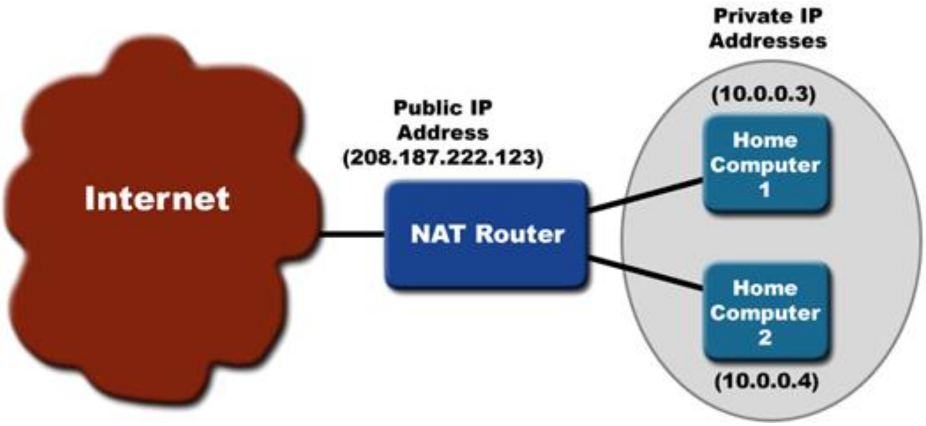
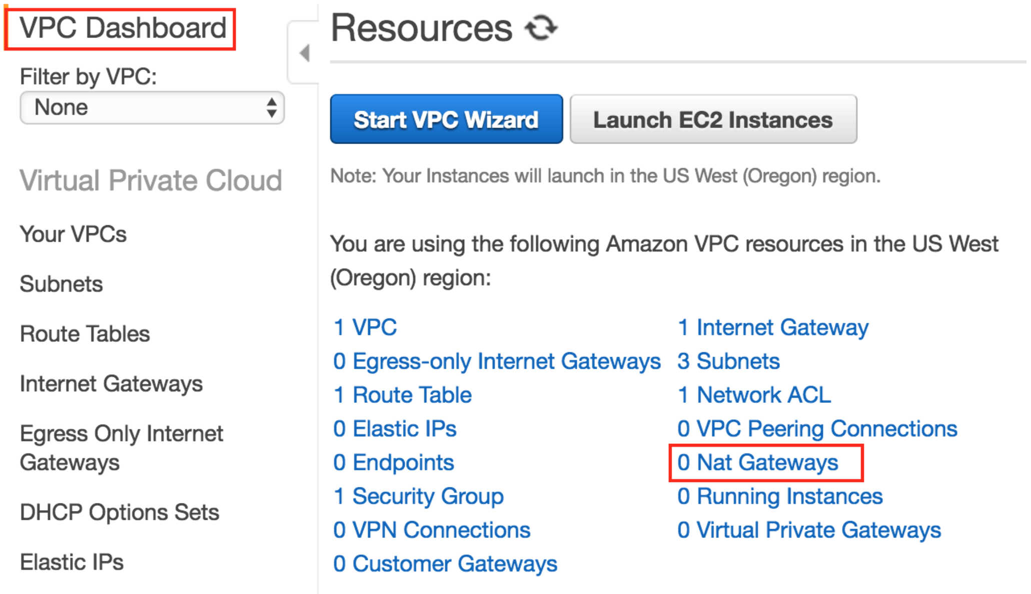
Overview:

When accessing the internet, the user needs to have a public IP address provisioned to them or they're going to need to be connected to an Elastic Load Balancer (ELB) instance which will provision the access for the user. The ELB advertises the DNS name but will not advertise the IP address. An issue with IP addresses and ELB is if the attacker is aware that the user does not have an IP address, then they will be using the ELB. If the user does have a public IP address, then there might be controls that can prevent access to that public IP address.



Discovery:

Go to the VPC Console in the Amazon Web Services Console. Visit the security groups tab to determine if the instances are being restricted correctly. If the instance is communicating with the outside network after being sent through a NAT (Network Address Translation), the user can tell whether or not the IP address is public.



