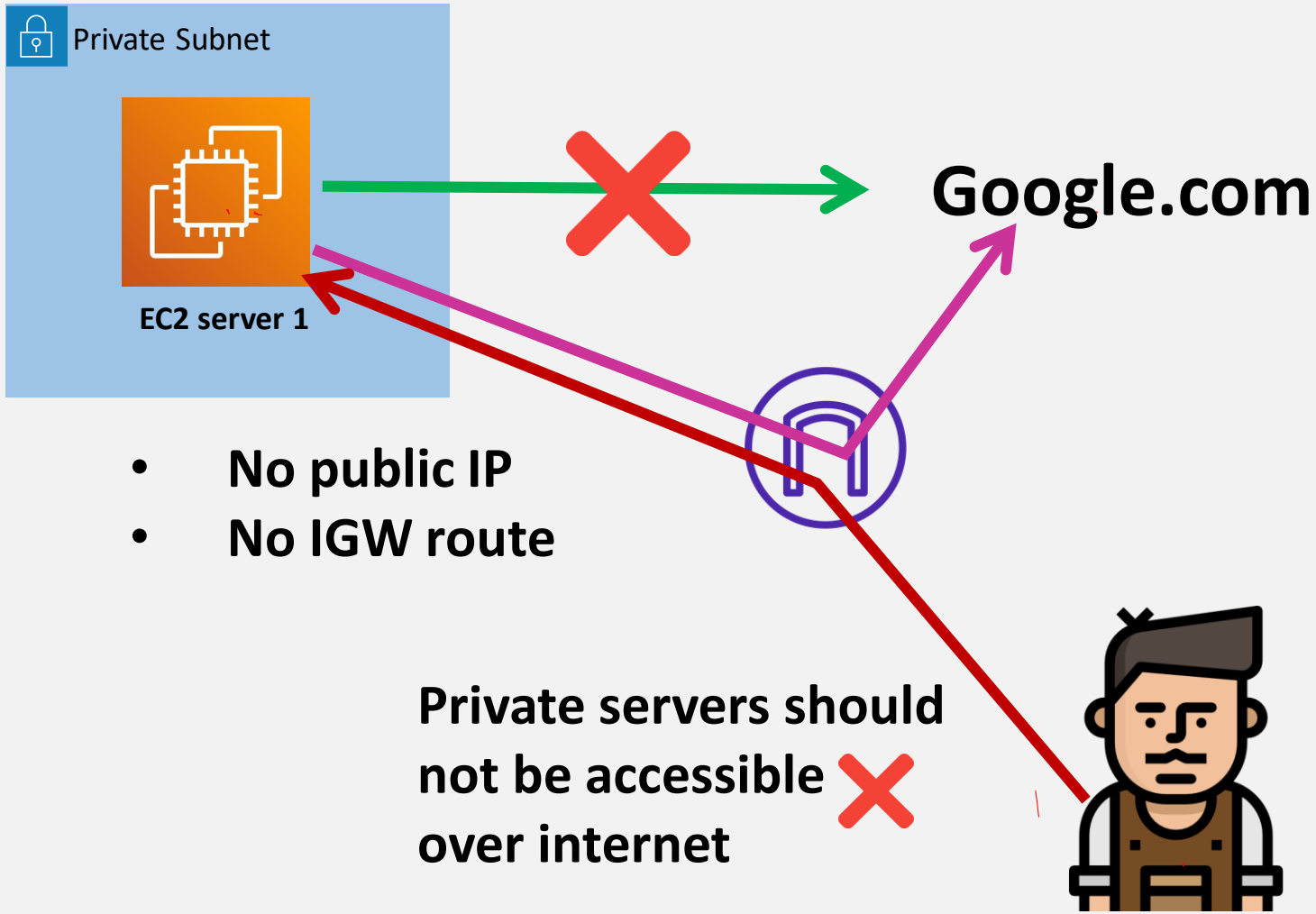


Security Group – Self references



Allows any communication b/w servers

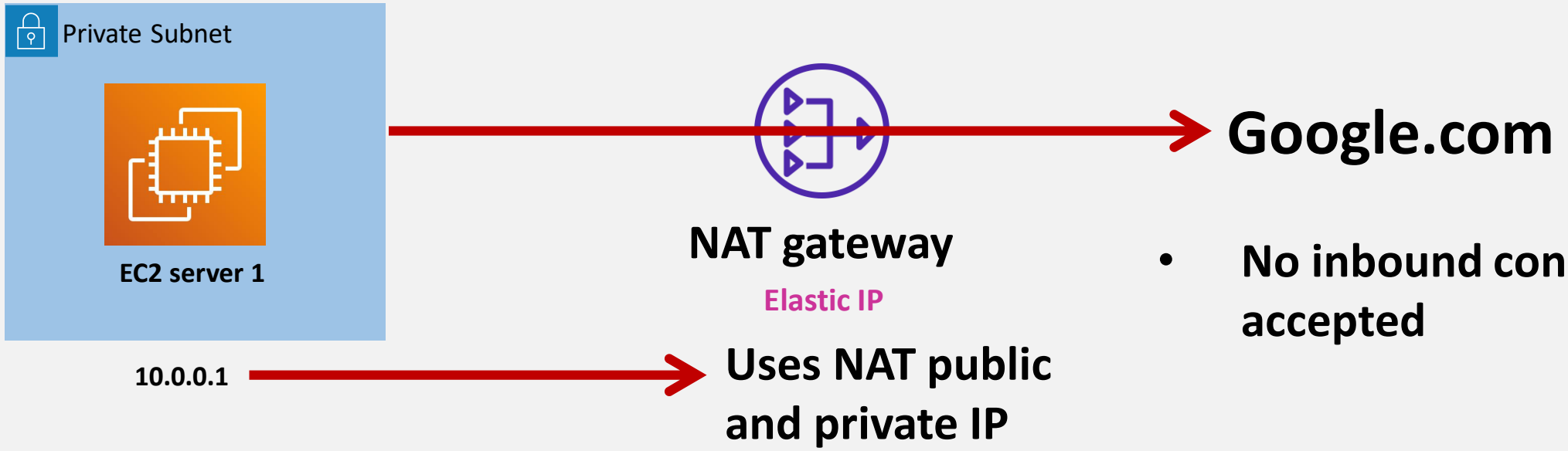
NAT – Network Address Translation



- No public IP
- No IGW route

Private servers should not be accessible over internet

NAT – Network Address Translation



- No inbound connections are accepted

IP Masquerading: Hiding the original IP while making the request

NAT – Key Points

- Runs from a public Subnet
- Uses elastic IP
- AZ resilient – multiple NATs can be created
- One NAT can scale up to 45 GBPS network out.
- Only for IPv4, for IPv6 – egress only gateway can be used
- NAT Instance can be used – but customer need to manage it
  - Source / Destination checks need to be disabled

Demos

Thank you, will meet in tomorrow's session