AviatrixACE

Aviatrix ACE (Aviatrix Certified Engineer) Multi-Cloud Networking Associate Exam Study Notes

Aviatrix

Aviatrix Systems is a software company headquartered in Santa Clara, California, the heart of Silicon Valley. Aviatrix software provides a platform for companies to build networking and security infrastructure in the public cloud. The platform provides architecture applicable to both single and multiple public cloud deployments. Currently, the software supports public clouds such as AWS, Azure, GCP, and OCI. Aviatrix Systems was the recipient of the Gartner Cool Vendor award in Cloud Computing in 2017 and is the pioneer of Multi-Cloud Network Architecture (MCNA).

Aviatrix Platform

- **A Centralized Controller**
  Aviatrix offers a centralized controller to make complex networking easy and does not require any background knowledge of networking command-line interfaces. This controller is also the entry-point for multi-cloud automation, which can be done using Application Programming Interface or Terraform. It is a browser-based, point-and-click management console that orchestrates both native (AWS, Azure, GCP, and OCI) constructs and advanced services from Aviatrix. This centralized controller also deploys Aviatrix Gateway instances for multi-cloud, on-premise, and edge connectivity.

- **A Distributed and Common Data-Plane**
  The Aviatrix platform embraces native cloud constructs and extends the functionality using advanced networking and security, which are both provided by Aviatrix Controller and Gateways. The Aviatrix gateways can be considered as service nodes, providing a robust and common data-plane within a Cloud or across multiple Clouds. 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.

- **Operational Visibility**
  CoPilot, one of Aviatrix's many services, allows users to have full operational visibility in their network, all while informing them if their cloud network has any issues.

- **Multiple Accounts and Clouds**
  Aviatrix is also able to integrate multiple accounts and clouds seamlessly and on one single interface.

This allows customers to interconnect AWS, Azure, and Google Cloud with the same point and click flow.

- **Security & Compliance**
  To help its service run smoothly, Aviatrix provides many security and compliance measures. It allows users to manage security domains, such as the Development domain and the Production domain, and also allows for Virtual Private Cloud connectivity through Connection Policies. Users are able to easily apply firewall filters based on tags or specific address ranges, CIDR, protocols, and ports. Aviatrix services are also integrated with AWS GuardDuty to block malicious activity automatically at the Virtual Private Cloud network level.

Features of Aviatrix

- **Centralized Controller**
  Networking VPCs and VNETs don't have to be complex. Take full control of your cloud network. No knowledge of networking command line interfaces (CLIs) needed.
  i. Browser-based, point-and-click management console
  ii. Orchestrates both native (AWS, Azure & GCP) constructs and advanced services from Aviatrix
  iii. Aviatrix Gateway instances for direct connect, multi cloud, and edge connectivity
  iv. Makes complex networking easy for all your use cases
- **Operational Visibility**
  It's hard to "see" your network in the cloud. CoPilot makes it visible to you and informs when your cloud network has issues.
  i. Get a complete picture of your cloud network
  ii. Visualize all connectivity status, performance and latency in real-time
  iii. Call up monitoring, displays and alerts
  iv. Make informed VPC connectivity decisions
  v. Share findings with colleagues and staff
- **Multiple Accounts and Clouds**
  Get the most out of the public cloud. Most virtual routers are from the datacenter era, forcing you to uniquely build every point-to-pont connection. Instead, operate with a cloud-native platform for all your accounts, regions, VPCs and VNETs
  i. Manage multiple accounts and regions in one place
  ii. Network cloud regions from a global view, not point-to-point
  iii. Interconnect AWS, Azure, and Google Cloud with the same point & click flow
- **Security & Compliance**
  Handle your part of the cloud Shared Responsibility Model. Meet your regulatory compliance requirements. Implement VPC network segmentation and isolation to reduce your blast radius.
  i. Manage Security Domains (e.g, Dev, Prod, Shared Services VPCs)
  ii. VPC connectivity is allowed by Connection Policies
  iii. User friendly tags to specify network ranges for security rules
  iv. Easily apply firewall filters based on tags or specific address ranges, CIDR, protocols, and ports.
  v. Control outbound traffic from your VPCs with egress filtering

vi. Make audits easier as security policy events (and packets) can be logged to Splunk, SumoLogic, Syslog, ELK and Datadog.

vii. Integration with AWS GuardDuty to block malicious activity automatically at the VPC network level

- **Simplify with Automation**
  Automate your cloud networking by delivering the network as code, rather than as a series of manually configured virtual routers. With Aviatrix, networking functionality easily becomes part of your cloud stack. No CCIE, no problem.
  i. Orchestrate your network in the same way as your compute
  ii. Leverage DevOps processes using change and revision control
  iii. Controller has fully documented REST APIs
  iv. Easily leverage our Terraform provider and CloudFormation templates
- **Faster Troubleshooting**
  Easily handle your daily calls to fix problems. Usually the network is blamed, even when it's not the culprit. Quickly determine if networking is the issue. Minimize downtime with faster troubleshooting.
  i. Integrated diagnostic tools for easier and faster troubleshooting
  ii. Limited use of Border Gateway Protocol (BGP)
  iii. Automated EC2 FlightPath tool helps identify EC2 instance connectivity problems
  iv. Continuous monitoring of your multi-cloud network with alerts available from the deployment dashboard
  v. Move at the speed of the cloud
- **Integrated Analytics**
  Drive your cloud networking decisions with intuitive, meaningful, real-time reports. Plug in your modern tool stack for an integrated view of all your infrastructure.
  i. Integrated monitoring, alerting and troubleshooting
  ii. Comprehensive syslog for network statistics, policy violations and more
  iii. API integration with modern cloud tools: Splunk, SumoLogic, Syslog, ELK and Datadog.
  iv. Robust API to easily integrate with Netflow and CloudWatch

High Availability working with Aviatrix

There are many aspects to the Aviatrix Software Defined Cloud Routing platform that can claim the title of High Availability. But the way that some of these components deploy can differ depending upon which component or gateway configuration you are working with. This article attempts to explain them all - for both the AVX Controller and AVX Gateway.

