AVIATRIX

ACE

★★★★

PROFESSIONAL

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

aviatrix

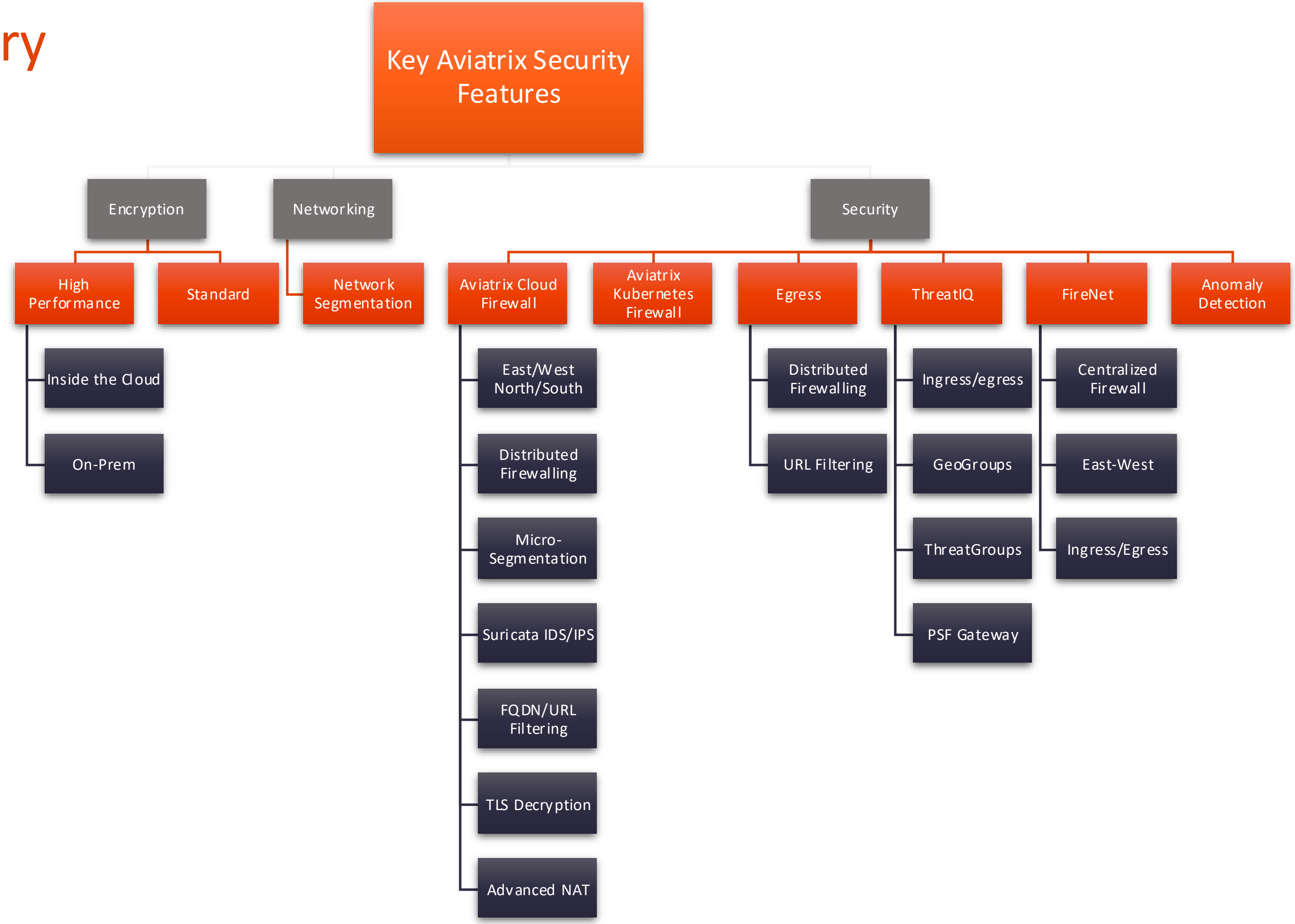
The Security Architect's Guide to Multi-Cloud Networking

Treat cloud networking as its own domain. Cloud networking has its own technology and operational practices and deserves focused attention.

Simon Richard, Gartner Analyst May 2020

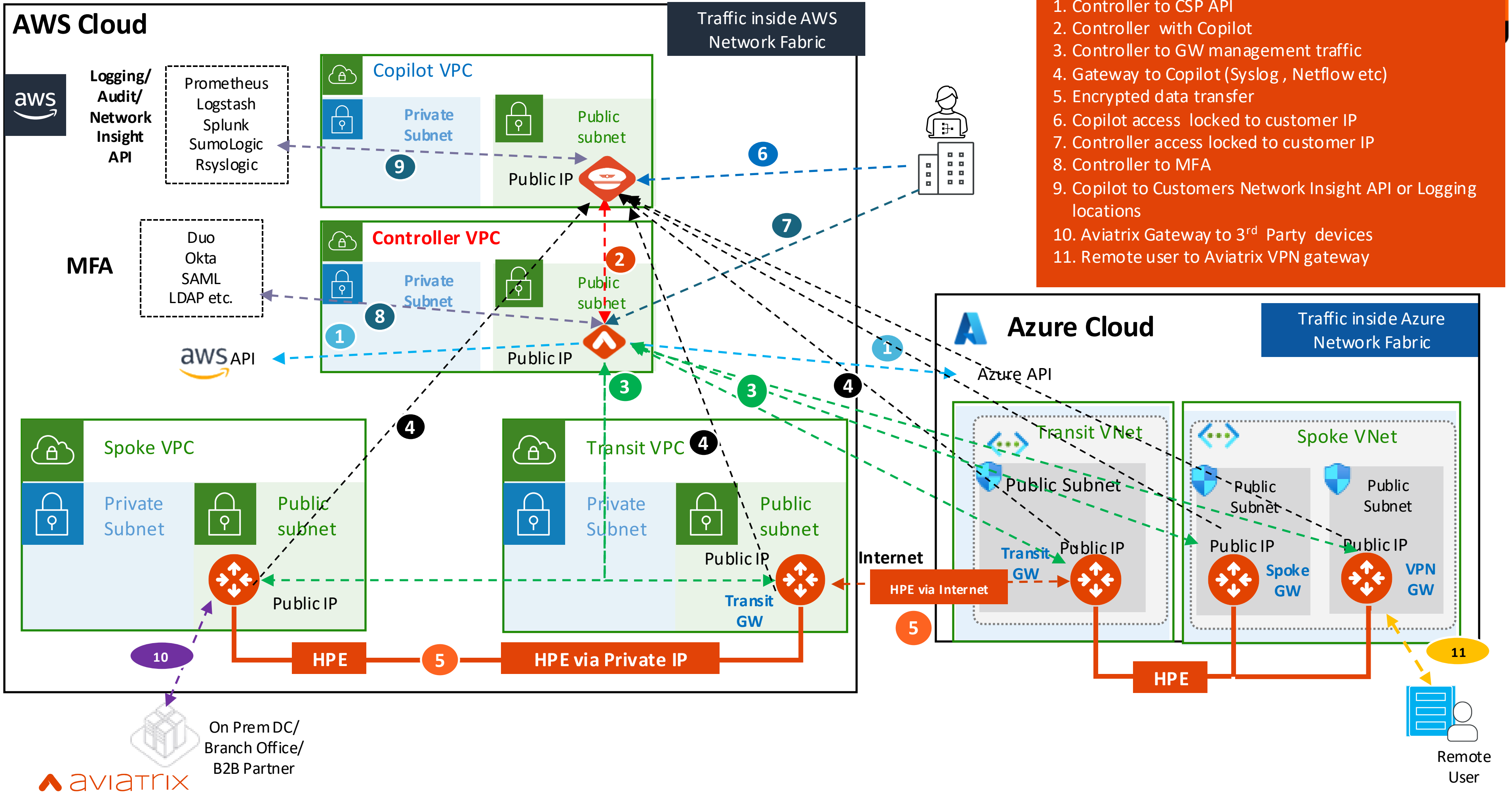
https://aviatrix.com/resources/ebooks/security-architects-guide-multi-cloud-networking-v2

