Secure Egress

ACE Solutions Architecture Team

Problem Statement

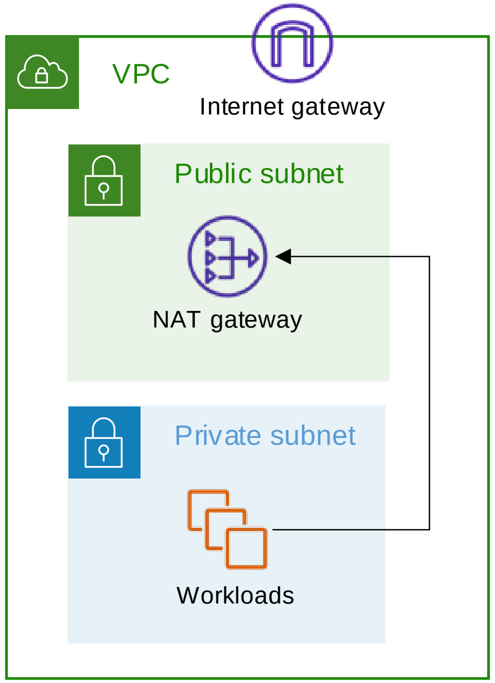
aviatrix ACE Aviatrix Certified Engineer

Private workloads need internet access

- SaaS integration
- Patching
- Updates

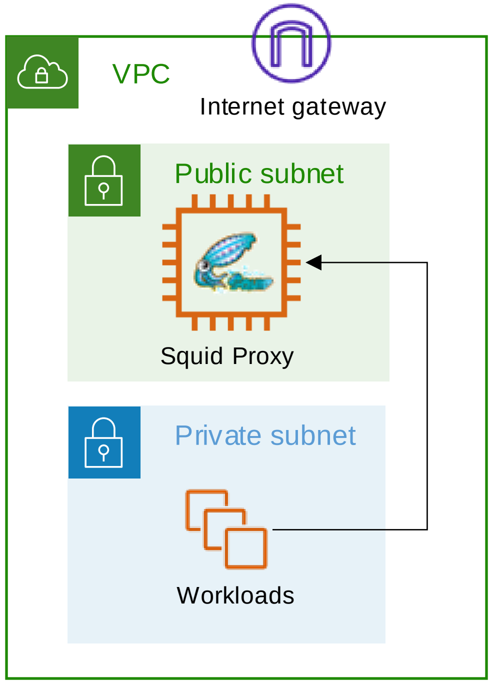
NAT Gateway

- Layer-4 only
- NACLs management



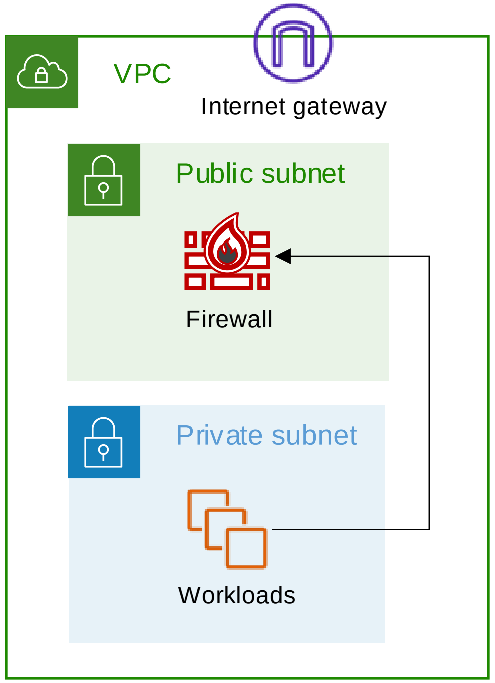
