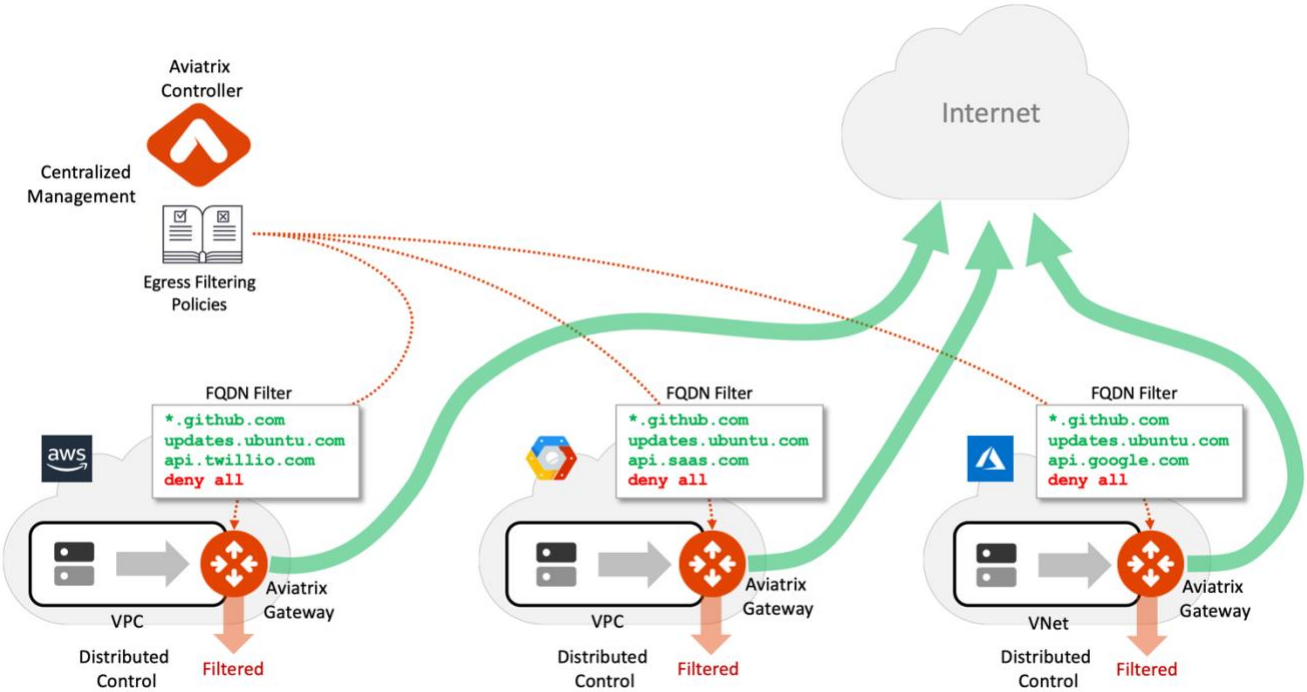
Aviatrix Policy-Based Egress FQDN Filtering Solution

Overview

Aviatrix Egress FQDN Filtering is a multi-cloud service specifically designed to deliver centralized control over Internet-bound traffic from VPCs or VNets using Fully Qualified Domain Name (FQDN) filtering. The solution satisfies organizational and regulatory compliance initiatives for restricting outbound traffic to the Internet, such as PCI, HIPAA and SOC2, while eliminating the complexity of manually creating filtering rules at an instance level using constantly changing IP address lists. Powered by the Aviatrix cloud network platform, the solution delivers enterprise-class visibility, centralized control, and multi-cloud optionality not available from native cloud services or open source proxy software.

Cloud applications with unrestricted access to the Internet-based services expose your environment to attack. Best practices limit applications communicate 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 your applications are communicating with and gives you the control to filter those communication by Fully Qualified Domain Names (FQDN).



Aviatrix Egress FQDN Filtering provides visibility and control for traffic leaving VPCs or VNets. Aviatrix Gateways provide this filtering capability by filtering egress traffic by Fully Qualified Domain Names (FQDN), "Allowing" or "Blocking" lists of domain names to control the egress traffic based on policies. Filtering supports HTTP, HTTPS or other non-HTTP applications such as SFTP/SSH.

