



Egress

Problem Statement

Private workloads need internet access

- SaaS integration



- Patching

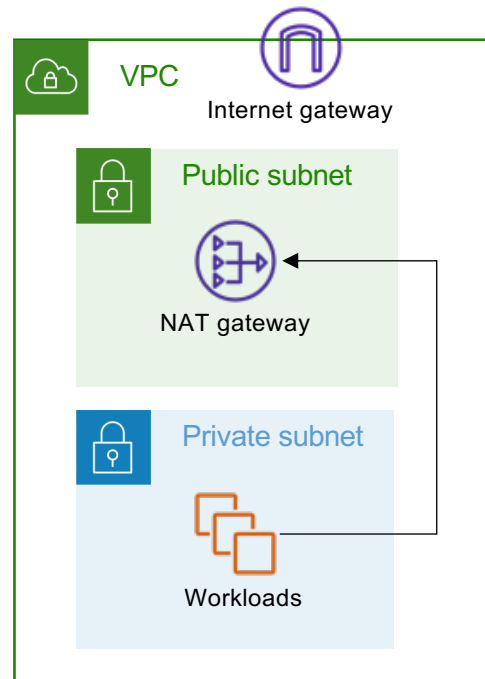


- Updates



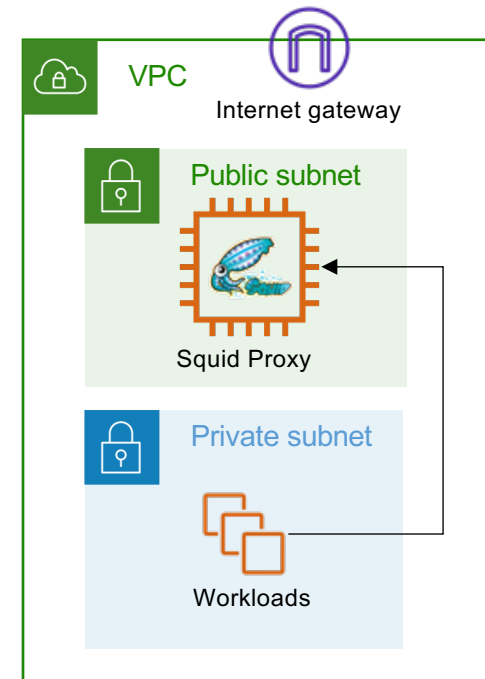
