Security Close to the Applications

AVIATRIX DISTRIBUTED CLOUD FIREWALL

NIST Tenets Covered

This module will cover two tenets of NIST Zero-Trust Architecture (ZTA)

1. Security Close to the Applications
2. Global, Dynamic and Centralized Policy Model

Related Aviatrix Features

- Aviatrix Distributed Cloud Firewall
- Network Segmentation
- Micro-Segmentation
- ThreatIQ / ThreatGuard
- GeoBlocking
- URL Filtering / Internet Egress Traffic Filtering
- Centralized Policy Engine

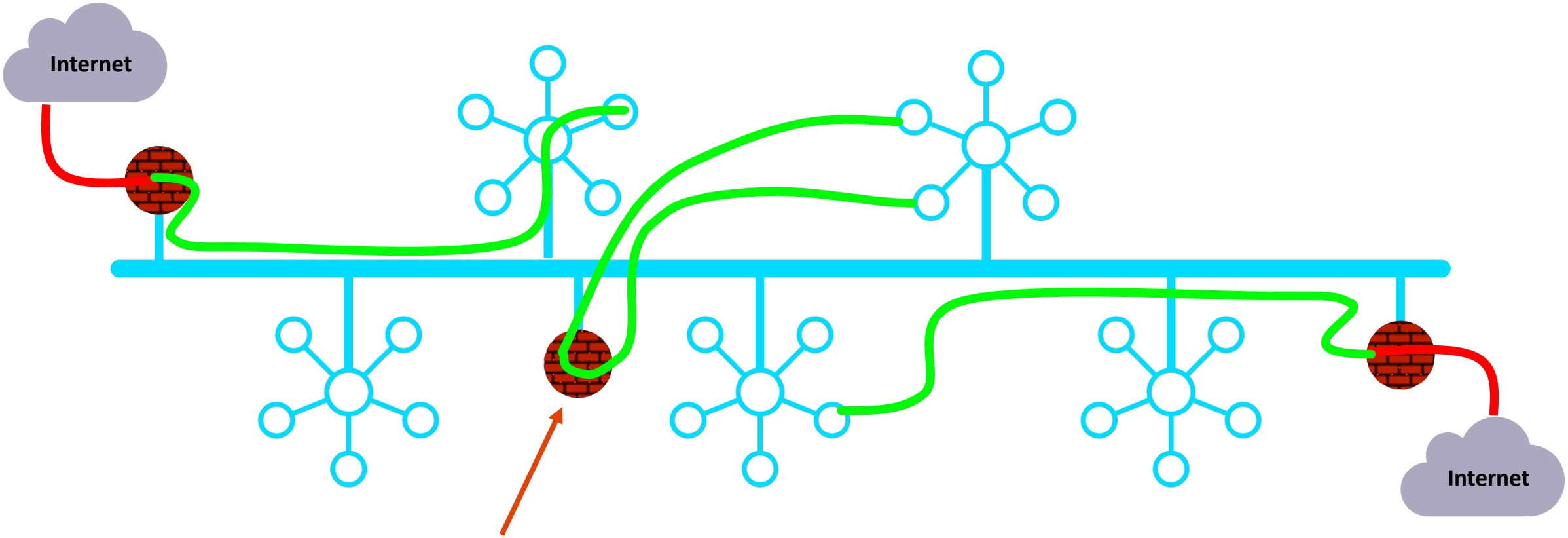
Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture. Workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise networks. This also includes workloads migrating from on-premises data centers to non-enterprise cloud instances.

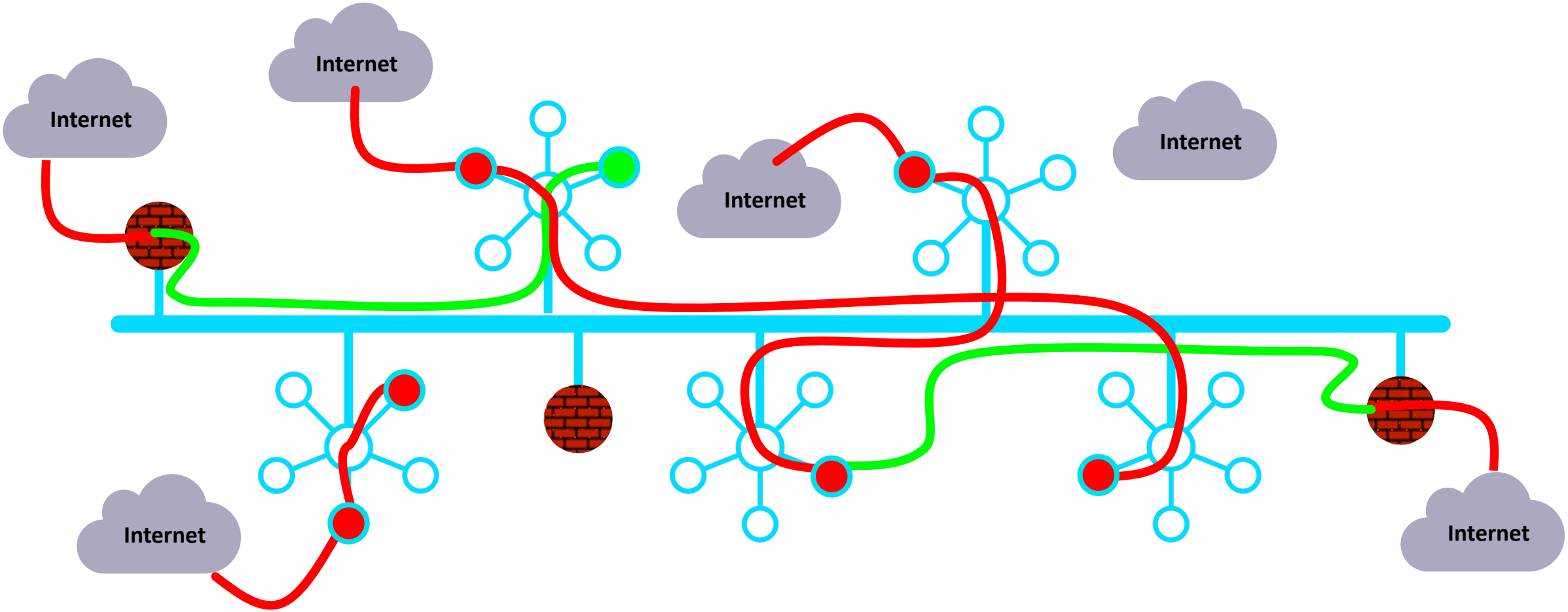
Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

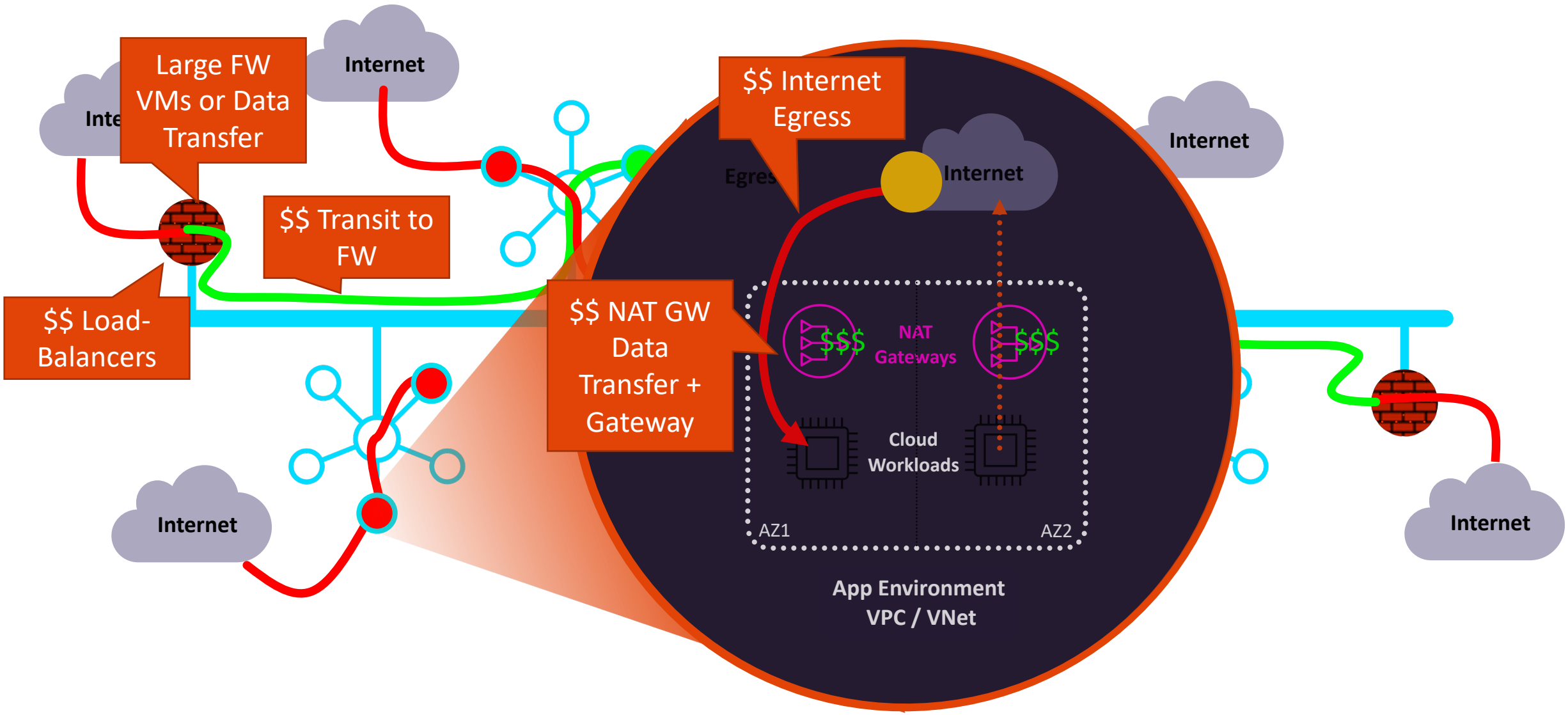
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…



