BATCH: 149

29.08.2023

DT/NT : NT

LESSON : AWS

SUBJECT: VPC - 4

TECHPRO EDUCATION

techproeducation.com

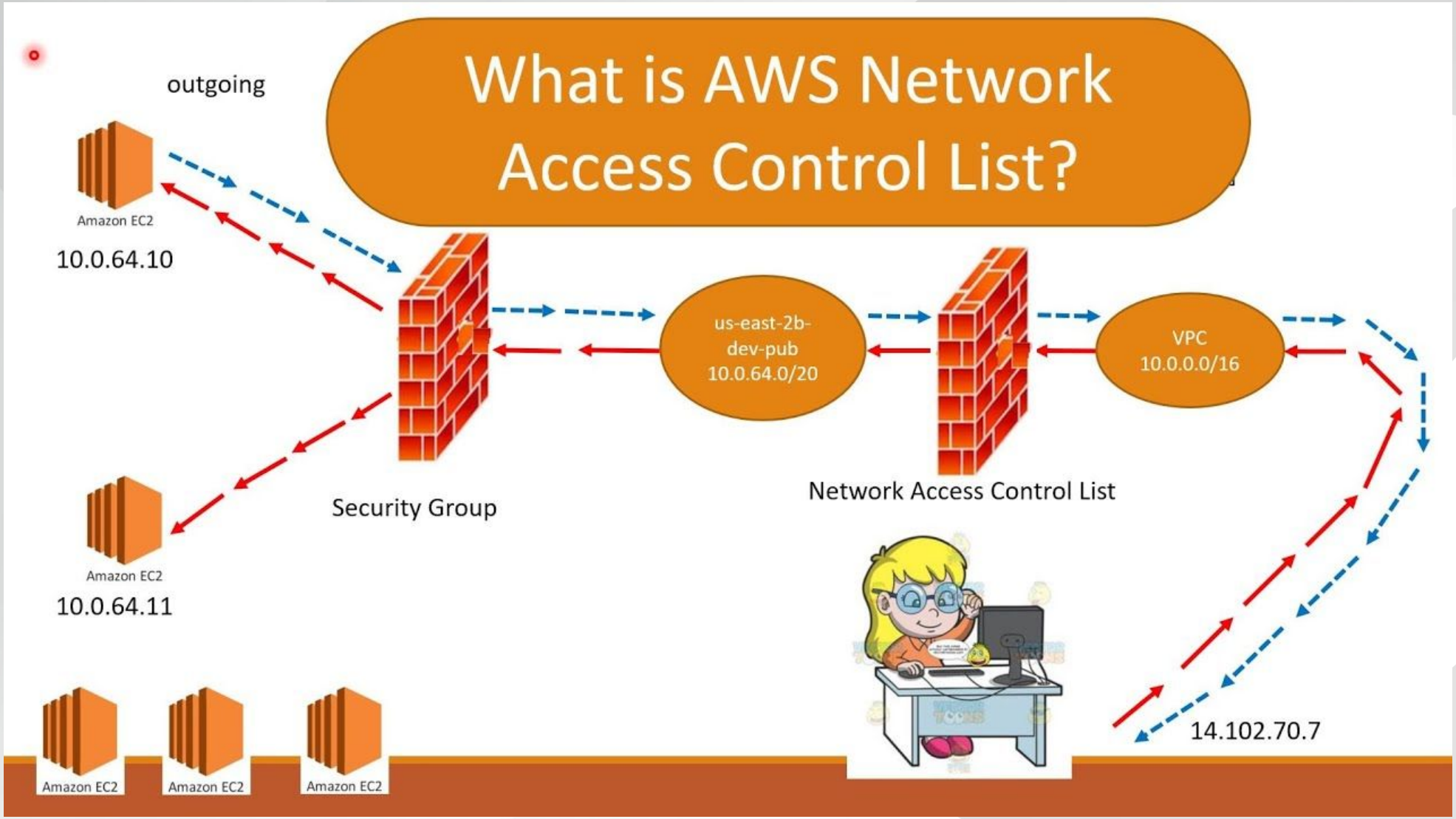
+1 (585) 304 29 59

VPC - NACL

- **Subnet** — A segment of VPC's IP address range.
- **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- **Egress only Internet Gateway** — Internet Gateway for IPv6
- **CIDR block** — Classless Inter-Domain Routing.
- **Elastic IP**
- **Bastion Host/ Jump Box**
- **NAT Gateway/ NAT Instance**
- **VPC Peering**
- **VPC Endpoint**

