aviatrix

Egress

Problem Statement

Private workloads need internet access

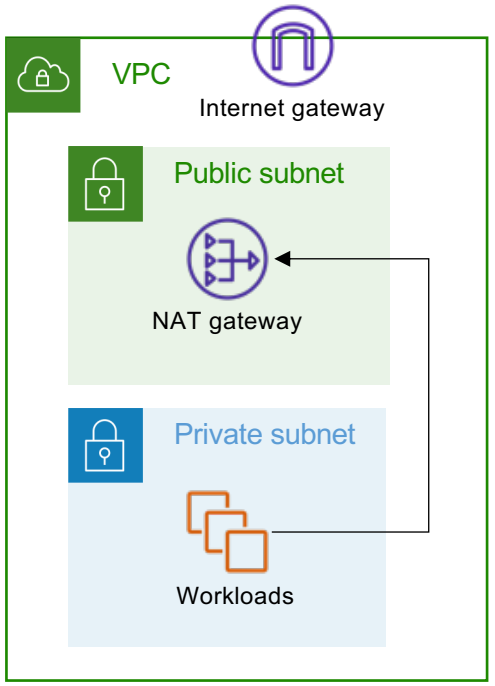
- **SaaS integration**

- **Patching**

- **Updates**

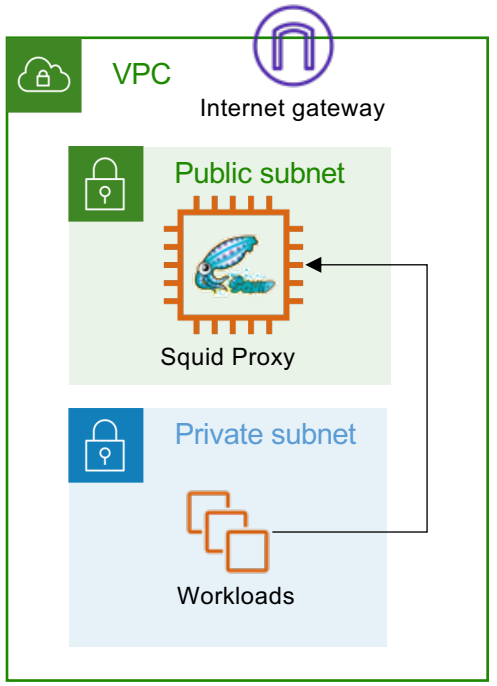
NAT Gateway

- Layer-4 only
- NACLs management



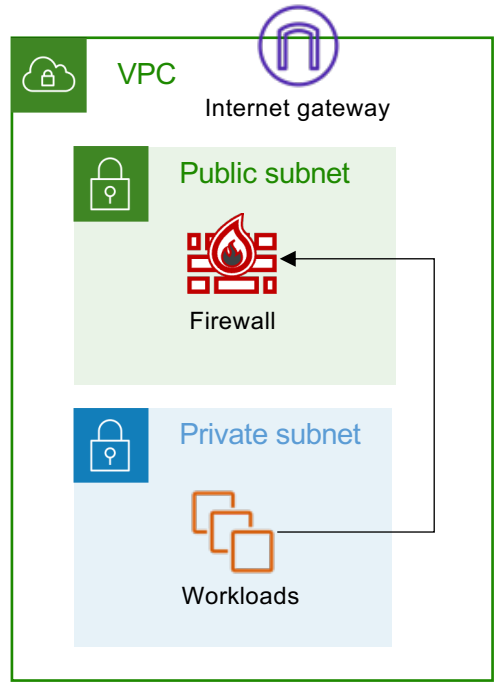
Squid Proxy

- Hard to manage
- Scale and HA issues

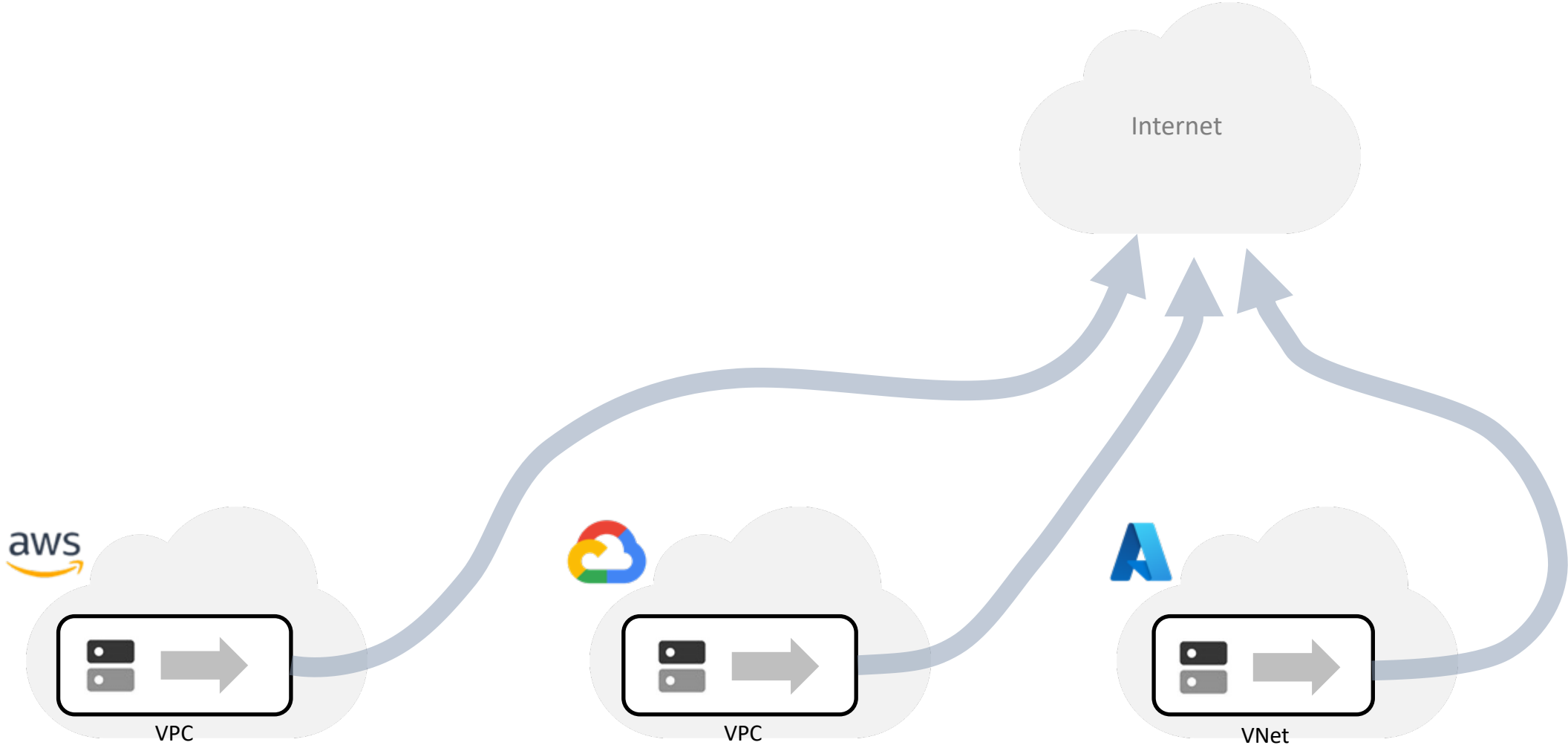


