Aviatrix Cloud Firewall

SECURE EGRESS

ACE Team

Problem Statement

Private workloads need internet access

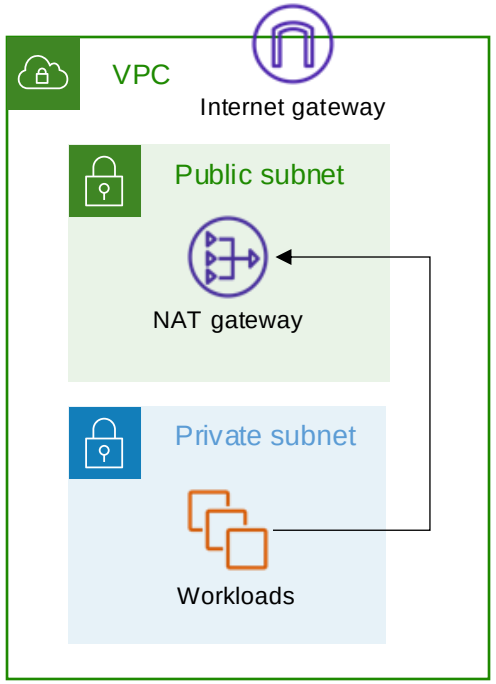
- **SaaS integration**

- **Patching**

- **Updates**

