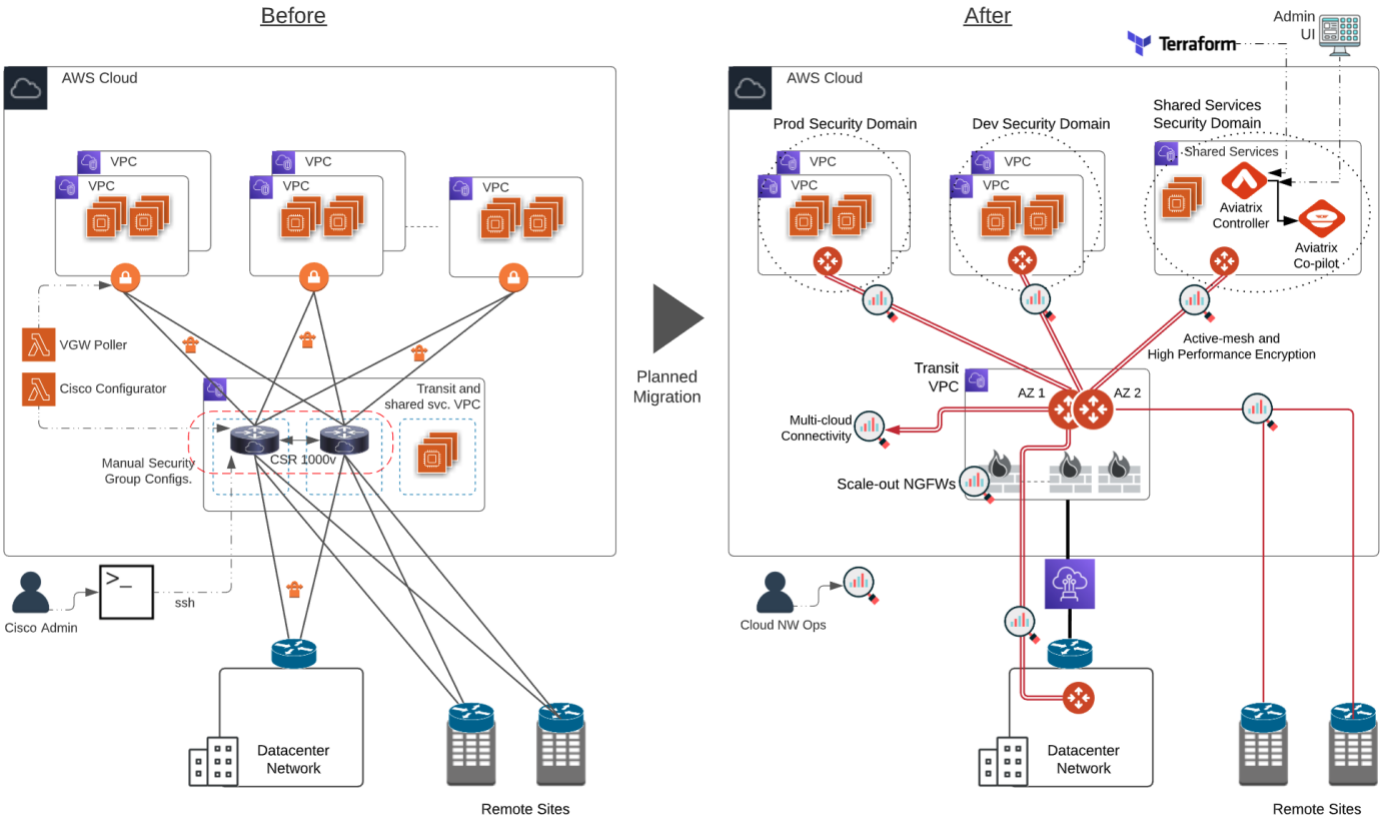
Aviatrix Designs for Cisco CSR 1000v Migrations

Overview

The Aviatrix cloud network platform offers enterprise customers a superior, cloud aware alternative to Cisco Cloud Services Router (CSR) deployments. In the past, many early cloud adopters sought to maintain operational familiarity with Cisco hardware products they have on-premise by using the CSR 1000v virtual appliances. Enterprises who have migrated away from a CSR-based transit network to Aviatrix Transit did so for several reasons that we will detail in this validated design guide, including:

- **Operational Gain –** Modern, central control replaces legacy device-by-device discrete config file CLI mgt
- **Visibility –** Detailed multi-cloud topology and flow visualization, overcomes effectively no cloud network visibility
- **Performance –** CSR link throughput is < 1.25 Gbps with ~5 Gbps backplane; Aviatrix delivers up to 70 Gbps on both
- **Route Table Limitations –** Aviatrix delivers thousands of route table entries; CSR is limited by VGW attachment to 100

This validated design guide explores these drivers for migrating from CSRs to Aviatrix Transit and provides several network designs and migration plans that have been proven by Aviatrix customers.



