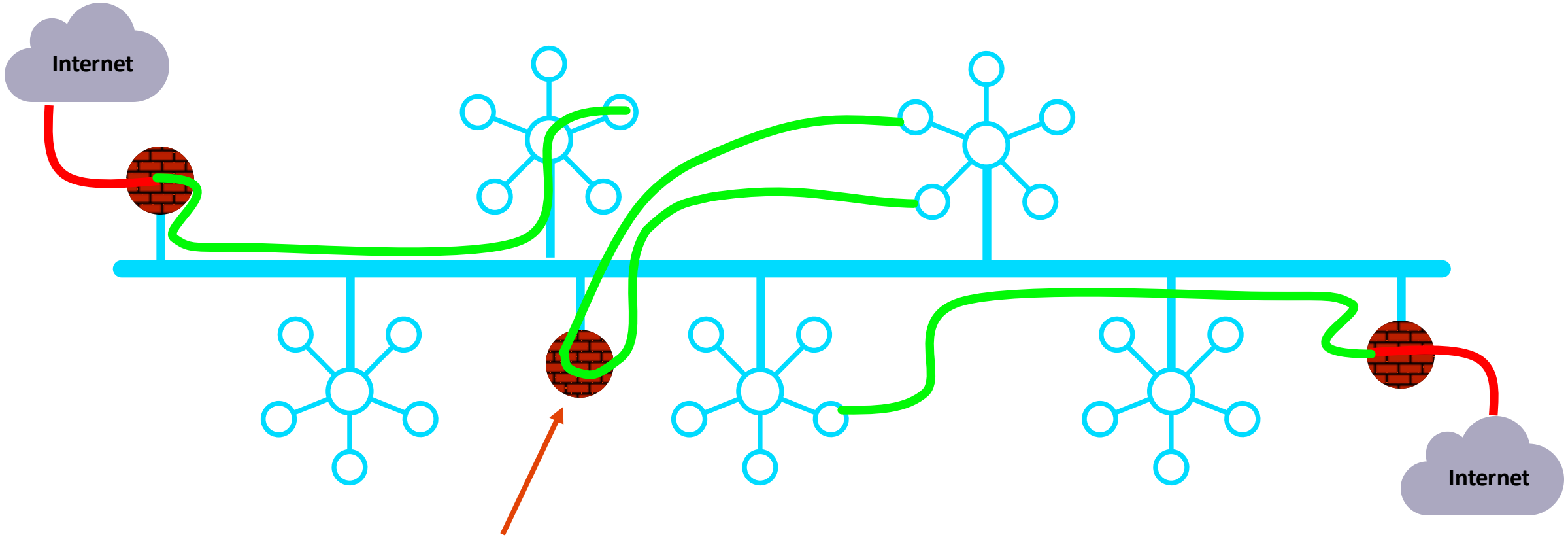
Distributed Cloud Firewall

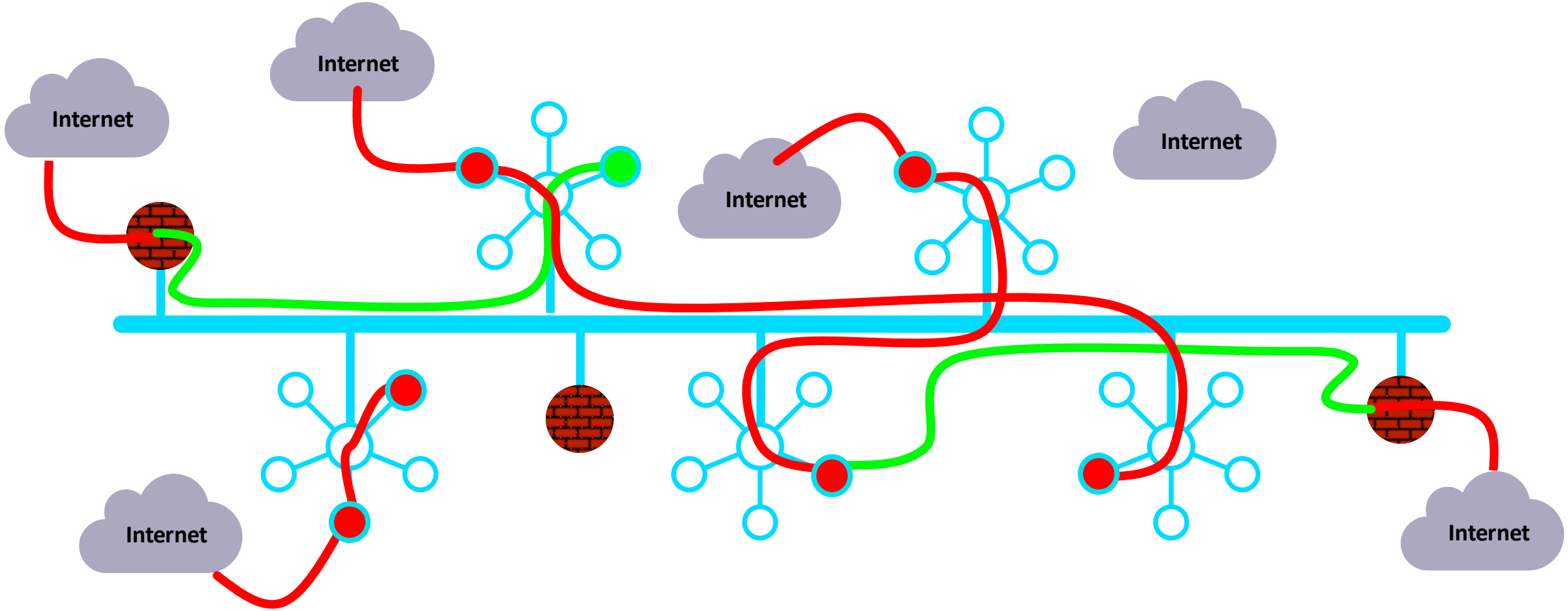
ACE Team

As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…

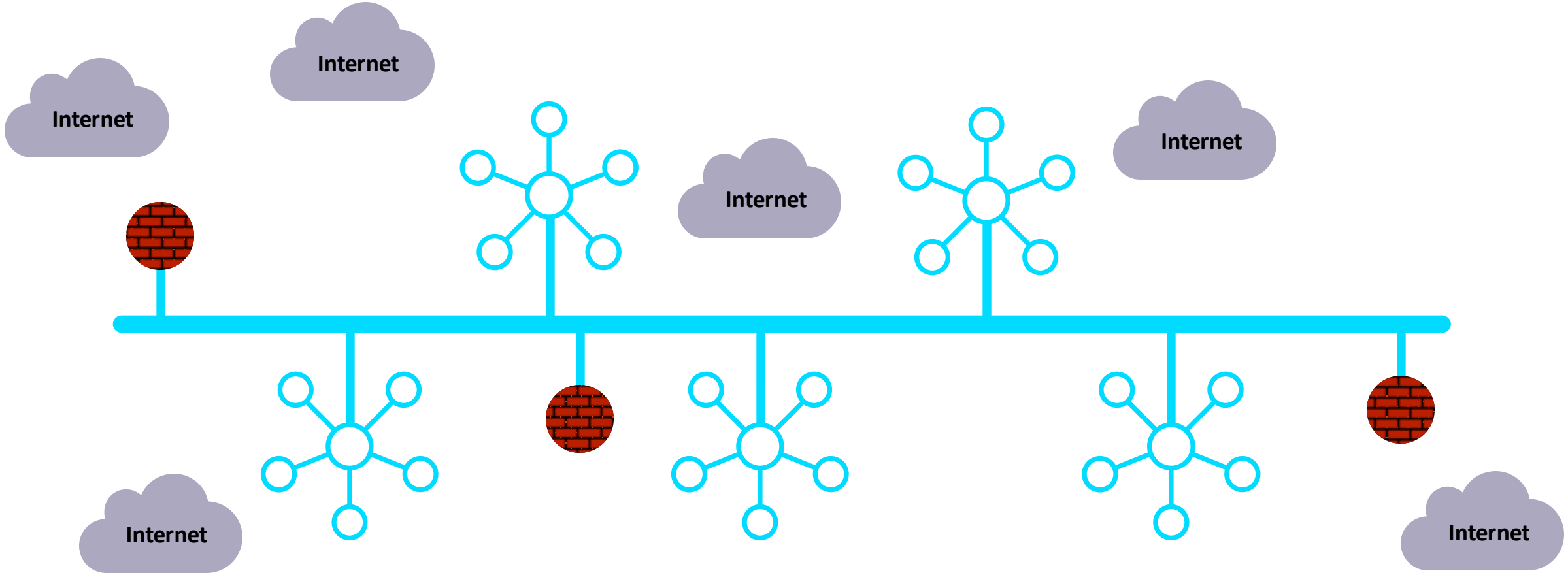


"Last Generation Firewalls"

