



## Secure Egress

ACE Solutions Architecture Team

# Problem Statement

## Private workloads need internet access

- SaaS integration



- Patching

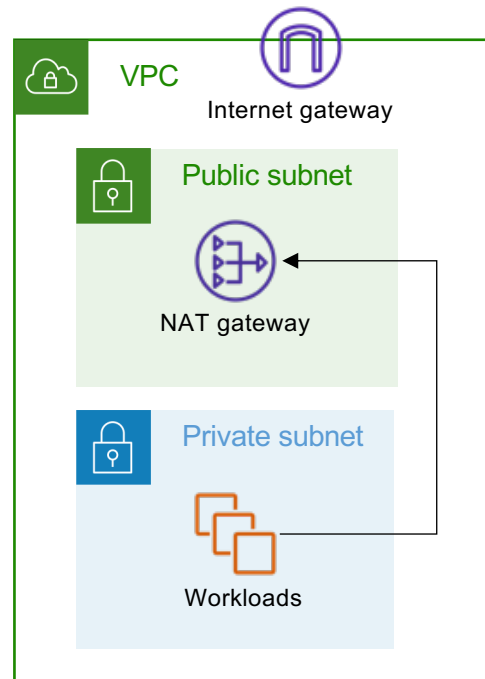


- Updates



