Aviatrix Certified Engineer
Multi-Cloud Network Associate

* About Aviatrix -

→ Public Cloud Networking & Security Product helping enterprises build - fast & right.

→ Provides Multi-Cloud Networking & Security reference architecture. (MCNA)

→ Defines Best Practices for building & operationalizing in Public Cloud.

→ Multi-Region, Multi-cloud ready.

Section 1 - Public Cloud Networking

* Networking Principles in the Cloud -

→ Needs of Businesses / Apps changed over the years.

→ On-Prem is slow.
↳ Hence, DevOps moved to the cloud.

→ Cloud is a New Data Center in the Enterprise Networking Transformation to Cloud.

→ But there is no Multi-Cloud Network Architecture & Customer has no access to underlying infrastructure.

* IaaS, PaaS, SaaS

1	Applications
2	Data
3	Runtime
4	Middleware
5	O/S
6	Virtualization
7	Servers
8	Storage
9	Networking

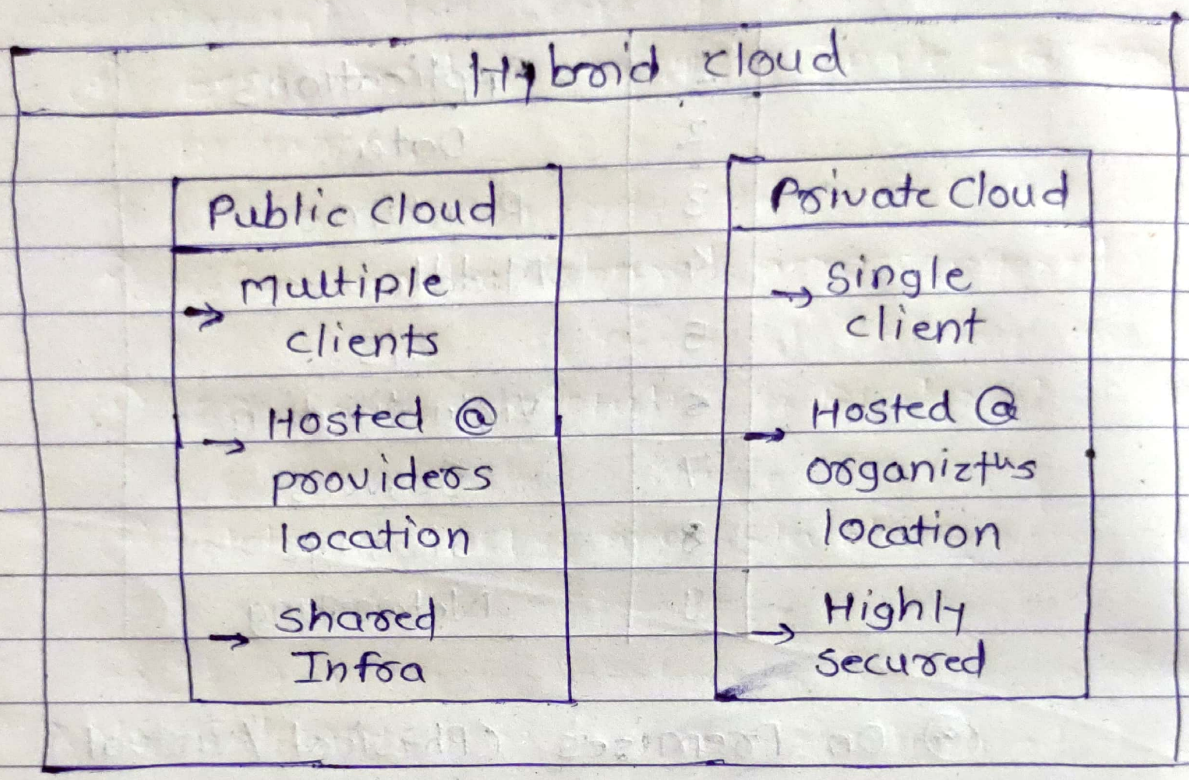
(*) On-Premises (Physical / Virtual)
- ↳ You Scale, make resilient & manage
- ↳ All through 1 to 9

(*) IaaS
- ↳ You Scale, make resilient & manage.
- ↳ All through 1 to 5, rest by CSPs.
- ↳ e.g. Azure VMs

(*) PaaS
- ↳ You manage (1 & 2)
- ↳ Scale, resilience & mgmt by CSPs. (3 to 9)
- ↳ e.g. Azure Cloud Services

(*) SaaS
- ↳ You just consume the service.
- ↳ Scale, Resilience & mgmt by CSPs (All through 1 to 9)
- ↳ e.g. Office 365, Salesforce, etc.

* Cloud Deployments -



* Public cloud Basics -

→ Public cloud is just someone else's data center!
↳ Your DC is/was not perfect & had issues, same is the case with cloud service Provider's DC,
↳ Except you have no visibility over it, neither the control.

DataCenter

→ CSPs use DCs to host cloud services & cloud-based resources.
→ Faster & Automated

Region

→ DCs are grouped in Regions & geographic areas to provide regional service availability.

Availability zones

→ Distinct locations within CSPs network that are engineered to be isolated from failures in other AZs

* AWS Networking 101

⊛ AWS services

EC2 → VM Instances
IAM → Identity & Access Mgmt
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

⊛ Subnet is confined to a single AZ.
⊛ Subnets in the same VPC can talk to each other.

(*) Security Groups can only be used in a single VPC.

(*) Best practice to use Single SG per instance.

(*) SGs can be shared across peered VPCs.

(*) SGs are Stateful. (Bi-directional)

(*) Network ACLs are Stateless

(*) AWS Gateways -

(1) Internet Gateway (IGW)
→ AWS Router that provides internet access from VPC.

(2) NAT Gateway (NGW)
→ for instances in private subnets to get Internet Access
→ only for connections that the instance initiates.
→ No SSH allowed to the instance from outside.

(3) Transit Gateway (TGW)
→ A Network transit hub that can interconnect VPCs & on-prem networks.

