aviatrix

Security

SOLUTIONS ENGINEERING

www.aviatrix.com

Agenda

- Aviatrix Security Features Overview
- Securing Aviatrix Platform
- Egress

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

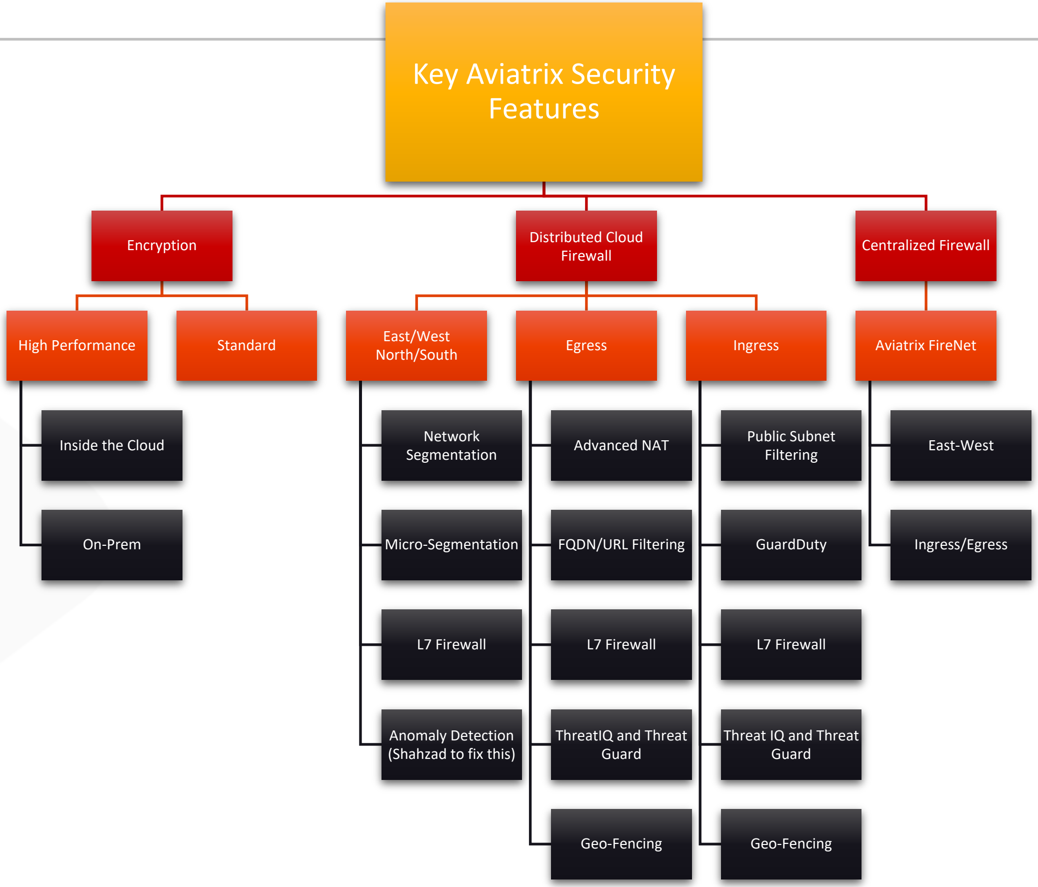
The Security Architect’s Guide to Multi-Cloud Networking

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

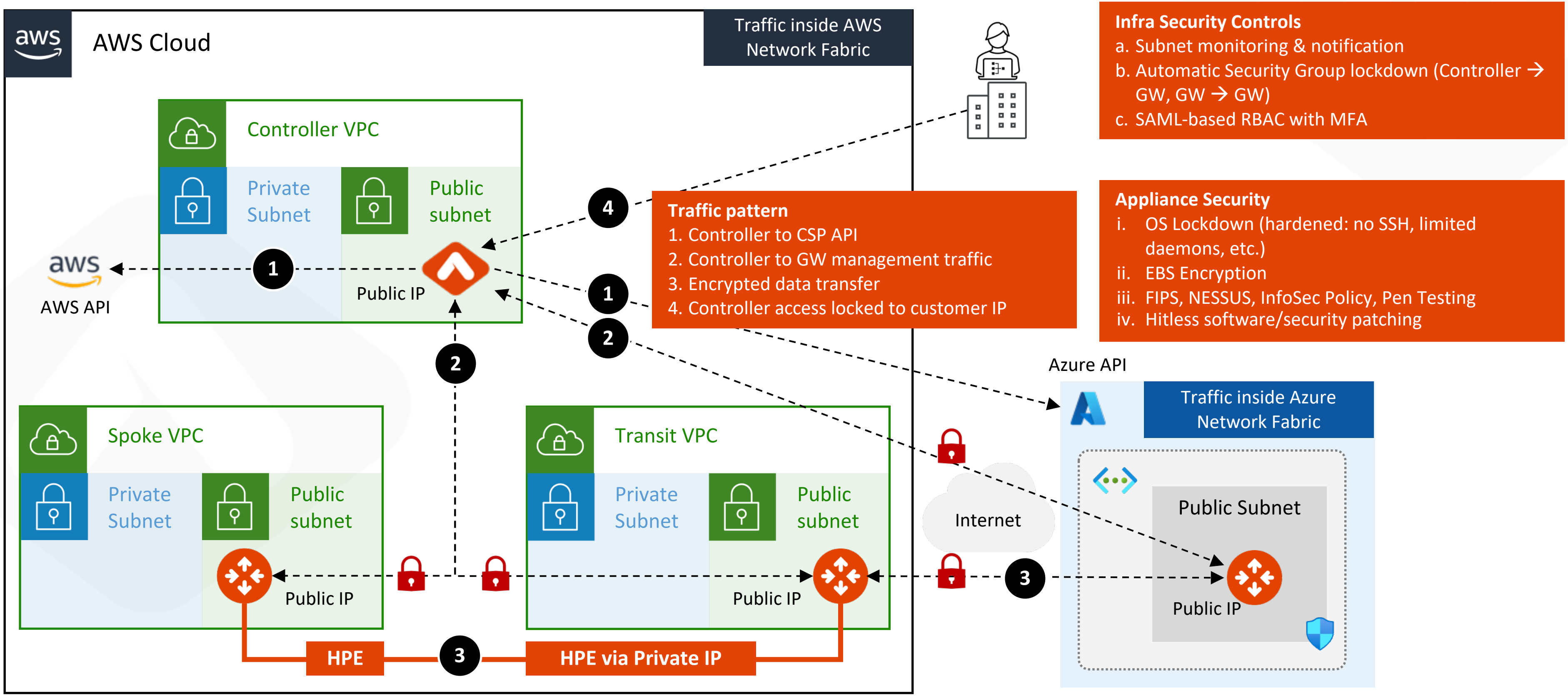


- Key Aviatrix Security Features
  - Encryption
    - High Performance
      - Inside the Cloud
      - On-Prem
    - Standard
  - Distributed Cloud Firewall
    - East/West North/South
      - Network Segmentation
      - Micro-Segmentation
      - L7 Firewall
      - Anomaly Detection (Shahzad to fix this)
    - Egress
      - Advanced NAT
      - FQDN/URL Filtering
      - L7 Firewall
      - ThreatIQ and Threat Guard
      - Geo-Fencing
    - Ingress
      - Public Subnet Filtering
      - GuardDuty
      - L7 Firewall
      - Threat IQ and Threat Guard
      - Geo-Fencing
  - Centralized Firewall
    - Aviatrix FireNet
      - East-West
      - Ingress/Egress

aviatrix

Built-in Security of the Aviatrix Platform

Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



Infra Security Controls

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

Traffic pattern

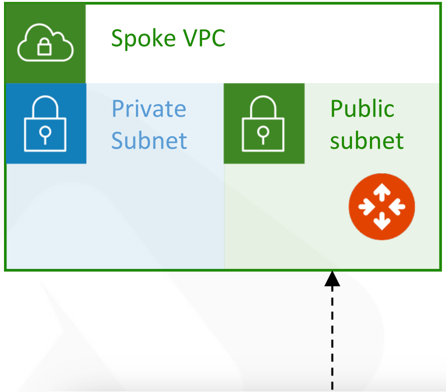
1. Controller to CSP API
2. Controller to GW management traffic
3. Encrypted data transfer
4. Controller access locked to customer IP