Squid Proxy

- Hard to manage
- Scale and HA issues

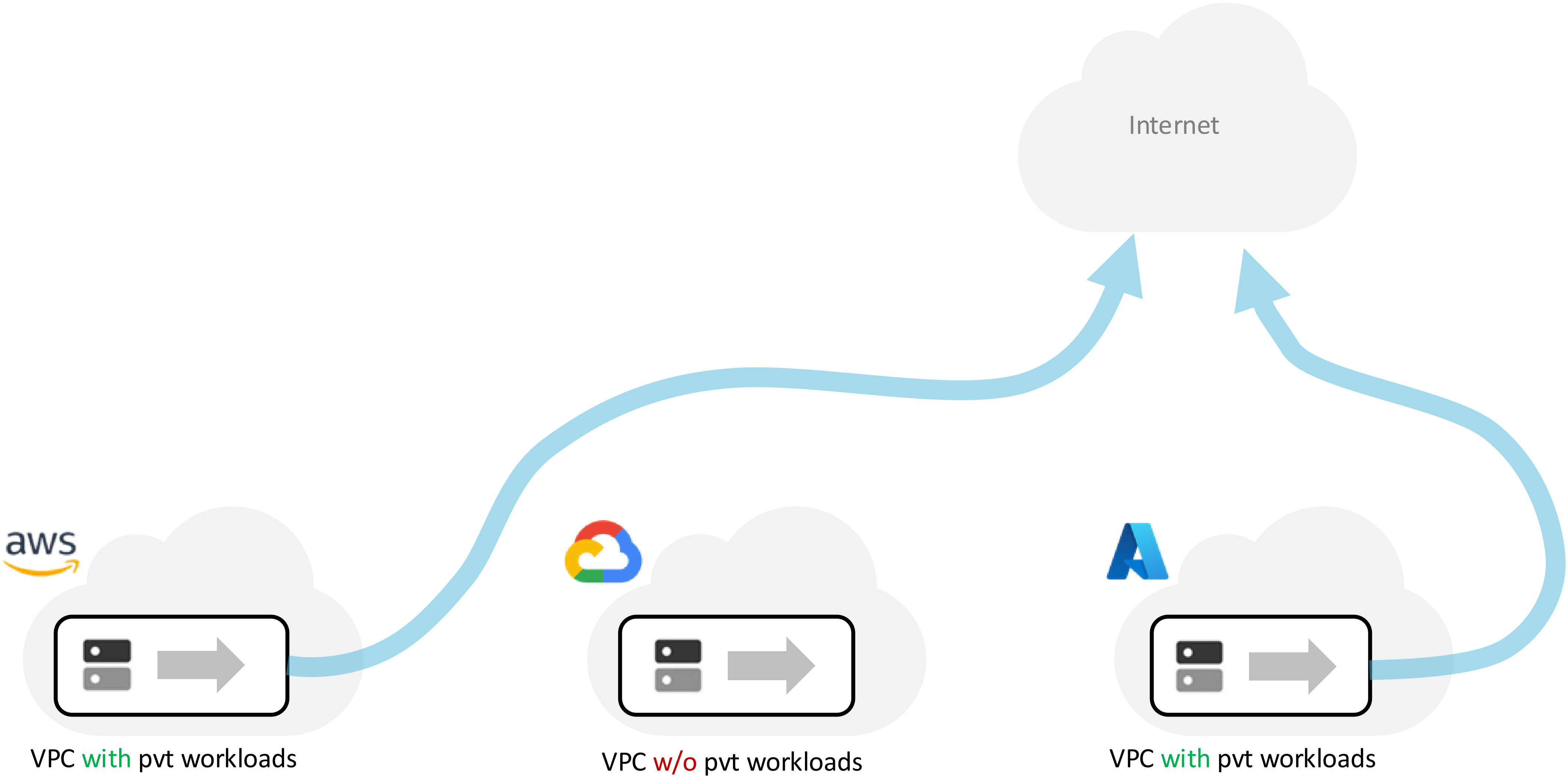


Layer-7 Firewall

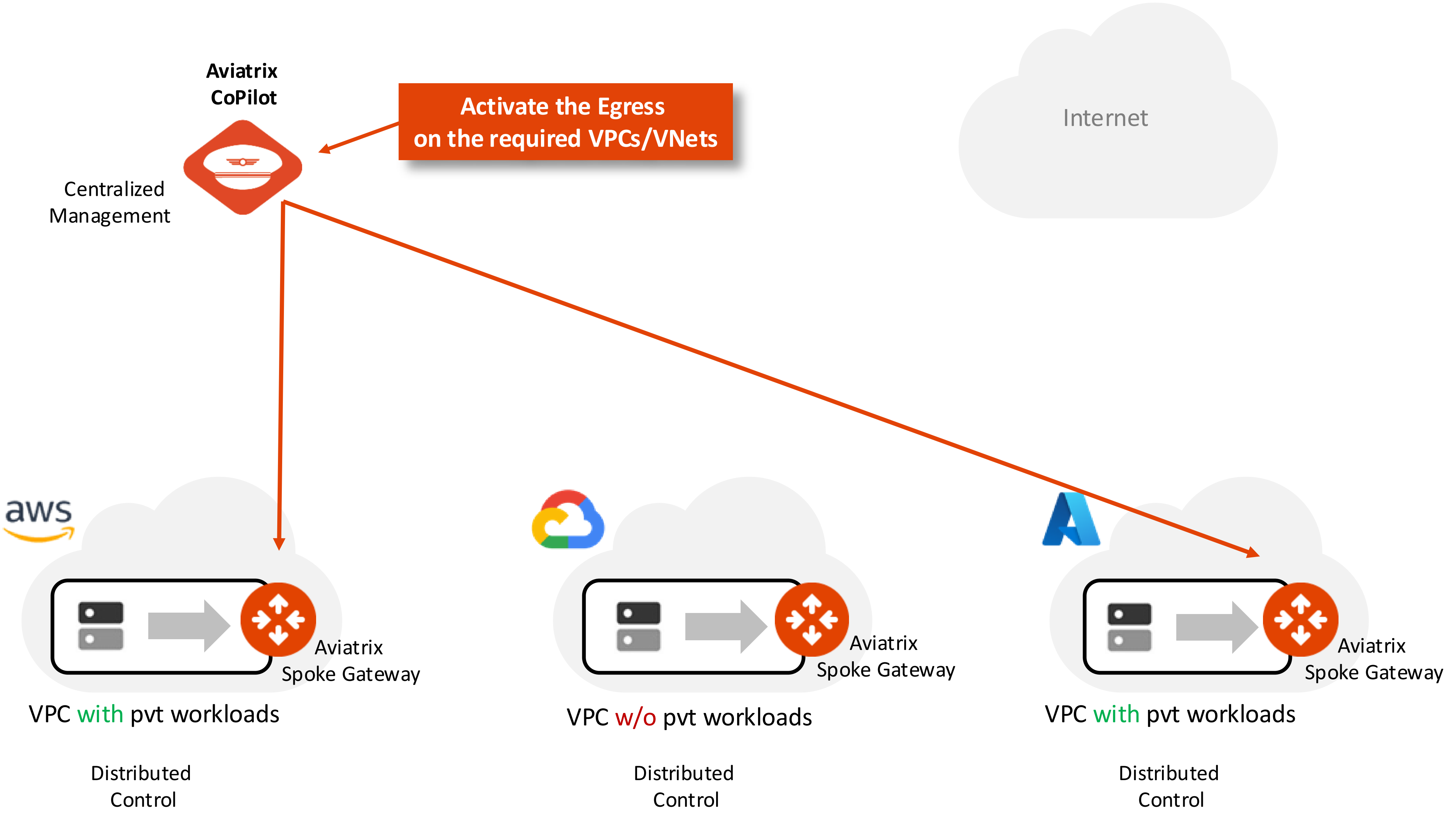
- Overkill
- Expensive



Aviatrix Secure Egress Filtering Feature



Aviatrix Secure Egress Filtering

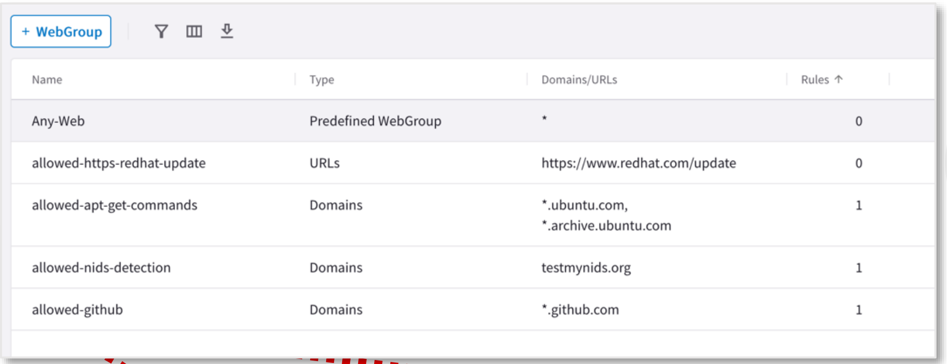


Activate the Egress on the required VPCs/VNets

Aviatrix Secure Egress Filtering

