AWS Solutions Architect Associate

Session 401

Networking &CDN: VPC

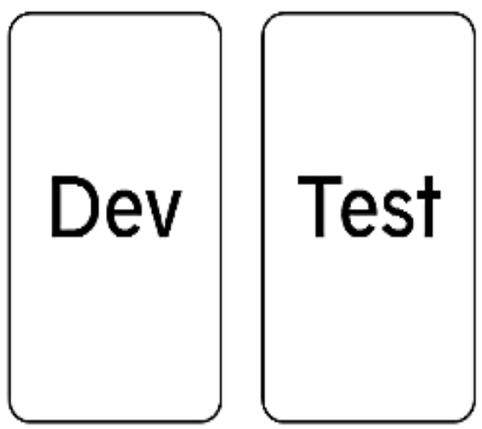
July/2024

Virtual Private Cloud - VPC

- (..) enables you to **launch AWS resources into a virtual network that you've defined**.

- This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Your private network space in the AWS Cloud



Provides logical isolation for your workloads

Allows custom access controls and security settings for your resources

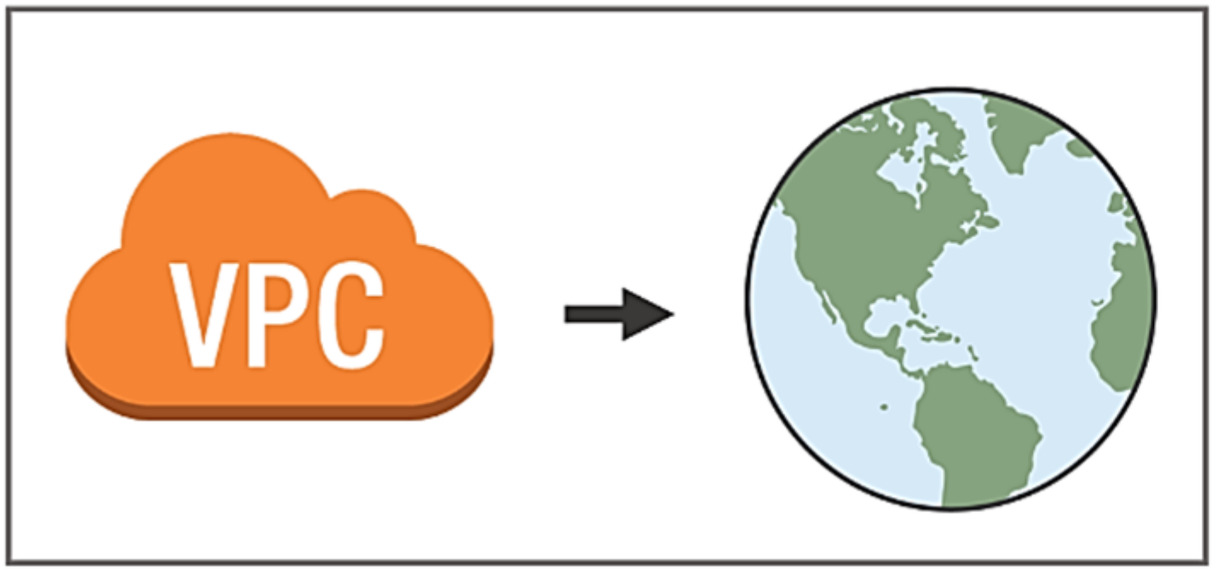
Amazon VPC

A VPC is a virtual network dedicated to your AWS account

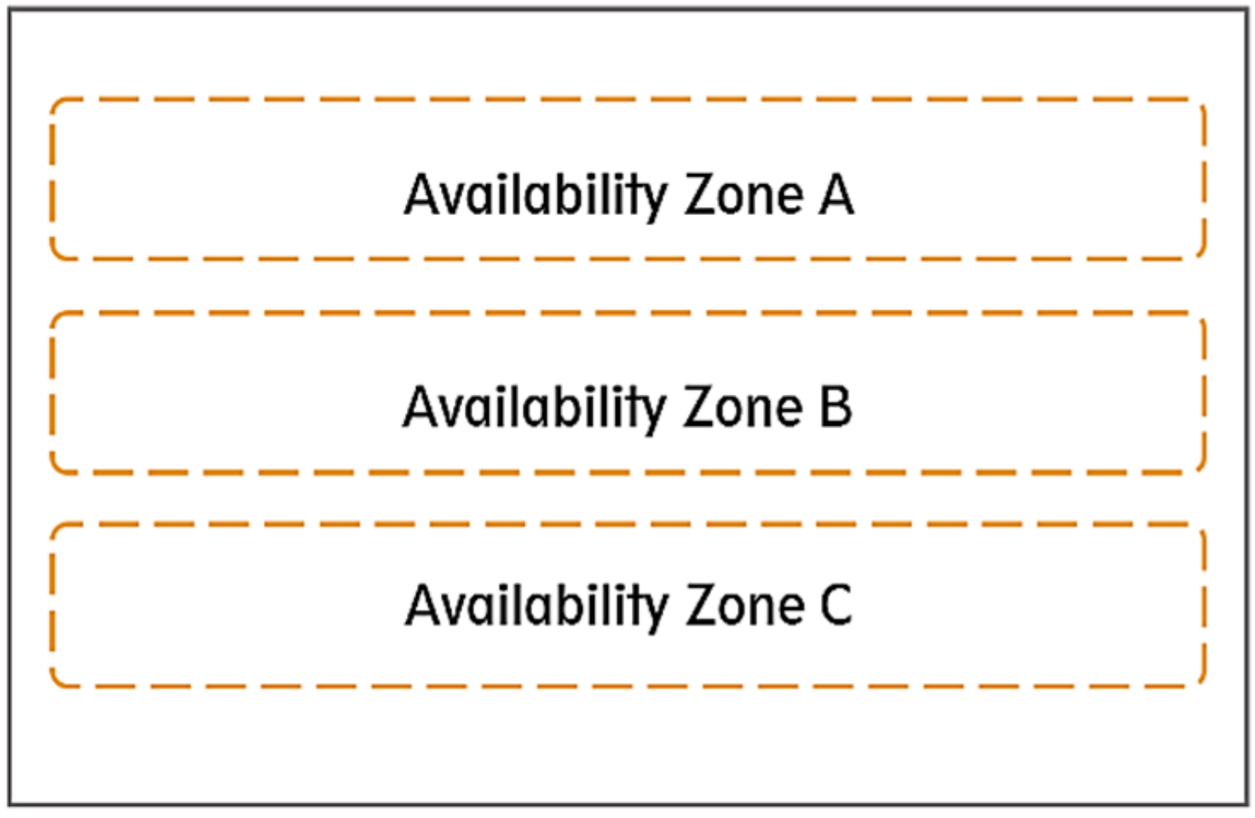
Exists either in the IPv4 or IPv6 address ranges

Enables you to create specific CIDR ranges for your resources to occupy

Provides strict access rules for inbound and outbound traffic.



VPCs deploy into **1** of the **24** AWS Regions



A VPC can host resources from **any** Availability Zone within its region

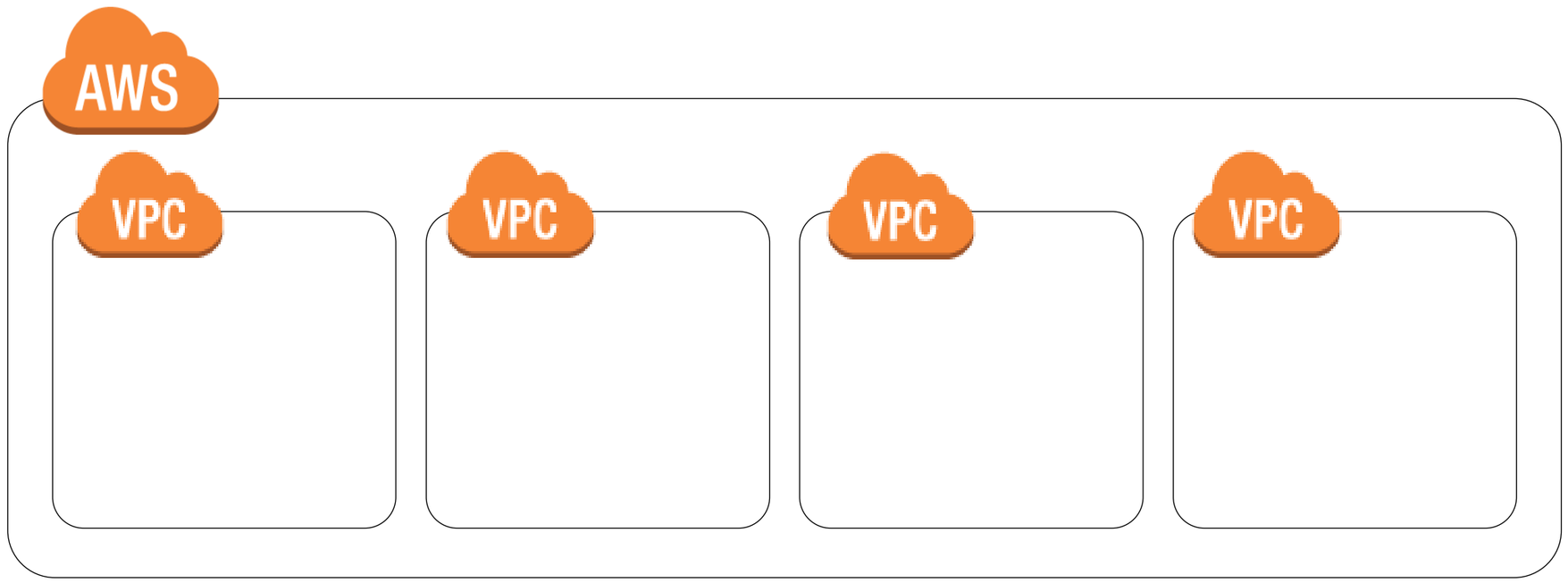
Multi- VPC

Best suited for:

- Single team or single organizations, such as managed service providers
- Limited teams, which makes it easier to maintain standards and manage access

Exception:

- Governance and compliance standards may require greater workload isolation regardless of organizational complexity.



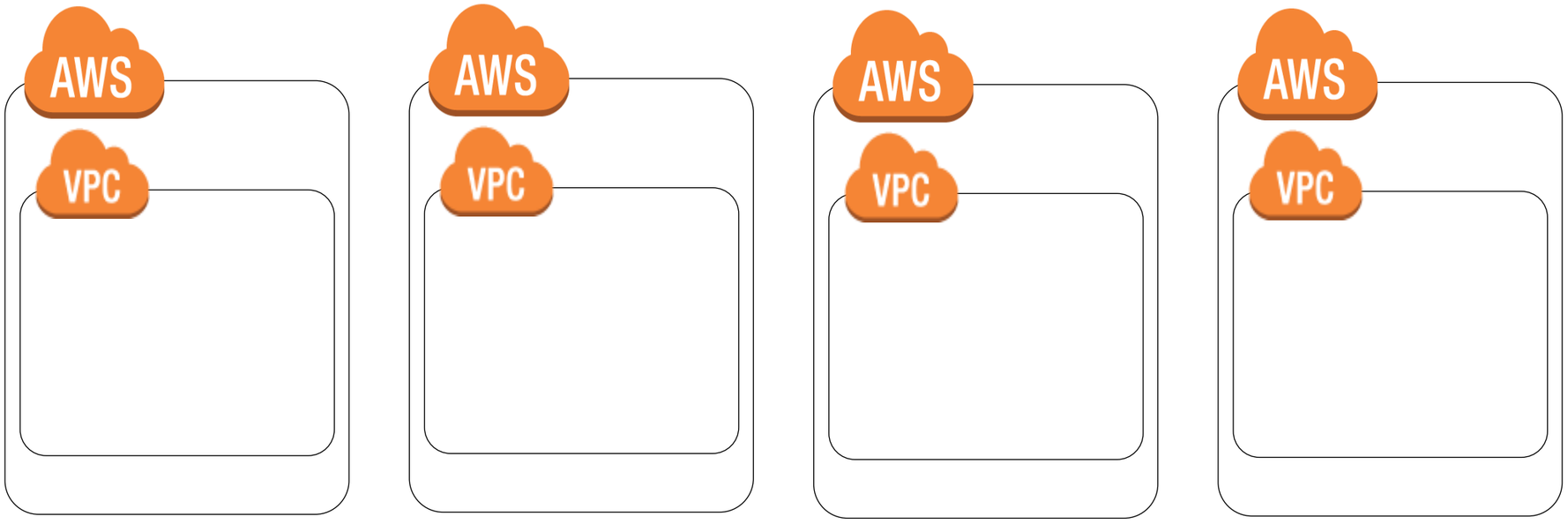
Multi- Account

Best suited for:

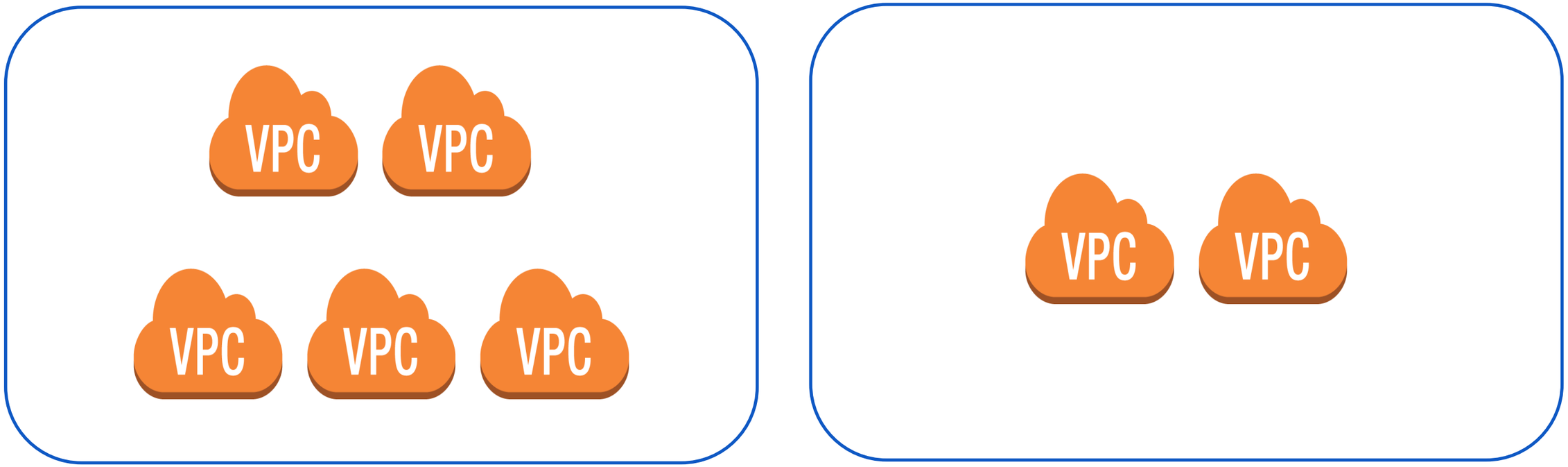
- Large organizations and organizations with multiple IT teams
- Medium-sized organizations that anticipate rapid growth

Why?

- Managing access and standards can be more challenging in more complex organizations.



