aviatrix

# Justifying a Multi-Cloud Network Strategy powered by Aviatrix

03 — Version

For Government Agencies & Integrators

# About this Document

## Justifying a Multi-Cloud Network Strategy


This document is designed to help organizations understand ways in which government agencies are moving forward with the Aviatrix multi-cloud network platform in order to deliver business or mission value, increase agility, and strengthen cyber posture in the cloud.

Considerations made by these agencies include:

*Is the solution easy to build?*

*Can it be automated with existing toolsets such as Ansible or Terraform?*

*Does the solution provide greater cloud network visibility above and beyond any existing alternatives?*

*Does the solution support multi-cloud packet capture and the ability to view network forensics?*

The design, implementation, and operational management of a multi-cloud network platform is a strategic decision for any enterprise and Aviatrix is ready to support the most demanding of mission sets.

**"And suddenly you know: It's time to start something new and trust the magic of beginnings."**

- Meister Eckhart

# ABOUT AVIATRIX

**One Architecture.**

**Your Sovereign Network.**

**Any Government Cloud.**

Aviatrix is a multi-cloud network platform built to meet the stringent requirements of the US Federal government.

Aviatrix is available in the AWS, Azure, and Google GovCloud marketplaces as well as ICMP for those serving the US Intelligence Community.

> **When the rubber meets the road, my team is accountable and it's our network.**

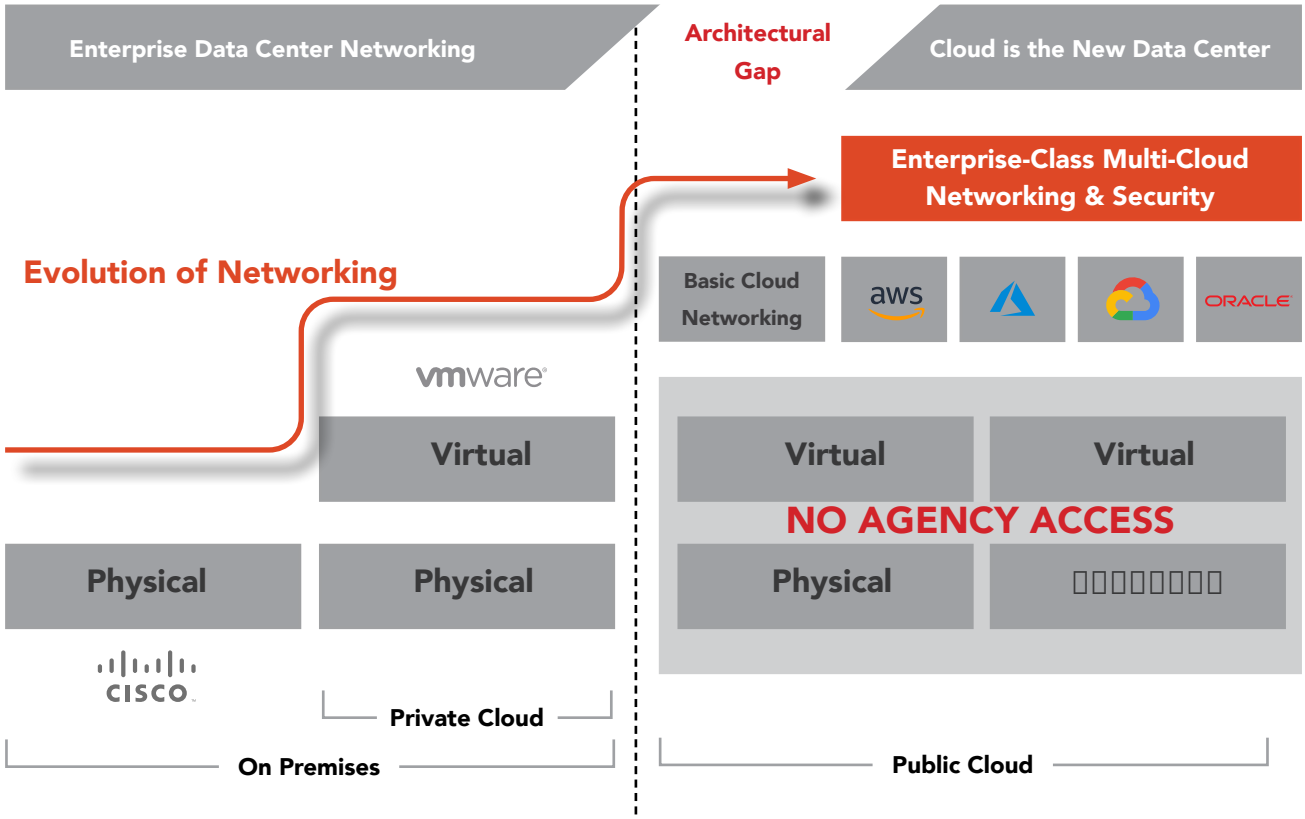
How does your agency build repeatable virtual private networks in the cloud?
How do you overcome the performance bottlenecks of encryption in the cloud?
How do you manage account and VPC sprawl?
How does your agency troubleshoot with full visibility in the cloud when an application isn't performing?

