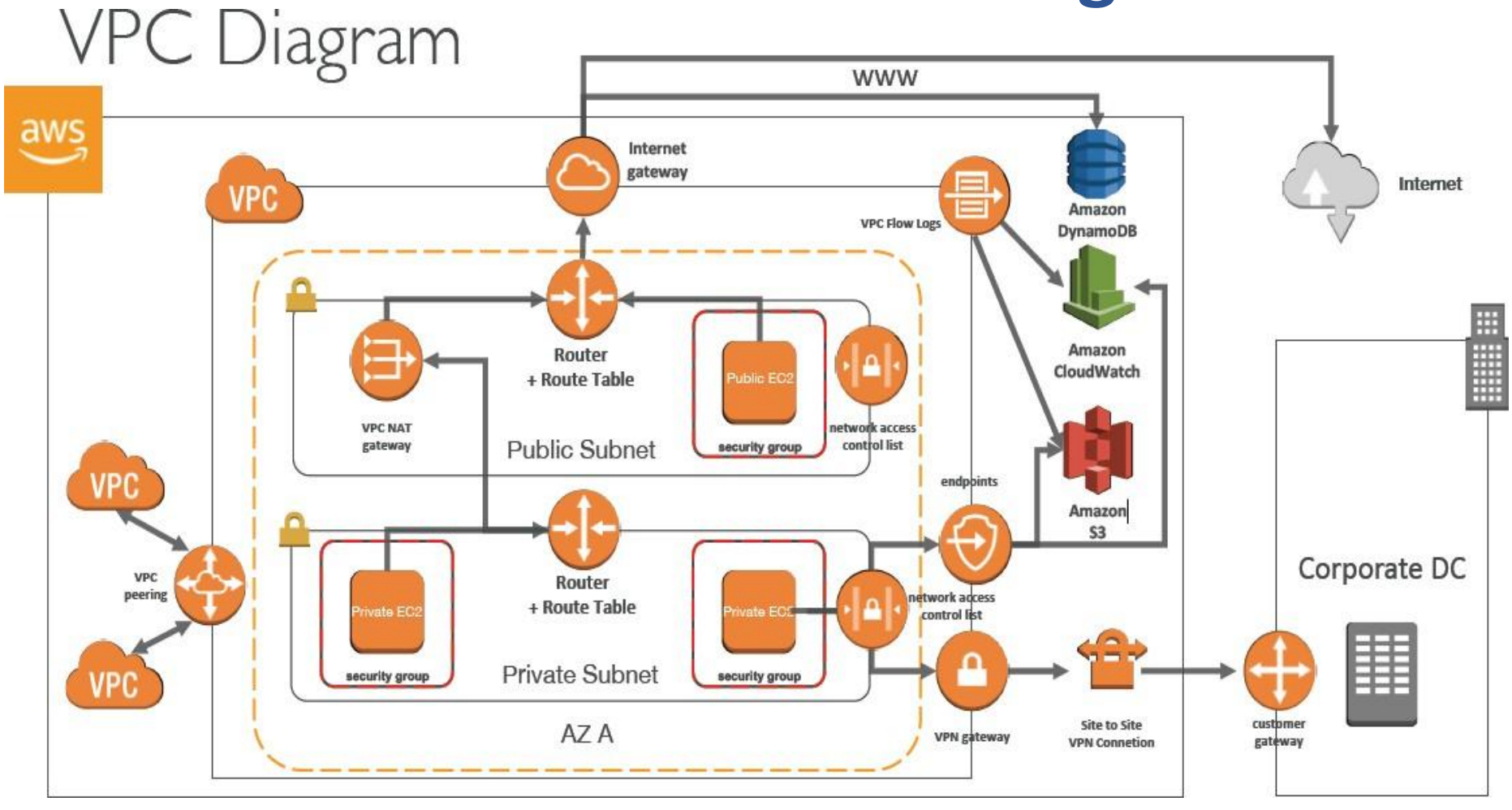
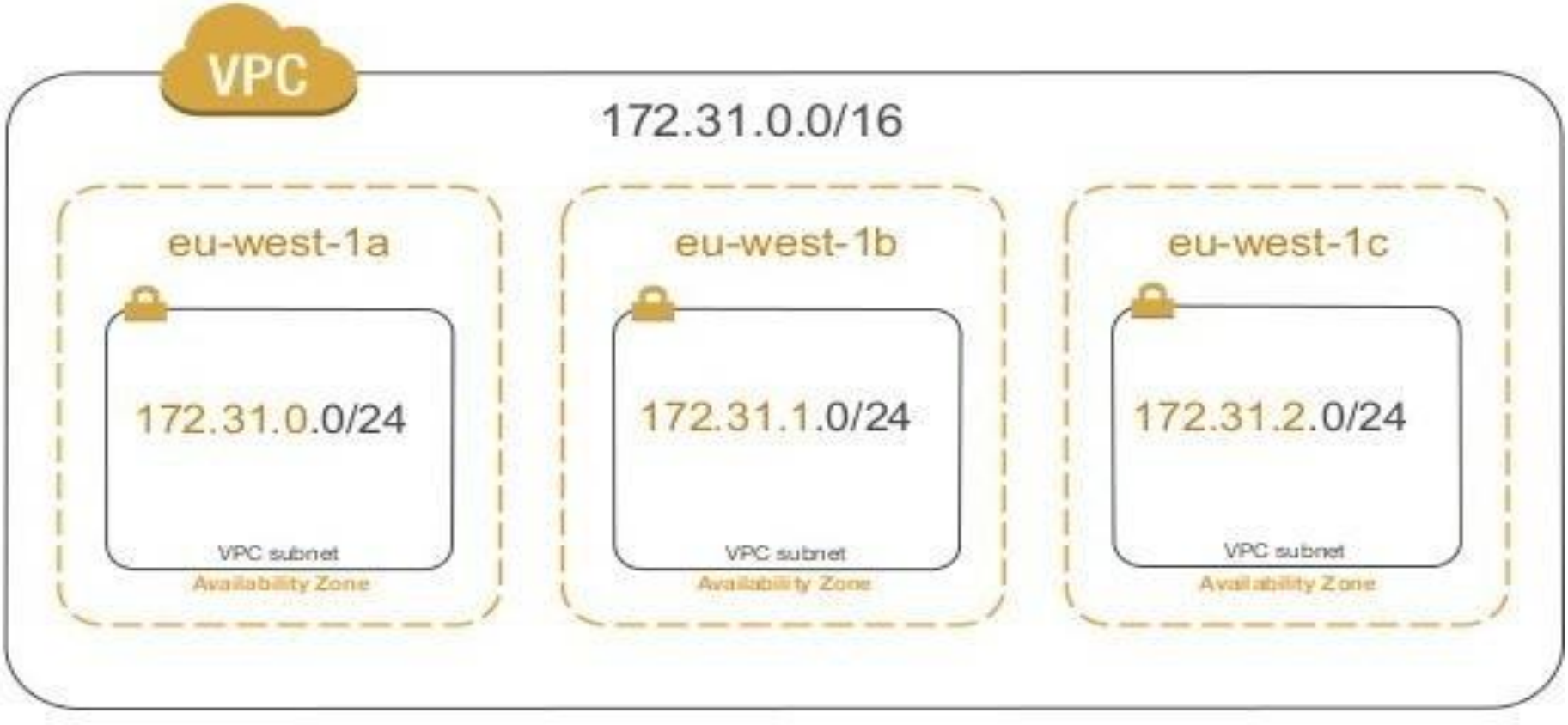
VPC