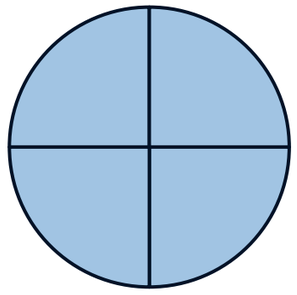
You can have multiple VPCs in the same region or in different regions



Service Limit: 5 VPCs per region per account

More info at https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html and https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html (18/07/2024)

Subnet - VPC



- Subnets are a subset of the VPC CIDR block
- Subnet CIDR blocks cannot overlap
- Each subnet resides entirely within one Availability Zone
- An Availability Zone can contain multiple subnets

Service Limit: 200 Subnets per VPC

Name	Default	Adjustable	Comments
VPCs per Region	5	Yes	Increasing this quota increases the quota on internet gateways per Region by the same amount. You can increase this limit so that you can have 100s of VPCs per Region.
Subnets per VPC	200	Yes	
IPv4 CIDR blocks per VPC	5	Yes (up to 50)	This primary CIDR block and all secondary CIDR blocks count toward this quota.
IPv6 CIDR blocks per VPC	5	No	

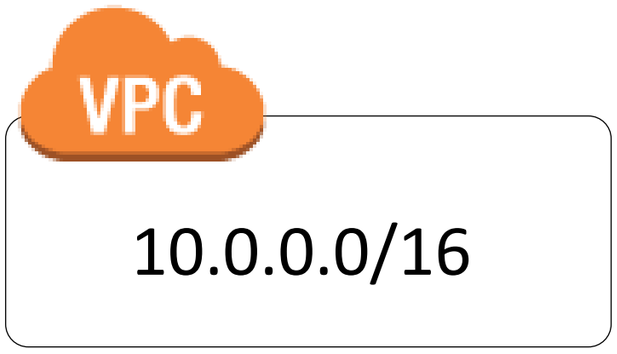
Taken from https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html (18/07/2024)

Route Tables - VPC

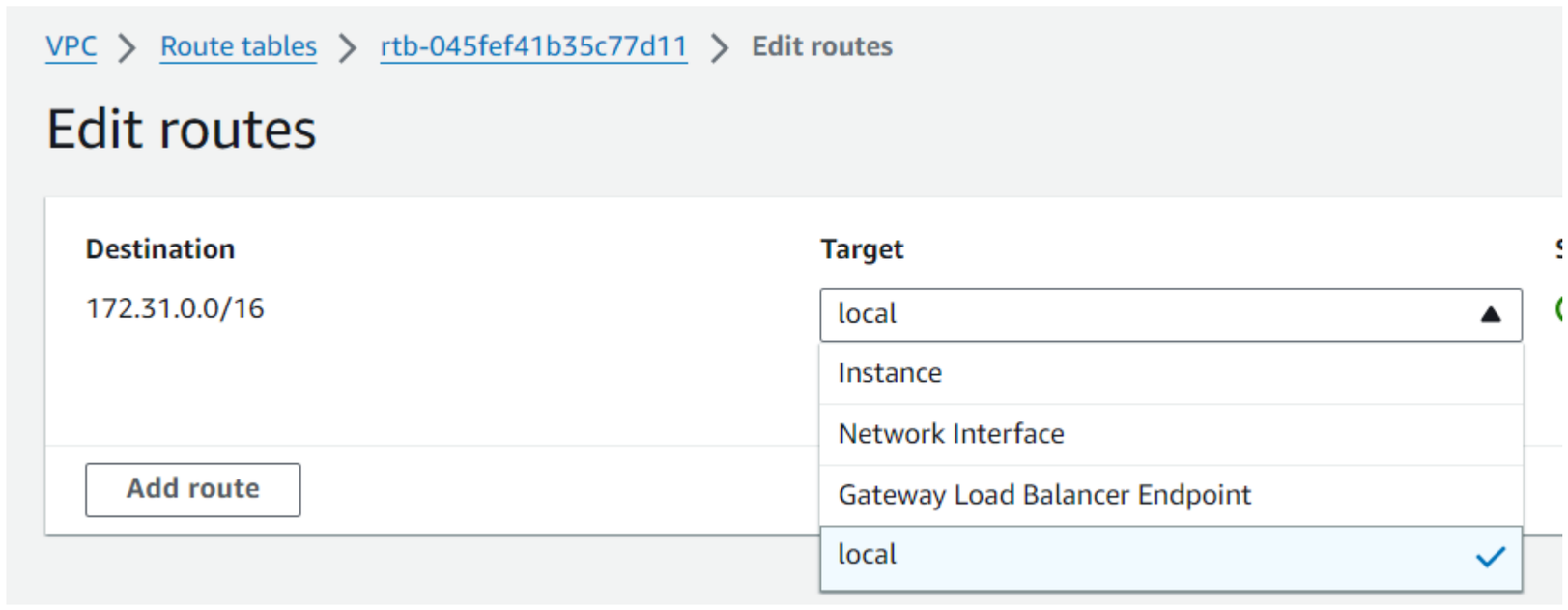
Route tables:

- Required to direct traffic between VPC resources
- Each VPC has a main (default) route table
- You can create custom route tables
- All subnets must have an associated route table

Destination	Target
10.0.0.0/16	local

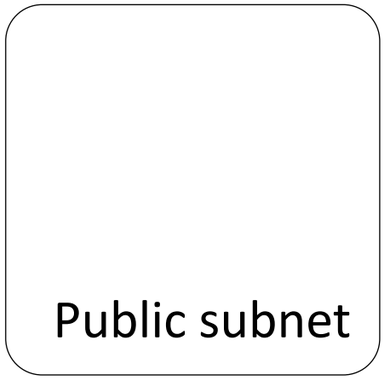


Best practice: Use custom route tables for each subnet



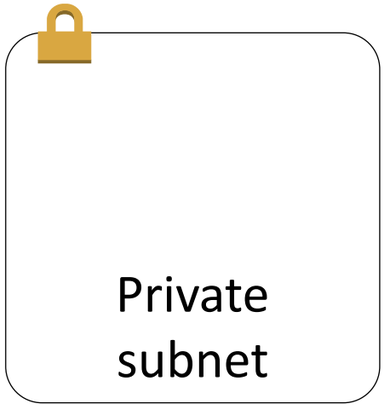
Subnets Isolation - VPC

Use subnets to define internet accessibility.



Public subnets

- Include a routing table entry to an internet gateway to support inbound/outbound access to the public internet



Private subnets

- Do not have a routing table entry to an internet gateway
- Are not directly accessible from the public internet
- Typically use a NAT gateway to support restricted, outbound public internet access

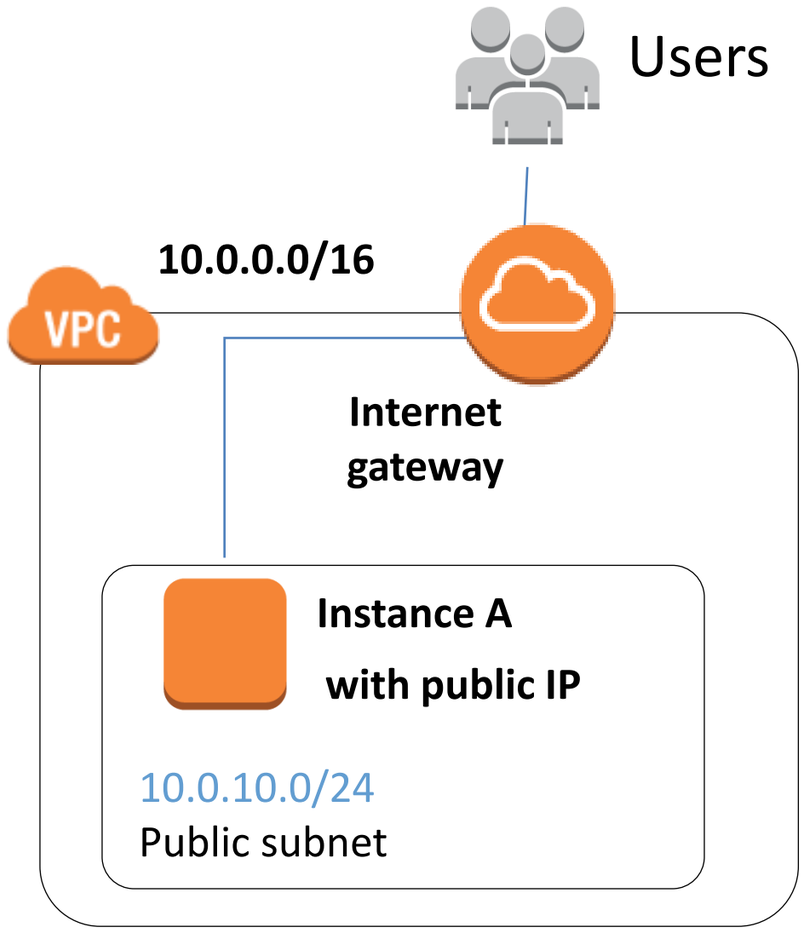
Public Subnets - IGW

Internet Gateways

- Allow communication between instances in your VPC and the internet
- Are horizontally scaled, redundant, and highly available by default
- Provide a target in your subnet route tables for internet-routable traffic

Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>



Private Subnets – NAT Gateway

NAT Gateways

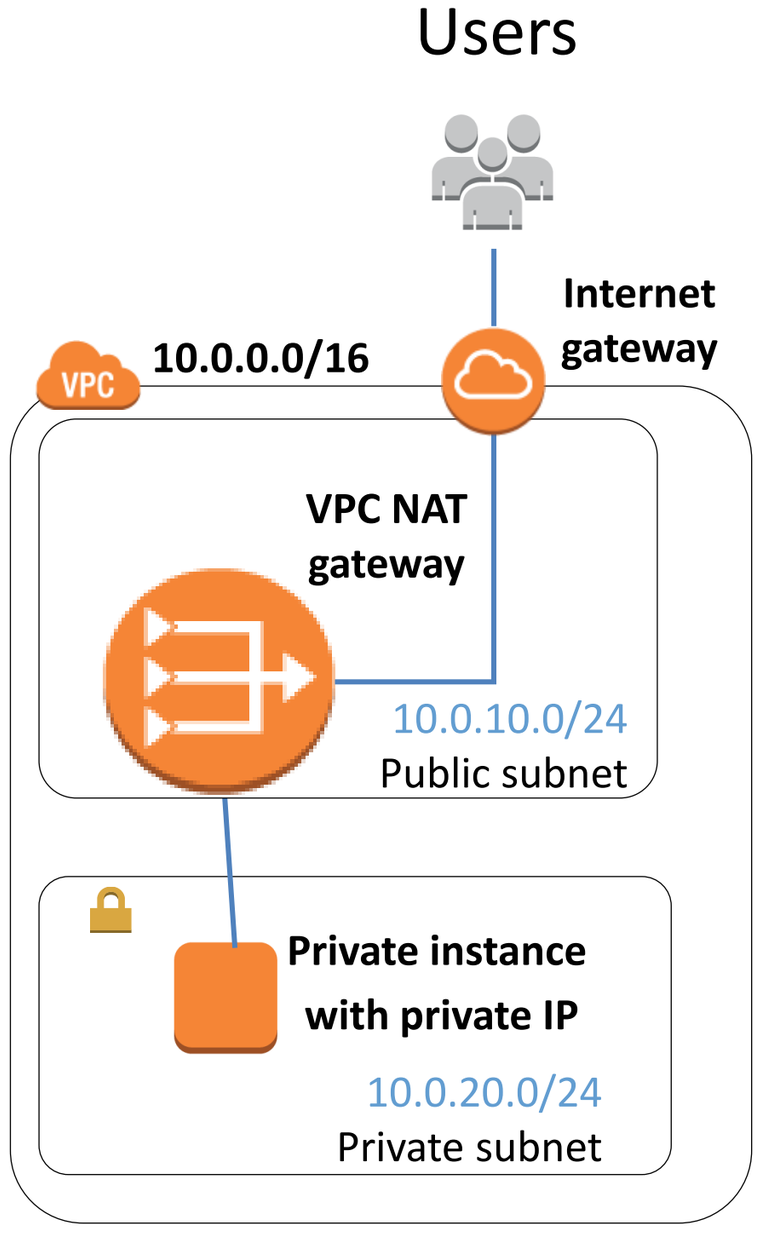
- Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- Prevent private instances from receiving inbound traffic from the internet.

Public route table

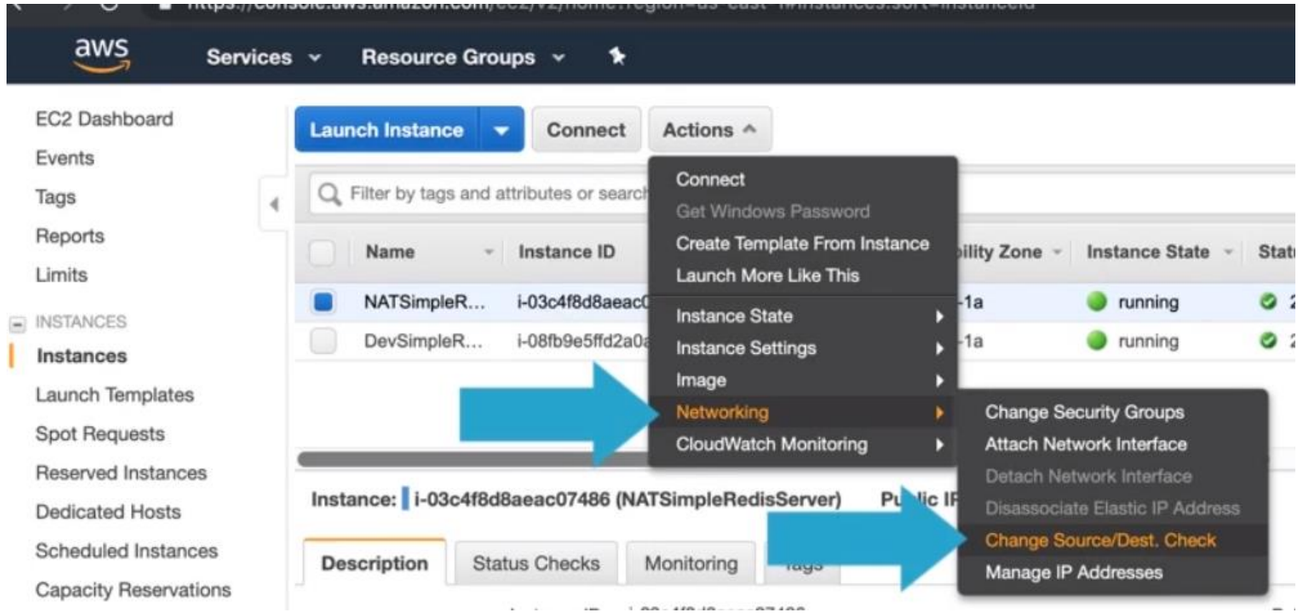
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Private route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