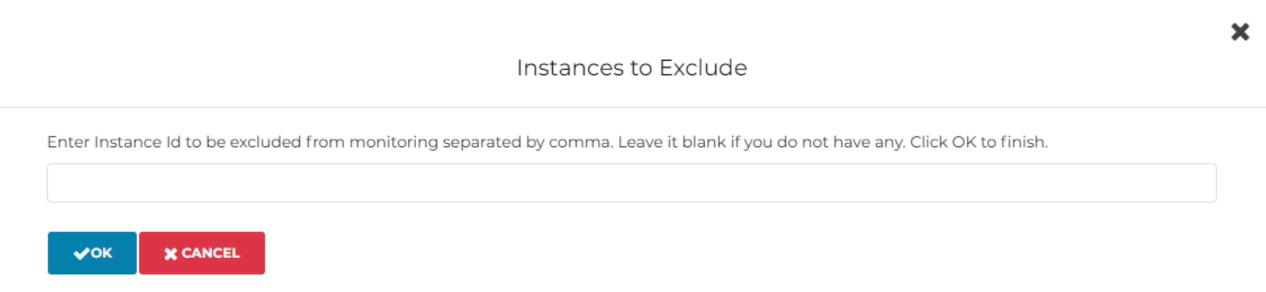
Appliance Security

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

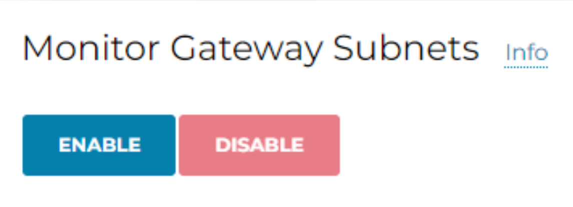
Prevents unauthorized VMs from being launched in the same subnet as the gateways



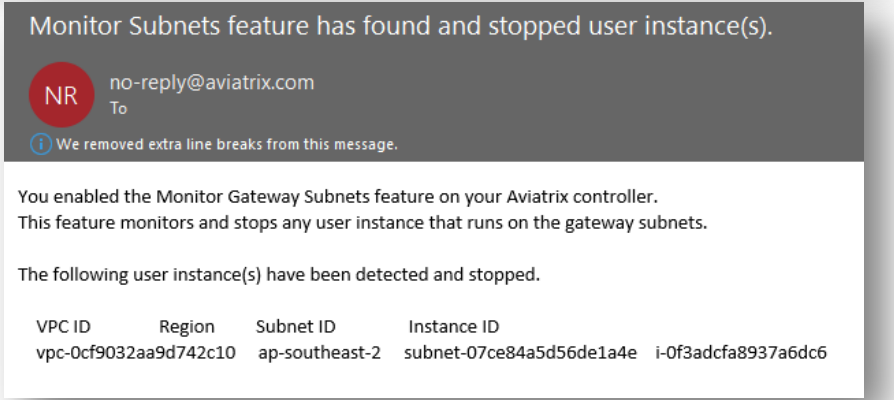


Instances to Exclude

Enter Instance Id to be excluded from monitoring separated by comma. Leave it blank if you do not have any. Click OK to finish.



Monitor Gateway Subnets



Monitor Subnets feature has found and stopped user instance(s).

no-reply@aviatrix.com
To

ⓘ We removed extra line breaks from this message.

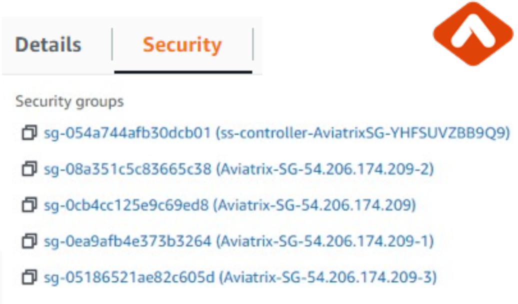
You enabled the Monitor Gateway Subnets feature on your Aviatrix controller.
This feature monitors and stops any user instance that runs on the gateway subnets.

The following user instance(s) have been detected and stopped.

VPC ID	Region	Subnet ID	Instance ID
vpc-0cf9032aa9d742c10	ap-southeast-2	subnet-07ce84a5d56de1a4e	i-0f3adcfa8937a6dc6

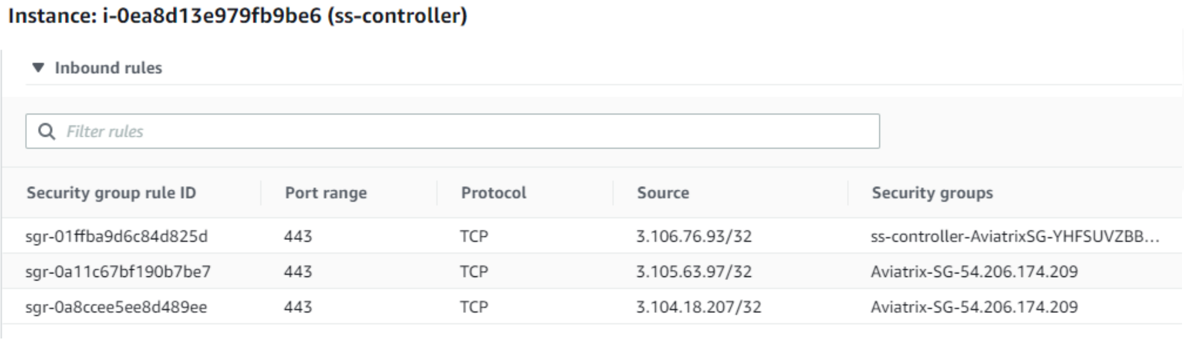
https://docs.aviatrix.com/HowTos/gateway.html#monitor-gateway-subnet

Controller Security Group Management | Automatic Security Group lockdown



Security groups

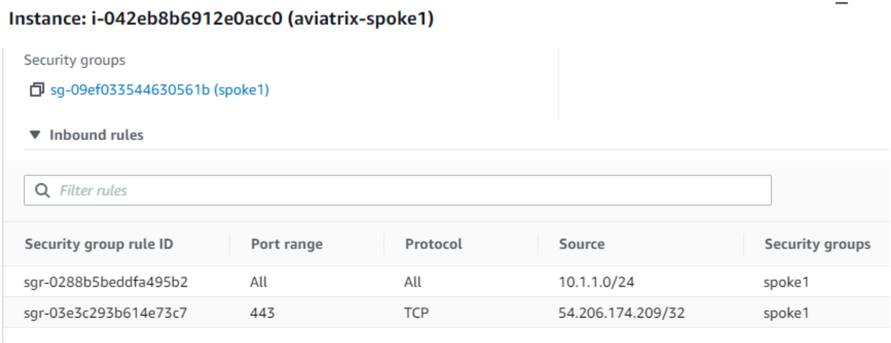
- sg-054a744afb30dcb01 (ss-controller-AviatrixSG-YHFSUVZBB9Q9)
- sg-08a351c5c83665c38 (Aviatrix-SG-54.206.174.209-2)
- sg-0cb4cc125e9c69ed8 (Aviatrix-SG-54.206.174.209)
- sg-0ea9afb4e373b3264 (Aviatrix-SG-54.206.174.209-1)
- sg-05186521ae82c605d (Aviatrix-SG-54.206.174.209-3)



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

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?

