

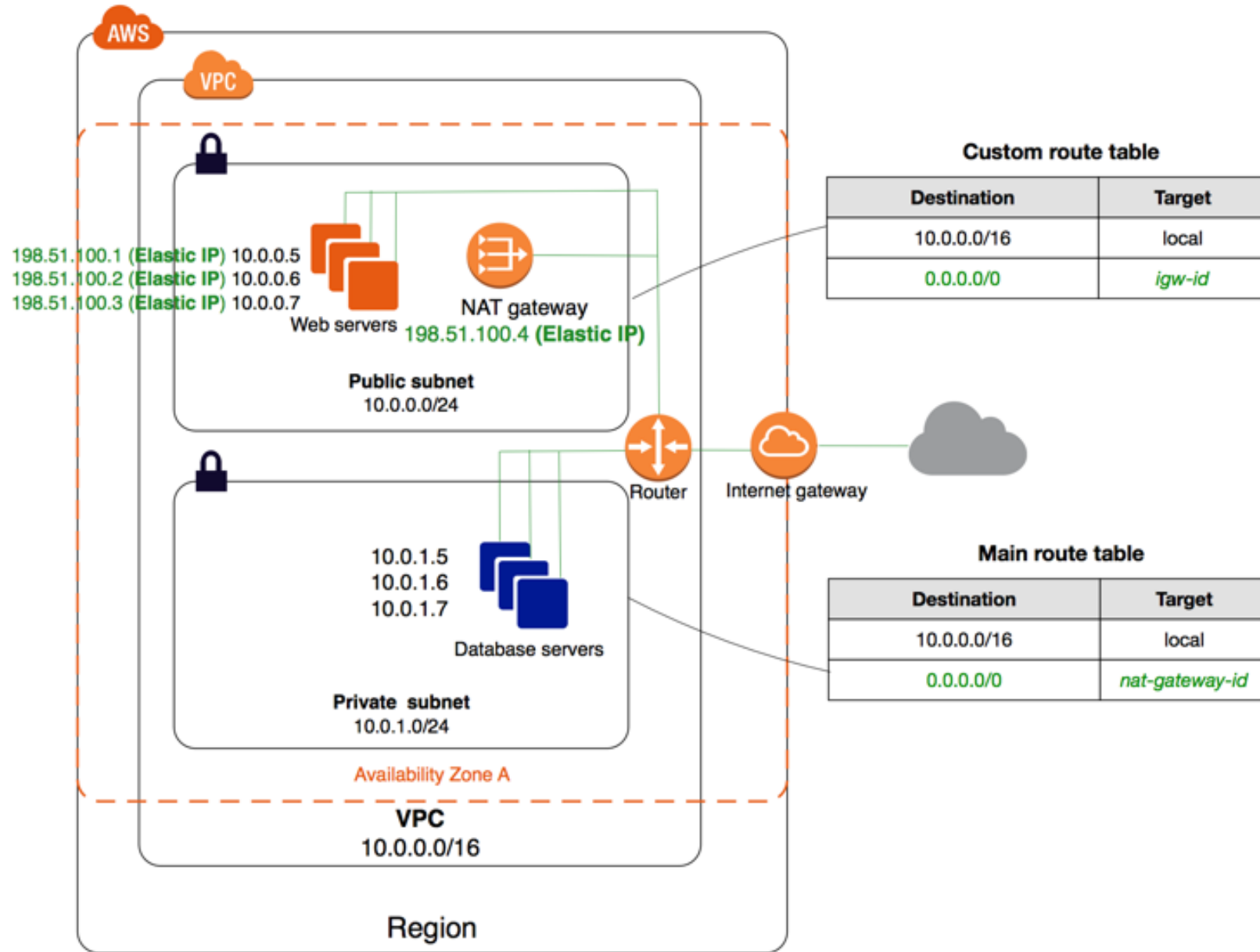


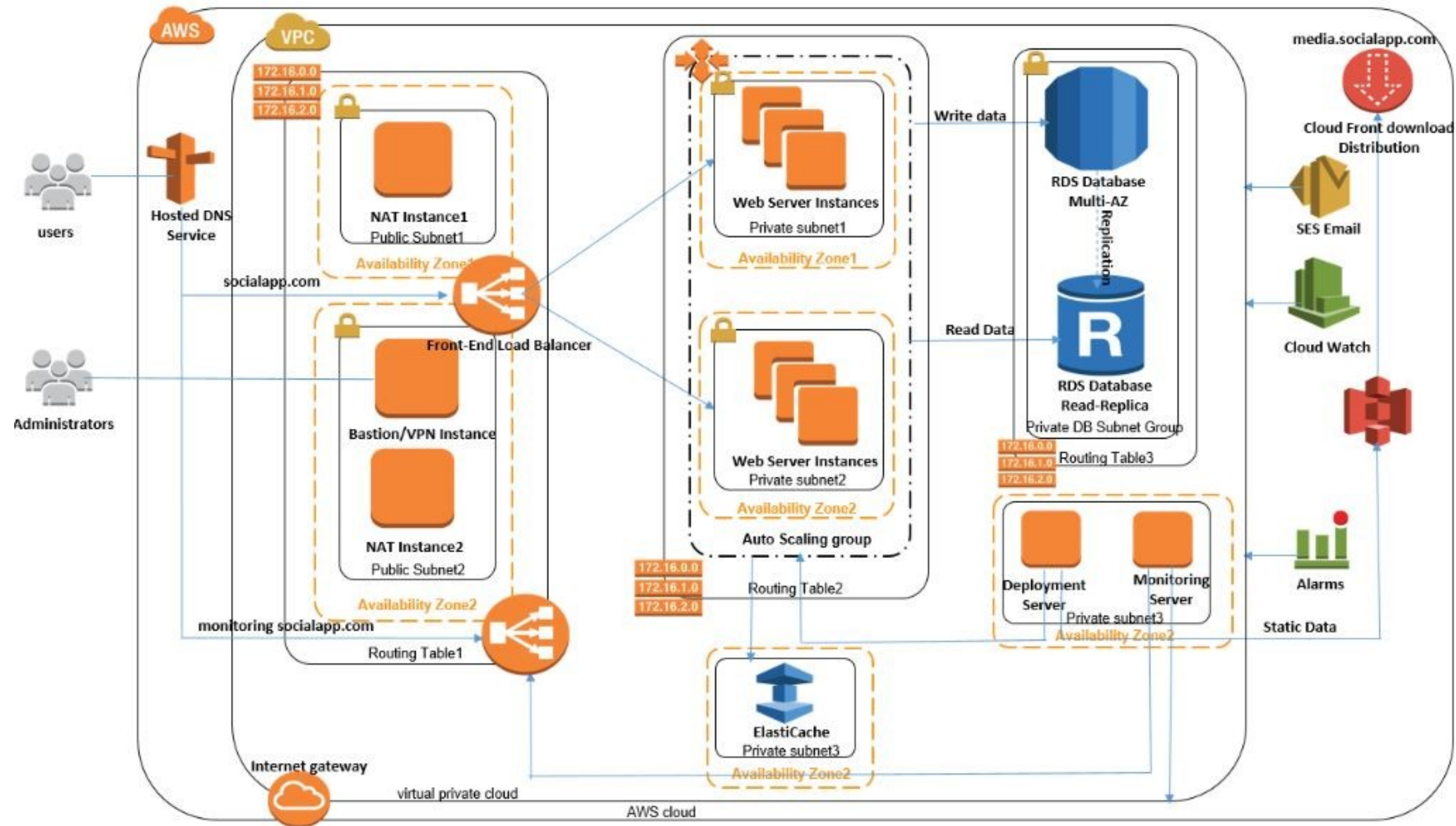
AWS Virtual Private Cloud (VPC)

What is VPC?



- Amazon VPC is your own private network inside Amazon's cloud infrastructure.
- It is an alternative to maintaining your own data center and is cheaper since it creates resources on demand.
- It is also more secure since Amazon takes care of the infrastructure security for you.

