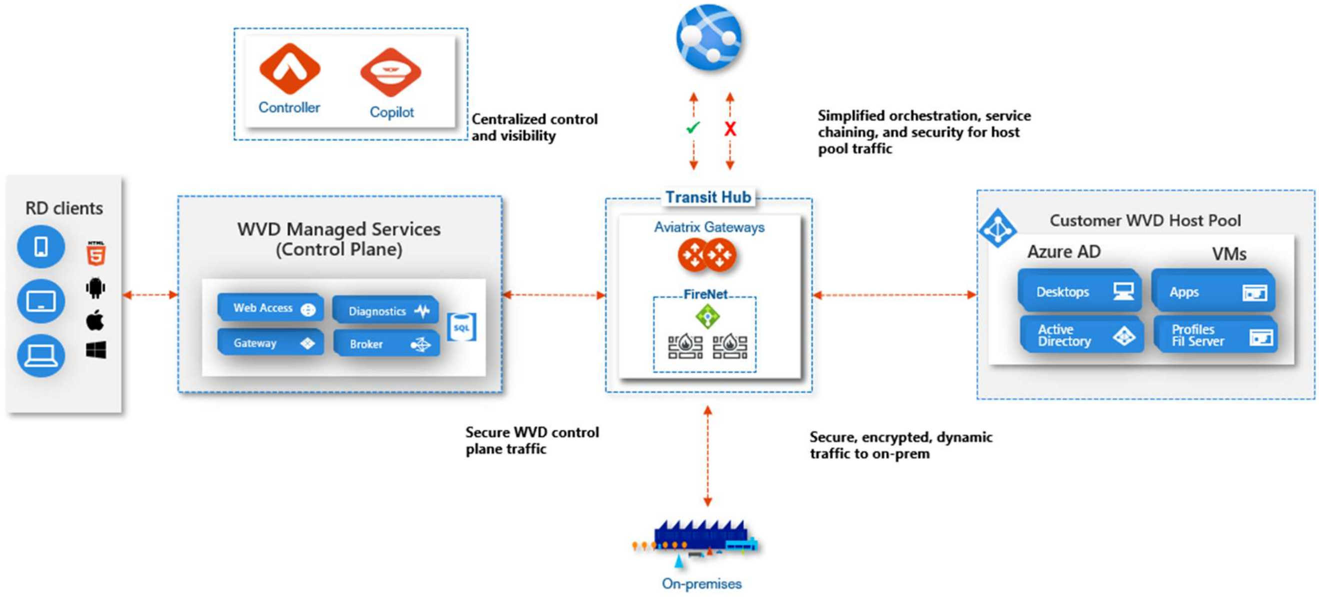
Azure Windows Virtual Desktop (WVD) on Aviatrix Cloud Network Platform

Overview

Windows Virtual Desktop (WVD) is Microsoft's managed virtual desktop service in Azure. It provides customers with simplified management, multi-session Windows 10, optimizations for Microsoft 365 Apps, and support for remote desktop services. Windows Virtual Desktop is made up of Windows desktops and apps you deliver to users and the full management solution hosted as a service on Azure by Microsoft. Desktops and apps are deployed on virtual machines (VMs) in any Azure region, and the management solution and data for these VMs resides in the United States.

As a result of COVID-19 work from home policies, enterprises around the globe have moved quickly to deploy the Azure Windows Virtual Desktop service to allow employees and contractors to maintain access to critical business applications. Azure WVD is extremely simple to deploy in a basic, Azure cloud only design. However, there are significant challenges enterprises encounter to meet and maintain corporate and regulatory security requirements and gain operational visibility and control that IT teams require to reduce operational overhead and associated costs.

The Aviatrix cloud network platform provides enterprises advanced networking, security features, including functionality required for a seamless and secure deployment of the Windows Virtual Desktop service environments. Leveraging this Aviatrix validated design, enterprises will address the critical networking and security challenges associated with workloads being deployed in public clouds.