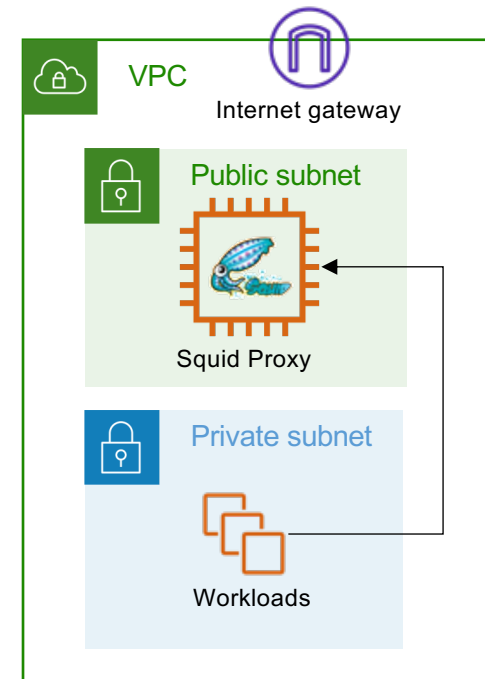
### NAT Gateway

- Layer-4 only
- NACLs management



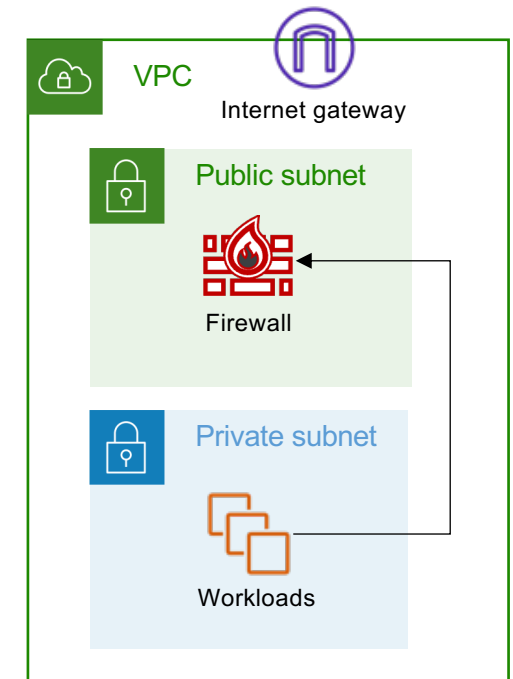
### Squid Proxy

- Hard to manage
- Scale and HA issues