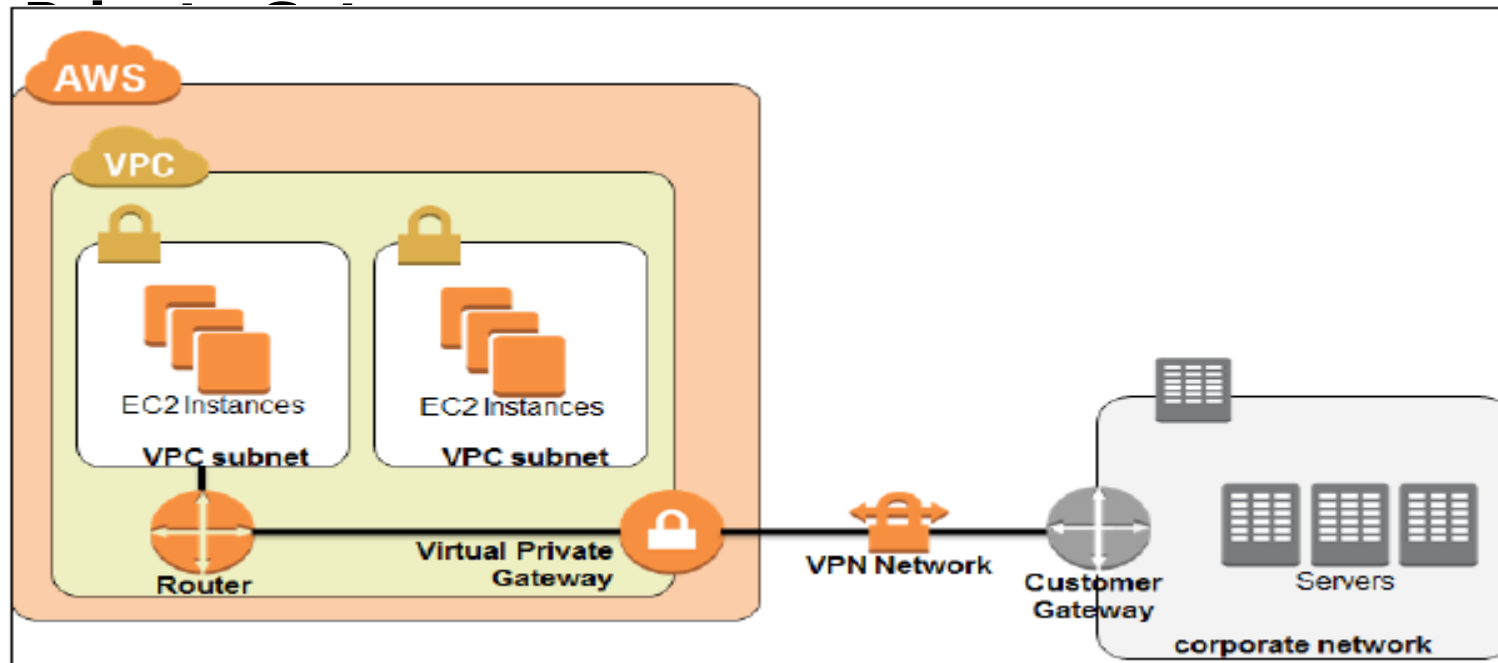




VPC and VPN



- VPCs also provide an added functionality using which you can connect and extend your on premise datacenters to the AWS cloud.
- This is achieved using an IPsec VPN tunnel that connects from your on premise datacenter's gateway device to the VPC's **Virtual**



VPC concepts and terminologies



- VPC is nothing more than a network service provided by AWS using which you can create logically isolated environments for your EC2 instances.
 - **CIDR Block**
 - **Subnets**
 - **Security groups and network ACLs**
 - **Routing tables**
 - **Internet Gateways**
 - **NAT instances/Gateways**

CIDR



- CIDR or Classless Inter-Domain Routing is used to allocate IP address within a network.
- We will use CIDR blocks to mark a range of IP addresses for each subnet within a VPC.
- The VPC itself would have a CIDR block that lists all the IP addresses available with it.

CIDR

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Create VPC

Actions ▾

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name ▾	VPC ID ▴	State ▾	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>		vpc-974efbed	available	172.31.0.0/16	-

Subnets



- The subnets are nothing more than a range of valid IP addresses that you specify.
- VPC provides you with two different subnet creation options: a publically or Internet routed subnet called as a **Public subnet** and an isolated subnet called as a **private subnet**.

Security Groups



- Security groups are nothing but simple firewall rules that you can configure to safeguard your instances.
- You can create a maximum of 100 security groups for a single VPC, with each Security Group containing up to 50 firewall rules in them.
- Also, it is very important to remember that a Security Group does not permit inbound traffic by default.
- You have to explicitly set inbound traffic rules to allow traffic to flow to your instance.
- However, all outbound traffic from the instance is allowed by default.

Network ACLs



- These provide an added security measure over security groups as they are instance specific, whereas Network ACLs are subnet specific.
- Unlike your security groups, however, you can both allow and restrict inbound and outbound traffic using ACL rules.
- Each ACL rule is evaluated by AWS based on a number. The number can be anything from 100 all the way up to 32,766.
- When you create a new NACL, both inbound and outbound rules are deny by default
- One subnet is associated with one NACL, however NACL can have multiple subnets associated
- Deny will apply first and then allow

Network ACLs



View

All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	<u>HTTP (80)</u>	TCP (6)	80	<u>0.0.0.0/0</u>	<u>ALLOW</u>
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
400	<u>HTTP (80)</u>	TCP (6)	80	<u>107.16.110.187/32</u>	<u>DENY</u>
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
<u>99</u>	<u>HTTP (80)</u>	TCP (6)	<u>80</u>	<u>107.16.110.187/32</u>	<u>DENY</u>
<u>100</u>	<u>HTTP (80)</u>	TCP (6)	<u>80</u>	<u>0.0.0.0/0</u>	<u>ALLOW</u>
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Example of how ACL rules

VPC Dashboard

Filter by VPC:
Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create network ACL Actions

Filter by tags and attributes or search by keyword

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-93e9f5e9	6 Subnets	Yes	vpc-974efbed	289857919920

Network ACL: acl-93e9f5e9

Details Inbound Rules Outbound Rules Subnet associations Tags

Edit inbound rules

View All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

What do these rules mean?