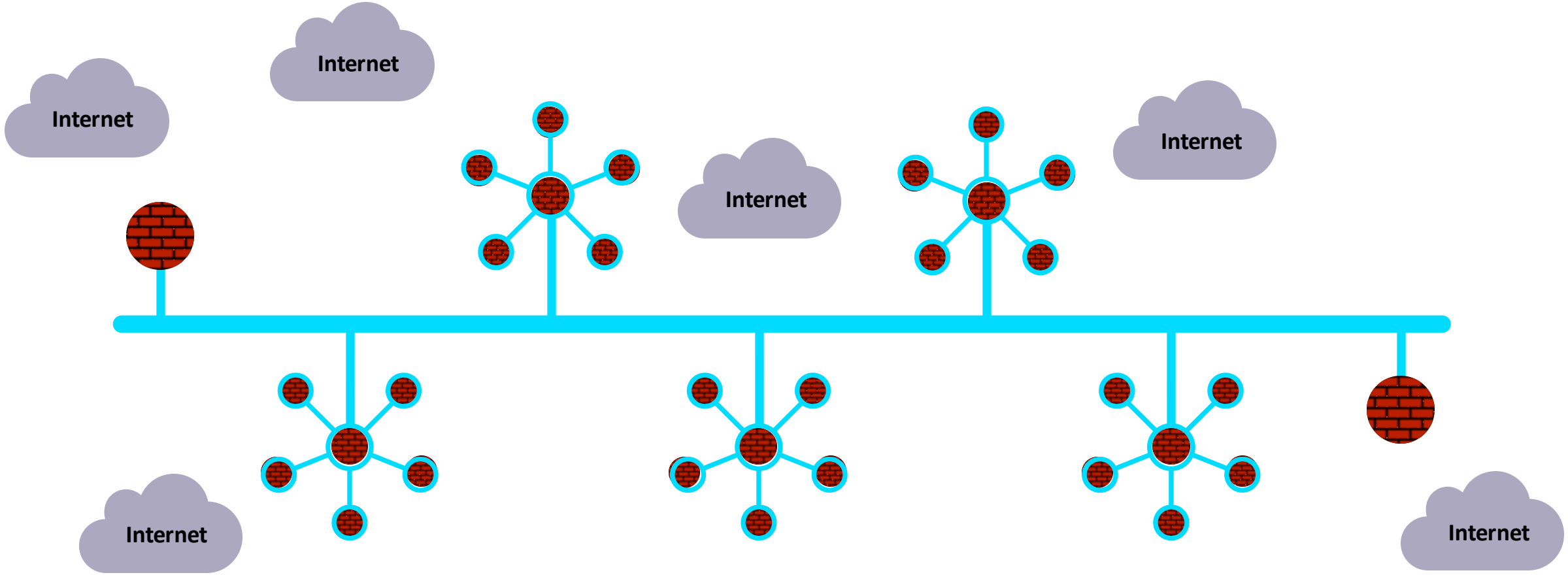
In Reality…



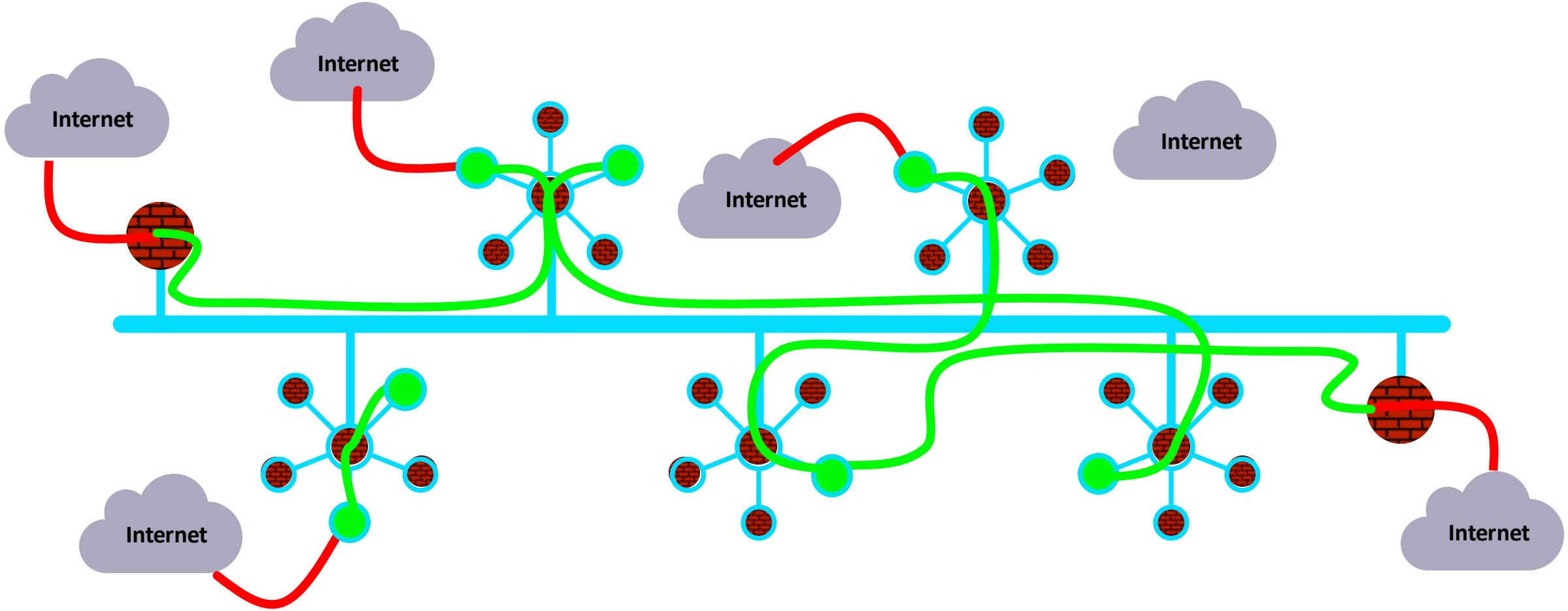
What If… the architecture was built for cloud



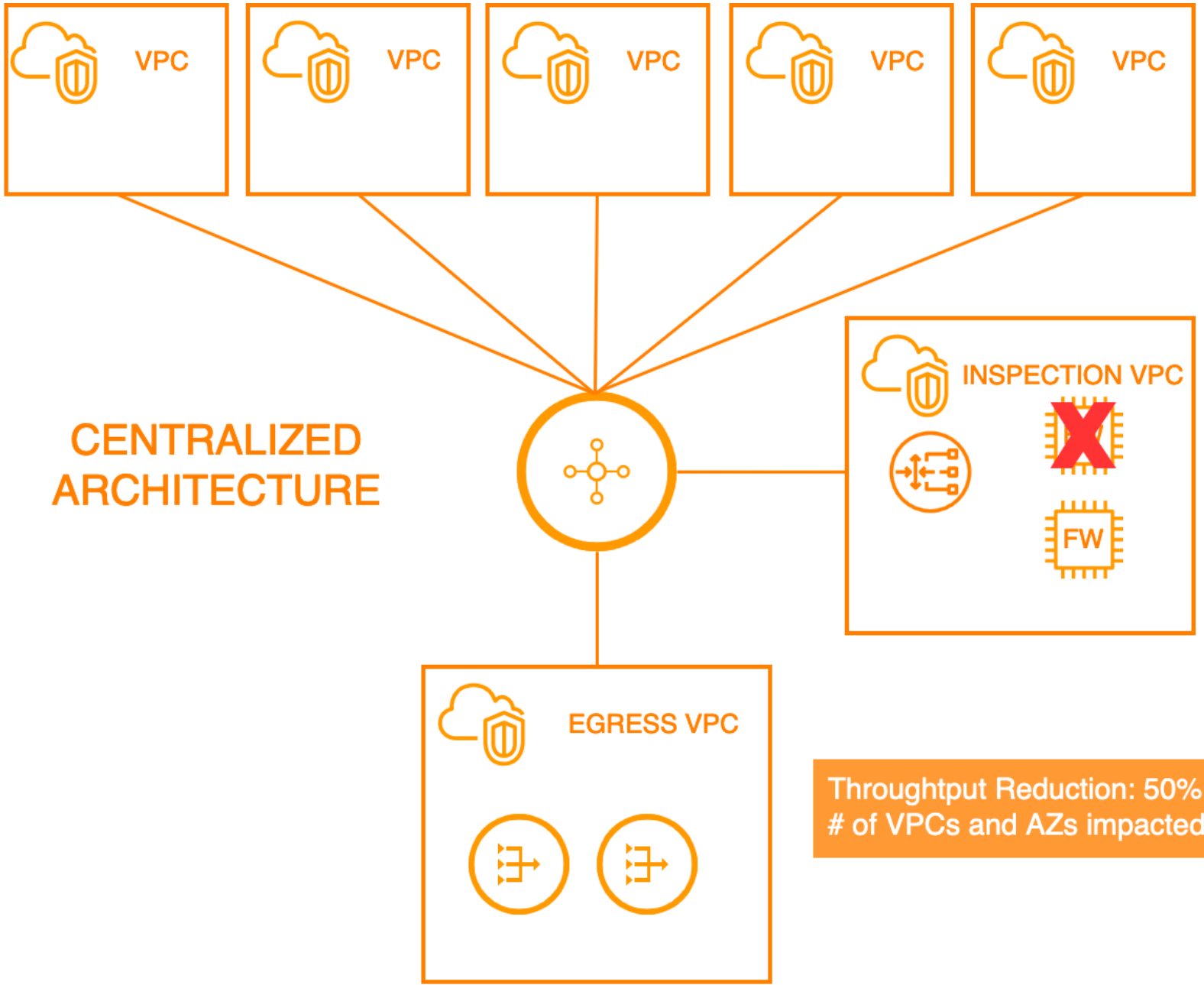
Firewalling Functions were Embedded in the Cloud Network Everywhere…