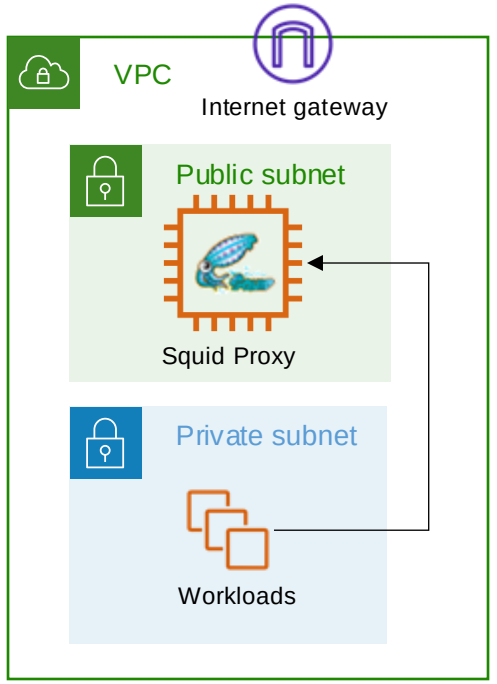
NAT Gateway

- Layer-4 only
- NACLs management



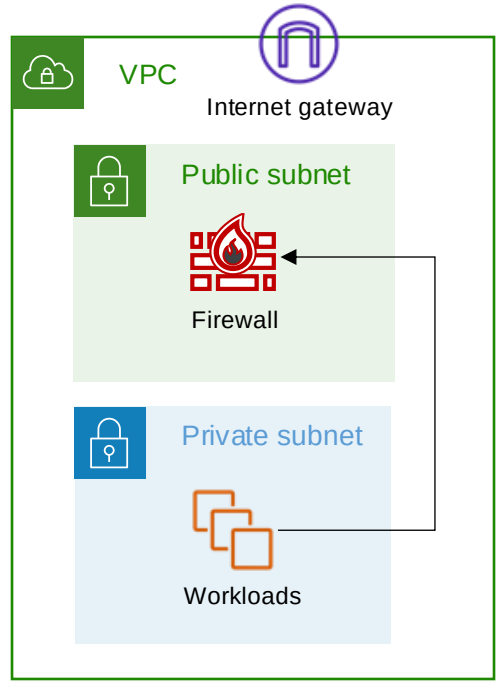
Squid Proxy

- Hard to manage
- Scale and HA issues

