Networking Principles - Bird Eye View

Why multi-Cloud?

Quite a debatable topic as there are two communities with strong opinions, we should NOT go multi-cloud & we should GO multi-cloud. My personal opinion, no one can decide based on personal perceptions but let the use case decide if it really makes sense to go multi-cloud or not.

In one or other sense, we have been using multi-* since quite long.

For e.g.

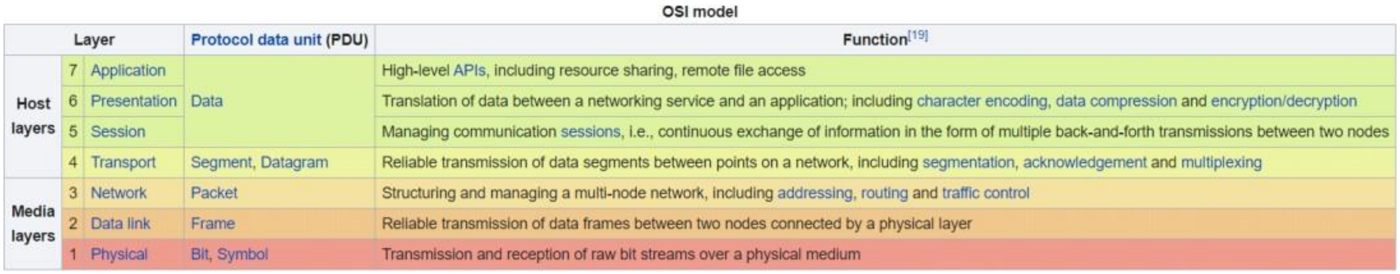
An enterprise will have combination of Cisco and Brocade switches, they may have multiple hypervisors like VMware and KVM/Xen, they may have blend of Dell and Cisco UCS hardware. Why so? Well, could be because of :

- Avoid or minimize vendor locking
- Cost governance and optimization
- Better disaster recovery
- Lastly, the most important aspect: "Get best of breed" for the supported use case

Likewise, same is applicable for Cloud environment. Modern applications leverage best of the breed services from various cloud environment to build best possible consumable service which is optimized for performance, user experience while reducing overall cost using various services from multi-cloud strategy.

There is lot to study, analyze on this topic but I will park this for some other day. I just wanted to touch base on topic to set the context and giving a basic idea of why using multi-cloud.

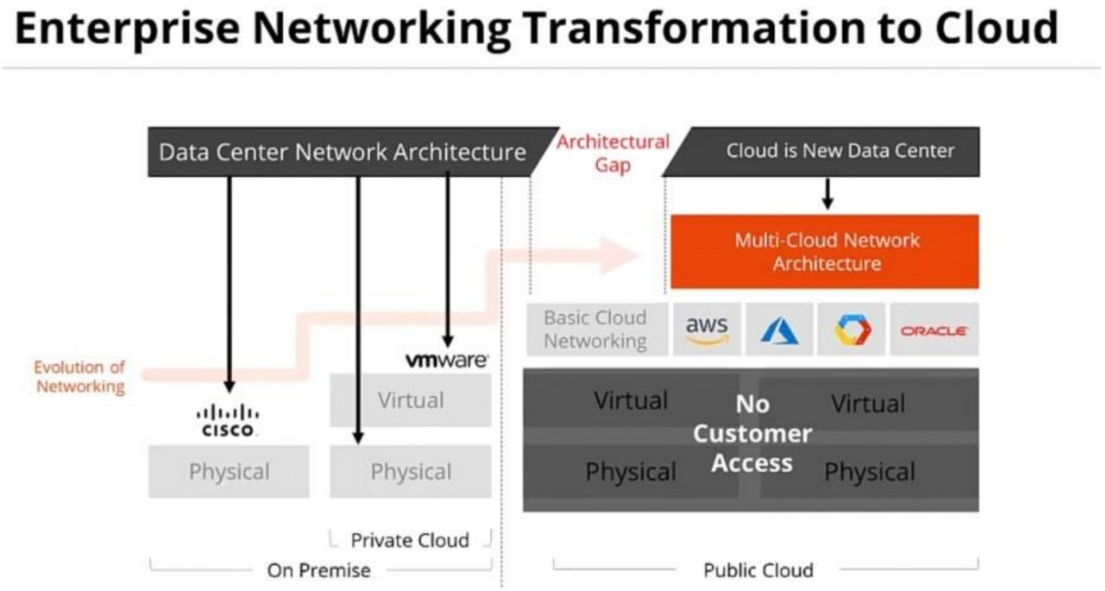
Basics of networking :: OSI Layers



OSI model

Layer			Protocol data unit (PDU)	Function[19]
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

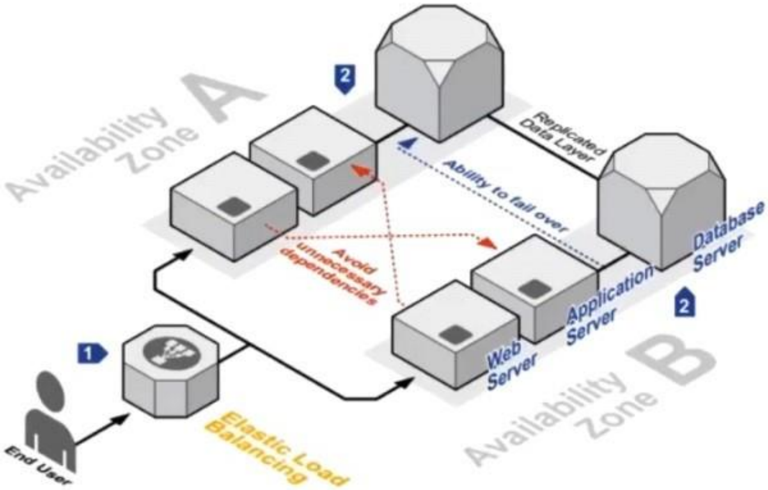
Embarking cloud journey

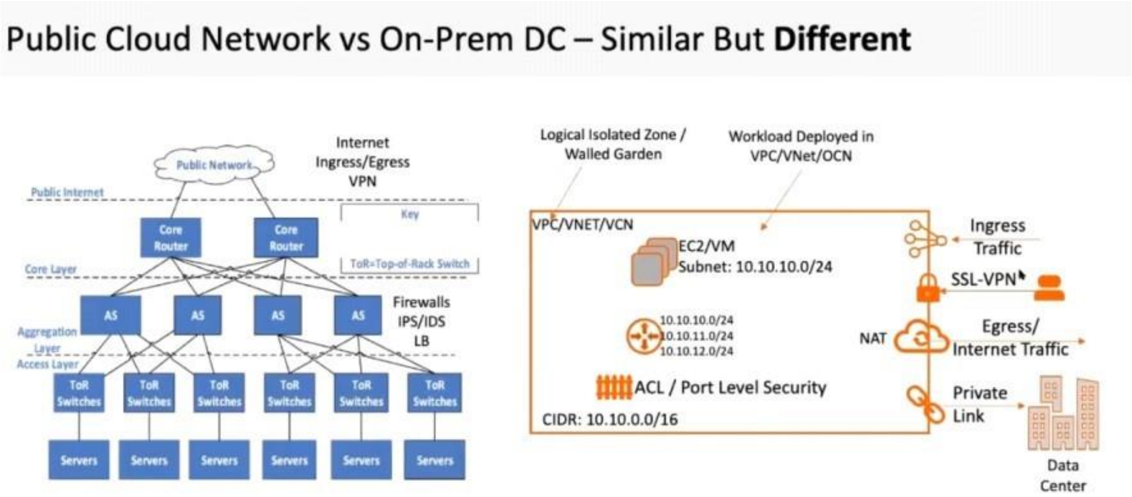


Some key terms of cloud to begin with:

- Regions
- Availability zones and Availability Sets
- Zonal services and Regional Services
- VPC/VNET/VCN
- Peering/Transit

Typical example for Availability zones:



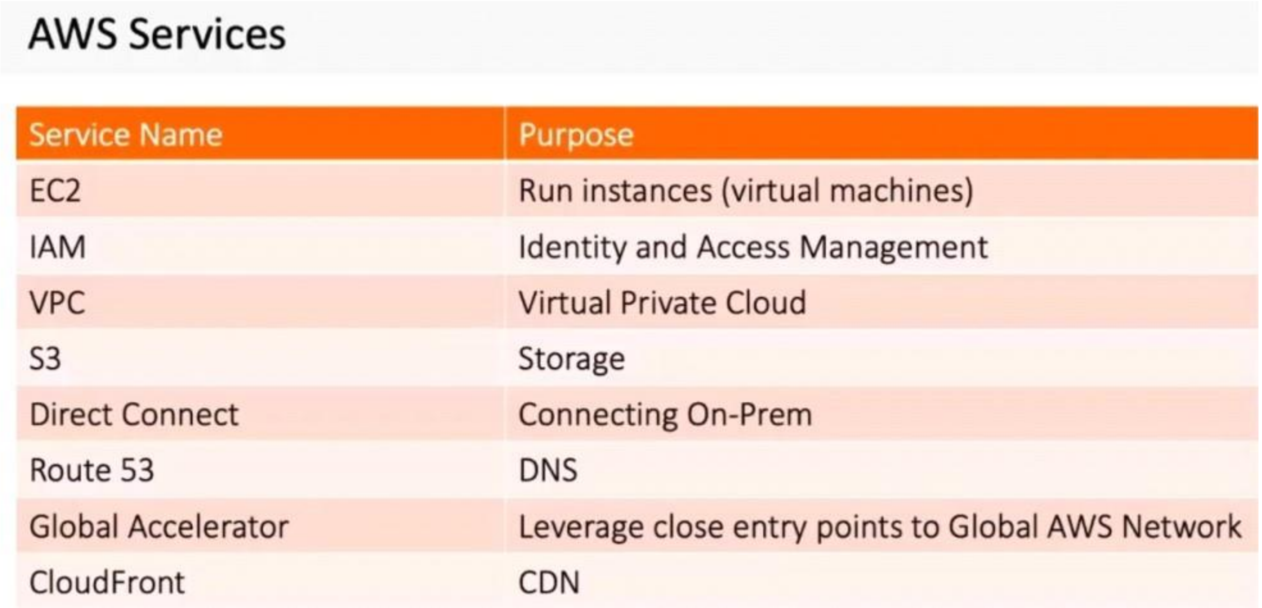


Public Cloud Network vs On-Prem DC – Similar But **Different**

★ **In today's leaf-spine topology, the ToR (Top-of-Rack) switches are the leaf switches and they are attached to the spine switches.**

AWS Networking 101

Before getting into networking one must understand the AWS services. Below are few most used AWS services.

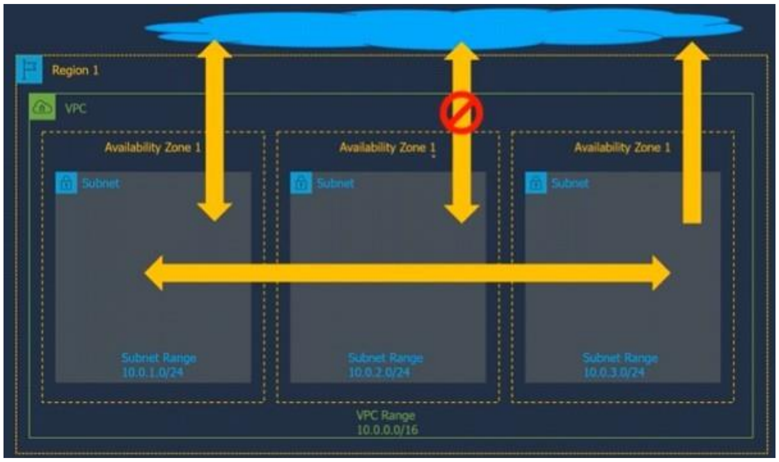


AWS Services

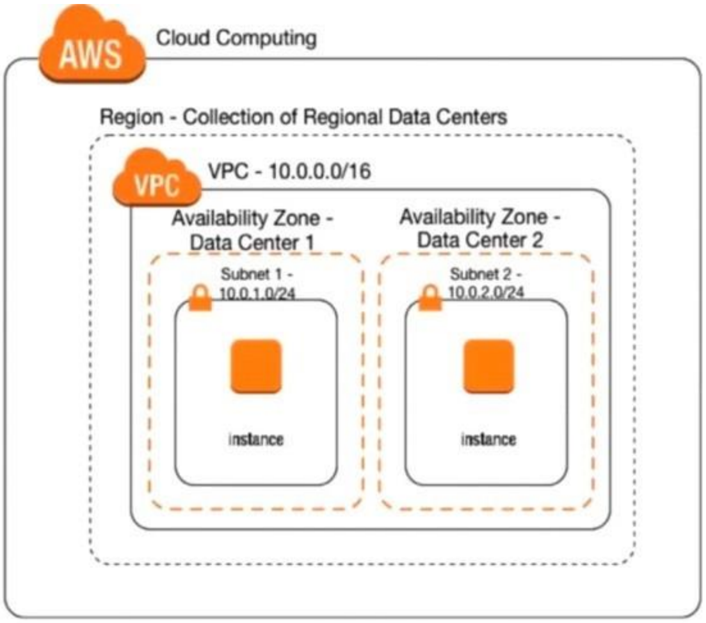
Service Name	Purpose
EC2	Run instances (virtual machines)
IAM	Identity and Access Management
VPC	Virtual Private Cloud
S3	Storage
Direct Connect	Connecting On-Prem
Route 53	DNS
Global Accelerator	Leverage close entry points to Global AWS Network
CloudFront	CDN

AWS Cloud networking 5 rules:

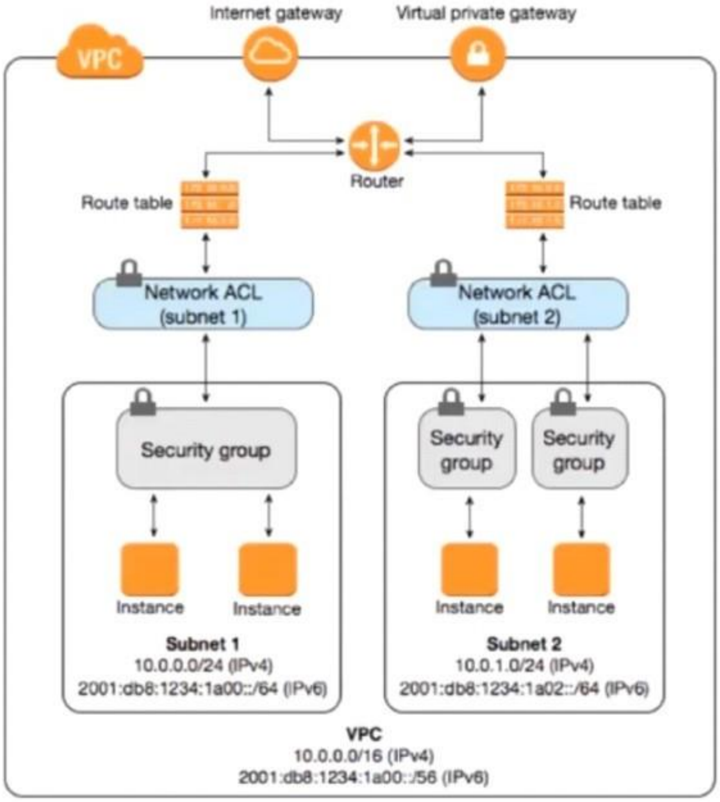
1. **Scope**:
   a. VPC limited to single region
   b. Subnet limited to single datacenter (availability zone)
2. **Size**:
   a. /16 is maximum size and /28 is minimum size in AWS.
   b. Create a bigger range like /16 for VPC so you can slice network into multiple subnets.
3. **IP Addressing**:
   a. Use any RFC 1918 (10.0.0.0, 172.16.0.0, 192.168.0.0) a.k.a. private IP ranges.
4. **Reserved IP addresses**:
   a. Any network always reserved at least **2** IP addresses stating as "network address and GW address" and "broadcast address" and AWS also reserved some IP addresses like, DNS, Reserved for future hence total 5 IP addresses are always reserved in AWS (**first 4 and last IP**) the subnet formula is = $2^{32 - n} - 5$
5. **Subnet Properties**:
   a. Every subnet have their own purpose and properties. Like, what kind of subnets are they? (Public or Private)
   b. Two way, No way and One way.
   c. Two way - internet can talk to your VM and VM can talk to Internet. No Way - Complete isolation and One Way - VM can talk to internet but not vice-e-versa.
   d. Access among subnets (internal access)



Let's understand AWS VPC at a very broader level:


AWS
Cloud Computing
Region - Collection of Regional Data Centers
VPC
VPC - 10.0.0.0/16
Availability Zone - Data Center 1
Availability Zone - Data Center 2
Subnet 1 - 10.0.1.0/24
Subnet 2 - 10.0.2.0/24
instance
instance

Let's take a look at security pieces:

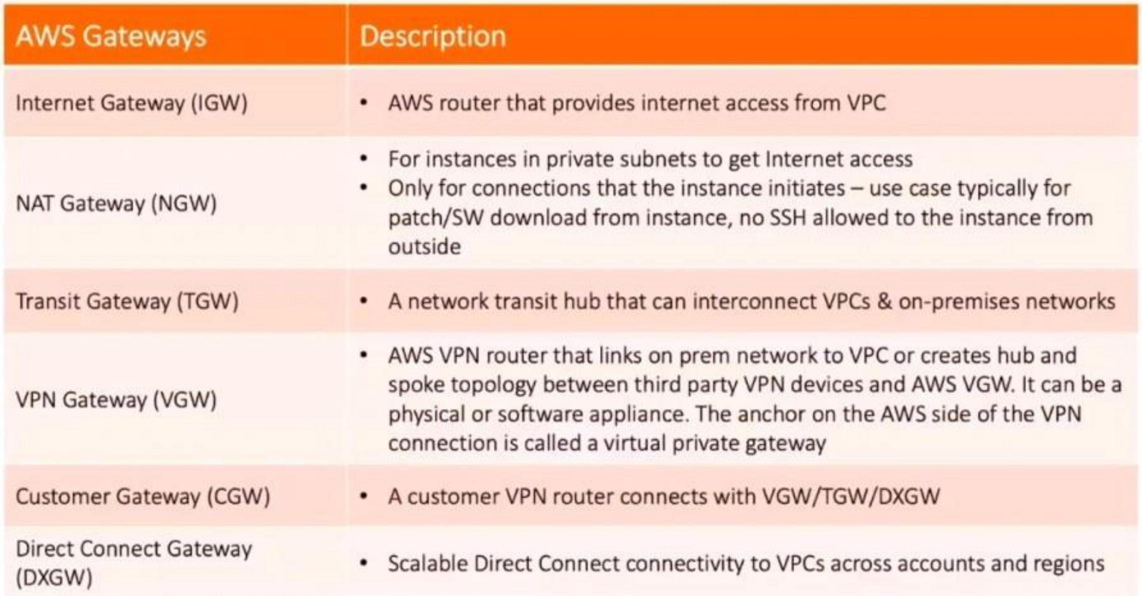


There are two main components as far as basic security concerned.