Aviatrix is simple to deploy; our intelligent central controller is launched from cloud provider marketplaces and automates the deployment of additional network and security services, as required. Most customers launch and begin using Aviatrix services in an afternoon, easy to try and evaluate.

The Aviatrix Federal team also has experts available to assist.

# Challenges of the Cloud

**NETWORKING HAS EVOLVED.**
Initially network teams managed physical assets on-prem. These assets, primarily delivered by Cisco gave rise to a wave of Cisco certified professionals. The era of server virtualization matured to eventually virtualize the network, with VMware NSX. This was a second wave of evolution which saw VMware certifications come to the forefront. However, cloud adoption has abstracted much of the networking components required to properly troubleshoot and audit a cloud infrastructure. The move to multi-cloud means skills obtained and sharpened for one cloud provider have little value in another cloud. These are the problems Aviatrix is solving for agencies today.




How do you benefit from the agility of the cloud while ensuring security best practices are followed?

How do you ensure interoperability across Government clouds for true resiliency, advantageous economics, and maximum capability?

When your team has to troubleshoot cloud performance, do they have the visibility and tools they need to properly identify the root cause?

# Table of Contents

# Introduction

For most US Government agencies and supporting Federal System Integrators a multi-cloud environment is the current or near-term reality. Typically, the first cloud an agency deploys in (e.g. AWS) becomes their primary cloud. Yet innovative services and mission requirements may require an agency to deploy in a secondary or even tertiary cloud. Personnel are often forced to learn these alternate clouds but never reach the same level of comfort as they have in an agency's primary cloud. This leads to operational gaps and operational inefficiencies. In a worst case scenario these operational gaps can contribute to cyber events which can be extremely difficult to analyze in a multi-cloud environment.

A multi-cloud network strategy helps address these challenges by utilizing a common platform, a central Terraform or network API provider, and by delivering multi-cloud network visibility for both proactive and reactive cyber scenarios.

For any agency considering a multi-cloud network strategy, the following platform considerations must be made:

**Mission-Grade.**
The platform should be able to handle the stress and emphasize performance, resilience, and intelligence within the multi-cloud premise.

**Cyber Secure.**
The multi-cloud network platform should secure cloud network communication to include encryption and egress filtering. In addition third-party virtual firewalls (e.g. Palo Alto) should be able to be deployed at scale through the multi-cloud network platform.

**Operationally Ready.**
The multi-cloud network platform should be easy and efficient to use both from a graphical user interface (GUI) perspective as well as through programmatic interaction (e.g. via Ansible, Terraform, et al.). The platform should deliver a focus on multi-cloud network visibility, and detailed flow analysis for troubleshooting purposes.