Private Subnets – NAT Instance



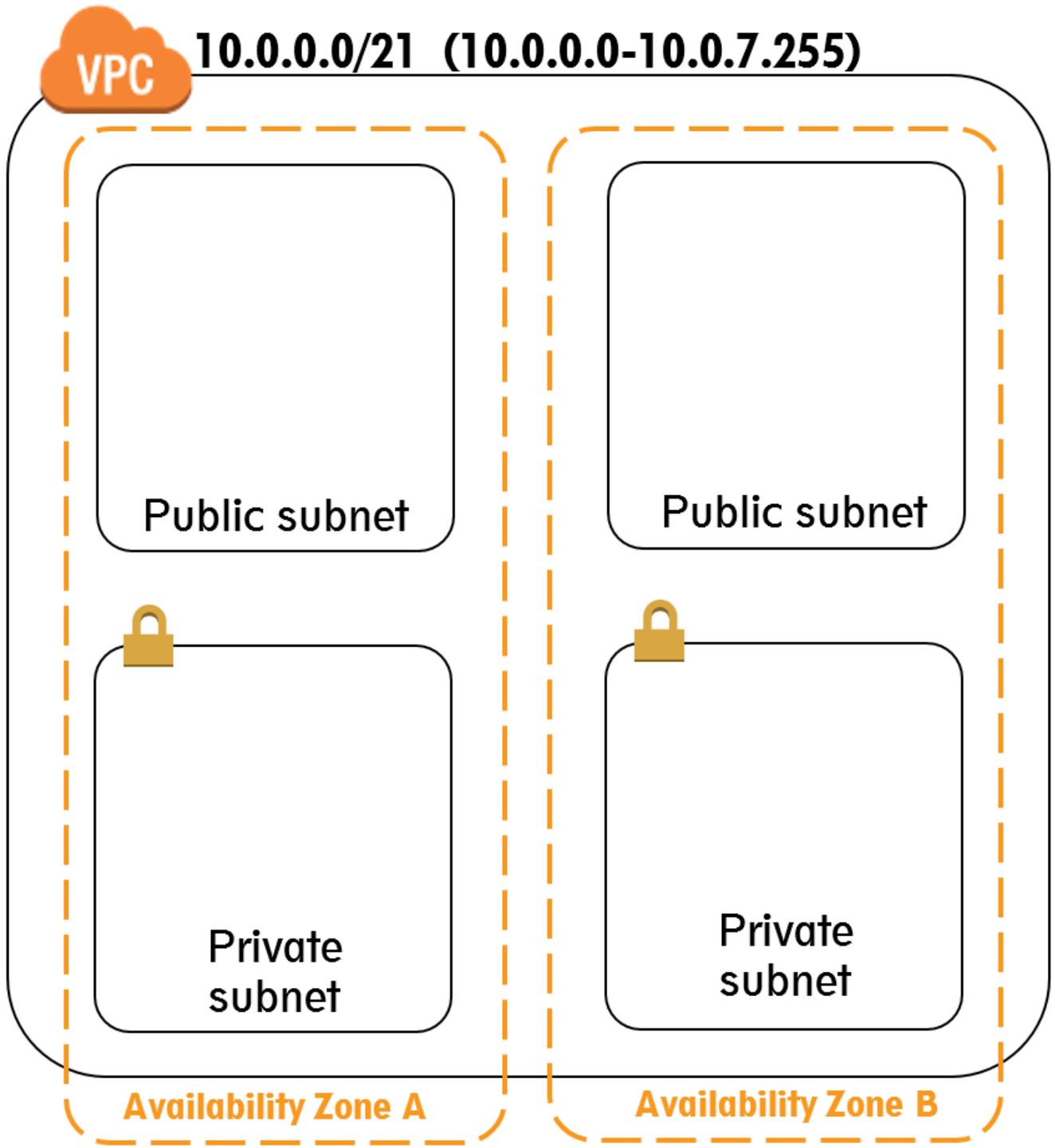
- NAT-Defined AMI: Search by "nat"
- Allow redirect disable Source/Dest Check
- Advantage: You have port-forwarding enter to EC2 instance and use iptables
- Disadvantage:
  - Traffic allowed

```
[ec2-user@ip-10-0-1-12 ~]$ sudo su
[root@ip-10-0-1-12 ec2-user]# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 6379 -j DNAT --to 10.0
.2.227:6379
[root@ip-10-0-1-12 ec2-user]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

Subnet Configuration

If you are unsure of the best way to set up your subnets:

Start with one public and one private subnet per Availability Zone.

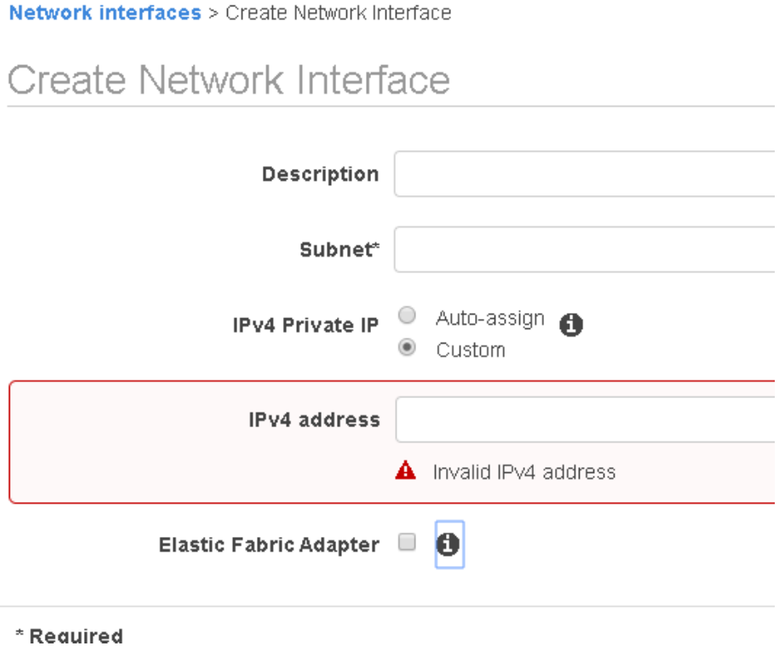


Elastic Network Interface

An elastic network interface is a
virtual network interface
that can be moved across EC2 instances
in the same Availability Zone.

When moved to a new instance, a network interface maintains its:

- Private IP address
- Public IP address
- MAC address



Attributes:
Primary Private IPv4
+ Sec Private IPv4
1 EIP per Private IPv4
1 Public IPv4
1..* IPv6
1..* Sec Groups
1 MAC Address
1 Source/Dest Check Flag
Description

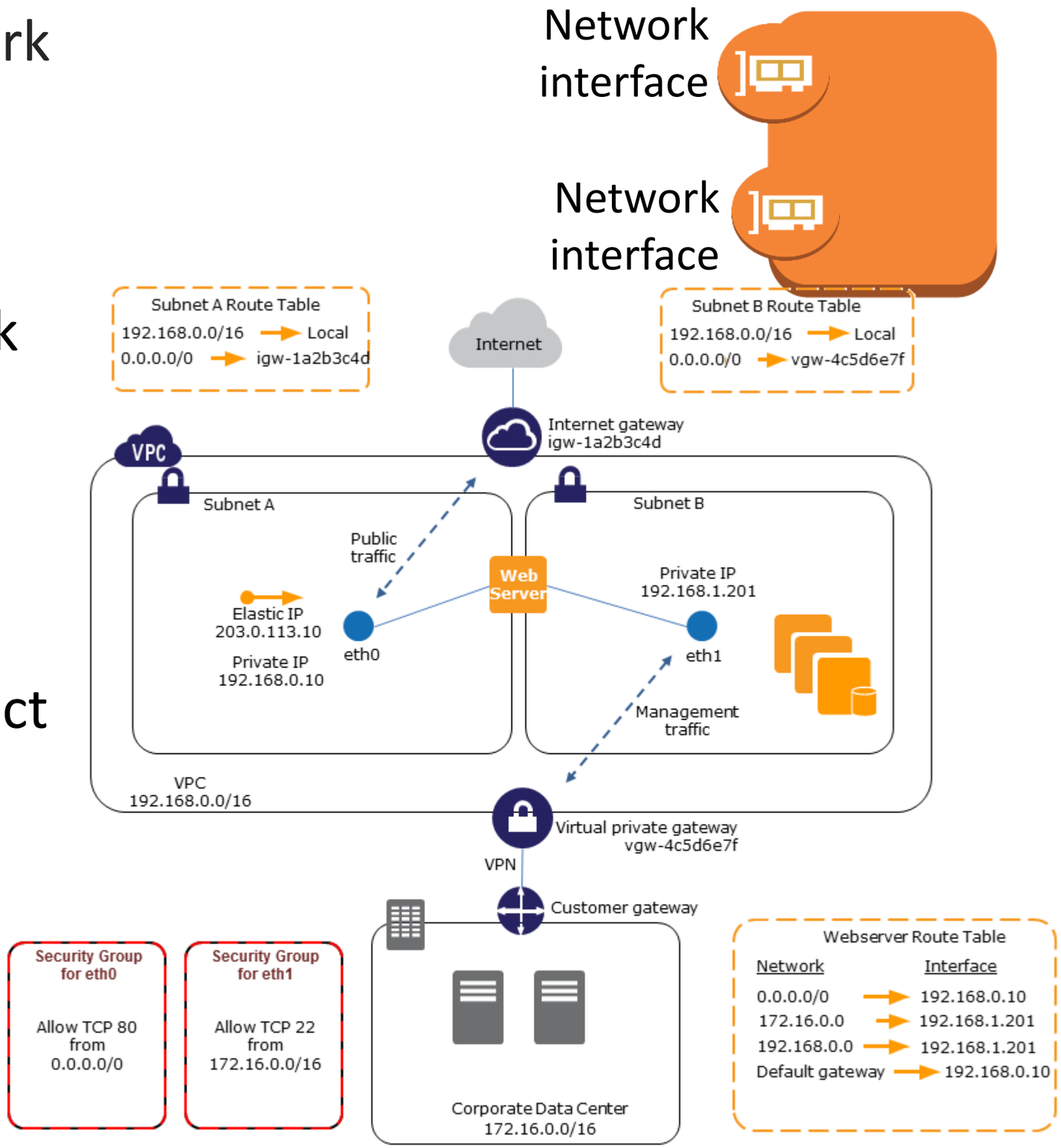
Taken from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html (18/07/2024)

Elastic Network Interface

Why have more than one network interface on an instance?

If you need to:

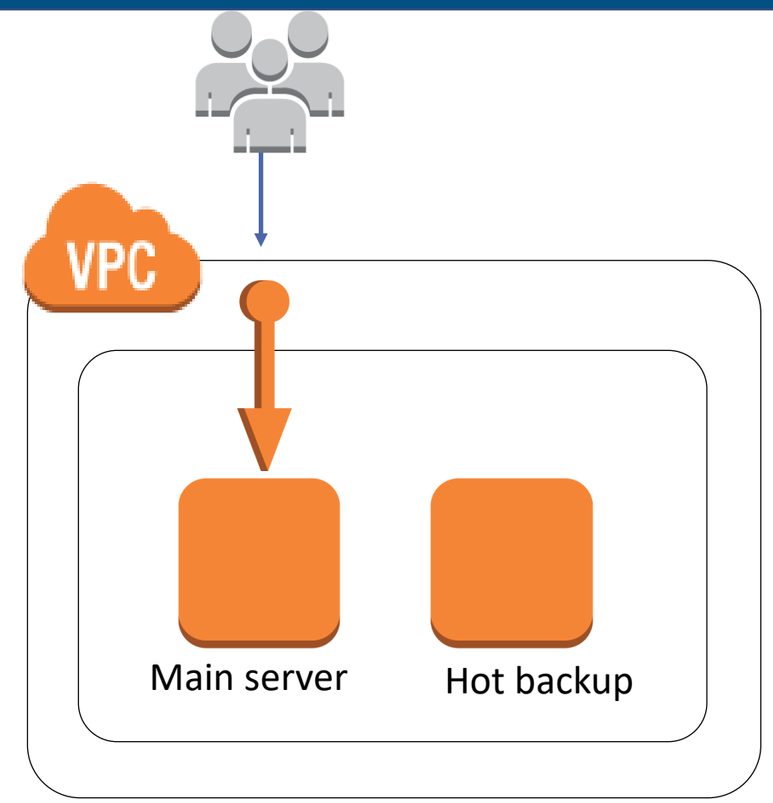
- Create a management network
- Use network and security appliances in your VPC
- Create dual-homed instances with workloads/roles on distinct subnets

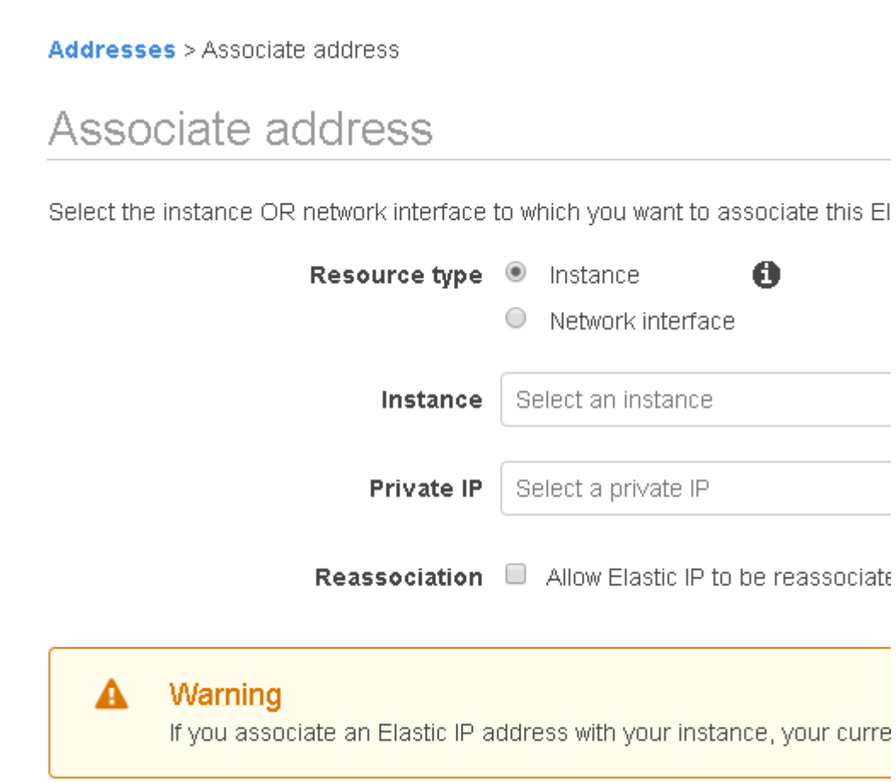


Taken from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html and https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/scenarios-enis.html (18/07/2024)

