AWS VPC

Virtual Private Cloud

Sterling
Talent Solutions

Introduction

- The *Amazon Virtual Private Cloud (Amazon VPC)* is a custom-defined virtual network within the AWS Cloud.
- Amazon VPC is the networking layer for Amazon Elastic Compute Cloud (Amazon EC2).
- You control various aspects of your Amazon VPC, including selecting your own IP address range; creating your own *subnets* and configuring your own route tables, network gateways, and security settings. Within a region, you can create multiple Amazon VPCs, and each Amazon VPC is logically isolated.
- When you create an Amazon VPC, you must specify the IPv4 address range by choosing a *Classless Inter-Domain Routing (CIDR)* block, such as 10.0.0.0/16. The address range of the Amazon VPC cannot be changed after the Amazon VPC is created.

- The Amazon VPC service was released after the Amazon EC2 service; because of this, there are two different networking platforms available within AWS: EC2-Classic and EC2-VPC.
- Amazon EC2 originally launched with a single, flat network shared with other AWS customers called EC2-Classic. As such, AWS accounts created prior to the arrival of the Amazon VPC service can launch instances into the EC2-Classic network and EC2-VPC. AWS accounts created after December 2013 only support launching instances using EC2-VPC. AWS accounts that support EC2-VPC will have a default VPC created in each region with a default subnet created in each Availability Zone. The assigned CIDR block of the VPC will be 172.31.0.0/16.

An Amazon VPC consists of the following components:

- Subnets
- Route tables
- Dynamic Host Configuration Protocol (DHCP) option sets
- Security groups
- Network Access Control Lists (ACLs)

An Amazon VPC has the following optional components:

- Internet Gateways (IGWs)
- Elastic IP (EIP) addresses
- Elastic Network Interfaces (ENIs)
- Endpoints
- Peering
- Network Address Translation (NATs) instances and NAT gateways
- Virtual Private Gateway (VPG), Customer Gateways (CGWs), and Virtual Private
- Networks (VPNs)

Subnets

- A *subnet* is a segment of an Amazon VPC's IP address range where you can launch Amazon EC2 instances, Amazon Relational Database Service (Amazon RDS) databases, and other AWS resources. CIDR blocks define subnets (for example, 10.0.1.0/24 and 192.168.0.0/24). The smallest subnet that you can create is a /28 (16 IP addresses). AWS reserves the first four IP addresses and the last IP address of every subnet for internal networking purposes. For example, a subnet defined as a /28 has 16 available IP addresses; subtract the 5 IPs needed by AWS to yield 11 IP addresses for your use within the subnet.
- After creating an Amazon VPC, you can add one or more subnets in each Availability Zone. Subnets reside within one Availability Zone and cannot span zones. So remember that one subnet equals one Availability Zone. You can, however, have multiple subnets in one Availability Zone.
- Subnets can be classified as public, private, or VPN-only
- Default Amazon VPCs contain one public subnet in every Availability Zone within the region

Route Tables

- A *route table* is a logical construct within an Amazon VPC that contains a set of rules (called routes) that are applied to the subnet and used to determine where network traffic is directed. A route table's routes are what permit Amazon EC2 instances within different subnets within an Amazon VPC to communicate with each other. You can modify route tables and add your own custom routes. You can also use route tables to specify which subnets are public (by directing Internet traffic to the IGW) and which subnets are private (by not having a route that directs traffic to the IGW).
- Each route table contains a default route called the local route, which enables communication within the Amazon VPC, and this route cannot be modified or removed.

You should remember the following points about route tables:

- Your VPC has an implicit router.
- Your VPC automatically comes with a main route table that you can modify.
- You can create additional custom route tables for your VPC.
- Each subnet must be associated with a route table, which controls the routing for the subnet. If you don’t explicitly associate a subnet with a particular route table, the subnet uses the main route table.

Internet Gateways

- An *Internet Gateway (IGW)* is a horizontally scaled, redundant, and highly available Amazon VPC component that allows communication between instances in your Amazon VPC and the Internet. An IGW provides a target in your Amazon VPC route tables for Internet-routable traffic, and it performs network address translation for instances that have been assigned public IP addresses.
- Amazon EC2 instances within an Amazon VPC are only aware of their private IP addresses. When traffic is sent from the instance to the Internet, the IGW translates the reply address to the instance's public IP address (or EIP address) and maintains the one-to-one map of the instance private IP address and public IP address. When an instance receives traffic from the Internet, the IGW translates the destination address (public IP address) to the instance's private IP address and forwards the traffic to the Amazon VPC.