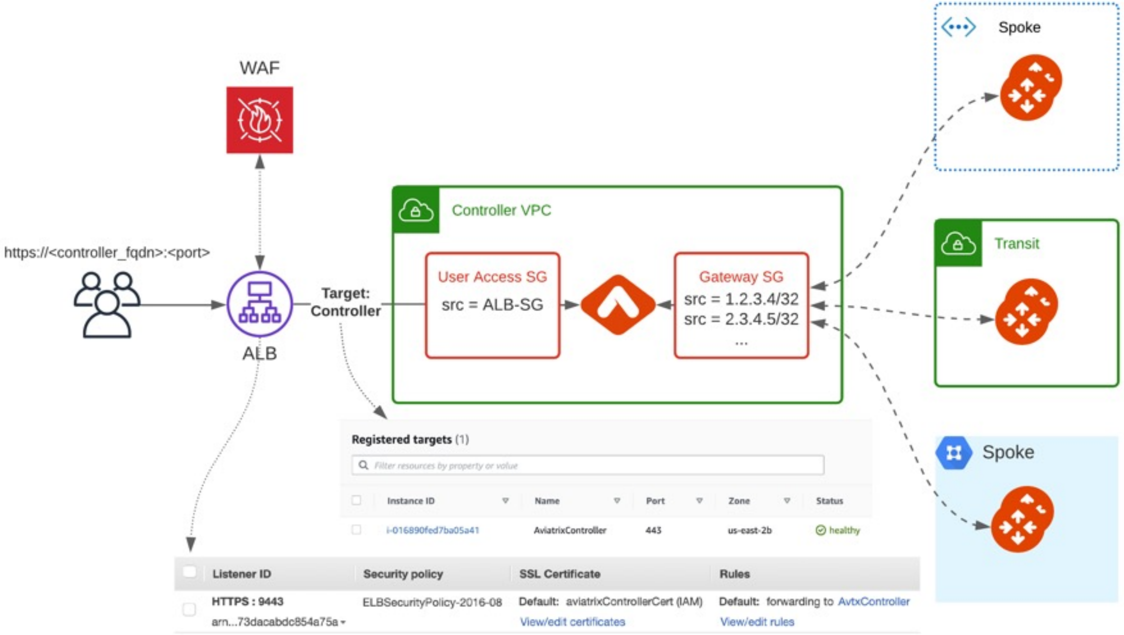
1. Limit access using cloud native L4 stateful firewalls such as:
   - AWS Security Groups
   - Azure Network Security Groups
   - GCP Firewall Rules
2. Deploy a third-party Firewall in front of controller
3. Deploy an Application (L7) Load Balancer in front of Aviatrix Controller

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

- Enable Controller Security Group Management to only allow access to the Controller EIP from Aviatrix Gateways
- 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)

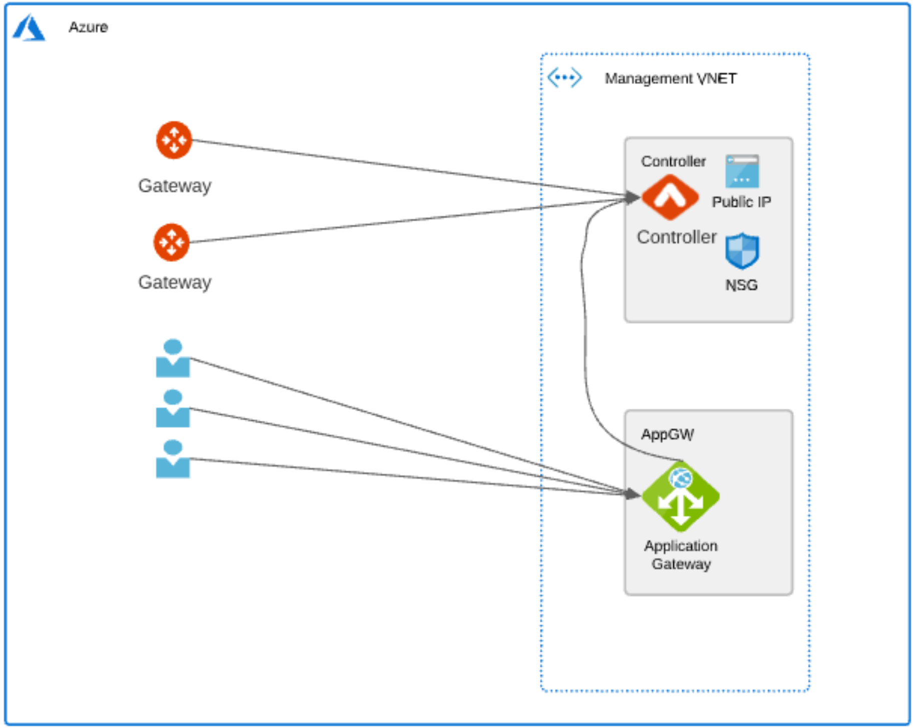
Filter resources by property or value

□	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

Azure

- Use WAF with Azure Managed rules on Application Gateway to limit usual web hacks/attacks against Controller
- Only allow user access from the Application Gateway subnet to Controller on port 443 (Controller Security Groups management feature is a pre-requisite for gateway communication to Controller)
- Allow configuring user access on non-standard HTTPS listener port
- Terminate SSL connection on Application Gateway to leverage cloud native certificate management and WAF capability to inspect and log requests
- L7 health-check on the Controller



