



BATCH : BATCH 85

LESSON : AWS

DATE : 30.08.2022

SUBJECT : AWS NACL



techproeducation



techproeducation



techproeducation



techproeducation



techproedu

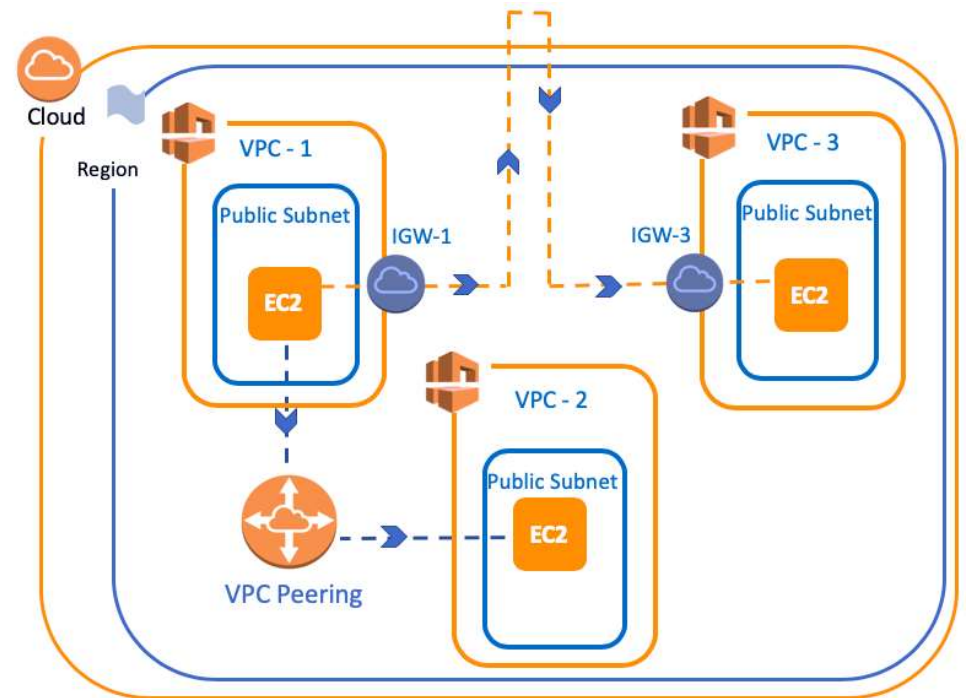


Network Access Control Lists



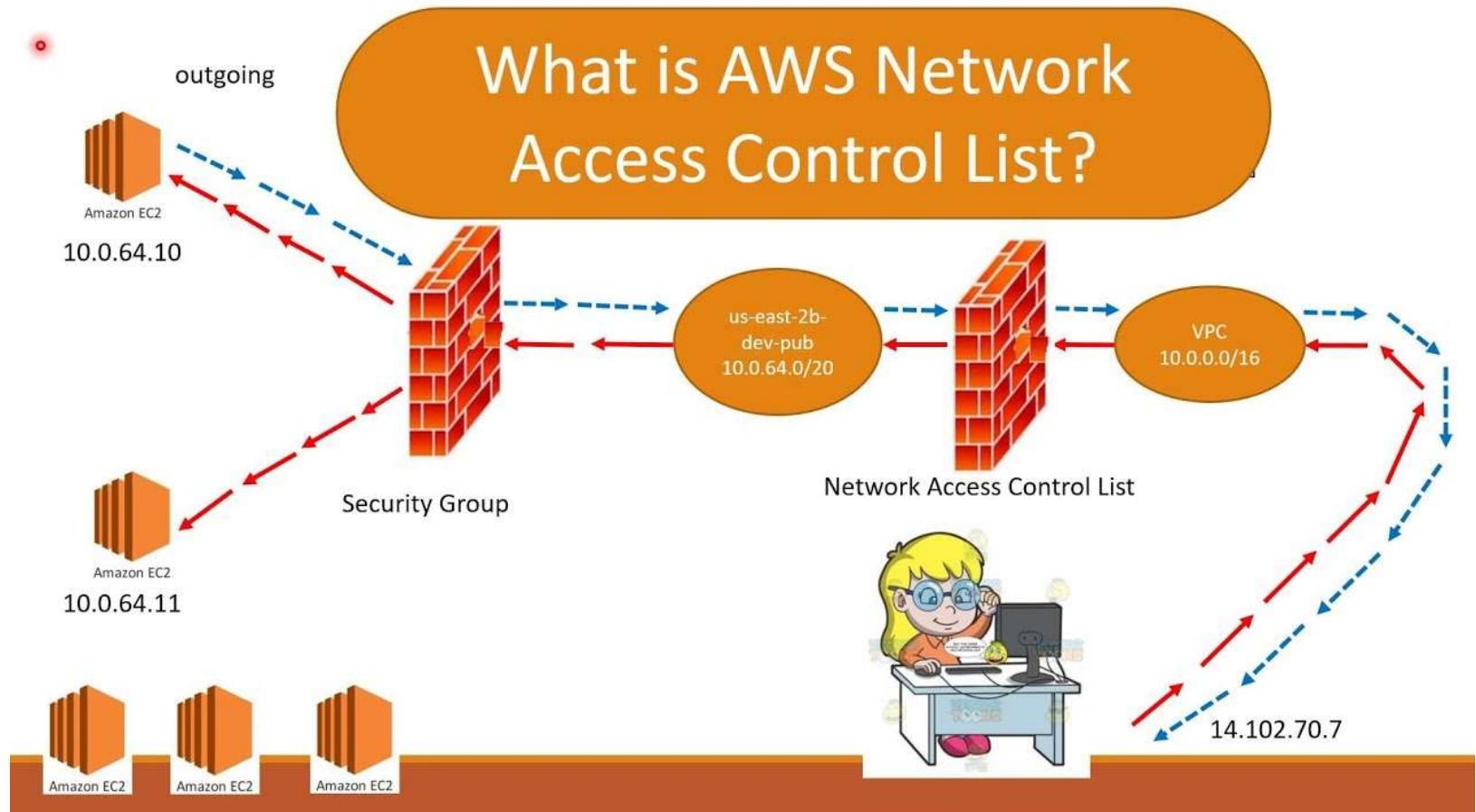
VPC Peering

- ✓ A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).