Aviatrix make it simple to migrate from legacy CSR implementations to Aviatrix Transit and if desired, Aviatrix "White Glove" service teams are available to help plan and execute the transition with you.

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 vertical industry 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 counterparts to work together to ensure network designs meets 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.

Customer Challenges with Cisco CSR-based Cloud Networking

- Operational Pain – Device-by-device discrete config file through a legacy CLI is an artifact of a 1990's hardware centric operational model that enterprise customers moving into the cloud want to leave behind. Customers are looking for a modern, intelligent operational model that allows IT to operate at "cloud speed".
- Automation – While application teams have been embracing a DevOps approach to services delivery for years, traditional hardware-centric deployment models, even when virtualized, have not evolved to keep pace. Enterprise customers must have multi-cloud Terraform Infrastructure as Code automation that fits seamlessly into existing DevOps CI/CD pipelines.
- Visibility – CSR-based cloud transit networks offer almost no visibility and troubleshooting capabilities. Enterprise customers what dynamic multi-cloud topology mapping, intelligent flow visualization and detailed analytics, they want the troubleshooting capabilities such as ping, traceroute, and packet capture, which were available on-premises, but now are required in the cloud.
- Performance – Customers discover serious performance limitations of link throughput. CSRs are limited to < 1.25 Gbps with ~5 Gbps backplane because of IPSec tunnel and processing overhead. Aviatrix can provide up to 75 Gbps throughput leveraging unique tunnel aggregation and processing distribution over multiple host cores.
- Route Table Limitations –CSRs limited by AWS VGW attachment to 100 route table entries, and while this may satisfy the requirements for very small deployments, Aviatrix customers are often challenged by this limitation and are forced to summarize or make unnatural architectural compromises that add to design complexity. Aviatrix delivers unlimited route table entries.
- NextGen Firewall Service Insertion – Cisco CSRs are effectively unaware they are even operating in a cloud environment, so they offer no leverage or interaction with native cloud constructs or dynamic integration with third party cloud services such as virtual next generation firewalls. Aviatrix simplifies both deployment and operations of native cloud services and next gen security service insertion, while maximizing throughput performance and source address visibility.

Design Elements and Features

Aviatrix Intelligent Centralized Controller

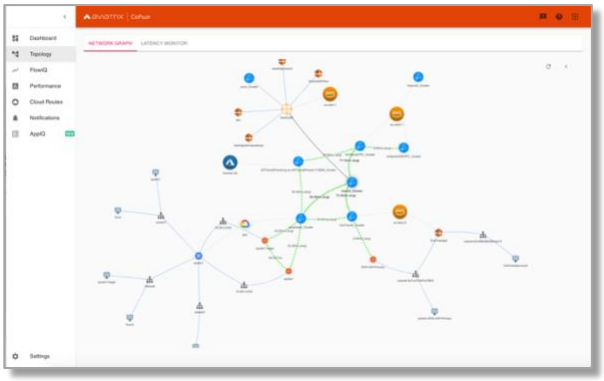
The Aviatrix controller is the brain of the cloud network platform. The platform leverages the centralized intelligence and knowledge of the controller to dynamically program both native cloud network constructs and Aviatrix's own gateway's advanced services. Combined with Aviatrix's Terraform provider this design enables network and security Infrastructure-as-Code automation across a multi-cloud environment. The Aviatrix controller provides the central point of control and management either through the controller UI or directly via the Aviatrix multi-cloud Terraform Provider API, giving customers central operational control over the fully distributed data plane.

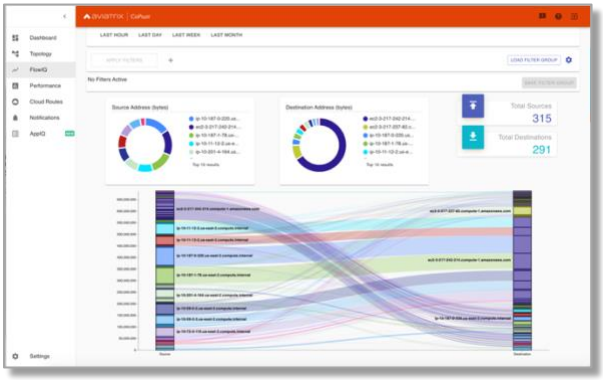
Aviatrix Gateways

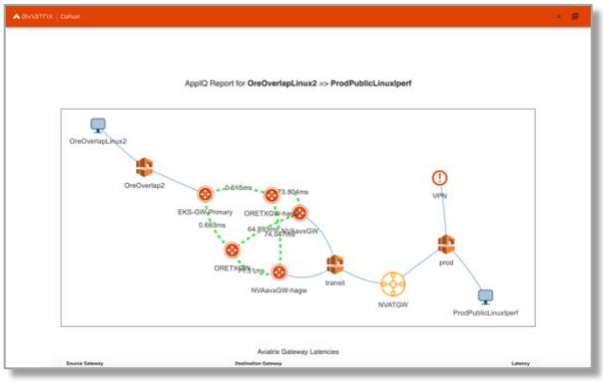
Aviatrix gateways deliver advanced cloud networking and security services. In this validated design guide Aviatrix Gateways are mostly deployed to provide advanced transit network and security features such as intelligent dynamic routing, active-active network high-availability, end-to-end and high-performance encryption and collect operational visibility data that feeds CoPilot, Aviatrix's powerful visibility platform. Aviatrix gateways replace Cisco CSR 1Kv appliances and provide optimized high throughput with limited compute requirements, in most cases dramatically reducing the costs of the underlying compute capacity. Aviatrix Gateways are multi-functional, and services can be aggregated on a single compute platform or deployed individually to optimize for performance, cost, security or any combination.