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 counter parts 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.

Design Requirements

- Filtering Control – Native cloud constructs such as Internet or NAT Gateways filter on IP address, but not on FQDN's. This creates a gap in visibility for cloud operations and security teams. Provide FQDN context in centralized security policies for your VPC/VNET egress traffic across regions and clouds.
- Domain Name Discovery – Log internet sites (domains, URLs) apps in VPCs or VNets visit to help create filtering policies.
- White Listing – Create FQDN "Allow" lists to reduce an attacker's ability to exfiltrate data and limits the ability for malicious traffic to communicate with your cloud applications and resources.
- Security Policies – Centrally manageable white listed domains that enable policies to be applied easily to any VPC or VNet through deployment workflows or Terraform automation.
- Compliance – Ensure egress filtering meets corporate or regulatory compliance, such as PCI, HIPAA and SOC2.
- High Performance at Low Cost – Optimize costs by enabling distributed FQDN filtering to operate on low cost cloud compute platforms (e.g. EC2 T2-micro instances).
- Automation – Support for Terraform Infrastructure as Code automation and integration with CI/CD pipeline.

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.

Aviatrix Gateways

Aviatrix gateways deliver advanced cloud networking and security services. For this validated design Aviatrix Gateways are deployed to provide the distributed filtering services, based on policies (FQDN White lists or IP addresses) to limit VPC or VNet egress traffic to known domain names or domain paths with wild card support. Aviatrix gateway replaces native NAT gateways and provide high throughput with limited compute requirements. Aviatrix Gateways are primarily deployed to deliver transit network and security services such as intelligent dynamic routing, active-active network high-availability, end-to-end and high-performance encryption and collect operational visibility data. Egress FQDN gateways can also operate as spoke gateways to deliver these services but may require higher-performance underlying cloud compute capacity.

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.

Filtering Control

Native cloud constructs such as Internet or NAT gateways filter on IP address, but not on FQDN's. This creates a gap in visibility for cloud operations and security teams. Aviatrix provides the FQDN context in centralized security policies for VPC/VNET egress traffic across regions and clouds. FQDN filtering rules can utilize wildcard. The rules not only support HTTP/HTTPS but also additional protocols such as SFTP, FTP, ICMP etc. Traffic can be filtered by IP/port/protocol.

Discovery Mode and Security Policies

Discover what internet sites apps visit before creating filtering policies. This gives egress traffic visibility without disrupting the existing policies and control. The results can be exported and analyzed to create fine grained FQDN based rules. Centrally managed groups of white listed domains allow policies to be applied easily in deployment workflows. FQDN "Allow" lists, reduces an attacker's ability to exfiltrate data and limits the ability for malicious traffic to communicate with cloud services.

Compliance

Many cloud workloads are subject to corporate or regulatory compliance, such as PCI. Aviatrix FQDN filtering based egress security is an easy and quick to deploy solution to achieve compliance and audit requirements. The solution could also be integrated with 3rd party audit and logging systems such as Splunk, Sumologic, Datadog and any other system that supports syslog and/or netflow.

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 designing for secure egress solution, organizations should consider availability, manageability, performance and cost to make sure proposed design meet the business and technical requirements.

High-Availability

This validated design recommends the Egress FQDN Filtering solution be deployed with at least two Aviatrix gateways, each in different AZ to provide high availability. Gateways are deployed in Active/Active mode. In case of an outage, the Aviatrix Controller will automatically rebalance the load to the available gateway. Therefore, it is recommended that the sizing for those gateways is done in such a way that a single gateway can handle the entire egress traffic load, in case of gateway outage. For added availability more than two gateways can be deployed in Active/Active mode.

Manageability

Simple manageability is an important factor when designing for the Egress FQDN Filtering egress solution. The Aviatrix cloud network platform allows several options including UI, API and Terraform. The egress traffic is controlled using a policy-based approach. Egress FQDN policies are abstracted and can be applied to a single or groups of gateways. FQDN tag and CIDR based granular rules can be programmed to allow or block internet-bound traffic. Using the policy-based approach, either a "Block all but allow a few FQDNs" (aka Zero Trust) approach or an "Allow all but block a few FQDNs" approach can be

implemented quickly and easily. Aviatrix also provides a discovery mechanism that allows organizations to log the sites their apps visit before creating the filtering policies.

