

VPC Design and New Capabilities for Amazon VPC



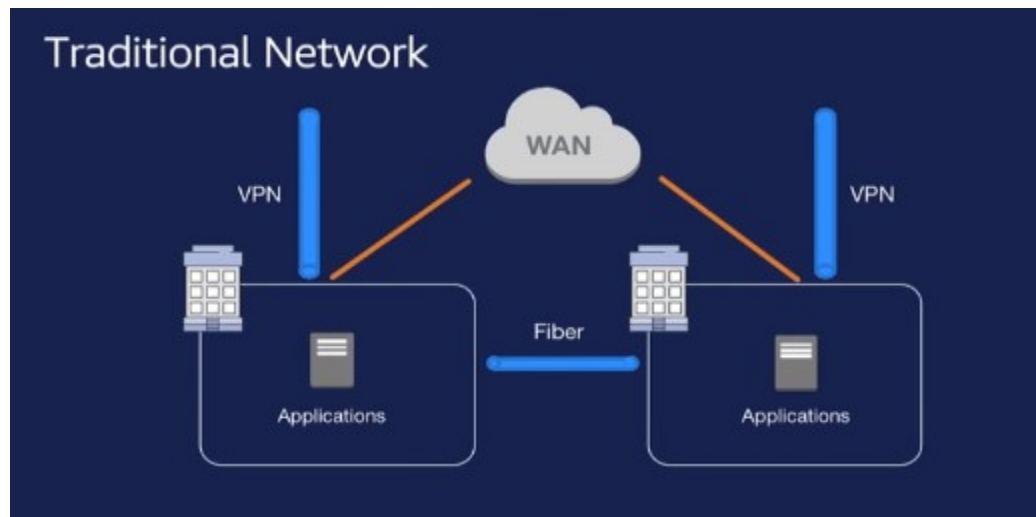
Traditional On-Premise Networks

Data centers have applications inside them.

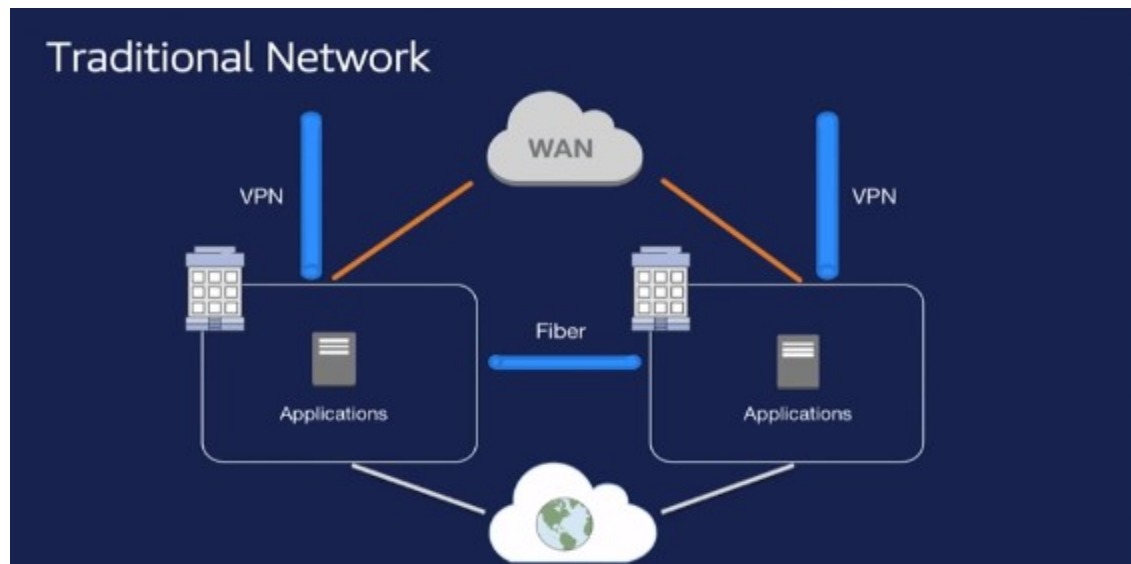
Data centers are connected to each other with Fiber (when required)

Data centers are connected to the corporate environment using VPN and WAN

You can provide internet access to the data centers when required (with proper security)



Traditional On-Prem Network with Internet Access

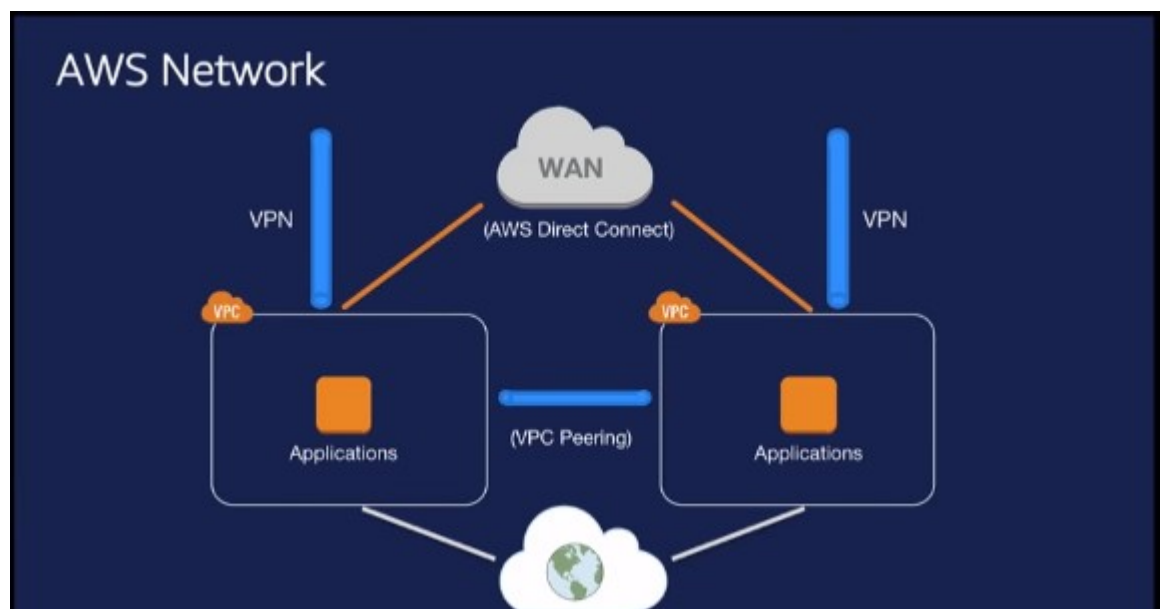


Similar network model implementation on AWS Platform

Data center concept is replaced with VPC

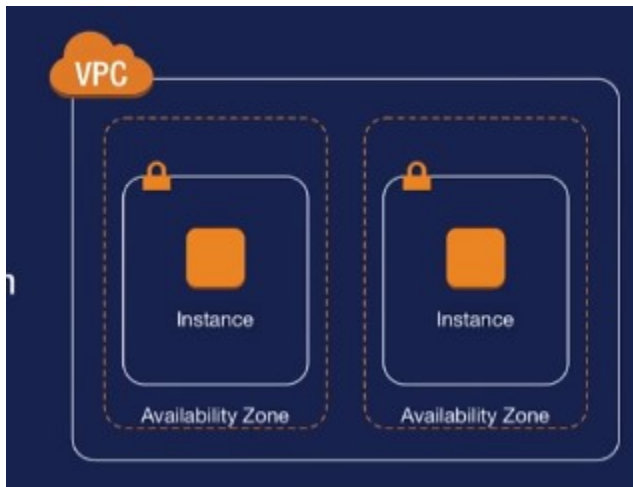
VPCs are connected with VPC Peering

AWS Direct connect and VPN/VPG are used to connect to on-premise.

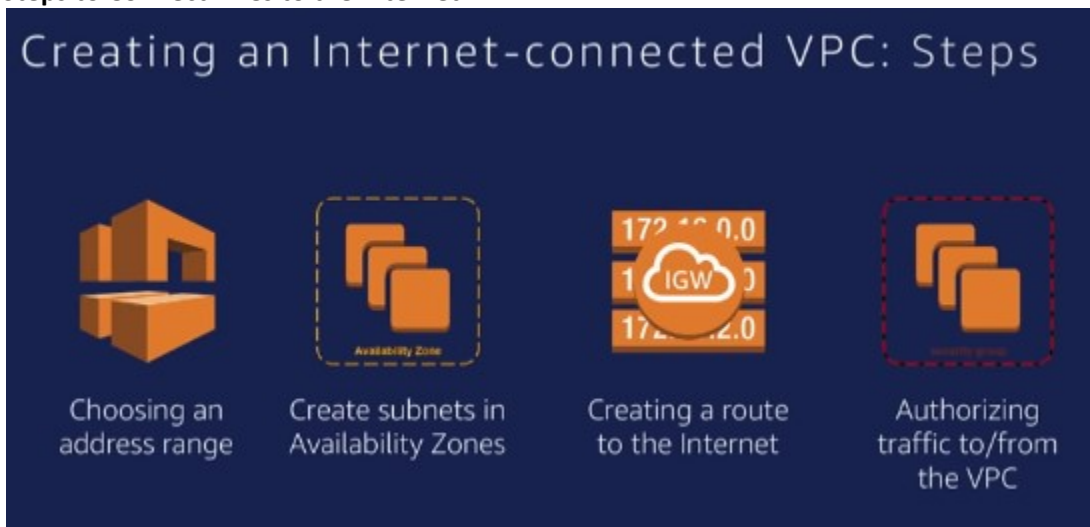


VPC, Region, Availability Zones, Subnet, Elastic Computing (EC2) Cloud

- Deploy your VPCs/Data Centers in one of 18 Regions of AWS (Do not confuse, Regions and Availability Zones)
- Then use Availability zones for High Availability and Disaster Recovery. Availability Zones are independent of each other
- Create subnets inside Availability zones
- Inside subnets create/place your EC2 instances
- **EC2 = Virtual Servers**



Steps to Connect VPCs to the Internet





Choosing an IP address range

IP Address Range that we will use in this example

Classless Inter-Domain Routing: CIDR

16 bit is the network address

CIDR notation review

CIDR range example:

172.31.0.0/16

1010 1100 0001 1111 0000 0000 0000 0000

Choosing an IP address range for your VPC



172.31.0.0/16

How to choose an IP Address Range

Use a long range (16 bit network address), and avoid overlap with other networks that you might want to connect to

Choosing an IP address range for your VPC

VPC

Avoid ranges that overlap with other networks to which you might connect.

