Lesson 6 VPC

Michael Yang

What is VPC

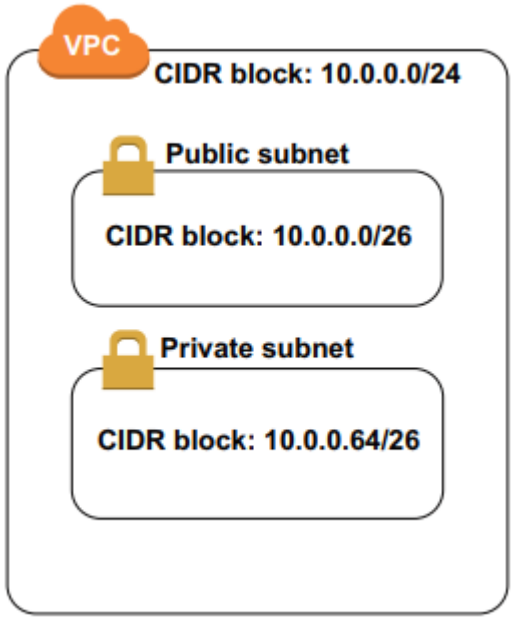
- A VPC is a virtual network. If you want to create any networked resources in AWS, you're going to first have to create a VPC.
- This is a relatively easy task, as a VPC has only a couple of options. The main one is the CIDR block. This is the range of IP addresses that will be available for use in your network. CIDR stands for classless inter-domain routing

CIDR block	Equivalent IP range	Note
10.0.0.0/24	10.0.0.0–10.0.0.255	Contains the 256 addresses, starting at 10.0.0.0
192.168.1.1/32	192.168.1.1	Only contains 1 address
0.0.0.0/0	0.0.0.0–255.255.255.255	Covers the entire IPv4 address space

Create a VPC

```
$ aws ec2 create-vpc \
--cidr-block 10.0.0.0/24
```

Create a Subnet



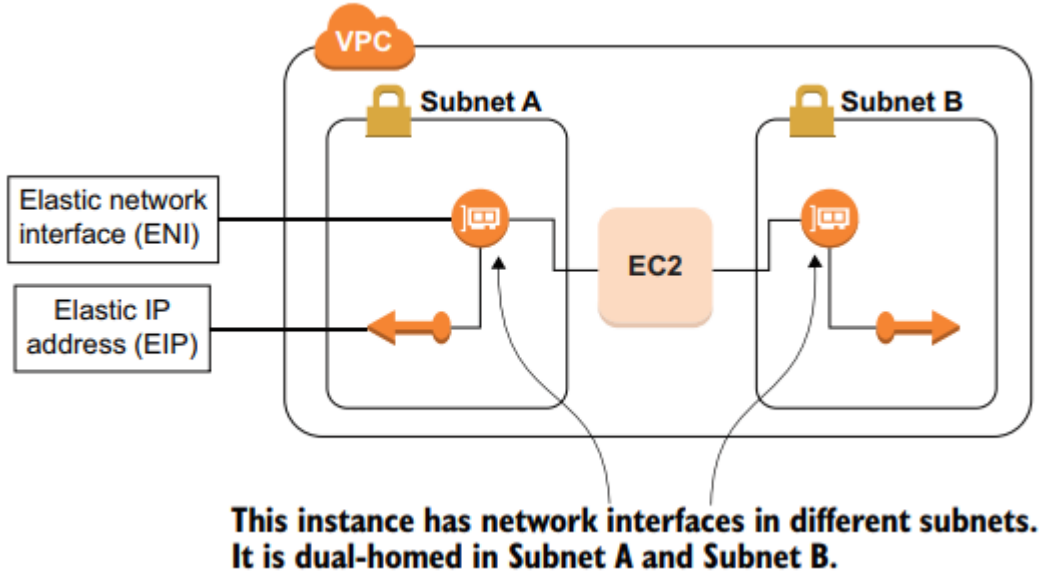
This is the ID of the VPC created earlier.

```
$ aws ec2 create-subnet \
    --vpc-id vpc-1234
    --cidr-block 10.0.0.0/26

$ aws ec2 create-subnet \
    --vpc-id vpc-1234
    --cidr-block 10.0.0.64/26
```