Aviatrix CoPilot (optional)

Aviatrix CoPilot provides a global operational view of your multi-cloud network not available from AWS, Azure or any other cloud provider. Enterprise IT teams – who need day-two operational visibility for cloud networking – use CoPilot's dynamic topology mapping to maintain an accurate view of their global multi-cloud networks, FlowIQ to analyze global network traffic flows and global heat maps and time series trend charts to easily pinpoint and troubleshoot traffic anomalies. CoPilot leverages the intelligence and advanced network and security services delivered by the Aviatrix cloud network platform. With Aviatrix, cloud network and security operations teams have familiar day-two operational capabilities such as packet capture, trace route and ping to resolve problems faster. Operational features include resource tagging, resource clustering, infrastructure monitoring and alerting, all specifically built for multi-cloud network operations.







End-to-End and High-Performance Encryption

The Aviatrix Transit defaults to end-to-end encryption, however standard IPSec encryption is limited to 1.25 Gbps, so in active-active ECMP high-availability mode provides 5Gbps bi-directional throughput. To achieve much higher IPSec encrypted throughput, Aviatrix's high-performance encryption distributes processing across multiple cores and aggregates IPSec tunnels to reach wire speed encryption across private connections, such as AWS Direct Connect or Azure Express Route and up to 75 Gbps for intra-cloud links.

Multi-Cloud Network Segmentation and Security Policy Compliance

Most enterprise corporate or regulatory security policies require network segmentation. While it is possible to filter traffic with ACLs in CSR-based cloud network configurations, this is a tedious manual process that is prone to human error. Aviatrix designs deliver an automated solution that extends secure network segmentation beyond cloud boundaries, enabling multi-cloud security domains, with consistent, centrally managed, global network segmentation and connection policies.

VPC and VNet Internet Egress and Ingress filtering

Aviatrix Transit provides a secure point of access for network and security services such as next-generation firewalls, IDS/IPS and SD-WAN cloud edge connections. Aviatrix gateways provide load balancing to scale out connected services and ensure redundant and failover high availability. While many enterprises leverage the Aviatrix Transit FireNet centralized design, others opt for a distributed solution that provides filtering directly from within each VPC or VNet. Aviatrix gateways offer both ingress and egress L4 and Fully Qualified Domain Name (FQDN) filtering. Centrally managed filter groups with distributed execution ensure consistent multi-cloud security for any cloud application communicating with Internet-based resources and service.

Optimal Path Routing and Traffic Engineering

ActiveMesh allows gateways to leverage BGP metrics such as MED, AS-PATH into consideration for the same route from different neighbors and use that to make the optimal path selection. The path selection algorithm is prescriptive and provides significant flexibility options for multi-region designs. For example, allowing for on-prem route manipulation setting preference between neighbors in different regions. To support, for example multi-region HA, both on-prem data centers advertise the same routes into multiple regions through the cloud access layer into each of the Aviatrix Transit gateways. Overlapping CIDRs learned by Aviatrix Transit gateways in both regions are advertised over the transitive peering connections to the other region's transit pair. This would normally cause serious asymmetric routing or routing loop challenges. However, the Aviatrix Controller has the intelligence to ensure the local region route is preferred over the transitive peering route, avoiding any loops or asymmetric issues.

Automation, Visibility and Operational Control

Deployment and updates easily fit into existing CI/CD pipelines with Terraform and the Aviatrix API. Visibility and operational control over internet bound traffic is an important element of any enterprise cloud architecture. Cloud applications with unrestricted access to the Internet-based services expose environment to attack. Best practices limit application network communications to only known Internet-based services. For example, app tier services that require build packages from GitHub must have access to github.com, but all other access should be filtered and blocked. Aviatrix provides the visibility to understand what Internet-based services applications are communicating with and gives the control to filter those communications by Fully Qualified Domain Names (FQDN).

Design Considerations

When evaluating a possible migration to Aviatrix cloud network platform from an existing Cisco CSR deployment or evaluating whether to use Aviatrix or CSRs, there are a number of factors you should consider that can have significant impact on your design and your end result. These design considerations include performance, large frame support, network segmentation, centralized management and visibility, route limitations, third-party service insertion, cloud native awareness and intelligent network correctness.

