Security

ACE Solutions Architecture Team

Agenda

Aviatrix Security Features Overview

Securing Aviatrix Platform

Secure Egress

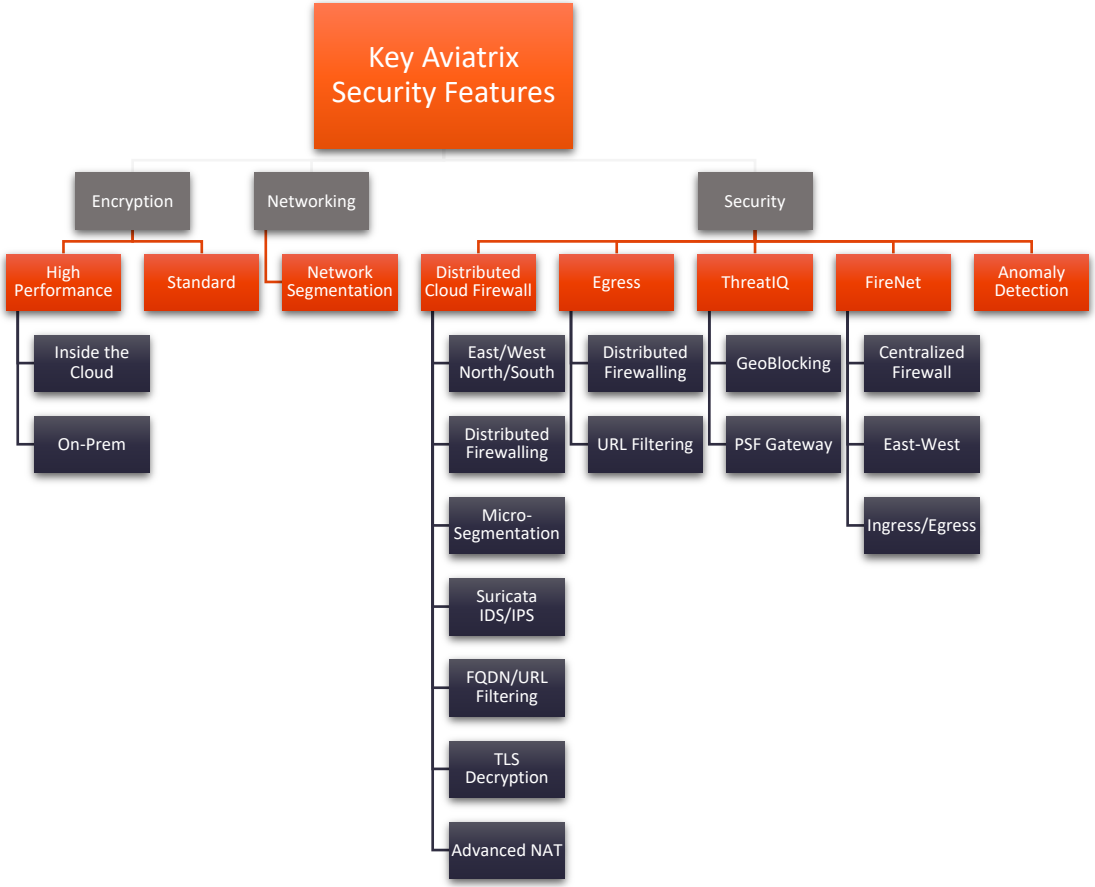
Public Subnet Filtering Gateway

Challenges for CISO, CIO/CTO and NetSec Architects

- Apps/Business requirements dictate the Multi-Cloud
  - Some Apps simply operate better in one cloud vs another
  - New Customer Requirements a particular cloud OR M&A
- **Security and Compliance is NOT shared responsibility**
  - It is YOUR responsibility
- SaaS or Managed Services are often a Black-Boxes
- Understaffed Team, Skill Gap and Learning Curve issue
- Time-to-Market causes short-cuts
- Hacked or Not, doesn't matter Audit will happen regardless

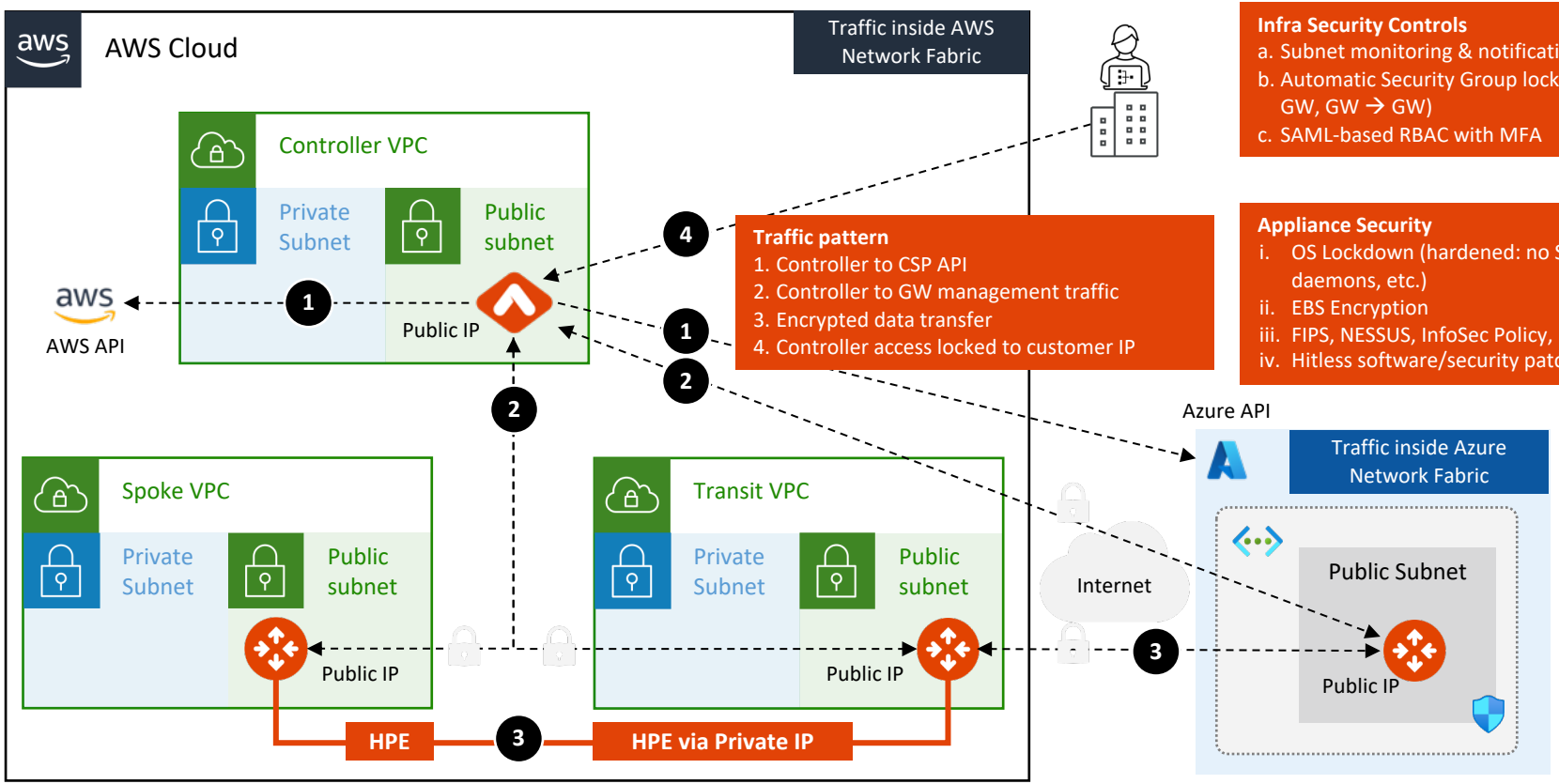
https://aviatrix.com/resources/ebooks/security-architects-guide-multi-cloud-networking-v2