Aviatrix CoPilot

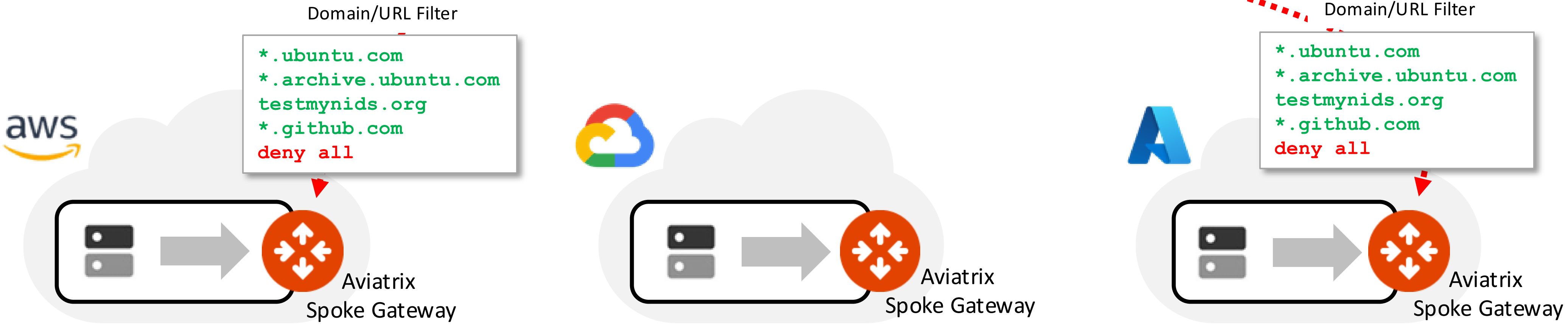
Centralized Management



Name	Type	Domains/URLs	Rules ↑
Any-Web	Predefined WebGroup	*	0
allowed-https-redhat-update	URLs	https://www.redhat.com/update	0
allowed-apt-get-commands	Domains	*.ubuntu.com, *.archive.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-github	Domains	*.github.com	1