- NACL
- NAT Gateway
- VPC Peering
- VPC Endpoint
- VPC Flow Logs
- Bastion Host
- VPN and Direct Connect

Goal : Understand this Diagram



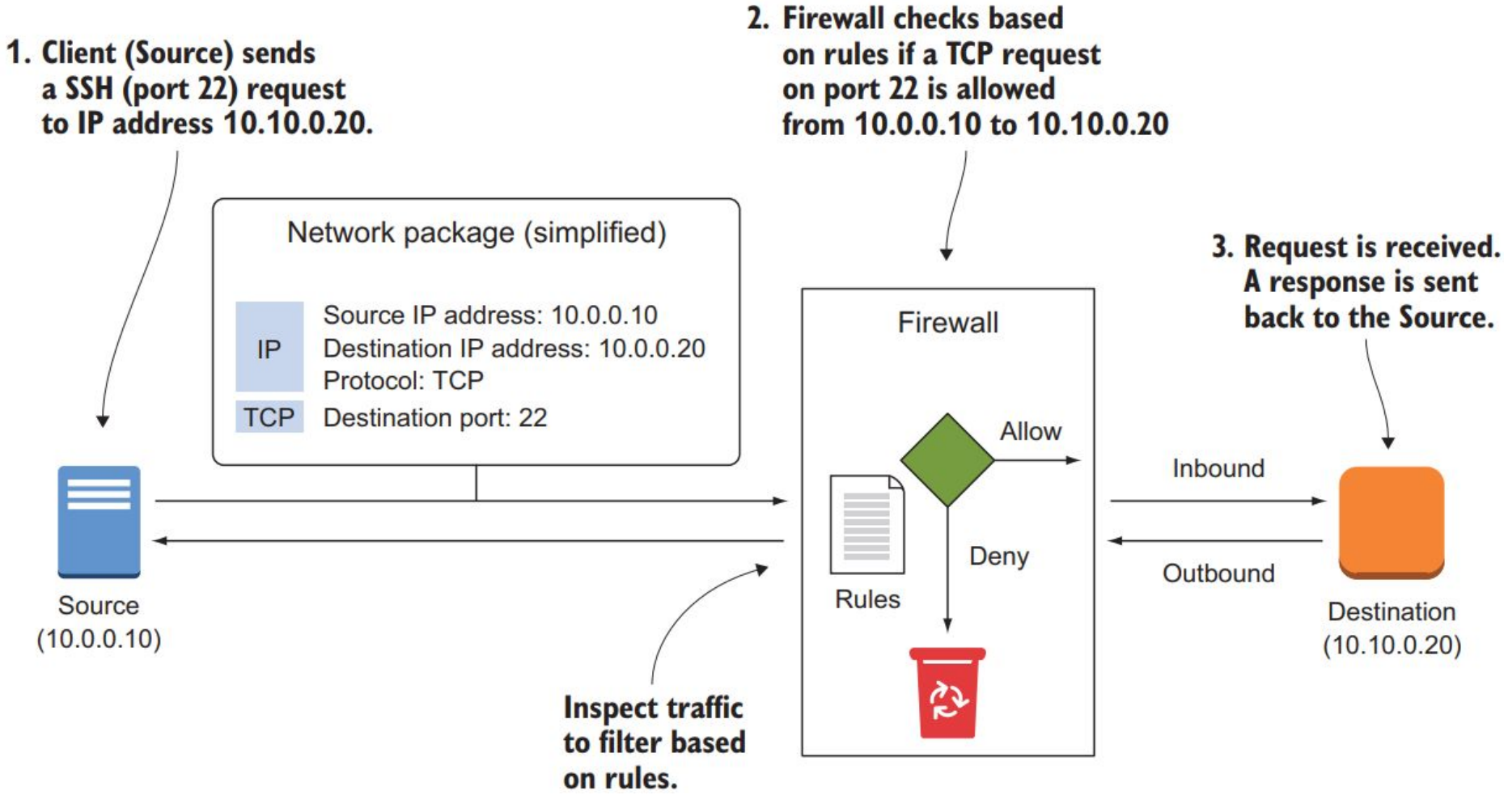
VPC Subnet and AZ



Topics Covered…

- IP Address
- IPv4 and IPv6
- IP address Classes
- Public IP
- Private IP
- CIDR
- Default VPC in AWS
- Subnets
- Internet Gateway

SSH request - From Source to Destination



Internet Gateway

- Internet gateways(IG)helps our VPC instances connect with the internet.
- One VPC can only be attached to one IGW and vice versa.
- Internet Gateways on their own do not allow internet access…
- For this , Route tables must also be edited!

Public Subnet & Private Subnet

Public subnet

- If a subnet’s default traffic is routed to an internet gateway, the subnet is known as a public subnet. For example, an instance launched in this subnet is publicly accessible if it has an Elastic IP address or a public IP address associated with it.

Private subnet

- If a subnet's default traffic is routed to a NAT instance/gateway or completely lacks a default route, the subnet is known as a private subnet. For example, an instance launched in this subnet is not publicly accessible even if it has an Elastic IP address or a public IP address associated with it.