Transit Network Performance

Aviatrix directly programs cloud native constructs using the cloud service provider's published APIs. Leveraging this capability, the Aviatrix controller is able to update native VPC or VNet route tables without relying on native constructs to propagate routes and limit performance. Establishing logical tunnels between Aviatrix Gateways that reside in each VPC/VNET and leveraging native peering allows Aviatrix to provide a near line rate (~50Gbps) encrypted transit data plane. This is achieved using Aviatrix ActiveMesh, deploying two gateways in each VPC/VNet to deliver a highly redundant, active/active ECMP design that ensures traffic is load balanced in a full mesh between hub and spoke gateways. The gateways can be deployed on a variety of instance types depending on the VPC/VNET performance requirements.

In contrast, CSR deployments require the CSRs to terminate IPSec tunnels on native constructs, such as AWS VGW, in order to propagate routes to spoke VPCs/VNets. This limits connection throughput to less than 1.25 Gbps or requires a CSR in every spoke, creating a very expensive and generally unmanageable design.

Multi-Cloud Network Segmentation

As enterprises move to the cloud, corporate and regulatory policies require network isolation to limit the blast radius in event of a security breach. This becomes even more critical when enterprises must enable partners and/or customers to directly to their cloud-based services, while having full control on what networks or areas of the cloud those third parties are able to access. The Aviatrix cloud network platform provides the ability to segment network traffic within, between and across cloud environments using route-based connection policies. The resulting security domains are global in scope and deliver end-to-end network segmentation, giving enterprises the ability to logically combine similar networks their entire multi-cloud and hybrid on-prem environments. The connection policies define a set of rules that easily facilitate cross security domain communication.

In contrast, a CSR based implementations make it hard to implement cloud-scale segmentations and the maintenance of the constructs over time. The lack of cloud aware controls leaks all the routes via BGP to the connected networks.

Centralized Cloud Network Control

An Aviatrix controller creates a unified management plane to build and control cloud networks across clouds. The Aviatrix controller is the brain of the cloud network platform. The Aviatrix cloud network platform leverages the intelligence and network-wide knowledge of the centralized controller to dynamically program both native cloud network constructs and Aviatrix Gateways which provide the advanced network and security services that helps differentiate the Aviatrix solution. Combined with Aviatrix's multi-cloud Terraform provider this design enables network and security Infrastructure-as-Code automation across multi-cloud environment.

In contrast, CSR manageability is a complex and manual device-by-device exercise that requires a combination of legacy Cisco CLI configuration and independent CSP networking construct management tools.

Centralized Visibility Platform

The Aviatrix controller enables centralized monitoring and logging for all Aviatrix components as well as built in tools that can provide visibility into CSP route tables, security groups and network ACL's to provide insights into communication between instances. Additionally, all Aviatrix gateways support built-in packet capture capabilities and real-time data plane diagnostics. Lastly, the Aviatrix cloud network platform provides data to Co-Pilot, Aviatrix's visualization platform, which in turn delivers real-time, dynamic, multi-cloud network topology mapping, intelligent traffic flow analytics and visualization and advanced alert management. CoPilot has been applauded by enterprise operations teams as one of the most valuable solutions for solving networking and application level issues in complex cloud network environments.

In contrast, a CSR-based infrastructure offers little or no visibility without a tedious combination of Cisco + CSP + third-party tools, which dramatically increases complexity and time to resolution.

Route Table Limitations

Enterprises often have scenarios that require the propagation of thousands of routes across their multi-cloud and on-prem cloud environments. Summarizing these routes is not an option for various reasons. Most native cloud networking constructs have route limitations and, making it difficult or impossible to easily accommodate this enterprise requirement and often forces undesired network design compromises. For example, AWS VGW has a BGP route limitation of 100 routes. The Aviatrix gateways are capable of handling thousands of routes, both static and dynamic, in any cloud environment which gives enterprises flexibility to design their networking the way they want to.

In contrast, CSR implementations provide no value in overcoming cloud route limitations especially at enterprise scale.

Next Gen Firewalls and Other Third-Party Service Insertion

Aviatrix platform allows enterprises to insert next generation firewalls of their choice from Palo Alto Networks, Check Point, Fortinet and others directly to the Aviatrix multi-cloud transit network. This enables security controls to be centrally defined, automatically directing specified traffic to be routed for inspection, without complex manual route reconfigurations. Aviatrix gateways in this design load balance the traffic across the firewalls, manage session mapping to specific firewalls, so that there is no need of SNAT, enables line rate throughput performance and allows scale-out based on the network load to as many firewalls as required.

In contrast, CSRs do not provide any value for third party service insertion of any kind.

Cloud Awareness

Aviatrix was developed in the cloud and has been built from the ground up to be cloud aware. Meaning the Aviatrix cloud network platform is aware of, leverages and directly programs native cloud constructs and adds advanced network and security features enterprises require, but are missing from native cloud network offerings. The Aviatrix platform utilizes centralized visibility and advanced network capabilities to deliver common, repeatable designs, regardless of the underlying CSP networking constructs, leveraging where we can and adding or replacing where required. In addition to visibility and network connectivity, the Aviatrix platform leverages CSP API to deploy load balancers, enable cloud services, Next Generation Firewall's and much more.