NACL (Network Access Control List)

TECHPRO EDUCATION

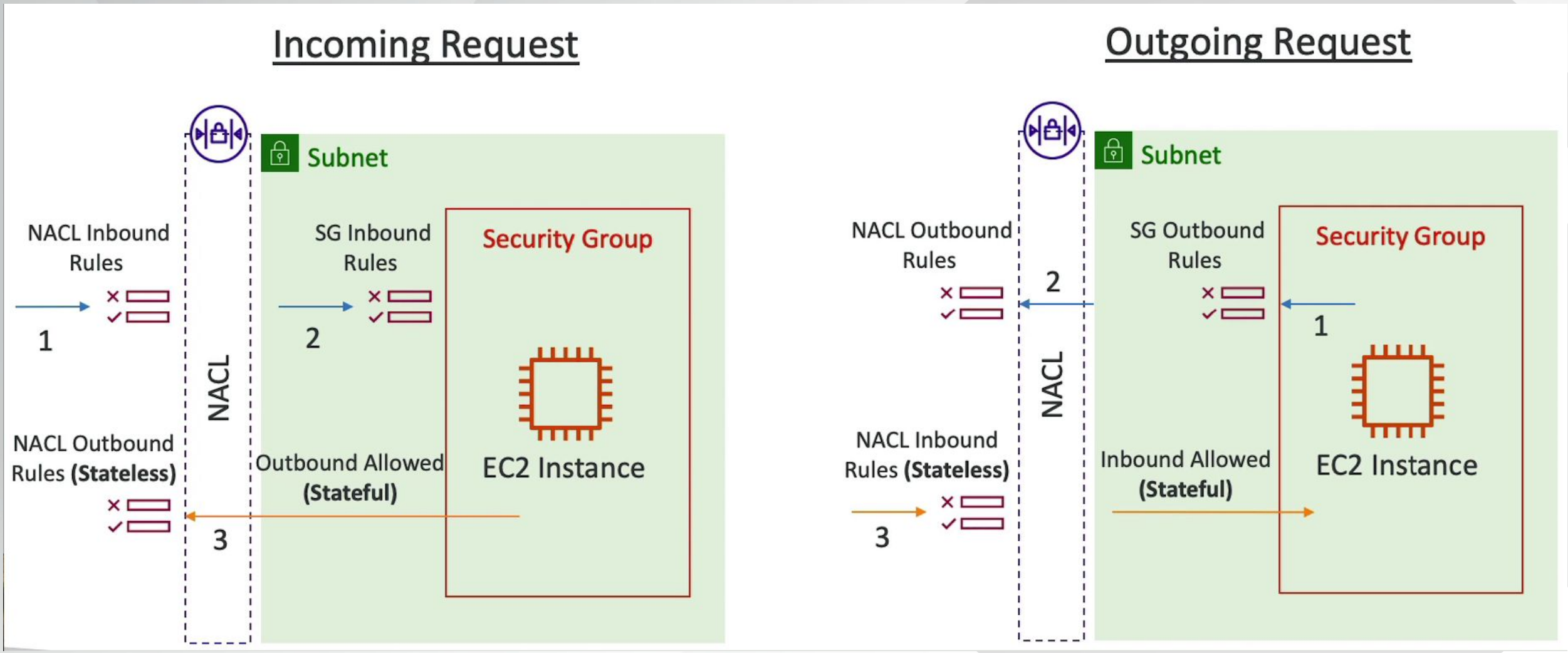


NACL (Network Access Control List)

Security Group	Network ACL (NACL)
stateful	stateless
instance-level interface	subnet-level
permit rules only	permit and deny rules
all rules examined first	rules processed until match
enabled with instance launch configuration	assigned to subnet for all instances

NACL (Network Access Control List)

TECHPRO EDUCATION



NACL (Network Access Control List)