Controller
Copilot
Centralized control and visibility
✓
X
Simplified orchestration, service chaining, and security for host pool traffic
RD clients
WVD Managed Services (Control Plane)
Web Access
Diagnostics
Gateway
Broker
SQL
Transit Hub
Aviatrix Gateways
FireNet
Customer WVD Host Pool
Azure AD
VMs
Desktops
Apps
Active Directory
Profiles Fil Server
Secure WVD control plane traffic
Secure, encrypted, dynamic traffic to on-prem
On-premises

Microsoft Windows Virtual Desktop service (WVD) provides enterprises with a comprehensive desktop and application virtualization service in the cloud. Leveraging the Aviatrix platform, WVD adopters seamlessly integrate security, advanced networking, multi-cloud transit, and visibility into this environment.

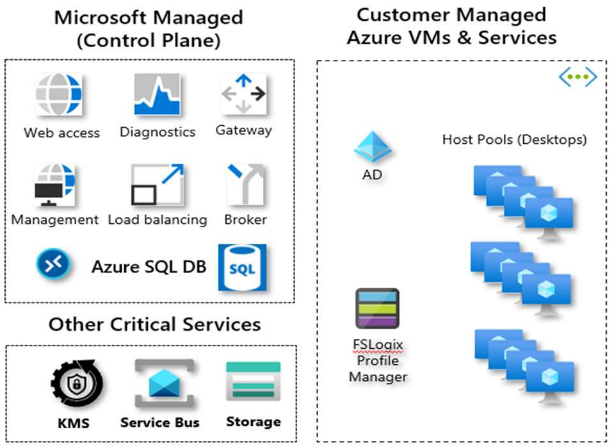
Aviatrix Introduction – Multi-Cloud Network Architecture

Aviatrix Validated Designs are created based on a Multi-Cloud Network Architecture (MCNA), which has been proven with hundreds of enterprise customers building cloud network infrastructure in AWS, Azure, Google and Oracle clouds across almost every industry vertical around the world. An MCNA is not a product, it is an architectural framework that is used to organize design requirements. An MCNA outlines how architectural pillars such as networking, security, day-one automation and day-two operational visibility span across cloud access, cloud networking and cloud application layers. Similar to a building architecture, the MCNA becomes the go to plan that allows cloud and security architects and their operational counter parts to work together to ensure network designs meet all cross-functional requirements.

To realize their multi-cloud network designs, Aviatrix customers leverage the Aviatrix cloud network platform to deliver multi-cloud networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers. Aviatrix software leverages public cloud provider APIs to interact with and directly program native cloud networking constructs. This abstracts the unique complexities of each cloud, simplifying deployments and forming one multi-cloud network data plane with advanced networking and security features and one, consistent multi-cloud operational model. Aviatrix Transit delivers a superset of enterprise-class capabilities that becomes the foundation of our enterprise customer's multi-cloud network architecture.

Why Microsoft Windows Virtual Desktop Service

Windows Virtual Desktop service delivers enterprises a simplified, managed infrastructure for virtual desktop deployments. The Coronavirus COVID-19 pandemic has made tele-commuting (working remotely) a critical requirement for IT teams around the globe. The result, for Microsoft, has been an exponential increase in the demand for Windows Virtual Desktop deployments. Enterprises now have an urgent need to deliver secure remote access to business applications and data. Microsoft has made substantial investments in the infrastructure and technology needed to deliver a scalable managed service. By abstracting much of the complexity related to supporting a VDI/WVD infrastructure Microsoft has simplified the entire process for enterprise IT operations.



Windows Virtual Desktop Service Delivery Challenges

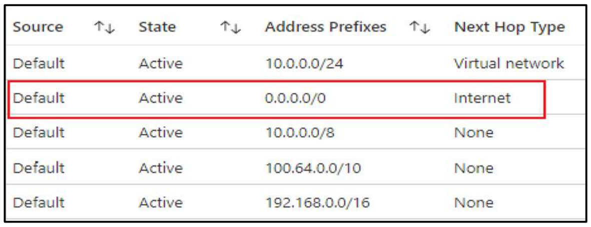
Azure Windows Virtual Desktop is a Microsoft managed service. However, the host pools (virtual desktops) are deployed in Azure Virtual Networks (VNets), managed by the customer. The WVD VNet implementation, by default, has the same connectivity and security implications as any other IaaS workload in Azure and the WVD service control plane connectivity requires careful up-front planning to ensure regulatory and corporate security requirements are met and Day-2 operational best practices, such as visibility, availability and resiliency can be achieved.