In contrast, CSRs are unaware that they are even operating in a cloud and are simply providing legacy network connectivity as if a simple router operating in an on-premise data center.

Large Frame Support

If a cloud provider's native constructs support jumbo frames, the Aviatrix data-plane can be used to transmit and receive jumbo frame packet sizes, up to 9k frames. This ensures that if applications support and choose to use jumbo frames the transit architecture can forward without fragmentation.

In contrast, CSR, again is limited by native bottlenecks to 1,500-byte frames.

Centralized Intelligent Network Correctness

The Aviatrix controller automatically evaluates network configurations before network insertion to identify potential issues such as overlapping CIDRs and holds suspected conflicts for approval or NATing. Also, as network changes take place across the organizations, the Aviatrix controller actively manages cloud route propagation including route approval workflows. The controller, in conjunction with CoPilot AppIQ, performs path evaluation to verify both routing correctness and security configurations for application communications and monitors latency and workload analytics to reduce time to resolution network troubleshooting.

In contrast, CSR deployments have no centralized knowledge and no intelligence to identify misconfigurations or scenarios such as overlapping CIDRs, either in the cloud or from connected customers or partners.

Cost Optimization

The Aviatrix cloud network platform's main infrastructure components include the centralized Aviatrix Controller and distributed Aviatrix Gateways. Both of these components are deployed on cloud compute instances or VMs. The controller only has one function as the brain of the platform and requires a medium sized compute platform. Gateways leverage the same software but are deployed to deliver specific advanced networking and security services. Services can be combined or separated, and compute capacity varies based on service performance requirements. This ability allows cloud network operations teams to optimize the size and therefore the cost of the underlying infrastructure.

In contrast, CSR software was developed and optimized to leverage dedicated hardware. Porting this software to run on standard cloud compute requires large, expensive compute with little or no ability to optimize underlying infrastructure cost.

Design Options

The Aviatrix Cloud Network Platform is extremely flexible and can be deployed number of different ways based on your business and technical requirements. It is a low friction solution that fits easily in existing processes without requiring significant modifications to the existing cloud provisioning workflows.

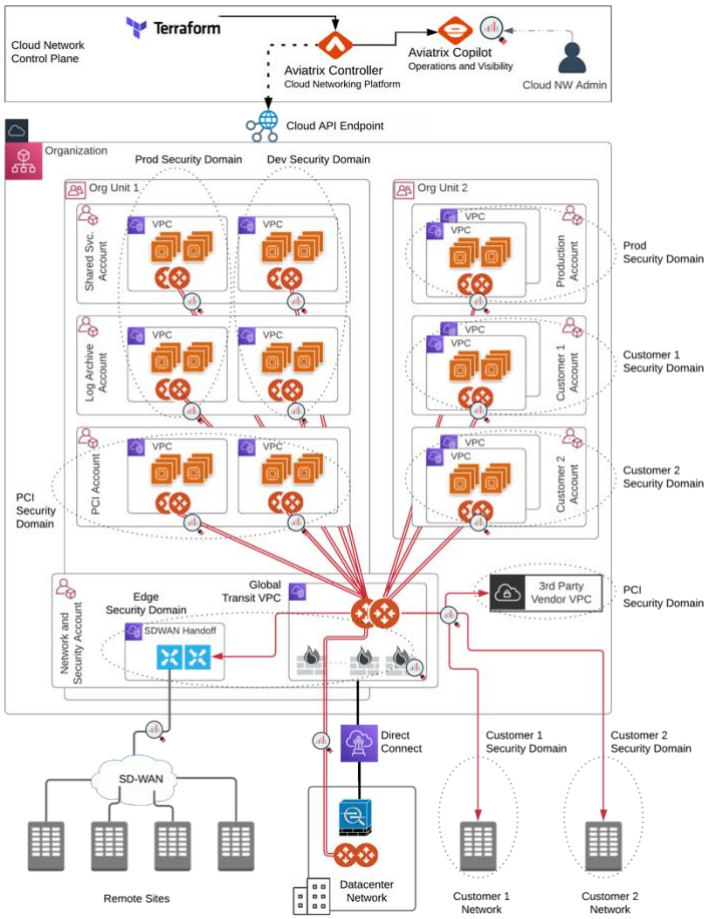
The following are number of different deployment models and designs. This document focuses on three validate designs that are widely deployed by the Aviatrix customers, including single cloud, single region; single cloud, multi-region; multi-cloud; and multi-cloud with SD-WAN handoff.