Distribution of the Security Services into the Spokes

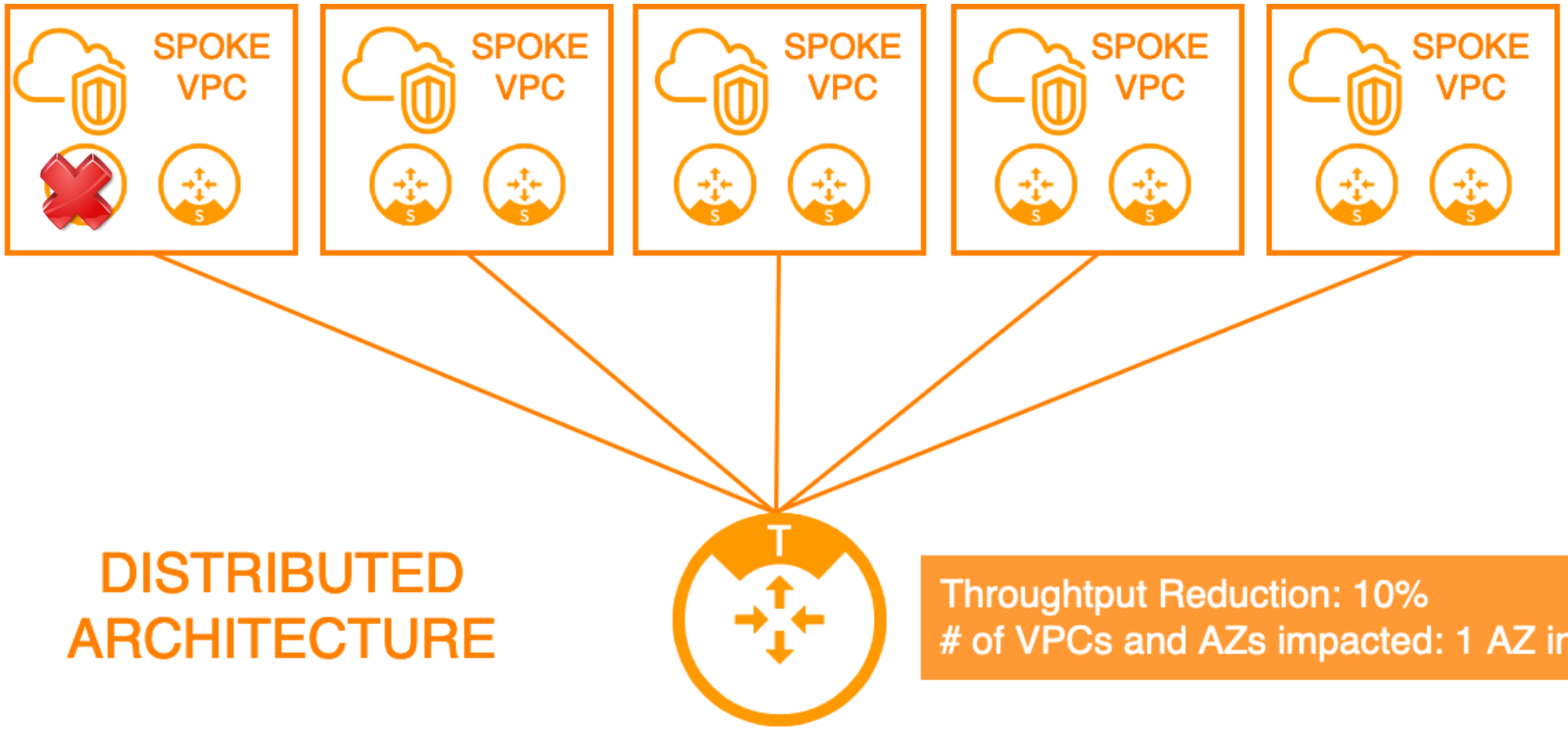


Impact of Failure – Centralized Architecture



Throughtput Reduction: 50%
# of VPCs and AZs impacted: ALL

Impact of Failure – Distributed Architecture



DISTRIBUTED ARCHITECTURE

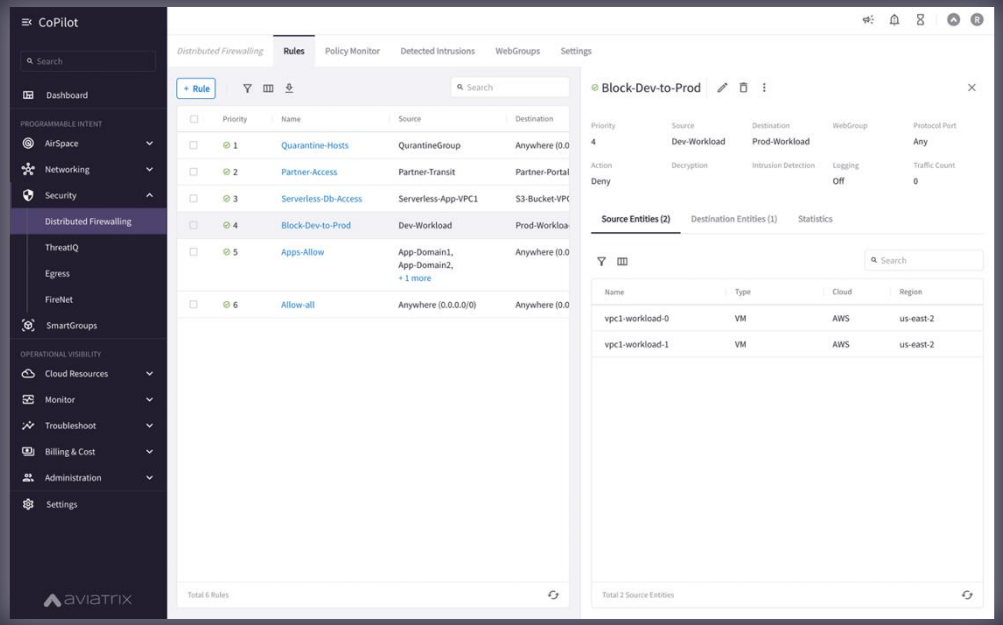
Throughtput Reduction: 10%
# of VPCs and AZs impacted: 1 AZ in 1 VPC

Centralized Vs Distributed Firewalling Architecture

Aspect	Cloud Centralized Firewall Model	Aviatrix Distributed Cloud Firewall
Blast Radius (Fault Tolerance and Resilience)	Single point of failure risks, although mitigated by redundant systems; still, failure can affect entire network traffic.	Enhanced fault tolerance by distributing firewalls, reducing impact of localized failures and increasing overall network resilience.
Performance	Potential latency issues due to traffic bottlenecks through a centralized point; performance can degrade under high load.	Optimized for low latency by distributing firewall capabilities close to application workloads, improving overall network performance.
Cost	Maintaining centralized Firewall architectures is increasingly expensive. Cloud providers and firewall vendors profit from costly data processing charges, oversized VMs, and pricey licenses.	DCF's cloud-native design enables organizations to sidestep the costly data processing fees, oversized virtual machines, and exorbitant licensing often encountered with traditional centralized models.
Deployment Speed	Longer deployment times due to hardware installations and configurations.	Quick deployment and provisioning, leveraging cloud-native tools for rapid scaling and implementation
Noisy Neighbor	Since all network traffic is funneled through a limited set of centralized appliances, high traffic from one tenant or application can degrade the performance of others sharing the same resources	Effectively mitigates the "Noisy Neighbor" issue through its decentralized design

And, What If Policy Creation Looked Like One Big Firewall…

Centralized Policy Creation → Distributed Enforcement



Aviatrix CoPilot

SURICATA IDS / IPS

Micro-Segmentation

Threat Prevention

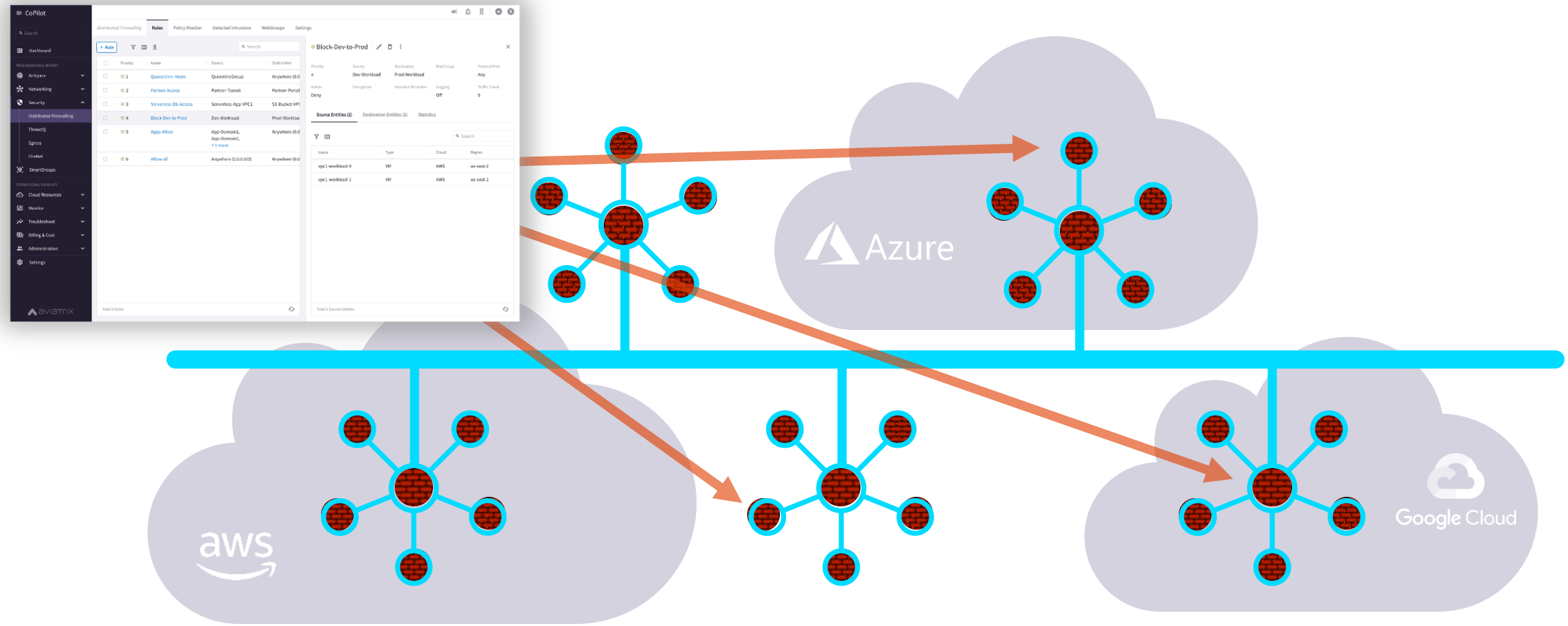
Advanced NAT

Distributed Firewalling

Decryption

URL Filtering

Policy Creation Looked Like One Big Firewall … A Distributed Cloud Firewall…



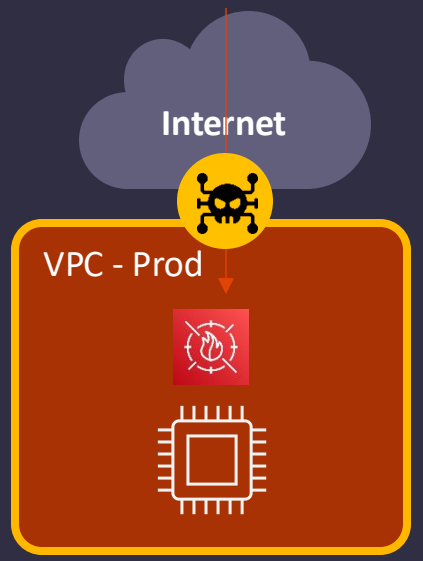
Where and How Policies Are Enforced Is Abstracted…

Firewall The 3 Perimeters

Aviatrix Solution

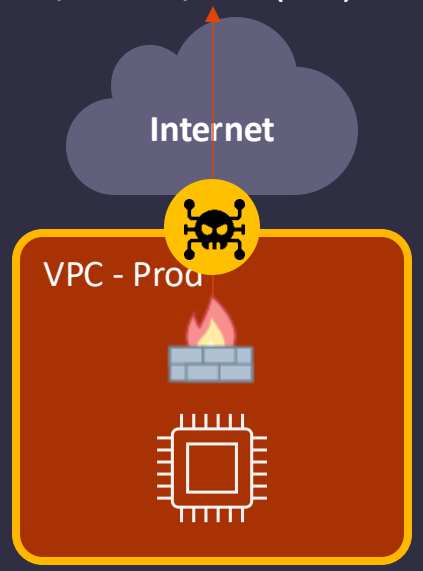
Easy Ingress

- **Why?** Detect and Block MITRE ATT&CK™ Recon, Initial Access, and Execution Phases. OWASP Top 10
- **Tools:**
  - Cloud-Native WAF and DDoS
  - CloudFlare, Akamai, F5



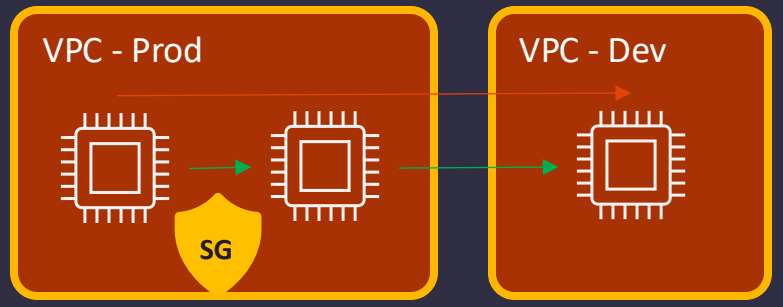
Easy Egress

- **Why?** Detect and Block MITRE ATT&CK™ Establish Execution, Command and Control and Data Exfil Phases
- **Tools:**
  - NAT Gateways
  - Network Firewalls
  - URL/FQDN/IDS (IPS)



Moderate East-West

- **Why?** Detect and Block MITRE ATT&CK™ Lateral Movement Phase
- **Tools:**
  - Network Firewalls
  - Security Groups
  - Agents
  - L4, Microsegmentation, Zero Trust