Internet

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



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

Distributed Control

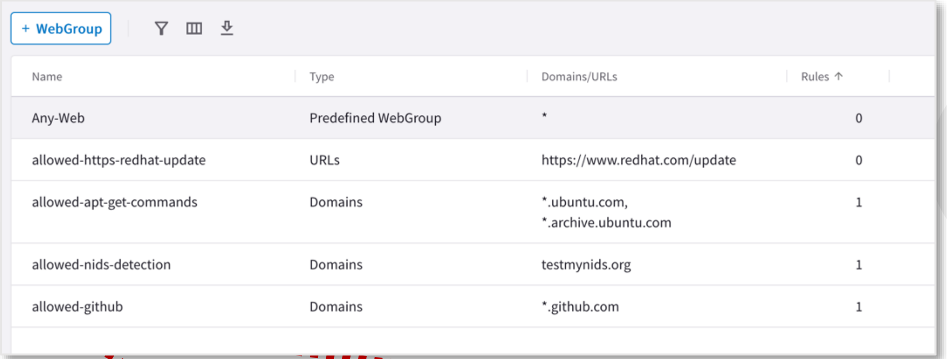
Distributed Control

Distributed Control

Aviatrix Secure Egress Filtering

Aviatrix CoPilot

Centralized Management

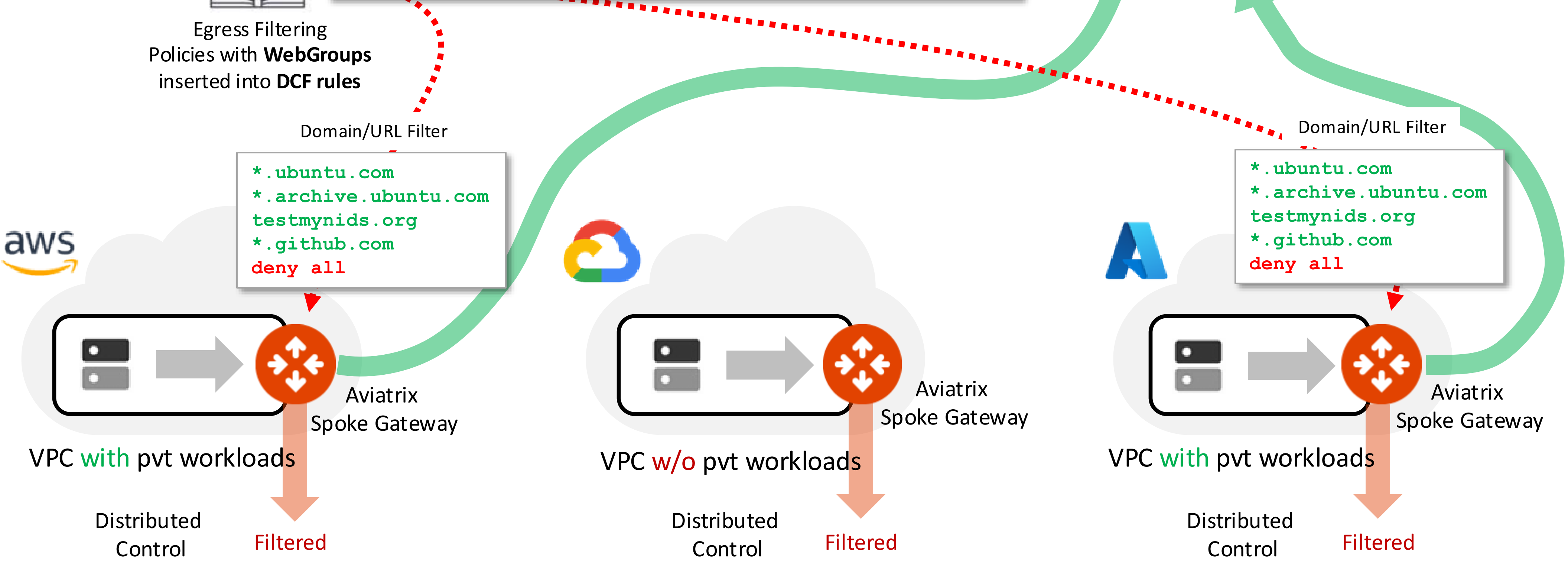


+ WebGroup

Name	Type	Domains/URLs	Rules ↑
Any-Web	Predefined WebGroup	*	0
allowed-https-redhat-update	URLs	https://www.redhat.com/update	0
allowed-apt-get-commands	Domains	*.ubuntu.com, *.archive.ubuntu.com	1
allowed-nids-detection	Domains	testmynids.org	1
allowed-github	Domains	*.github.com	1

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

Internet



Domain/URL Filter

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

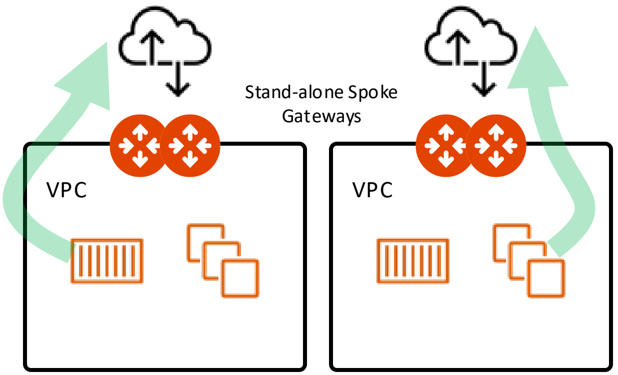
Domain/URL Filter

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

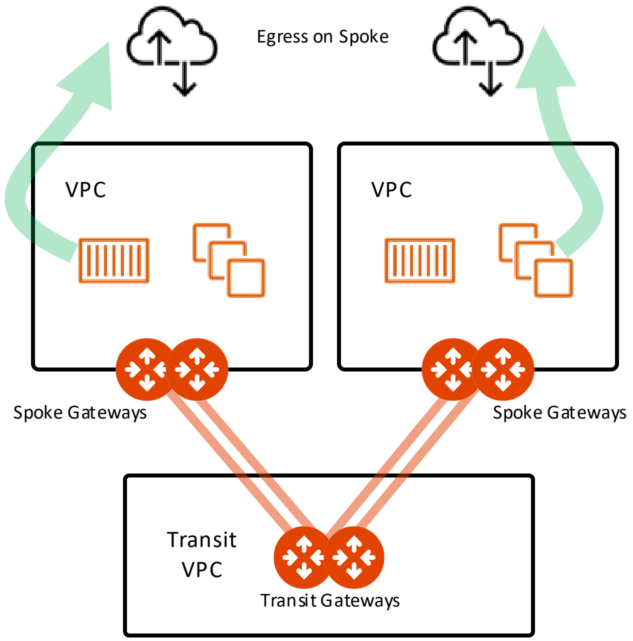
Aviatrix Secure Egress Filtering Design Patterns

aviatrix ACE Aviatrix Certified Engineer

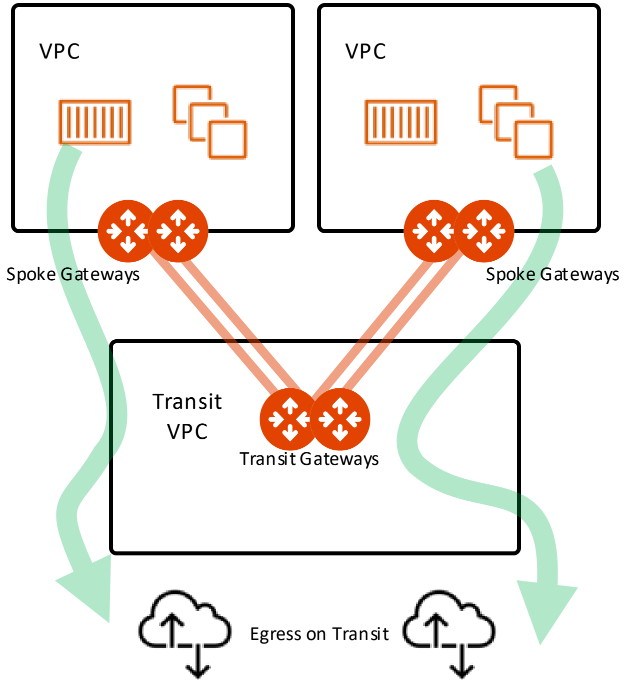
Stand-alone Spoke GW (Distributed)



