Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

72%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Task 3 Cloud Security Concepts

Task 4 Cloud Security Risks Concerning Deployment Models

Task 5 Security Through Access Management

Task 6 Security Through Policies

Task 7 Security Through Network Management

Network security is an essential component of cloud security to protect the infrastructure from intruders. Cloud computing is inherently different from the on-premises model, wherein various approaches, including physical firewalls, protect on-premises deployments. Generally, network security of cloud infrastructure is maintained by following a layered approach:

- **Layer 1 – Network Security through Security Groups:** Security groups are the most fundamental aspect of maintaining network security in cloud infrastructure. In simple terms, security groups are a set of “allow rules” that allows specific traffic. Contrary to traditional firewalls, security groups do not have “deny rules”. The absence of any "allow rule" against particular traffic means it is denied. So we can say that security groups operate on the principle of “**deny all unless allowed explicitly**”.
- **Layer 2 – Network Security through Network Access Control Lists (NACLs):** The concept of NACL is related to protecting the Virtual Private Cloud (VPC). NACLs are used to create rules to protect specific instances of VPC. NACLs are different from Security Groups in that NACLs contain "deny rules" as well; e.g. we may make a rule to block a particular IP address from accessing the VPC.
- **Layer 3 - Vendor Specific Security Solutions:** Cloud computing service providers are also well aware of the inherent weaknesses & cyber-attacks that can target their infrastructure. So they have deployed their specific security solutions. These solutions vary from vendor to vendor, e.g. AWS has DNS Firewall & Network Firewall both.

Network Security in AWS

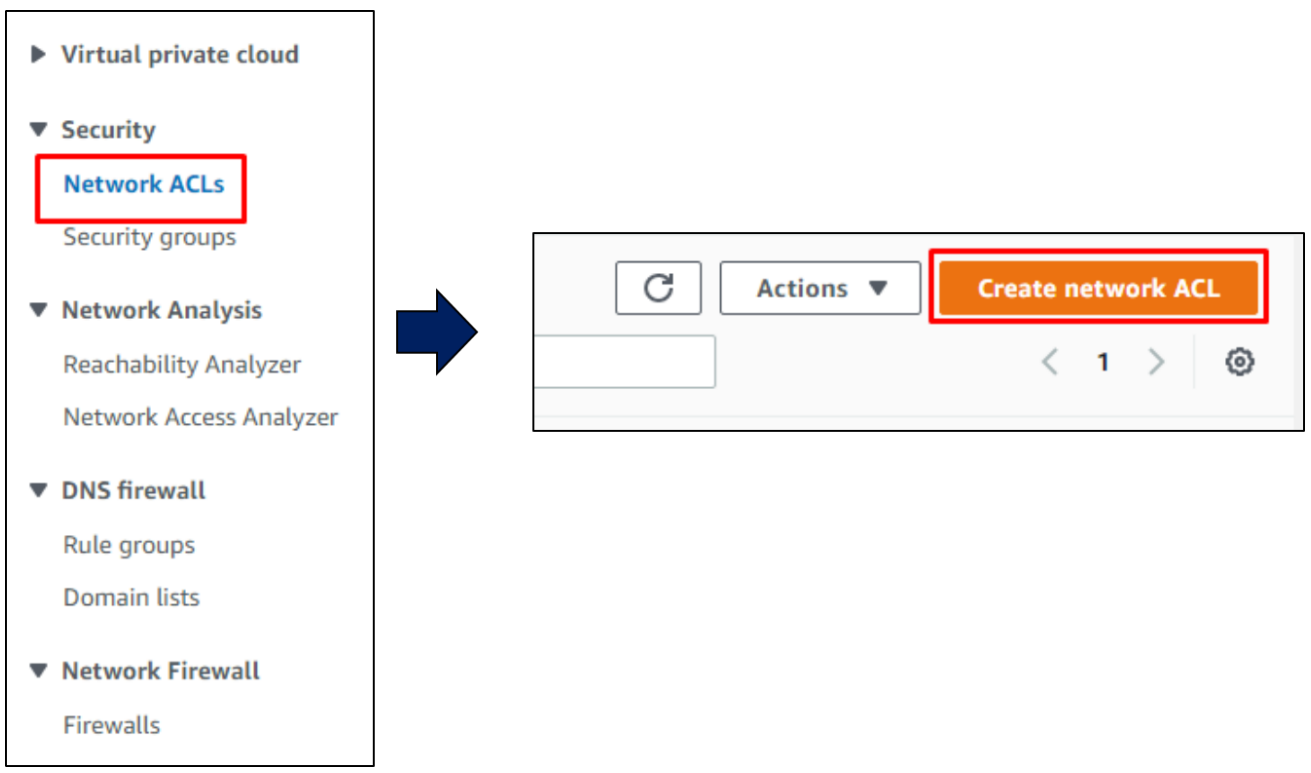
The following components manage network security in AWS:

- Security Groups.
- Network Access Control List.
- DNS Firewall.
- Network Firewall

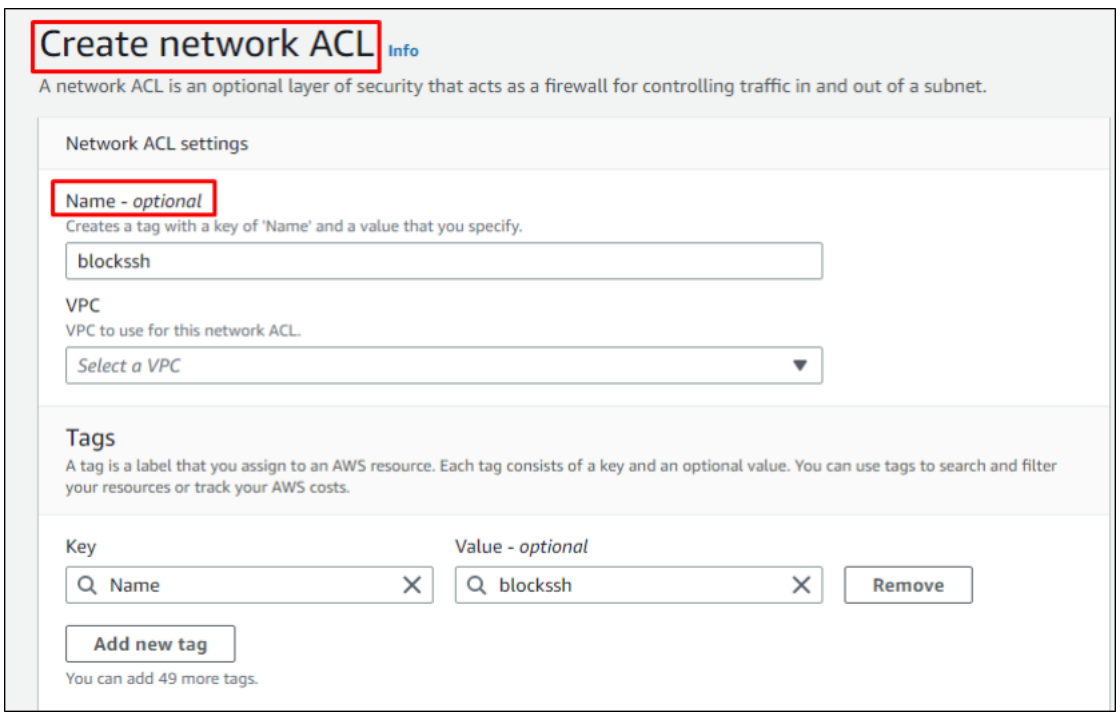
Practical Exercise

In this exercise, we will Deny All traffic on Port 22 via NACL through the following steps:

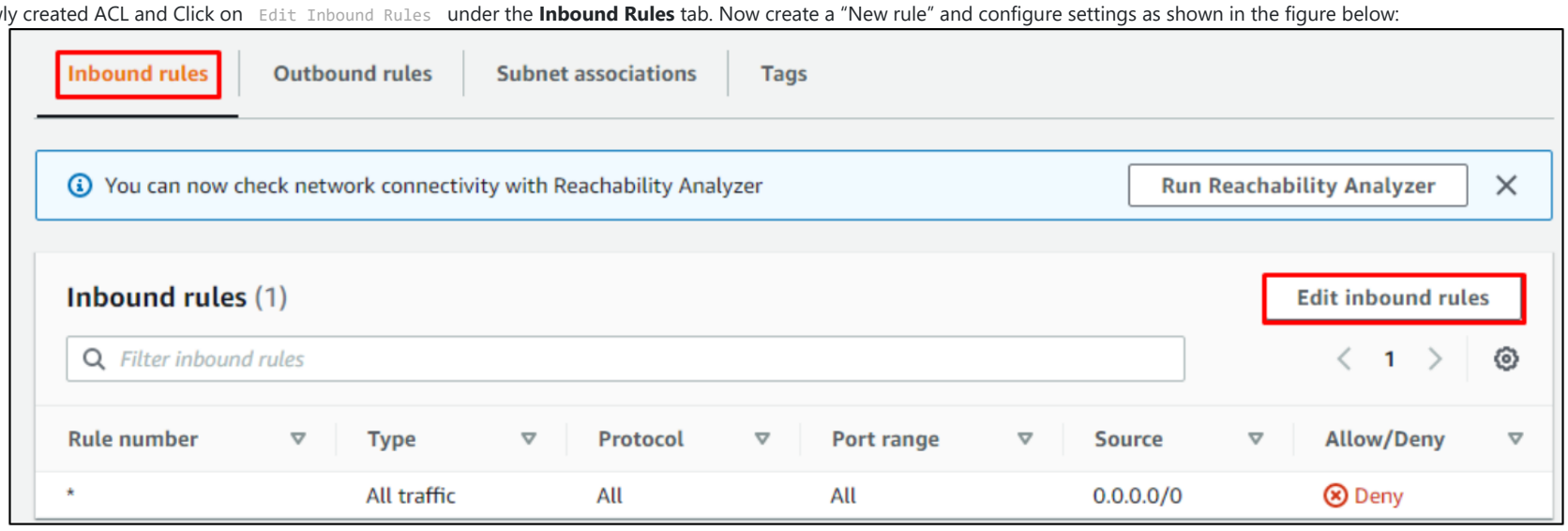
- Login to your AWS account & Navigate to VPC in the services menu
- Open NACL in the left pane & Click on `Create Network ACL`

