

AWS – Security

VISHWANATH M S
VISHWACLOUDLAB.COM

List of Security options in AWS

- Network SECURITY
 - Security Groups
 - Network Access Control List (NACL)
- Authentication
 - Keys
- Data Security
 - Encryptions

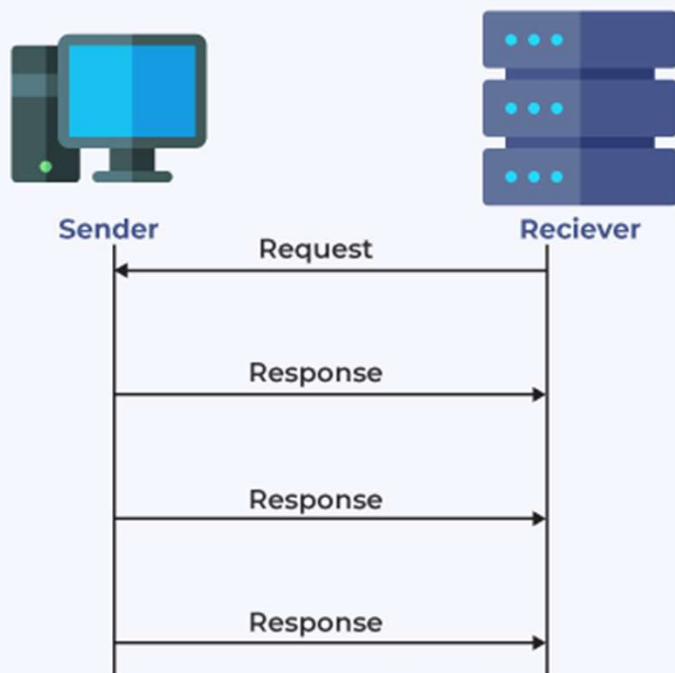
What are some common ports

Port	Request type
7	ECHO
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
79	Finger
80	HTTP
110	POP3
115	Simple File Transfer Protocol (SFTP)

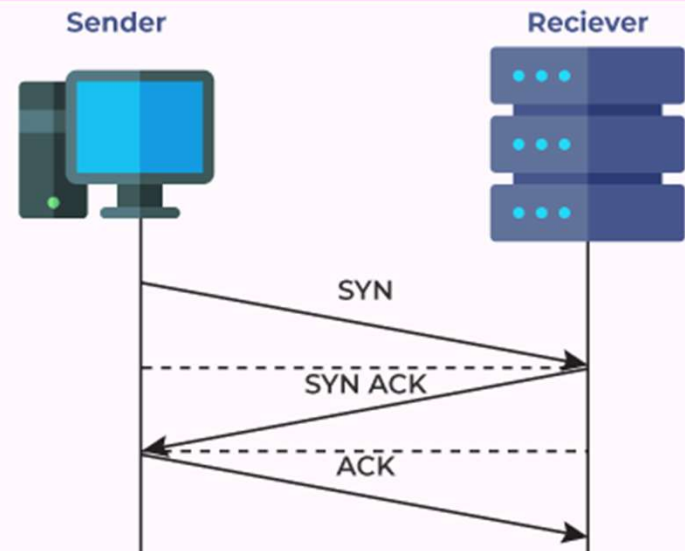
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
156	SQL Server
161	SNMP
194	Internet Relay Chat (IRC)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server