④ VPN Gateway (VGW)

→ AWS VPN Router that links on-prem network to VPC.

→ Can be a physical or software appliance.

→ Anchor on the AWS side of VPN connⁿ is called Virtual Private Gateway.

⑤ Customer Gateway (CGW)

→ A customer VPN router connects with VGW / TGW / DXGW

⑥ Direct connect Gateway (DXGW)

→ Scalable Direct connect connectivity to VPCs across accounts & regions.

⊛ AWS Transit Gateway (TGW) Fundamentals

→ Native Service

→ Its a fleet of ec2 instances.

→ You Attach a VPC to TGW

→ 5000 Attachments per TGW.

→ 50 Gbps VPC ↔ TGW throughput

→ can have multiple route tables in TGW

→ Also has VPN attachment type

⊛ → AWS specific.

⊛ AWS Native Transit Limitations (TGW)

→ Manual VPC Routing Table mgmt.
  ↳ Initial creation
    ↳ Subsequent Updates
      ↳ VPC to VPC Routes
      ↳ Propagating on-prem routes to spoke VPC route table.
      ↳ Network correctness

→ If you are connecting a on-prem site through VPN, you are limited to a throughput of 1.25 Gbps.

→ TGW Route Scalability
  ↳ Maximum 100 BGP routes per RT.
  ↳ No VPC CIDR summarization

→ Limited static Multi-Region support.

→ No overlapping IP support.

→ Native firewall Insertion has performance limitation.

→ No ITGW peering support within a region.

⊛ TGW & RT orchestration by Aviatrix

→ Removes VPC peering limitations & complexities.

→ Orchestrates VPC routing tables.

→ Simplifies BGP over Direct Connect.

→ Provides additional route control & traffic engineering options.

→ Propagates on-prem routes to VPC

→ New CIDRs/ VPC routes updated on all other VPCs

* Azure Networking 101 -

⊛ Azure Networking components -

1. VNet (Virtual Network) - (VPC)
2. Availability Zones
3. Network Security Groups
4. Public & Private IP Addresses
5. VNet Gateways
6. VNet Peering
7. Routing : User Defined Route, BGP & System Routes
8. Network Virtual Appliance (NVA)

(*) Transit in Azure -

→ Most imp part of any cloud network.

→ It provides intra-region, inter-region & inter-cloud connectivity.

(*) 3 Deployment models for Intra-region traffic:

(1) Via ExpressRoute Edge Routers -

→ Uses the shared ExpressRoute edge router as a transit for inter-VNet connectivity.

→ common method to start for many.
- ↳ Easy to start with but poses severe issues in long term.
- ↳ Default any to any for all spokes
- ↳ Limited visibility & control.

→ Not officially documented.

→ Sub-optimal traffic paths
- ↳ Hair pinning via ER Edge Router
- ↳ Traffic behaviour changes when single region vs multi-region.

→ BW limited to ExpressRoute Gateway (ERGW) SKU.

② Using Network Virtual Appliance -

→ Uses Azure FW or a 3rd party appliance for transit connectivity.

→ common method for security
  ↳ can provide NGFW features.
  ↳ Manual scaling & HA.
  ↳ Intra VNet traffic is SNATd.
  ↳ No encryption for intra-VNet traffic.

→ challenges in manageability.
  ↳ BW limited to NVA BW.
  ↳ UDR mgmt at scale is problematic.
  ↳ Long failover times
  ↳ If NVA is being used as FW then you need SNAT.

→ Routing
  ↳ UDR required in Spokes
  ↳ change of CIDR in VNet requires you to break peering.

③ VNet Peering

→ Preferred method by Microsoft
→ No real BW limitation
→ 1-to-1 mapping & doesn't scale
→ No granularity
→ VNet Peering data charges for ingress & egress in both directions.
→ VNet Peering needs to be broken to add CIDR/subnets to a VNet.

(*) 3 options for Inter-region transit :

→ Same 3 options as IntraRegion but with some nuances.

(1) ExpressRoute Hairpinning
↳ No summary or Default Required.

(2) NVA -
↳ Requires additional peerings & UDRs for Hub to Hub.

(3) Peering -
↳ only difference is in naming convention & cost - Global VNet peering

(*) Azure Virtual WAN

→ A big hub providing connectivity for all types of entities in Azure or connecting to Azure.

Challenges & Design considerations :

→ Not multicloud friendly
→ Cost: Need to buy 'all or nothing'
→ No 3rd party device support in hubs
→ No NAT capability
→ Limited troubleshooting & visibility
→ Several features still in preview

* GCP Networking 101 -

⊛ Resources in GCP

① Global

→ can be accessed by any other resource, across regions & zones.

→ e.g. Creating a VPC is global operation bcoz a Network is a Global resource.

② Regional

→ Resources can be accessed by other resources that are in the same region.

→ e.g. Reserving an IP address is a regional operation bcoz the address is a regional resource.

③ Zonal

→ Resources can be accessed only by resources that are in the same zone.

→ e.g. Disks can only be attached to VMs 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 & other metadata that describe applications

→ contains computing, Storage & networking resources.

* → A project cant access another project's resources unless you use

↳ Shared VPC or
↳ VPC Network Peering

* Basic GCP Networking components -

① VPC / Subnets -
→ VPC in GCP is a Global resource.
→ Subnets in the same VPC can talk to each other.

② VPC Peering - (Non-transitive)
→ VPC peering enables two VPCs to talk to each other.

③ VPN Gateway -
→ To connect to the on-prem.

④ Implicit Routing -
→ No public / private subnets.

⑤ Global Routing -

→ Since VPC is a Global resource, all the subnets, irrespective of region are inherently routable within a VPC.

→ In traditional VPC
↳ subnet & VPC are regional

→ In GCP VPC
↳ VPC is global, Subnets are regional.

→ Projects can contain multiple VPC networks.

