



Aviatrix Cloud Firewall

SECURE EGRESS

ACE Team

Problem Statement

Private workloads need internet access

- SaaS integration



- Patching

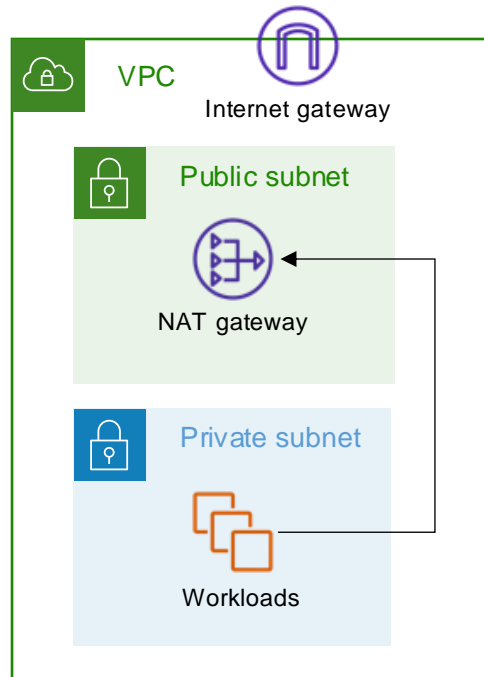


- Updates



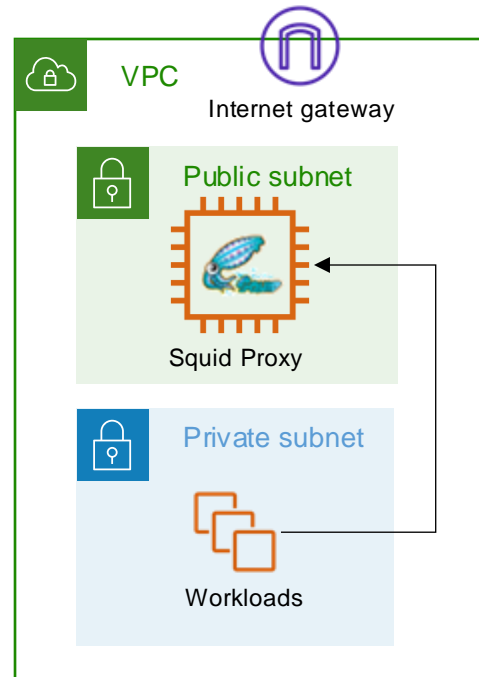
NAT Gateway

- Layer-4 only
- NACLs management