The AVX Controller **HA Model: Active / Passive [Recovery Time Objective: 2-3 mins]** The Controller can be deployed to be highly available in an active/passive failover model. The mechanism is dependent on several moving parts that need to be configured so that the service layers within AWS are properly accessible. It leverages an autoscaling group and a Lambda function that monitors the Controller instance which fires off the creation of a new one should the controller suddenly become unreachable. You will notice a link to a CloudFormation stack which will run you through a similar process for firing up the Controller the first time, but a few more details are needed this time such as designating a role for access to the S3 bucket where your backup files will live and designating the neighboring subnets that

will house the new Controller in the event of a failover. The process requires a lot of detailed steps so it is a good idea to test out the failover process once you have completed the setup. To do this, once you have completed the HA setup, simply wall up the controller using a security group to make it unreachable and watch the EC2 register spawn a new instance that has the same EIP as your initial controller.

Aviatrix Gateway-based HA There are three kinds of Gateway-based HA:

- Peering
- Egress Filtering
- Site2Cloud The gateways are the most critical point of failover support provided by the Aviatrix platform, even more so than the Controller itself. If a gateway were to come down, then data stops flowing. If the Controller were to come down, then you wouldn't be able to make any more changes to your gateway configurations until you launched another one from backup, but it doesn't affect network connectivity.

To start using the HA use-cases, you need to put the gateway into HA mode. To do this, you create a gateway via the controller per the usual course, but then you pop back in to edit mode once the gateway shows available in the gateway display screen. From this Gateway edit mode, you will find the option to make the gateway ready for High Availability Peering – but don't let this fool you. This option prepares the gateway for much more than just HA peering. This is the step you will need to complete as a first step to enable HA for Peering, VPC Egress Filtering, and Site2Cloud connections.

Peering / Tunnels: Active / Passive [Recovery Time Objective: 30sec / 2-3 mins] The primary function of the HA Gateway as depicted in the description in the Controller is to create a pair for high availability peering. This will allow you to connect two sets of gateway pairs to each other across VPCs to give you an industry standard internetworking cloud connection that is highly available. This comes in two different failover times of 30 seconds and 2-3 minutes, the first of which represents a second tunnel that is up and available, but with no active routes through it. The failover time is simply a matter of modifying the route tables so that traffic is rerouted in case of an endpoint failure. The second option is less expensive, as you don't have to pay for the second tunnel, but you are saddled with the wait time for the Controller to spin up a new gateway instance, create the tunnel and modify the route tables.

FQDN Egress Filter: Active / Active If your egress traffic demands are great and you would like to lighten the load beyond scaling up the size of the Gateway instance, you can do so via the same method you did to get a Gateway ready for HA peering. Simply use the same function, "Gateway for High Availability Peering" after you select your Gateway and hit Edit, choose the public subnet you want your Egress Filter pair to be in and hit Create. What this will do is create another gateway with the same Egress Filtering configuration as the other, and then it will assume the egress target routes for half of the private subnets in the VPC. If one of these gateways were to go down, the route tables would be updated to point to the remaining Egress Filter Gateway until the controller could spin up a new one in its place.

Site2Cloud: Active / Passive [RTO: 30sec] Site2Cloud is a direct descendant of Aviatrix Encrypted Peering, so naturally, it falls into this same category of Gateway-based HA. To create an HA Site2Cloud connection, you must first create the HA pair in the Gateway Edit screen per usual and then when you get to the lower half of the IPSec Tunnel configuration options, you can check the 'Enable HA' box, and this will open up three more forms for you to fill out based upon the backup gateway that you will be enlisting in your Site2Cloud connection. If you use a backup Gateway that is not an HA pair of the first, it will not work.

Load Balanced HA Configurations User2Cloud UserVPN Gateway: Active / Active If you want to have more than one Gateway support the load of the incoming connections of your VPN users, there is a trick that you can perform during the Gateway creation dialogue screen. The option to Enable ELB is in the enable position by default where you select the advanced options of your VPN Gateway ('VPN Access' is the name of the checkbox). To create a set of load balanced UserVPN Gateways, leave the ELB set to enabled and give the ELB Name a designation. To put another Gateway into this load balanced stack, you have but to repeat this process and use the same name in the ELB Name box.

Workflow Bound HA Configurations: You may notice that there are ways to enable HA embedded right into the Transit Network Setup workflow. Step 2 and step 5 both allow you to enable HA for a particular Gateway at a particular step in your build process and creating an HA pair for these types of Gateways are unique and follow slightly different procedures than simply creating the pair from the Gateway Edit function. In almost every Transit build enabled by Aviatrix, Step 1 of the Transit Network workflow has been executed to create the Transit VPC Gateway, which is a gateway deployed with special feature sets that enable it to manage the traffic coming and going through the Transit VPC. This gateway is different from the others given that it is a critical build for the Transit VPC.

That being said, these workflows bound Gateway-based HA enablement functions that originate from the workflows via these buttons are the same as if you did it from the Gateway edit screen. Both ways will get you an HA configuration.

Multi Cloud Network Architecture (MCNA)

MCNA is unlike any other architecture because it embraces, controls, and manages not only the native cloud constructs but also provides advanced services beyond what the Cloud Services Providers (AWS, Azure, GCP, and OCI) can provide. It provides a consistent and repeatable architecture across multiple clouds, being the first in the industry to do so, making it an essential part of the present and future of the public cloud. Aviatrix creates a purpose-built Multi-Cloud Network Architecture (MCNA) by implementing a data plane through dynamic and software-defined routing with a centralized control plane. Security is built into the network architecture through segmentation, encryption, ingress and egress filtering, and security services insertion. Aviatrix also leverages orchestrating cloud-native constructs, where necessary, in building and controlling the enterprise network and life-cycle management of the overall architecture. The architecture is valid for single-cloud-single-region, single-cloud-multiple-regions, or multiple-clouds-multiple-regions and can be easily referenced by both green and brownfield businesses with no issues. This is a common and repeatable architecture across multiple clouds, which creates simplicity and abstraction for the users by hiding all the underlying complexities and limitations of Cloud Service Providers. Because this architecture functions as a reference, it is vendor-agnostic.Architecture defines four distinct layers at a high level. These are Cloud Core, Cloud Security, Cloud Access, and Cloud Operations.

