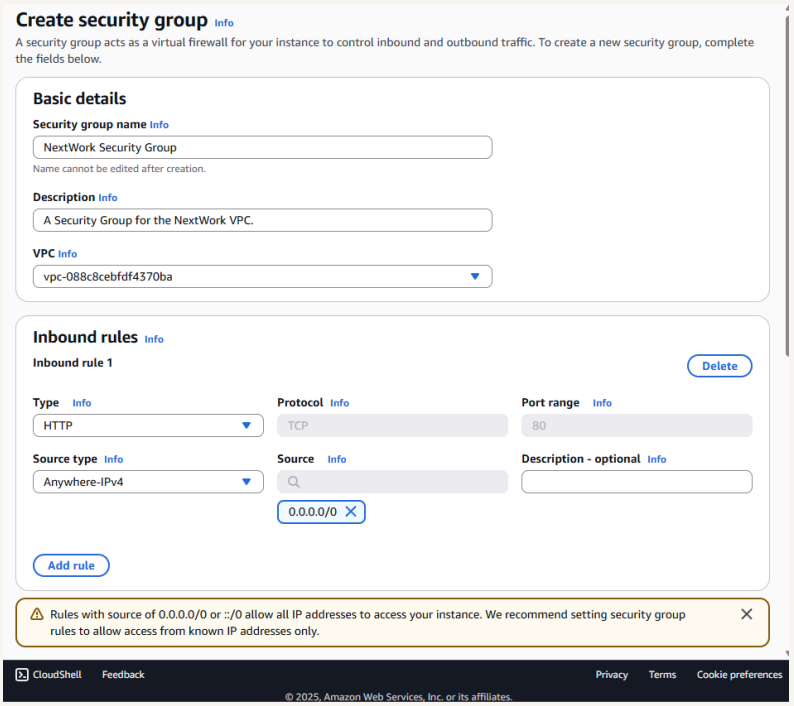
nextwork.org

VPC Traffic Flow and Security

D Duc Thai



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is your private network in AWS. You pick IP ranges, create subnets, and set routes/firewalls. It lets you isolate and secure apps, control internet access, and connect safely to your office network.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to controll traffic between my resource and the pubic internet, I do that by creating route table to get subnet to ig, sg for resources in subnet and NACL for guarding subnet in and out traffic.

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

One thing I didn't expect in this project was a public subnet can still not be public even tho it has public IP and internet gateway. A public IP + an attached IGW aren’t enough—without route table, traffic can’t enter or leave.

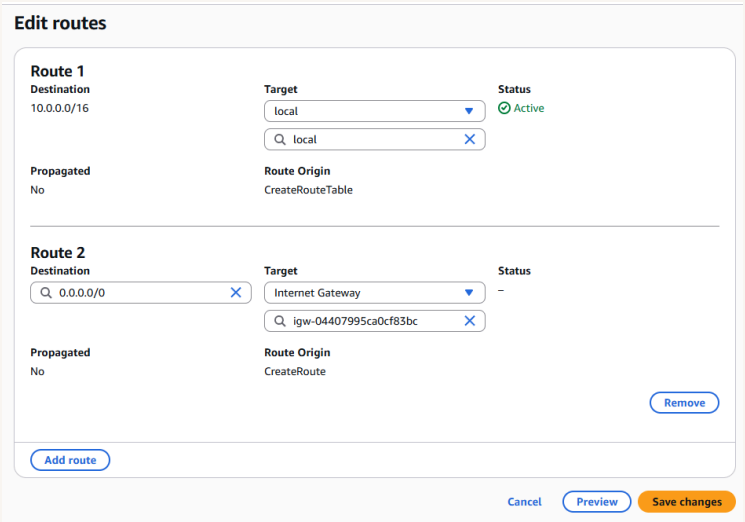
This project took me...

This project took me 2 hours.

Route tables

Route tables are rules list in a VPC that tell traffics where to go. Each subnet uses one to send traffic to the internet, other subnets, or your office (via VPN). They define paths; security groups and network ACLs control who can access.

