



NextWork.org

VPC Traffic Flow and Security



itsbryantgonzalez@gmail.com

Security group (sg-038e54df9af36baf7 | NextWrok Security Group) was created successfully

Details

Security group name	sg-038e54df9af36baf7	Description	VPC ID
NextWrok Security Group	sg-038e54df9af36baf7	Security group for the NextWrok VPC	vpc-0b7c179f73586a16e
Owner	664418982988	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)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-0657894f7d90cf208	IPv4	HTTP	TCP	80	0.0.0.0/0

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is useful because this creates a layer of security and privacy for your assets. This is the equivalent of creating a gated community for your assets.

How I used Amazon VPC in this project

I used Amazon VPC to create security groups and ACLS for the inbound and outbound traffic communicating with my VPC.

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

One thing I didn't expect in this project was how easy to use AWS is.

This project took me...

This project took a little more than an hour to complete.

Route tables

Route tables are equivalent to highways or a GPS system. Essentially they make it easier for IP addresses to efficiently communicate with the internet gateway.

Route tables are needed to make a subnet public because a subnet needs to have a route to an internet gateway to be considered public. A routing table is the only way to establish this connection.

⌚ Updated routes for rtb-042ad123f2897e95e successfully

► Details

Details Info

Route table ID	<input checked="" type="checkbox"/> rtb-042ad123f2897e95e	Main	<input checked="" type="checkbox"/> Yes	Explicit subnet associations	-	Edge associations	-
VPC	vpc-0b7c179f73586a16e NextWork VPC	Owner ID	<input checked="" type="checkbox"/> 664418982988				

Routes (2) Both Edit routes < 1 > ⚙️

Destination	Target	Status	Propagated
0.0.0.0/0	igw-03f6b7add78aa3930	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 is the range of IP ranges that you want to route and the target is the path they will take which is the internet gateway.

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

A screenshot of the AWS Route Table configuration page. At the top, a green success message says "Updated routes for rtb-042ad123f2897e95e successfully". Below it, there's a "Details" section with tabs for "Info" (selected) and "Logs". The "Info" tab shows:

Route table ID rtb-042ad123f2897e95e	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0b7c179f73586a16e NextWork VPC	Owner ID 664418982988		

Below this are tabs for "Routes", "Subnet associations", "Edge associations", "Route propagation", and "Tags". The "Routes" tab is selected and shows a table of routes:

Routes (2)			
<input type="text"/> Filter routes			
Destination	Target	Status	Propagated
0.0.0.0/0	igw-03f6b7add78aa3930	<input checked="" type="checkbox"/> Active	No
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No

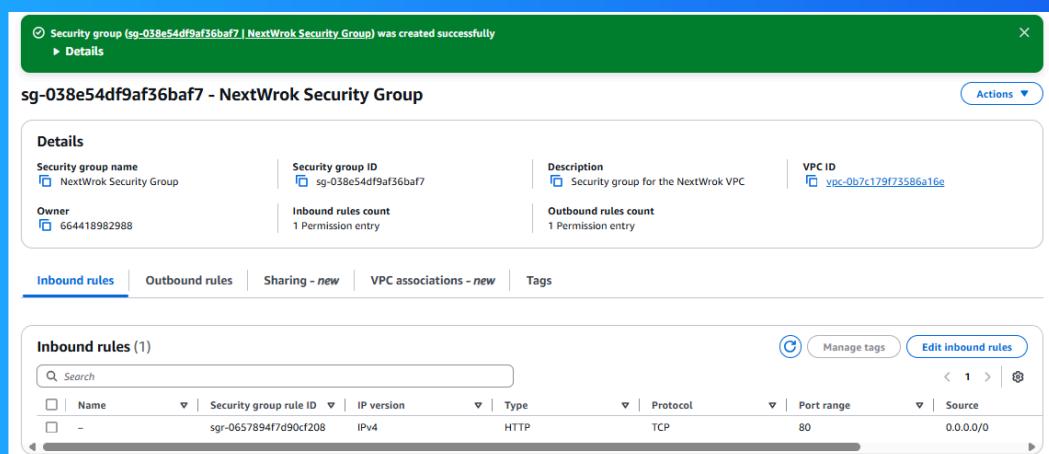
Security groups

Security groups are rule sets for assigned sections of traffic. This can be for inbound or outbound traffic.

Inbound vs Outbound rules

Inbound rules are to restrict or allow certain types of traffic. I configured an inbound rule over port 80 (HTTP) that allows for inbound traffic to communicate with our VPC.

Outbound rules rules to restrict or allow outgoing traffic outside the VPC. By default my security group's outrule allows all traffic.



Network ACLs

Network ACLs are a set of rules to restrict or allow inbound/outbound traffic for the VPC.

Security groups vs. network ACLs

The difference between a security group and a Network ACL is that they secure networks at different levels. Network ACL secure subnet layer traffic and security groups secure traffic accessing traffic accessing assets in the VPC.

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 deny inbound and outbound traffic until you add a rule to allow the traffic in and out of your VPC.

In contrast, a custom ACL's inbound and outbound rules are automatically set to allow.

The screenshot shows the AWS Network ACLs interface. At the top, there is a search bar labeled "Find resources by attribute or tag". Below it is a table titled "Network ACLs (1/3) Info" with the following data:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
NextWork ACL	ac1-05cec3223da83e4fd	subnet-035613708a74864d5 / Public 1	No	vpc-0b7c179f73586a16e / NextWork VPC	2 Inbound rules
-	ac1-0c0a93835a00116f7	6 Subnets	Yes	vpc-0f87833cb2e02668a	2 Inbound rules
-	ac1-0e2bd77940f26e26	-	Yes	vpc-0b7c179f73586a16e / NextWork VPC	2 Inbound rules

Below this, there is a section titled "Inbound rules (2)" with the following data:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
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