Summary


Key Aviatrix Security Features
Encryption
Networking
Security
High Performance
Standard
Network Segmentation
Distributed Cloud Firewall
Egress
ThreatIQ
FireNet
Anomaly Detection
Inside the Cloud
On-Prem
East/West North/South
Distributed Firewalling
Micro-Segmentation
Suricata IDS/IPS
FQDN/URL Filtering
TLS Decryption
Advanced NAT
Distributed Firewalling
URL Filtering
GeoBlocking
PSF Gateway
Centralized Firewall
East-West
Ingress/Egress

Built-in Security of the Aviatrix Platform

Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



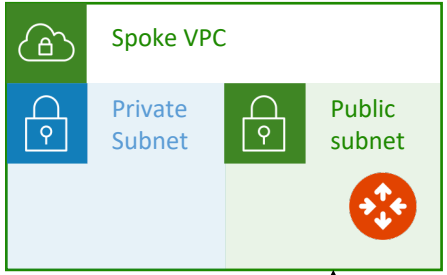
Traffic pattern
1. Controller to CSP API
2. Controller to GW management traffic
3. Encrypted data transfer
4. Controller access locked to customer IP

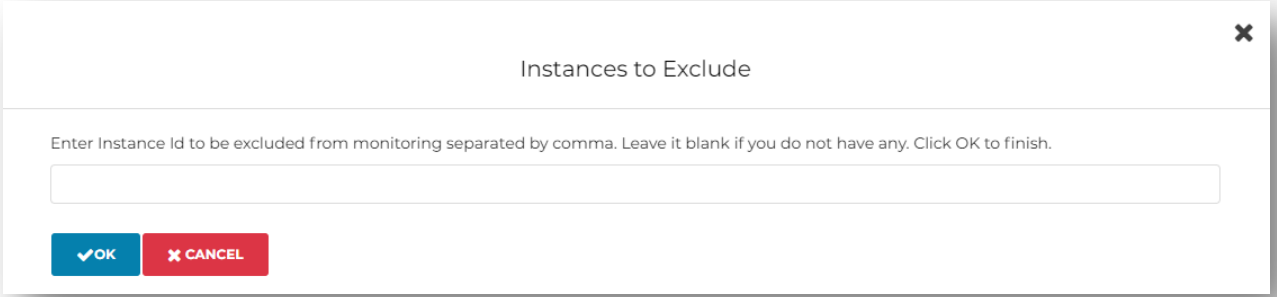
Infra Security Controls
a. Subnet monitoring & notification
b. Automatic Security Group lockdown (Controller → GW, GW → GW)
c. SAML-based RBAC with MFA

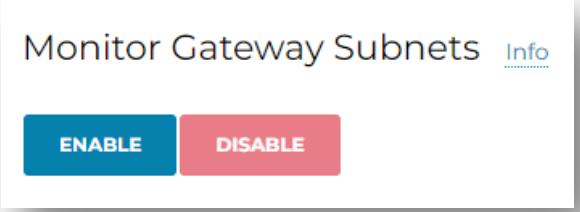
Appliance Security
i. OS Lockdown (hardened: no SSH, limited daemons, etc.)
ii. EBS Encryption
iii. FIPS, NESSUS, InfoSec Policy, Pen Testing
iv. Hitless software/security patching

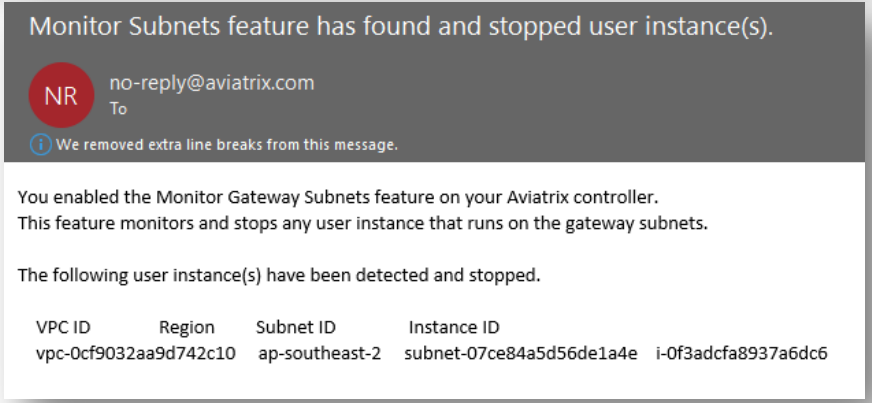
Monitor Gateway Subnets

Prevents unauthorized VMs from being launched in the same subnet as the gateways









https://read.docs.aviatrix.com/HowTos/gateway.html - monitor-gateway-subnet

Controller Security Group Management | Automatic Security Group lockdown

Details | Security

Security groups

- sg-054a744afb30dcb01 (ss-controller-AviatrixSG-YHFSUVZBB9Q9)
- sg-08a351c5c83665c38 (Aviatrix-SG-54.206.174.209-2)
- sg-0cb4cc125e9c69ed8 (Aviatrix-SG-54.206.174.209)
- sg-0ea9afb4e373b3264 (Aviatrix-SG-54.206.174.209-1)
- sg-05186521ae82c605d (Aviatrix-SG-54.206.174.209-3)

Instance: i-0ea8d13e979fb9be6 (ss-controller)

▼ Inbound rules

Filter rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-01ffba9d6c84d825d	443	TCP	3.106.76.93/32	ss-controller-AviatrixSG-YHFSUVZBB...
sgr-0a11c67bf190b7be7	443	TCP	3.105.63.97/32	Aviatrix-SG-54.206.174.209
sgr-0a8ccee5ee8d489ee	443	TCP	3.104.18.207/32	Aviatrix-SG-54.206.174.209

Instance: i-042eb8b6912e0acc0 (aviatrix-spoke1)

Security groups

- sg-09ef033544630561b (spoke1)

▼ Inbound rules

Filter rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0288b5beddfa495b2	All	All	10.1.1.0/24	spoke1
sgr-03e3c293b614e73c7	443	TCP	54.206.174.209/32	spoke1

Securing the Platform with Cloud Native Load Balancers

Problem Statement

- Enterprise concerns around putting Aviatrix Controller with a public IP in a Public subnet
- Enterprises need tighter security and availability
- What are the options?

