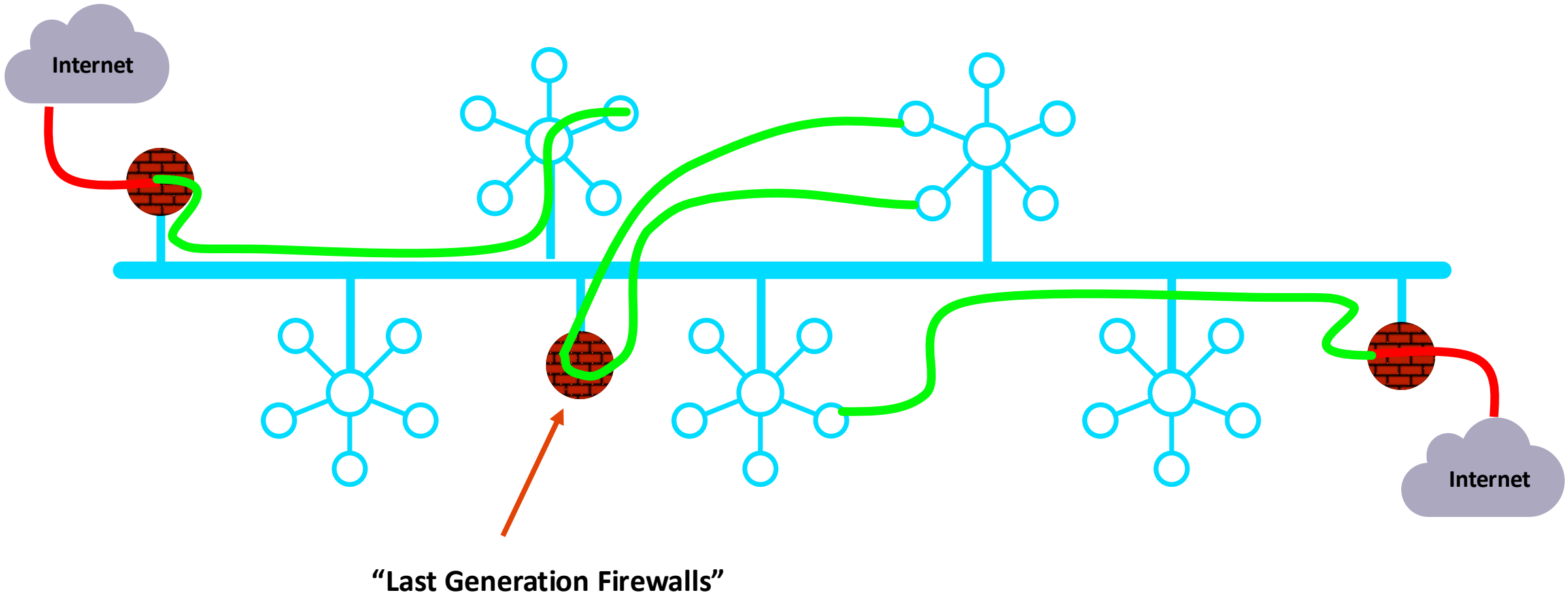
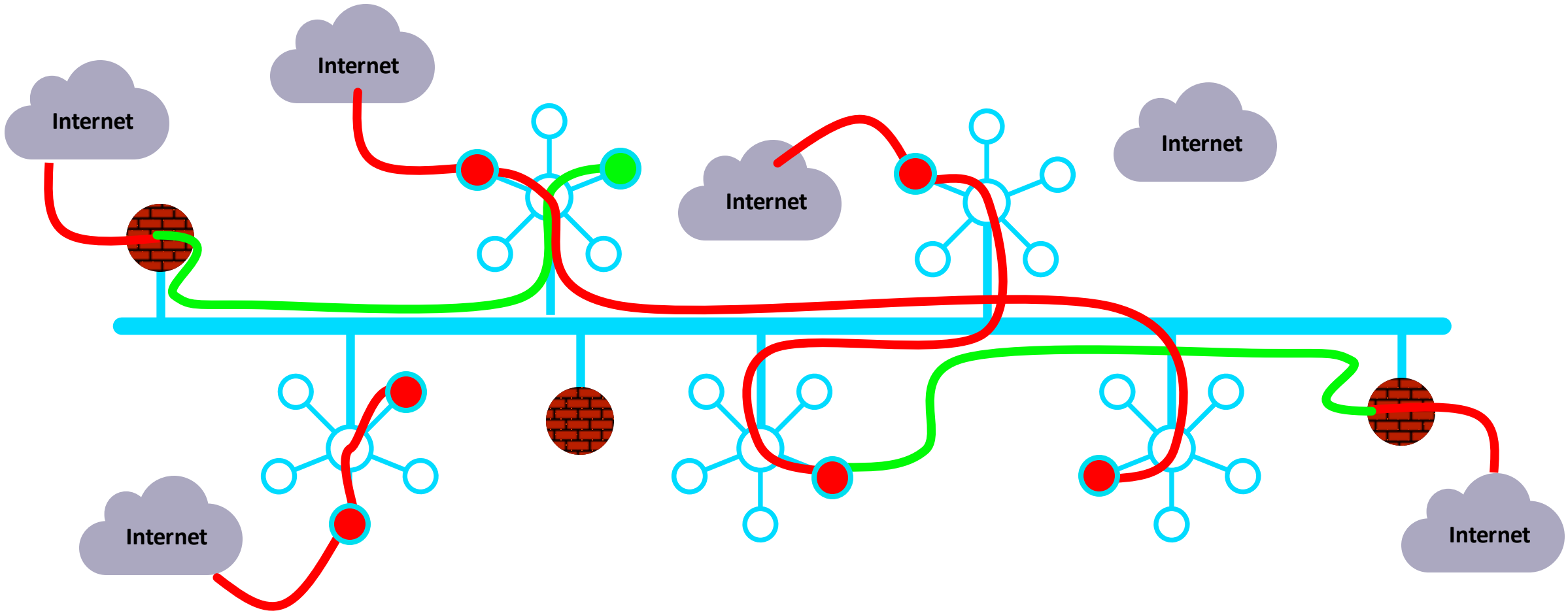
Distributed Cloud Firewall

ACE Team

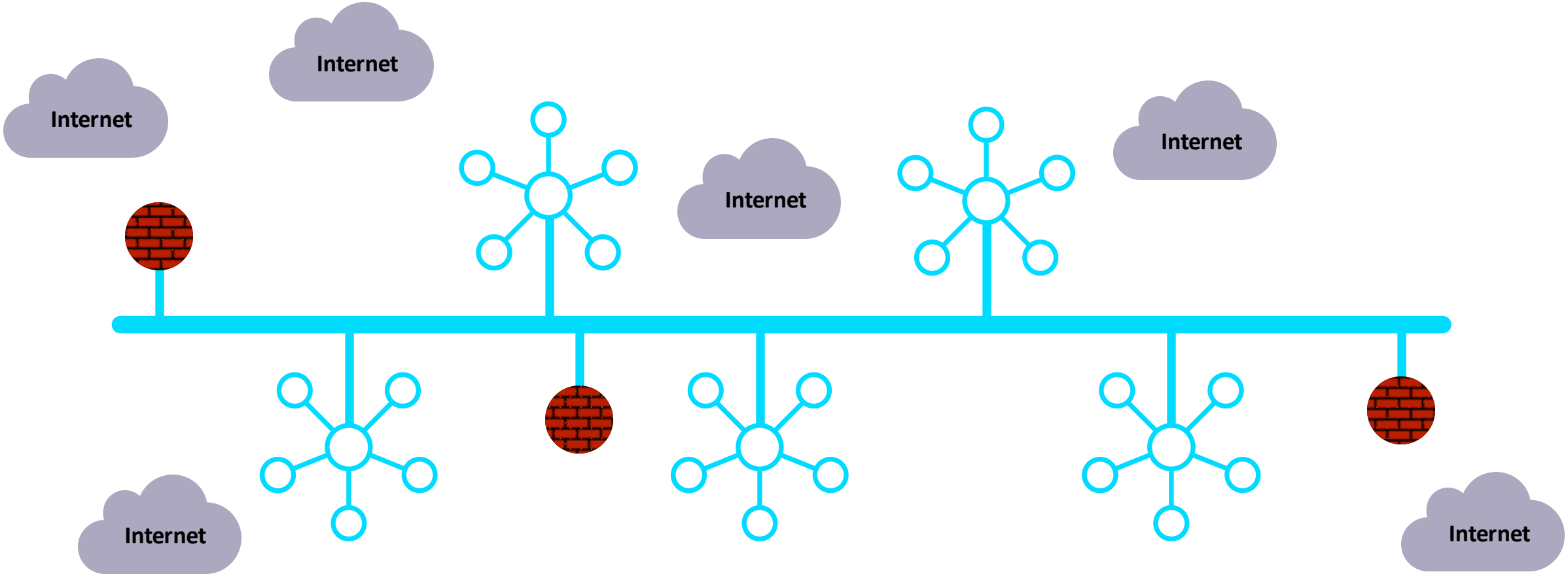
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…