④ VPC Networks & Subnets

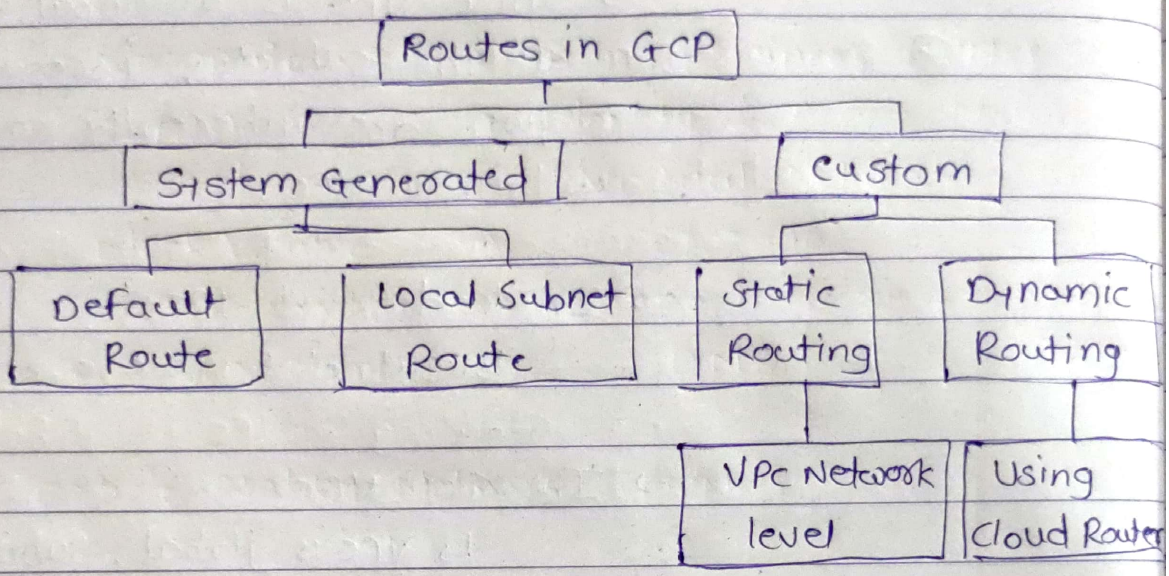
→ VPC Networks consist of one or more subnets.

→ VPC Networks dont have any IP address ranges associated with them.
↳ IP ranges are associated at subnet level.

→ VPC subnets can be created in:
① Auto mode - subnets in each region

② Custom mode - VPC Network starts with no subnets.
↳ You can create more than one subnet per region.

⊛ Routes in GCP -



⊛ Transit (Inter-VPC) Networking

→ Lacks native Transit solution to inter-connect VPCs :
  ↳ VPC Peering is preferred
  ↳ Preaching Single VPC

⊛ Cloud Interconnect

→ connect your on-prem network to GCP VPC network through a private connection.

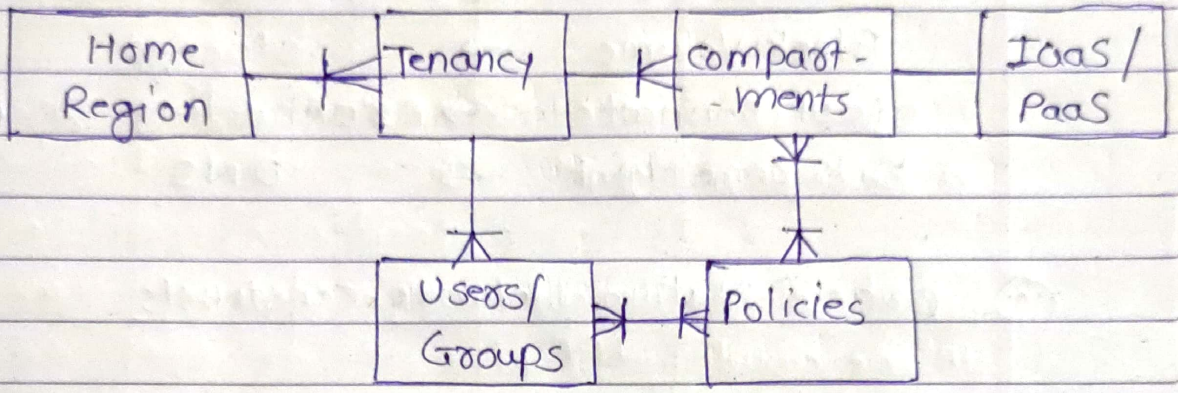
→ Not Encrypted.

① Dedicated Interconnect
  → 10 Gbps or 100 Gbps pipes
  → connect directly to GCP

② Partner Interconnect
  → 50 Mbps to 10 Gbps

* OCI Networking 101 -

⊛ Oracle OCI organizational structure



Tenancy

→ master paying account.

→ Tenancies are setup in a Home Region.

IAM Resources -

→ Users / Groups exist within a Tenancy.

→ Their metadata is bound to Home region

Compartments

→ logical containers used to isolate resources.
i.e. Business Units or Projects.

Policies

→ Define who can perform actions on resources tied to a compartment.

(*) Oracle Important services

compute → Run instances (VMs)
IAM → Identity & Access Mgmt
VCN → Virtual Network
Block Volume → storage
fast Connect → connecting on-prem
DNS Zone Mgmt → DNS

(*) Oracle Native Network constructs

(1) DRG (Dynamic Routing Gateway)
→ Virtual Router that provides a single point of entry for remote network paths coming into your VCN (IPSec VPN + fastConnect)

(2) SG (Service Gateway)
→ Service Gateway is regional & enables access only to supported Oracle services in the same region as VCN.

(3) IG (Internet Gateway)
→ Provides a path for network traffic between your VCN & the Internet.

(4) Subnet
→ Regional, spanning Availability Domains.

(5) Route Table
→ Set of route rules that provide mapping for traffic from subnets via gateways to destn outside VCN.