- 100 = traffic to flow from any protocol running on any port in and out of the subnet.
- * = That you drop any packets that do not match the ACL's rules

Routing Table



- A route table contains rules for routing traffic within a subnet and from the subnet to outside world.
-
- Amongst other things, we use routing tables to add internet gateways and NAT gateways to the subnet.

Internet Gateways



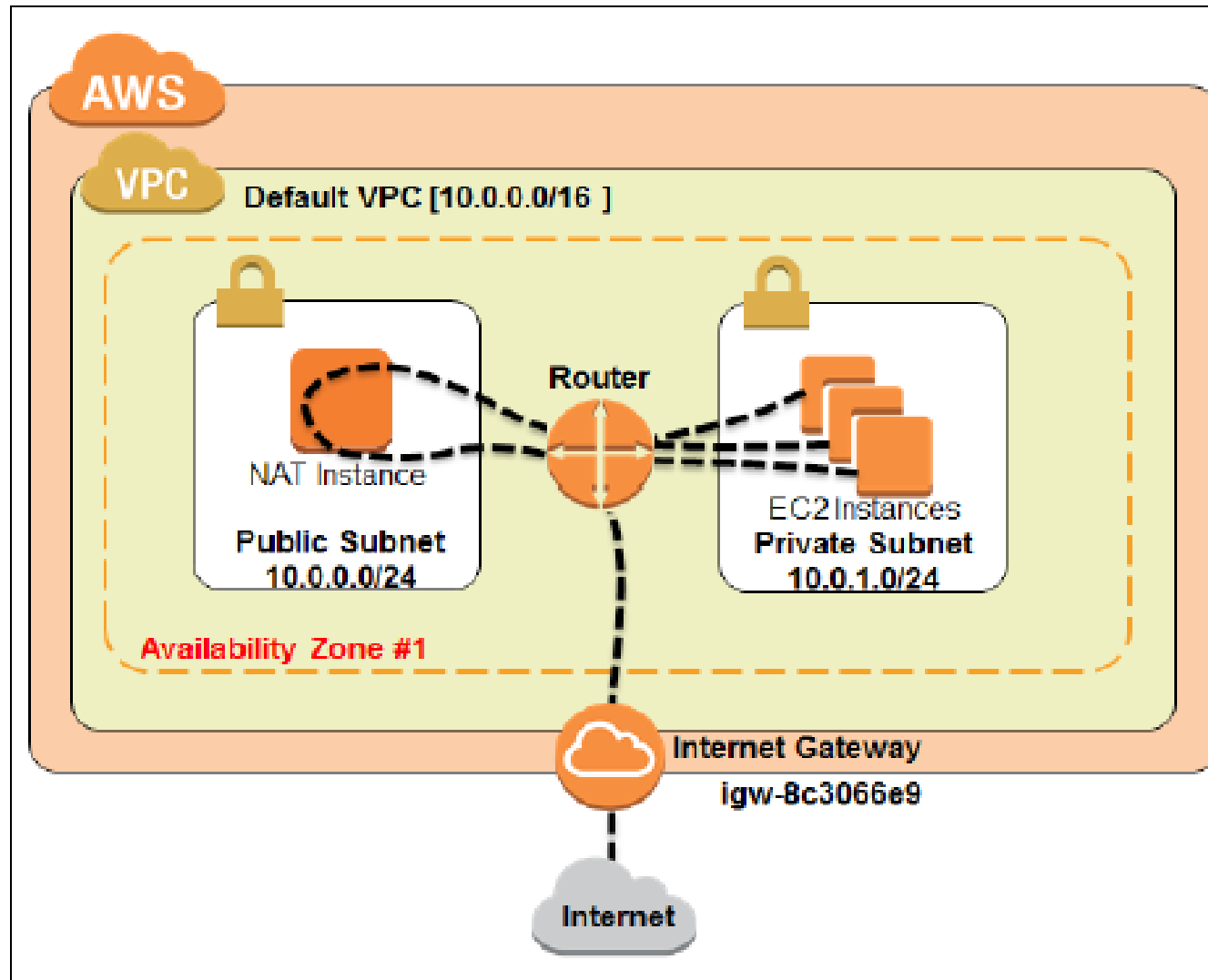
- Internet Gateways, as the name suggest, are primarily used to provide Internet connectivity to your VPC instances.
- An Internet Gateway allows you to make a subnet public by providing a route to the internet.
- All instances within the subnet can access the internet only through this gateway. Also, resources from the internet can access the instances in your subnet using this gateway.

NAT Gateway



- You can allow instances from your private subnet to connect to the internet using a NAT gateway.
- The instances in the private subnet do not have an public IP address, so the NAT gateway translates the private IP to a public IP before routing the traffic out to the internet.
- NAT stands for Network Address Translation and it does just that – translates private IPs to public IP.

