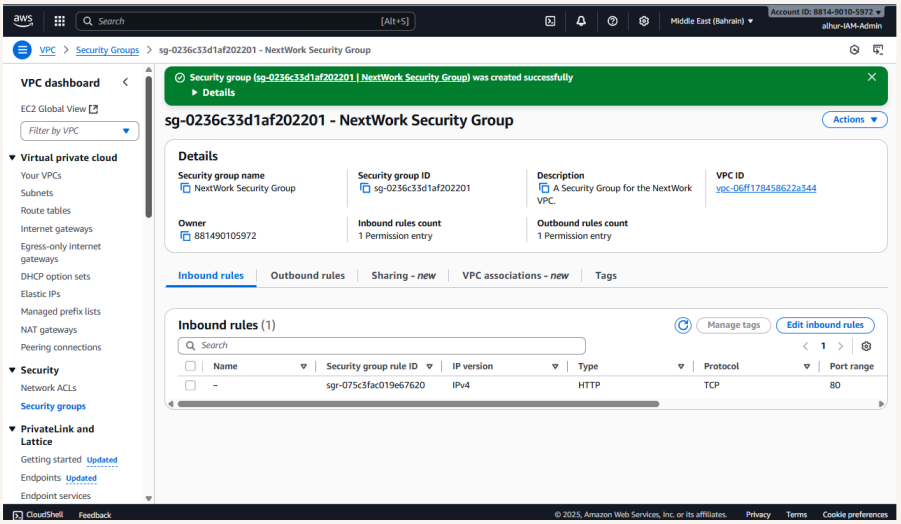
nextwork.org

VPC Traffic Flow and Security

al7r



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a private, isolated network in the AWS cloud where you can launch and manage your resources. It is useful because it gives you control over your network environment, including IP address ranges, subnets, route tables, and security settings, allowing secure and organized communication between resources

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a private network, divide it into subnets, attach an internet gateway, set up route tables for traffic flow, and configure security groups and a network ACL to control access and protect resources.

One thing I didn't expect in this project was...

One thing I didn’t expect was how many different layers of traffic control and security—route tables, security groups, and network ACLs—are needed to properly manage and protect a single VPC.

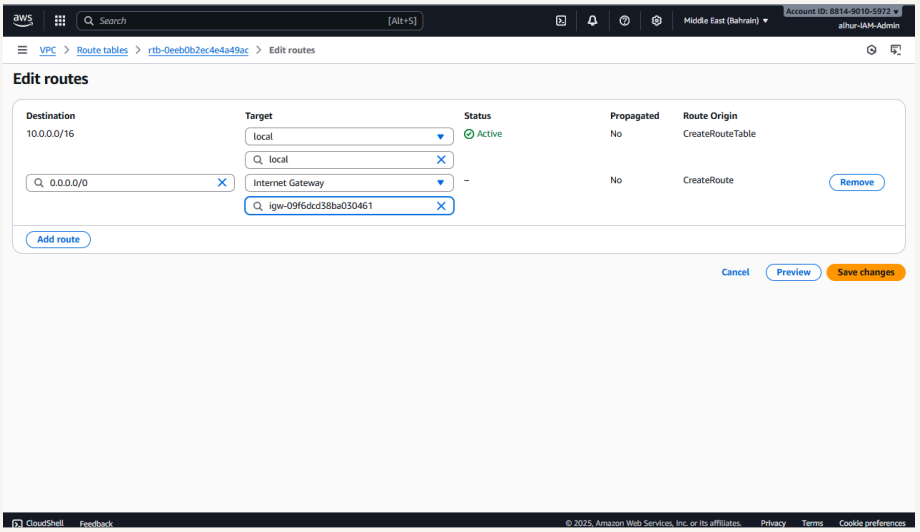
This project took me...

This project took approximately 1 hour to complete, including setting up the VPC, subnets, route tables, security group, and network ACL, and verifying that everything was configured correctly.

Route tables

Route tables are rules that control where network traffic goes inside a VPC. Every subnet in your VPC must be associated with a route table, and the rules in that table decide how traffic is directed. For example, if the route table has a rule that says all traffic going to the internet (0.0.0.0/0) should use the internet gateway, then resources in that subnet can connect to the internet. Without a proper route in the table, traffic would stay stuck inside the VPC and never reach its destination.