The Components of the MCNA

1. The Cloud Core has the applications connecting to the Global Transit Layer, which is a unified, global data plane across multiple/single clouds.
2. The Cloud Access Layer is where the on-prem components connect to the cloud.

3. The Cloud Security should be embedded in the Cloud Core Layer and the Cloud Access layer, because the public cloud is a shared infrastructure. This can be seen in the MCN Architecture when the Cloud Security layer cuts through the others.
4. Similarly, the Cloud Operations layer makes Day 1, 2, and 3 operations accessible to all the parts of the cloud. This allows troubleshooting and visibility.

Cloud Core
The cloud core of the multi-cloud network architecture goes beyond simple connectivity. It scales and supports the rapid evolution of applications and businesses. It also delivers a common data plane by supporting native cloud constructs, APIs, and adds advanced capabilities to form a common data plane with the visibility and control required to optimize the multi-cloud network. Within the cloud core, there are two subdivisions: The applications layer and the global transit layer.

- **The Applications Layer**
  This is where the applications are. These applications could be sitting in VPC/VNET and running as instances or VMs. The Aviatrix controller embraces the native constructs of the cloud from this layer. This is the area where applications are deployed using their respective operating systems.

- **The Global Transit Layer**
  Aviatrix software enables enterprise IT to easily deploy a high-availability, multi-cloud network data plane with end-to-end encryption, high-performance encryption, multi-cloud security domains, and operational telemetry operations teams need. This is the main point of connection for every aspect of the cloud. This global transit layer also has the notion of inserting services in its platform, which is done through the service insertion framework.

Cloud Security
Cloud security is a crucial part of the MCN architecture. This layer encompasses all the other layers of the cloud. It ensures that all the areas in the cloud, such as the applications, transit, and access layer are secure. The MCNA model enforces cloud security in many aspects, such as when connecting cloud to on-premise, ingress, egress, and security within the cloud security with encryption and security segmentation.

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. This architecture sets the multi-cloud foundation by securely bringing employees, partners, customers, branch offices, and legacy data centers into the cloud as one cohesive unit.

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.

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

The Benefits of the MCNA Approach

- The architecture is easily replicated in the Aviatrix controller.
- There is a normalized data plane.
- Service insertion and chaining are easily configured through the transit layer.

AWS Direct Connect virtual interfaces

You must create one of the following virtual interfaces to begin using your AWS Direct Connect connection.

- **Private virtual interface:**
  A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- **Public virtual interface:**
  A public virtual interface can access all AWS public services using public IP addresses.
- **Transit virtual interface:**
  A transit virtual interface should be used to access one or more Amazon VPC Transit Gateways associated with Direct Connect gateways. You can use transit virtual interfaces with 1/2/5/10 Gbps AWS Direct Connect connections. For information about Direct Connect gateway configurations, see Direct Connect gateways.

VNet

A Virtual Network, or a VNet, is an isolated network within the Microsoft Azure cloud. A VNet in Azure provides a range of networking functions comparable to AWS Virtual Private Cloud (VPC). These functions include DNS, routing, enabling customization of DHCP blocks, access control, connectivity between virtual machines (VM) and virtual private networks (VPN).

An Azure VNet is a representation of a network in the cloud and is logical isolation of the Azure cloud dedicated to a subscription. In the background, it's a software abstraction of a network that overlays Azure's infrastructure to provide isolation from resources outside of the VNet, practically making it a private network.

Operationally, a VNet follows common IP routing principles to connection resources inside. So, it needs to have one or more address spaces associated with it (CIDR), which can be segmented into subnets, within which resources will reside. The scope of a virtual network is a single region; however, several virtual networks of the same or different regions can be connected together by virtual network peering.

VNets can be used to:

Create a dedicated private cloud-only VNet to allow services and VMs within the VNet to communicate directly and securely in the cloud. Securely extend a data center, by building traditional site-to-site (S2S) VPNs or Express Route private circuits, to securely scale capacity. Deploy hybrid clouds by securely connecting cloud-based applications to on-premises systems.

Key components of Azure VNets, include:

Subnets: Subdivide a VNet into multiple networks which can be used for more granular separation of services **IP addresses:** Assign public or private IP addresses to an Azure VNet.

- Use public IP address for public-facing communications. A dynamic or static IP can be assigned.
- Use private IP address for connectivity within a VNet when using a VPN gateway or ExpressRoute. A dynamic IP assignment is a default, but a static IP can also be assigned. **Network Security Groups (NSG):** Network traffic ACLs which can be applied at a subnet or NIC level for filtering **Application Security Groups (ASG):** Group common workloads in world readable tags for use in NSGs **Service Endpoints:** secure critical Azure services resources to your VNET **Private Link:** private connectivity from a VNET to an Azure PaaS resource, customer-owned service, or Microsoft partner platform. **Firewall:** Azure offers a managed Firewall service that provides the ability to define L3-7 connectivity policies for granular control of what enters and leaves the network **Load balancing:** Load balancing solutions offered by Azure include:
- Azure Traffic Manager – comparable to Route53 in AWS
- Azure Load Balancer
- Azure Application Gateway
- Azure Front Door **Routing tables:** As with general routing, anytime traffic needs to leave a subnet, it needs a routing function to forward packets to other subnets and networks. A router does this using a routing table, and that route table configuration is exposed in Azure for customized configuration. Route table can have rules that define where traffic should be sent to, i.e a virtual network, virtual network gateway or virtual machine. **User Defined Route (UDR):** A static entry in a Route Table which can be used to forward traffic to a different Vnet, Network Virtual Appliance, . This can be a powerful tool to build a connection between hubs. **Network Virtual network Appliance (NVA):** Optional, for integration of 3rd party solutions, a virtual network appliance can be inserted into a VNet. This appliance is a virtual machine that executes a network function, such as a firewall, WAN optimization or other network function. To see a list of virtual network applications that can be deployed in a virtual network, see Azure Marketplace.

