DATE : 24.02.2025

DT/NT : DT

LESSON : AWS

SUBJECT: VPC-4

BATCH : B 303

AWS-DEVOPS

TECHPRO EDUCATION

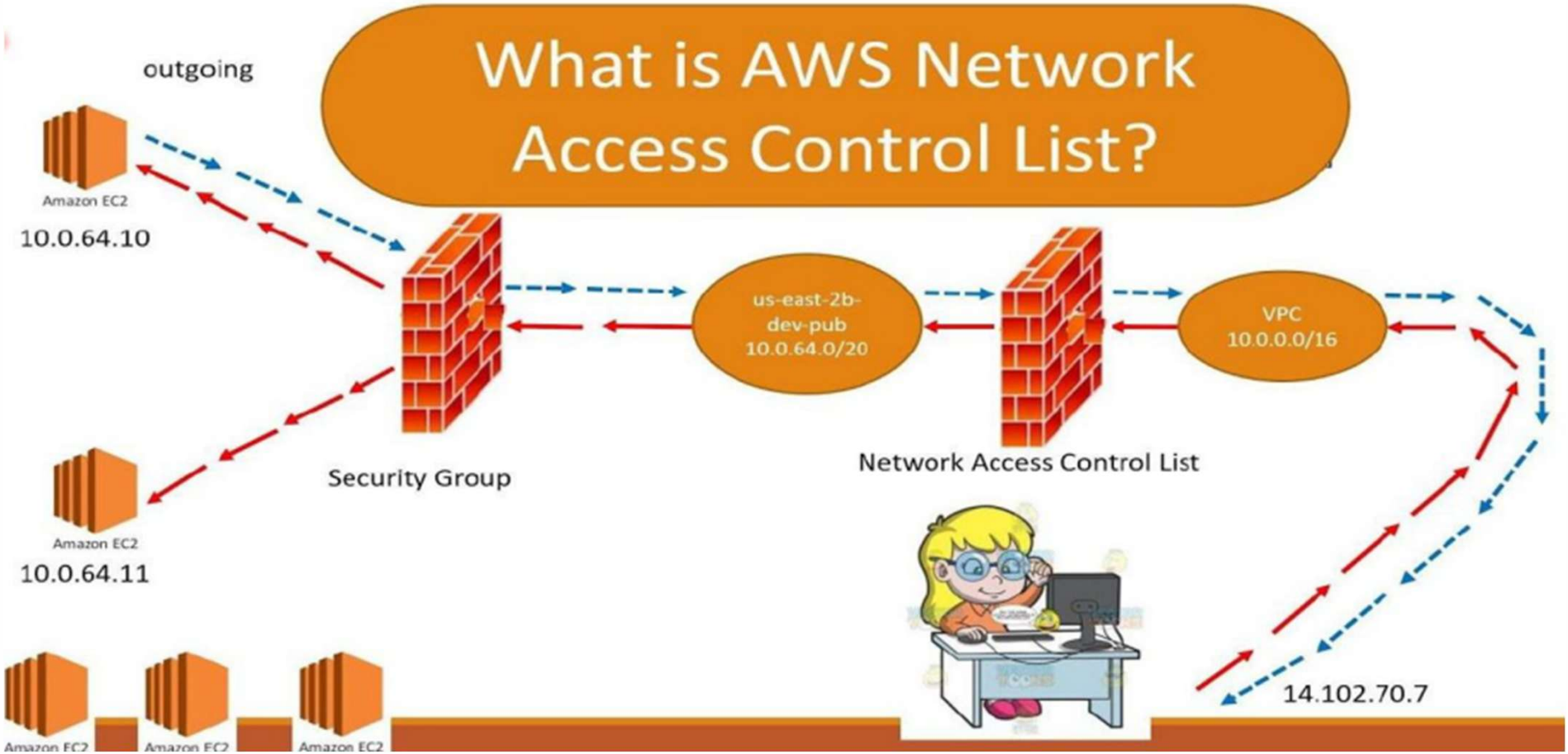
techproeducation.com +1 (585) 304 29 59

Table of Contents

- NACL (NETWORK ACCESS CONTROL LIST)

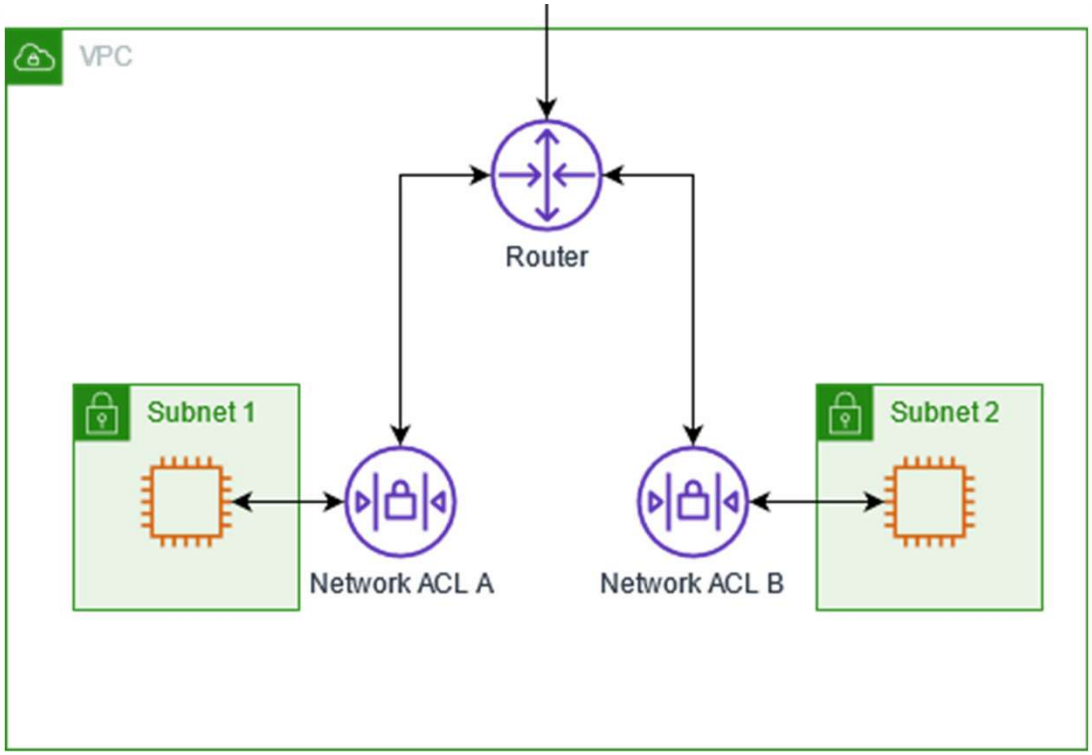
NACL (NETWORK ACCESS CONTROL LIST)

NACL


What is AWS Network Access Control List?
outgoing
Amazon EC2
10.0.64.10
us-east-2b-dev-pub
10.0.64.0/20
VPC
10.0.0.0/16
Security Group
Network Access Control List
Amazon EC2
10.0.64.11
14.102.70.7
Amazon EC2
Amazon EC2
Amazon EC2

