AVIATRIX EGRESS FQDN FILTERING

Control outbound traffic to the Internet using fully qualified domain names

HIGHLIGHTS

Aviatrix Egress FQDN Filtering is delivers several benefits including:

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.

Reduce Security Risks

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, HIPAA and SOC2. Aviatrix FQDN filtering is an easy to deploy solution to achieve compliance requirements.

High Performance at Low Cost

Aviatrix Gateways replace native NAT gateways and provide high throughput with low cost compute requirements.

Automation

Leverage Aviatrix's Multi-Cloud Terraform Provider to simplify Infrastructure as Code automation and integration with CI/CD pipeline

GAIN CENTRALIZED CONTROL OVER YOUR CLOUD EGRESS

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.

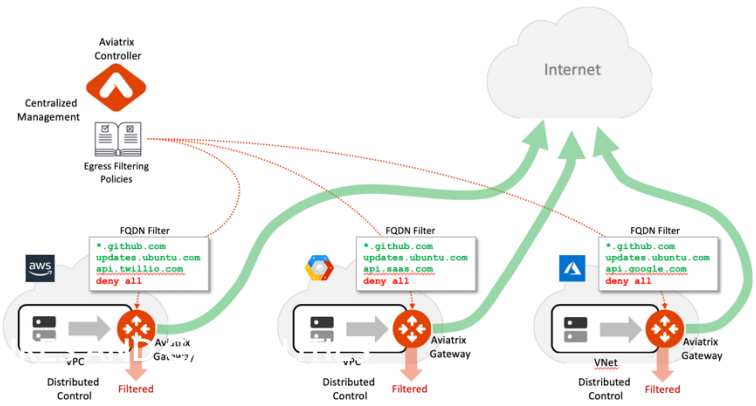
Powered by the Aviatrix cloud network platform, the solution delivers enterprise-class visibility, centralized control, and multi-cloud optionality not available from native cloud services or open source proxy software.

SIMPLE. EASY TO DEPLOY. ENTERPRISE-CLASS.

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 Egress FQDN Filtering provides visibility and control for traffic leaving a 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 traffic control egress traffic based on policies. Filtering supports HTTP, HTTPS or other non-HTTP applications such as SFTP/SSH.



Aviatrix Gateways are deployed using the Aviatrix cloud network platform leveraging simple, step-by-step workflows or automated Terraform scripts. Some key deployment benefits include:

- Aviatrix ActiveMesh (Active/Active) mode with an Aviatrix Gateway in each Availability Zone. This provides high availability for both the Aviatrix Gateway and cloud infrastructure.
- The Aviatrix Gateway 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, Aviatrix Gateways can ingest AWS Guard Duty malicious IP lists and leverage them in a dynamic ingress security policy.

HOW AVIATRIX COMPARES TO OTHER ALTERNATIVES

Functions	Aviatrix Egress FQDN Filtering	AWS NAT Gateway	Azure Firewall	Squid
HTTP and HTTPS FQDN filter (*supports wildcard)	Yes *	No	Yes	Yes
Non-HTTP/HTTPS FQDN filter	Yes	No	No	No
Multi-AZ High Availability (*load balanced)	Yes	Yes	Yes	No
Centrally Managed	Yes	Yes	Yes	No
Egress Traffic Discovery	Yes	No	No	No
API support	Yes	Yes	Yes	No
Terraform support	Yes	Yes	No	No
Integrated Audit Logging	Yes	No	Yes	No
Allow private network to be filtered	Yes	No	No	No
Filter Traffic by IP Address *must update security group of each instance (maximum 50 IPs)	Yes	Partial*	Yes	Yes
Filter Traffic by FQDN (*currently available in preview)	Yes	No	Yes*	Yes
FQDN filtering Using Wildcards	Yes	No	Yes	Yes
Allow specified source CIDR to bypass a rule	Yes	No	No	No
Allow specified source CIDR to apply to rule	Yes	No	No	No
Visibility on allowed/Denied sessions	Yes	No	No	No
Search a specified rule match history	Yes	No	No	No
Vendor product support	Yes	Yes	Yes	No
Supports Additional Protocols (sftp, *ftp, icmp, etc.)	Yes	No	Yes	Partial*

Try Aviatrix Today or Schedule a Technical Review Session

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. We have experts available to help you.

Contact your Aviatrix account executive or email info@aviatrix.com to schedule an architectural overview or design session with one of our solution architects. Learn about Aviatrix Certified Engineer (ACE) training or for more information go to aviatrix.com.