WVD host pools are deployed in a VNet and require networking connectivity design considerations, including:

- On-prem (Private connection, VPN, Encryption)
- Internet routing/security
- UDR management
- Route management for local VNets and VNets in other Geos (regions)
- Local and remote application reachability, (e.g. apps or data residing in another region, cloud or physical data center
- How users access data and what data/apps they can access
- Operational visibility, troubleshooting
- Network high-availability and resiliency

Key Service Delivery Considerations

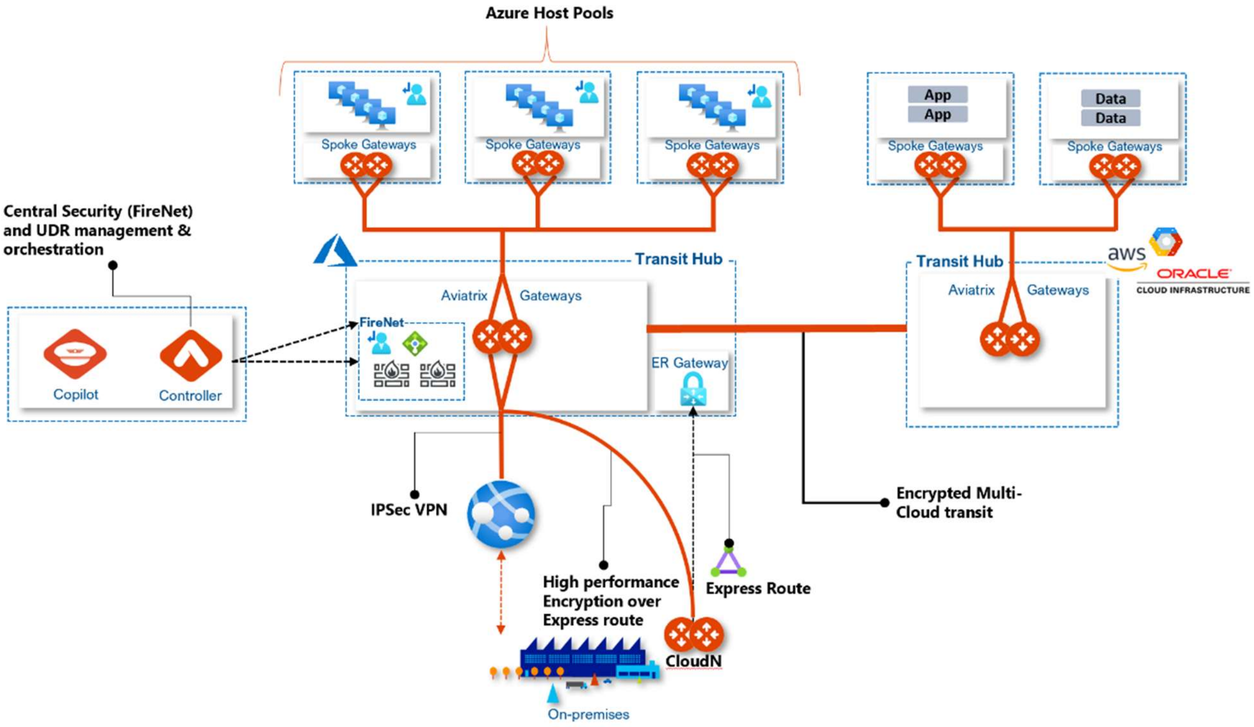
- Private On-Premise Connectivity – Cloud service providers today cannot offer line-rate encryption between data center and the cloud. WVD on-prem connectivity, over Express Route or VPN, requires end-to-end privacy and security design considerations.
- Multi-Cloud Connectivity – If a desktop requires access to applications or data in a second public cloud, it requires unique/explicit connectivity and security design and implementation considerations.
- WVD Control Plane Security – The WVD control plane is not secured by default from virtual machines in the host pool VNet and should be viewed as a security risk.
- Direct Internet Access – Desktop host pools will have Internet access (default VNet configuration) with NO security policy by default. As shown in the screenshot below, a virtual machine's effective route table has a default Next Hop Type set to "Internet".
- Segmentation – Customers with multiple host pools may have requirements to segment host pools from each other or granularly control communication from a host pools to applications locally in other clouds.
- Secure Remote Access – WVD users need secure access to WVD hosts and in many cases require end-to-end encryption to comply with regulatory requirements or corporate security policies.
- Other Architectural Components – Dependencies (e.g. Windows activation) each have specific connectivity and security requirements.