NAT Gateway

- Layer-4 only
- NACLs management



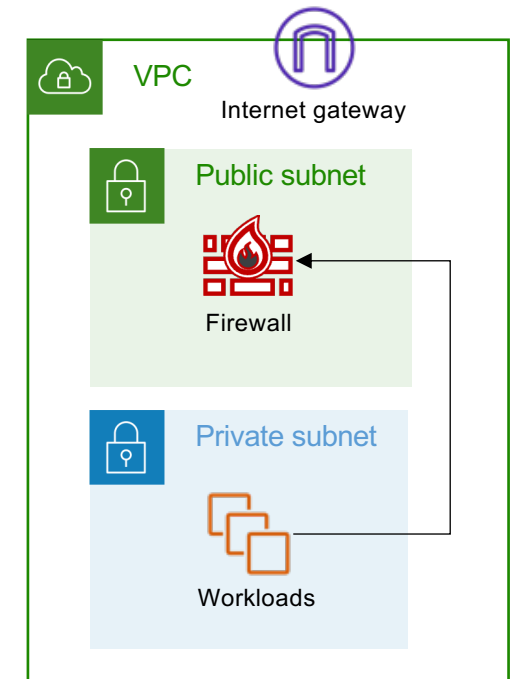
Squid Proxy

- Hard to manage
- Scale and HA issues

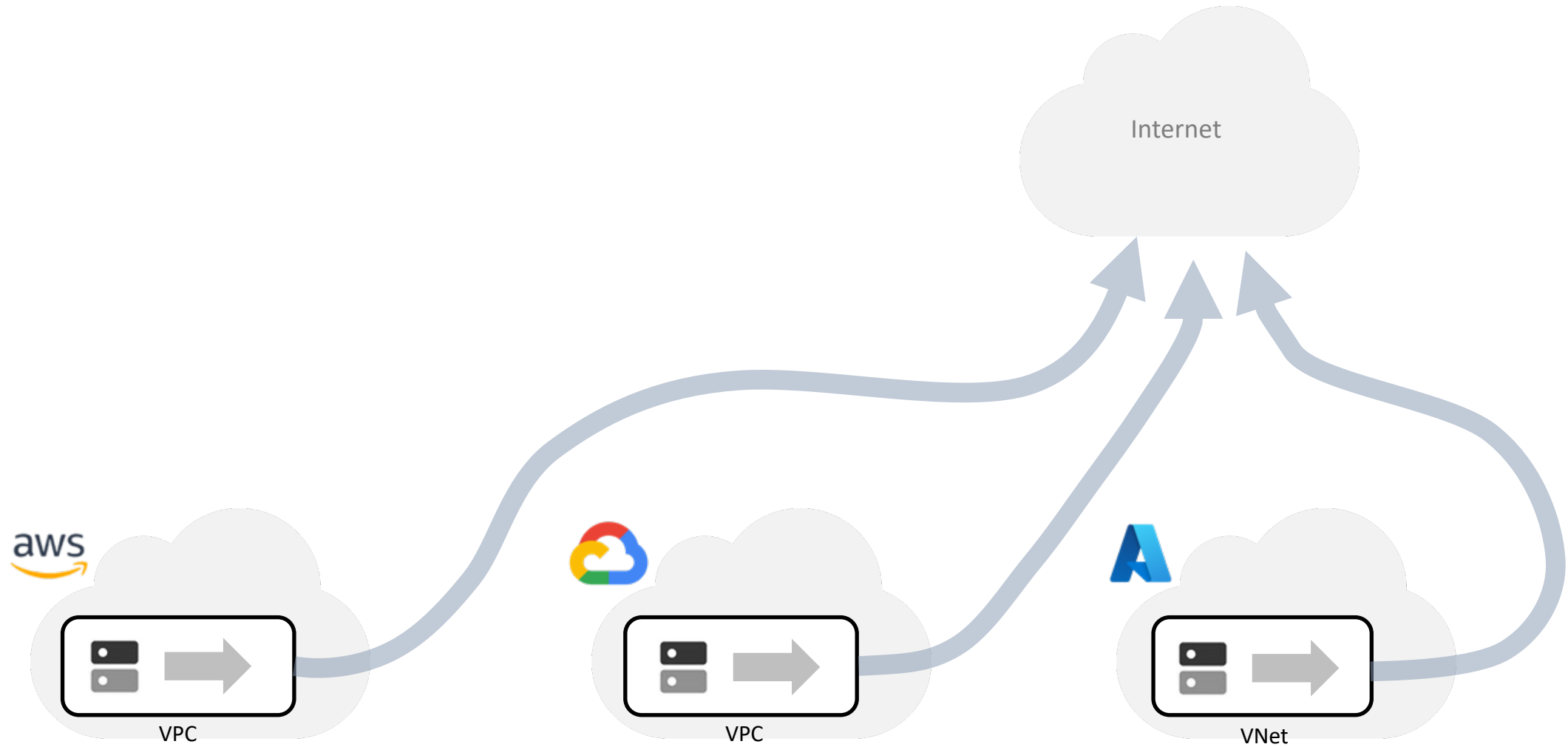