TCP vs UDP

UDP



TCP

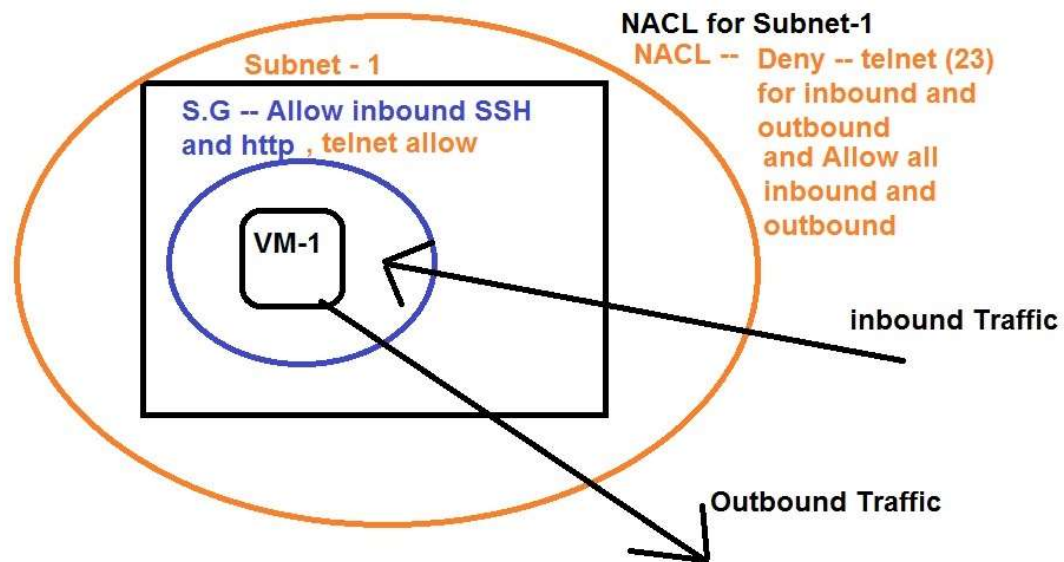


Security Group and NACL

- These are used to Control the Traffic , IN and OUT of the Sytem.
- The Traffic is controlled based on “Port” numbers and “IP address”.
- Port number ranges from 1 to 65536.
- IP address can be controlled either as single IP or range of IP's
- SG is a STATEFULL firewall
- NACL is a STATELESS firewall

TCP/IP Models

Application Layer	Ports – 1- 65536
Transport layer	TCP /UDP
Network Layer	IP Address
Data link Layer	MAC ID