172.31.0.0/16

Recommended:
RFC1918 range

Recommended:
/16
(65,536 addresses)

How to assign IPv6 IP address range

Configure to use IPV6. However, you do not need to manually assign. IPv6 will be assigned automatically.

Subnet mask in the image 56 bit

The EC2 instance will communicate using IPv4 or IPV6 address depending on the env.

IPv6 in Amazon VPC – Dual-stack

VPC

172.31.0.0/16

2001:db8:1234:1a00::/56

Amazon Global Unicast Addresses (GUA) – Internet Routable

Associate an /56 IPv6 CIDR (Automatically allocated)

VPC subnets and Availability Zones

Availability zones in a Region



Subnets and Availability Zones with IP address Ranges

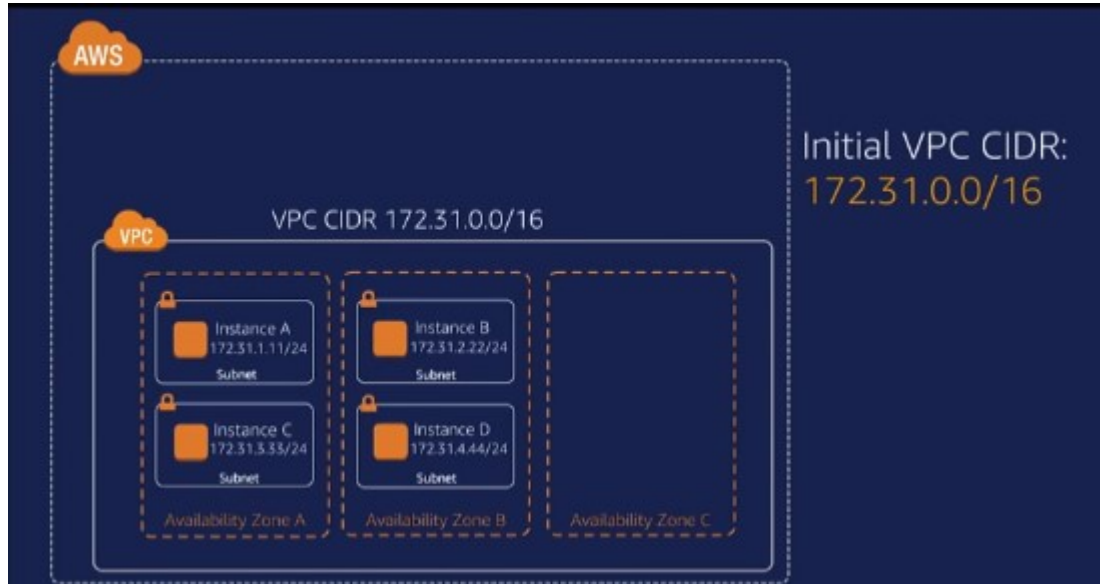
Note: 24 bit mask. Networks: 172.31.0, 172.31.1, 172.31.2



Expand your existing Amazon VPC

Extend IP address range or
Extend to an additional Availability Zones

Problem Case:



Solution:

Go to VPC and ask for another CIDR range. Use the new CIDR range in the new Availability zone.



VPC subnet recommendations



- **/16** VPC (65,536 addresses)
- **Expand** your VPC when necessary
- At least **/24** subnets (251 addresses)
- Use **multiple Availability Zones** per VPC through multiple subnets

Start big such as /16 VPC address range



Route to the Internet

Routing in your VPC

- **Route tables** contain rules for which packets go where
- Your VPC has a **default** (main) route table
- But, you can assign **different route tables** to different subnets

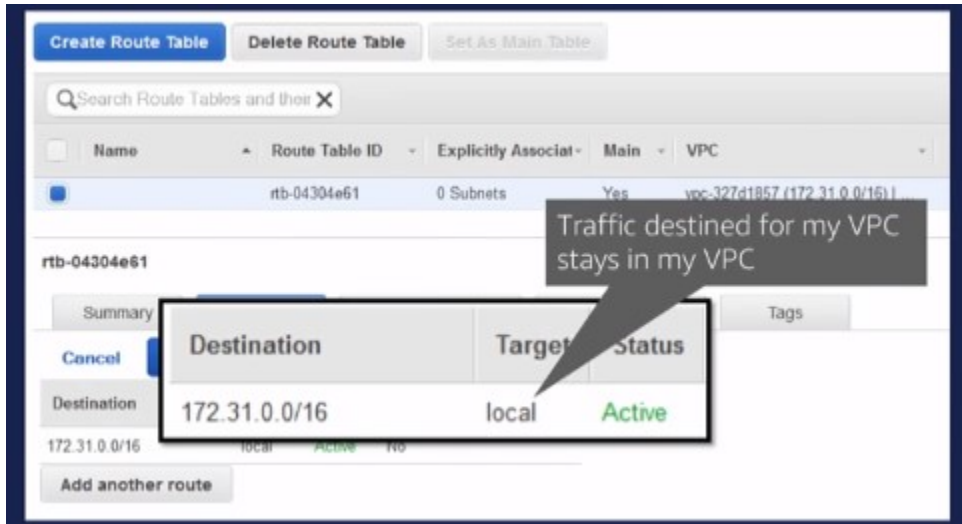
Main Route Table

Traffic destined for any VPC IP range will stay inside that VPC.

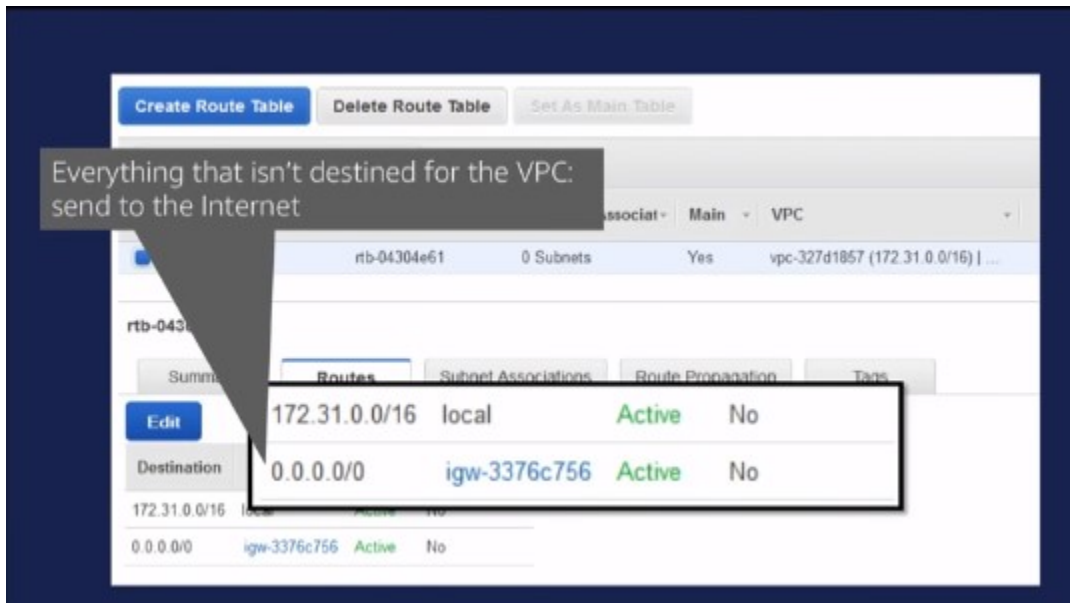
When destination is outside, the packets will drop.

To send packets to outside, we need to create an Internet Gateway.

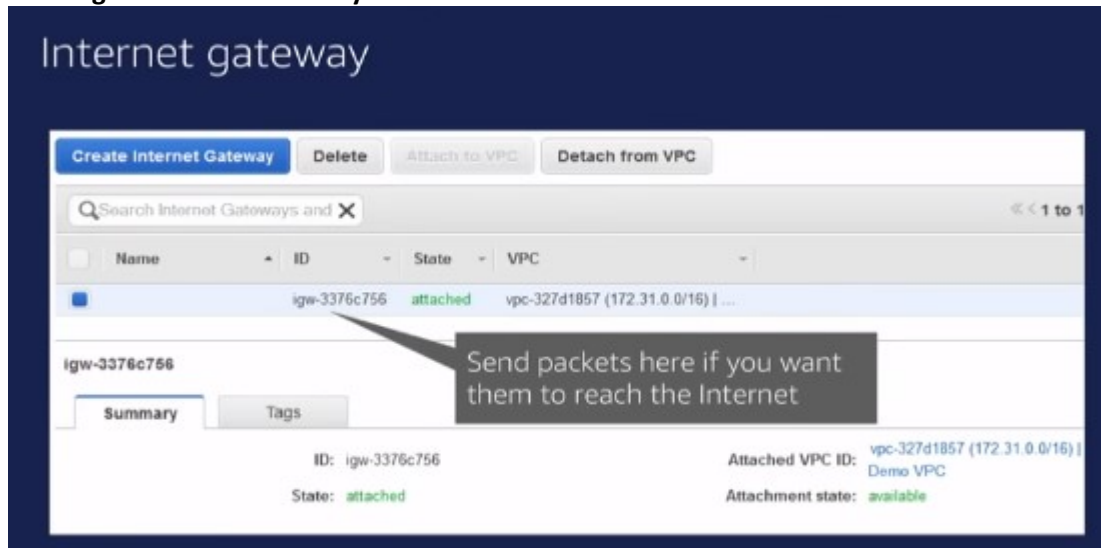
And then create another route table entry here



Igw in the image is the internet gateway. IGW is an Amazon object. You will be able to create using UI.



Creating an Internet Gateway



The Internet Gateway – provides bi-directional communication to/from the internet.