Performance

Instance/VM size plays an important role in achieving desired performance goals. Instances/VMs provide performance limits published by the Cloud Service Providers (CSP). It is important to determine the egress throughput required upfront before implementing the solution.

Cost Optimization

The Aviatrix Egress FQDN Filtering solution eliminates the need to implement expensive 3rd party solutions just to provide the Internet egress filtering for compliance. The Aviatrix solution, unlike others that only offer Active/Standby, allows all Egress FQDN Filtering gateways to be deployed in Active/Active mode. This Active/Active approach makes sure that organizations are not paying for additional license and standby compute costs that are not being used. Aviatrix allows organization to deploy the smallest size gateways (e.g. EC2 t2.micro) to design the egress FQDN filtering solution. Further cost optimization can be achieved through a centralized egress filtering design pattern, which allows organizations to deploy Aviatrix gateways in a central VPC/VNET.

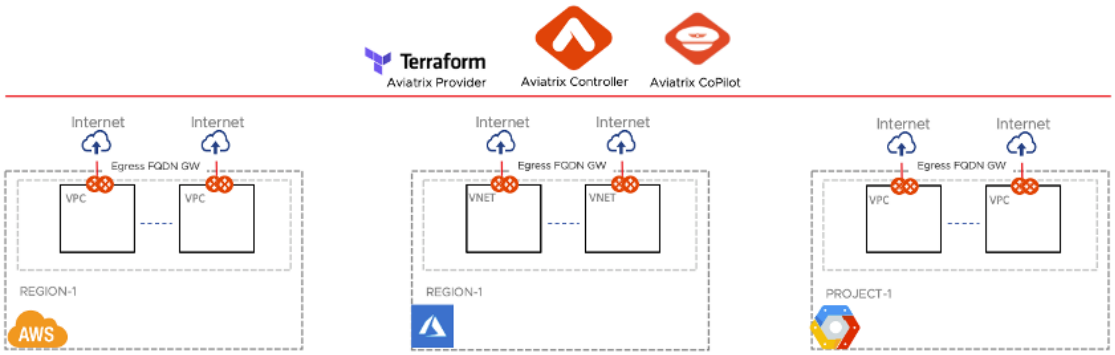
Design Options

The Aviatrix Egress FQDN Filtering solution is extremely flexible and can be deployed number of different ways based on 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.

There are number of different deployment models and design patterns. This document focuses on four major designs that are widely deployed by the Aviatrix customers. In all the designs presented here, Aviatrix gateways provide NAT for the egress traffic and FQDN filtering for VPC or VNet egress to the Internet.

Design One: Local Egress FQDN Filtering without Aviatrix Transit

In this design the Aviatrix Egress FQDN Filtering gateways are deployed in each application VPC and/or VNET where the egress filtering is required.



Local Egress FQDN Filtering without Aviatrix transit design is deployed by organizations that are providing services to tenants residing in those application VPC/VNETs. Usually those tenants are completely isolated from a traffic flow perspective and have unique filtering requirements.

In this design, Aviatrix gateway deployment is automated by the Aviatrix controller, which takes care of necessary route updates in VPC/VNET and manages the lifecycle of entire interaction.

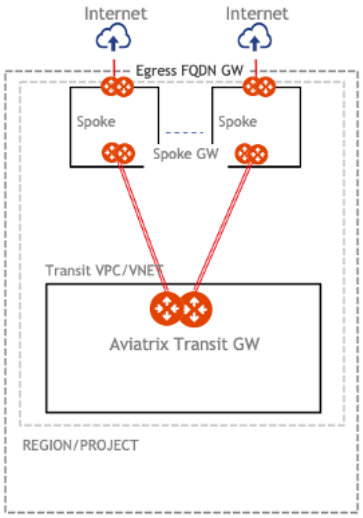
This design is highly available. Aviatrix recommends provisioning at least two gateways per VPC/VNET, each in separate availability zones for service high availability and redundancy. The Aviatrix Egress FQDN Filtering gateways are deployed in Active/Active mode to deliver great optimized throughput performance.