⊛ OCI VCN Peering

challenges

- → Route Table Mgmt
- → Max of 10 LPG's per VCN
- → max of 10 RPCs per Tenancy
- → Max of 10 VCNs per Region
- → Max of ~~10~~ 5 DRGs per Region
- → No Overlapping IP
- → Lack of Visibility.

→ Within a Region, Local Peering Gateways (LPGs) are used to peer VCNs.

→ When spanning Regions, Dynamic Routing Gateways are needed.

⊛ OCI Azure MVP

→ No FastConnect / ExpressRoute required.

→ Aviatrix Terraform provider can spin up OCI <> Azure Transit Infrastructure in under 30 mins.

→ Automated / nomous NACL Limited to Aviatrix Transit spoke VCN.

Section 2 - Multi-Cloud Network Architecture

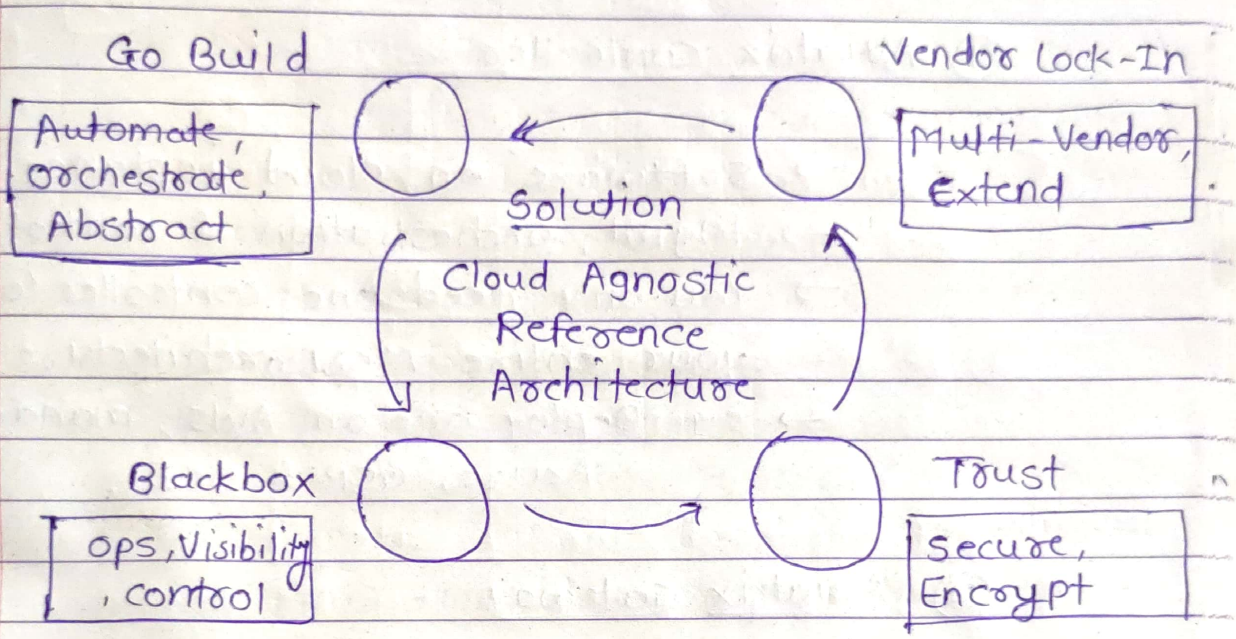
Construct	on-prem DC	AWS	Azure	GCP	OCI
Physical DC in the region	DC	Az	AZ	zone	AD (Domain)
Logical Isolation in the cloud	Tenant / VRF	VPC	VNet	VPC	VCN
VM / Server	Server / VM	AMI / EC2	VM	VM	VM
Private link to on-prem DC	DCI	Direct Connect	Express Route	Cloud Inter-connect	FastCo--nnect
Multi-Tenants	Tenant / customer	Account	Sub-Scription	Project	compa--rtment

