Documentation

Implementing Egress in an Aviatrix-Managed Network

The Aviatrix Distributed Cloud Firewall (DCF) Egress solution offers a comprehensive approach to securing egress traffic to the internet in cloud environments. This solution is designed to enhance visibility, enforce centralized policies, and optimize traffic for performance and cost efficiency. It addresses the growing complexity of managing security across multi-cloud environments by operating within individual VPCs or VNets. By inspecting and enforcing security rules directly in the cloud network where the traffic originates, this approach ensures that all traffic is inspected before it leaves the cloud network, providing real-time visibility and policy enforcement at the spoke level.

Distributed Cloud Firewall (DCF) is the recommended method for configuring egress. If you want to implement egress this way, you must first enable SNAT on the egress Spoke gateways and create DCF policies that use WebGroups.

NOTE

Access to Egress Security Score features require Controller 8.0 and for the DCF feature to be enabled.

If these are both present:

- The Security > Egress > Overview tab displays, where you can view a summary of your protected VPC/VNets; the Egress Security Score for those protected VPC/VNets; and view how the Egress Security Score is calculated.
- You can monitor and protect VPC/VNets from the Security > Egress > Egress VPC/VNets tab.

Applying Local Egress to Spoke Gateways

Local egress ensures that all outbound traffic is inspected and enforced directly within the cloud network where it originates. This provides real-time visibility and policy enforcement at the spoke level, preventing unauthorized access and defending against threats aimed at outgoing traffic.

When you enable local egress, SNAT is automatically enabled. This translates all outbound traffic originating from the Spoke VPC/VNet to use the gateway's public IP address. Also, the default route on the VPC/VNet changes to point to the Spoke gateway.

NOTE

- Use at least t3.medium for an AWS VPC if applying local egress.
- Use at least Standard_B2ms for an Azure VNet if applying local egress.

Prerequisites

- Ensure additional CPU resources are created on the Spoke gateway to support Local Egress.
- Deploy a Spoke gateway in the VPC/VNet where you want to apply Local Egress. This is done from the Security > Egress > Egress VPC/VNets tab.

Monitoring Egress Traffic

NOTE

Controller 8.0 is required to monitor VPC/VNets.

Before attempting to monitor your egress traffic:

- Ensure that your IAM policies are up to date (for AWS)
- Ensure that ports 50441-50443 on CoPilot are open to the Aviatrix Controller
- If you have a GCP cloud account, ensure that these APIs are enabled:
  - Container: `container.googleapis.com`
  - Cloud Resource Manager: `cloudresourcemanager.googleapis.com`

When you monitor your VPC/VNets from the Egress VPC/VNets tab, in addition to local egress being applied, your egress traffic is logged.

After monitoring your VPC/VNets for a certain time period, you may decide that one or more of them require protection.

Protecting Egress Traffic

NOTE

Controller 8.0 is required to protect VPC/VNets using the egress protection workflow.

You can protect your egress traffic using the egress protection workflow or manually with DCF policies.

The charts on the Egress > Overview tab show you how well your VPC/VNets are protected (Egress Security Score), as well as which of your VPC/VNets are in which state (Unprotected, Monitored, Partially Protected, Protected, No Egress, Unknown).

Egress Protection Workflow

The protection workflow on the Security > Egress > Egress VPC/VNets tab automatically creates the necessary rules and groups to protect your traffic, based on the egress traffic flows that you trust.

Prerequisites

- Local Egress must be enabled on the VPC/VNet.
- The VPC/VNet must be in Monitor state for a period of time.

Manual DCF Policy Creation

You can manually create Distributed Cloud Firewall policies for your egress traffic. You can use the following groups to assist in protecting your traffic:

- SmartGroups: Logical groups of resources based on tags or attributes.
- WebGroups: Groups of trusted domains or URLs.
- ExternalGroups: Groups synchronized from external identity providers (such as GitHub or Azure Services).

You must create your groups before you can create DCF rules. These groups can be used to define the source and destination of your egress traffic.

To create Distributed Cloud Firewall rules manually, navigate to Security > Distributed Cloud Firewall and define policies that align with your security requirements.

Applying Egress to Transit Gateways (Legacy)

NOTE

You should only apply egress to your Transit gateways if you are already using the Egress Control feature in the Aviatrix Controller.

Regardless of if you originally configured egress rules in Aviatrix Controller, or use DCF with WebGroups, you can view statistics on the Analyze tab, and view when rule conditions were met for a VPC/VNet on the FQDN Monitor (Legacy) tab.

You may want to apply egress to your Transit gateways so that they can act as centralized egress points, where outbound traffic from Spoke gateways is inspected and managed before it leaves the cloud network. This set-up allows for consistent policy enforcement and visibility across multiple VPC/VNets.

This gathers data from attached Spoke gateways and sends it to the internet.

Prerequisites

- Ensure that Transit gateways have Transit Egress Capability enabled.
- For GCP, ensure that you have three VPCs available: one for the Transit gateway (that has Transit Egress Capability enabled); one for the Egress instance; and one for LAN. The Egress gateway VPC must have a route to the Internet.

Related Topics

- Overview of Egress Security Score Protection
- Managing Egress Security for VPC/VNets
- Enabling Local Egress
- Monitoring Egress Traffic
- Protecting Egress Traffic with the Egress Protection Workflow
- Configuring Distributed Cloud Firewall
- Enabling Transit Egress