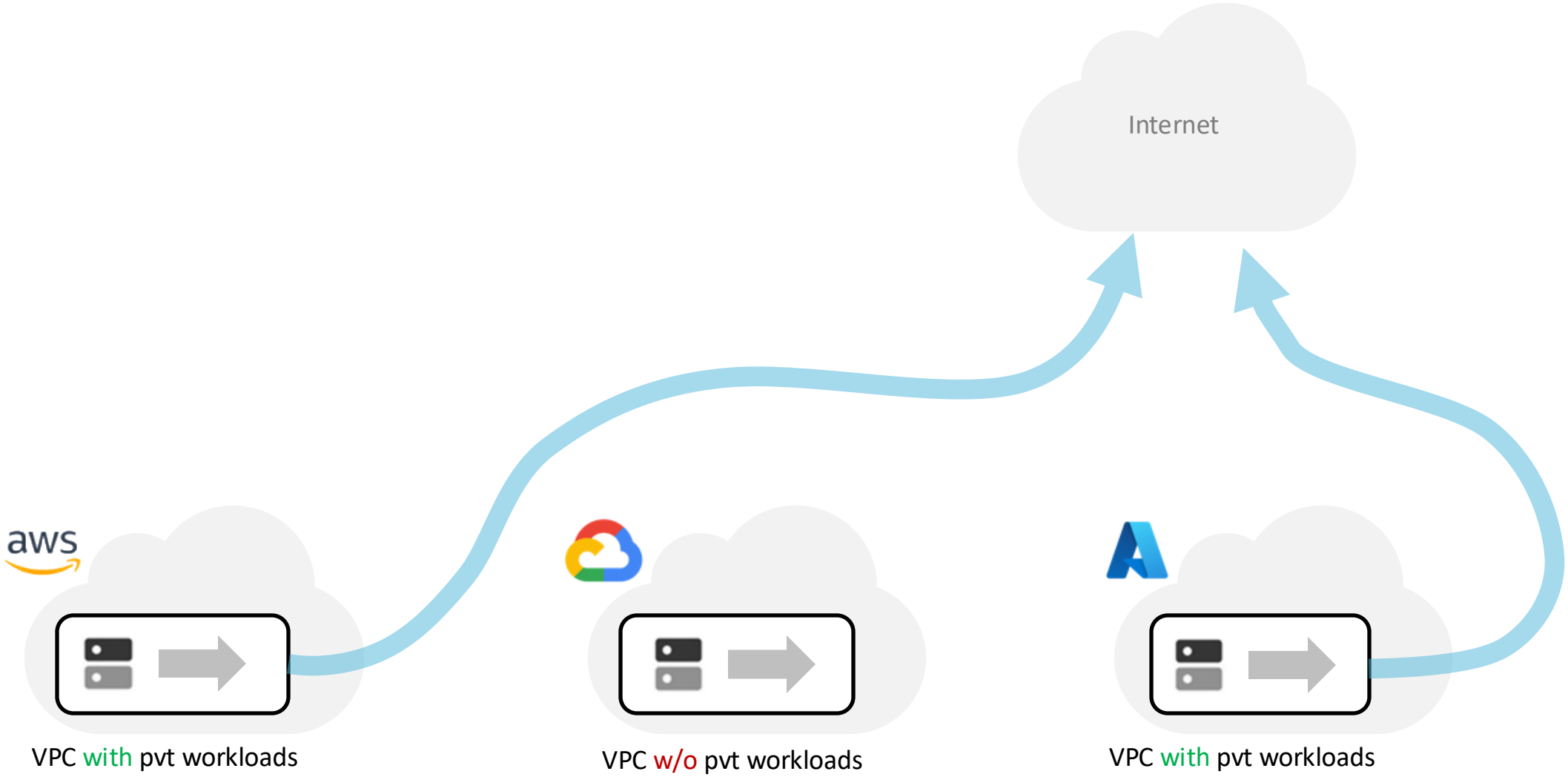


Layer-7 Firewall

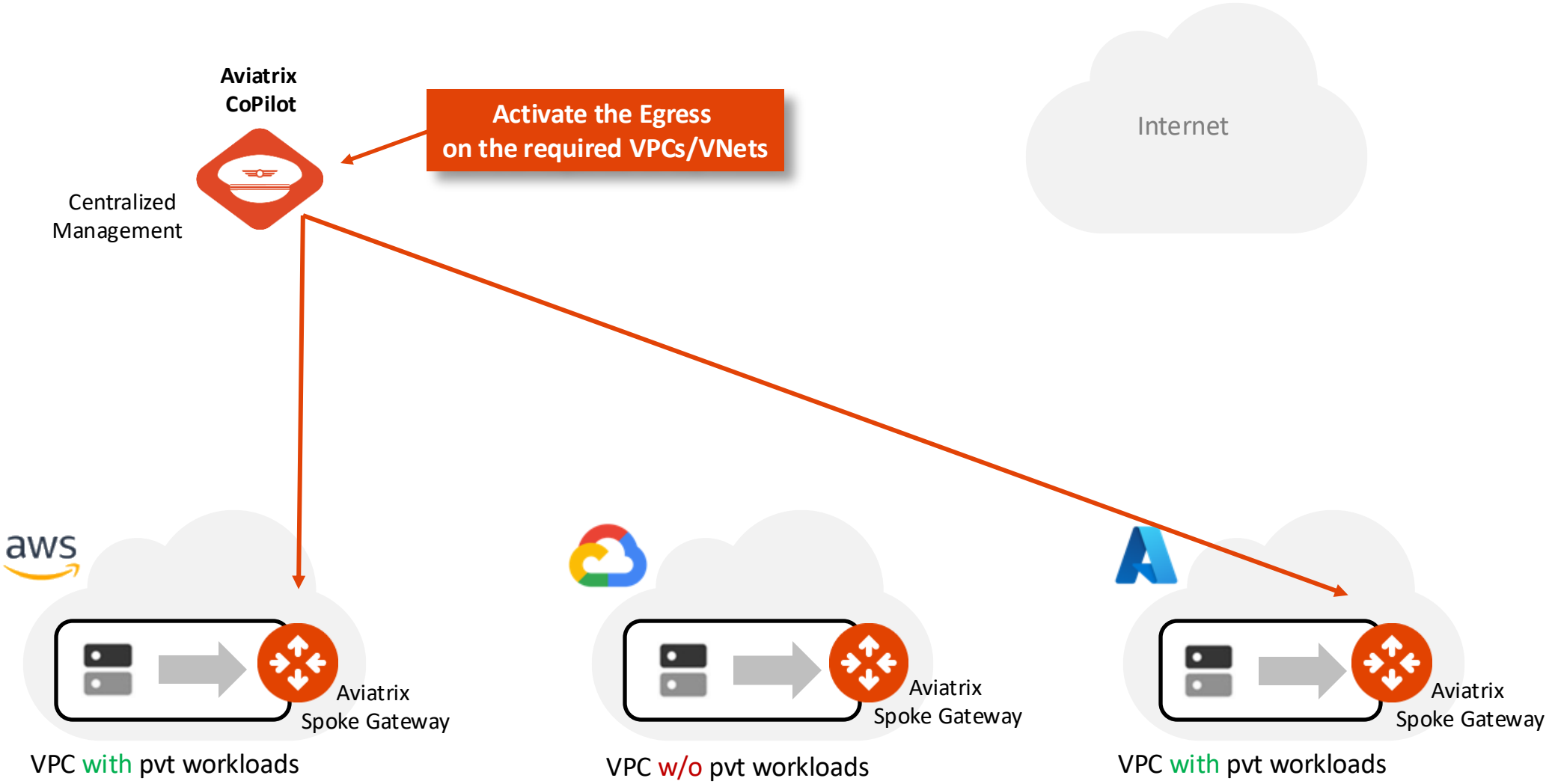
- Overkill
- Expensive



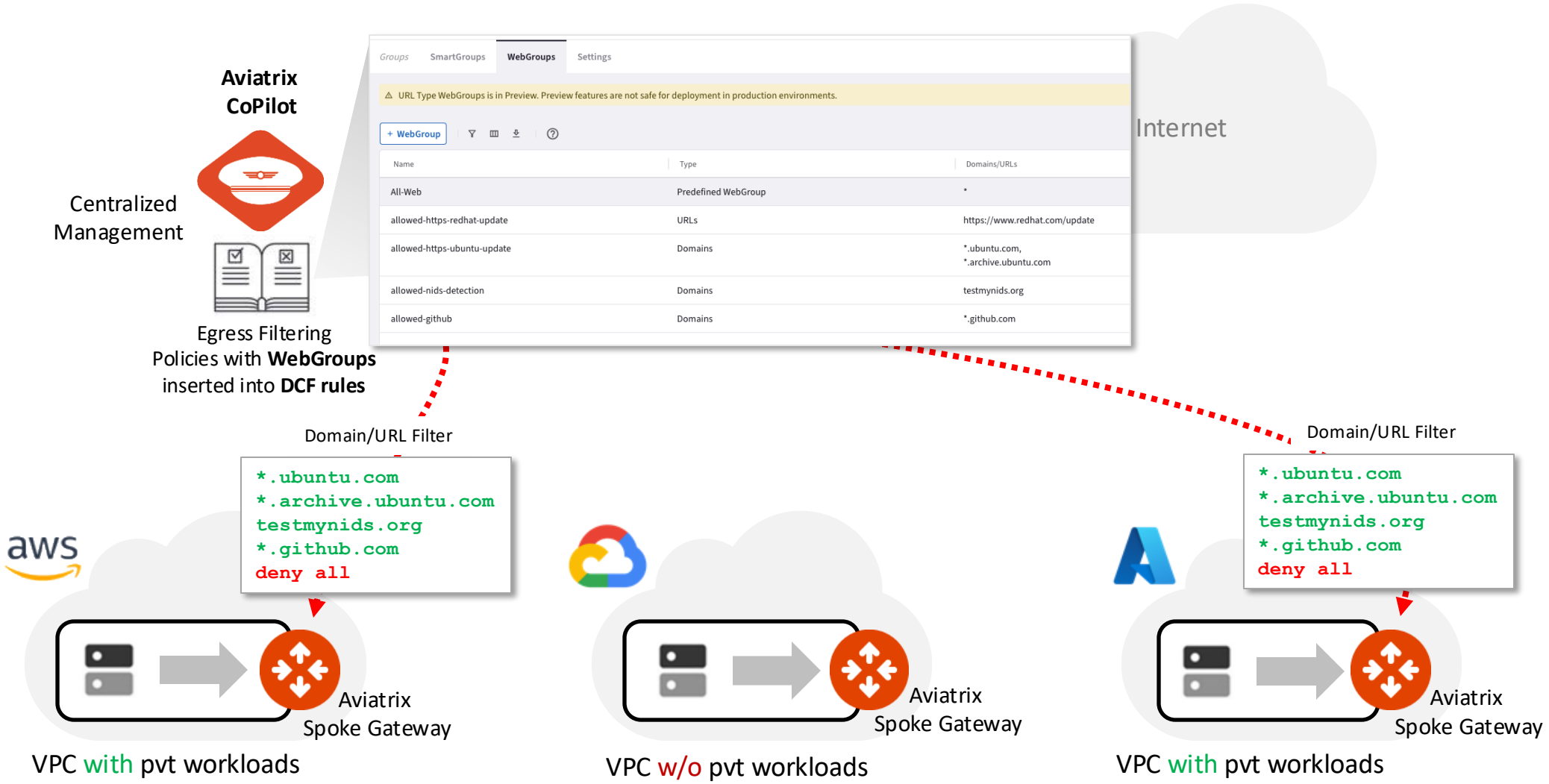
Aviatrix Secure Egress Filtering Feature