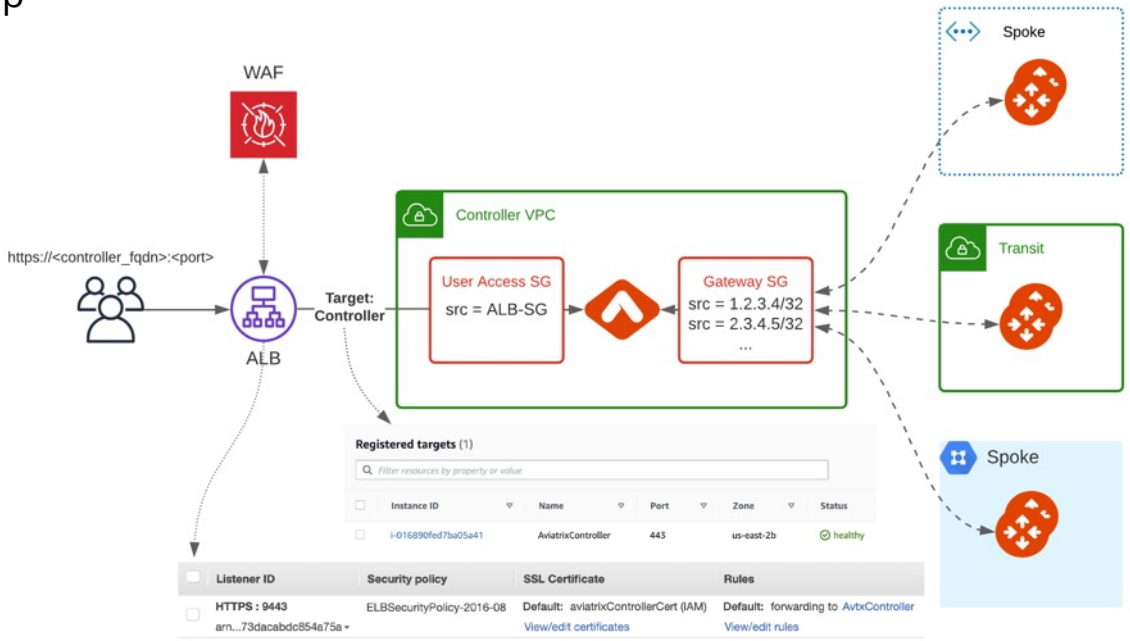
  1. Limit access using cloud native L4 stateful firewalls such as:
     - AWS Security Groups
     - Azure Network Security Groups
     - GCP Firewall Rules
  2. Deploy a third-party Firewall in front of controller
  3. Deploy an Application (L7) Load Balancer in front of Aviatrix Controller

Advantages: L7 Load Balancer in Front of Aviatrix Controller

- **Limit management access to Controller**
  - Only allow access from the LB internal IPs to Controller on port 443
- **WAF capability on LBs**
  - Stops usual web hacks/attacks against controller
- **L7 LB managing Controller certificate**
  - Potentially terminating the SSL connection on LB [cloud native process]
- **Adhere to SoPs and best practices**
  - Around alerts, operational features, logging integration, etc.
  - Putting an LB in front means Controller access can fit right into your existing operational model
- **Leverage LB health checks**
  - Monitor the Controller at an application layer
  - If the LB health check goes down, it again fits right into existing operational best practices and SoPs of customer making it easier for them to monitor the control plane
- Any access to controller, including API, UI login, etc., would go through LB, and the LB logging can provide easier, faster integration to existing tools

AWS

- Verify that the Controller Security Group Management feature is NOT disabled. This feature allows access to the Controller EIP from Aviatrix Gateways, solely
- Create a new internet facing ALB
- Modify main Controller Security Group to only allow access from the ALB Security Group
- Enable WAF on the ALB with AWS Managed Rules
- Adjust ALB idle timeout, modify rulesets
- Modify ALB Security Group to only allow access from the admin user IP



