



VPC Traffic Flow and Security



Juncheng Wang

Security group (sg-007ed03d41f734798 | NextWork-Security-Group) was created successfully

Details

VPC > Security Groups > sg-007ed03d41f734798 - NextWork-Security-Group

sg-007ed03d41f734798 - NextWork-Security-Group

Actions

Details

Security group name NextWork-Security-Group	Security group ID sg-007ed03d41f734798	Description A security group for NextWork VPC	VPC ID vpc-0ff2f6592aad47c0a
Owner 691784454033	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (1)

Search

	Name	Security group rule...	IP version	Type	Protocol	Port range	
<input type="checkbox"/>	-	sgr-0aa32d0fe2795cff9	IPv4	HTTP	TCP	80	



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC enables you to build a virtual network in the AWS cloud. You can define your own network space by controlling how your network and the Amazon EC2 resources inside your network are communicating to the internet.

How I used Amazon VPC in this project

I set up a security group for my resource in the subnet and a network ACL for my subnet.

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

There are more layer of security options than I thought.

This project took me...

1 hour



Route tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed.

Routes tables are needed to make a subnet public because route table acting like a GPS telling the resources in your subnet where to go. Without it, the resources wouldn't know where to send or receive data.

VPC > Route tables > rtb-055a8e3d94b5b0dc8 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>	-	No
	Internet Gateway	-	No
	<input type="text" value="igw-011d2b9ddf1780659"/>	-	No



Route destination and target

Routes are defined by their destination and target, which means the destination is The IP address range that traffic wants to reach and the target is the road or path that the traffic will have to take to get to its 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 internet gateway.

VPC > Route tables > rtb-055a8e3d94b5b0dc8 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No
	igw-011d2b9ddf1780655		

Add route

Cancel Preview Save changes



Security groups

Security group is like a security guard, at the entrance of each resource in the subnet. It has strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources in your security group such as visitors to your website and receive form submissions. I configured an inbound rule that allows any IP address to access my resource.

Outbound rules control what data your resources can send out, such as server requests data from another service, and sends out an email notification. My security group's outbound rule has allowed all outbound traffic by default.

The screenshot displays the AWS Management Console interface for a security group. At the top, a green notification bar states: "Security group (sg-007ed03d41f734798 | NextWork-Security-Group) was created successfully". Below this, the breadcrumb navigation shows "VPC > Security Groups > sg-007ed03d41f734798 - NextWork-Security-Group". The main heading is "sg-007ed03d41f734798 - NextWork-Security-Group" with an "Actions" dropdown menu to its right.

The "Details" section contains a table with the following information:

Security group name NextWork-Security-Group	Security group ID sg-007ed03d41f734798	Description A security group for NextWork VPC	VPC ID vpc-0ff2f6592aad47c0a
Owner 691784454033	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Below the details, there are tabs for "Inbound rules", "Outbound rules", and "Tags". The "Inbound rules" tab is selected, showing "Inbound rules (1)". There is a search bar and buttons for "Manage tags" and "Edit inbound rules". At the bottom right, there are navigation controls showing "1" and arrows.



Network ACLs

Network ACLs are network access control lists that act as an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. A subnet can be associated with only one network ACL at a time.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that the security group is acting at the resource level in the subnet while ACL act 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 rules will allow all inbound and outbound traffic.

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

You have successfully updated subnet associations for acl-Off1aa5160fa3f670 / NextWork Network ACL.

Details

VPC > Network ACLs > acl-Off1aa5160fa3f670 / NextWork Network ACL

acl-Off1aa5160fa3f670 / NextWork Network ACL

Actions

Details Info

Network ACL ID acl-Off1aa5160fa3f670	Associated with subnet-0e3e7f355ce088e8e / public-1	Default No	VPC ID vpc-Off2f6592aad47c0a / NextWork VPC
Owner 691784454033			

Inbound rules Outbound rules Subnet associations Tags

Inbound rules (2) Edit inbound rules

Filter inbound rules

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