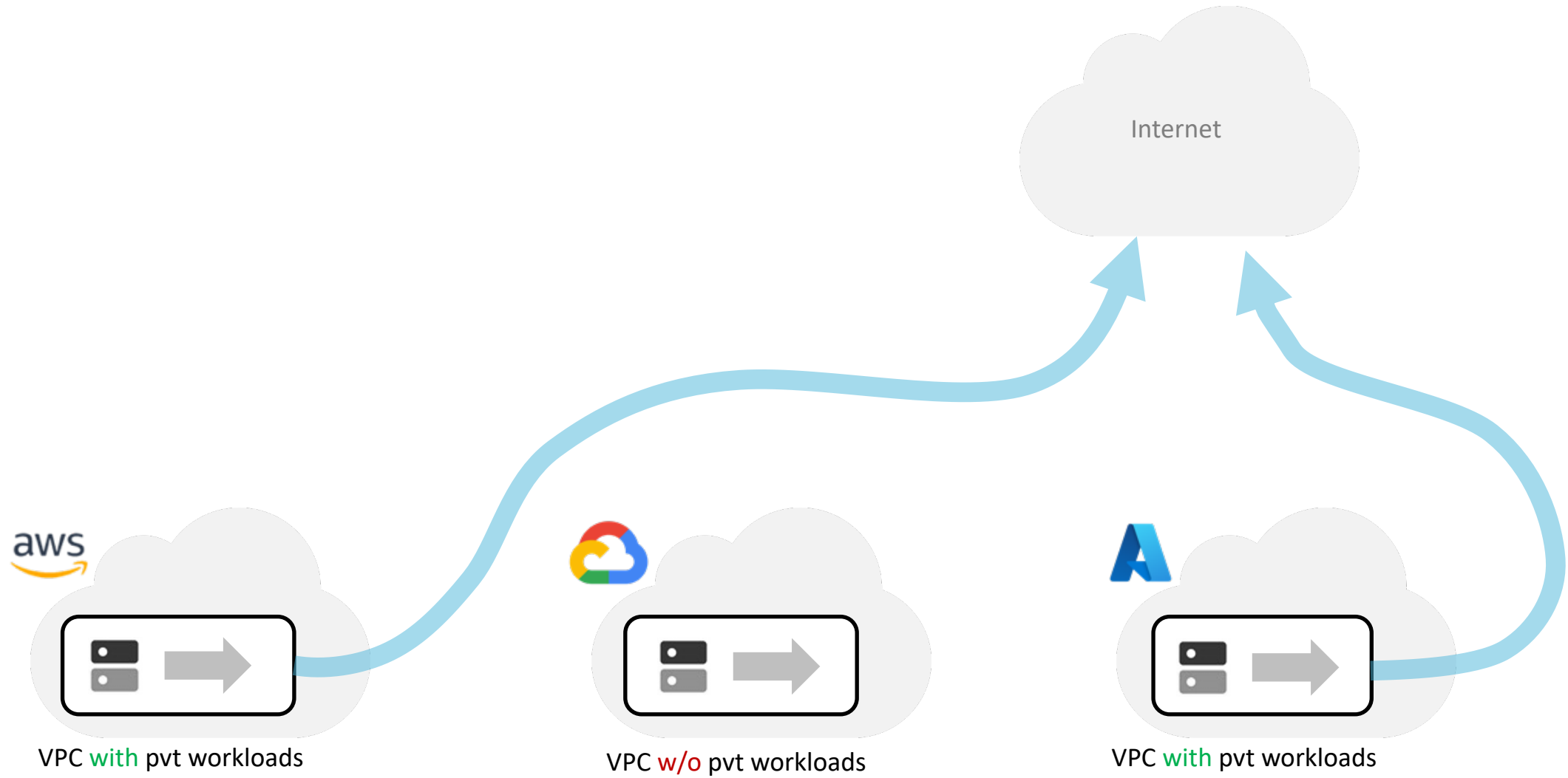


### Layer-7 Firewall

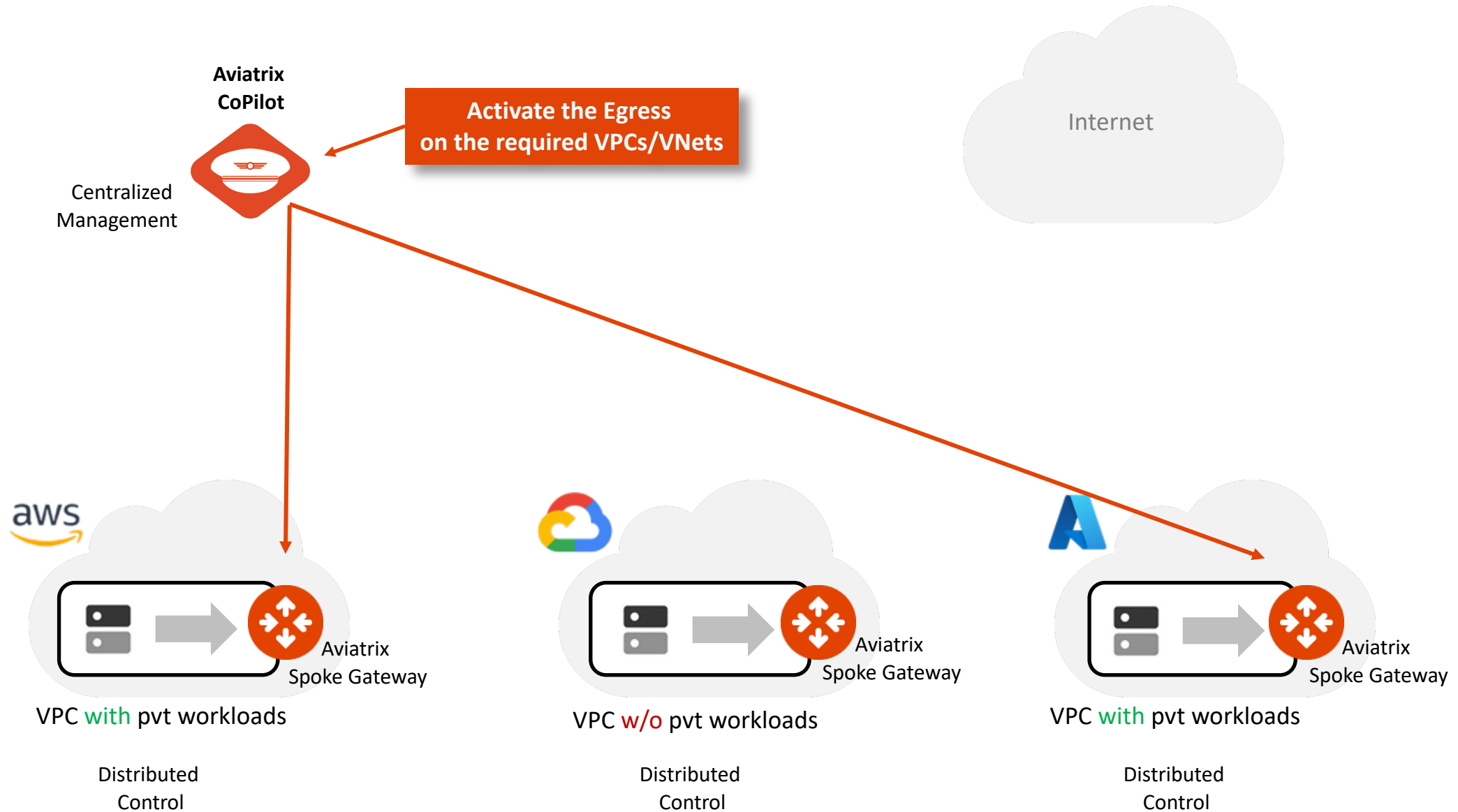
- Overkill
- Expensive



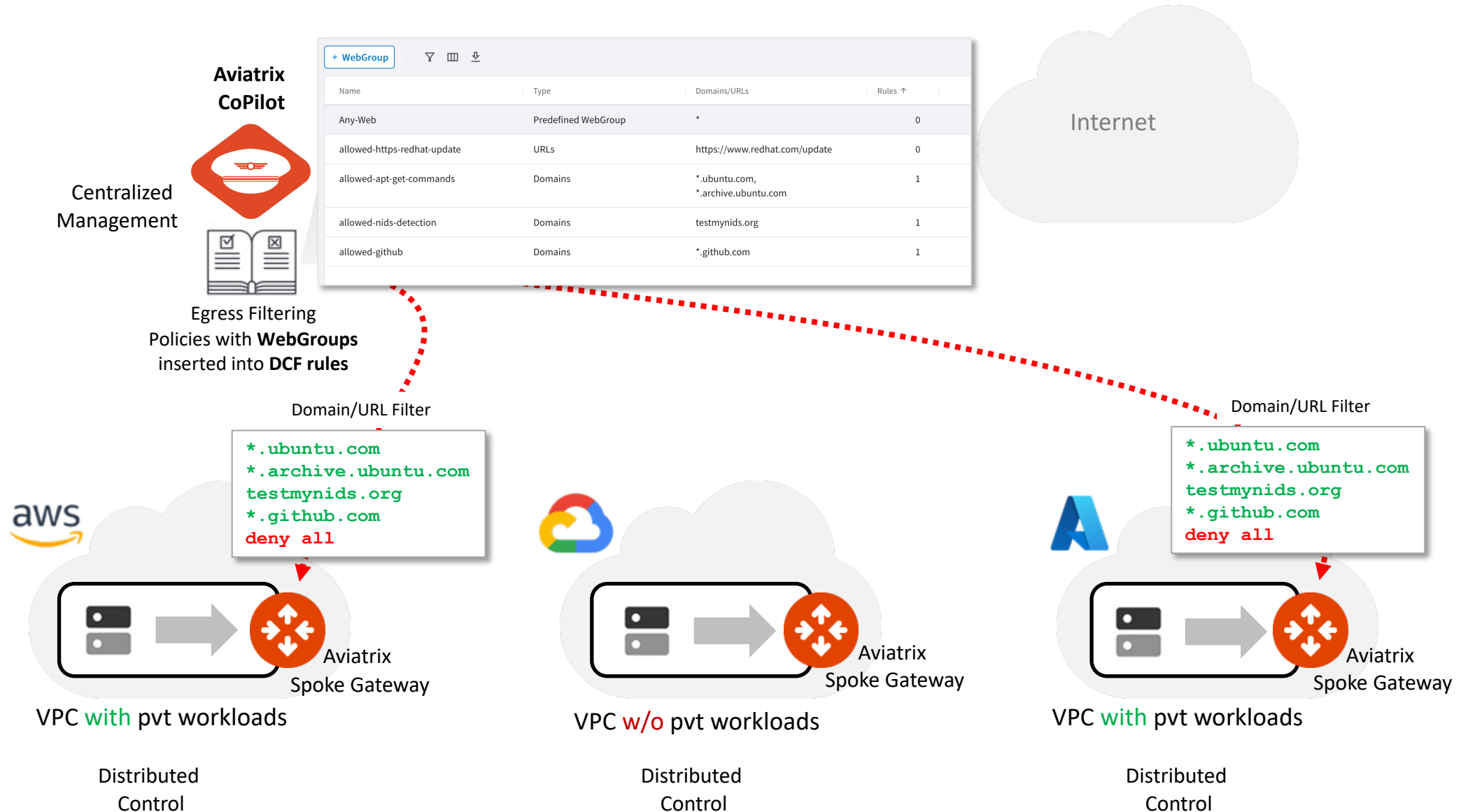
# Aviatrix Secure Egress Filtering Feature