Secure Egress

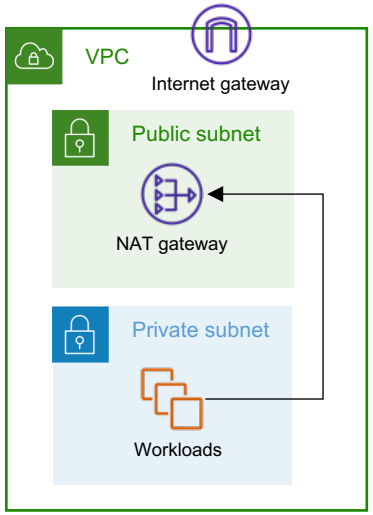
Problem Statement

Private workloads need internet access

- **SaaS integration**
- **Patching**
- **Updates**

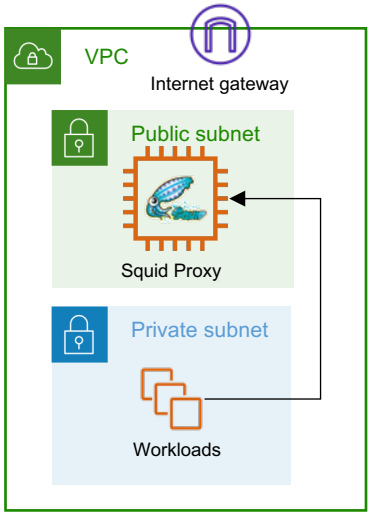
NAT Gateway

- NACLs management
- Layer-4 only



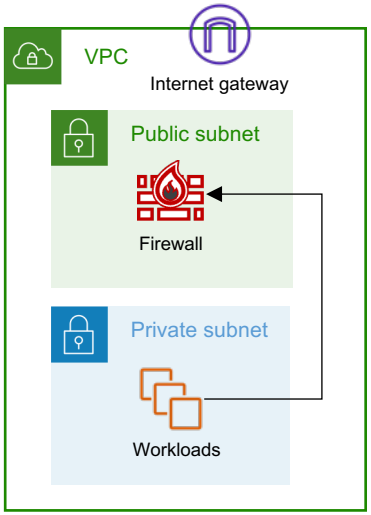
Squid Proxy

- Hard to manage
- Scale and HA issues

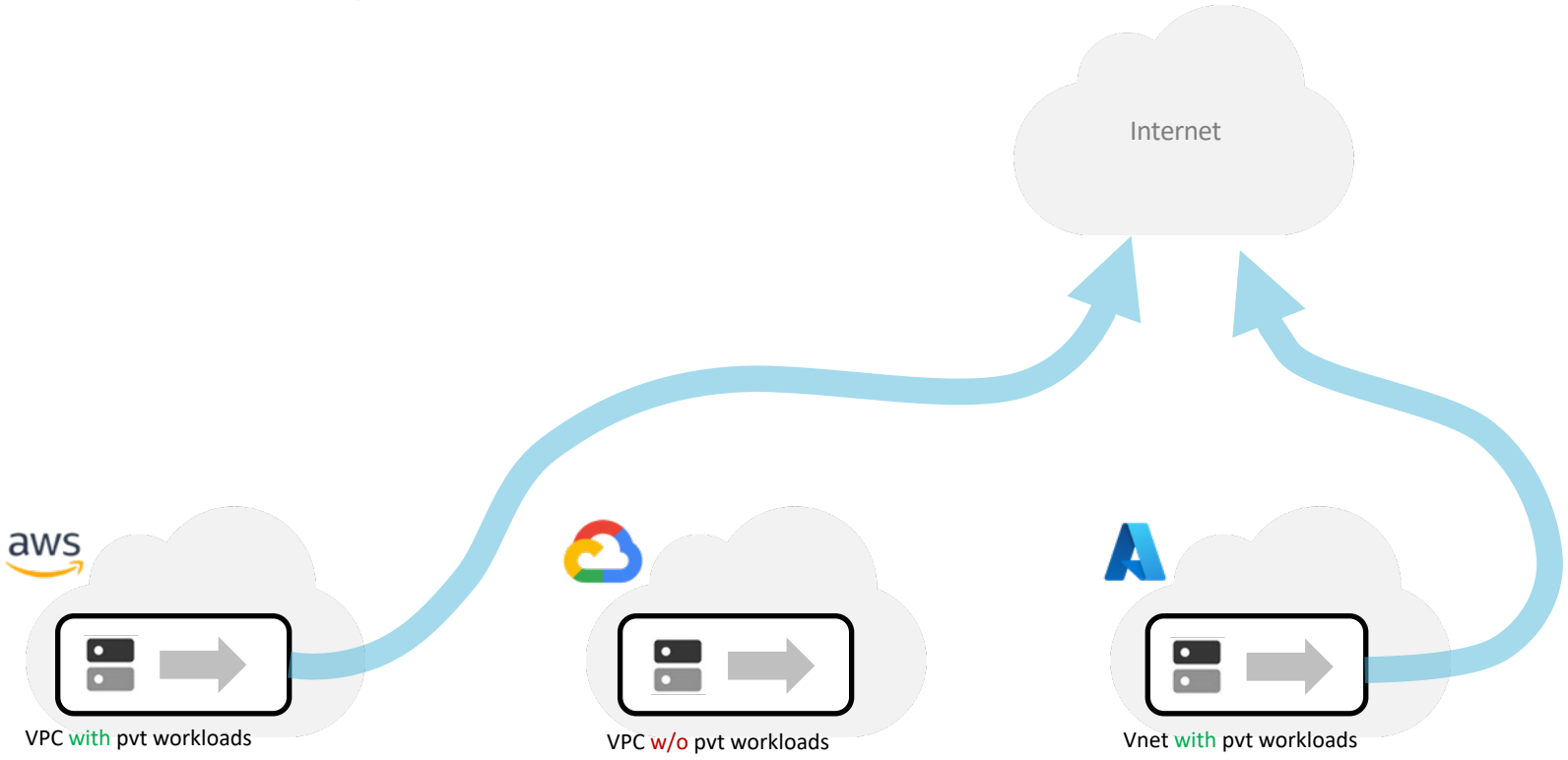


Layer-7 Firewall

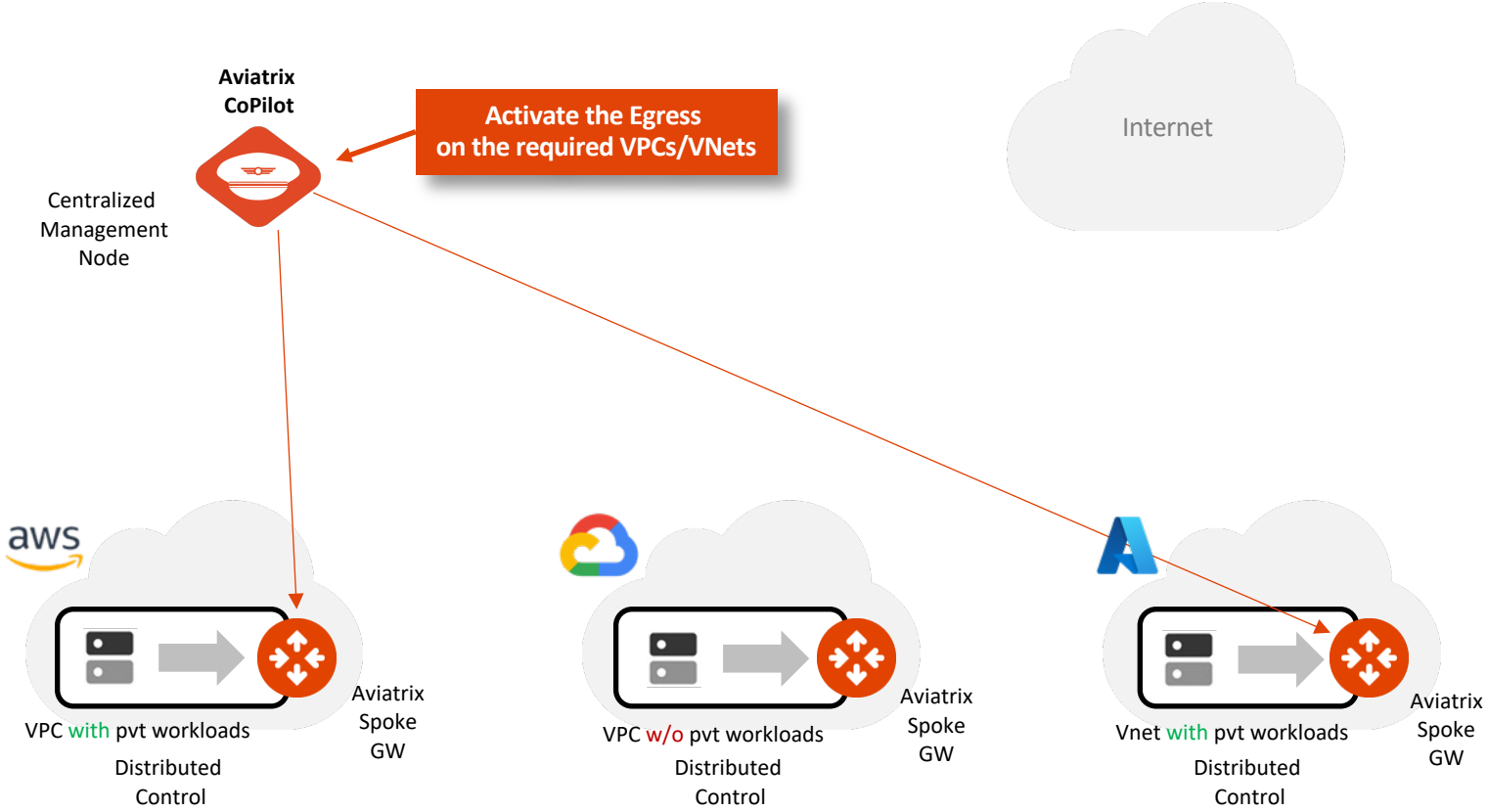
- Overkill
- Expensive