Bastion Host

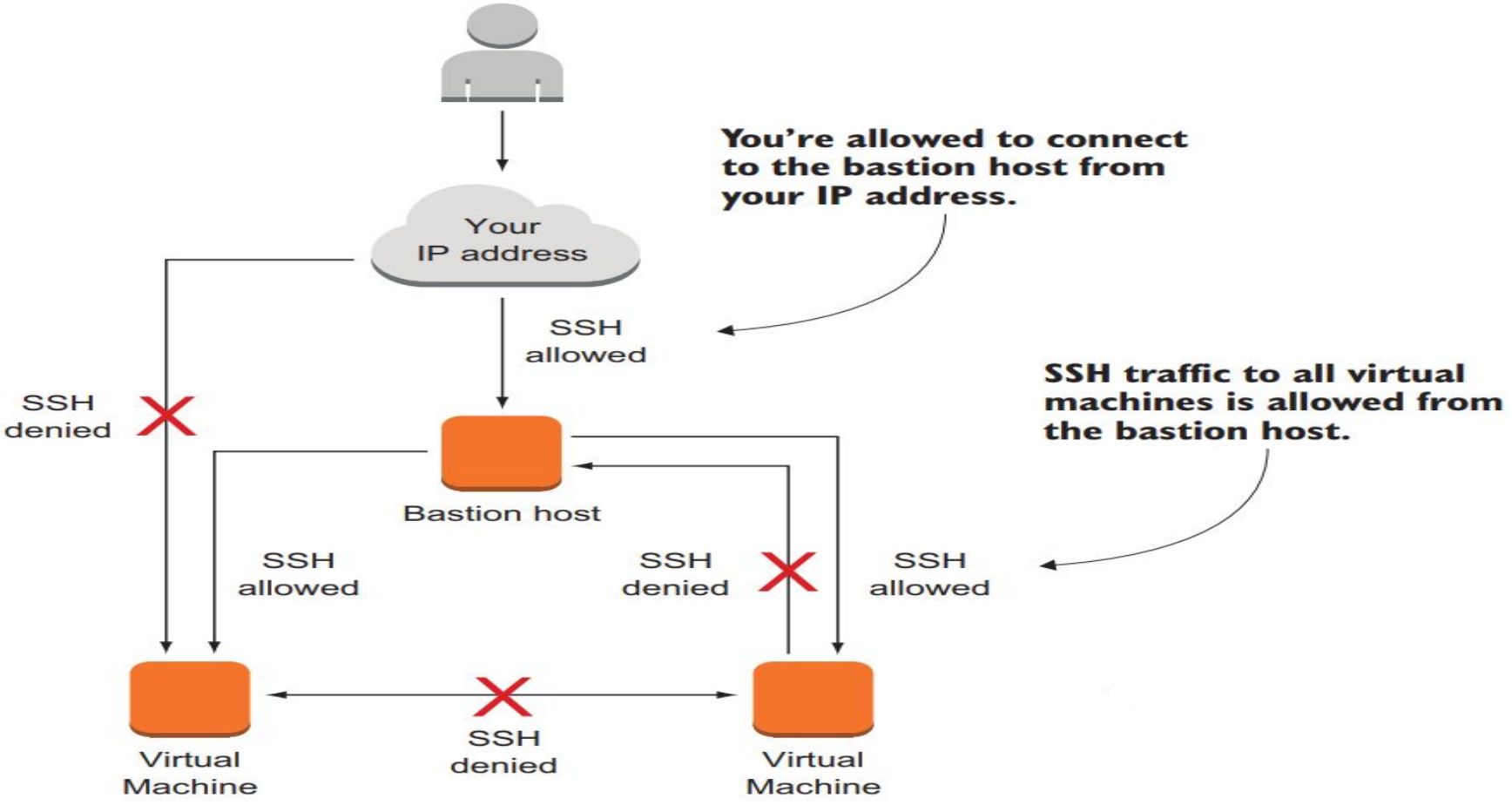
- Only one virtual machine, the bastion host, can be accessed via SSH from the internet (it should be restricted to a specific source IP address).
- All other virtual machines can only be reached via SSH from the bastion host.
- The bastion is in the public subnet which is then can be used to connect instances in other private subnets.
- Bastion Host security group must be restrictive.

Bastion Host

- You have only one entry point into your system, and that entry point does nothing but SSH.

- Bastion Host security group must be restrictive.

Bastion Host - Setup



Network ACLs

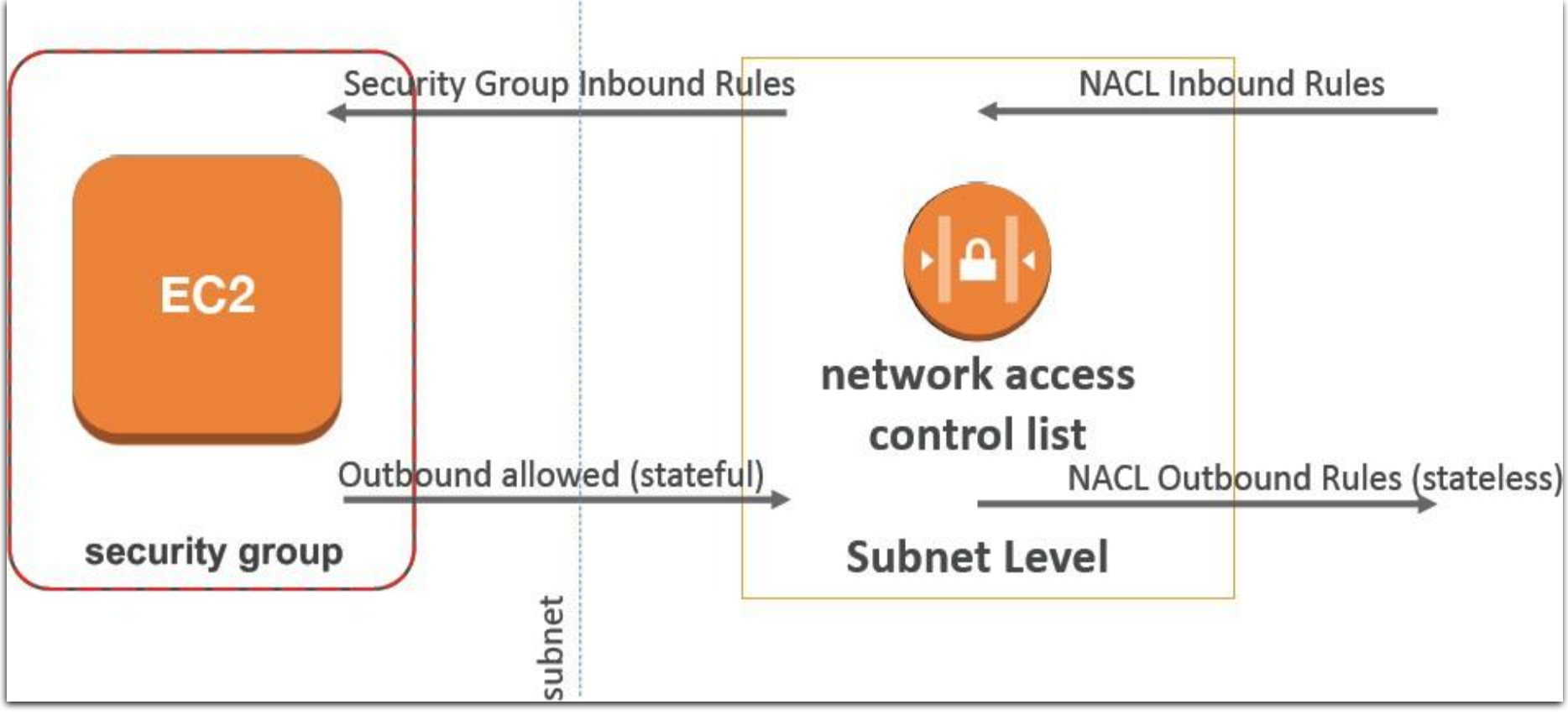
- NACL are like a firewall which control traffic from and to subnet
- Default NACL allows everything outbound and everything inbound
- One NACL per Subnet, new Subnets are assigned the Default
- NACL
- Define NACL rules:

- *Rules have a number (1-32766) and higher precedence with a lower number*
- *E.g. If you define #100 ALLOW <IP> and #200 DENY <IP> , IP will be allowed*
- *Last rule is an asterisk (*) and denies a request in case of no rule match*

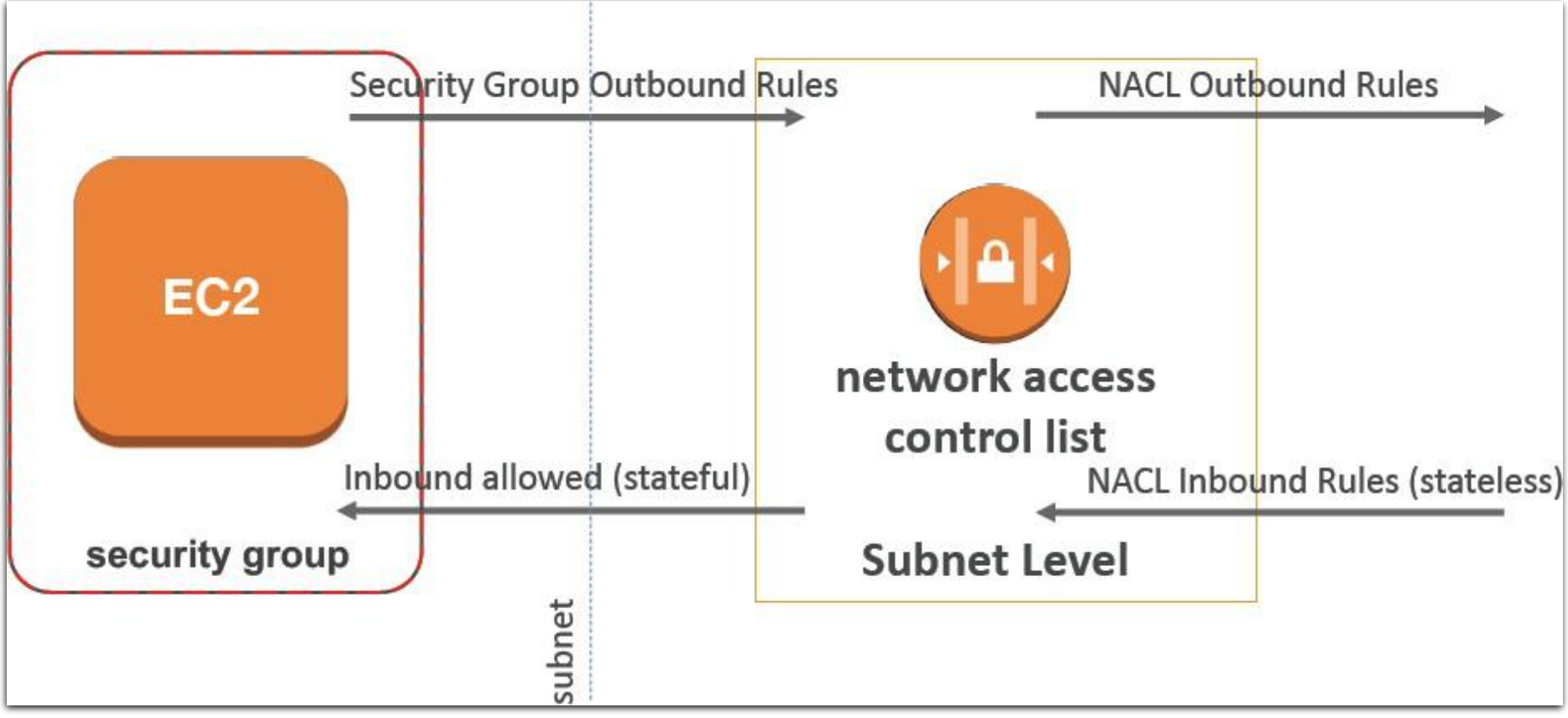
Network ACLs

- AWS recommends adding rules by increment of 100
- Newly created NACL will deny everything
- NACL are a great way of blocking a specific IP at the subnet level