Network security in your VPC: Security groups

Internet gateway opens door to both way traffic. We have opened stuff from routing point of view. We did not open anything yet from security point of view.

However, we need to use security to stop traffic that we do not want.

Two types of security

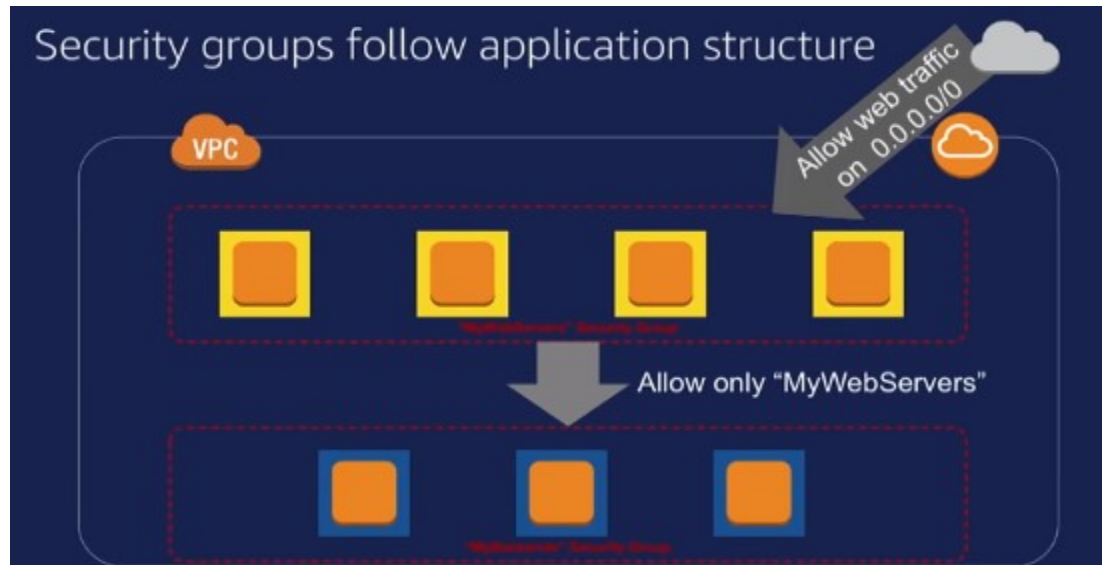
1. NAC (Network Access Control)
2. Security Groups

One Good Approach to provide security

Two layer security.

First layer, only web-servers that can be accessed on port 80 from the internet.

2nd layer, backend services such as databases that can be only accessed from the first layer – not from the internet



First layer – security configuration for web-servers.

Two entries. One for IPv4, another for IPv6

Security groups example: Web servers

Create Security Group Actions

search vpc-5995ce3e Add filter

Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/> WebServersGroup	sg-067c927d	MyWebServers	vpc-5995ce3e	Group for web servers
<input type="checkbox"/> BackendsGroup	sg-a57896d1	MyBackends	vpc-5995ce3e	Group for backend hosts
<input type="checkbox"/>	sg-1c7c9267	default	vpc-5995ce3e	default VPC security group

Security Group: sg-067c927d

Description Inbound Outbound Tags

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Allow all HTTP traffic
HTTP	TCP	80	:::0	Allow all HTTP traffic

Rule descriptions

© 2016 Amazon Web Services, Inc. or its affiliates. AWS SUMMIT

2nd layer security

Allow the first layer security group to access the backend services

Security groups example: Backends

The screenshot shows the AWS Management Console interface for security groups. At the top, there's a 'Create Security Group' button and an 'Actions' dropdown. Below is a search bar with the text 'search : vpc-5999ce3e'. A table lists three security groups:

Name	Group ID	Group Name	VPC ID	Description
WebServersGroup	sg-067c927d	MyWebServers	vpc-5999ce3e	Group for web servers
BackendsGroup	sg-aa7896d1	MyBackends	vpc-5999ce3e	Group for backend hosts
	sg-1c7c9267	default	vpc-5999ce3e	

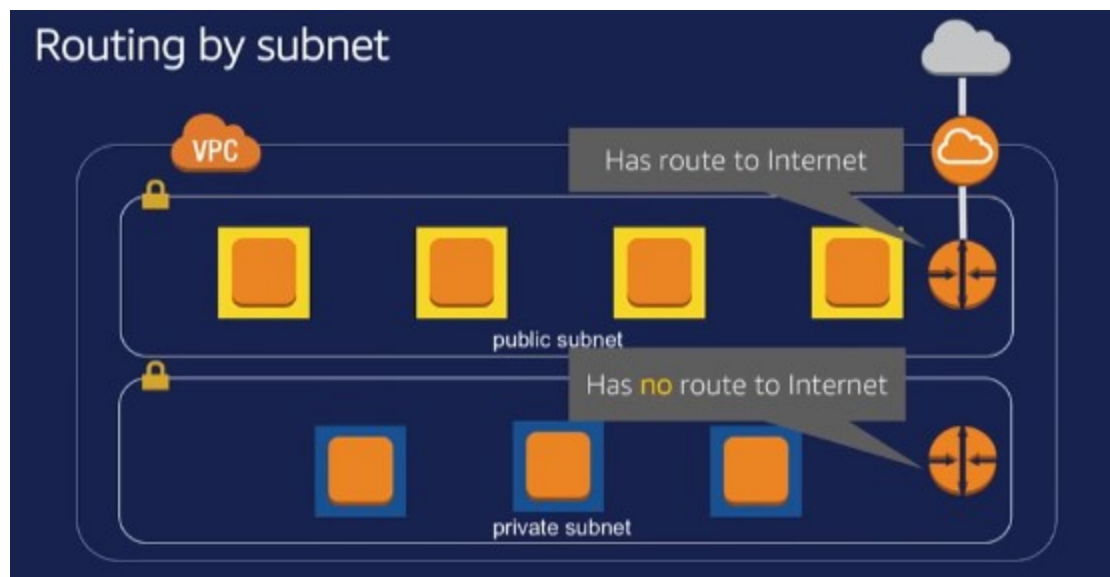
Below the table, the 'Security Group: sg-aa7896d1' is selected, showing its 'Inbound' rules. The rules table is as follows:

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-067c927d (MyWebServers)	Allow traffic from...
Custom TCP Rule	TCP	2345	sg-067c927d (MyWebServers)	Allow traffic from...

A callout bubble points to the 'Source' column of the first rule, containing the text: 'Allow application traffic from web servers only'.

Though we can close the data communications (to the internet or not) completely using Security Groups. You might want to use routing level blocking as well for different reasons.

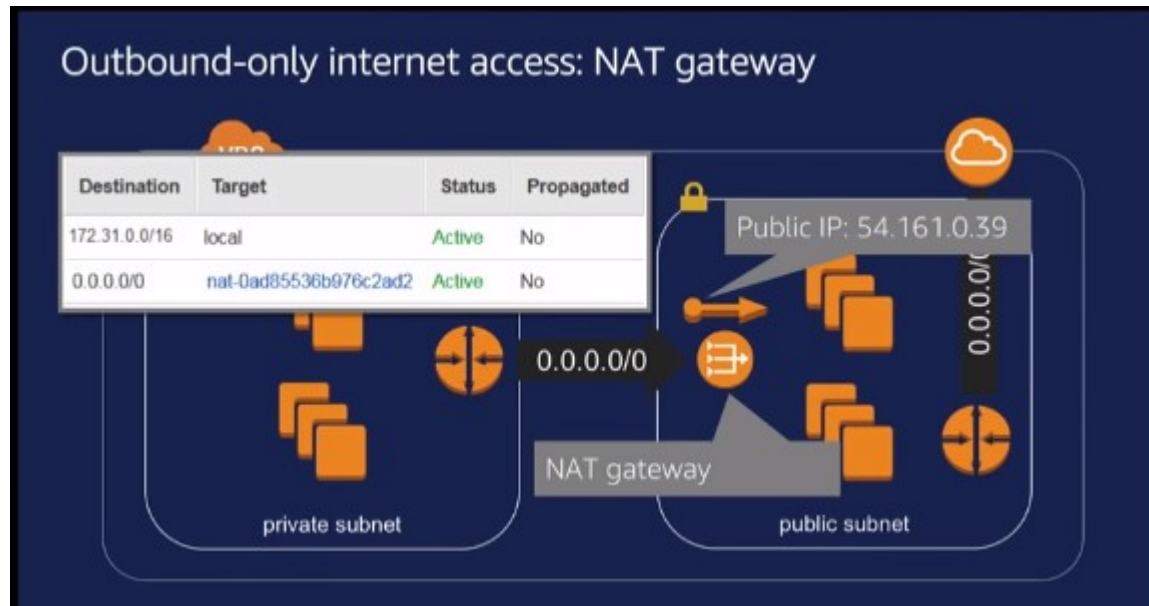
Modify Route Tables to control Internet Access



Provide internet access to the private subnet through NAT.

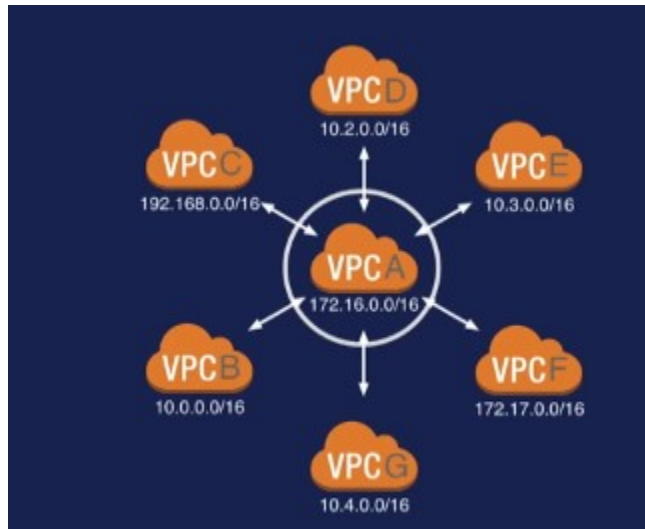
However, they (private subnets) cannot be accessed from the internet.