In Reality…

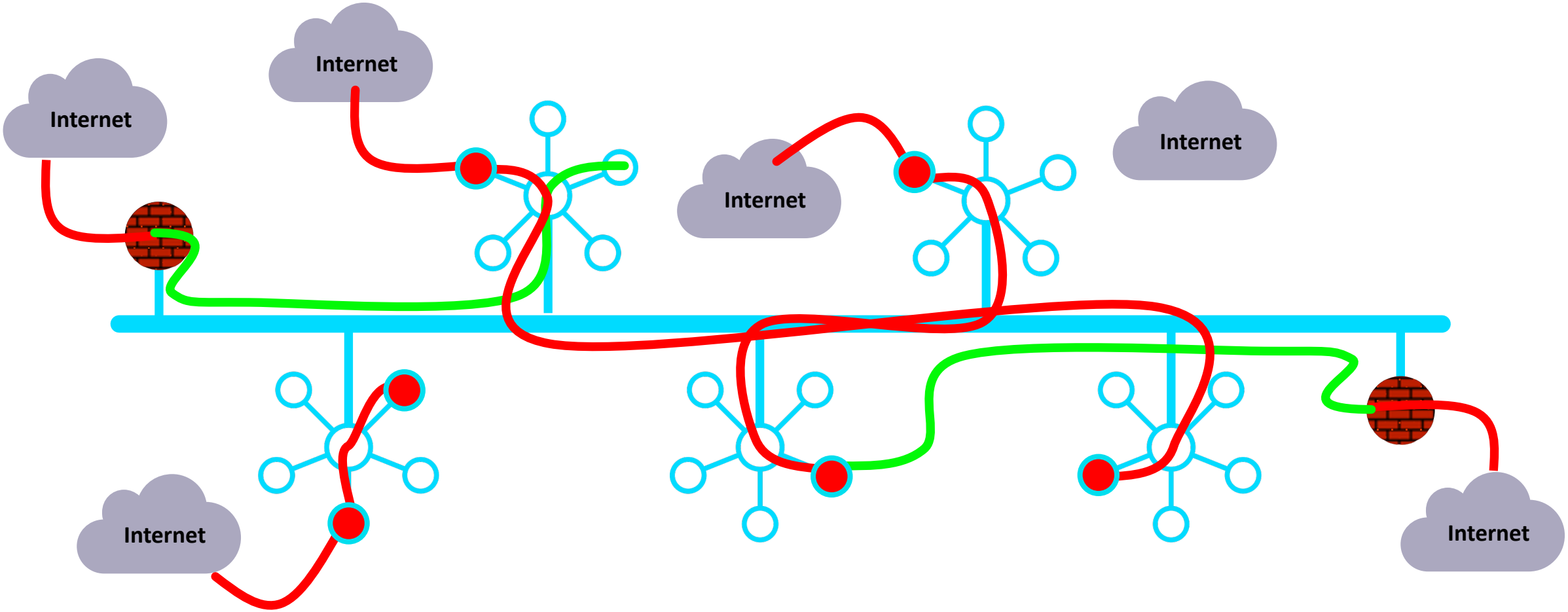

Internet
Internet
Internet
Internet
Internet
Internet
Internet

This is bad! Expensive and Lacks Enterprise-Grade Security

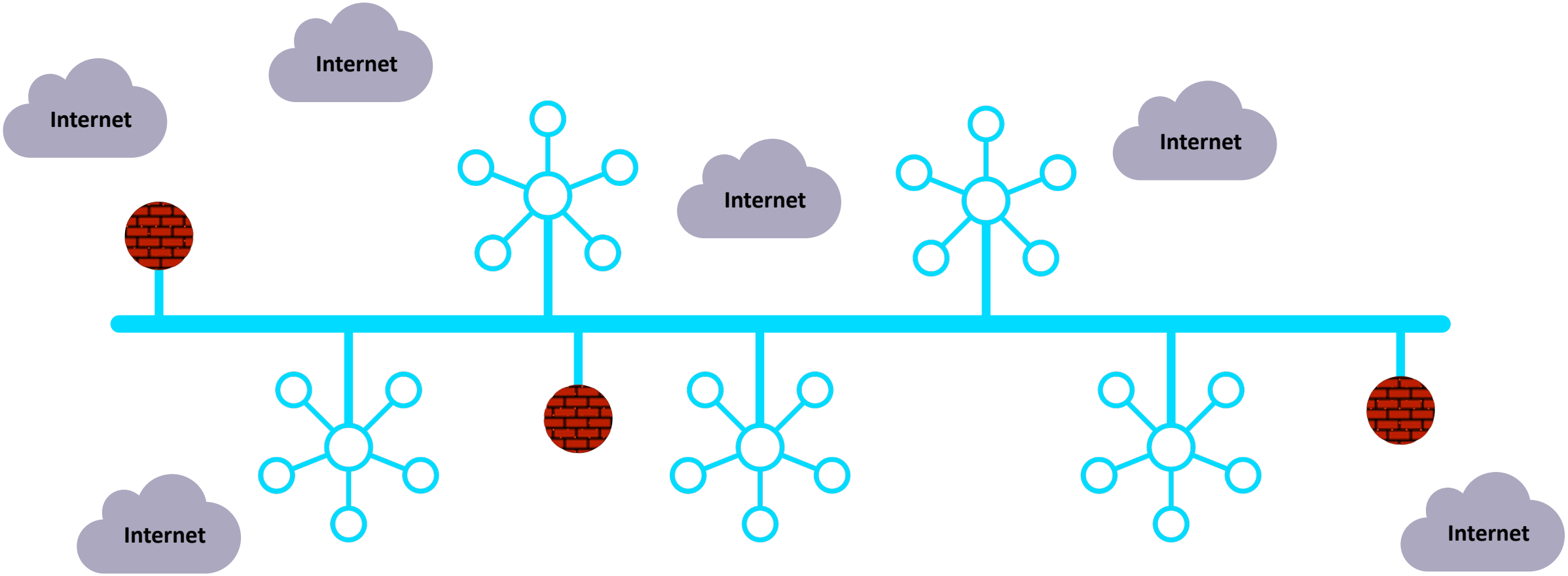


aviatrix

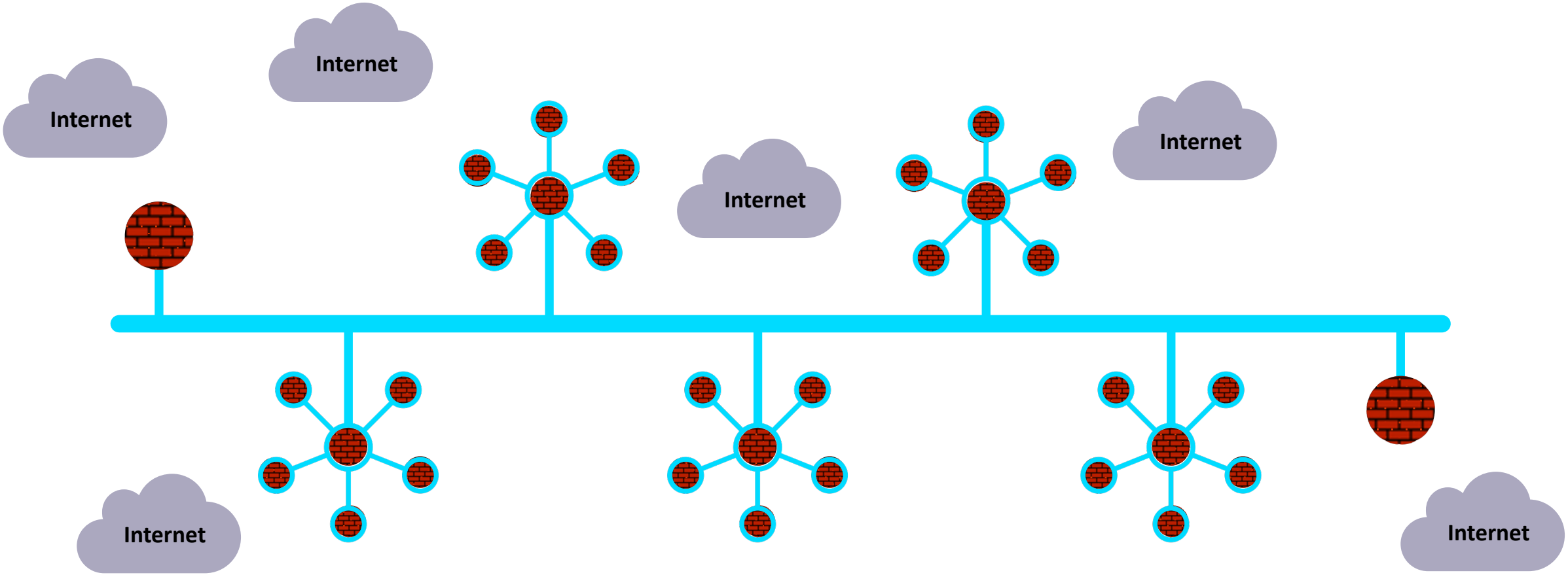
In Reality…


Internet
Internet
Internet
Internet
Internet
Internet
Internet

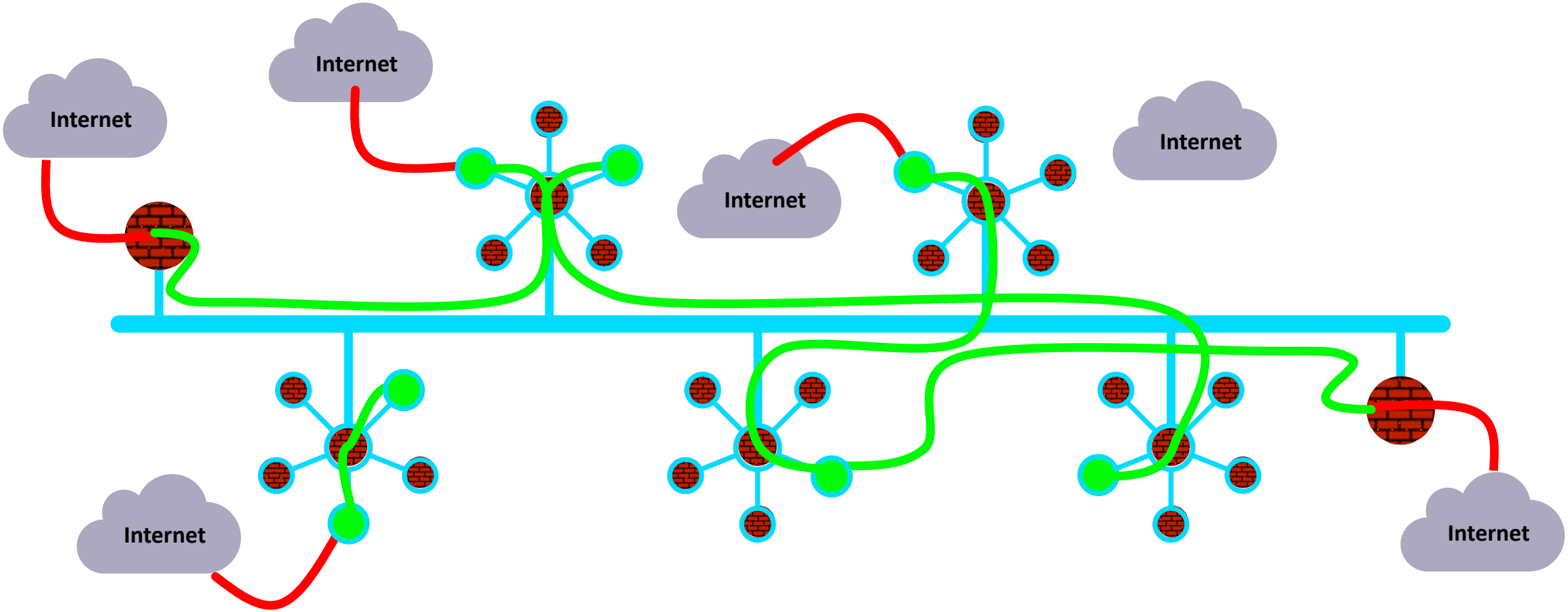
What If…


Internet
Internet
Internet
Internet
Internet
Internet
Internet

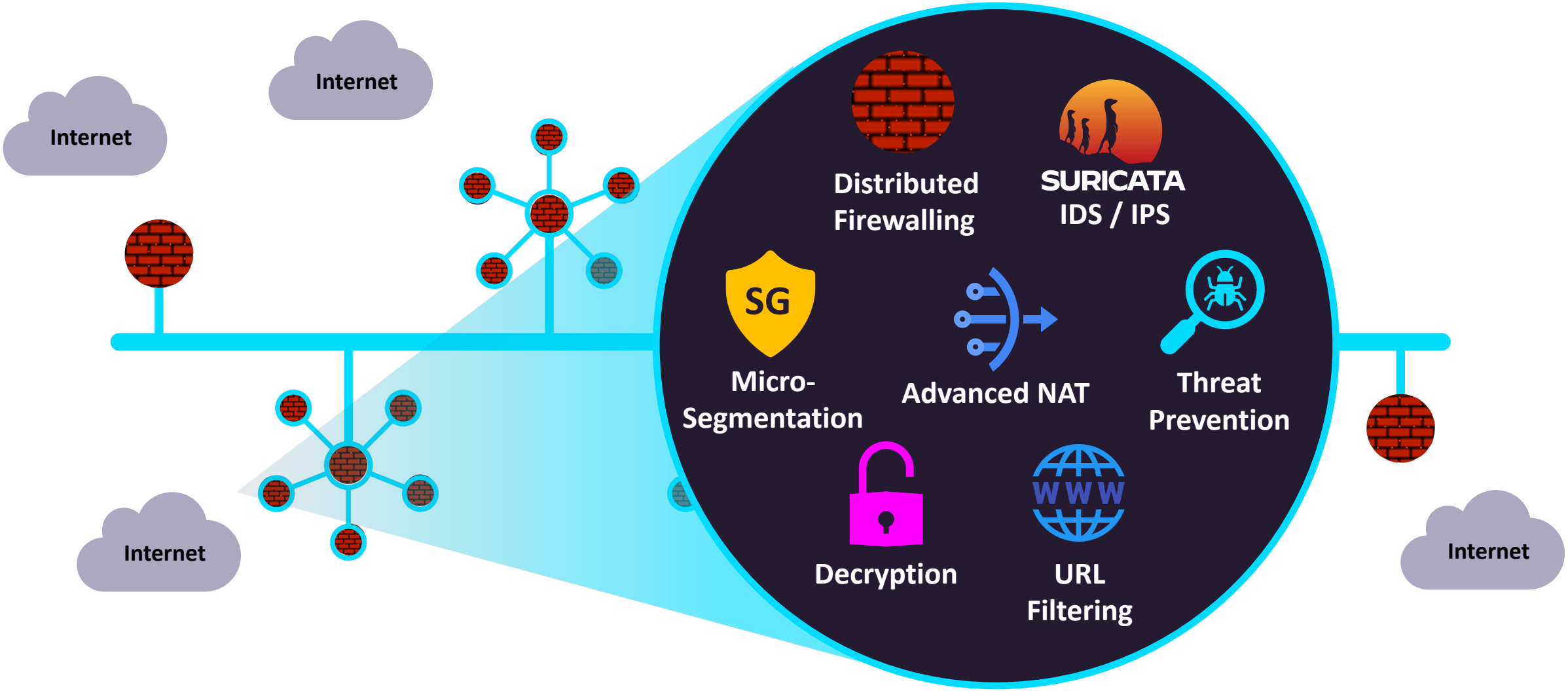
Firewalling Functions were Embedded in the Cloud Network Everywhere…