NIP

- Elastic network interfaces are the virtual equivalent of an NIC or network card on a physical machine. These ENIs are the connection between networked resources like EC2 instances and your virtual network. In fact, you can attach additional ENIs to your instances, and those ENIs can be in two different subnets. This creates what are called *dual-homed* instances, which can be visualized below



ENI

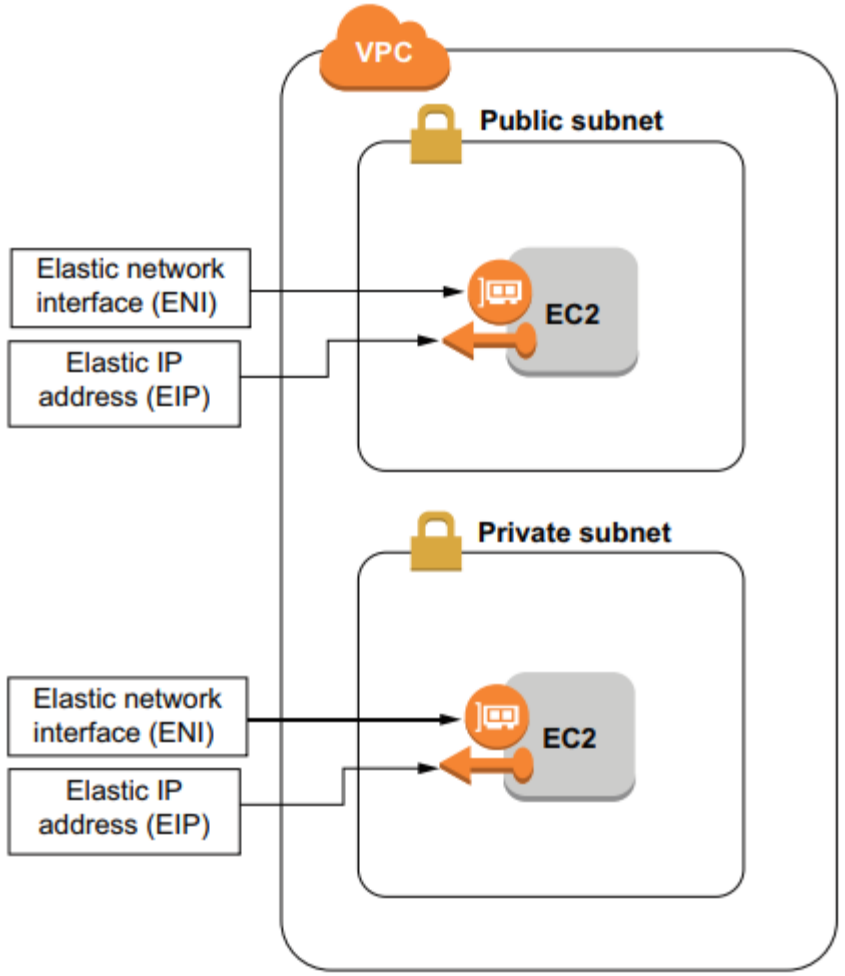
```
$ aws ec2 run-instances \
--instance-type t2.micro \
--subnet-id subnet-1234
--image-id ami-1234

$ aws ec2 run-instances \
--instance-type t2.micro \
--subnet-id subnet-5678
--image-id ami-1234 #B
```

Replace with the ID of the public subnet.

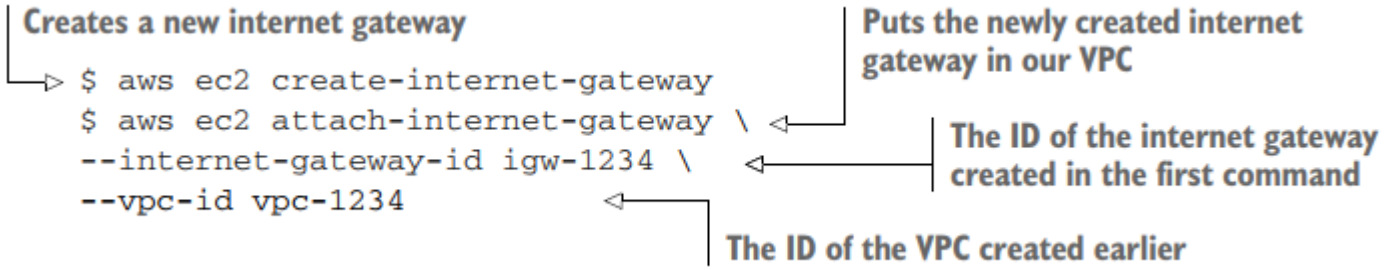
Replace with the ID of the AMI you want to use.

