COURSEWARE

EC2 VPC Security Groups

Contents

Overview

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.
When you launch an instance in a VPC, you can assign up to five security groups to the instance.
Security groups act at the instance level, not the subnet level.
Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups.
If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.
This section describes the basic things you need to know about security groups for your VPC and their rules.

Security Group basics

The following are the basic characteristics of security groups for your VPC:

- You have limits on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups you can associate with a network interface. For more information, see Amazon VPC Limits.
- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
- By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
- Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of

inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

- Instances associated with a security group can't talk to each other unless you add rules allowing it (exception: the default security group has these rules by default).
- Security groups are associated with network interfaces. After you launch an instance, you can change the security groups associated with the instance, which changes the security groups associated with the primary network interface (eth0). You can also change the security groups associated with any other network interface. For more information about network interfaces, see Elastic Network Interfaces.
- When you create a security group, you must provide it with a name and a description. The following rules apply:
- Names and descriptions can be up to 255 characters in length.
- Names and descriptions are limited to the following characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*.
- A security group name cannot start with sg-.
- A security group name must be unique within the VPC.

Creating Security Groups

Security groups can be created and applied to a VPC; instances within this VPC will then be affected, unless a Security Group has been applied to them directly.

```
# aws ec2 create-security-group --group-name [SECURITY_GROUP_NAME] --description [DESCRIPTION] --vpc-id [VPC_ID]
aws ec2 create-security-group --group-name my-sg --description "My security group" --vpc-id vpc-1a2b3c4d
```

Listing Security Groups

Basic Usage

The Security Groups that you have can be listed:

```
# aws ec2 describe-security-groups
aws ec2 describe-security-groups
```

Filtering Out Security Groups by Name

Viewing Security Groups by name can be useful when you have a lot of them:

```
# aws ec2 describe-security-groups --group-names [GROUP_NAMES]
aws ec2 describe-security-groups --group-names my-sg
```

Security Group Rules

Overview

You can add or remove rules for a security group (also referred to as authorizing or revoking inbound or outbound access). A rule applies either to inbound traffic (ingress) or outbound traffic (egress). You can grant access to a specific CIDR range, or to another security group in your VPC or in a peer VPC (requires a VPC peering connection).

The following are the basic parts of a security group rule in a VPC:

- (Inbound rules only) The source of the traffic and the destination port or port range. The source can be another security group, an IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.
- (Outbound rules only) The destination for the traffic and the destination port or port range. The destination can be another security group, an IPv4 or IPv6 CIDR block, a single IPv4 or IPv6 address, or a prefix list ID (A service is identified by a prefix list—the name and ID of a service for a Region).

- Any protocol that has a standard protocol number (for a list, see Protocol Numbers). If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- An optional description for the security group rule to help you identify it later. A description can be up to 255 characters in length. Allowed characters are a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=;{}!$*.

When you specify a CIDR block as the source for a rule, traffic is allowed from the specified addresses for the specified protocol and port. When you specify a security group as the source for a rule, traffic is allowed from the elastic network interfaces (ENI) for the instances associated with the source security group for the specified protocol and port. Adding a security group as a source does not add rules from the source security group.

If you specify a single IPv4 address, specify the address using the /32 prefix length. If you specify a single IPv6 address, specify it using the /128 prefix length. For example to specify the address `216.58.213.14`, you can use the following: `216.58.213.14/32`

Some systems for setting up firewalls let you filter on source ports. Security groups only let you filter on destination ports.

When you add or remove rules, they are automatically applied to all instances associated with the security group.

Basic Usage

To make a rule allowing incoming traffic, we must provide the Security Group ID, the Protocol being used, the address range where the requests will be coming from and the port that will be used:

```
# aws ec2 authorize-security-group-ingress --group-id [SECURITY_GROUP_ID] --
protocol [PROTOCOL] --port [PORT] --cidr [ADDRESS_RANGE]
aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp -
-port 443 --cidr 0.0.0.0/0
```

Example for Allowing SSH from Anywhere

Here is an example that will allow anyone in the world to attempt an SSH connection to your machine:

```
# aws ec2 authorize-security-group-ingress --group-id [SECURITY_GROUP_ID] --
protocol [PROTOCOL] --port [PORT] --cidr [ADDRESS_RANGE]
aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp -
-port 22 --cidr 0.0.0.0/0
```

Allow SSH Only from Your IP Address

Allowing access from anywhere may be a security concern, so it's good to know how to control access.
We can use https://checkip.amazonaws.com to check our public IP address:

```
$ curl https://checkip.amazonaws.com
203.0.113.57
```

Once you know your public IP address, this can be used when configuring the SSH rule in our Security Group:

```
# aws ec2 authorize-security-group-ingress --group-id [SECURITY_GROUP_ID] --
protocol [PROTOCOL] --port [PORT] --cidr [ADDRESS_RANGE]
aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp -
-port 22 --cidr 203.0.113.57/32
```

You can also use command substitution in bash to get this working in a single command:

```
# aws ec2 authorize-security-group-ingress --group-id [SECURITY_GROUP_ID] --protocol [PROTOCOL] --port [PORT] --cidr [ADDRESS_RANGE]
aws ec2 authorize-security-group-ingress --group-id sg-903004f8 --protocol tcp --port 22 --cidr $(curl https://checkip.amazonaws.com)/32
```

Deleting a Security Group

Basic Usage

You must provide the ID of the Security Group when you are deleting it:

```
# aws ec2 delete-security-group --group-id [SECURITY_GROUP_ID]
aws ec2 delete-security-group --group-id sg-903004f8
```

Tutorial

There is no tutorial for this module.

Exercises

1. Create a new EC2 instance in your default VPC.
   SSH on to the machine and install a web application, NGINX for example, make sure that it is running.
   Use the AWS CLI to allow access to port of your web application on the machine (port `80` for NGINX), you should be able to access it from the internet if you did it correctly.
2. Same as Exercise 1 but you should only be able to access the site from your current public IP address.