Centrally Managed, with Distributed Inspection & Enforcement…

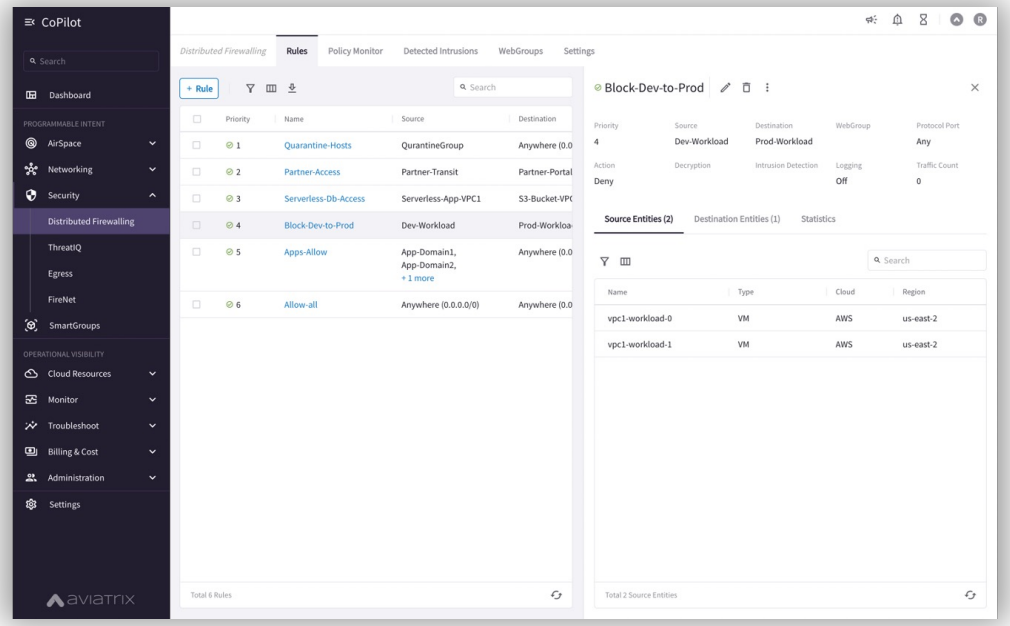


And, What If it was more than just firewalling…



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

Centralized Policy Creation → **Distributed Enforcement**



Aviatrix CoPilot

IDS / IPS

Micro-Segmentation

Threat Prevention

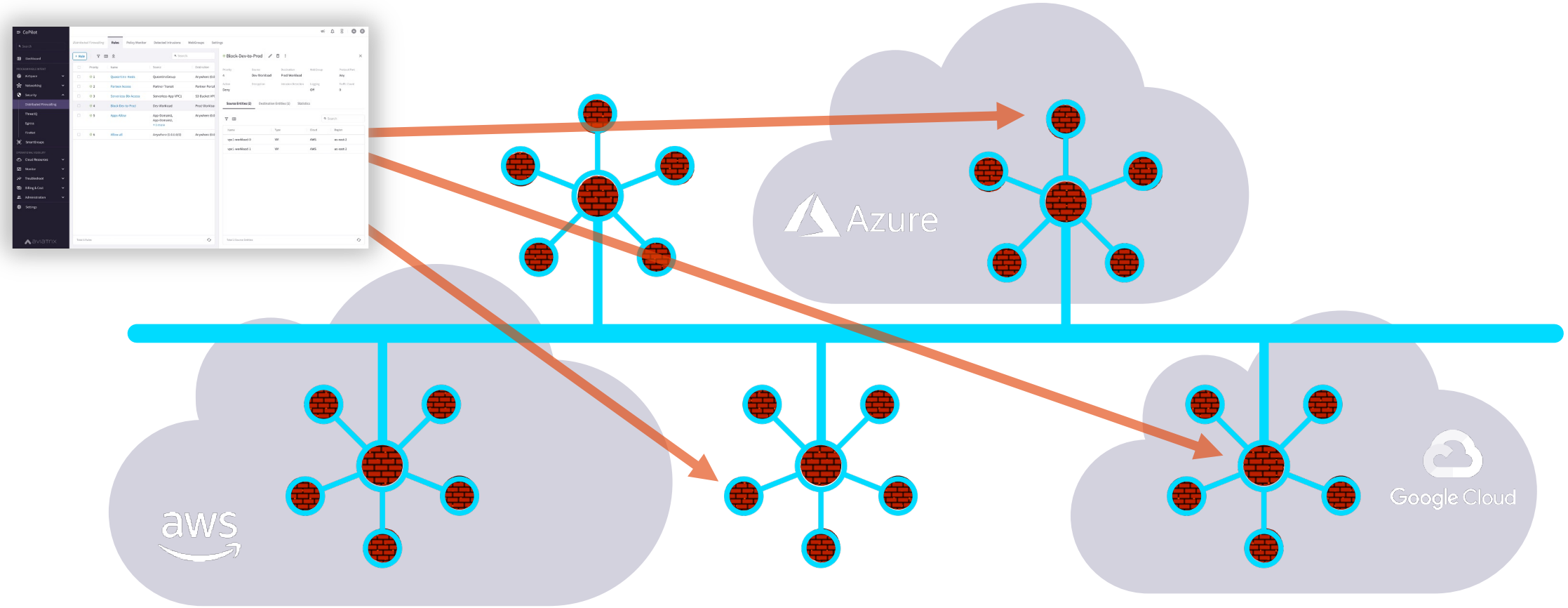
Advanced NAT

Distributed Firewalling

Decryption

URL Filtering

A Distributed Cloud Firewall…

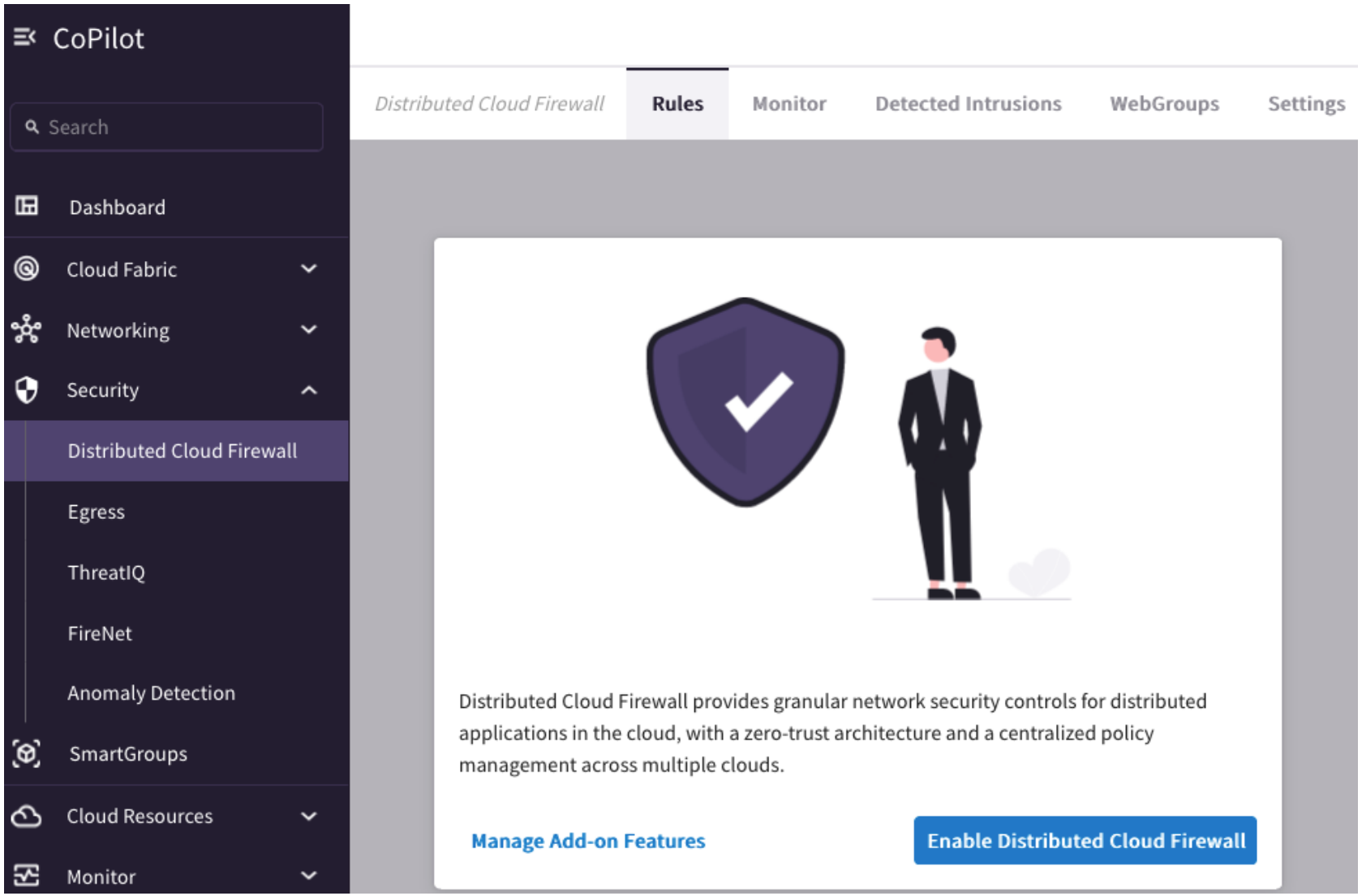


Where and How Policies Are Enforced Is Abstracted…

Enabling Aviatrix Distributed Cloud Firewall (DCF)