- Security Group
  - Can be only used within VPC. It's not a global resource available across multiple VPCs
  - But SG can be shared across peered VPCs
  - Best practice is to have dedicated SG per EC2 instance
  - SG is stateful

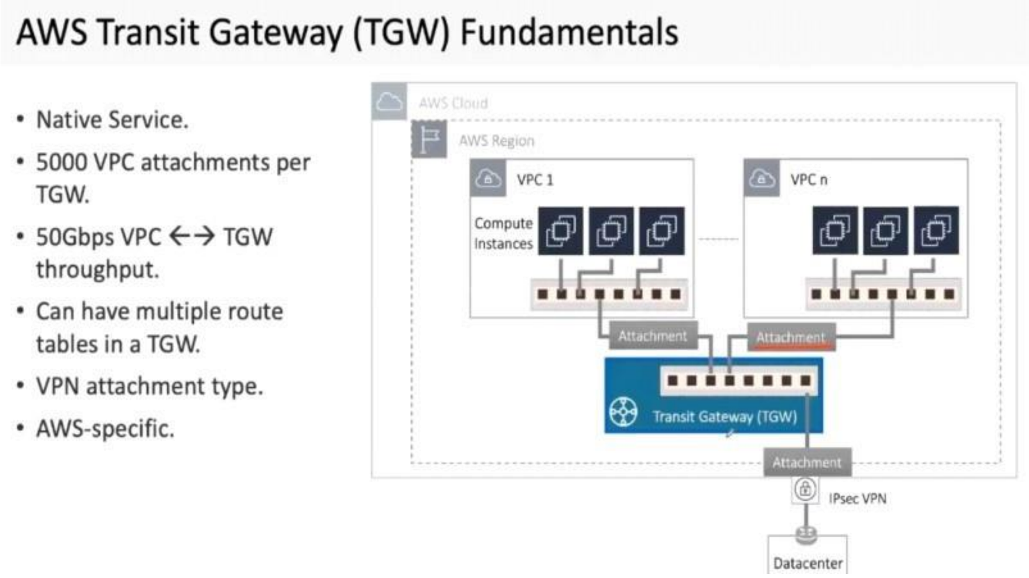
- NACL
  - At subnet level
  - NACLs are stateless

Different types of gateways:



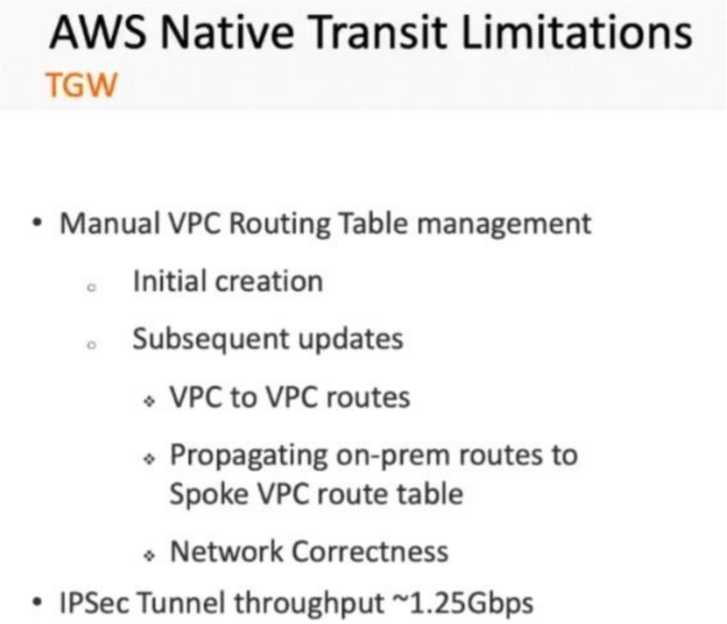
AWS Gateways	Description
Internet Gateway (IGW)	• AWS router that provides internet access from VPC
NAT Gateway (NGW)	• For instances in private subnets to get Internet access • Only for connections that the instance initiates – use case typically for patch/SW download from instance, no SSH allowed to the instance from outside
Transit Gateway (TGW)	• A network transit hub that can interconnect VPCs & on-premises networks
VPN Gateway (VGW)	• AWS VPN router that links on prem network to VPC or creates hub and spoke topology between third party VPN devices and AWS VGW. It can be a physical or software appliance. The anchor on the AWS side of the VPN connection is called a virtual private gateway
Customer Gateway (CGW)	• A customer VPN router connects with VGW/TGW/DXGW
Direct Connect Gateway (DXGW)	• Scalable Direct Connect connectivity to VPCs across accounts and regions

TGW:



AWS Transit Gateway (TGW) Fundamentals

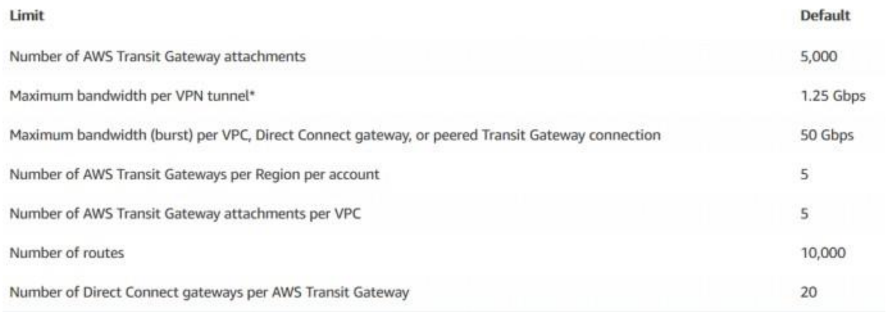
- Native Service.
- 5000 VPC attachments per TGW.
- 50Gbps VPC <-> TGW throughput.
- Can have multiple route tables in a TGW.
- VPN attachment type.
- AWS-specific.



AWS Native Transit Limitations

TGW

- Manual VPC Routing Table management
  - Initial creation
  - Subsequent updates
    - VPC to VPC routes
    - Propagating on-prem routes to Spoke VPC route table
    - Network Correctness
- IPSec Tunnel throughput ~1.25Gbps



Limit	Default
Number of AWS Transit Gateway attachments	5,000
Maximum bandwidth per VPN tunnel*	1.25 Gbps
Maximum bandwidth (burst) per VPC, Direct Connect gateway, or peered Transit Gateway connection	50 Gbps
Number of AWS Transit Gateways per Region per account	5
Number of AWS Transit Gateway attachments per VPC	5
Number of routes	10,000
Number of Direct Connect gateways per AWS Transit Gateway	20

How Aviatrix is helping here?

- Aviatrix manages and controls the AWS TGW which removes the routing limitations.
- Aviatrix takes care of the initial configuration of the routes and any updates.
- It helps to simplify the BGP over Direct Connect.
- Aviatrix provides network correctness and propagates all the on-prem routes to the VPCs.

As we learned, AWS TGW makes peering of VPC's easier BUT it does not make routing easy. Attaching AWS TGW to VPC does not propagate routes to the VPCs. Also, route propagation isn't supported for routes in TGW to VPC route table. VPC RT needs to be updated with static route to send traffic to TGW.

The formula of how many route tables (routes) need to be managed, reviewed and updated when using a AWS Transit Gateway (TGW) is equal to:

n (s + r – 1)

where,

n is the number of VPCs attached to the AWS Transit Gateway (TGW),
s is the number of subnets in each VPC
r is the number of route tables in the AWS Transit Gateway (TGW).

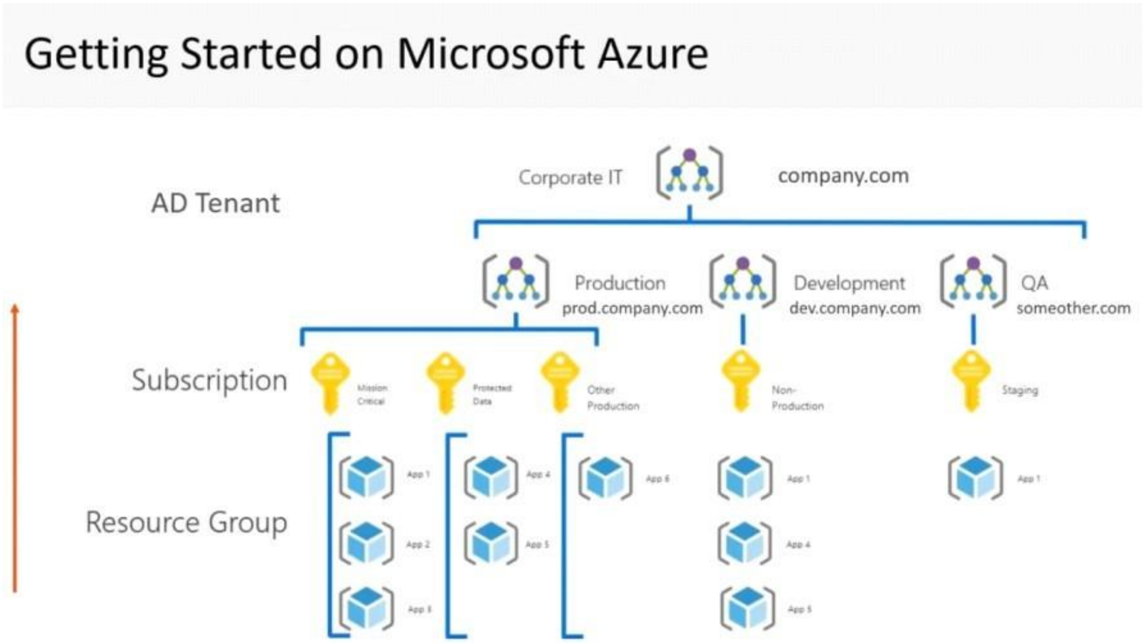
Let's take an example of a mid-size environment: if you have 20 VPCs with 4 subnets in each spread across 3 route tables, the total number of routes you need to manage, update and troubleshoot is:

20 (4 + 3 – 1) = 120 route entries.

NOTE: This does not include VPN and/or Direct Connect links from on-premises to the AWS Transit Gateway (TGW).

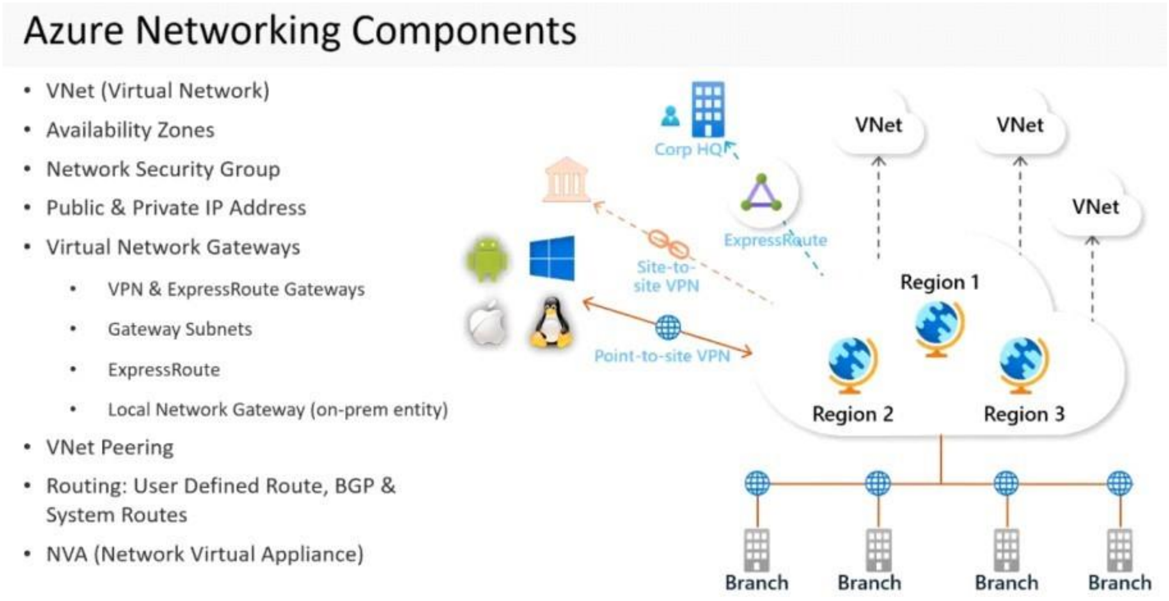
Aviatrix addresses all these challenges and hence AWS enlisted Aviatrix to collaborate making AWS Transit Gateway easier.

Azure Networking 101



Getting Started on Microsoft Azure

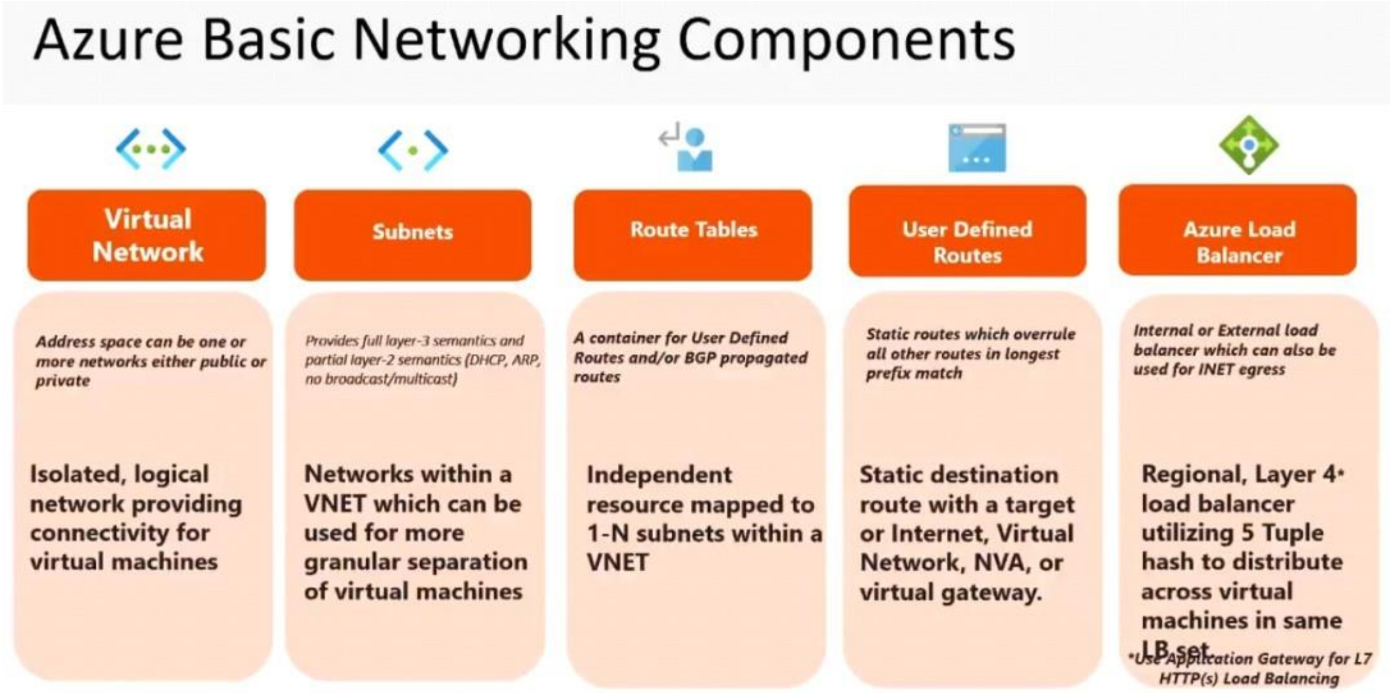
Subscriptions are used for charge-back analysis, billing etc.
Resource groups used to bundle the resources together.



Azure Networking Components

- VNet (Virtual Network)
- Availability Zones
- Network Security Group
- Public & Private IP Address
- Virtual Network Gateways
  - VPN & ExpressRoute Gateways
  - Gateway Subnets
  - ExpressRoute
  - Local Network Gateway (on-prem entity)
- VNet Peering
- Routing: User Defined Route, BGP & System Routes
- NVA (Network Virtual Appliance)

Subnets are private by default.



Azure Basic Networking Components

Virtual Network

Address space can be one or more networks either public or private

Isolated, logical network providing connectivity for virtual machines

Subnets

Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast/multicast)

Networks within a VNET which can be used for more granular separation of virtual machines

Route Tables

A container for User Defined Routes and/or BGP propagated routes

Independent resource mapped to 1-N subnets within a VNET

User Defined Routes

Static routes which overrule all other routes in longest prefix match

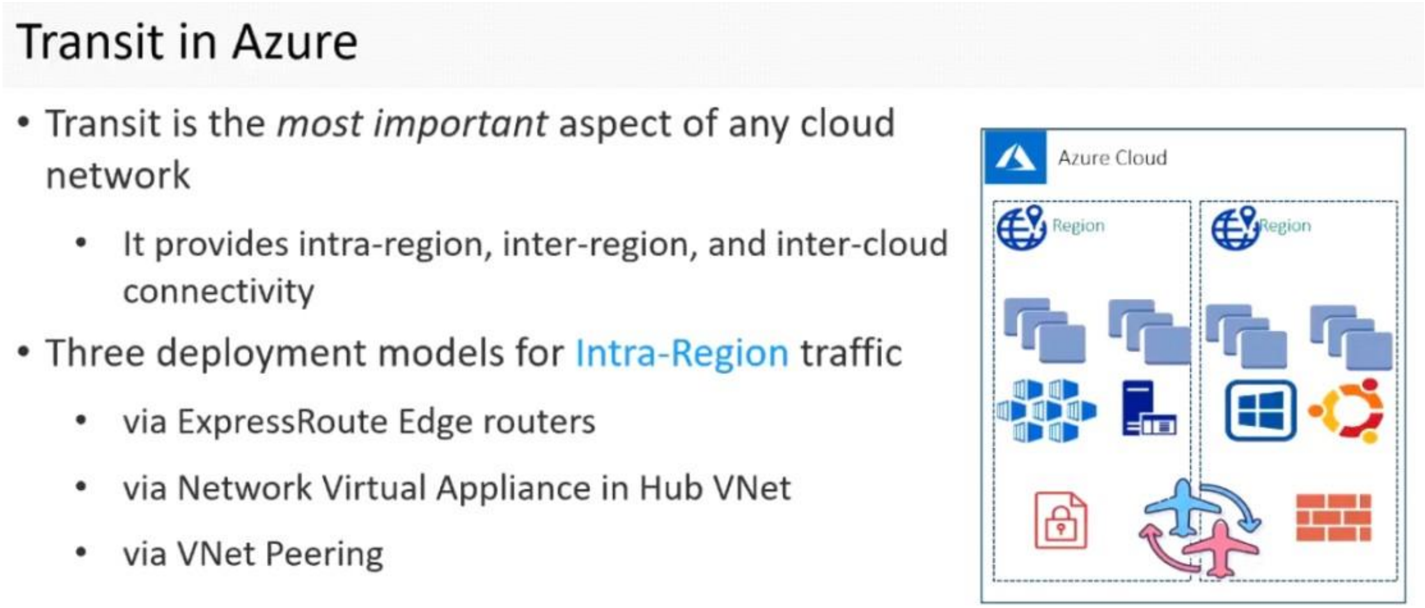
Static destination route with a target or Internet, Virtual Network, NVA, or virtual gateway.