NACL

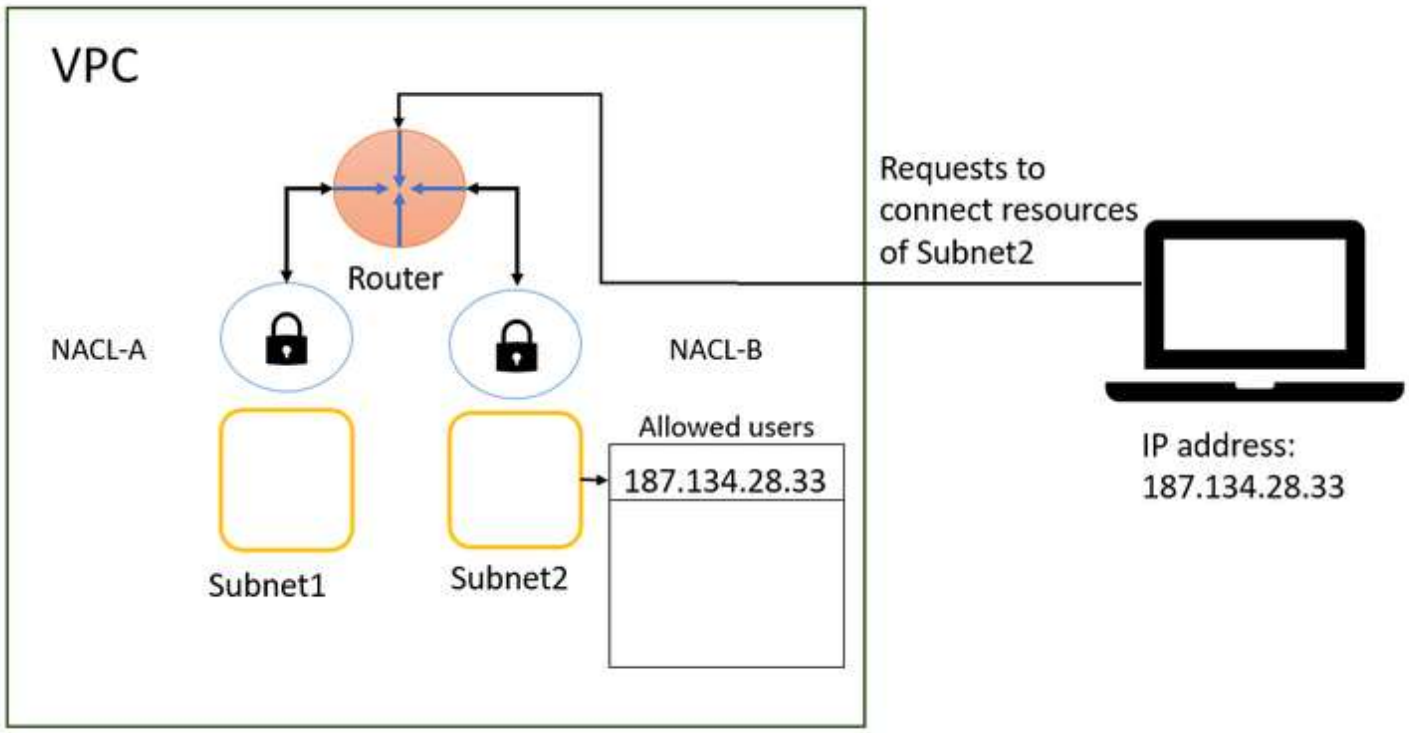
What is NACL?



A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level. You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are similar to the rules for your security groups in order to add an additional layer of security to your VPC.

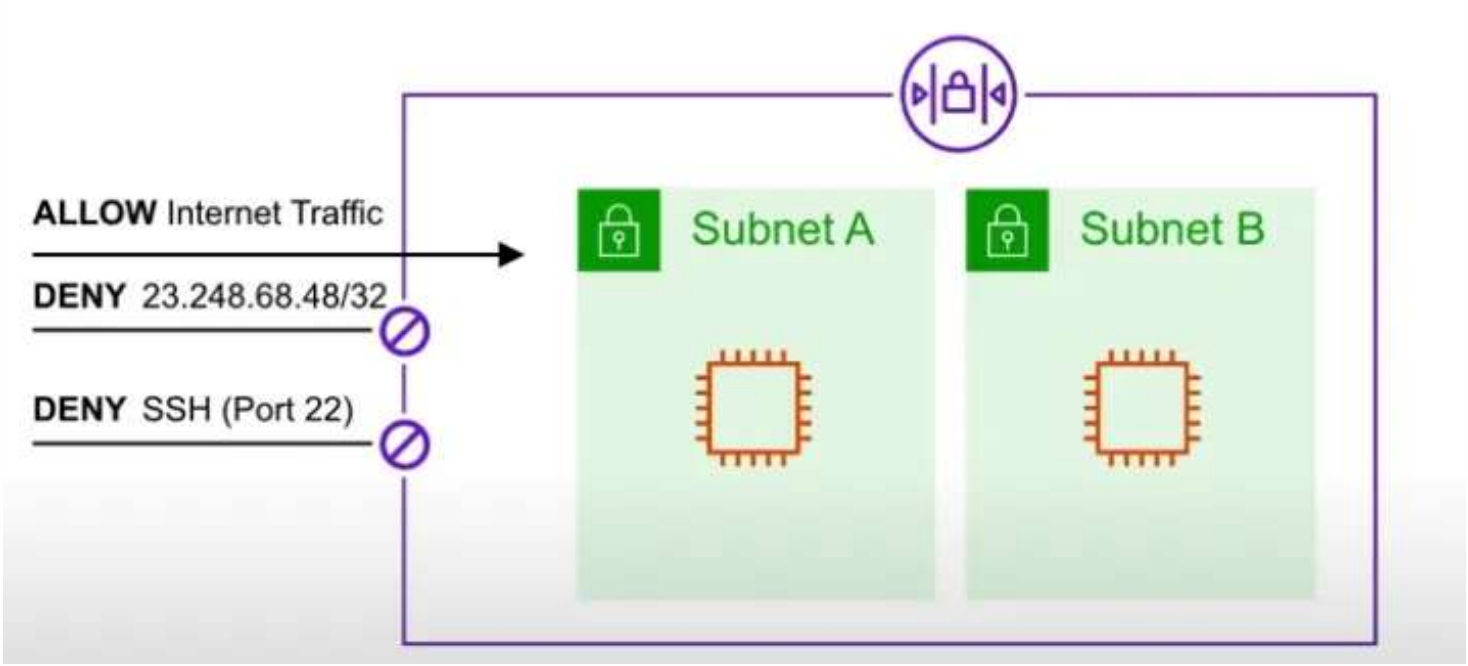
NACL

Why Use NACLs?



NACL

Why Use NACLs?



