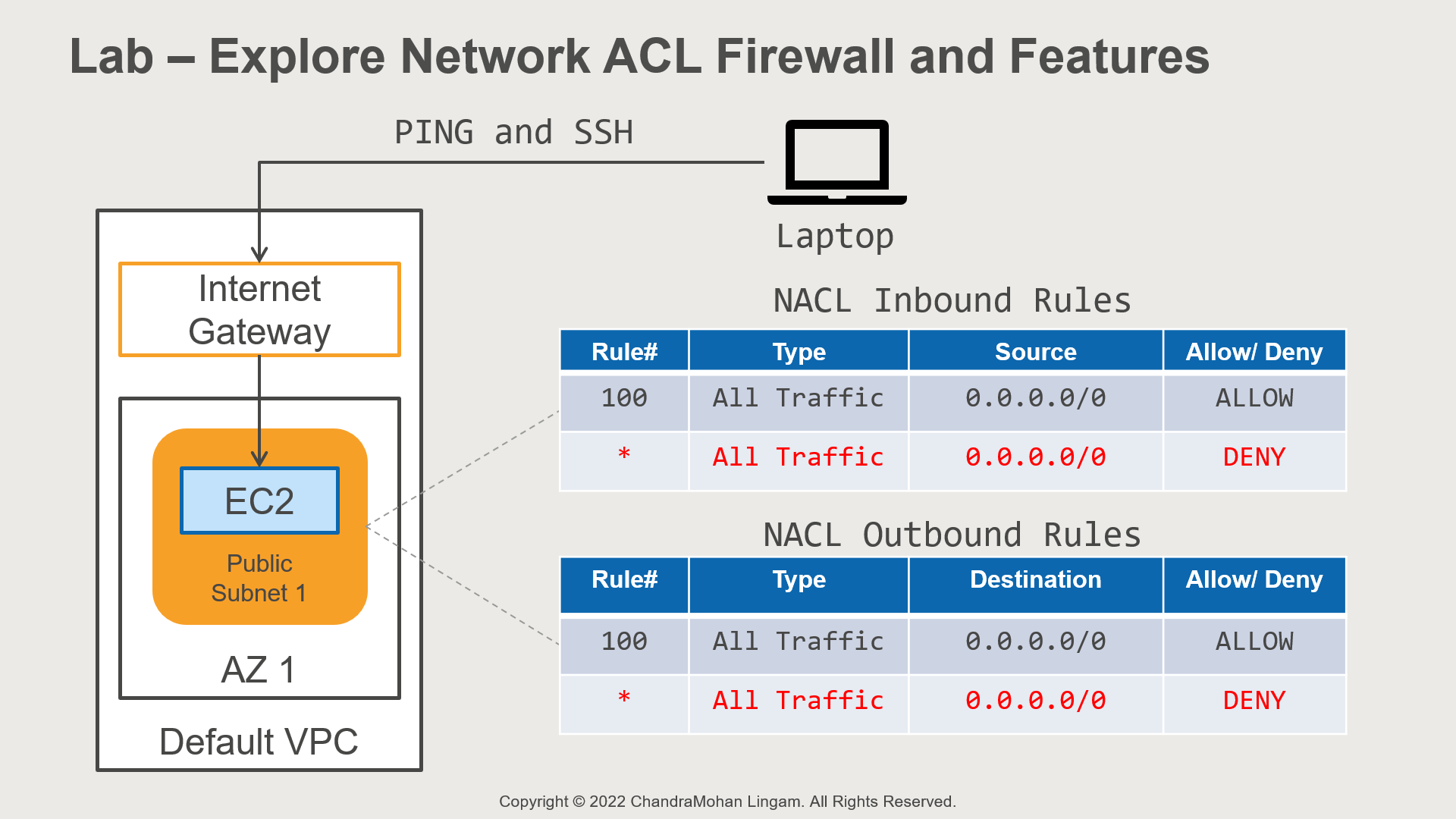
**Lab Instructions – Explore Network ACL Firewall and Features**

This instruction complements the next video **Lab – Explore Network ACL Firewall and Features**. I recommend watching the video first and following these instructions to complete the lab.



For this lab, we will launch a Linux instance in the public subnet of the default VPC and configure a security group to allow Ping and SSH traffic.

You will then learn about how to configure the Network ACL firewall to protect your subnet

We start with the default Network ACL firewall that allows all inbound and outbound traffic

And then create a new Network ACL firewall and attach it to the subnet

After this hands-on exercise, you will have a clear understanding of why a network ACL is called a stateless firewall, the purpose of inbound and outbound rules, how to allow or deny traffic

**Updated: April 2023 [Use Amazon Linux 2 AMI. Do not use Amazon Linux 2023]**

Steps

1. Open EC2 console

2. Launch an Instance

3. Name the instance: FirewallTest

4. We will use the Amazon Linux AMI

a. Choose Amazon Linux AMI

b. From AMI drop down: Select **Amazon Linux 2**

***NOTE: Do NOT use Amazon Linux 2023 AMI. This version uses a different setting for SSH and may not work correctly***

5. For instance type, use t2.micro or t3.micro – these are free-tier eligible instances. If you don’t see t2.micro, simply choose t3.micro