Replace with the ID of the private subnet.



Internet gateway

- An internet gateway, sometimes called an IGW, is a resource that is created in a VPC. When an internet gateway is attached to a VPC, then traffic can be routed from inside the VPC to the internet through that IGW, and vice versa.



Internet gateway

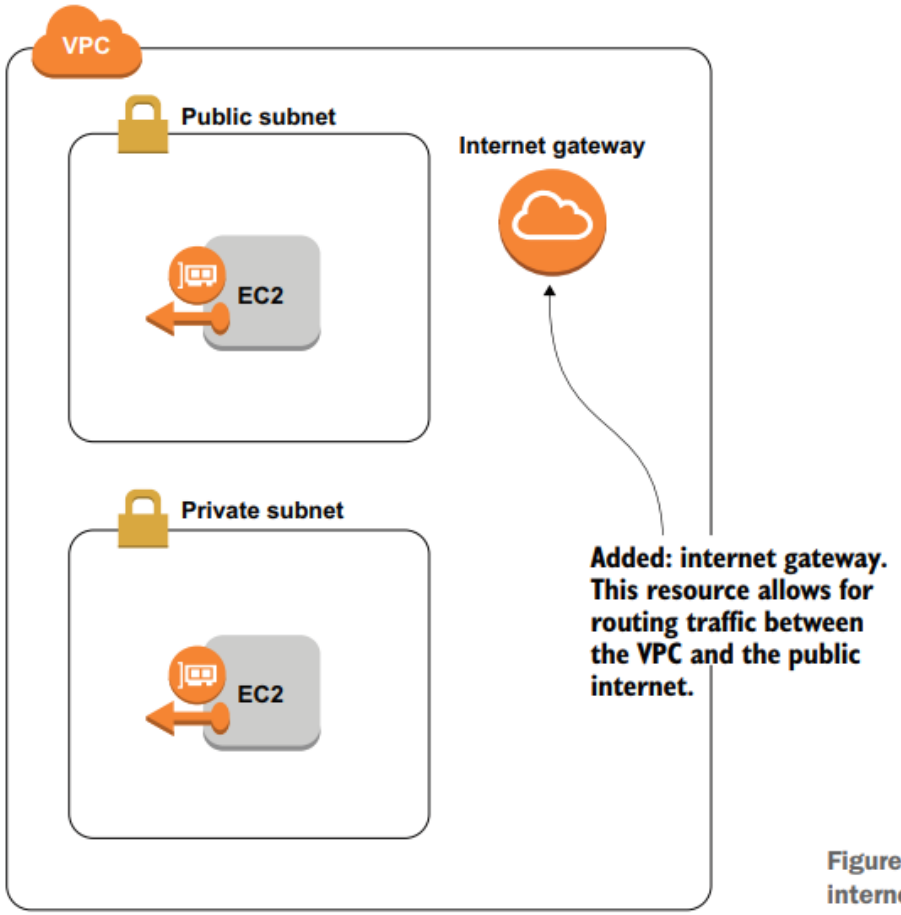
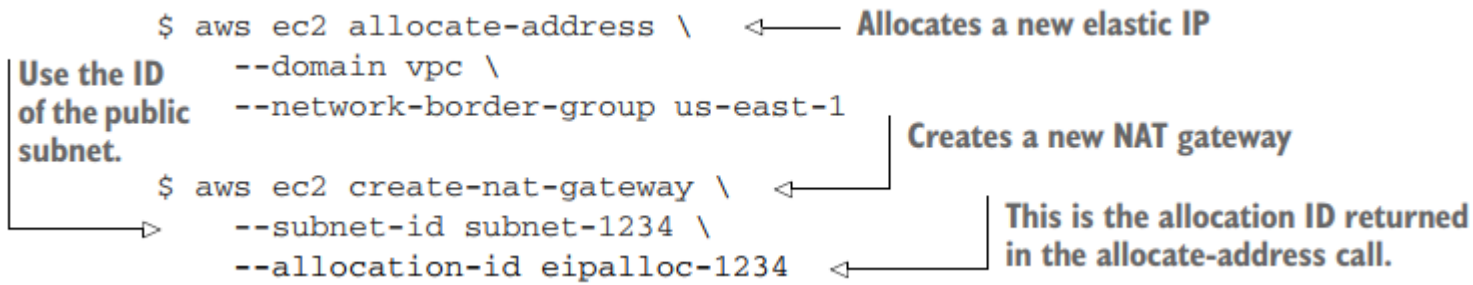