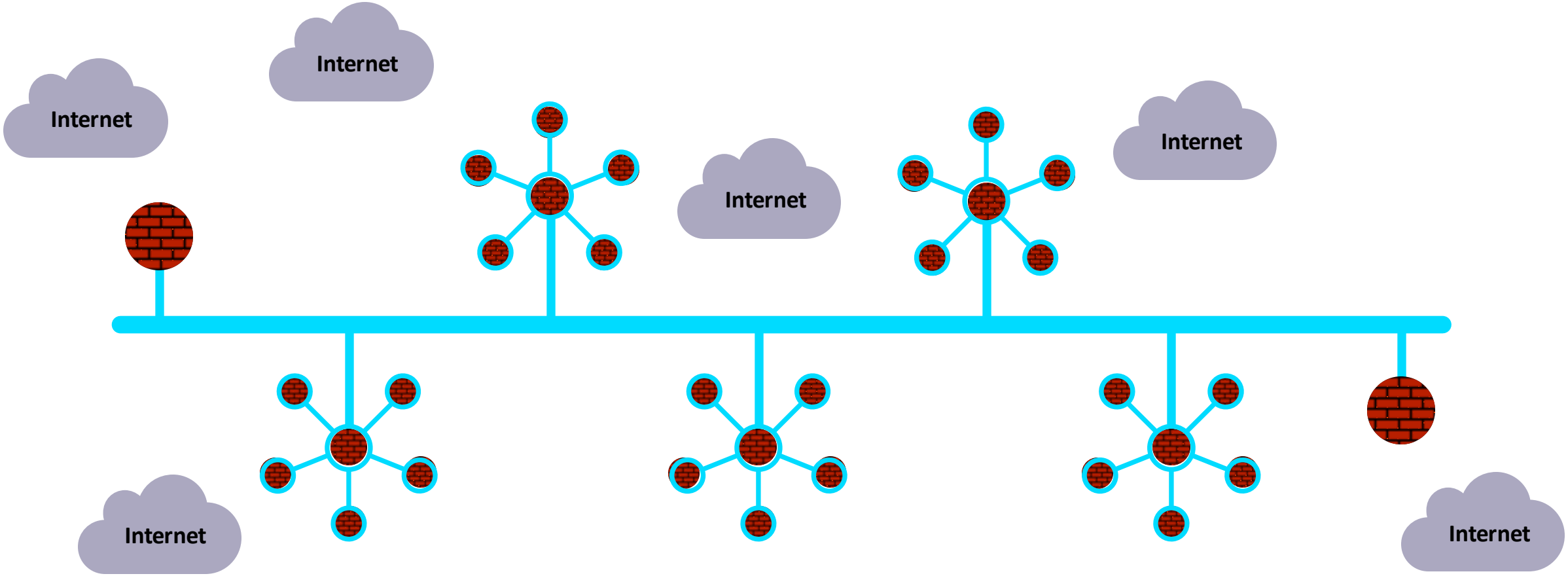
In Reality…


Internet
Internet
Internet
Internet
Internet
Internet
Internet

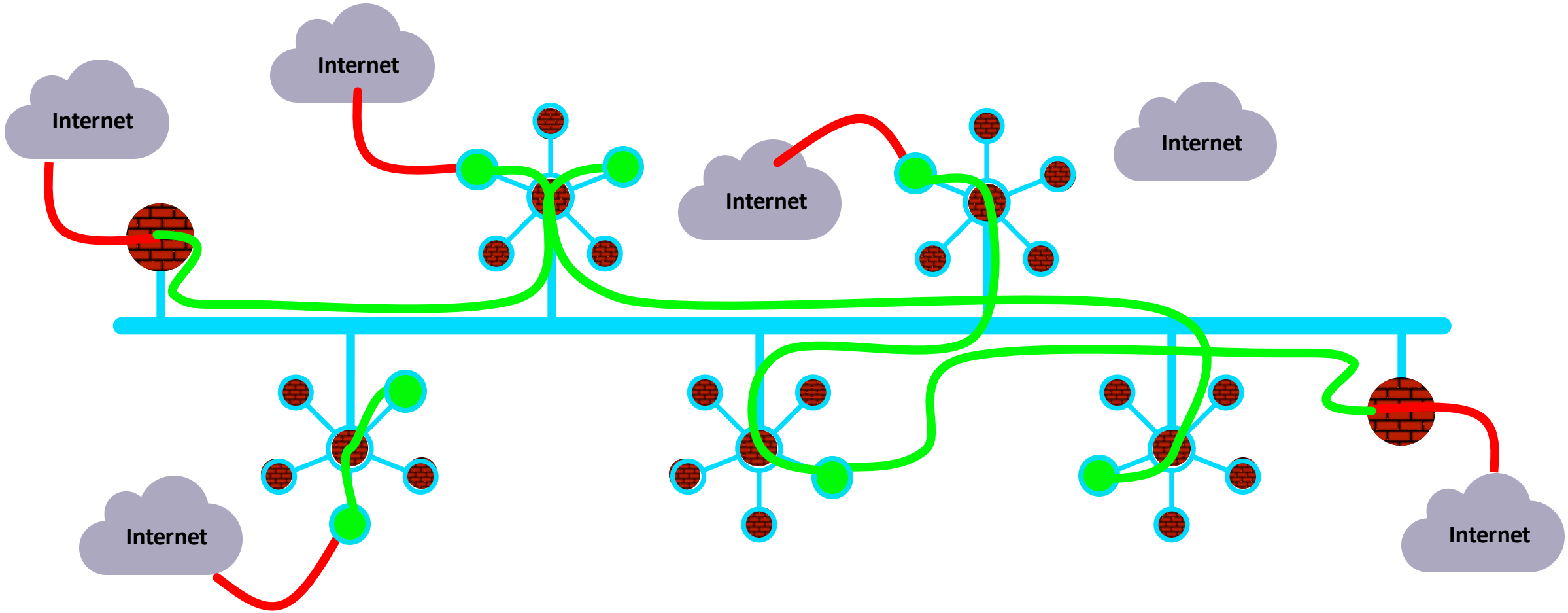
What If… the architecture was built for cloud



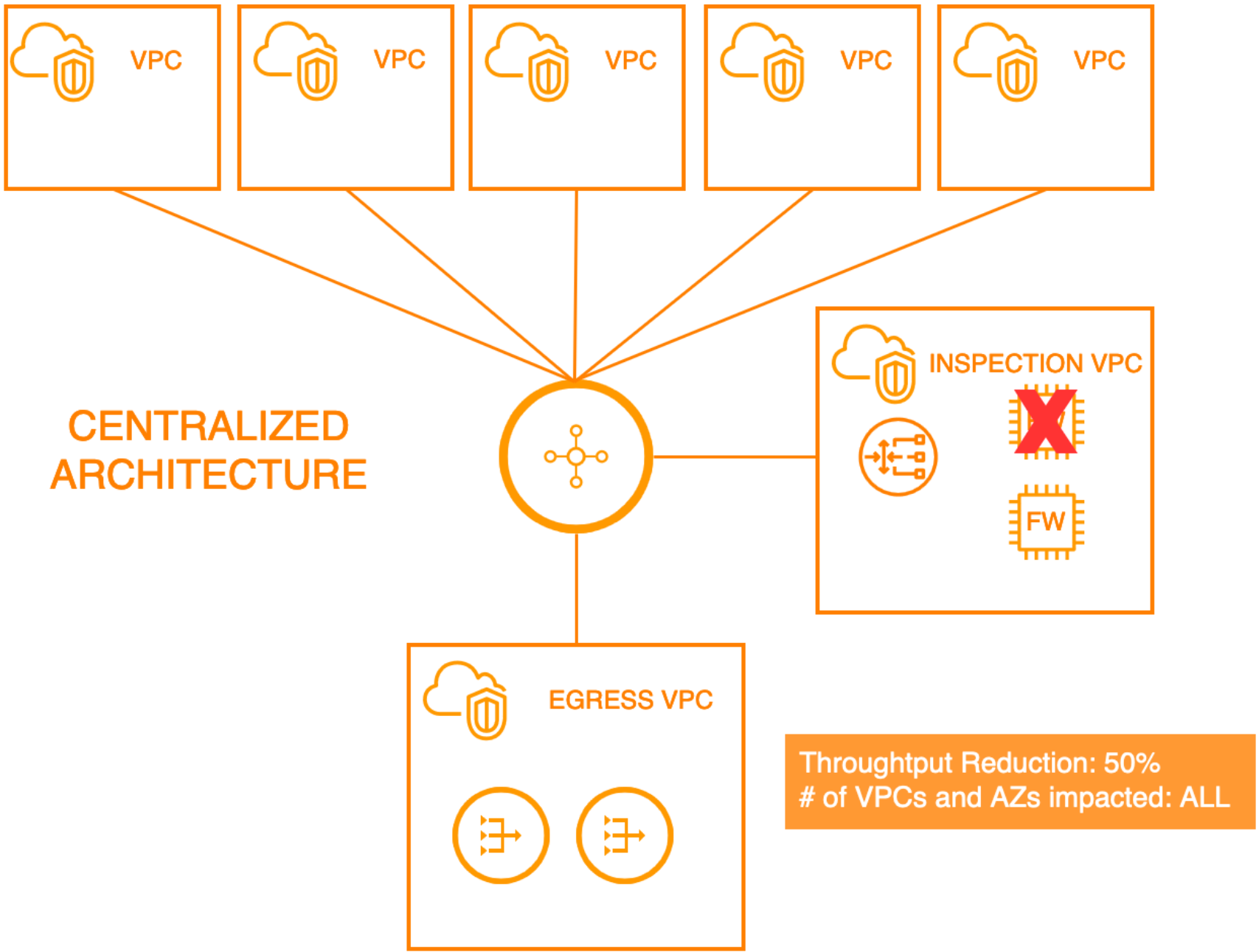
Firewalling Functions were Embedded in the Cloud Network Everywhere…



Distribution of the Security Services into the Spokes

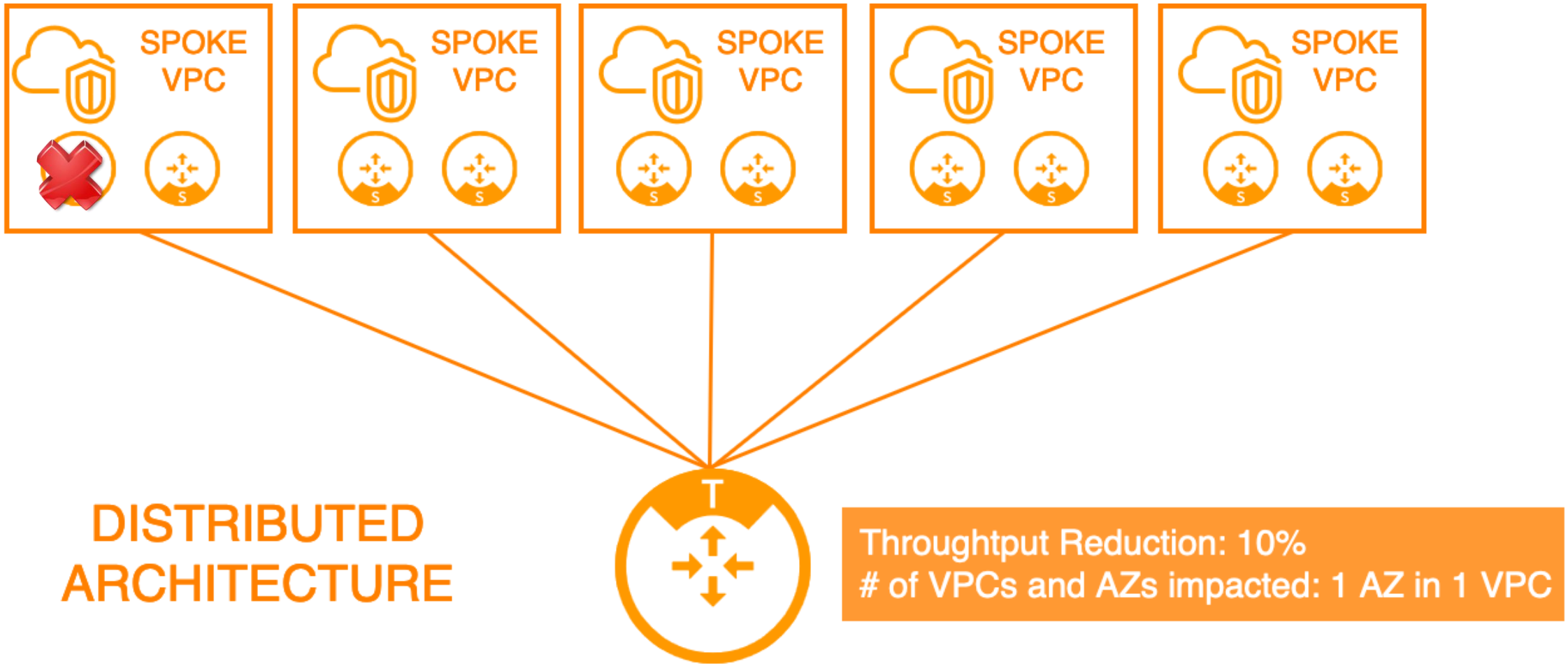


Impact of Failure – Centralized Architecture

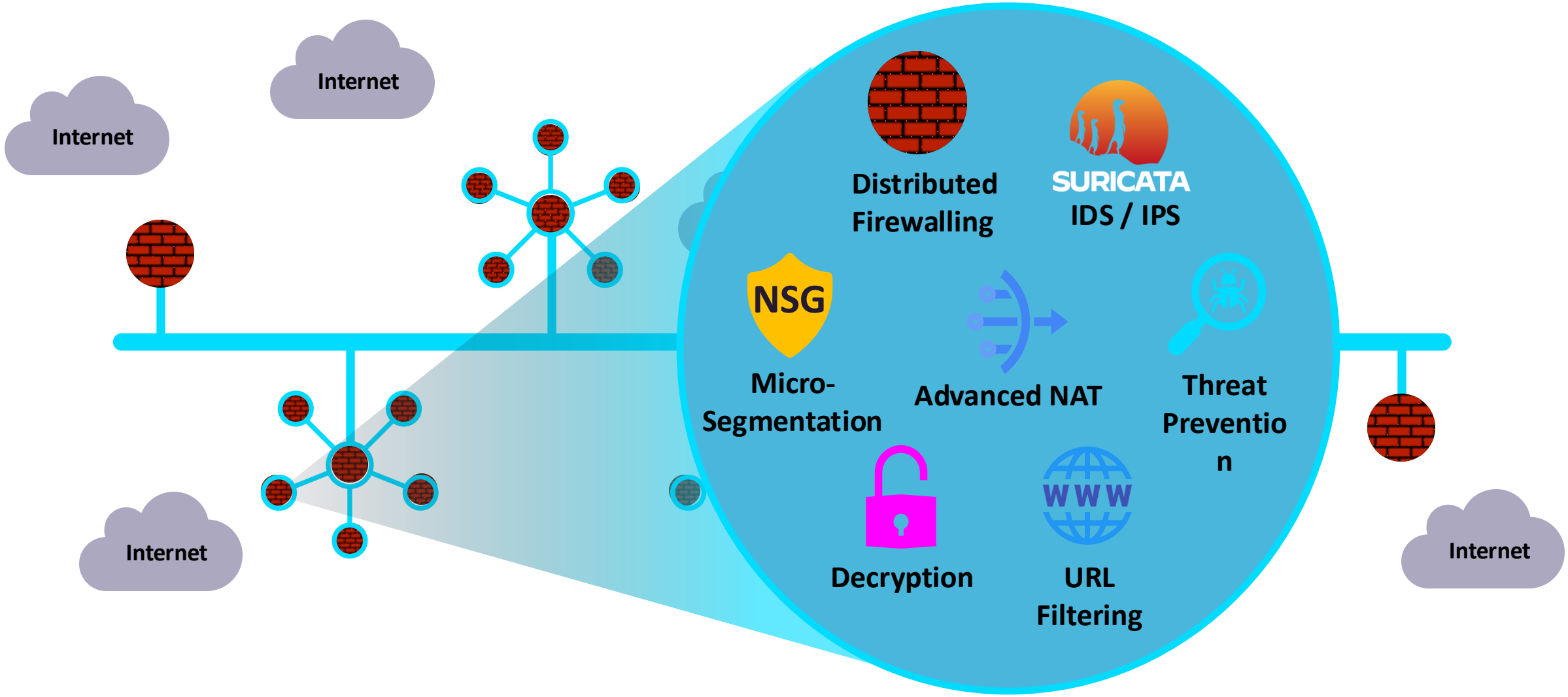


Throughtput Reduction: 50%
# of VPCs and AZs impacted: ALL

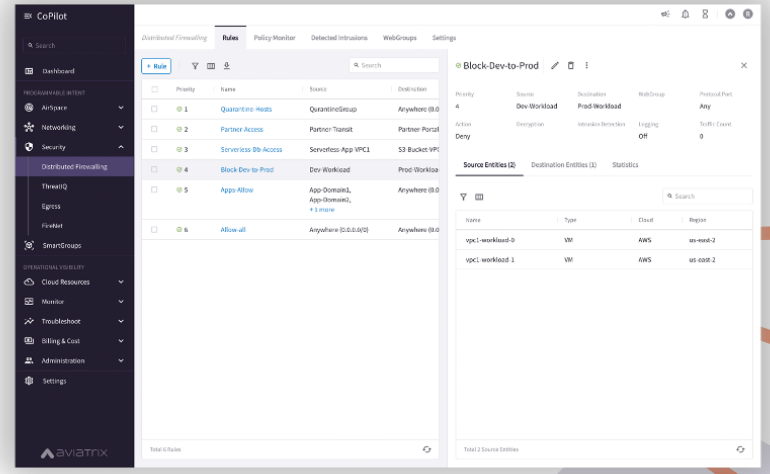
Impact of Failure – Distributed Architecture