Egress

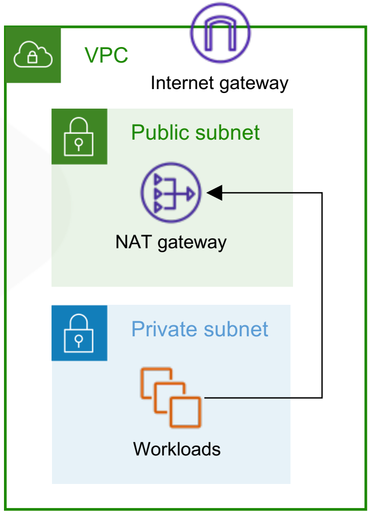
Problem Statement

Private workloads need internet access

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

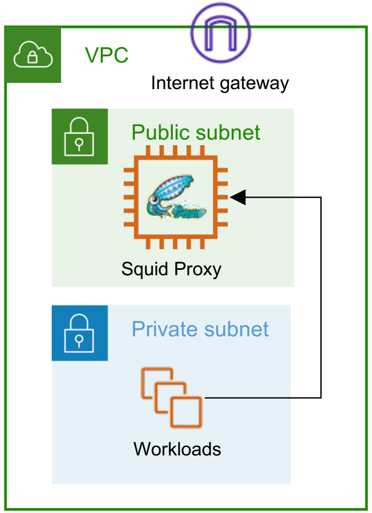
NAT Gateway

- NACLs management
- Layer-4 only



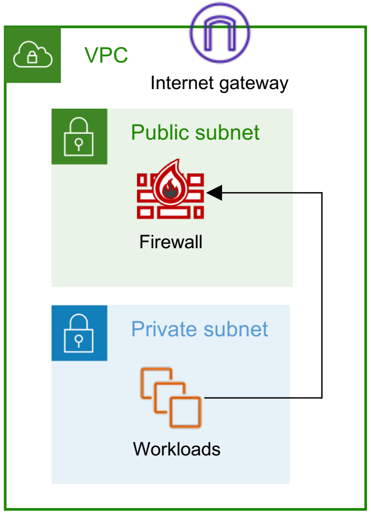
Squid Proxy

- Hard to manage
- Scale and HA issues

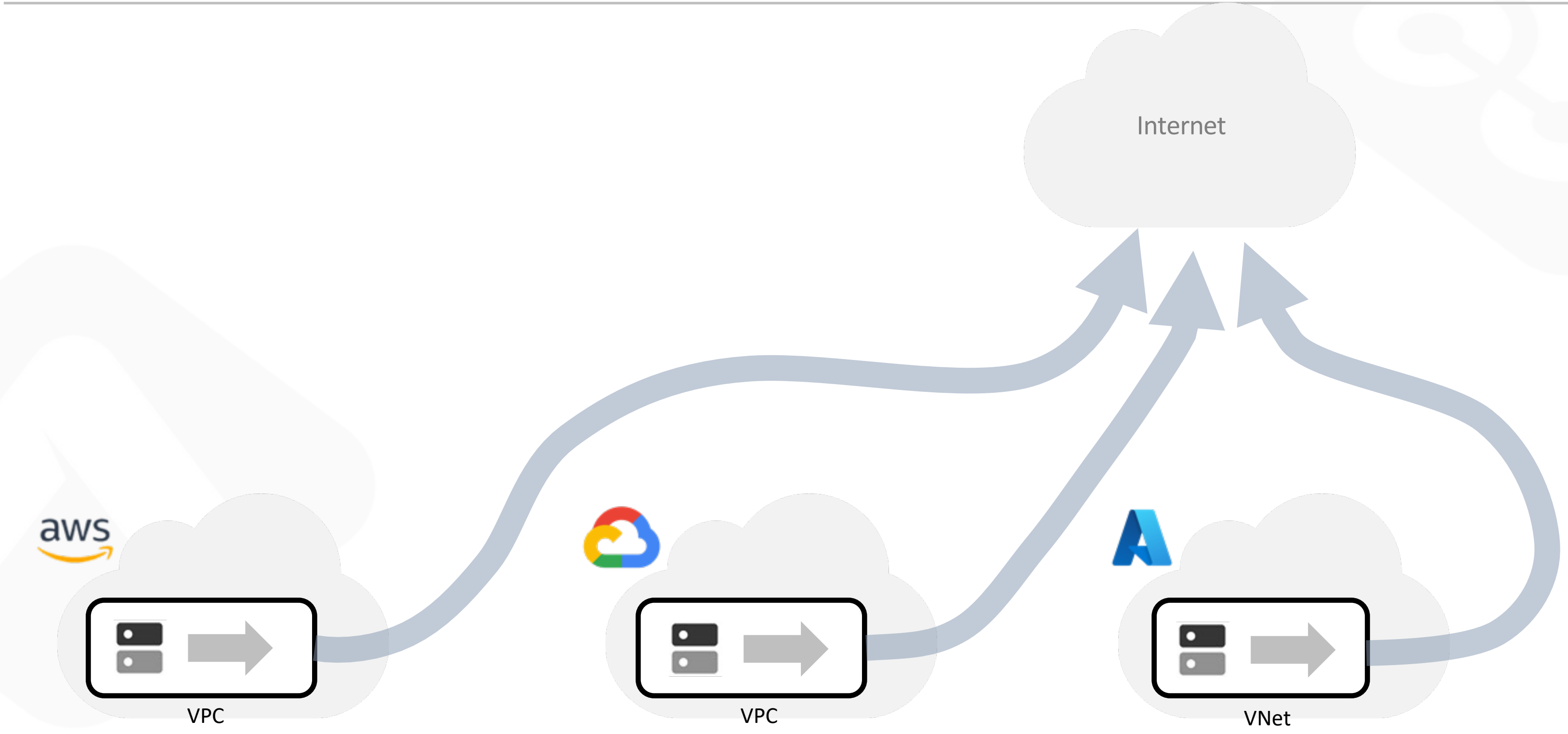


Layer-7 Firewall

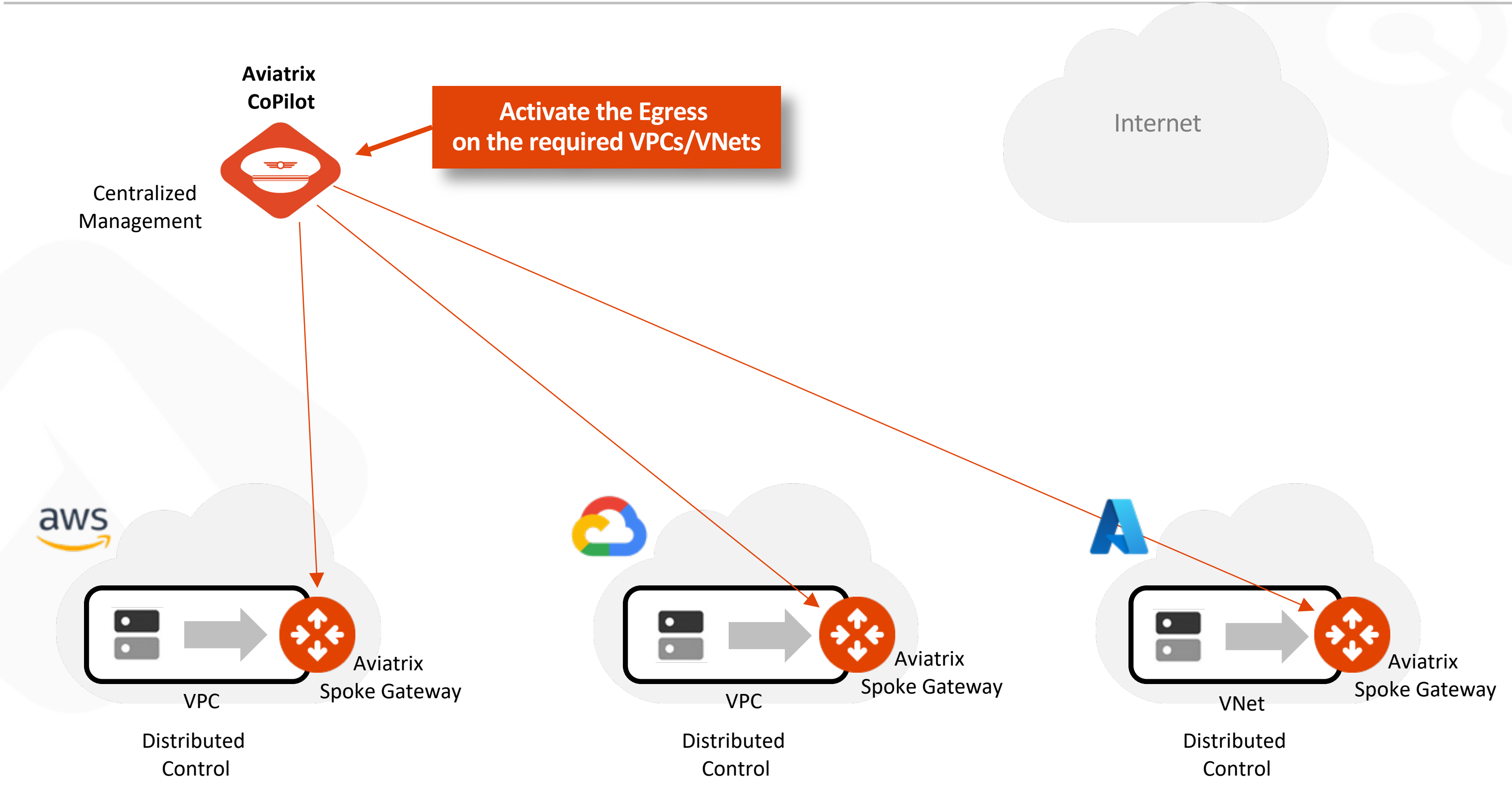
- Overkill
- Expensive



Aviatrix Secure Egress Filtering Feature



Aviatrix Secure Egress Filtering

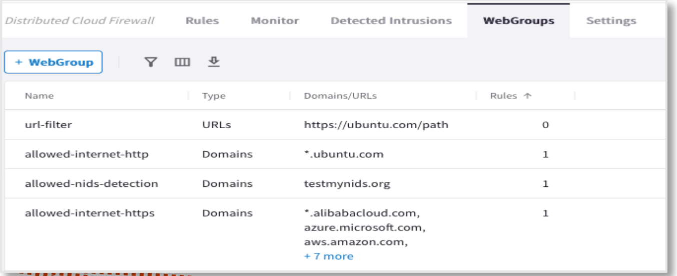


Aviatrix Secure Egress Filtering

Aviatrix CoPilot

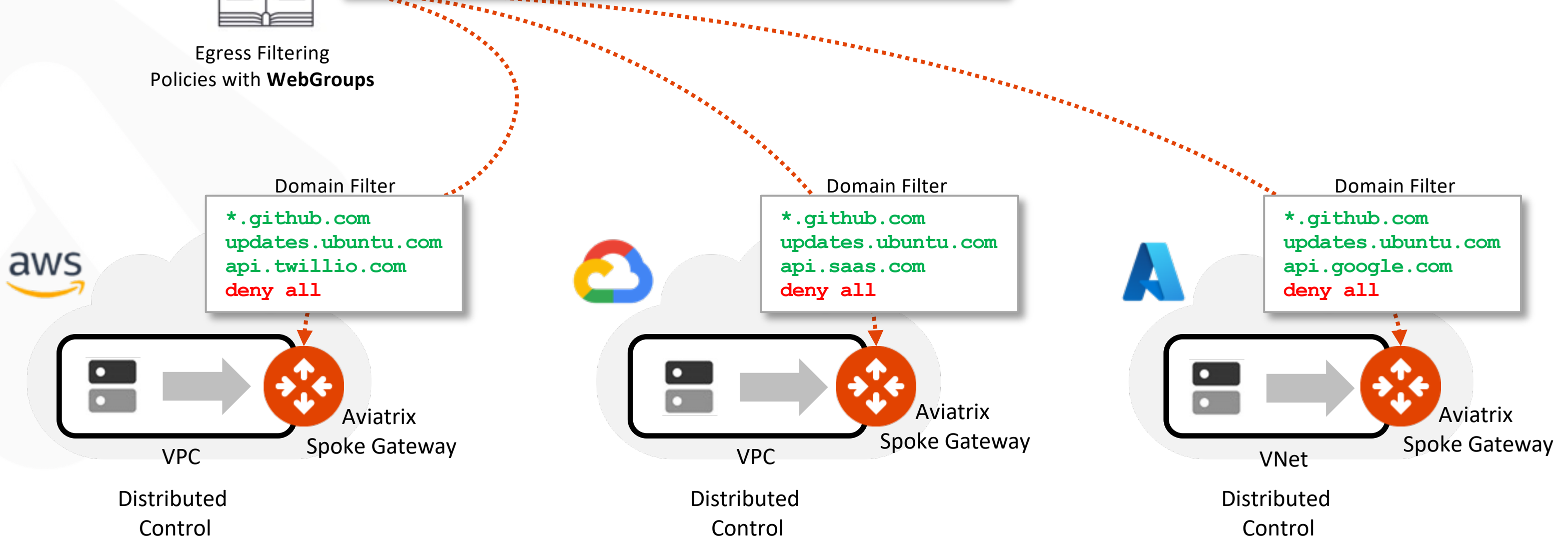
Centralized Management

Egress Filtering Policies with **WebGroups**

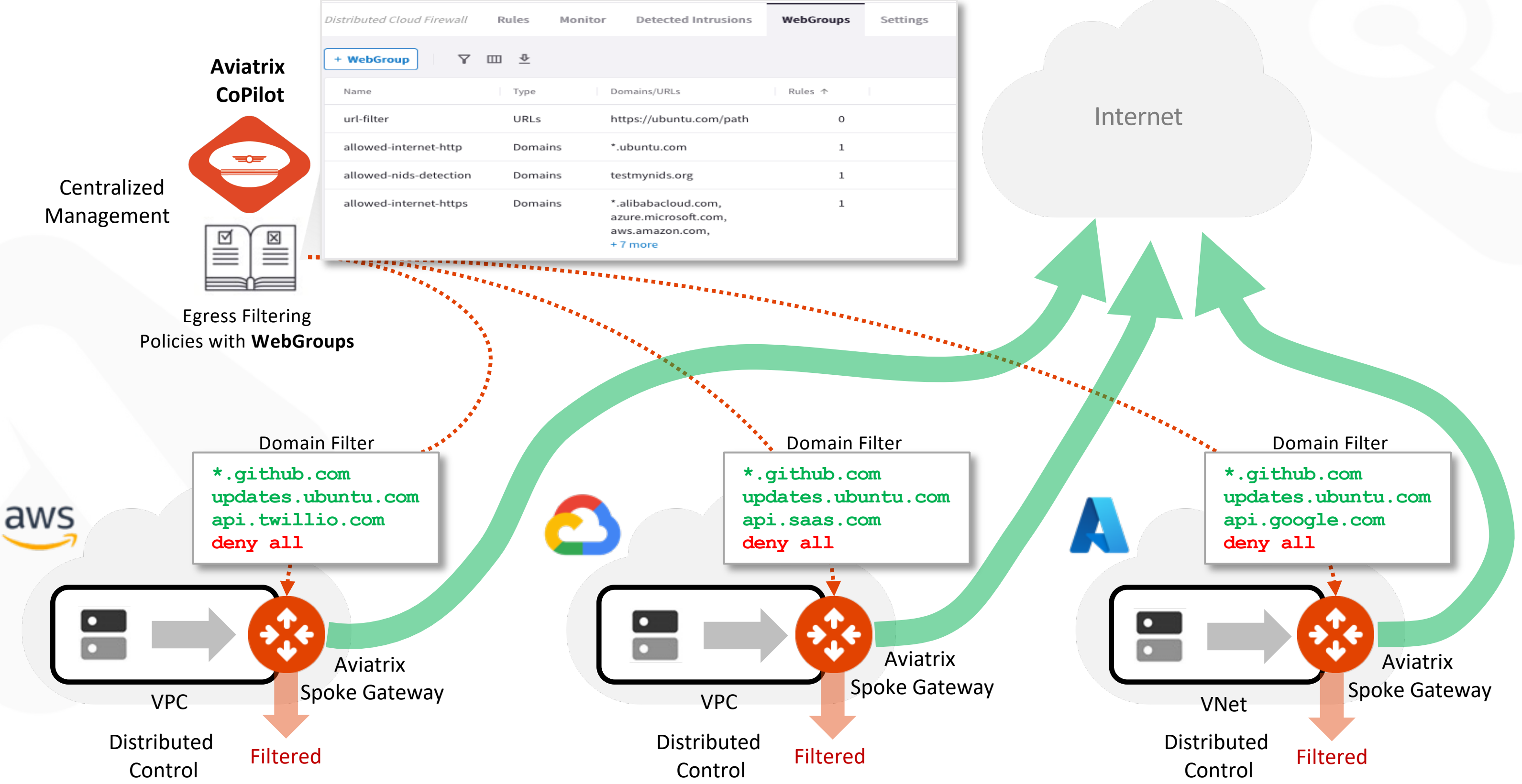


Name	Type	Domains/URLs	Rules ↑
url-filter	URLs	https://ubuntu.com/path	0