Local Egress (Distributed) with Aviatrix Spoke GW



Centralized Egress with Aviatrix Transit GW



aviatrix

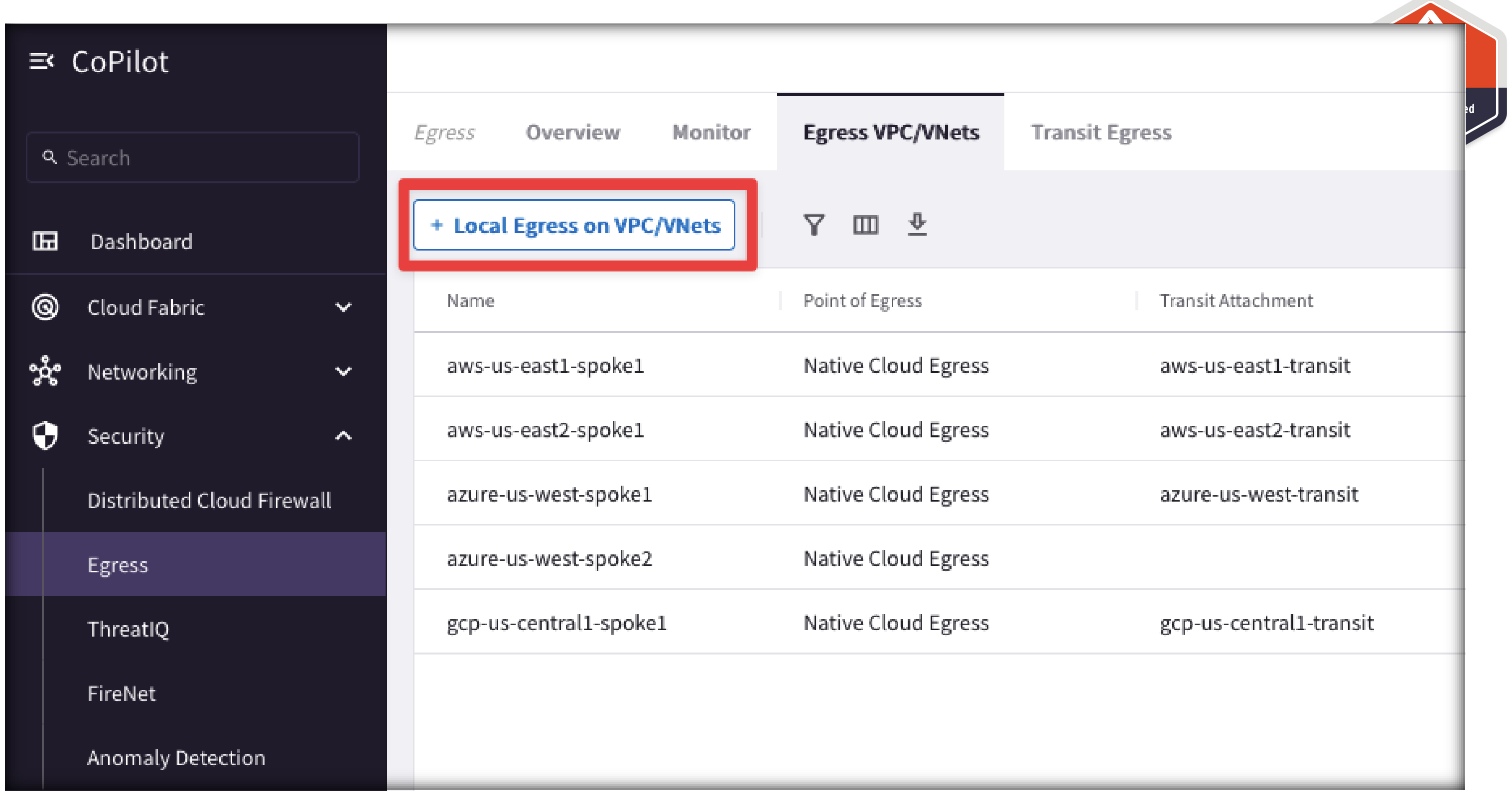
ACE

Aviatrix Certified Engineer

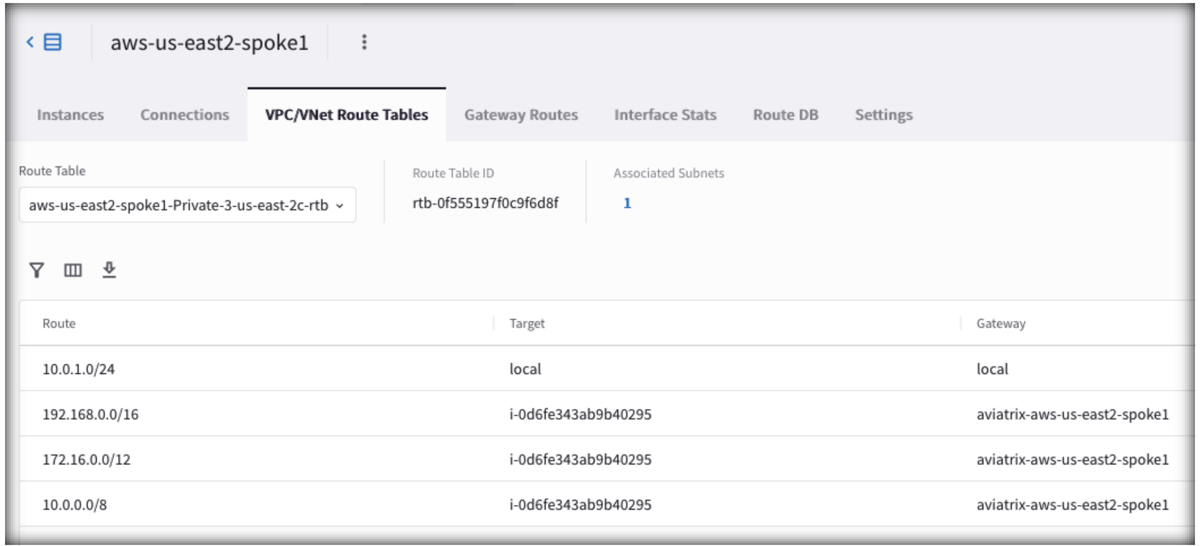
Tools for Troubleshooting Secure Egress

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

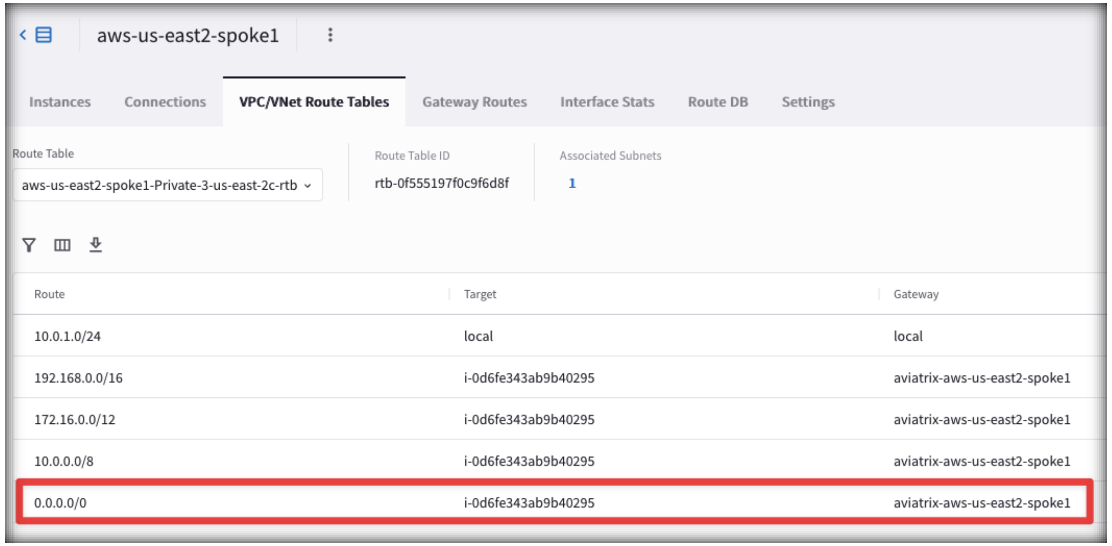


Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb

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

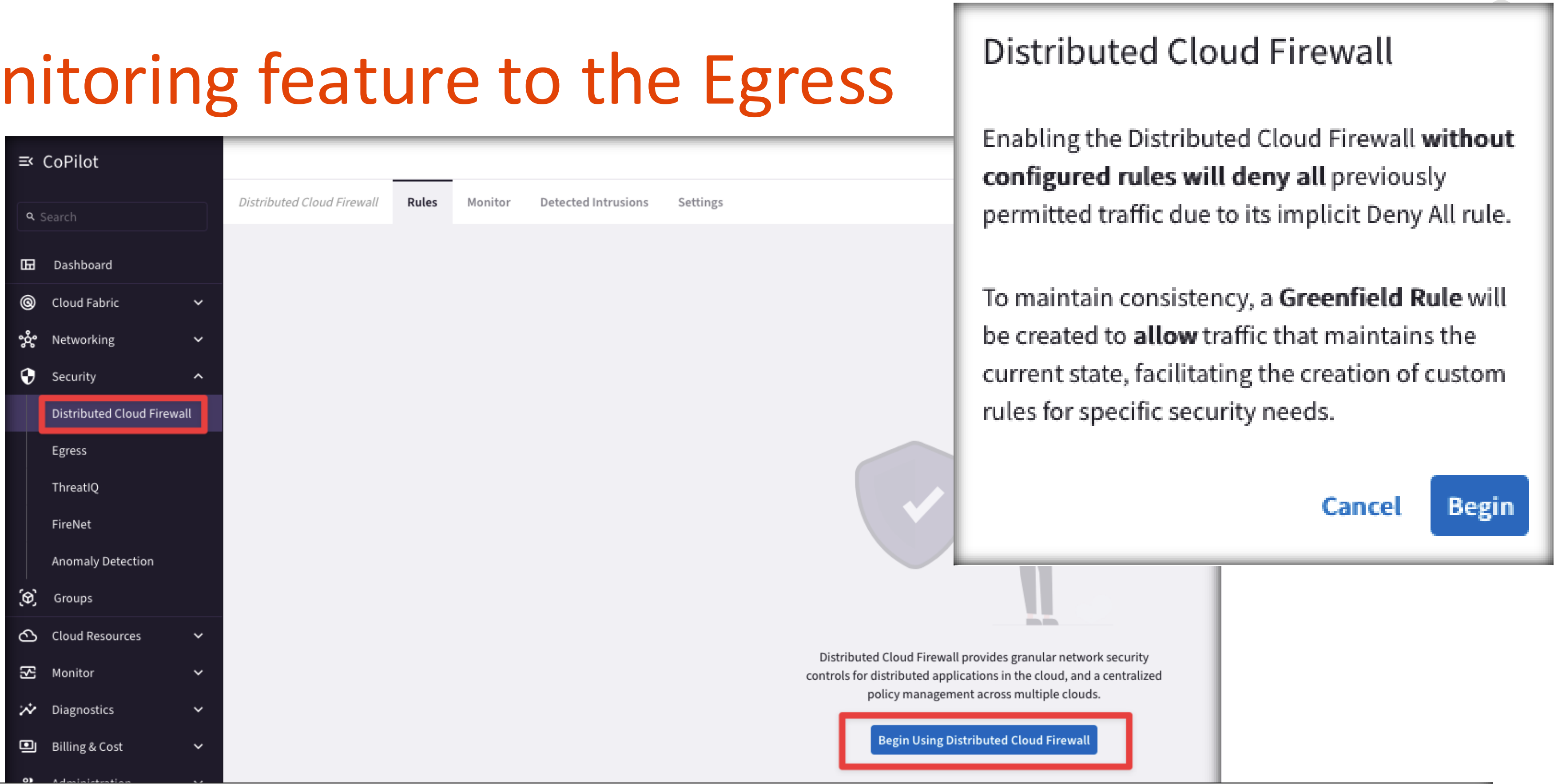
Route Table ID: rtb-0f555197f0c9f6d8f

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

Adding Filtering/Monitoring feature to the Egress

- 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.