Figure 5.5 Adding an internet gateway to a VPC

NAT gateway

- A NAT gateway is not an alternative to an internet gateway; they actually work in tandem.



NAT gateway

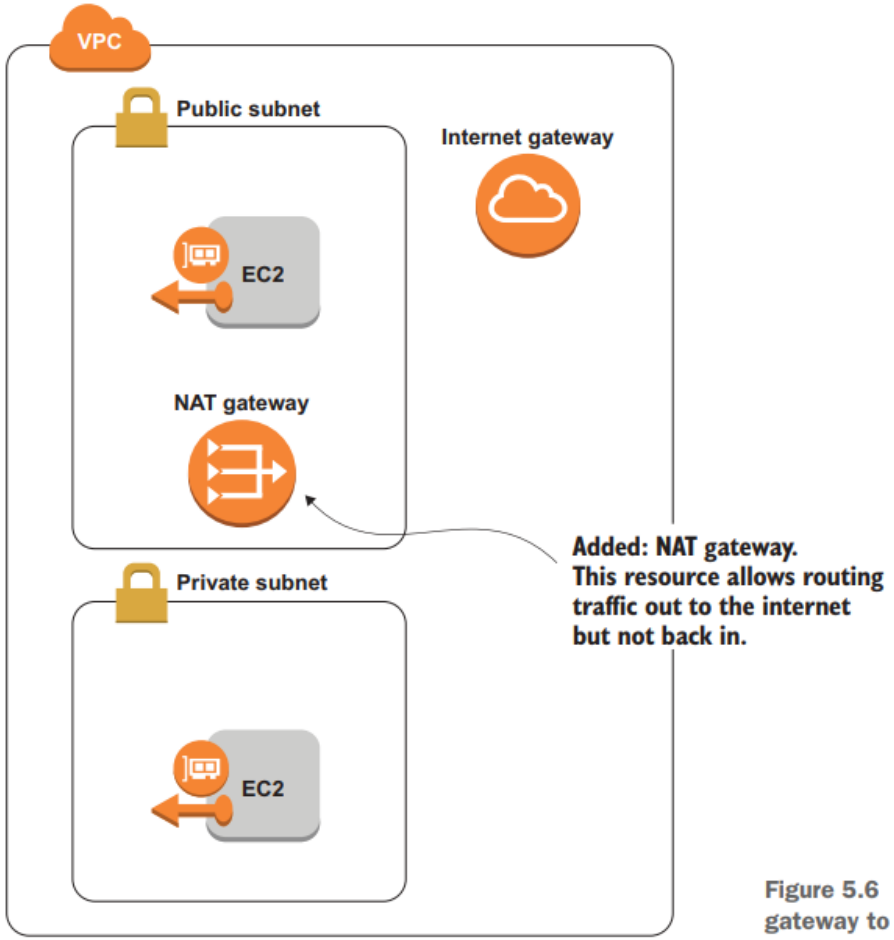


Figure 5.6 Adding a NAT gateway to a public subnet

Route table

- A route table defines how traffic is routed throughout your VPC. It is a set of rules that say where traffic should be directed based on the IP address it was sent to. Each of these rules is aptly called a *route*. Every route consists of two parts: a destination and a target.

- Whenever you create a VPC, a route table is automatically created and attached to that VPC for you.