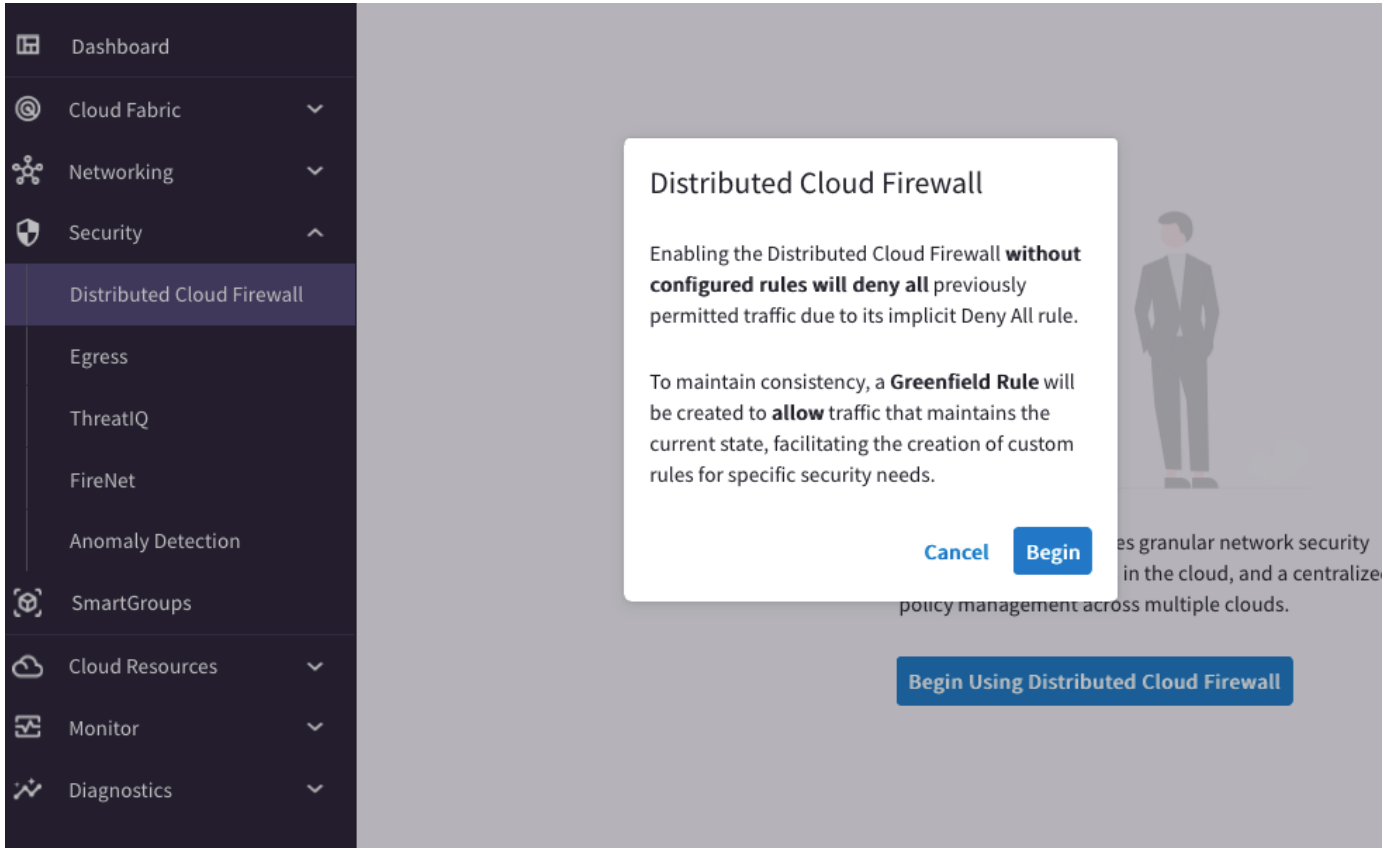
Global Policy – Distributed Enforcement

Enable Distributed Cloud Firewall



Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

Enable Distributed Cloud Firewall

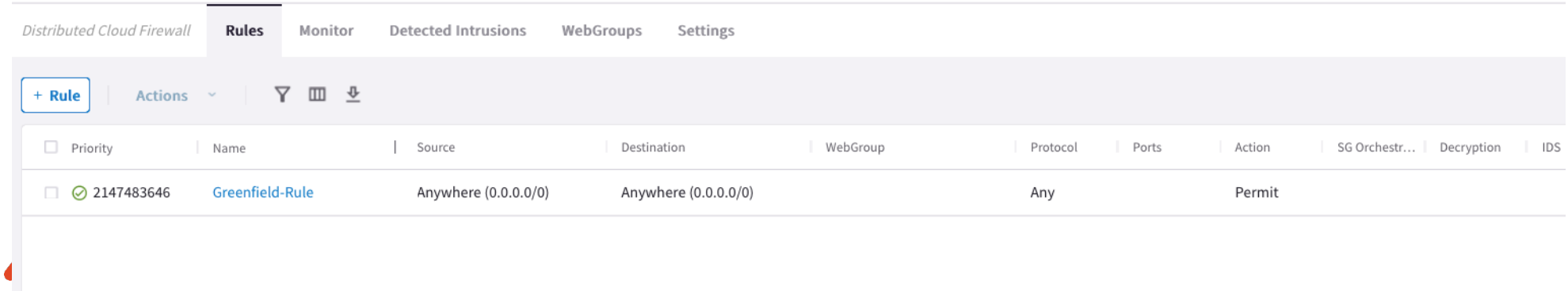


Enabling the Distributed Cloud Firewall **without configured rules will deny all** previously permitted traffic due to its implicit Deny All rule.

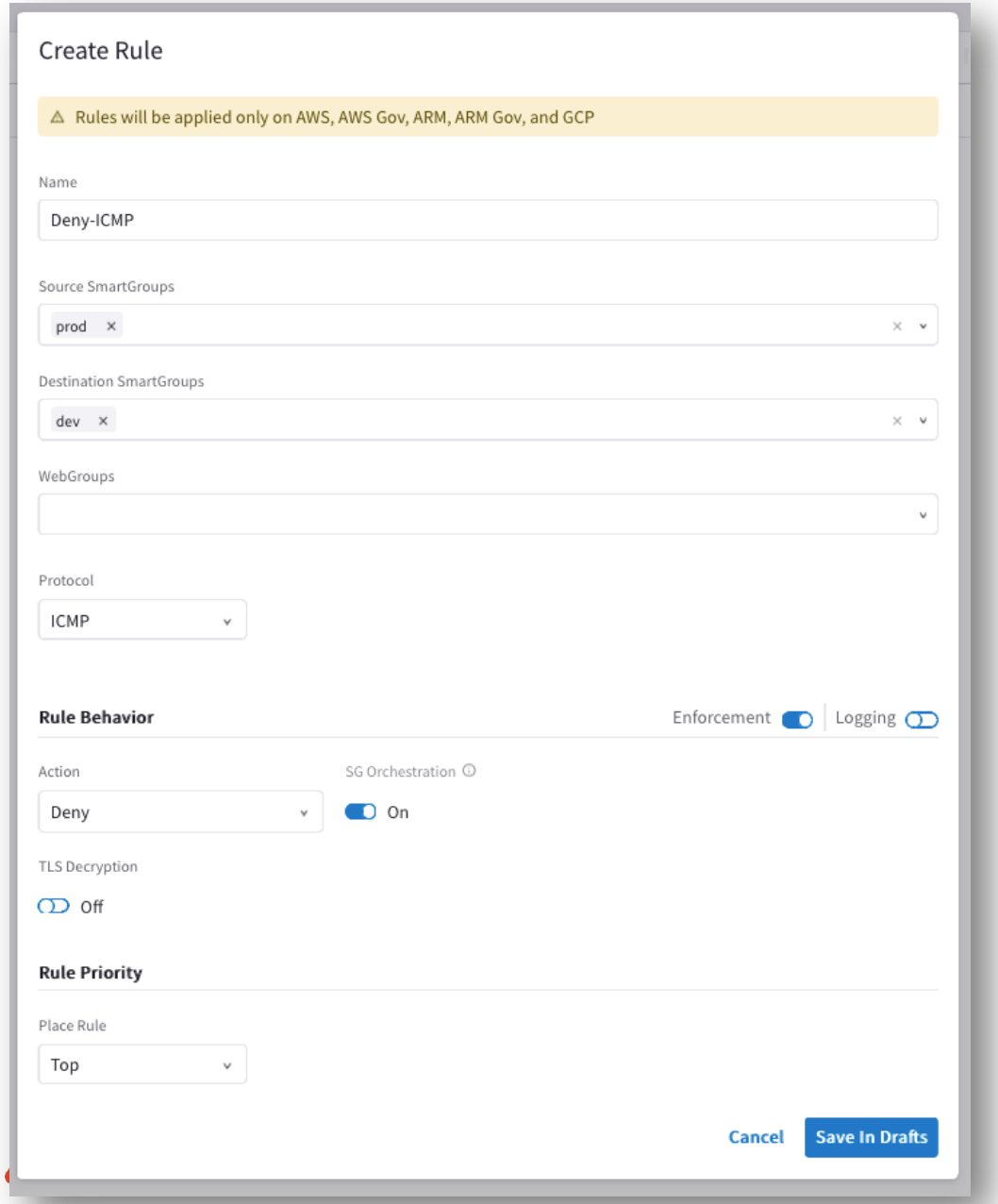
To maintain consistency, a **Greenfield Rule** will be created to **allow** traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.