Private subnets can access internet through the NAT gateway. NAT gateways will be in the public subnet. On private subnet routing table, give a route where destination is the internet (0.0.0.0/0) and target is the NAT. NAT will not be a single point of failure (Amazon will take care of high availability of NAT)



Inter-VPC connectivity: VPC peering

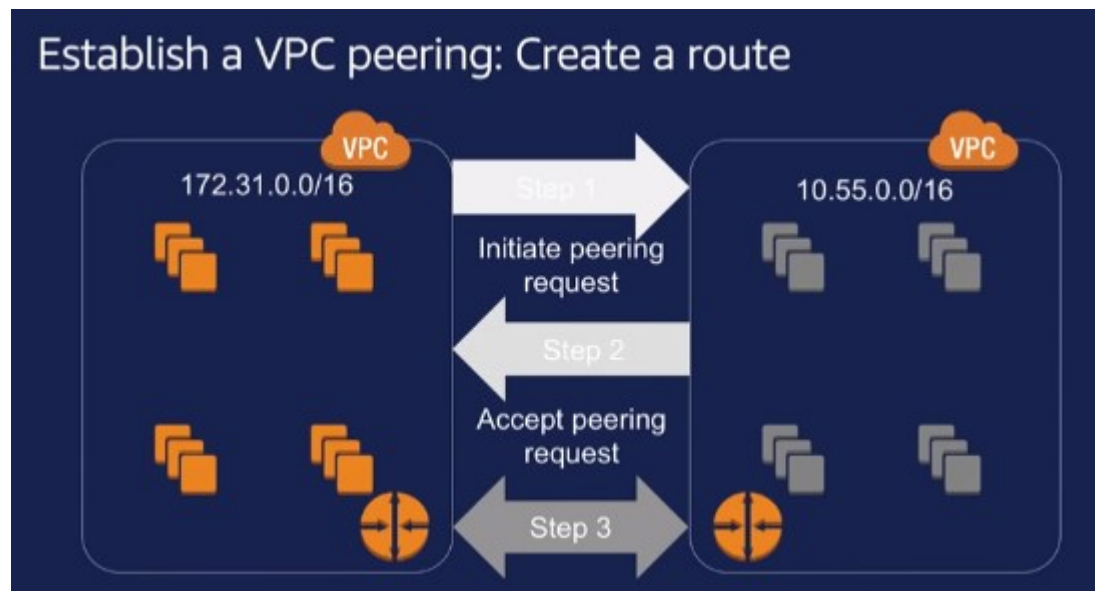
Example VPC peering use:
Shared services VPC



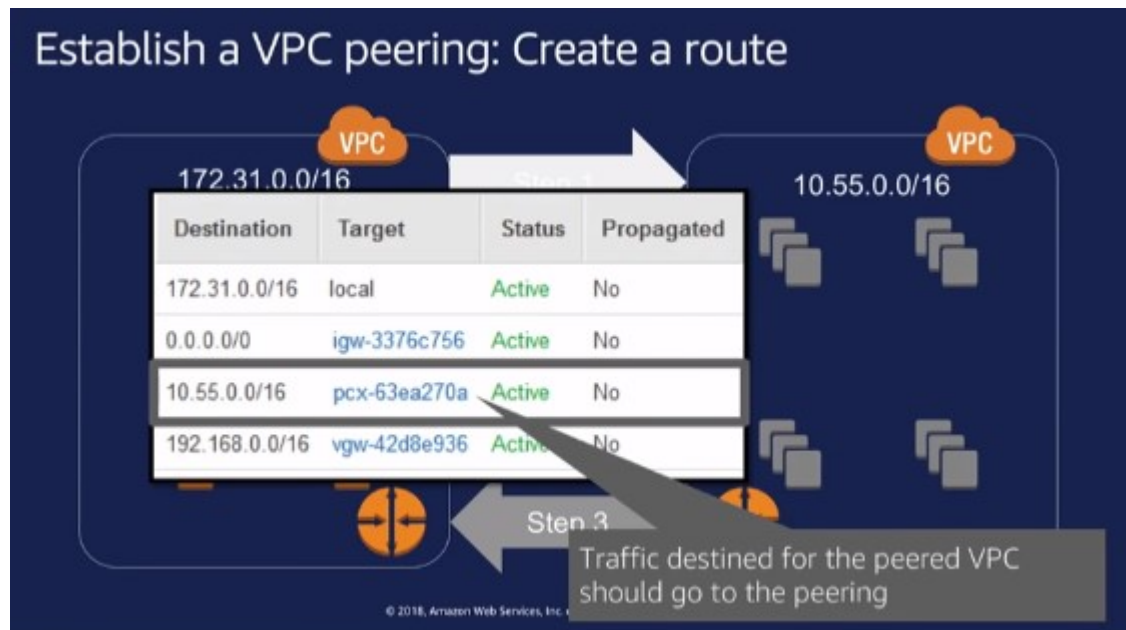
- Common/core services

- Authentication/directory
- Monitoring
- Logging
- Remote administration
- Scanning

The following image is showing, 3 steps out of 4 in VPC peering.
3rd step is the routing adjustment. 4th step is the Security Group Adjustment.

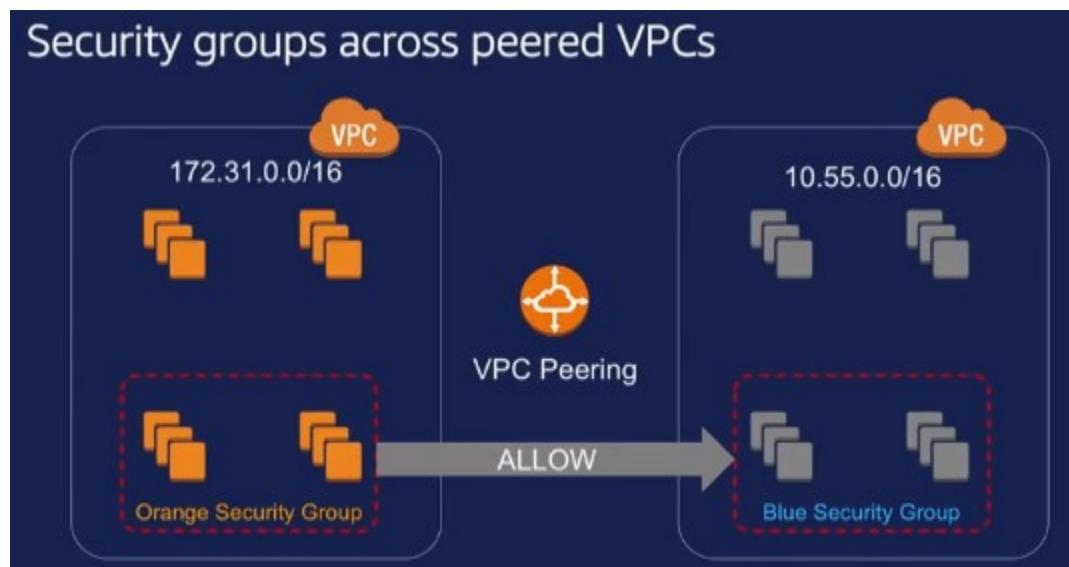


3rd step of VPC peering – create route table entries.

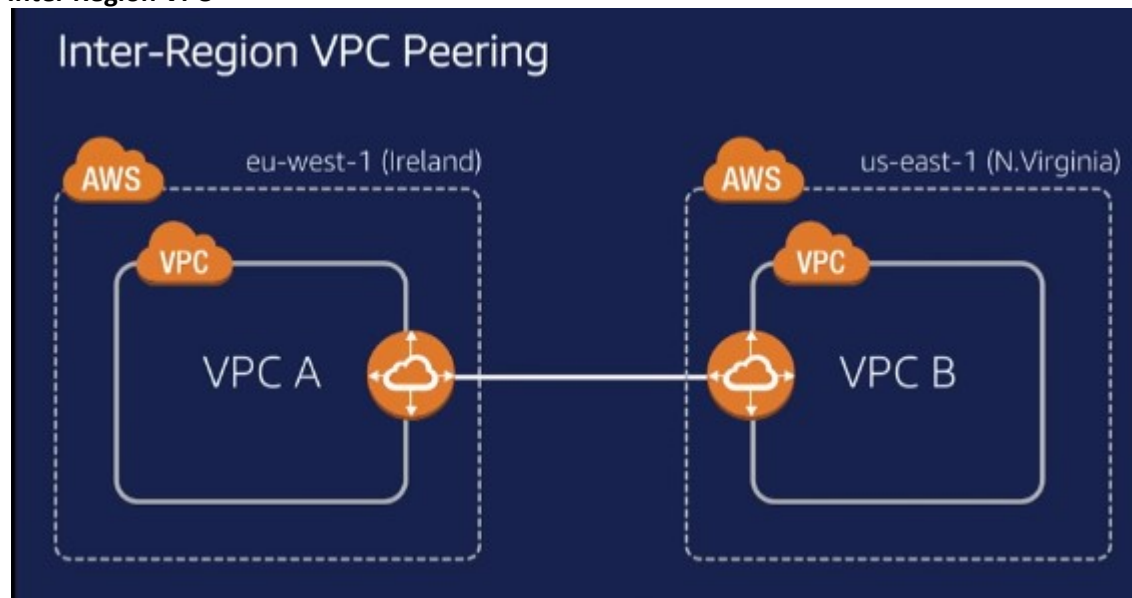


Security Groups and VPC Peering

When VPC peering is established, one VPC can use the security groups of another VPC. In the image, Blue security group can be configured to use the Orange security group



Inter Region VPC



Some notes...