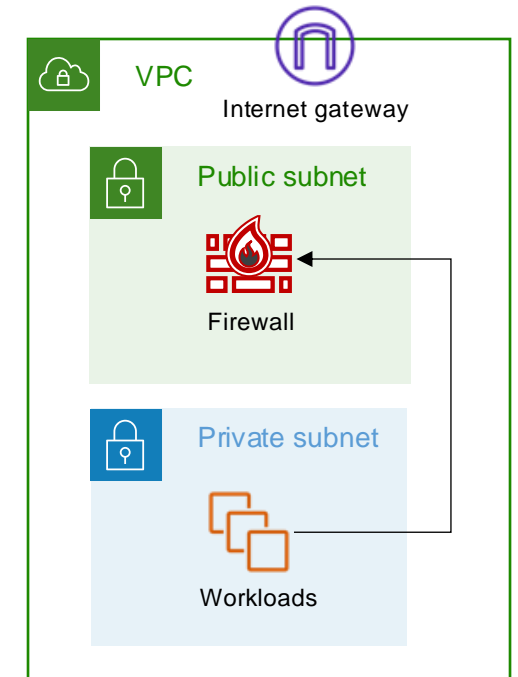
Squid Proxy

- Hard to manage
- Scale and HA issues

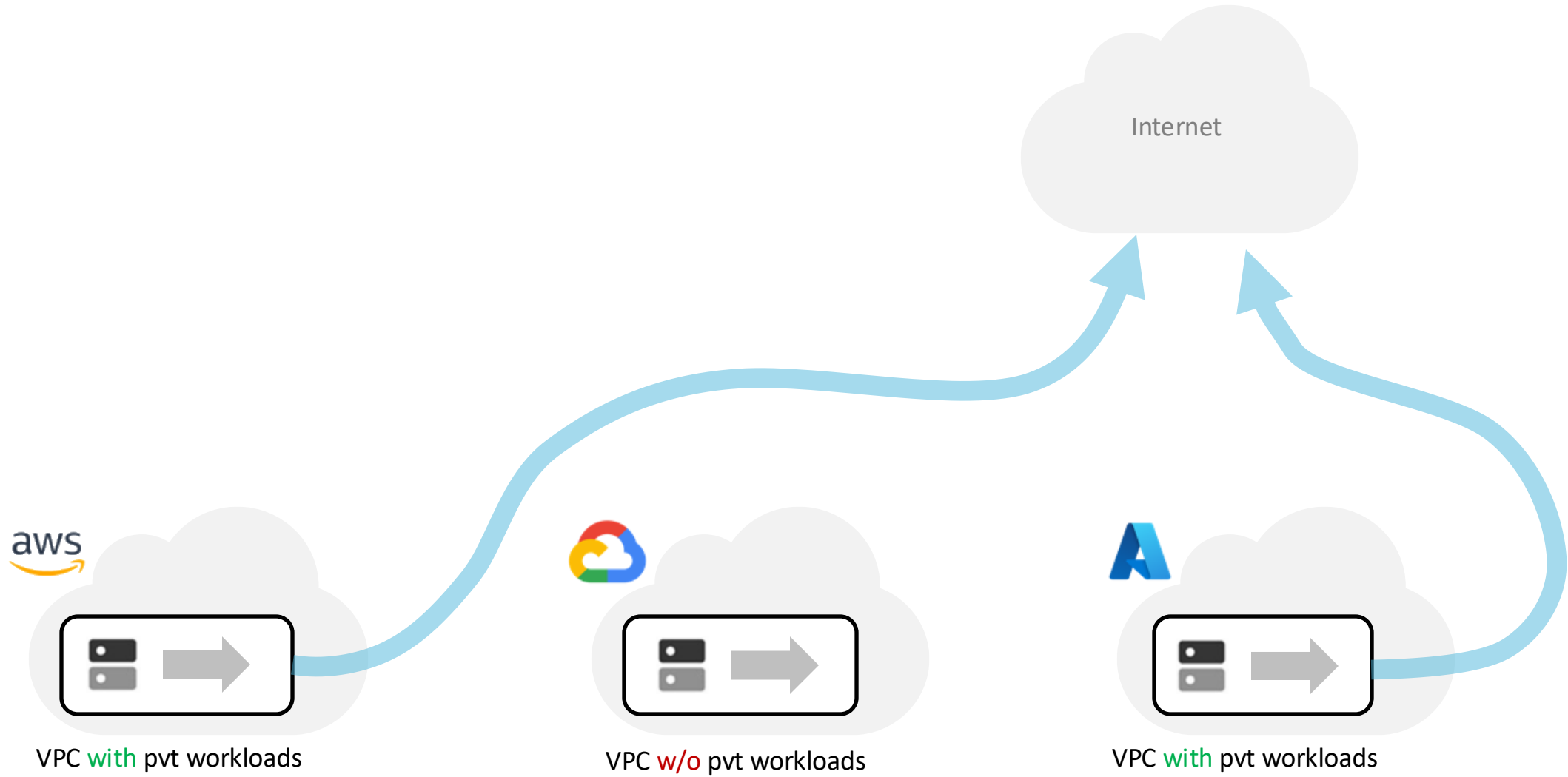


Layer-7 Firewall