DENY LIST MODEL

- ❑allow all data to flow, except for exactly what you say should be stopped.



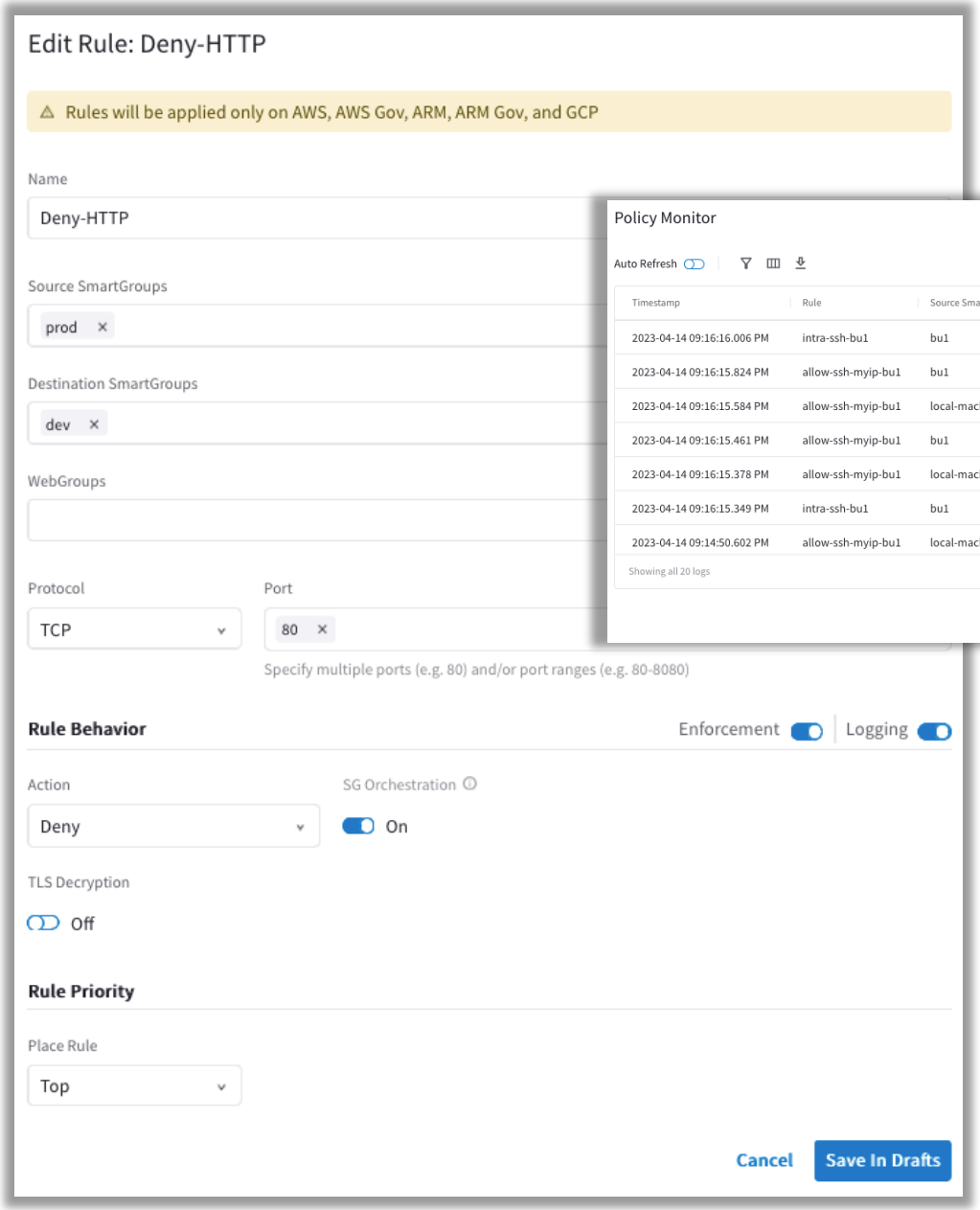
Global Policy Rule Creation and Enforcement

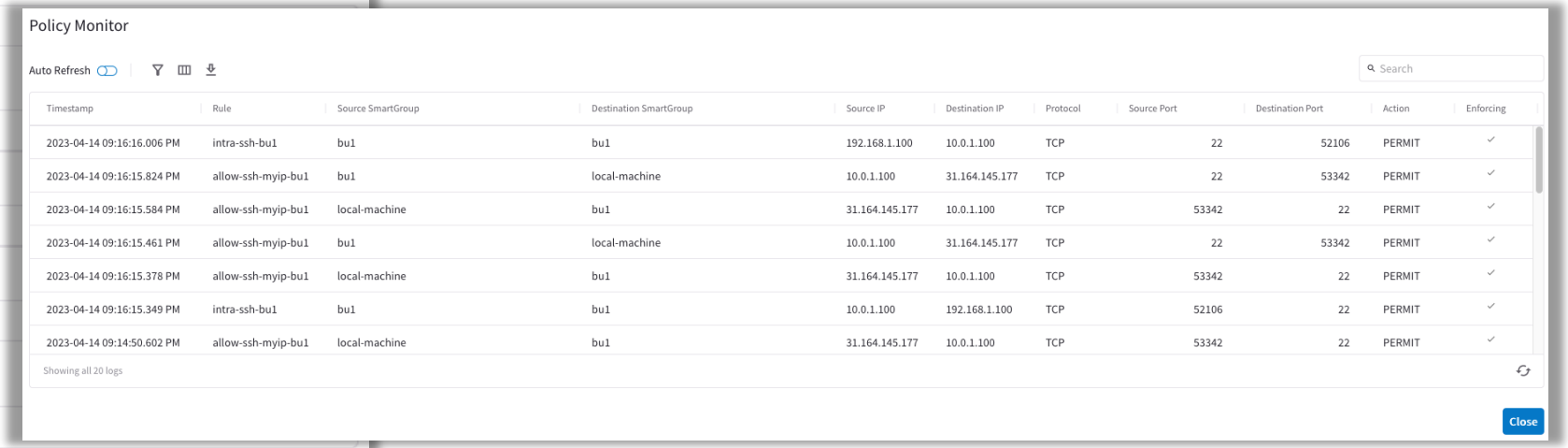


- **Enforcement ON**
  - The policy is enforced in the Data Plane
- **Enforcement OFF**
  - The policy is NOT enforced in the Data Plane
  - The option provides a *Watch/Test* mode
  - Watch what traffic hits the deny rule before enforcing the rule in the Data Plane.
- Security Group Orchestration
  - Provides both Intra VPC/VNET traffic and Inbound Internet Access Control

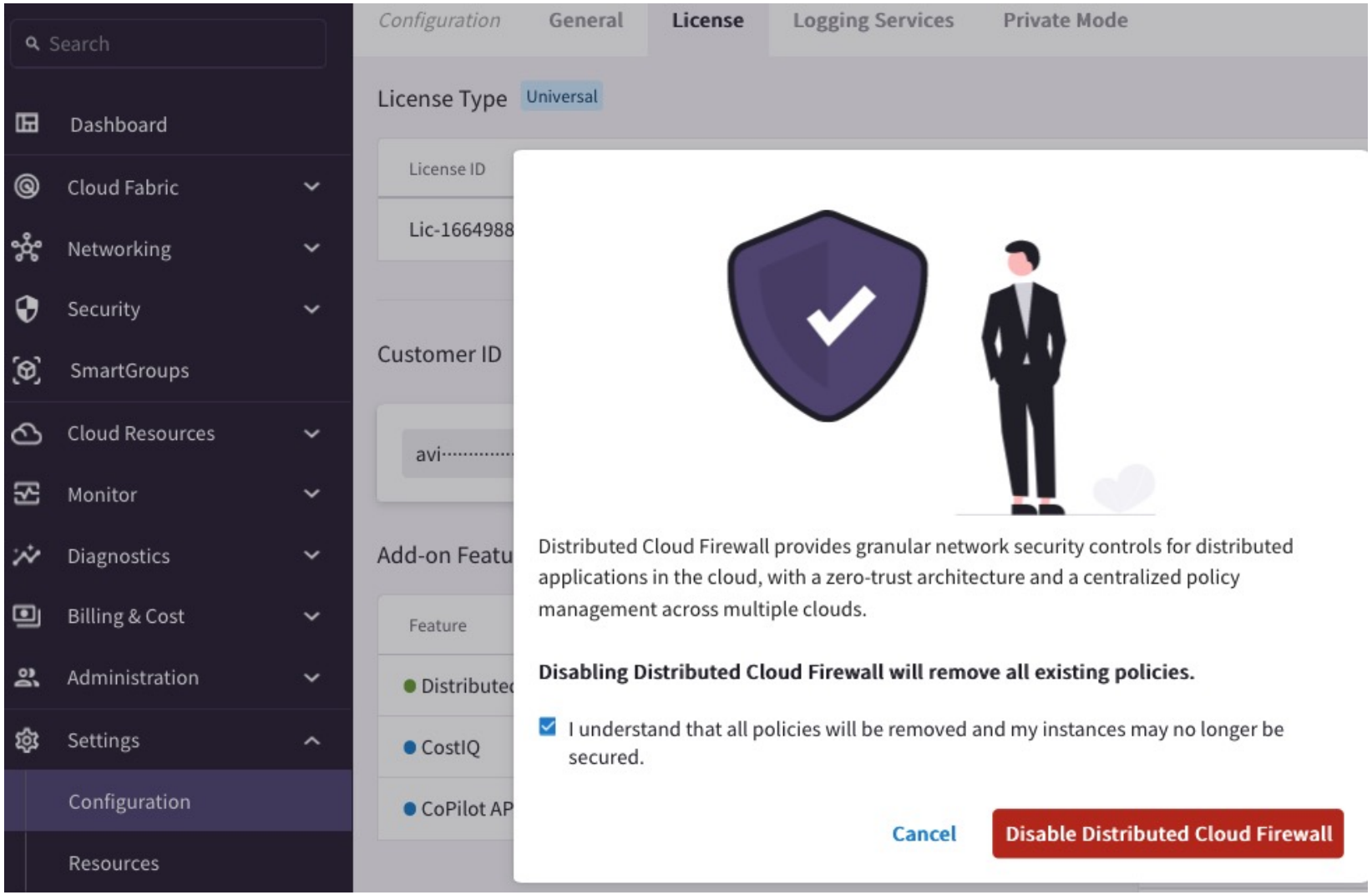
Rule Logging

- Logging can be turned ON/OFF per rule
- Aviatrix CoPilot Syslog/Netflow captures all logs