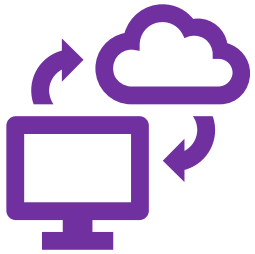
SmartGroups: Definition

- A firewall rule consists of two important initial elements (i.e. *L3 info*):
  - **Source**
  - **Destination**

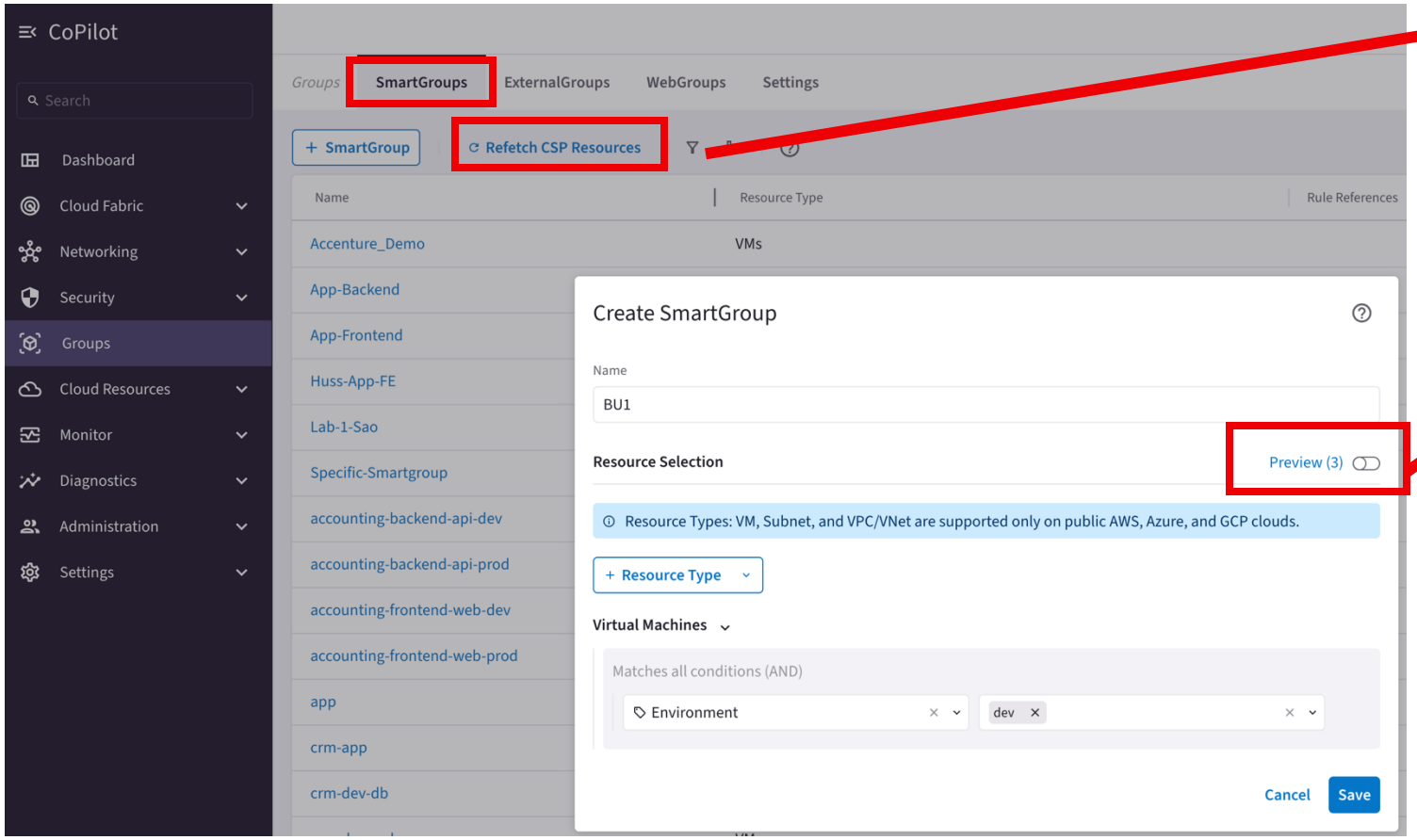
- **What is a SmartGroup?**

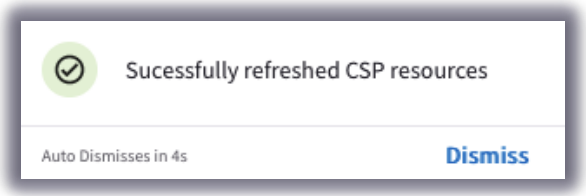
A SmartGroup identifies a group of resources that have similar policy requirements and are associated to the same *logical container*.

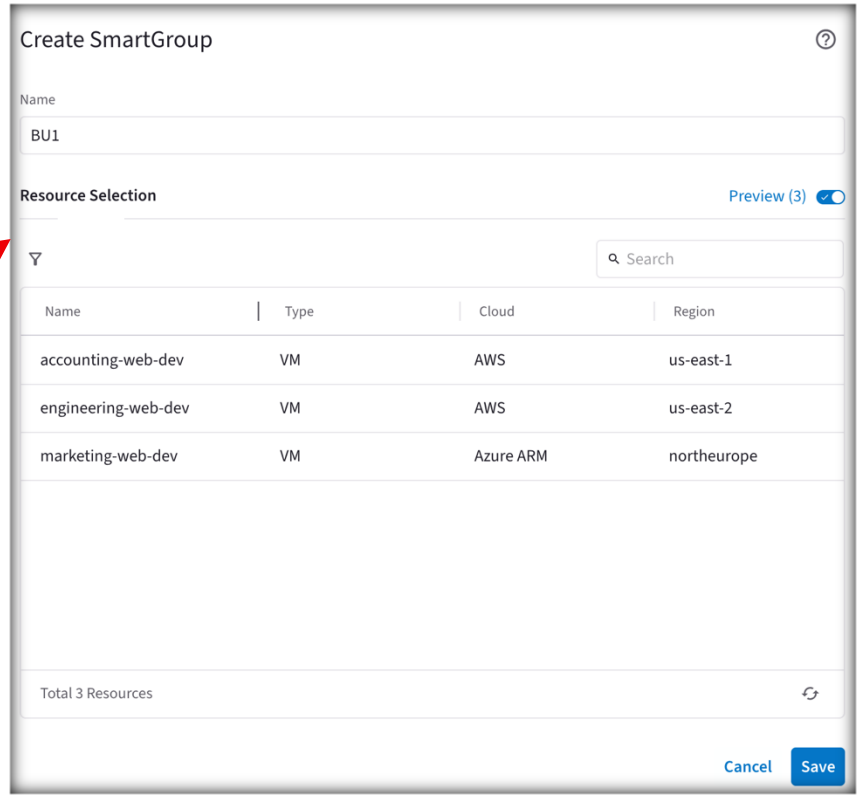
- The members of a SmartGroup can be classified using *different* methods:
  - CSP Tag
  - Subnets
  - VPC/Vnets
  - Kubernetes
  - Hostnames
  - External Connections (S2C)



