



NextWork.org

VPC Traffic Flow and Security



shravanirg03@gmail.com

Details

Security group name NextWork Security Group	Security group ID sg-0c1828202597418cc	Description A Security Group for the NextWork VPC.	VPC ID vpc-0a93d66ed60ea65ee
Owner 975050239788	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Tags](#)

Inbound rules (1)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0682a6d97b7ec94...	IPv4	HTTP	TCP	80

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create an isolated, secure network in the AWS cloud, giving you control over IP ranges, subnets, etc. It is useful as it enhances security, and lets you scale resources while ensuring privacy and flexibility.

How I used Amazon VPC in this project

To ensure optimal traffic flow and security, I created a subnet within an Amazon VPC and configured routing tables, security groups, and network ACLs.

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

This project provided valuable insights and deeper understanding of various networking concepts.

This project took me...

The entire process took me approximately 60 minutes.

Route tables

Route tables in AWS define how network traffic is directed within a VPC. They contain a set of rules, or routes, that specify where to send network traffic based on its destination IP address.

Routes tables are needed to make a subnet public because they have a route pointing to an Internet Gateway for all outbound traffic. This route allows resources in the subnet to communicate with the internet, making it publicly accessible.

Destination	Target	Status
10.0.0.0/16	local	Active
<input type="text" value="0.0.0.0/0"/> X	<input type="text" value="local"/> X	
	Internet Gateway	Active
	<input type="text" value="igw-06cdd282bebd28104"/> X	
<button>Add route</button>		

Route destination and target

Routes are defined by their destination and target, where the destination is the range of IP addresses the traffic in my VPC is trying to reach and the target is the road/path that the traffic will use to get to their destination.

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

Destination	Target	Status
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active
<input type="text" value="0.0.0.0/0"/> X	<input type="text" value="local"/> X	
	Internet Gateway	<input checked="" type="checkbox"/> Active
	<input type="text" value="igw-06cdd282bebd28104"/> X	
<input type="button" value="Add route"/>		

Security groups

Security groups are used for controlling inbound and outbound traffic to resources like EC2 instances. They define the allowed traffic based on protocols, ports, and IP ranges. Every single resource in a subnet/VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that specifies which traffic from outside the security group can enter instances. E.g. Users visiting a web app I'm hosting. I configured an inbound rule that allows all HTTP inbound traffic.

Outbound rules are the rules that specifies which traffic from instances can leave the security group. E.g. My web app requesting data from a public source. By default, my security group's outbound rule will allow all outbound traffic.

The screenshot shows the AWS Management Console interface for a security group named 'NextWork Security Group'. The 'Details' tab is selected, displaying the following information:

Security group name	Security group ID	Description	VPC ID
NextWork Security Group	sg-0c1828202597418cc	A Security Group for the NextWork VPC.	vpc-0a93d66ed60ea65ee
Owner	Inbound rules count	Outbound rules count	
975050239788	1 Permission entry	1 Permission entry	

Below the details, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is active, showing one rule entry:

Inbound rules (1)

Search bar: Manage tags: [Edit inbound rules](#)

Pagination: < 1 > | [@](#)

Network ACLs

Network ACLs are control traffic at the subnet level in AWS. They allow or deny traffic based on IP addresses, protocols, and ports for both inbound and outbound traffic.

Security groups vs. network ACLs

The difference between a security group and a network ACL is their scope i.e. a security group secures my network at the resource level, while network ACLs secure my network at the subnet level.

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 rule is set up to allow all incoming and outgoing traffic, respectively. This means that no restrictions are applied unless explicitly modified.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all incoming/outgoing traffic, requiring you to manually configure specific rules to allow the desired traffic.

Inbound rules (2)							Edit inbound rules			
<input type="text"/> Filter inbound rules							<	1	>	①
Rule number	Type	Protocol	Port range	Source	Allow/Deny	Actions				
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow					
*	All traffic	All	All	0.0.0.0/0	<input type="checkbox"/> Deny					



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