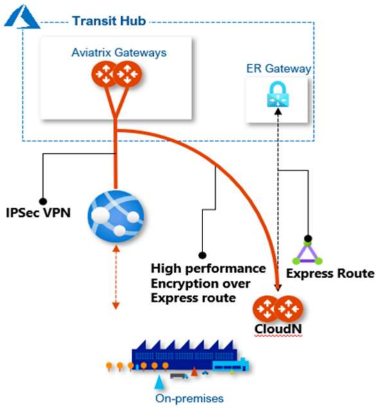


Source ↑↓	State ↑↓	Address Prefixes ↑↓	Next Hop Type
Default	Active	10.0.0.0/24	Virtual network
Default	Active	0.0.0.0/0	Internet
Default	Active	10.0.0.0/8	None
Default	Active	100.64.0.0/10	None
Default	Active	192.168.0.0/16	None

How Aviatrix Addresses Windows Virtual Desktop Challenges in Azure Cloud

The Aviatrix cloud network platform enables enterprises deploying Azure WVD to quickly put an intelligent, secure cloud networking infrastructure in place as the foundation for their Azure WVD managed service. This Aviatrix validated design brings a standardized approach applicable whether you are in a single, or multiple clouds. The design specifically applies to WVD deployments. The Aviatrix cloud network platform quickly solves all of the inherent challenges with the service, accelerating the onboarding of users.