TECHPRO EDUCATION

Inbound

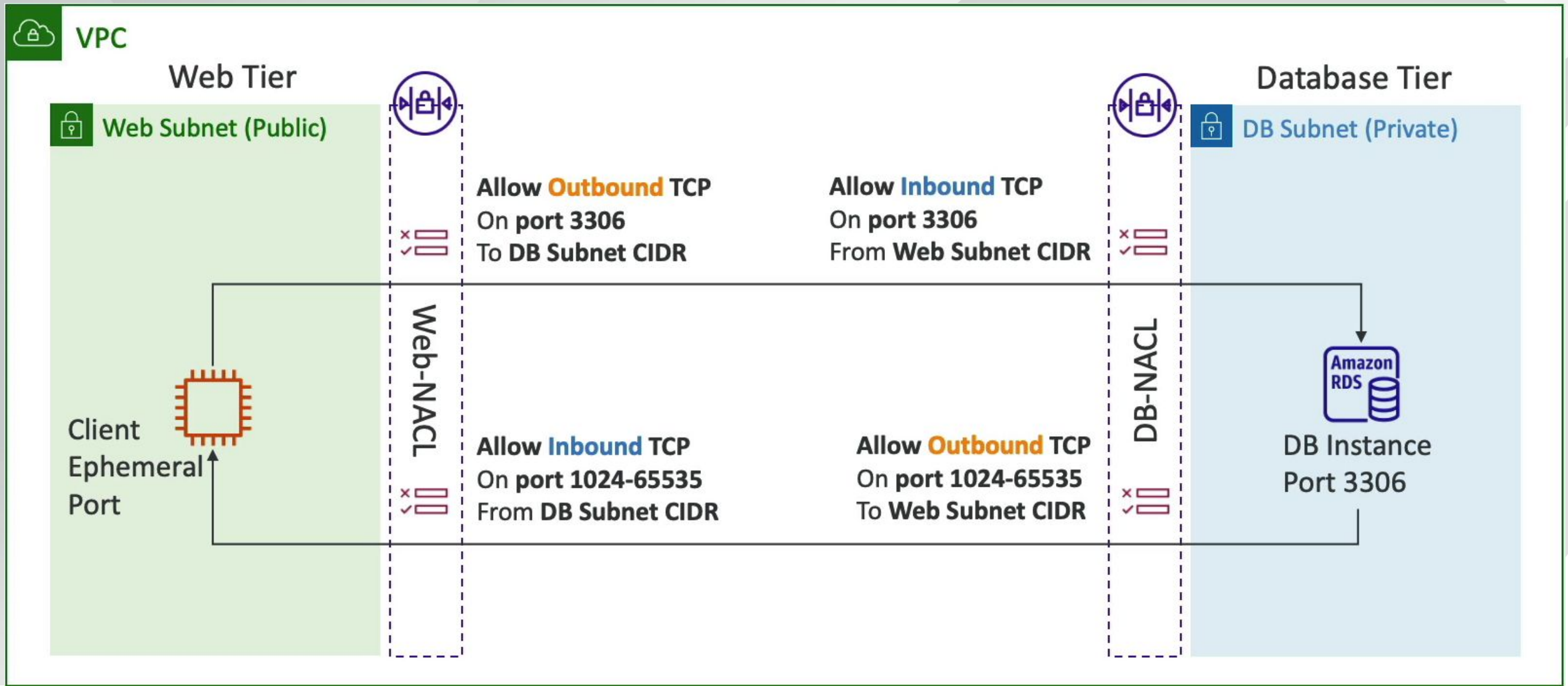
Rule #	Type	Protocol	Port range	Source	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows inbound return IPv4 traffic from the internet (that is, for requests that originate in the subnet). This range is an example only. For more information about how to select the appropriate ephemeral port range, see Ephemeral ports.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Outbound

Rule #	Type	Protocol	Port range	Destination	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTP traffic from the subnet to the internet.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTPS traffic from the subnet to the internet.
120	SSH	TCP	1024-65535	192.0.2.0/24	ALLOW	Allows outbound SSH traffic from your home network's public IPv4 address range (over the internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows outbound IPv4 responses to clients on the internet (for example, serving webpages to people visiting the web servers in the subnet). This range is an example only. For more information about how to select the appropriate ephemeral port range, see Ephemeral ports.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all outbound IPv4 traffic not already handled by a preceding rule (not modifiable).