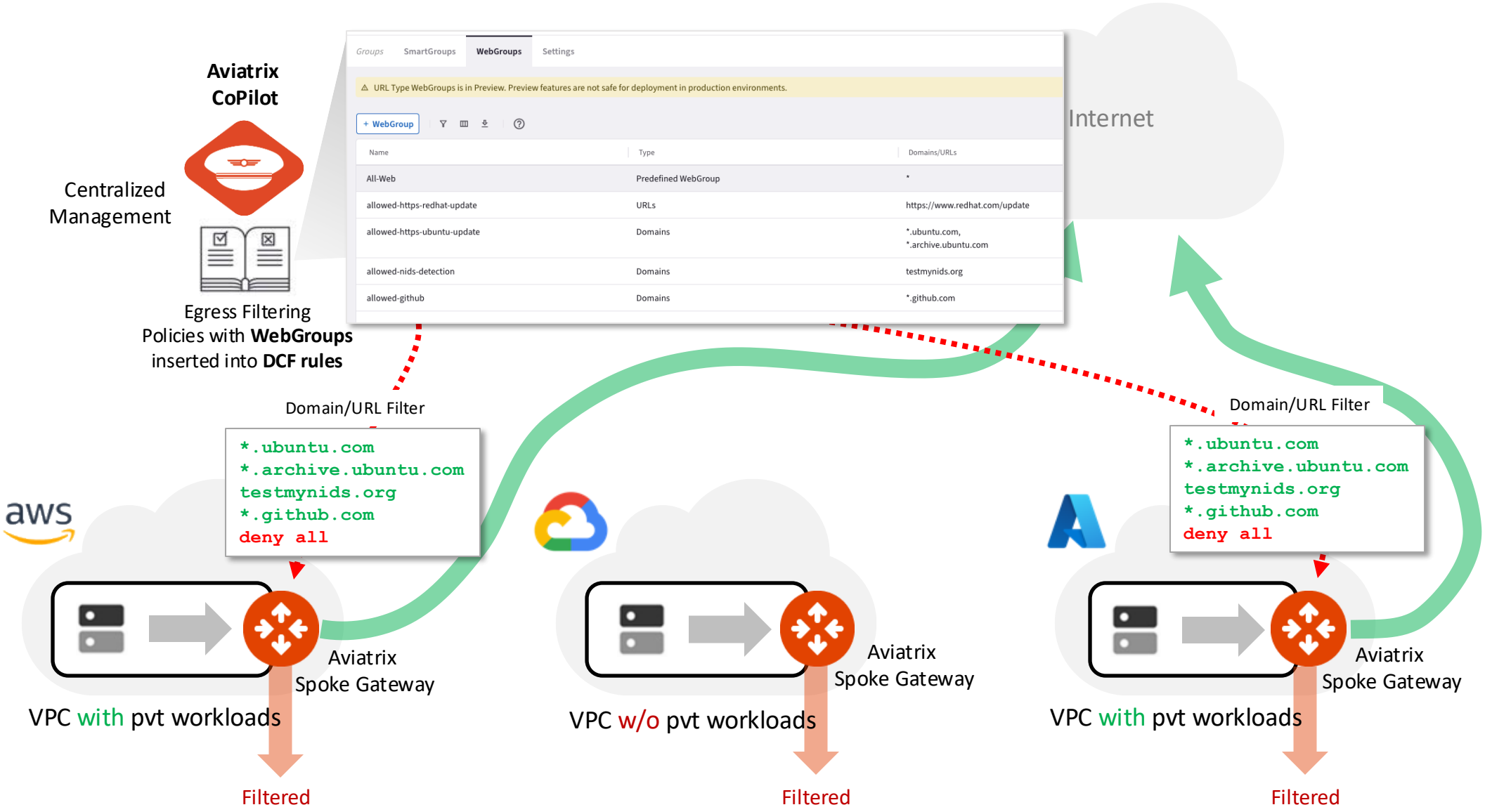
Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering



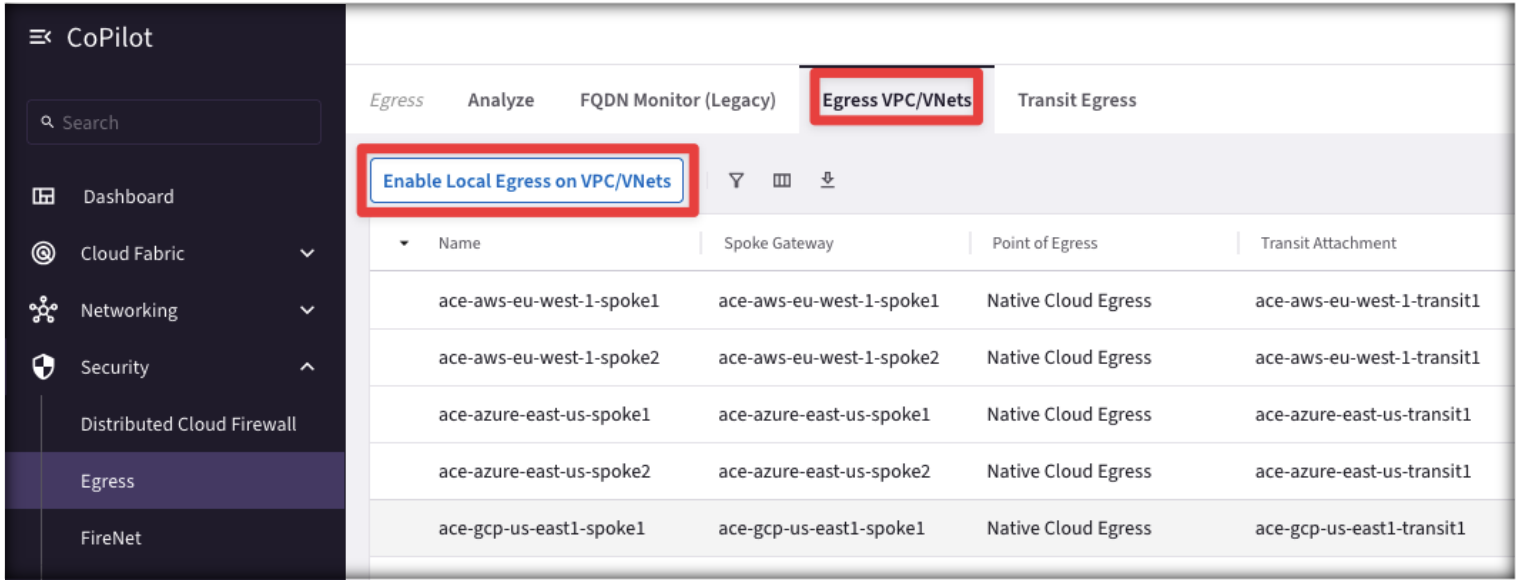
Aviatrix Secure Egress Filtering

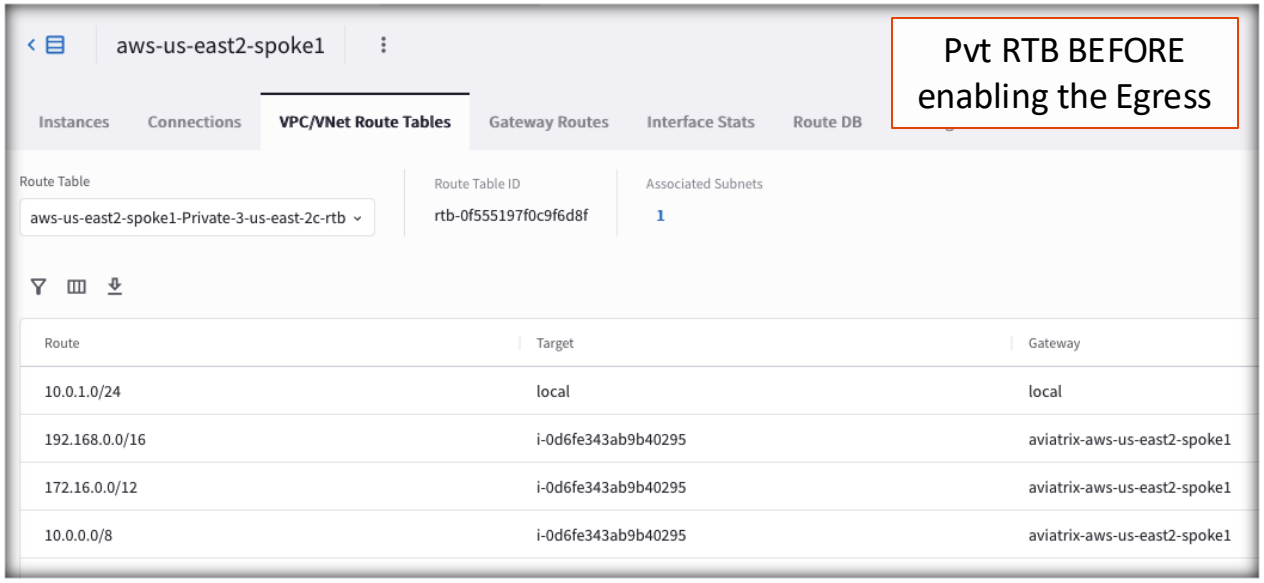


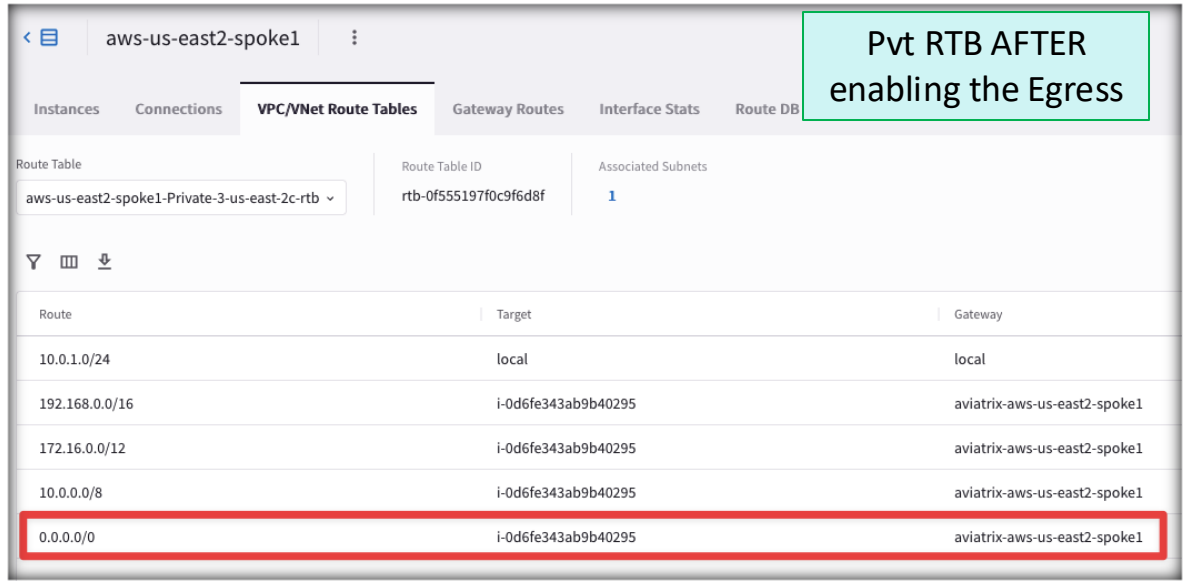
Tools for Troubleshooting Secure Egress

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.