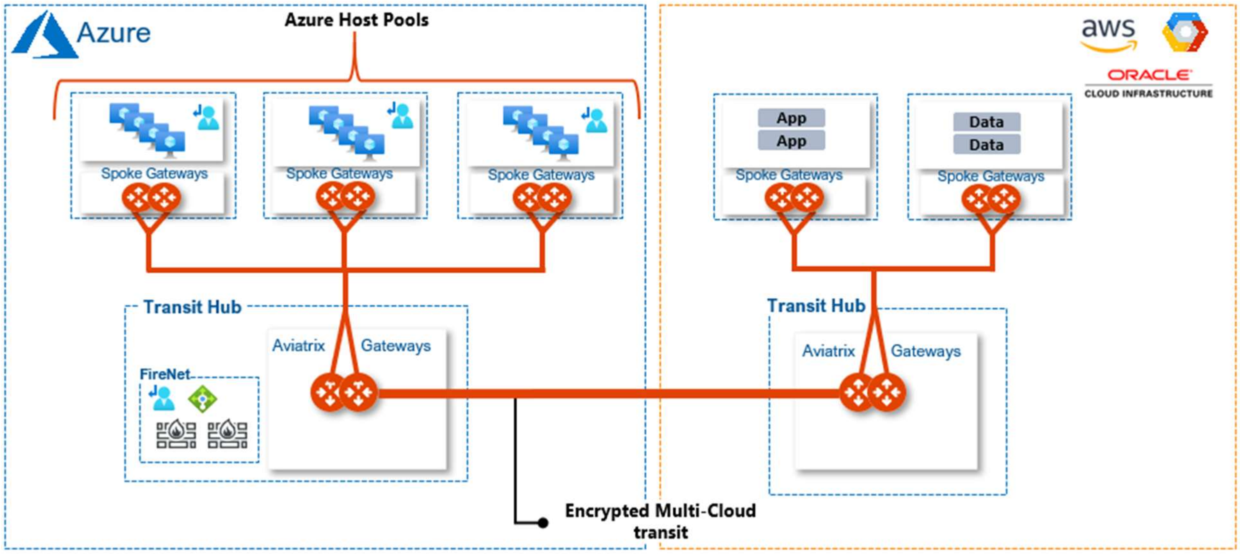




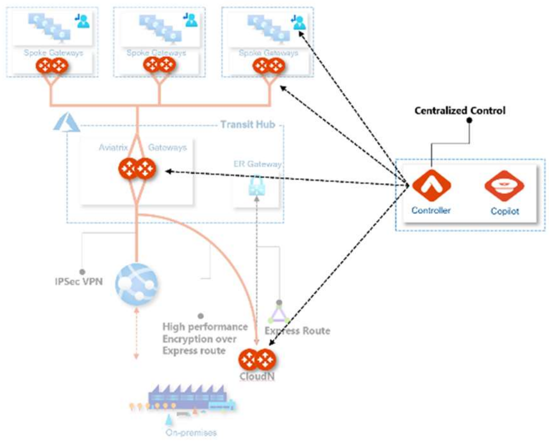
While employees, partners and other WVD users are now working remotely from home and their Azure WVD is accessed over the internet using their home broadband connection, the backend applications are often operating on workloads still on-prem, or in a cloud other than Azure. There are two key features the Aviatrix design delivers:

Private On-Prem Connectivity - Express Route + Aviatrix CloudN appliances deliver enterprises line-rate encryption capabilities as well as extends visibility to on-premises. Standard IPSec encryption imposes a 1.25 Gbps performance limitation, Aviatrix allows customers to take full advantage of the throughput offered by Express Route connectivity (e.g 10 Gbps), while delivering private on-prem connectivity by aggregating multiple 1.25 Gbps tunnels and processing cores.

Multi-Cloud Network Connectivity – Utilizing Aviatrix transit gateways, host pools can easily and securely access workloads in other public clouds. The Aviatrix Multi-Cloud Network Architecture (MCNA) builds on its overlay transit network, which provides complete end-to-end encryption, and seamless connectivity into and across other cloud providers (AWS, GCP, and OCI). This design simplifies host connectivity to application services and/or data that reside in other clouds, while delivering a consistent, repeatable, auditable security model across all clouds.

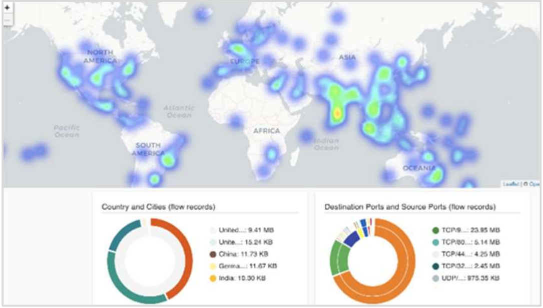


Centralized Control, VNet Deployment Automation and Route Table Orchestration, Visibility and Troubleshooting



The brain of the Aviatrix cloud network platform is the Aviatrix intelligent controller. The Aviatrix controller allows you to leverage the native constructs in Azure and delivers an enterprise-grade cloud network. The controller allows you to take full control of your cloud networking, including on-prem connectivity, native construct orchestration (e.g VNet route tables), security orchestration (e.g. host pool segmentation), next gen firewall service insertion (e.g. Palo Alto Networks VM-series, Check Point Cloud Guard IaaS), Day2 operational visibility, and multi-cloud transit. The platform leverages the centralized intelligence and knowledge of the controller to dynamically program both native cloud network constructs and advanced services on Aviatrix's own gateways. Combined with Aviatrix's multi-cloud Terraform provider this design enables network and security Infrastructure-as-Code automation with a repeatable architecture across a multi-cloud environment. Three key features delivered by the Aviatrix design:

1. **Direct Internet Access Control** – The controller orchestrates VNet routing tables to connect through the Aviatrix Transit network, ensuring end-to-end routing correctness, including UDR management critical to secure VNet default routing behavior (0.0.0.0 default) so that network communications meet corporate and regulatory security requirements. Visibility and operational control over internet bound traffic is an important element of any enterprise cloud architecture. Aviatrix provides the visibility to understand what applications are communicating with and enables filtering control over those communications.
2. **Host pool segmentation** – Enterprises leverage our multi-cloud network segmentation to create security domains and isolate WVD host pools and their respective applications. This includes extending segmentation connection policies to other clouds, without requiring access to each cloud provider specific policy interfaces.
3. **Visibility & Troubleshooting –** Default deployments of WVD do not provide visibility into any traffic, and native tools offer silos of information which is not easily correlated to provide a complete picture. Aviatrix CoPilot delivers operational visibility that goes far beyond what any cloud provider delivers today. This includes dynamic multi-cloud network topology mapping, Aviatrix FlowIQ intelligent traffic flow analysis and several features which help cloud operations teams quickly isolate and troubleshoot network and/or application issues.

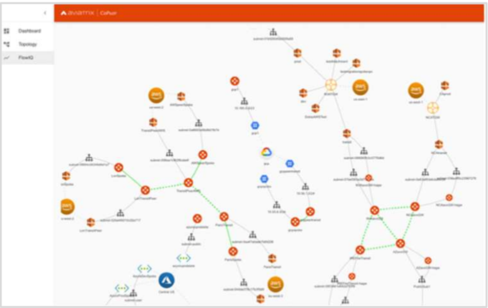


Country and Cities (flow records)

- United...: 9.41 MB
- Unite...: 15.24 KB
- China: 11.73 KB
- Germa...: 11.67 KB
- India: 10.30 KB

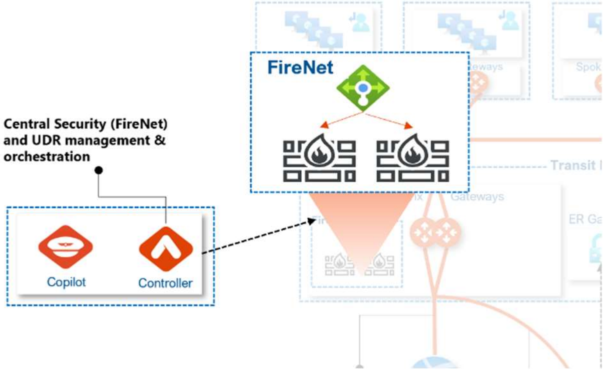
Destination Ports and Source Ports (flow records)

- TCP/9...: 23.95 MB
- TCP/80...: 5.14 MB
- TCP/44...: 4.25 MB
- TCP/32...: 2.45 MB
- UDP/...: 975.35 KB

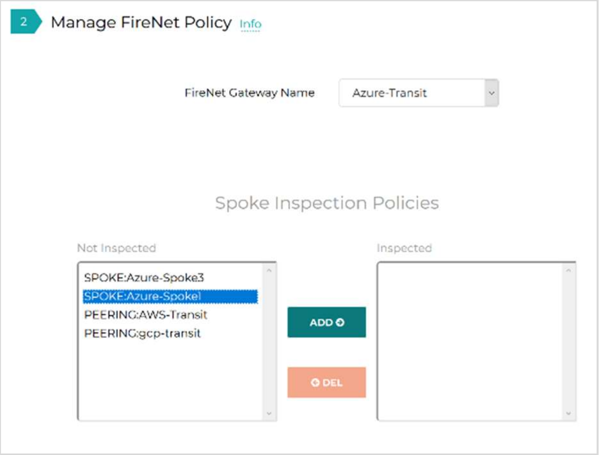


Security Service Insertion – Aviatrix Firewall Network

A critical part of this Aviatrix Validated Design is the Aviatrix Firewall Network or "FireNet" service. WVD traffic flows can be classified into two groups – WVD service control plane traffic and host pool traffic. By default, both of these flows have access to both the Internet and the WVD control plane. Both WVD host pool communications and WVD control plane connections should be secured by routing inter-pool communication for firewall inspection. Other WVD dependencies (e.g. Windows Activation and Updates) should also be routed and secured through centralized firewalls.