# Aviatrix Secure Egress Filtering



# Aviatrix Secure Egress Filtering

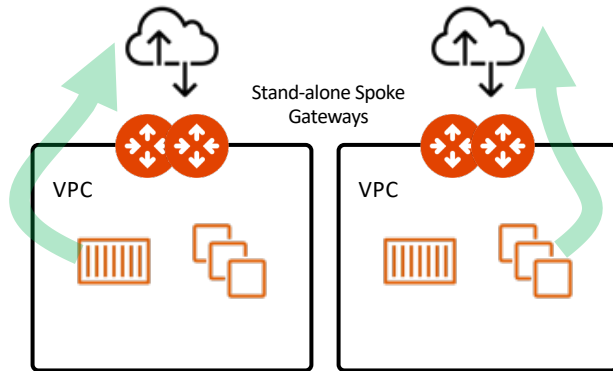




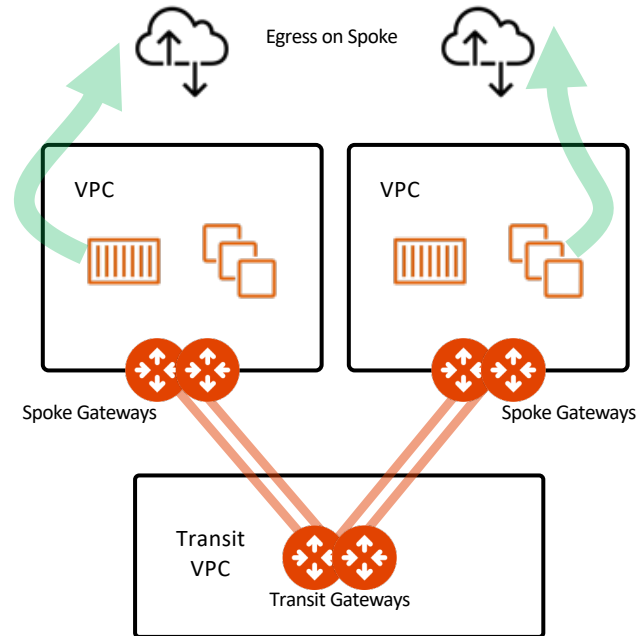
# Aviatrix Secure Egress Filtering Design Patterns