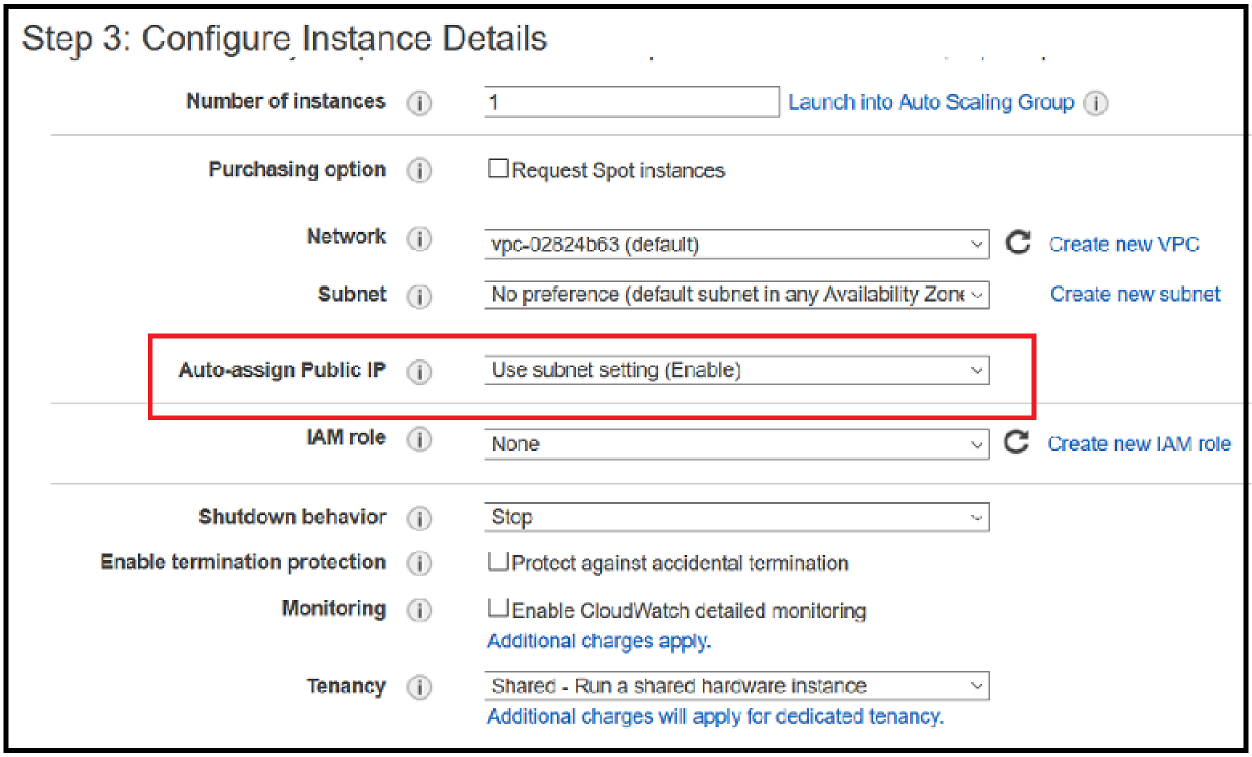
Note: Your Instances will launch in the US West (Oregon) region.

You are using the following Amazon VPC resources in the US West (Oregon) region:

1 VPC	1 Internet Gateway
0 Egress-only Internet Gateways	3 Subnets
1 Route Table	1 Network ACL
0 Elastic IPs	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
1 Security Group	0 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

Remediation:

Go the EC2 console in Amazon Web Services, and select Instances to go to the Instances page. Edit the properties for each instance's IP address, and set them to either public, private or elastic.