Single Cloud, Single Region Design

This design option enables organizations to utilize full suite of Aviatrix platform features and build their cloud network even with the presence in a single cloud and a single region. In a typical network design, usually, the workloads could be spread across multiple cloud accounts and networks (VPCs or VNETs) within a region. Aviatrix platform enables to connect these networks in a hub and spoke aka transit architecture and also build a consolidated edge connectivity to establish hybrid networks. The design is achieved by creating a global transit VPC with Aviatrix transit gateways in it. Each Spoke VPC (VPCs with workloads) also has Aviatrix spoke gateways in it. Spoke VPCs are connected to the Transit VPC by establishing full mesh encrypted connectivity between the spoke and the transit gateways. The hybrid connectivity is established by either building BGP or static connections from transit gateways.

Design Advantages

- The design could be deployed either through the Aviatrix controller or through automation using Aviatrix APIs or Aviatrix terraform provider
- Two gateways in each VPC for active-active, full mesh connectivity and highly available design
- Aviatrix Controller takes care of updating the VPC/VNET route tables to avoid human errors and ensures network correctness
- Option to introduce Next generation firewalls for inline traffic inspection
- Ability to segment the network traffic based on the business units, VPC/VNET owners, type of applications deployed etc.
- Ability to build as many edge connections, both BGP and static, as needed. Also, the flexibility to build edge connections to third parties i.e. customers or partners
- Aviatrix supports SD-WAN Handoff to easily connect any SD-WAN service to the Aviatrix transit in a way that simplifies SD-WAN configuration, maintains BGP traffic engineering and network segmentation and takes advantage of centralized NGFW services in the cloud
- Aviatrix platform provides deterministic and optimal path selection by taking BGP metrics into consideration for making routing decisions



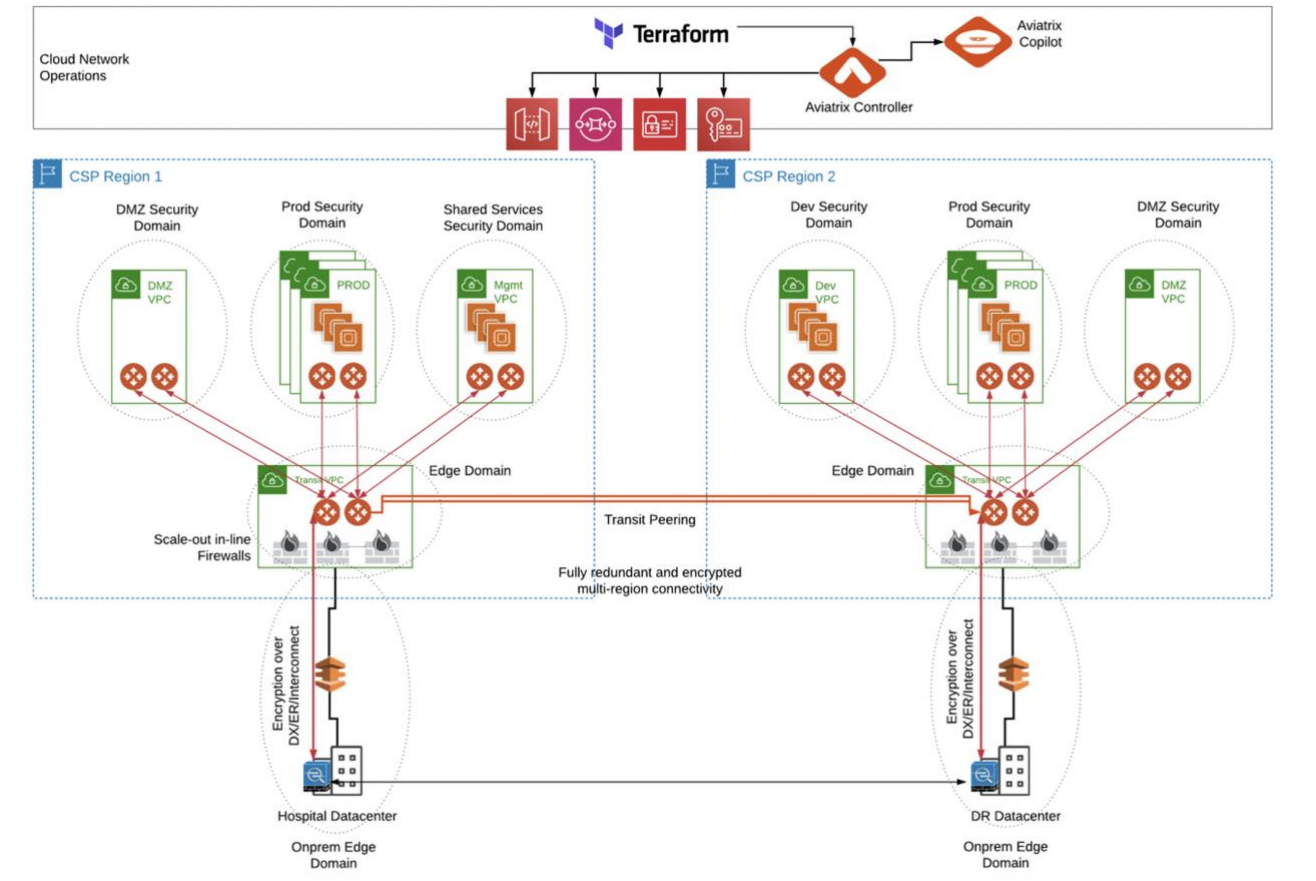
- All traffic between Aviatrix gateways is IPSec encrypted. Standard IPSec encryption is limited to 1.25 Gbps. Aviatrix's high-performance encryption distributes processing across multiple cores and aggregates IPSec tunnels to achieve wire speed encryption, up to 75 Gbps.