Layer-7 Firewall

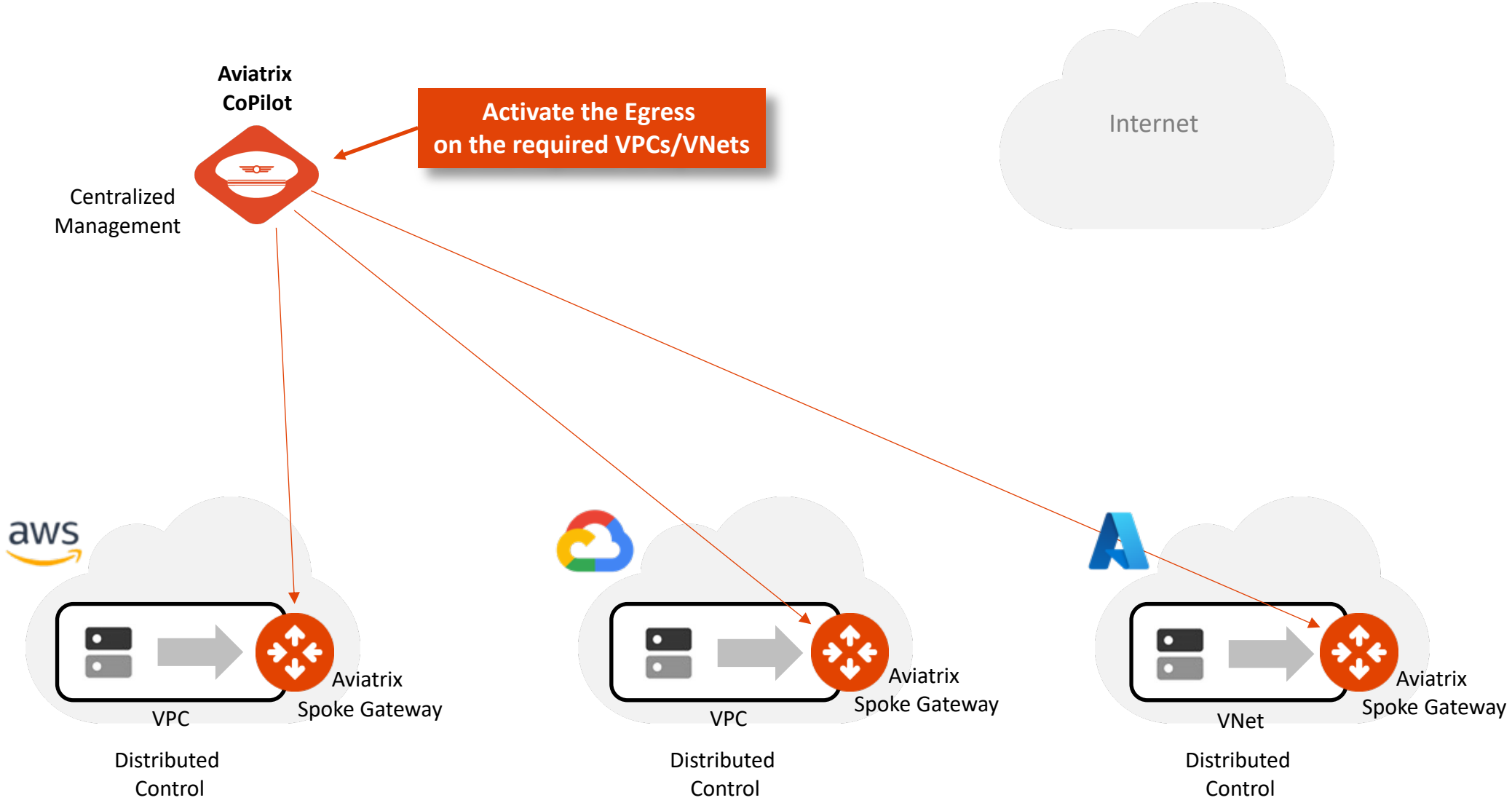
- Overkill
- Expensive



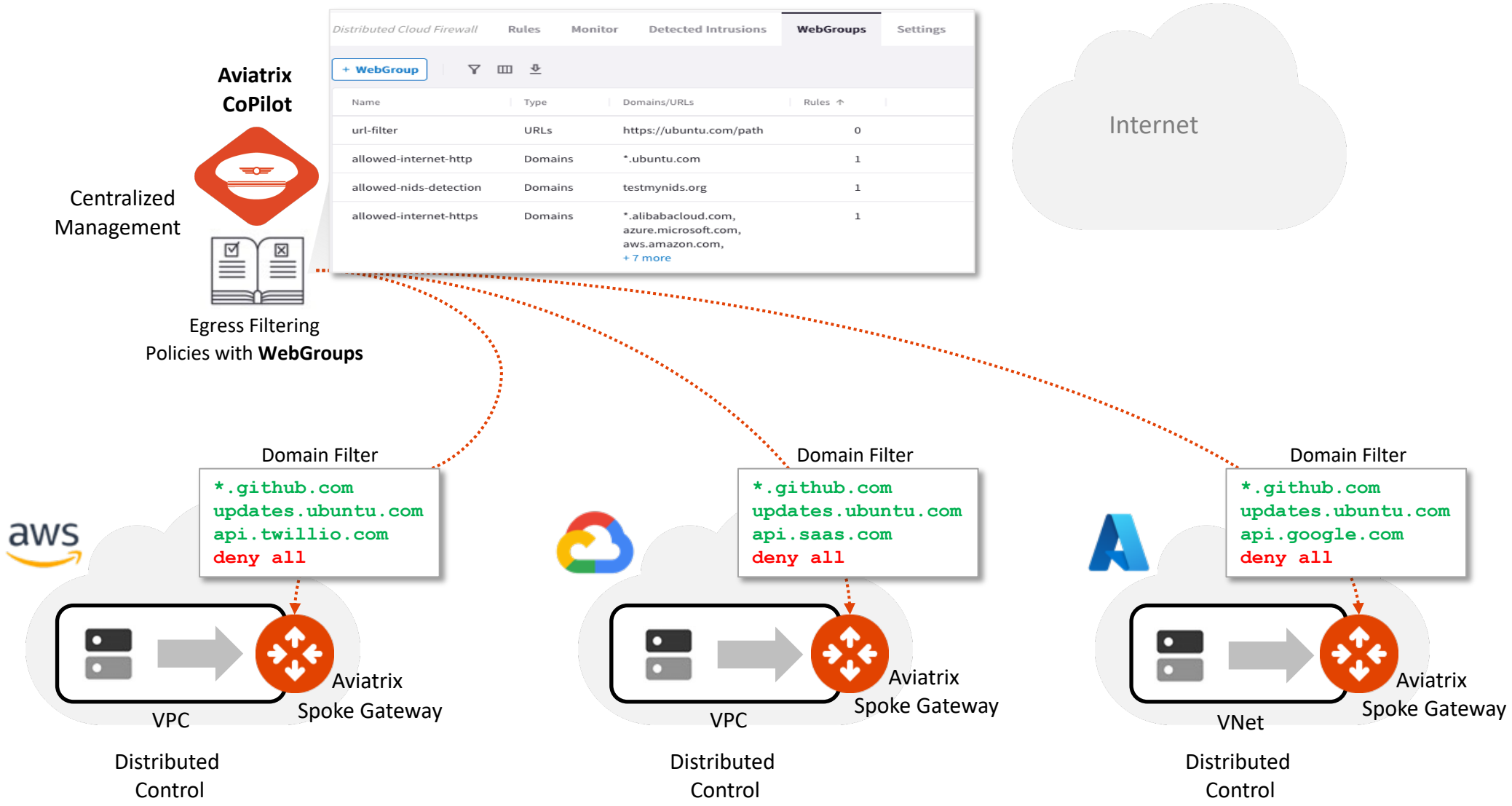
Aviatrix Secure Egress Filtering Feature