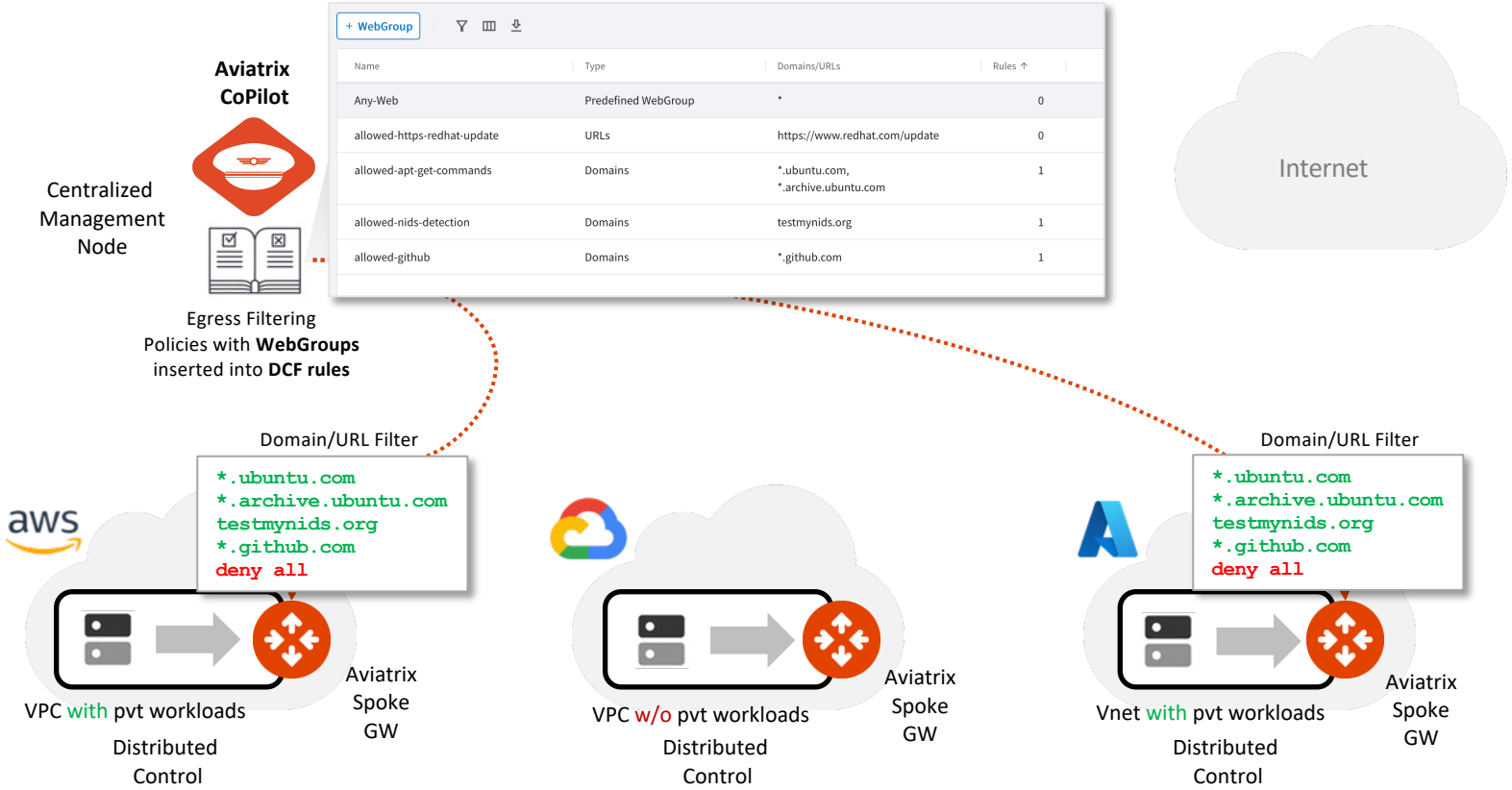
Aviatrix Secure Egress



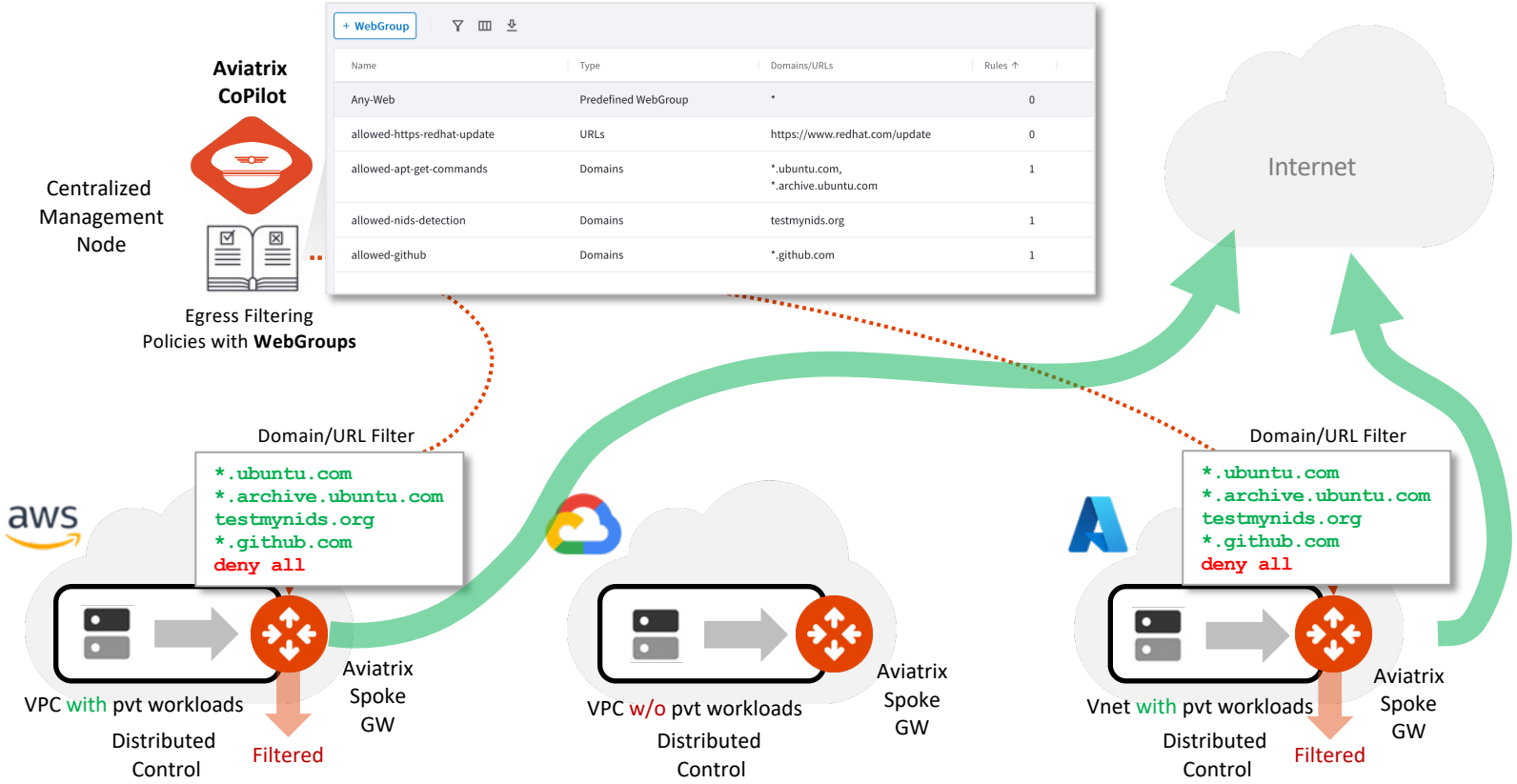
Aviatrix Secure Egress



Aviatrix Secure Egress

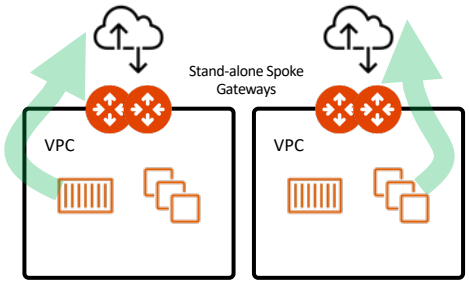


Aviatrix Secure Egress

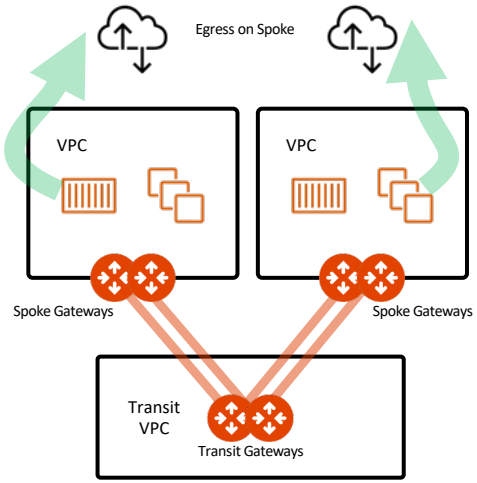


Aviatrix Secure Egress Design Patterns

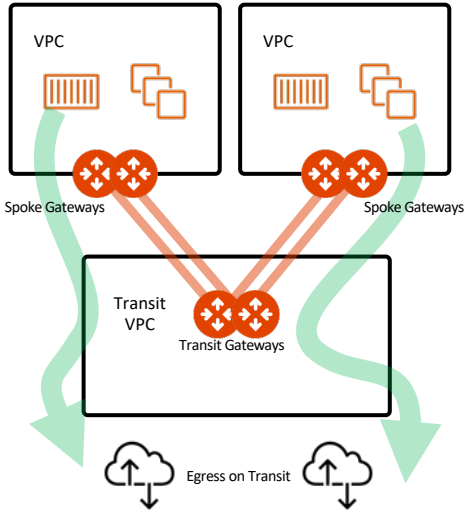
Unattached Spoke GW (Distributed)



Local Egress (Distributed) with Aviatrix Spoke GW

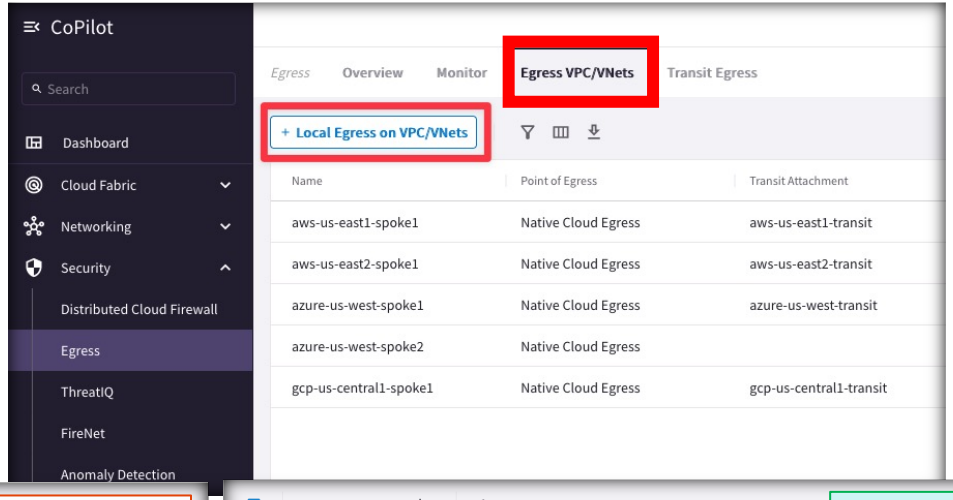