All management is done from the centralized Aviatrix controller. The FQDN rule creation and application is policy based. Organizations can easily make it part of their automation or CI/CD pipeline leveraging the Aviatrix Terraform Provider or API capabilities.

The cost of the Egress FQDN Filtering gateway can be charged-backed or shown-backed to the respective tenants.

Design Two: Local Egress FQDN Filtering with Aviatrix Transit

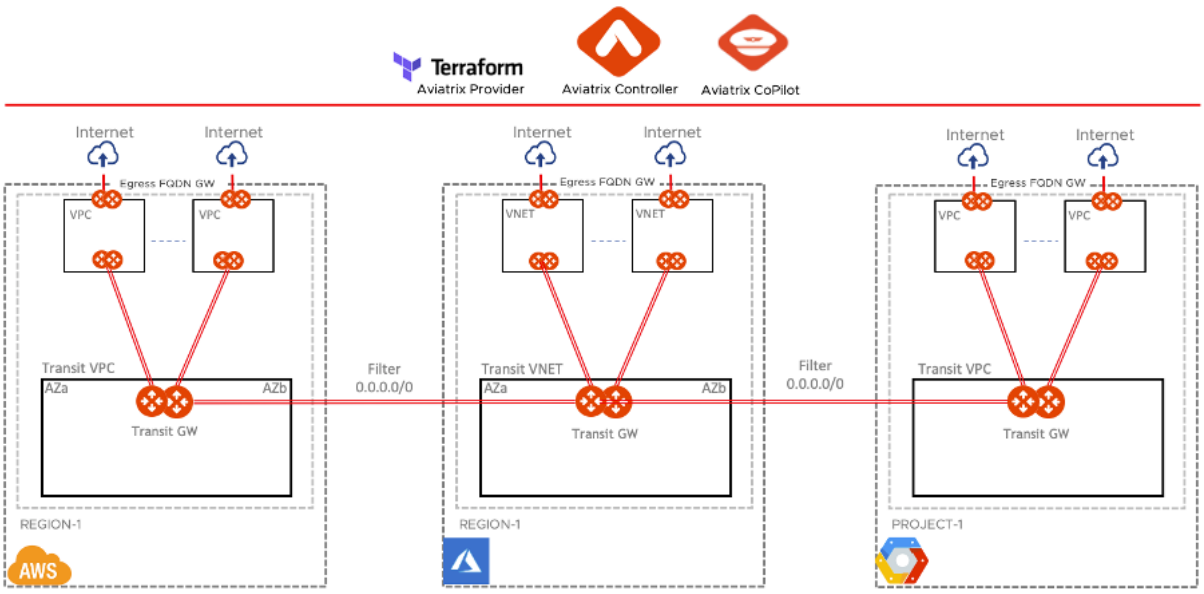
In this design the Aviatrix Egress FQDN Filtering gateways are deployed in each application or spoke VPC/VNET where the egress filtering is required. These applications or spoke VPCs/VNETs are also connected to Aviatrix Transit gateways deployed in Transit VPCs/VNETs.



This model is the recommended model for most organizations as it allows application VPCs/VNETs to connect to an Aviatrix Transit VPC/VNET in the same or other regions. The Aviatrix Transit provides a common architecture within and across clouds. This allows greater deployment and growth flexibility and optionality.