Inter-Region VPC Peering **encrypts** with no single point of failure or bandwidth bottleneck

Traffic using Inter-Region VPC Peering always **stays on the global AWS backbone**

Connecting to on-premises networks: AWS Virtual Private Network and AWS Direct Connect

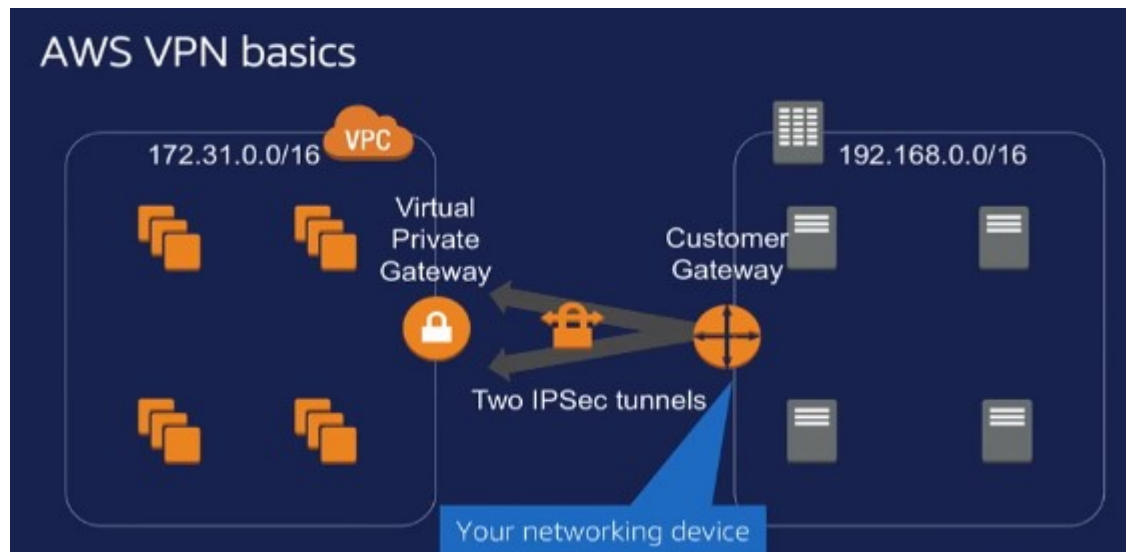
AWS VPN

Create end points on both sides.

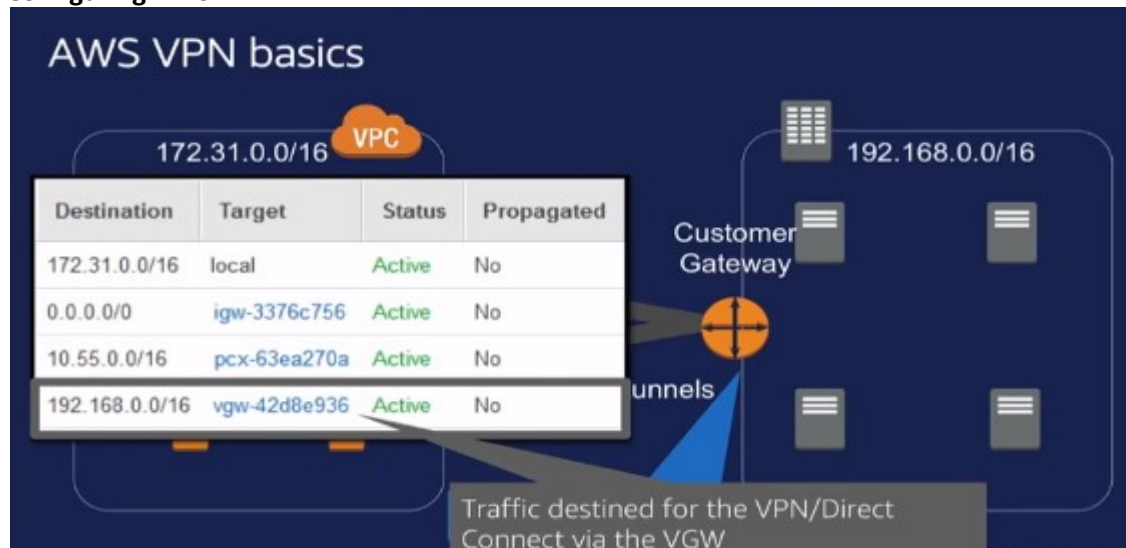
Customer Gateway – On Prem Side

Virtual Private Gateway on the AWS side

Connect using IPsec Tunnels



Configuring AWS VPN

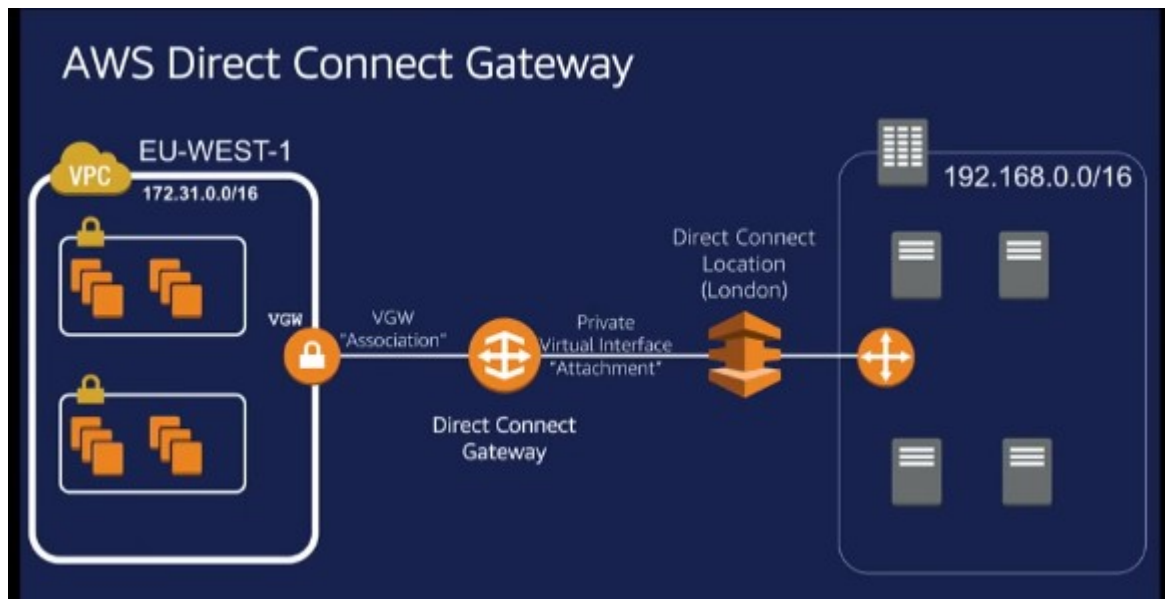


Propagated table/column might show BGP or similar when BGP is configured.

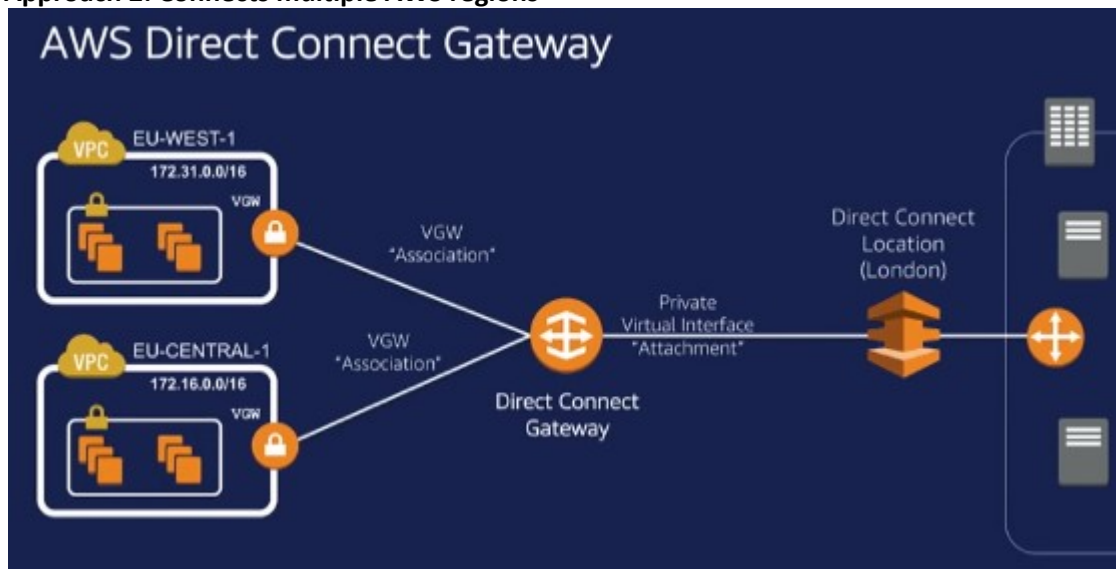
VPN is over the internet.

AWS direct connect is the another approach and technically better approach.

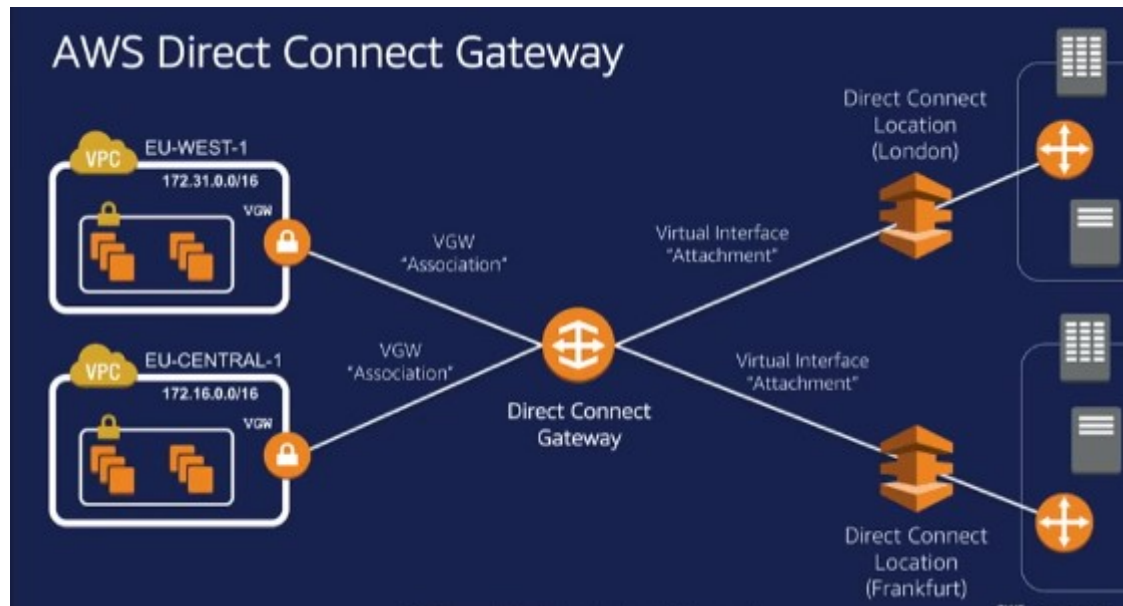
One of Multiple approaches of AWS Direct Connect. Direct connect Gateway can even be 3rd party