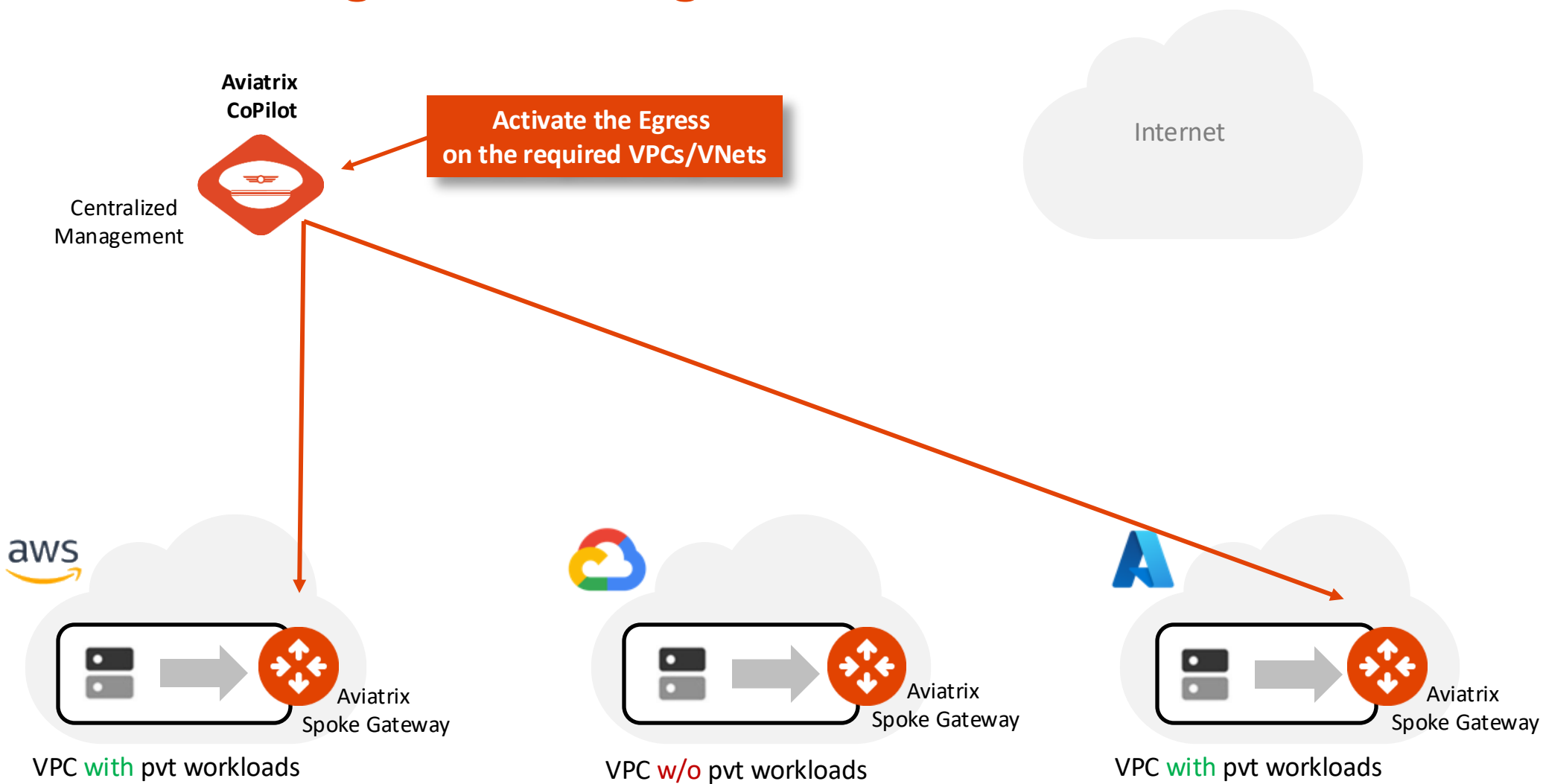
- Overkill
- Expensive



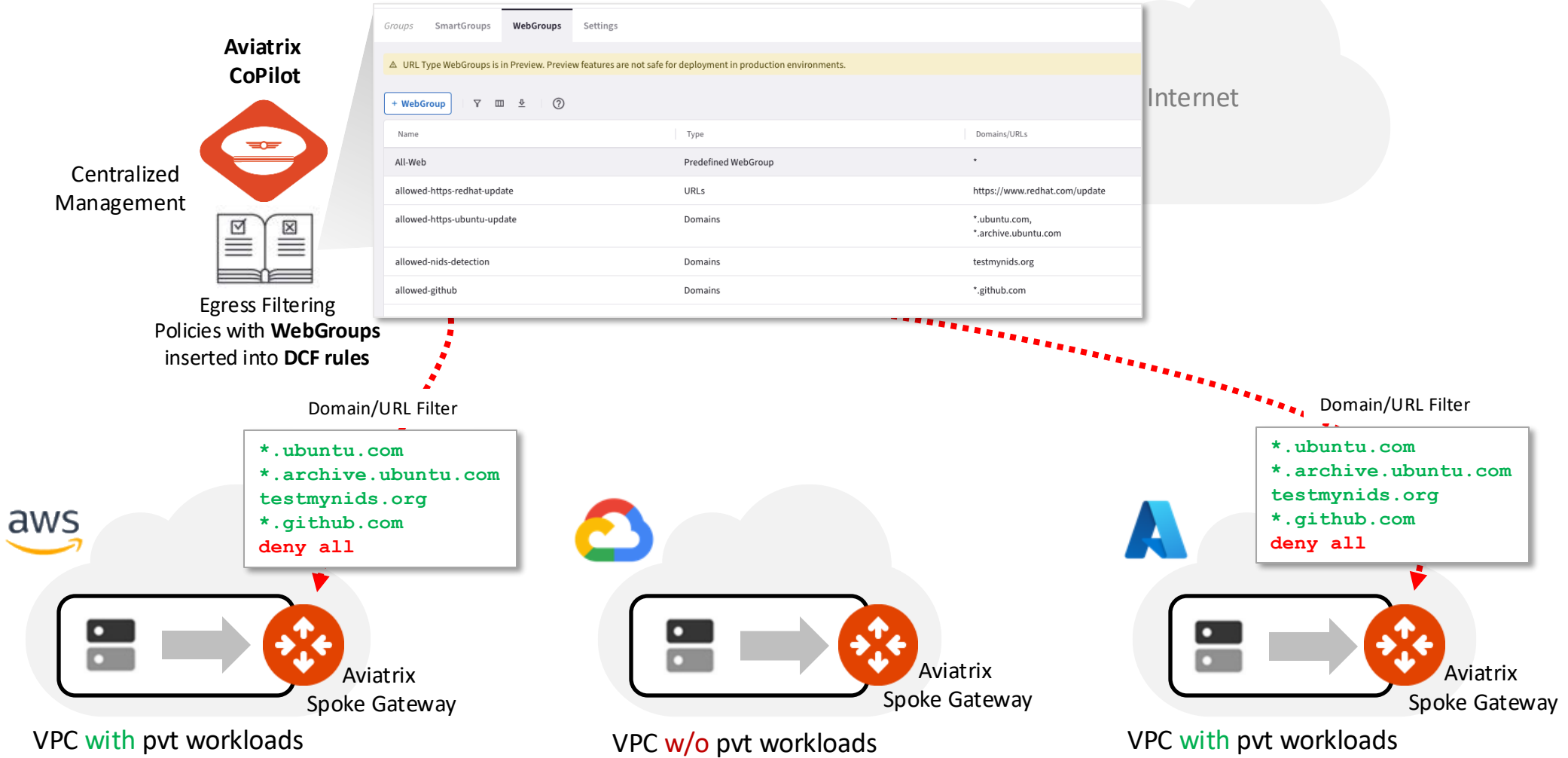
Aviatrix Secure Egress Filtering Feature



