Aviatrix Multi-Cloud Secure Egress with FQDN Filtering – Control Your Cloud Egress Traffic

Secure egress filtering is a powerful service enabled by the Aviatrix AVX Multi-Cloud Networking Platform. AVX Service nodes provide Enterprise IT with visibility and centralized control over internet bound traffic, restricting communication to Fully Qualified Domain Names (FQDN).

KEY HIGHLIGHTS

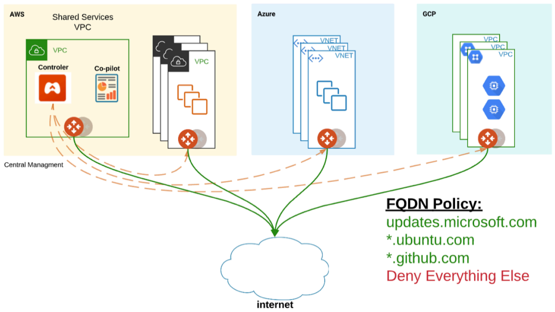
Aviatrix Secure Egress with FQDN Filtering delivers following benefits:

- 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 your VPC/VNET egress traffic across regions and clouds.
- Visibility and Discovery – Discover what internet sites your apps visit before you create your filtering policies.
- Reduced Security Risk – FQDN "Allow" lists, reduces an attacker's ability to exfiltrate data and limits the ability for malicious traffic to communicate with your cloud services
- Security Policies – Centrally managed groups of white listed domains allow policies to be applied easily in deployment workflows
- Compliance – Many cloud workloads are subject to corporate or regulatory compliance, such as PCI. Aviatrix FQDN filtering is an easy to deploy solution to achieve compliance requirements.
- High Performance at Low Cost – AVX service nodes replace native NAT gateways and provide high-throughput with limited compute requirements
- Automation – Deployment and updates easily fit into existing CICD pipelines with Terraform, the Aviatrix Rest API

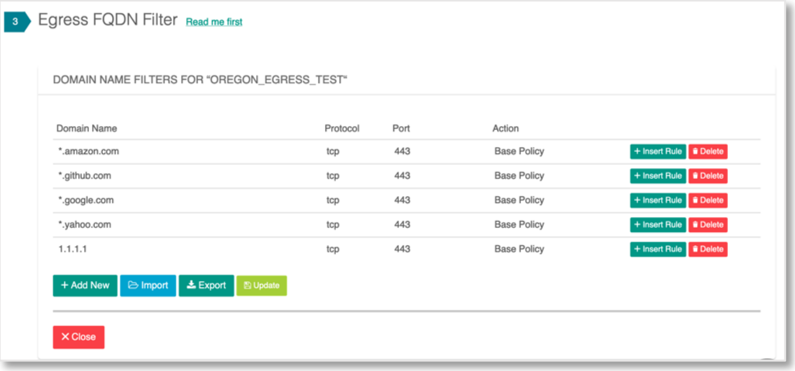
Visibility and operational control over internet bound traffic is an important element of an enterprise multi-cloud architecture. Cloud applications with unrestricted access to the Internet-based services expose your environment to attack. Best practices limit application and database tier network communications 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 your applications are communicating with and gives you the control to filter those communication by Fully Qualified Domain Names (FQDN).

HOW IT WORKS?

Aviatrix Multi-Cloud Egress Security solution provides visibility and control for traffic leaving a VPC or VNET. AVX service nodes do this by understanding egress traffic Fully Qualified Domain Names (FQDN), then "Allowing" or "Blocking" lists of domain names to control the traffic, including support for HTTP, HTTPS or other non-HTTP applications such as SFTP/SSH.



Groups of domain names are created as policies such as “dev” and “prod” and applied to AVX service nodes operating in VPCs or VNETs.