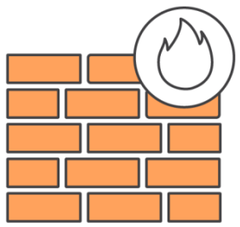
Elastic IP

- Can be associated with an instance or a network interface
- Able to re-associate and direct traffic changed immediately
- **Service Limit:** 5 allowed per AWS Region
- 2 Steps: a) Request an EIP (Amazon or Owned) b) Associate to ENI or Instance

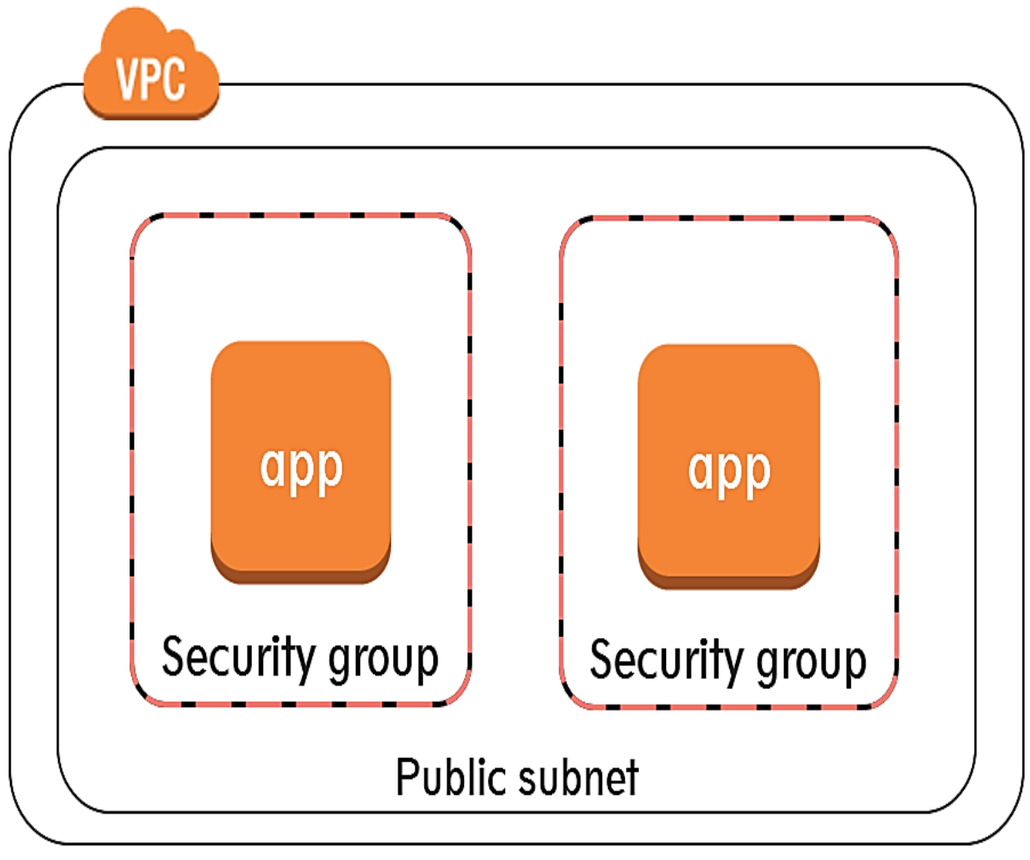




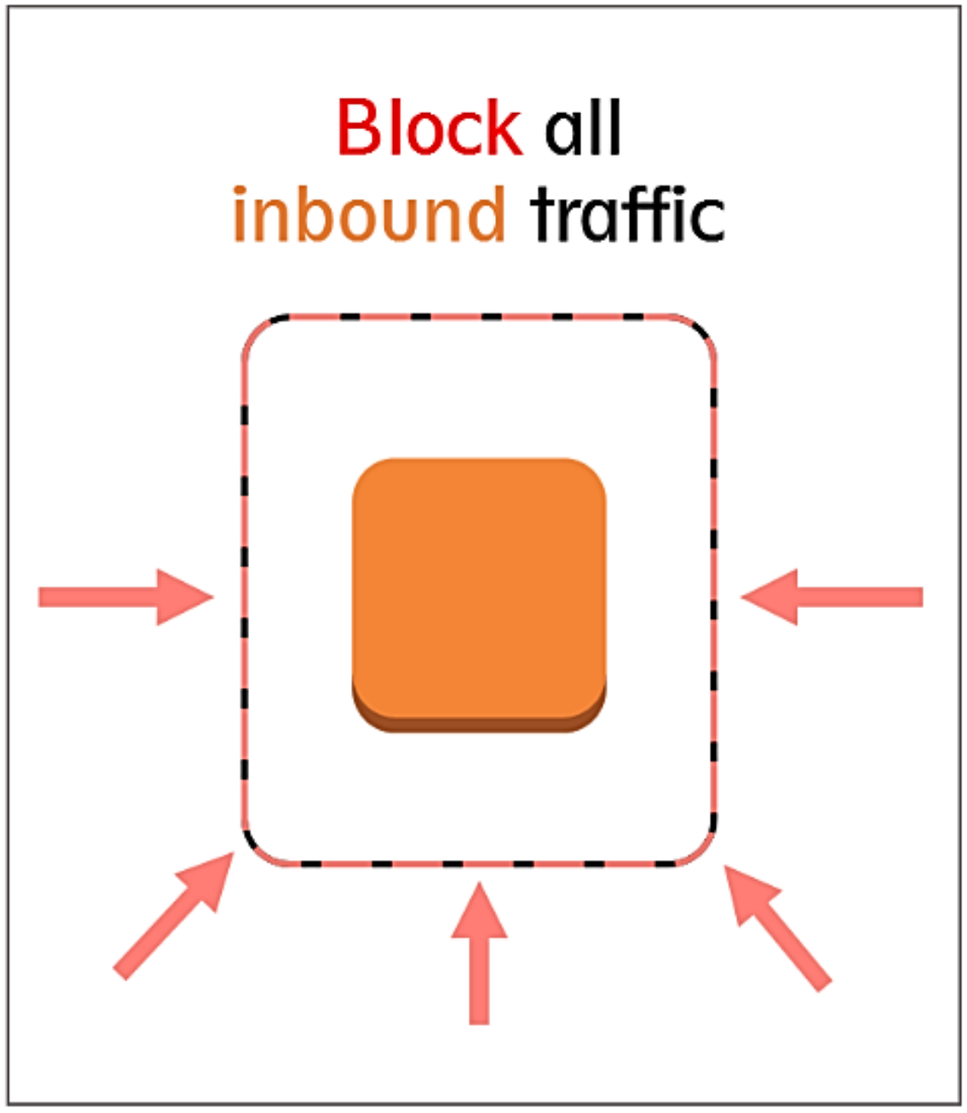
Security Groups

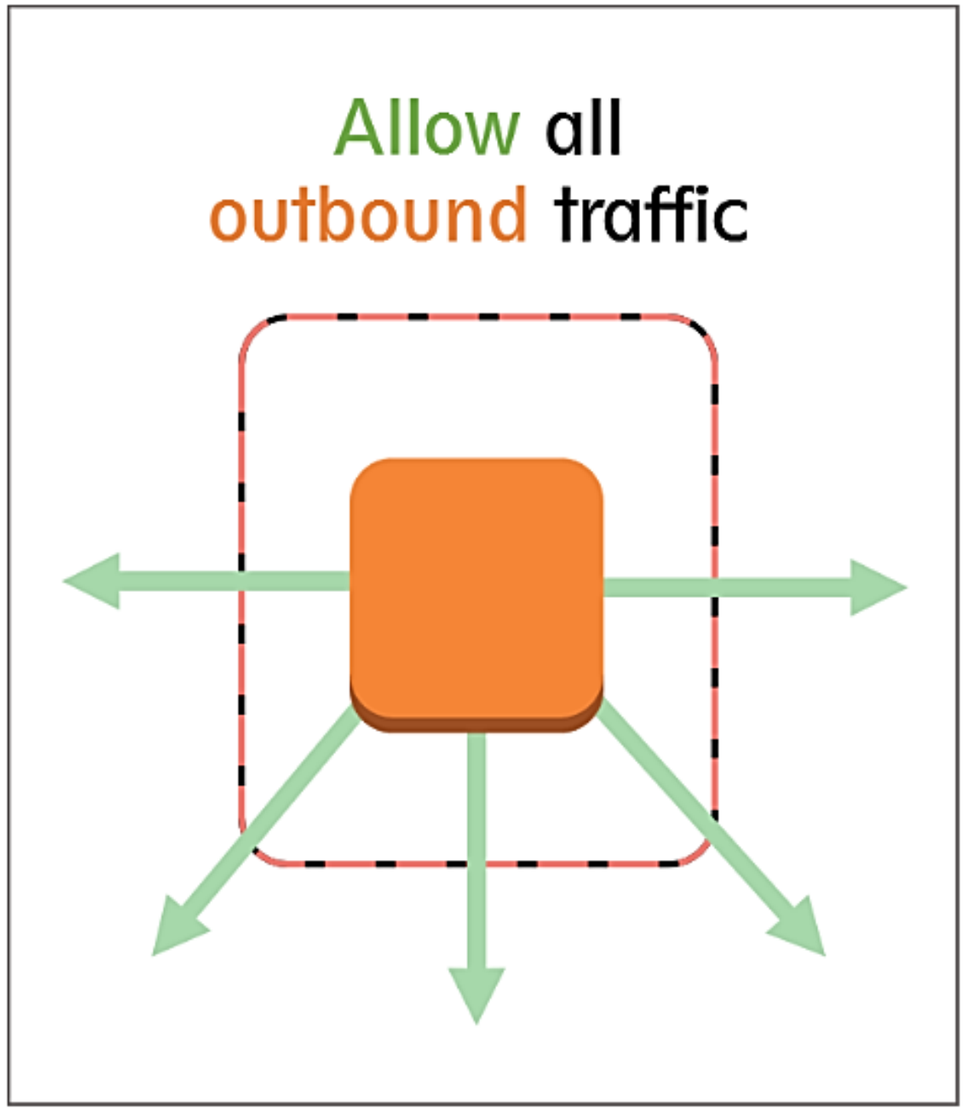


- Virtual firewalls that control inbound and outbound traffic into AWS resources (instance and/or service level)
- Traffic can be restricted by any IP protocol, port, or IP address
- Rules are stateful



New security groups:





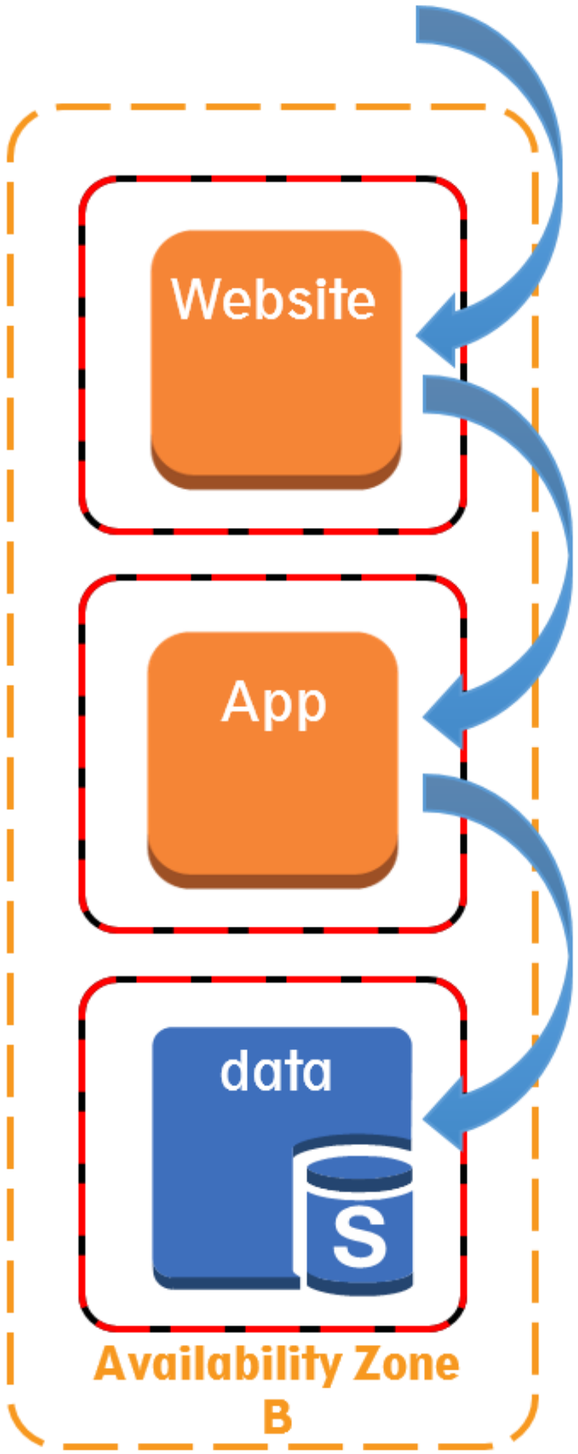
* Except for same security group

Security Groups

Web tier
Security group

Application
Security group

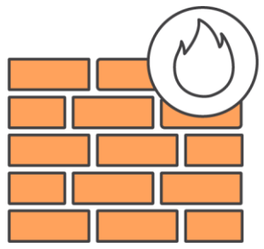
Database
Security group



Inbound rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (any)

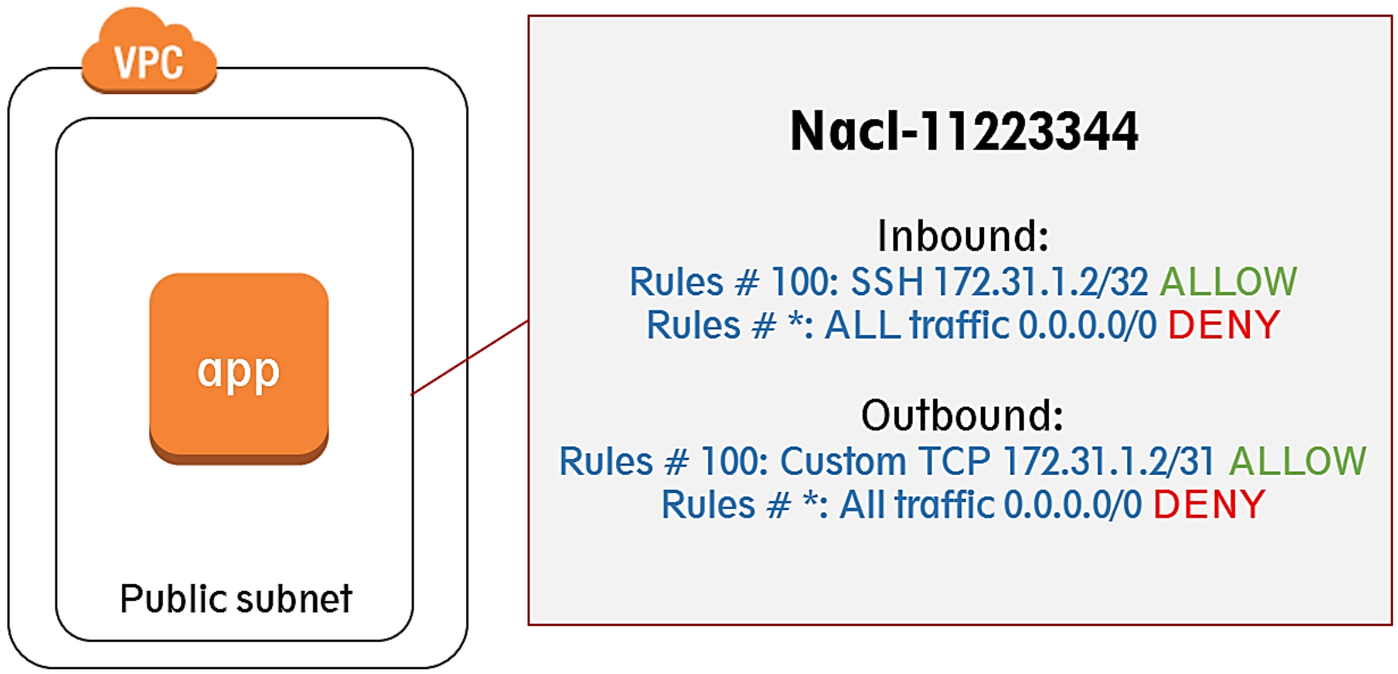
Inbound rule
Allow HTTP port 80
Source: Web tier

Inbound rule
Allow TCP port 3306
Source: App tier

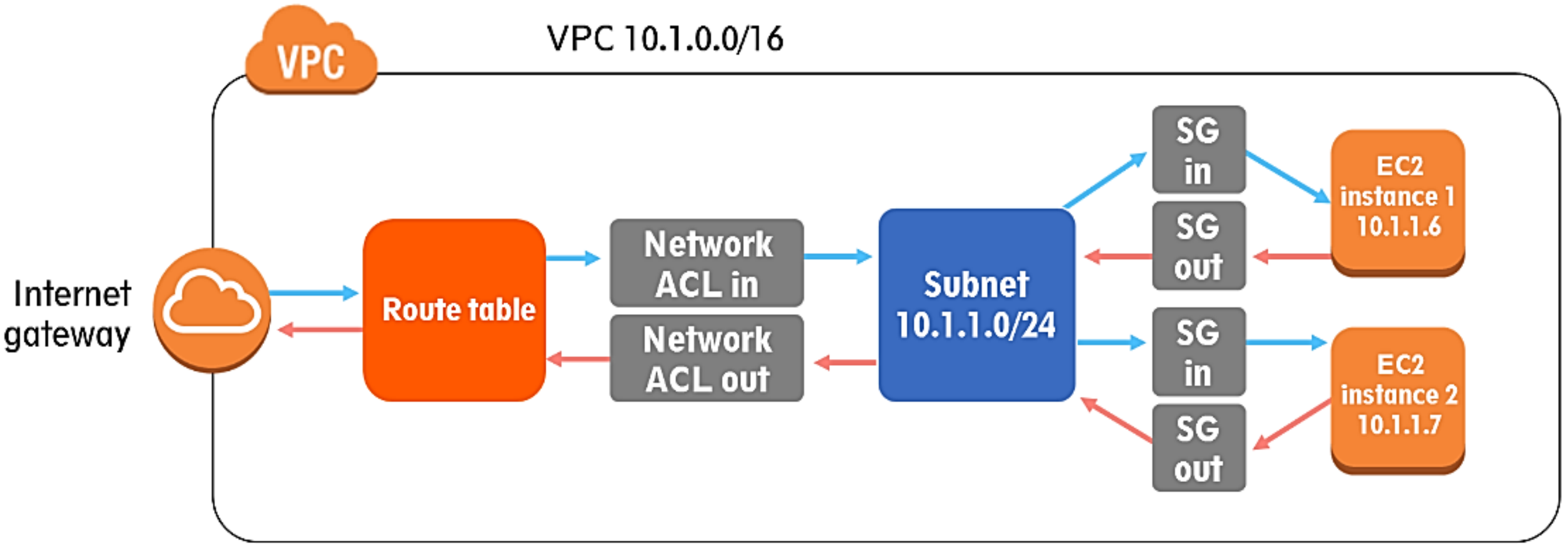


- Firewalls at the subnet boundary
- Will allow all inbound and outbound traffic by default
- Are stateless, requiring explicit rules for both inbound and outbound traffic

Recommended for
specific network security requirements
only



Security Components

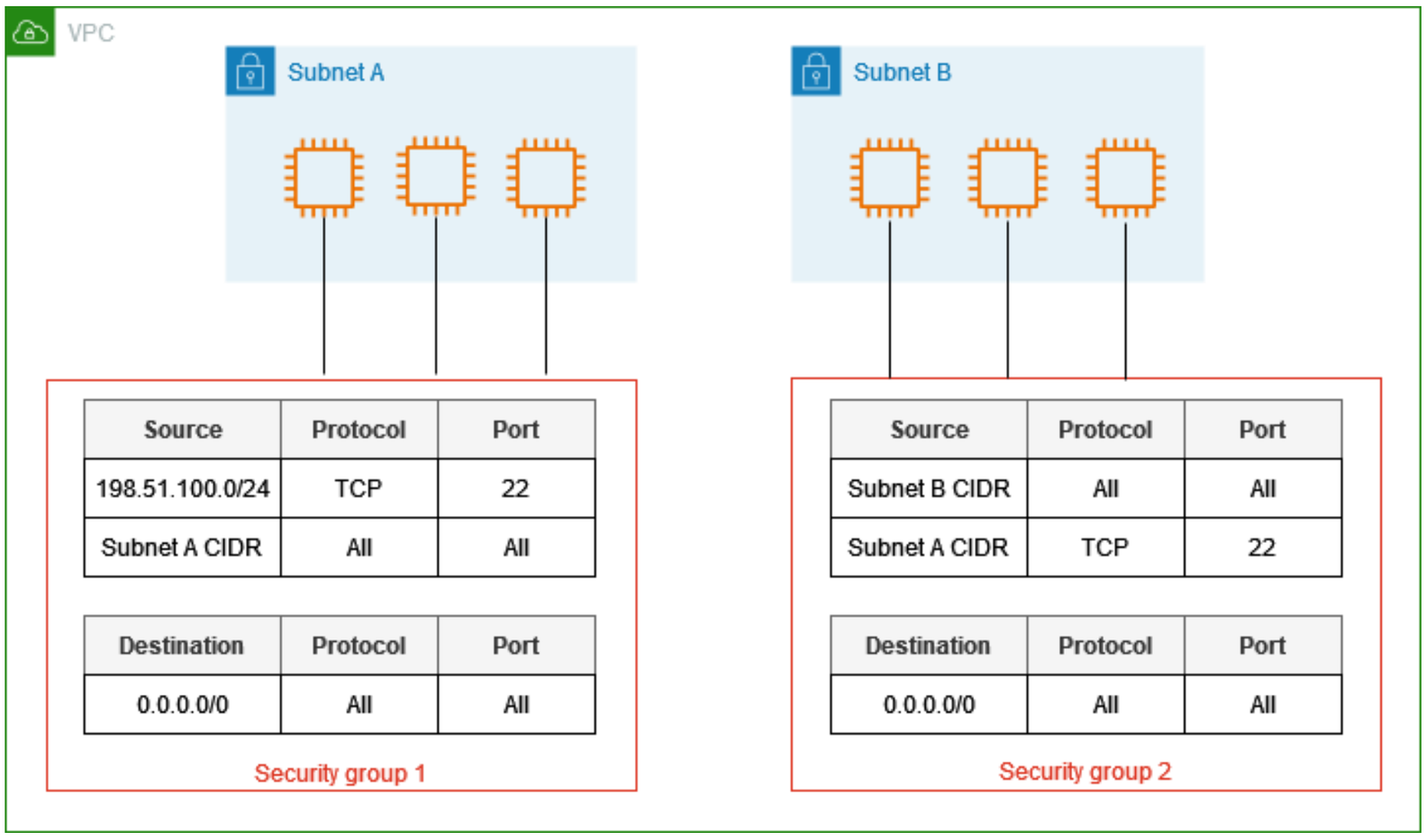


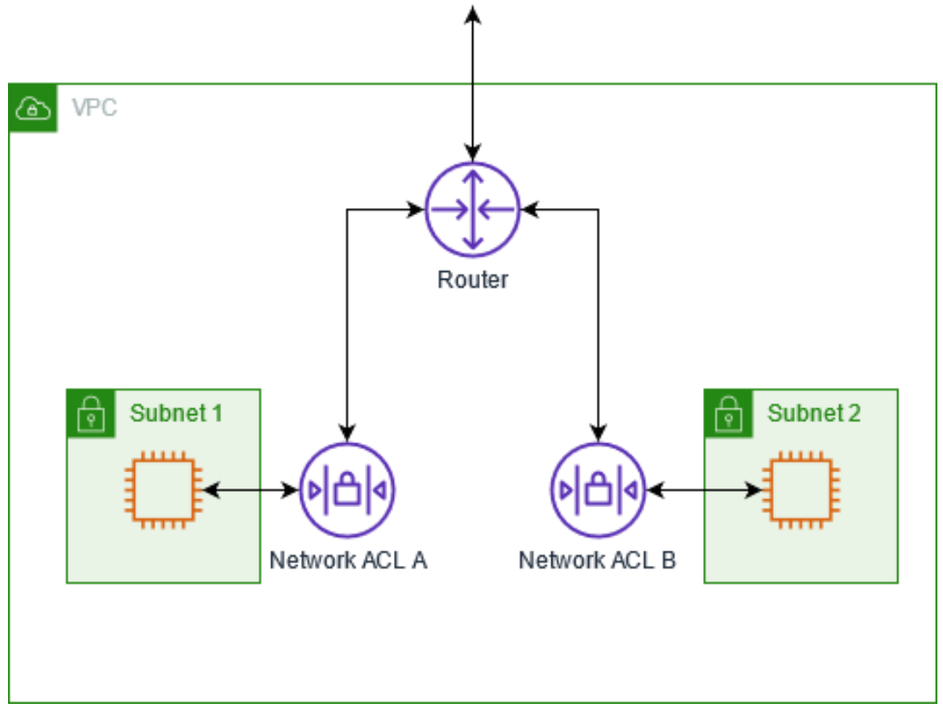
Security Groups vs ACL

Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
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 (backup layer of defense, so you don't have to rely on someone specifying the security group)

