



VPC Traffic Flow and Security

J

Michael K.

Security group (sg-01118d6fb1891797a | MyTestSecurityGroup) was created successfully

Details

Security group name MyTestSecurityGroup	Security group ID sg-01118d6fb1891797a	Description Allows HTTP traffic	VPC ID vpc-0fc1b956fd1260a62
Owner 109648734195	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing | VPC associations | Tags

Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-003f268f6526e4acb	IPv4	HTTP	TCP	80



Michael K.

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated virtual network within AWS where I can launch and manage AWS resources (such as EC2 instances, RDS databases, and load balancers) using my own defined IP address range, subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create my own virtual private network, and configure a secure traffic within it.

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

One thing I didn't expect in this project was the complexity to understand why and how to set up the subnet with the Route Table and Network ACL.

This project took me...

This project took me 2 hours

Route tables

Route tables are like GPS which guides the traffic within our VPC to its destination.

Route tables are needed to make a subnet public because for a subnet to be made public it has to be attached to a route which will lead its traffic to the Internet gateway. The subnet will be attached to that route through an explicit association to the route tables. As that traffic reaches the Internet gateway it will be sent to the Internet. As soon as the traffic from that subnet reaches the IGW, it is made public since it is sent to the Internet directly after.

rtb-04e9812a8d1e0b047 / My Test Route Table Actions ▾

Details <small>Info</small>	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0fc1b956fd1260a62 My Test VPC	Owner ID <input checked="" type="checkbox"/> 109648734195		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)		<small>Both ▾</small> Edit routes	
<small>Filter routes</small>		<small>Both ▾</small> Edit routes	
Destination	Target	Status	Propagated
0.0.0.0/0	igw-07c5fd923312603ae	<input checked="" type="radio"/> Active	No
10.0.0.0/16	local	<input checked="" type="radio"/> Active	No

Route destination and target

Routes are defined by their destination and target, which mean the place where the traffic needs to be sent and the route that the traffic needs to take to reach that 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 which means any destination (any ip-address) and a target of the already created IGW, since it is considered that the destination not being a resource in the VPC is automatically somewhere in the Internet.

rtb-04e9812a8d1e0b047 / My Test Route Table Actions ▾

Details <small>Info</small>	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -												
VPC vpc-0fc1b956fd1260a62 My Test VPC	Owner ID <input checked="" type="checkbox"/> 109648734195														
Routes Subnet associations Edge associations Route propagation Tags															
Routes (2) Filter routes Both Edit routes <table border="1"><thead><tr><th>Destination</th><th>Target</th><th>Status</th><th>Propagated</th></tr></thead><tbody><tr><td>0.0.0.0/0</td><td>igw-07c5fd923312603ae</td><td><input checked="" type="radio"/> Active</td><td>No</td></tr><tr><td>10.0.0.0/16</td><td>local</td><td><input checked="" type="radio"/> Active</td><td>No</td></tr></tbody></table>				Destination	Target	Status	Propagated	0.0.0.0/0	igw-07c5fd923312603ae	<input checked="" type="radio"/> Active	No	10.0.0.0/16	local	<input checked="" type="radio"/> Active	No
Destination	Target	Status	Propagated												
0.0.0.0/0	igw-07c5fd923312603ae	<input checked="" type="radio"/> Active	No												
10.0.0.0/16	local	<input checked="" type="radio"/> Active	No												



Michael K.

NextWork Student

nextwork.org

Security groups

Security groups are statements (security checkpoint) which control traffic in (inbound traffic) and out (outbound traffic) of EC2 Instances.

Inbound vs Outbound rules

Inbound rules are statements that define the kind of traffic that can enter a resource. I configured an inbound rule that ONLY HTTP traffics with an IPv4 address from anywhere can enter my resource.

Outbound rules are statements that define the kind of traffic that can leave a resource. By default, my security group's outbound rule is letting everything from the resource out.

J

Michael K.