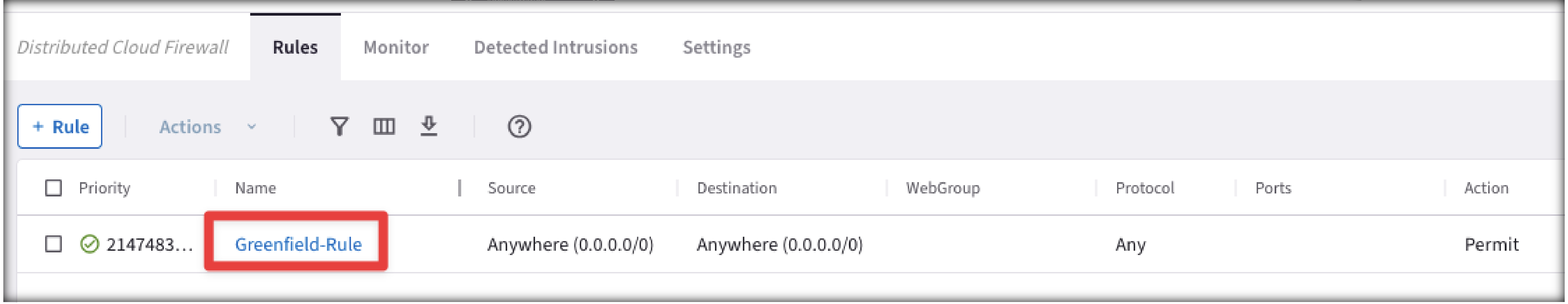


Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, and a centralized policy management across multiple clouds.

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.



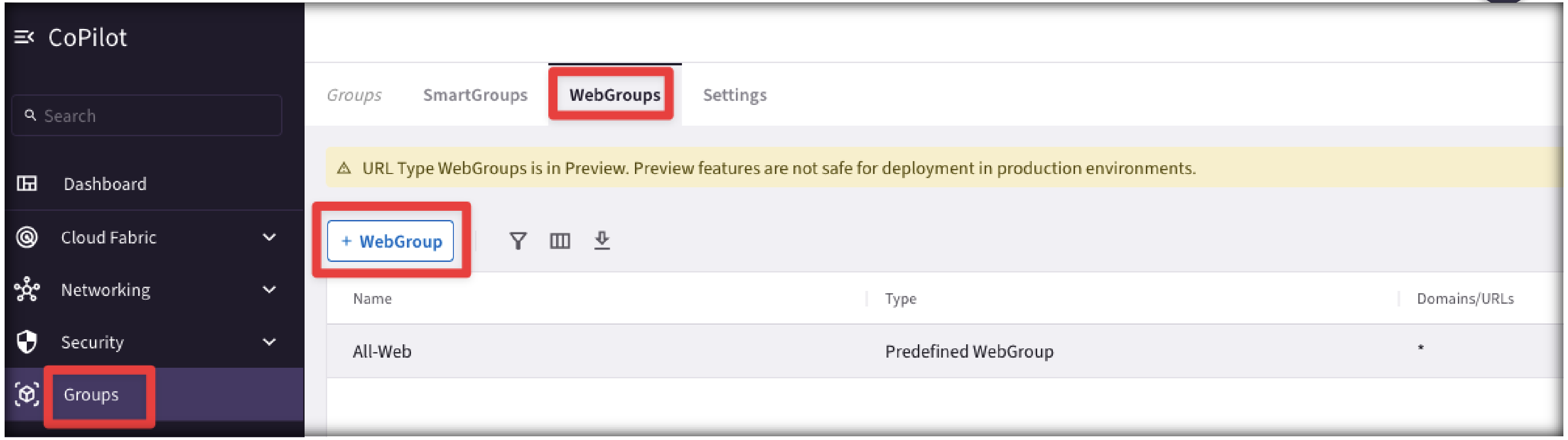
□ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
□ ✓ 2147483…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit

WebGroup Creation

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

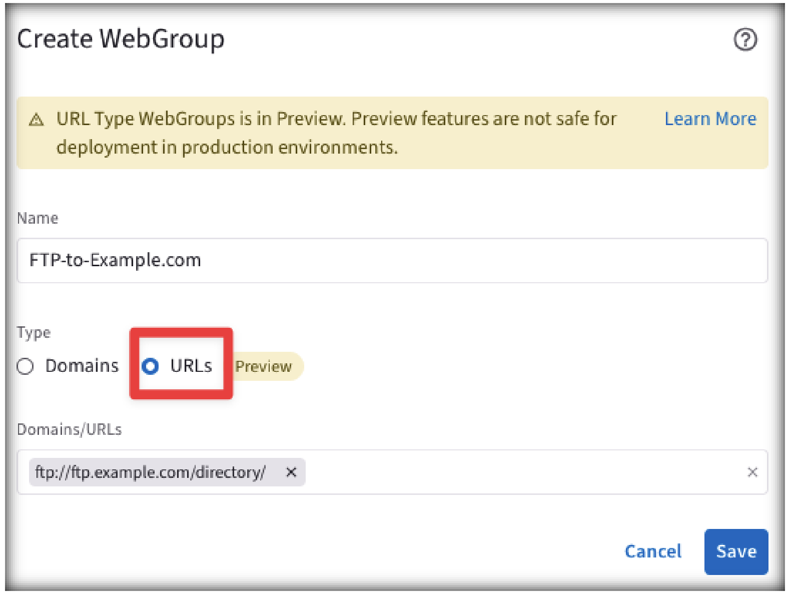
- In addition to the predefined WebGroup ***All-Web***, you can also create two kind of custom WebGroups:

  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	*



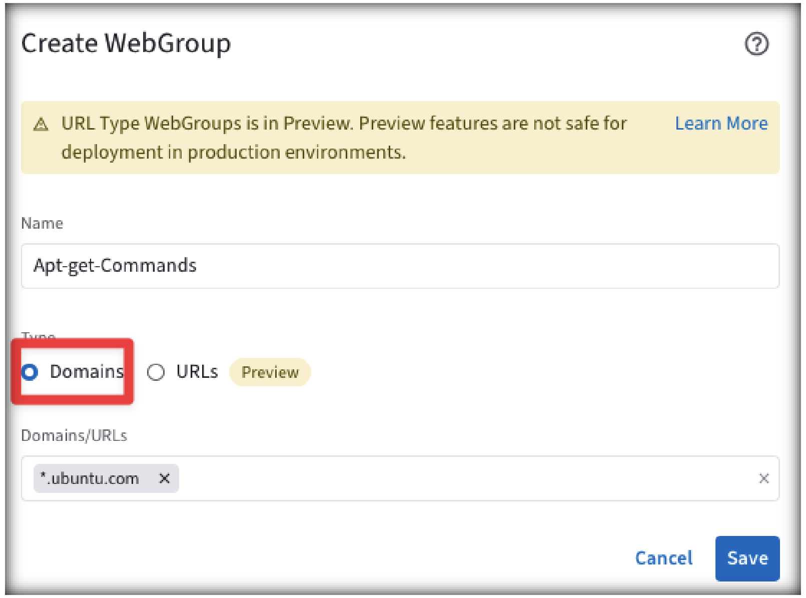
Create WebGroup

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

Name: FTP-to-Example.com

Type: ○ Domains ● URLs Preview

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



Create WebGroup

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

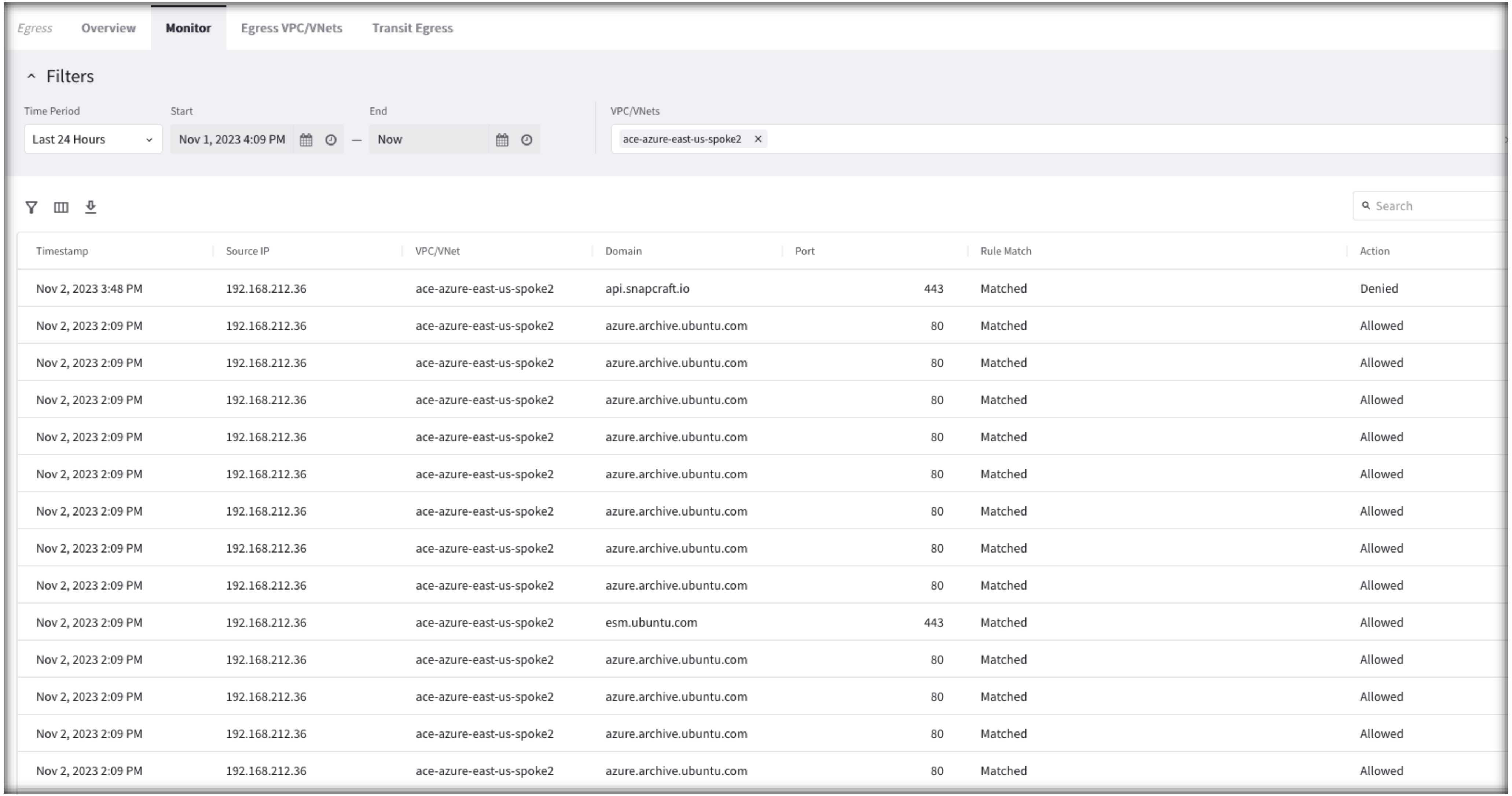
Name: Apt-get-Commands

Type: ● Domains ○ URLs Preview

Domains/URLs: *.ubuntu.com ×

Monitor

- **CoPilot > Security > Egress > Monitor**



Time Period: Last 24 Hours

Start: Nov 1, 2023 4:09 PM — End: Now

VPC/VNets: ace-azure-east-us-spoke2

Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
Nov 2, 2023 3:48 PM	192.168.212.36	ace-azure-east-us-spoke2	api.snapcraft.io	443	Matched	Denied
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	esm.ubuntu.com	443	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed
Nov 2, 2023 2:09 PM	192.168.212.36	ace-azure-east-us-spoke2	azure.archive.ubuntu.com	80	Matched	Allowed

aviatrix

ACE

Aviatrix Certified Engineer

Next:

Lab 7 Secure Egress