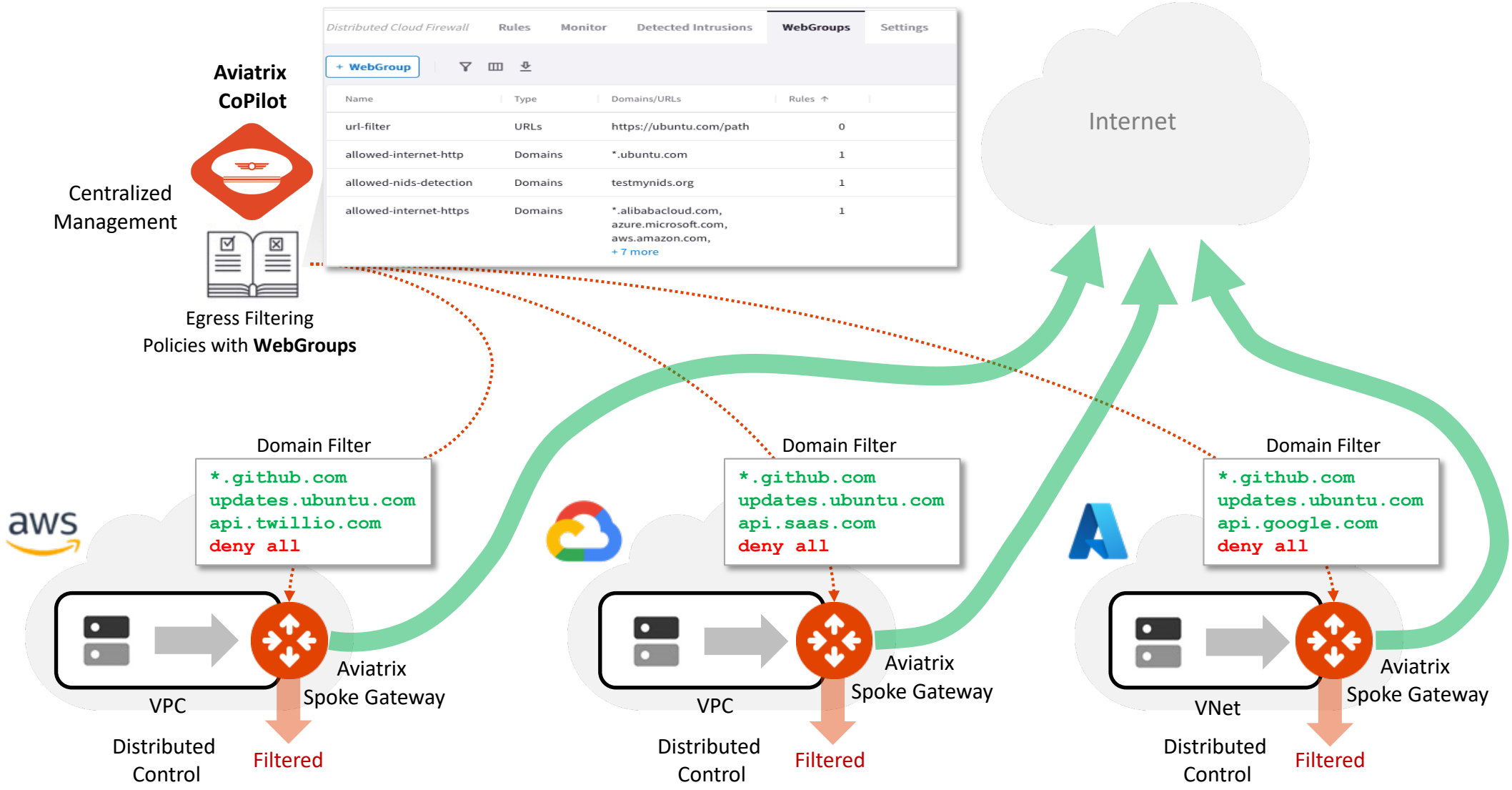
Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering

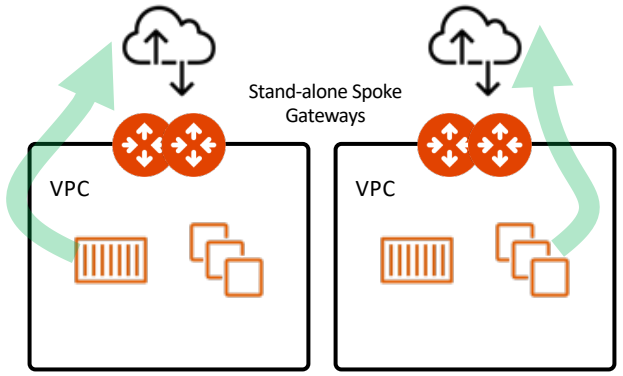


Aviatrix Secure Egress Filtering

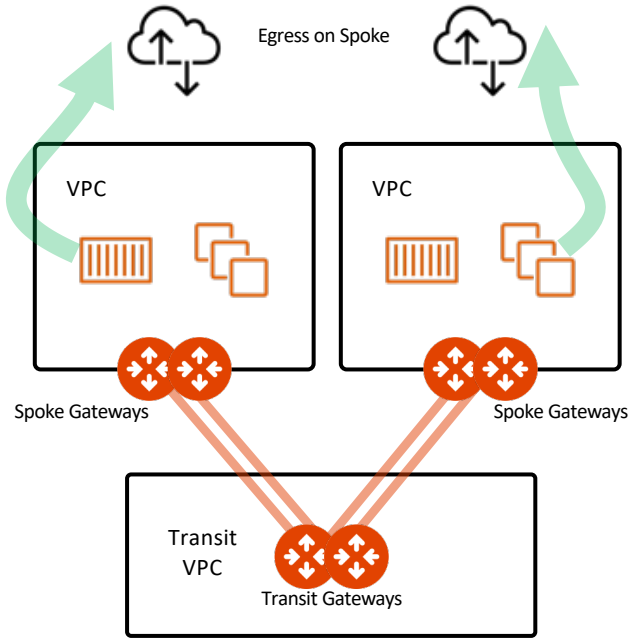


Aviatrix Secure Egress Filtering Design Patterns

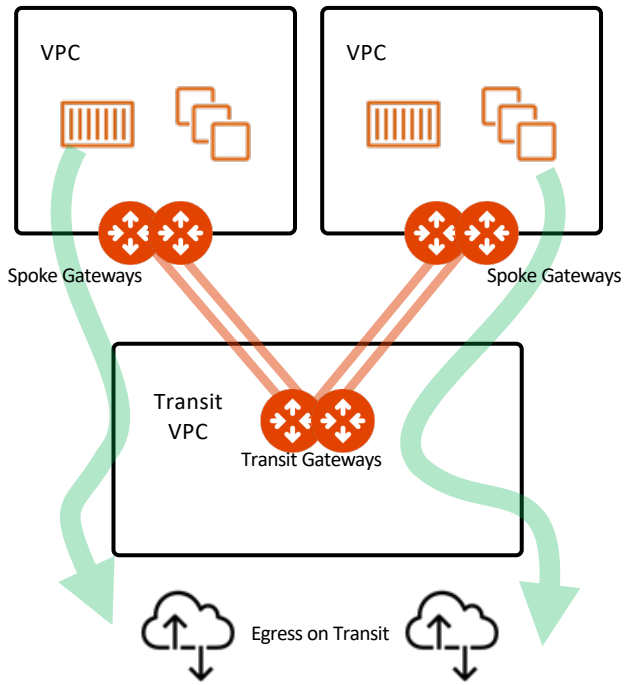
Stand-alone Spoke GW (Distributed)



Local Egress (Distributed) with Aviatrix Spoke GW



Centralized Egress with Aviatrix Transit GW



Zero Touch Network Access

There are two possible models:

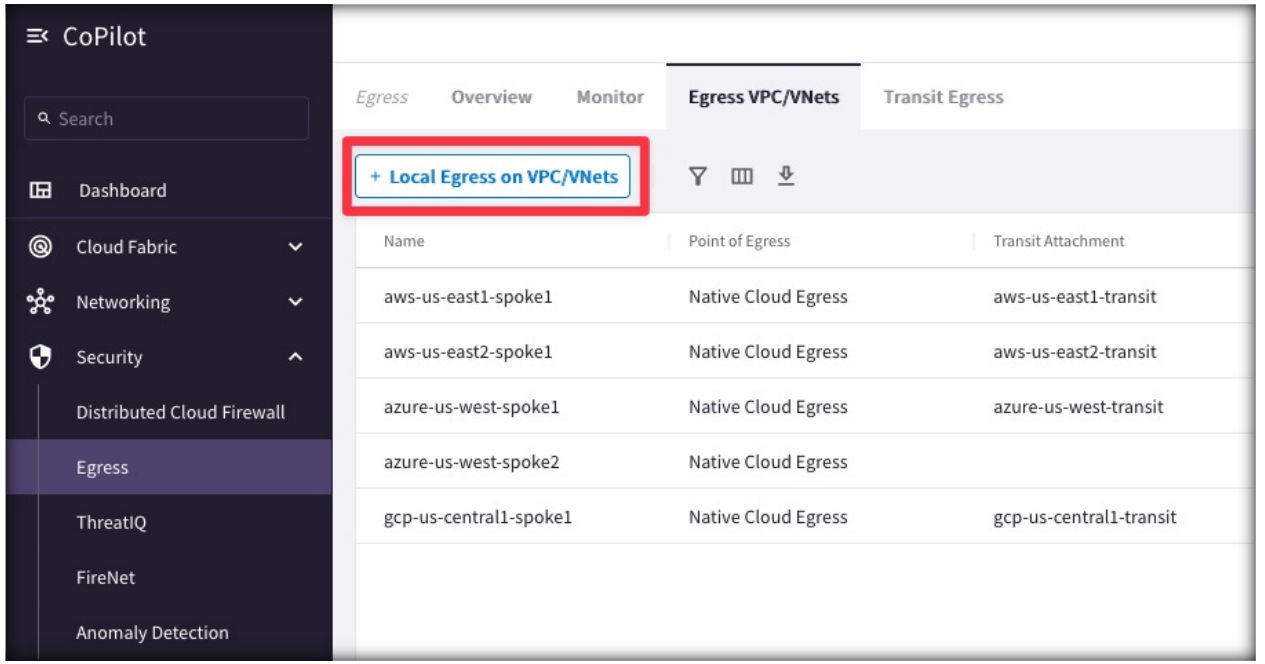
- **DENY LIST MODEL** (THREAT-CENTRIC MODEL):
  - allow all data to flow, except for exactly what you say should be stopped.

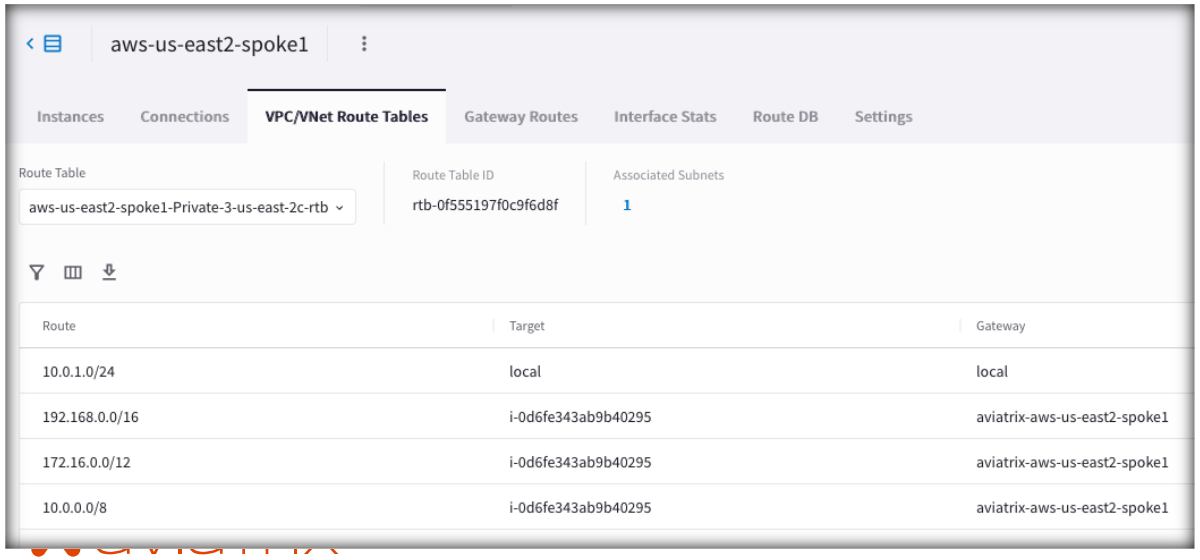
- **ALLOW LIST MODEL** (TRUST-CENTRIC MODEL):
  - deny everything and only permit what you explicitly allow.