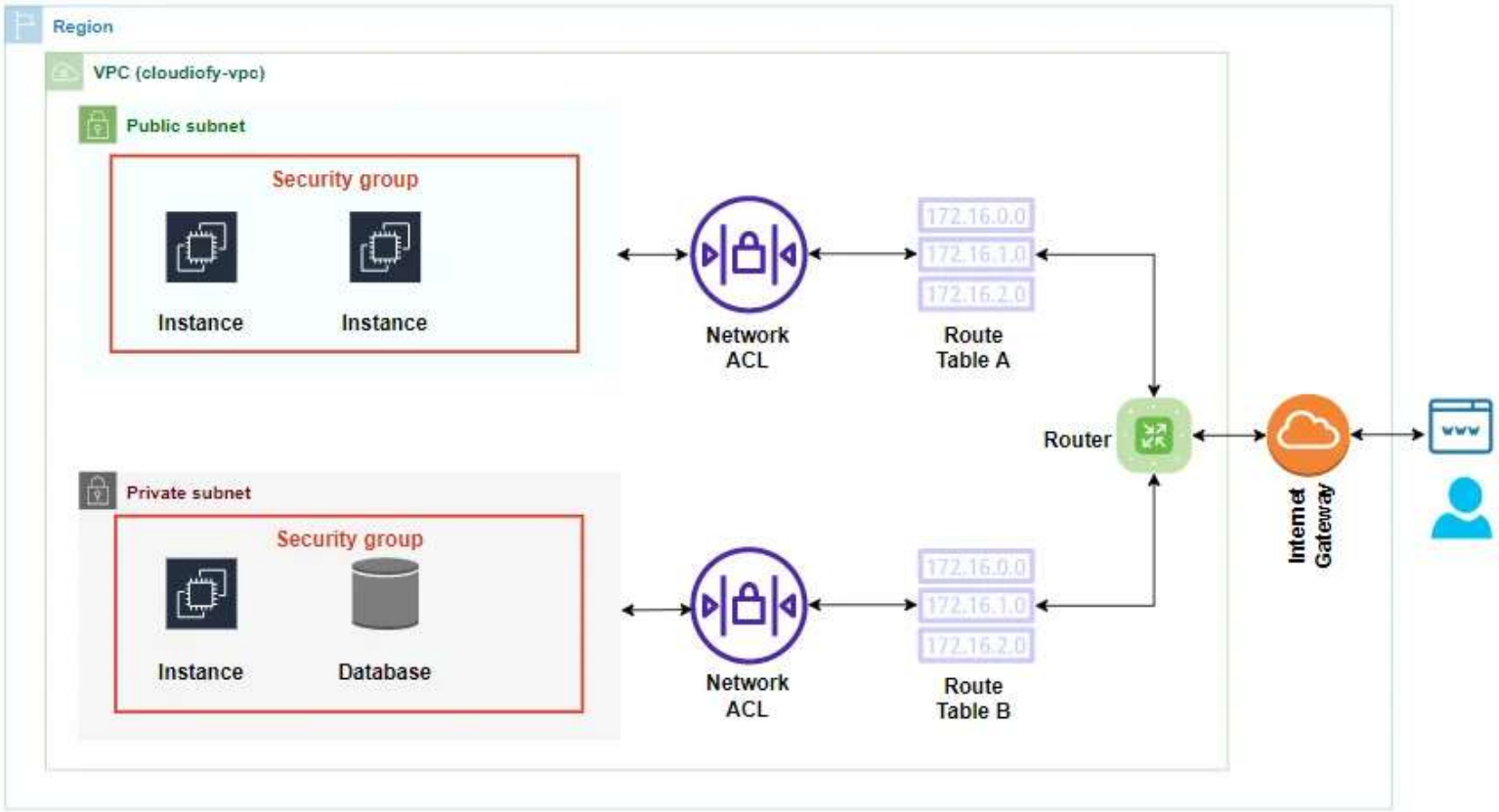
NACL

Features

- Stateless Filtering
- Subnet Level Security
- Rule Order Matters
- Manual Adjustment Required

NACL

Best Practices



NACL

Best Practices

Defense in Depth: Use Security Groups and NACLs to implement a defense-in-depth strategy. This multi-layered approach enhances security by providing redundancy and mitigating the impact of a single point of failure.

Least Privilege Principle: Adhere to the principle of least privilege when configuring rules for both SGs and NACLs. Only allow the necessary traffic, reducing the attack surface and potential security risks.

Regular Audits and Updates: Periodically review and update your security configurations. As your infrastructure evolves, ensure that your SGs and NACLs align with the current requirements and best practices.

NACL

Security Group Vs NACL

Feature	Security Groups (SGs)	Network Access Control Lists (NACLs)
Scope of Control	Operate at the instance level, controlling traffic for individual instances	Operate at the subnet level, controlling traffic for all instances within a subnet
Filtering Mechanism	Stateful filtering: Automatically allows corresponding outbound traffic	Stateless filtering: Separate rules required for inbound and outbound traffic
Flexibility and Dynamism	Dynamically adjust rules based on actual traffic, facilitating easy adaptation to changes	Manual adjustment is required for changes in rules; rules are evaluated based on order, requiring careful planning
Association	Associated with individual instances, providing granular control	Associated with subnets, enforcing security policies consistently across multiple instances

NACL

Security Group Vs NACL

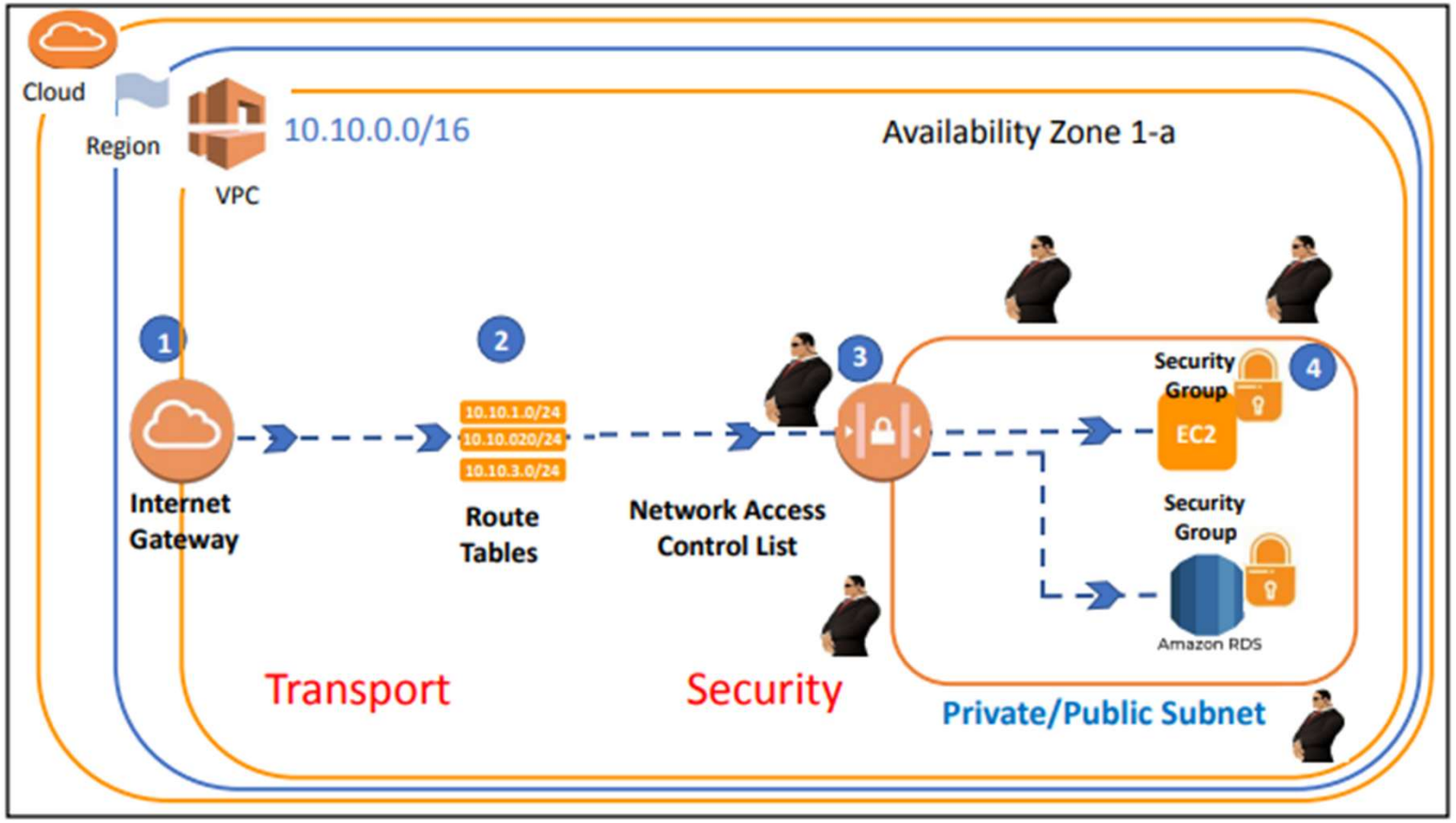
Feature	Security Groups (SGs)	Network Access Control Lists (NACLs)
Rule Order	Rule order is not explicitly defined or critical	Rule order matters; the first matching rule is applied
Ease of Use	User-friendly and easy to set up, ideal for scenarios where simplicity is key	It requires careful planning and understanding of rule order and is suited for scenarios where manual control is acceptable
Dynamic Port Configuration	Dynamically adjust allowed ports based on defined rules	Manual configuration required for port adjustments
Use Cases	Suitable for instance-level security, providing dynamic and adaptive security	Ideal for enforcing consistent security policies across multiple instances in a subnet