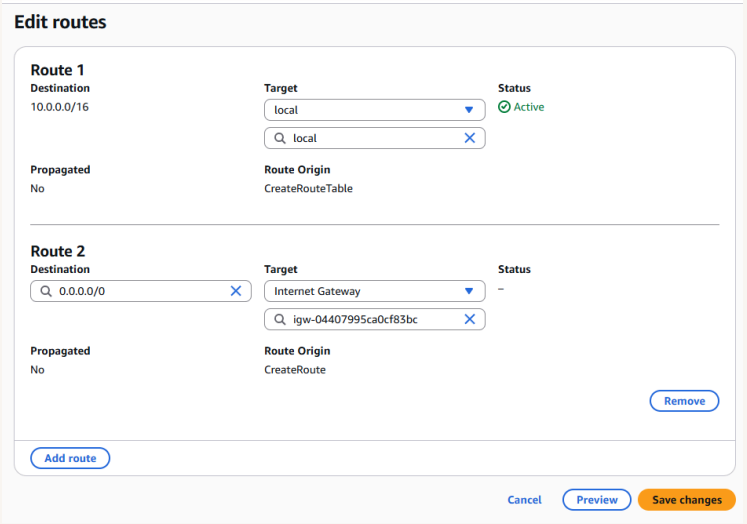
Routes tables are needed to make a subnet public because route table is the map. A subnet is public only when its route table sends all ipv4 to the Internet Gateway. A public IP + IG not enough, without that route, traffic can’t enter or leave.



Route destination and target

Routes are defined by their destination and target, which mean the range of IP that traffic wants to reach and the target is how is it gonna reach there (local, igw, vpn).

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of and a target of 0.0.0.0/0 and target is me newly set up IW (NextWork IG).



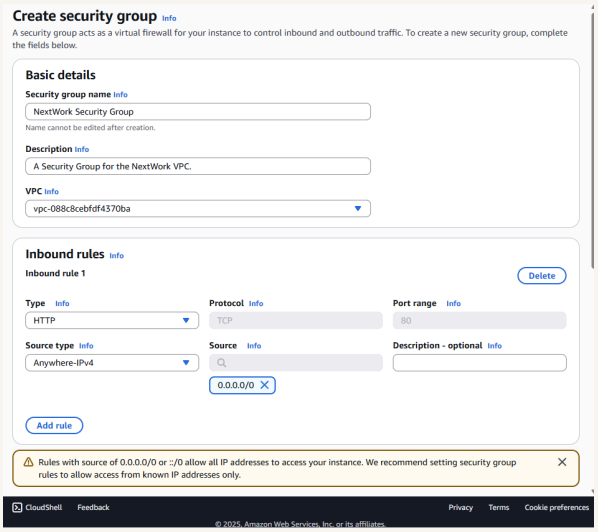
Security groups

Security groups are virtual firewalls for your VPC resources (like EC2). They use allow rules to control inbound and outbound traffic. They're stateful: replies are allowed automatically. By default, nothing passes unless you allow it.

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources in mysecurity group, I configured an inbound rule that allows all ip addresses to access your resource.

Outbound rules are rules which control data that my resources can send out. By default, my security group's outbound rule allow all outbound traffic.


Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
NextWork Security Group
Name cannot be edited after creation.
Description Info
A Security Group for the NextWork VPC.
VPC Info
vpc-088c8cebfdf4370ba
Inbound rules Info
Inbound rule 1
Delete
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
Anywhere-IPv4
Source Info
0.0.0.0/0
Description - optional Info
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

Network ACLs

Network ACLs are subnet firewalls in a VPC. They use allow/deny rules for traffic in and out. They are stateless: allow both inbound and outbound. Good for subnet guardrails.

Security groups vs. network ACLs

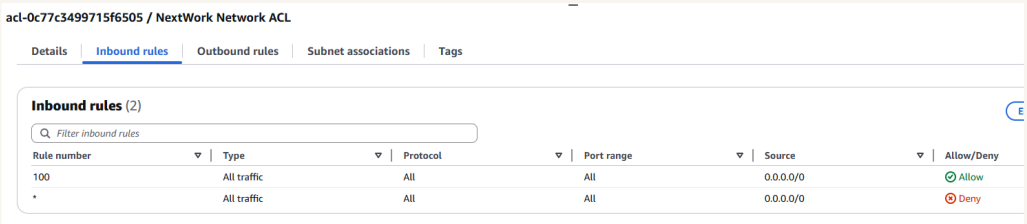
The difference between a security group and a network ACL is that security group protect one specific resource, allow-only. NACLs attach to subnets, stateless (must allow both in/out), allow or deny, rules checked in order.

Default vs Custom Network ACLs

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

By default, a network ACL's inbound and outbound rules will allow all inbound traffic into the Public Subnet, and allow all traffic out of the Public Subnet.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny any inbound access (request coming from outside to subnet) and denied all outbound access (from subnet to outside).



The place to learn & showcase your skills

Check out nextwork.org for more projects