NAT Gateway



VPC deployment scenarios



- VPC provides a simple, easy-to-use wizard that can spin up a fully functional VPC within a couple of minutes. All you need to do is select a particular deployment scenario out of the four scenarios provided and configure a few basic parameters such as subnet information, availability zones in which you want to launch your subnets, and so on, and the rest is all taken care of by AWS itself.
- **VPC with a single public subnet**
- **VPC with public and private subnets (NAT)**
- **VPC with public and private subnets and hardware VPN access**
- **VPC with a private subnet only and hardware VPN access**

VPC with a Single Public Subnet



Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

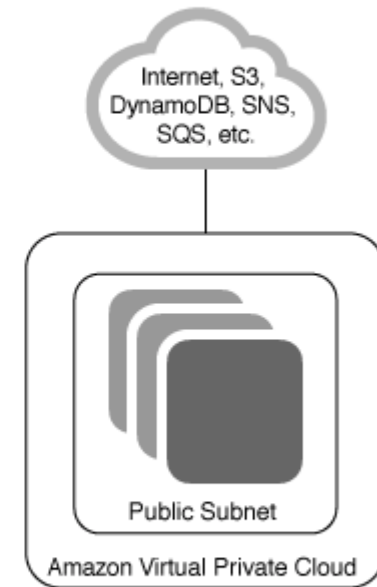
VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select



VPC with Public and Private Subnets



Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

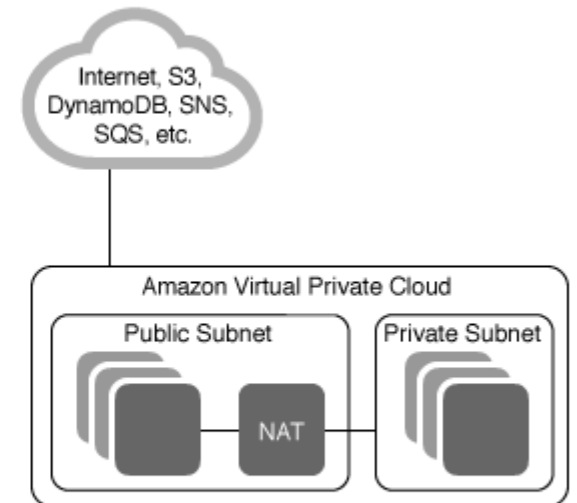
VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

Creates:

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

Select



VPC with Public and Private Subnets and Hardware VPN Access



Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

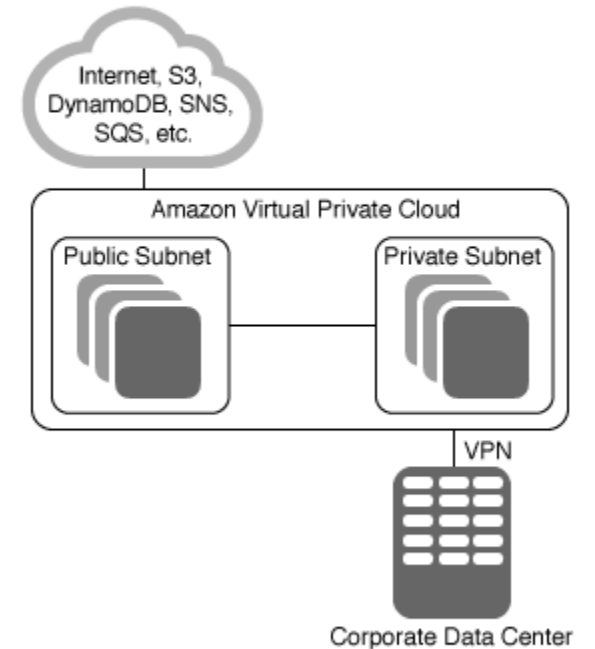
VPC with a Private Subnet Only and Hardware VPN Access

This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center - effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

Creates:

A /16 network with two /24 subnets. One subnet is directly connected to the Internet while the other subnet is connected to your corporate network via IPsec VPN tunnel. (VPN charges apply.)

Select



VPC with a Private Subnet Only and Hardware VPN Access



Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

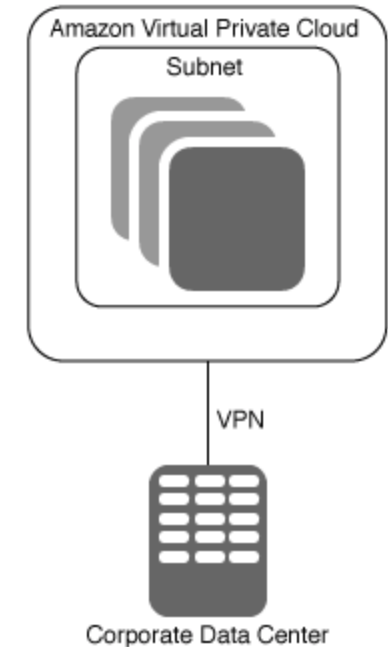
VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

Select



The Default VPC



The default VPC comes preconfigured with the following set of configurations:

The default VPC is always created with a CIDR block of /16, which means it supports 65,536 IP addresses in it.