NACLs & Security Group Incoming Request



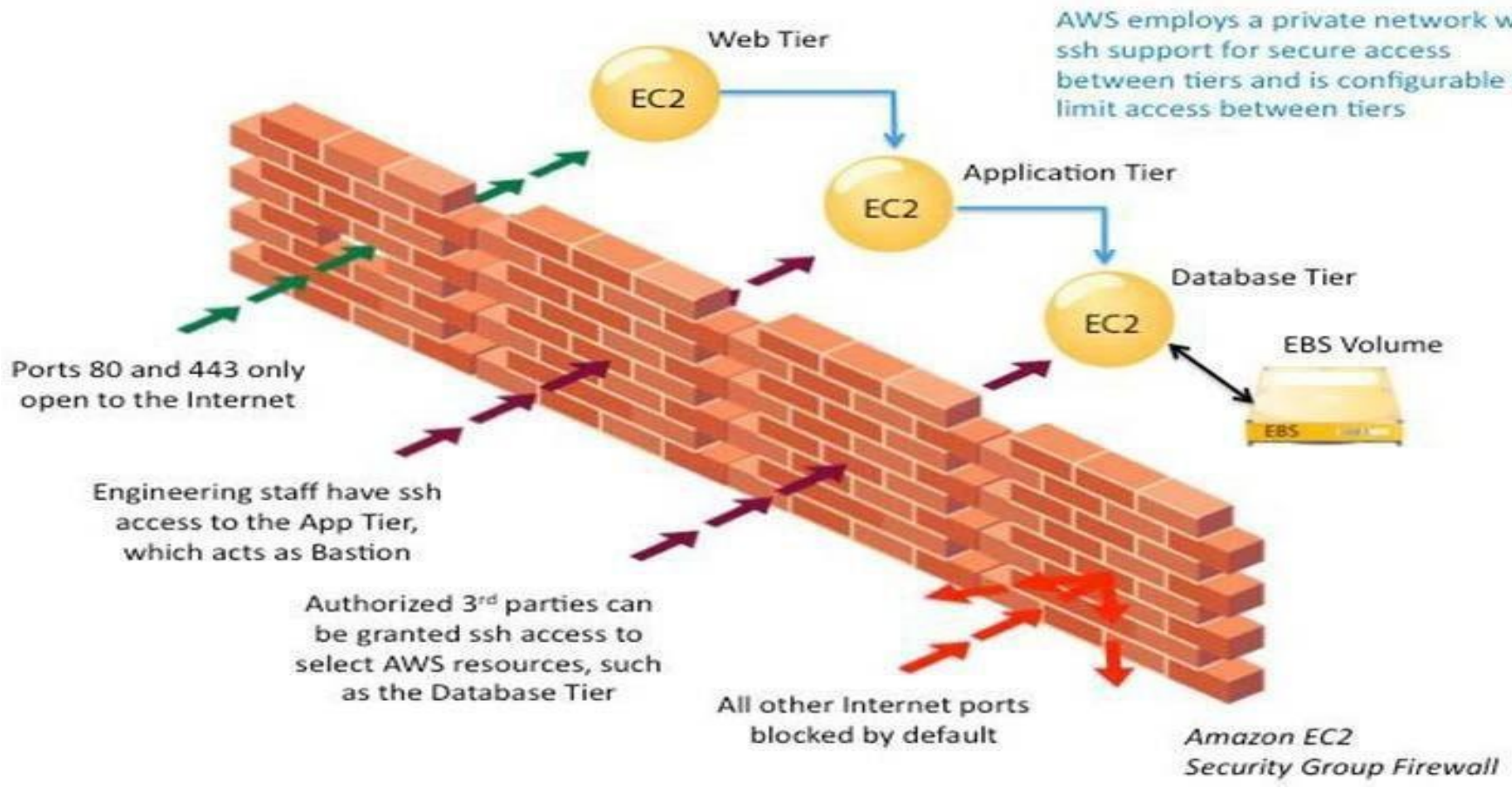
NACL & Security Group
Outgoing Request



Network ACLs v/s Security Group

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)

EC2 Security Group Firewall



NAT Gateway

- NAT stands for Network Address Translation.
- If you want your EC2 instance in a private subnet can access the internet, this can be achieved only when it can communicate to the internet, by still keeping the Subnet Private

VPC Peering

- Connect two VPC, privately using AWS' network.
- Must not have overlapping CIDR.
- VPC Peering connection is not transitive.
- You can do VPC peering with another AWS account.
- Update route tables in each VPC's subnets to make sure instances can communicate with each other.

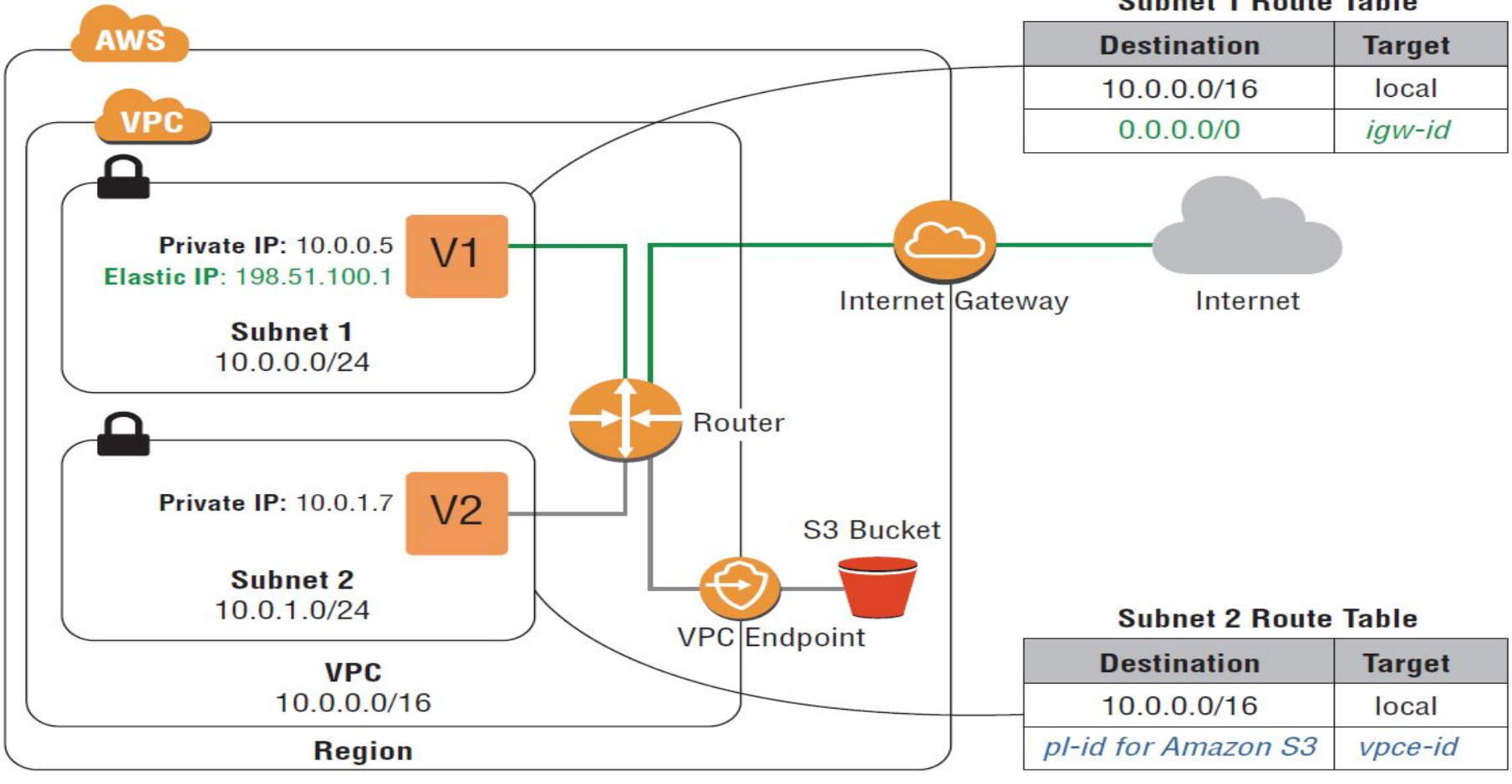
VPC Endpoint

- Endpoints allow you to connect to AWS Services using a private network instead of the public www network
- They redundant and scale horizontally.
- No need of IGW, NAT, etc.. to access AWS Services.