Network ACL



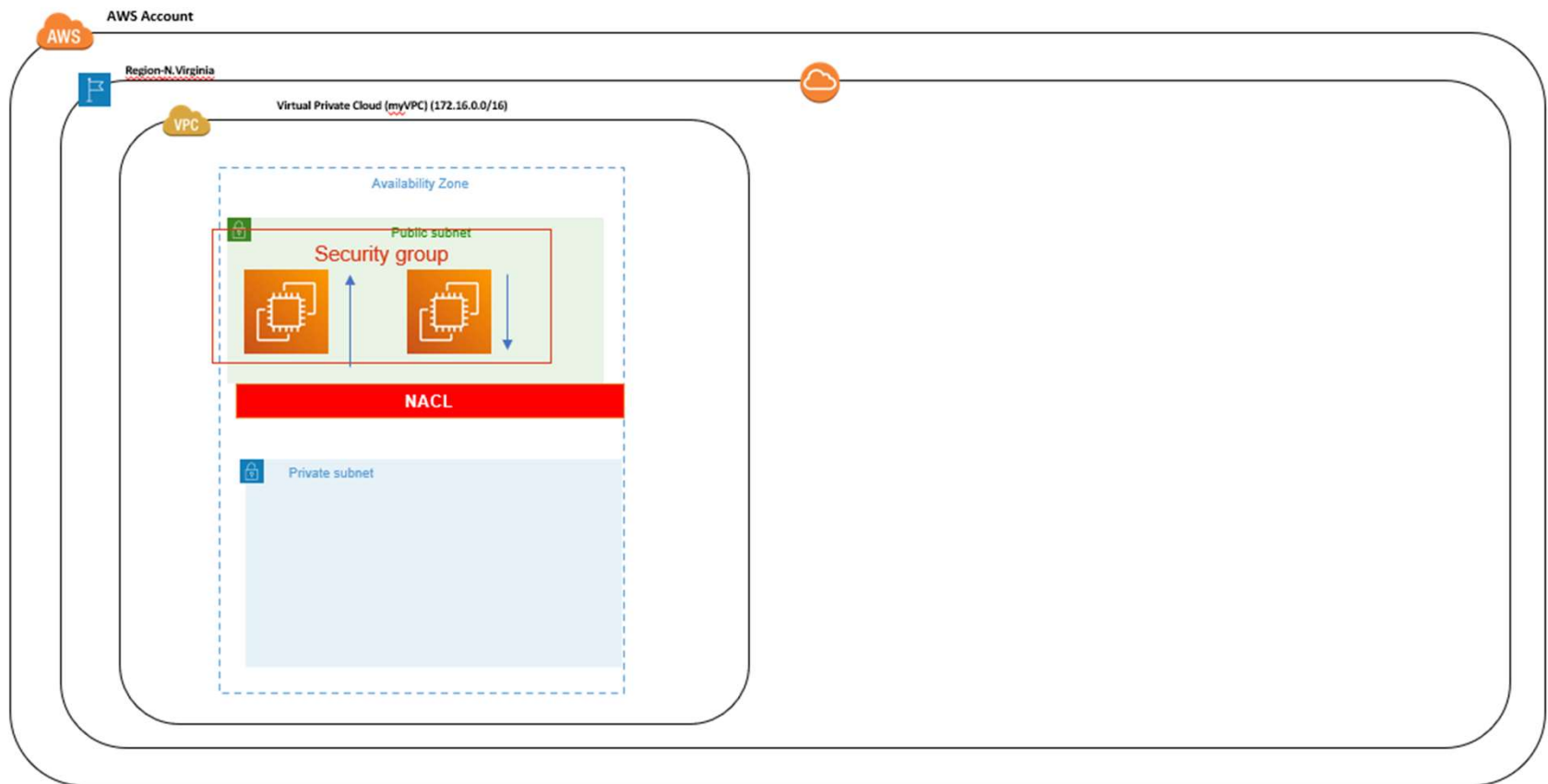


Network Access Control List

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



Network Access Control List





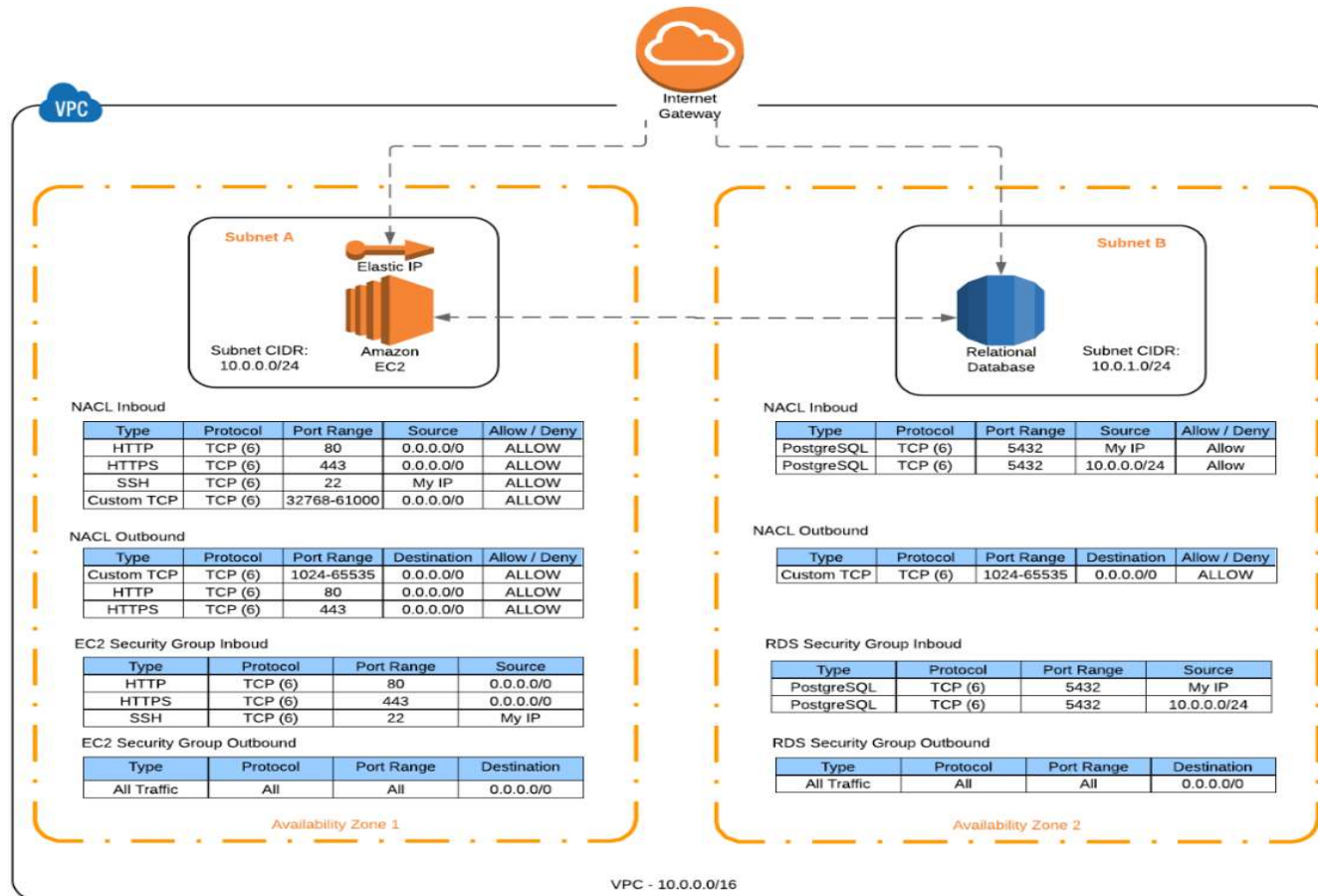
Network Access Control List

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 Example





Exam Tips:

- ✓ Your VPC automatically comes a default network ACL, and by default it allows all outbound and inbound traffic.
- ✓ You can create custom network ACLS. 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