Layer-7 Firewall

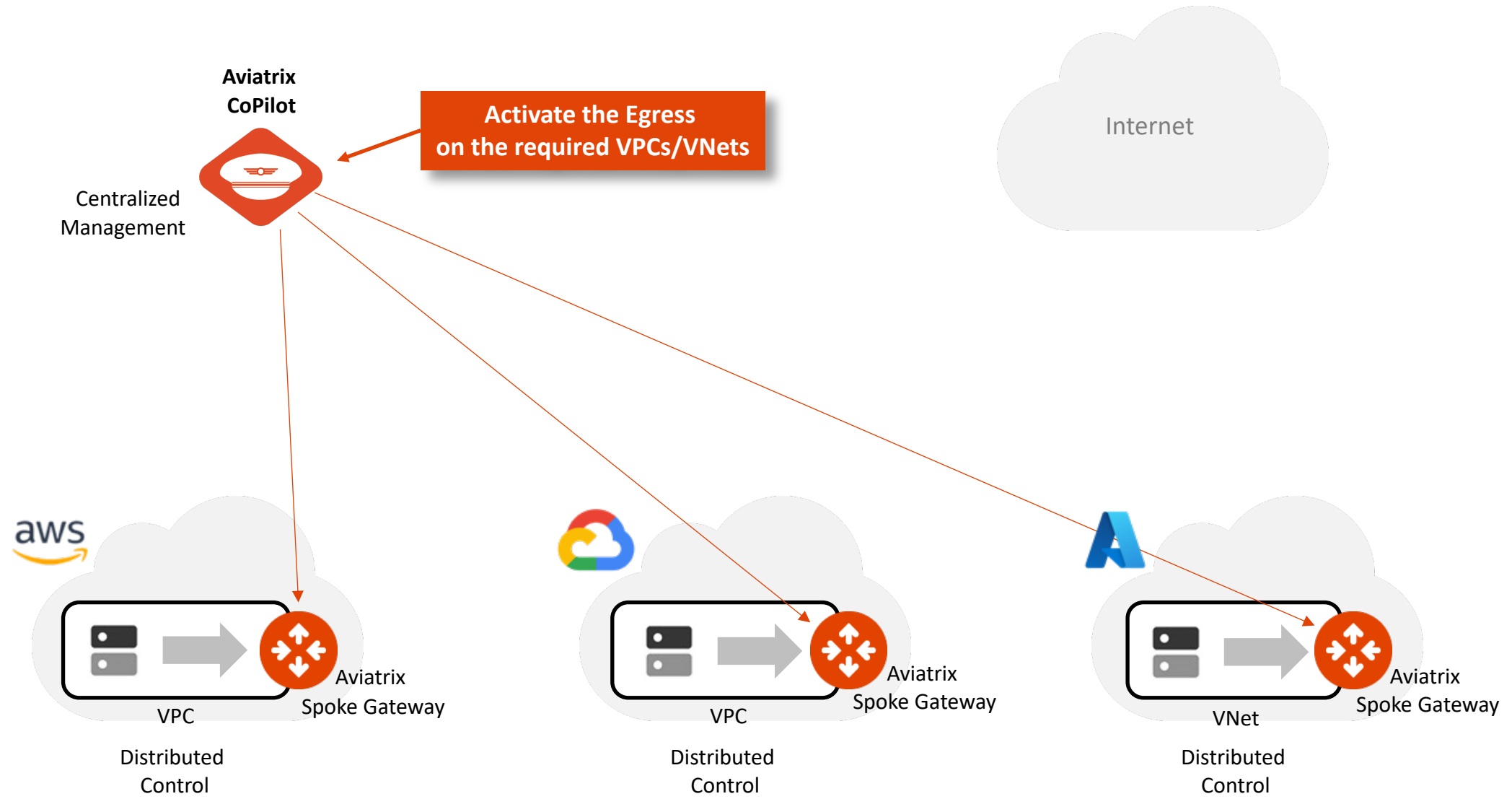
- Overkill
- Expensive



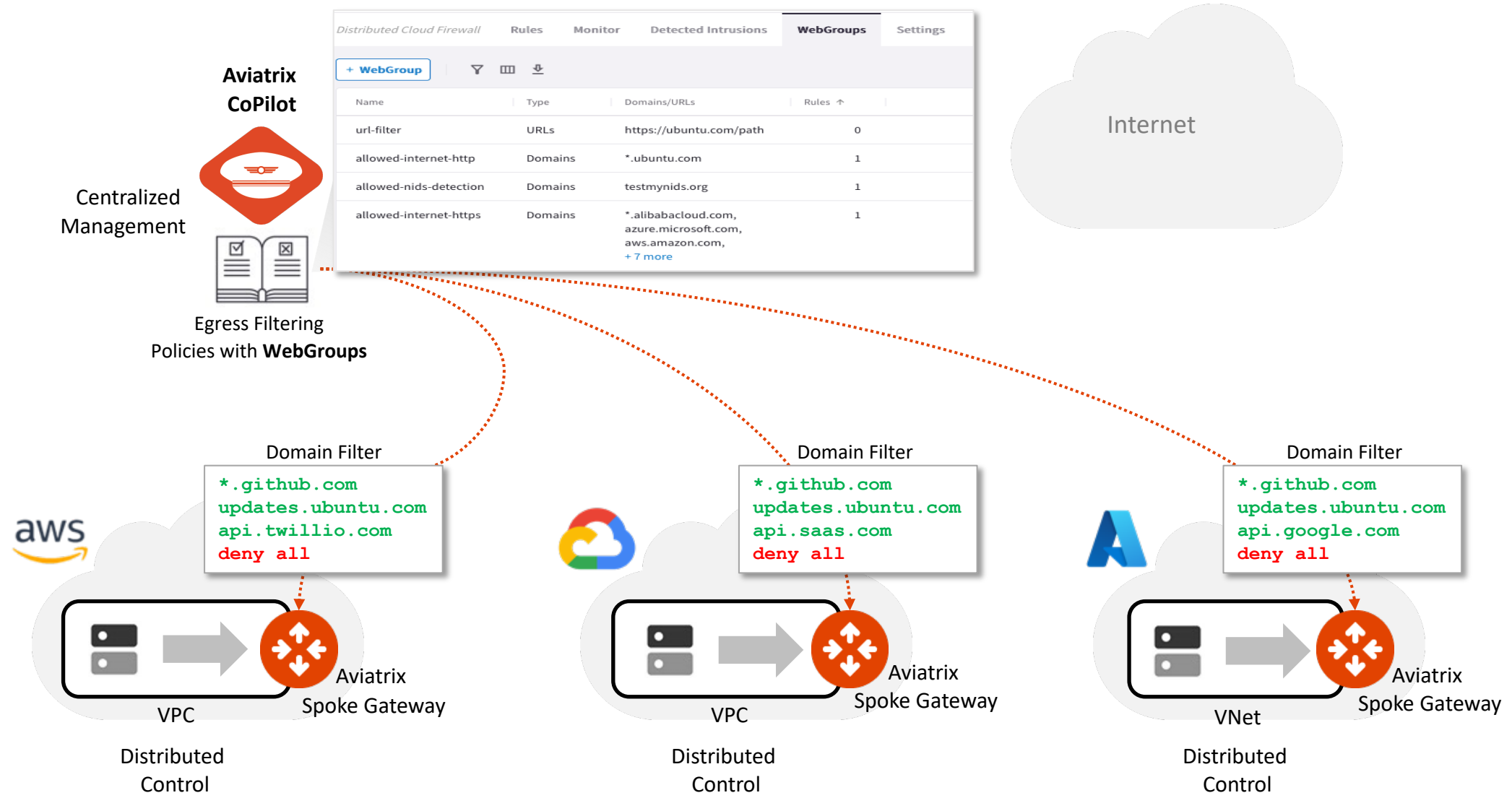
Aviaatrix Secure Egress Filtering Feature