You must do the following to create a public subnet with Internet access:

- Attach an IGW to your Amazon VPC.
- Create a subnet route table rule to send all non-local traffic (0.0.0.0/0) to the IGW.
- Configure your network ACLs and security group rules to allow relevant traffic to flow to and from your instance.

You must do the following to enable an Amazon EC2 instance to send and receive traffic from the Internet:

- Assign a public IP address or EIP address.

Elastic IP Addresses (EIPs)

- AWS maintains a pool of public IP addresses in each region and makes them available for you to associate to resources within your Amazon VPCs. An *Elastic IP Addresses (EIP)* is a static, public IP address in the pool for the region that you can allocate to your account (pull from the pool) and release (return to the pool).

Important points to understand about EIPs :

- You must first allocate an EIP for use within a VPC and then assign it to an instance.
- EIPs are specific to a region (that is, an EIP in one region cannot be assigned to an
- instance within an Amazon VPC in a different region).
- There is a one-to-one relationship between network interfaces and EIPs.
- You can move EIPs from one instance to another, either in the same Amazon VPC or a
- different Amazon VPC within the same region.
- EIPs remain associated with your AWS account until you explicitly release them.
- There are charges for EIPs allocated to your account, even when they are not associated with a resource.

Endpoints

- An Amazon VPC *endpoint* enables you to create a private connection between your Amazon VPC and another AWS service without requiring access over the Internet or through a NAT instance, VPN connection, or AWS Direct Connect. You can create multiple endpoints for a single service, and you can use different route tables to enforce different access policies from different subnets to the same service. Amazon VPC endpoints currently support communication with Amazon Simple Storage Service (Amazon S3), and other services are expected to be added in the future.

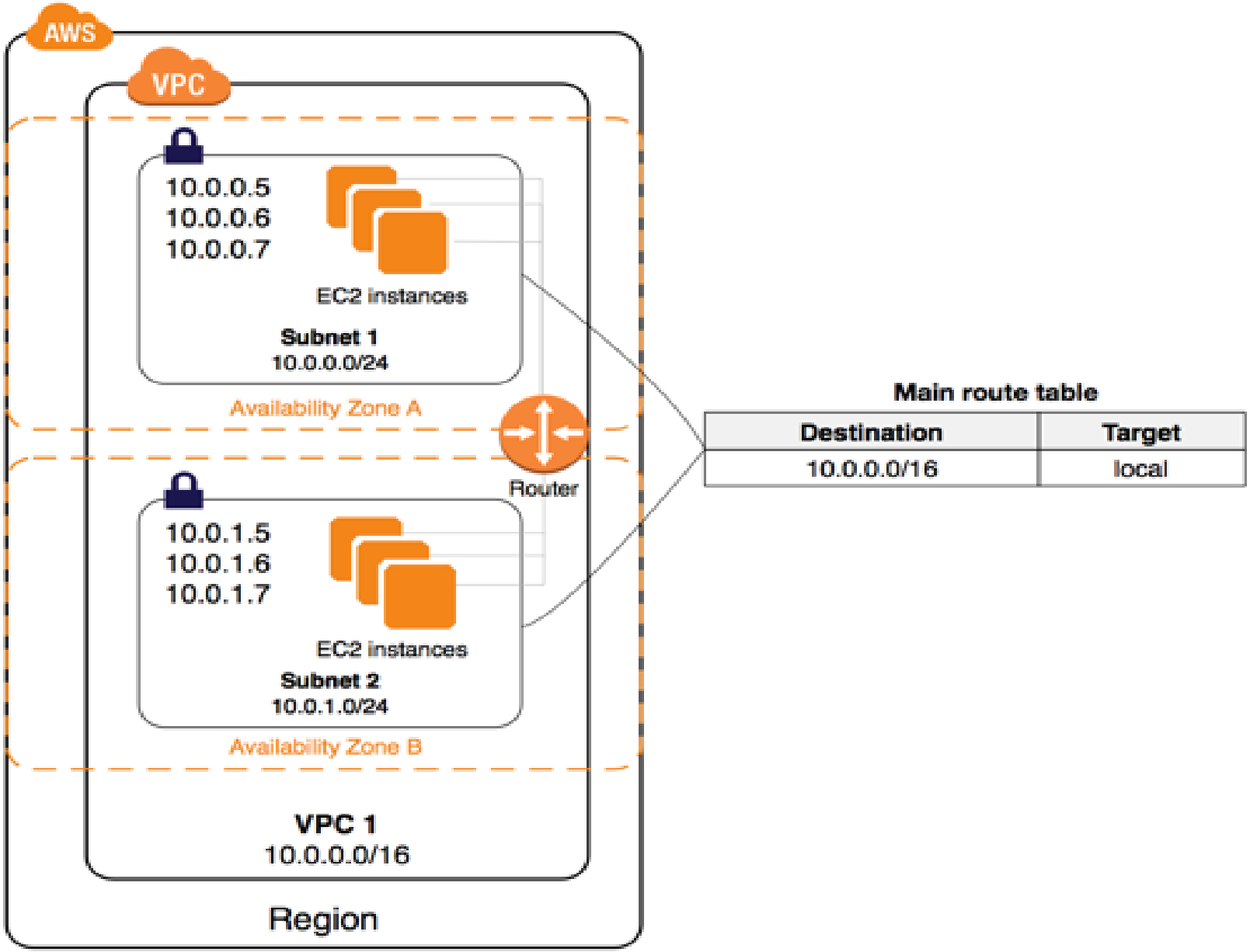
You must do the following to create an Amazon VPC endpoint:

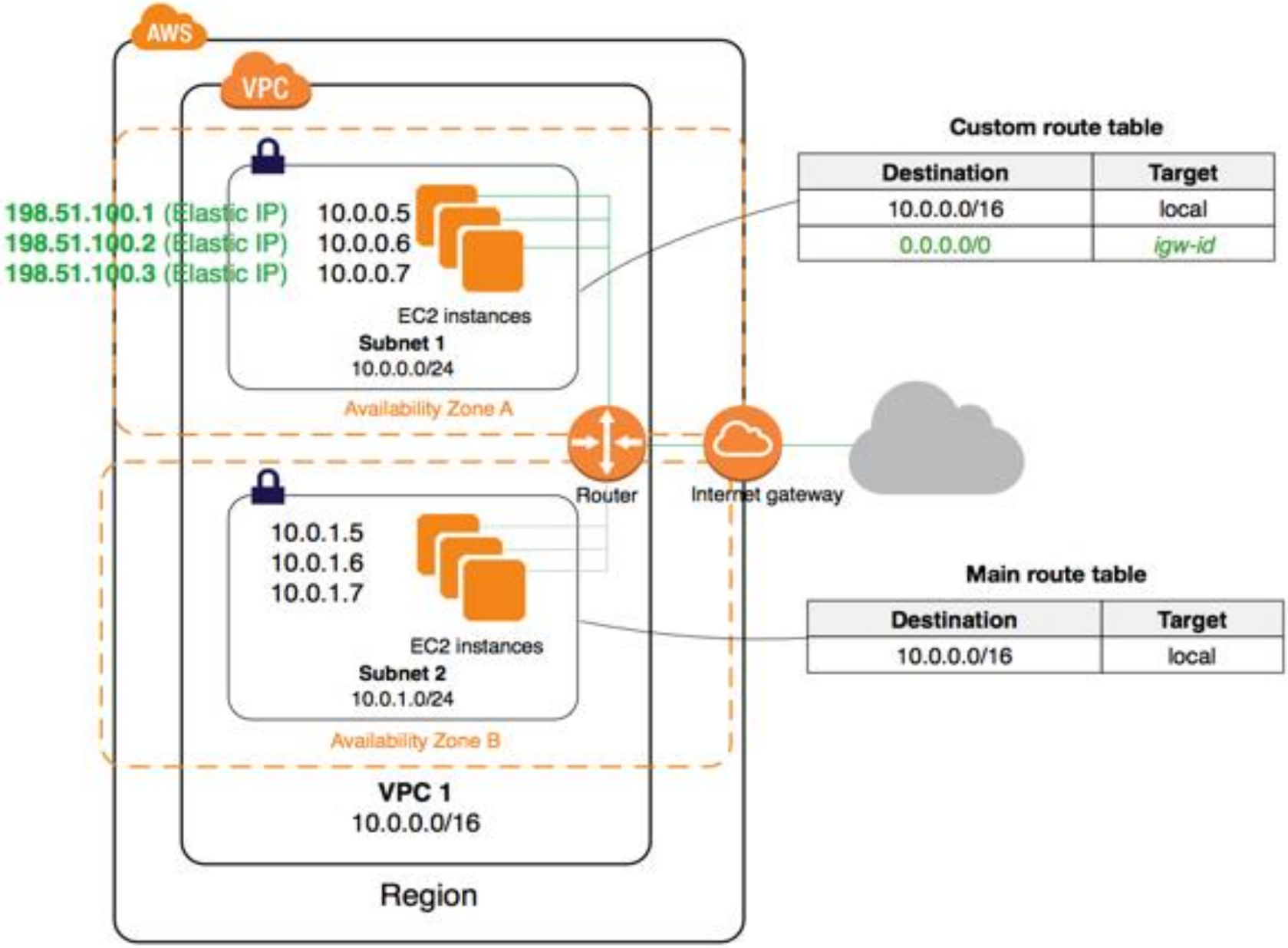
- Specify the Amazon VPC.
- Specify the service. A service is identified by a prefix list of the form com.amazonaws. <region>.<service>.
- Specify the policy. You can allow full access or create a custom policy. This policy can be changed at any time.
- Specify the route tables. A route will be added to each specified route table, which will state the service as the destination and the endpoint as the target