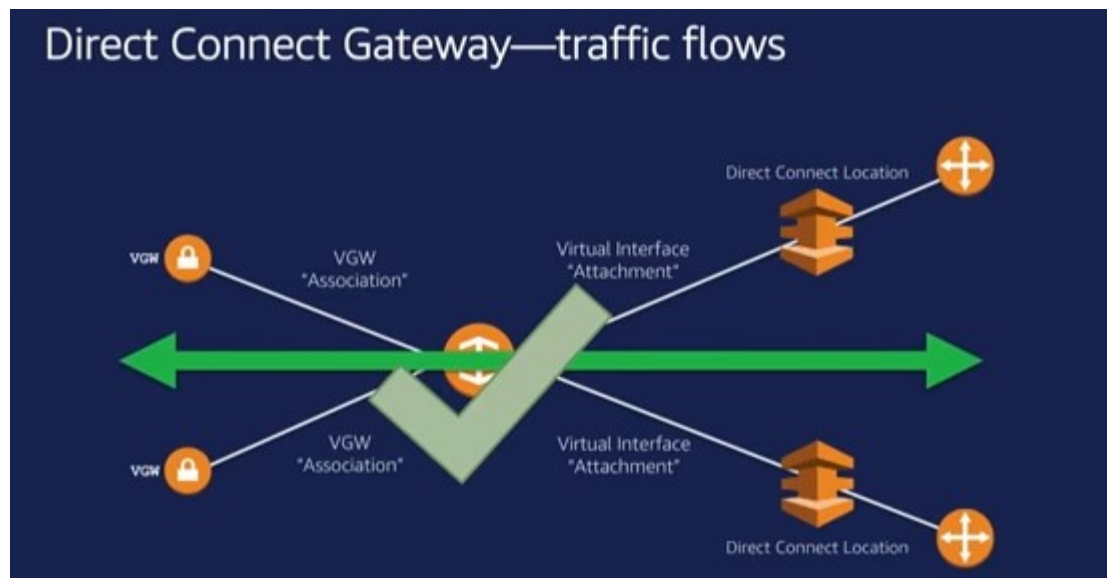
Approach 2: Connects multiple AWS regions



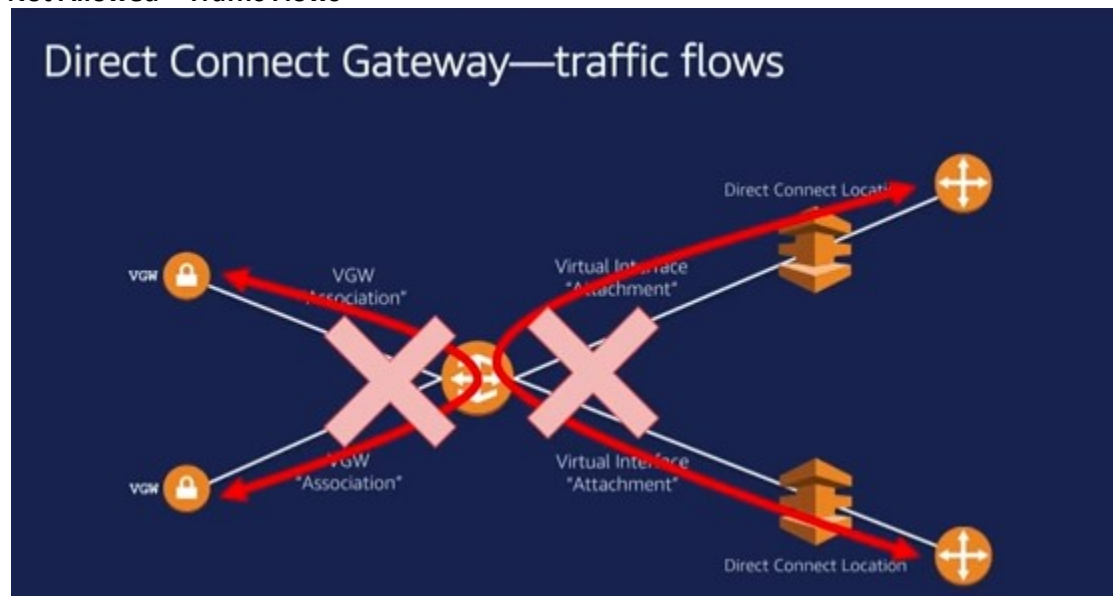
3rd approach – when data centers are in different locations – we might want to use multiple AWS direct connect gateways



AWS Direct Connect – Allowed Traffic Flows for the 3rd approach



Not Allowed – Traffic Flows



Use Both approaches of On-Prem connection

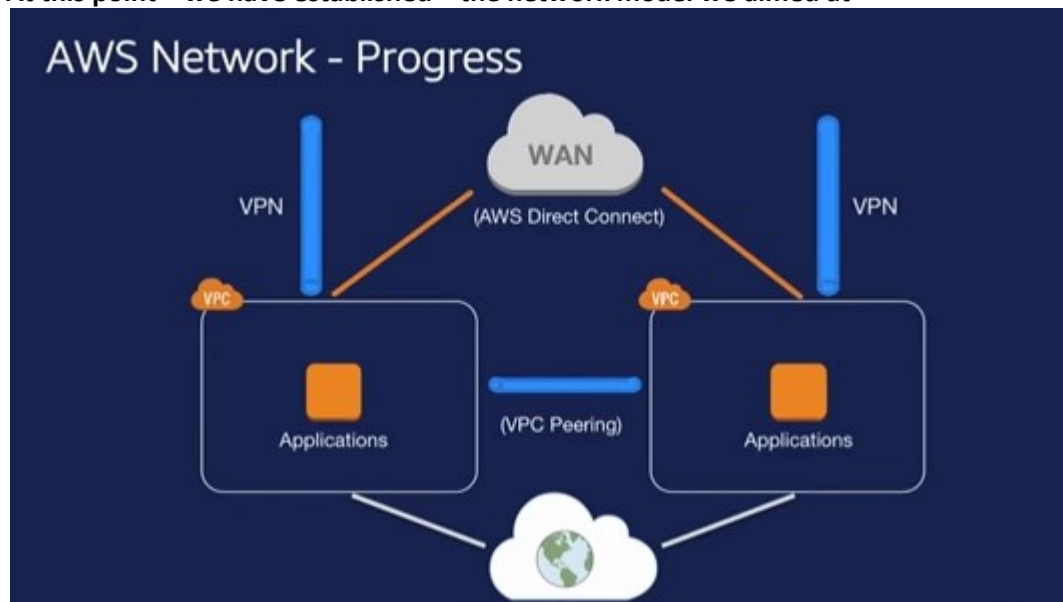
use VPN as a backup. Tools are there for fail-safe and switching

AWS VPN and AWS Direct Connect

- Both allow **secure connections** between your network and your VPC
- **VPN** is a pair of IPSec tunnels over the Internet
- **AWS Direct Connect** is a dedicated line with lower per-GB data transfer rates
- For **highest availability**: Use both