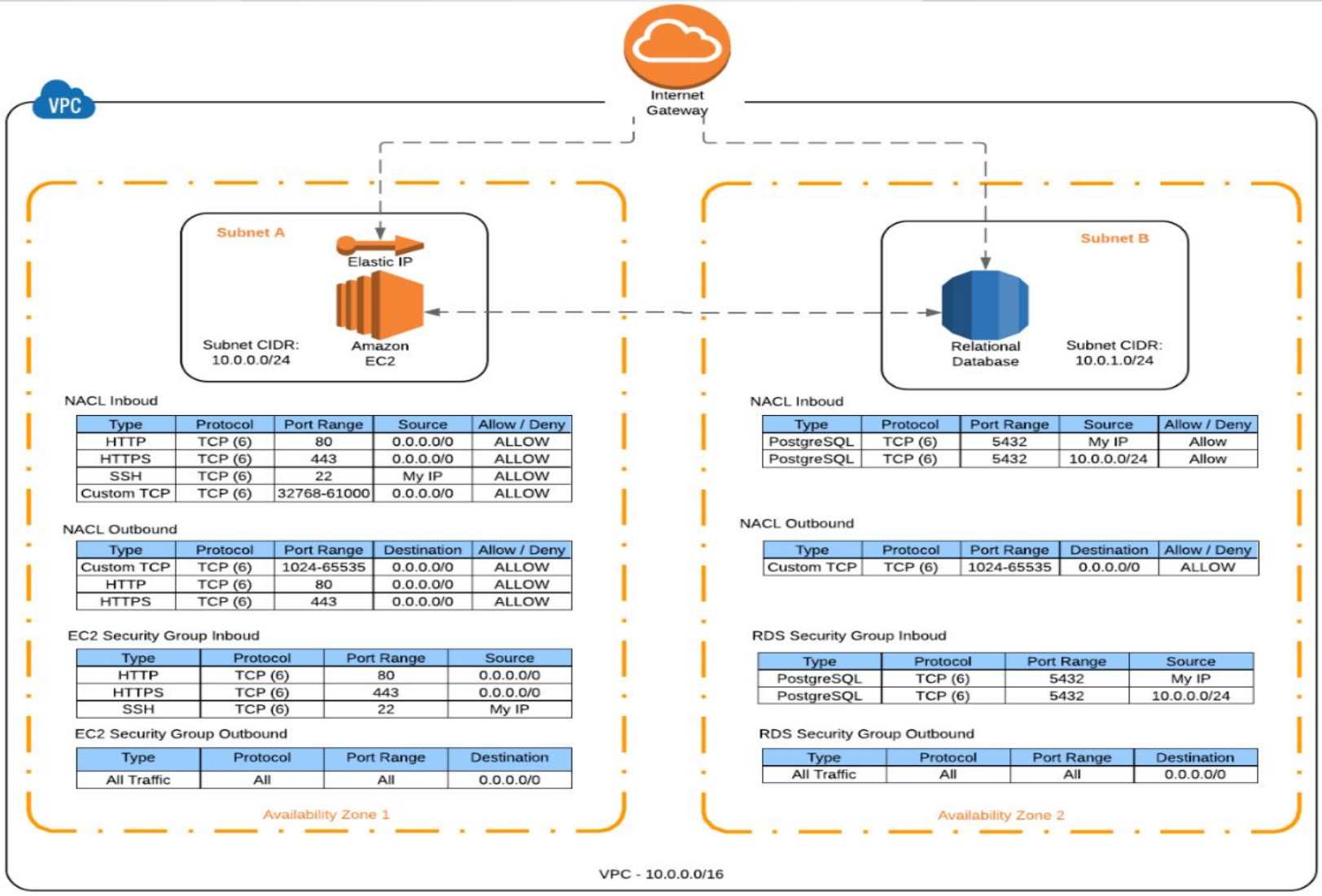
NACL Ephemeral Ports

TECHPRO EDUCATION



NACL Example

TECHPRO EDUCATION



NACL Inboud

Type	Protocol	Port Range	Source	Allow / Deny
HTTP	TCP (6)	80	0.0.0.0/0	ALLOW
HTTPS	TCP (6)	443	0.0.0.0/0	ALLOW
SSH	TCP (6)	22	My IP	ALLOW
Custom TCP	TCP (6)	32768-61000	0.0.0.0/0	ALLOW

NACL Outbound

Type	Protocol	Port Range	Destination	Allow / Deny
Custom TCP	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
HTTP	TCP (6)	80	0.0.0.0/0	ALLOW
HTTPS	TCP (6)	443	0.0.0.0/0	ALLOW

EC2 Security Group Inboud

Type	Protocol	Port Range	Source
HTTP	TCP (6)	80	0.0.0.0/0
HTTPS	TCP (6)	443	0.0.0.0/0
SSH	TCP (6)	22	My IP