Azure Load Balancer

Internal or External load balancer which can also be used for INET egress

Regional, Layer 4* load balancer utilizing 5 Tuple hash to distribute across virtual machines in same LB set

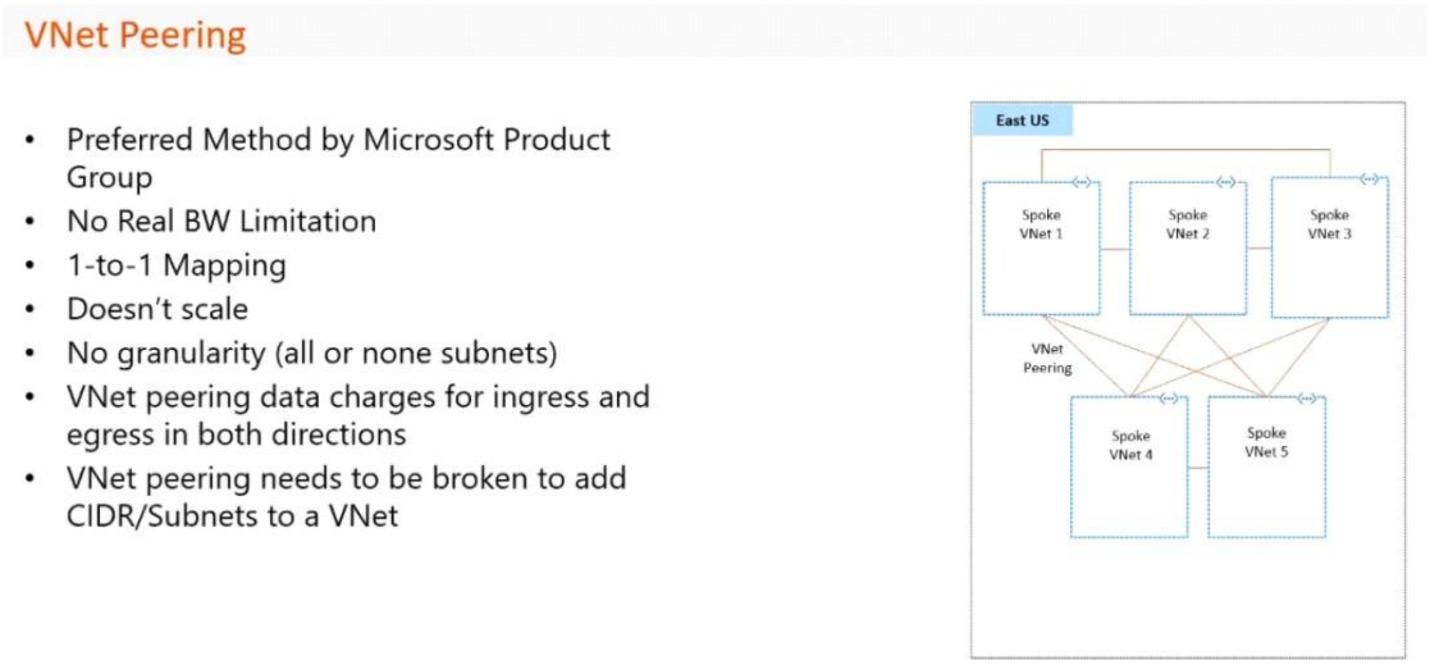
**Use Application Gateway for L7 HTTP(s) Load Balancing*



Transit in Azure

- Transit is the *most important* aspect of any cloud network
  - It provides intra-region, inter-region, and inter-cloud connectivity
- Three deployment models for Intra-Region traffic
  - via ExpressRoute Edge routers
  - via Network Virtual Appliance in Hub VNet
  - via VNet Peering

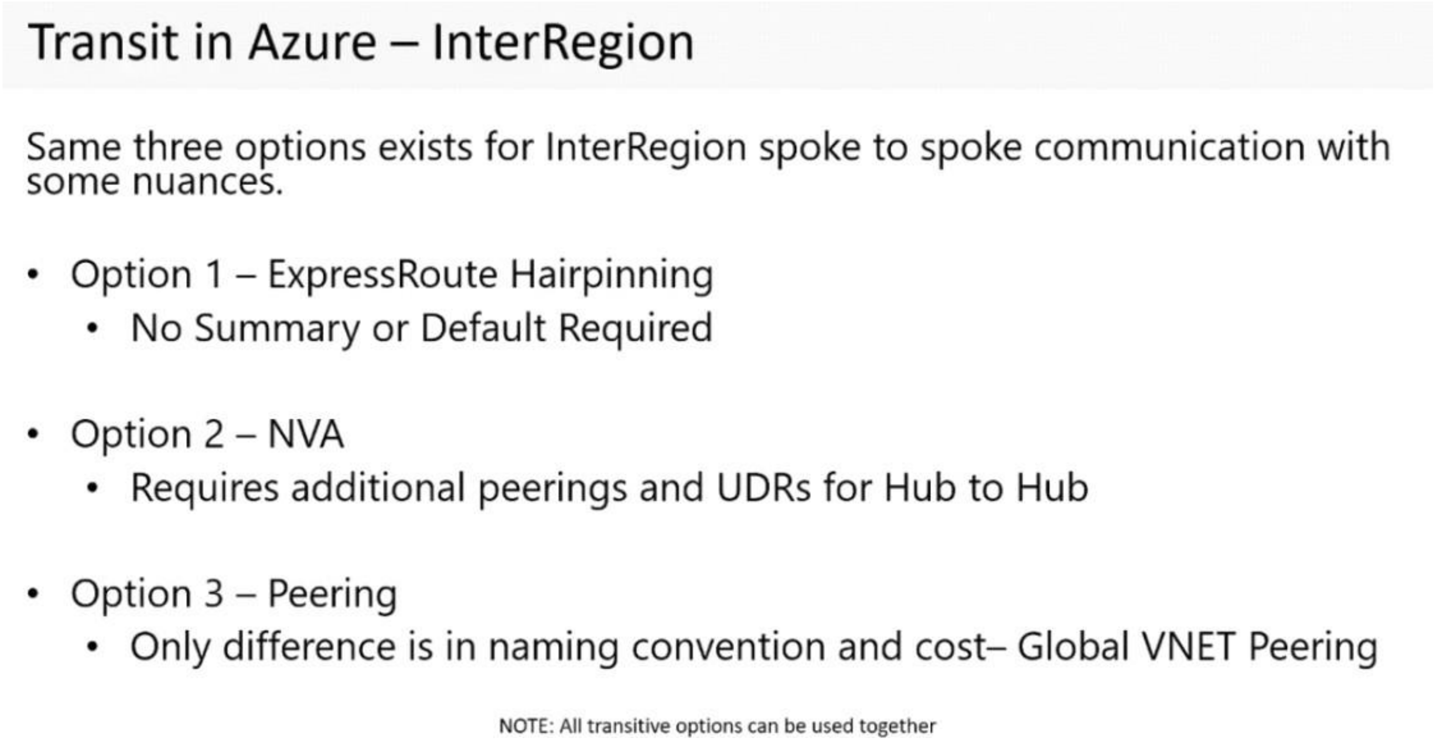
Azure Cloud
Region
Region



VNet Peering

- Preferred Method by Microsoft Product Group
- No Real BW Limitation
- 1-to-1 Mapping
- Doesn’t scale
- No granularity (all or none subnets)
- VNet peering data charges for ingress and egress in both directions
- VNet peering needs to be broken to add CIDR/Subnets to a VNet

★ **Scale is a big problem with VNet peering.**



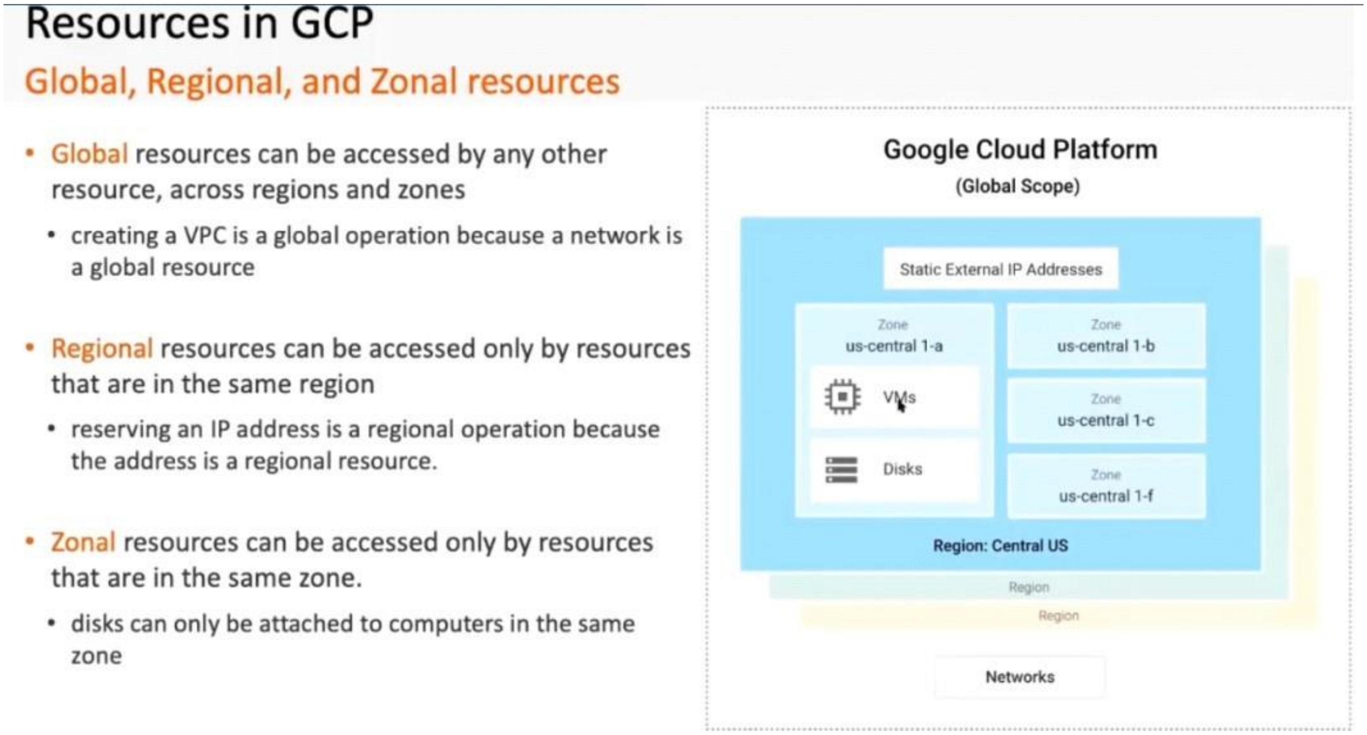
Transit in Azure – InterRegion

Same three options exists for InterRegion spoke to spoke communication with some nuances.

- Option 1 – ExpressRoute Hairpinning
  - No Summary or Default Required
- Option 2 – NVA
  - Requires additional peerings and UDRs for Hub to Hub
- Option 3 – Peering
  - Only difference is in naming convention and cost– Global VNET Peering

NOTE: All transitive options can be used together

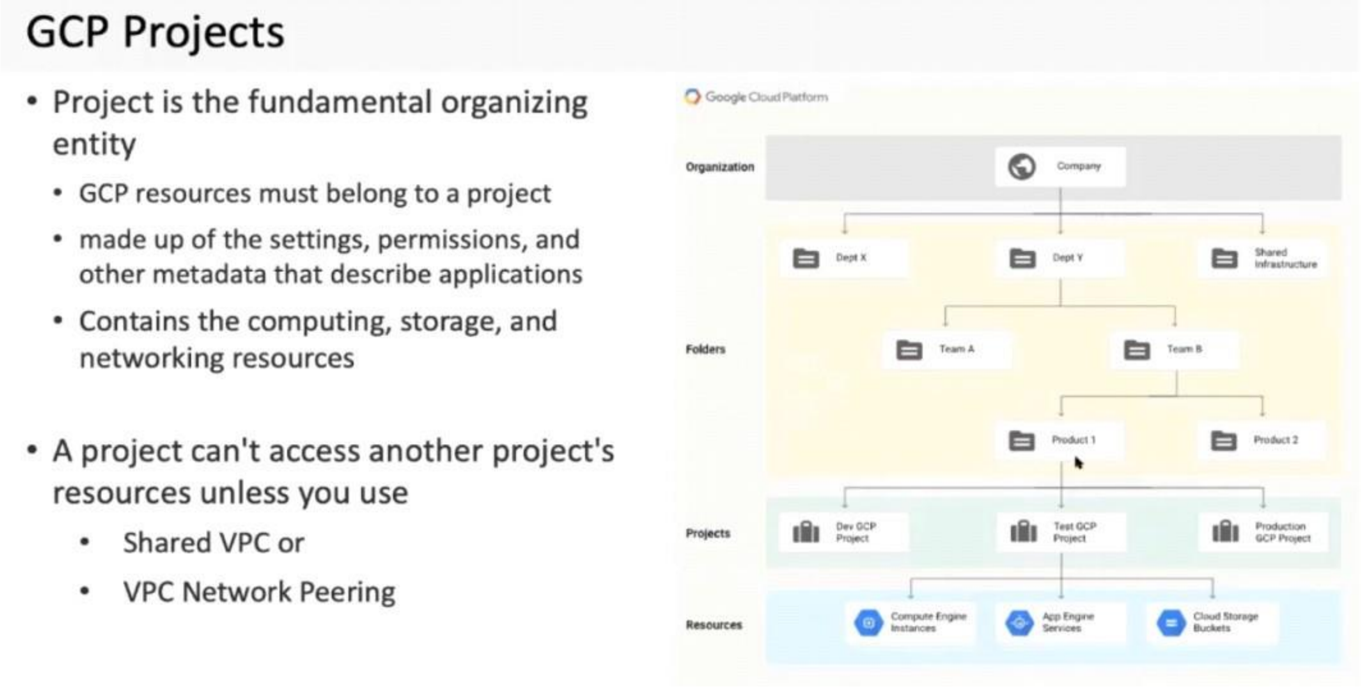
GCP Networking 101



Resources in GCP

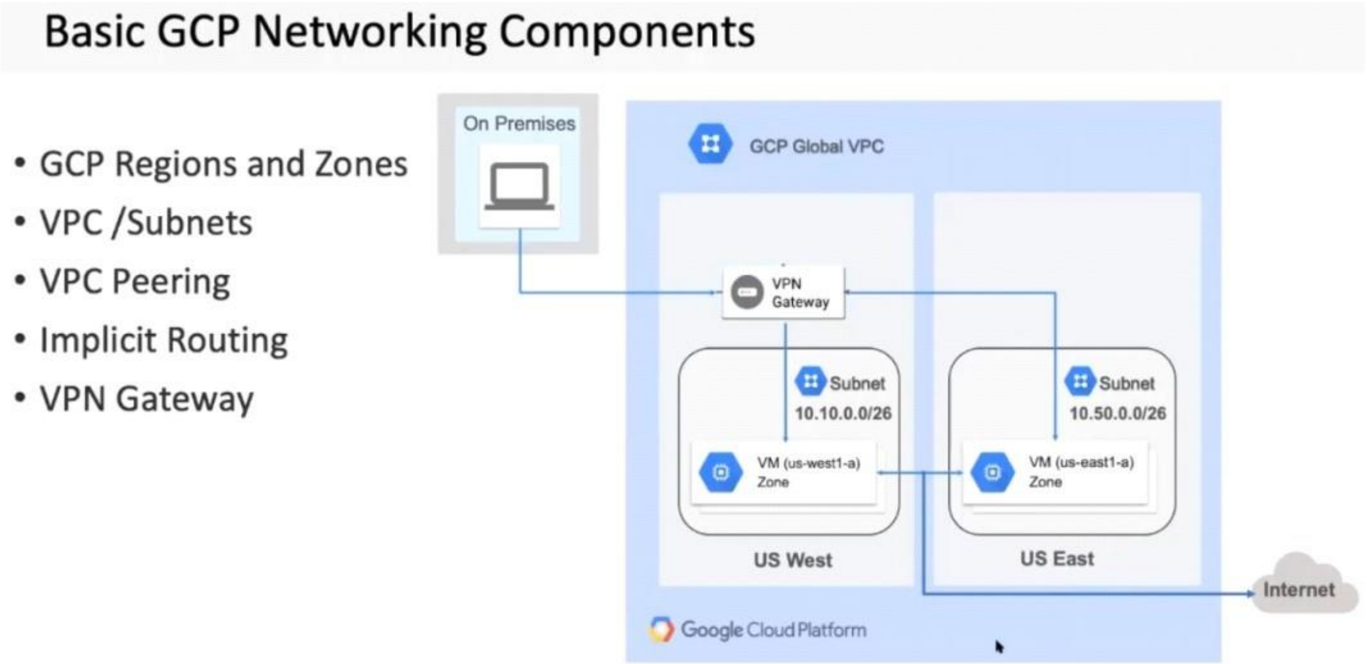
Global, Regional, and Zonal resources

- Global resources can be accessed by any other resource, across regions and zones
  - creating a VPC is a global operation because a network is a global resource
- Regional resources can be accessed only by resources that are in the same region
  - reserving an IP address is a regional operation because the address is a regional resource.
- Zonal resources can be accessed only by resources that are in the same zone.
  - disks can only be attached to computers in the same zone



GCP Projects

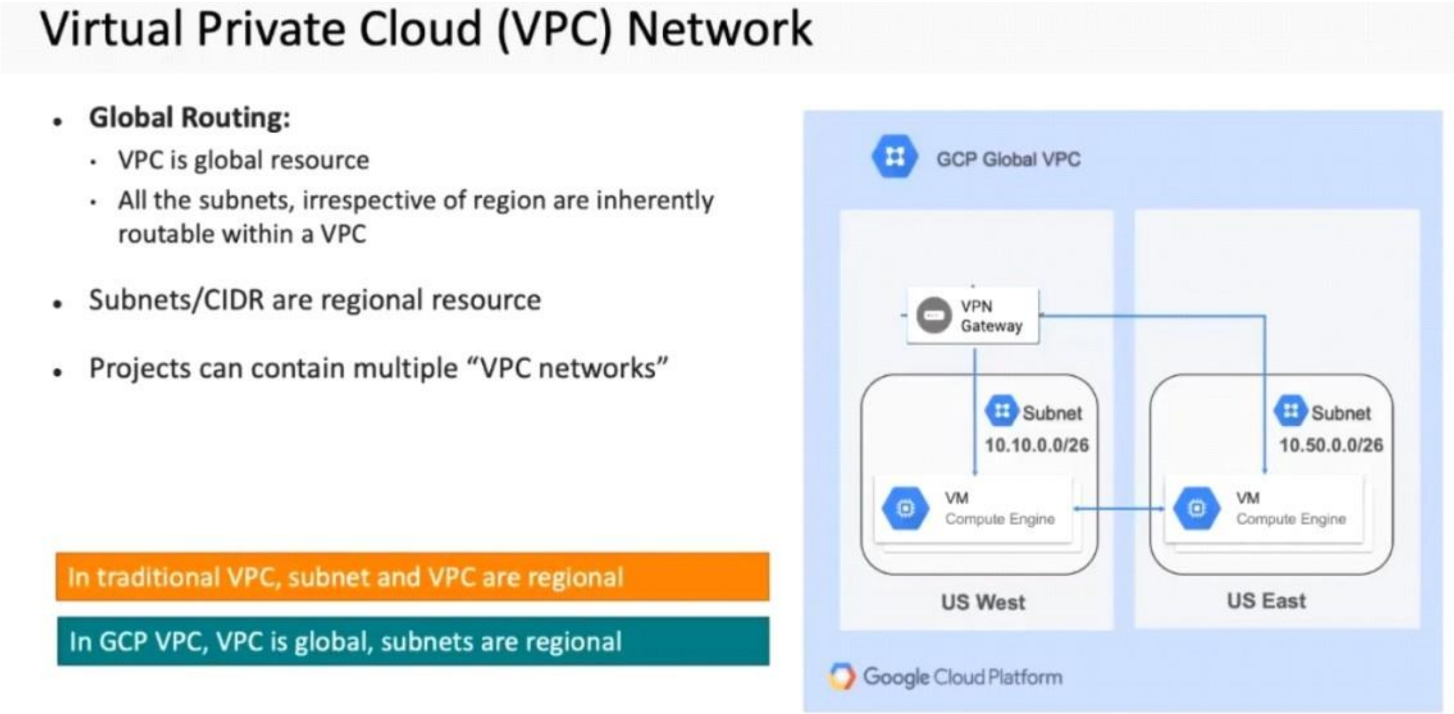
- Project is the fundamental organizing entity
  - GCP resources must belong to a project
  - made up of the settings, permissions, and other metadata that describe applications
  - Contains the computing, storage, and networking resources
- A project can't access another project's resources unless you use
  - Shared VPC or
  - VPC Network Peering



Basic GCP Networking Components

- GCP Regions and Zones
- VPC /Subnets
- VPC Peering
- Implicit Routing
- VPN Gateway

★ VPC is a Global Resource
★ No concept of public and private VNET.
★ There is NO high level CIDR.

