



NextWork.org

VPC Traffic Flow and Security



Honesty Dogunro

The screenshot shows the AWS VPC Security Groups console. A green success message at the top states: "Security group sg-0c9983993563a514e [NextWork Security Group] was created successfully". The main card displays the details of the security group "sg-0c9983993563a514e - NextWork Security Group".
Details:

- Security group name: NextWork Security Group
- Security group ID: sg-0c9983993563a514e
- Owner: 851725458922
- Inbound rules count: 1 Permission entry
- Description: Security Group for the NextWork VPC
- Outbound rules count: 1 Permission entry
- VPC ID: vpc-0ef1a95c1609071

Below the details, there are tabs for Inbound rules, Outbound rules, Sharing - new, VPC associations - new, and Tags. The Inbound rules table shows one rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
sgr-06947fa4a5f261d5f	sg-0c9983993563a514e	IPv4	HTTP	TCP	80	0.0.0.0/0

At the bottom of the page, there are links for CloudShell and Feedback, and a footer note: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a secure, isolated space in AWS for your resources, enabling control over network settings and enhancing security.

How I used Amazon VPC in this project

I used Amazon VPC to set up a secure network for our application, defining subnets, route tables, and security groups to control access and ensure data protection. This isolated environment enhanced our project's security and performance.

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

I didn't expect the complexity of configuring security groups to manage access effectively.

This project took me...

About 3 hours, i needed to understand those network concepts and configurations



Route tables

Route tables are lists of rules in networking that direct data packets between networks. They include destination IPs, subnet masks, next hops, and metrics to determine the best path for traffic, ensuring efficient communication and reliable data delivery.

Route tables are needed to make a subnet public because they direct traffic between the subnet and the internet, allowing external access through an internet gateway.

rtb-078a8e776fb47e30e / NextWork route table Actions ▾

Details Info		Main	Explicit subnet associations	Edge associations
Route table ID	rtb-078a8e776fb47e30e	Yes	-	-
VPC	vpc-04ff1f496c16698071 NextWork VPC	Owner ID	851725458922	

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)				Both ▾	Edit routes
<input type="text" value="Filter routes"/>				Both	Edit routes
Destination	Target	Status	Propagated		
0.0.0.0/0	igw-038243a2d90f9c8b8	Active	No		
10.0.0.0/16	local	Active	No		



Route destination and target

Routes are defined by their destination and target, which means the destination specifies the IP range being reached, while the target indicates where the traffic should go next, often a next-hop IP address or a gateway for forwarding packets.

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 the internet gateway's ID (e.g. igw-12345678).

rtb-078a8e776fb47e30e / NextWork route table

Actions ▾

Details		Info	
Route table ID	rtb-078a8e776fb47e30e	Main	Yes
VPC	vpc-04ff1f496c16698071 NextWork VPC	Owner ID	851725458922
Explicit subnet associations			
Edge associations			

Routes Subnet associations Edge associations Route propagation Tags

Both ▾ Edit routes

Routes (2)		Filter routes	
Destination	Target	Status	Propagated
0.0.0.0/0	igw-038243a2d90f9c8b8	Active	No
10.0.0.16	local	Active	No



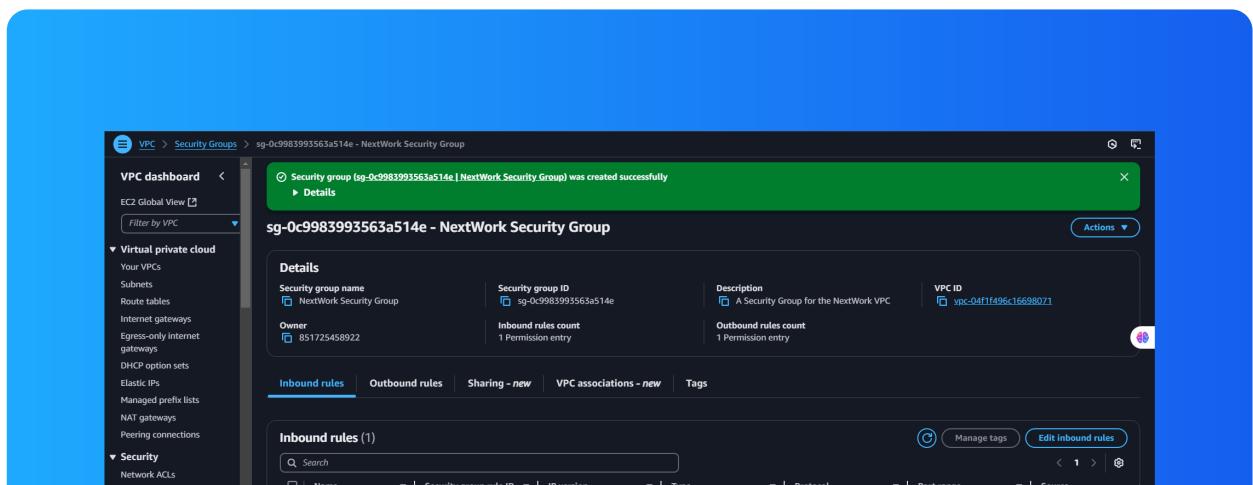
Security groups

Security groups are virtual firewalls in cloud computing that control inbound and outbound traffic to resources, like EC2 instances. They define which protocols and ports are allowed, helping to secure applications and manage access effectively.

Inbound vs Outbound rules

Inbound rules are the guidelines that determine which incoming traffic is allowed to reach your resources within a security group. I configured an inbound rule that permits HTTP traffic on port 80 from any IP address to allow web access.

Outbound rules are the guidelines that control the outgoing traffic from your resources within a security group. By default, my security group's outbound rule allows all traffic to any IP address, enabling free communication to the internet.





Network ACLs

Network ACLs are access control lists used in networking to define rules that govern incoming and outgoing traffic at the subnet level within a virtual private cloud (VPC). They enhance security by filtering traffic based on IP addresses and protocol

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and apply to instances, while network ACLs are stateless and apply to subnets, requiring explicit rules for both inbound and outbound traffic.



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 traffic, meaning they have an implicit rule that permits all IP traffic unless explicitly denied. This ensures that all connections are allowed by default.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until explicitly allowed, meaning you must define rules to permit specific traffic based on IP addresses, protocols, and ports.

The screenshot shows the AWS VPC Network ACLs console. A success message at the top indicates subnet associations were updated. The main page displays the details for a custom Network ACL named 'acl-09a5baf6cce26611b / NextWork Network ACL'. It shows it is associated with a specific subnet and has a 'Default' setting of 'No'. The 'Inbound rules' tab is selected, showing two rules:

Rule number	Type	Protocol	Port range	Source	Action
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