Taken from https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html and https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#default-network-acl on (10/05/2020)

Scenario with Sec Groups / NACL

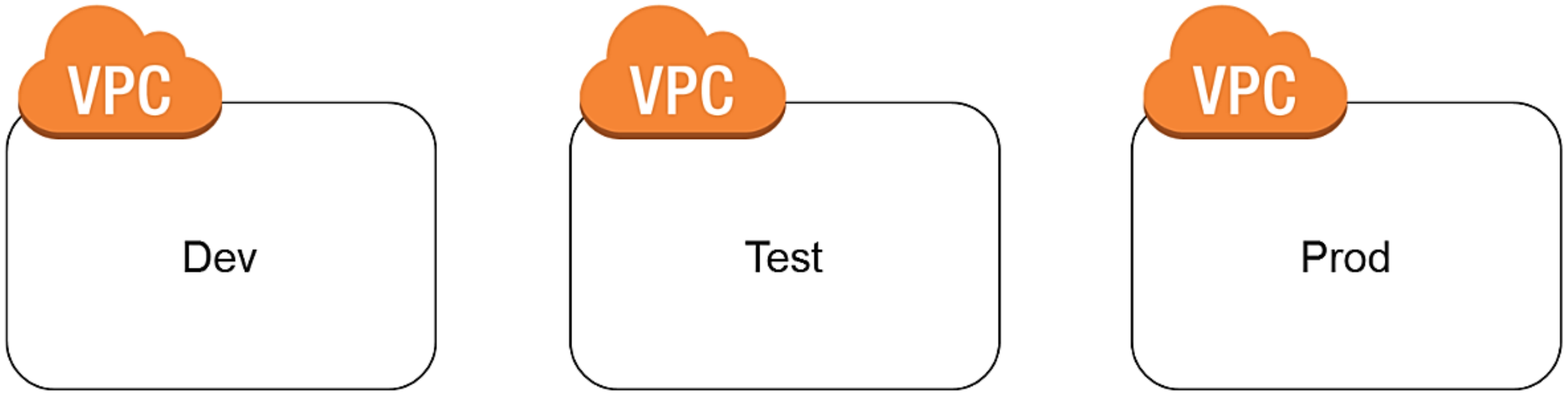




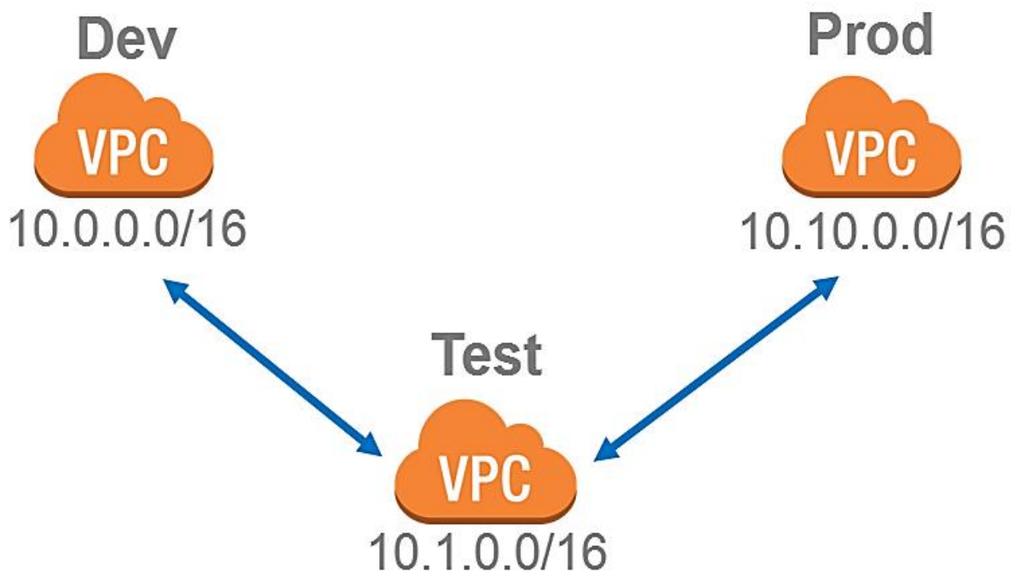
Taken from https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html and https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#default-network-acl on (10/05/2020)

Connecting VPCs

- Isolating some of your workloads is generally a good practice.
- But you may need to transfer data between two or more VPCs. Example: Test Data.



VPC Peering

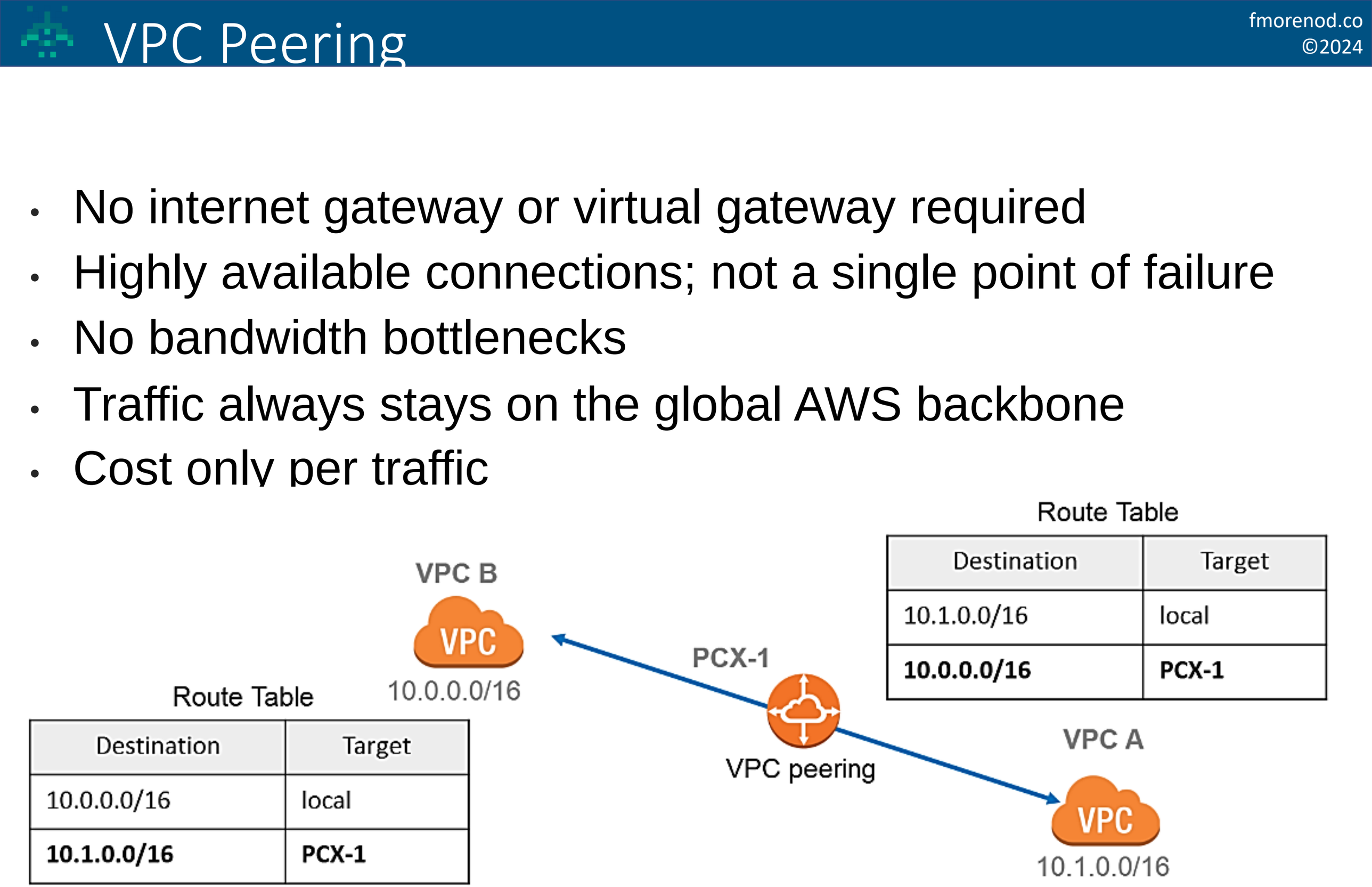


Instances can communicate across a peering connection as if they were in the same network.

- Use private IP addresses
- Intra and inter-region support
- IP spaces cannot overlap
- Only one peering resource between any two VPCs
- Transitive peering relationships are not supported
- Can be established between different AWS accounts

VPC Peering

- No internet gateway or virtual gateway required
- Highly available connections; not a single point of failure
- No bandwidth bottlenecks
- Traffic always stays on the global AWS backbone
- Cost only per traffic



VPC Peering: General Best Practices

When connecting multiple VPCs, there are some universal network-design principles to consider:

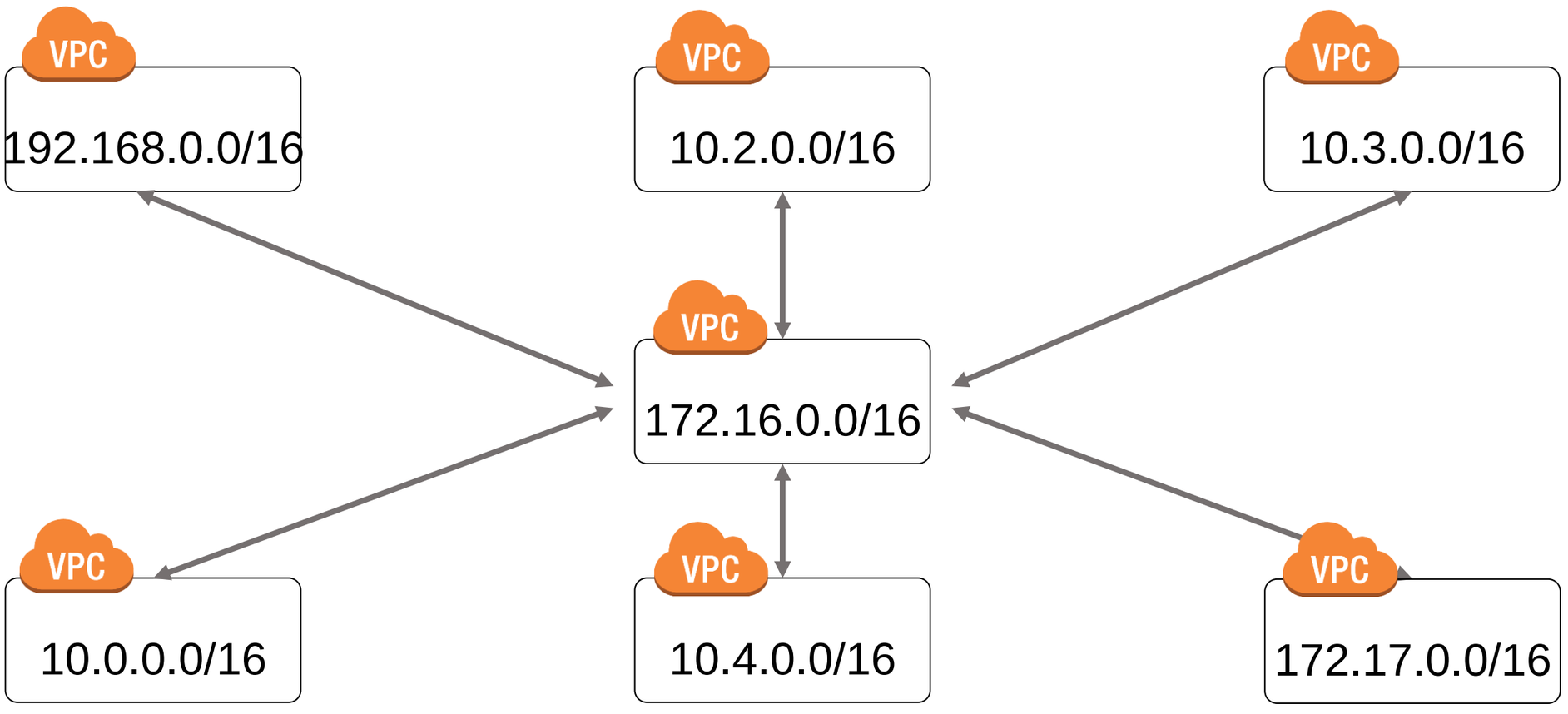
Destination	Target
10.0.0.0/16	local
10.1.0.0/16	**PCX-1**

No overlapping CIDR blocks

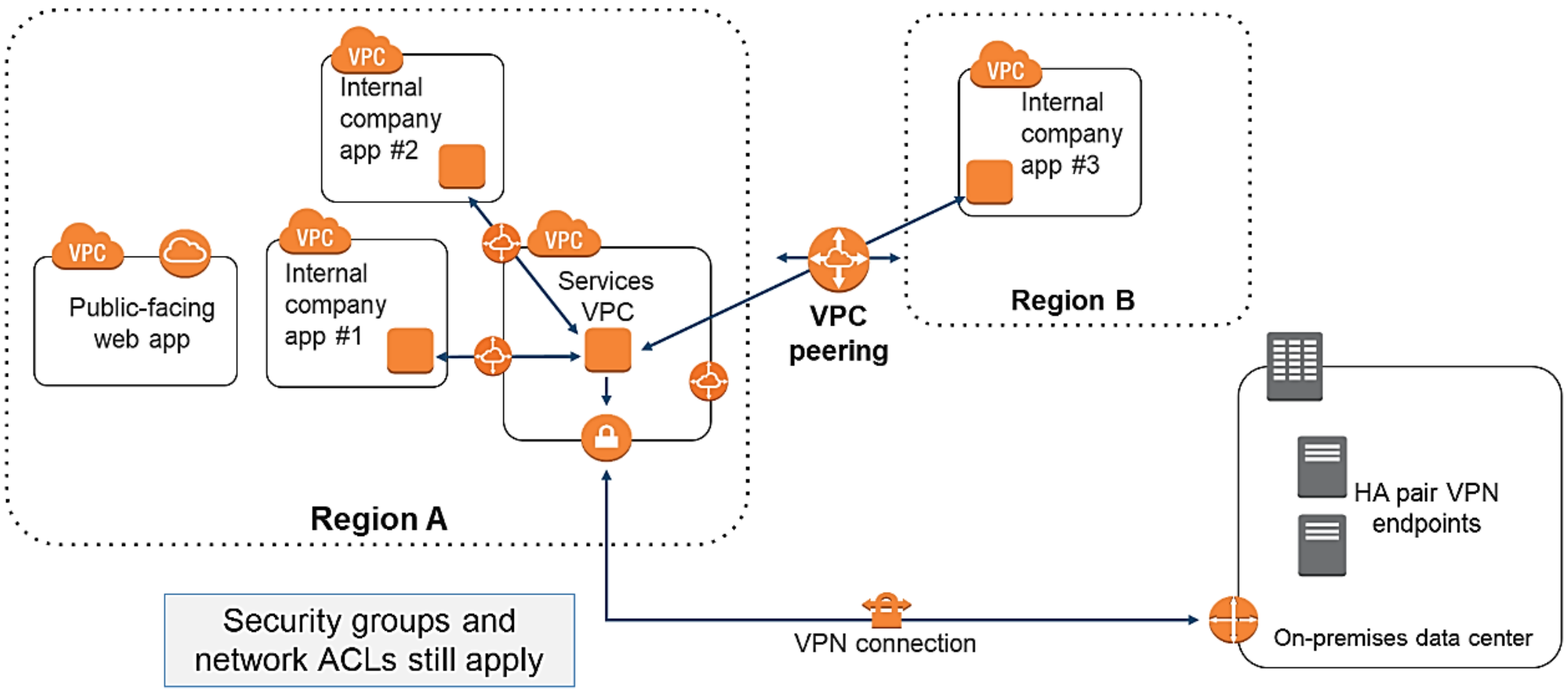
Only connect essential VPCs

Make sure your solution can scale

Connecting VPCs



Connecting VPCs

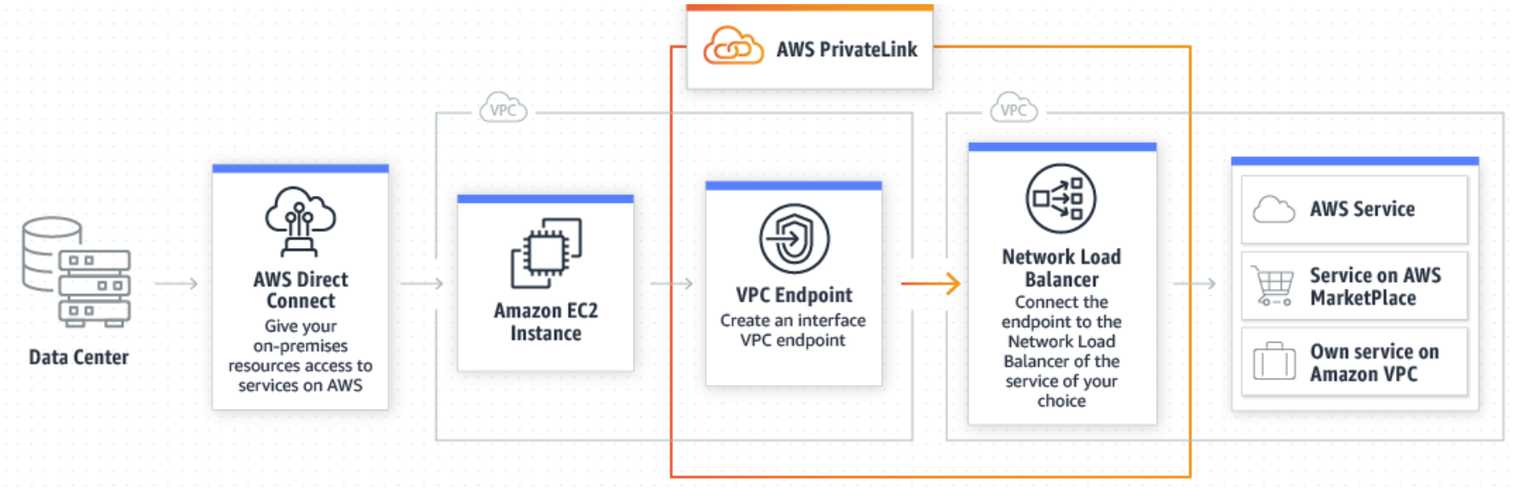


Private Connections: PrivateLink

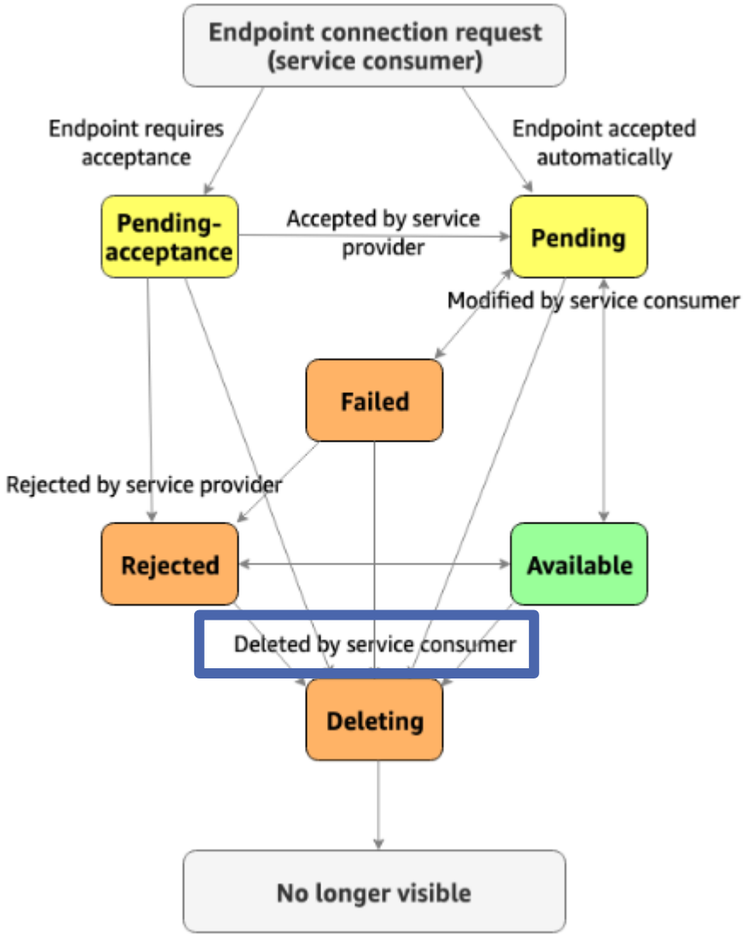
Privately connect your EC2 instances to services outside your VPC without leaving AWS.