① Cloud 1.0 - ~2006 - 2014

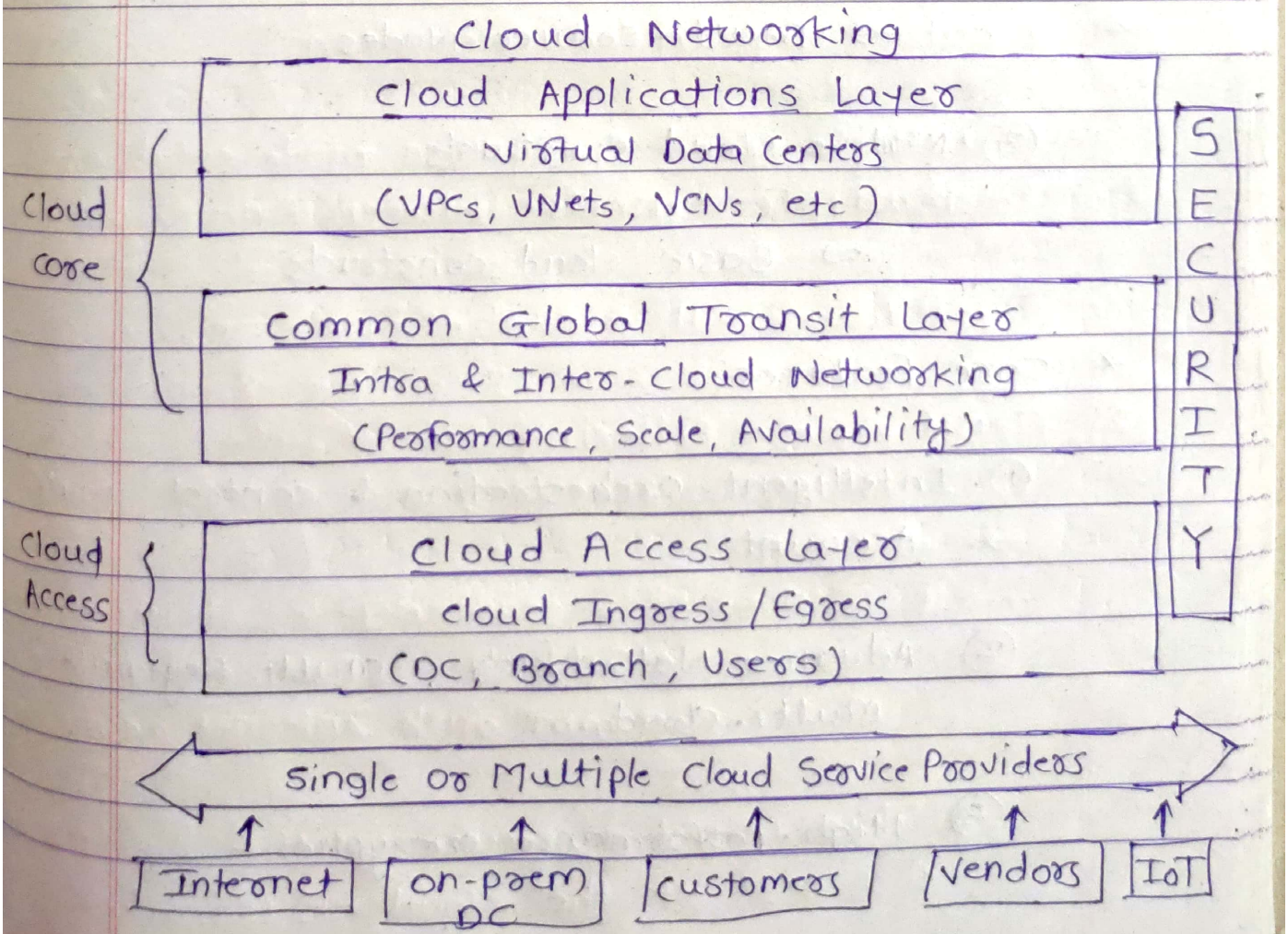
② Cloud 2.0 - ~2014 - 2019

③ Cloud 3.0 - Late 2019 & Beyond

⊛ Customer challenges in Public cloud & Aviatrix Solutions -



⊛ Multi-cloud Network Architecture -



Section 3 - Aviatrix Platform

* Aviatrix Software components -

① Aviatrix controller -

→ Software on cloud instance
→ Mgmt, orchestration & control plane.
→ You only need one controller to manage your entire MCN architecture.
→ e.g. Deploy one on AWS, manage AWS, Azure, GCP & OCI.

② Aviatrix Gateway -

→ Software on cloud instance
→ Data plane
→ Multi-service Nodes

③ Native Cloud Constructs -

→ Basic cloud constructs.

* Core features -

① Intelligent orchestration & control, Multi-Account.

② Advance Networking, Multi-Region & 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

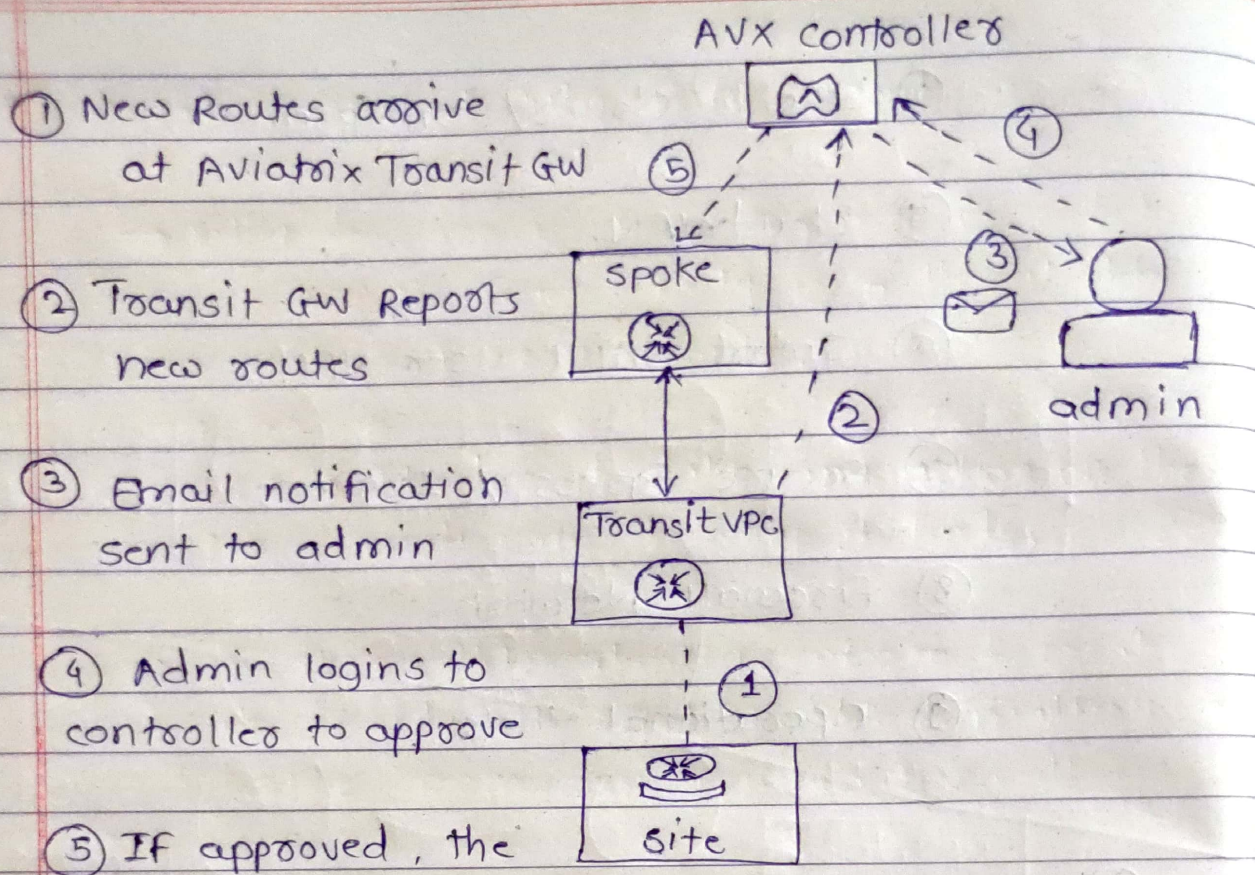
✱ Characteristics of Aviatrix Transit Arch.