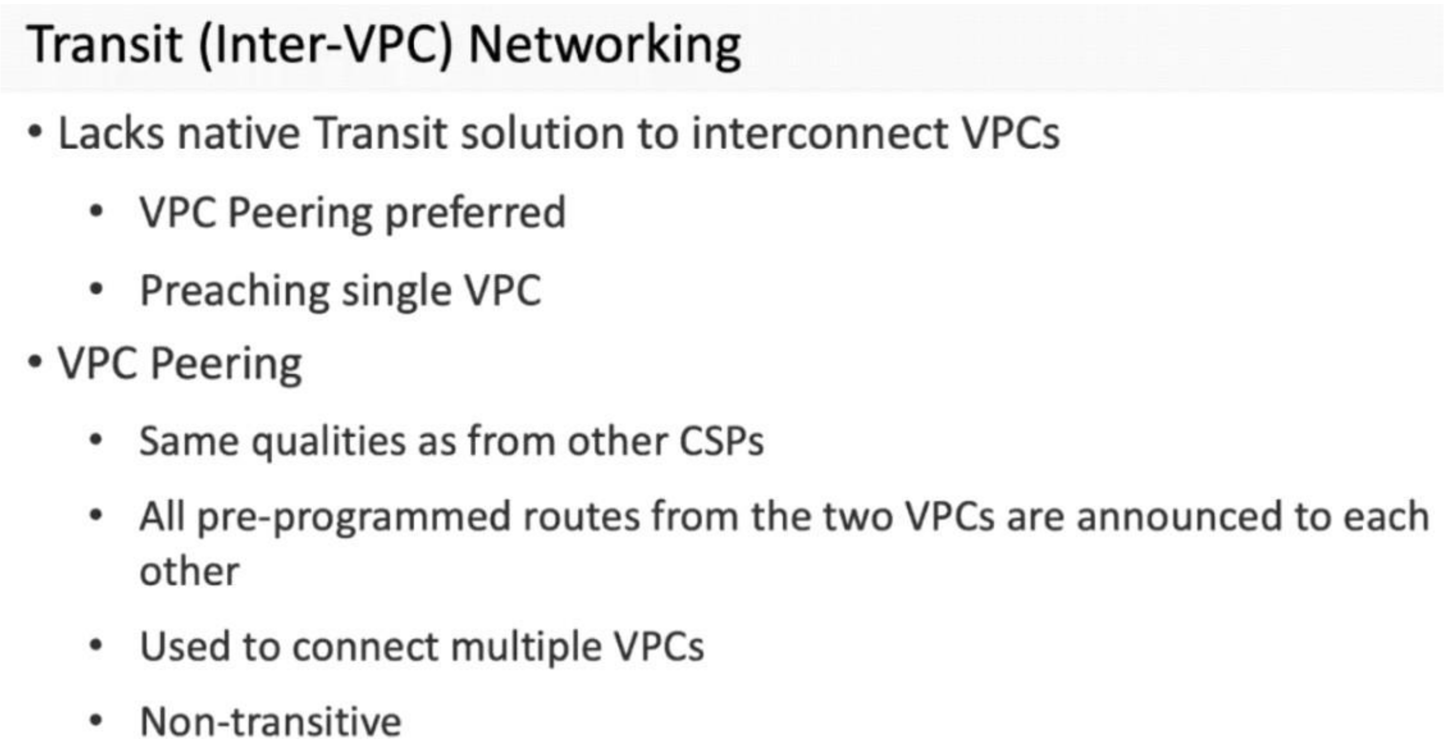


Virtual Private Cloud (VPC) Network

- **Global Routing:**
  - VPC is global resource
  - All the subnets, irrespective of region are inherently routable within a VPC
- Subnets/CIDR are regional resource
- Projects can contain multiple “VPC networks”

In traditional VPC, subnet and VPC are regional

In GCP VPC, VPC is global, subnets are regional

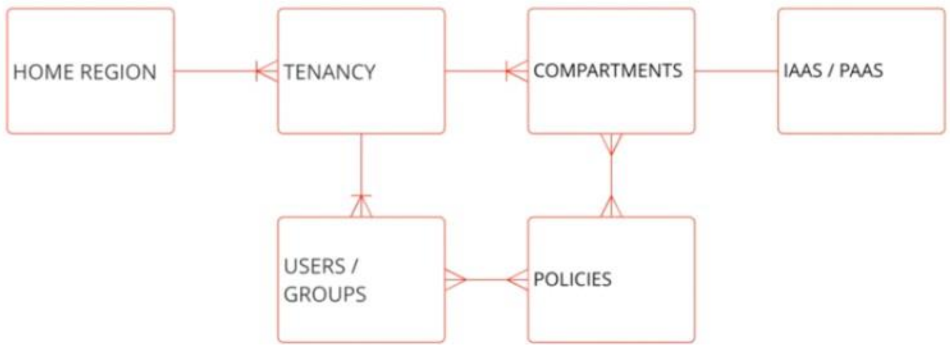


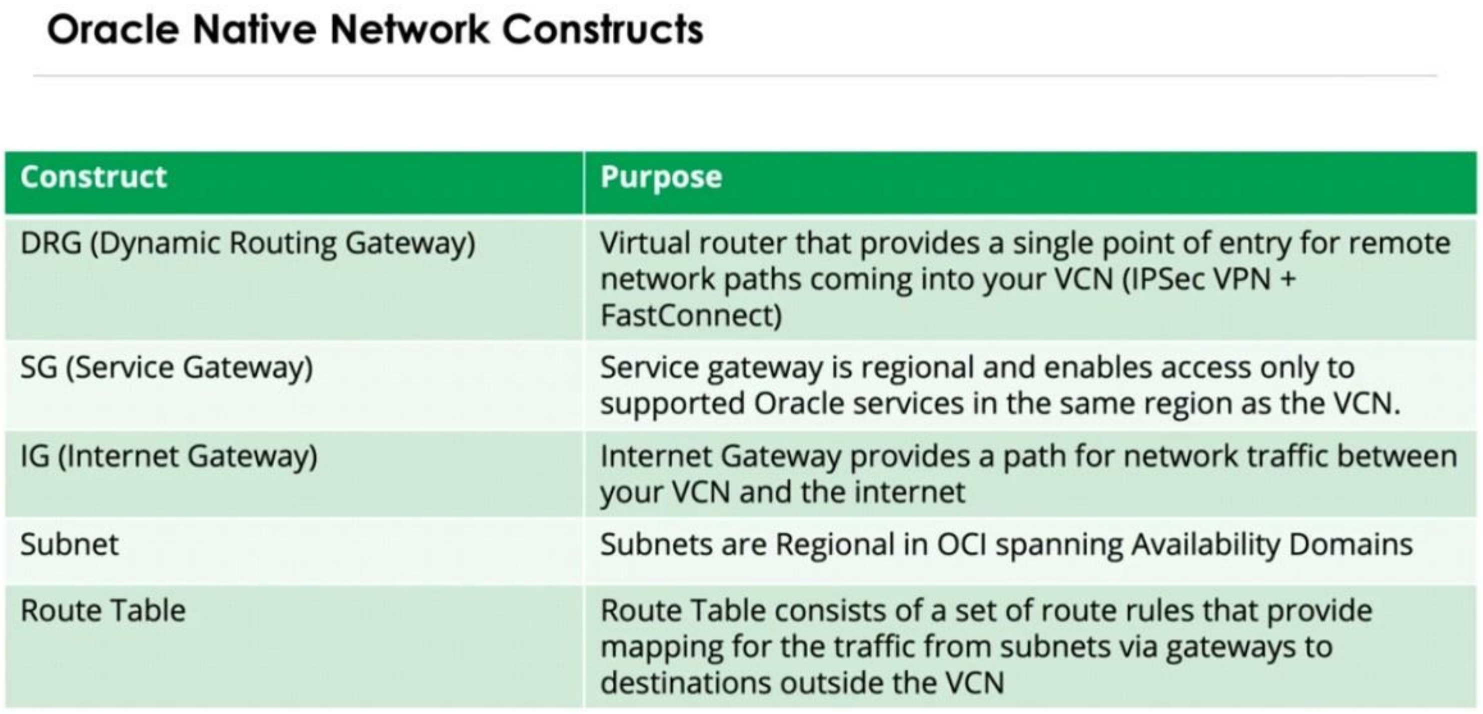
Transit (Inter-VPC) Networking

- Lacks native Transit solution to interconnect VPCs
  - VPC Peering preferred
  - Preaching single VPC
- VPC Peering
  - Same qualities as from other CSPs
  - All pre-programmed routes from the two VPCs are announced to each other
  - Used to connect multiple VPCs
  - Non-transitive

OCI Networking 101

Tenancy is the master paying account.
Tenancies are setup in a Home Region
IAM resources (like users and groups) metadata is bound to a Home Region
Compartments are logical containers used to isolate resources (i.e. Business Units or Projects)

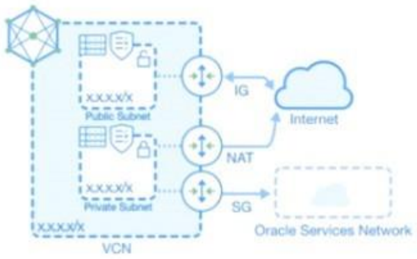




Oracle Native Network Constructs

Construct	Purpose
DRG (Dynamic Routing Gateway)	Virtual router that provides a single point of entry for remote network paths coming into your VCN (IPSec VPN + FastConnect)
SG (Service Gateway)	Service gateway is regional and enables access only to supported Oracle services in the same region as the VCN.
IG (Internet Gateway)	Internet Gateway provides a path for network traffic between your VCN and the internet
Subnet	Subnets are Regional in OCI spanning Availability Domains
Route Table	Route Table consists of a set of route rules that provide mapping for the traffic from subnets via gateways to destinations outside the VCN

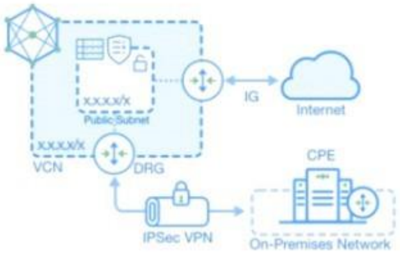
VCN with Internet Connectivity



Includes:

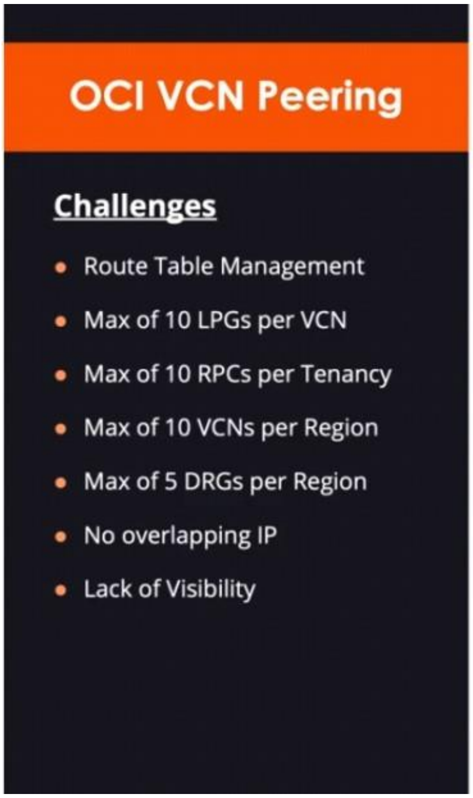
- VCN
- Public Subnet
- Internet Gateway (IG)
- NAT Gateway (NAT)
- Service Gateway (SG)

VCN with Internet Connectivity and VPN Connect



Includes:

- VCN
- Public Subnet
- Dynamic Routing Gateways (DRG)
- Virtual Customer-Premises Equipment (CPE)
- IPSec VPN Connection
- Internet Gateway (IG)

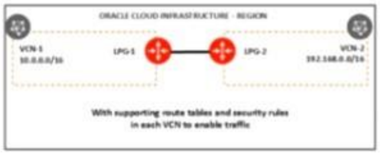


OCI VCN Peering

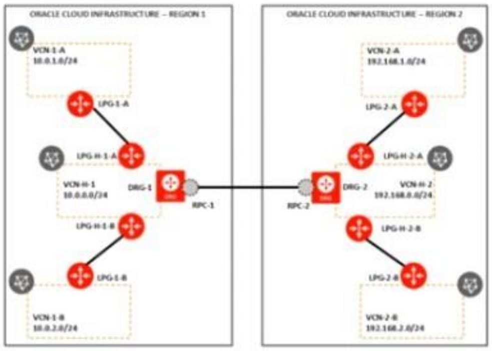
Challenges

- Route Table Management
- Max of 10 LPGs per VCN
- Max of 10 RPCs per Tenancy
- Max of 10 VCNs per Region
- Max of 5 DRGs per Region
- No overlapping IP
- Lack of Visibility

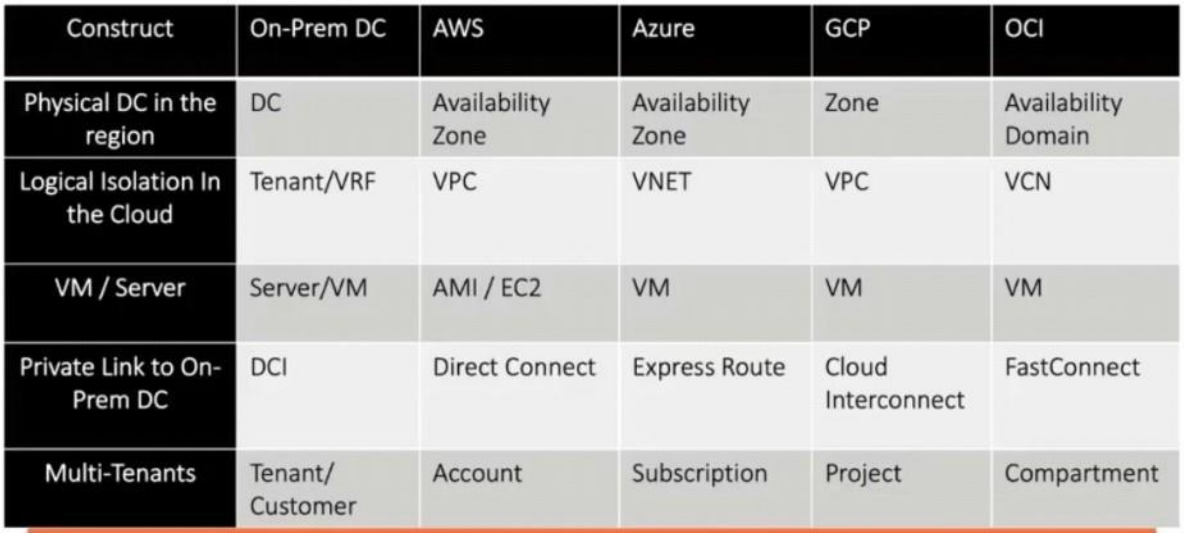
Basic VCN Peering
(within a Region)


ORACLE CLOUD INFRASTRUCTURE – REGION
VCN-1
10.0.0.0/16
LPG-1
LPG-2
VCN-2
192.168.0.0/16
With supporting route tables and security rules
in each VCN to enable traffic

Remote Peering
(across Regions)



Multi-Cloud Network Architecture (MCNA)



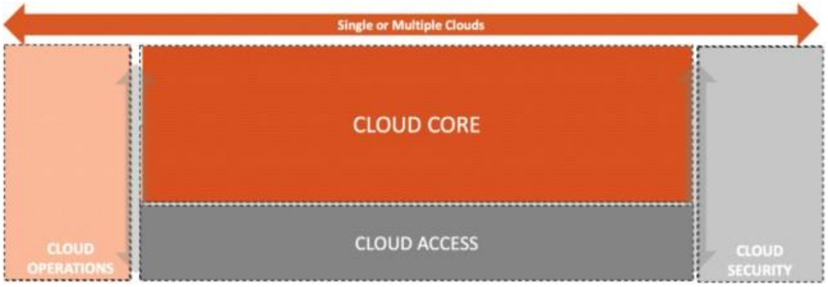
Construct	On-Prem DC	AWS	Azure	GCP	OCI
Physical DC in the region	DC	Availability Zone	Availability Zone	Zone	Availability Domain
Logical Isolation In the Cloud	Tenant/VRF	VPC	VNET	VPC	VCN
VM / Server	Server/VM	AMI / EC2	VM	VM	VM
Private Link to On-Prem DC	DCI	Direct Connect	Express Route	Cloud Interconnect	FastConnect
Multi-Tenants	Tenant/ Customer	Account	Subscription	Project	Compartment

Some of current challenges of an Enterprise Architecture:

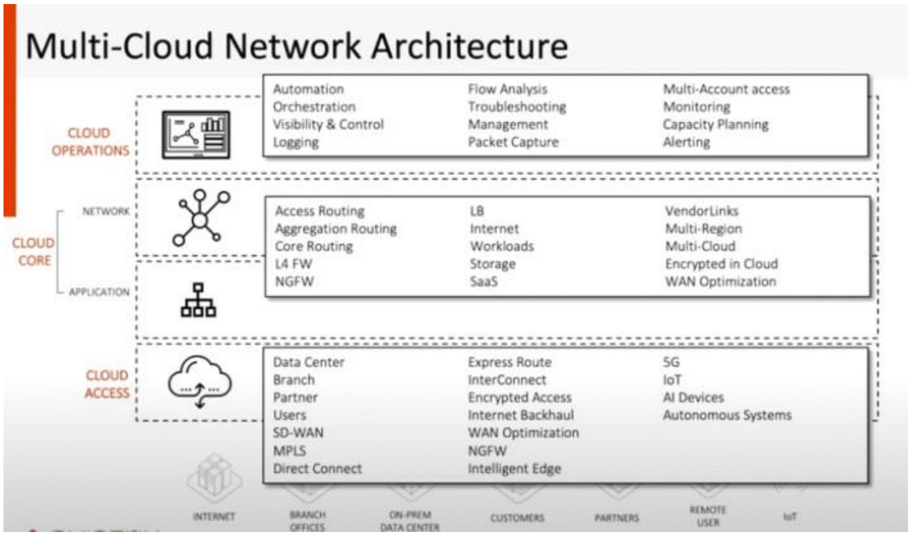
- VPC/VNET inter connectivity via peering in scalable manner, route propagation and routing management in a large/complex environment is a challenge!
- End-to-end encryption, inserting NGFW (Next Generation Firewall) services in multi-cloud environment
- Skill gaps when it comes to multi-cloud networking
- Lack of reference architecture

MCNA

The core principal of MCNA is to have a multi-cloud network and security framework for consistent deployment across clouds. MCNA defines four distinct layers at high level:



1. **Cloud Core**
   - Cloud core delivers a common data plane by supporting native cloud constructs, APIs, and adds advance functionalities to form that common data plane which helps optimizing multi-cloud networking and gives better visibility with control.
   - Cloud core divided into two sub categories
     - ***The Application Layer***
       - □ This is where applications resides. The Aviatrix controller embraces the native constructs of the cloud from this layer.
     - ***Global Transit Layer***
       - □ This layer enables deploy HA, multi-cloud network data plane with end-to-end encryption, high performance encryption, multi-cloud security domains and operational telemetry operations functionalities. This layer also leverages "Service Insertion Framework" to insert services in its pla tform.
2. **Cloud Security**
   - This component makes sure all the areas of a cloud, namely - application, transit and access layers are secured. Security is enforced by-default using encryption, segmentation et al.
3. **Cloud Access**
   - The multi-cloud access layer is a crucial layer of the multi-cloud network when interconnecting to on-premise resources. This layer ensures that the cloud is securely accessible by all the components of a business.
4. **Cloud Operations**
   - This layer provides full visibility for all aspects of the cloud, meaning that it encompasses each layer. It is a centralized operations plane. This is also the layer of the cloud that encompasses the most crucial tools, such as troubleshooting, visibility, and automation.