# Notional Multi-Cloud Network Architecture

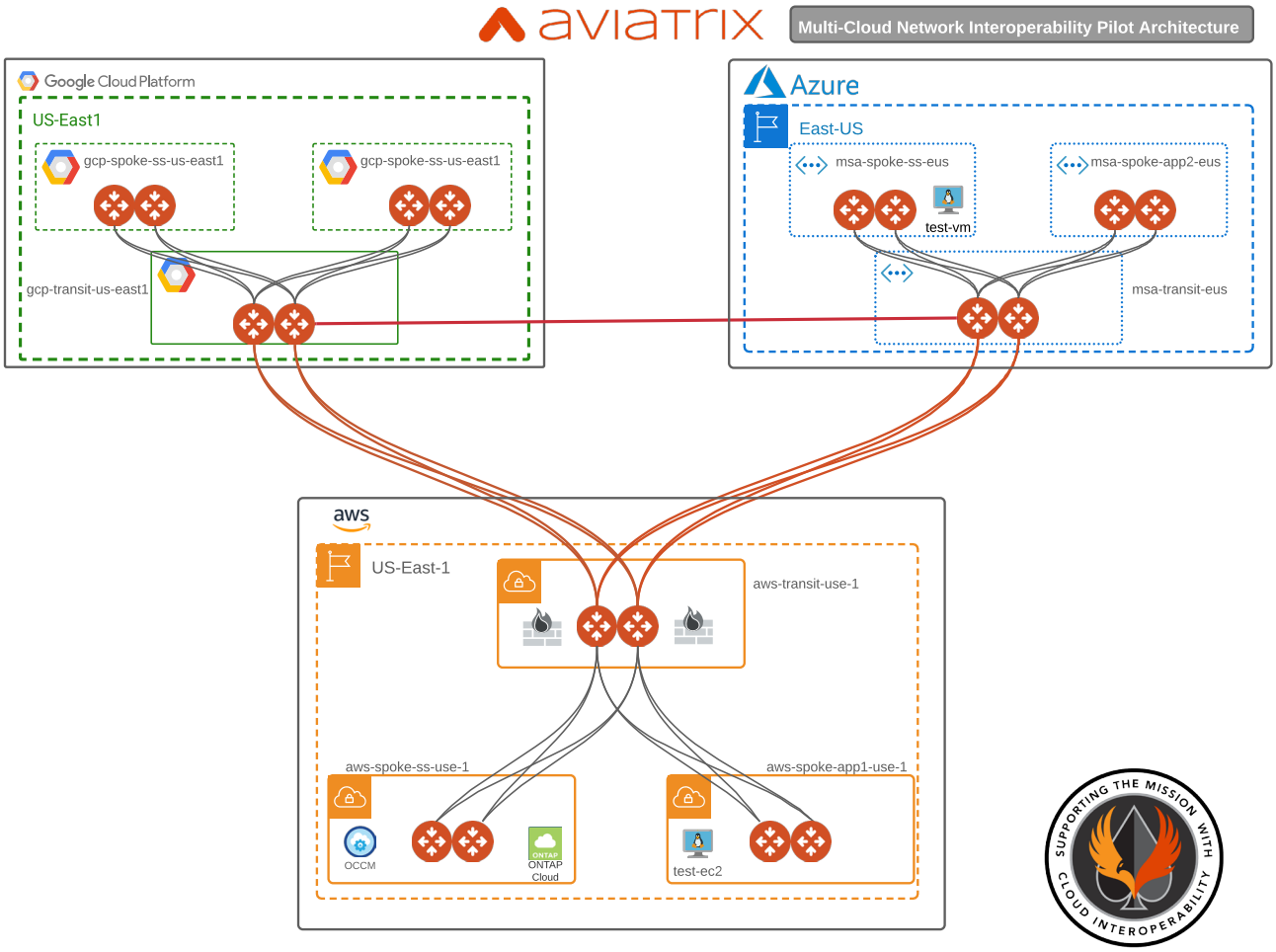



*Figure 1*

The above diagram is meant to represent a typical multi-cloud interoperabilty pilot design. It is a robust environment building secured transit with and between AWS, Azure, and GCP. Other clouds, such as OCI, could also be architected into the design.

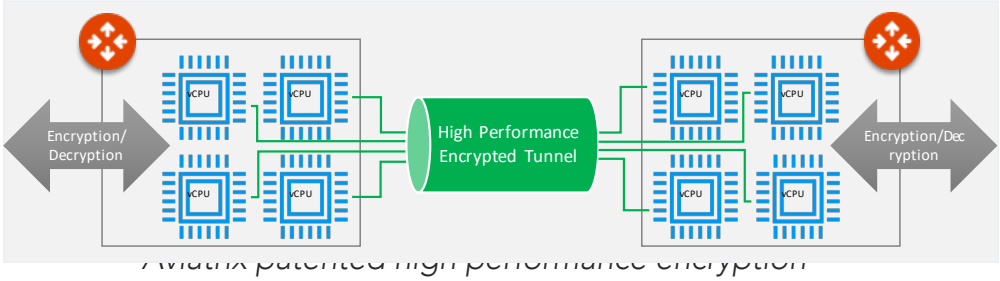
# Justification 1

High Performance Encryption
In the Cloud

# Justification 1: High Performance Encryption

**PROBLEM & SOLUTION:** A Department of Defense (DOD) agency has mandated that all cloud network traffic must be encrypted. This agency delivers a capability through an application stack of webservers and databases that supports a secured mission. Most of these resources reside within the same AWS GovCloud region, but the database team has decided that moving forward they would be deploying into Azure. The reason for this expansion into Azure is that the database team felt that Azure was better aligned to their specific requirements and existing skill set. As usage of the capability continued to increase over time, the application performance degraded massively. This impact was felt by the community of daily users of the capability through lost time and agility.

Upon analysis, the limiting factor was determined to be encryption performance of the native cloud networking tunnel, which averaged ~2Gbps. The agency was now saturating this cloud network link within a single cloud, and in some cases, within the same region.