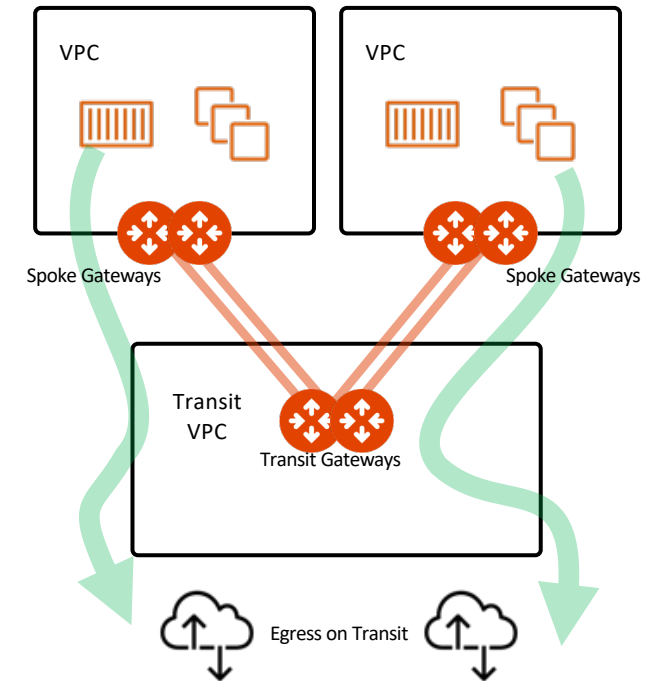
## Stand-alone Spoke GW (Distributed)