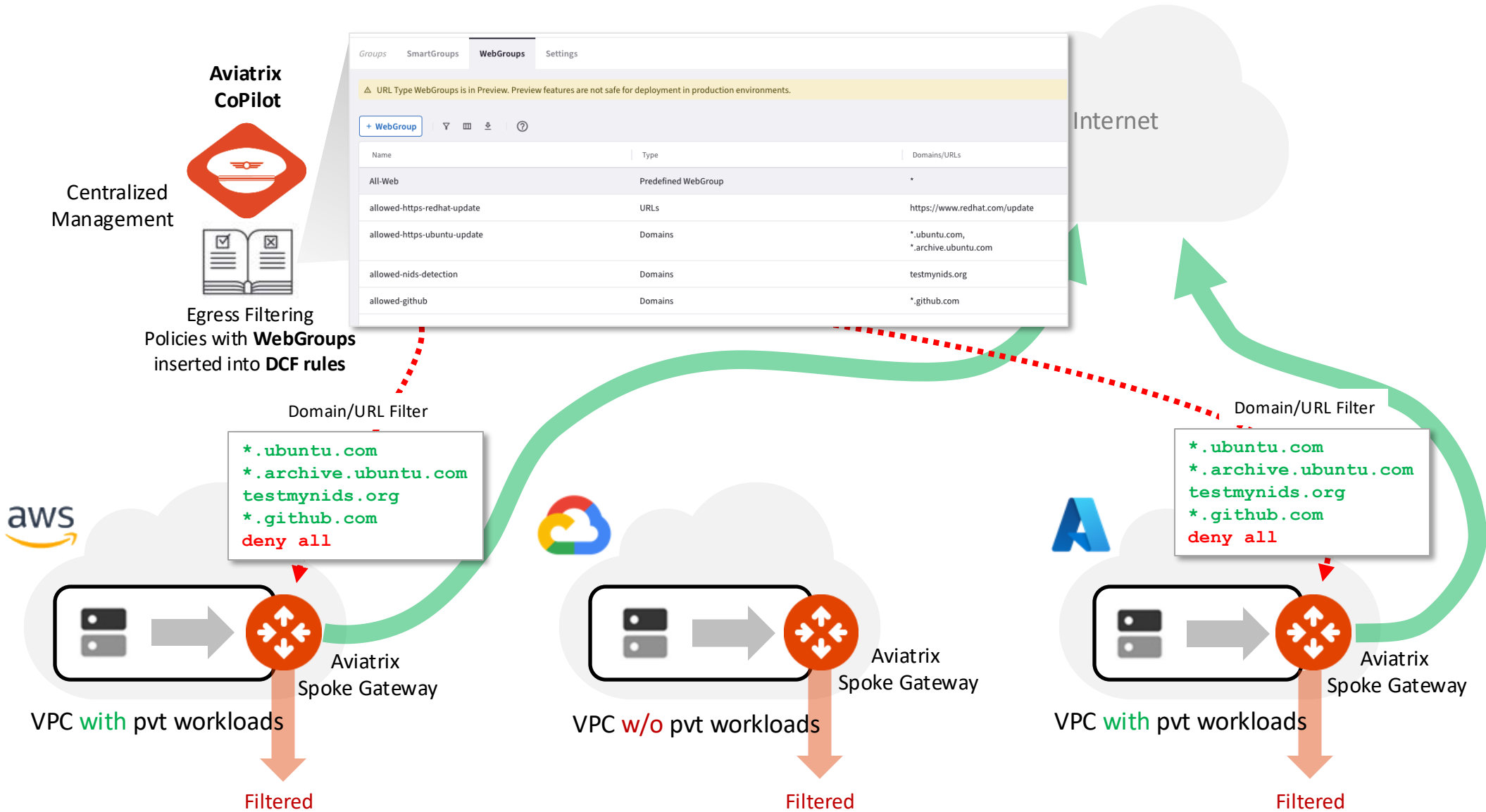
Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering





Tools for Troubleshooting Secure Egress

Verify the Local 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 requires additional resources 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
ace-aws-eu-west-1-spoke1	ace-aws-eu-west-1-spoke1	Native Cloud Egress	ace-aws-eu-west-1-transit1
ace-aws-eu-west-1-spoke2	ace-aws-eu-west-1-spoke2	Native Cloud Egress	ace-aws-eu-west-1-transit1
ace-azure-east-us-spoke1	ace-azure-east-us-spoke1	Native Cloud Egress	ace-azure-east-us-transit1
ace-azure-east-us-spoke2	ace-azure-east-us-spoke2	Native Cloud Egress	ace-azure-east-us-transit1
ace-gcp-us-east1-spoke1	ace-gcp-us-east1-spoke1	Native Cloud Egress	ace-gcp-us-east1-transit1

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	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.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- 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: do not edit this rule*, although it can be recreated if it is accidentally deleted.