*Aviatrix patented high performance encryption*

The solution was to implement the Aviatrix multi-cloud network platform. Aviatrix has a patented multi-core approach to encrypting network traffic in the cloud, and as such can deliver ~70Gbps of encrypted throughput between cloud networks. This is essentially *cloud line-rate*, the same speeds found in on-prem networking, but in the cloud.

**CLOUD PREMISE:** The cloud premise for this justification is described below:

Current Cloud Service Provider(s): AWS
Region(s): GovCloud-West, GovCloud-East

Future Cloud Service Provider(s) in Scope: Azure

**ALTERNATIVES:** The alternate solution considered for the encrypted connectivity performance problem was to use 3rd party transit networking with IPSEC tunnels. Also, AWS TGW with equal-cost multi-path routing (ECMP) enabled was considered. Using native AWS transit networking for this requirement equates to having to manage four (4) IPSEC tunnels with ECMP from each firewall to a device. The max throughput the firewall could process is 6Gbps. In a typical hub and spoke architecture, that would require building and managing 4 to 8 IPSEC tunnels per spoke. For a highly available (HA) environment that equates to sixteen (16) tunnels. Ten (10) VPCs equates to ***160 tunnels that need to be managed***. In this solution that would require managing the 160 tunnels all *from a command line interface* (CLI).

**KEY ISSUES / DECISION CRITERIA:** Any potential solution to be considered would need to support AWS GovCloud regions and come from a company that could pass a FOCI investigation. Ideally, the solution would also support Azure which was in the process of coming online as a cloud service provider for this agency.

**JUSTIFICATION AND REASONING:**

The justification submitted to the review board asserted that the value received from the Aviatrix platform significantly exceeded its cost. The value to the agency was a fully functional capability that could meet the demands of its users now and well into the future. In addition to solving the encryption performance and management option in one cloud (AWS), the onboarding of Azure means the agency can easily use Aviatrix to build out encrypted networks in their Azure environment as well. Additionally, this will reduce sustainment cost.

**DEPLOYMENT METHOD:** The Aviatrix environment was deployed from the GUI through our **Launch Control program** which assists agencies with their design and launch of an Aviatrix network architecture.

**NUMBER OF AVIATRIX CERTIFIED ENGINEERS (ACE):** 7

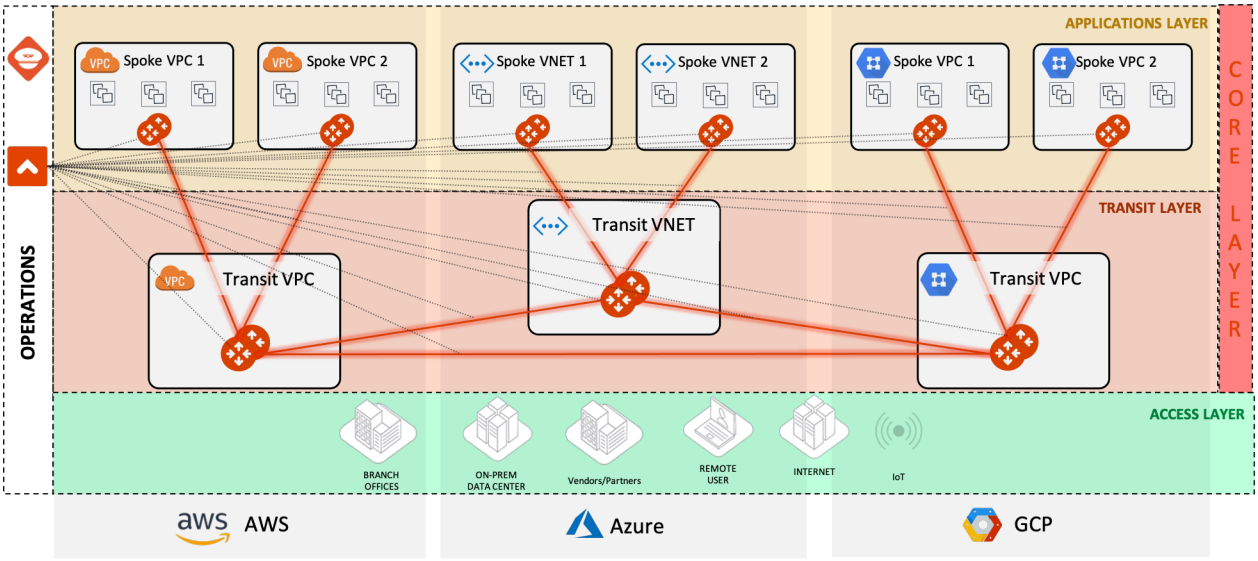
**RESULT:** The agency is now seeing up to 70Gbps of encrypted throughput within their cloud premise thanks to the Aviatrix network platform. In addition, the agency is currently testing extending this encrypted network into their premise in Azure. Management of the cloud networks for both AWS and Azure could all be managed and monitored from a single pane.