And, What If it was more than just firewalling…



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



Where and How Policies Are Enforced Is Abstracted…

aviatrix

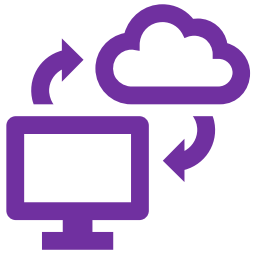
SmartGroups: Definition

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

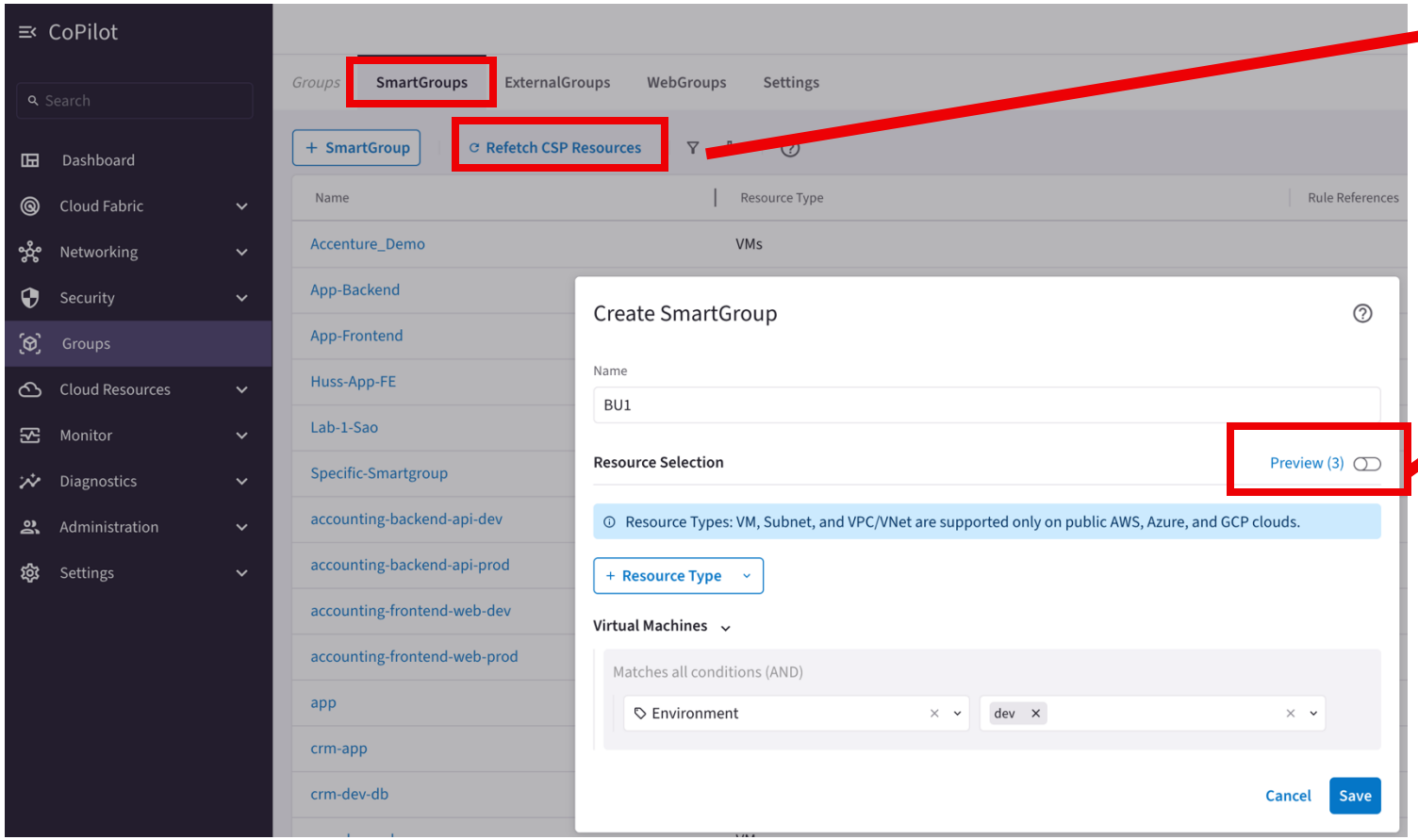
- **What is a SmartGroup?**

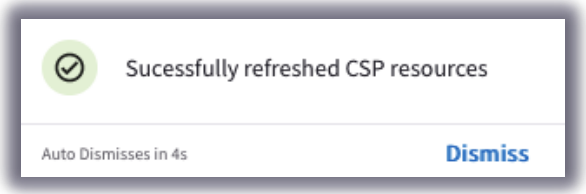
A SmartGroup identifies a group of resources that have similar policy requirements and are associated to the same *logical container*.

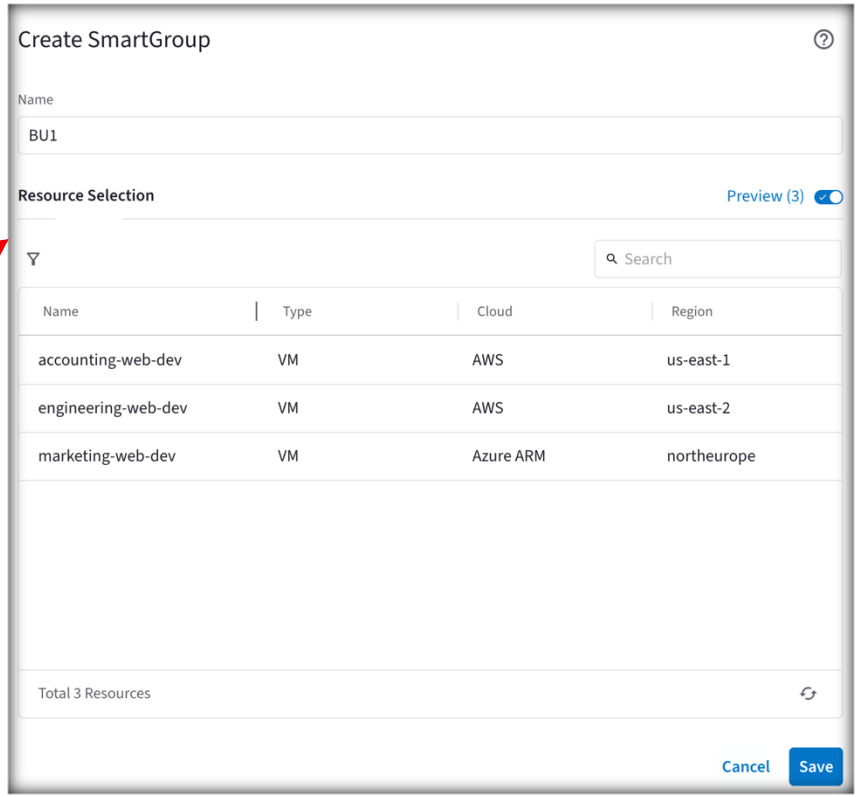
- The members of a SmartGroup can be classified using *different* methods:
  - CSP Tag
  - Subnets
  - VPC/Vnets
  - Kubernetes
  - Hostnames
  - External Connections (S2C)



Smart Groups Creation

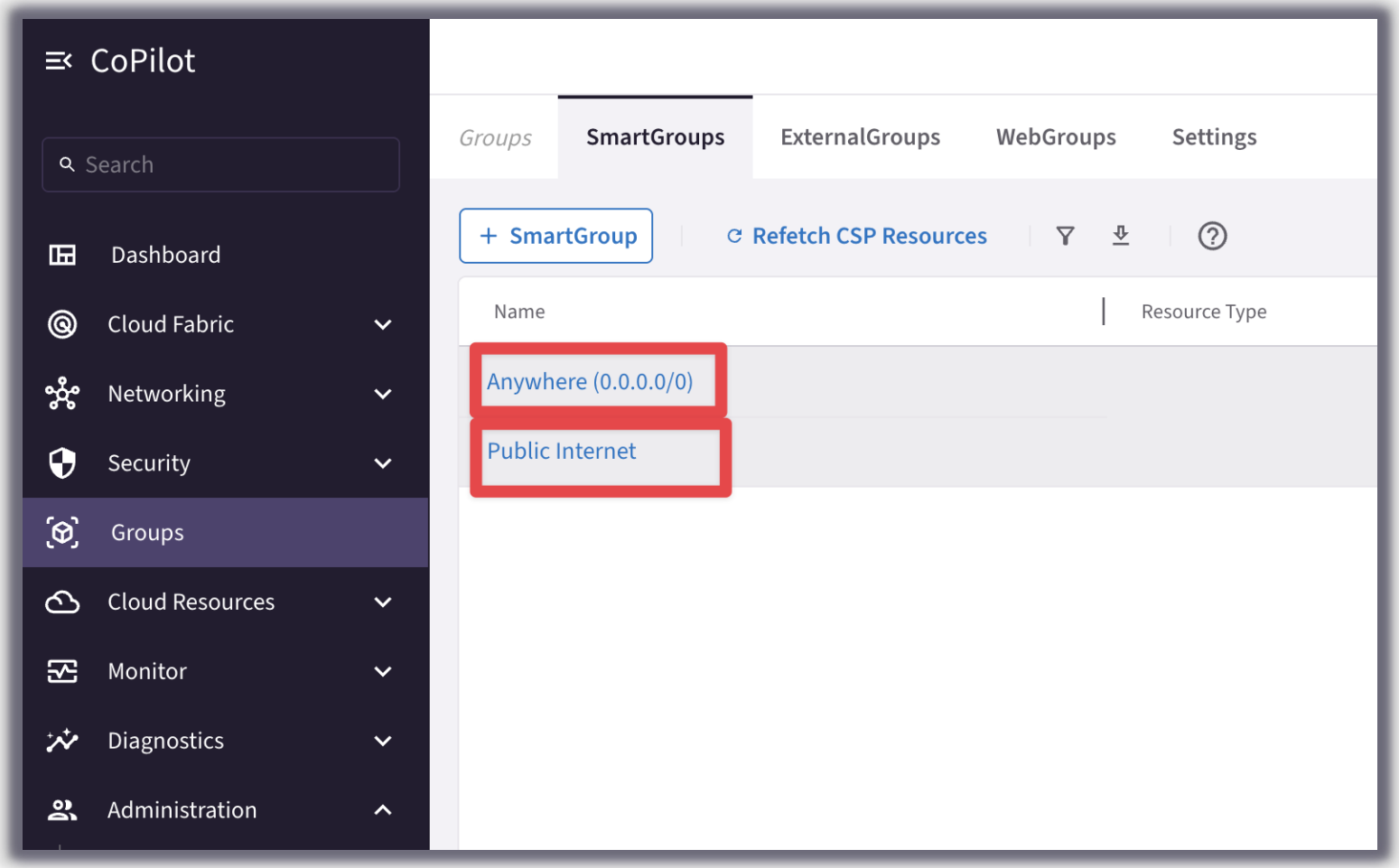






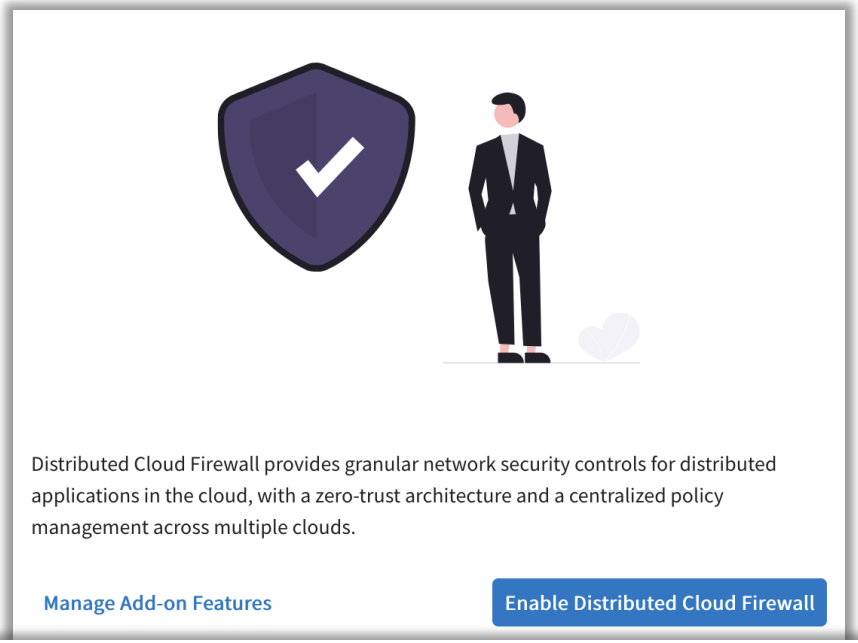
- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