Sample Route Table Entry

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

The route table depicted here will direct any traffic from the subnet that's destined for Amazon S3 in the same region to the endpoint. All other Internet traffic goes to your IGW, including traffic that's destined for other services and for Amazon S3 in other regions.





Sterling
Talent Solutions

Peering

- An Amazon VPC *peering* connection is a networking connection between two Amazon VPCs that enables instances in either Amazon VPC to communicate with each other as if they are within the same network. You can create an Amazon VPC peering connection between your own Amazon VPCs or with an Amazon VPC in another AWS account within a single region.
- Peering connections are created through a request/accept protocol. The owner of the requesting Amazon VPC sends a request to peer to the owner of the peer Amazon VPC. If the peer Amazon VPC is within the same account, it is identified by its VPC ID. If the peer VPC is within a different account, it is identified by Account ID and VPC ID. The owner of the peer Amazon VPC has one week to accept or reject the request to peer with the requesting Amazon VPC before the peering request expires.
- Peering connections do not support transitive routing.

Security Groups

- A *security group* is a virtual stateful firewall that controls inbound and outbound network traffic to AWS resources and Amazon EC2 instances. All Amazon EC2 instances must be launched into a security group. If a security group is not specified at launch, then the instance will be launched into the default security group for the Amazon VPC. The default security group allows communication between all resources within the security group, allows all outbound traffic, and denies all other traffic.

Security Group Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
sg-xxxxxxxx	All	All	Allow inbound traffic from instances within the same security group.

Outbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound traffic.

Sterling
Talent Solutions

Security Group Rules for a Web Server

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound traffic from the Internet to port 80.
Your network's public IP address range	TCP	22	Allow Secure Shell (SSH) traffic from your company network.
Your network's public IP address range	TCP	3389	Allow Remote Desktop Protocol (RDP) traffic from your company network.

Here are the important points to understand about security groups.

- You can create up to 500 security groups for each Amazon VPC. You can add up to 50 inbound and 50 outbound rules to each security group
- You can specify allow rules, but not deny rules. This is an important difference between security groups and ACLs.
- You can specify separate rules for inbound and outbound traffic.
- By default, no inbound traffic is allowed until you add inbound rules to the security group.
- By default, new security groups have an outbound rule that allows all outbound traffic.
- You can remove the rule and add outbound rules that allow specific outbound traffic only.
- Security groups are stateful. This means that responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules and vice versa. This is an important difference between security groups and network ACLs.
- Instances associated with the same security group can’t talk to each other unless you add rules allowing it (with the exception being the default security group).
- You can change the security groups with which an instance is associated after launch, and the changes will take effect immediately.