Route	Destination	Target
Route 1	10.0.0.0/26	local
Route 2	0.0.0.0/0	igw-1234

Route tables

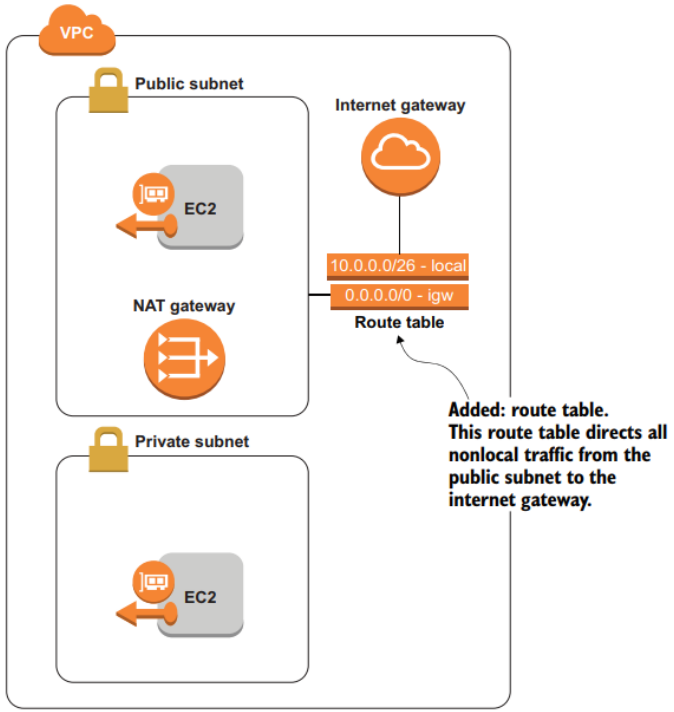
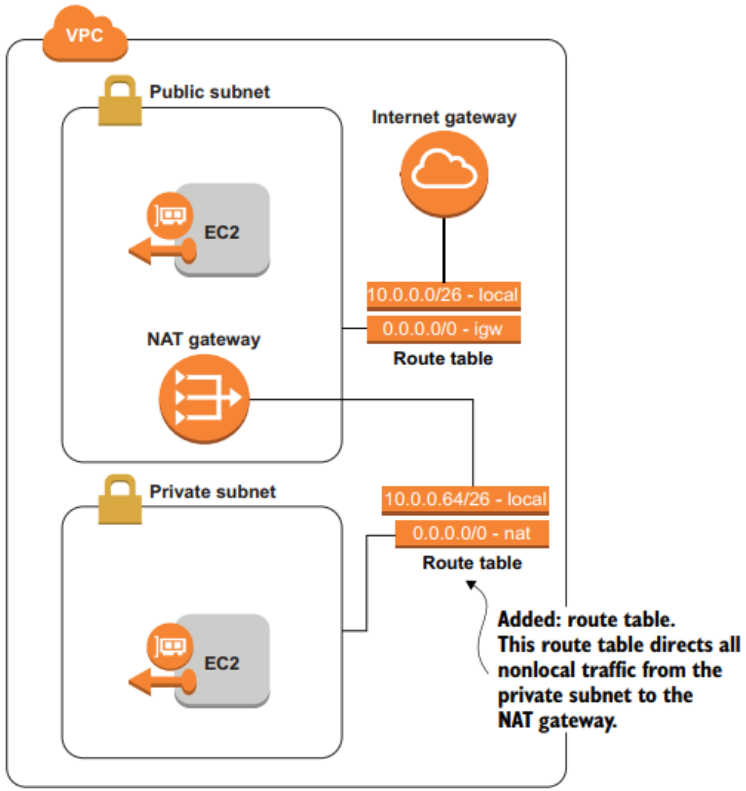
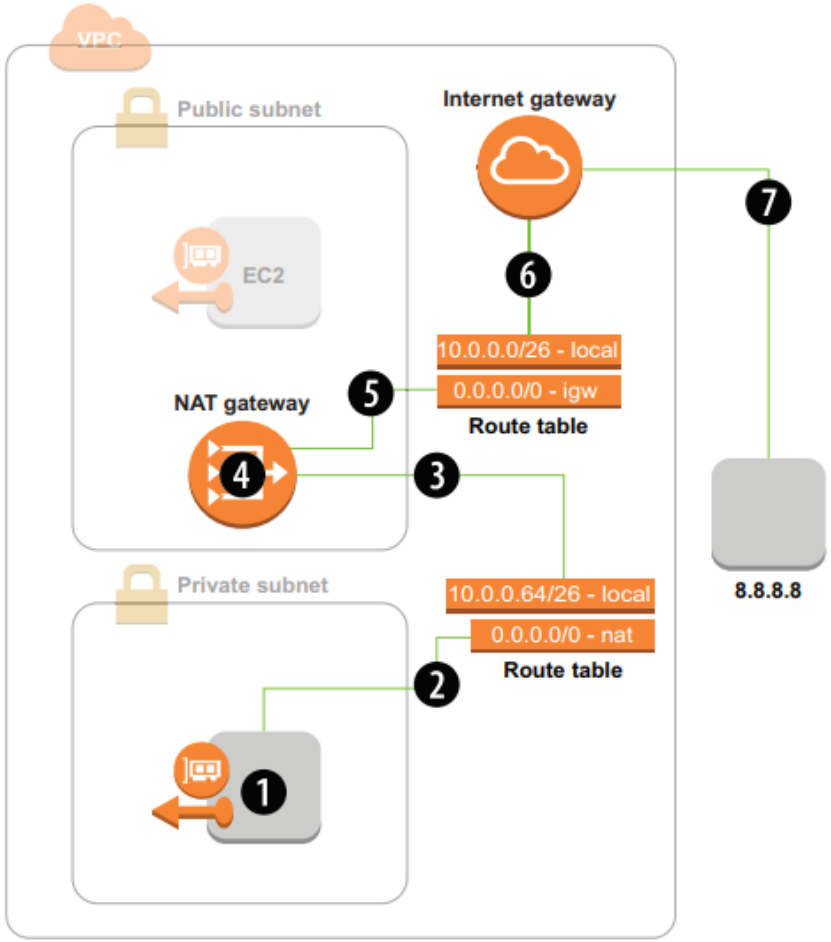