Pre-defined Smart Groups



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

Enabling Distributed Cloud Firewall



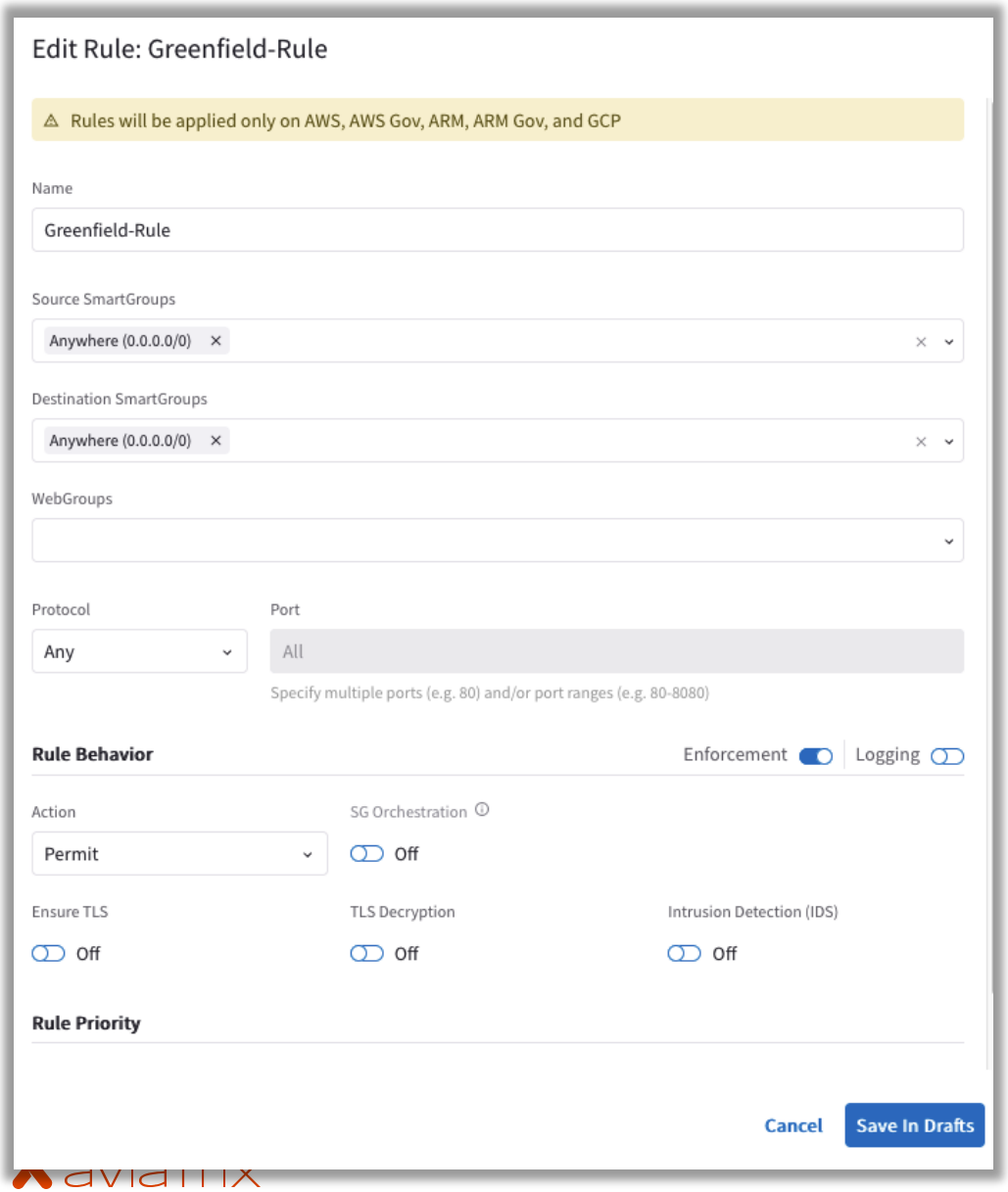
- Enabling the Distributed Cloud Firewall without configured rules will deny all previously permitted traffic due to its implicit Deny All rule.
- To maintain consistency, a **Greenfield Rule** will be created to allow traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.

Distributed Cloud Firewall | **Rules** | **Monitor** | **Detected Intrusions** | **Settings**

+ Rule | Actions | Search

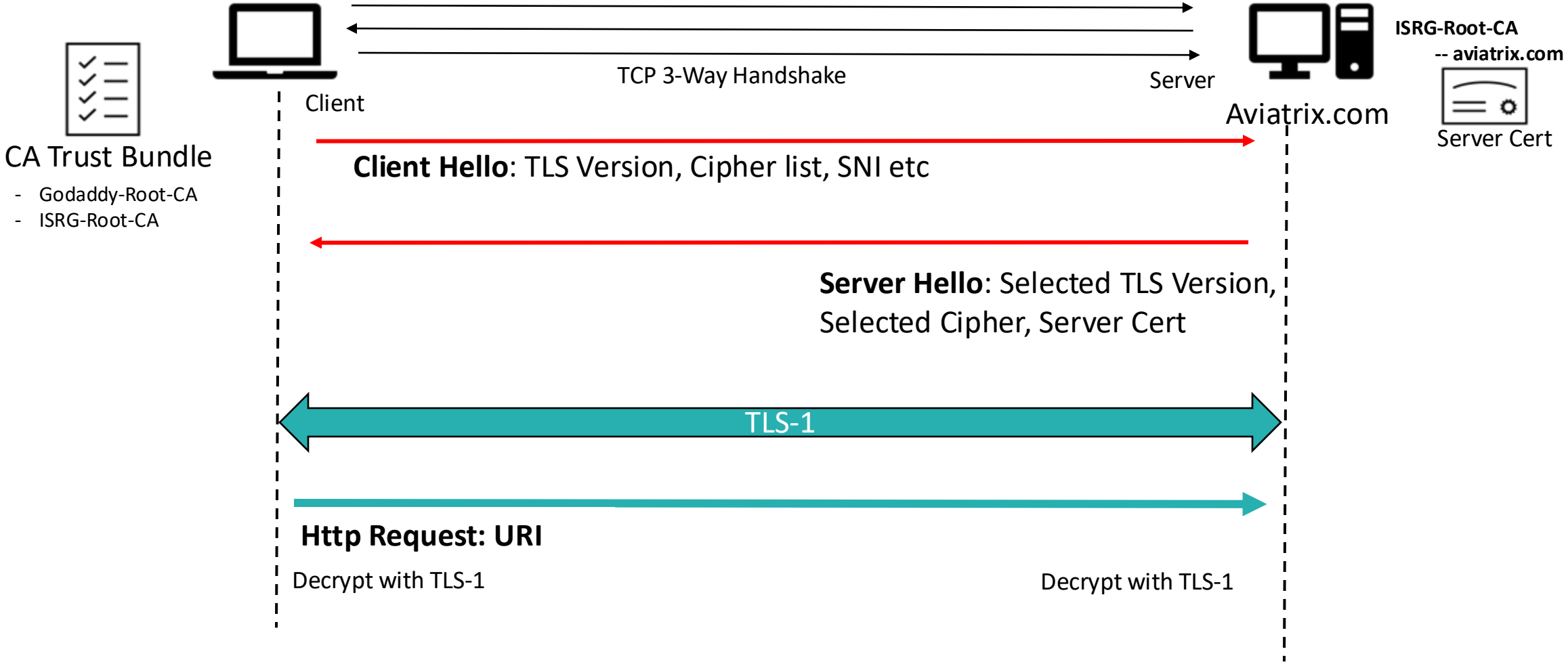
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
214748…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0…		Any		Permit
214748…	DefaultDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0…		Any		Deny

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 above the implicit deny-all rule

TLS Decryption: Basic TLS Connection



TLS Decryption: PKI/ KMS and Trust Bundle

Certificate Hierarchy

- Root
  - Intermediate
    - Server Cert (Leaf Cert)