Summary



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

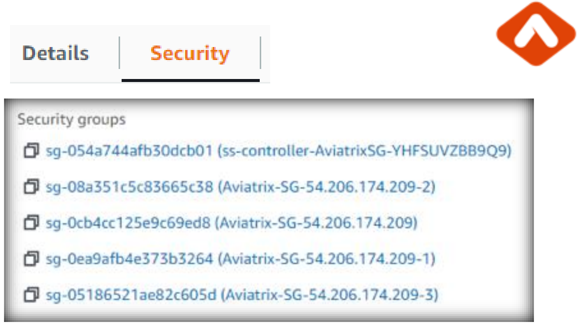
Built-in Security of the Aviatrix Platform



Traffic Pattern

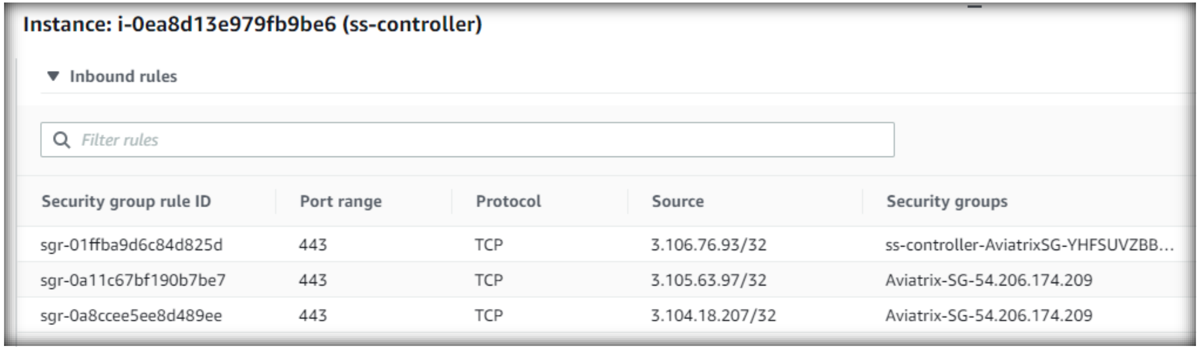
1. Controller to CSP API
2. Controller with Copilot
3. Controller to GW management traffic
4. Gateway to Copilot (Syslog , Netflow etc)
5. Encrypted data transfer
6. Copilot access locked to customer IP
7. Controller access locked to customer IP
8. Controller to MFA
9. Copilot to Customers Network Insight API or Logging locations
10. Aviatrix Gateway to 3rd Party devices
11. Remote user to Aviatrix VPN gateway

Controller Security Group Management | Automatic Security Group lockdown



Security groups

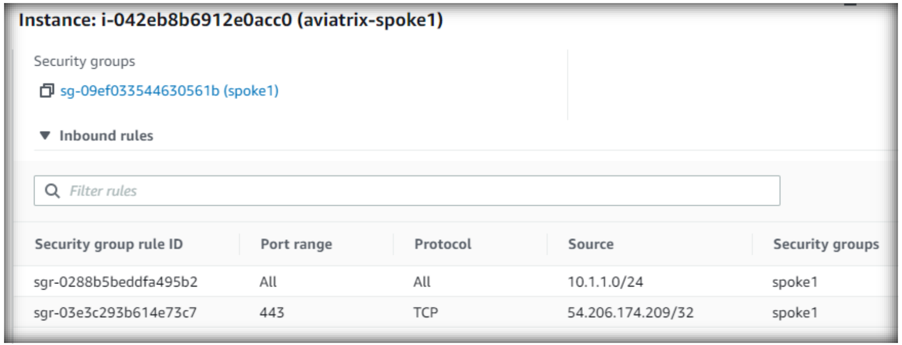
- sg-054a744afb30dcb01 (ss-controller-AviatrixSG-YHFSUVZBB9Q9)
- sg-08a351c5c83665c38 (Aviatrix-SG-54.206.174.209-2)
- sg-0cb4cc125e9c69ed8 (Aviatrix-SG-54.206.174.209)
- sg-0ea9afb4e373b3264 (Aviatrix-SG-54.206.174.209-1)
- sg-05186521ae82c605d (Aviatrix-SG-54.206.174.209-3)



Instance: i-0ea8d13e979fb9be6 (ss-controller)

▼ Inbound rules

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

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

AVIATRIX
ACE
★★★★
PROFESSIONAL

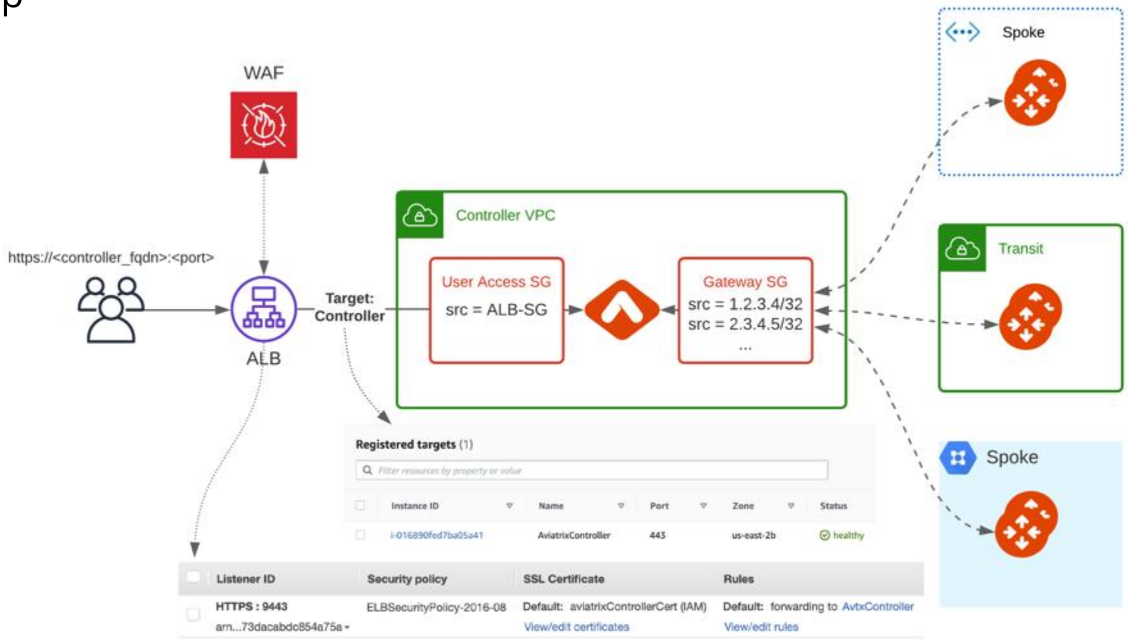
Securing the Platform with Cloud Native Load Balancers

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

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



Registered targets (1)

Filter resources by property or value

Instance ID	Name	Port	Zone	Status
i-016890fed7ba05a41	AviatrixController	443	us-east-2b	healthy

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 9443 arn...73dacabdc854a75a	ELBSecurityPolicy-2016-08	Default: aviatrixControllerCert (IAM) View/edit certificates	Default: forwarding to AvtxController View/edit rules