Multi-Cloud Network Architecture

CLOUD OPERATIONS

Automation	Flow Analysis	Multi-Account access
Orchestration	Troubleshooting	Monitoring
Visibility & Control	Management	Capacity Planning
Logging	Packet Capture	Alerting

CLOUD CORE: NETWORK, APPLICATION

Access Routing	LB	VendorLinks
Aggregation Routing	Internet	Multi-Region
Core Routing	Workloads	Multi-Cloud
L4 FW	Storage	Encrypted in Cloud
NGFW	SaaS	WAN Optimization

CLOUD ACCESS

Data Center	Express Route	5G
Branch	InterConnect	IoT
Partner	Encrypted Access	AI Devices
Users	Internet Backhaul	Autonomous Systems
SD-WAN	WAN Optimization	
MPLS	NGFW	
Direct Connect	Intelligent Edge	

Multi-Cloud Network Architecture offers:

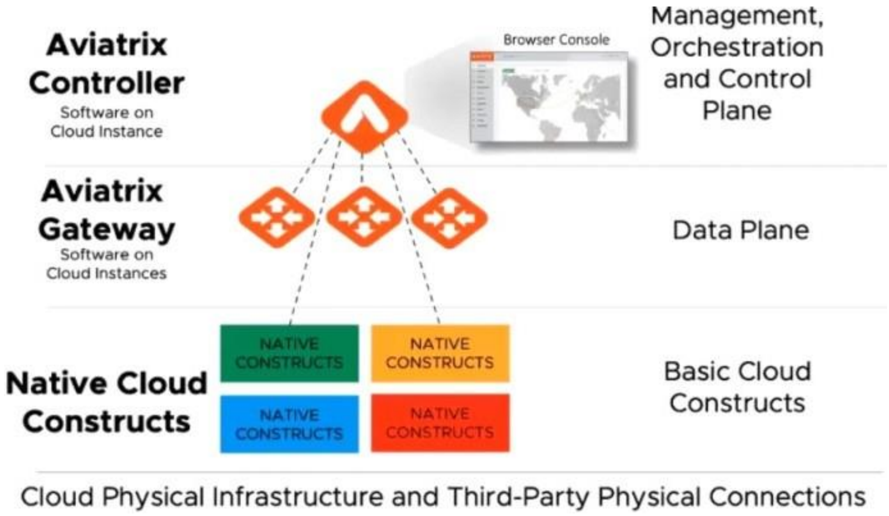
- Common Multi-cloud Control, Data and Operations Plane
- Normalized Data Plane
- Centralized Control Plane
- Centralized Operations Plane
- Repeatable across cloud providers
- Service Insertion and chaining

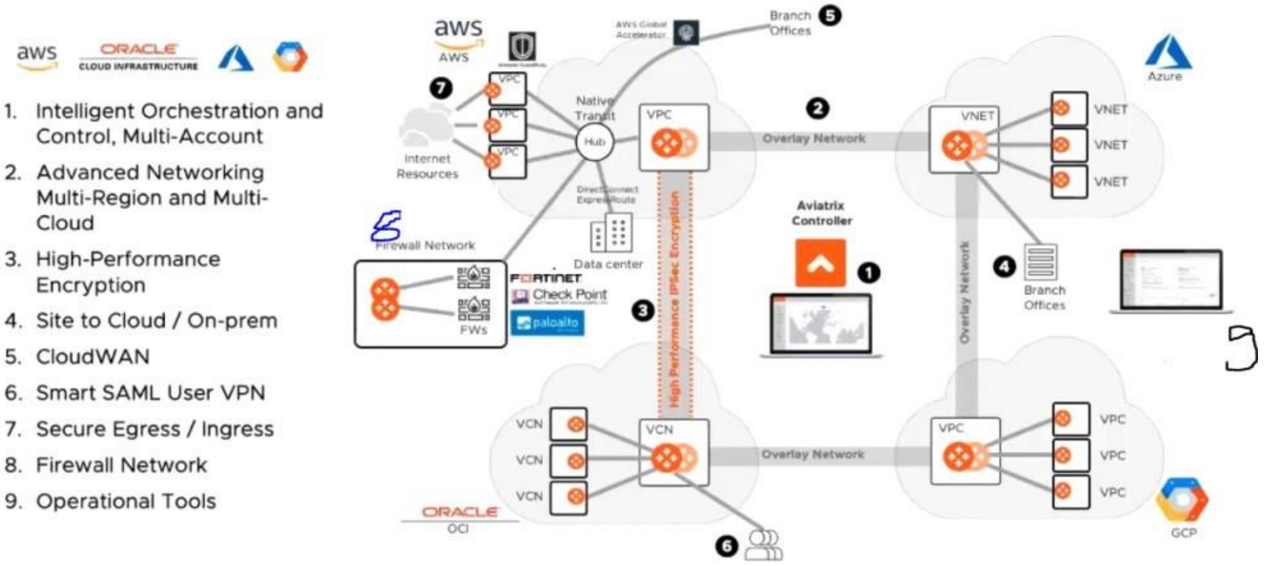
MCNA showcases a centralized controller to manage single or multiple clouds with a global, distributed, unified and normalized data plane.

Aviatrix Features Overview

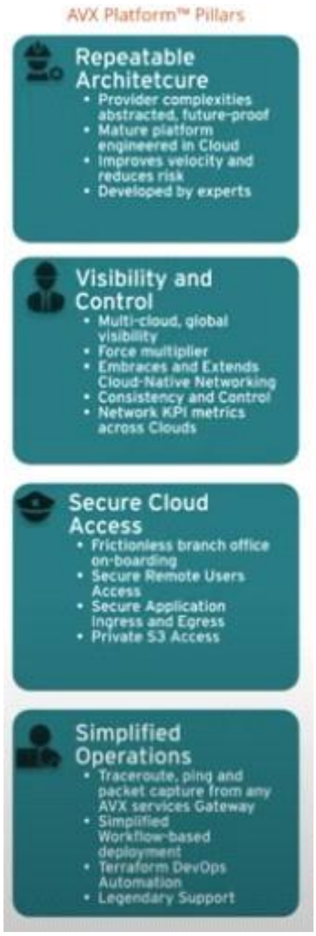
Aviatrix Software Components

- **Aviatrix Controller**: Available on Market Place as software instance. Not a SaaS or Managed Service having said that it gets deployed and controlled by you. In nutshell, it's a Management, Orchestration and Control Plane. This centralized controller also deploys Aviatrix Gateway instances for multi-cloud, on-premise, and edge connectivity. This controller is also the entry-point for multi-cloud automation, which can be done using API or Terraform.
- **Aviatrix Gateway**: Available on Market Place as software instance. This is Data Plane. These can be used as a multi service nodes, as part of the data-plane, these gateways work to provide services such as transit routing, high-performance encryption, egress and ingress control, edge connectivity, on-premise connectivity, and user-VPN services.
- **Native Cloud Constructs**: Embrace the cloud native construct. E.g. Leverage AWS ALB to load balance aviatrix gateways.




1. Intelligent Orchestration and Control, Multi-Account
2. Advanced Networking Multi-Region and Multi-Cloud
3. High-Performance Encryption
4. Site to Cloud / On-prem
5. CloudWAN
6. Smart SAML User VPN
7. Secure Egress / Ingress
8. Firewall Network
9. Operational Tools

AVX Pillars:



AVX Platform™ Pillars

Repeatable Architetcure

- Provider complexities abstracted, future-proof
- Mature platform engineered in Cloud
- Improves velocity and reduces risk
- Developed by experts

Visibility and Control

- Multi-cloud, global visibility
- Force multiplier
- Embraces and Extends Cloud-Native Networking
- Consistency and Control
- Network KPI metrics across Clouds

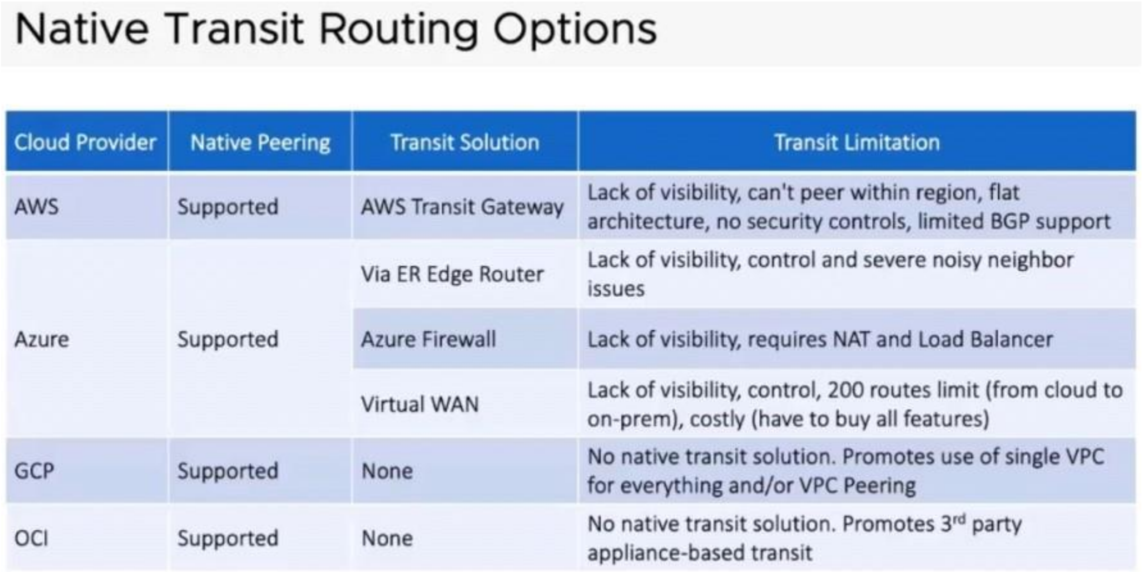
Secure Cloud Access

- Frictionless branch office on-boarding
- Secure Remote Users Access
- Secure Application Ingress and Egress
- Private S3 Access

Simplified Operations

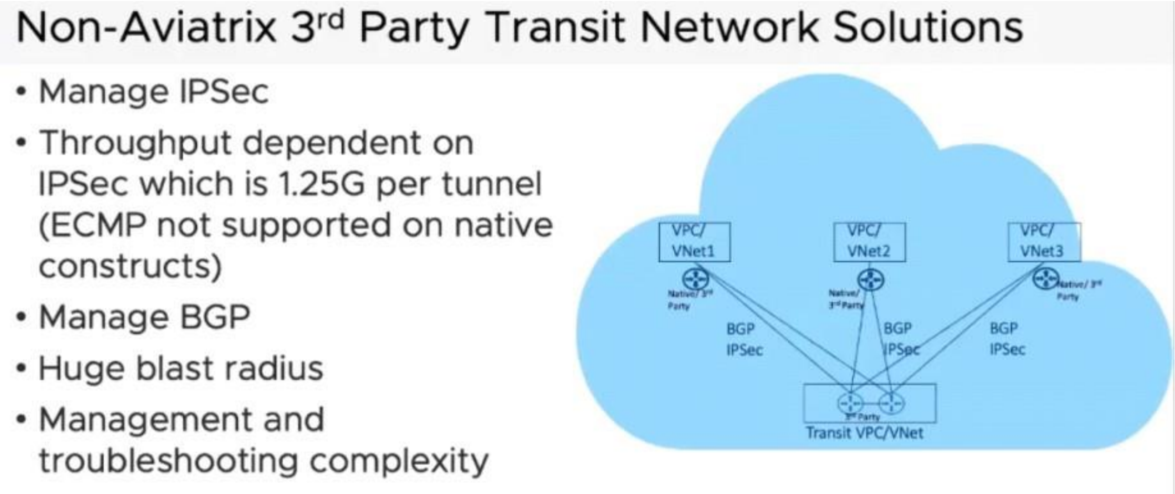
- Traceroute, ping and packet capture from any AVX services Gateway
- Simplified Workflow-based deployment
- Terraform DevOps Automation
- Legendary Support

Transit Routing Options in various CSP's:



Native Transit Routing Options

Cloud Provider	Native Peering	Transit Solution	Transit Limitation
AWS	Supported	AWS Transit Gateway	Lack of visibility, can't peer within region, flat architecture, no security controls, limited BGP support
Azure	Supported	Via ER Edge Router	Lack of visibility, control and severe noisy neighbor issues
		Azure Firewall	Lack of visibility, requires NAT and Load Balancer
		Virtual WAN	Lack of visibility, control, 200 routes limit (from cloud to on-prem), costly (have to buy all features)
GCP	Supported	None	No native transit solution. Promotes use of single VPC for everything and/or VPC Peering
OCI	Supported	None	No native transit solution. Promotes 3rd party appliance-based transit



Non-Aviatrix 3rd Party Transit Network Solutions

- Manage IPSec
- Throughput dependent on IPSec which is 1.25G per tunnel (ECMP not supported on native constructs)
- Manage BGP
- Huge blast radius
- Management and troubleshooting complexity

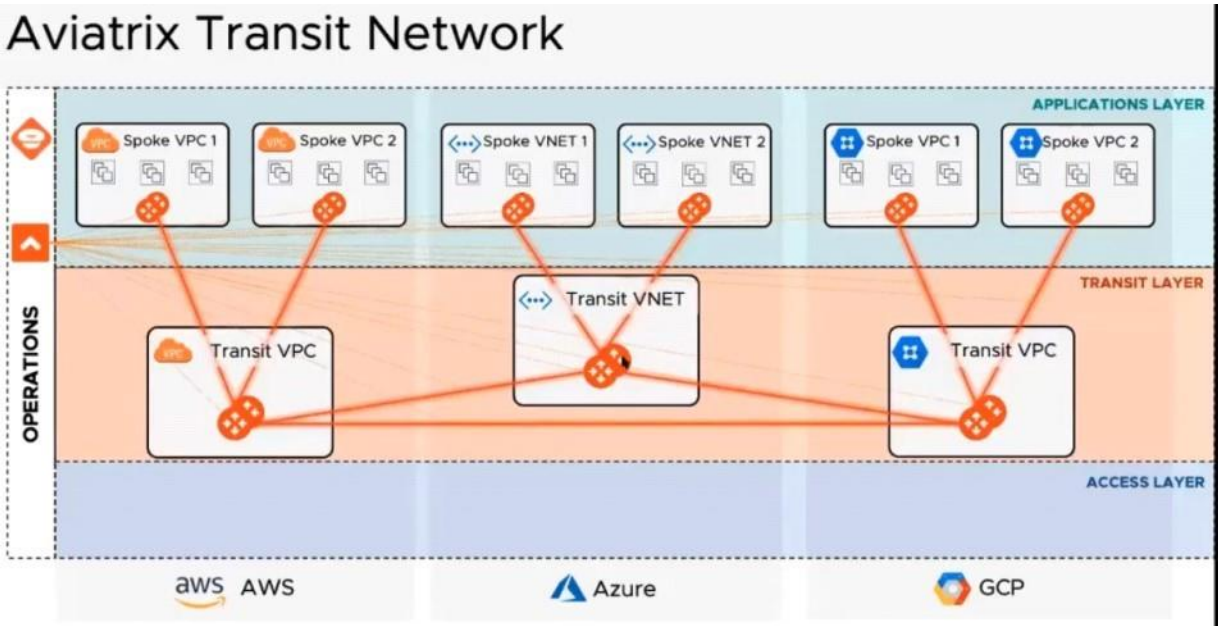
ECMP: Equal-Cost Multi-Path Routing

What is Blast Radius?

- Blast radius is a way of measuring the total impact of a potential security event (DDOS attack, comprised credentials, insecure interfaces and platform misconfiguration) or a disaster (whole region, DC going down) or bugs or anything that potentially breaks a working eco-system.
- Failures isn't binary! Rather, there is always a degree of impact to consider.

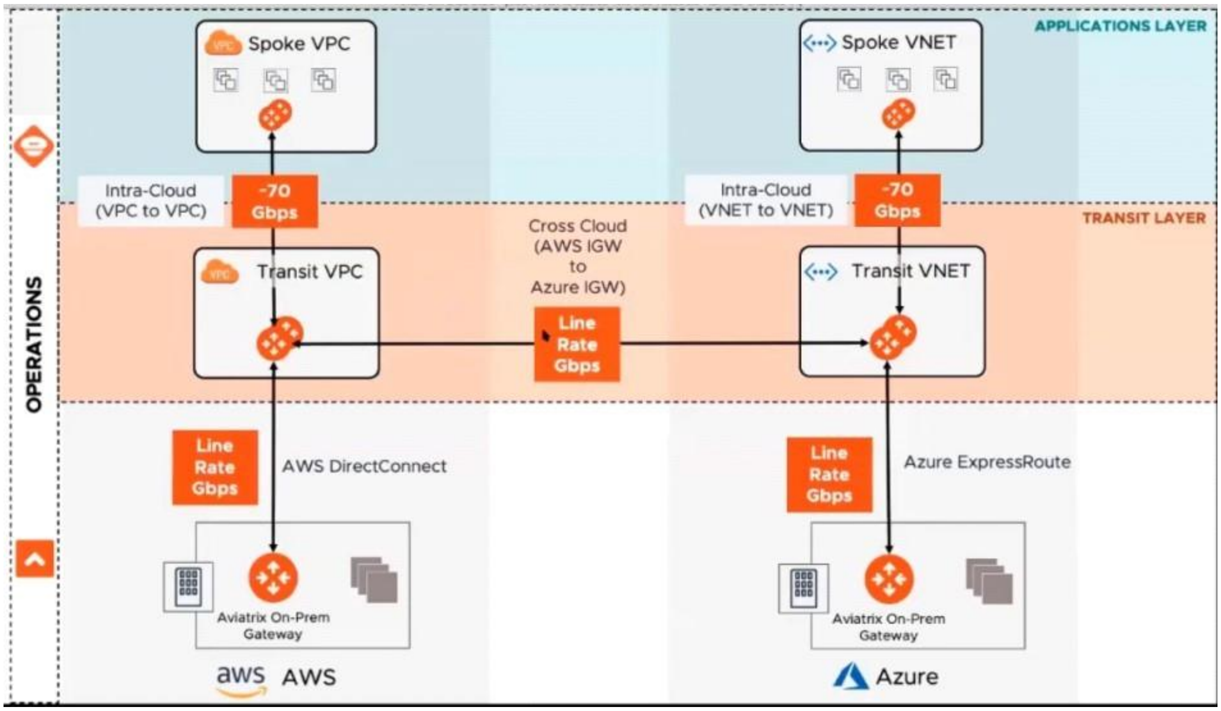
How to limit the blast radius?

- One of the most effective ways of limiting your blast radius is to isolate your cloud accounts. Create different accounts for developers, security teams, operations, and business units, and grant access only as needed.
- Beyond access control, it's also important to relentlessly monitor all of your data, resources, and microservices. Consider investing in a security platform that provides complete visibility into where your data lives, who is accessing it, and from where.
- Have multi-region, multi-AZ design (zero-blast radius)
- Separating control plane from data plane reduces blast radius.