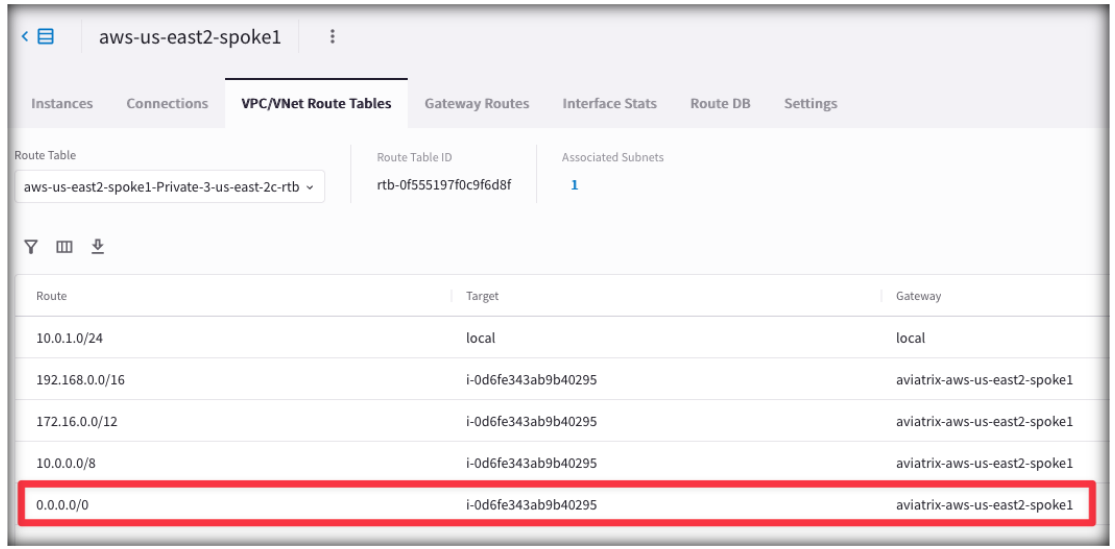
Tools for troubleshooting Egress

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.