  Gateway: provisions a target and must be used in a route table – S3 and DynamoDB

  Interface: provisions an ENI (private IP address) as an entry point (must attach security group) – most AWS services

VPC Endpoint - S3



Subnet 1 Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Subnet 2 Route Table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	*vpce-id*

VPC Flow Logs

Capture information about IP traffic going into your interfaces:

- VPC Flow Logs
- Subnet Flow Logs
- Elastic Network Interface Flow Logs
- Helps to monitor & troubleshoot connectivity issues
- Flow logs data can go to S3 / CloudWatch Logs

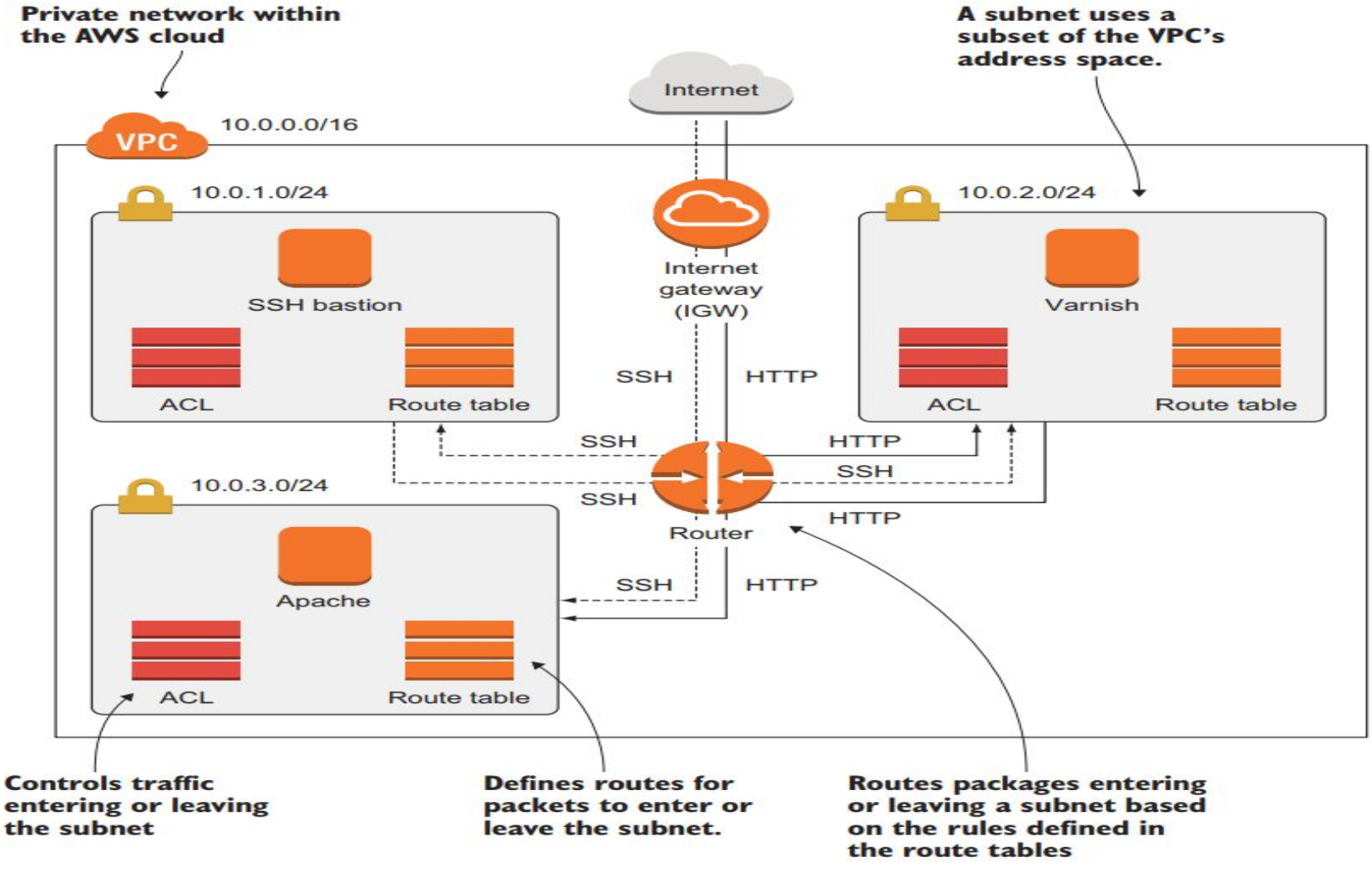
Flow Logs – How do they Look

- ***<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <logstatus>***

- *<srcaddr>, <dstaddr>* => to identify problematic IP
- *<srcport> <dstport>* => to help identity problematic ports
- *Action* : success or failure of the request due to Security Group or NACL

- *Used for analytics on usage patterns, or malicious behavior*
- Query VPC flow logs using Athena on S3 or CloudWatch Logs Insights.

VPC Subnets Setup for secure Web Application



VPN

- You can optionally connect your VPC to your own corporate data center using an IPsec AWS Site-to-Site VPN connection, making the AWS Cloud an extension of your data center.
- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network.

- How to enable the access to your remote network from your VPC :

❑ By attaching a virtual private gateway to the VPC

❑ Creating a custom route table, updating your security group rules

❑ Creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection

- VPN connection: A secure connection between your on- premises equipment and your VPCs.

- VPN tunnel: An encrypted link where data can pass from the customer network to or from AWS.

- Customer gateway: An AWS resource which provides information to AWS about your customer gateway device.

- Customer gateway device: A physical device or software application on your side of the Site-to-Site VPN connection