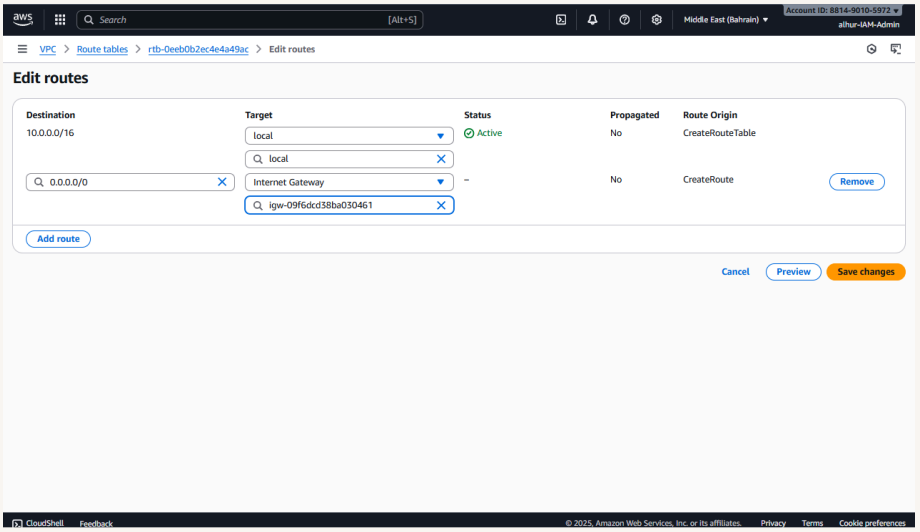
You need a route table to make a subnet public because, even if the subnet has an internet gateway attached to the VPC, the subnet itself won't know how to reach the internet unless the route table explicitly tells it where to send the traffic. By adding a rule in the route table that sends all outbound traffic (0.0.0.0/0) to the internet gateway, resources inside that subnet gain internet access, which is what makes it a public subnet. Without that route, the subnet would remain private and isolated.


Search
[Alt+S]
Middle East (Bahrain)
Account ID: 8814-9010-5972
alhur-IAM-Admin
VPC
Route tables
rtb-0eeb0b2ec4e4a49ac
Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
–
No
CreateRoute
Remove
igw-09f6dcd38ba030461
Add route
Cancel
Preview
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Route destination and target

A route's destination defines the IP range for the traffic, and the target defines where that traffic should be sent. For example, a destination of 0.0.0.0/0 with a target of an internet gateway sends all internet-bound traffic from the subnet through that gateway.

The new route's destination is 0.0.0.0/0, which means all IPv4 addresses, and the target is the Internet Gateway (NextWork IG), which directs traffic from the subnet to the internet.



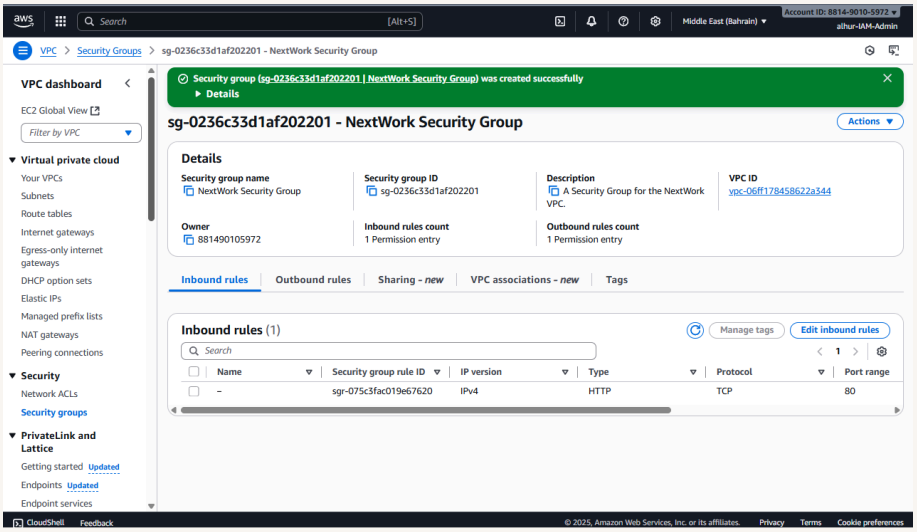
Security groups

Security groups are virtual firewalls attached to individual resources in a VPC that control inbound and outbound traffic. They allow or block traffic based on rules specifying protocols, port numbers, and source or destination IP addresses, ensuring that only authorized connections can reach the resource.