Single Cloud Multi-Region Design

As the organizations grow their footprint in the cloud, a multi-region cloud design is often required. This design enables organizations to build and manage their cloud network using Aviatrix cloud network platform across multiple regions within a single cloud platform. Multi-region connectivity allows organizations to meet additional requirements such as multiple data centers, customers, partners and employee locations that require access to cloud-based applications or regionally specific resources. This design builds on the principles laid out in "Single Cloud, Single Region design" and extends them to deliver multi-region network requirements. The architecture delivers an inter-region transit network leveraging Aviatrix gateways in each region and peers them together to enable communication among the workloads spread across regions. The Aviatrix Multi-Region High-Availability Cloud Network Validated Design Guide provides more detail on this design pattern.

Design Advantages (includes all of the advantages described above for the Single Cloud, Single Region Design, plus)

- Provides full control on network route propagation across the connected regions
- Delivers multi-region fault tolerance and high availability for cloud services and applications
- Extends secure network segmentation across the regions
- Allows multiple cloud-to-on-premises connections, enabling network redundancy and multi-path reachability
- Reduces latency by allowing users to access cloud workloads via the closest point of entry in their region

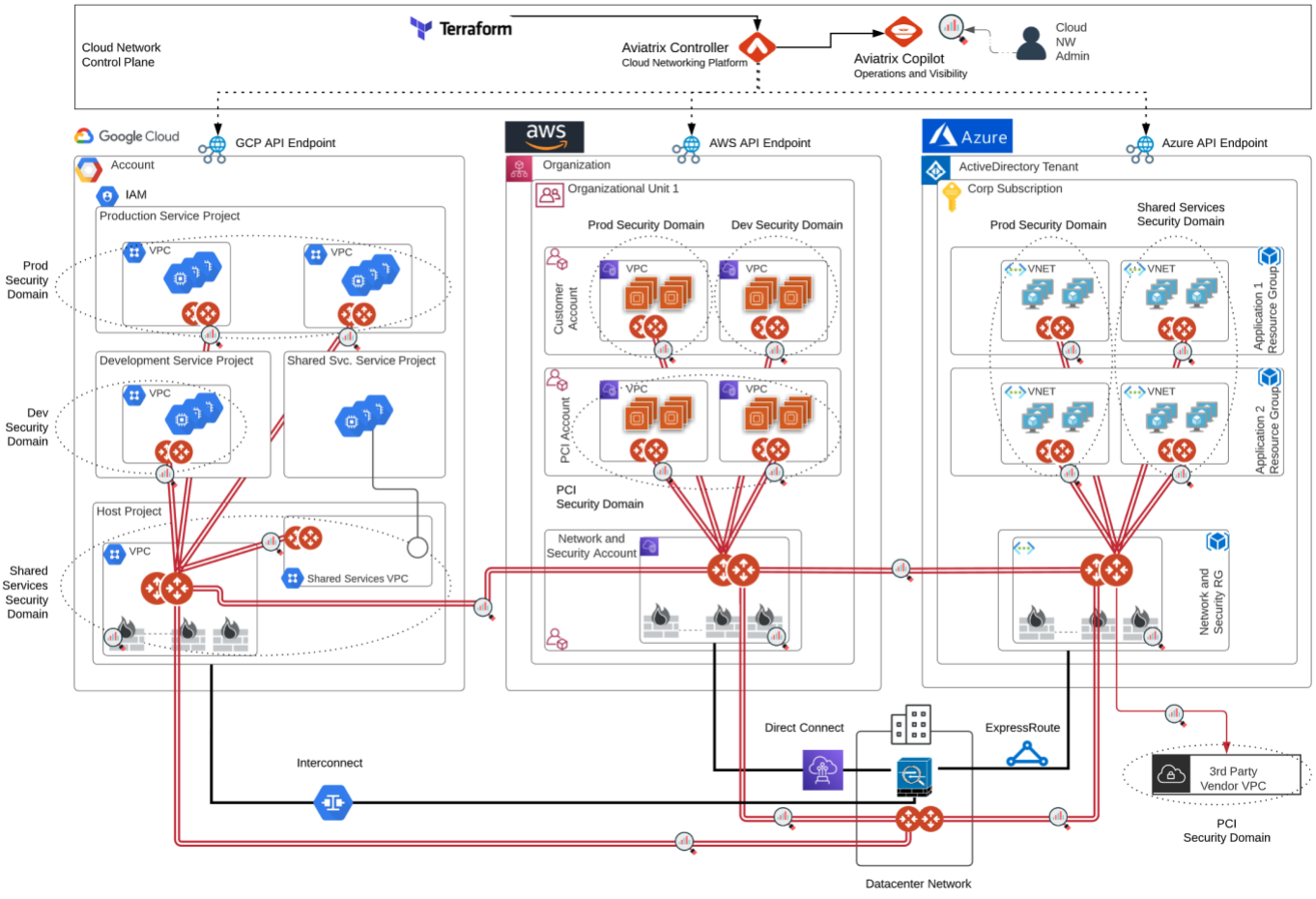


Multi-Cloud Design

This design fully leverages a multi-cloud network architecture to enable businesses to leverage any combination of cloud service providers required to best support their applications, business and customers. The Aviatrix cloud network platform delivers the architectural flexibility and enterprise-class features IT organizations need to design a multi-cloud network. Aviatrix cloud network platform avoids service provider lock-in by delivering a superset of capabilities that meet enterprise requirements for advanced networking, security, operational visibility and multi-cloud optionality. This design builds upon the principles of both the above Single Cloud, Single Region and the Single Cloud, Multi-Region designs and extends them to a complete multi-cloud design. The Aviatrix Transit network traverses cloud providers, creating a common, repeatable hub and spoke design in each cloud, leveraging and controlling the underlying native cloud constructs and adding advanced features to create a common multi-cloud network data plan and operational visibility. This is achieved by leveraging Aviatrix gateways in both transit and application VPCs or VNETs and connecting them together to build the multi-cloud transit network.

Design Advantages: (includes all of the advantages described above for the Single Cloud, Single and Multi-Region Designs, plus)

- Empowers organizations to choose best-of-breed cloud platform based on the application, business and customer needs
- Delivers full control over network route propagation across any connected cloud environments
- Provides multi-cloud fault tolerance and high availability for cloud applications
- Extends secure network segmentation across clouds