① well-rounded architecture
- ↳ centrally managed
- ↳ Robust connectivity
- ↳ Scale-out repeatable arch.
- ↳ End-to-end network awareness
- ↳ Simplified service-chaining (NGFW)
- ↳ operational visibility & troubleshooting.

✱ BGP Route Approval

→ can explicitly approve any BGP-learned route from on-prem into the cloud network.

→ Prevents unwanted advertisement of routes such as 0/0.



⊛ Aviatrix High Speed Encryption

→ High speed encryption mode establishes multiple tunnels between Aviatrix Gateways.

→ Utilizes all available CPU cores.

⊛ FQDN Egress Filtering -

→ why ?

→ Workloads require Internet access
↳ Github ↳ Download patches
↳ comm^n with Internet resources

→ This is not a secure way & highly risky for rest of the cloud environment.

→ Aviatrix FQDN is a highly available security service specifically designed for workloads or applications in the public cloud.

→ It is centrally managed by the controller & executed by an Aviatrix Gateway Instance in the VPC in the distributed or centralized architecture.

→ It filters internet bound egress traffic initiated from VPCs.

→ Filters any TCP & UDP traffic including HTTP, HTTPS & SFTP traffic.

→ Filtering function allows only the destination host names (whitelist/blacklist) specified in the list to pass or drop all other destinations.

→ Supports wildcards & tags

→ Supports both private & public network filtering.

→ Supports instances in private/public subnets.

→ Supports NAT.

Deployment Models

① Centralized Egress
② Distributed Egress

(*) Aviatrix Guard Duty Enforcement

→ Why ?

↳ AWS Guard Duty is a threat detection (IDS) service only.

↳ It doesnt take any action on the malicious activity it finds.

→ Aviatrix automatically enforce & creates a rule inside the GW to block malicious traffic from coming in.

→ Programmatically Pulls threat intelligence from Guard Duty.

* Firewall Service Insertion

Why ?

→ Security Policy mandates that certain or all traffic must go through a firewall.

↳ Business Drivers : Security, Compliance, Audit, etc.

↳ Technical Need : NGFW, DPI, IDS/IPS, etc

→ Traffic could be East-West or North-South

↳ East-West : (VPC ↔ VPC || VPC ↔ on-prem)

↳ North-South : (Egress : To Internet || Ingress ; From Internet)

* Aviatrix Firewall Network -

→ Utilizes full performance of firewalls.

→ Sits in a Transit VPC / VNet.

→ Each AZ can have max of 10 firewalls.

→ Upto 70 Gigs of throughput.

* Aviatrix AWS TGW Firenet -

→ Active / Active Firewalls
  ↳ Maximising 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.

Advantages
  ↳ NO IPsec needed betn TGW & FW.
  ↳ No BGP required
  ↳ No SNAT
  ↳ Maintain Session Stickiness

  ↳ Monitor FW health for failover
  ↳ Zero-touch VM-series deployment.
  ↳ Bootstrap firewalls for ease of config.
  ↳ Integration with Panorama.

* Aviatrix Security Domain -

→ Provides isolation & segmentation between VPCs.

→ Group VPCs with similar security policies.

Types of security domains:

① Firewall Domain
↳ Any type of traffic (EW/ NS) redirection to firewalls)

② VPC Domains (user created)

③ Shared Services Domain

④ Default Domain

(*) VPCs in diff. SD can talk to each other through a conn^n policy.

* Aviatrix Azure Native Peering Firenet

→ Active / Active firewalls.

→ Spoke VPC Inspection policy for easier mgmt.

→ No encryption without Aviatrix Gateways in the Spoke VNets.

* Aviatrix Private S3 -

→ Without Aviatrix, the only way to access S3 over DX (Direct connect) is to advertise the public S3 IPs over DX to on-prem.

→ But this also gives access to all possible S3 buckets the users have access to, such as their personal buckets.

→ So this could lead to info. leak and/or excess data usage, bcoz of people sending data to their personal S3 buckets over the corporate DX connection.

What Aviatrix Private S3 does:

→ Transfers objects betn on-prem & S3 by leveraging direct connect without using public ~~Iff~~ VIf.

→ controls which S3 buckets can be accessed.

→ scale out architecture to load balance traffic to S3.

* Aviatrix site to Cloud

→ Builds an encrypted connection betⁿ two sites over the Internet, in an easy & template driven manner.

→ On one end of the tunnel is an Aviatrix GW.

→ On the other end could be a on-prem router, firewall or another public cloud VPC/VNet where the Aviatrix Controller does not manage.

→ Supports both TCP & UDP tunnels.

→ Supports overlapping IPs.

* CloudWAN -

① Aviatrix controller logs in to CISCO IOS branch routers.

② Aviatrix Controller automatically configure VPN & BGP settings to attach existing IOS routers to Aviatrix Transit GW, with AWS Global Accelerator Service.

* User VPN -

→ Connects users to public cloud resources.

→ No need to back-haul to on-prem DC first.

→ Least latency accessing cloud resources.

→ Automated firewall rules.

→ Security based on User, not source IP.

→ Supports both Split & full tunnel modes.

→ Supports multiple profiles.

Section 4 - Operations, Visibility & Troubleshooting

* Operational challenges in cloud -

1. A flat world in Public cloud
2. Tier-3 becomes Tier-1
3. Scaling out
4. Infrastructure as a Code
5. Blackbox - no visibility
6. Unfamiliar Toolset
7. Event Evidential Data

* Controller HA

→ Aviatrix Controller HA in AWS leverages following native AWS constructs to perform monitoring :

↳ S3 based backup
↳ An auto scaling group
↳ SNS
↳ Lambda function

→ When a new controller is launched

↳ Existing controller is terminated
↳ EIP is associated to the newly launched controller.
↳ Existing config is restored.