Direct Connect

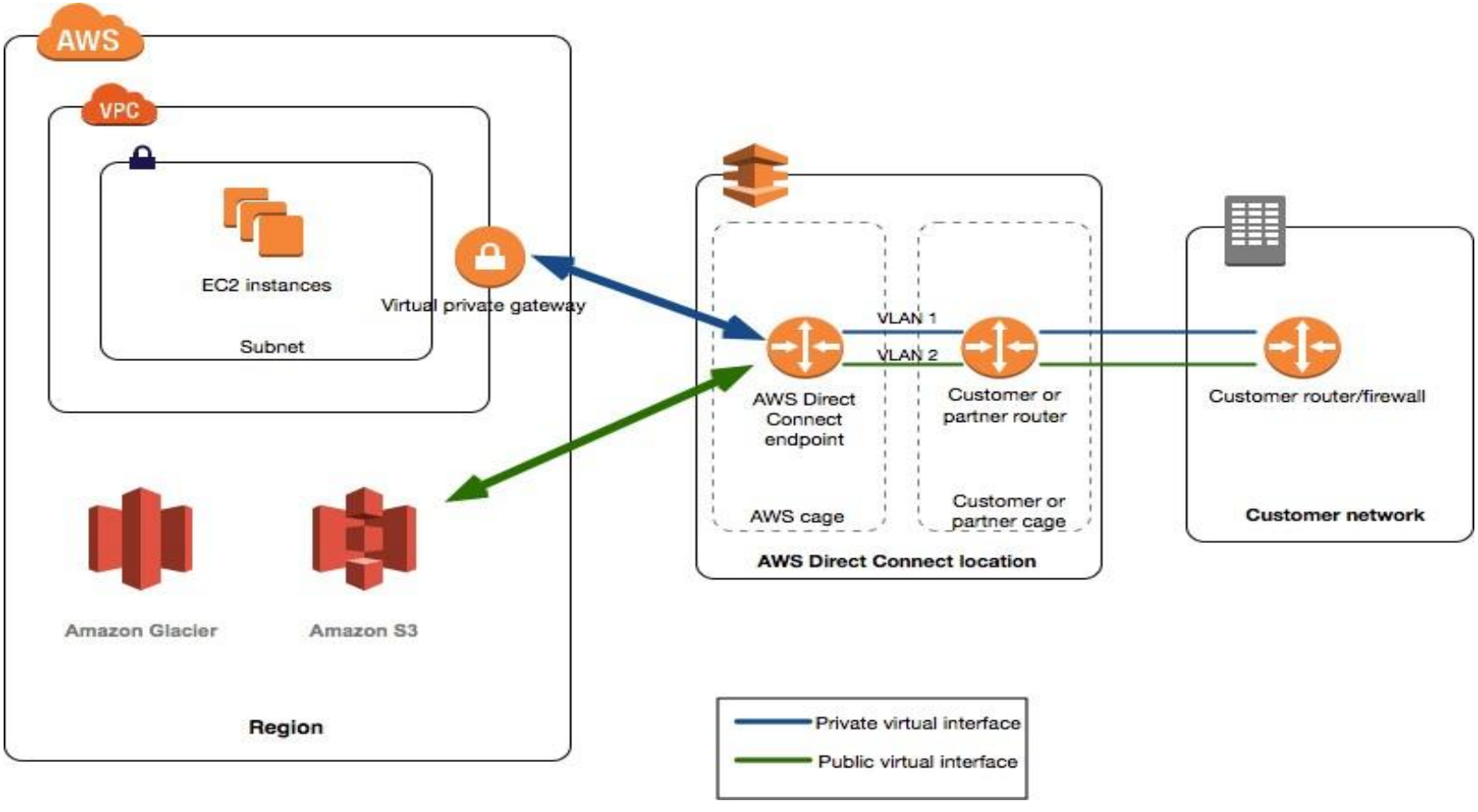
- Provides a dedicated private connection from a remote network to your VPC
- Dedicated connection must be setup between your DC and AWS Direct Connect locations
- You need to setup a Virtual Private Gateway on your VPC
- Access public resources (S3) and private (EC2) on same connection
- Use Cases:

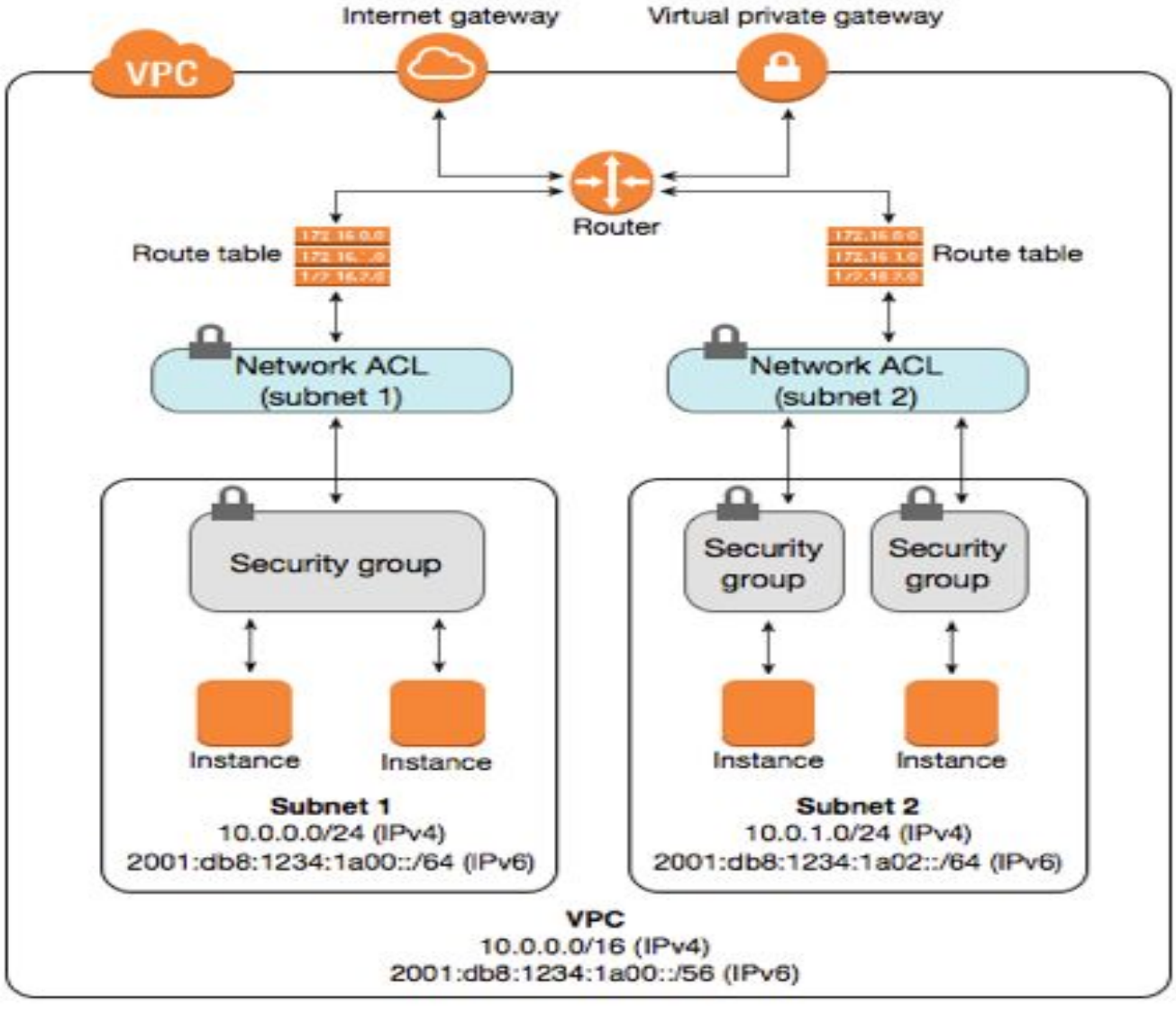
❑ Increase bandwidth throughput - working with large data sets – lower cost