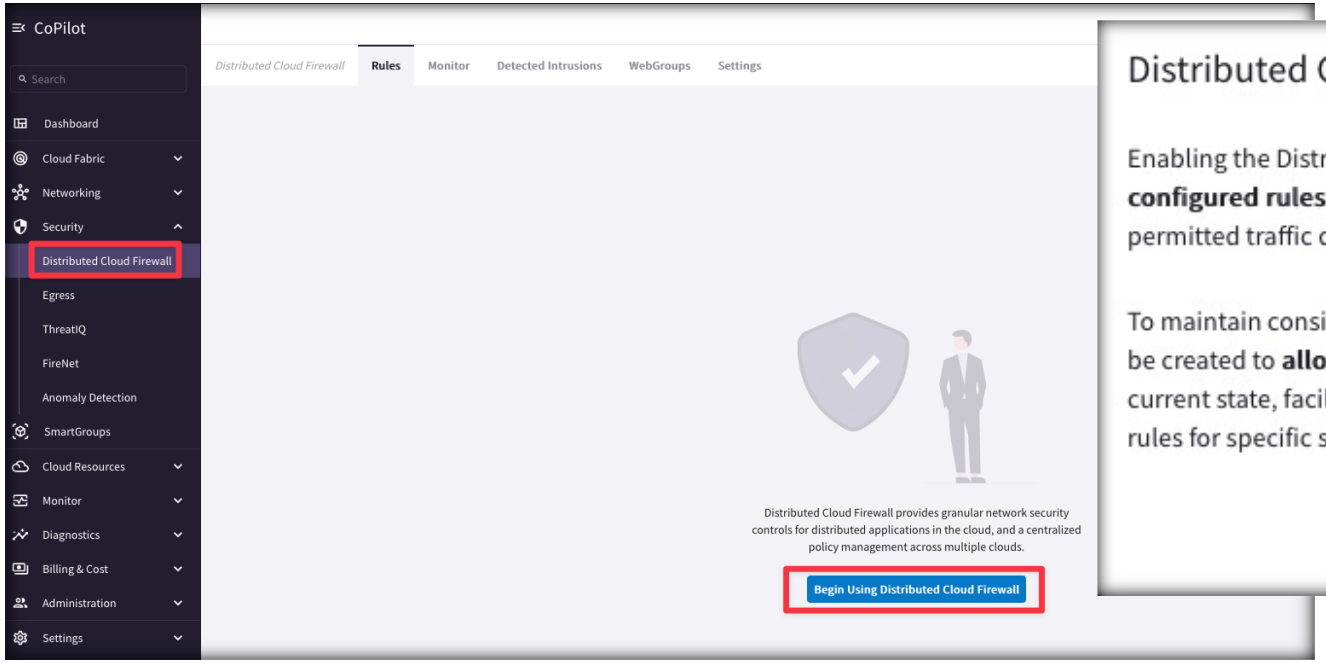


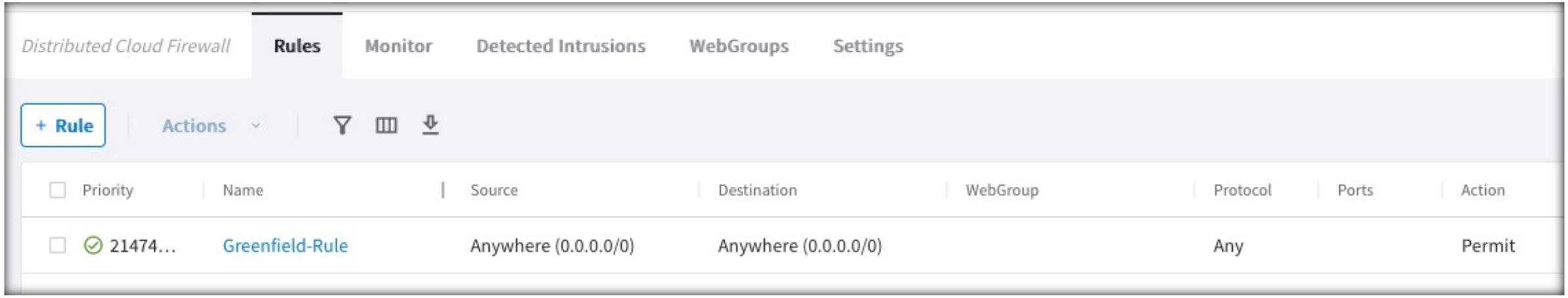




Adding Filtering/Monitoring feature to the Egress

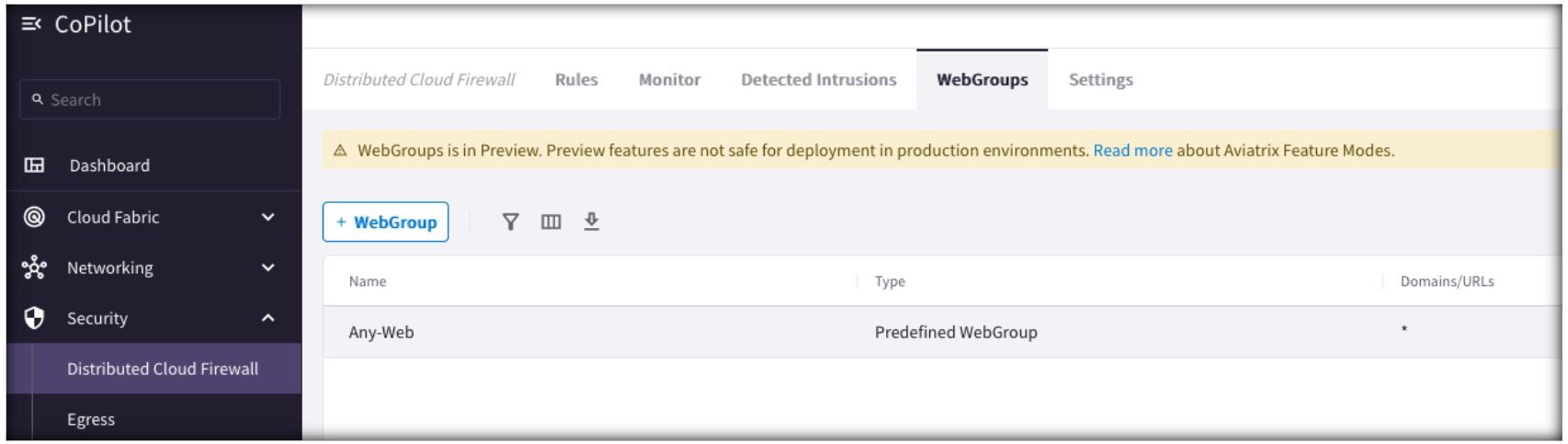
- The Egress control is part of the Distributed Cloud Firewall service.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.