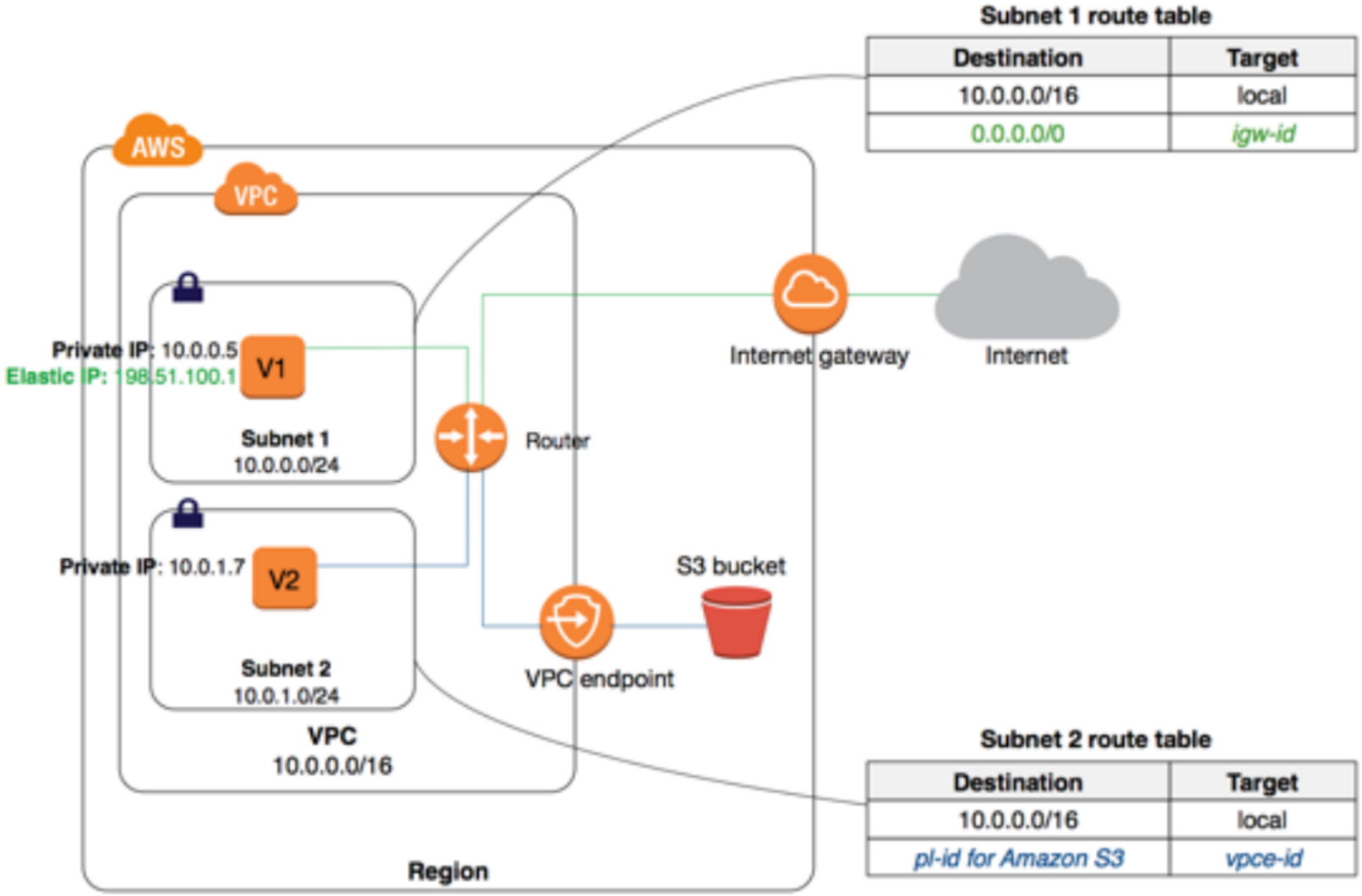
Don't need to use an internet gateway, VPN, network address translation (NAT) devices, or firewall proxies.

- Does not require traversal over the internet
- Must be in the same region
- Endpoints are logical devices, so AWS make them horizontally scaled, redundant, and highly available.



VPC Endpoints – Key Concepts

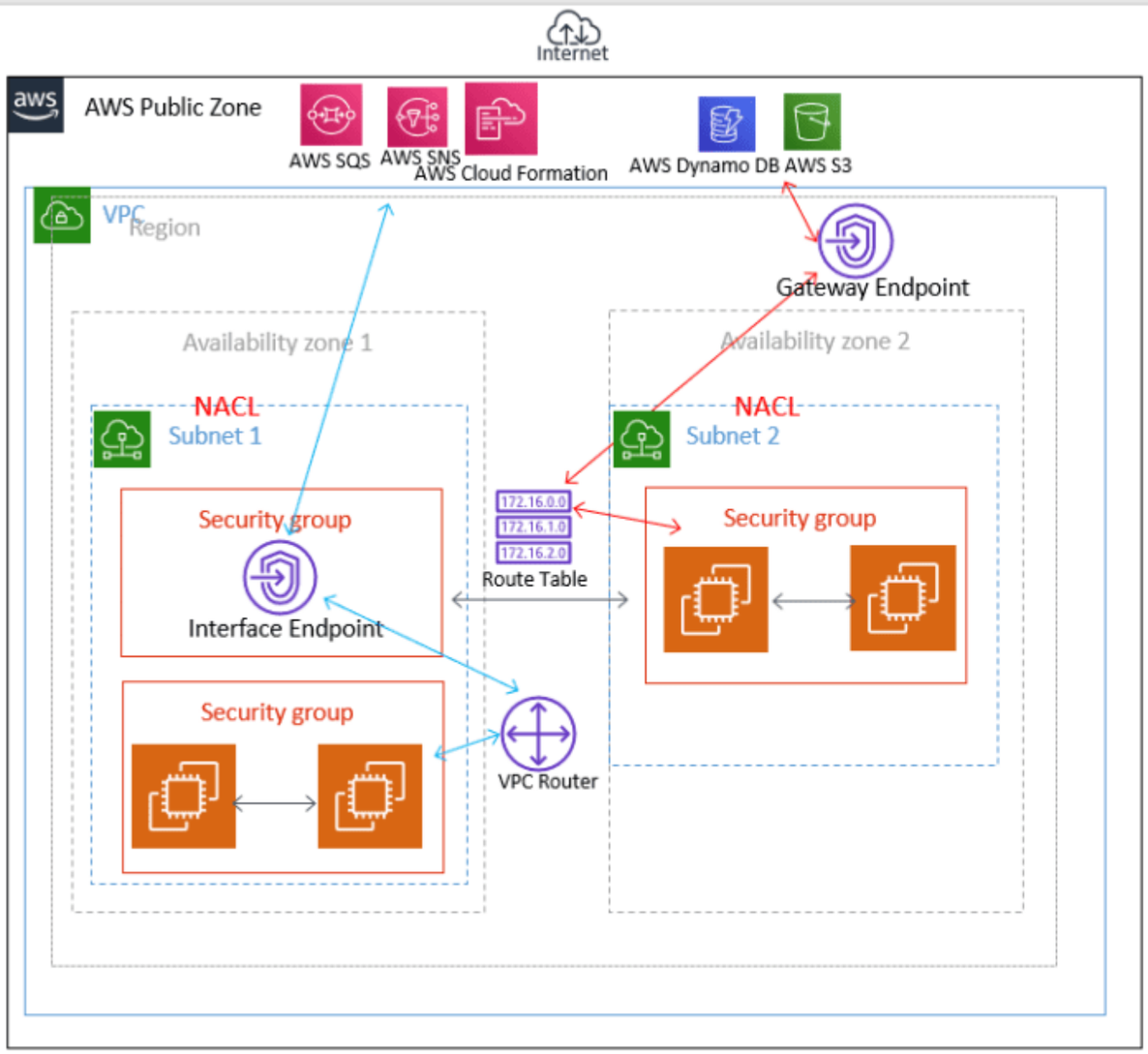




Endpoint service: To whom I will serve on you VPC: AWS Service or Partner Service
Gateway endpoint: Entry point on your VPC to connect privately to AWS Services (Route table).
Interface endpoint: An ENI in your VPC that manage the private connections to AWS Services.
Gateway Load Balancer Endpoint: A GW Load Balancer is more to have a proxy on a net. More information at: https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/introduction.html (18/07/2024)

Taken from https://varunmanik1.medium.com/aws-vpc-endpoints-its-type-33585ff27d7b (18/07/2024)

VPC Endpoints – Key Concepts



VPC Endpoints

Gateway Endpoints:

- Sit inside a VPC not a subnet and are highly available
- When associated with a route table, the route table automatically updates the prefix list of service and target endpoints
- Can use an IAM policies or resource policies to restrict access
- Supports S3 and Dynamo DB
- Must be inside the VPC to use

Interface Endpoints:

- Sit inside a subnet and need to be in an Availability Zone (for HA, put one in each AZ)
- Do not use route tables
- Is an elastic network interface (ENI) and is associated with a security group
- Has its own set of DNS names, including one for AZ and region
- Can be used with Route 53 Resolver to return private IP address
- Supports most of AWS services
- Available to be used outside of the VPC with VPN, Direct Connect, or VPC peering