NextWork Student

nextwork.org

⌚ Security group (sg-01118d6fb1891797a | MyTestSecurityGroup) was created successfully

► Details (X)

sg-01118d6fb1891797a - MyTestSecurityGroup

Actions ▾

Details			
Security group name MyTestSecurityGroup	Security group ID sg-01118d6fb1891797a	Description Allows HTTP traffic	VPC ID vpc-0fc1b956fd1260a62
Owner 109648734195	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Sharing VPC associations Tags

Inbound rules (1)

Manage tags Edit inbound rules

Search (C) Manage tags Edit inbound rules [] [] []

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-003f268f6526e4acb	IPv4	HTTP	TCP	80

Network ACLs

Network ACLs are security guards at the entry and exit of subnets, controlling data packets (traffic) with the use of ACLs rules before letting them in or out.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups work at the resource level while NACL works at the subnet level. NACL is stateless while Security groups are stateful.

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 entering or leaving the subnet.

In contrast, a custom ACL's inbound and outbound rules are automatically set to allow or deny the entry or exit of data packet (traffic) whose features (protocols, IP Addresses etc.) are or are not part of the customized or defined rule.

The screenshot shows the AWS Network ACLs interface. At the top, a message says "You have successfully updated outbound rules for acl-0ed266e7fc130bfd0 / My Test NACL". Below this, there are two tabs: "Network ACLs (1/3)" and "Info". The "Actions" dropdown menu is open, showing options like "Edit", "Delete", and "Tags". A "Create network ACL" button is also present. The main table lists one Network ACL:

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-03939030cbb56f405	-	Yes	vpc-0fc1b956fd1260a62 / My Test VPC
-	acl-0191f8e120663db5	6 Subnets	Yes	vpc-086c814283b364f04
My Test NACL	acl-0ed266e7fc130bfd0	subnet-036c315df04b4fb / My-test-public-s... No	No	vpc-0fc1b956fd1260a62 / My Test VPC

Below the table, the title "acl-0ed266e7fc130bfd0 / My Test NACL" is displayed. At the bottom, there are tabs for "Details", "Inbound rules", "Outbound rules", "Subnet associations", and "Tags". The "Inbound rules" tab is selected, showing two 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



Michael K.

NextWork Student

nextwork.org

Tracking VPC Resources

I created additional resources (VPC, Internet Gateway and Security Groups) through the CLI. Instead of my usual region, I used another region. Teams would use multiple regions to reduce latency and enable fault tolerance.

EC2 Global View is a tool where you can find all the resources created in my account. I could even narrow down my search by searching for resources in a particular region. Without EC2 Global View, you'd have to everything said up manually.

Now that I've learnt about EC2 Global View, I'd use it again to have an insight to the resources created in my account.

J

Michael K.

NextWork Student

nextwork.org

AWS Global View (refresh)

Region Explorer
Global search
Regions and Zones: New
Settings

Summary
Summary of your resources across all Regions for which your account is enabled.
Fetching resources for all areas in regions
Resource update complete
Resource totals will be inaccurate until complete

Compute	Storage	Networking	Security
0	1	348	44

Show all resource summary

Enabled regions	Instances	VPCs	Subnets
17 regions	0 in 0 regions	19 in 17 regions	56 in 17 regions
Security groups	Volumes	Auto scaling groups	Route tables
24 in 17 regions	0 in 0 regions	0 in 0 regions	19 in 17 regions
VPC endpoints	NAT gateways	Egress only internet gateways	Internet gateways
0 in 0 regions	0 in 0 regions	0 in 0 regions	19 in 17 regions
DHCP option sets	Elastic IPs	Endpoint services	Managed prefix lists
17 in 17 regions	0 in 0 regions	0 in 0 regions	216 in 17 regions
Network ACLs	Network interfaces	VPC peering connections	Capacity Reservations
20 in 17 regions	0 in 0 regions	0 in 0 regions	0 in 0 regions
S3 buckets	RDS clusters	RDS DB instances	Outposts
1 in 1 regions	0 in 0 regions	0 in 0 regions	0 in 0 regions

To discover more resources, visit [AWS Resource Explorer](#).



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