Aviatrix Cloud Firewall

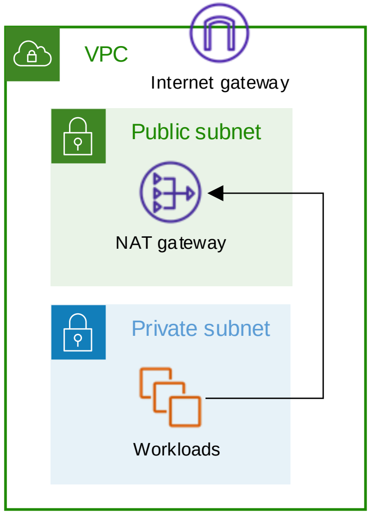
Problem Statement

Private workloads need internet access

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

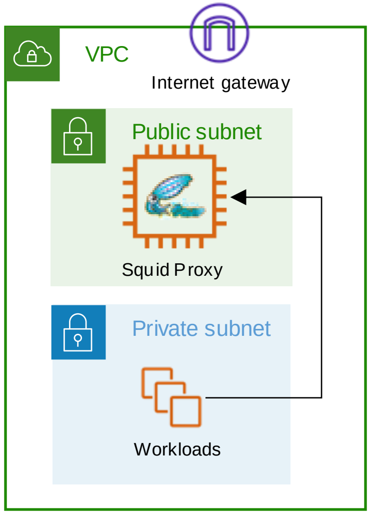
NAT Gateway

- NACLs are necessary
- Layer-4 only



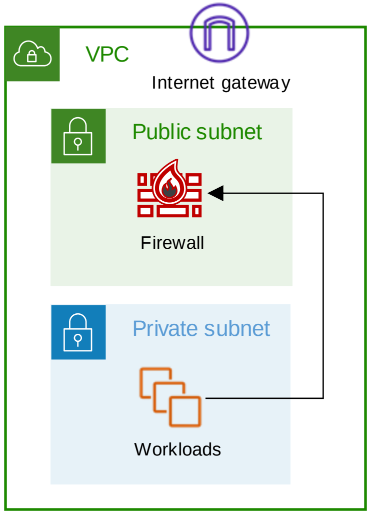
Squid Proxy

- Hard to manage
- Scale and HA issues

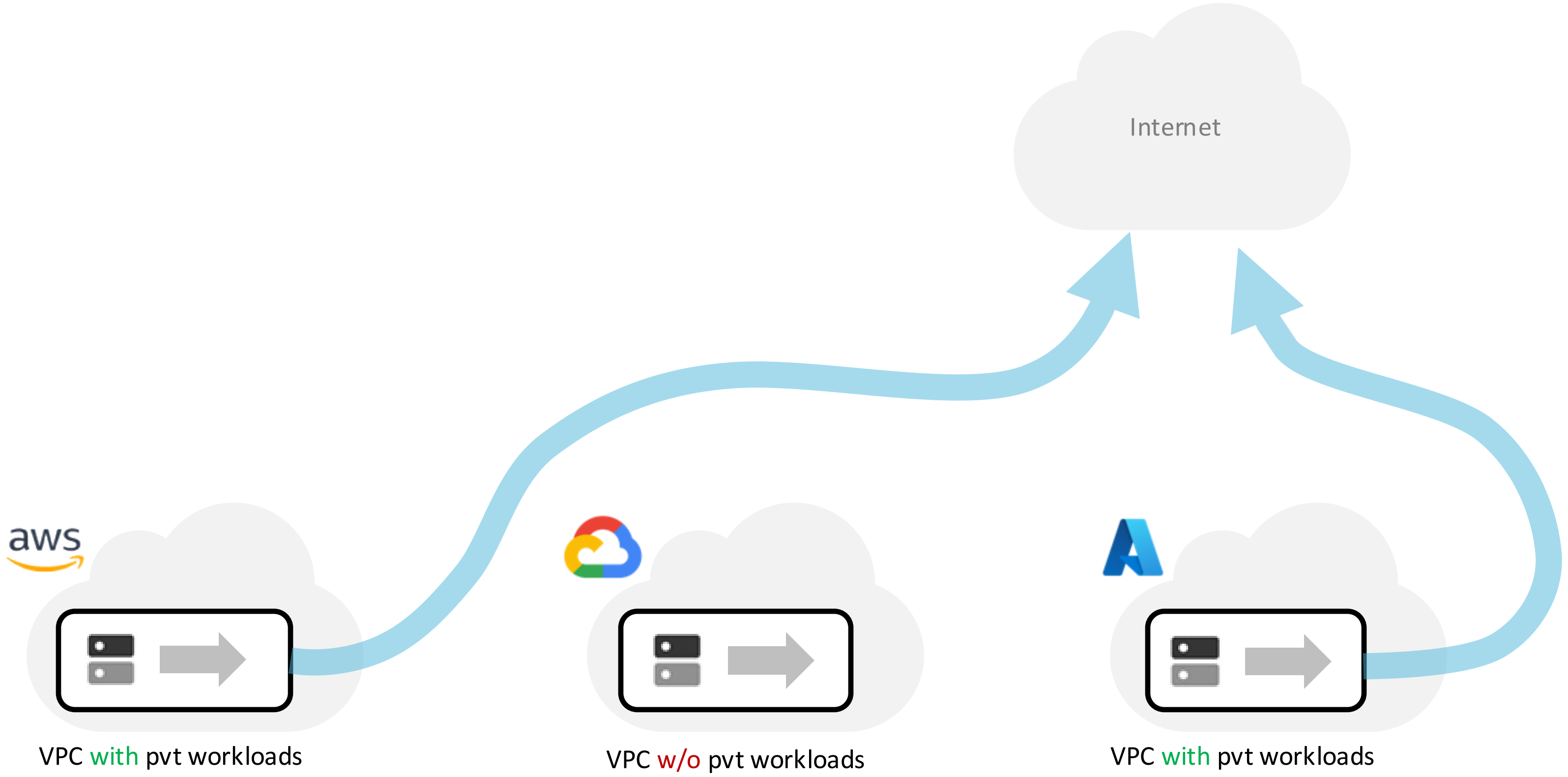


Layer-7 Firewall

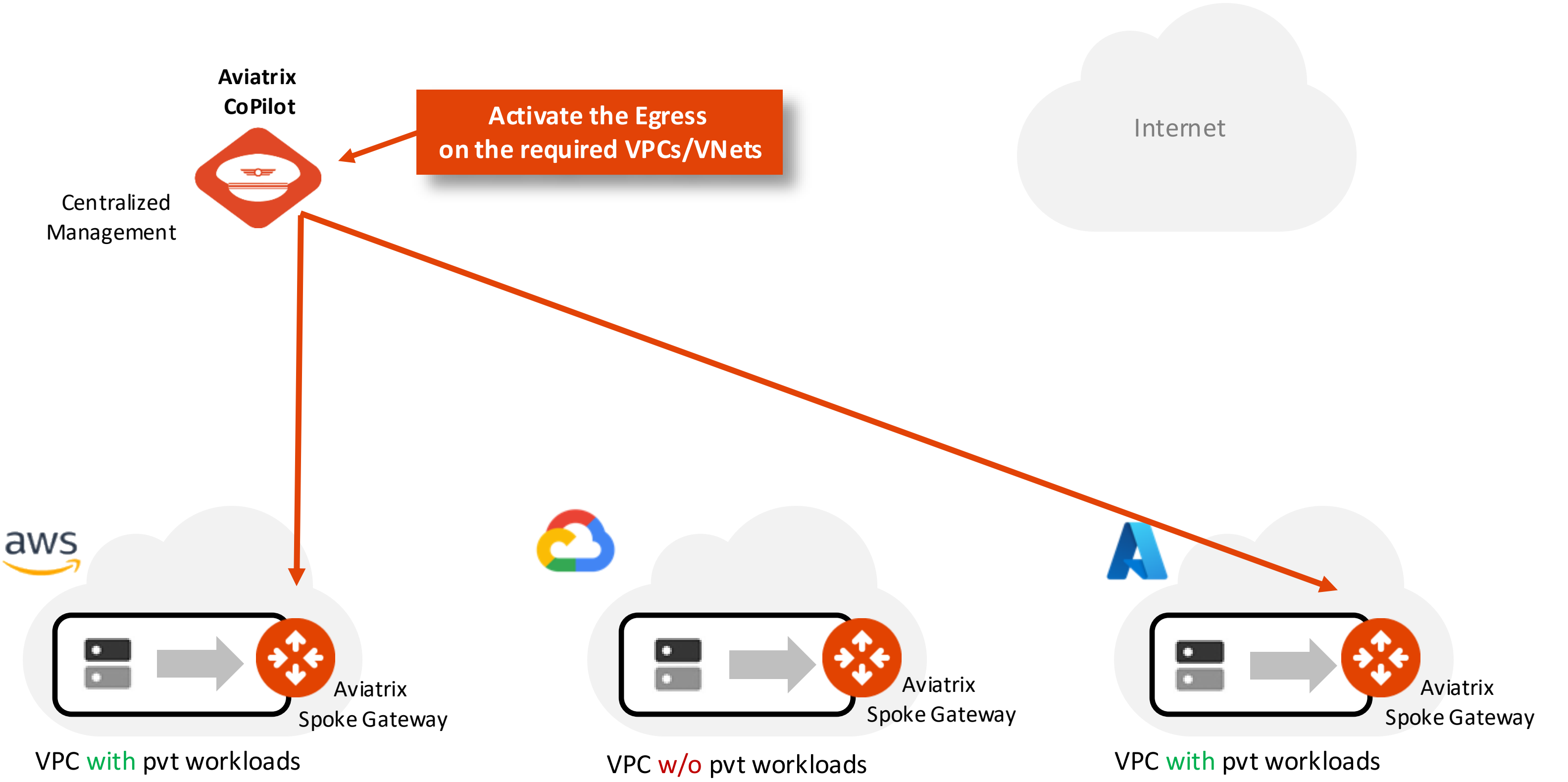
- Overkill
- Expensive



Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



Activate the Egress on the required VPCs/VNets

VPC with pvt workloads

VPC w/o pvt workloads

VPC with pvt workloads

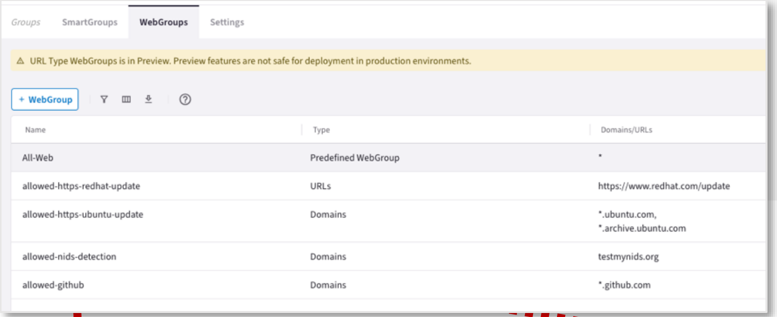
Aviatrix Cloud Firewall

AVIATRIX ACE PROFESSIONAL

Aviatrix CoPilot

Centralized Management

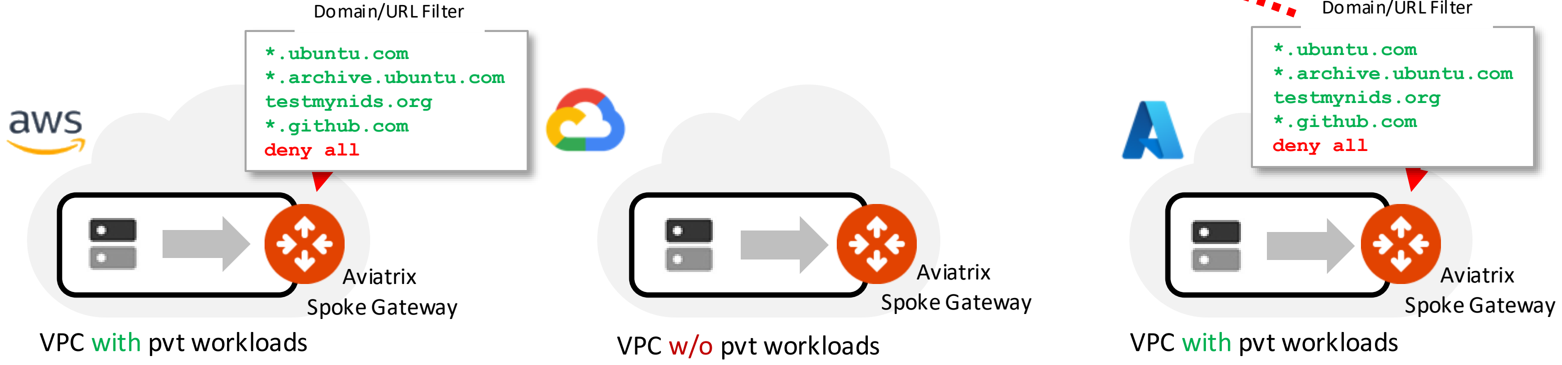
Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	URLs	https://www.redhat.com/update
allowed-https-ubuntu-update	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com

Internet



Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

VPC with pvt workloads

VPC w/o pvt workloads

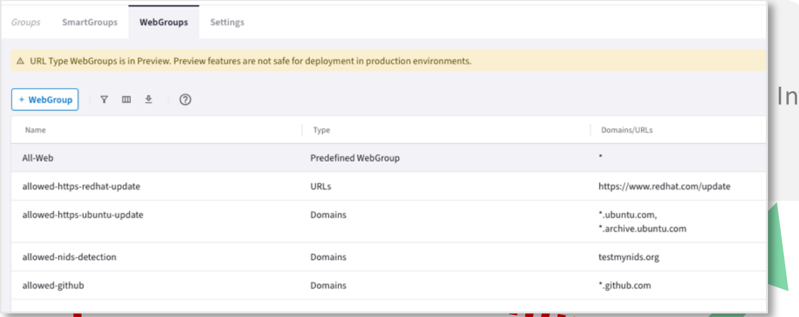
VPC with pvt workloads

Aviatrix Cloud Firewall

Aviatrix CoPilot

Centralized Management

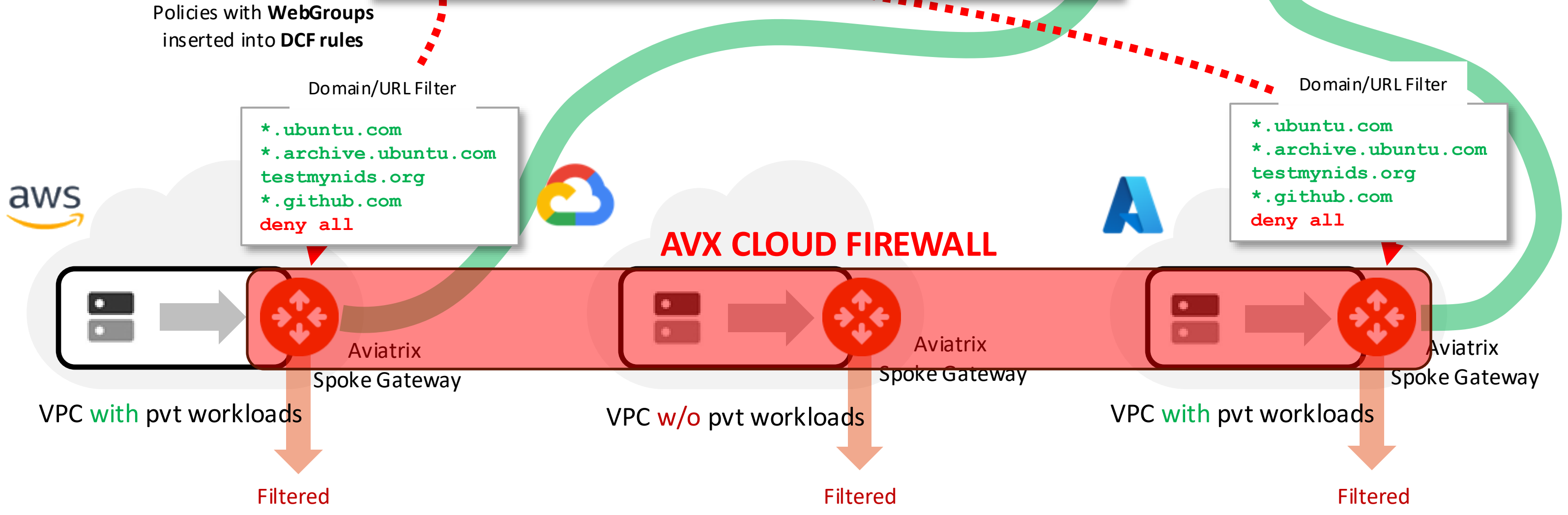
Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	URLs	https://www.redhat.com/update
allowed-https-ubuntu-update	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com

Internet



Domain/URL Filter

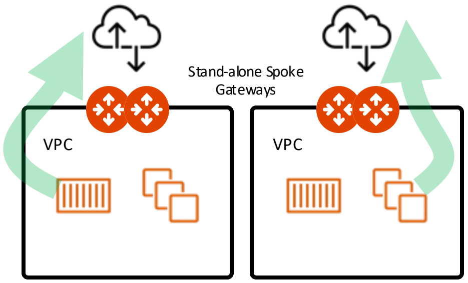
```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Domain/URL Filter

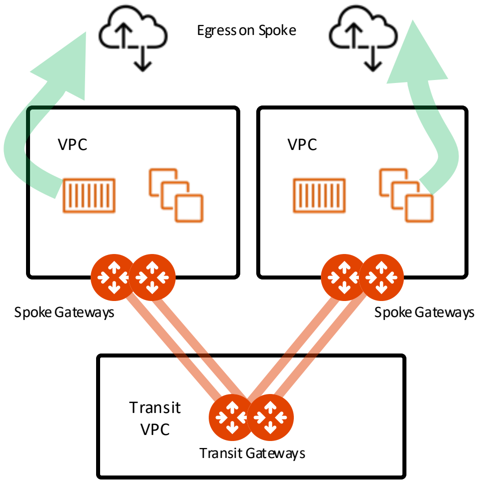
```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Aviatrix Cloud Firewall - Filtering Design Patterns