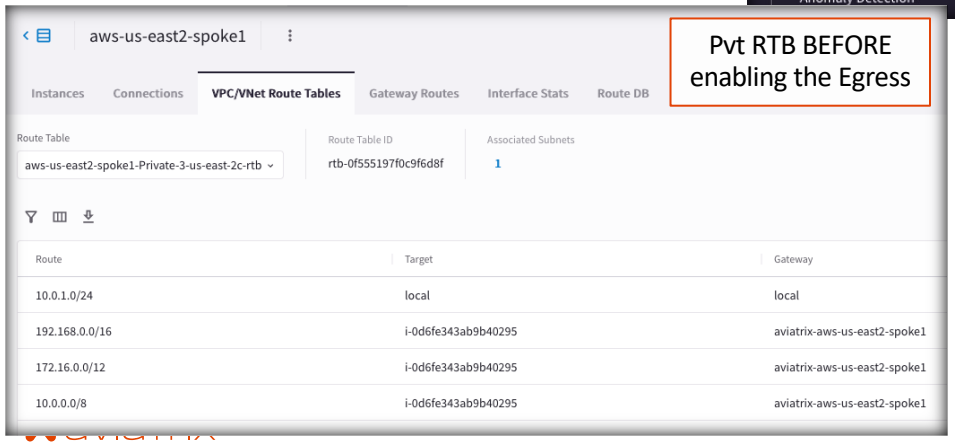
Centralized Egress with Aviatrix Transit GW



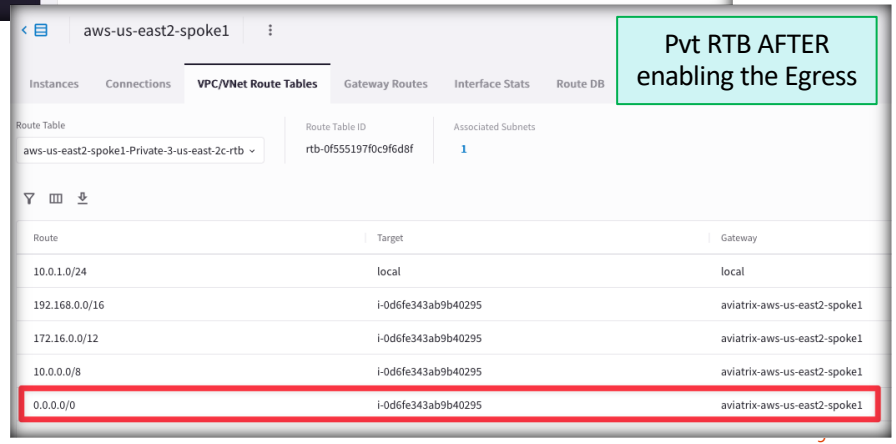
Enabling Egress

- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be injected.
- CAVEAT: Egress Control also <u>requires additional resources</u> on the Spoke Gateway (i.e. scale up the VM size). Before enabling Egress Control on Spoke Gateways, ensure that you have created the additional CPU resources on the Spoke Gateway required to support Egress Control.





