



VPC Traffic Flow and Security



Ronson Lobo

The screenshot shows the AWS VPC traffic flow rules configuration interface. It consists of two main sections: 'Inbound rules' and 'Outbound rules'.
Inbound rules: This section allows filtering by Type (HTTP), Protocol (TCP), Port range (80), Source (Anywhere), and Destination (0.0.0.0/0). An 'Add rule' button is present.
Outbound rules: This section allows filtering by Type (All traffic), Protocol (All), Port range (All), Destination (Custom, 0.0.0.0/0), and Destination (0.0.0.0/0). An 'Add rule' button is present.



Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (VPC) Security It can be useful for: Security (Inbound outbound filtering), Scalability (scalable infrastructure) Customization (Own ip range, subnets and route tables)

How I used Amazon VPC in this project

I used VPC to check the Traffic Flow and Security of a data packet. A virtual private cloud was created to check the flow of data, security checks, the internet gateway etc

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

I wasn't expecting so many checks happen when a data flow is done

This project took me...

I was able to complete this project in 45 minutes

Ronson Lobo
NextWork Student

NextWork.org

Route tables

A route table is a set of rules that help network devices determine the best path for data packets to travel from a source to a destination. Route tables are stored in routers and networked computers, and are often viewed in table format.

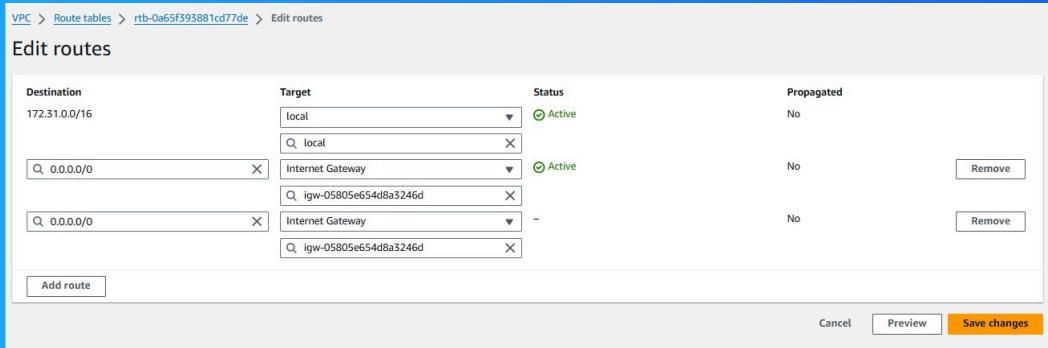
A route table is needed to make a subnet public because it controls the routing of network traffic to an internet gateway, which connects the subnet to the internet and other AWS services:

VPC > Route tables > rtb-0a65f393881cd77de > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0/16	local	Active	No
[Q] 0.0.0.0	[X] local		
[Q] 0.0.0.0	[X] Internet Gateway	Active	No
[Q] 0.0.0.0	[X] igw-05805e654d8a3246d		
[Q] 0.0.0.0	[X] Internet Gateway	-	No
[Q] 0.0.0.0	[X] igw-05805e654d8a3246d		

Add route Cancel Preview Save changes





Ronson Lobo
NextWork Student

NextWork.org

Route destination and target

In a route table, a route's destination is the range of IP addresses where traffic is to go, and the target is the network device used to reach that destination:

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of all ip and a target of my VPC

The screenshot shows the AWS VPC Route Tables interface. The URL in the top navigation bar is [VPC > Route tables > rtb-0a65f393881cd77de > Edit routes](#). The main title is "Edit routes". Below it is a table with four columns: "Destination", "Target", "Status", and "Propagated".

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No
0.0.0.0/0	Internet Gateway	-	No

At the bottom of the table, there is a "Remove" button next to each row. At the very bottom of the interface, there are three buttons: "Cancel", "Preview", and "Save changes".

Ronson Lobo
NextWork Student

NextWork.org

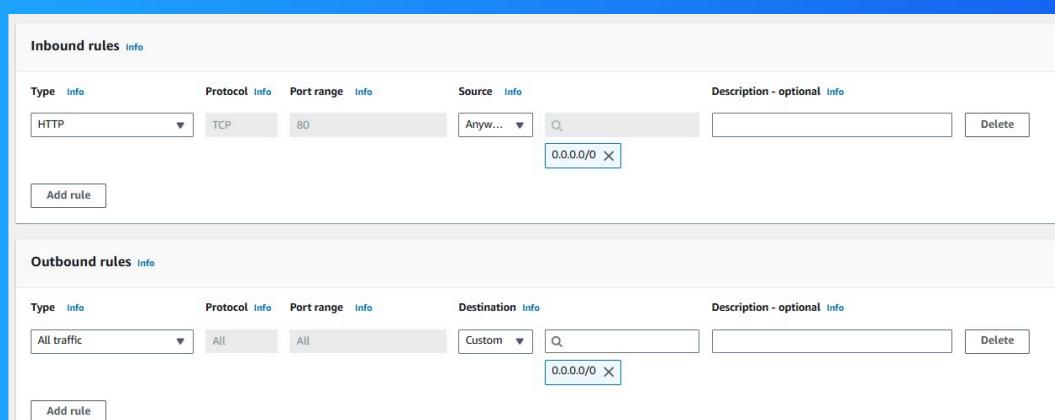
Security groups

Security groups are a way to control traffic to resources and assign permissions to users:

Inbound vs Outbound rules

An inbound rule is a firewall rule that controls traffic coming into a network from other networks or the internet. Inbound rules protect a network from unauthorized access by filtering incoming requests based on criteria like: IP addresses, Port num

Outbound rules control the traffic that leaves a network, and are a type of firewall policy that helps protect internal network resources:





Ronson Lobo
NextWork Student

NextWork.org

Network ACLs

A network access control list (ACL) is a set of rules that controls access to a network, allowing or denying specific traffic:

Security groups vs. network ACLs

Security groups control traffic at the instance level, while NACLs control traffic at the subnet level. Security groups are associated with an EC2 instance, while NACLs are associated with a subnet.

Ronson Lobo
NextWork Student

NextWork.org

Default vs Custom Network ACLs

Similar to security groups, network ACLs use inbound and outbound rules

The default rule for all inbound and outbound rules in a network access control list (ACL) is to deny all traffic:

A custom network access control list (ACL) inbound or outbound rule allows or denies specific traffic to a subnet:

The screenshot shows the AWS Network ACLs console. 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 columns: Name, Network ACL ID, Associated with, Default, and VPC ID. There are three entries: one with ID "acl-0f5a87a96271c0b8d" associated with "3 Subnets", another with ID "acl-05253ef6febbabed" associated with none, and a third entry "NextWork Network A..." with ID "acl-0e0d0a4caf466bde2" associated with "subnet-05354c978a39e6177 / Public 1". The "Default" column shows "Yes" for the first two and "No" for the third. The "VPC ID" column shows "vpc-00ac6a99e5efa868b" for the first, "vpc-0c1d88a073cf87eb / NextWork VPC" for the second, and "vpc-0c1d88a073cf87eb / NextWork VPC" for the third.

Below the table, there are tabs for "Details", "Inbound rules" (which is selected), "Outbound rules", "Subnet associations", and "Tags".

The "Inbound rules (2)" section shows a table with columns: Rule number, Type, Protocol, Port range, Source, and Allow/Deny. There are two rules: rule 100 with "All traffic" type, "All" protocol, "All" port range, "0.0.0.0/0" source, and "Allow" status; and a wildcard rule "*" with "All traffic" type, "All" protocol, "All" port range, "0.0.0.0/0" source, and "Deny" status.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