- Allows multi-cloud-to-on-premises connections, enabling network redundancy and multi-path reachability



Making the Switch – A Simple Step-by-Step Migration with Almost Zero Downtime

Aviatrix offers a Professional Services engagement specifically for planning for, automating, executing and testing CSR migrations to ensure your application environments are transferred to the Aviatrix Transit without incident.

In the end the migration is actually very simple and consists of the following steps:

1. **Plan the migration.** A good plan ensures that all transit network and application requirements are taken into account and any unique connectivity details have been considered and prepared for.
2. **Deploy the Aviatrix Controller and Transit hub**. This is a simple process of launching the Aviatrix controller and transit gateways. This can be done at any time prior to the migration and takes less than 30 mins.
3. **Deploy Aviatrix Spoke Gateways in each VPC or VNet**. This step is usually automated and performed without impacting the existing environment.
4. **Duplicate the Route tables in each Spoke VPC or VNet**. This step is automated and will result in the duplicated copy of each Route table and ensure the same VPC to be attached to the Aviatrix transit and CSR transit at the same time
5. **Attach Spoke Gateways to the Aviatrix Transit Hub**. Again, this step is usually automated and performed without impacting the existing environment. This step attaches the Spoke VPCs to the Aviatrix transit VPC using the duplicate route tables (Aviatrix managed Route tables). Once attached, the Aviatrix controller will inject the appropriate routes in all Aviatrix managed Route table. This step ensures existing traffic flowing through the CSRs is not impacted until you are ready to make the final switch over to the Aviatrix Transit.
6. **Disengage the CSR Connections by changing the subnet associations to the Aviatrix managed route tables**. This is an automated process for each VPC/VNet that disassociates the subnets from the existing route tables and associates them to the Aviatrix managed Route tables thus directing all the application traffic through the Aviatrix Gateway and Aviatrix Transit Hub.
7. **Transfer any Direct Connect or Express Route Connections to Aviatrix Transit**. This removes the final remaining connection to the CSR environment.
8. **Remove CSRs and CSR Transit VPC/VNet**.
9. **Test Plan Execution**. During the planning stage a test pan will be established to confirm that all expected application connectivity is still operational and performing as expected.

To find out more about Aviatrix Professional Services please send an email to info@aviatrix.com.

Engage with Aviatrix

Online Documentation: docs.aviatrix.com

Help with MCNA Architecture or these validated designs: info@aviatrix.com

Schedule a demo

Join the Aviatrix Community

About the Authors

Gaurav Thakur is a Senior Sales Engineer at Aviatrix based in Santa Clara and Tom Davis is a Senior Systems Engineer at Aviatrix and is based out of Olympia, WA.

Tom and Gaurav first created these validated designs for customers in Enterprise Data Management and Gaming industries. These designs have now been adopted by dozens of Aviatrix enterprise customers across industry verticals.

Gaurav can be reached at gaurav@aviatrix.com
Tom can be reached at tdavis@aviatrix.com