Remote User VPN

Aviatrix provides a cloud-native and feature-rich client VPN solution. The solution is based on OpenVPN® and is compatible with all OpenVPN® clients. In addition, Aviatrix provides its own client that supports SAML authentication directly from the client.

Aviatrix Transit Architecture for Azure

- **Azure Native Transit**
  The most common design topology within Azure is the Hub and Spoke model. The hub is a virtual network (VNet) in Azure that acts as a central point of connectivity to your on-premises network. The spokes are VNets that peer with the HUB and can be used to isolate workloads, departments, subscriptions, etc... Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection. It is common in these environments for spoke to spoke communication to be desired both within and across regions. To facilitate spoke to spoke communication, Azure natively provides three methods for performing this functionality. Each of

these options has advantages and disadvantages however, these options can be used simultaneously for customers to apply the right transit method for the desired outcome.

- **Intra-Region Transitive Options:** The options for spoke to spoke communication across regions follow the same patterns above with a few notable nuances.

1. **Leveraging ExpressRoute-** the most common transitive method is for customers to leverage their ExpressRoute circuits to provide spoke to spoke communication. This method requires a default (0.0.0.0/0) or summary route to be advertised from on-prem to allow spoke to spoke traffic to hairpin off the Microsoft Edge Routers. The advantage to this method is that this traffic will not incur VNET peering charges and this provides any to any spoke connectivity. The disadvantage to this approach is that bandwidth is limited by the ExpressRoute gateway SKU, traffic takes a longer path from spoke to spoke, a lack of granular control as this method provides any to any communication, and the fact that this is not a recommended approach as there is no dedicated bandwidth allocation on the Microsoft Edge Routers for this configuration.
2. **Leveraging a HUB Network Virtual Appliance (NVA)-** in this option, an NVA is deployed in the HUB VNET and User Defined Routes (UDRs) are created in each spoke to route traffic from spoke to spoke. The advantage to this approach is that traffic takes a more ideal path, does not require any route advertisements from on-prem, and potentially provides additional security functionality depending upon the NVA being leveraged. The disadvantage to this approach comes with the management of UDRs at scale, potential bandwidth limits of the NVA itself, and the configuration of NVA high availability (HA) to ensure redundancy in case of failure.
3. **VNET Peering-** the recommended approach for spoke to spoke communication is VNET peering as this leverages the MSFT backbone directly and always takes the preferred path. This option provides the lowest latency possible and has no bandwidth restrictions as opposed to the options previously discussed. The disadvantage of this model is this connectivity is a 1 to 1 mapping. Each spoke much be peered directly with another spoke in order to facilitate communication which at scale becomes a web of interconnected fully meshed VNETS. As such, customers often have challenges in managing the scale of VNET peers.

- **Inter-Region Transitive Options:** The options for spoke to spoke communication across regions follow the same patterns above with a few notable nuances.

1. **Leveraging ExpressRoute-** this method is similar to what was described in Intra-Region however, as ExpressRoute circuits are terminated across regions the routes are propagated automatically. To facilitate cross region spoke to spoke communication, no summary or default route is required. The same advantages and disadvantages apply.
2. **Leveraging a HUB Network Virtual Appliance (NVA)-** this method is also similar to what was previously described however, the number of UDRs increases as additional routes must be defined in the HUB VNETs to facilitate routing across regions to another HUB. Additionally, a VNET peer must be leveraged between the HUB to facilitate this HUB to HUB transit path.
3. **VNET Peering-** the only change in VNET peering across regions is in naming convention. Microsoft refers to this as Global VNET Peering but still has the same advantages and disadvantages previously discussed. Azure Virtual WAN is another native architectural approach which can also provide transitive functionality. Aviatrix Transit can integrate with Azure Virtual WAN and is not covered in detail here.

Aviatrix Transit for Azure

Aviatrix Transit for Azure is an architecture to interconnect multiple VNets and on-prem leveraging the hub and spoke deployment model while adding additional functionality and features. The Aviatrix Controller is a VM that manages all networking connections from VNETs to on-prem as well as between VNETs themselves. It deploys one Aviatrix gateway (two for redundancy) in each VNet. The Transit gateway is deployed in the transit VNet and connects to on-prem over Express Route or Internet. The Transit Gateway is then peered to each spoke VNET gateway to provide end to end communication. Communication can be granularly controlled to provide any to any communication between the spokes and to/from on-prem however, the transit gateway can also block certain traffic to keep spokes isolated. Additionally, all Spoke UDRs are orchestrated from the controller based on desired traffic flows.

For cross region communication, multiple Transit Gateways can also be interconnected. Spoke VNets can communicate to remote Spoke VNets through the two connected Transit Gateways with the same granular controls mentioned previously. Additionally, route advertisements between the two transit gateways can be controlled to provide additional functionality like summarization, route exclusion, etc. Another important advantage of using Aviatrix Transit is that all communications are encrypted by default providing additional levels of security. Azure does not provide any native encryption across the Microsoft Backbone and depends upon third party NVAs to provide this functionality should customers require it.

The Aviatrix controller also has the ability to orchestrate native VNET peering for Azure VNETs should customers not wish to deploy gateways within spoke VNETs. While customers will lose the encryption and visibility benefits across these links, all appropriate UDRs will be orchestrated to facilitate transitive communication as desired. It is also important to note that certain native limitations may apply as to the number of peerings allowed as well as restricitions to overlapping IP space when native peering is leveraged.