CoPilot

Search

Dashboard
Cloud Fabric
Networking
Security
Distributed Cloud Firewall
Egress
FireNet
Anomaly Detection
Groups
Cloud Resources
Monitor
Diagnostics
Administration
Settings

Distributed Cloud Firewall

Rules Monitor Detected Intrusions Settings

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.

Cancel Begin

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

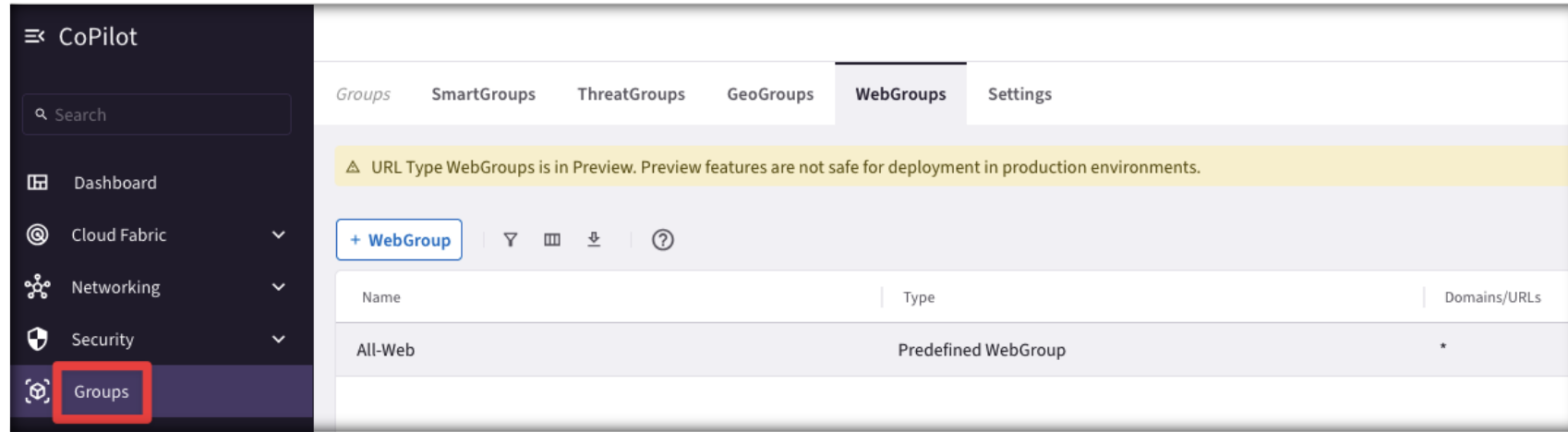
Manage Add-on Features **Enable Distributed Cloud Firewall**

+ Rule Actions

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
<input type="checkbox"/>	214748... Greenfield-Rule	Anywhere (0.0.0.0...	Anywhere (0.0.0.0...		Any		Permit
<input type="checkbox"/>	214748... DefaultDenyAll	Anywhere (0.0.0.0...	Anywhere (0.0.0.0...		Any		Deny

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).



This is the 'Create WebGroup' form for a URL-based WebGroup. It includes a yellow warning banner. The 'Name' field contains 'FTP-to-Example.com'. The 'Type' section has two radio buttons: 'Domains' and 'URLs' (the latter is selected and highlighted with a red box). A 'Preview' label is next to the 'URLs' option. The 'Domains/URLs' field contains 'ftp://ftp.example.com/directory/' with a clear button (x). At the bottom are 'Cancel' and 'Save' buttons.

This is the 'Create WebGroup' form for a Domain-based WebGroup. It includes a yellow warning banner. The 'Name' field contains 'Apt-get-Commands'. The 'Type' section has two radio buttons: 'Domains' (selected and highlighted with a red box) and 'URLs'. A 'Preview' label is next to the 'URLs' option. The 'Domains/URLs' field contains '*.ubuntu.com' with a clear button (x). At the bottom are 'Cancel' and 'Save' buttons.

Monitor



CAVEAT: Logging must be enabled

- CoPilot > Security > Egress > FQDN Monitor (Legacy)

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

Logging



Next:

Lab 7 Aviatrix Cloud Firewall