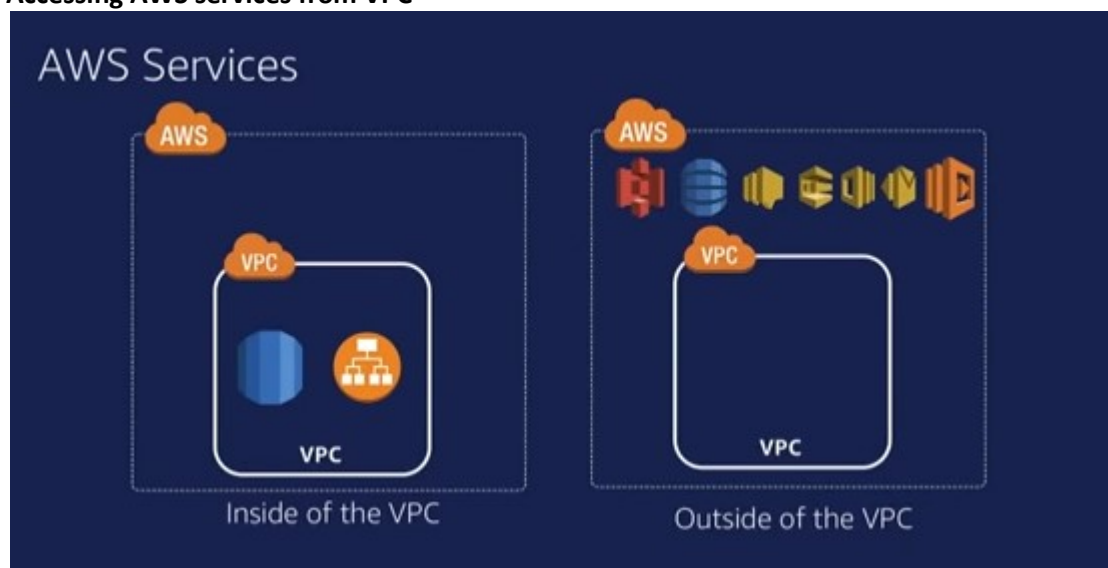


At this point – we have established – the network model we aimed at



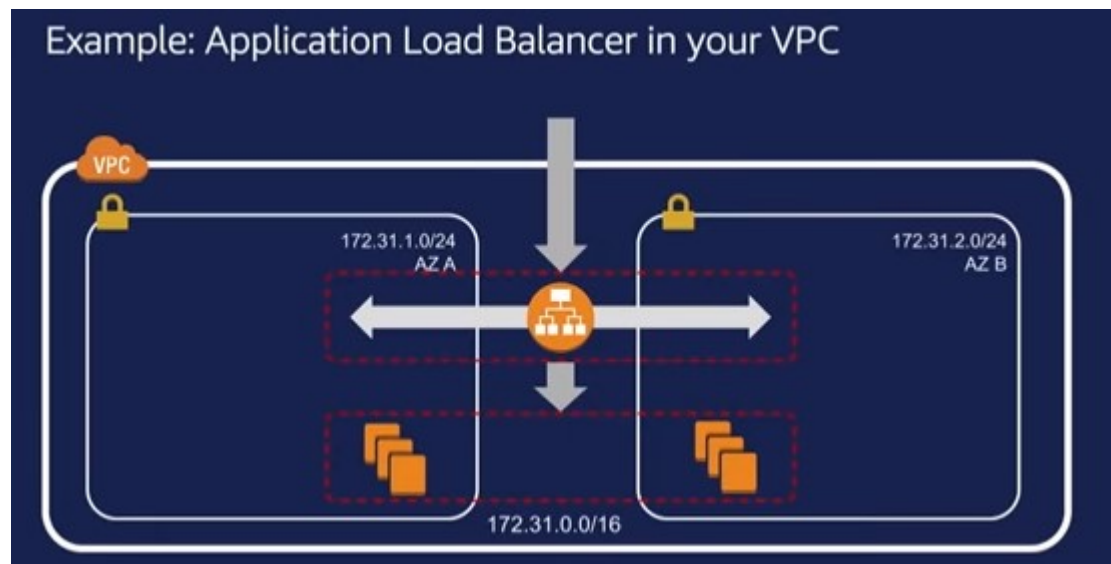
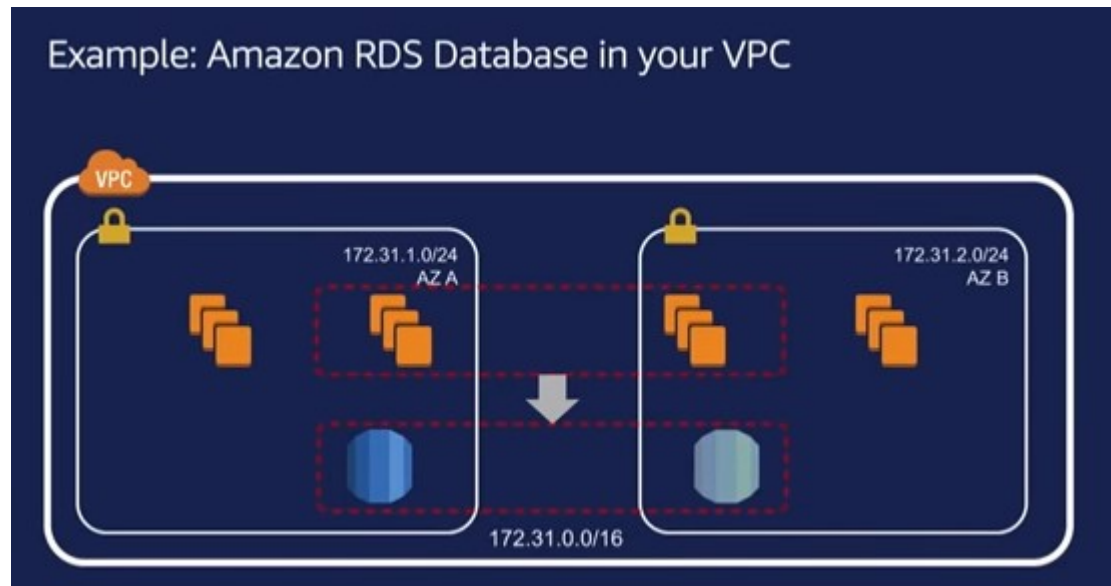
So the network model is there. Now, how do you connect to and use different services. Some services run inside VPC such as RDS, Elastic Load balancers. Many run outside such as S3, DynamoDB

Accessing AWS services from VPC



RDS service and Load Balancer: AWS Service Access from VPC Example

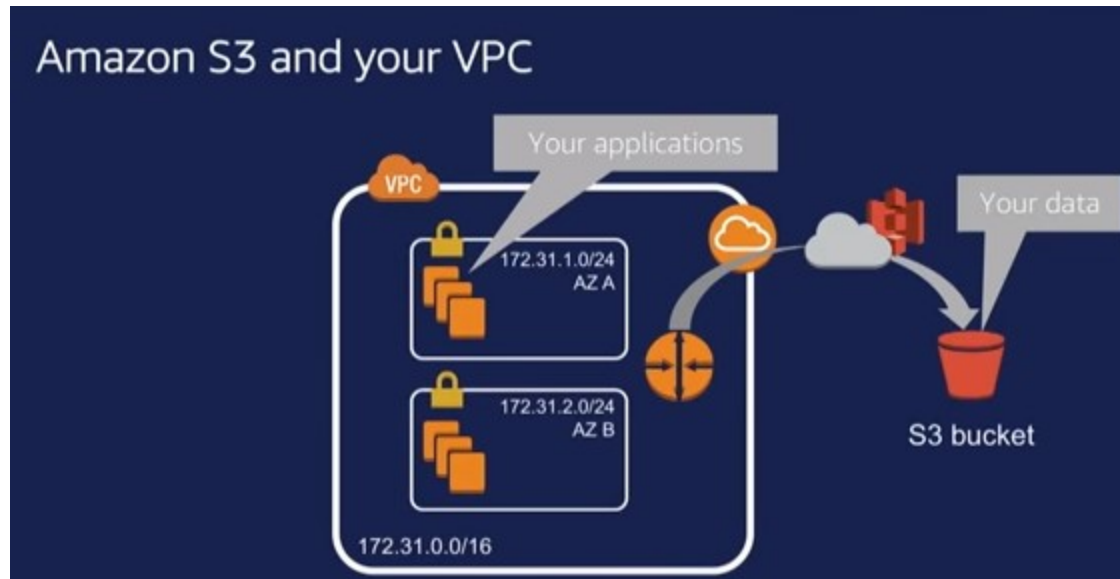
Note: there are multiple availability zones



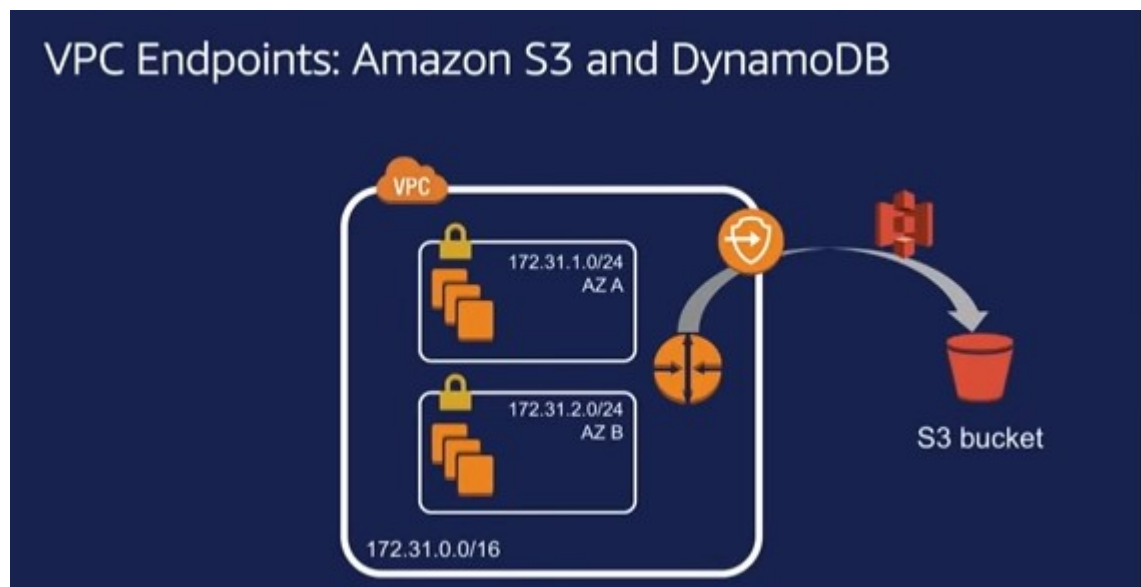
Access External AWS services from your VPC

Use external AWS services from your VPC when you have an IGW (Internet Gateway)

If you do not have IGW, you can use AWS endpoints (example will be coming). AWS endpoints in general have some advantages over IGW.