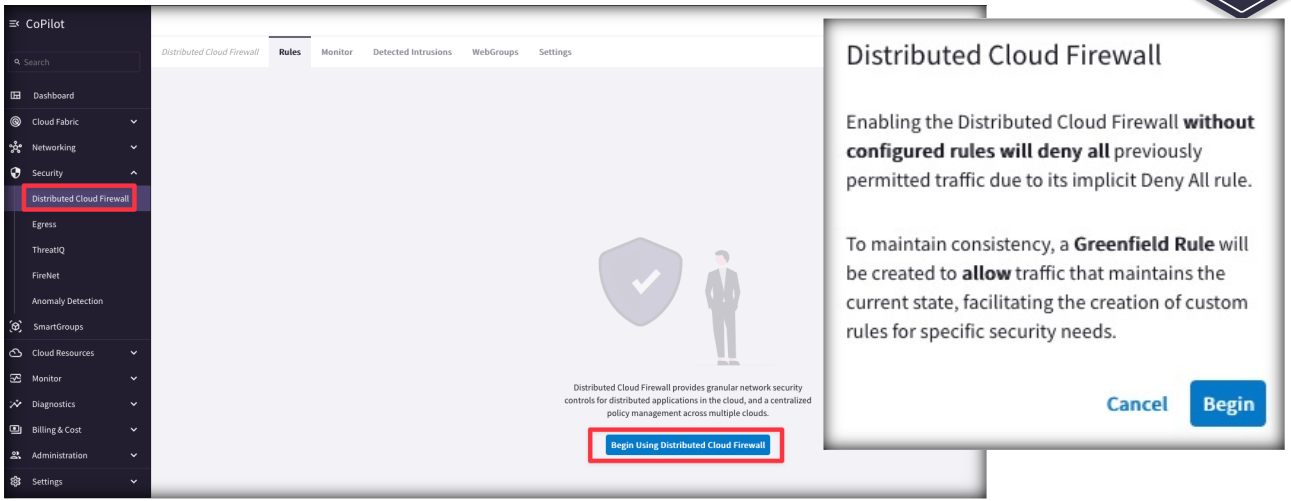
Pvt RTB BEFORE enabling the Egress

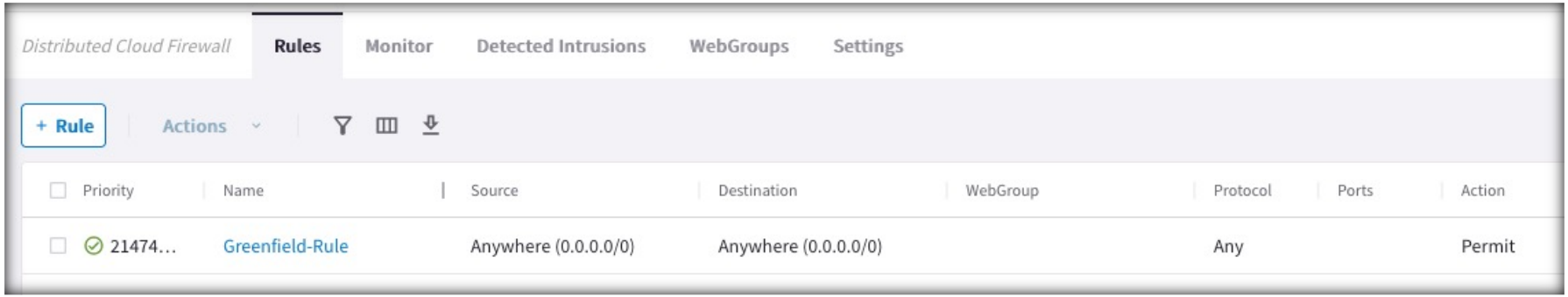


Pvt RTB AFTER enabling the Egress

The Greenfield-Rule

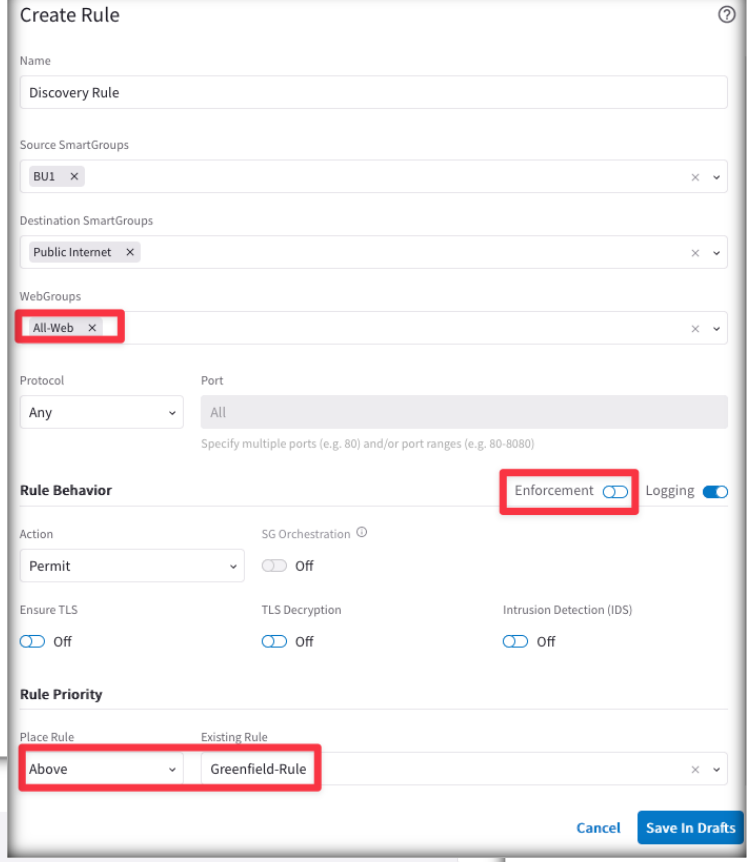
- If you want to apply policies on your Egress traffic, you must enable the Distributed Cloud Firewall.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.
- *Best Practice:* do not edit this rule, although it can be recreated if it is accidentally deleted.

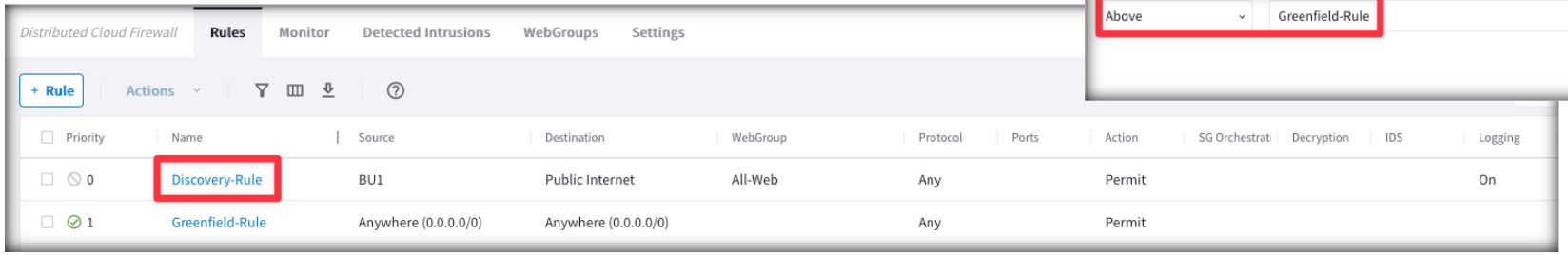




Discovery Process

- If you don't know the sites that your applications visit, an ad-hoc *Discovery-Rule* can be enabled, temporarily.
  - a) Attach the SmartGroup that identifies the private workloads affected by the Egress feature, previously enabled, as *Source SmartGroup.*
  - b) Attach the Predefined SmartGroup **"Public Internet"**, as *Destination SmartGroup.*
  - c) Attach the Predefined ***All-Web*** WebGroup.
  - d) Turn On the ***"Logging"*** toggle
  - e) Turn Off the ***"Enforcement"*** toggle
- The *Discovery-Rule* allows to intercept the logs generated only by HTTP (port 80) and HTTPS (port 443) traffic, from the VPC where the Egress control was enabled.
- *Best Practice*: Place your Discovery-Rule always above the Greenfield-Rule.
- The result will be displayed on the ***Monitor*** TAB.