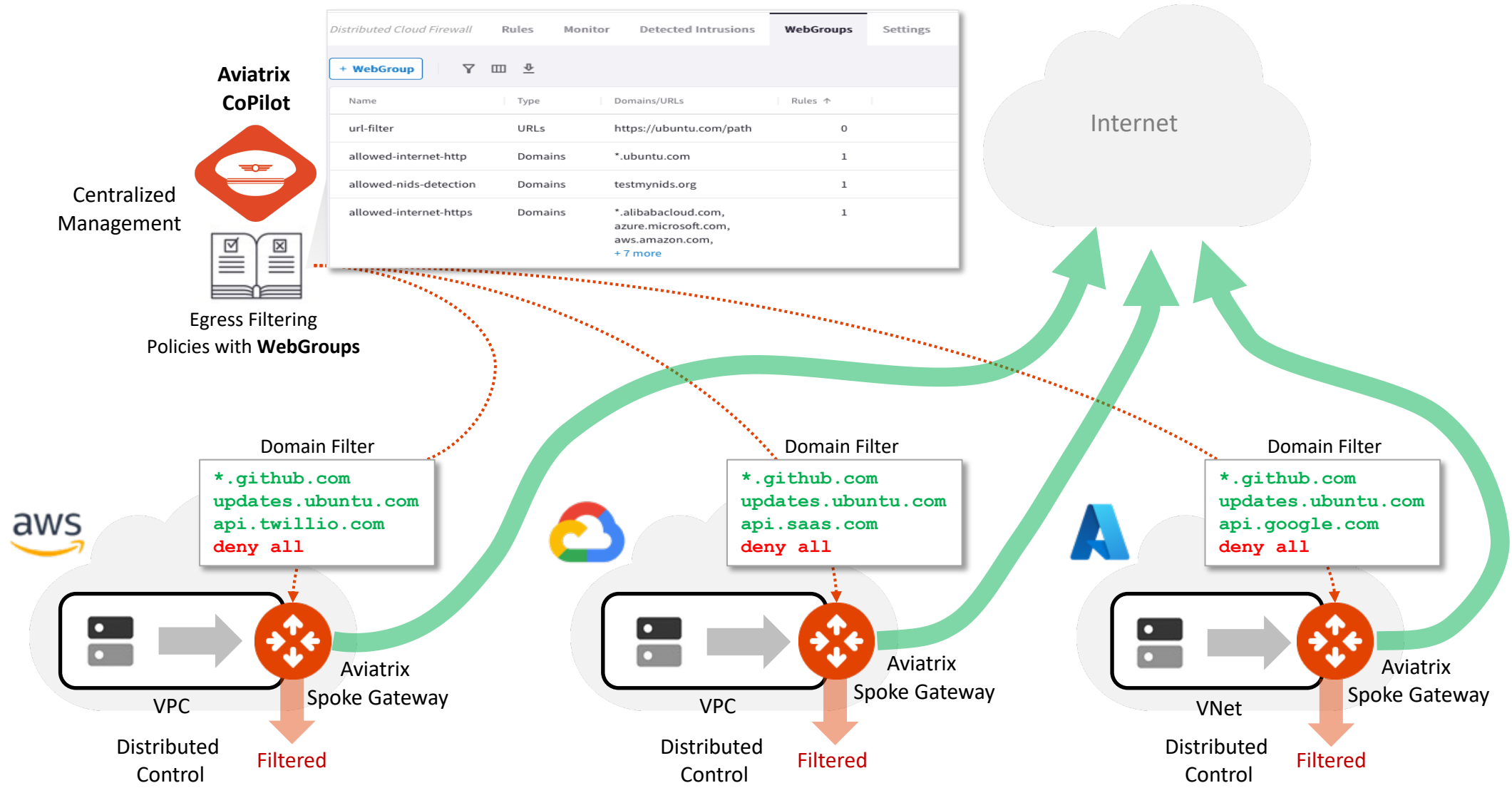
Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering

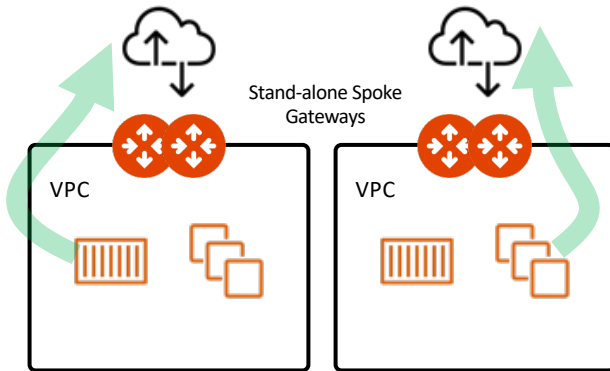


Aviatrix Secure Egress Filtering

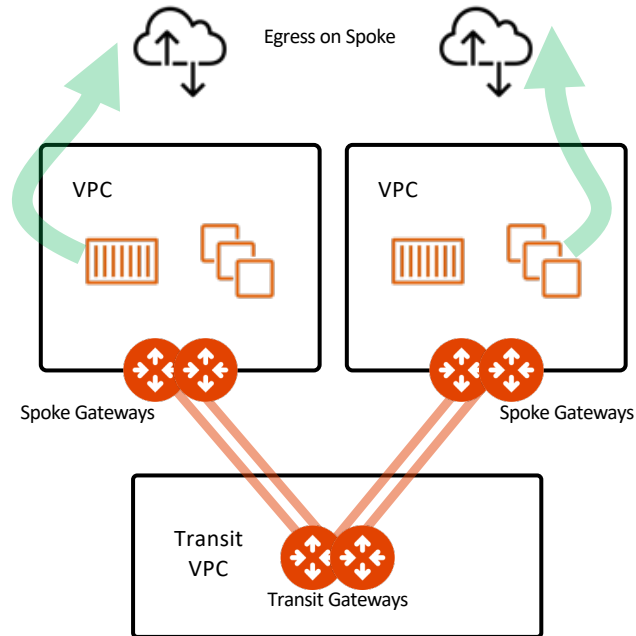


Aviatrix Secure Egress Filtering Design Patterns

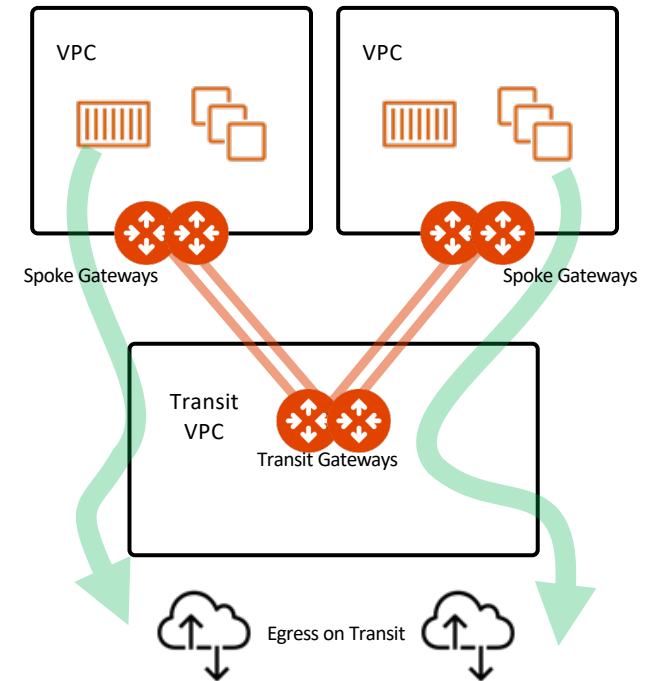
Stand-alone Spoke GW (Distributed)