Certificate Fields

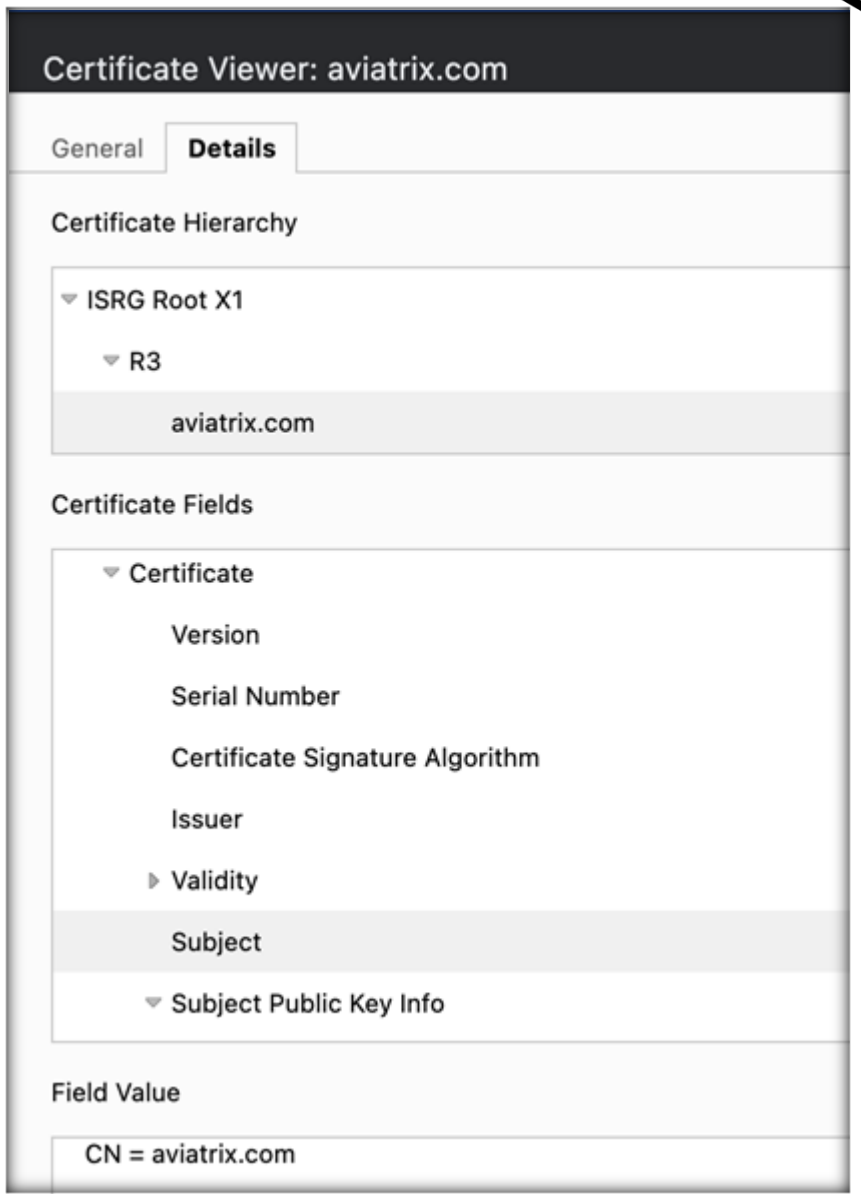
- Issuer
- Validity
- Subject

Trusted Root CA Bundle

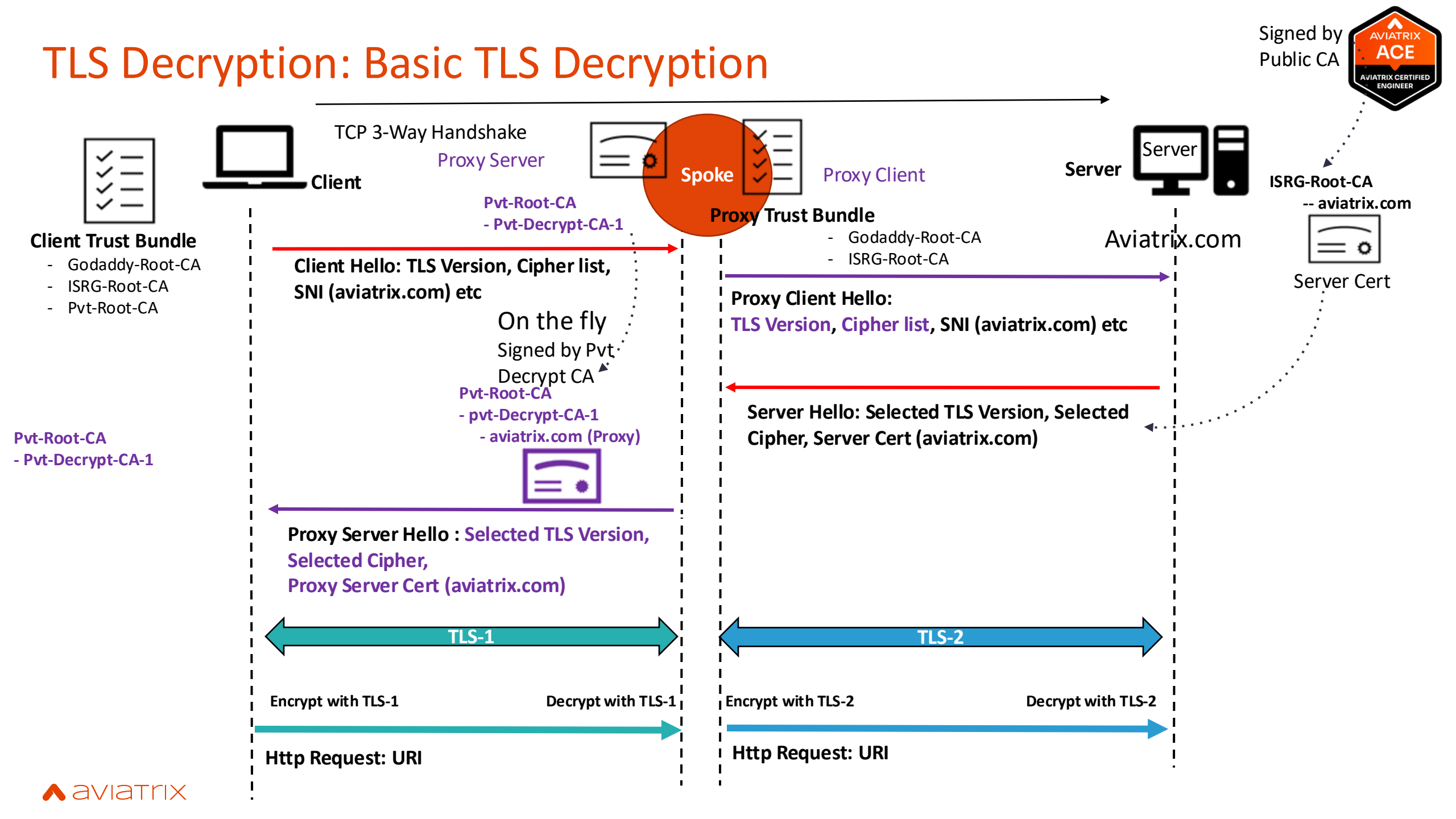
Used by the Client and/or Proxy Gateway to Identify/ Trust the Original Server Cert

Decryption CA Cert

Used by the Decryption/Proxy gateway to generate a new Proxy-Server Cert and Sign it with the Decryption CA Cert