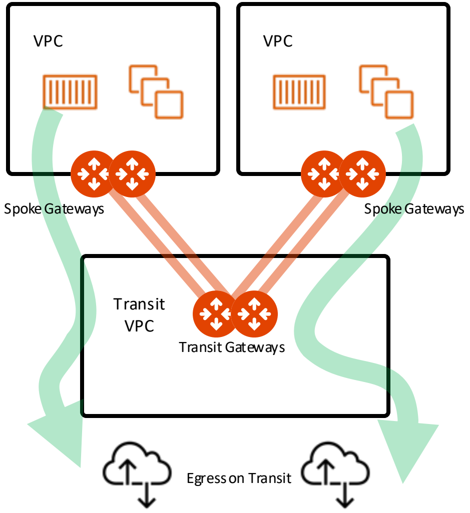
Stand-alone Spoke GW (Distributed)



Local Egress (Distributed) with Aviatrix Spoke GW

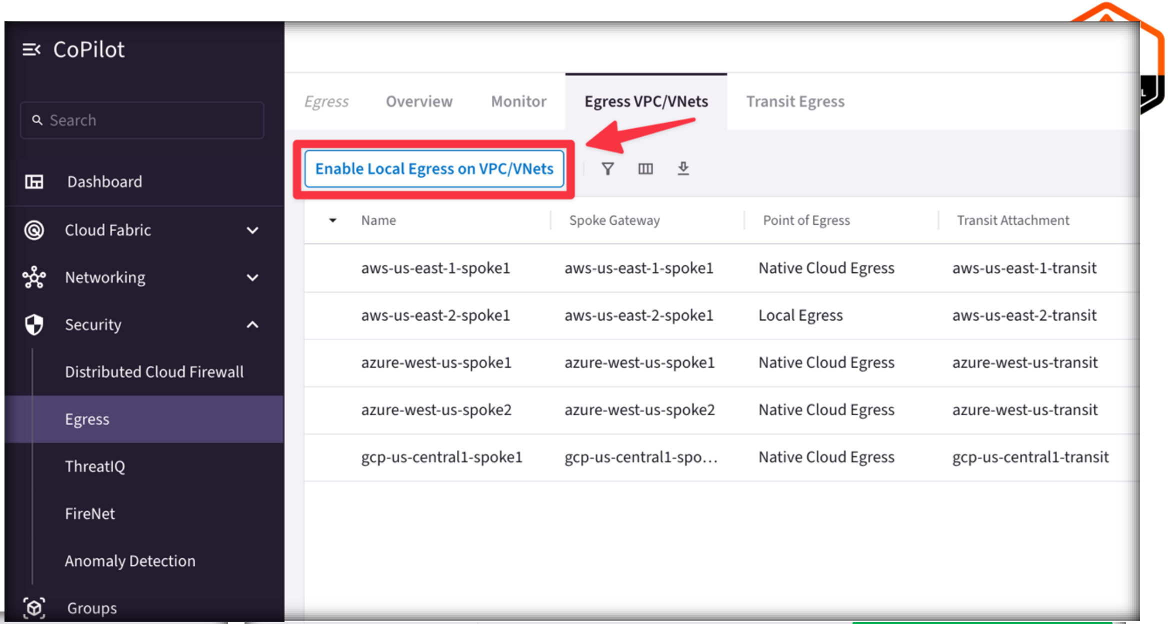


Centralized Egress with Aviatrix Transit GW

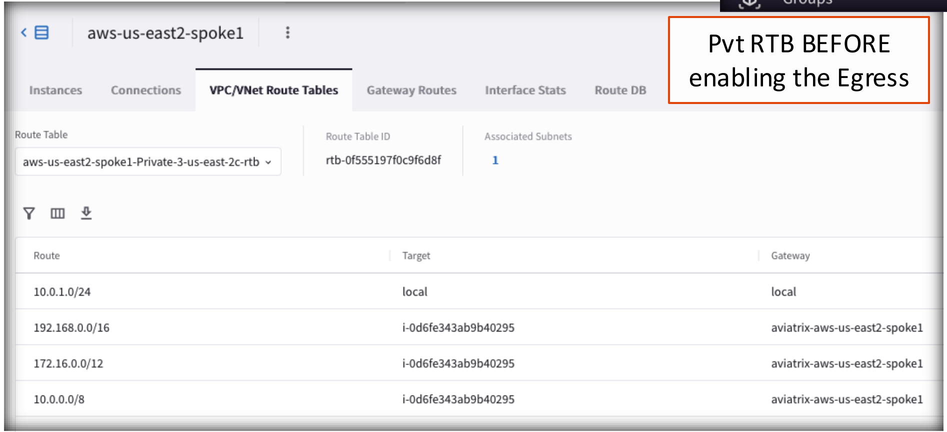


Enabling Egress

- 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.



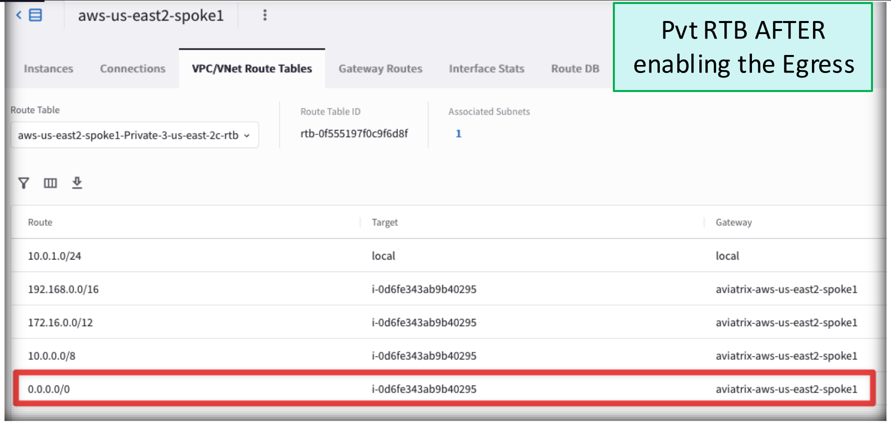
Name	Spoke Gateway	Point of Egress	Transit Attachment
aws-us-east-1-spoke1	aws-us-east-1-spoke1	Native Cloud Egress	aws-us-east-1-transit
aws-us-east-2-spoke1	aws-us-east-2-spoke1	Local Egress	aws-us-east-2-transit
azure-west-us-spoke1	azure-west-us-spoke1	Native Cloud Egress	azure-west-us-transit
azure-west-us-spoke2	azure-west-us-spoke2	Native Cloud Egress	azure-west-us-transit
gcp-us-central1-spoke1	gcp-us-central1-spo…	Native Cloud Egress	gcp-us-central1-transit



Pvt RTB BEFORE enabling the Egress

Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb
Route Table ID: rtb-0f555197f0c9f6d8f
Associated Subnets: 1

Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1



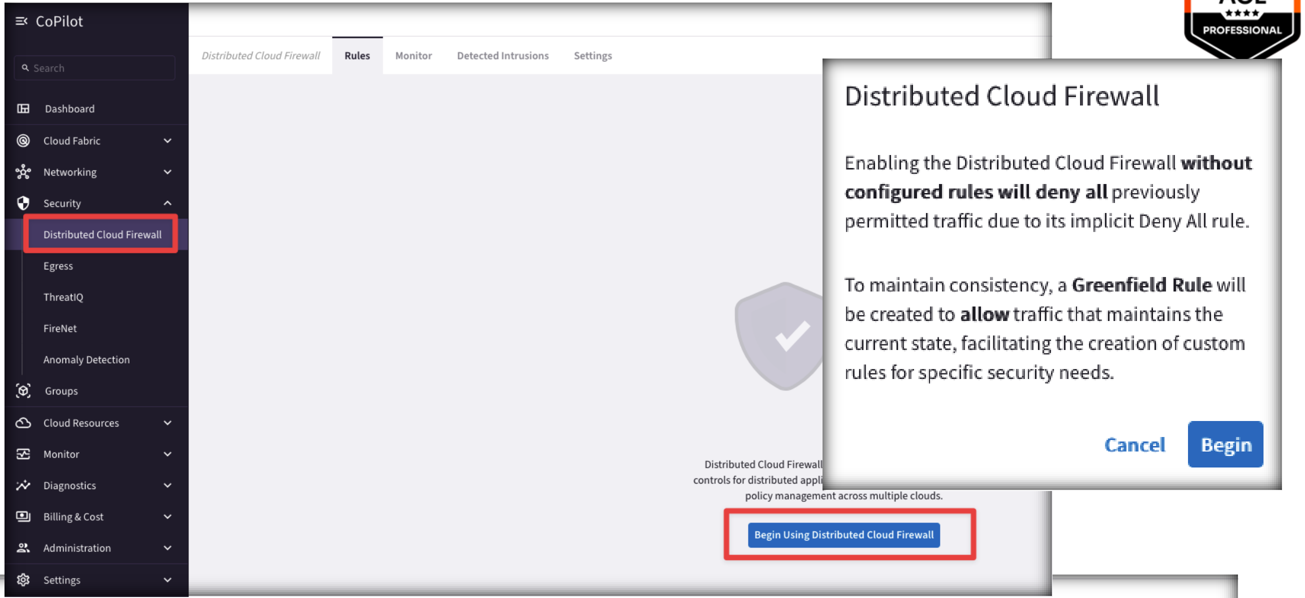
Pvt RTB AFTER enabling the Egress

Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb
Route Table ID: rtb-0f555197f0c9f6d8f
Associated Subnets: 1

Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
0.0.0.0/0	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1

The Greenfield-Rule

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

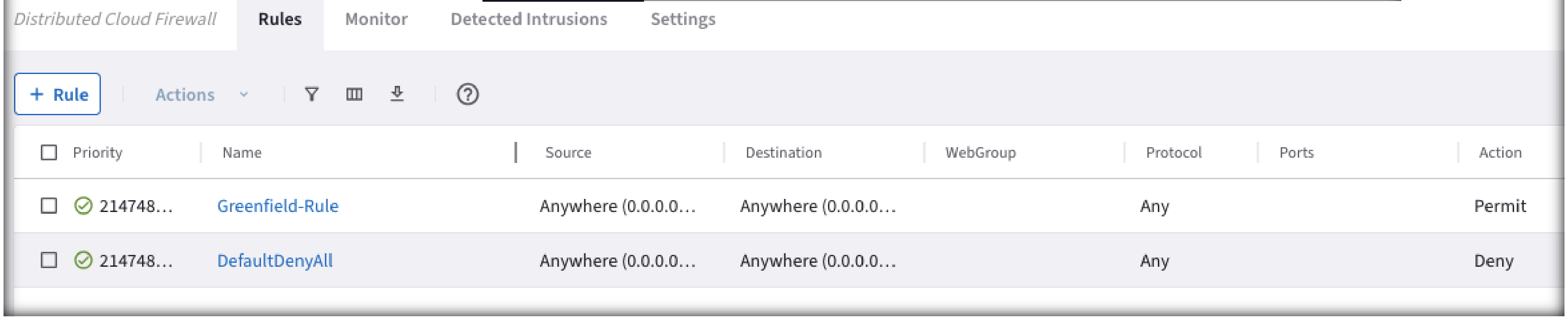


Distributed Cloud Firewall
controls for distributed appli
policy management across multiple clouds.

Distributed Cloud Firewall

Enabling the Distributed Cloud Firewall **without configured rules will deny all** previously permitted traffic due to its implicit Deny All rule.

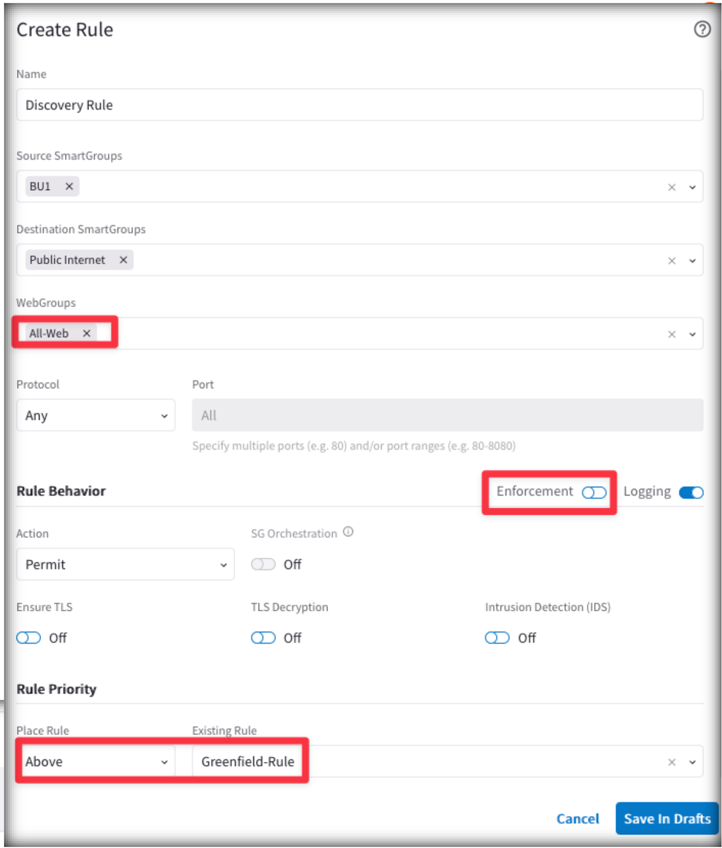
To maintain consistency, a **Greenfield Rule** will be created to **allow** traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.



□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
□	✓ 214748…	Greenfield-Rule	Anywhere (0.0.0.0…	Anywhere (0.0.0.0…		Any		Permit
□	✓ 214748…	DefaultDenyAll	Anywhere (0.0.0.0…	Anywhere (0.0.0.0…		Any		Deny

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.



Create Rule

Name: Discovery Rule

Source SmartGroups: BU1 ×

Destination SmartGroups: Public Internet ×

WebGroups: All-Web ×

Protocol: Any

Port: All

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement ○ Logging ●

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

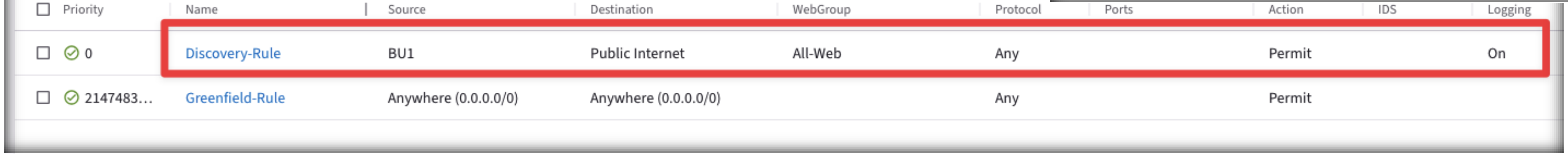
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule: Above