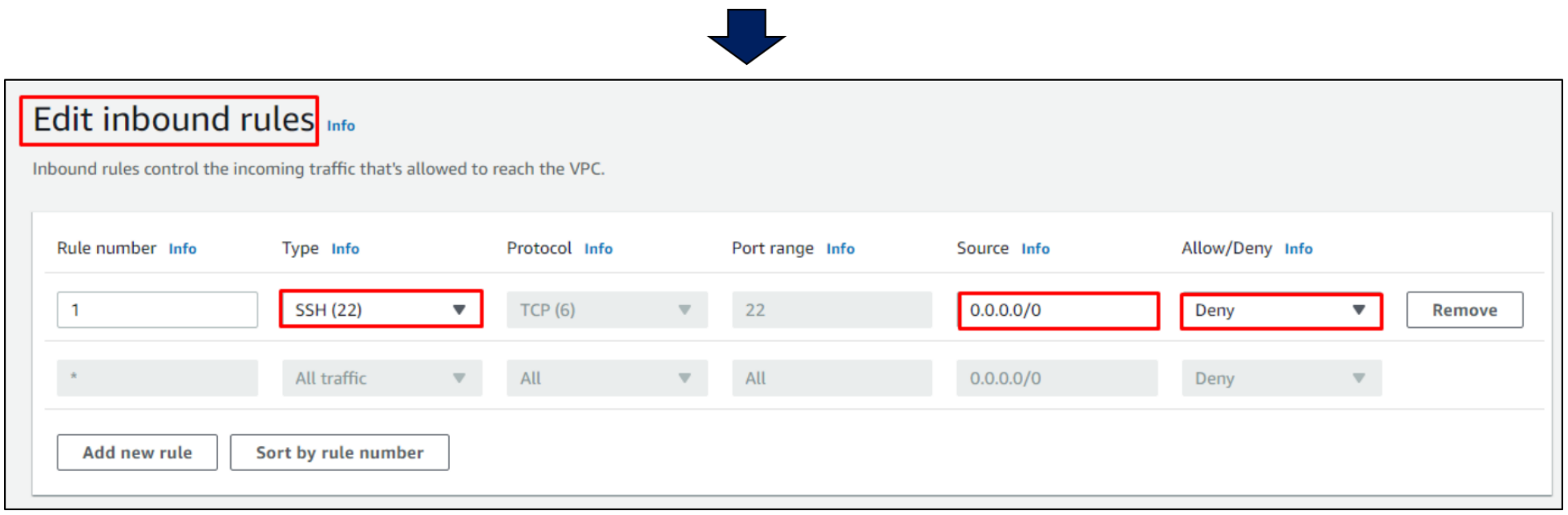


- Enter basic settings such as name, VPC and tags (optional) and click create network ACL



- Select the newly created ACL and Click on `Edit Inbound Rules` under the **Inbound Rules** tab. Now create a "New rule" and configure settings as shown in the figure below:





The above rule will deny all the traffic at port 22. We can also allowlist/blocklist specific IPs for connecting to any port to limit the attack surface for the intruder.

Answer the questions below

Is it a good practice to operate security groups on the principle of "deny all unless allowed explicitly" (yea/nay)?

yea — Correct Answer

I have completed the practical exercise.

No answer needed — Correct Answer

Task 8 ○ Security Through Storage Management

Task 9 ○ Cloud Security - Some Additional Concepts

Task 10 ○ Conclusion