EC2 Security Group Outbound

Type	Protocol	Port Range	Destination
All Traffic	All	All	0.0.0.0/0

NACL Inboud

Type	Protocol	Port Range	Source	Allow / Deny
PostgreSQL	TCP (6)	5432	My IP	Allow
PostgreSQL	TCP (6)	5432	10.0.0.0/24	Allow

NACL Outbound

Type	Protocol	Port Range	Destination	Allow / Deny
Custom TCP	TCP (6)	1024-65535	0.0.0.0/0	ALLOW

RDS Security Group Inboud

Type	Protocol	Port Range	Source
PostgreSQL	TCP (6)	5432	My IP
PostgreSQL	TCP (6)	5432	10.0.0.0/24

RDS Security Group Outbound

Type	Protocol	Port Range	Destination
All Traffic	All	All	0.0.0.0/0

NACL Exam Tips

TECHPRO EDUCATION

- ✔ Your VPC automatically creates **a default network ACL**, and by **default it allows all outbound and inbound** traffic.
- ✔ You can create **custom network ACL**s. By default, each **custom network ACL denies all inbound and outbound traffic** until you add rules.
- ✔ Each **subnet in your VPC must be associated** with a network ACL. **If you don't explicitly associate** a subnet with a network ACL, the **subnet is automatically associated with the default network ACL**.
- ✔ You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- ✔ Network **ACLs contain a numbered list of rules that is evaluated in order**, starting with the lowest numbered rule.
- ✔ Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.
- ✔ Network **ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic** (and vice versa.)
- ✔ Block **IP Addresses using network ACLs not Security Groups**.

Solution Architect Cases

TECHPRO EDUCATION

1 Malicious traffic is reaching some EC2 instances in a public subnet from a few identified public IP addresses. What do you suggest?

Use a Network ACL to deny access based on the source IP addresses

2 You have attached an Internet Gateway to your VPC, but your EC2 instances still don't have access to the internet. Which is NOT a possible issue?

a) Route Table entries are missing
b) EC2 instances do not have Public IP
c) Instances are created on Private Subnets
d) There is no VPC endpoint
e) NACL does not allow network traffic out