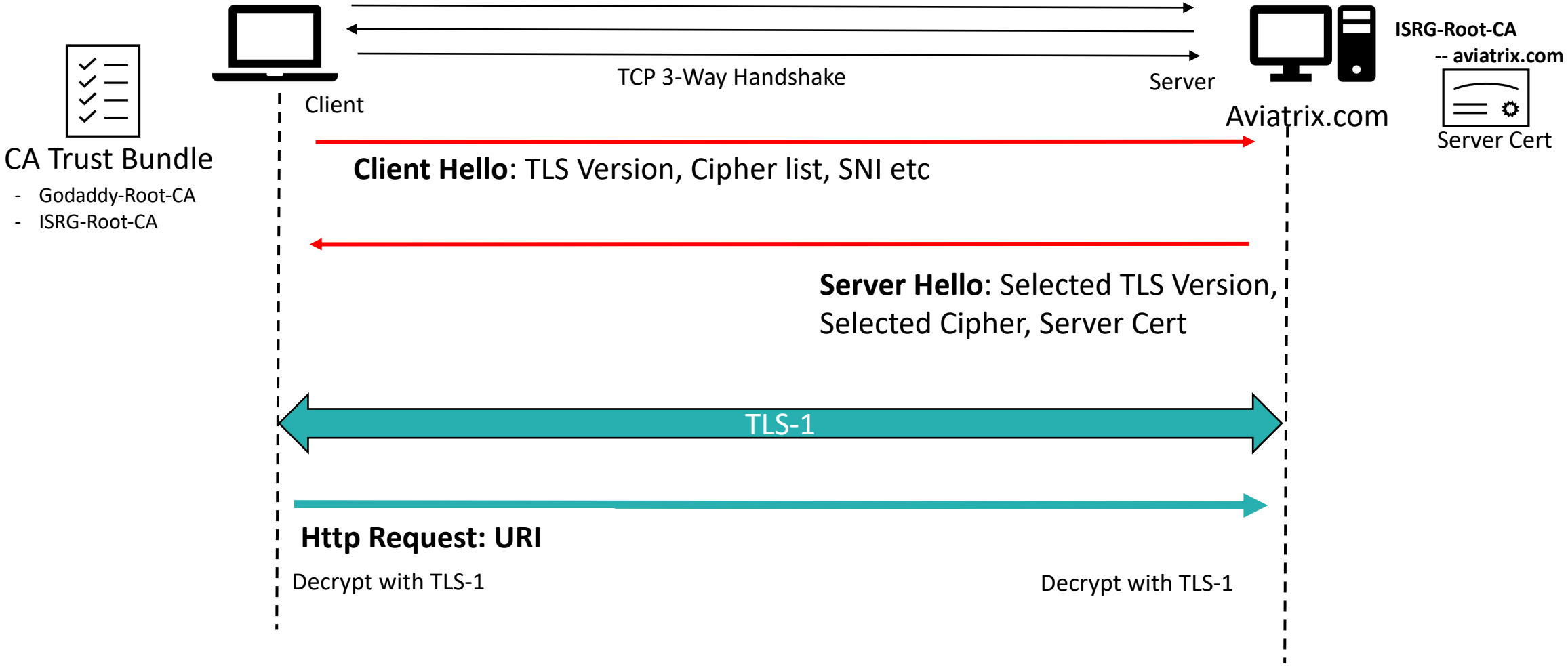




Disabling Distributed Cloud Firewall



TLS Decryption: Basic TLS Connection



TLS Decryption: PKI/ KMS and Trust Bundle

Certificate Hierarchy

- Root
  - Intermediate
    - Server Cert (Leaf Cert)

Certificate Fields

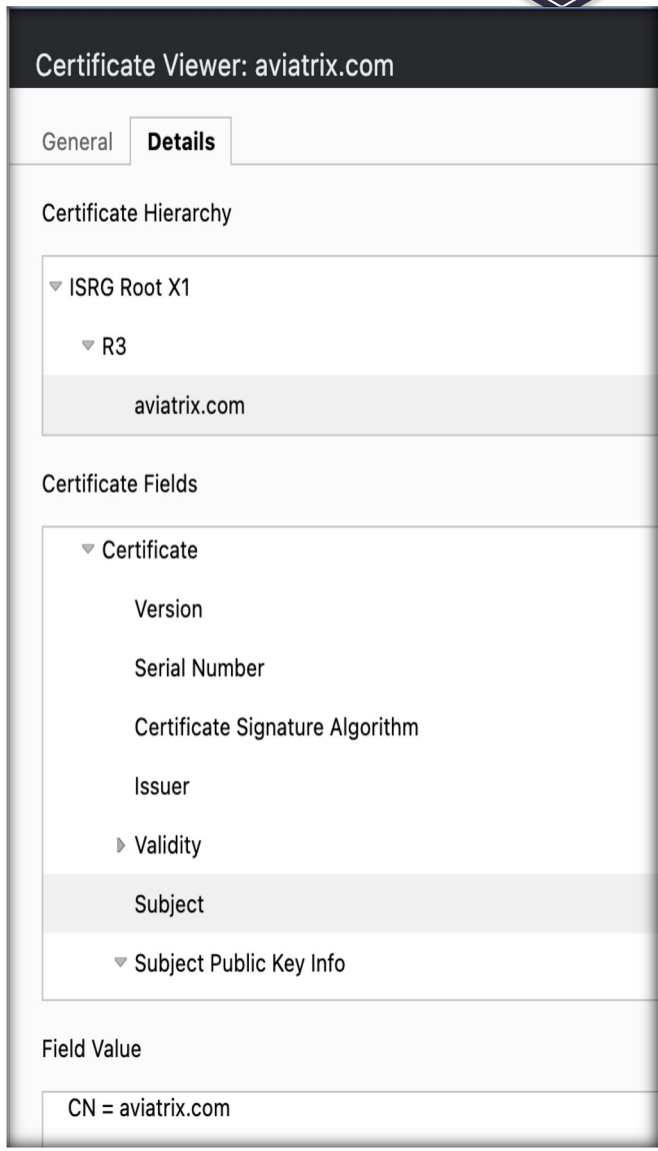
- Issuer
- Validity
- Subject

Trusted Root CA Bundle

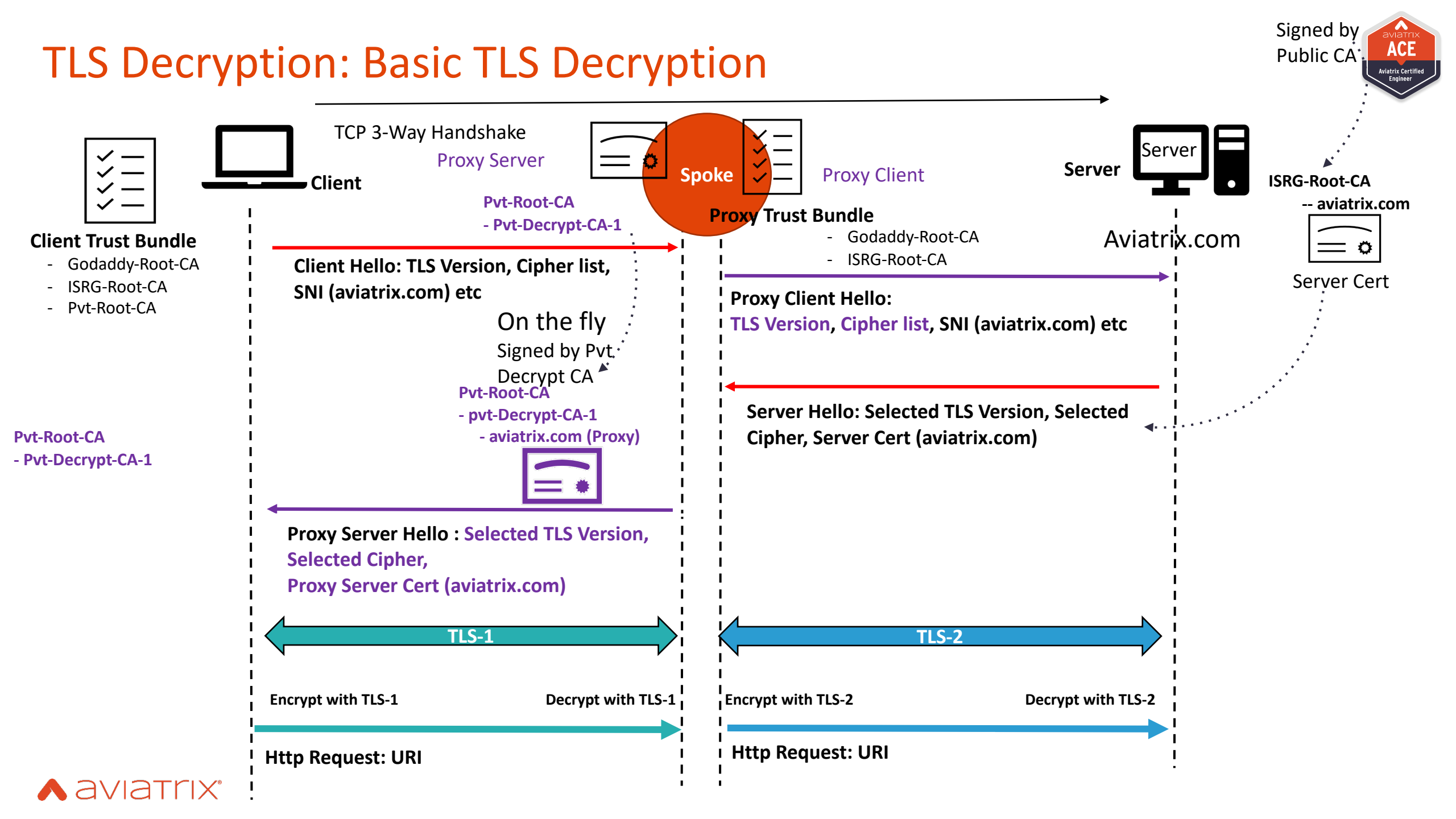
Used by the Client and/or Proxy Gateway to Identify/ Trust the Original Server Cert