NACL

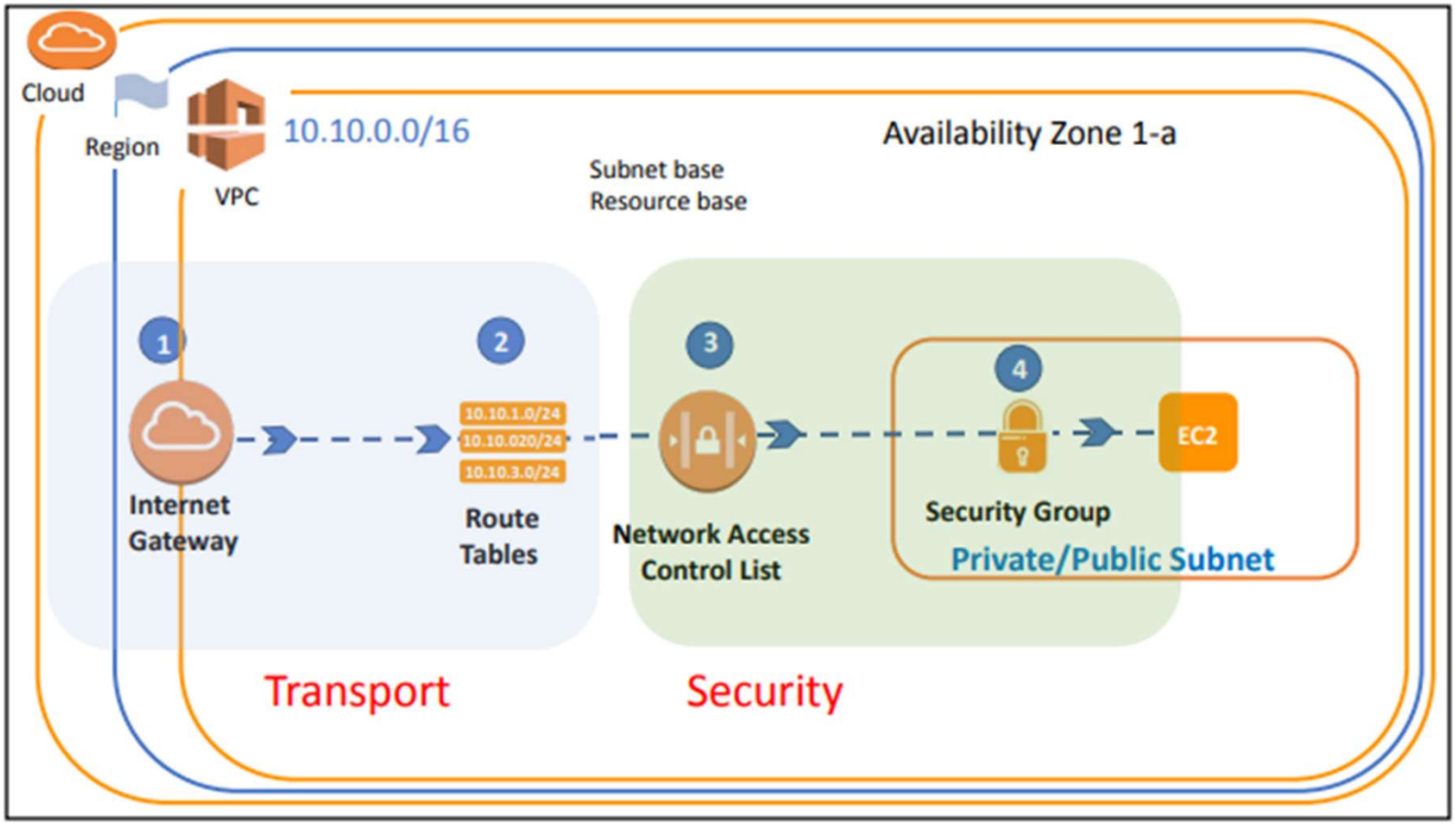
Security Group Vs NACL

Feature	Security Groups (SGs)	Network Access Control Lists (NACLs)
Redundancy and Defense-in-Depth	Both components contribute to a robust defense mechanism, implementing a defense-in-depth strategy	Implementing a defense-in-depth strategy enhances overall security
Audits and Updates	Regular audits and updates are crucial for maintaining security	Regular audits and updates are crucial for maintaining security

NACL


Cloud
Region
VPC
10.10.0.0/16
Availability Zone 1-a
1
2
3
4
Internet Gateway
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Route Tables
Network Access Control List
Security Group
EC2
Security Group
Amazon RDS
Transport
Security
Private/Public Subnet

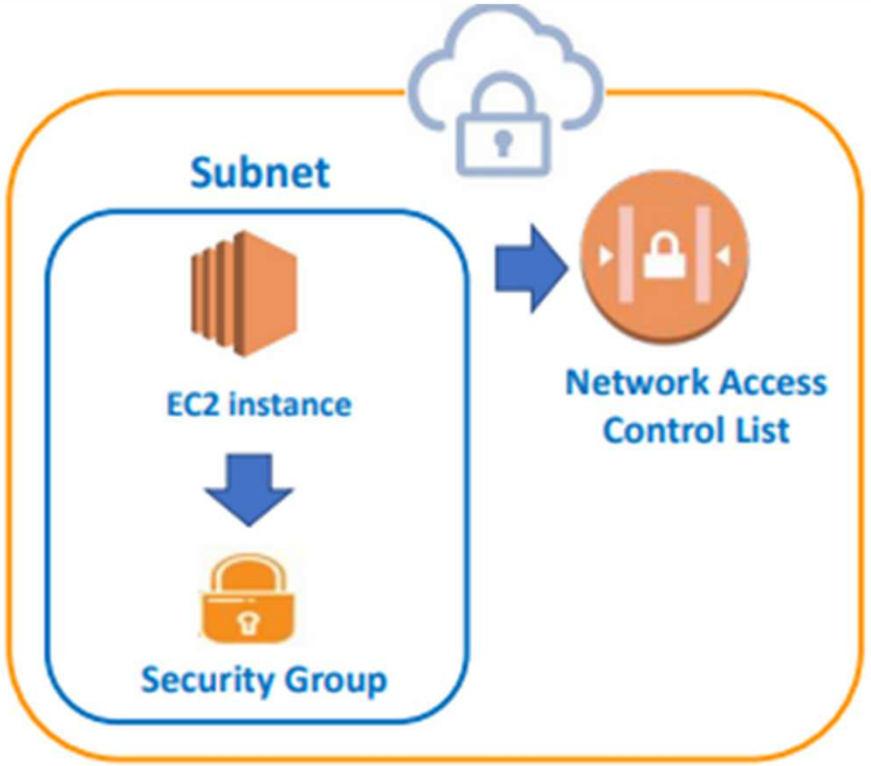
NACL


Cloud
Region
VPC
10.10.0.0/16
Availability Zone 1-a
Subnet base
Resource base
1
2
3
4
10.10.1.0/24
10.10.020/24
10.10.3.0/24
Internet
Gateway
Route
Tables
Network Access
Control List
Security Group
EC2
Private/Public Subnet
Transport
Security