Smart Groups Creation

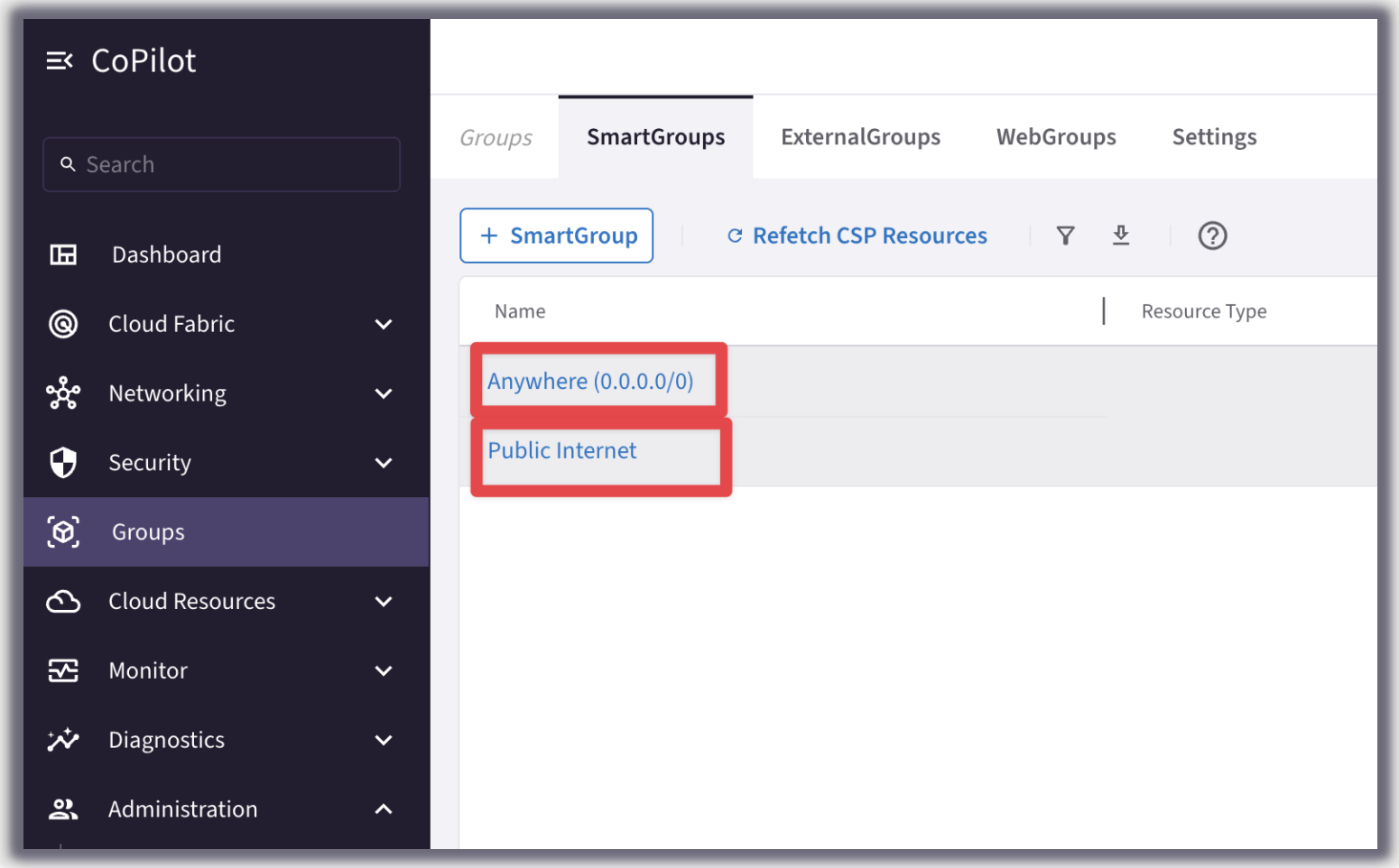






- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

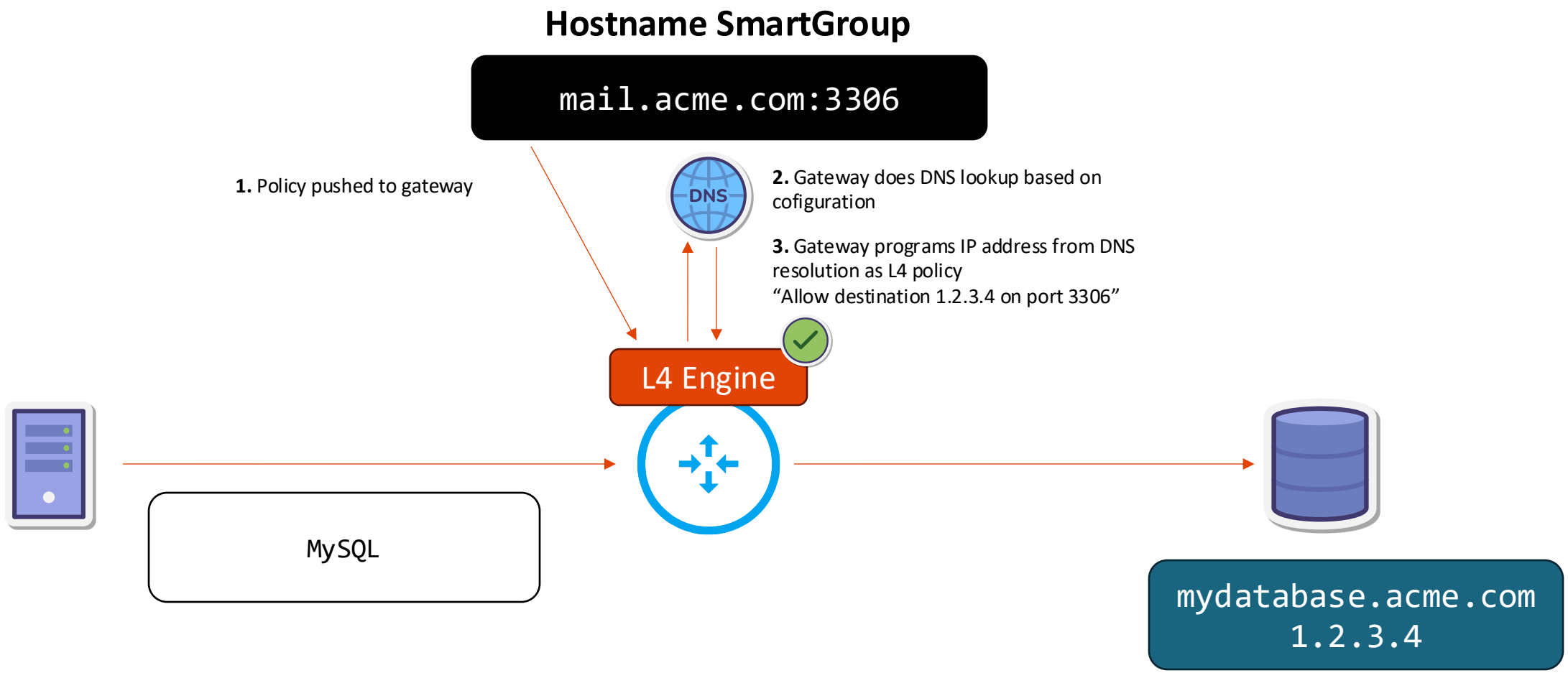
Pre-defined Smart Groups



- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

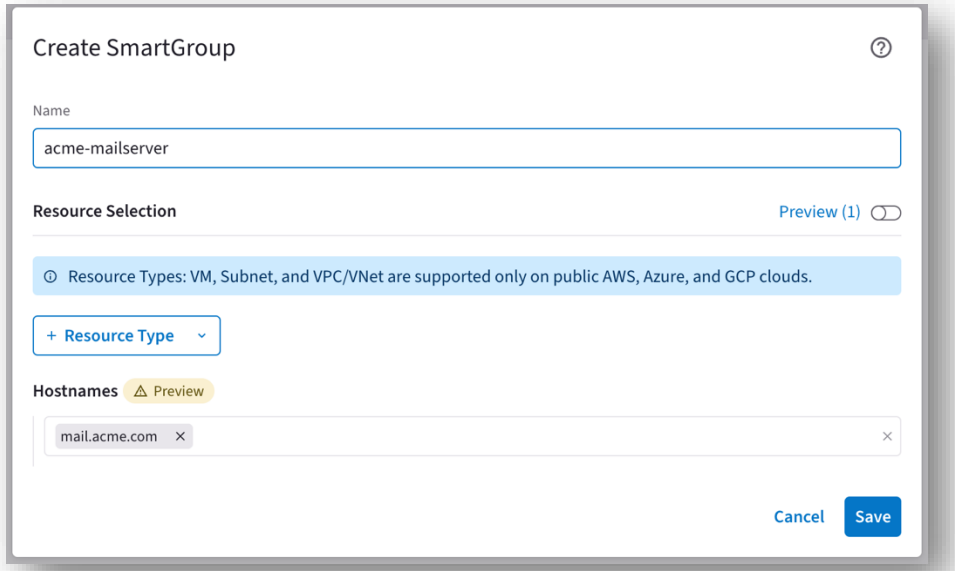
Hostname SmartGroups

Enables FQDN-based policies for non-TLS/HTTP Connections

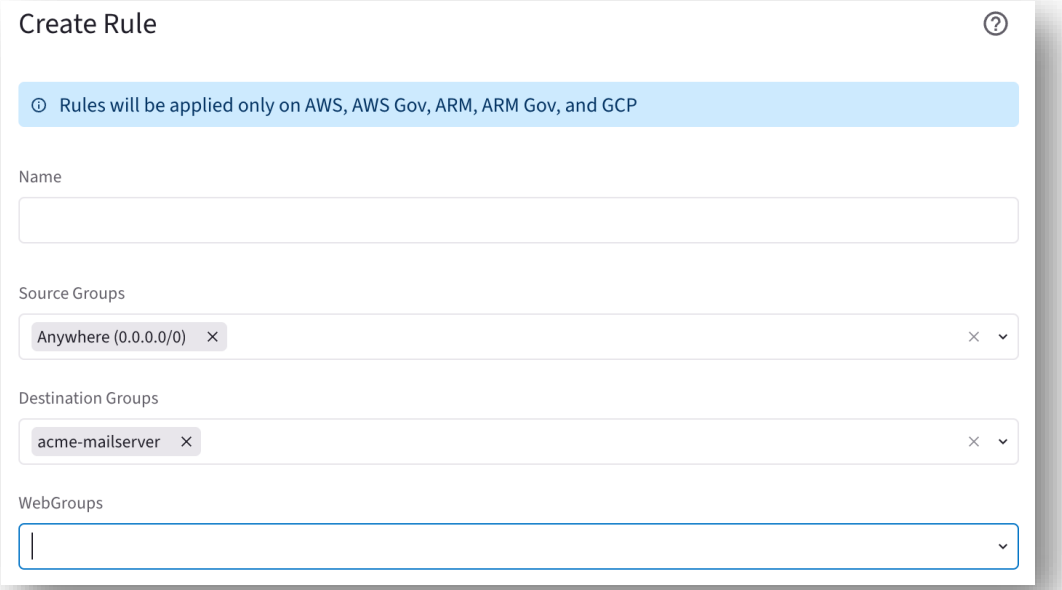


Configuring a Hostname SmartGroup