Network Access Control Lists (ACLs)

- A network *access control list (ACL)* is another layer of security that acts as a stateless firewall on a subnet level.
- A network ACL is a numbered list of rules that AWS evaluates in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL.
- Amazon VPCs are created with a modifiable default network ACL associated with every subnet that allows all inbound and outbound traffic.
- When you create a custom network ACL, its initial configuration will deny all inbound and outbound traffic until you create rules that allow otherwise.
- You may set up network ACLs with rules similar to your security groups in order to add a layer of security to your Amazon VPC, or you may choose to use the default network ACL that does not filter traffic traversing the subnet boundary. Overall, every subnet must be associated with a network ACL.

Network Address Translation (NAT) Instances and NAT Gateways

By default, any instance that you launch into a private subnet in an Amazon VPC is not able to communicate with the Internet through the IGW. This is problematic if the instances within private subnets need direct access to the Internet from the Amazon VPC in order to apply security updates, download patches, or update application software. AWS provides NAT instances and NAT gateways to allow instances deployed in private subnets to gain Internet access.

NAT Instance

- A *network address translation (NAT) instance* is an Amazon Linux Amazon Machine Image (AMI) that is designed to accept traffic from instances within a private subnet, translate the source IP address to the public IP address of the NAT instance, and forward the traffic to the IGW.
- In addition, the NAT instance maintains the state of the forwarded traffic in order to return response traffic from the Internet to the proper instance in the private subnet. These instances have the string amzn-ami-vpc-nat in their names, which is searchable in the Amazon EC2 console.

To allow instances within a private subnet to access Internet resources through the IGW via a NAT instance, you must do the following:

- Create a security group for the NAT with outbound rules that specify the needed Internet resources by port, protocol, and IP address.
- Launch an Amazon Linux NAT AMI as an instance in a public subnet and associate it with the NAT security group.
- Disable the Source/Destination Check attribute of the NAT.
- Configure the route table associated with a private subnet to direct Internet-bound traffic to the NAT instance (for example, i-1a2b3c4d).
- Allocate an EIP and associate it with the NAT instance.

This configuration allows instances in private subnets to send outbound Internet communication, but it prevents the instances from receiving inbound traffic initiated by someone on the Internet associate it with the NAT instance.

NAT Gateway

- *NAT gateway* is an Amazon managed resource that is designed to operate just like a NAT instance, but it is simpler to manage and highly available within an Availability Zone.

To allow instances within a private subnet to access Internet resources through the IGW via a NAT gateway, you must do the following:

- Configure the route table associated with the private subnet to direct Internet-bound traffic to the NAT gateway (for example, nat-1a2b3c4d).
- Allocate an EIP and associate it with the NAT gateway.