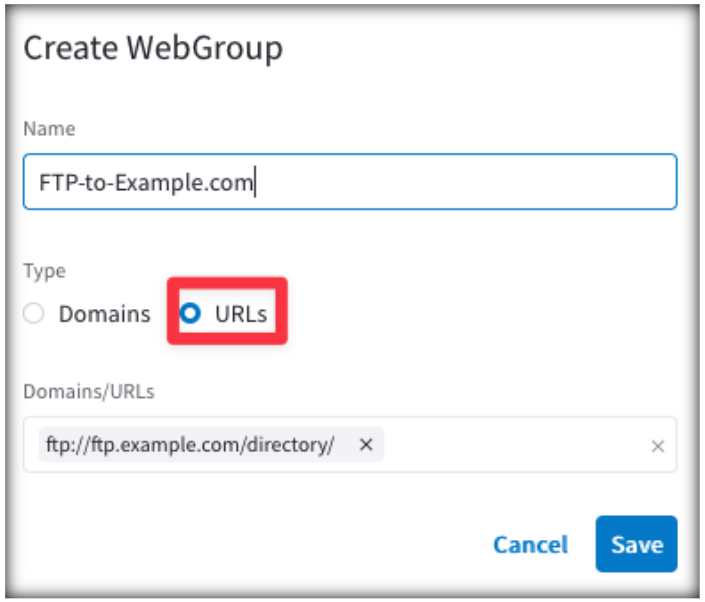


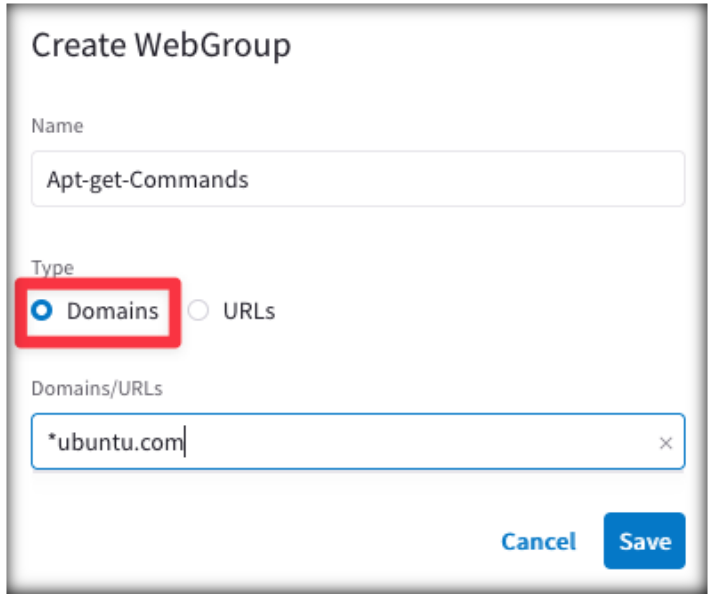


WebGroup Creation

- **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.

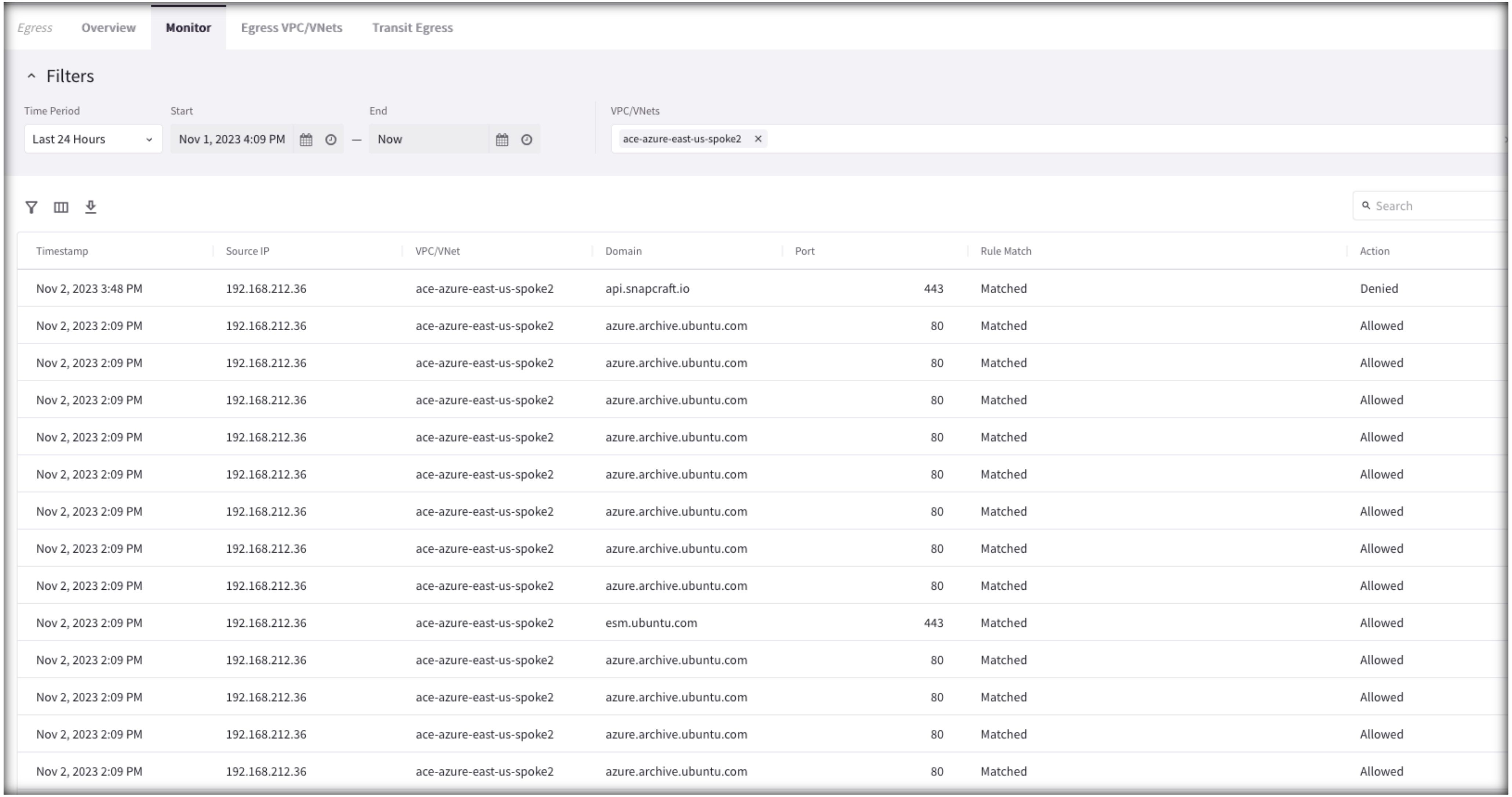






Monitor

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



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

Next:

Lab 7 Egress