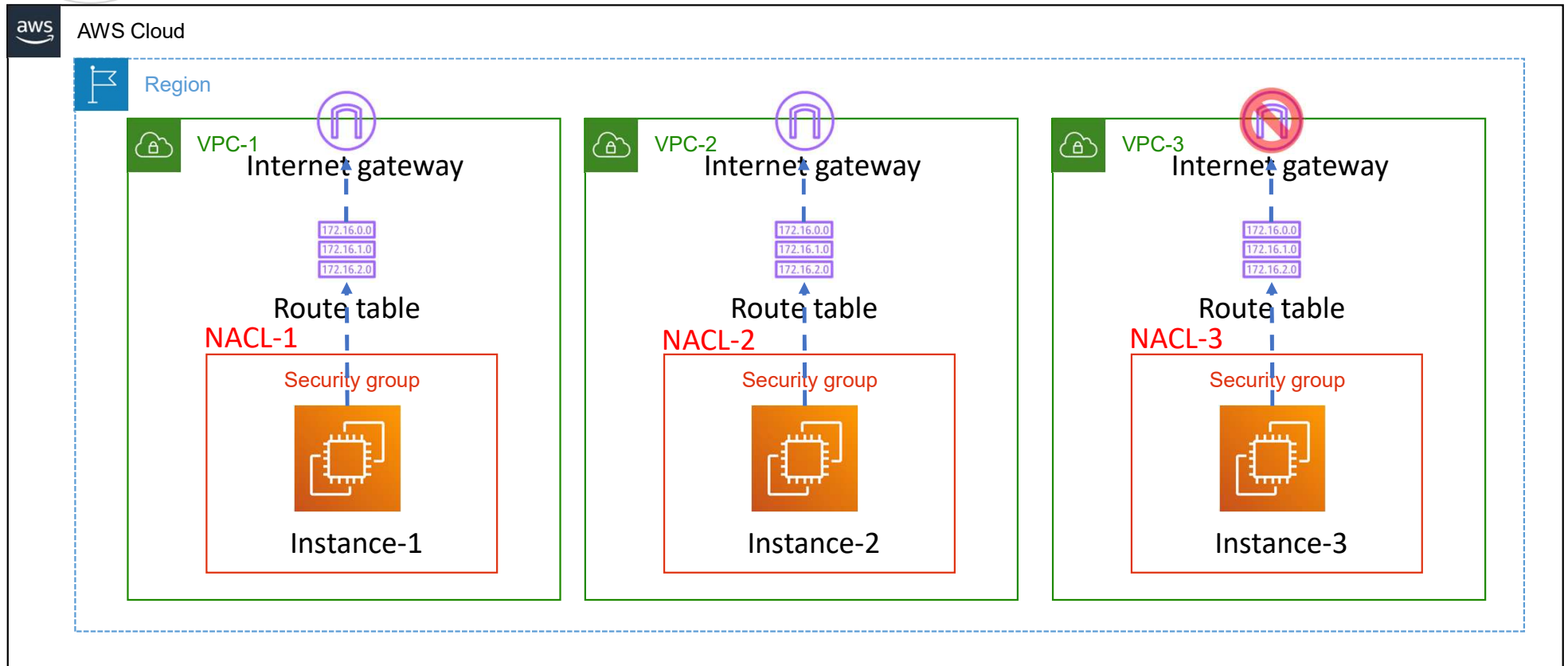
Troubleshooting AWS Network Connectivity: Security Groups and NACLs

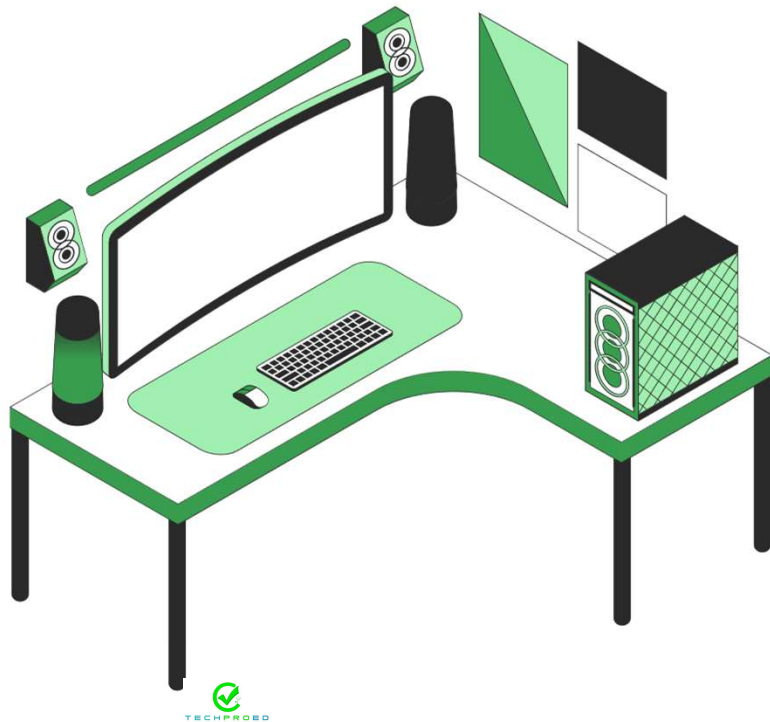
► Scenario :

In this scenario, a Junior AWS/Devops Engineer has deployed a VPC and instances, 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





Do you have any questions?

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