Taken from https://gkzz.medium.com/what-is-the-differences-between-vpc-endpoint-gateway-endpoint-ae97bfab97d8 (18/07/2024)

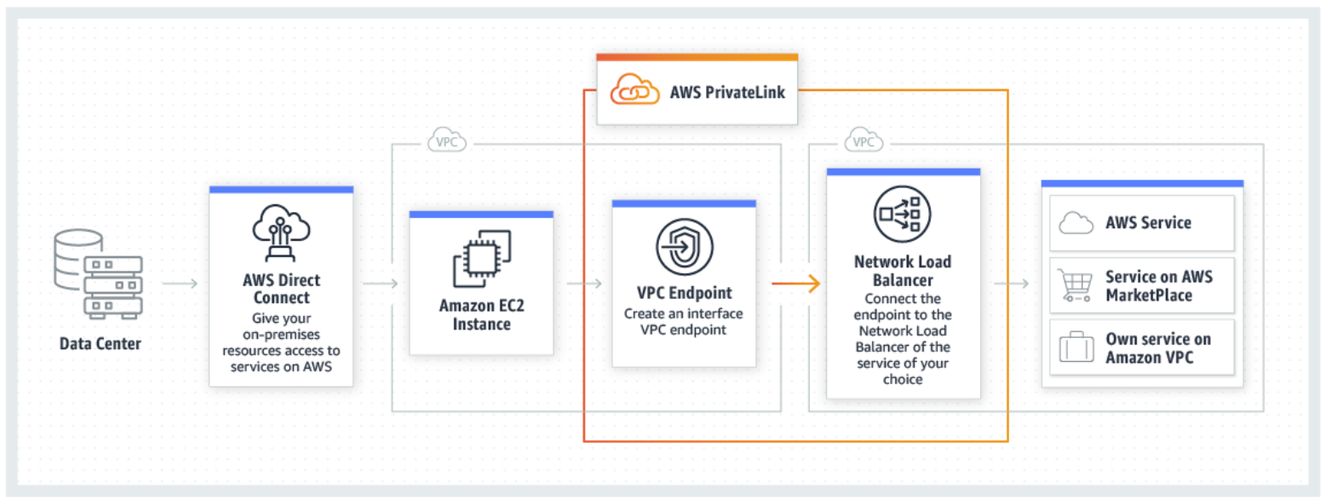
VPC Endpoints: Interface or Gateway

Interface Endpoint

- Amazon CloudWatch Logs
- AWS CodeBuild
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service (AWS KMS)
- Amazon Kinesis Data Streams
- AWS Service Catalog
- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager
- Endpoint services hosted by other AWS accounts

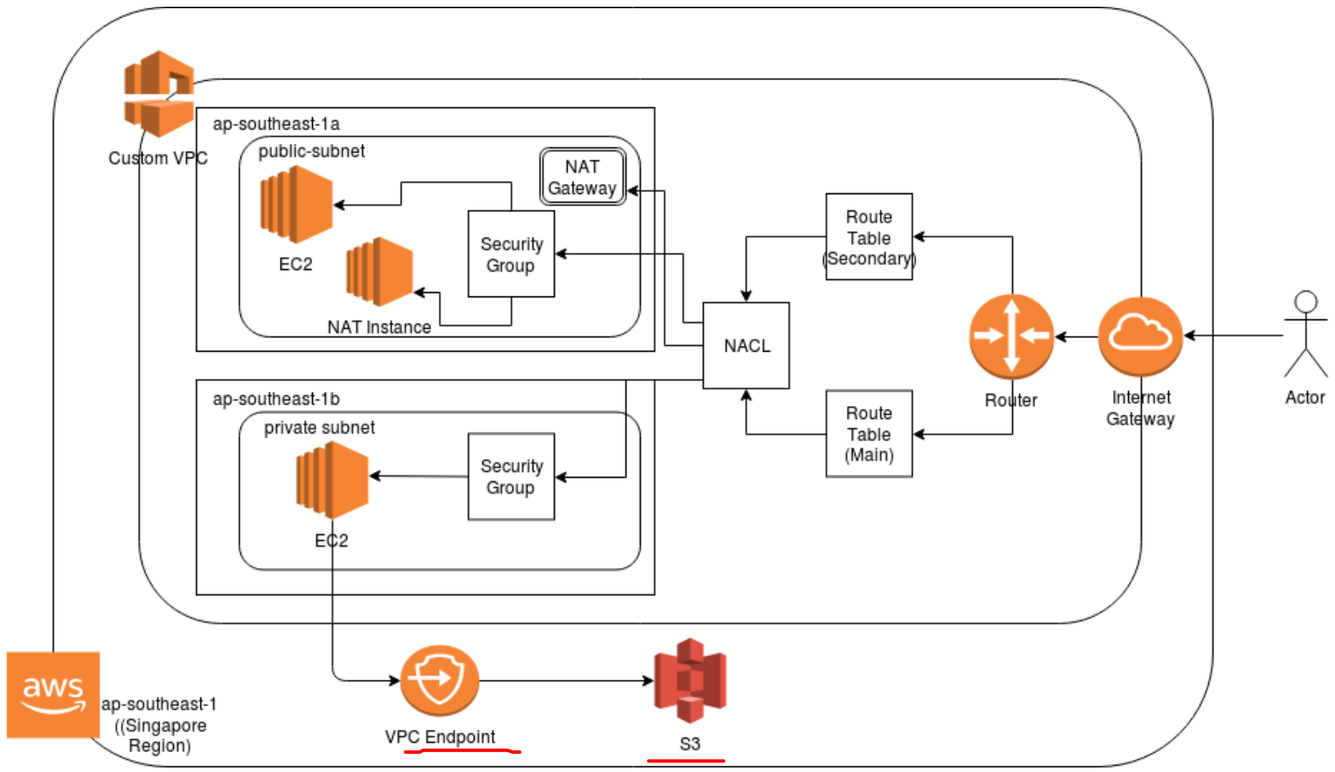
Gateway Endpoint

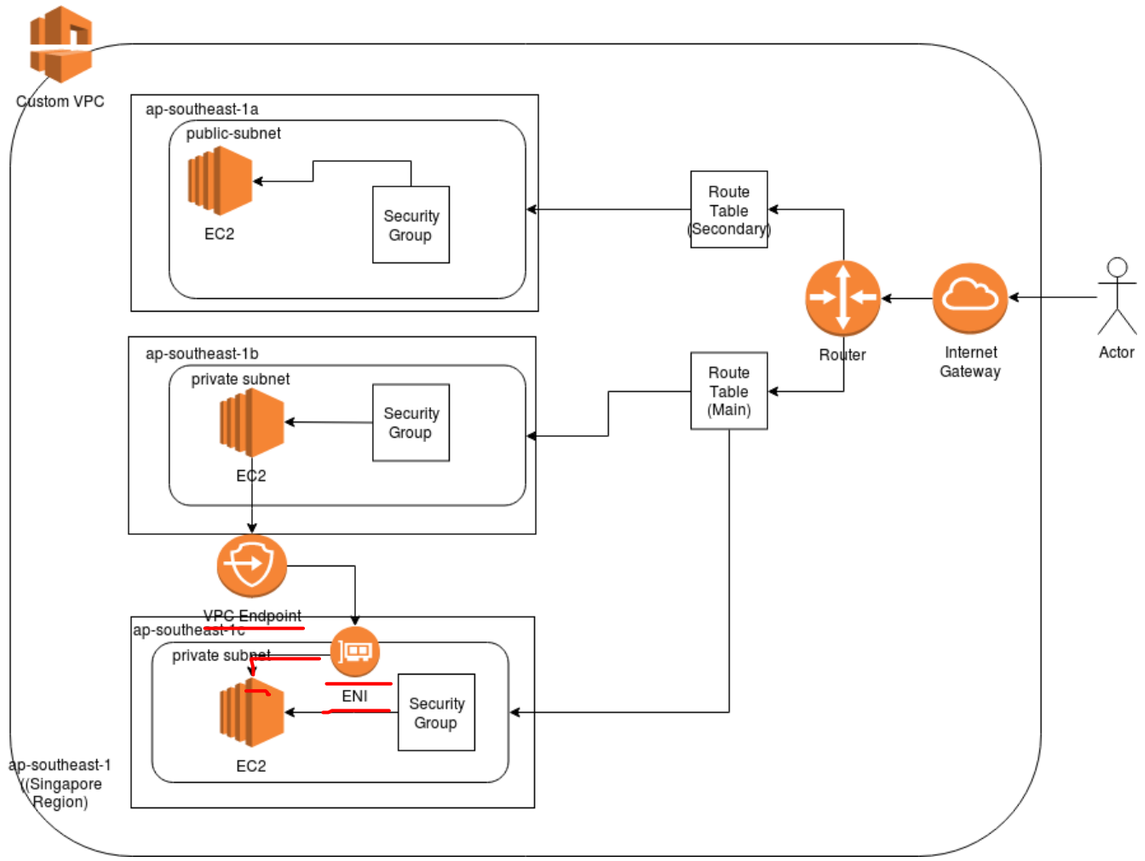
- Amazon S3
- Amazon DynamoDB

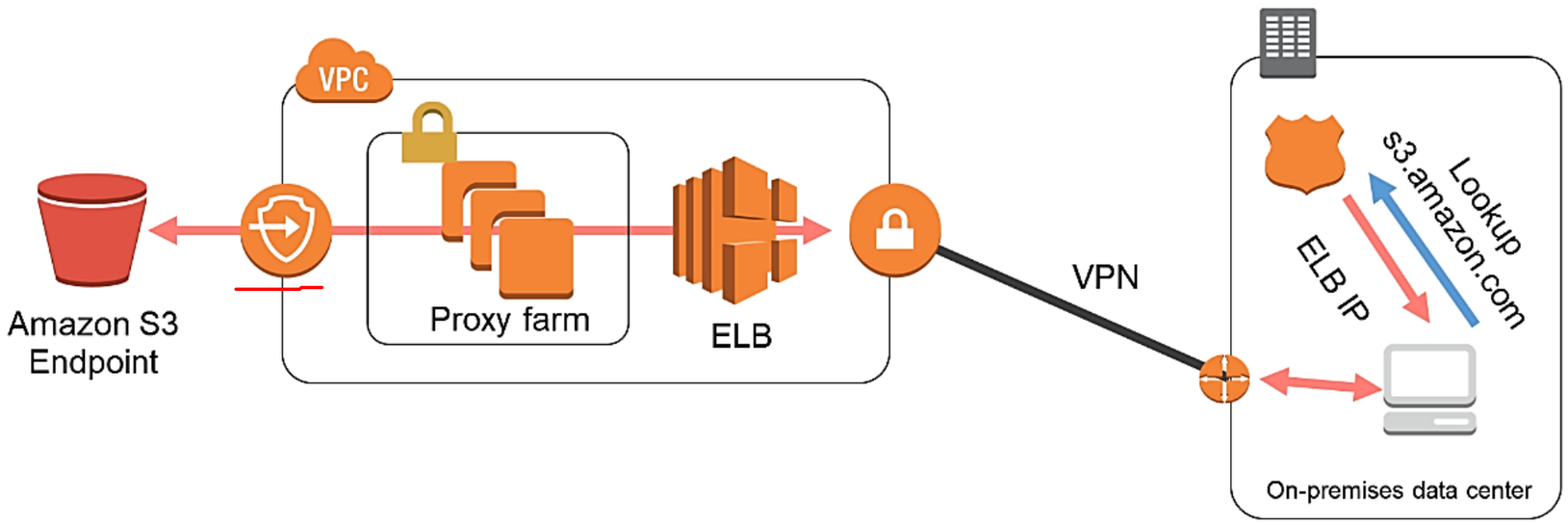


The traffic is on AWS Network Infra Only.
On GW, you need to modify the route table.
On Endpoint, AWS create an ENI on your source subnet to reach the another service.

VPC Endpoints







Taken from https://medium.com/@crishantha/handling-vpc-endpoints-ac192b0361a5 (18/07/2024)

VPC Flow Logs

Flow logs

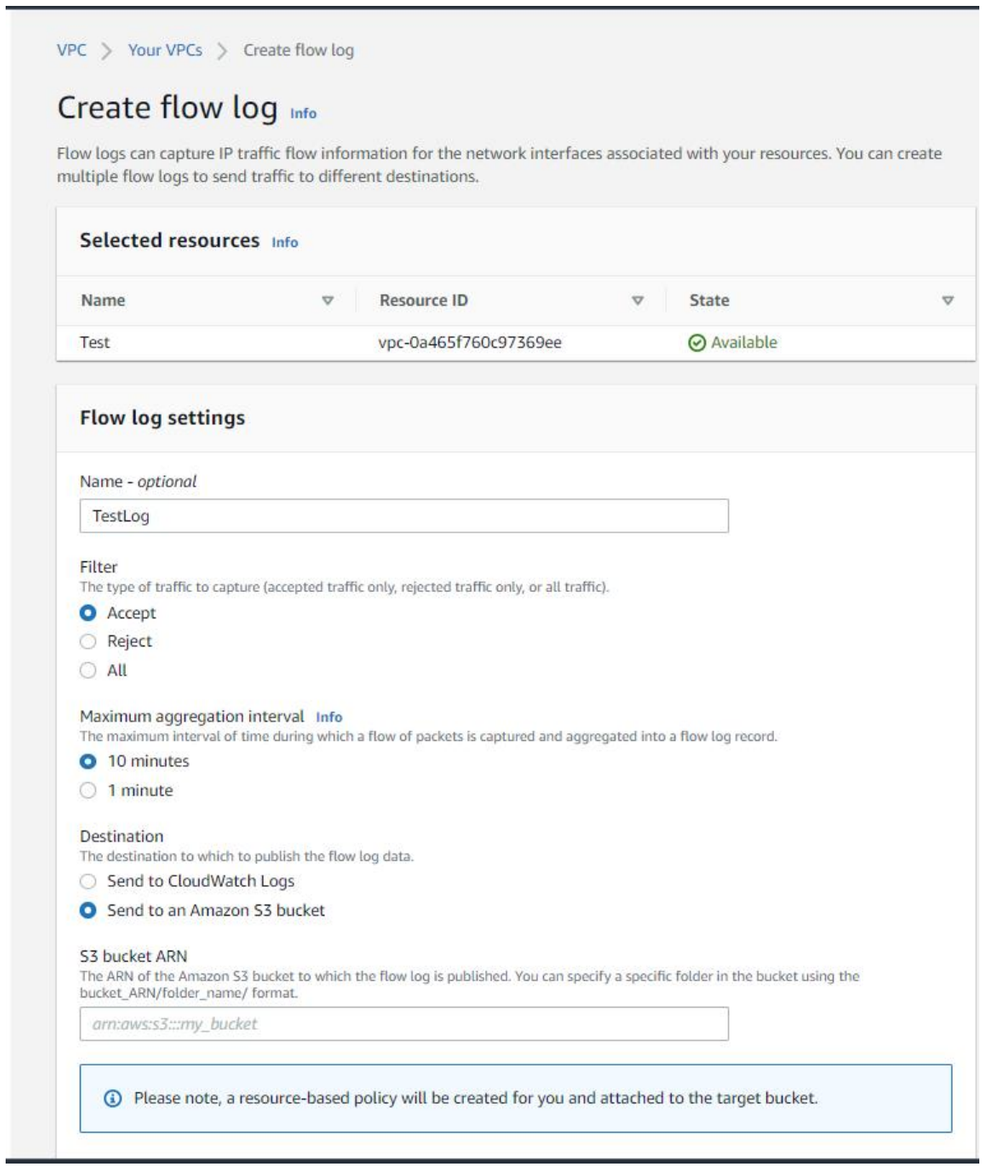
Auditing at VPC, Subnet and ENI Level. Filter to All, Accepted, Reject Traffic. Some exceptions (DHCP, DNS, Win Act, Metadata URL).

Destination: S3 Bucket or Cloudwatch Logs.

IAM Role for Cloudwatch or Resource-Based Policy for S3.

Change Log Format.

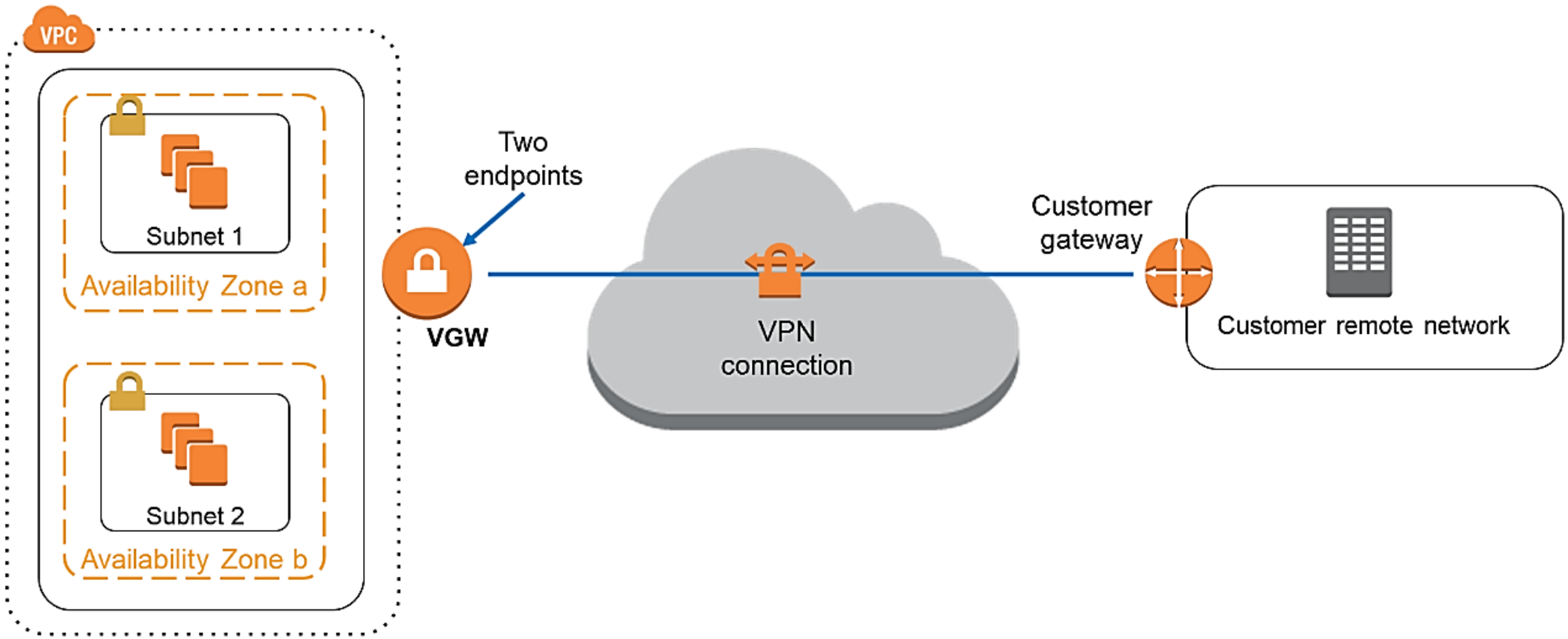
Not change after launch.



Virtual Private Gateway (VGW)

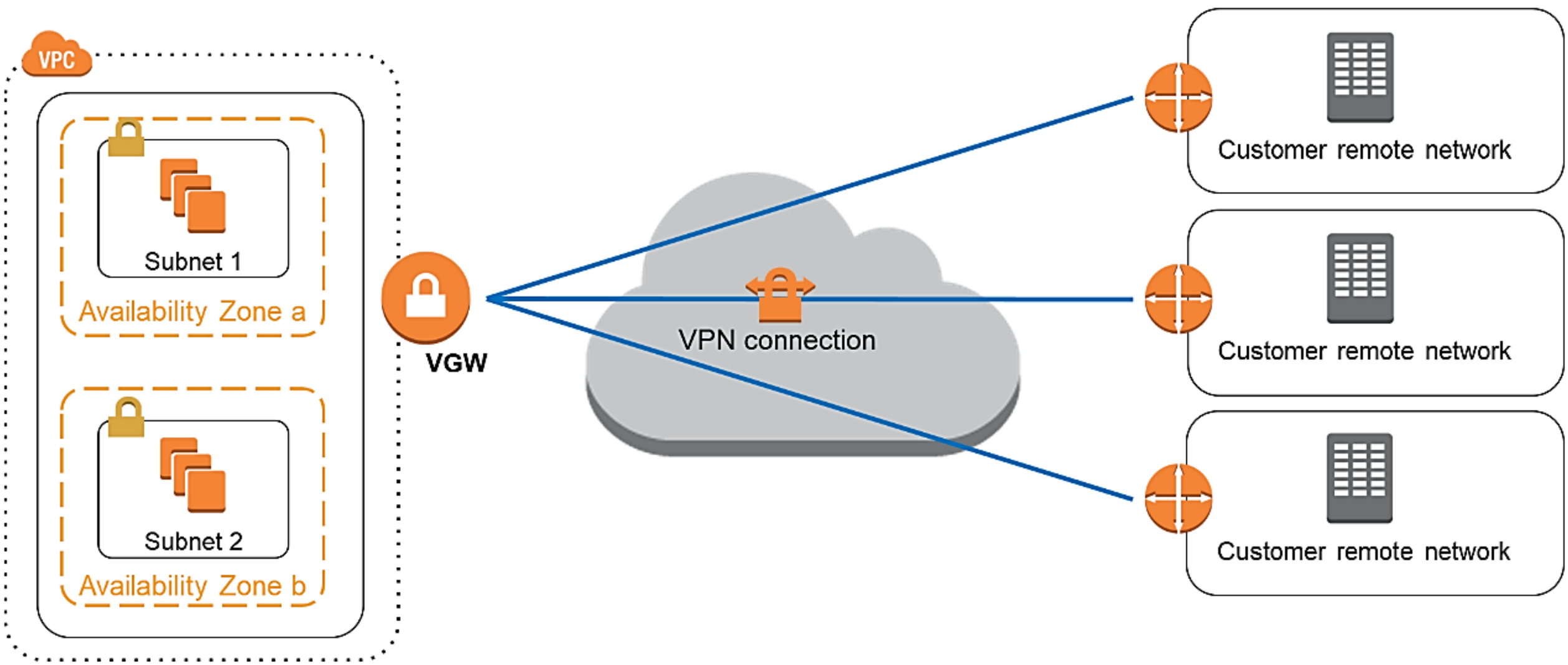
Enables you to establish private connections (VPNs) between an Amazon VPC and another network

Virtual Private Gateway (VGW)



Two Endpoints are 2 Tunnels for redundancy, 1.25 GBps each one. Reduced FT because we have 2 tunnels on AWS, and only one on Customer Side.

Virtual Private Gateway (VGW)

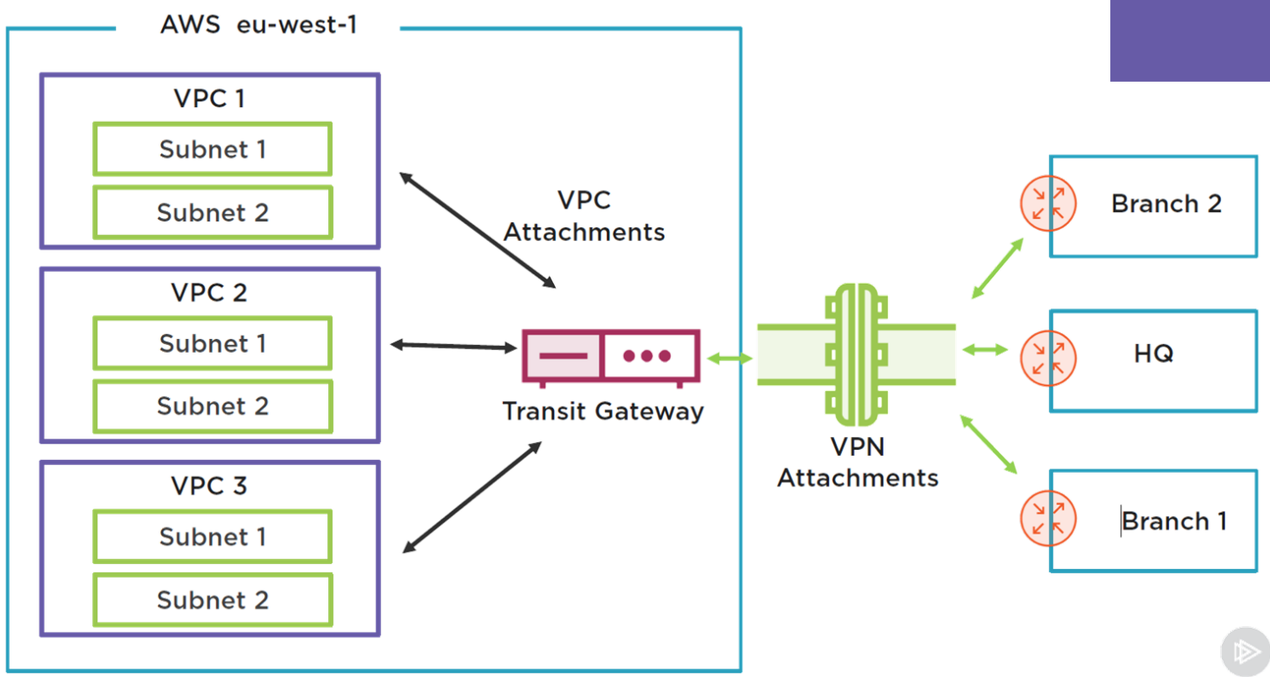