# Justification 2

Multi-Cloud Network Architecture

# Justification 2: Multi-Cloud Network Architecture

**PROBLEM & SOLUTION:** A US Government Cyber program has currently fielded a cyber capability with services available entirely through AWS. This capability resides in the higher enclaves of AWS. The program constantly monitors capabilities available in the other primary cloud service providers (Azure, GCP, OCI) and identified several services in GCP that could potentially be of value to their mission. This program did not want to spend the time to learn GCP's networking constructs as they simply wanted to rapidly prototype GCP services like Cloud AutoML and the GCP Looker Business Intelligence Platform.




*Aviatrix multi-cloud network platform*

The solution was to implement the Aviatrix multi-cloud network platform. Aviatrix allows this program to easily build, connect, monitor, and maintain Aviatrix-powered cloud networks in both AWS and GCP. Aviatrix CoPilot was also heavily utilized to understand traffic flow, usage patterns, and to perform forensics through multi-cloud packet capture.

**CLOUD PREMISE:** The cloud premise for this justification is described below:

Current Cloud Service Provider(s): AWS
Region(s): GovCloud-West, GovCloud-East, higher enclaves

Future Cloud Service Provider(s) in Scope: GCP

**ALTERNATIVES:** The alternate solutions considered for building a multi-cloud transit layer were Cisco Cloud Service Router (CSR) 1000V as well as Google Anthos multi-cloud kubernetes platform. The Cisco CSR-based solution was deemed to be too complicated to manage as it still required a lot of manual intervention to perform basic functions. The cost was also prohibitive.

Google Anthos only offered a potential solution to the kubernetes components of the solutions and did not solve connectivity, cloud network security, or cyber visibility.

**KEY ISSUES / DECISION CRITERIA:** Any potential solution to be considered would need to support AWS GovCloud regions and come from a company that could pass a FOCI assessment. The solution would also need to support GCP.

**JUSTIFICATION AND REASONING:**

The technical justification for selecting Aviatrix was that Aviatrix is the only multi-cloud network platform available and suitable for US Government agencies. In addition, a financial assessment was requested to understand the economic impact of an Aviatrix-powered multi-cloud network strategy. For a native cloud transit solution, which did not meet the technical requirements, the total cost of ownership per year was approximately 60% more expensive than the Aviatrix solution. The other alternative, a Cisco CSR based solution, was 80% more expensive than the Aviatrix solution.

**DEPLOYMENT METHOD:** The Aviatrix environment was deployed from the GUI through our **Launch Control program** which assists agencies with their design and launch of an Aviatrix network architecture. This configuration was exported to native Terraform directly from the Aviatrix GUI.

**NUMBER OF AVIATRIX CERTIFIED ENGINEERS (ACE):** 2

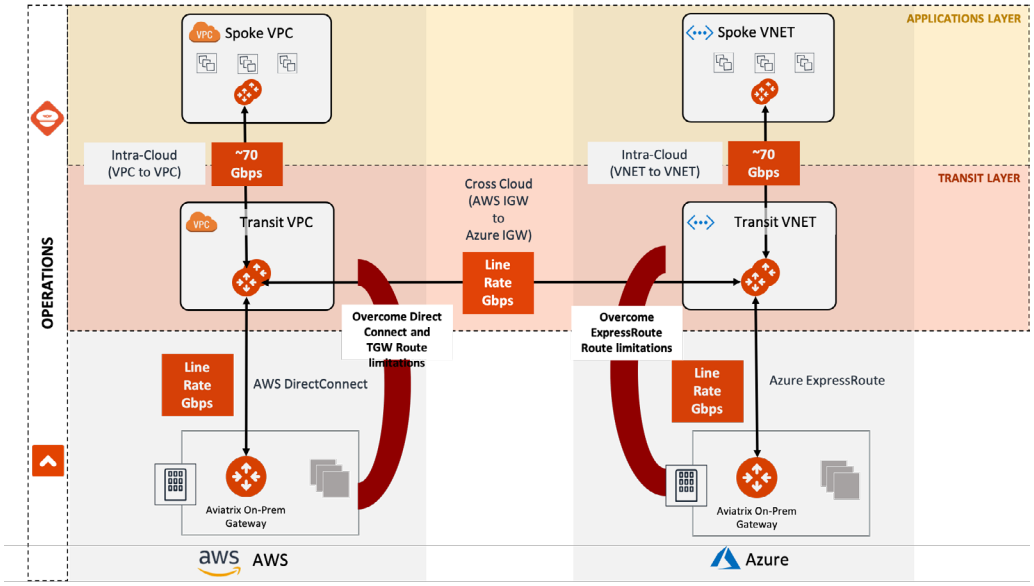
**RESULT:** This Cyber program can now easily prototype new capabilities in both GCP and AWS. In addition, they are operationally ready to onboard other CSPs such as Azure or OCI without having to learn the native networking constructs of those respective cloud environments. Aviatrix CoPilot gives this government program the ability to quickly perform troubleshooting, multi-cloud packet capture, and visualize the topology of their multi-cloud environment.