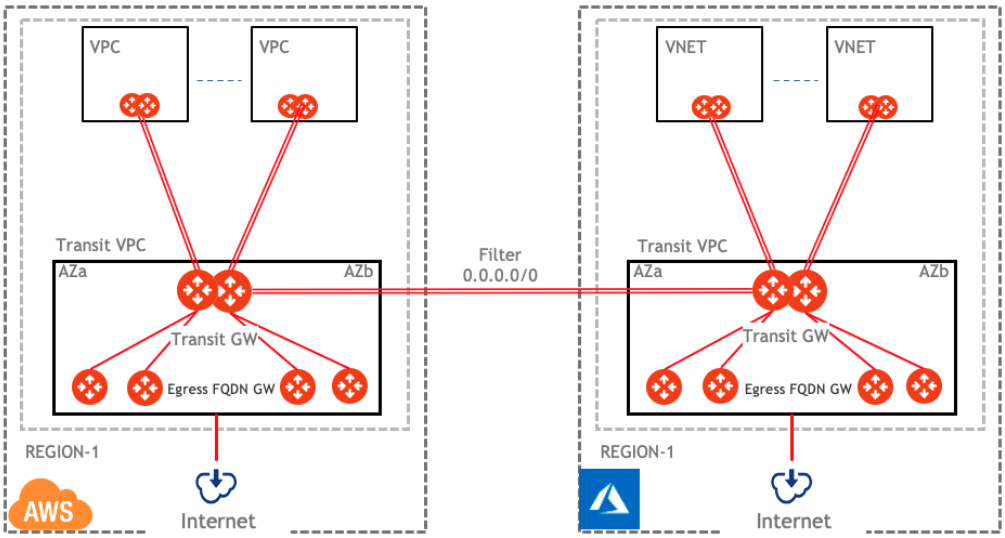
This design also forms the basic building block for adding additional features such as Aviatrix FireNet, multi-cloud network segmentation, multi- cloud transit and advanced network and security connectivity with traffic engineering to on-premise, just to name few.

The diagram below shows how easy and seamless it is to connect additional clouds with the same operational model and capabilities without reinventing or re-architecting the entire design.



Design Three: Centralized Egress FQDN Filtering with Aviatrix Transit

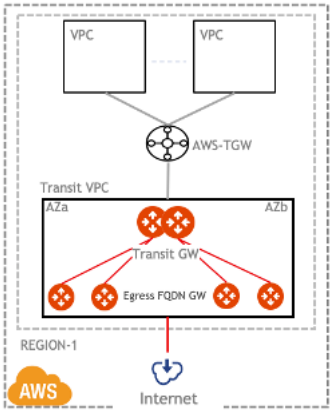
In this design the Aviatrix Egress FQDN Filtering gateways are deployed in a central VPC or VNET. This centralized VPC/VNET is called the Transit VPC/VNET. This design provides both scale-up and scale-out depending on throughput requirements. Organizations can increase instance sizes or increase the number of Egress FQDN Filtering gateways directly from the controller.



Design Four: Centralized Egress FQDN Filtering with AWS Transit Gateway

This design pattern is mainly applicable to following type of businesses:

1. Organizations that are already using AWS Transit Gateway and due to internal policies or strategy are not willing or able to migrate to Aviatrix Transit-based design
2. Organizations that will only be in AWS cloud. Note that 100% of Aviatrix customers who have believed this, were multi-cloud within 6 months.



The biggest drawback is that this design pattern cannot be repeated across multiple clouds. It is dependent on the native AWS Transit Gateway service.

The Aviatrix controller provides centralized deployment, management and control for AWS Transit Gateway and connected VPCs. All necessary routes and security policies in the application VPC, AWS Transit Gateway, and Egress FQDN Filtering Gateways are automatically programmed, managed and controlled by Aviatrix Controller.

Customers opting for this design should be aware about following:

- The VPC attachments to AWS Transit Gateway are in the clear (not encrypted).
- There are limited monitoring and troubleshooting options provided by AWS for AWS Transit Gateway. Customers looking for advance monitoring and troubleshooting should consider the “Centralized Egress with Aviatrix Transit” design to leverage Aviatrix enterprise -class visibility.
- The Aviatrix Transit Gateway is a multi-purpose service node that can perform various functions. In this design the Aviatrix Transit Gateways are providing high-availability and load balancing for the Aviatrix Egress FQDN Filtering Gateways
- High availability for AWS Transit Gateway is provided by AWS
- This design provides both scale-up and scale-out depending on throughput requirements. Organizations can increase instance sizes or increase the number of Egress FQDN Filtering gateways directly from the controller.

Engage with Aviatrix

Online Documentation: docs.aviatrix.com

More Egress FQDN Filtering Resources

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

Join the Aviatrix Community

About the Author

Shahzad Ali is a Principal Solutions Architect at Aviatrix based in Santa Clara. Shahzad created these validated designs for several different customers in the Financial Services, Healthcare, Technology and Manufacturing industries. These designs have been validated and adopted by dozens of Aviatrix enterprise customers.

Shahzad can be reached at shahzad@aviatrix.com