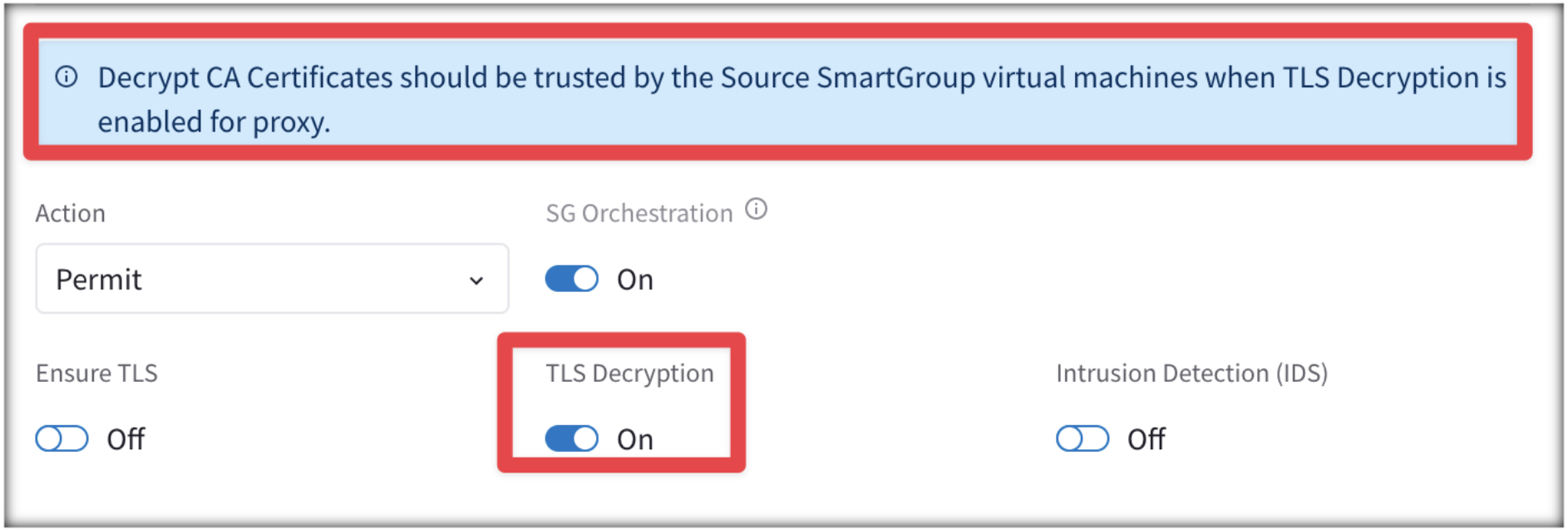


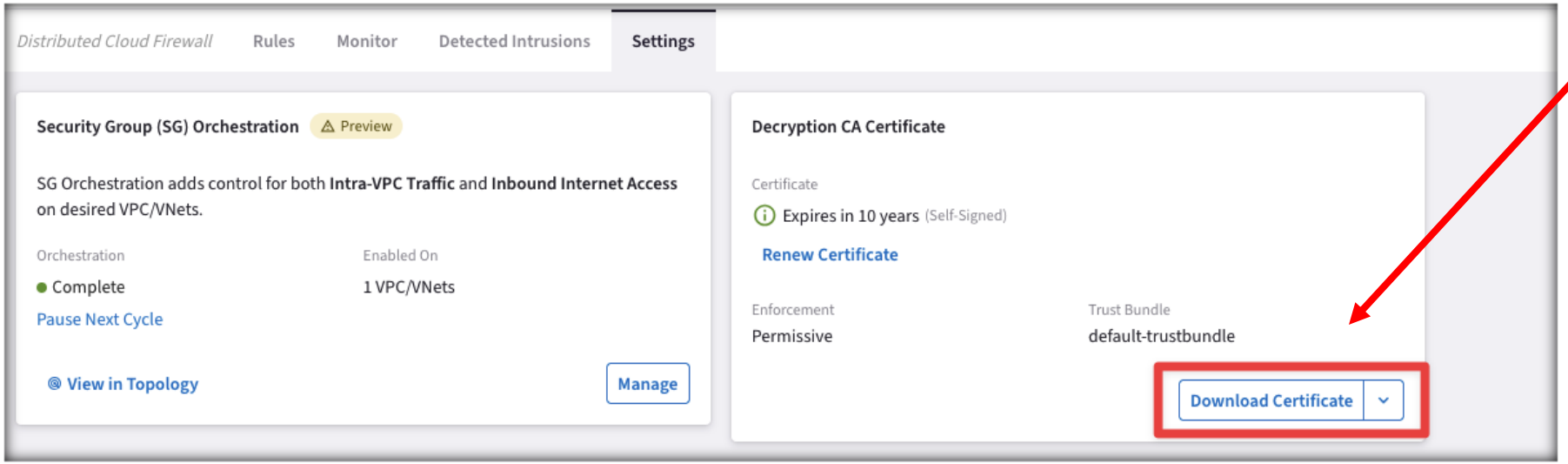
TLS Decryption: Basic TLS Decryption



aviatrix

TLS Decryption: Decryption CA Cert

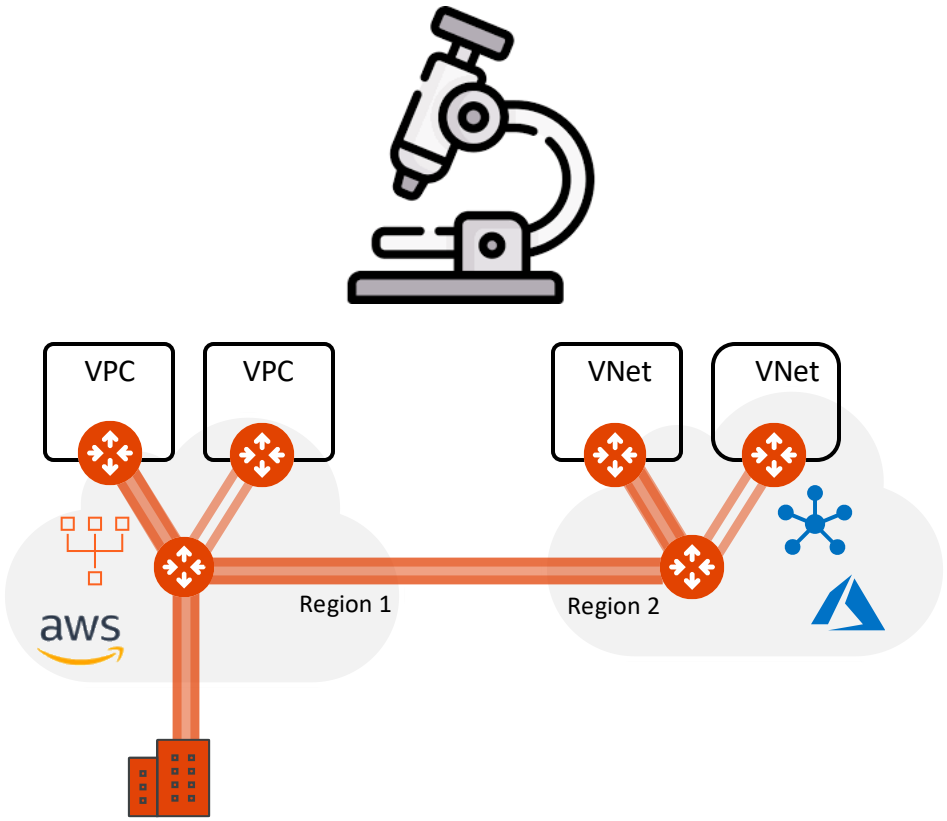


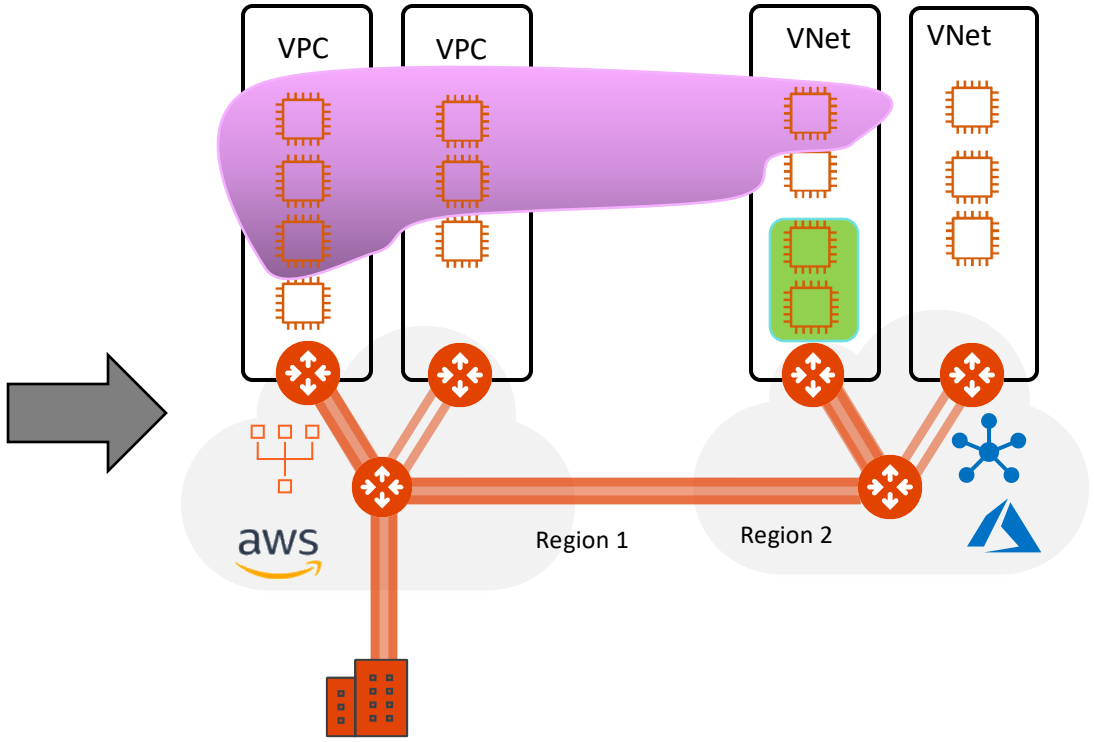


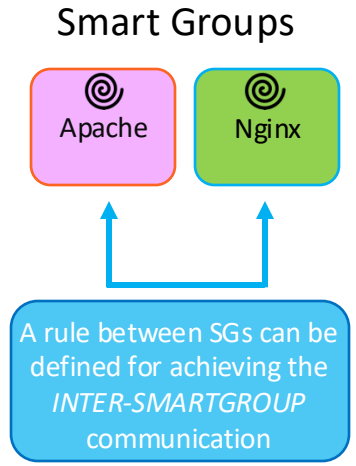
1. Download the Decryption CA Bundle.
2. Distribute the bundle across all the workloads.

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

Distributed Cloud Firewall Rule Types: Intra-rule vs. Inter-rule



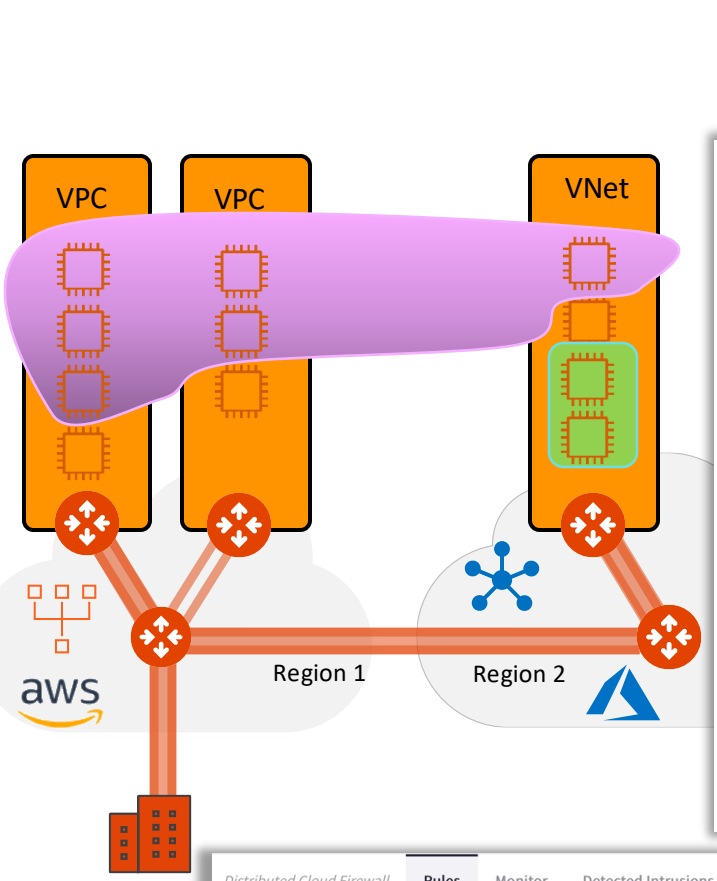


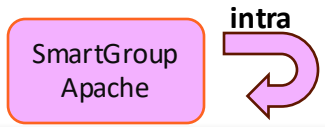


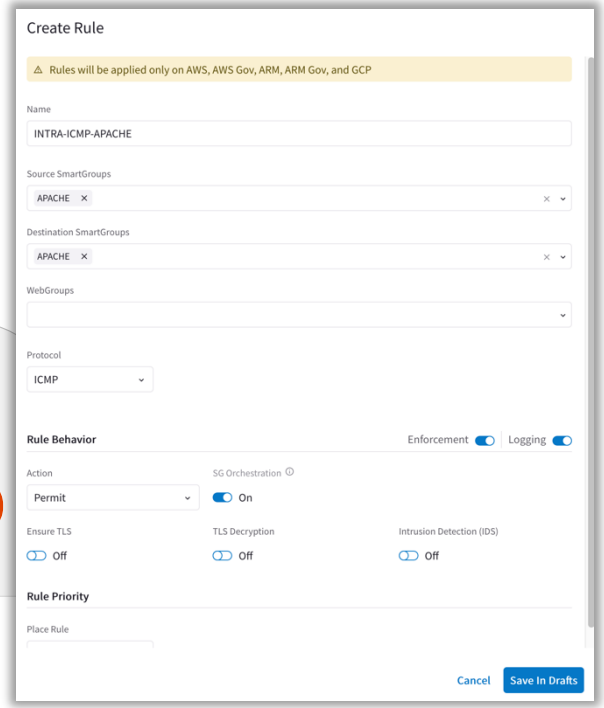
- **INTRA-RULE**: is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

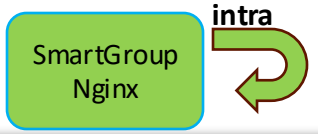
- **INTER-RULE:** is defined among Smart Groups, for dictating what kind of traffic is allowed/prohibited among two or more Smart Groups.

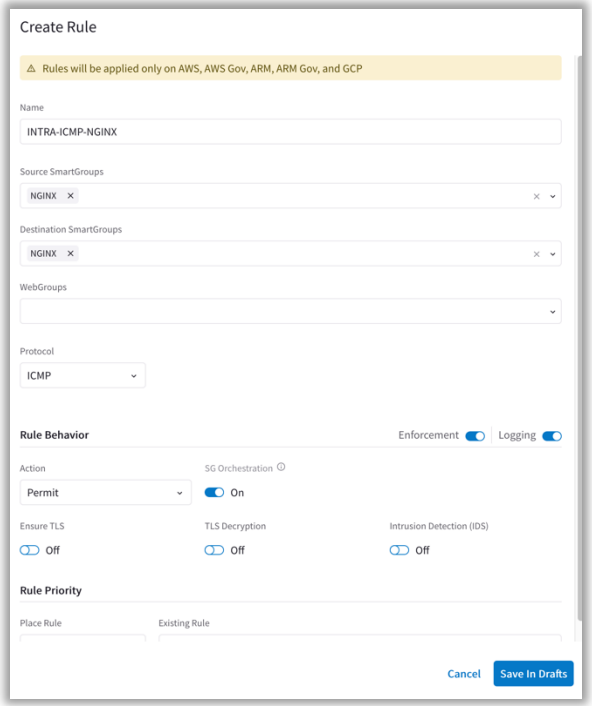
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules

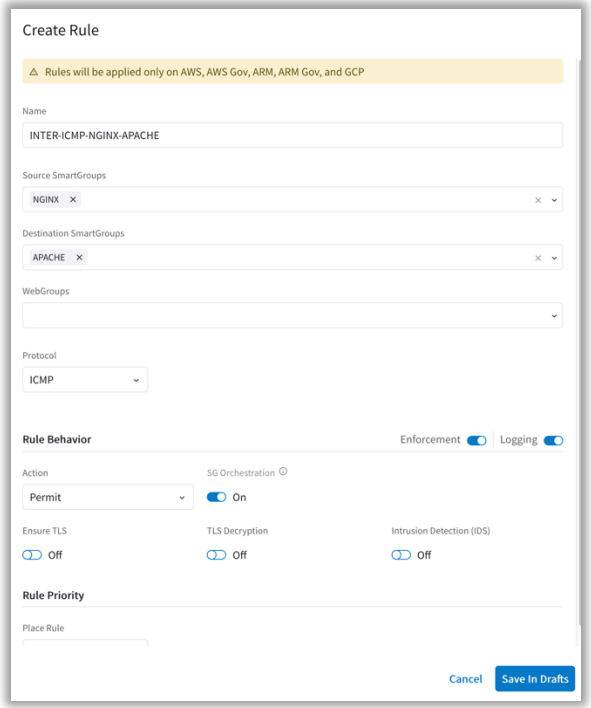


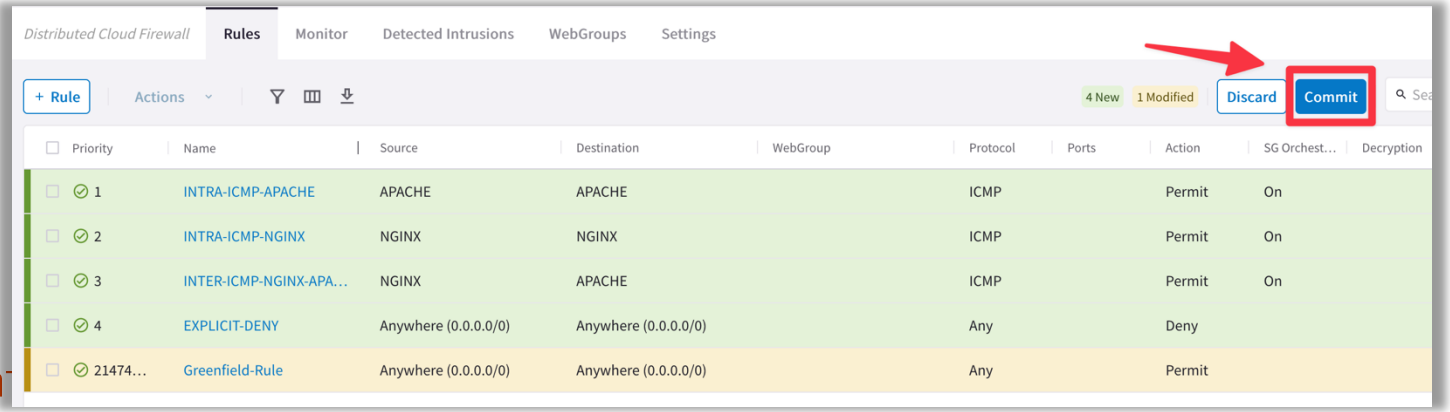






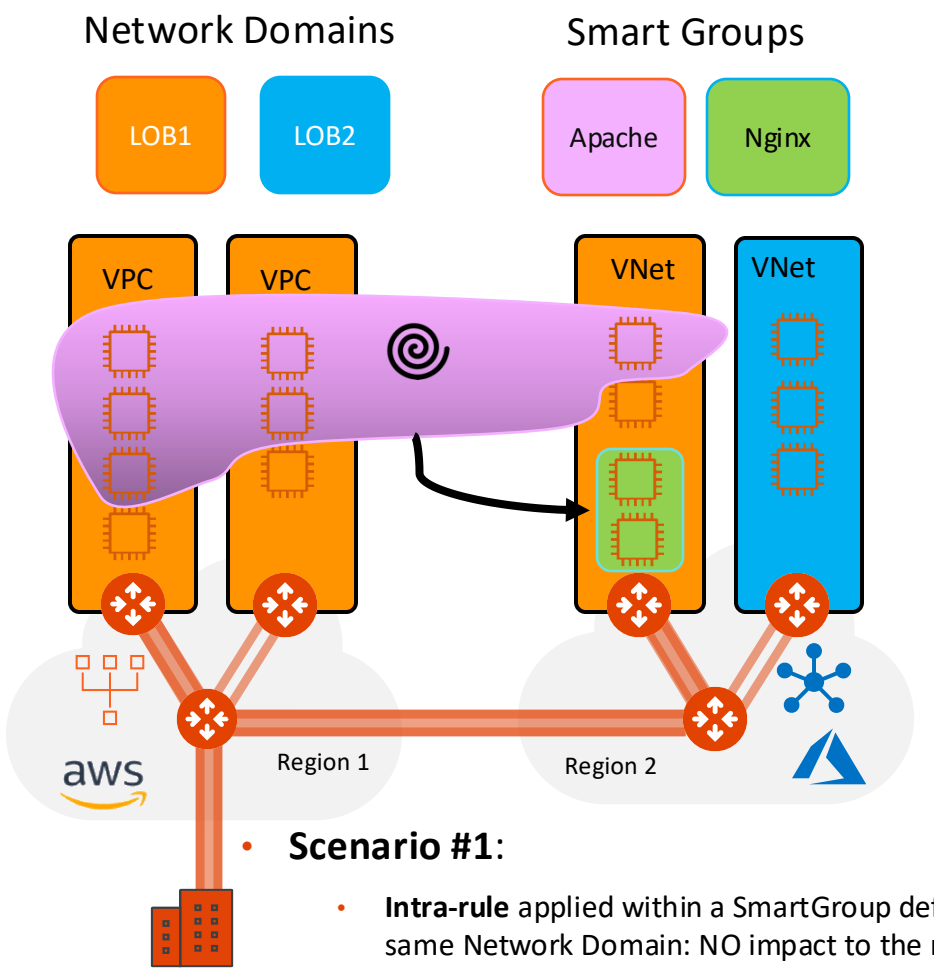




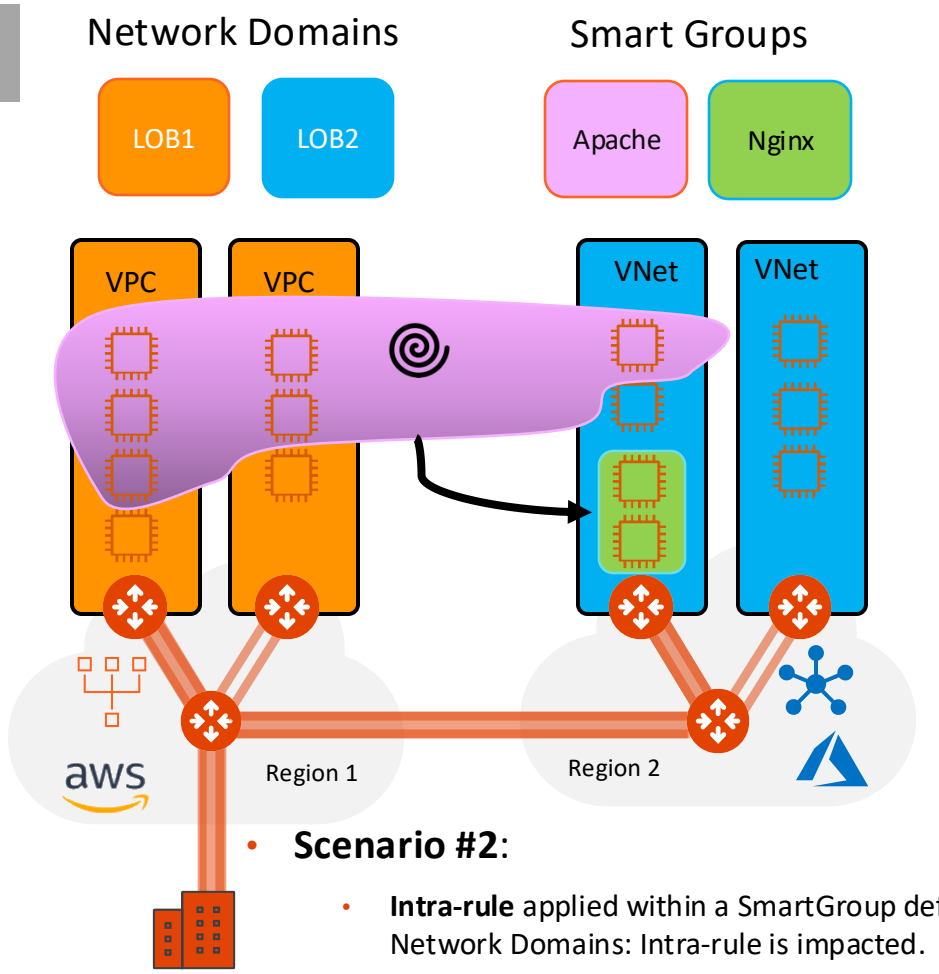


- **Micro-Segmentation**: Combination of SmartGroups and DCF Rules
- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return traffic is allowed automatically

Network Segmentation & Distributed Cloud Firewall Rule together



NO connection policy is applied



- **Scenario #1**:
  - **Intra-rule** applied within a SmartGroup defined within the same Network Domain: NO impact to the rule
  - **Inter-rule** applied between SmartGroups defined within the same Network Domains: NO impact to the rule

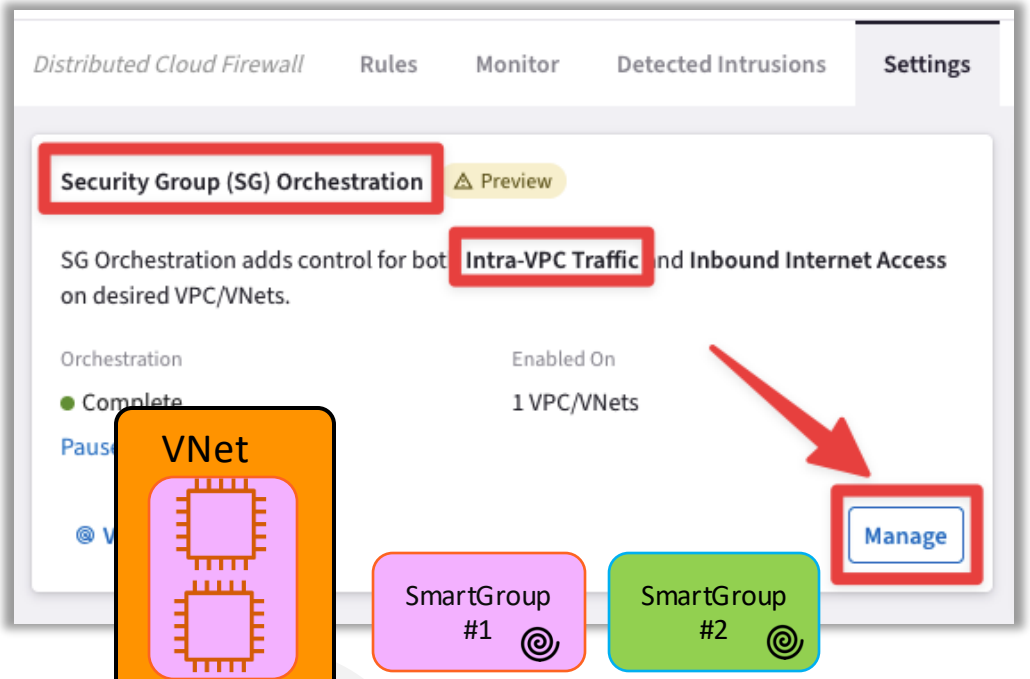
- **Scenario #2**:
  - **Intra-rule** applied within a SmartGroup defined across two Network Domains: Intra-rule is impacted.
  - **Inter-rule** is applied between SmartGroups defined across two different Network Domains: Inter-rule is impacted

Caveat:

- Network Segmentation and Distributed Firewalling are **NOT** mutually exclusive!
- Network Segmentation takes **precedence** over the extent of a SmartGroup

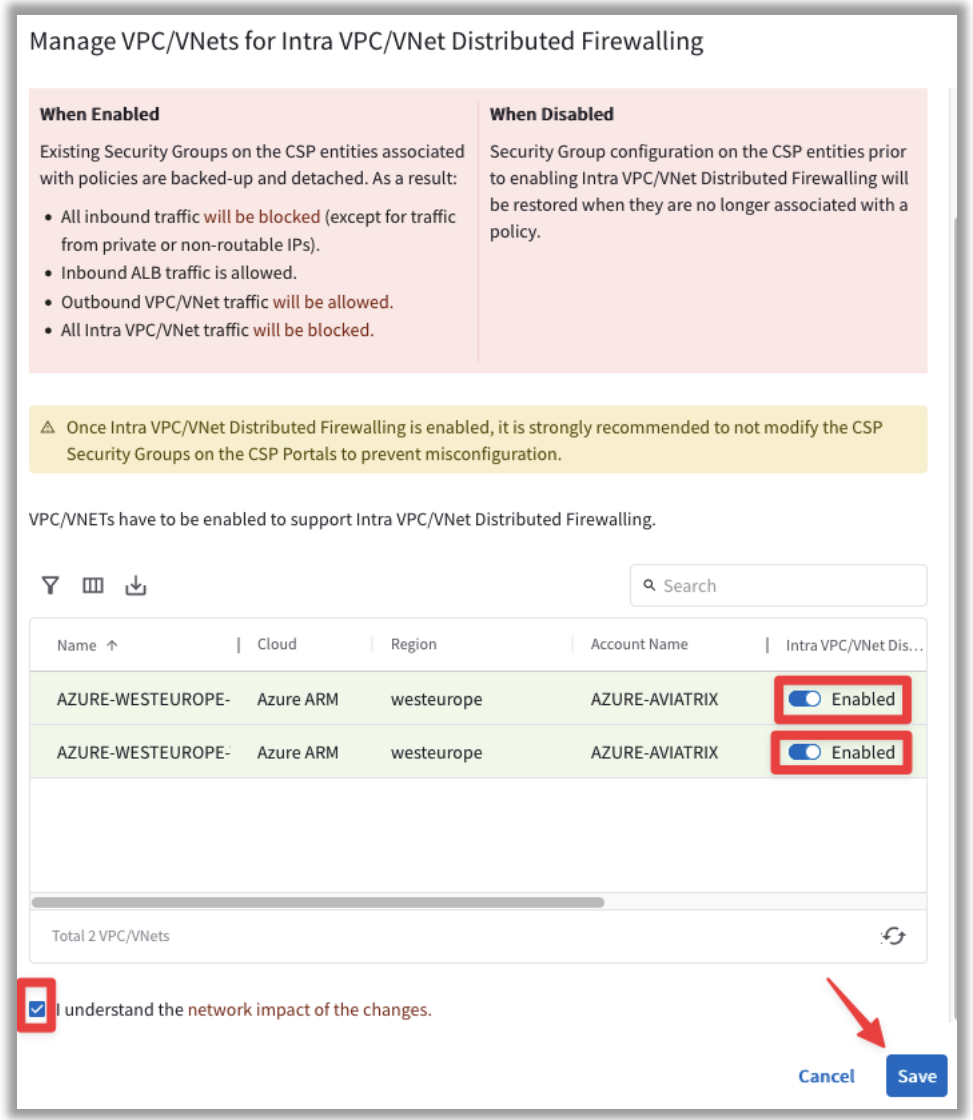
Security Group (SG) Orchestration: Intra VPC/VNET Traffic Control

❑ Enable the feature on the relevant VPC/VNet

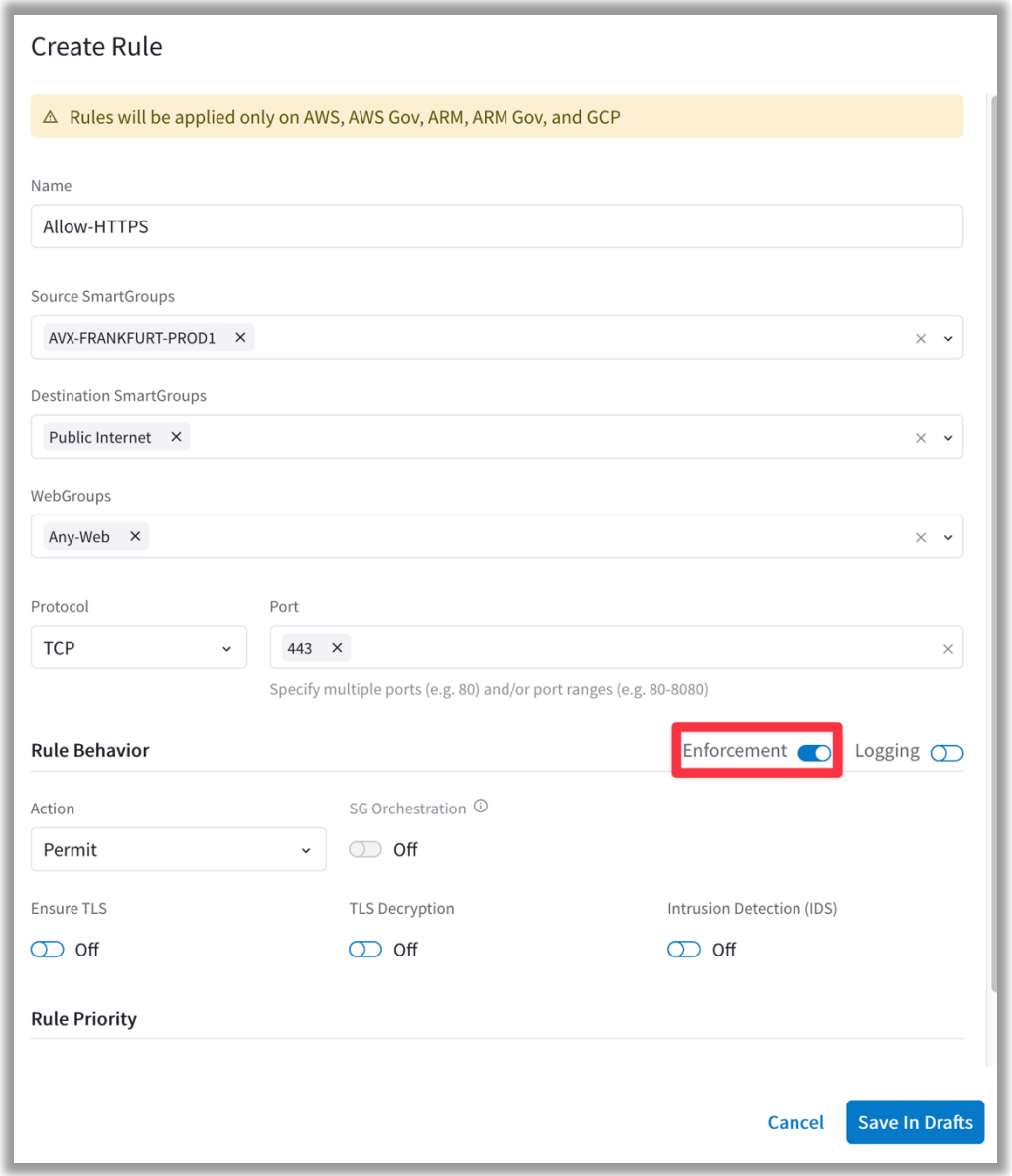


- If you enable the **Security Group (SG) Orchestration** (*aka Intra-VPC Traffic Control*), the SmartGroups defined within the same VPC/VNet will not be able to communicate with each other, unless an inter rule is applied between them.
- This is pure L4 separation, leveraging the Native Cloud Constructs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