allowed-internet-http	Domains	*.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-internet-https	Domains	*.alibabacloud.com, azure.microsoft.com, aws.amazon.com, + 7 more	1

Internet



Aviatrix Secure Egress Filtering



Name	Type	Domains/URLs	Rules ↑
url-filter	URLs	https://ubuntu.com/path	0
allowed-internet-http	Domains	*.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-internet-https	Domains	*.alibabacloud.com, azure.microsoft.com, aws.amazon.com, + 7 more	1

Domain Filter

```
*.github.com
updates.ubuntu.com
api.twillio.com
deny all
```

Domain Filter

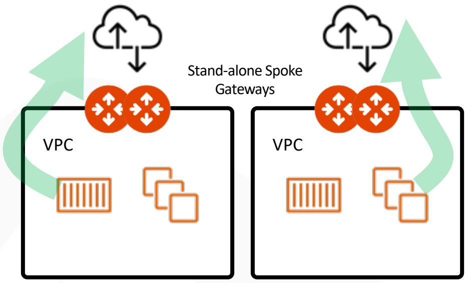
```
*.github.com
updates.ubuntu.com
api.saas.com
deny all
```

Domain Filter

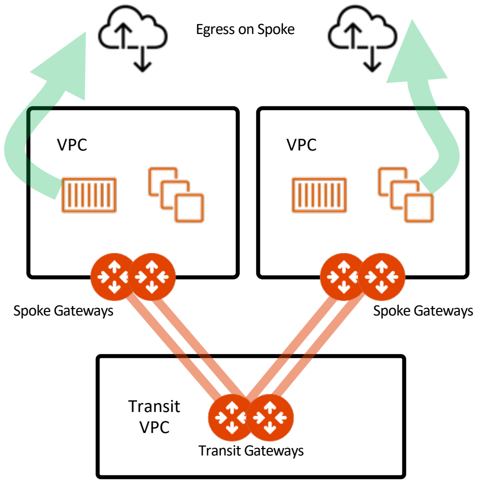
```
*.github.com
updates.ubuntu.com
api.google.com
deny all
```

Aviatrix Secure Egress Filtering Design Patterns

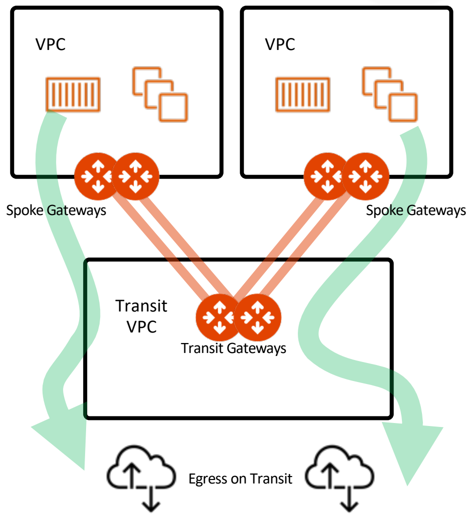
Stand-alone Spoke GW (Distributed)