Need of Aviatrix Transit for Azure

Transit architecture is about building connectivity between cloud and on-prem in the most agile manner possible. In the Transit architecture, there is one connection (not including the backup) between on-prem and a Transit Hub VNet. Everything else (the Spoke VNet to on-prem traffic) is routed through the Transit Hub VNet.

The alternative to Transit architecture is to leverage the native options already mentioned or is to build one connection (often referred to as “flat” architecture), either IPSEC over Internet or Express Route, each time you spin up a new VNet in Azure. This requires changes at the on-prem edge, which requires a change control process that takes from days to weeks. Additionally, this method often facilitates the default any to any connectivity which may require additional configuration to prevent.

The Benefits of Aviatrix Transit for Azure

- **Simplicity** The Aviatrix Controller provides an abstraction layer and workflow to build the Transit network. You do not need to program any Azure route tables, manage the route entries or understand the significant details about Azure networking.
- **Multi Subscriptions Support** The Controller provides a single pane of glass to manage the entire cloud network of multiple Azure subscriptions.

- **Logging Service Integration** Out-of-the-box integration with Splunk, Sumo Logic, DataDog, ELK, remote syslog and Netflow.
- **Visibility** View connectivity status, network latency and traffic statistics from a central dashboard.
- **Granular Routing Control** Route redistribution can be controlled to selectively allow specific route propagation and/or summarization.
- **Advanced Networking Features** Support for Network Address Translation, NGFW Insertion, FQDN filtering, etc.
- **No Route Limits** The Aviatrix solution auto summarizes the on-prem and Spoke VNet routes so that Spoke VNet route entries do not exceed the route limits.
- **End-to-End Encryption** All traffic in flight, between Spoke VNets and between Spoke to on-prem, is encrypted.

Aviatrix Stateful Firewall Rule

Aviatrix stateful firewall is feature on the Aviatrix gateway. It is a L4 stateful firewall that filters network CIDR, protocol and port on the packet forwarding path. The stateful firewall allows each individual rule to be defined as Allow, Deny and Force Drop, in addition to a base rule.

- **How many rules can be configured on a gateway?** Currently you can configure up to 500 rules on each gateway. This limitation is not due to the lack of capacity in the gateways, but is because of the implementation of how rules are sent to the gateways. In the next release (5.2), the limitation will be removed.

- **What is the API to configure stateful firewall?** Currently the API call requires you to input the entire set of the rules for each call. There is no incremental append or delete functions. In the next release (5.2), there will be new APIs to append new rules and delete a specific rule.

Transit VNet using VNet peering

Azure Virtual Network (VNet) is the fundamental building block for any customer network. VNet lets you create your own private space in Azure, or as I call it your own network bubble. VNets are crucial to your cloud network as they offer isolation, segmentation, and other key benefits. Read more about VNet's key benefits in our documentation, With VNets, you can connect your network in multiple ways. You can connect to on-premises using Point-to-Site (P2S), Site-to-Site (S2S) gateways or ExpressRoute gateways. You can also connect to other VNets directly using VNet peering.

Customer network can be expanded by peering Virtual Networks to one another. Traffic sent over VNet peering is completely private and stays on the Microsoft Backbone. No extra hops or public Internet involved. Customers typically leverage VNet peering in the hub-and-spoke topology. The hub consists of shared services and gateways, and the spokes comprise business units or applications.

Gateway transit

Today I'd like to do a refresh of a unique and powerful functionality we've supported from day one with VNet peering. Gateway transit enables you to use a peered VNet's gateway for connecting to on-premises instead of creating a new gateway for connectivity. As you increase your workloads in Azure, you need to scale your networks across regions and VNets to keep up with the growth. Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered VNets and lets you manage the connectivity in one place. Sharing enables cost-savings and reduction in management overhead.

With Gateway transit enabled on VNet peering, you can create a transit VNet that contains your VPN gateway, Network Virtual Appliance, and other shared services. As your organization grows with new applications or business units and as you spin up new VNets, you can connect to your transit VNet with VNet peering. This prevents adding complexity to your network and reduces management overhead of managing multiple gateways and other appliances.

VNet peering works across regions, across subscriptions, across deployment models (classic to ARM), and across subscriptions belonging to different Azure Active Directory tenants.

Transit Gateway Peering in AWS (TGW)

You can peer two transit gateways and route traffic between them, which includes IPv4 and IPv6 traffic. To do this, create a peering attachment on your transit gateway, and specify a transit gateway in another AWS Region. The peer transit gateway can be in your account or a different AWS account. After you create a peering attachment request, the owner of the peer transit gateway (also referred to as the accepter transit gateway) must accept the request. To route traffic between the transit gateways, add a static route to the transit gateway route table that points to the transit gateway peering attachment. We recommend using unique ASNs for the peered transit gateways to take advantage of future route propagation capabilities. Transit gateway cross-region peering does not support resolving public IPv4 DNS host names to private IPv4 addresses across VPCs on either side of the transit gateway peering attachment. Transit gateway peering attachments are not supported in the following AWS Regions: Asia Pacific (Hong Kong), Asia Pacific (Osaka-Local), and Middle East (Bahrain).

AWS TGW Orchestrator

1. Orchestrates VPC to VPC and on-prem to VPC connectivities via AWS Transit Gateway.
2. Automates AWS Resource Access Manager (RAM) for multi account support.
3. Creates security boundaries between groups of VPCs to achieve network segmentation.
4. Out-of-the-box integration of AWS Transit Gateway and Direct Connect and Internet to re-use what has been built.
5. Provides Insane Mode high performance and features rich hybrid network for connecting to on-prem.
6. Supports Bring Your Own Firewall to TGW deployment for inline traffic inspection (Firewall Network)
7. Orchestrate AWS TGW Inter Region Peering and expand the Security Domains to be global.
8. Advanced mode for end to end encryption where Aviatrix gateways are deployed in the AWS Spoke VPCs and Azure Spokes VNet.