6. Key pair: Specify the Keypair to Login to the machine

7. Network settings - Specify VPC information

a. Edit

b. Network: Select default VPC

c. Subnet: No preference (any public subnet in default VPC is okay)

d. Auto-assign Public IP: Enable

e. Create a new security group

f. Security group name: SSHPingSG

g. Add two rules, one for SSH and another for Ping Traffic

h. Type: SSH, Protocol: TCP, Port: 22, Source: Select Anywhere [this rule should already be there]

i. Type: Custom ICMP – IPv4, Protocol: Echo Request, Source: Anywhere

8. Review and Launch

9. Wait until server state is Running

10. From your laptop, open the command line terminal and ping your EC2 instance’s public IP address

ping PublicIP

11. You would see a ping response from the instance

Steps – Create a new Network ACL firewall

1. Open VPC console

2. From the left navigation pane – select Network ACLs (it is under Security)

3. Create network ACL

a. Name: customNACL

b. VPC: default VPC

c. Create

4. From the network ACL list, select customNACL

5. Go to the Inbound rules tab

6. For new NACL, all inbound and outbound traffic is denied by default

7. Let’ add a new inbound rule to allow ALL traffic

8. Edit inbound rules

9. Add rule

a. Rule Number: 100 [rules are evaluated from smallest number first, and the first rule that matches the traffic decides the outcome]

b. Type: All traffic

c. Protocol: All

d. Port range: All

e. Source: 0.0.0.0/0

f. Allow/Deny: Allow

g. Save changes

10. Let’s add a new outbound rule to allow ALL traffic

11. Go to the Outbound rules tab

12. Edit outbound rules

13. Add rule

a. Rule Number: 100 [rules are evaluated from smallest number first. The first rule that matches the traffic decides the outcome]

b. Type: All traffic

c. Protocol: All

d. Port range: All

e. Destination: 0.0.0.0/0

f. Allow/Deny: Allow

g. Save changes

14. customNACL now allows all inbound and outbound traffic

15. We now need to attach the customNACL to all our subnets in the default VPC

16. Go to the Subnet associations tab

17. Edit subnet associations

18. Select all the subnets in the default VPC

19. Save changes

20. Let’s check the connectivity to our instance

21. From your laptop, ping your EC2 instance’s public IP address

ping PublicIP

22. The EC2 instance will respond to ping requests, and requests are now passing through the customNACL firewall

Steps – Stateless Nature of the Firewall

1. What will happen if we remove all the outbound rules in the Network ACL?

2. The inbound NACL rule allows all traffic, and we are going to remove the outbound rules

3. From the left navigation pane in the VPC console – select Network ACLs

4. Choose customNACL

5. In the details pane, go to the Outbound Rules tab

6. Edit outbound rules

a. Remove the first rule (Rule number 100)

b. Save changes

7. From your laptop, ping your EC2 instance’s public IP address

ping PublicIP

8. The server receives the ping request, but the response from the server is blocked. This is because the Network ACL is stateless, and it evaluates inbound and outbound traffic separately

9. In the outbound rule, the default rule \* is denying all the response traffic

10. Let’s allow all Outbound traffic again

11. Edit outbound rules

12. Add rule

a. Rule Number: 100 [rules are evaluated from smallest number first. The first rule that matches the traffic decides the outcome]

b. Type: All traffic

c. Protocol: All

d. Port range: All

e. Destination: 0.0.0.0/0

f. Allow/Deny: Allow

g. Save changes

13. From your laptop, ping your EC2 instance’s public IP address

ping PublicIP

14. You should now see the ping response from the server!

Steps – Block Ping Requests

1. Let’s look at how we can block traffic using Network ACL

2. We are going to block all Ping requests

3. Choose customNACL

4. Go to the Inbound Rules tab

5. Edit inbound rules

6. Rule 100 allows all traffic

7. Add a new inbound rule

a. Rule Number: 50 – this has to be smaller than 100, so that deny rule is evaluated first

b. Type: Custom ICMP – IPv4

c. Protocol: Echo Request

d. Source: 0.0.0.0/0

e. Allow/Deny: Deny

f. Save rules

8. So, the inbound rule 50 is going to block ping requests, and all other requests are allowed

9. From your laptop, ping your EC2 instance’s public IP address

ping PublicIP

10. You should not see any response as the ping request is blocked

11. However, other traffic like SSH is allowed

12. Let’s log in to the instance using SSH. I am using putty

13. And we can connect to the server

14. So, using Network ACL, we can decide what traffic is allowed in and out of a subnet

Steps – Cleanup

1. From the EC2 console, terminate the FirewallTest instance and wait until the instance state is Terminated

2. From the VPC console, let’s remove customNACL

3. Go to Network ACLs in the left navigation pane

4. We need to reassign default NACL to all our subnets

5. Select the default NACL for the default VPC

6. Select Subnet associations tab

7. Edit subnet associations

8. Choose all the four subnets in the default VPC

9. Save changes

10. Let’s remove the customNACL

11. Select customNACL

12. From the Actions menu, choose Delete network ACLs

13. Confirm and delete

14. Let’s delete the SSHPingSG security group

15. Select Security Groups in the left navigation pane

16. Choose SSHPingSG security group

17. From the Actions menu, select Delete security groups

18. Confirm and delete

Summary

In this lab, we learned how to configure the Network ACL firewall to protect your subnet

All traffic to the subnet must pass through the NACL firewall.

We also saw the stateless nature of the NACL firewall, where inbound and outbound traffic is evaluated separately.

With NACL, we can put an explicit Deny rule to block traffic. Compared to this, we can put only allow rules in a security group.