NACL for Subnet-2

Inbound Rules

Allow -- SSH -- from 100.100.100.10

Deny -- SSH -- ALL

Deny -- 8080 -- ALL

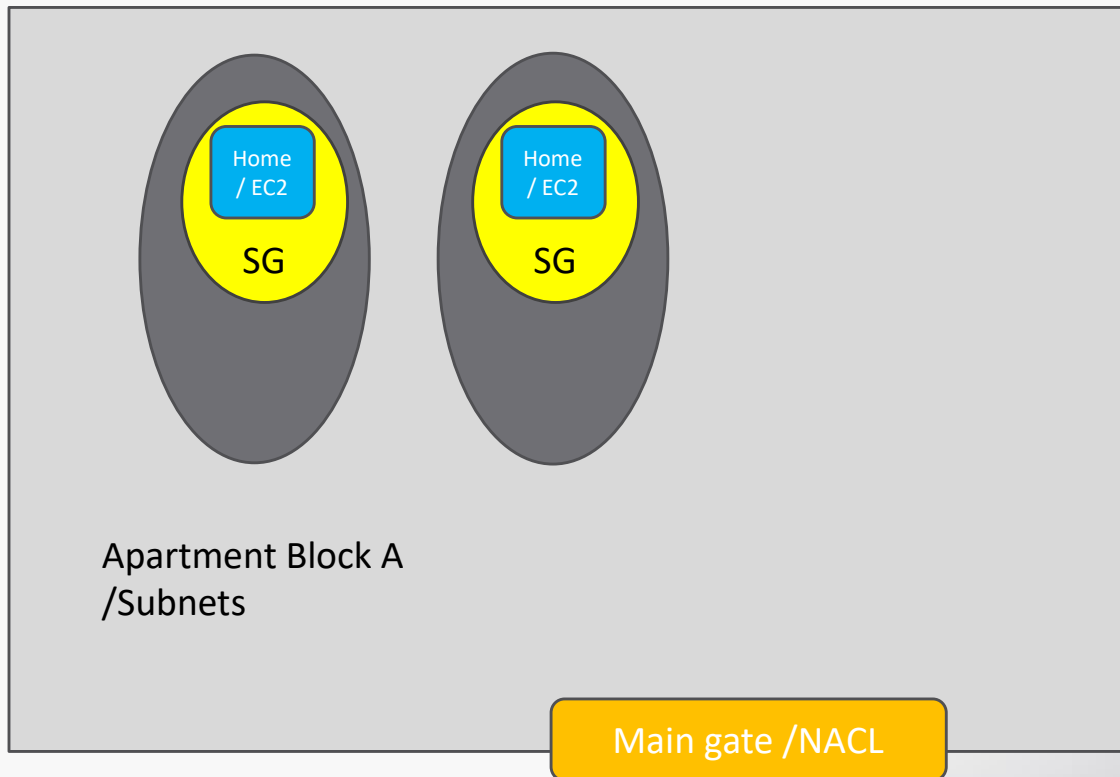
Deny -- 9000-9999 -- ALL

Allow -- ALL

Outbound

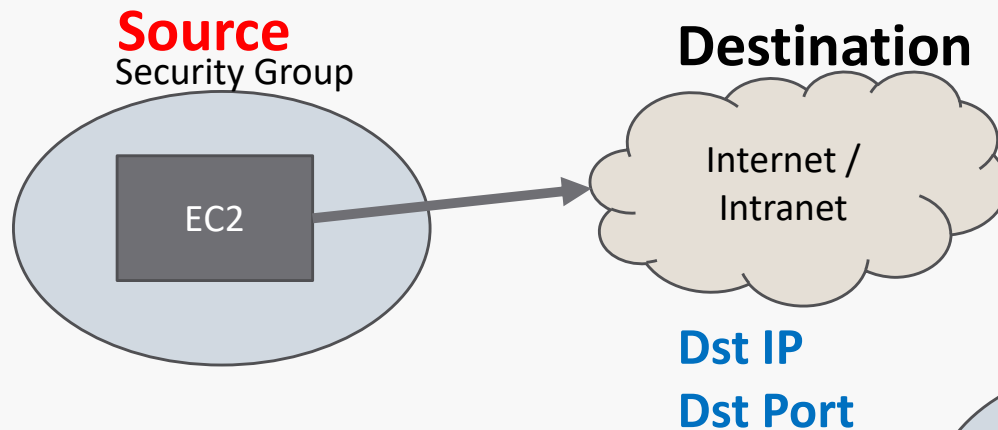
Deny -- ssh -- ALL

Allow -- ALL

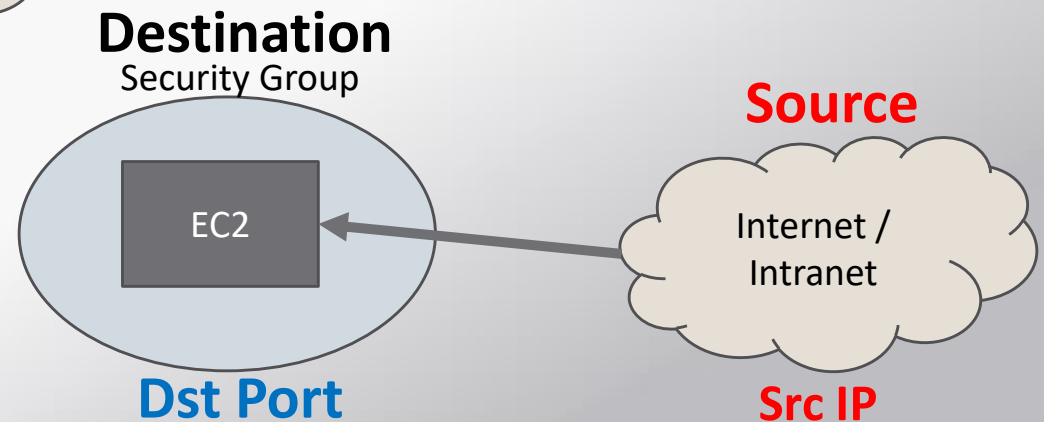


SG – Configuration rules

Outbound Traffic



Inbound Traffic



Example of Security Group

sg-06a7193bc9d359aba | SSH-HTTP-ICMP-8080

Summary

Inbound Rules

Outbound Rules

Tags

Edit

Type	Protocol	Port Range	Source	Description
HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLow all for HTTP
HTTP* (8080)	TCP (6)	8080	0.0.0.0/0	
SSH (22)	TCP (6)	22	157.49.174.50/32	allowed from my lapt...
SSH (22)	TCP (6)	22	2409:4071:2318:3ba5:68d1:b28:9f7d:5c11/128	allowed from my lapt...
All ICMP - IPv6	IPv6-ICMP (58)	ALL	::/0	Allow all for ICMP o...
MySQL/Aurora (3306)	TCP (6)	3306	192.168.0.0/16	
All ICMP - IPv4	ICMP (1)	ALL	0.0.0.0/0	Allow all for ICMP