## Local Egress (Distributed) with Aviatrix Spoke GW



## Centralized Egress with Aviatrix Transit GW



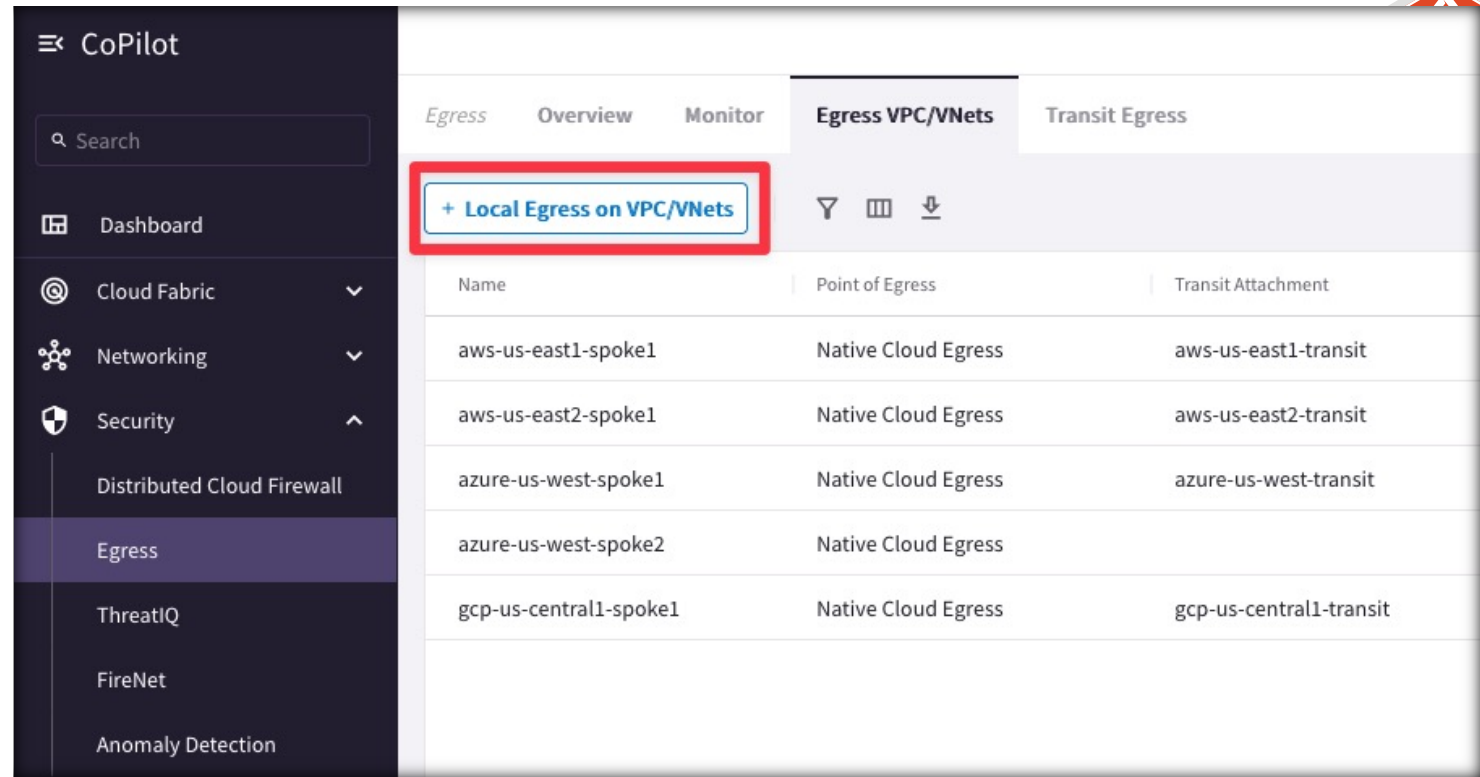


# Tools for Troubleshooting Secure Egress



# 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 requires additional resources 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.