# Justification 3

High Performance Encryption of a Direct Connect or ExpressRoute

# Justification 3: High Performance Encryption of a Direct Connect

**PROBLEM & SOLUTION:** A US government program supporting the research and development of strategic capabilities in support of the DOD was saturating their AWS Direct Connect link. This program was currently exploring adding Azure ExpressRoute but was no concerned about link saturation in general. This program maintains a physical datacenter as well as a colocated cage at an Equinix facility which house several datalakes required for ongoing capability development.




The solution was to implement the Aviatrix multi-cloud network platform to include the Aviatrix high performance encryption appliances in both the on-prem datacenter and the Equinix cage. Aviatrix has a patented multi-core approach to encrypting network traffic in the cloud, and as such can deliver ~70Gbps of encrypted throughput between cloud networks. In addition, this technology can be used to encrypt a private connection, such as a Direct Connect or ExpressRoute, at line-rate speeds. These are the same speeds found in on-prem networking, but in and up to the cloud.

**CLOUD PREMISE:** The cloud premise for this justification is described below:

Cloud Service Provider(s): AWS
Region(s): GovCloud-West, GovCloud-East

Future Cloud Service Provider(s) in Scope: Azure

**ALTERNATIVES:** Several secure access service edge (SASE) solutions were considered but were disqualified due to not understanding a multi-account cloud environment or not being a fully functional cloud network solution.

**KEY ISSUES / DECISION CRITERIA:** Any potential solution to be considered would need to support AWS GovCloud regions and come from a company that could pass a FOCI assessment. The solution had to deliver a *soverign multi-cloud network platform*, owned by the agency. No hosted or managed offerings would be considered.

**JUSTIFICATION AND REASONING:**

The justification submitted to the review board asserted that Aviatrix had the only solution on the market to meet the high performance requirements from a technical perspective while adhering to the key issues and decision criteria required for this agency.

**DEPLOYMENT METHOD:** The Aviatrix environment was deployed completely through Terraform in conjunction with the Aviatrix **Launch Control program,** which assists agencies with their design and launch of an Aviatrix network architecture.

**NUMBER OF AVIATRIX CERTIFIED ENGINEERS (ACE):** 1

**RESULT:** The agency is now seeing up to 80Gbps of encrypted throughput from their on-prem points of presence up to their cloud premise. In addition, this program is well situated to embrace a pending Azure rollout as the Aviatrix platform delivers freedom of choice.