Decryption CA Cert

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

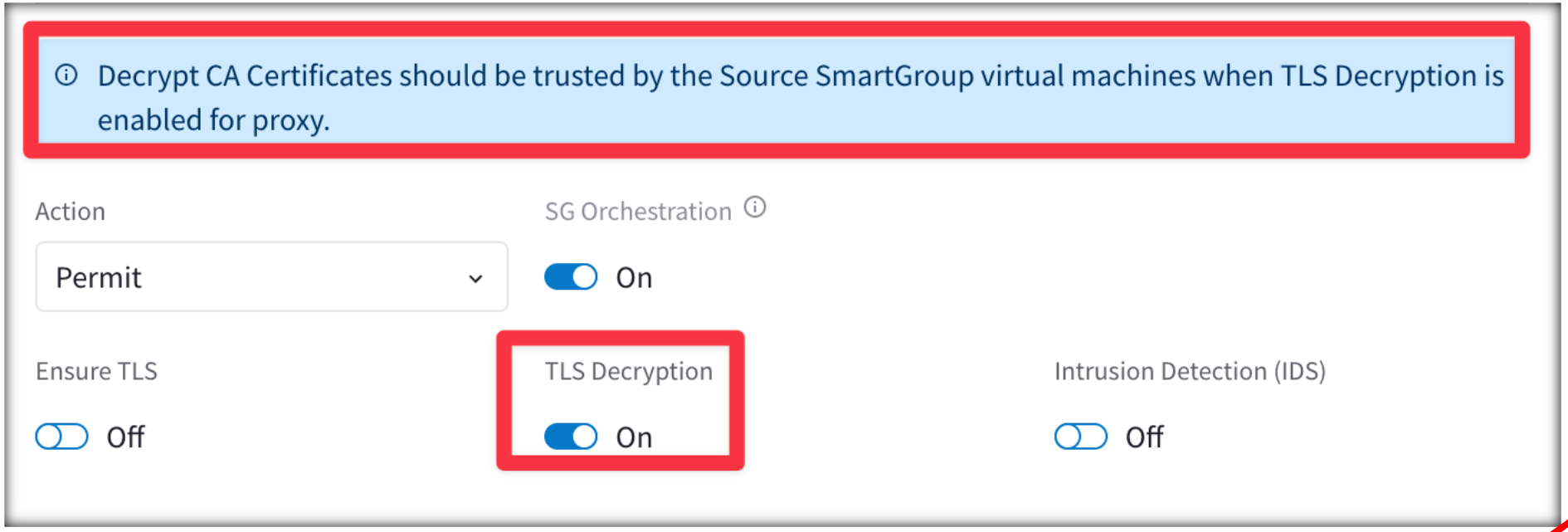


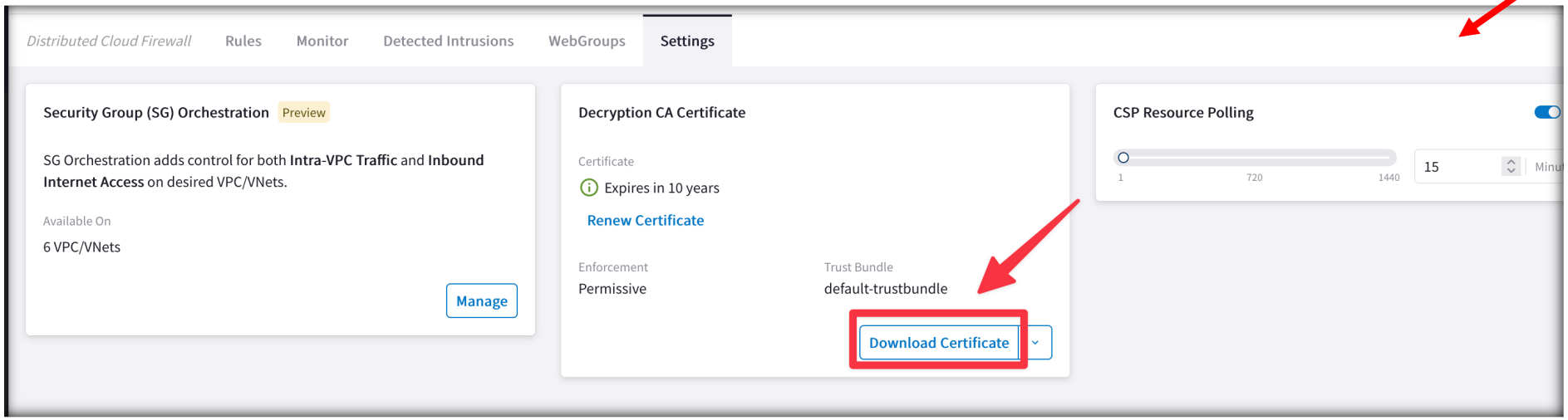
TLS Decryption: Basic TLS Decryption



aviatrix

TLS Decryption: Decryption CA Cert

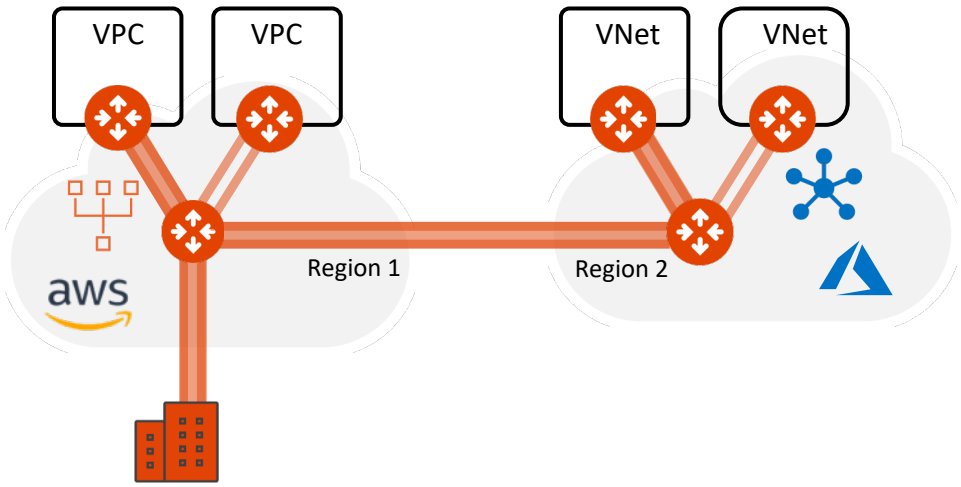


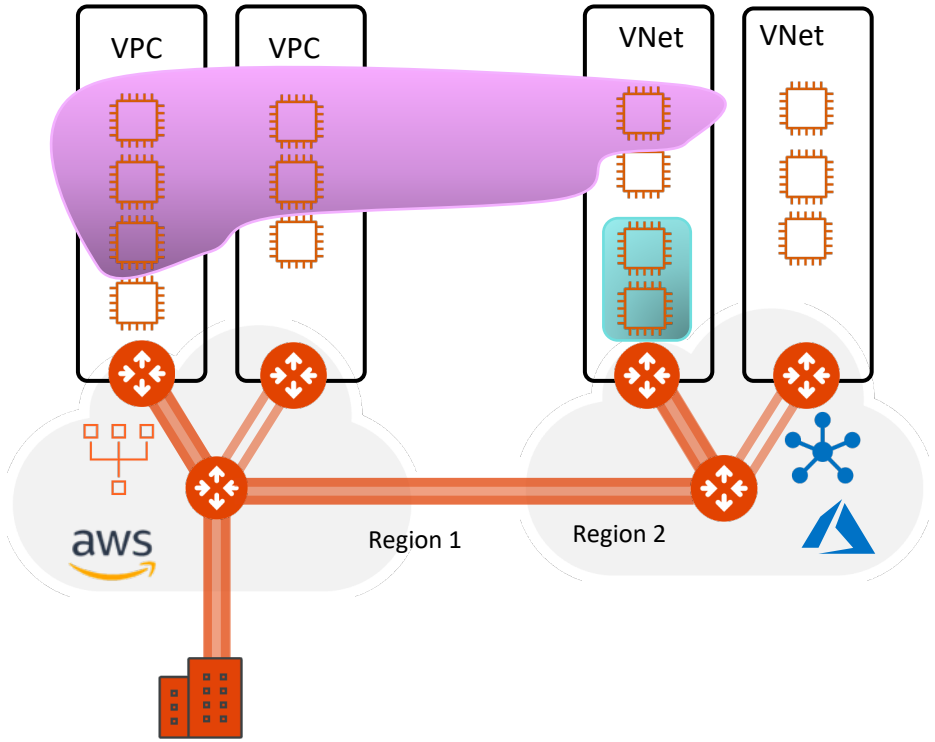


1. Download the Decryption CA Bundle.
2. Distribute the bundle across all the workloads.

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

Aviatrix DCF: Intra and Inter SmartGroups Rules





Smart Groups

Apache

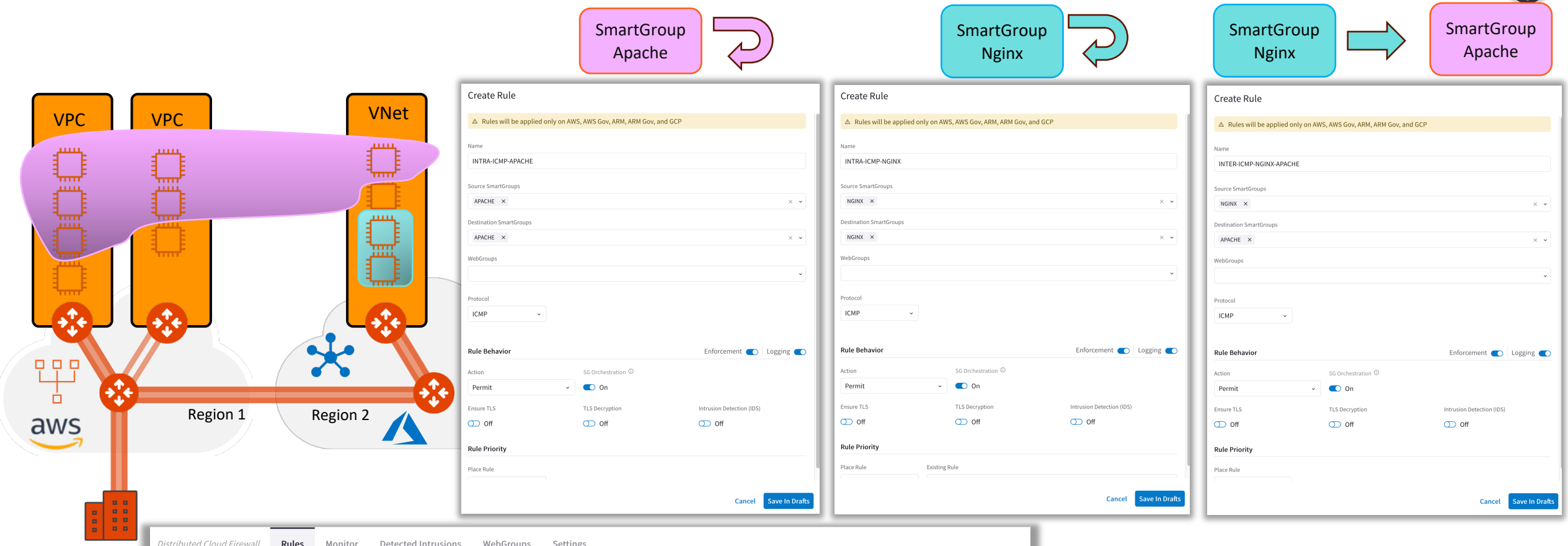
Nginx

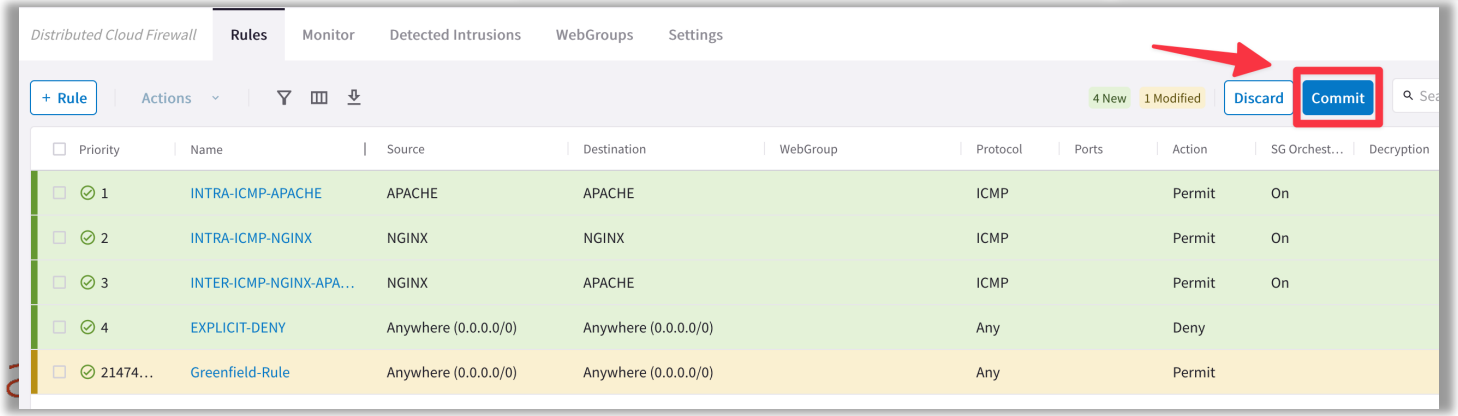
A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

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

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

Aviatrix DCF: Intra and inter SmartGroups Rules

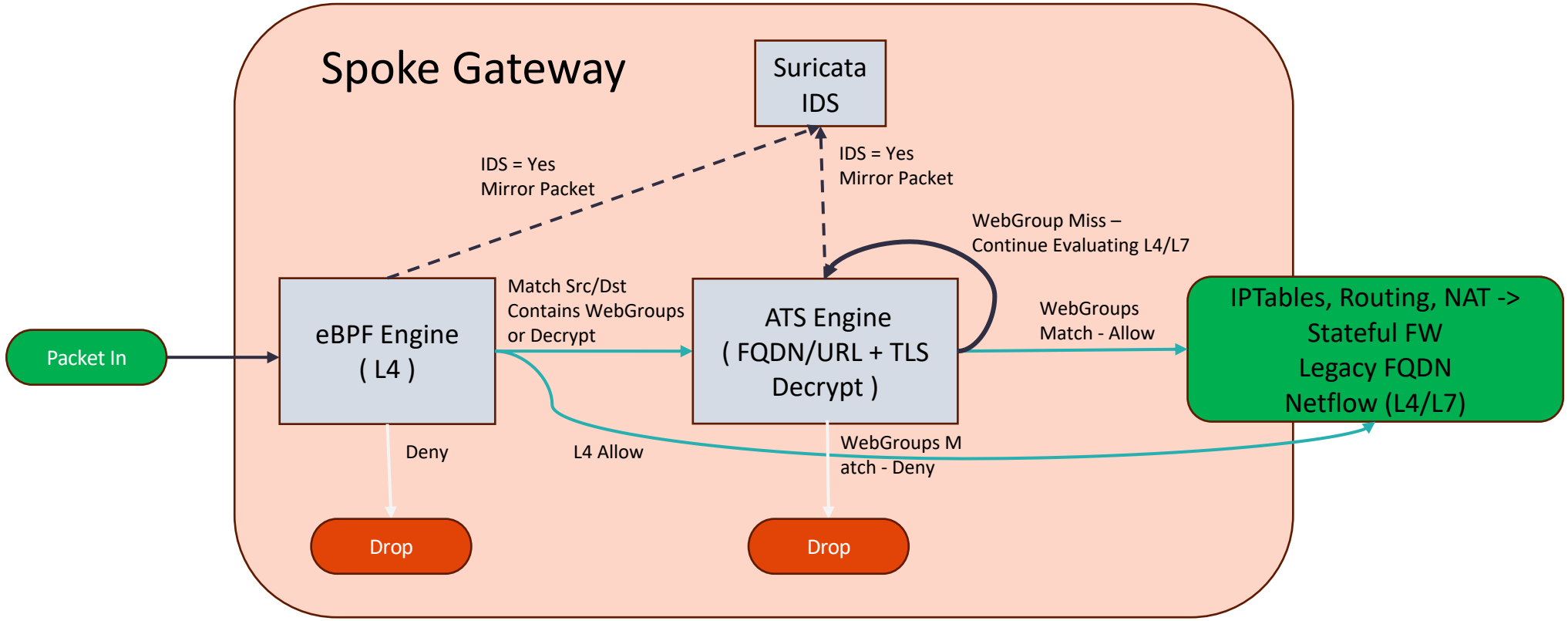




- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return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

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>)



Supported Capabilities

Capability	6.7	6.8	6.9	7.0	7.1
Distributed Cloud Firewall is supported in the following cloud providers:	AWS, Azure	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP
You can configure up to 500 SmartGroups	x	x	x	x	x
You can have up to 3000 CIDRs per SmartGroup	x	x	x	x	x
Number of rules per policy	64	2000	2000	2000	2000
Number of port ranges	1	64	64	64	64
Security Group Orchestration is supported				x (Azure)	x (AWS and Azure)

3rd Party Firewall Service Insertion (Aviatrix FireNet)

Centralized model

Use as necessary

Aviatrix FireNet For 3rd Party FW Service Insertion/Chaining

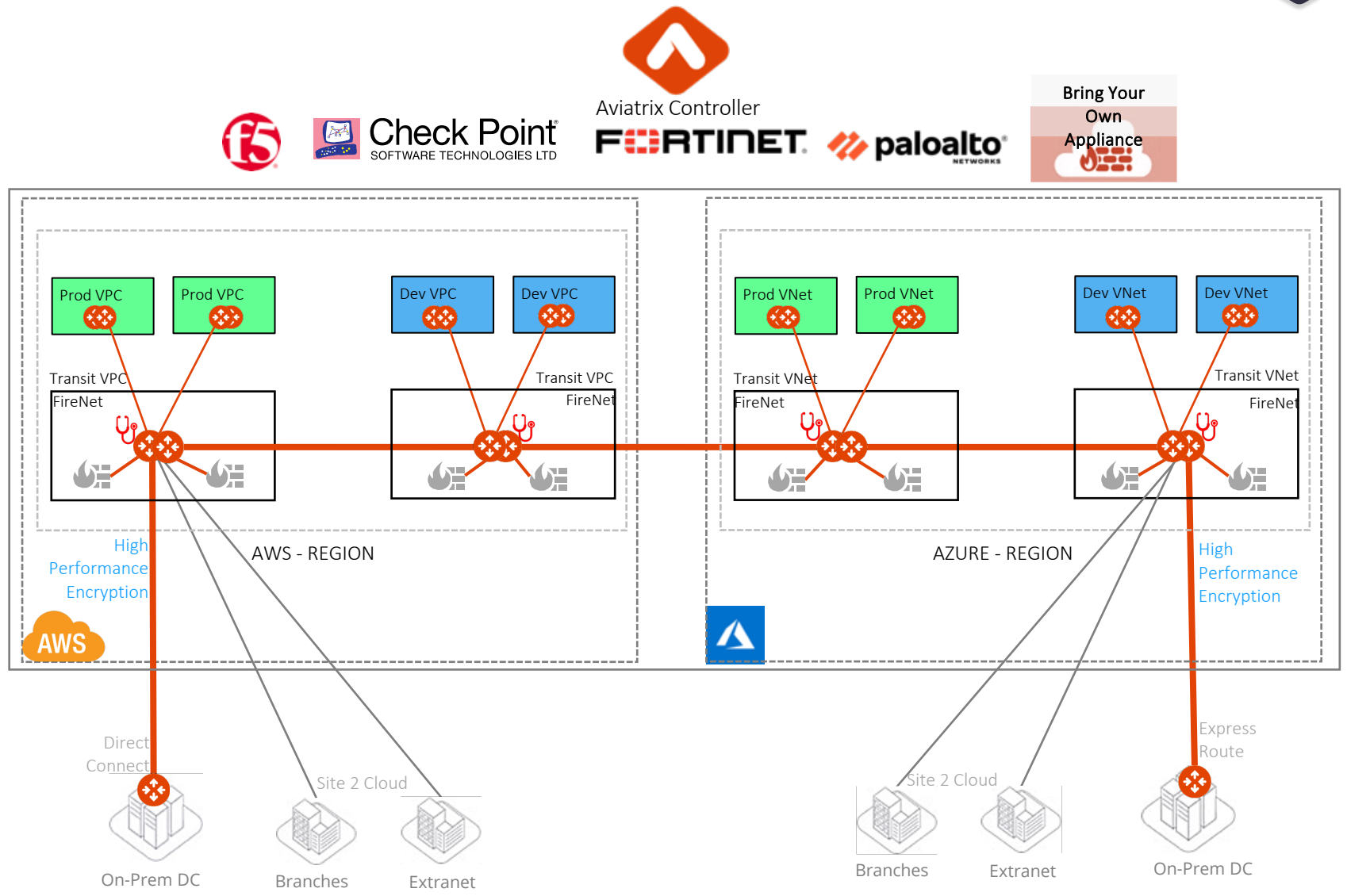
Firewall Service Insertion
- E-W / Egress / Ingress / all traffic
- High Performance Encryption (HPE)
- Active / Active – Across AZs
- No IPsec / No BGP / No SNAT required

Automated Control and Management
- Repeatable architecture across regions/clouds
- Centralized firewall deployment
- Vendor API integration
- UDR and VPC Route propagation

Improved Failure Detection and Failover
- Health Check monitoring

Forwarding Algorithm Options
- Intelligent traffic steering and firewalling based on traffic type
- 5-tuple and 2-tuple

Firewall Bootstrap Support
- Firewall zero-touch deployment capability in Azure and AWS



aviatrix

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com