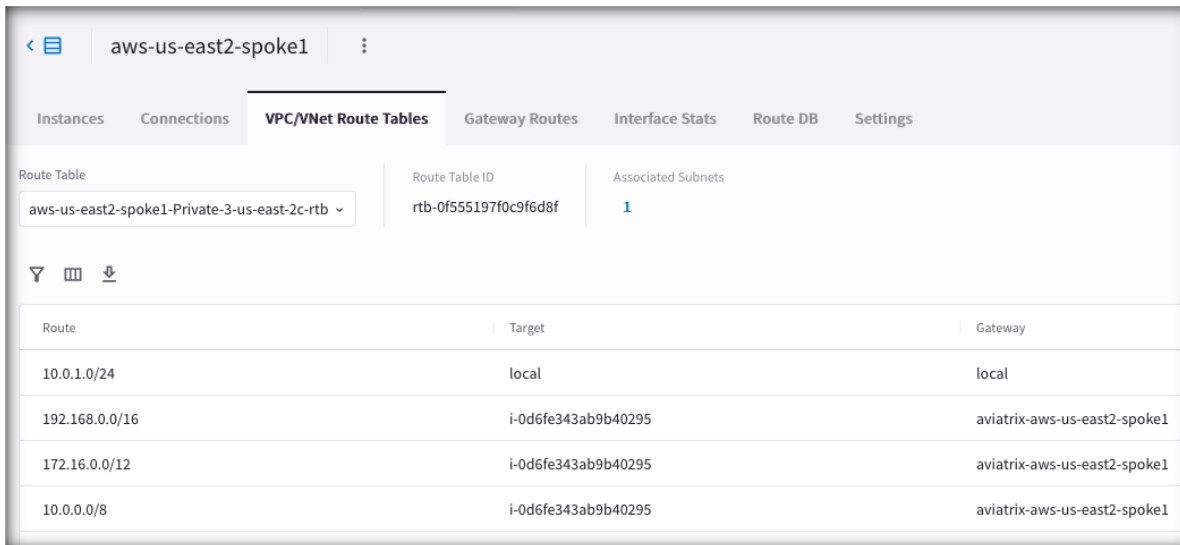


CoPilot

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

+ Local Egress on VPC/VNets

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



aws-us-east2-spoke1

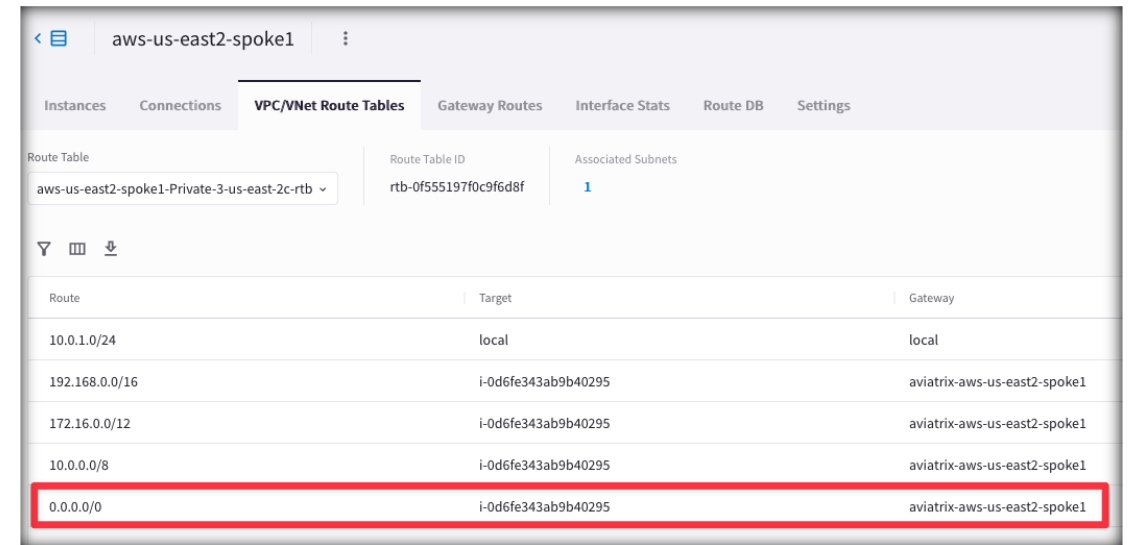
Instances Connections **VPC/VNet Route Tables** Gateway Routes Interface Stats Route DB Settings

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



aws-us-east2-spoke1

Instances Connections **VPC/VNet Route Tables** Gateway Routes Interface Stats Route DB Settings