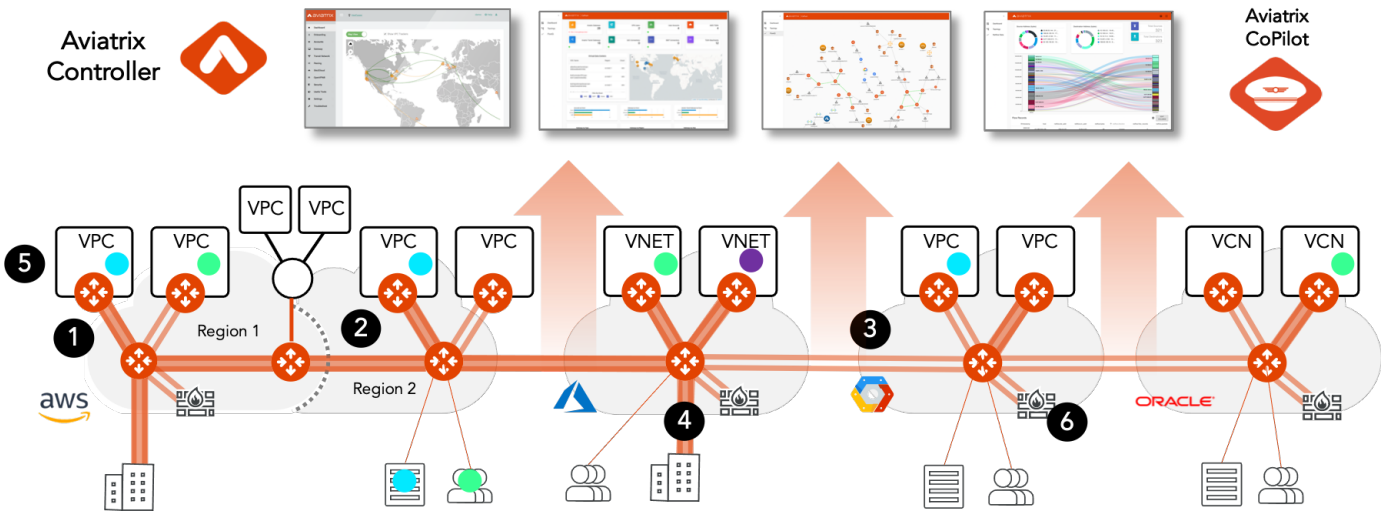
# Justification 4

Cloud Network Security
Through Service Insertion
& Microsegmentation

# Justification 4: Cloud Network Security Through Service Insertion

**PROBLEM & SOLUTION:** A large Federal System Integrator (FSI) was looking for a better way to manage its firewall footprint in AWS and Azure, offload routing services from the firewalls to a more purpose-built solution, and have a deeper understanding of traffic flow within their multi-region AWS and Azure footprints. This FSI was also looking for a microsegmentation solution in the cloud. The FSI wanted granular control over access to ensure that even when teams needed to collaborate, they could do so in a secured fashion.

The solution was to implement the Aviatrix multi-cloud network platform. Aviatrix leverages the combination of its intelligent orchestration and control as well as gateway services to remove AWS and Azure networking complexities such as lack of route propagation to VPCs, IPSec tunnels, and BGP; or use of source address translation (SNAT) between the firewall and the TGW. Eliminating these constraints allows Palo Alto VM-Series firewalls to operate at optimal performance and at TGW-native throughput. Removing the need to use SNAT allows session stickiness and source address to be retained for full visibility. The firewall network service is often deployed in multiple availability zones for active redundancy and scale-out load balancing. With Aviatrix, Palo Alto Networks VM-Series can achieve optimal performance, scale, and visibility.



**CLOUD PREMISE:** The cloud premise for this justification is described below:

Cloud Service Provider(s): AWS, Azure
Region(s): Multiple commercial and GovCloud regions

Future Cloud Service Provider(s) in Scope: None in scope

**ALTERNATIVES:** The alternate solutions considered were Cisco CSR 1000V, Palo Alto Panorama, and native AWS and Azure networking constructs. None of these solutions delivered the throughput, multi-cloud capability, or operational efficiency required.

**KEY ISSUES / DECISION CRITERIA:** Any potential solution to be considered would need to support AWS and Azure GovCloud regions and come from a company that could pass a FOCI assessment.

**JUSTIFICATION AND REASONING:**

The justification submitted to the review board asserted that the value received from the Aviatrix platform significantly exceeded its cost. The value to the agency was a fully functional capability that could meet the demands of its users now and well into the future. In addition to solving the encryption performance and management option in one cloud (AWS), the onboarding of Azure means the agency can easily use Aviatrix to build out those encrypted networks as well. This will reduce sustainment costs as well.

**DEPLOYMENT METHOD:** The Aviatrix environment was deployed from the GUI through our **Launch Control program** which assists agencies with their design and launch of an Aviatrix network architecture.

**NUMBER OF AVIATRIX CERTIFIED ENGINEERS (ACE):** 11

**RESULT:** This Federal System Integrator can now efficiently manage their complex network routing in the cloud while also delivering cloud network segmentation to easily understand the level of access per a given entity.

# Justification 5

Replacement of Cisco CSR 1000V

# Justification 5: Replacement of Cisco CSR 1000V

**PROBLEM & SOLUTION:** A US Federal agency was looking to modernize the way they manage routing and network connectivity in their public cloud environments. The agency used Cisco CSR 1000Vs as their cloud transit during their initial move to the public cloud for two reasons. The first reason was the in-house familiarity with Cisco products. The second was an existing Cisco enterprise license agreement that made it easy to acquire Cisco CSR 1000V licenses.

However, the underlying instance requirements, the lack of centralized management, the fact that most of the platform needed to be managed from a command line interface, and the overall slow performance left much to be desired.

The solution was to migrate to the Aviatrix multi-cloud network platform. 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. This agency also required the propagation of hundreds (nearing 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.