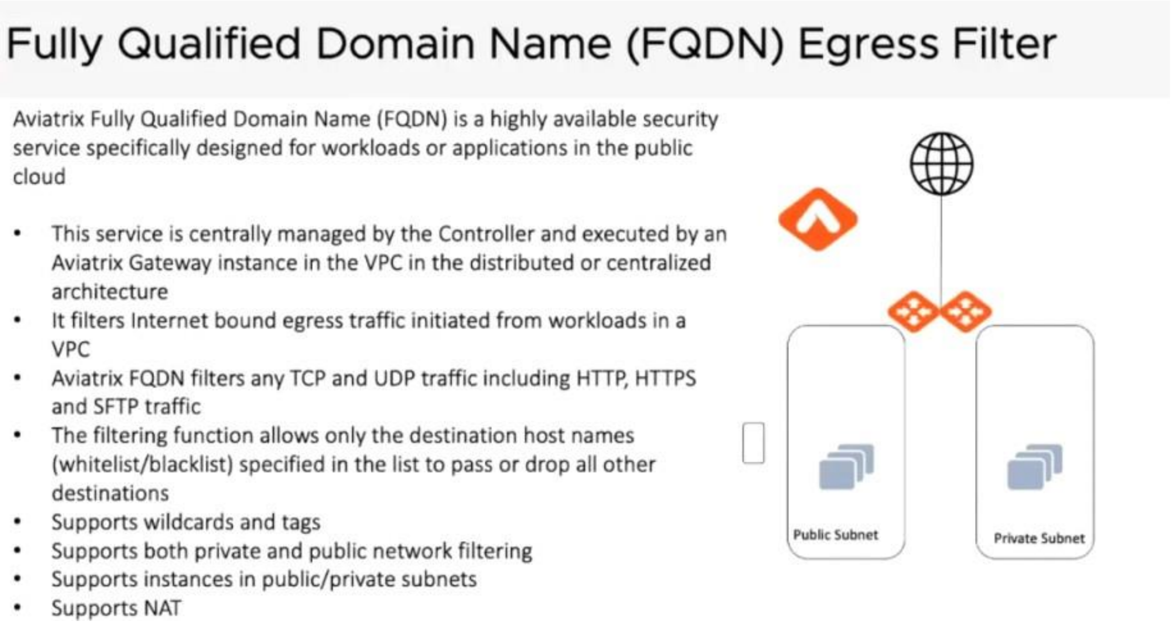


Aviatrix Transit Network

High Performance Encryption:



Fully Qualified Domain Name Egress Filter:



Fully Qualified Domain Name (FQDN) Egress Filter

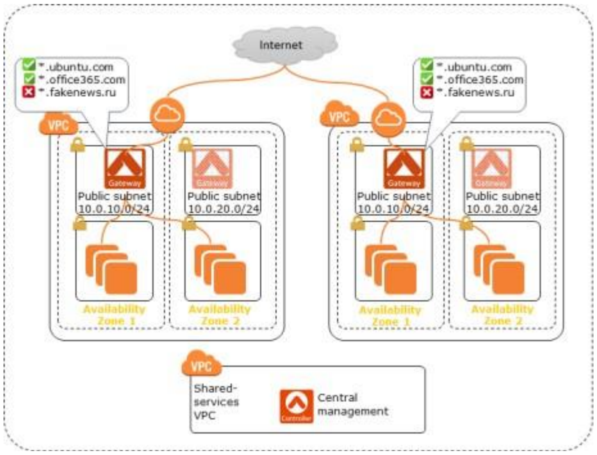
Aviatrix Fully Qualified Domain Name (FQDN) is a highly available security service specifically designed for workloads or applications in the public cloud

- This service is centrally managed by the Controller and executed by an Aviatrix Gateway instance in the VPC in the distributed or centralized architecture
- It filters Internet bound egress traffic initiated from workloads in a VPC
- Aviatrix FQDN filters any TCP and UDP traffic including HTTP, HTTPS and SFTP traffic
- The filtering function allows only the destination host names (whitelist/blacklist) specified in the list to pass or drop all other destinations
- Supports wildcards and tags
- Supports both private and public network filtering
- Supports instances in public/private subnets
- Supports NAT

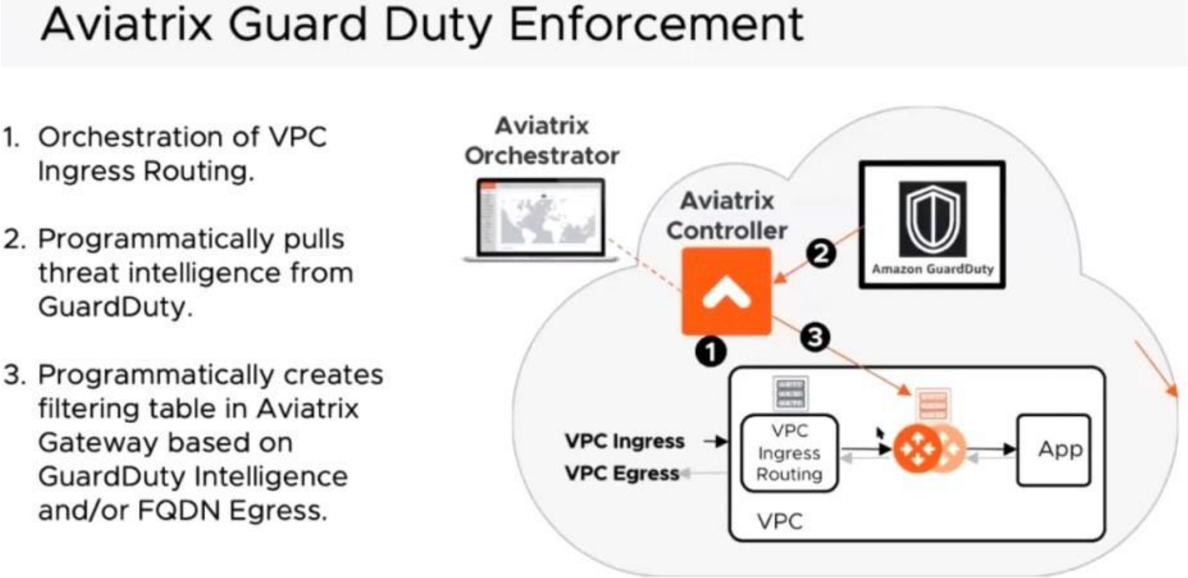
For Internet bound egress traffic, specifying outbound policy at the IP address level is not sufficient as the domain names of a site can be translated to many different IP addresses. An AWS NAT gateway does not offer security group functions; it relies on security groups by each instance. The egress filtering needs to happen at Layer 7.

On the other hand, workloads in AWS are mostly applications or programs where it is deterministic which outbound APIs the application program calls. For example, an application runs API queries to www.salesforce.com for data retrieving and runs API queries to www.google.com for app authentication. In these cases, making sure that only these sites are allowed for egress traffic is sufficient from a security point of view.

Another use case is for PCI DSS compliance. PCI DSS specifies that if you handle any payment and sensitive data, there must be firewall policy enforcement at the egress. In the cloud, the logical egress point is per VPC.



Ingress security:



Aviatrix Guard Duty Enforcement

1. Orchestration of VPC Ingress Routing.
2. Programmatically pulls threat intelligence from GuardDuty.
3. Programmatically creates filtering table in Aviatrix Gateway based on GuardDuty Intelligence and/or FQDN Egress.

Leverage AWS GuardDuty to make an innovative IDS solution.

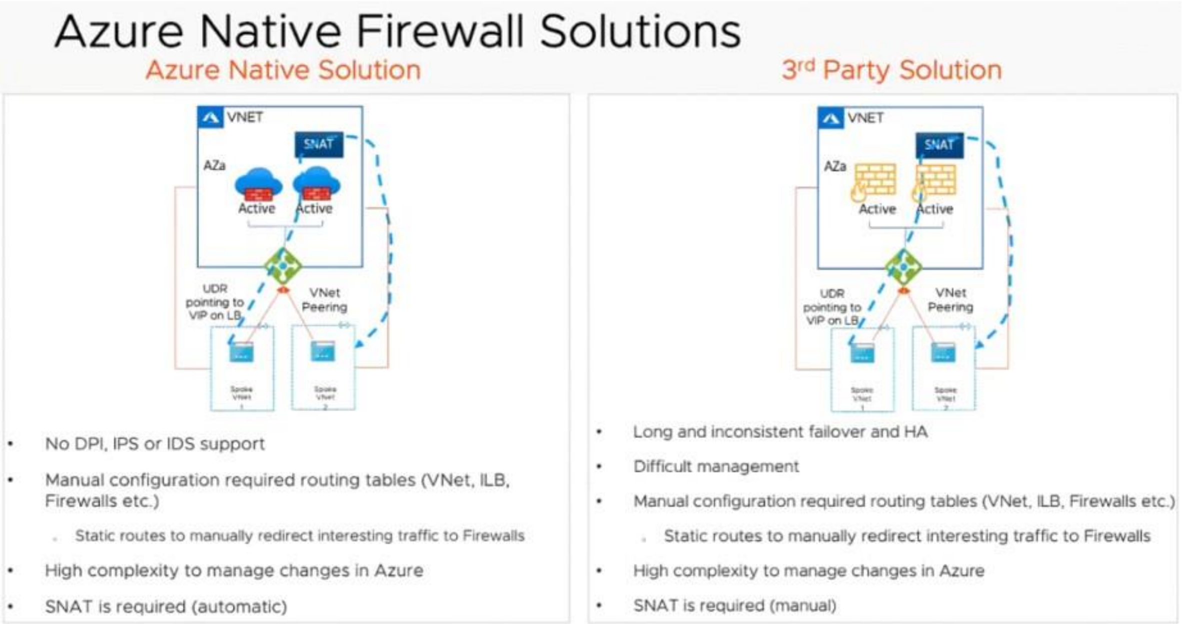
NOTE:

East-West Traffic:

- **East west traffic is anything that's under your control. VPC <-> VPC, VPC <-> On-Prem**

North-South Traffic:

- **Traffic that is destined to internet. Egress to Internet or Ingress to Internet.**



Azure Native Firewall Solutions

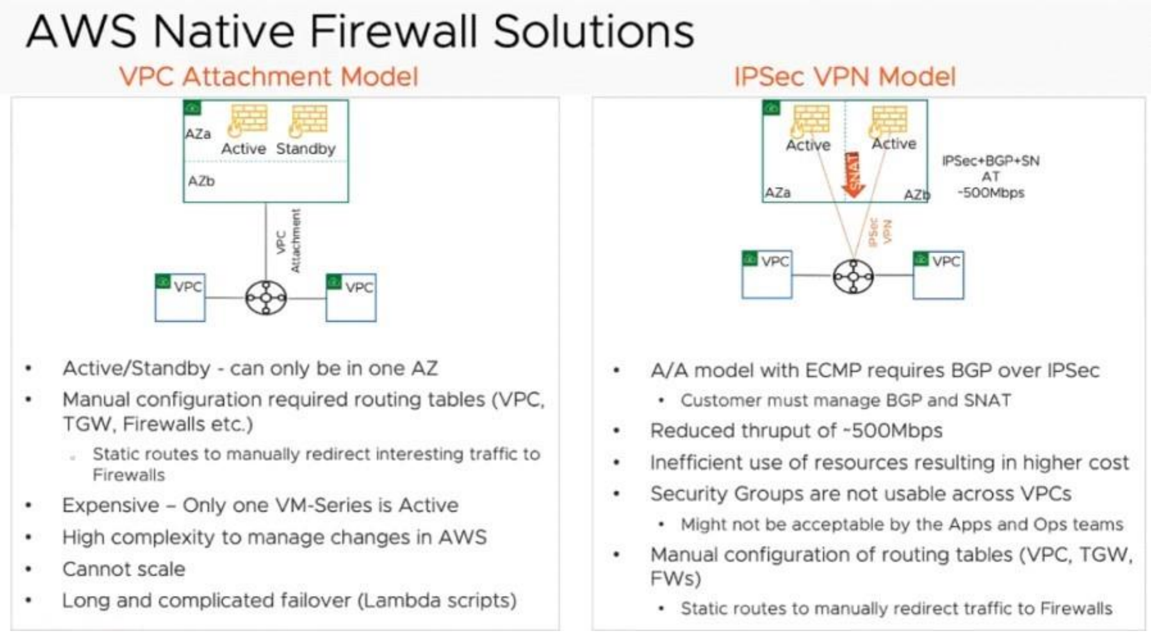
Azure Native Solution

- No DPI, IPS or IDS support
- Manual configuration required routing tables (VNet, ILB, Firewalls etc.)
  - Static routes to manually redirect interesting traffic to Firewalls
- High complexity to manage changes in Azure
- SNAT is required (automatic)

3rd Party Solution

- Long and inconsistent failover and HA
- Difficult management
- Manual configuration required routing tables (VNet, ILB, Firewalls etc.)
  - Static routes to manually redirect interesting traffic to Firewalls
- High complexity to manage changes in Azure
- SNAT is required (manual)

Layer 4 firewall Azure native firewall.	With 3rd party you get benefit of having layer 7 functionality
UDR management on your own	UDR (static routes) on your own
Enable SNAT by default Azure firewall only.	Enable SNAT manually



AWS Native Firewall Solutions

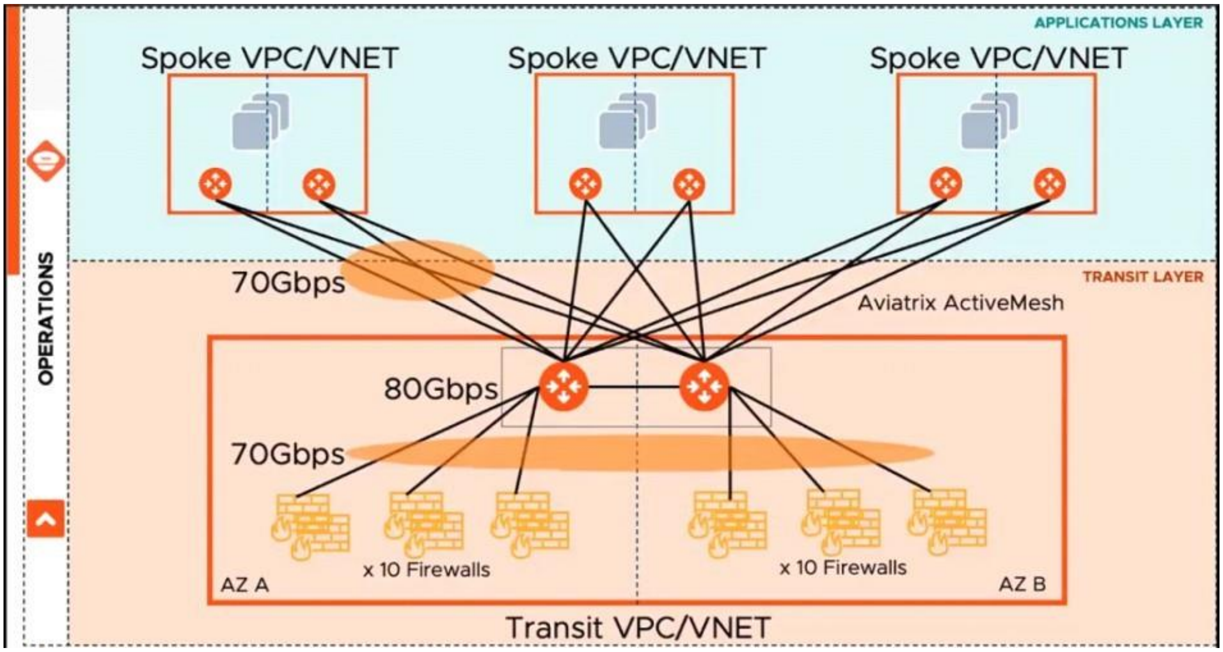
VPC Attachment Model

- Active/Standby - can only be in one AZ
- Manual configuration required routing tables (VPC, TGW, Firewalls etc.)
  - Static routes to manually redirect interesting traffic to Firewalls
- Expensive – Only one VM-Series is Active
- High complexity to manage changes in AWS
- Cannot scale
- Long and complicated failover (Lambda scripts)

IPSec VPN Model

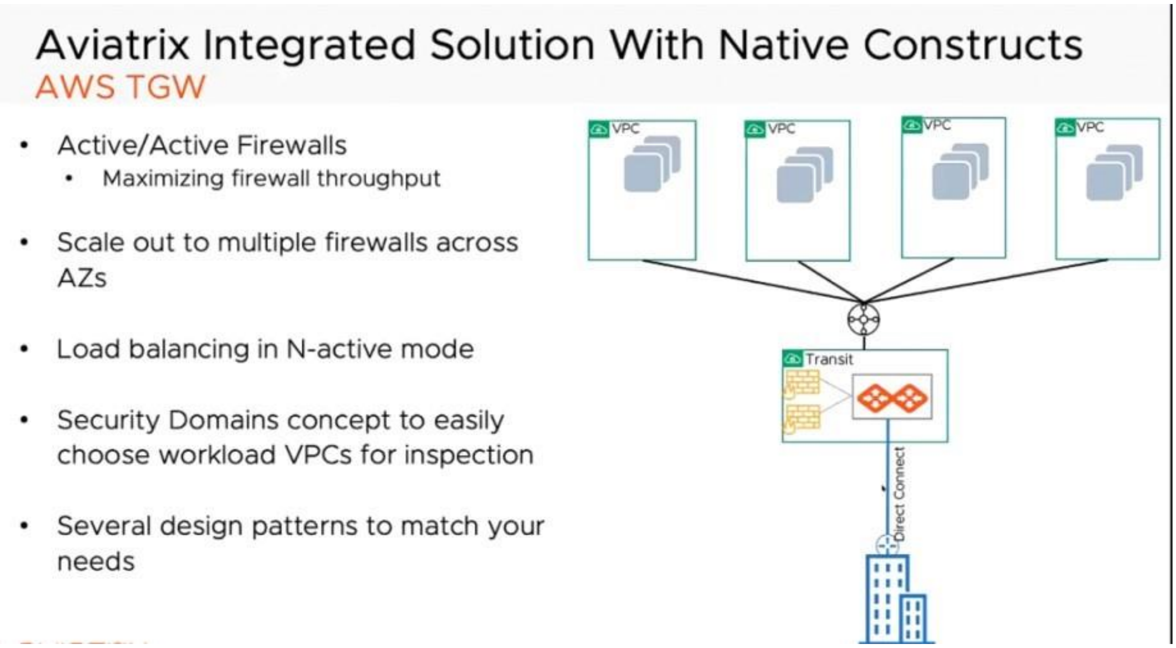
- A/A model with ECMP requires BGP over IPSec
  - Customer must manage BGP and SNAT
- Reduced thruput of ~500Mbps
- Inefficient use of resources resulting in higher cost
- Security Groups are not usable across VPCs
  - Might not be acceptable by the Apps and Ops teams
- Manual configuration of routing tables (VPC, TGW, FWs)
  - Static routes to manually redirect traffic to Firewalls

In Azure/AWS both the solution isn't ideal hence the Aviatrix Firewall Network comes to rescue.



