AWS security groups

Tags: ACG

Many lab problems stem from a poor understanding of what a Security Group is. This article describes it in basic terms so that students can understand and build from there.

What is an AWS security group?

A Security group is two things:

- It is a set of filter rules. "Allow this type of traffic from this location."
- It is a way of creating a group of interfaces (and the instances they are attached to) so that you can manage them as a single group with a single rule.

Filters

The filters control traffic that is allowed to pass in though the Security Group, and out though the security group (although we don't manipulate that very often).

The filter rules are applied to the interface that the SG is attached to or associated with. So if you have an instance and you associate that SG with one of 't's interfaces, those rules will be applied to that instance. If you have an RDS or ELB service/appliance and attach the same SG to them, they will be subject to the same rules. But keep in mind that the rules are applied form the context of that interface (not the network).

Groups

The grouping aspect is a real advantage once you understand it.

When you associate and SG with an interface (and the device that is attached to), you are creating a 'group' of interfaces that use this SG. You can use this 'group' in a Security Group filter rule to define a location.

For example, instead of saying:

> Allow MySQL traffic from 10.1.2.1/24 and Allow MySQL traffic from 10.2.2.1/24 and Allow MySQL traffic from 10.3.2.1/24 and Allow MySQL traffic from 10.4.2.1/24 and ... .. .

You can say:

> Allow MySQL traffic from SG-MyWebDMZ

If you add a new bank of web server, instead of adding the subnet to this SG filter set it assess the membership of SG-MyWebDMZ.

If is is also useful if some interfaces in that 10.1.2.1/24sub net should not have access. It can also be used to refer to itself. So you can say "Allow this traffic if it comes from any interface that is part of this SG".

Discipline how you think about and SG as a set of filters that say "Allow this type of traffic from this location." Remember that you can refer to all the interfaces that use a SG by that SG name.

Note: Generally you will be better to have multiple small SGs each with a purpose, than to try and maintain a few large multi purpose SGs.

More info

- Control traffic to resources using security groups (external site, opens in new tab)