Aviatrix Firewall Network (FireNet)

Aviatrix Firewall Network (FireNet) is a turn key network solution to deploy firewall instances in the cloud. FireNet significantly simplifies firewall instance deployment and allows the firewall instances to inspect VPC to VPC (East West) traffic, VPC to Internet (Egress) traffic, and VPC to on-prem (North South) traffic

Benefits of FireNet Deployment Model

For enterprises that wish to deploy a firewall in AWS, Aviatrix's FireNet deployment model provides the best performance and automation.

- **Simplicity** The Aviatrix Firewall Network significantly simplifies firewall deployment in the cloud while providing the maximum performance and scale.
- **Full Traffic Inspection** With FireNet, North South (on-prem and cloud), East West (VPC to VPC) and Internet bound egress traffic can be inspected by firewall instances.
- **No IPSEC Tunnels** There are no IPSEC tunnels connecting to firewall instances as opposed to ECMP VPN deployment model, maximizing each firewall instance throughput.
- **No SNAT** SNAT function is not required to be performed by firewall instances for east west traffic inspection as opposed to the ECMP VPN deployment model, resulting in instances in Spoke VPCs having complete visibility of source traffic.
- **No BGP** The Firewall does not need to run BGP. All routes programming is done by the Controller through Palo Alto APIs.
- **Scale Out** Multiple firewall instances can be deployed as a group to meet the demand of increasing workload.
- **Policy Driven** Policy driven workflow allows you to customize which VPCs traffic should be inspected.
- **Vendor Integration** Launch Palo Alto Networks VM-Series from the Aviatrix Controller console to simplify deployment.
- **Automation** The Aviatrix Controller automatically updates Palo Alto VM-Series route tables when on-prem route changes or VPC attachment changes.

AWS Global Accelerator

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your traffic by as much as 60%. You can test the performance benefits from your location with a speed comparison tool. AWS Global Accelerator continually monitors the health of your application endpoints and redirects traffic to healthy endpoints in less than 30 seconds.

Benefits of AWS Global Accelerator

- **Improve global application availability**
  AWS Global Accelerator continually monitors the health of your application endpoints, such as your Network Load Balancers, Application Load Balancers, EC2 Instances, or Elastic IPs, instantly reacting to changes in their health or configuration. AWS Global Accelerator will then redirect user traffic to healthy endpoints that deliver the best performance and availability to your users.

- **Accelerate your global applications**
  AWS Global Accelerator optimizes the network path, taking advantage of the vast, congestion-free AWS global network. Regardless of where your users are located, AWS Global Accelerator intelligently routes traffic to the endpoint that provides the best application performance.

- **Easily manage endpoints**
  AWS Global Accelerator's static IP addresses make it easy to move endpoints between Availability Zones or AWS Regions without needing to update your DNS configuration or change client-facing applications. You can use static IP addresses from the Amazon IP address pool or you can bring your own IP addresses (BYOIP) to AWS Global Accelerator.

AWS Global Accelerator - Use cases

- **Scale for increased application utilization**
  When application usage grows, the number of IP addresses and endpoints that you need to manage also increase. AWS Global Accelerator allows you to scale your network up or down. AWS Global Accelerator lets you associate regional resources, such as load balancers and EC2 instances, to two static IP addresses. You only whitelist these addresses once in your client applications, firewalls, and DNS records. With AWS Global Accelerator, you can add or remove endpoints in the AWS Regions, run blue/green deployment, and A/B test without needing to update the IP addresses in your client applications. This is particularly useful for IoT, retail, media, automotive and healthcare use cases in which client applications cannot be updated frequently.

- **Accelerate latency-sensitive applications**
  Many applications, such as gaming, media, mobile applications, and financial applications, need very low latency for a great user experience. To improve the user experience, AWS Global Accelerator directs user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It routes the traffic to the closest edge location via Anycast, then by routing it to the closest regional endpoint over the AWS global network. AWS Global Accelerator quickly reacts to changes in network performance to improve your users' application performance.

- **Disaster recovery for multi-region & multi-Availability Zone resiliency**
  You need to rely on your network to always be available. You might be running your application across multiple Availability Zones (AZs) or AWS Regions for disaster recovery, higher availability, lower latency, or compliance. If AWS Global Accelerator detects failure of your application endpoint in the primary AZ or AWS Region, it instantly triggers traffic re-routing to your application endpoint in the next available, closest endpoint in another AZ or AWS Region.

- **Protect your applications**
  When making your Application Load Balancers internet-facing or your EC2 instances public to serve your end users, you also increase your exposure to attacks from the internet. AWS Global Accelerator allows you to add an internal Application Load Balancer or a private EC2 instance as an

endpoint. By using AWS Global Accelerator as the single internet-facing access point, you protect your applications running on AWS from distributed denial of service (DDoS) attacks and control how your end users reach your applications. AWS Global Accelerator creates a peering connection between the AWS Global Accelerator and your Amazon Virtual Private Cloud (Amazon VPC). The traffic between the two VPCs uses private IP addresses.

Aviatrix OpenVPN

OpenVPN is a registered trademark of OpenVPN Inc. OpenVPN is open-source commercial software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

Aviatrix OpenVPN® Feature Highlights

VPN Management

- **Centrally Managed** A single pane of glass allows you to manage all VPN users, VPN certificates and VPN user visibility.
- **OpenVPN® Compatible** Built on OpenVPN® and is compatible with all OpenVPN® client software.
- **Split Tunnel** Supports split tunnel mode where only specified CIDRs ranges go through the VPN tunnel.
- **Full Tunnel** Supports full tunnel mode where all user IP sessions including Internet browsing go through the VPN tunnel.
- **PKI Management** Supports Bring Your Own (BYO) PKI management system.
- **Force Disconnect** Any admin can force disconnect a VPN user from the controller console.
- **Dashboard** View all active VPN users and their connection history from the controller console dashboard.
- **API** Support API for all management activities.