- Up to 10 firewalls per AZ
- Magic happens at transit gateways
- Supports all major firewall vendors
- Supports hub-spoke topology
- AZ level redundancy

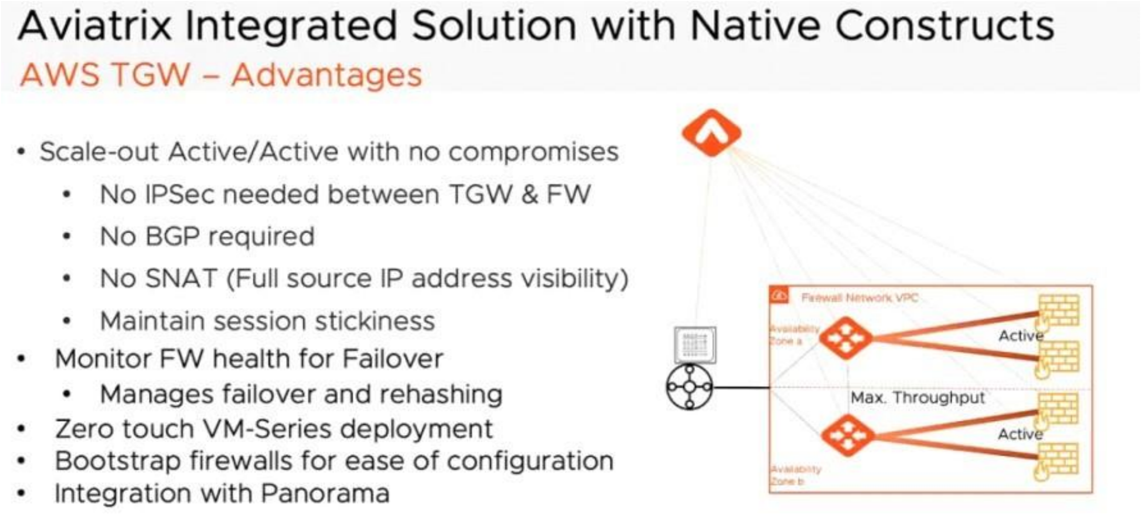
Aviatrix AWS TGW FireNet:



Aviatrix Integrated Solution With Native Constructs

AWS TGW

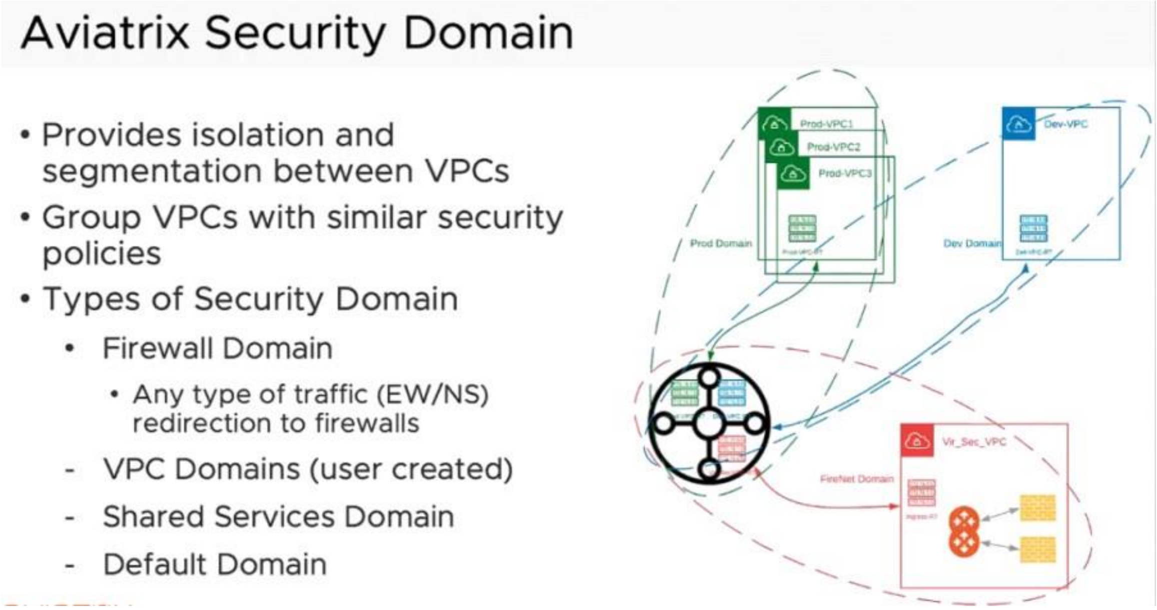
- Active/Active Firewalls
  - Maximizing firewall throughput
- Scale out to multiple firewalls across AZs
- Load balancing in N-active mode
- Security Domains concept to easily choose workload VPCs for inspection
- Several design patterns to match your needs



Aviatrix Integrated Solution with Native Constructs

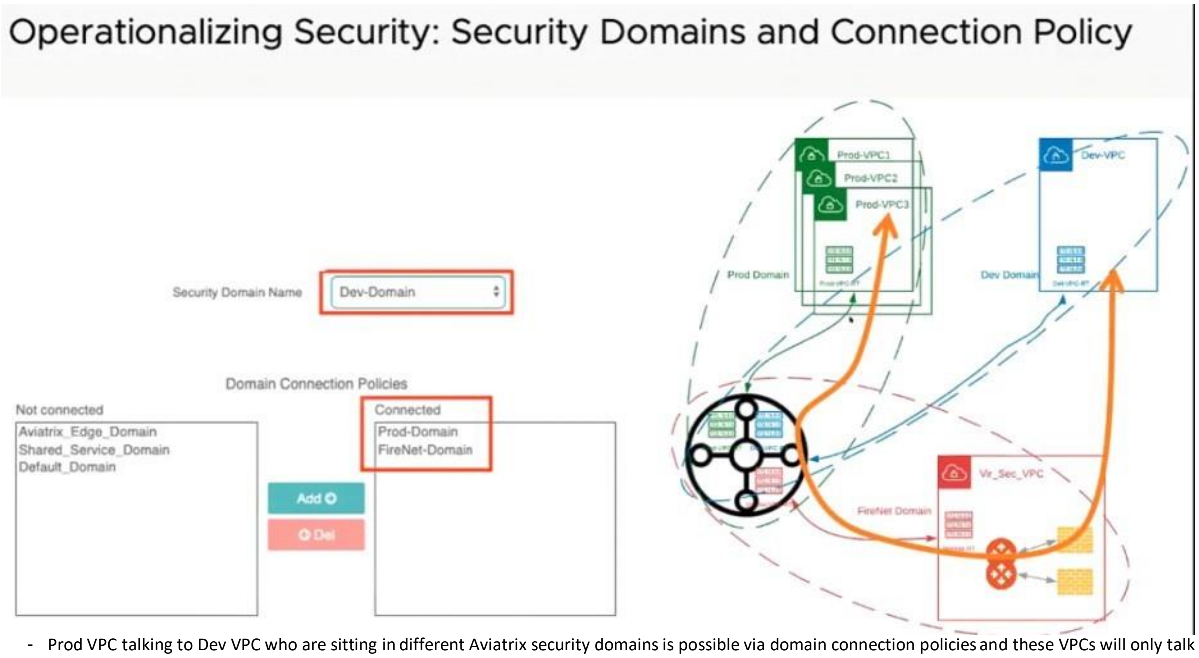
AWS TGW – Advantages

- Scale-out Active/Active with no compromises
  - No IPSec needed between TGW & FW
  - No BGP required
  - No SNAT (Full source IP address visibility)
  - Maintain session stickiness
- Monitor FW health for Failover
  - Manages failover and rehashing
- Zero touch VM-Series deployment
- Bootstrap firewalls for ease of configuration
- Integration with Panorama



Aviatrix Security Domain

- Provides isolation and segmentation between VPCs
- Group VPCs with similar security policies
- Types of Security Domain
  - Firewall Domain
    - Any type of traffic (EW/NS) redirection to firewalls
  - VPC Domains (user created)
  - Shared Services Domain
  - Default Domain



Operationalizing Security: Security Domains and Connection Policy

Security Domain Name: Dev-Domain

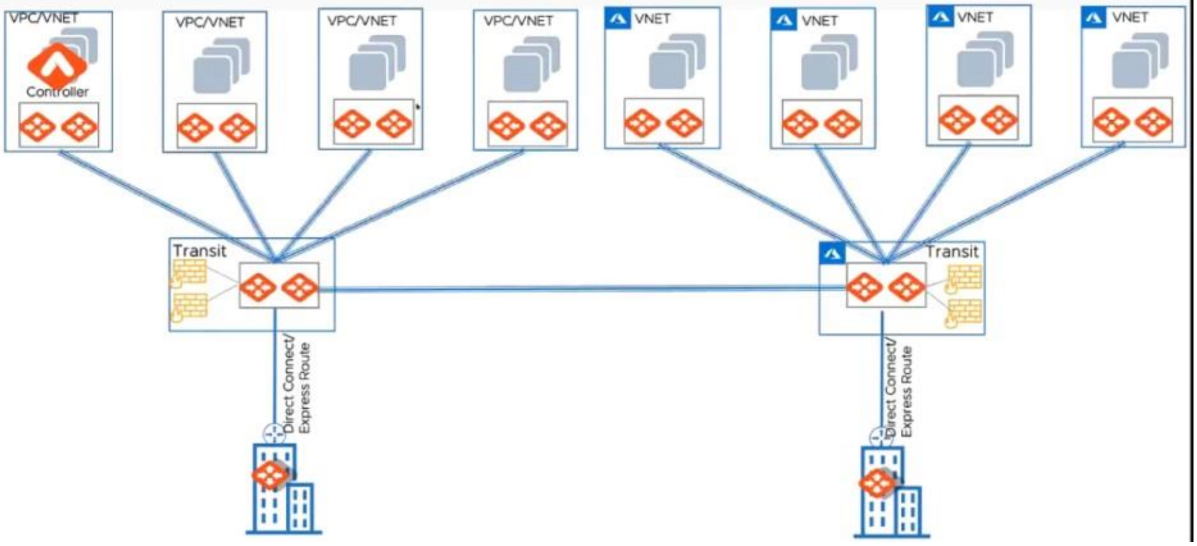
Domain Connection Policies

Not connected:
Aviatrix_Edge_Domain
Shared_Service_Domain
Default_Domain

Connected:
Prod-Domain
FireNet-Domain

- Prod VPC talking to Dev VPC who are sitting in different Aviatrix security domains is possible via domain connection policies and these VPCs will only talk to each other via firewall so traffic inspection can be done properly.

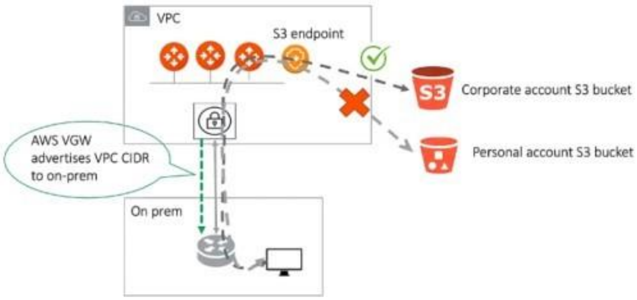
Multi-Region/Multi-Cloud Transit with Aviatrix Edge



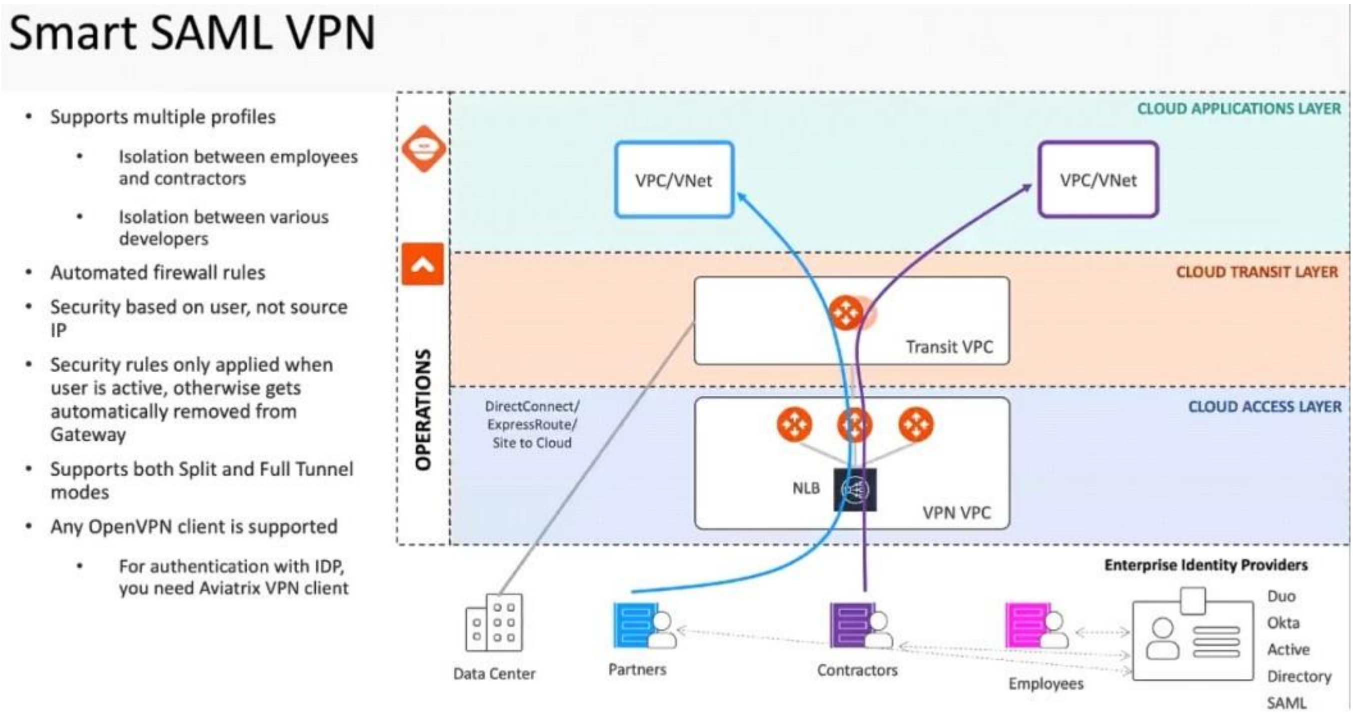
Aviatrix Private S3

Enterprise Customer Requirements

- Transfers objects between on-prem and S3 by leveraging Direct Connect without using public VIF
- Controls which S3 buckets can be accessed
- Scale out architecture to load balance traffic to S3


VPC
S3 endpoint
Corporate account S3 bucket
Personal account S3 bucket
AWS VGW advertises VPC CIDR to on-prem
On prem

- Not advertising the entire S3 public IP ranges from AWS to on-prem.
- Customer on-prem DNS resolves all corporate S3 bucket names to the private IP address of the gateway/LB
- On the Aviatrix controller, configure allowed S3 bucket names
- Aviatrix Gateway uses its FQDN feature to allow only approved S3 buckets

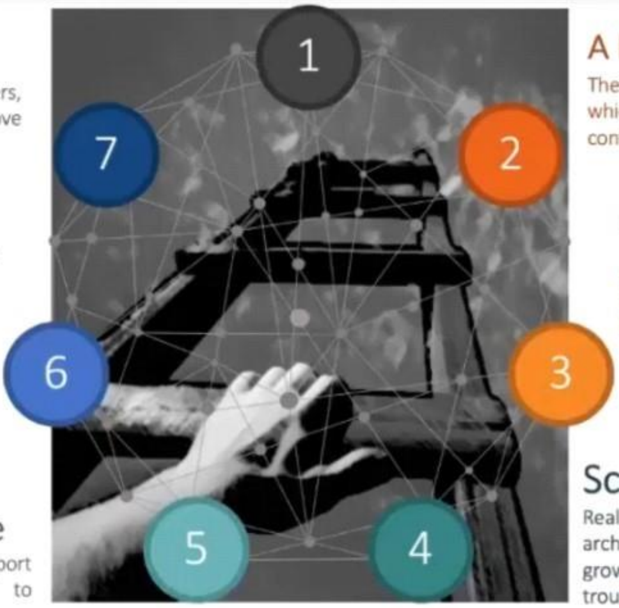


Smart SAML VPN

- Supports multiple profiles
  - Isolation between employees and contractors
  - Isolation between various developers
- Automated firewall rules
- Security based on user, not source IP
- Security rules only applied when user is active, otherwise gets automatically removed from Gateway
- Supports both Split and Full Tunnel modes
- Any OpenVPN client is supported
  - For authentication with IDP, you need Aviatrix VPN client

Operations

Operational Challenges in Public Cloud



Evidential Data

When working with Cloud Providers, often customer is challenged to prove providers fault/issues

Unfamiliar Toolset

Native cloud lacks familiar tools like ping, packet capture, traceroute

Blackbox – No visibility

Native cloud constructs want you to trust all is well always. No visibility into logs, current state, routing tables etc.

Infrastructure as Code

Solves agility problem, creates support issues as tier-1 is not able to troubleshoot code problems

A Flat World in Public Cloud

There is a lack of hierarchy in the cloud which means its hard to insert security, control and visibility

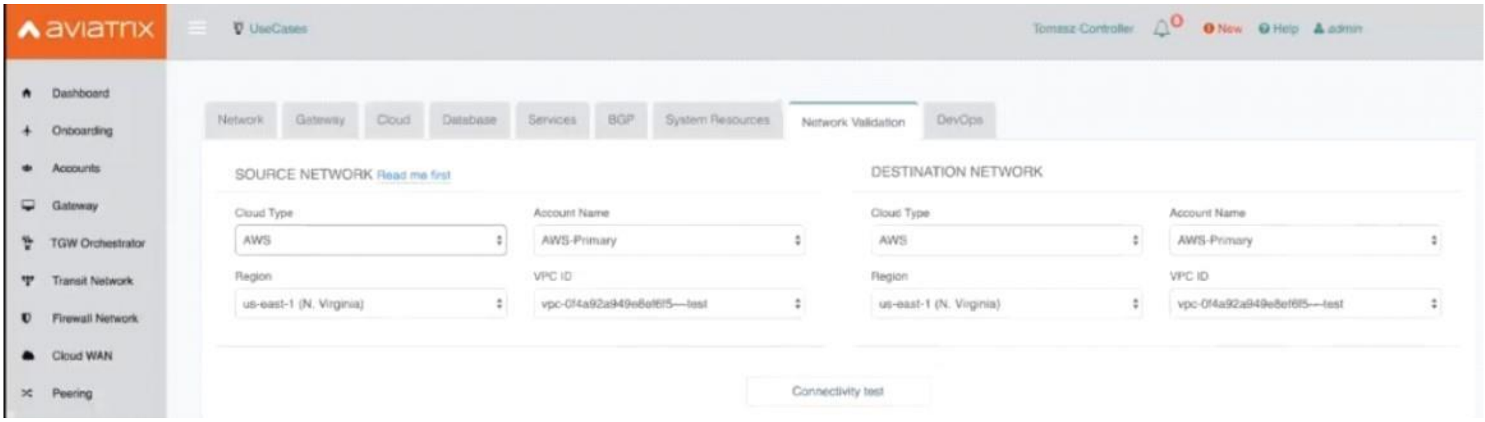
Tier-3 becomes Tier-1

Frontline support teams don't have the skill and tools in public cloud requiring senior network engineers to assist with most support issues

Scaling Out

Real problems are experienced when architecture scales out as it very quickly grows to be complex and very hard to troubleshoot

Troubleshooting network issues are really complex and needs a lot of time and thorough understanding of network topology.
Aviatrix provides bunch of sophisticated network troubleshooting tools.