FireNet
Central Security (FireNet) and UDR management & orchestration
Copilot
Controller
Transit
Gateways
ER Ga
Spok

The Aviatrix controller seamlessly orchestrates Firewall insertion (e.g. Palo Alto Networks VM-Series or Check Point Cloud Guard, Fortinet) as part of the FireNet deployment. The controller then automatically manipulates VNet route tables to direct specific traffic to service chain through the centralized firewalls. This allows traffic flows to be inspected and controlled. Leveraging a combination of security domains, connection policies and firewall inspection delivers granular, intent based isolation within region, across multiple regions, or across multiple clouds.



2 Manage FireNet Policy Info

FireNet Gateway Name: Azure-Transit

Spoke Inspection Policies

Not Inspected:
SPOKE:Azure-Spoke3
SPOKE:Azure-Spoke1
PEERING:AWS-Transit
PEERING:gcp-transit

Inspected:

Aviatrix FireNet is used through a simple point a click interface or infrastructure-as-code Terraform automation. Operations teams easily select which traffic requires inspection by selecting which on-prem connections, spoke VNet connections, or transit hub connections should be inspected and controlled. FireNet provides a number of additional services including firewall scale-out and Source Network Address Translation (SNAT) elimination, allowing network teams to maintain source address visibility for VNet-to-VNet traffic flows.

Infrastructure as Code Automation

Deployment and updates easily fit into existing CI/CD pipelines with the Aviatrix multi-cloud Terraform Provider. The Aviatrix Terraform Provider leverages the multi-lingual capabilities of the Aviatrix Controller. The controller communicates with the unique, native network constructs in each cloud through public APIs, creating a multi-cloud abstraction layer. Terraform modules are then developed with the Aviatrix Terraform Provider to deploy repeatable network designs in different clouds with a single Terraform module.

Secure Remote Access (SAML SSL VPN) – Leverage Active Directory, Okta, Duo or other enterprise identity provider for SAML Authentication, then leverage Aviatrix OpenVPN Client to establish encrypted connectivity to Aviatrix transit VPN gateways. This provides customers secure, end-to-end encrypted connectivity to only their WVD hosts.

Additional Windows Virtual Desktop in Azure Design Considerations

Performance

In Azure, VM sizing determines the performance of an instance. Customers should do careful planning to ensure proper sizing is in place for the initial deployment. Aviatrix does provide resizing capabilities, which allows customers to grow gateway instances on demand. Our Aviatrix "InsaneMode" high-performance encryption provides capability to aggregate multiple tunnels and processing cores to deliver wire speed encryption to create high-performance private connections over data center to cloud connections such as Express Route. The Aviatrix patented solution overcomes the 1.25 Gbps limit delivered by native cloud solutions, to provide 10 Gbps of IPSec encrypted throughput. This same solution can be provided in the cloud with performance up to 75 Gbps.

High Availability

This validated design for WVD in Azure recommends Aviatrix gateways to be deployed in high-availability pairs, each in a different availability zone. Aviatrix ActiveMesh is automatically enabled, creating an active-active full mesh ECMP connection between Aviatrix gateways. The Aviatrix controller monitors all gateways that make up the ActiveMesh to ensure that traffic is directed across the optimal path, CoPilot highlights latency spikes and any connectivity failures and gateway automatically recover and resume position in the ActiveMesh network topology.

Engage with Aviatrix

Help with MCNA Architecture or this validated design: info@aviatrix.com

Online Documentation: docs.aviatrix.com

Join the Aviatrix Community

About the Author

Manny Calero is a Principal Solutions Architect at Aviatrix and a former Microsoft Azure Networking "Black Belt" and led the creation of this validated design.

Manny can be reached at mcalero@aviatrix.com