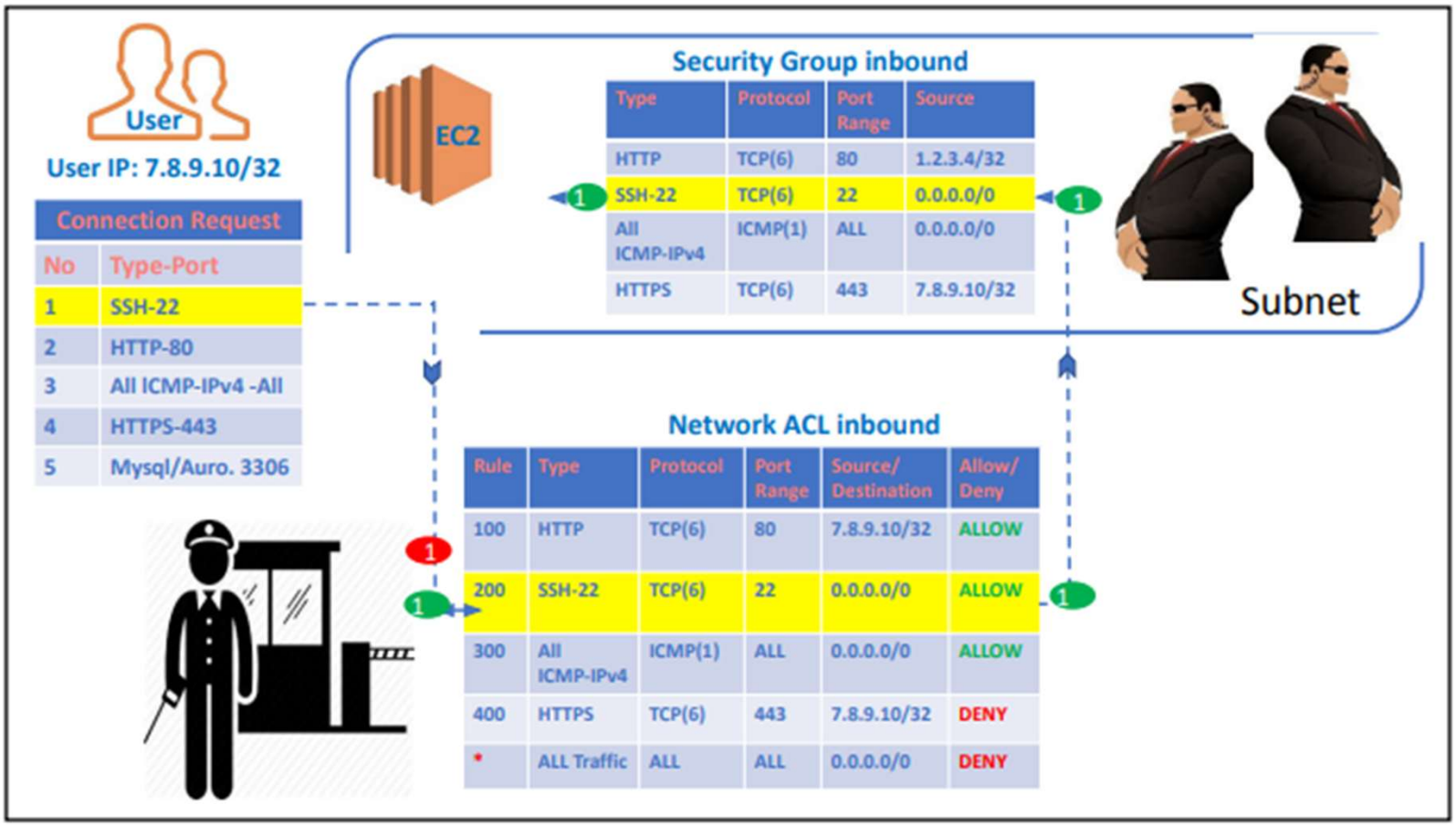
NACL

Subnet obeys the NACL rules

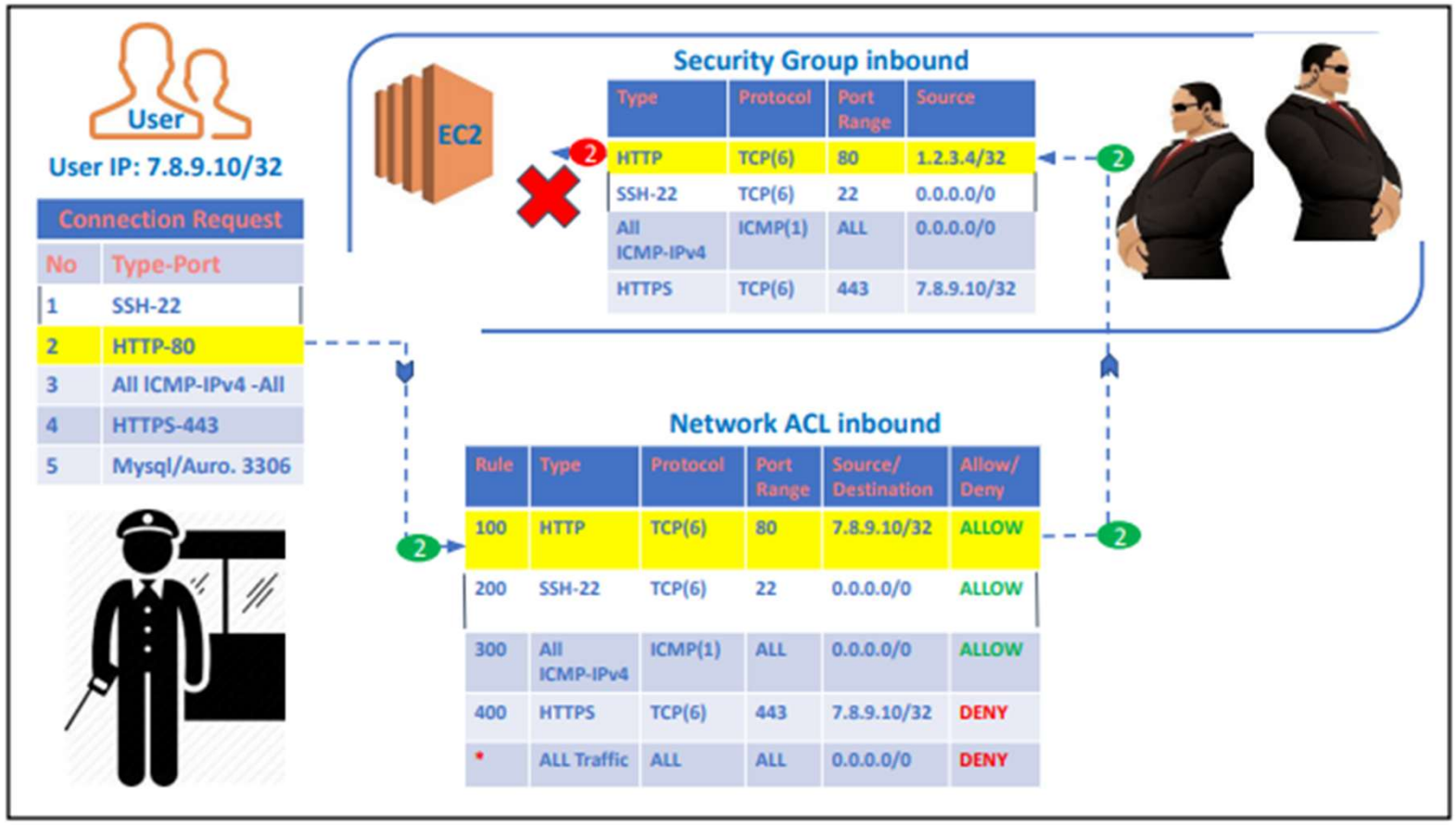
Resources obeys NACL and Sec. Group



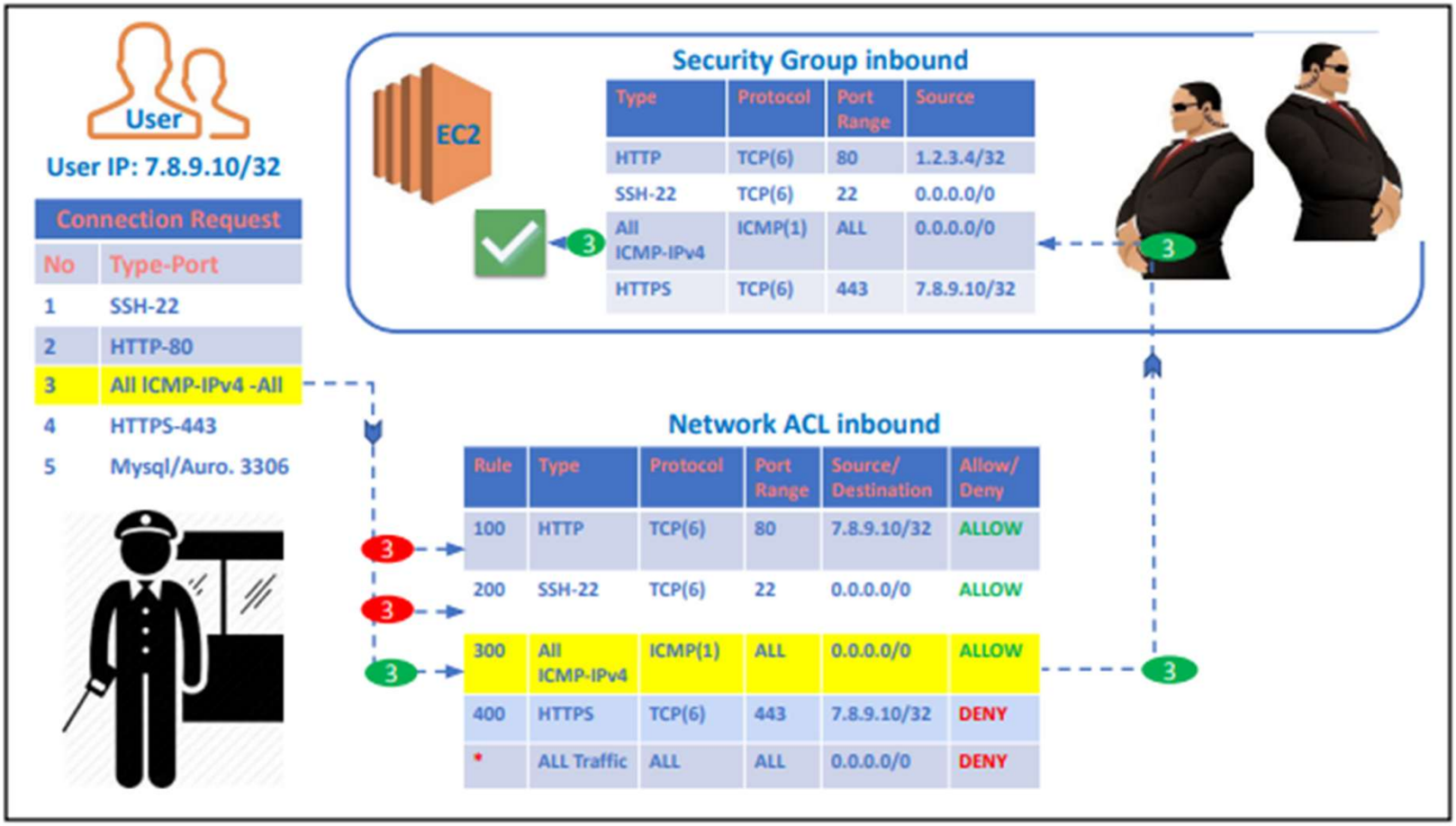
NACL


User
User IP: 7.8.9.10/32
Connection Request
No | Type-Port
1 | SSH-22
2 | HTTP-80
3 | All ICMP-IPv4 -All
4 | HTTPS-443
5 | Mysql/Auro. 3306
EC2
Security Group inbound
Type | Protocol | Port Range | Source
HTTP | TCP(6) | 80 | 1.2.3.4/32
SSH-22 | TCP(6) | 22 | 0.0.0.0/0
All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0
HTTPS | TCP(6) | 443 | 7.8.9.10/32
Subnet
Network ACL inbound
Rule | Type | Protocol | Port Range | Source/ Destination | Allow/ Deny
100 | HTTP | TCP(6) | 80 | 7.8.9.10/32 | ALLOW
200 | SSH-22 | TCP(6) | 22 | 0.0.0.0/0 | ALLOW
300 | All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0 | ALLOW
400 | HTTPS | TCP(6) | 443 | 7.8.9.10/32 | DENY
* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY

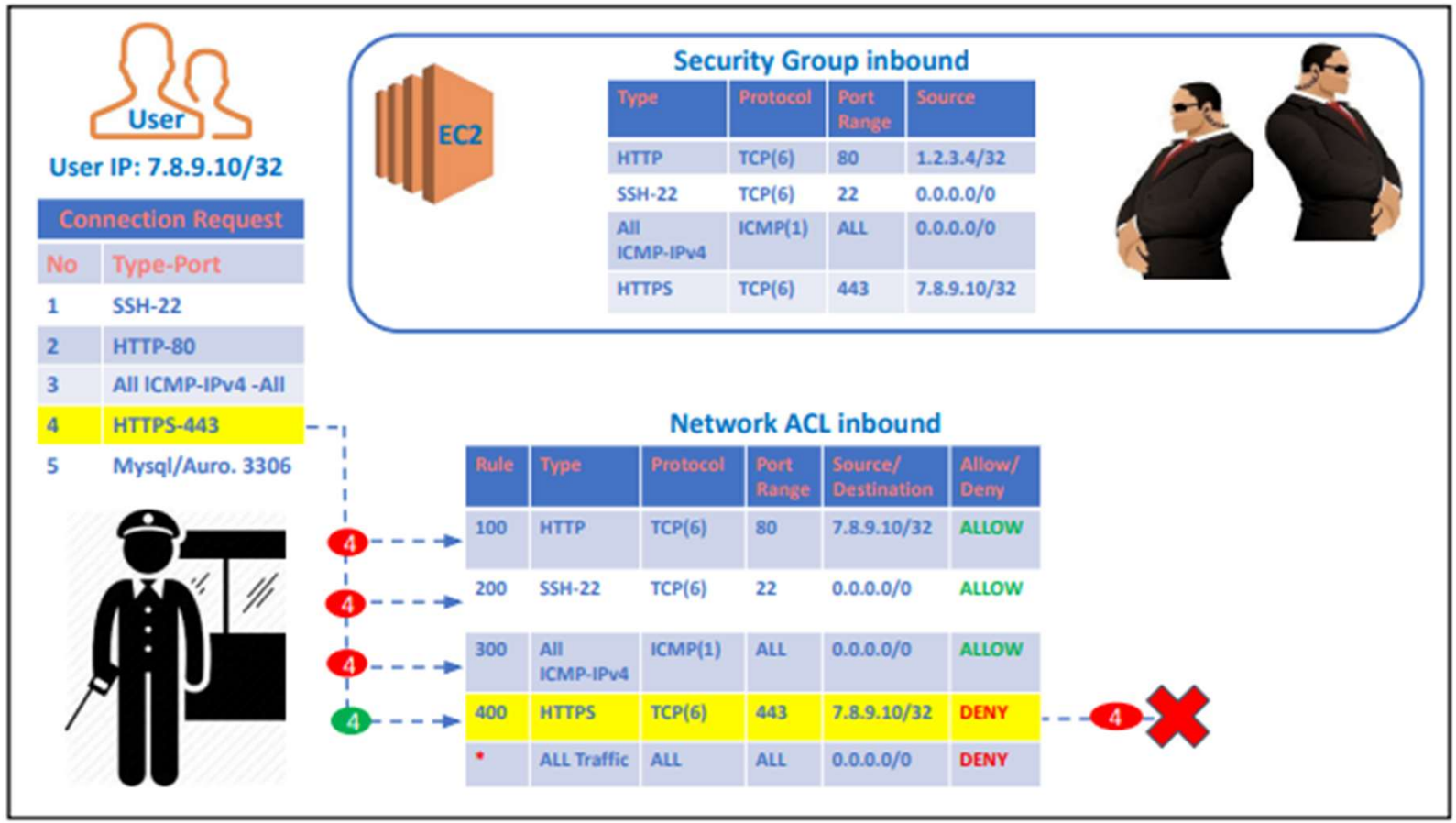
NACL


User
User IP: 7.8.9.10/32
Connection Request
No | Type-Port
1 | SSH-22
2 | HTTP-80
3 | All ICMP-IPv4 -All
4 | HTTPS-443
5 | Mysql/Auro. 3306
EC2
Security Group inbound
Type | Protocol | Port Range | Source
HTTP | TCP(6) | 80 | 1.2.3.4/32
SSH-22 | TCP(6) | 22 | 0.0.0.0/0
All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0
HTTPS | TCP(6) | 443 | 7.8.9.10/32
Network ACL inbound
Rule | Type | Protocol | Port Range | Source/ Destination | Allow/ Deny
100 | HTTP | TCP(6) | 80 | 7.8.9.10/32 | ALLOW
200 | SSH-22 | TCP(6) | 22 | 0.0.0.0/0 | ALLOW
300 | All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0 | ALLOW
400 | HTTPS | TCP(6) | 443 | 7.8.9.10/32 | DENY
* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY

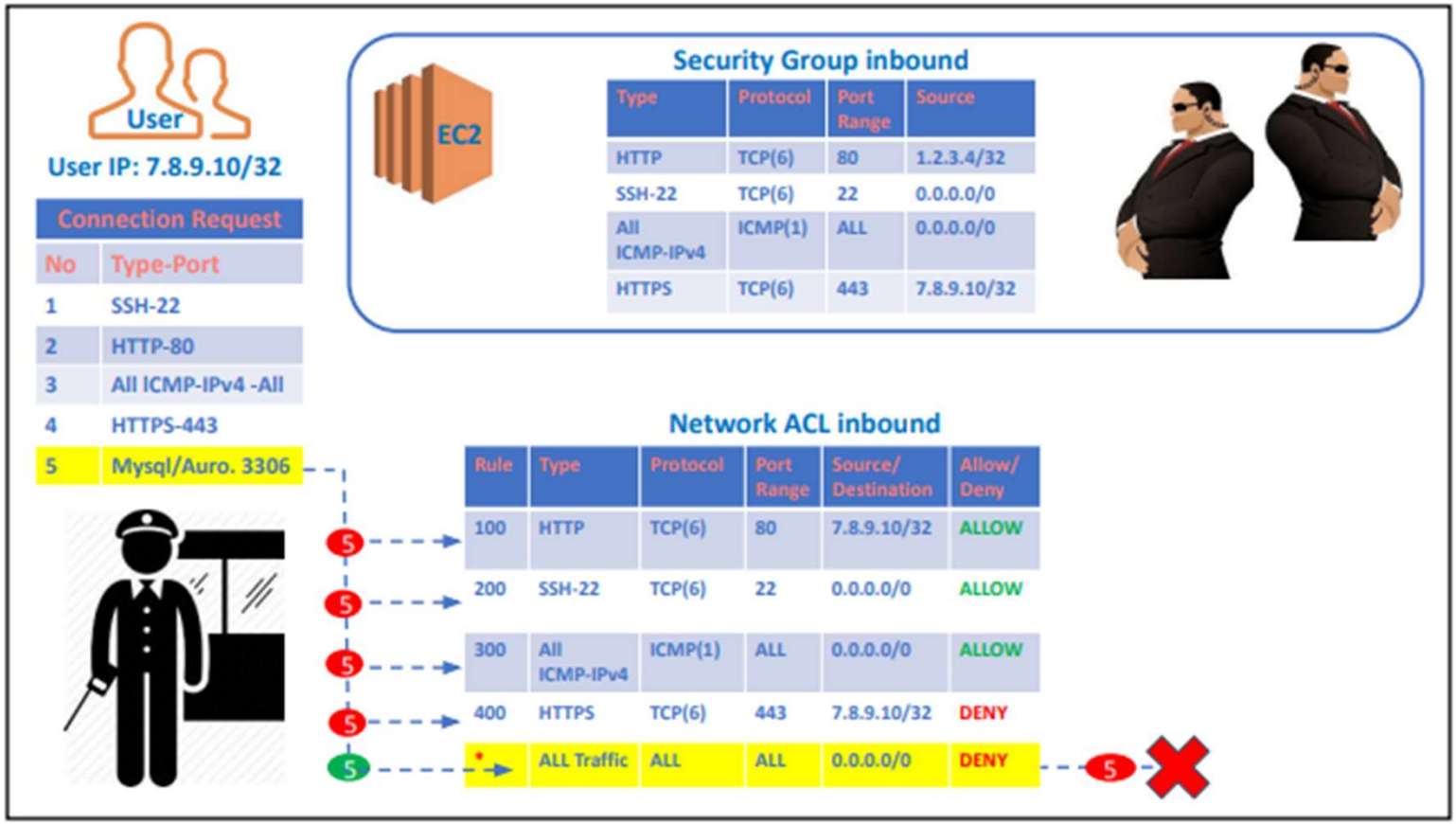
NACL


User
User IP: 7.8.9.10/32
Connection Request
No | Type-Port
1 | SSH-22
2 | HTTP-80
3 | All ICMP-IPv4 -All
4 | HTTPS-443
5 | Mysql/Auro. 3306
EC2
Security Group inbound
Type | Protocol | Port Range | Source
HTTP | TCP(6) | 80 | 1.2.3.4/32
SSH-22 | TCP(6) | 22 | 0.0.0.0/0
All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0
HTTPS | TCP(6) | 443 | 7.8.9.10/32
Network ACL inbound
Rule | Type | Protocol | Port Range | Source/ Destination | Allow/ Deny
100 | HTTP | TCP(6) | 80 | 7.8.9.10/32 | ALLOW
200 | SSH-22 | TCP(6) | 22 | 0.0.0.0/0 | ALLOW
300 | All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0 | ALLOW
400 | HTTPS | TCP(6) | 443 | 7.8.9.10/32 | DENY
* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY

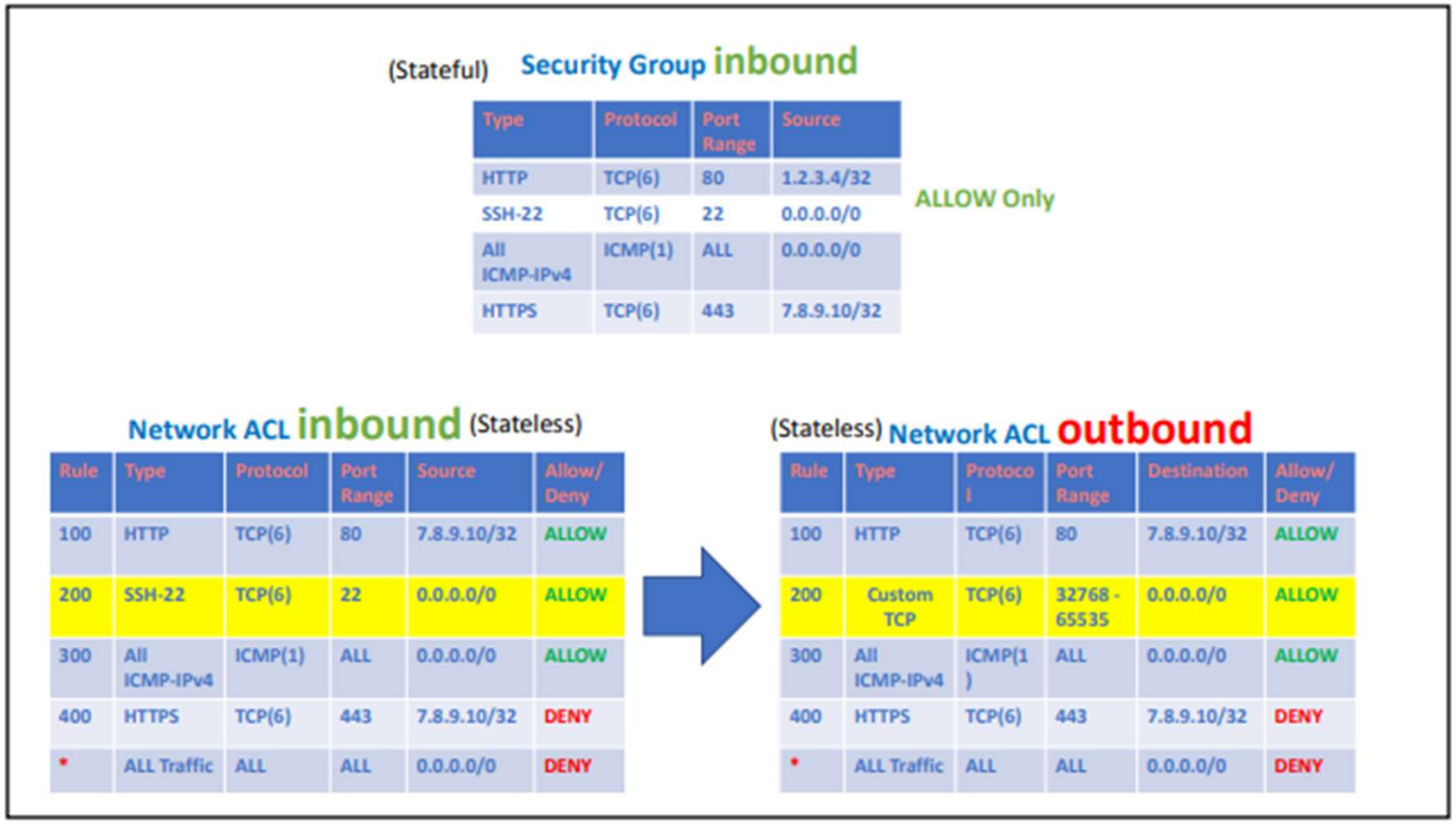
NACL


User
User IP: 7.8.9.10/32
Connection Request
No
Type-Port
1
SSH-22
2
HTTP-80
3
All ICMP-IPv4 -All
4
HTTPS-443
5
Mysql/Auro. 3306
EC2
Security Group inbound
Type
Protocol
Port Range
Source
HTTP
TCP(6)
80
1.2.3.4/32
SSH-22
TCP(6)
22
0.0.0.0/0
All ICMP-IPv4
ICMP(1)
ALL
0.0.0.0/0
HTTPS
TCP(6)
443
7.8.9.10/32
Network ACL inbound
Rule
Type
Protocol
Port Range
Source/ Destination
Allow/ Deny
100
HTTP
TCP(6)
80
7.8.9.10/32
ALLOW
200
SSH-22
TCP(6)
22
0.0.0.0/0
ALLOW
300
All ICMP-IPv4
ICMP(1)
ALL
0.0.0.0/0
ALLOW
400
HTTPS
TCP(6)
443
7.8.9.10/32
DENY
*
ALL Traffic
ALL
ALL
0.0.0.0/0
DENY

NACL


User
User IP: 7.8.9.10/32
Connection Request
No | Type-Port
1 | SSH-22
2 | HTTP-80
3 | All ICMP-IPv4 -All
4 | HTTPS-443
5 | Mysql/Auro. 3306
EC2
Security Group inbound
Type | Protocol | Port Range | Source
HTTP | TCP(6) | 80 | 1.2.3.4/32
SSH-22 | TCP(6) | 22 | 0.0.0.0/0
All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0
HTTPS | TCP(6) | 443 | 7.8.9.10/32
Network ACL inbound
Rule | Type | Protocol | Port Range | Source/ Destination | Allow/ Deny
100 | HTTP | TCP(6) | 80 | 7.8.9.10/32 | ALLOW
200 | SSH-22 | TCP(6) | 22 | 0.0.0.0/0 | ALLOW
300 | All ICMP-IPv4 | ICMP(1) | ALL | 0.0.0.0/0 | ALLOW
400 | HTTPS | TCP(6) | 443 | 7.8.9.10/32 | DENY
* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY

NACL



(Stateful) Security Group inbound

Type	Protocol	Port Range	Source
HTTP	TCP(6)	80	1.2.3.4/32
SSH-22	TCP(6)	22	0.0.0.0/0
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0
HTTPS	TCP(6)	443	7.8.9.10/32

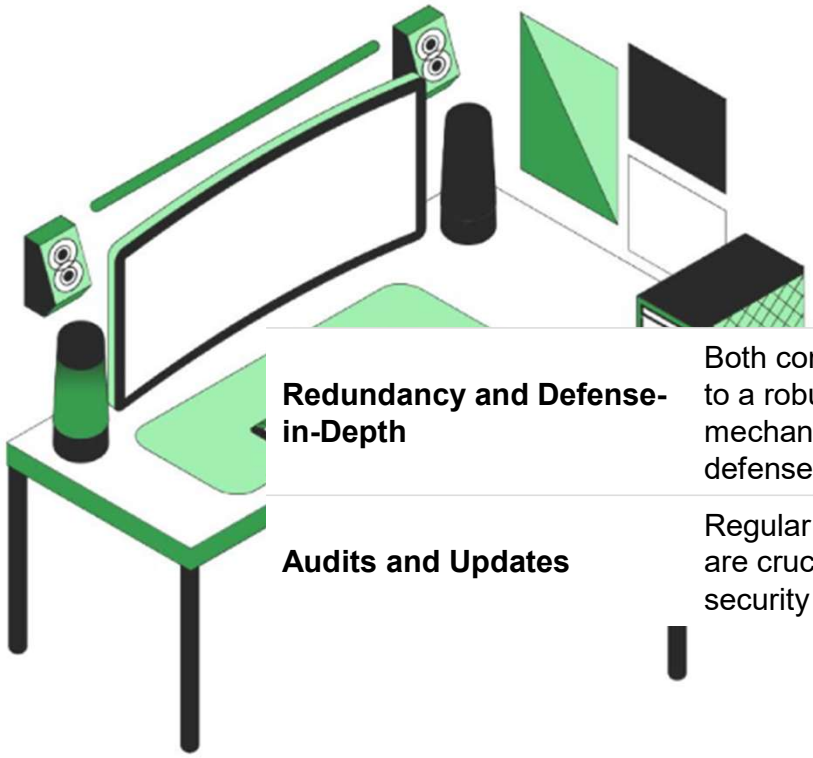
ALLOW Only

Network ACL inbound (Stateless)

Rule	Type	Protocol	Port Range	Source	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

(Stateless) Network ACL outbound

Rule	Type	Protocol	Port Range	Destination	Allow/ Deny
100	HTTP	TCP(6)	80	7.8.9.10/32	ALLOW
200	Custom TCP	TCP(6)	32768 - 65535	0.0.0.0/0	ALLOW
300	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
400	HTTPS	TCP(6)	443	7.8.9.10/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



Redundancy and Defense-in-Depth	Both components contribute to a robust defense mechanism, implementing a defense-in-depth strategy	Implementing a defense-in-depth strategy enhances overall security
Audits and Updates	Regular audits and updates are crucial for maintaining security	Regular audits and updates are crucial for maintaining security

Do you have any ons?

Send it to us! We hope you learned something new.