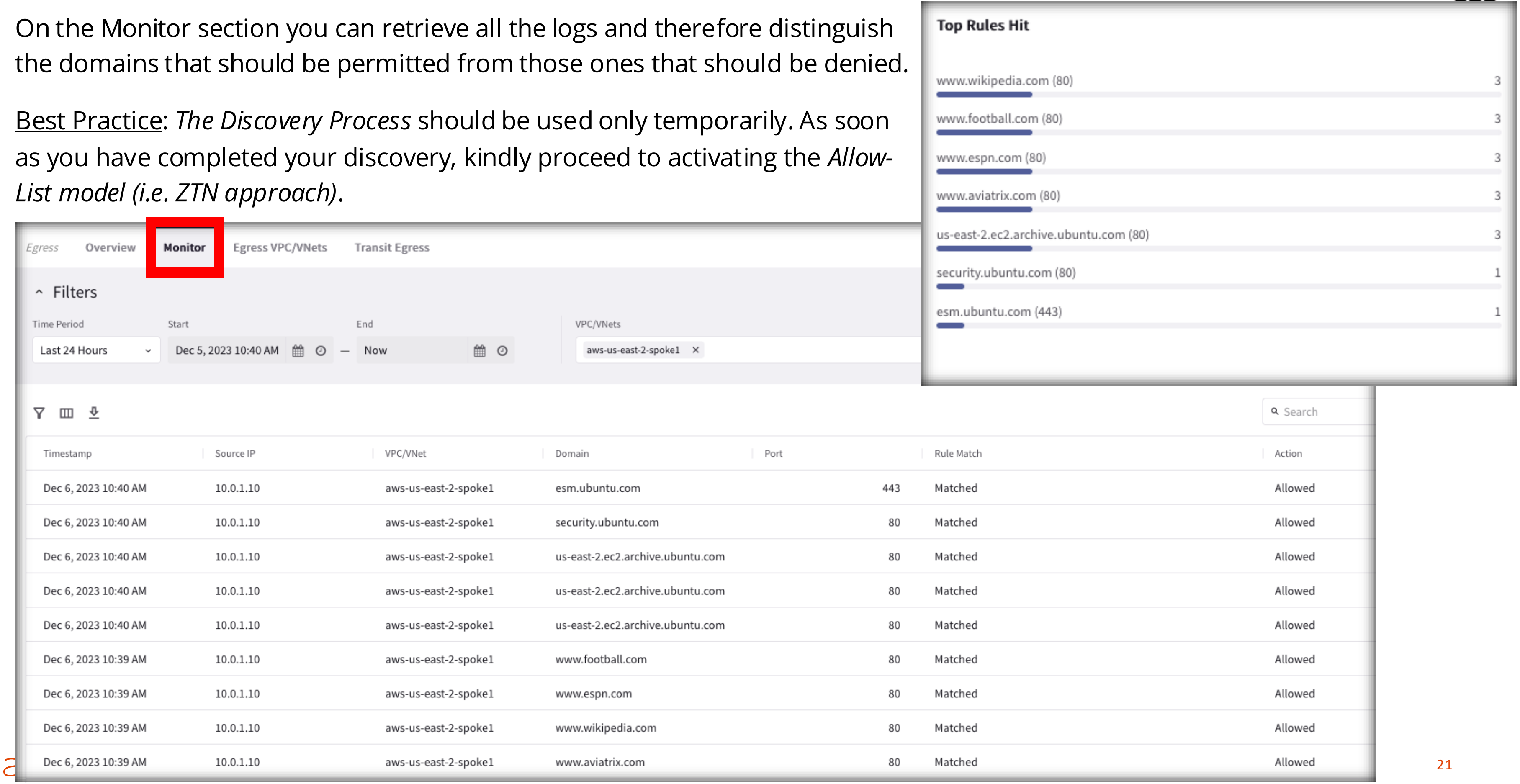
Existing Rule: Greenfield-Rule



□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	IDS	Logging
□	✓ 0	Discovery-Rule	BU1	Public Internet	All-Web	Any		Permit		On
□	✓ 2147483…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit		

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.
- Best Practice: *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)*.



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

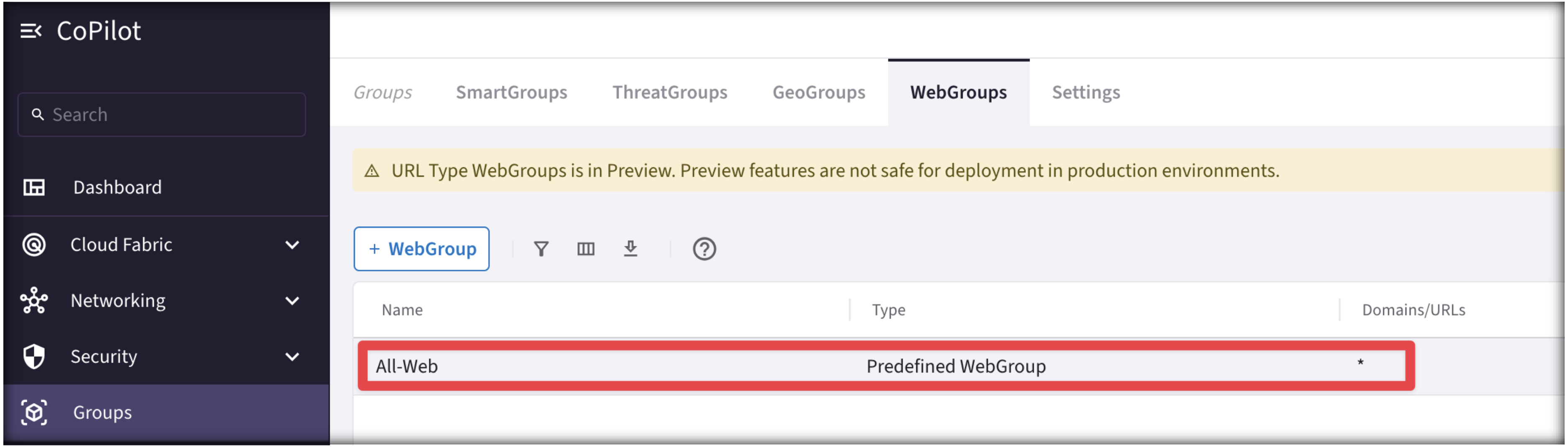
Top Rules Hit

www.wikipedia.com (80)	3
www.football.com (80)	3
www.espn.com (80)	3
www.aviatrix.com (80)	3
us-east-2.ec2.archive.ubuntu.com (80)	3
security.ubuntu.com (80)	1
esm.ubuntu.com (443)	1

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 **CoPilot > Groups**, a predefined WebGroup, *All-Web*, has already been created for you.
- This is an "*allow-all*" WebGroup that you must select in a Distributed Cloud 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.



⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

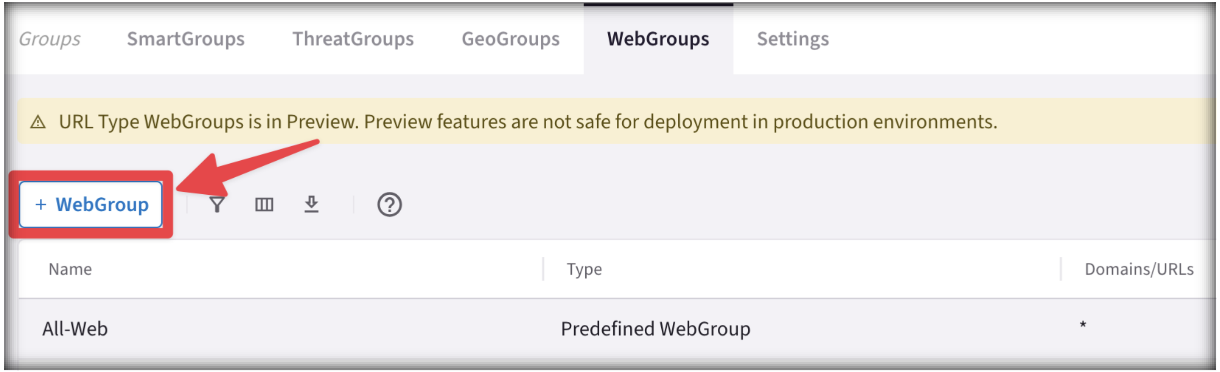
Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*

WebGroup Creation

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

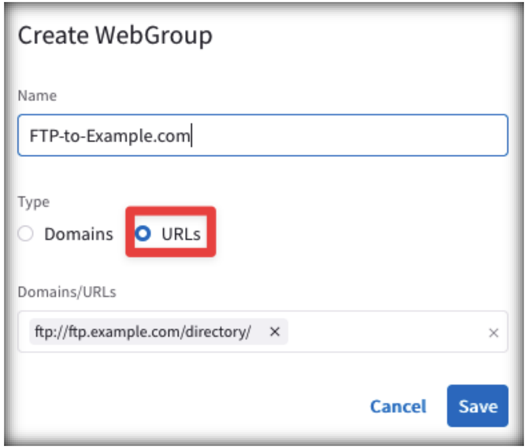
- In addition to the predefined WebGroup ***All-Web***, you can also create two kind of custom WebGroups:

  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).



⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*

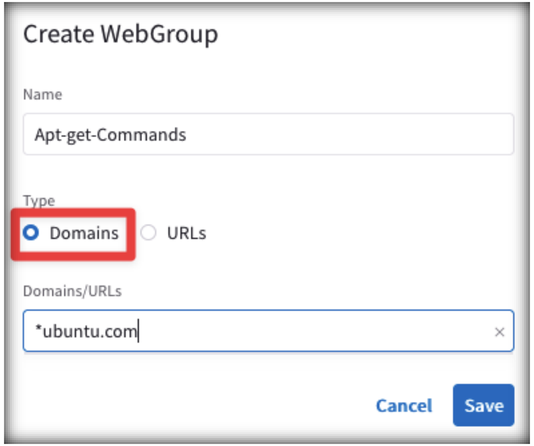


Create WebGroup

Name: FTP-to-Example.com

Type: ○ Domains ● URLs

Domains/URLs: ftp://ftp.example.com/directory/ ×



Create WebGroup

Name: Apt-get-Commands

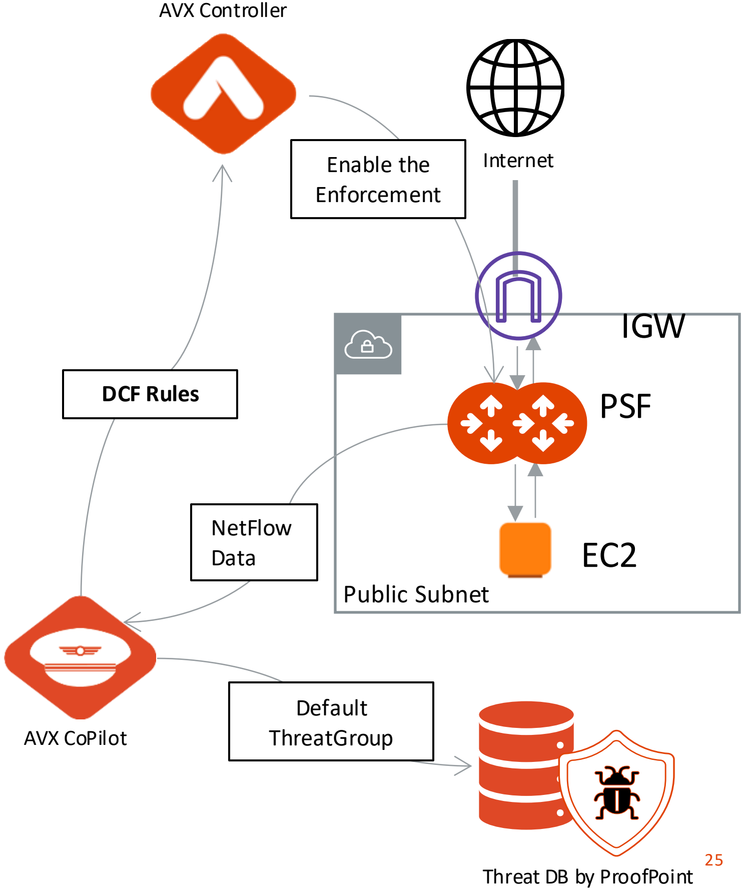
Type: ● Domains ○ URLs

Domains/URLs: *ubuntu.com

Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

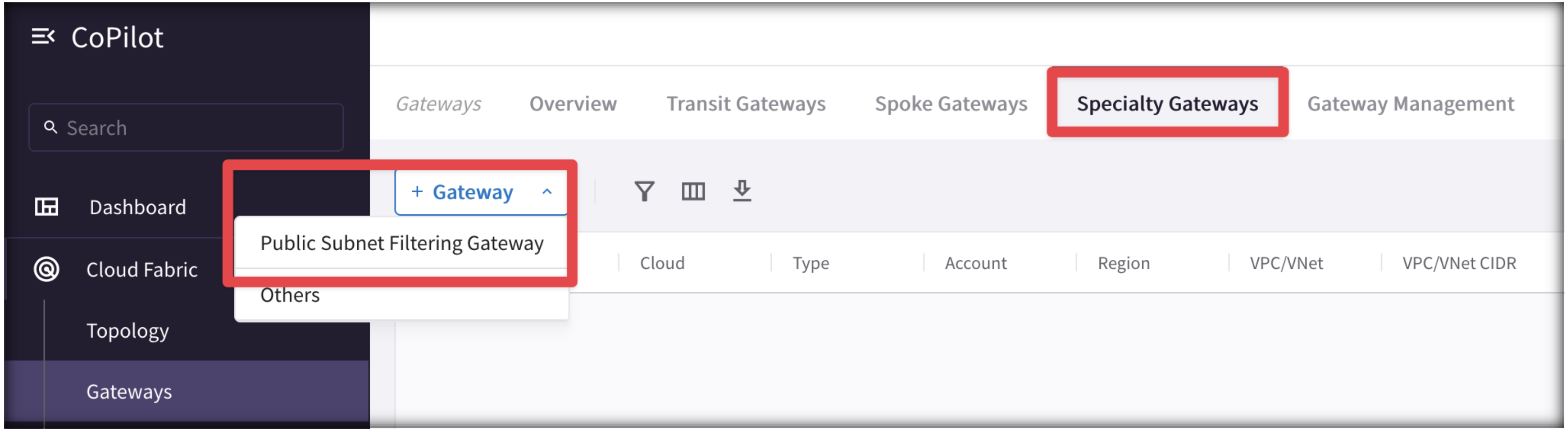
- **Public Subnet Filtering Gateways** (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be enabled.*
- The PSF Gateway acts as a **standalone Gateway** (it’s neither a Spoke nor a Transit).
- Leverage the **Default ThreatGroup** (i.e. a Malicious IP addresses DB supplied by ProofPoint) if you want to prevent attacks towards your public-facing workloads.



Aviatrix PSF Deployment Workflow (part.1)

To deploy a Public Subnet Filtering Gateway:

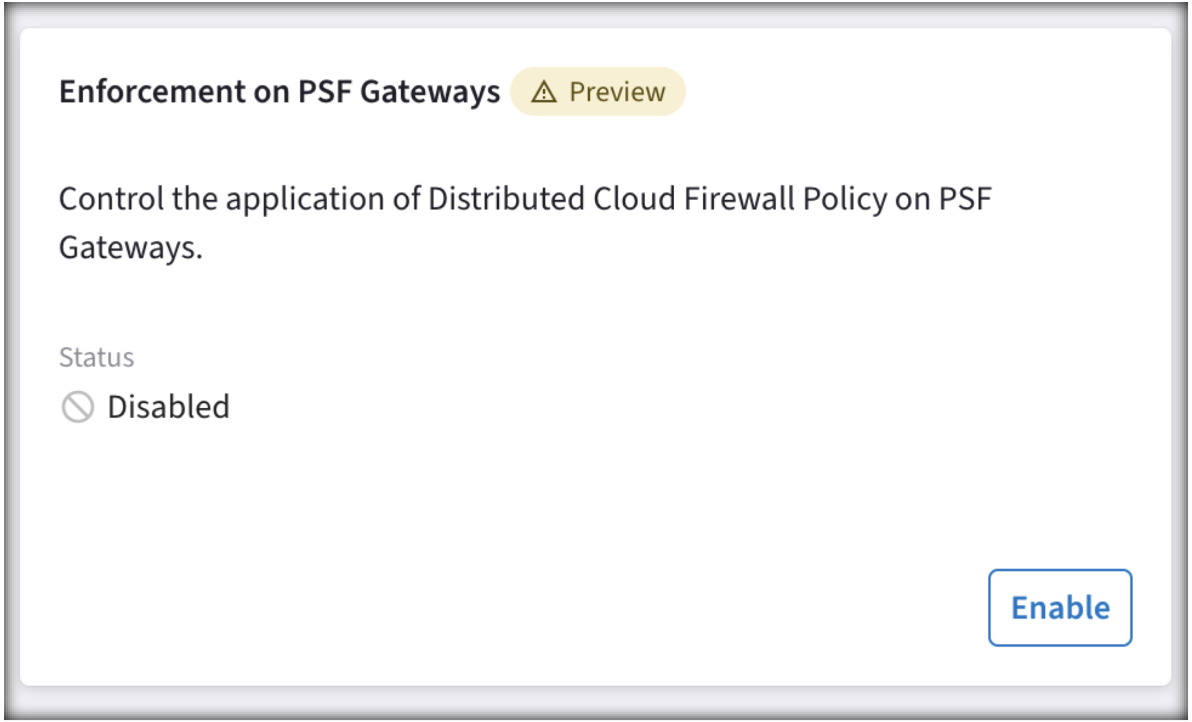
1. In CoPilot, navigate to **Cloud Fabric** > **Gateways** > **Speciality Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



Enforcement on PSF

The Enforcement of DCF (Distributed Cloud Firewall) rules on the PSF Gateway is *disabled* by default.

- This feature needs to be enabled if you want the AVX Controller to push DCF Rules also on this standalone Gateway.



Enforcement on PSF Gateways ⚠ Preview

Control the application of Distributed Cloud Firewall Policy on PSF Gateways.

Status

⃠ Disabled

AVIATRIX
ACE
★★★★
PROFESSIONAL

Lab 5 – **Aviatrix Cloud Firewall (with Secure Egress)**