Local Egress (Distributed) with Aviatrix Spoke GW



Centralized Egress with Aviatrix Transit GW



Zero Touch Network Access

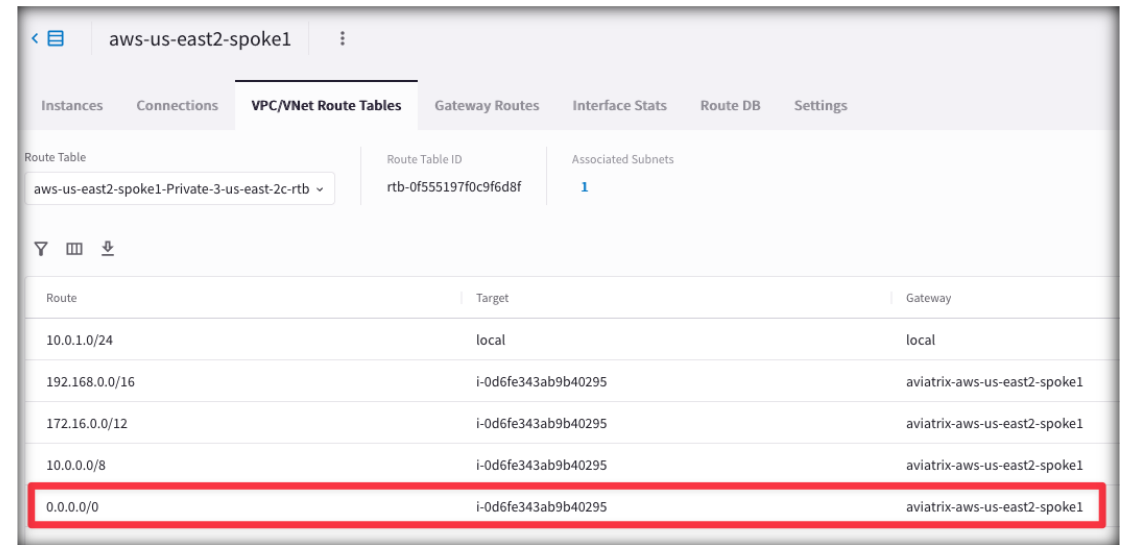
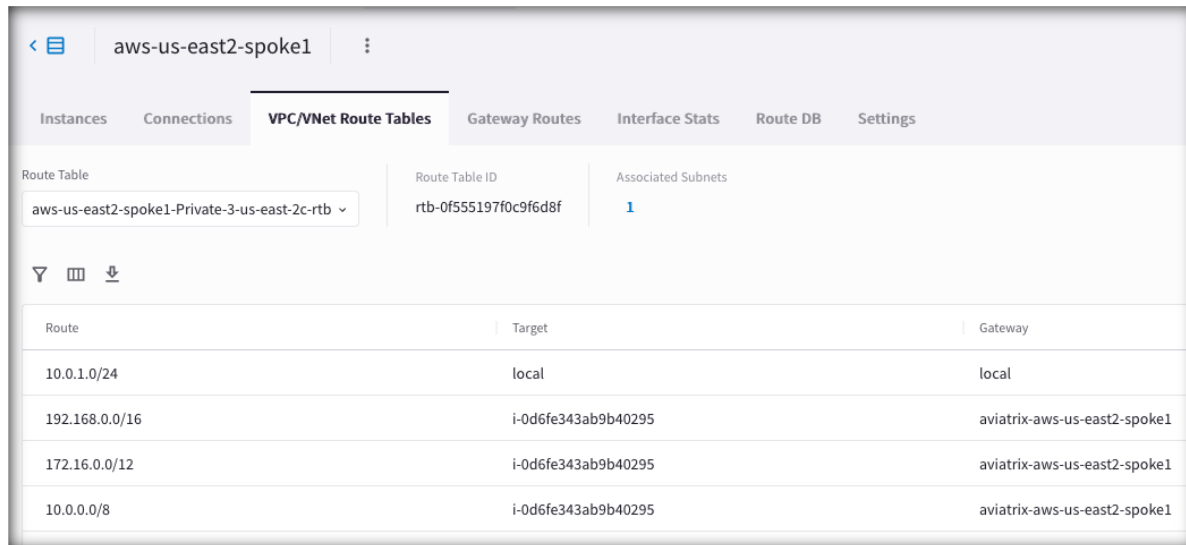
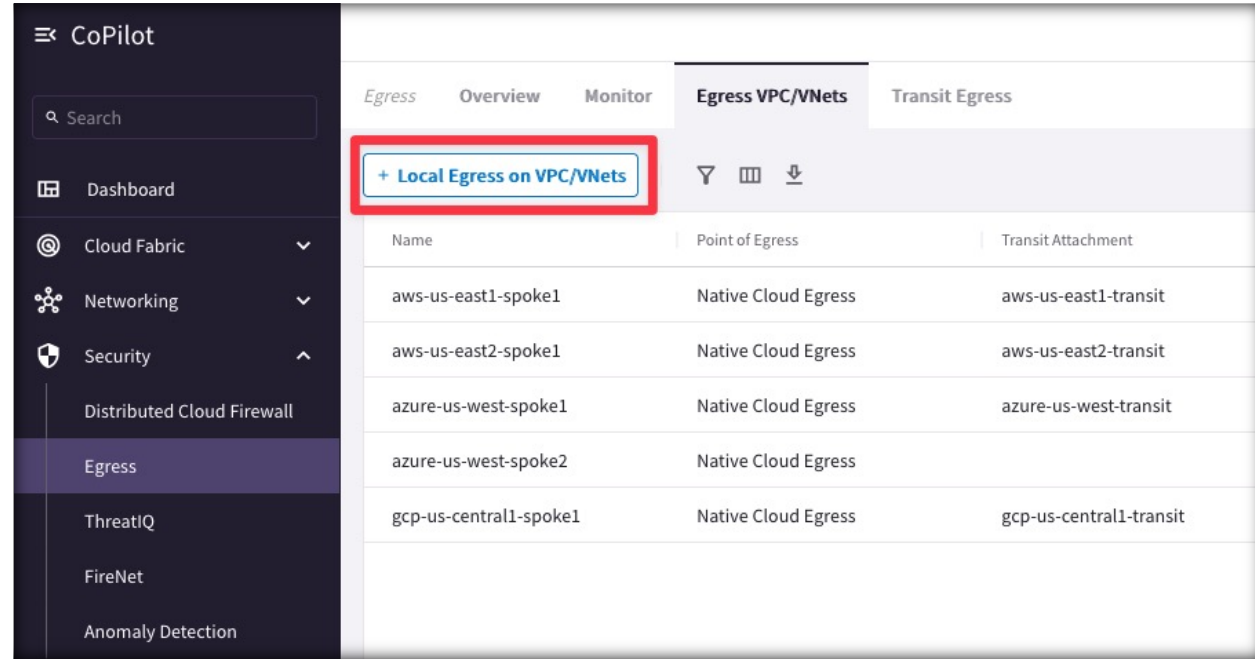
There are two possible models:

- **DENY LIST MODEL** (THREAT-CENTRIC MODEL):
 - ❑ allow all data to flow, except for exactly what you say should be stopped.
- **ALLOW LIST MODEL** (TRUST-CENTRIC MODEL):
 - ❑ deny everything and only permit what you explicitly allow.