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

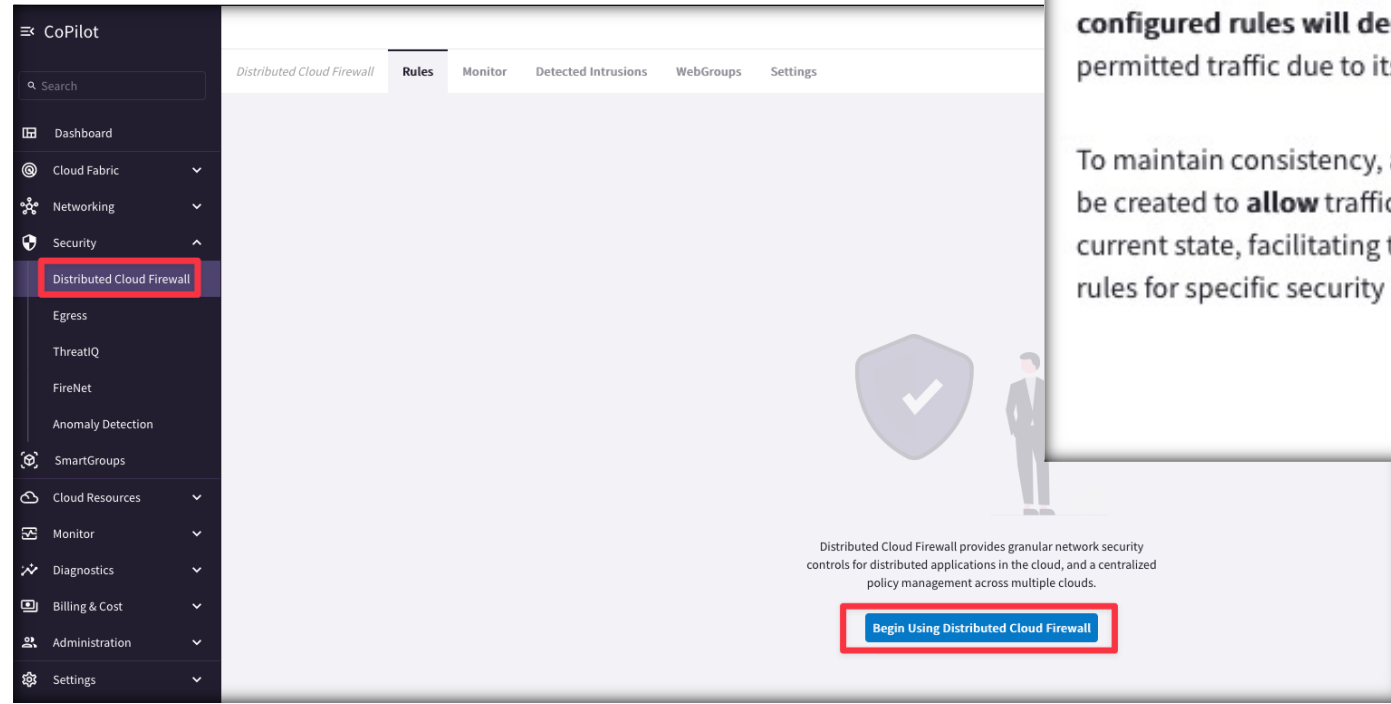
Route Table ID: rtb-0f555197f0c9f6d8f

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.

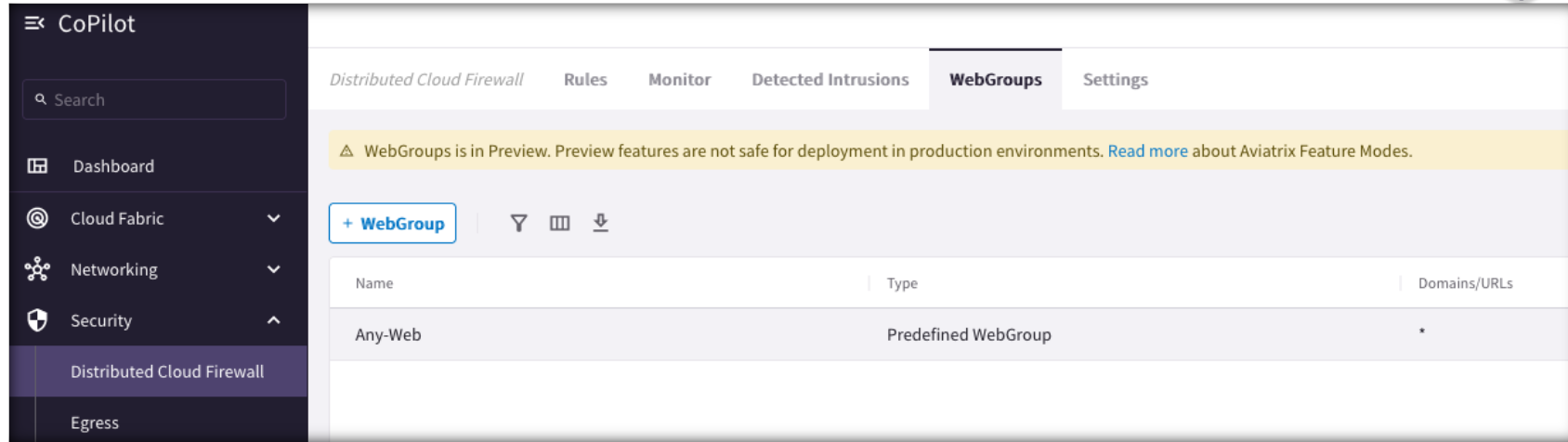


Distributed Cloud Firewall								
Rules								
Monitor								
Detected Intrusions								
WebGroups								
Settings								
<a href="#">+ Rule</a>   <a href="#">Actions</a>   <a href="#">Filter</a>   <a href="#">Grid</a>   <a href="#">Download</a>								
<input type="checkbox"/>	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
<input type="checkbox"/>	21474...	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.
- 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.



# Monitor



- CoPilot > Security > Egress > Monitor

Egress

Overview

Monitor

Egress VPC/VNets

Transit Egress

^ Filters

Time Period

Last 24 Hours

Start

Nov 1, 2023 4:09 PM

End

Now

VPC/VNets

ace-azure-east-us-spoke2

Search

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	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



Next:

## Lab 7 Secure Egress