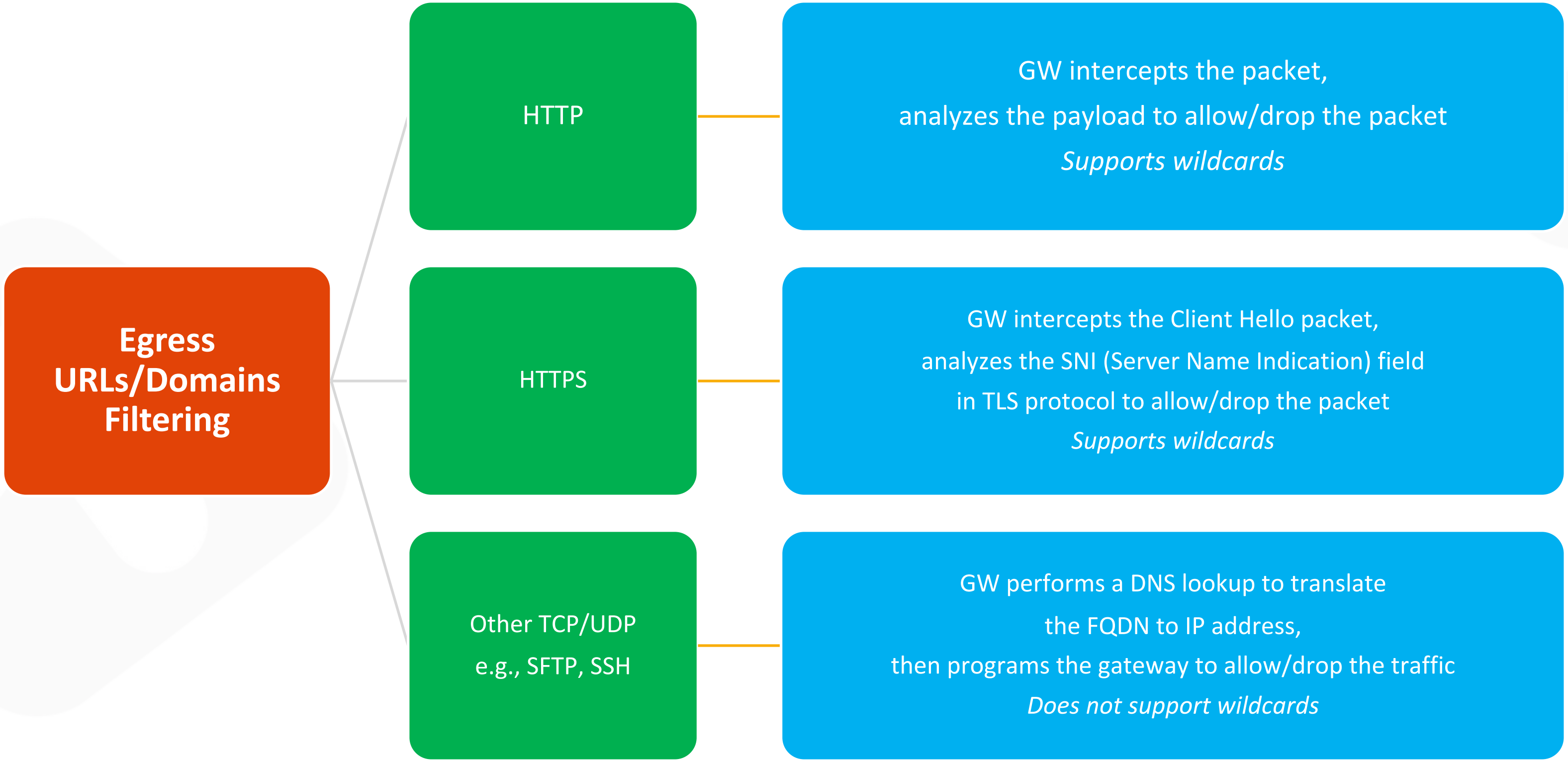
Local Egress (Distributed) with Aviatrix Spoke GW



Centralized Egress with Aviatrix Transit GW



Egress FQDN Filter – Traffic Types



Egress URLs/Domains Filtering

HTTP

GW intercepts the packet,
analyzes the payload to allow/drop the packet
Supports wildcards

HTTPS

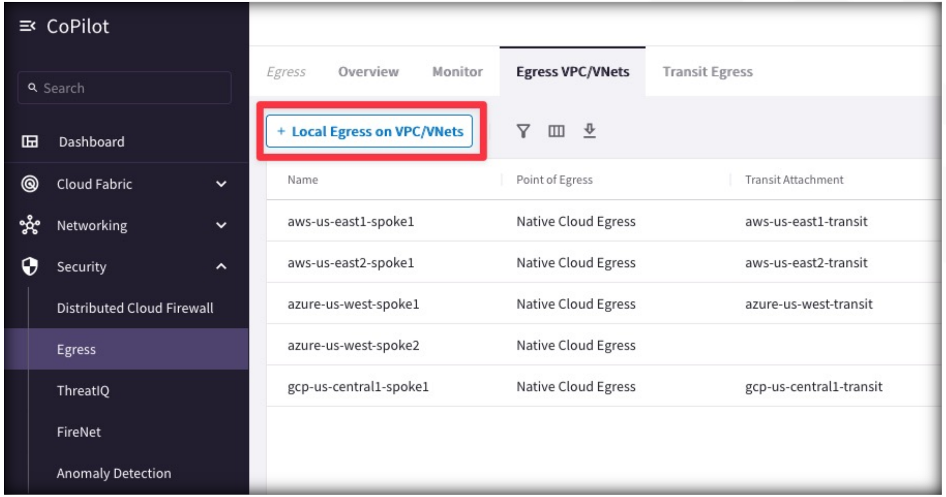
GW intercepts the Client Hello packet,
analyzes the SNI (Server Name Indication) field
in TLS protocol to allow/drop the packet
Supports wildcards

Other TCP/UDP
e.g., SFTP, SSH

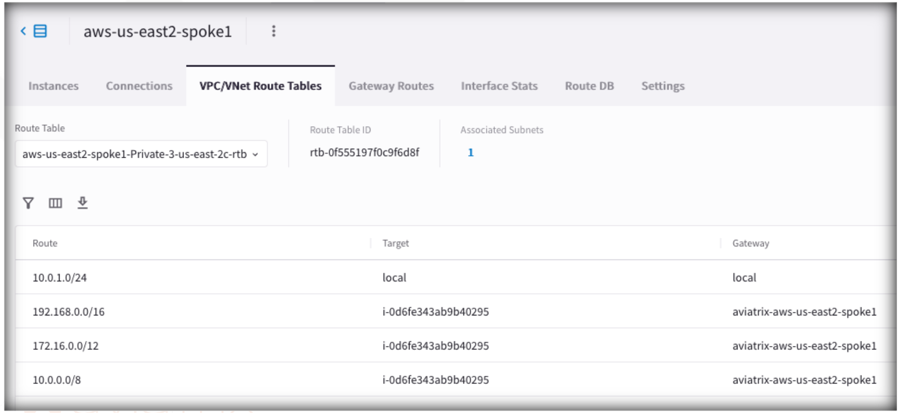
GW performs a DNS lookup to translate
the FQDN to IP address,
then programs the gateway to allow/drop the traffic
Does not support wildcards

Enabling Egress

- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- Egress Control also <u>requires additional resources</u> on the Spoke Gateway (i.e. scale up the VM size).
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be injected.