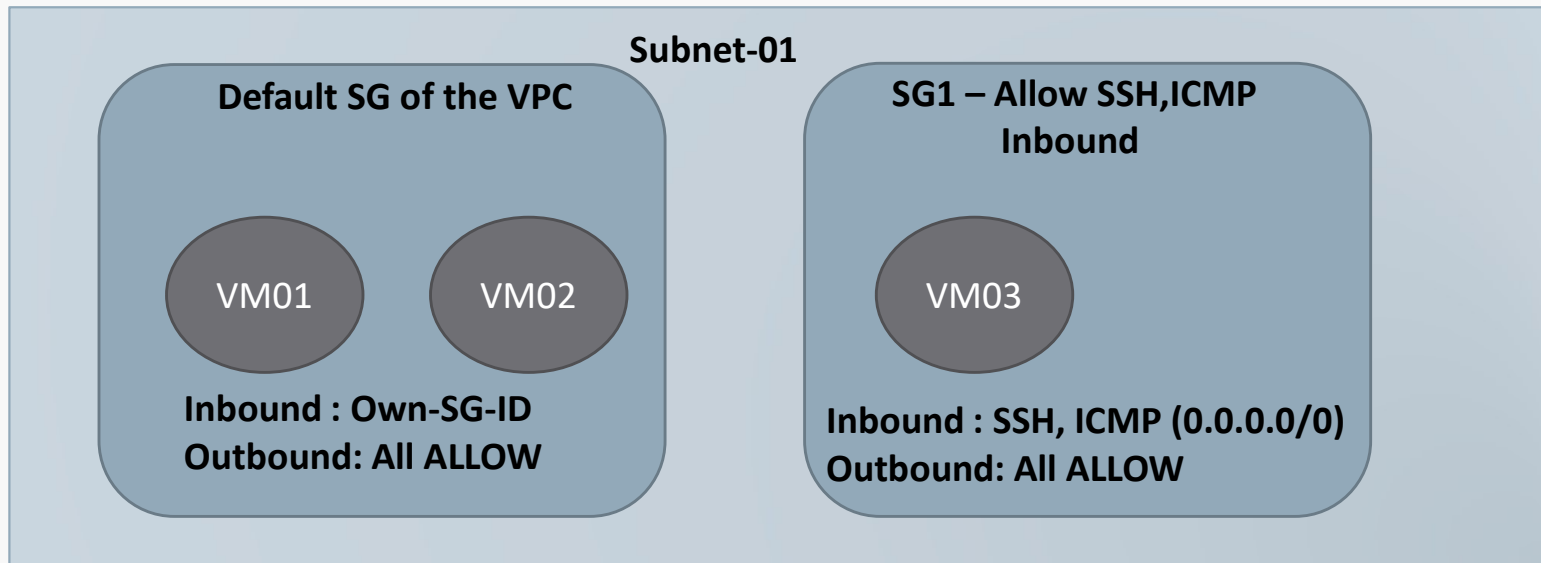
Security Group(SG) - Properties

- Security Group – We can apply the rule INBOUND or OUTBOUND
- It is applied to a EC2, Load Balancer, EFS, Autoscaling.
- SG is local to a VPC.
- By default a SG is created for every VPC.
- Default, ALL outbound traffic is allowed in a new Security Group
- Default, All Inbound traffic is denied in a new Security Group.
- **Single Security Group** can be assigned to **Multiple Virtual machine**.
- **Single Virtual Machine** can have **Multiple Security Groups**
- We can Control **both IPV4** and **IPV6** traffic

SG – Configuration rules

- Inbound rules are created only with “Source IP” and DST port”
- Here → source ip == Internet IP add & DST port == EC2 ports
- Outbound rules are created only with “Dst IP” and “Dst port”
- If you create a rule , that Rule will be allowed.
- Source or Destination has 3 option
 - Custom – specific Network or IP’s
 - My IP address – My Source Public IP (Of my Laptop Internet IP)
 - Any IP – All network. (0.0.0.0/0 for IPv4 and ::/0 for IPv6)

SG – Default Security



- Can VM01 access VM02 on SSH ?? -- Yes
- Can VM02 access VM01 on SSH ?? -- Yes
- Can VM01 access VM03 on SSH ?? -- Yes
- Can VM03 access VM01 on SSH ?? -- No

Security Group

- **Limitation**
- We cannot deny a PARTICULAR traffic in Security Group.