SOURCE NETWORK

Cloud Type: AWS

Account Name: AWS-Primary

Region: us-east-1 (N. Virginia)

VPC ID: vpc-0f4a92a949e8ef6f5---test

DESTINATION NETWORK

Cloud Type: AWS

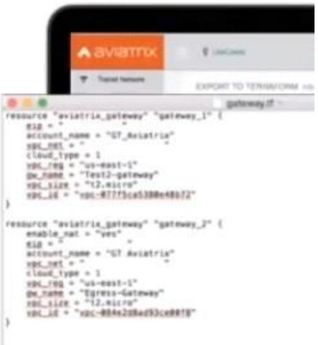
Account Name: AWS-Primary

Region: us-east-1 (N. Virginia)

VPC ID: vpc-0f4a92a949e8ef6f5---test

DevOps Automation

- Automation
- DevOps Workflows
- Export to Terraform
- CloudFormation
- Official Terraform Provider

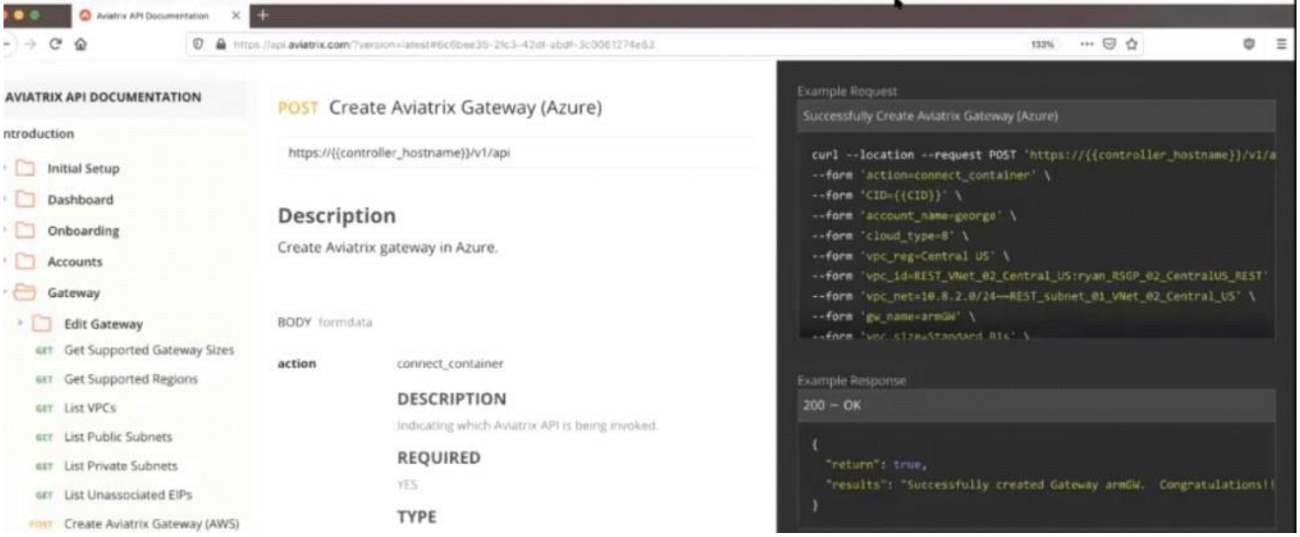


```
resource "aviatrix_gateway" "gateway_1" {
    eip = "              "
    account_name = "GT_Aviatrix"
    vpc_net = "                    "
    cloud_type = 1
    vpc_reg = "us-east-1"
    gw_name = "Test2-gateway"
    vpc_size = "t2.micro"
    vpc_id = "vpc-077f5ca5300e48b72"
}

resource "aviatrix_gateway" "gateway_2" {
    enable_nat = "yes"
    eip = "              "
    account_name = "GT Aviatrix"
    vpc_net = "                    "
    cloud_type = 1
    vpc_reg = "us-east-1"
    gw_name = "Egress-Gateway"
    vpc_size = "t2.micro"
    vpc_id = "vpc-084e2d8ad93ce0818"
}
```

Infrastructure as Code with REST API

https://api.aviatrix.com


Aviatrix API Documentation
https://api.aviatrix.com/?version=latest#6c6bee35-2fc3-42df-abdf-3c0061274e53
132%
AVIATRIX API DOCUMENTATION
ntroduction
Initial Setup
Dashboard
Onboarding
Accounts
Gateway
Edit Gateway
GET Get Supported Gateway Sizes
GET Get Supported Regions
GET List VPCs
GET List Public Subnets
GET List Private Subnets
GET List Unassociated EIPs
POST Create Aviatrix Gateway (AWS)

POST Create Aviatrix Gateway (Azure)

https://{{controller_hostname}}/v1/api

Description

Create Aviatrix gateway in Azure.

BODY formdata

action connect_container

DESCRIPTION

Indicating which Aviatrix API is being invoked.

REQUIRED

YES

TYPE

Example Request

Successfully Create Aviatrix Gateway (Azure)

```
curl --location --request POST 'https://{{controller_hostname}}/v1/a
--form 'action=connect_container' \
--form 'CID={{CID}}' \
--form 'account_name=george' \
--form 'cloud_type=8' \
--form 'vpc_reg=Central US' \
--form 'vpc_id=REST_VNet_02_Central_US:ryan_RSGP_02_CentralUS_REST'
--form 'vpc_net=10.8.2.0/24~~REST_subnet_01_VNet_02_Central_US' \
--form 'gw_name=armGW' \
--form 'vpc_size=Standard_B1s' \
```

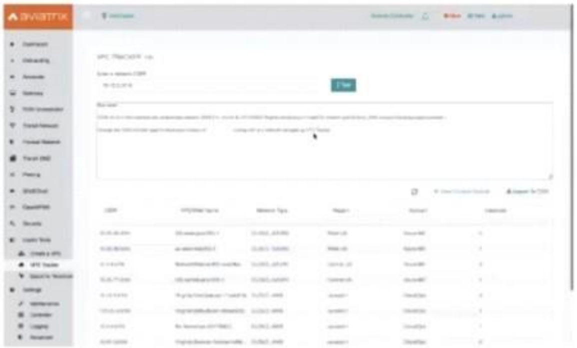
Example Response

200 – OK

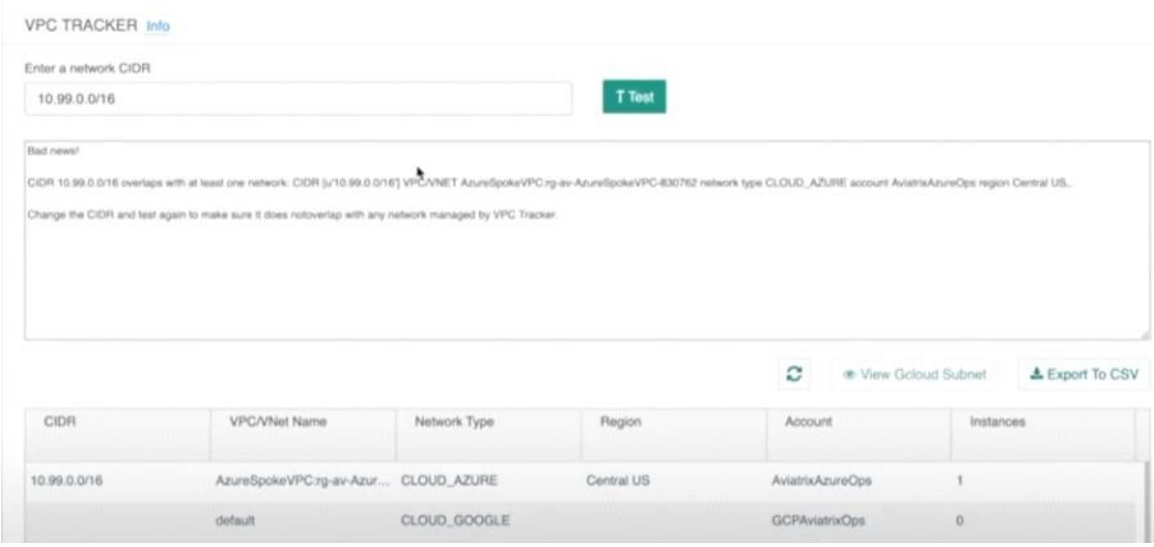
```
{
  "return": true,
  "results": "Successfully created Gateway armGW.  Congratulations!!
}
```

VPC Tracker

- Automatically collects and helps you manage your network CIDR ranges at a central place
  - Eliminates the need to keep an Excel sheet on VPC network addresses
- No Gateway launches are required
  - Just add accounts to the Controller
- Records CIDRs in AWS, Azure, Site2Cloud remote network CIDRs and Transit Network on-prem CIDRs
  - Displays VPCs with at least 1 running instance
  - VPC Tracker auto updates once a day
- On-demand test to detect overlapping CIDRs before creating a new one



VPC Tracker is similar to IP Management tool with few advancement.



Enter a network CIDR

10.99.0.0/16

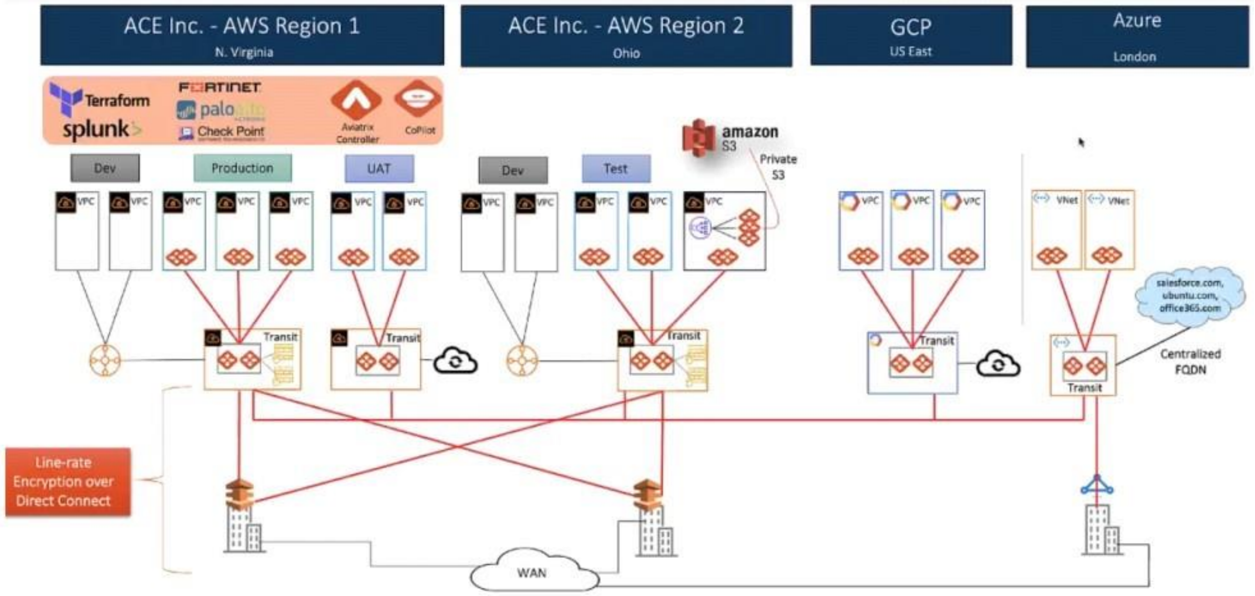
```
Bad news!

CIDR 10.99.0.0/16 overlaps with at least one network: CIDR [u'10.99.0.0/16'] VPC/VNET AzureSpokeVPC:rg-av-AzureSpokeVPC-830762 network type CLOUD_AZURE account AviatrixAzureOps region Central US,.

Change the CIDR and test again to make sure it does notoverlap with any network managed by VPC Tracker.
```

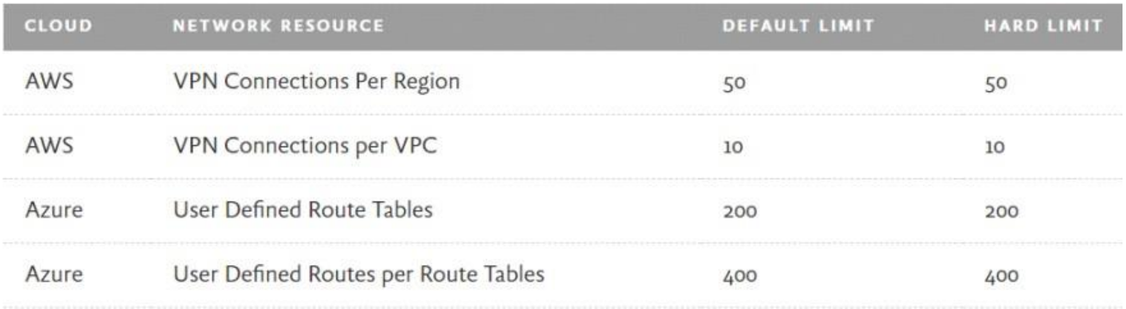
CIDR	VPC/VNet Name	Network Type	Region	Account	Instances
10.99.0.0/16	AzureSpokeVPC:rg-av-Azur...	CLOUD_AZURE	Central US	AviatrixAzureOps	1
	default	CLOUD_GOOGLE		GCPAviatrixOps	0

Reference Architecture for Public Cloud



Aviatrix and Cloud Native Construct Limitations (AWS & Azure)

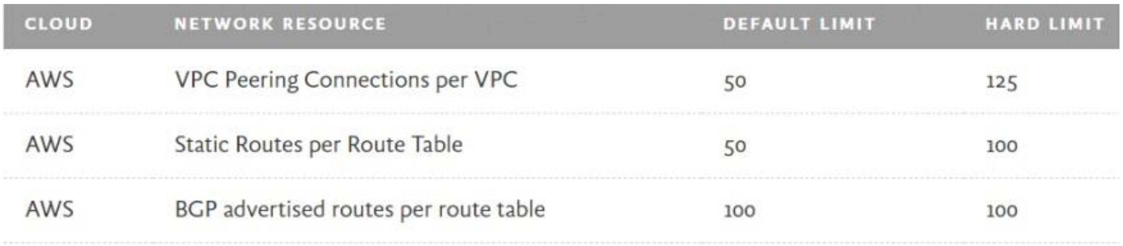
VPN Connection Limits



CLOUD	NETWORK RESOURCE	DEFAULT LIMIT	HARD LIMIT
AWS	VPN Connections Per Region	50	50
AWS	VPN Connections per VPC	10	10
Azure	User Defined Route Tables	200	200
Azure	User Defined Routes per Route Tables	400	400

💡 **Aviatrix Site2Cloud feature is an easy, manageable way to overcome these provider limits on VPN connectivity. It also has advanced features like handling overlapping IP addresses.**

Peering and Routing Table Limits

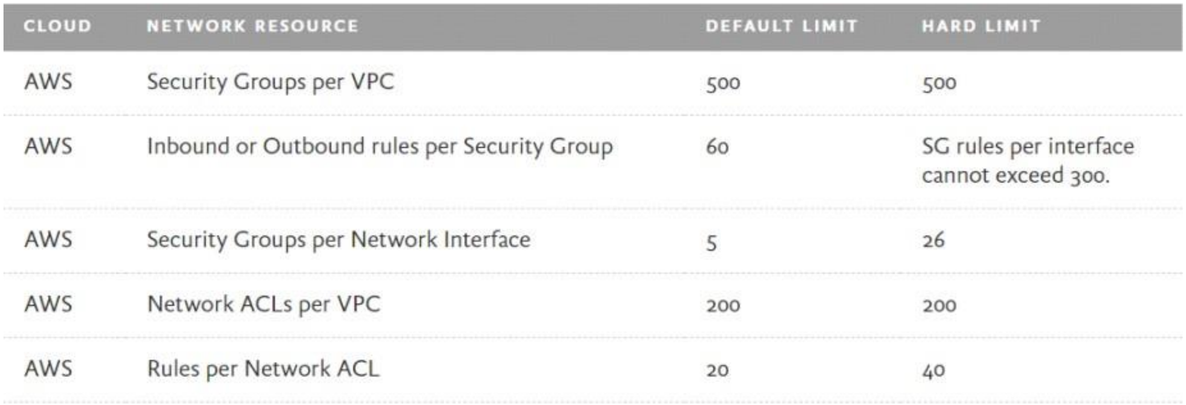


CLOUD	NETWORK RESOURCE	DEFAULT LIMIT	HARD LIMIT
AWS	VPC Peering Connections per VPC	50	125
AWS	Static Routes per Route Table	50	100
AWS	BGP advertised routes per route table	100	100

Amazon's route table has a hard limit of 200 routes total per VPC. 50 non-propagated routes (Static) and 100 propagated routes (through BGP) per routing table.

💡 **Aviatrix AVX Gateways** offer encrypted, high performance peering without filling up the Cloud Route Tables.

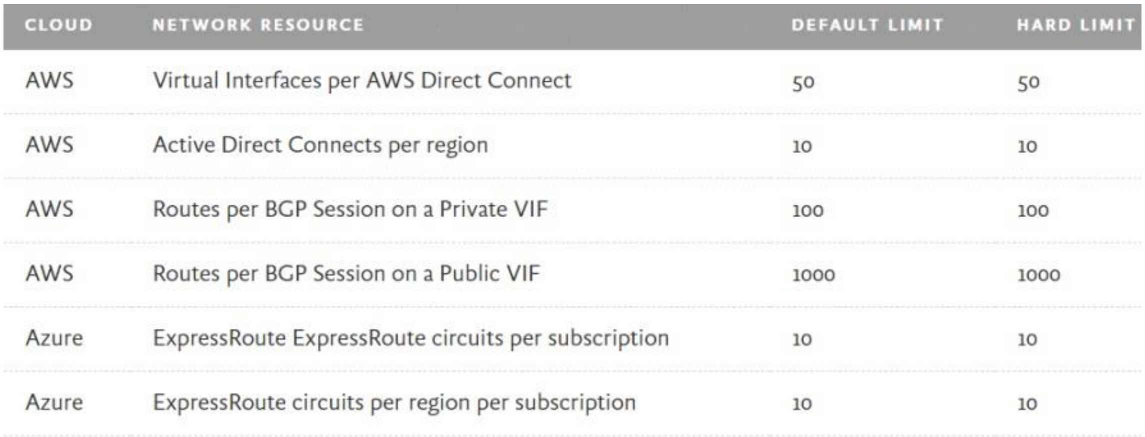
Security Groups and NACL Limits



CLOUD	NETWORK RESOURCE	DEFAULT LIMIT	HARD LIMIT
AWS	Security Groups per VPC	500	500
AWS	Inbound or Outbound rules per Security Group	60	SG rules per interface cannot exceed 300.
AWS	Security Groups per Network Interface	5	26
AWS	Network ACLs per VPC	200	200
AWS	Rules per Network ACL	20	40

💡 Aviatrix can operate as a light-weight stateful firewall (layer 4) to avoid cumbersome host level security configurations.

Limits of Peering, Route Table Entries, Direct Connenct and ExpressRoutes



CLOUD	NETWORK RESOURCE	DEFAULT LIMIT	HARD LIMIT
AWS	Virtual Interfaces per AWS Direct Connect	50	50
AWS	Active Direct Connects per region	10	10
AWS	Routes per BGP Session on a Private VIF	100	100
AWS	Routes per BGP Session on a Public VIF	1000	1000
Azure	ExpressRoute ExpressRoute circuits per subscription	10	10
Azure	ExpressRoute circuits per region per subscription	10	10

- **Aviatrix transit** is a software defined, low TCO solution so you can practice network-as-code and scale beyond provider limits.

References

Friday, July 10, 2020 11:59 PM

https://community.aviatrix.com
Webinar: Multi Cloud Network Specialist
https://aviatrixsystems.github.io/terraform-solutions/pages/mcna-video-series/
https://github.com/cloudcommunity/Certification-Study-Guides/tree/master/Aviatrix
https://community.aviatrix.com/

aviatrix

Aviatrix Certified Engineer

The Aviatrix Certified Engineer (ACE) program is the first multi-cloud networking and security certification available to technical professionals and cloud practitioners. The ACE certification prepares engineers and operations staff with the working knowledge of native networking constructs in AWS, Azure, Google Cloud, and Oracle Cloud Infrastructure as well as the proficiency to build use cases and multi-cloud architectures using Aviatrix software.

ISSUEDTO

Surender Aireddy

ACECERTIFICATIONLEVEL

Multi-Cloud Networking Associate

ACECERTIFICATIONNUMBER

2021-9479

VALIDTHROUGH

January 05, 2024

ISSUEDBY

Nauman Mustafa

Nauman Mustafa
VP Solutions Engineering
Aviatrix
2901 Tasman Drive
Santa Clara, CA

Aviatrix reserves the right to make any modifications to the ACE program, and/or revoke your certification designation at any time, without notice.