Name	Point of Egress	Transit Attachment
aws-us-east1-spoke1	Native Cloud Egress	aws-us-east1-transit
aws-us-east2-spoke1	Native Cloud Egress	aws-us-east2-transit
azure-us-west-spoke1	Native Cloud Egress	azure-us-west-transit
azure-us-west-spoke2	Native Cloud Egress	
gcp-us-central1-spoke1	Native Cloud Egress	gcp-us-central1-transit

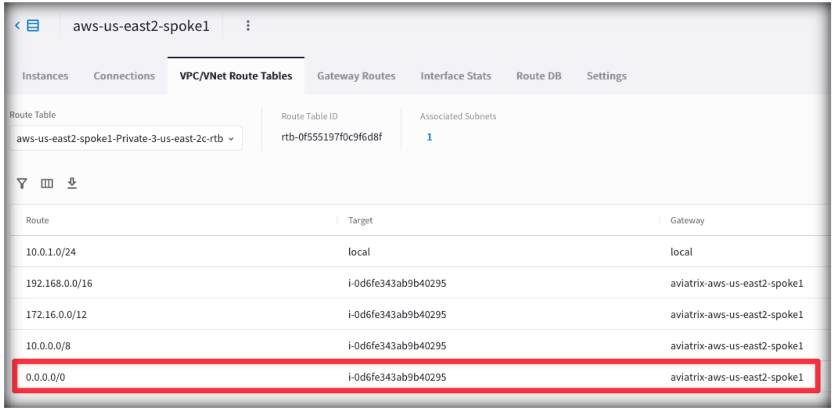


Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb

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



Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb

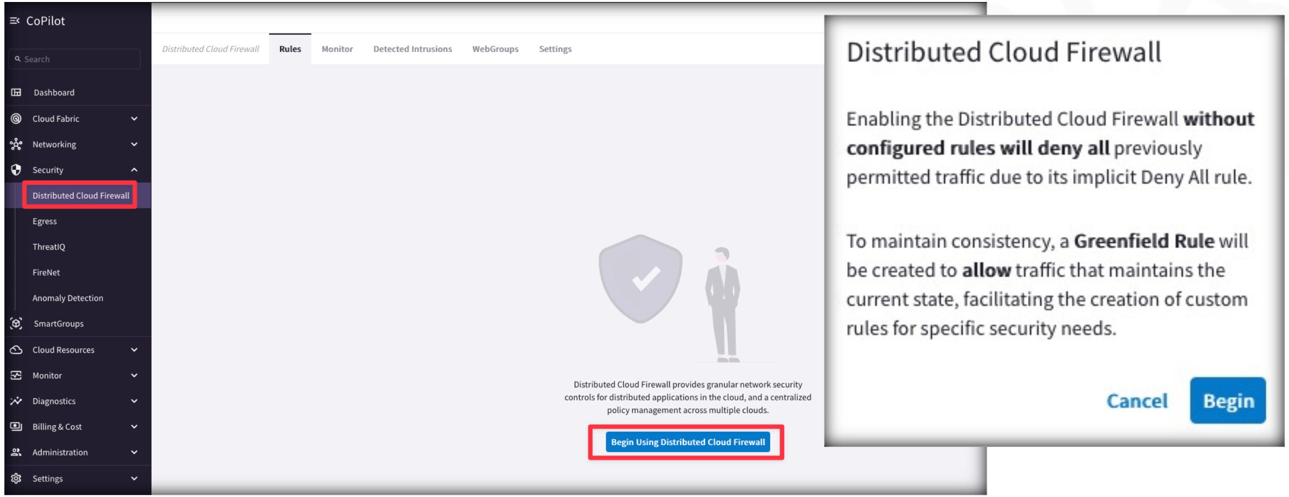
Route Table ID: rtb-0f555197f0c9f6d8f

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 = Deny-List Model

- The Egress control is part of the Distributed Cloud Firewall service.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.

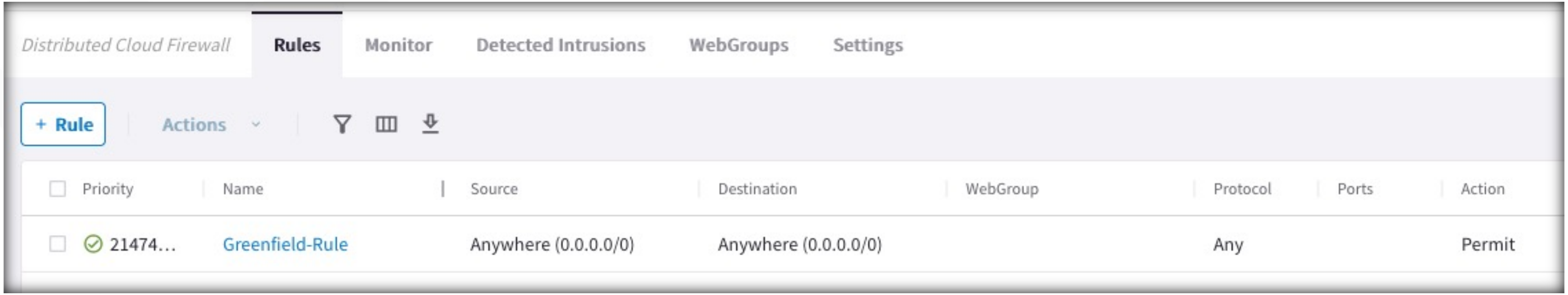


Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, and a centralized policy management across multiple clouds.

Distributed Cloud Firewall

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

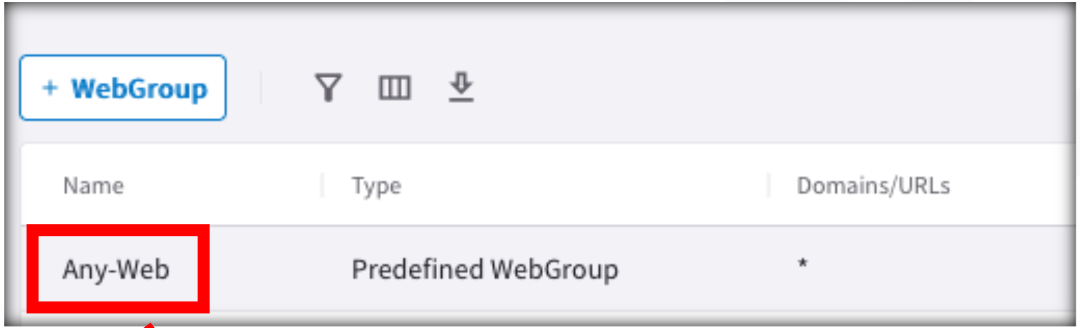
To maintain consistency, a **Greenfield Rule** will be created to **allow** traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.



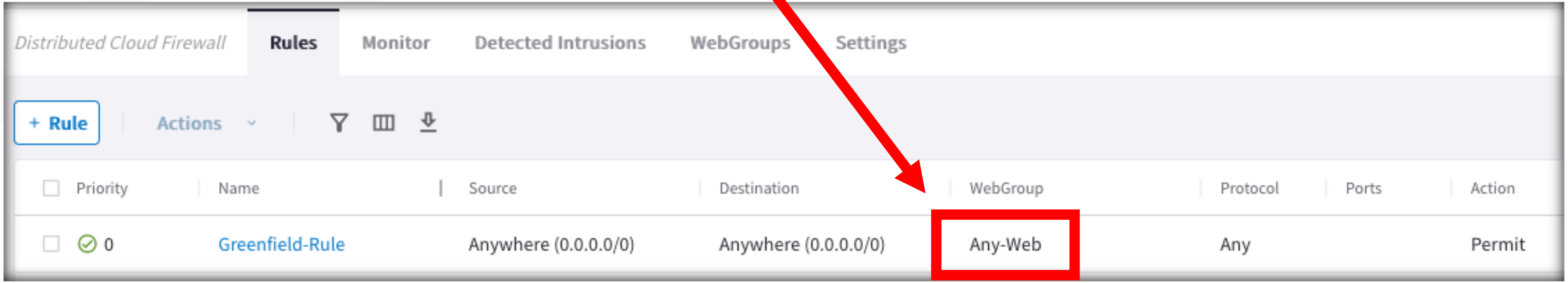
□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
□	✓ 21474...	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit

Discovery Mode = Greenfield-Rule + Any-Web (part.1)

- When you navigate to **Security > Distributed Cloud Firewall > WebGroups**, a predefined WebGroup, *Any-Web*, has already been created for you.
- If you attach this predefined WebGroup to the Greenfield-Rule you can log the FQDNs that are being accessed