NACL Example - outbound

For 1st 5 Subnets,

Allow ALL traffic outbound and Inbound – Deny SSH all traffic except my laptop IP.

acl-08495ae65c971ad82

Summary

Inbound Rules

Outbound Rules

Subnet Associations

Tags

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules ▼

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	::/0	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

NACL Example - Inbound

For 1st 5 Subnets,

Allow ALL traffic outbound and Inbound – Deny SSH all traffic except my laptop IP.

acl-08495ae65c971ad82

Summary Inbound Rules Outbound Rules Subnet Associations Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules ▼

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1000	SSH (22)	TCP (6)	22	157.49.174.50/32	ALLOW
1001	SSH (22)	TCP (6)	22	0.0.0.0/0	DENY
1100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
1101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	::/0	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

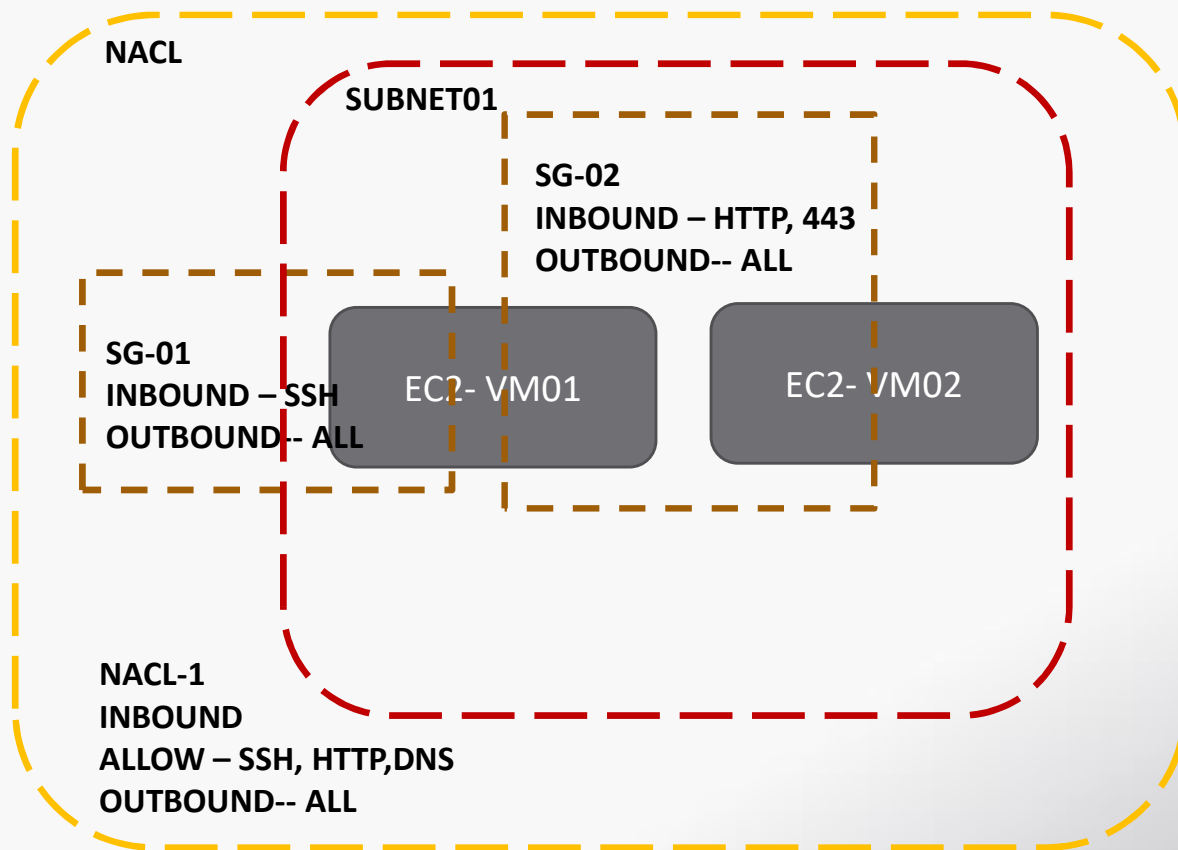
Network Access Control List - NACL

- **NACL is applied to an Subnet.**
- Default NACL is created when a VPC is created.
- Default NACL has **Allow ALL traffic for both “Inbound” and “OutBound”**.
- NACL is local to a VPC
- We can have separate NACL for individual Subnets.
- Unlike SG, We can Allow or Deny a particular Traffic.
- Also we can assign Rule “numbers” for each rule.
- We can Control both **IPV4 and IPV6** traffic