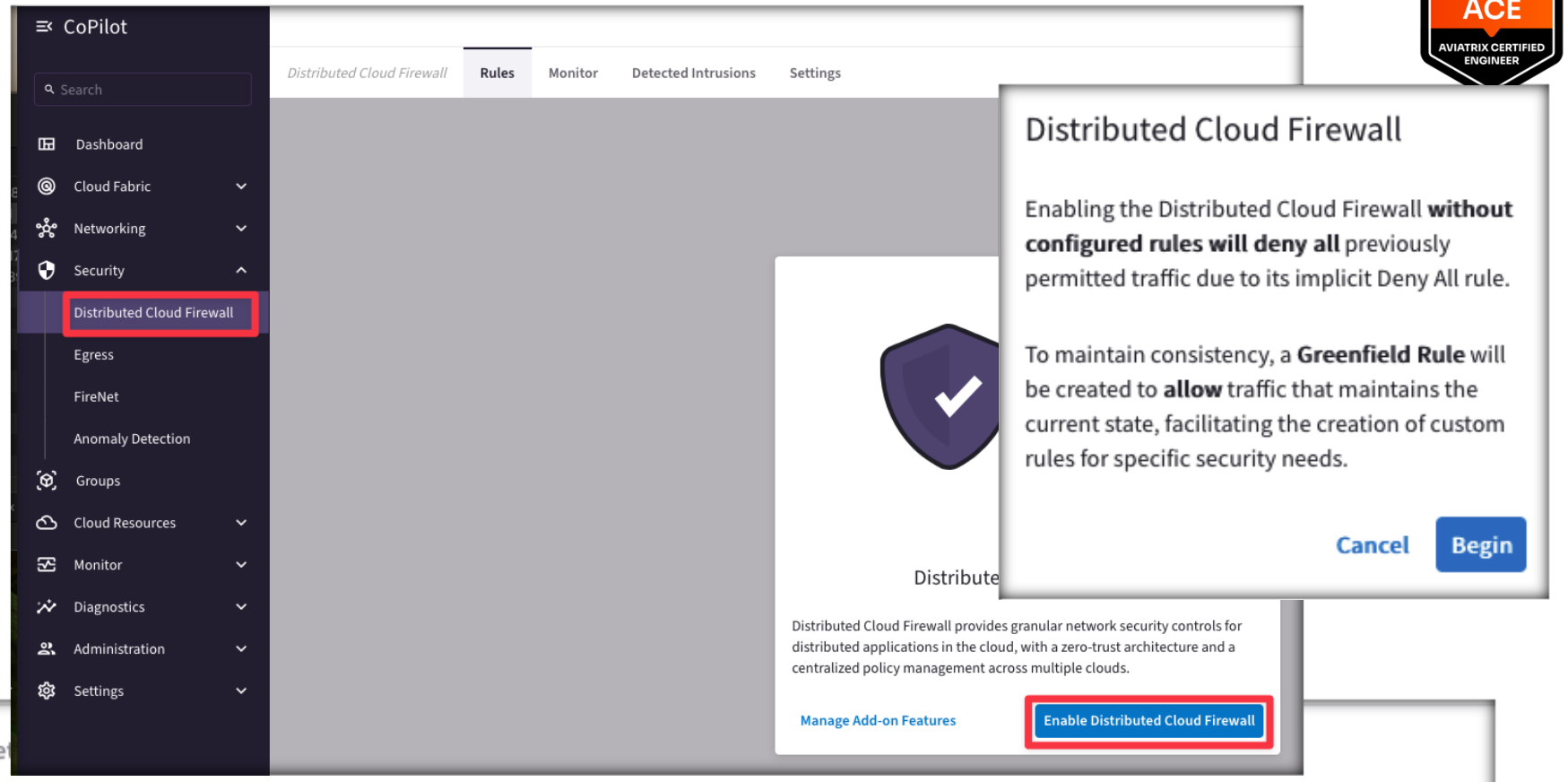


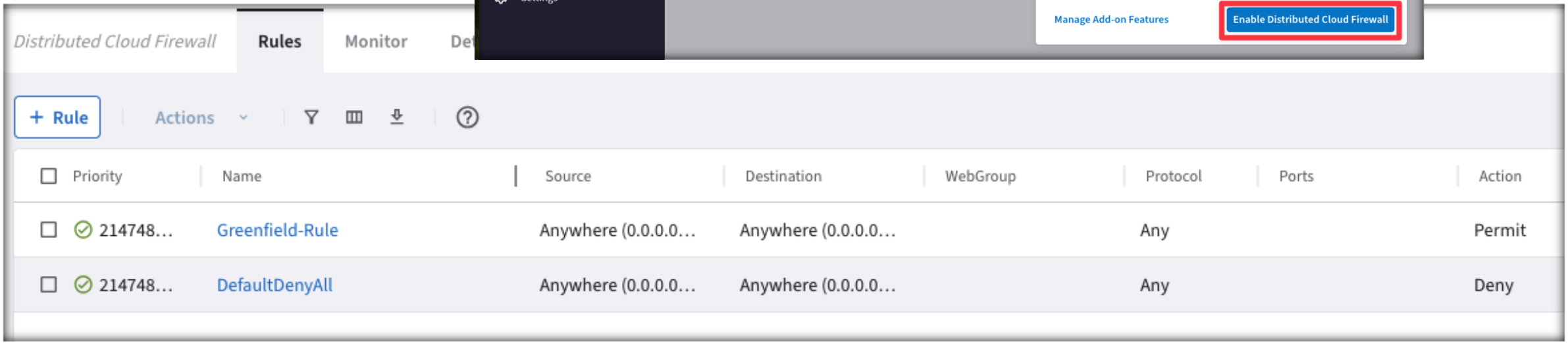




The Greenfield-Rule

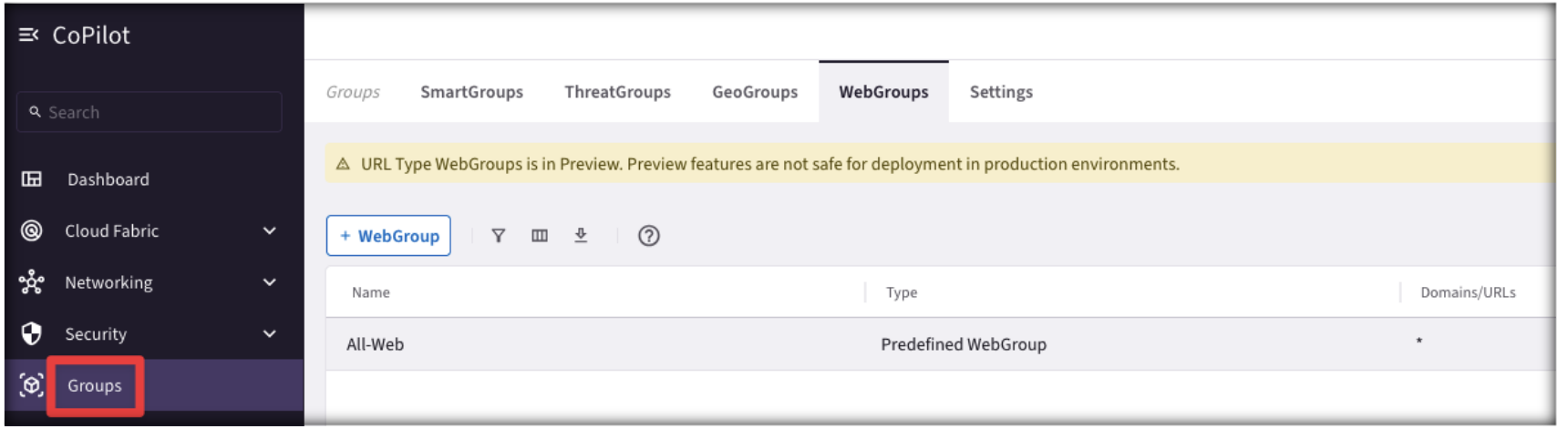
- If you want to apply policies on your Egress traffic, you must enable the Distributed Cloud Firewall.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.
- An Explicit Deny Rule, named **DefaultDenyAll,** is also added below the Greenfield-Rule.
- *Best Practice:* do not edit this rule, although it can be recreated if it is accidentally deleted.