❑ More consistent network experience - applications using real-time data feeds

❑ Hybrid Environments (on prem + cloud)

Direct Connect




Internet gateway
Virtual private gateway
VPC
Router
Route table
Route table
Network ACL
(subnet 1)
Network ACL
(subnet 2)
Security group
Security group
Security group
Instance
Instance
Instance
Instance
Subnet 1
10.0.0.0/24 (IPv4)
2001:db8:1234:1a00::/64 (IPv6)
Subnet 2
10.0.1.0/24 (IPv4)
2001:db8:1234:1a02::/64 (IPv6)
VPC
10.0.0.0/16 (IPv4)
2001:db8:1234:1a00::/56 (IPv6)

VPC Summary

- AWS is a shared-responsibility environment in which security can be achieved only if you and AWS work together. You're responsible for securely configuring your AWS resources and your software running on EC2 instances, while AWS protects buildings and host systems.
- Traffic to or from AWS resources like EC2 instances can be filtered based on protocol, port, and source or destination.
- A bastion host is a well-defined single point of access to your system. It can be used to secure SSH access to your virtual machines. Implementation can be done with security groups.
- A VPC is a private network in AWS where you have full control. With VPCs, you can control routing, subnets, ACLs, and gateways to the internet or your company network via VPN.
- A NAT gateway enables access to the internet from private subnets. You should separate concerns in your network to reduce potential damage if, for example, one of your subnets is hacked.
- Keep every system in a private subnet that doesn't need to be accessed from the public internet, to reduce your attackable surface.

Linux Networking Commands

- **ifconfig –a**
- to check the IP address assigned to the system
- **traceroute google.com**
- print the route packets take to network host.
- **dig google.com**
- dig (Domain Information Groper) is a flexible tool for interrogating DNS name servers.
- **telnet google.com 443**
- telnet connect destination host:port via a telnet protocol if connection establishes means connectivity between two hosts is working fine.

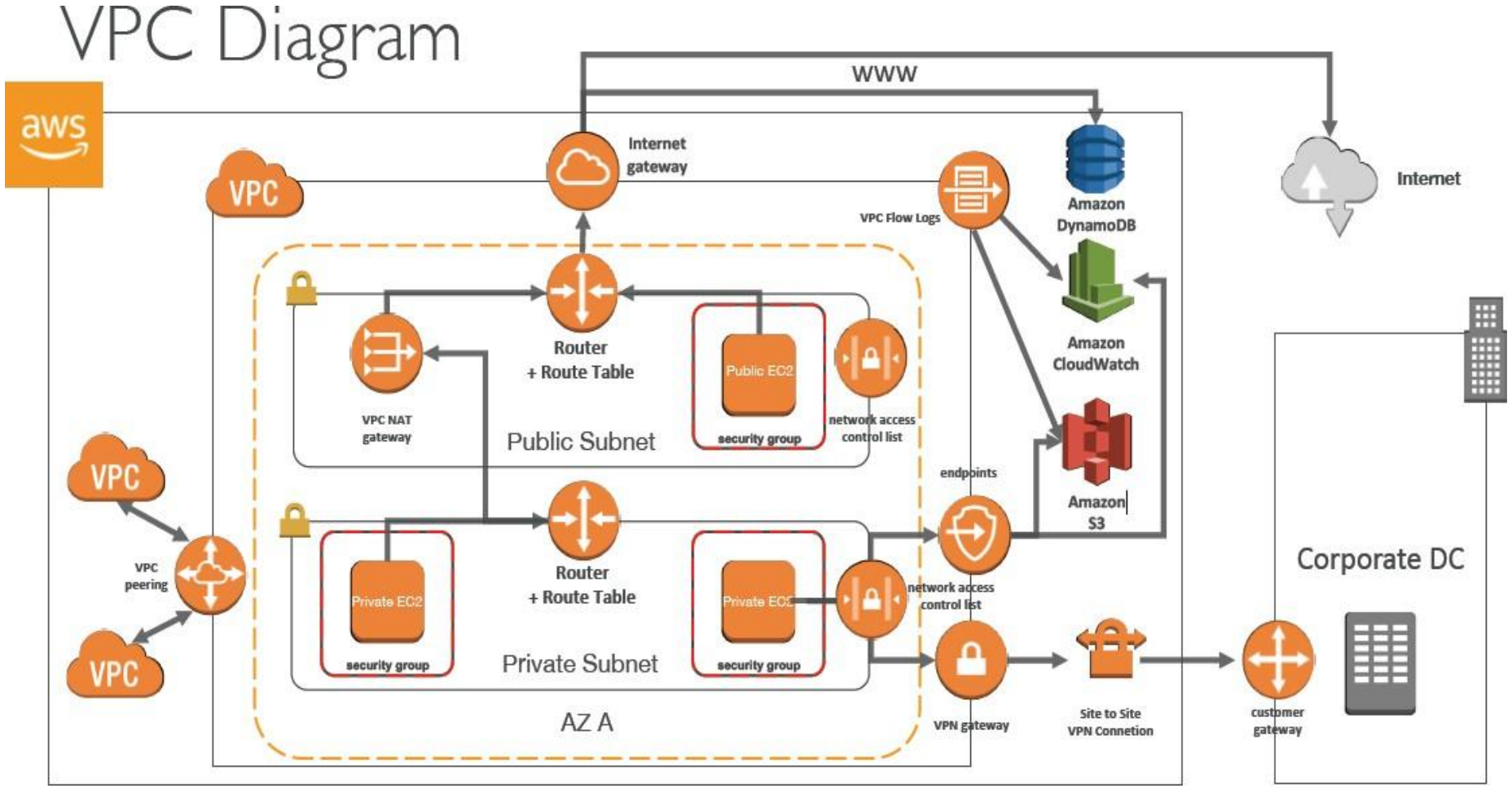
Linux Networking Commands

- **nslookup google.com**
- nslookup is a program to query Internet domain name servers.

- **nmap google.com**
- nmap is a one of the powerful commands, it checks the opened ports on the server.
- **Netstat**
  netstat -nltp
- allows you a simple way to review each of your network connections and open sockets.

- **scp**
  scp $filename user@targethost:/$path
  scp allows you to secure copy files to and from another host in the network.

Understanding Level?



Pricing components

Elastic ip : https://aws.amazon.com/ec2/pricing/on-demand/
Nat Gateway : https://aws.amazon.com/vpc/pricing/
VPC interface endpoint : https://aws.amazon.com/privatelink/pricing/

ANY Questions?