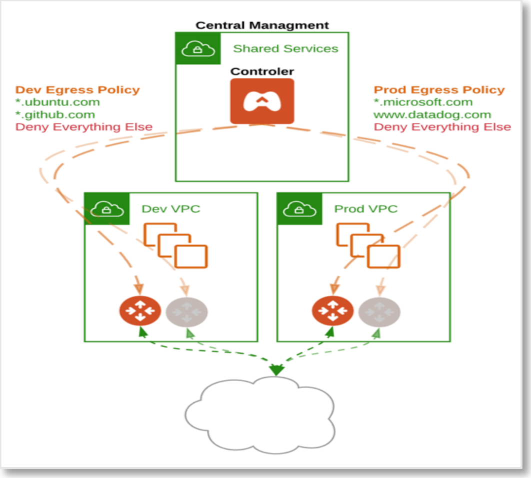
3 Egress FQDN Filter Read me first

DOMAIN NAME FILTERS FOR “OREGON_EGRESS_TEST“

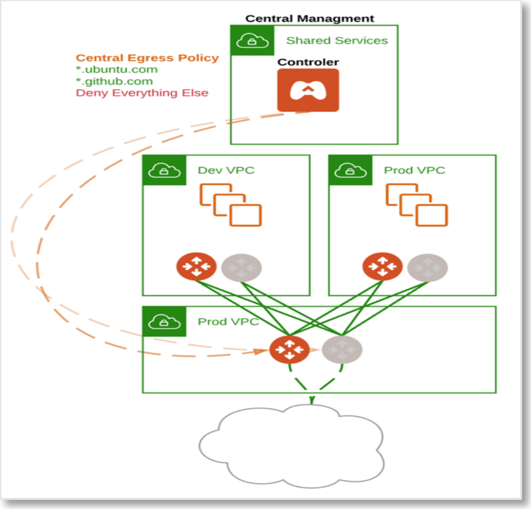
Domain Name	Protocol	Port	Action	
*.amazon.com	tcp	443	Base Policy	+ Insert Rule Delete
*.github.com	tcp	443	Base Policy	+ Insert Rule Delete
*.google.com	tcp	443	Base Policy	+ Insert Rule Delete
*.yahoo.com	tcp	443	Base Policy	+ Insert Rule Delete
1.1.1.1	tcp	443	Base Policy	+ Insert Rule Delete

USE CASE SCENARIOS

VPC/VNET Egress: Secure Egress with FQDN is deployed in each VPC/VNET to provide direct internet connectivity visibility and control.



Centralized Egress: All VPC/VNET internet bound traffic is aggregated into a centralized egress VPC/VNET to provide internet connectivity visibility and control.



AVX service nodes are deployed using the AVX Multi-Cloud Networking Platform through step-by-step workflows or automated leveraging Terraform scripts. Some key deployment benefits include:

- ActiveMesh (Active/Active) mode with an AVX service node in each Availability Zone. This provides high availability for both the AVX service node and cloud infrastructure.
- The AVX service node is also a Stateful Firewall, providing the ability to leverage traditional address/port/protocol-based filtering policy for your egress security.
- Combined with AWS Ingress Routing service, AVX services nodes can ingest AWS Guard Duty malicious IP lists and use them in a dynamic ingress security policy.

SUMMARY

Aviatrix Egress Security solution provides enterprise IT cloud networking and security architects with egress FQDN filtering for VPCs/VNETs with centralized policy management through the AVX Controller and Console. The service blocks all outbound internet traffic except specific whitelisted domain names (FQDN). This cost-effective solution, priced at a fraction of other popular solutions, directs outbound traffic through the AVX service node, to deliver visibility and control not offered by native cloud services.

Technical Benefits

- Highly Available; Fault Tolerant
- Filters traffic by FQDN
- FQDN filtering using wildcards
- Supports HTTP/HTTPS protocols
- Supports additional protocols (SFTP, FTP, ICMP, etc.)
- Filters traffic by IP address/port/protocol
- Centralized management console
- Integrated audit logging (view in AVX or export logs to Splunk, Sumologic, Datadog, and other tools)

For more details, check out docs.aviatrix.com or connect with our technical solution engineer through aviatrix.com online chat.