Tools for troubleshooting 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.



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.

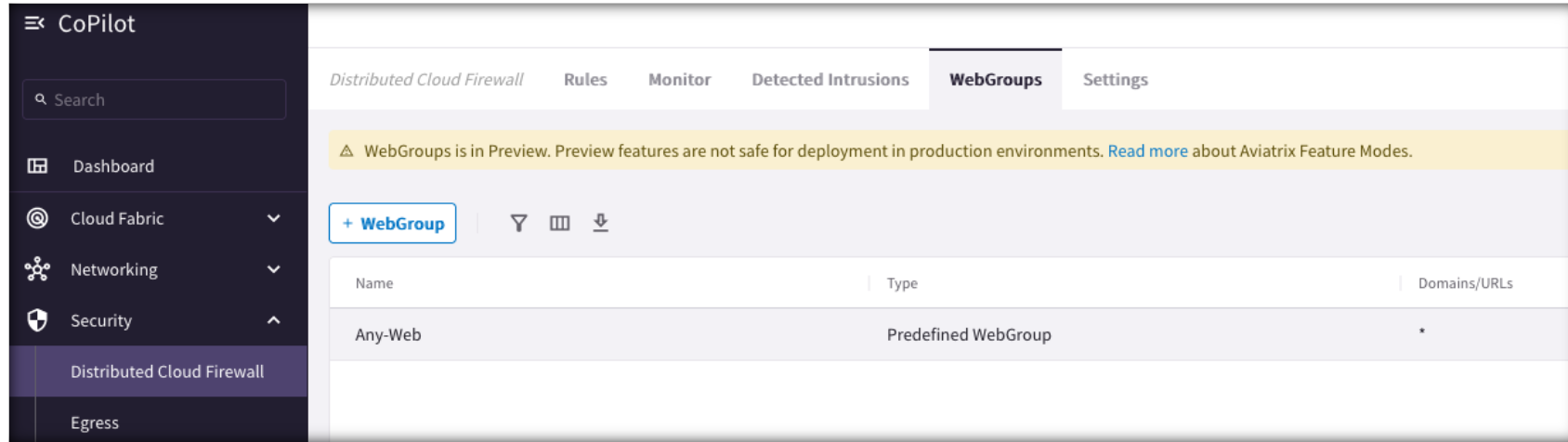
The screenshot shows the CoPilot interface with a sidebar on the left containing a search bar and a list of navigation items: Dashboard, Cloud Fabric, Networking, Security, Distributed Cloud Firewall (highlighted with a red box), Egress, ThreatIQ, FireNet, Anomaly Detection, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The main panel displays the 'Distributed Cloud Firewall' setup screen with tabs for Rules, Monitor, Detected Intrusions, WebGroups, and Settings. The 'Rules' tab is active, showing a shield icon with a checkmark and a person icon. Below the icon, text states: 'Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, and a centralized policy management across multiple clouds.' A red box highlights a button labeled 'Begin Using Distributed Cloud Firewall'. To the right, a modal window titled 'Distributed Cloud Firewall' contains the following text: 'Enabling the Distributed Cloud Firewall **without configured rules will deny all** previously permitted traffic due to its implicit Deny All rule.' and '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.' At the bottom of the modal are 'Cancel' and 'Begin' buttons.

The screenshot shows the 'Rules' tab of the Distributed Cloud Firewall interface. It features a '+ Rule' button, an 'Actions' dropdown, and icons for filter, table view, and download. Below is a table with the following data:

<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.



The 'Create WebGroup' dialog box shows the following fields and options:

- Name:** FTP-to-Example.com
- Type:** ☐ Domains ☒ URLs (The 'URLs' option is highlighted with a red box.)
- Domains/URLs:** ftp://ftp.example.com/directory/ (The input field has a red border.)
- Buttons:** Cancel, Save

The 'Create WebGroup' dialog box shows the following fields and options:

- Name:** Apt-get-Commands
- Type:** ☒ Domains ☐ URLs (The 'Domains' option is highlighted with a red box.)
- Domains/URLs:** *ubuntu.com (The input field has a red border.)
- Buttons:** Cancel, Save

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 Egress