Access external (to your VPC) services using Endpoint (first type, there is another type of Endpoint)



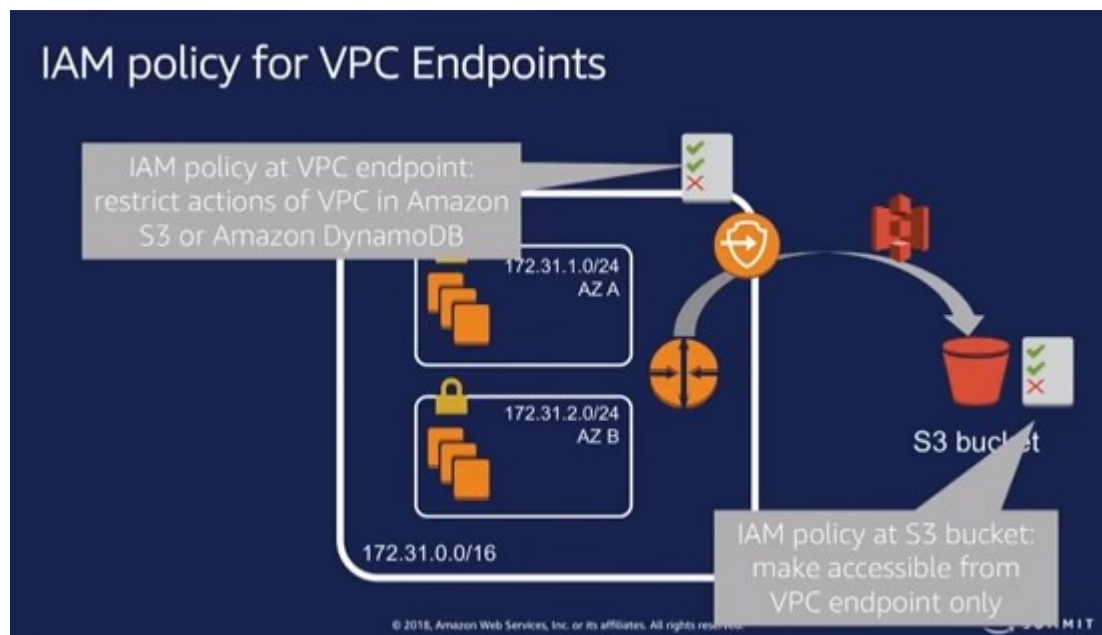
One advantage of Endpoint (over IGW), it keeps track of the dynamically changing S3 bucket IP addresses

Endpoint Entries

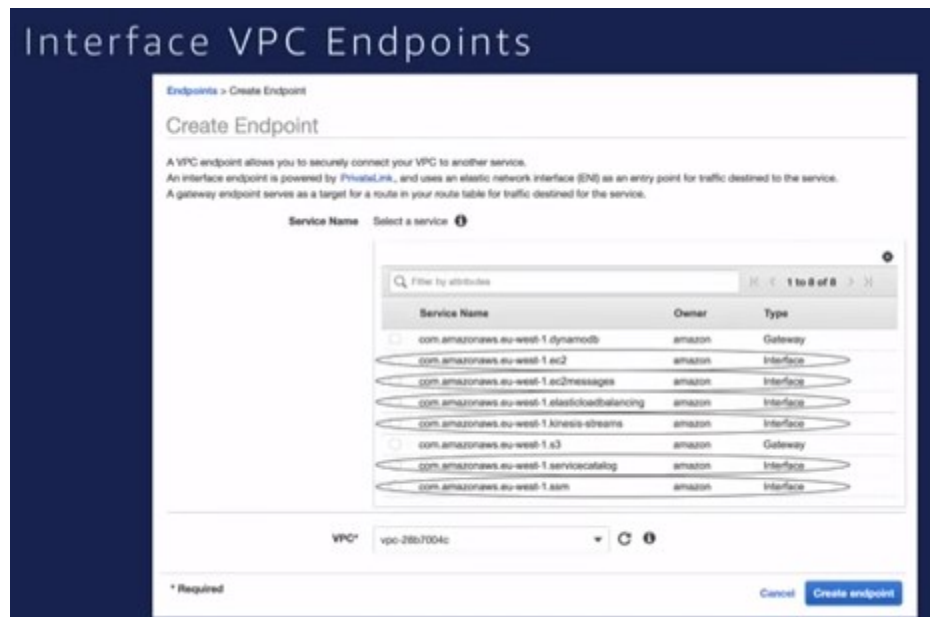


IAM Policies at the End Point Level

Another Advantage of Endpoint: you can apply IAM policies both at the Endpoint level and S3 bucket (external service) level

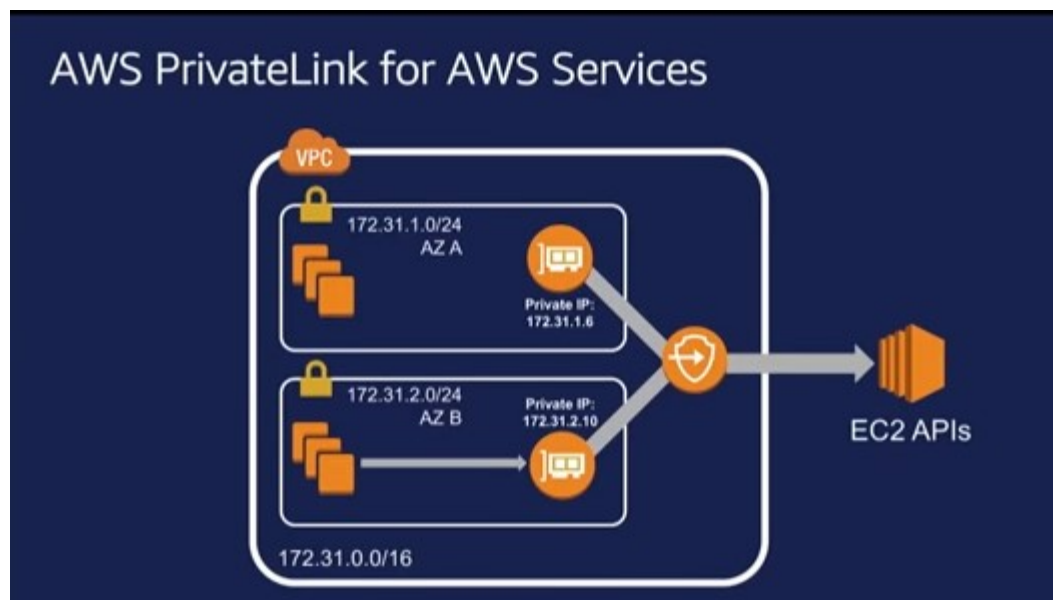


Interface VPC endpoints



Interface VPC Endpoints

Notice the newly created network interfaces inside availability zones. These provides high availability. Interface endpoints use PrivateLink technologies. Using this technology, you can offer your own Services.



Privatelink and External (external to AWS) services using Interface Endpoints

AWS PrivateLink for Customer & Partner Applications

Share services privately and securely between VPCs, AWS accounts, and on-premises networks



- 
Powered by Network Load Balancer
- 
Secure endpoint within Client VPC
- 
Integrated with AWS Marketplace

Customers and partners



Available in all public AWS regions, except CN-NORTH-1

VPC Flow Logs: VPC traffic metadata in Amazon CloudWatch Logs

It's not about traffic and packets but about Meta Data

VPC Flow Logs

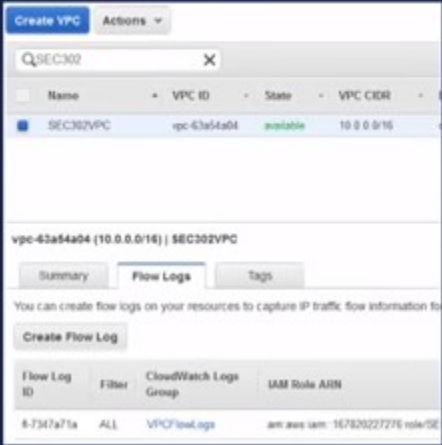


The diagram illustrates a VPC with a CIDR of 172.31.0.0/16. It contains two subnets: AZ A (172.31.1.0/24) and AZ B (172.31.2.0/24). Both subnets have a security group icon. Arrows from these subnets point to a central icon representing a log or data storage, which then points to a green 3D bar chart icon, symbolizing analysis or visualization of the flow log data.

- **Visibility** into effects of security group rules
- **Troubleshooting** network connectivity
- Ability to **analyze** traffic

Where to enable VPC flow Logs

VPC Flow Logs: Setup



The screenshot shows the AWS VPC console interface. At the top, there's a 'Create VPC' button and an 'Actions' dropdown. Below is a search bar with 'SEC302' entered. A table lists VPCs, with 'SEC302VPC' (vpc-43a54a04) in a 'available' state, having a CIDR of 10.0.0.0/16. Below the table, the details for 'vpc-43a54a04 (10.0.0.0/16) | SEC302VPC' are shown. The 'Flow Logs' tab is selected, displaying a 'Create Flow Log' button. Below this, a table shows the configuration for the flow log: Flow Log ID is 'fl-7347a71a', Filter is 'ALL', CloudWatch Logs Group is 'VPCFlowLogs', and IAM Role ARN is 'arn:aws:iam:167826227276:role/SE'.

Name	VPC ID	State	VPC CIDR
SEC302VPC	vpc-43a54a04	available	10.0.0.0/16

vpc-43a54a04 (10.0.0.0/16) | SEC302VPC

Summary Flow Logs Tags

You can create flow logs on your resources to capture IP traffic flow information for

Create Flow Log

Flow Log ID	Filter	CloudWatch Logs Group	IAM Role ARN
fl-7347a71a	ALL	VPCFlowLogs	arn:aws:iam:167826227276:role/SE

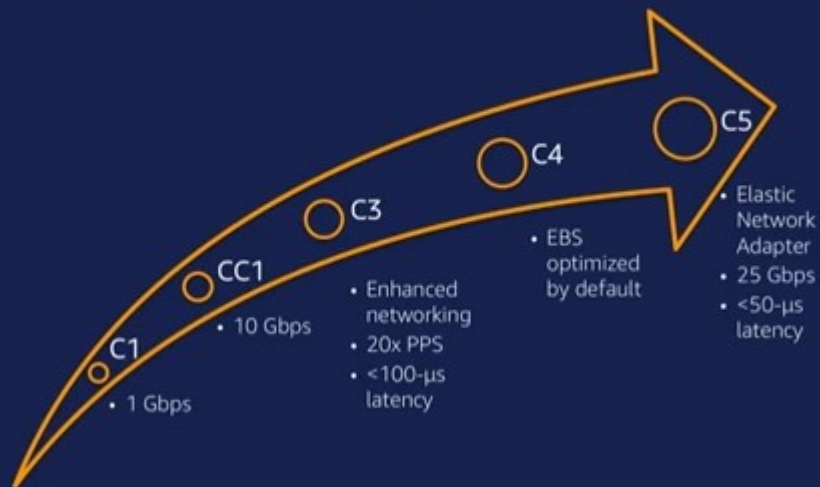
VPC Flow log data and what do they mean

VPC Flow Logs data in CloudWatch Logs

[illegible]

Misc AWS

On-Instance Networking Improvements



Instance Bandwidth Limits



25 Gbps
within placement group



25 Gbps
within region



25 Gbps
to Amazon S3



5 Gbps
for other sources

Time Sync Service

Amazon Time Sync Service

Highly reliable service with a redundant array of satellite and atomic clock sources

Available globally today!