Monitor

- On the Monitor section you can retrieve all the logs and therefore distinguish the domains that should be permitted from those ones that should be denied.
- <u>Best Practice</u>: *The Discovery Process* should be used only temporarily. As soon as you have completed your discovery, kindly proceed to activating the *Allow-List model (i.e. ZTN approach)*.

Egress | Overview | **Monitor** | Egress VPC/VNets | Transit Egress

Filters

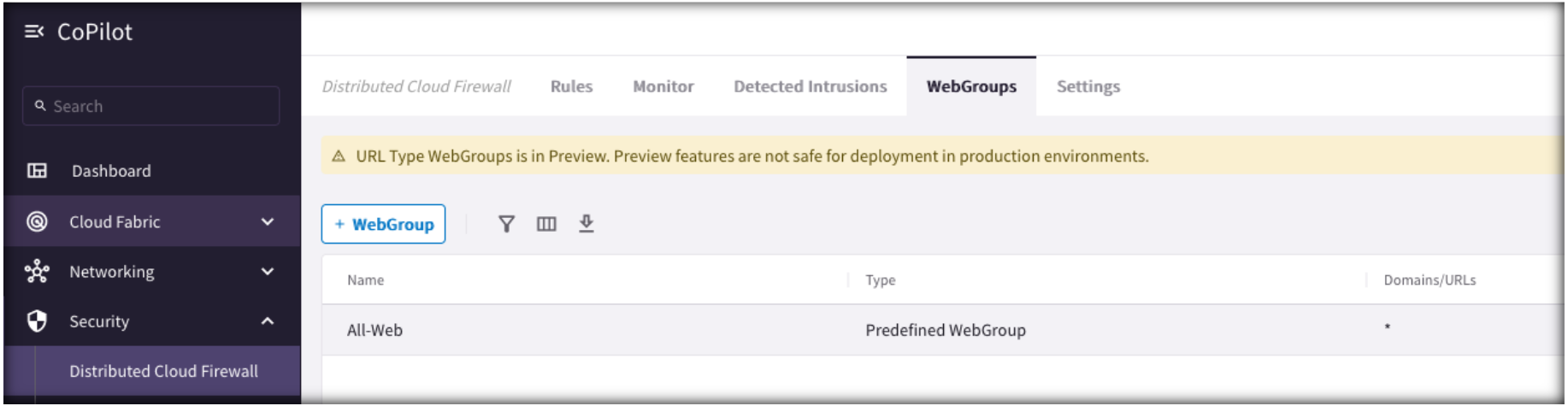
Time Period: Last 24 Hours | Start: Dec 5, 2023 10:40 AM | End: Now | VPC/VNets: aws-us-east-2-spoke1

Search

Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	esm.ubuntu.com	443	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	security.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.wikipedia.com	80	Matched	Allowed
Dec 6, 2023 10:39 AM	10.0.1.10	aws-us-east-2-spoke1	www.aviatrix.com	80	Matched	Allowed

Predefined WebGroup: All-Web

- When you navigate to **Security > Distributed Cloud Firewall > WebGroups**, a predefined WebGroup, *All-Web*, has already been created for you.
- This is an *"allow-all"* WebGroup that you must select in a Distributed Cloup Firewall rule if you do not want to limit the Internet-bound traffic for that rule, but you still want to log the FQDNs that are being accessed.



WebGroup Creation

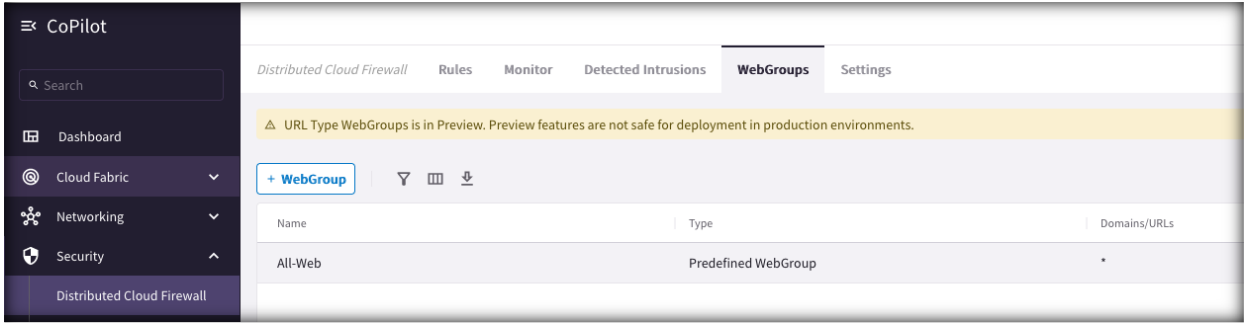
- **WebGroups** are groupings of domains and URLs, inserted into Distributed Cloud Firewall rules, that filter (and provide security to) Internet-bound traffic.

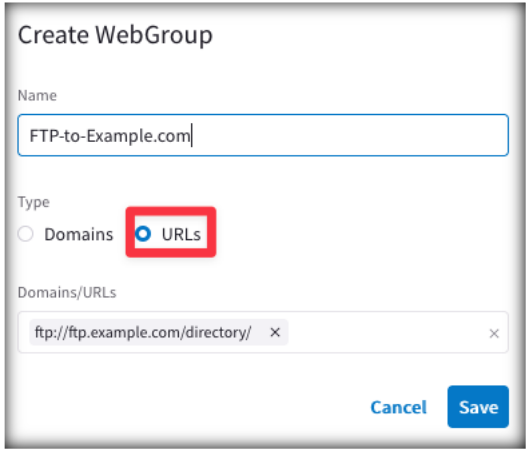
- In addition to the predefined WebGroup ***All-Web***, you can also create two kind of custom WebGroups:

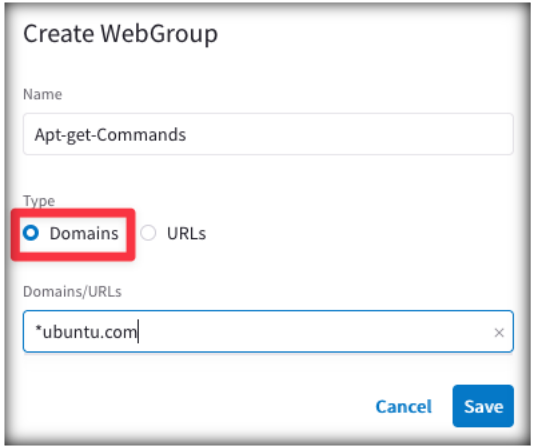
  1. **URLs WebGroup:** for HTTP/HTTPS and for other protocols, but you need to define the full Path.

     - CAVEAT: TLS Decryption must be turned on when URLs-based WebGroups are used.

  2. **Domains WebGroup:** for HTTP and HTTPS traffic (wild cards are supported – i.e. partial names).







Lab 5 – Egress