NACL – Configuration rules

- Inbound rules are created only with “Source IP” and Dst port”
- Outbound rules are created only with “Dst IP” and “Dst port”
- If you create a rule , that Rule can be **ALLOWED** or **DEINED** .
- Source or Destination has 3 option
 - Custom – specific Network or IP’s
 - My IP address – My Source Public IP (Of my Laptop Internet IP)
 - Any IP – All network. (0.0.0.0/0 for IPv4 and ::/0 for IPv6)

NACL and SG Working together

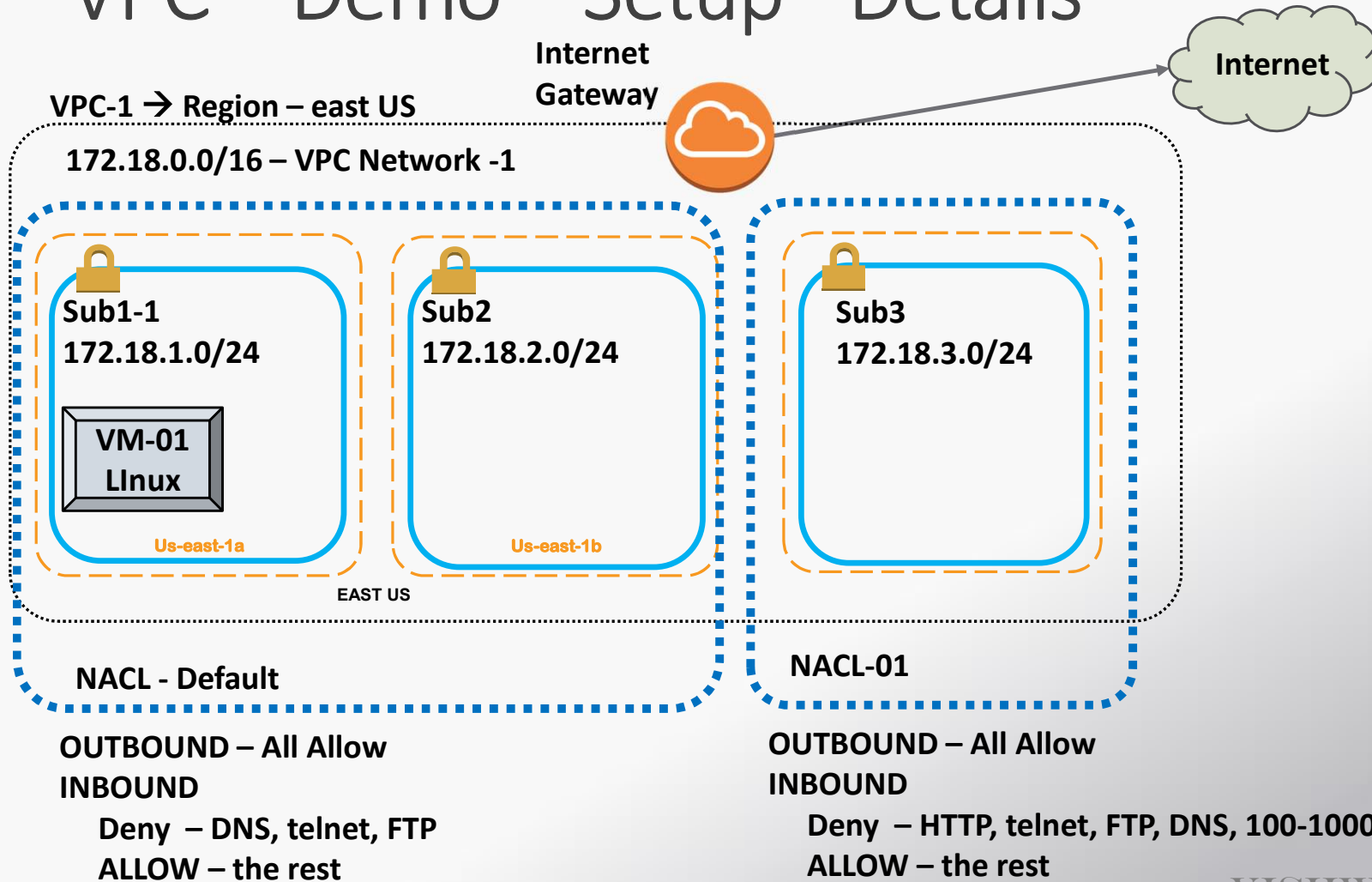


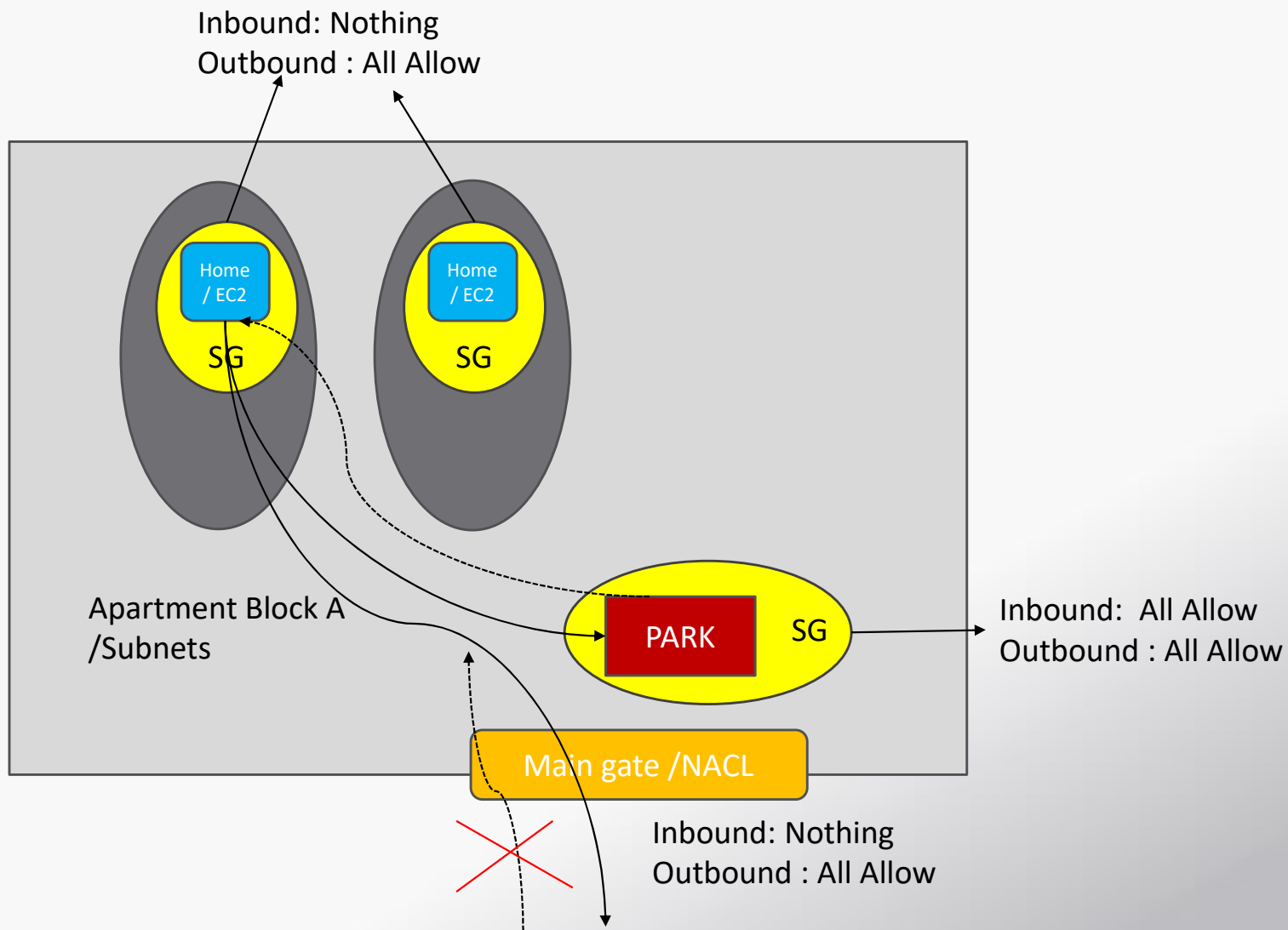
Will the DNS inbound on VM2 allowed? –

Will the HTTP inbound on Vm01 Allowed? –

Will the HTTP inbound on Vm02 Allowed? –

VPC – Demo – Setup - Details





Troubleshooting issue and Other Contents on Security

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>