Create a SmartGroup – Not a WebGroup

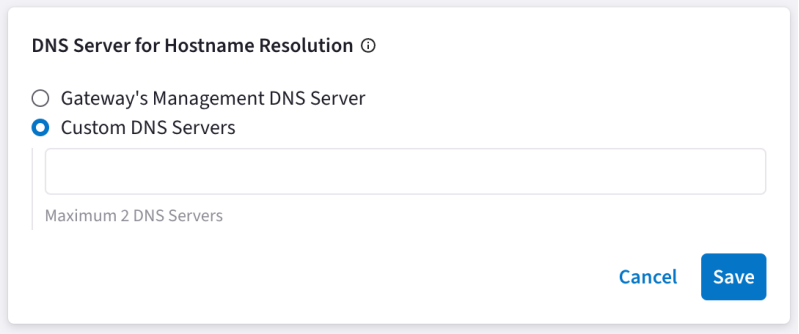


Used as a Destination Group, not a WebGroup

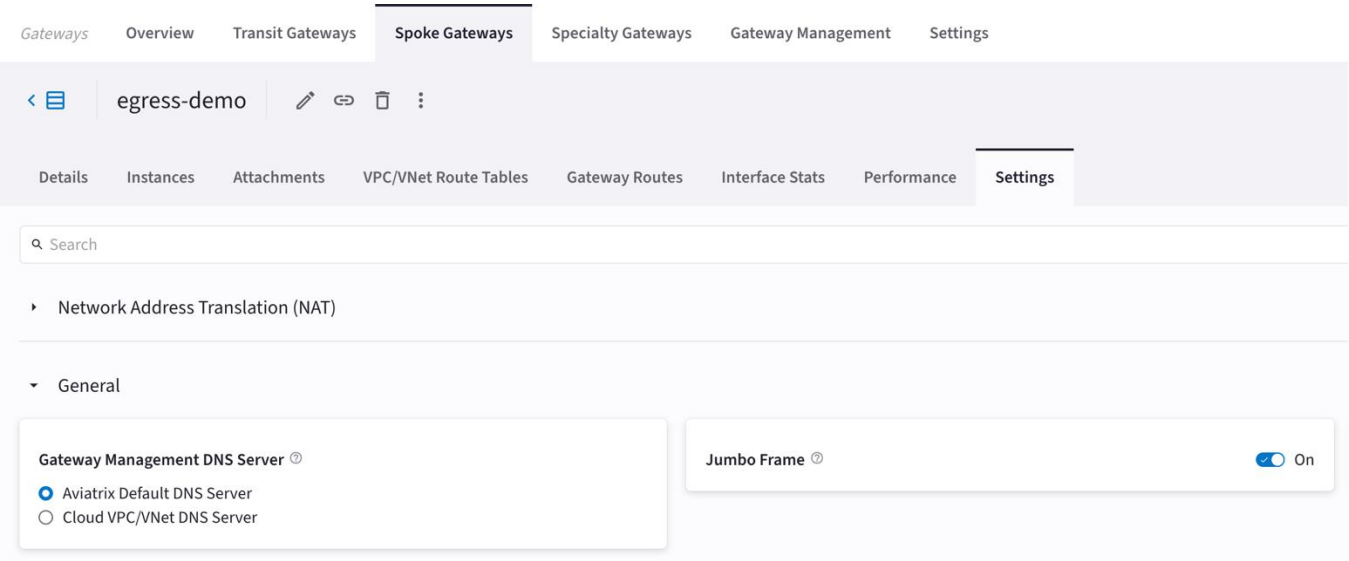


Configuring a Hostname DNS

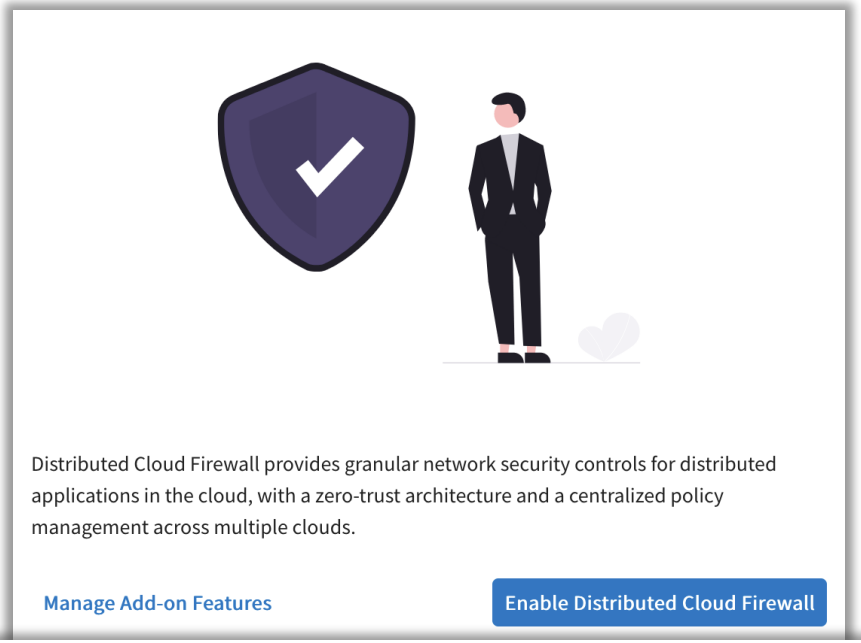
Groups→ Settings



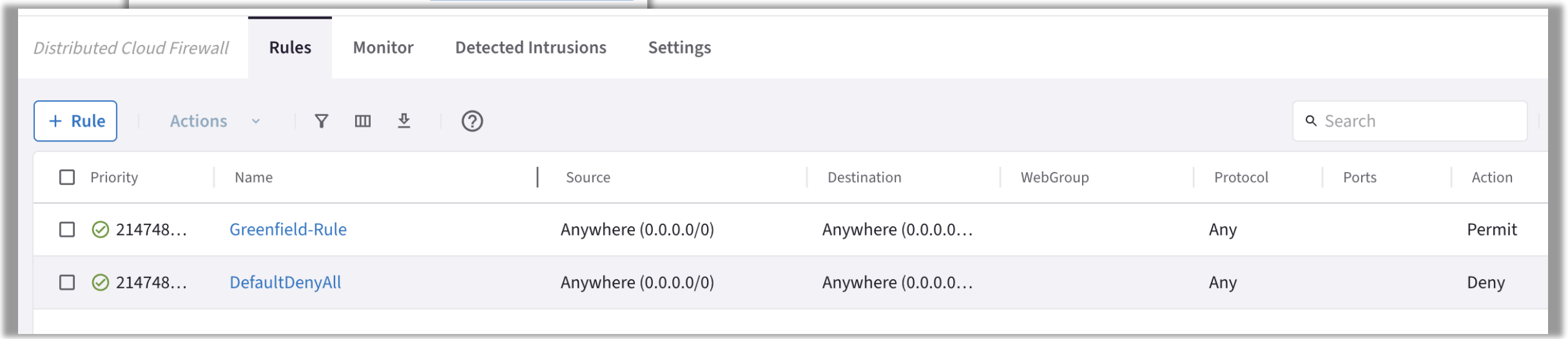
Spoke Gateways -> Settings



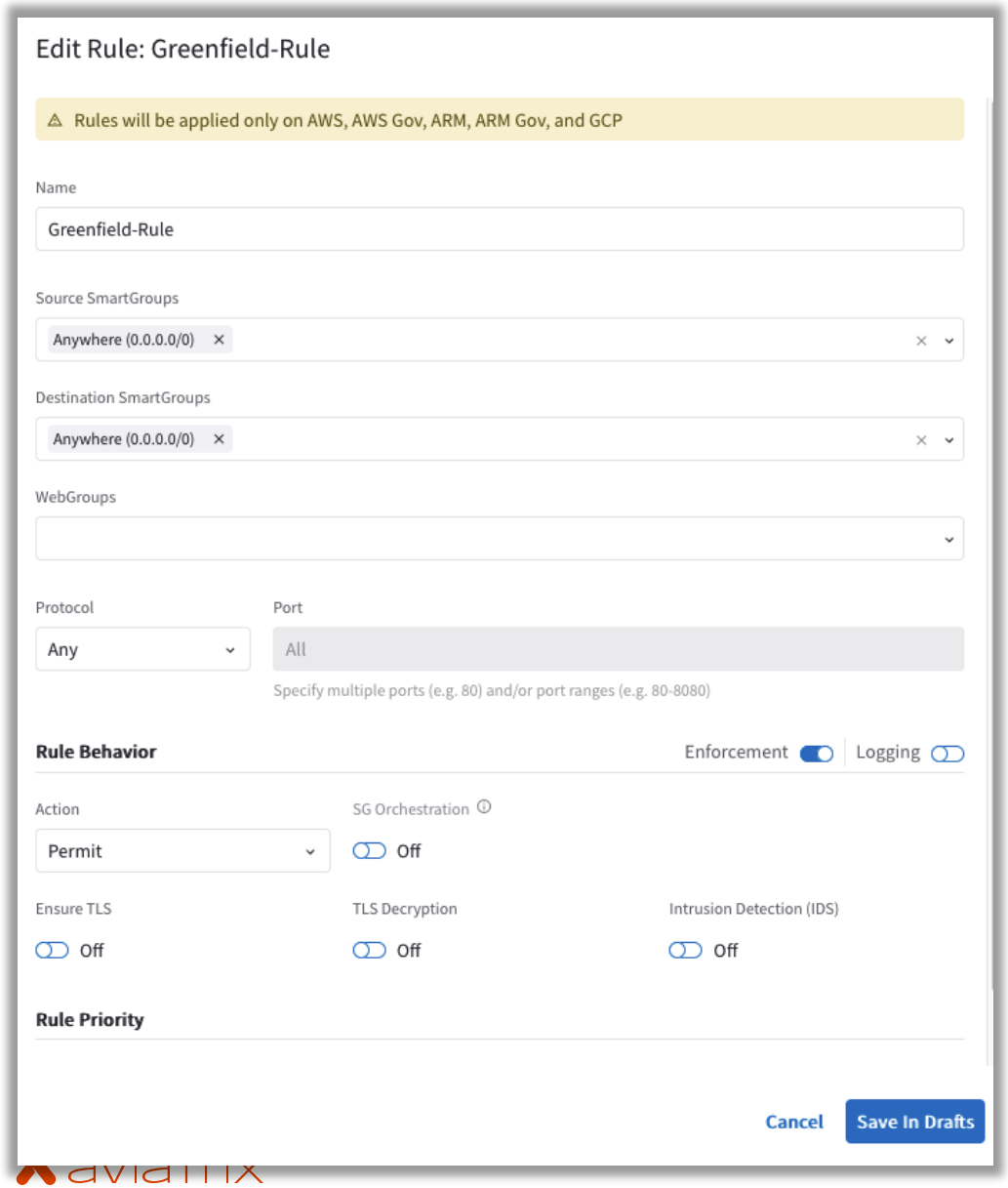
Enabling Distributed Cloud Firewall



- 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.