Troubleshooting AWS Network Connectivity

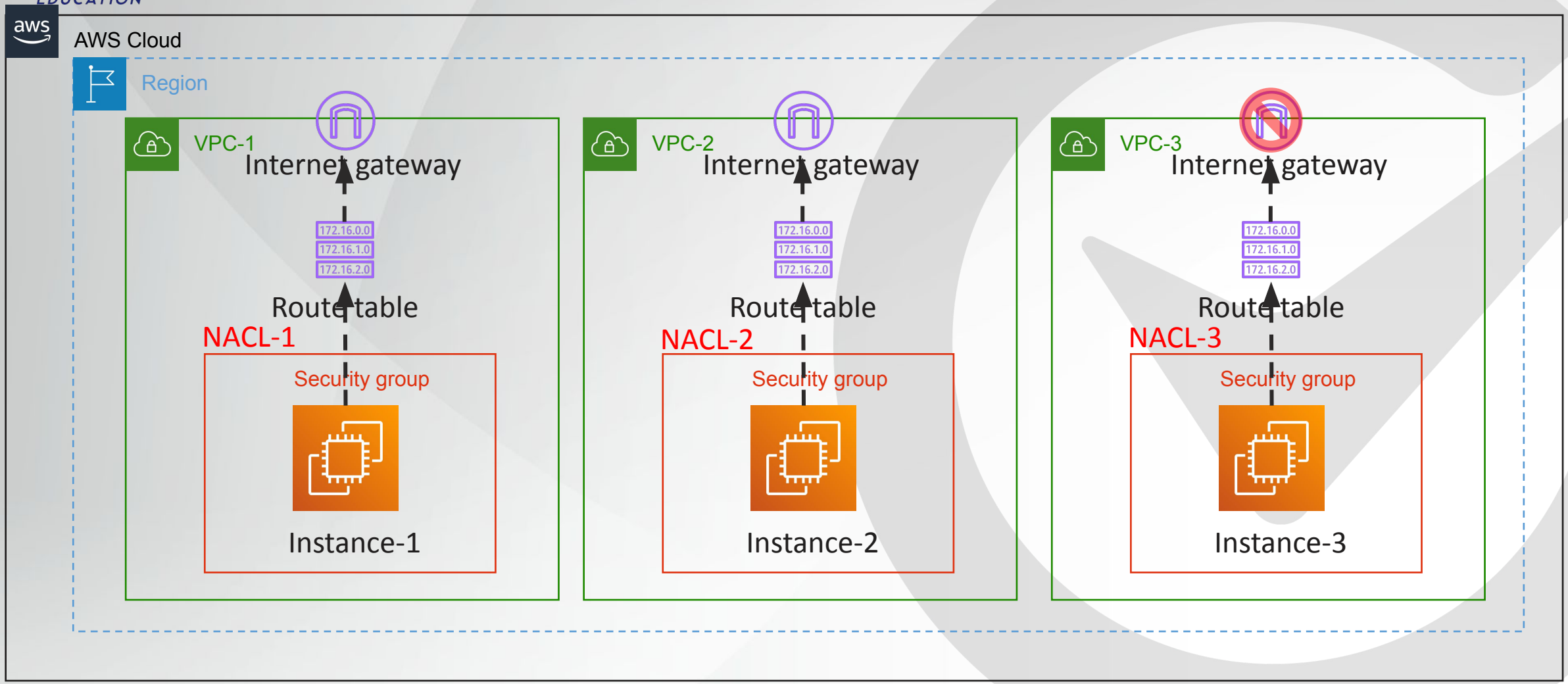
TECHPRO EDUCATION

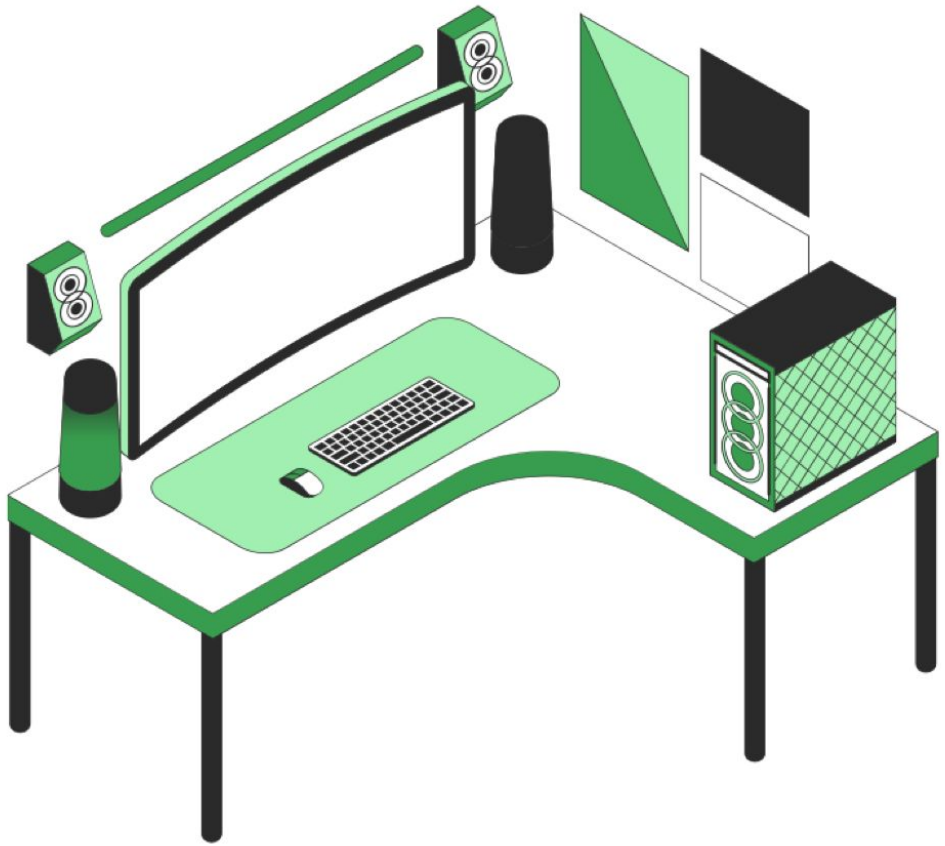
- **Scenario** :

A Junior AWS/Devops Engineer has deployed 3 instances in 3 VPCs, but there are a few things wrong. Instance-3 is not able to connect to the internet and the junior AWS/Devops Engineer can't determine why. Being a senior AWS/Devops Engineer, it's your responsibility to troubleshoot the issue and ensure the instance has connectivity to the internet so that you can ping and log in to the instance using SSH.

Troubleshooting AWS Network Connectivity: Security Groups and NACLs

TECHPRO EDUCATION





Do you have any questions?

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