Authentication Options

- **LDAP/AD Integration** Authenticates VPN user from Aviatrix gateways in addition to VPN certificate authentication.
- **DUO Integration** Authenticates VPN user from Aviatrix gateways in addition to VPN cert authentication.
- **OKTA Integratio** Authenticates VPN user from Aviatrix gateways in addition to VPN cert authentication.
- **MFA Integration** Combines LDAP and DUO for multi-factor authentication.
- **Shared Certificate** Supports a shared certificate arrangement among VPN users. (When this option is is selected, you should enable additional authentication options to ensure secure access.)
- **Client SAML Integration** Authenticates a VPN user directly from the Aviatrix VPN client to any IDP via SAML protocol.

Authorization Profile-Based Access Control Each VPN user can be assigned to a profile that is defined by access privileges to network, host, protocol and ports. The access control is dynamically enforced when a VPN user connects to the public cloud via an Aviatrix VPN gateway.

Scale Out Performance

- **TCP-based VPN** For a universal/no firewall/no fuss user VPN solution, use an Aviatrix integrated NLB to load balance multiple Aviatrix VPN gateways. When NLB is used, OpenVPN® client software runs on TCP port 443. TCP-based VPN requires no special corporate firewall rules when VPN client is on-prem.
- **UDP-based VPN** For a high performance user VPN solution, use Aviatrix integrated AWS Route53 round robin routing to load balance multiple Aviatrix VPN gateways. When Route53 round robin routing is used, OpenVPN® client software runs on UDP port 1193. UDP-based VPN has improved file transfer performance.
- **Geo VPN** For TCP-based VPN, you can use Aviatrix integrated AWS Route53 latency-based routing to load balance clients residing in different geographic locations.

Logging Integration

- **VPN User** connection history and bandwidth usage can be logged to Splunk, SumoLogic, ELK, Remote Syslog and DataDog.
- **User Activity** Each VPN user TCP/UDP session can be logged to Splunk, SumoLogic, ELK, Remote Syslog and DataDog.

Client Software
OpenVPN® Client Software All OpenVPN® client software is supported. The supported clients are macOS, Windows, iOS, Android, Chromebook, Linux and BSD. Aviatrix VPN Client Aviatrix VPN Client supports macOS, Windows and Linux Debian distribution and BSD distribution. Choose Aviatrix VPN Client if you require SAML authentication directly from VPN client software.

VPC Tracker

VPC Tracker is a tool that collects and helps you manage your network CIDR ranges at a central place, eliminating the need to keep an Excel sheet on all your VPC network addresses allocations. No gateway launches are required. Start by logging into your controller and going into the dashboard. Once in the dashboard in the upper right corner of the map uncheck the option Only show AVX gateways then add all your other AWS accounts on the Controller, and VPC Tracker will retrieve the information. To see what the VPC tracker has recorded please go to your menu and then select Usefull Tools » VPC Tracker. If you are not seeing all of your VPC's please click on the refresh button and this will have the VPC tracker search for unfound VPCs. When you do this please select OK in the pop menu and understand this may take some time depending on the number of VPCs and Accounts on your controller. Currently, VPC Tracker can record network CIDRs in AWS, Azure, Site2Cloud remote network CIDRs and Transit Network on-prem CIDRs. All VPCs with at least 1 instance will be displayed VPC Tracker auto updates once a day and will only list VPC's which have at least one instance deployed in them. You can conduct an on-demand update by clicking the refresh button.

About BGP with Azure VPN Gateway

BGP is the standard routing protocol commonly used in the Internet to exchange routing and reachability information between two or more networks. When used in the context of Azure Virtual Networks, BGP enables the Azure VPN Gateways and your on-premises VPN devices, called BGP peers or neighbors, to exchange “routes” that will inform both gateways on the availability and reachability for those prefixes to go through the gateways or routers involved. BGP can also enable transit routing among multiple networks by propagating routes a BGP gateway learns from one BGP peer to all other BGP peers.

- **Why use BGP?** BGP is an optional feature you can use with Azure Route-Based VPN gateways. You should also make sure your on-premises VPN devices support BGP before you enable the feature. You can continue to use Azure VPN gateways and your on-premises VPN devices without BGP. It is the equivalent of using static routes (without BGP) vs. using dynamic routing with BGP between your networks and Azure.

FlightPath

FlightPath is a troubleshooting tool. It retrieves and displays, in a side by side fashion, AWS EC2 related information such as Security Groups, Route table and route table entries and network ACL. This helps you to identify connectivity problems.

ActiveMesh Insane Mode Encryption Performance

Aviatrix High Performance Encryption (HPE), also known as ActiveMesh Insane Mode, achieves line rate performance with encryption in AWS when Jumbo frames are deployed (the default setting for AWS instances). The test benchmark baseline is the native AWS peering where no Aviatrix gateways are deployed in the VPCs. Adding 500 stateful firewall rules have little impact to the performance.

If your enterprise security policy requires encryption for data in motion, Aviatrix InsaneMode encryption provides the best and most efficient single instance encryption performance.

InsaneMode Benefits

- **30Gbps IPSEC** Using a single instance from C5 series to the latest C5n series, single instance IPSEC performance reaches up to 30Gbps.
- **Private Link** InsaneMode connectivity is supported over AWS Peering and AWS Direct Connect.
- **Stateful Firewall** Aviatrix gateways support stateful firewall for additional security policies, event and packet logging.
- **Unlimited Routes** Aviatrix gateways have no limit to how many on-prem routes or VPC routes they can have.
- **Advanced NAT** Advanced NAT function for any packet transforming before and after routing function.

Internet Protocol Security (IPsec)

IPsec (Internet Protocol Security) is a suite of protocols that secure network communication across IP networks. It provides security services for IP network traffic such as encrypting sensitive data, authentication, protection against replay and data confidentiality.