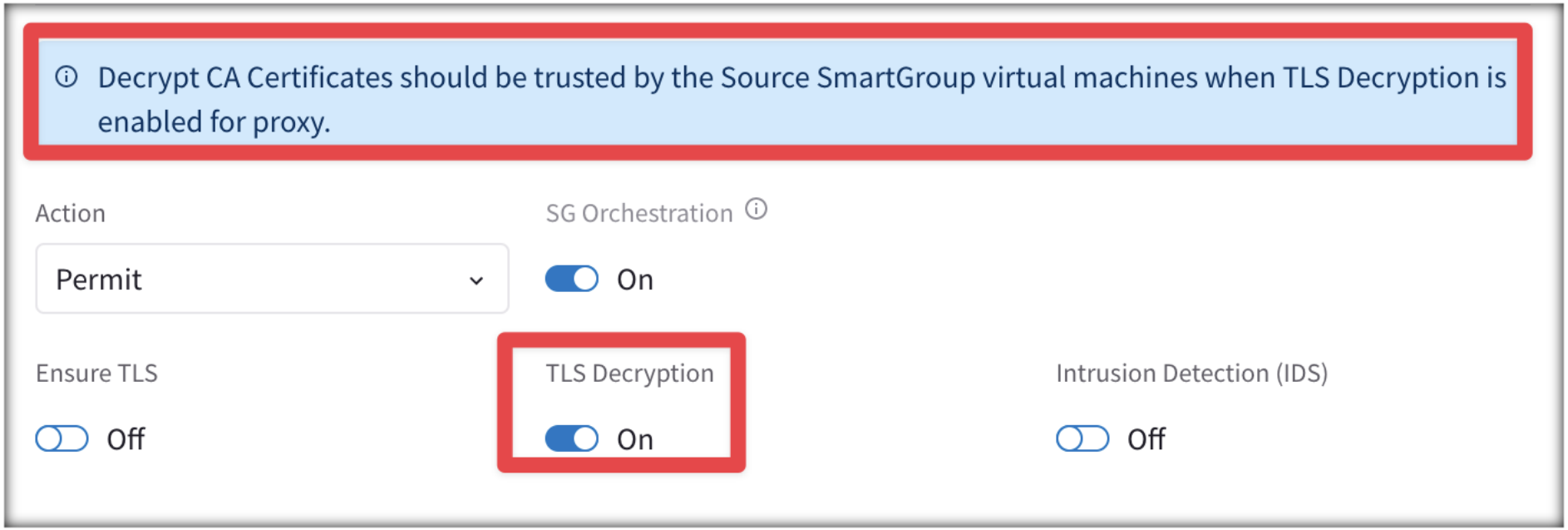


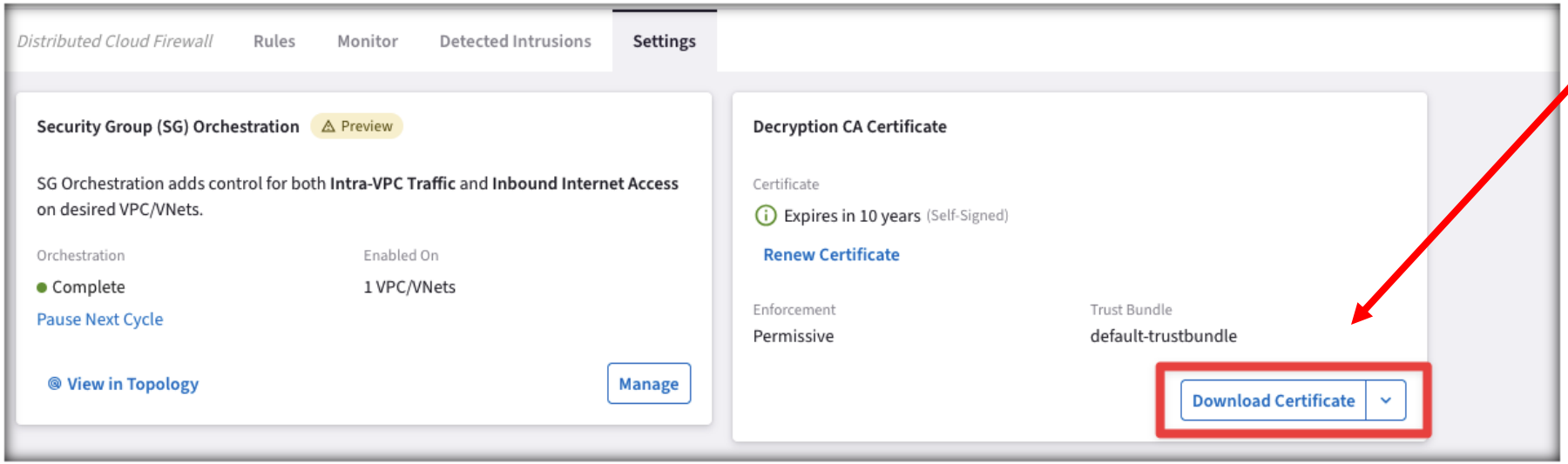
The Greenfield-Rule Structure



- **Source SmartGroups:** Anywhere(0.0.0.0/0)
- **Destination SmartGroups:** Anywhere(0.0.0.0/0)
- **Protocol:** Any
- **Action:** Permit
- Can be **edited** and **deleted**
- It can be **moved** when new rules are created like any other rules
- If it is the only rule present in the rules base, it is allocated <u>above the implicit deny-all rule</u>

TLS Decryption: Decryption CA Cert



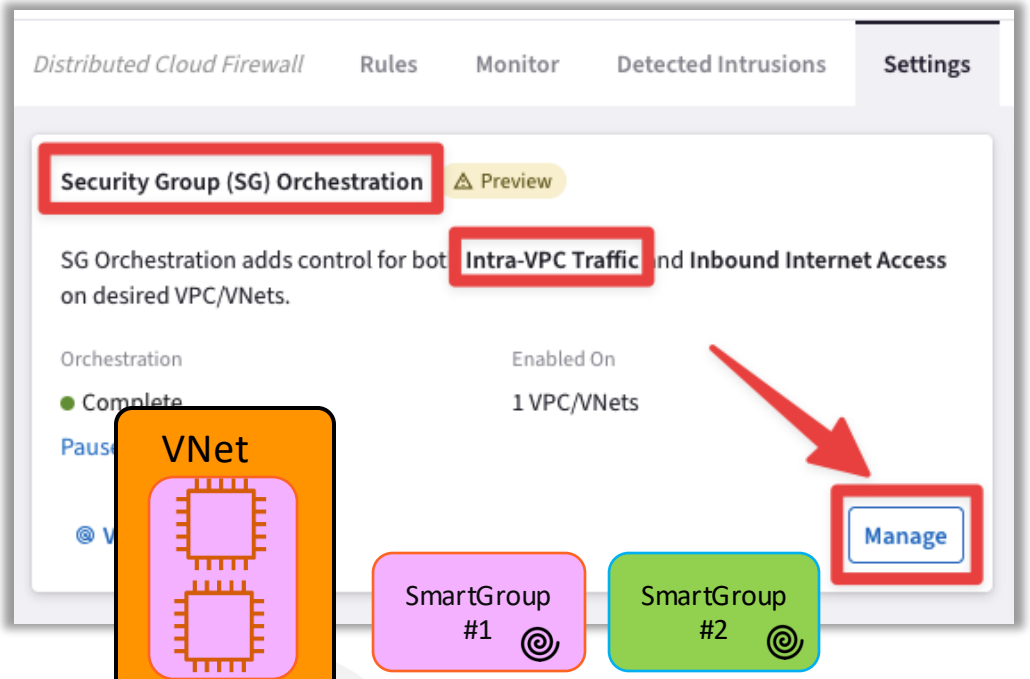


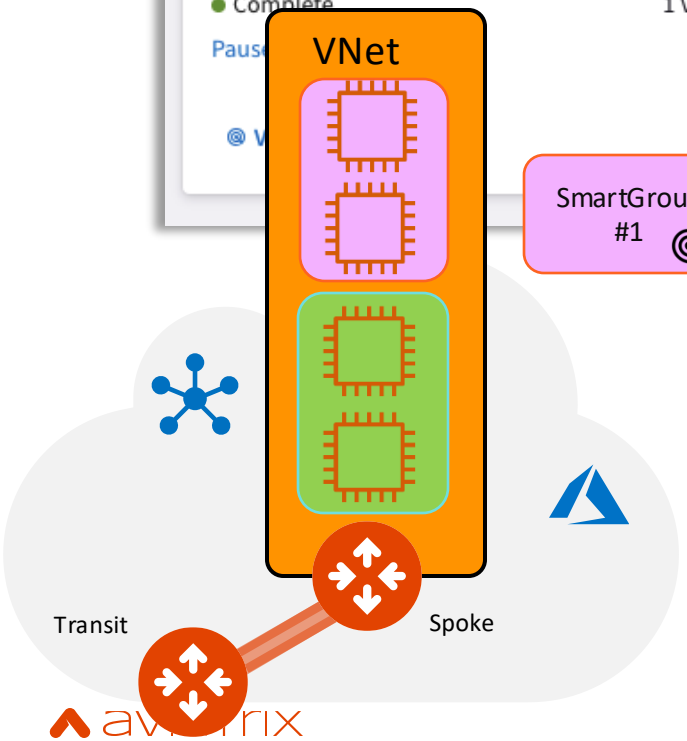
1. Download the Decryption CA Bundle.
2. Distribute the bundle across all the workloads.

Decrypt CA Certificates should be trusted by the **Source SmartGroup** virtual machines when TLS Decryption is enabled for proxy.

Security Group (SG) Orchestration: Intra VPC/VNET Traffic Control

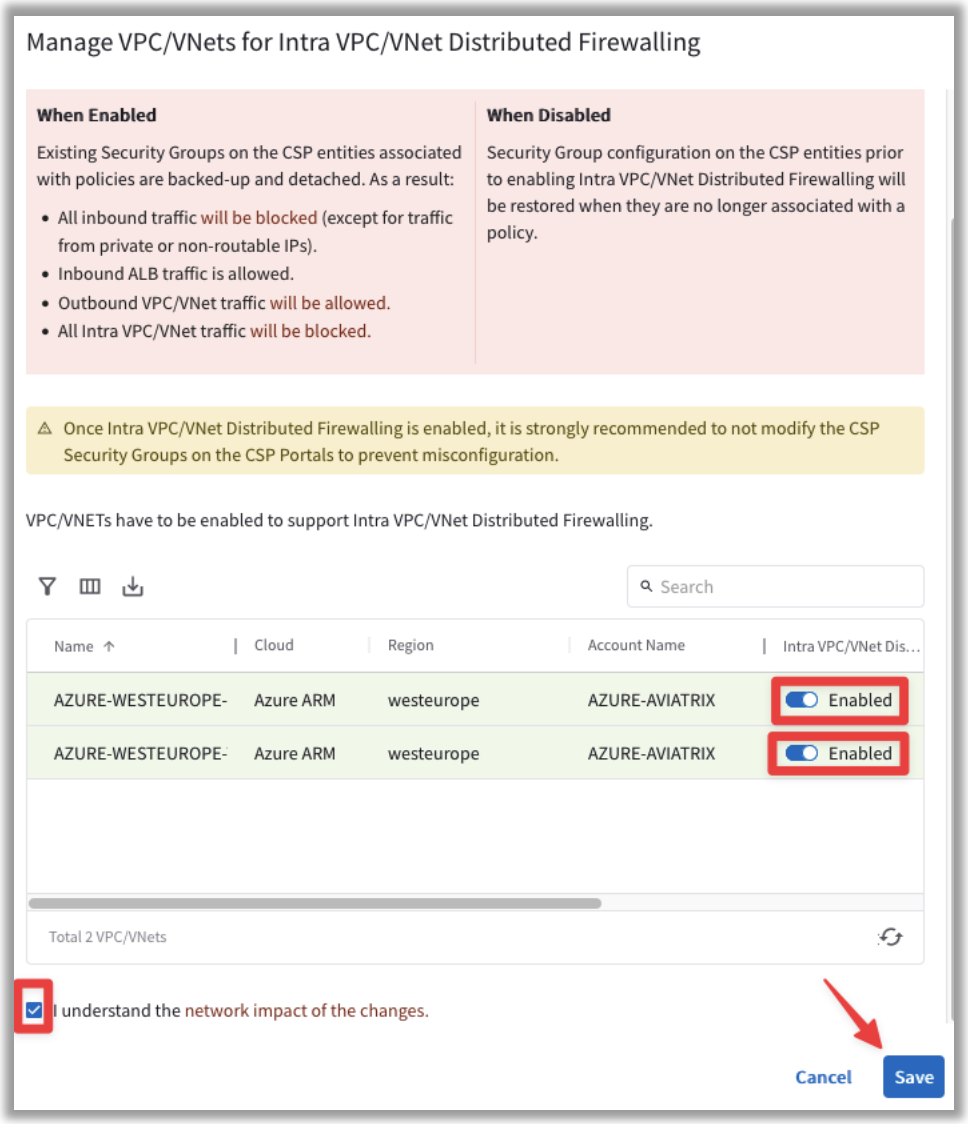
❑ Enable the feature on the relevant VPC/VNet