**CLOUD PREMISE:** The cloud premise for this justification is described below:

Cloud Service Provider(s): AWS, Azure

Region(s): US-East, US-West, GovCloud-West, GovCloud-East

**ALTERNATIVES:** The alternative was to stay with a Cisco CSR 1000V based architecture.

**KEY ISSUES / DECISION CRITERIA:** Any potential solution to be considered would need to support AWS GovCloud regions and come from a company that could pass a FOCI assessment. The solution would also require a centralized management console, support for 3rd party firewalls, and dynamic route management.

**JUSTIFICATION AND REASONING:**

The justification submitted to the review board asserted that the value received from the Aviatrix platform significantly exceeded its cost. The value to the agency was a fully functional capability that could meet the demands of its users now and well into the future. In addition to solving the management overhead and performance limitations of a Cisco CSR 1000V environment, Aviatrix also delivered deep flow analysis into the cloud networks for both troubleshooting and incident response.

**DEPLOYMENT METHOD:** The Aviatrix environment was deployed from the GUI through our Launch Control program which assists agencies with their design and launch of an Aviatrix network architecture.

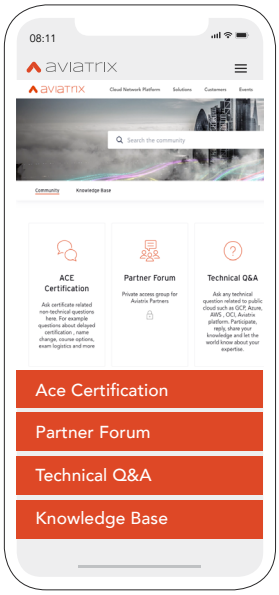
**NUMBER OF AVIATRIX CERTIFIED ENGINEERS (ACE):** 5

**RESULT:** The deployment of Aviatrix has allowed the cloud and network teams to spend less time managing the cloud network infrastructure and more time on the design of a strategic Kubernetes initiative to speed up the development and deployment of mission-supporting applications.

# Additional
## Resources

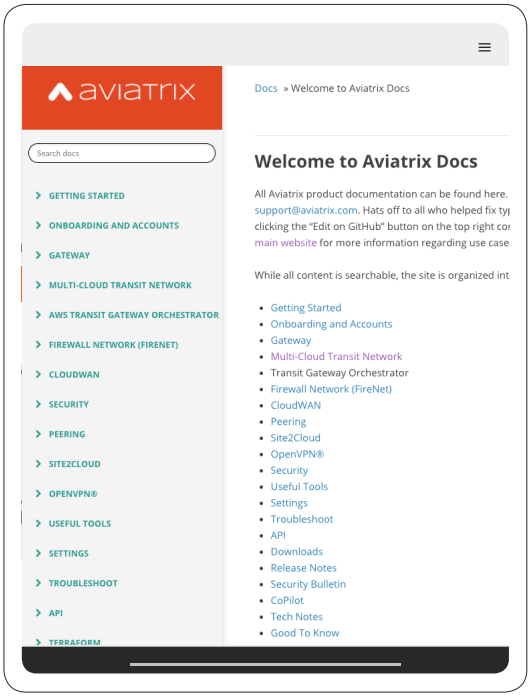
### community.aviatrix.com

Ask any technical question related to public cloud such as GCP, Azure, AWS , OCI, Aviatrix platform. Participate, reply, share your knowledge and let the world know about your expertise.




### docs.aviatrix.com

All Aviatrix product documentation can be found here. If you cannot find what you need, email us at support@aviatrix.com. Hats off to all who helped fix typos and mistakes. You can do that too by clicking the “Edit on GitHub” button on the top right corner of any document.



# Here to Help

## Deployment Assistance

Aviatrix appreciates the time and consideration it takes to formulate a multi-cloud strategy. Our team can share best practices we've seen from other deployments as well as lessons learned along the way.

Aviatrix Federal offers the following to this next step:

- **Multi-Cloud Network Design Session**
  No-cost design session with a Federal solution architect. Schedule via jason@aviatrix.com
- **Assisted Launch**
  No-cost whiteglove assistance from a Federal solution architect to assist with pre-launch preparations and launch of the Aviatrix platform in a production environment
- **Operational Readiness Workshop**
  No-cost 2 hour workshop to educate, prepare , and train O&M teams to accept and manage a production Aviatrix deployment.
- **Mission Acceleration Manager**
  A fully or partially dedicated technical resource that works directly with your organization as you design, deploy, and manage your Aviatrix


# Aviatrix Federal

Contact:
Jason Langone, Federal SALES CONUS & OCONUS
+1 202 630 3363
jason@aviatrix.com

Aviatrix
2901 Tasman Dr #109
Santa Clara, CA 95054

aviatrix.com