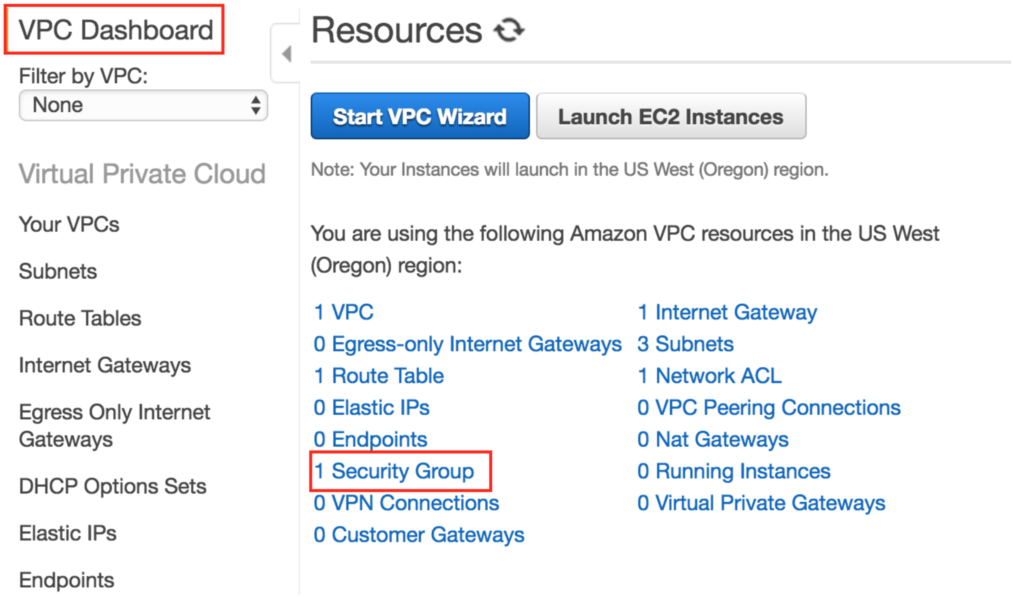


Step 3: Configure Instance Details

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances	
Network	vpc-02824b63 (default)	Create new VPC
Subnet	No preference (default subnet in any Availability Zone	Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
IAM role	None	Create new IAM role
Shutdown behavior	Stop	
Enable termination protection	□ Protect against accidental termination	
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	

http://docs.aws.amazon.com/storagegateway/latest/userguide/ec2-gateway-file.html

Go to the VPC Console in the Amazon Web Services Console. Visit the security groups tab to view the instances configured. Set the specific restrictions to avoid another attack of a similar fashion.



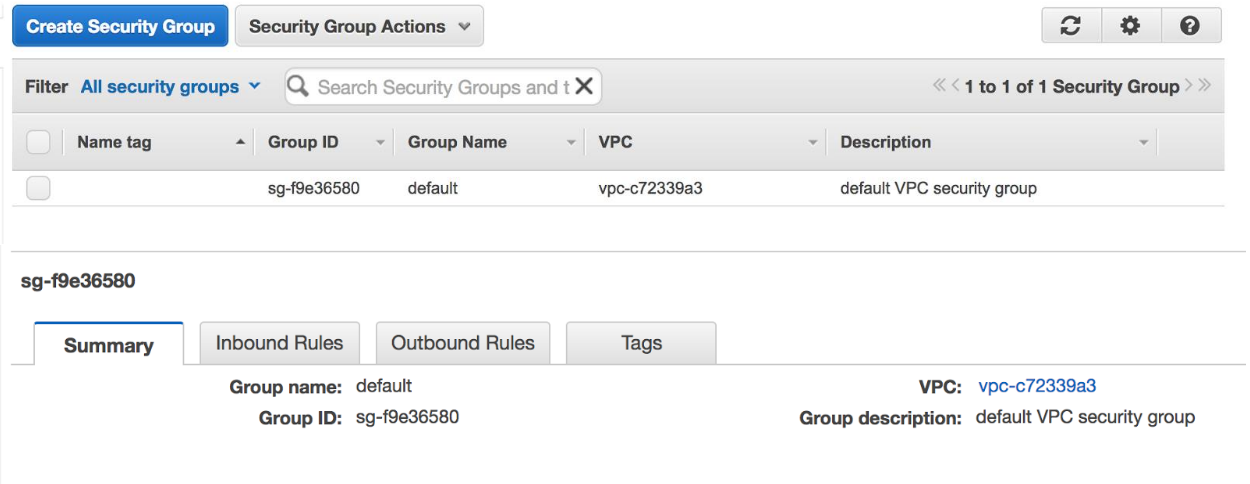
Resources

Note: Your Instances will launch in the US West (Oregon) region.

You are using the following Amazon VPC resources in the US West (Oregon) region:

1 VPC	1 Internet Gateway
0 Egress-only Internet Gateways	3 Subnets
1 Route Table	1 Network ACL
0 Elastic IPs	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
1 Security Group	0 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

Create a new security group and edit the inbound and outbound rules using the tabs at the bottom of the page



Name tag	Group ID	Group Name	VPC	Description
	sg-f9e36580	default	vpc-c72339a3	default VPC security group

sg-f9e36580

Group name: default

Group ID: sg-f9e36580

VPC: vpc-c72339a3

Group description: default VPC security group

Prevention:

Depending on the functionality of the instance, the instance may or may not need the outside network connectivity. The IP addresses should be provisioned in regards to the functionality of the instance they are being attached to.