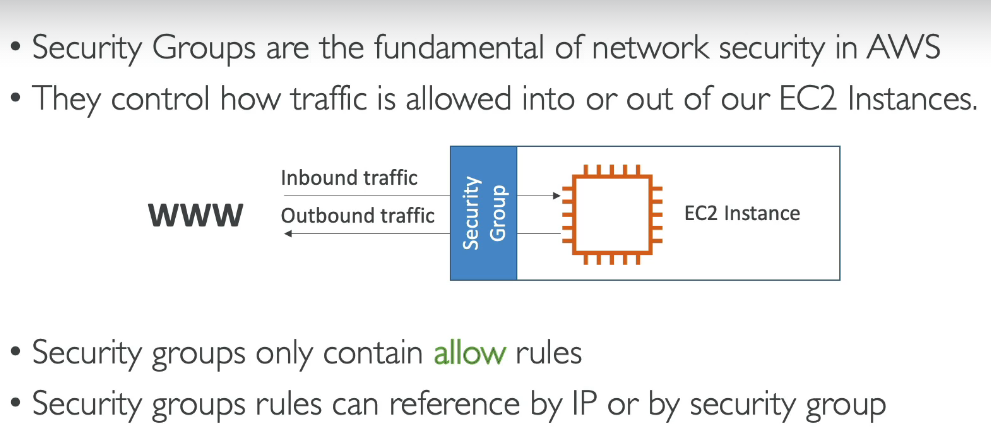
**SECURITY GROUP AND CLASSIC PORTS**

Security groups act as a firewall around our EC2 instances security groups yet again, are going to be fundamental into doing network security in the AWS cloud.

* They will control how the traffic is allowed into and out of your EC2 instances.
* Security groups are going to be very easy, they only contain allow rules,we can say what is allowed to go in and to go out,
* security groups can have rules that reference either by IP addresses, so, where your computer is from or by other security groups,security groups can reference each other



let's take an example, we are on our computer, so we are on the public internet and we're trying to access our EC2 instance from our computer. We are going to create a security group

around our EC2 instance, that is the firewall that is around it and then this security group is going to have rules. And these rules are going to say whether or not some inbound traffic, so from the outside into the EC2 instance is allowed, and also if the EC2 instance can perform some outbound traffic.

let's do a deeper dive, right?

Security groups are a firewall on our EC2 instancesand they're going to regulate access to ports. They're going to see the authorized IP ranges.

Table

Description automatically generated

**let's look at the diagram**

We have our EC2 instance and it has one security group allow attached to it that has inbound rules and outbound rules. So our computer is going to be authorized on say port 22.So the traffic can go through from our computer to the EC2 instance,but someone else's computer, that's not using my IP address because they don't live where I live, then if they're trying to access our EC2 instance they will not get through it because the firewall is going to block it

and it will be a timeout.

Then for the outbound rules by default, our EC2 instance for any security group is going to be by default allowing any traffic out of it. So our EC2 instance, if it tries to access a website and initiate a connection it is going to be allowed by the security group.

So this is the basics of how the firewall works.

Diagram

Description automatically generated

**Security groups attached to multiple instances at a time**

* There's not a one to one relationship between security group and instances and actually an instance can have multiple security groups too.
* Security groups are locked down to a region/VPC combination.So if you switch to another region, you have to create a new security group or if you create another VPC you have to recreate the security groups.
* The security groups live outside the EC2.So as I said, if the traffic is blocked the EC2 instance won't even see it.It's not like an application running on EC2 it's really a firewall outside your EC2 instance.

**NOTE:**

* If your application is not accessible, so timeout, then it is a security group issue.
* if you try to connect to any port and you computer just hangs and waits and waits that's probably a security group issue,
* but if you receive a connection refused error, okay, you actually get a response and connection refused, then the security group actually worked, the traffic went through and the application was errored or it wasn't launched or something like this.

**Graphical user interface, text, application, email

Description automatically generated**

**REFERENCING THE OTHER SECURITY GROUPS**

It is very easy to setup the security reference as can be seen in dig below:

Diagram

Description automatically generated

Here if we have setup an ec2 instance allowing the sg1 and sg2 inbound then the ec2 instances with which those security groups are attached will be able to access our ec2 instance despite having the other ip address.on the oter hand if we talk about the 3rd instance which has sg3 attached to it,it will not able to accesss our ec2 instance.

**CLASSIC PORTS**

**(imp)**

port 22: this allows you to login to an EC2 instance on Linux.

port 21:FTP or File Transfer Protocol which is used to upload files into a file share.

Port 22:SFTP, which is also using port 22, why?Well, because we're going to upload filebut this time using SSH because it's going to be a Secure File Transfer Protocol.

port 80: for HTTP This is to access unsecured websites.

port 443:for HTTPS, access secured websites

port3389 :for RDP, or the Remote Desktop Protocol which is the port that's used to log into a windows instance,

Text, letter

Description automatically generated