Figure 5.8 Using a route table to connect a subnet to an internet gateway. The route table has a default route that directs local traffic within the VPC, and a custom route that directs all other traffic through the IGW.

Route table


VPC
Public subnet
Internet gateway
EC2
10.0.0.0/26 - local
0.0.0.0/0 - igw
Route table
NAT gateway
Private subnet
10.0.0.64/26 - local
0.0.0.0/0 - nat
Route table
EC2
Added: route table.
This route table directs all
nonlocal traffic from the
private subnet to the
NAT gateway.

- The path of traffic as it flows between an instance in a private subnet to a server in the public internet, leveraging NAT and internet gateways



Security Group

- A *security group* is a set of rules that determine what network traffic is allowed in and out of an instance.
- There are two kinds of rules in a security group, inbound and outbound, and each is made up of three key elements.
- An example TCP outbound rule might look like what is shown in table

Destination	Protocol (number)	Port range
0.0.0.0/0	TCP (6)	443

Security Group

Inbound security group rule allowing TCP traffic on port 22 from anywhere

Source	Protocol (number)	Port range
0.0.0.0/0	TCP (6)	22

When you create a VPC, a default security group is created.

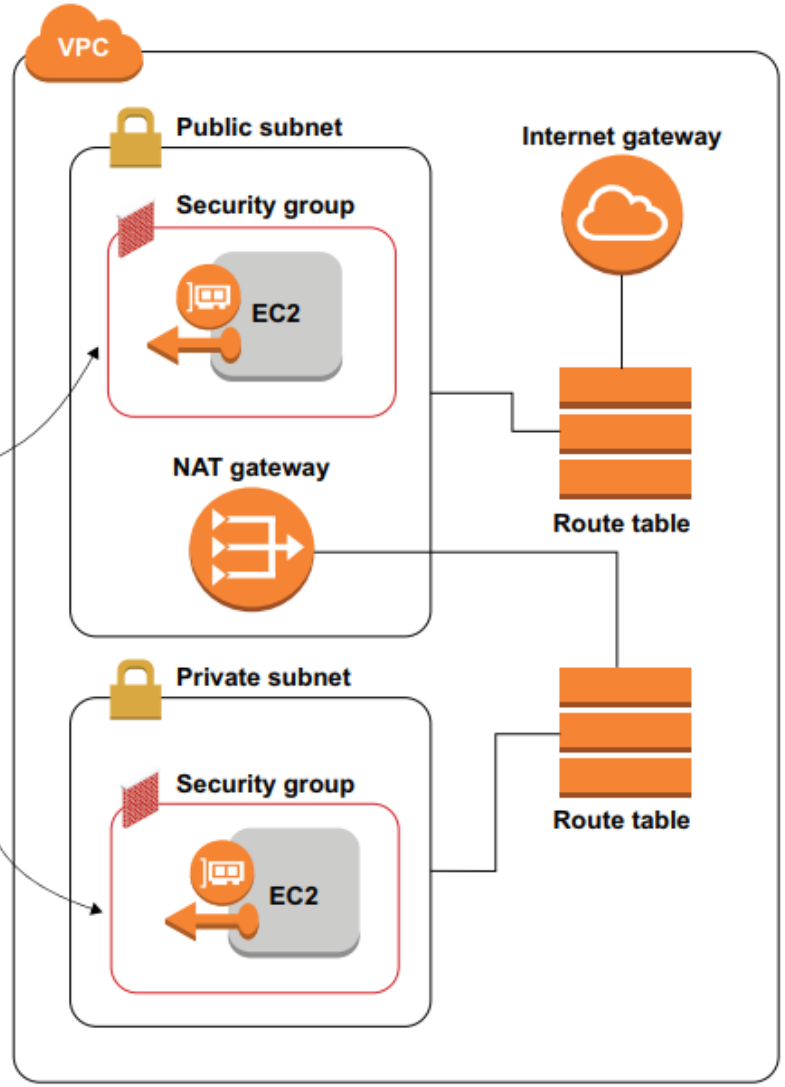
Type	Source/destination	Protocol	Port range
Inbound	self	All	All (0-65535)
Outbound	0.0.0.0/0	All	All (0-65535)

Bad Inbound

Source	Protocol (number)	Port range
0.0.0.0/0	TCP (6)	80
0.0.0.0/0	TCP (6)	443

Added: security group. The security group on the instance in the public subnet allows inbound SSH traffic from anywhere.

Both instances also have the default security group, which allows all outbound connections and any inbound connections from other instances in the same security group.



Network ACLs

- The first rule allows HTTPS traffic, while the second denies all TCP traffic. If an HTTPS connection were to be initiated, it would be allowed, since rule #100 is evaluated first, and it allows the traffic.

Rule #	Type	Protocol	Port range	Source	Allow or deny
100	HTTPS	TCP	443	0.0.0.0/0	Allow
200	ALL	TCP	ALL	0.0.0.0/0	Deny

Network ACLs

Security group rule allowing outbound HTTPS traffic

Type	Destination	Protocol (number)	Port range
Outbound	0.0.0.0/0	TCP (6)	443

Network ACL rules allowing outbound HTTPS traffic

Outbound/inbound	Rule #	Type	Protocol	Port range	Destination	Allow or deny
Outbound	100	HTTPS	TCP	443	0.0.0.0/0	Allow
Outbound	*	ALL	ALL	ALL	0.0.0.0/0	Deny
Inbound	*	ALL	ALL	ALL	0.0.0.0/0	Deny

Network ACLs In Practice

Network ACL rules allowing web traffic originating outside the VPC and traffic to a MongoDB server from within the VPC

Inbound/ outbound	Rule #	Type	Protocol	Port range	Source/ destination	Allow or deny
Outbound	100	HTTPS	TCP	443	0.0.0.0/0	Allow
Outbound	200	CUSTOM	TCP	27017	10.0.0.0/24	Allow
Outbound	*	ALL	ALL	ALL	0.0.0.0/0	Deny
Inbound	300	HTTPS	TCP	443	0.0.0.0/0	Allow
Inbound	400	CUSTOM	TCP	27017	10.0.0.0/24	Allow
Inbound	*	ALL	ALL	ALL	0.0.0.0/0	Deny