IPsec uses the following protocols to secure the IP network traffic:

- **Authentication Header (AH)** – Authentication header protects data within the IP packet from tampering. Tampering means anyone trying to change the contents of the packet sent from the server to the client. IPSec digitally signs the contents of the entire packet (including payload) using an Authentication Header thereby providing protection against replay attacks, spoofing, and tampering. While the authentication header protects data from tampering, it will not stop anyone from seeing it.
- **Encapsulating Security Payload (ESP)** – This protocol encrypts the payload of a data packet and provides authentication, replay proofing, and integrity checking. It provides confidentiality through encryption of the packet
- **Internet Key Exchange (IKE)** – IKE protocol allows hosts at both ends of a VPN tunnel to encrypt and decrypt data packets using mutually agreed upon keys/certificate and method for encryption IPSec can be broadly used for following purposes: to build a dedicated tunnel between two hosts using IPsec tunneling so that traffic between two hosts is encrypted, secure and encrypt the application layer data, providing security to routers sending data across the internet and to provide authentication without encryption

IPSec can be usually configured to operate in the following two modes:

- **Transport Mode** – Transport mode is used for end to end communications, for example, communication between a host and server. In this case, data contents (IP payload) are protected, but anyone looking at the network traffic can see network traffic patterns. In transport mode, the responsibility to perform any cryptographic operations like encryption etc. depends on the sender and receiver
- **Tunnel Mode** – Tunnel mode encrypts the entire IP packet. Usually, it is used to encrypt traffic between two routers/gateways connected over the Internet via IPSEC VPN tunnels. In tunnel mode, cryptographic operations like encryption etc., are handled by gateways/routers at both ends of the tunnels, in addition to the sender and receiver

Network Address Translation (NAT)

Network Address Translation (NAT) is a process that enables resources in private networks to connect to the Internet but prevents entities on the internet to initiate connections with the resources in private network. A device like a router with NAT capability translates the private addresses in the internal network into globally unique public IP addresses, thereby enabling resources in the private network to access resources outside its network (on the internet). In addition to this, NAT can also be configured in

such a way that one public IP address can represent a group of resources in the internal network thereby hiding the entire internal network behind the one public IP and giving an extra layer of security.

Different types of NAT

- **Static NAT** – One on one mapping between a singular private address and a public IP address.
- **Dynamic NAT** – One to many mapping between a private IP address and a pool of public IP addresses
- **Port Address Translation (PAT)** – A type of Dynamic NAT that maps multiple private IP addresses to a single public IP address by using different ports.

Aviatrix PrivateS3

Aviatrix PrivateS3 is a feature that allows you to leverage AWS Direct Connect to transfer objects and files between on-prem and S3 while giving you control of the S3 buckets by the ability to whitelist the S3 buckets.

Benefits of PrivateS3

- Transferring objects/data between on-prem and S3 by leveraging Direct Connect without using public VIF.
- The ability to control which S3 buckets can be accessed.
- The ability to deploy multiple Aviatrix gateways to load balance the data traffic.

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

FlightPath

FlightPath is a troubleshooting tool. It retrieves and displays, in a side by side fashion, AWS EC2 related information such as Security Groups, Route table and route table entries and network ACL. This helps

you to identify connectivity problems. You do not need to launch Aviatrix gateways to use this tool, but you need to create Aviatrix accounts so that the Controller can use the account credentials to execute AWS APIs to retrieve relevant information

Firewall Network (FireNet) Workflow

Aviatrix Firewall Network (FireNet) is a turn key network solution to deploy firewall instances in the cloud. FireNet is a solution for integrating firewalls in the AWS TGW deployment.

Aviatrix CloudWAN

The Aviatrix Multi-Cloud Networking Platform provides a frictionless Branch Office-to-Cloud Networking solution, delivering centralized, simple, cloud-based, automated reconfiguration of existing IOS branch routers to securely connect directly to the closest cloud access point. The automated reconfiguration includes IPSec crypto, BGP, intra- and inter-cloud route propagation, and more. CloudWAN will also take advantage of cloud-native anycast IP optimal-path routing features offered by some cloud providers.

As the center of enterprise IT gravity shifts to the cloud, optimal access to applications equals optimal access to cloud. Legacy application traffic patterns were based on WAN architectures and more recently SD-WAN refreshes, both optimized to connect branch offices to centralized data centers as efficiently as possible. However, in the cloud era, neither of these are the most efficient or cost-effective approach. A simpler and more cost optimized approach is to leverage existing branch office routers, without upgrading either hardware or software, to connect to the closest cloud access point and leverage the cloud provider's global network to reach cloud-based applications and resources.

CloudWAN provides centralized, simple, cloud-based, automated reconfiguration of existing IOS branch routers to securely connect directly to the optimal cloud access point.

Key Highlights

Aviatrix CloudWAN is designed to connect and manage branch office IOS routers to the cloud directly and has the following benefits:

- **Centrally managed** – Uses a single pane of glass to provision, onboard, and monitor ALL your Cisco IOS routers health and stats.
- **Automation and orchestration** – Automates reconfiguration of Cisco IOS branch routers from the cloud. Orchestrates connectivity directly to Aviatrix AVX Service Gateways, AWS Transit Gateways, or Azure Virtual WANs.
- **Low latency** – CloudWAN configures existing IOS routers to connect to the nearest cloud edge and routes traffic through the cloud provider to cloud-based applications and resources. When available, CloudWAN will take advantage of cloud-native anycast IP optimal-path routing across the cloud provider infrastructure.
- **Use existing hardware and software** – Leverage the investment you have already made in branch office routers to connect to the cloud.

- **Automated router reconfiguration** – Supports a range of configuration features such as version control, configuration rollback, diff, BGP routing and IPSec crypto.

Author Profile:

- LinkedIn: atuljkamble
- Twitter: atul_kamble
- Github: atulkamble
- Medium: atul_kamble