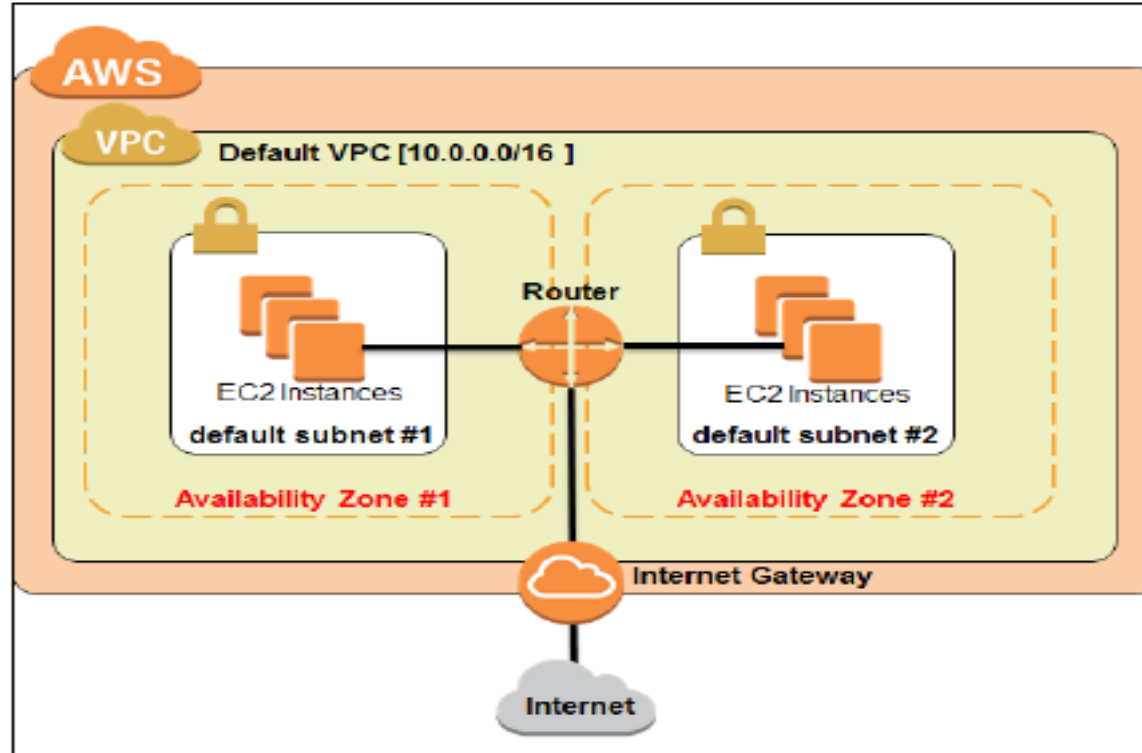
A default subnet is created in each AZ of your selected region. Instances launched in these default

subnets have both a public and a private IP address by default as well.

An Internet Gateway is provided to the default VPC for instances to have Internet connectivity.

A few necessary route tables, security groups, and ACLs are also created by default that enable the instance traffic to pass through to the Internet. Refer to the following figure:

The Default VPC



You can use this default VPC just as any other VPC by creating additional subnets in it, provisioning route tables, security groups, and so on.

Note: Any other VPC that you create besides the default VPC is called as the non-default VPC. Each non-default VPC in turn contains non-default subnets, and so on and so forth.

VPCs and flow logs



VPC flow logs are a way of capturing and recording IP traffic data that enters your VPC from its network interfaces.

As the data is collected it is stored in Amazon CloudWatch Logs. When a flow log is up and running you can review and retrieve data in Amazon CloudWatch Logs.

Flow logs can be created at 3 levels:

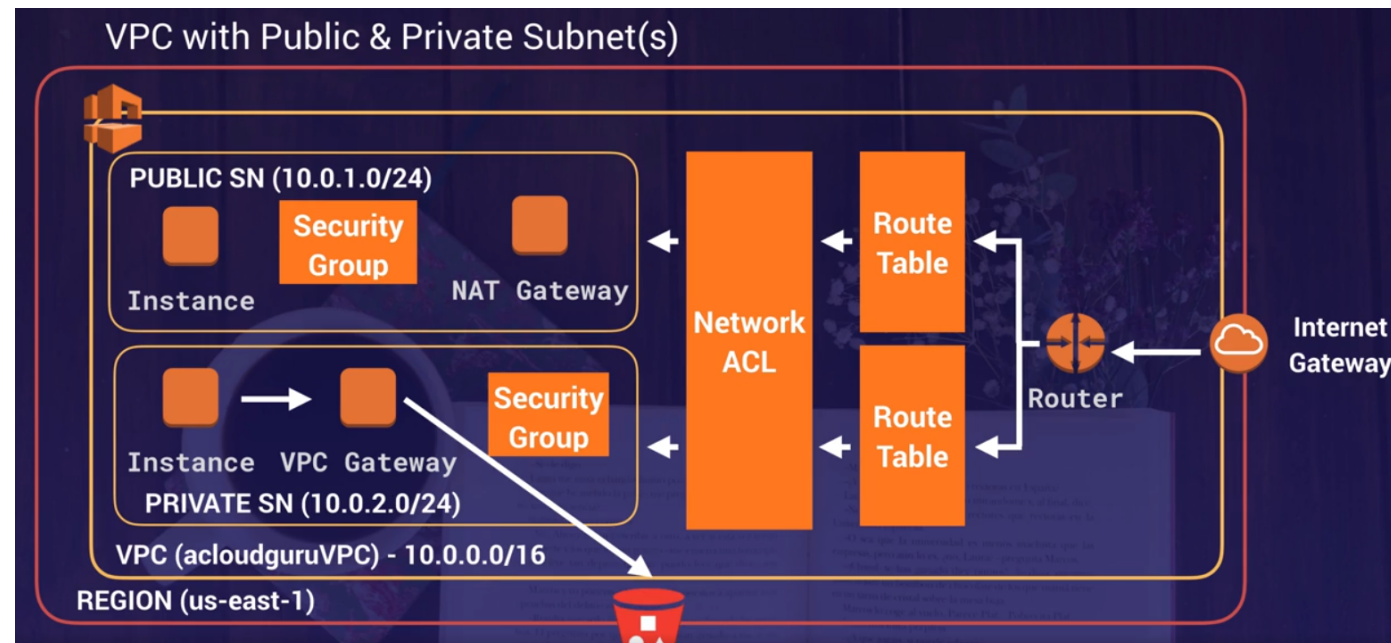
- VPC
- Subnet
- Network Interface Level

VPCs Endpoints



VPC endpoints simply allow for you private instances to access AWS resources such as S3 without the need to gain public internet access(IG), NAT etc. Which of course instances that reside in a private subnet won't have.

By configuring a VPC endpoint those private instances will now be able to access services such as S3 without the next to go via a NAT gateway.



VPCs Endpoints



A VPC endpoint allows you to securely connect your VPC to another service.

There are two types of ENDPOINTS

- An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
- A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Currently Gateway Endpoints supports Amazon S3 and DynamoDB

VPC Peering

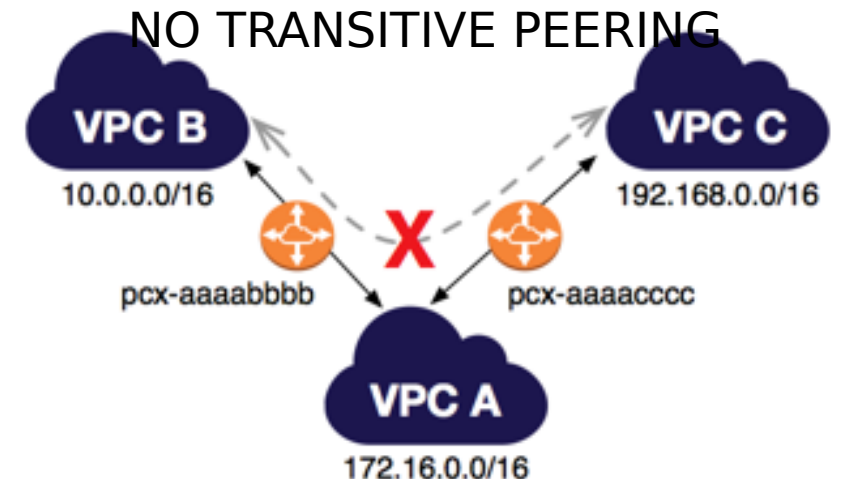
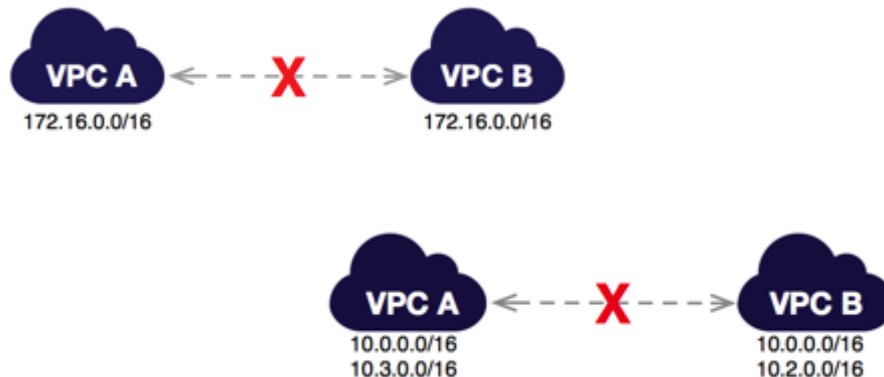


VPC peering is essentially a strong link between 2 separate VPCs.