CAVEAT: Available in AWS/Azure



Rule Enforcement



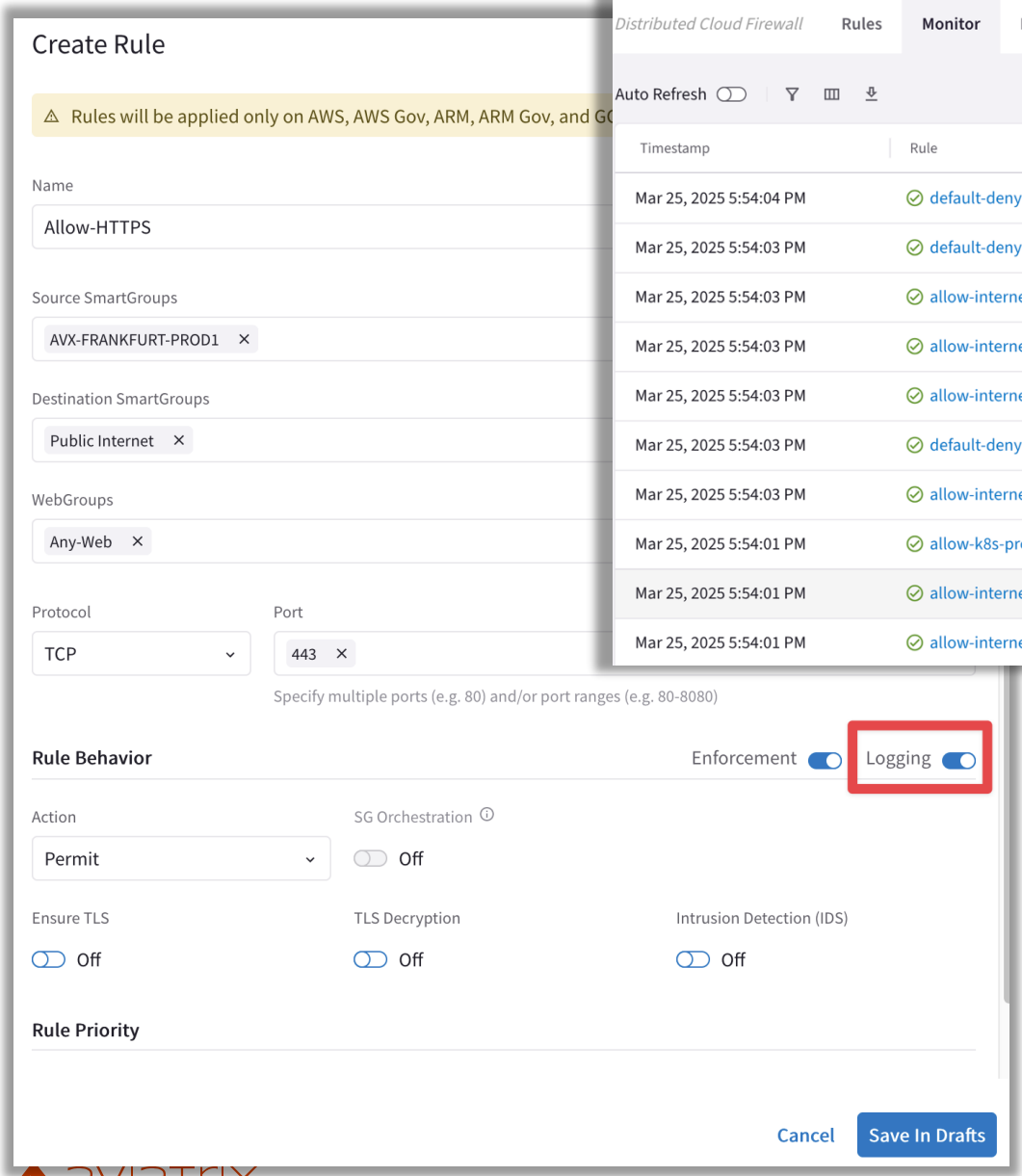
Enforcement ON

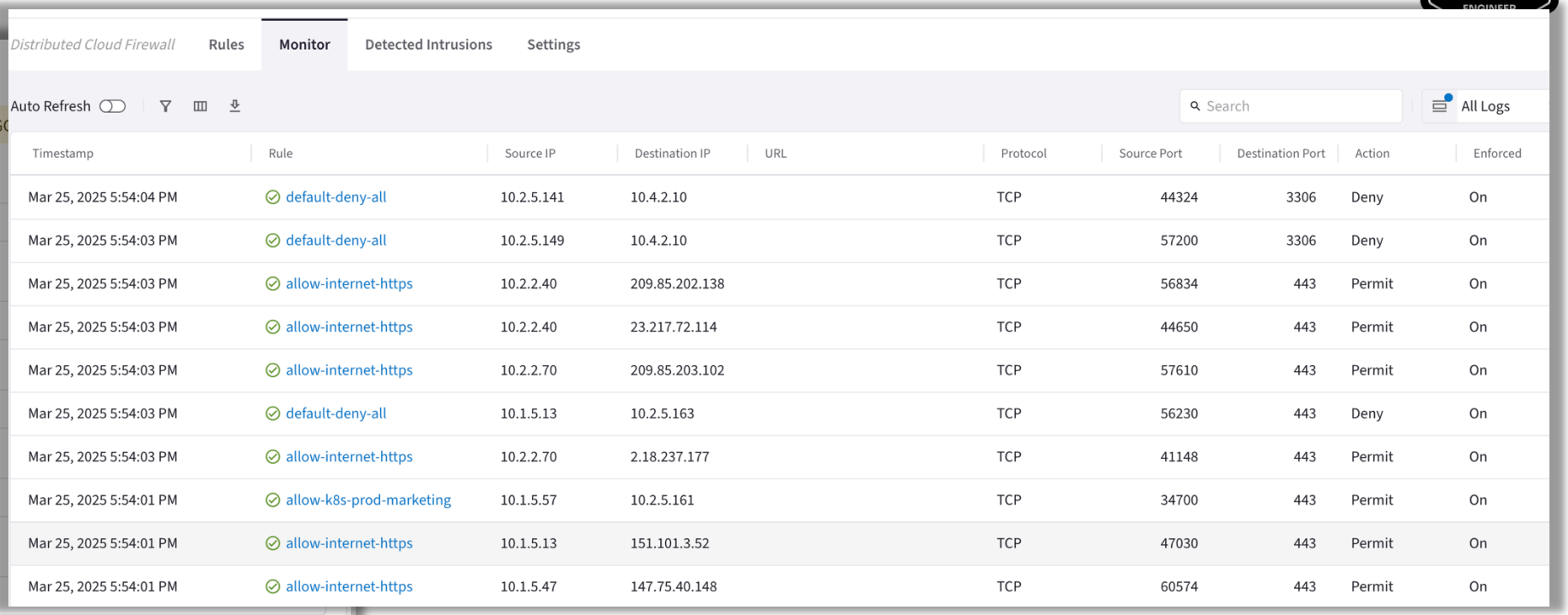
- Policy is enforced in the Data Plane

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



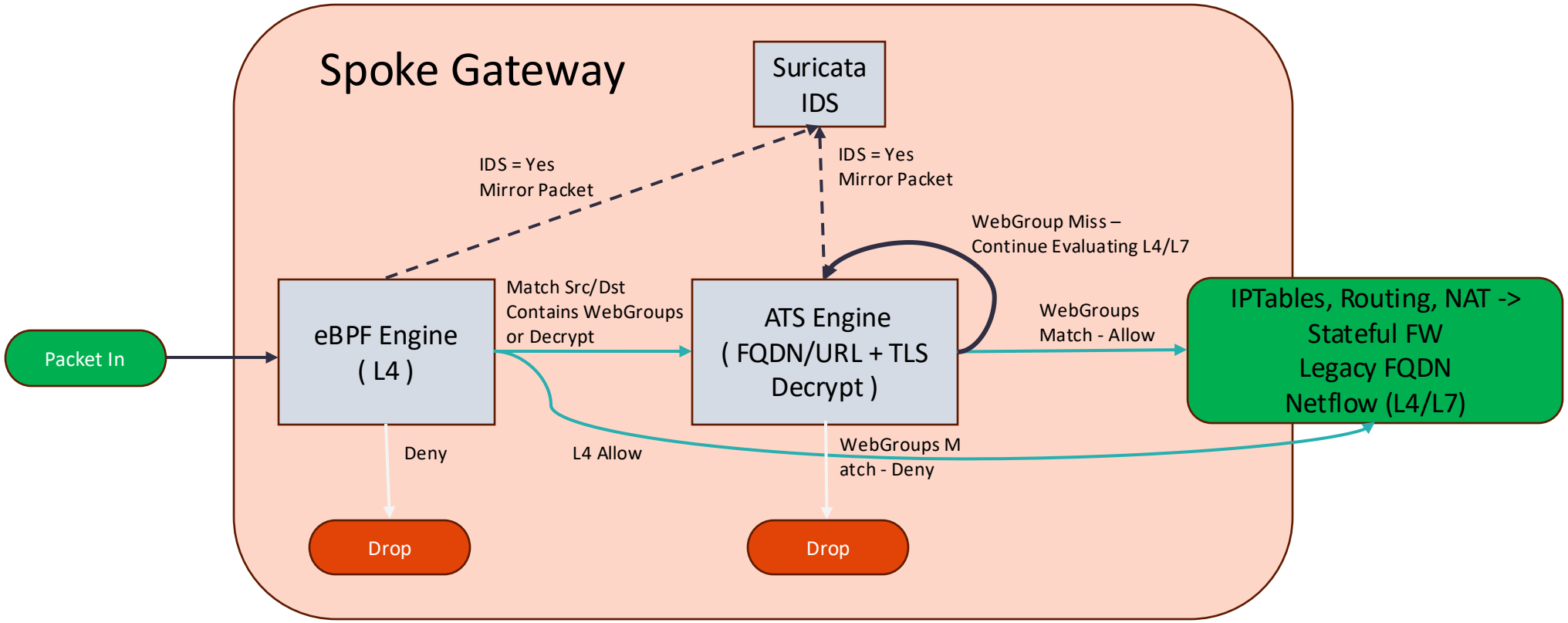


Timestamp	Rule	Source IP	Destination IP	URL	Protocol	Source Port	Destination Port	Action	Enforced
Mar 25, 2025 5:54:04 PM	default-deny-all	10.2.5.141	10.4.2.10		TCP	44324	3306	Deny	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.2.5.149	10.4.2.10		TCP	57200	3306	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	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**

DFW Engines At-a-Glance

- **eBPF** (extended Berkeley Packet Filter) Engine (L4) → Stateful Firewall Rule (forwarding path)
- WebProxy **ATS** (Apache Traffic Server) Engine (L7) → it is triggered whether WebGroups or TLS Decryption are required
- **Suricata** Engine (DPI) → Signature of the payload (<u>only in IDS mode at the moment</u>)



Next: Lab 11 – Distributed Cloud Firewall