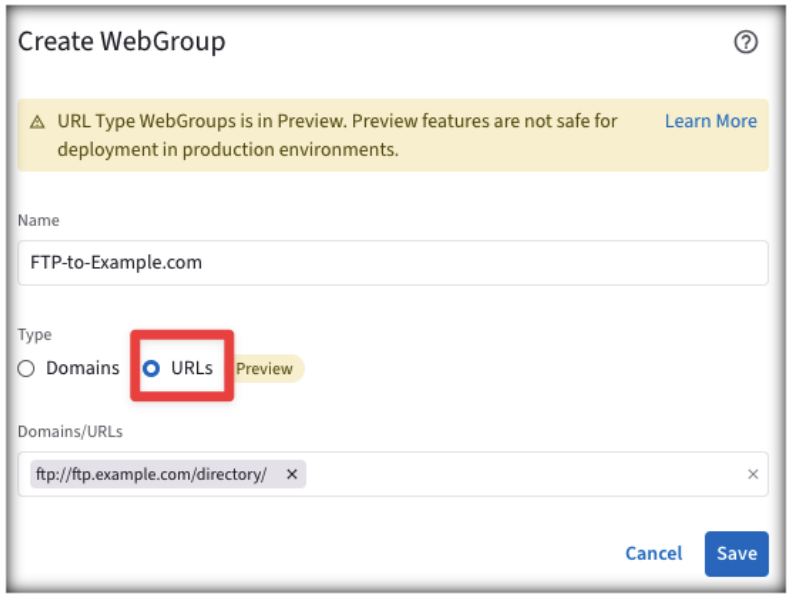


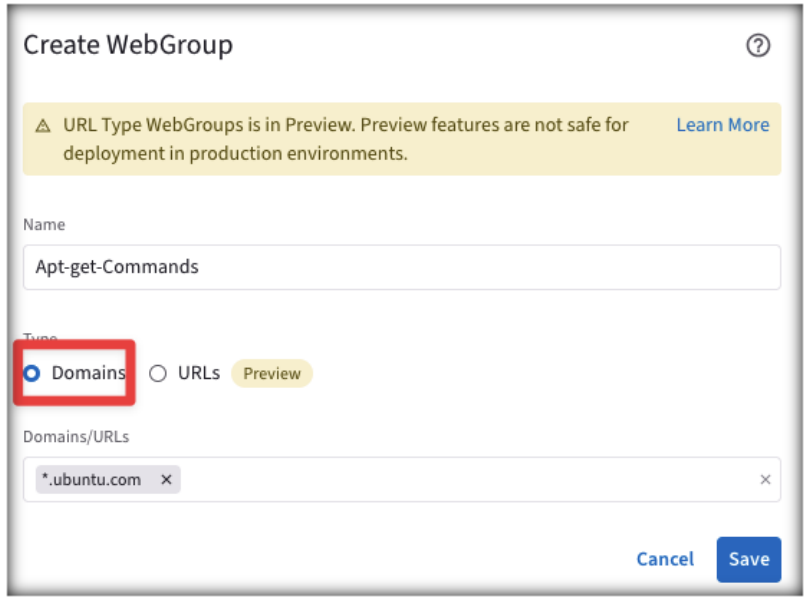


WebGroup Creation

- **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).



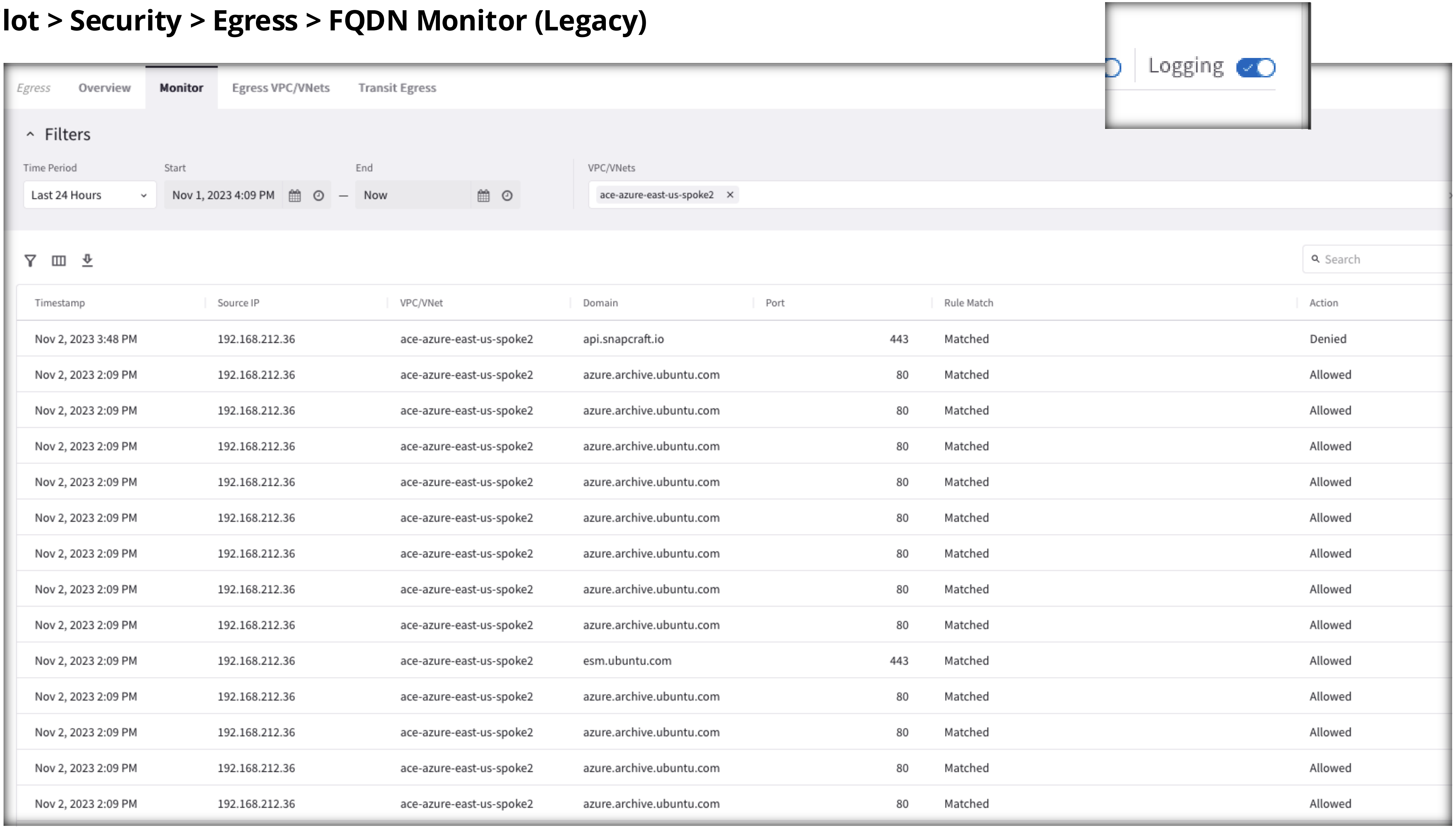




Monitor

CAVEAT: Logging must be enabled

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



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

Next:

Lab 7 Aviatrix Cloud Firewall