It allows for communication between the 2 VPCs over private IP addresses as if they were in the same network.

You create VPC peering between VPCs within the same account or even VPCs across multiple accounts provided they are in the same region.

Things to note about VPC peering is that you can't peer 2 VPCs if they share overlapping IP addresses.



What do I need to know about VPCs?



Internet Gateway: Each VPC has only one internet gateway. It allows the instances inside your VPC access to the internet and allows vice versa.

Virtual Private Gateway: Again, very similar to the internet gateway, allowing an entry point to access the VPC from a remote session.

Router: Dictates where traffic entering the VPC should be sent to.

Router Table: contains a subset of rules determining which subnet traffic is sent to. All subnets must be associated with a route table.

Network Access Control List (NACL): acts as an optional firewall that sits outside of your subnet. All the rules defined in the NACL apply to all of the instances in the subnet.

Subnet: a range of IP addresses that house instances. Each subnet must be allocated a availability zone.

NAT gateway: a means for instances that reside in private subnets to access the

VPC Overview



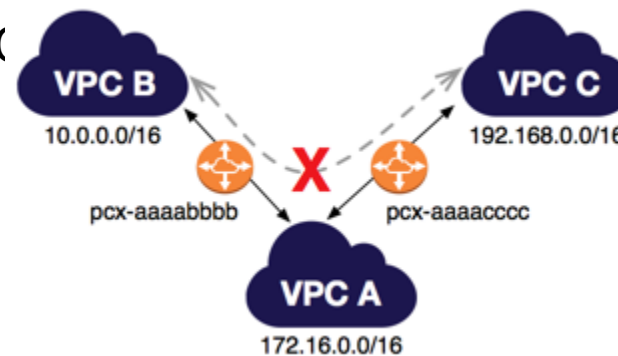
Think of a VPC as a logical datacenter in AWS

Consists of IGWs (or Virtual private Gateways), Route tables, NACLs, subnet and security groups

1 subnet = 1 AZ

Security groups are stateful , NACLs are stateless

NO TRANSITIVE PEERING



VPC Overview



When you create a VPC a default Route table, NACL and a default security group will be created

It won't create any subnets, nor it will create a default internet gateway

Amazon always reserves 5 IP addresses within your subnets (Example: 10.0.0.0/24)

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS for DNS
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address

You can have only 1 Internet Gateway per VPC

Security Groups can't span VPC's

VPC Exam Tips



- VPCs are region specific and there is a “limit” on the number of VPC’s you can have per region. That limit is 5. However you can easily increase that limit simply by contacting AWS support and requesting the limit be increased.
- You can not specify multiple internet gateways per VPC. You get only 1 per VPC. This shouldn’t be an issue as they are highly available and if one were to fail then another availability zone would take over.
- A concept that is important to get your head around early on is that a subnet does not span multiple availability zones.
- The default VPC that gets created when you account is setup has subnets associated with it. However they all have internet exposure. None of them are private. This is to make setting up AWS resources simpler initially.
- Lastly, Network Area Control Lists or NACLs for short let you block specific IP address and allow others for your VPC and subnets. This gives a much greater level of control.

Exam Tips: NAT instance & gateway summary



- NAT gateways are generally preferred against NAT instances.
- For NAT instance, you must remember to disable source/destination check for each NAT instance.
- NAT gateways/instances must be placed in public subnets.
- You'll need to configure the routing table of the private subnet to receive traffic via the NAT gateway/instance.
- Your bandwidth for NAT instances is limited by the size of the instance it's running on.
- You can achieve high availability from NAT instances via auto scaling groups and you can achieve high availability from NAT gateways via multiple availability zones.

Exam Tips: Network ACL's



- Your VPC automatically comes a default network ACL, and by default it allows all outbound and inbound traffic.
- You can create custom network ACLs. By default, each custom NACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a NACL, the subnet is automatically associate with default NACL.
- Block IP addresses using NACL not security groups
- You can associate a network ACL with multiple subnets; however a subnet can be associated with only one NACL at a time. When you associate a NACL with a subnet, previous association will be removed.
- NACL are stateless and it can deny traffic, where in SG it only allows.

Flow log Exam Tips



- Tags are currently not supported by flow logs.
- After a flow log is created, you can NOT change its configuration
- You cannot enable flow logs for VPCs that are peered with your VPC, unless you enable VPC peering for your account.
- After you have created a flow log, you cannot change the configuration like you cant associate IAM roles to flow logs etc

Not all traffic is monitored by flow logs, notable exceptions include:

- DNS server traffic from your VPC instances.
- Traffic generated by windows instances searching for windows license activation.
- DHCP traffic.
- Traffic from the reserved IP address for the default VPC router.

Tooooo Much