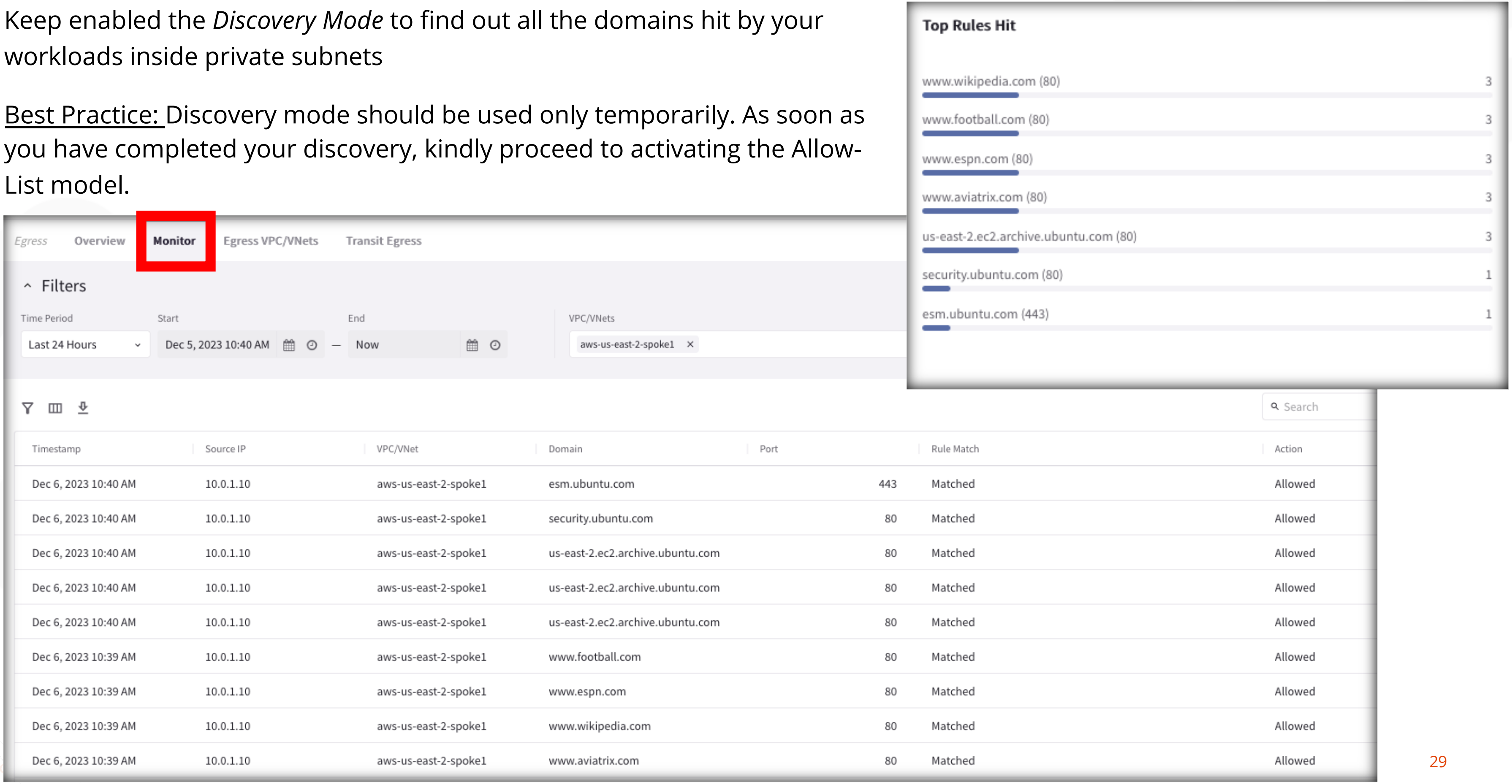
Name	Type	Domains/URLs
Any-Web	Predefined WebGroup	*



☐	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
☐	✓ 0	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)	Any-Web	Any		Permit

Discovery Mode = Greenfield-Rule + Any-Web (part.2)

- Keep enabled the *Discovery Mode* to find out all the domains hit by your workloads inside private subnets
- Best Practice: Discovery mode should be used only temporarily. As soon as you have completed your discovery, kindly proceed to activating the Allow-List model.



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

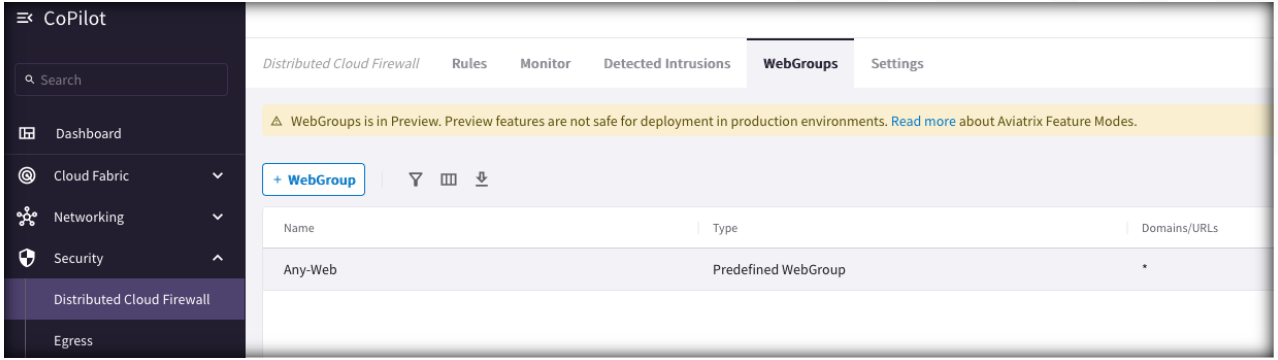
Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	esm.ubuntu.com	443	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	security.ubuntu.com	80	Matched	Allowed
Dec 6, 2023 10:40 AM	10.0.1.10	aws-us-east-2-spoke1	us-east-2.ec2.archive.ubuntu.com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

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

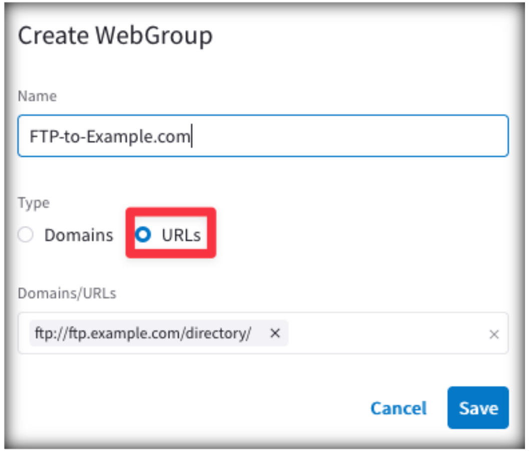
WebGroup Creation

- **WebGroups** are groupings of domains and URLs, inserted into Distributed Cloud Firewall rules, that filter (and provide security to) Internet-bound traffic.
- When you navigate to **Security > Distributed Cloud Firewall > WebGroups**, a predefined WebGroup, *Any-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.



⚠ WebGroups is in Preview. Preview features are not safe for deployment in production environments. Read more about Aviatrix Feature Modes.

Name	Type	Domains/URLs
Any-Web	Predefined WebGroup	*

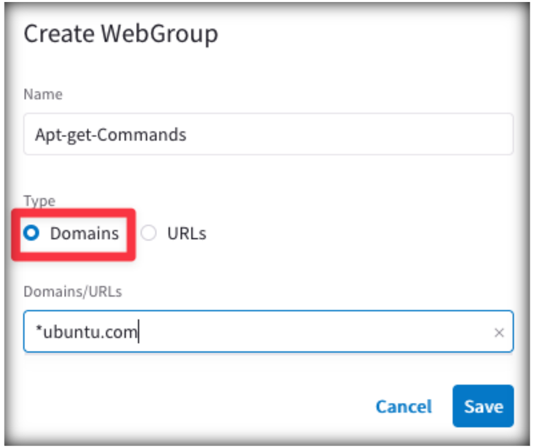


Create WebGroup

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

Lab 6 – Egress