Inbound vs Outbound rules

An inbound rule defines what traffic is allowed to enter a resource from the network. My security group's inbound rules specify which protocols, ports, and IP addresses can access the resource, controlling who can connect to it.

An outbound rule defines what traffic a resource can send out. In my security group, the outbound rules allow all traffic by default, meaning the resource can communicate freely with any IP address, whether inside the VPC or on the internet, while the inbound rules specifically control who can access the resource.


Search
[Alt+S]
Middle East (Bahrain)
Account ID: 8814-9010-5972
alhur-IAM-Admin
VPC
Security Groups
sg-0236c33d1af202201 - NextWork Security Group
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
Endpoints Updated
Endpoint services
Security group (sg-0236c33d1af202201 | NextWork Security Group) was created successfully
Details
sg-0236c33d1af202201 - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-0236c33d1af202201
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-06ff178458622a344
Owner
881490105972
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
–
sgr-075c3fac019e67620
IPv4
HTTP
TCP
80
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Network ACLs

Network ACLs (Access Control Lists) are optional, subnet-level firewalls in a VPC that control inbound and outbound traffic. They act as a second layer of defense, allowing or denying traffic for all resources within a subnet based on rules specifying protocols, ports, and IP addresses.

Security groups vs. network ACLs

Security groups act as virtual firewalls for individual resources, controlling traffic at the resource level, while network ACLs control traffic at the subnet level and apply to all resources within that subnet. Security groups are stateful (responses are automatically allowed), whereas network ACLs are stateless (responses must be explicitly allowed).

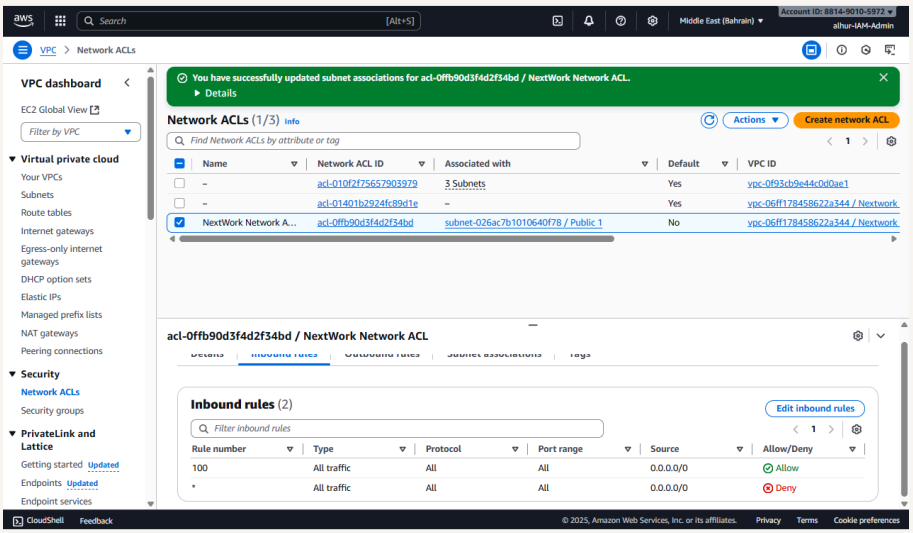
al7r
NextWork Student

Default vs Custom Network ACLs

Similar to security groups, network ACLs use inbound and outbound rules

The default network ACL allows all inbound and outbound traffic. This means any traffic can enter or leave the subnet unless you create custom rules to restrict it.

A custom network ACL's inbound or outbound rule explicitly allows or denies traffic based on protocol, port range, and source or destination IP. This gives you control over which traffic can enter or leave the subnet.



The place to learn & showcase your skills

Check out nextwork.org for more projects