→ Aviatrix supplies Cloudformation stack.

* VPC Tracker :

→ Automatically collects & helps you manage your network CIDR ranges at a central place.

→ No Gateway launches are required.
↳ just add accounts to controller.

→ Records CIDRs in AWS, Azure, on-prem.

→ on-demand test to detect overlapping CIDRs before creating new one.

* TGW Route Audit -

→ Allows you to audit & immediately discover the missing routes in Spoke VPC route tables & its associated TGW route tables.

* TGW Audit

→ Audits all route entries of attached VPC route tables in addition to route entries in TGW Route tables.

* VPC Diagnostics -

→ Provides info for a specific VPC / VNet such as:

- ↳ Tags
- ↳ CIDR
- ↳ ACLs
- ↳ SGs
- ↳ DHCP options
- ↳ Subnets
- ↳ Route Tables
- ↳ VM configs.

* chargeback -

→ Shows deployment per account.

- ↳ No. of encrypted Spoke GWs
- ↳ No. of VPC attachments, etc.

(*) Hitless Upgrades

(*) Security Patches

(*) High Availability

* Aviatrix MCN Architecture -

(1) Cloud Core -

→ Directly programs & controls native cloud networking constructs.

→ End-to-End encryption.

→ High performance & high availability.

→ Intelligent orchestration & control.

→ Central multi-cloud controller

→ Simplified integrations.

2 sub-divisions within Cloud Core:

A] Applications Layer
- → This is where applications are.
- → Apps could be sitting in VPC/VNET & running as instances or VMs.
- → Area where apps are deployed.

B] Global Transit Layer
- → main point of connection for every aspect of the cloud.
- → Inserts services in its platform, through service insertion framework.

(*) Transit Networking

→ Transit arch. is about building connectivity between cloud & on-prem.

→ In Transit Architecture :

↳ one connection (not including the backup) betn on-prem & a transit VPC.

↳ Everything else (spoke VPCs to on-prem traffic) is routed through the transit VPC.

→ All ~~Active~~ Aviatrix Transit Network should be deployed in ActiveMesh mode.

→ When AWS/Azure VGW carries more than 100 routes, its BGP session will crash unexpectedly, resulting in Network outage.

↳ Solutions

① Enable Spoke VPC route summarization so that transit GW advertise as few routes to VGW as possible.
Aviatrix controller sends alerts when total routes by VGW > 80.

② Bypass VGW
To permanently solve, use External Device option to connect to on-prem directly over Direct Connect or Internet.

⊛ Traffic Engineering

→ Aviatrix Controller runs & understands various routing stacks.

→ Examples of where routing stacks are being invoked:

① Static - Programmed in VPC / VNET
② BGP - Programmed when connecting to on-prem routers / firewalls, etc.
③ Software Defined (SD) - AVX-CTRL builds SD Routing overlay using Transit & Spoke gateways.
④ Cloud Native - AVX-CTRL manages AWS-TGW, Azure VNET, GCP VPC Routes & Azure Virtual WAN.

Route Approval

→ AVX TGW dynamically learns BGP routes from remote sites, which are reported AVX-CTRL which in turn programs route entries to Spoke VPC Route table.

Edge Segmentation

→ Allows you to specify edge segments on AVX TGW & which AWS Security Domain each of these segments can communicate with.

(*) TGW Plan -

→ AWS Transit GW orchestrator plan is the first stage in deploying a AVX Transit Network using AWS TGW.

→ Plan stage consist of 4 sections:

1. Create AWS Transit GW
2. Create Segmented Network
3. Create Hybrid, multi-region or multi-cloud connection.
4. TGW Native Edge connection.

Section 1 contains

↳ 1) Create AWS TGW

Section 2 contains

↳ 2) Create a new security domain
3) Build your Domain Connection Policies

Section 3 contains

↳ 4) Setup AVX Transit GW
5) Prepare AVX TGW for TGW attachment.
6) Attach AVX TGW to TGW

Section 4 contains

↳ 7) Setup ~~Direct~~ VPN connection
8) Download VPN configuration.

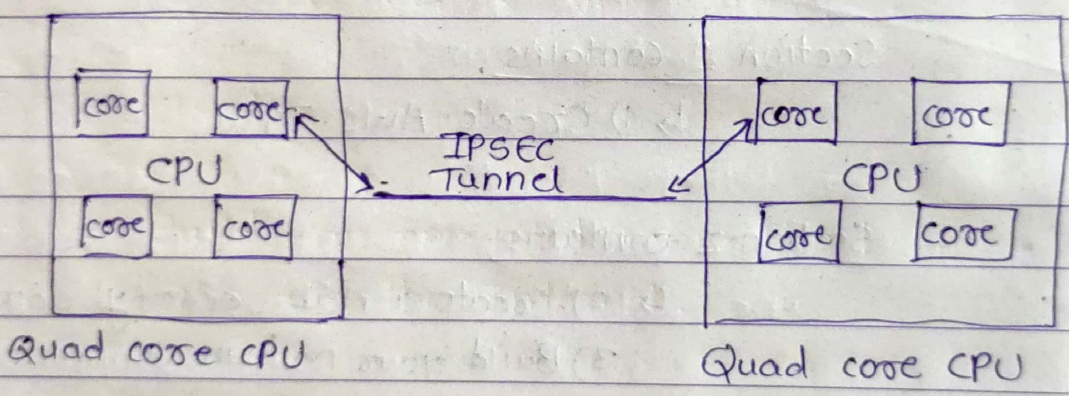
(2) Cloud Security -

→ Encompasses all other layers of the arch.

(*) Insane Mode Encryption -

→ In Transit VPC solution, throughput is capped at 1.25 Gbps because of an IPSEC session betn VGW & TGW as VGW has performance limitation.