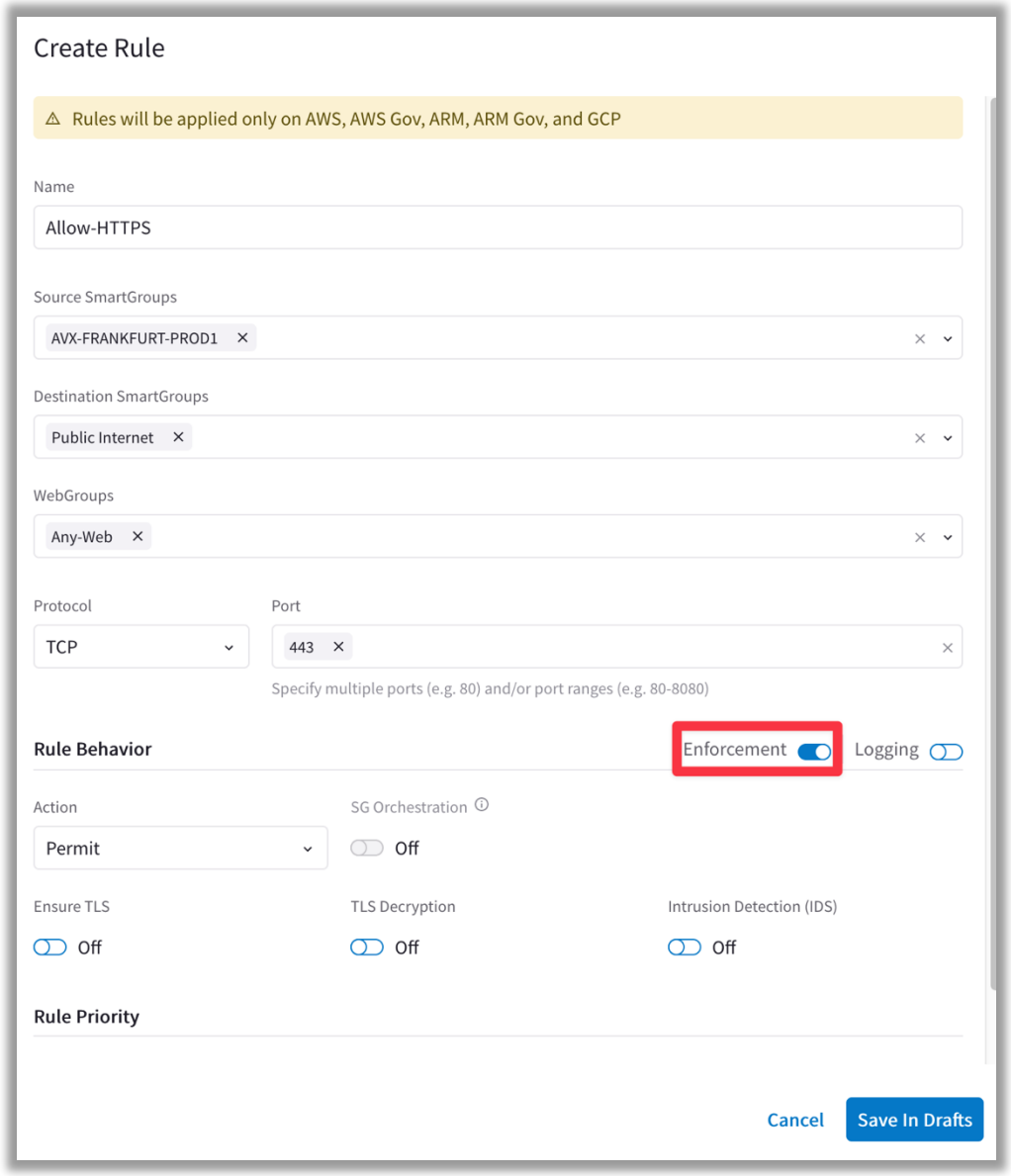


- If you enable the **Security Group (SG) Orchestration** (*aka Intra-VPC Traffic Control*), the SmartGroups defined within the same VPC/VNet will not be able to communicate with each other, unless an inter rule is applied between them.
- This is pure L4 separation, leveraging the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.

CAVEAT: Available in AWS/Azure



Rule Enforcement



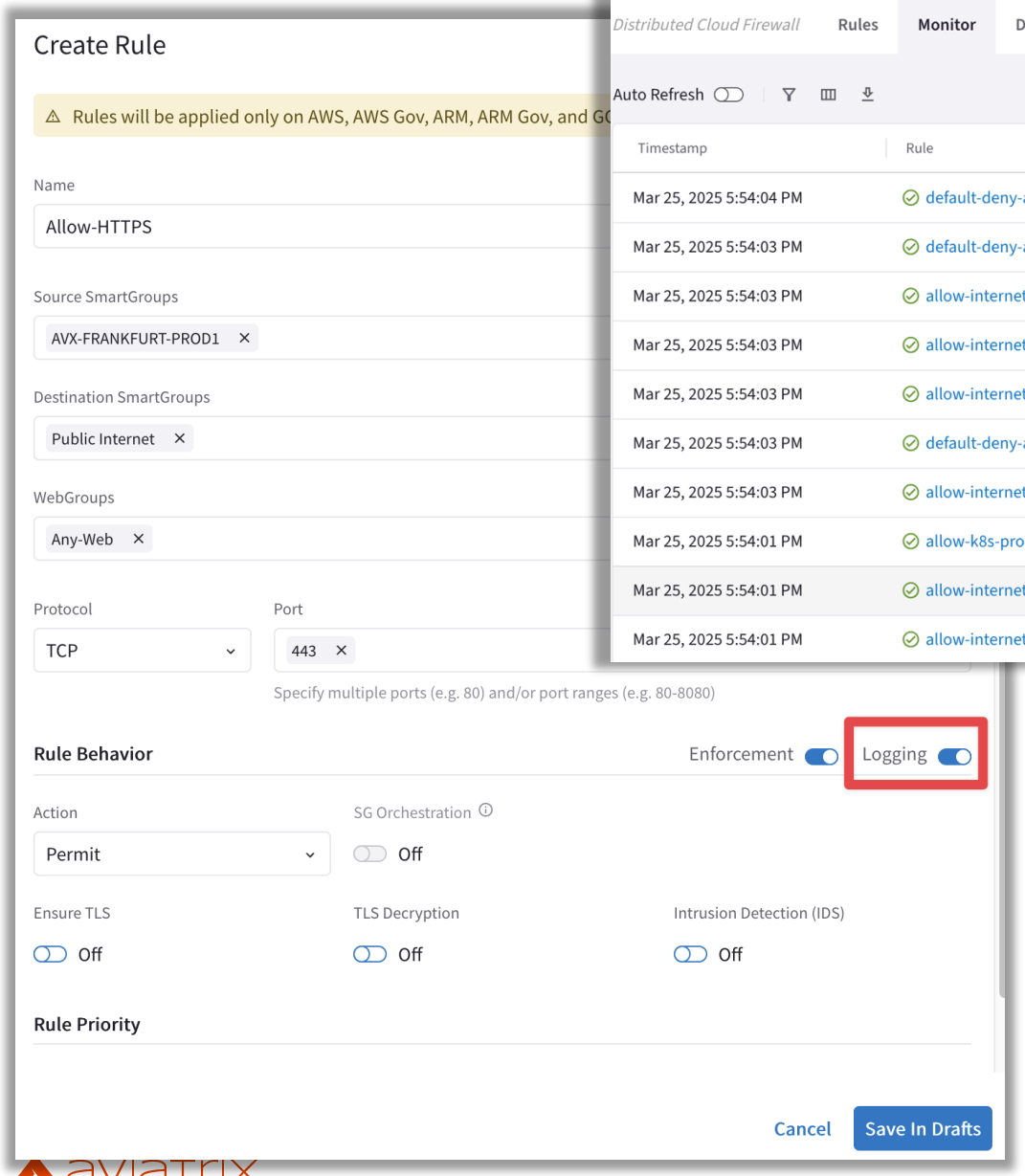
Enforcement ON

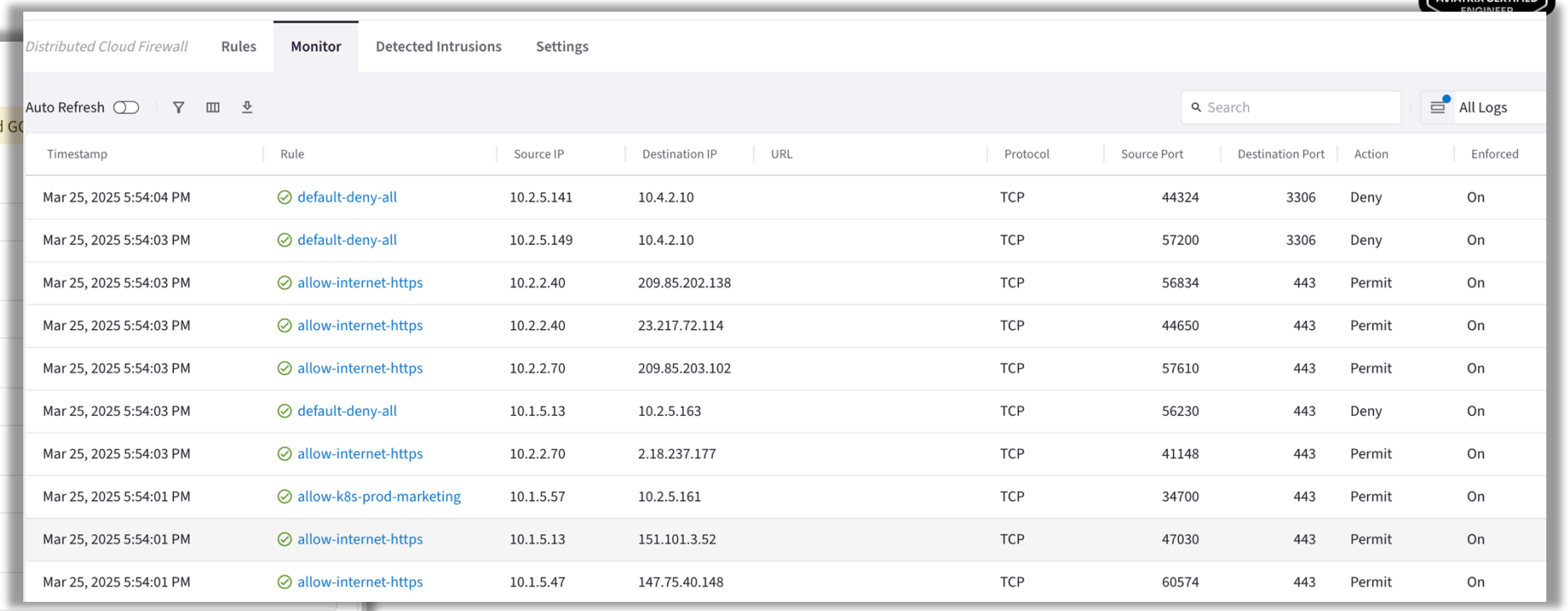
- Policy is enforced in the Data Plane

Enforcement OFF

- Policy is NOT enforced in the Data Plane
- The option provides a *Watch/Test* mode
- Common use case is with deny rule
- Watch what traffic hits the deny rule before enforcing the rule in the Data Plane.

Rule Logging





Timestamp	Rule	Source IP	Destination IP	URL	Protocol	Source Port	Destination Port	Action	Enforced
Mar 25, 2025 5:54:04 PM	default-deny-all	10.2.5.141	10.4.2.10		TCP	44324	3306	Deny	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.2.5.149	10.4.2.10		TCP	57200	3306	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.40	209.85.202.138		TCP	56834	443	Permit	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.40	23.217.72.114		TCP	44650	443	Permit	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.70	209.85.203.102		TCP	57610	443	Permit	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.1.5.13	10.2.5.163		TCP	56230	443	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.70	2.18.237.177		TCP	41148	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-k8s-prod-marketing	10.1.5.57	10.2.5.161		TCP	34700	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-internet-https	10.1.5.13	151.101.3.52		TCP	47030	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-internet-https	10.1.5.47	147.75.40.148		TCP	60574	443	Permit	On

- Logging can be turned ON/OFF per rule
- Configure Syslog to view the logs