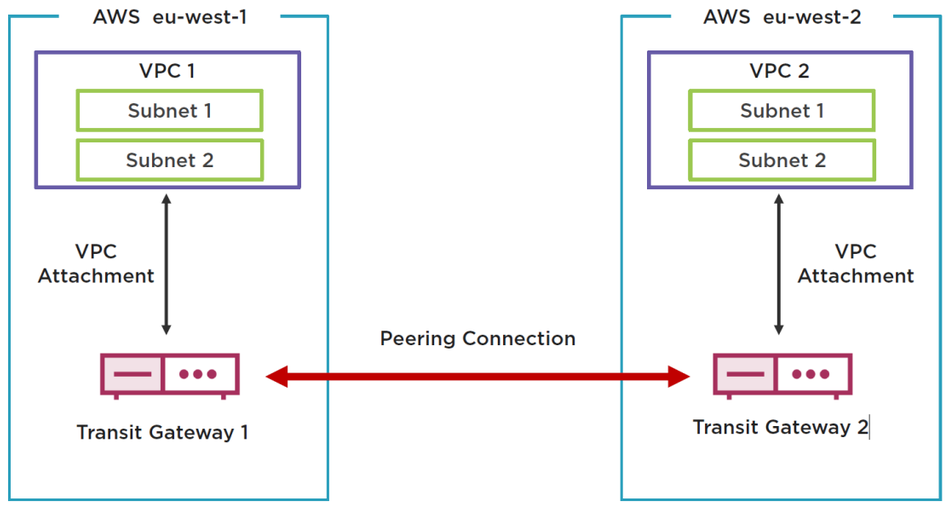
Transit Gateway

Attachments
VPCs, VPNs, peered transit gateways and direct connect

Routing
Control the flow of traffic between attachments

Hub and spoke
Provides transitive routing between attachments





DNS support
DNS resolution across attachments

ECMP support
Equal cost multipath routing

Route tables
Default and custom route tables

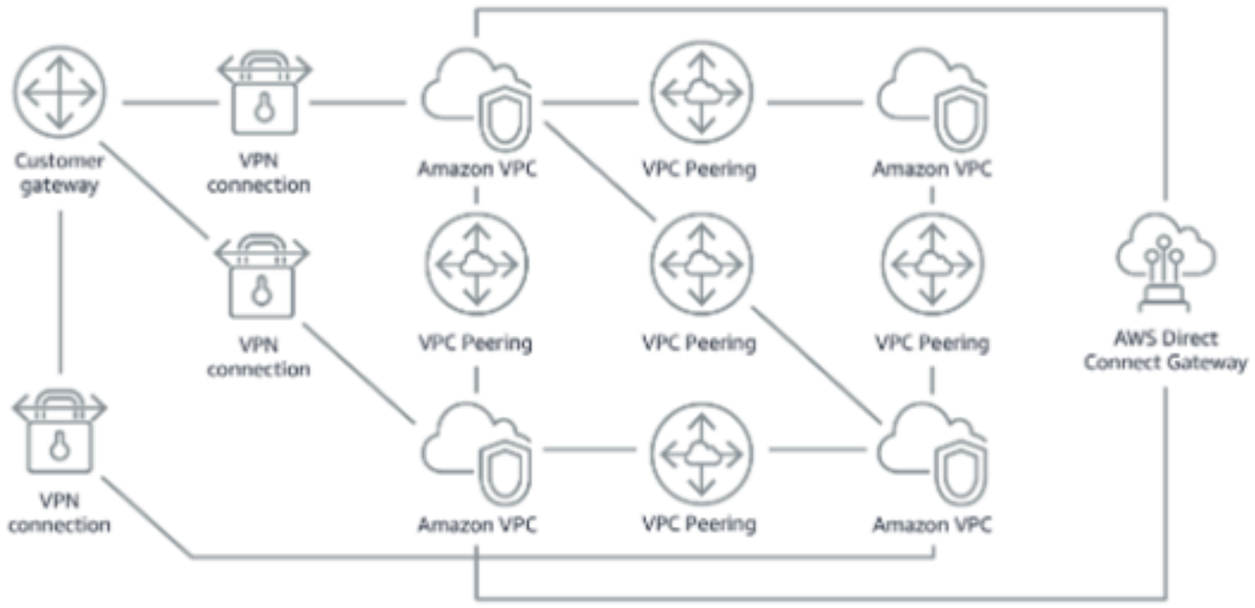
Static or dynamic
Support for static and dynamic routing

Sharing
Can be shared between accounts

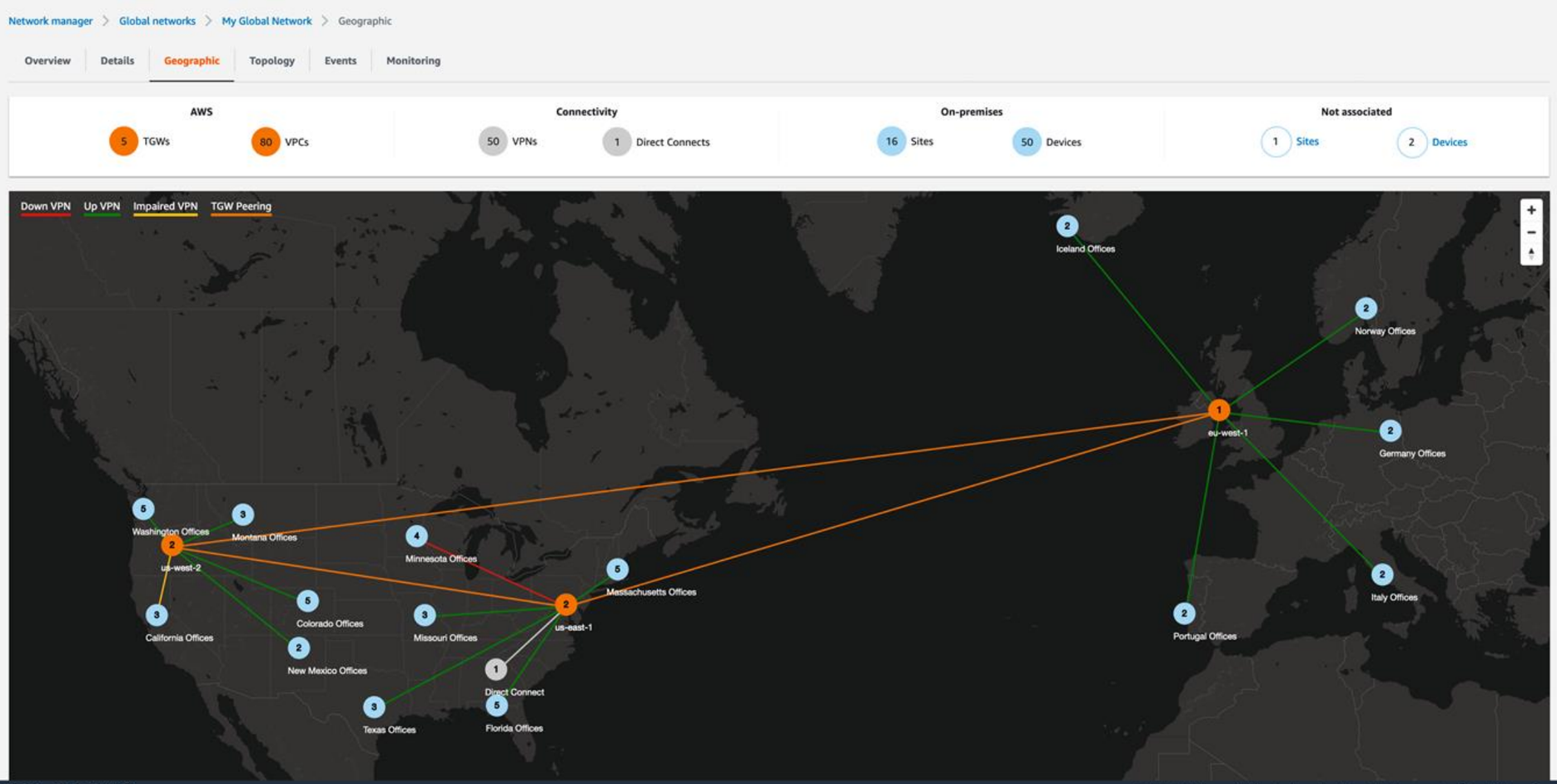
Taken from https://app.pluralsight.com/library/courses/designing-hybrid-networks-aws/table-of-contents (18/07/2024)

Transit Gateway

Without AWS Transit Gateway



With AWS Transit Gateway



Similar service to reach multiple VPC Peering in a hub-and-spoke topology.
Allow route propagation using BGP.
On-Premises and Cloud scope.
Replace of Transit VPC (Old Arch)
¿¿¿ Remember RAM ???

Taken from
https://aws.amazon.com/premiumsupport/knowledge-center/transit-gateway-migrate-vpn/ ,

https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html and

https://aws.amazon.com/transit-gateway/ (18/07/2024)

AWS-Managed VPN vs Transit GW

Transit Gateway	Virtual Private Gateway
$0.06 per transit gateway attachment hour	$0.05 per site-to-site VPN connection hour
~~$0.05 per site-to-site VPN connection hour~~	Data transfer out
Per GB of data processed $0.02	Attached to a single VPC
Multiple attachments	No additional configuration
Equal cost multipath routing	
Multiple route tables	

Region: US East (N. Virginia)

Price per AWS Transit Gateway attachment ($)	$0.05
Price per GB of data processed ($)	$0.02

Taken from https://aws.amazon.com/transit-gateway/pricing/ (18/07/2024). Updated info at https://calculator.aws/#/