→ Problem lies in nature of tunneling.

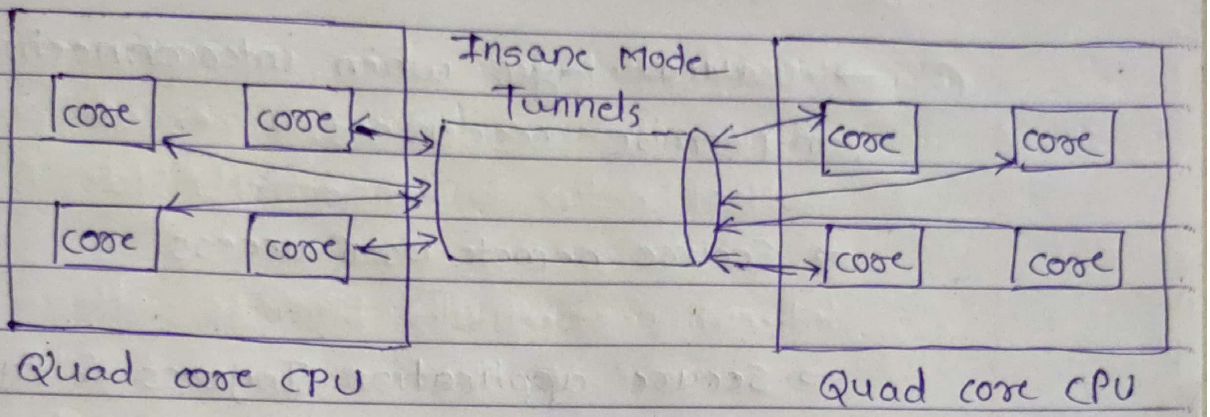


→ In above diagram, Virtual Router has multiple CPU cores, but since there is only one tunnel established, Ethernet interface can only direct incoming packets to a single core.

→ Thus the performance is limited to one CPU core, regardless of how many CPU cores you provide.

→ This is true for all tunneling protocols such as GRE, IPIP.

→ What Aviatrix Insane Mode Encryption does:



→ Aviatrix Insane mode tunneling establishes multiple tunnels, allowing all cores being used.

→ With Insane mode, IPSec encryption can achieve 10 Gbps, 25 Gbps & beyond.

⊛ Public subnet filtering GW

→ PSF GW provides both Ingress & Egress security for AWS public subnets where instances have public IP addresses.

→ It includes 2 parts:
- ① Ingress filtering via GuardDuty
- ② Egress FQDN

⊛ AVX FQDN

→ Filters any TCP & UDP traffic.
→ Allows only destn host names specified in the list to pass & drop all other destn.

③ Cloud Access -

→ Critical layer when interconnecting to on-premise resources.

→ Secure remote user access.

→ Secure application Ingress & Egress.

✱ User VPN -

client Software :

↳ OpenVPN client SW.

↳ Aviatrix VPN client.

✱ Site2Cloud

→ Builds an encrypted connection between 2 sites on the Internet.

Use cases -

↳ SaaS provider to its customer site

↳ Branch office to cloud.

④ Cloud Operations

→ Encompasses all other layers. It is a centralized operations plane.

(*) Flight Path

→ Troubleshooting tool.

→ Retrieves & displays AWS EC2 related info such as Security Groups, Route Table, etc.

(*) CoPilot

→ Provides a global operational view of your multi-cloud network.

Benefits :

Dashboard - ↳ Network Health Monitor
Topology - ↳ Dynamic Topology Map - Network topology
FlowIQ - ↳ FlowIQ - Detailed appn traffic flow analysis, global heat map & trends.

→ CoPilot is deployed as an all-in-one virtual appliance & available on AWS & Azure marketplace.

→ Traffic flows are sent from AVX GWs.
→ Uses REST API & HTTPS
→ 8vCPU & 32G of memory min for cp instance
→ 5 Tabs
① Overview ② Trends
③ Geolocation ④ Flows ⑤ Records

✳ Diagnostics

① Gateway Utility
→ Provides 3 tools (traceroute, ping & tracepath) to test network connectivity for Aviatrix GWs.

② Network connectivity Utility
→ Test if the controller / gateway is able to reach a host with specified protocol & port.

③ Packet Capture
→ Enables a GW to capture forwarding packets for a period of time with the specified host, port, nw interface & packet length.

④ controller Utility
→ Allows controller to perform a ping test to a specific host.

⑤ Force Upgrade
→ Allows you to upgrade a particular GW.

⑥ Service Actions
→ Status of services running in a GW & restart a service.

⑦ Keep GW on Error
→ Disables the rollback of GW if an error occurs. for Debugging purpose.

⑧ Gateway Replace
→ Replace a GW by launching a new GW & restoring the config.

(9) VPN User Diagnostics
→ Diagnostic info of a VPN user.

(10) VPN User history Search
→ Allows you to search VPN conn^n log on a particular VPN GW with filtering feature.

(11) VPN Diagnostics
→ Info of a specified VPC / VNet.

(12) VNet Route Diagnostics
→ Display RT, Display RT Details
→ Add / delete a RT
→ Add / delete a Route in RT
→ List RT, Routes
→ Turn IP FWD ON / OFF
→ Associate / Dissociate a subnet from a RT

(13) DB Diagnostics
→ View DB tables & restart a server

(14) Network Validation
→ When you select a Source NW & a Destn NW, AVX controller spin ups 2 instances & runs a connectivity test.

(*) Hit-less Upgrade
→ When upgrading a controller SW, all GWs are upgraded with new SW at the same time.

(*) AVX controller Deployment

Steps

(1) Subscribe to an Aviatrix AMI

(2) Launch controller with Cloudformation.

(3) Access the controller with public IP of the controller EC2 instance.

- ↳ Uname → admin
- ↳ Password → Private IP

(4) click Run to install Software.

(5) Access controller Dashboard.

(6) Under onboarding

- ↳ Create primary access account
  - ↳ Enter AWS Account name & no.