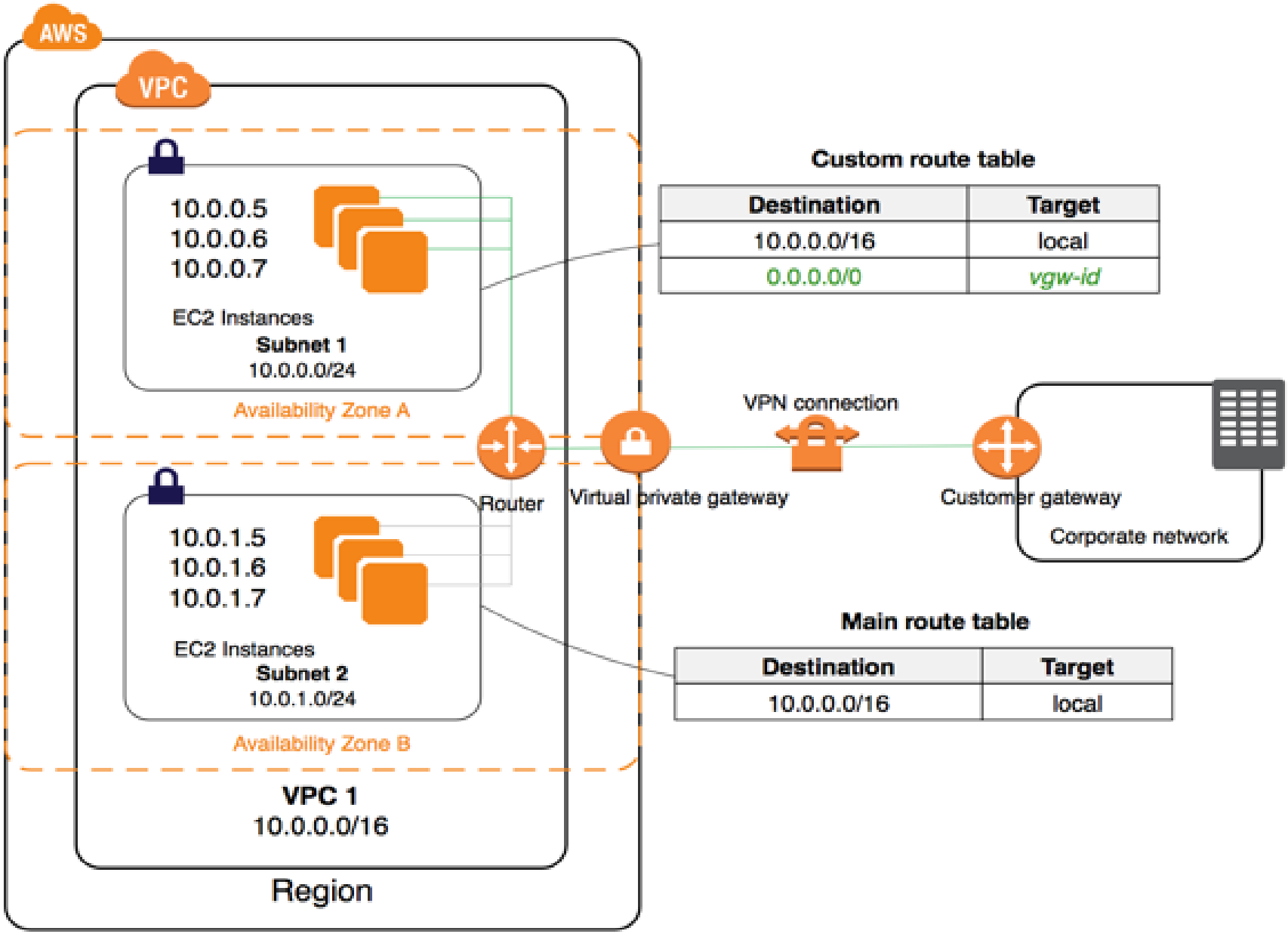
Virtual Private Gateways (VPGs), Customer Gateways (CGWs), and Virtual Private Networks (VPNs)

- You can connect an existing data center to Amazon VPC using either hardware or software VPN connections, which will make Amazon VPC an extension of the data center. Amazon VPC offers two ways to connect a corporate network to a VPC: VPG and CGW.
- A *virtual private gateway (VPG)* is the *virtual private network (VPN)* concentrator on the AWS side of the VPN connection between the two networks. A *customer gateway (CGW)* represents a physical device or a software application on the customer's side of the VPN connection. After these two elements of an Amazon VPC have been created, the last step is to create a VPN tunnel. The VPN tunnel is established after traffic is generated from the customer's side of the VPN connection.

- You must specify the type of routing that you plan to use when you create a VPN connection. If the CGW supports Border Gateway Protocol (BGP), then configure the VPN connection for dynamic routing. Otherwise, configure the connections for static routing. If you will be using static routing, you must enter the routes for your network that should be communicated to the VPG. Routes will be propagated to the Amazon VPC to allow your resources to route network traffic back to the corporate network through the VGW and across the VPN tunnel. Amazon VPC also supports multiple CGWs, each having a VPN connection to a single VPG (many-to-one design). In order to support this topology, the CGW IP addresses must be unique within the region.
- Amazon VPC will provide the information needed by the network administrator to configure the CGW and establish the VPN connection with the VPG. The VPN connection consists of two Internet Protocol Security (IPSec) tunnels for higher availability to the Amazon VPC.

Following are the important points to understand about VPGs, CGWs, and VPNs:

- The VPG is the AWS end of the VPN tunnel.
- The CGW is a hardware or software application on the customer's side of the VPN tunnel.
- You must initiate the VPN tunnel from the CGW to the VPG.
- VPGs support both dynamic routing with BGP and static routing.
- The VPN connection consists of two tunnels for higher availability to the VPC



Limitations

- 5 VPC per account per region
- 200 Subnet per VPC
- 5 EIP per account per region
- 1 IGW per VPC
- 5 VPG per account per region
- 50 CWG per account per region