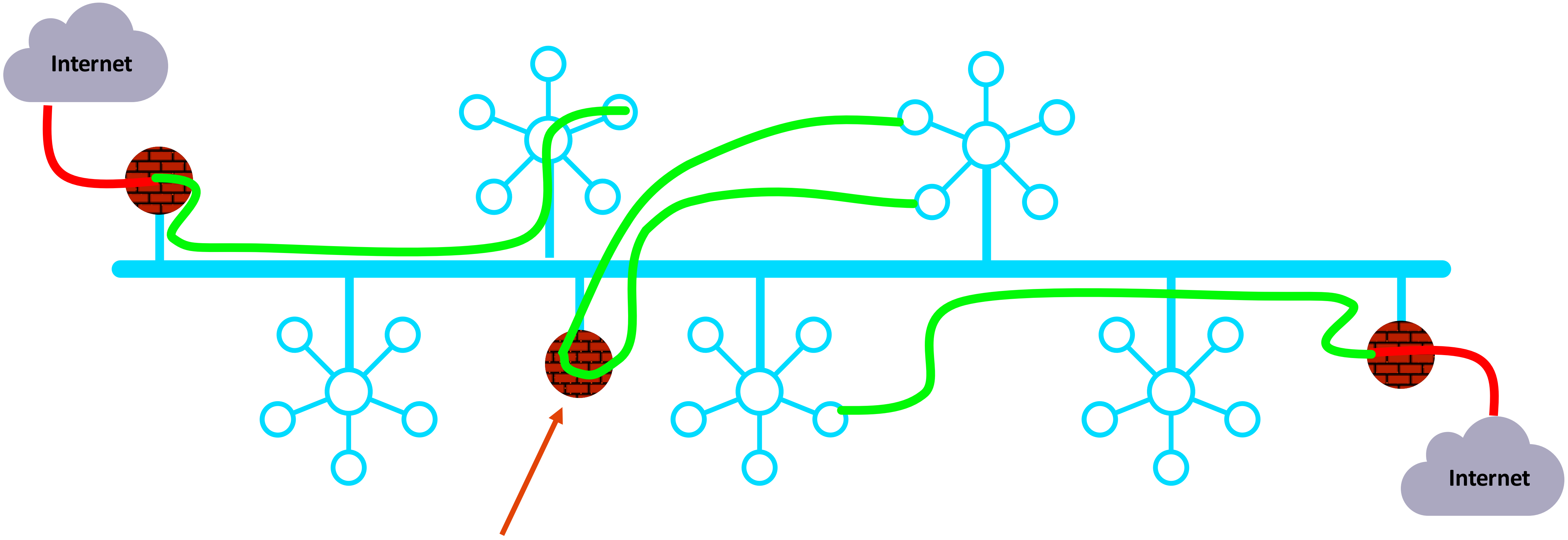
Distributed Cloud Firewall

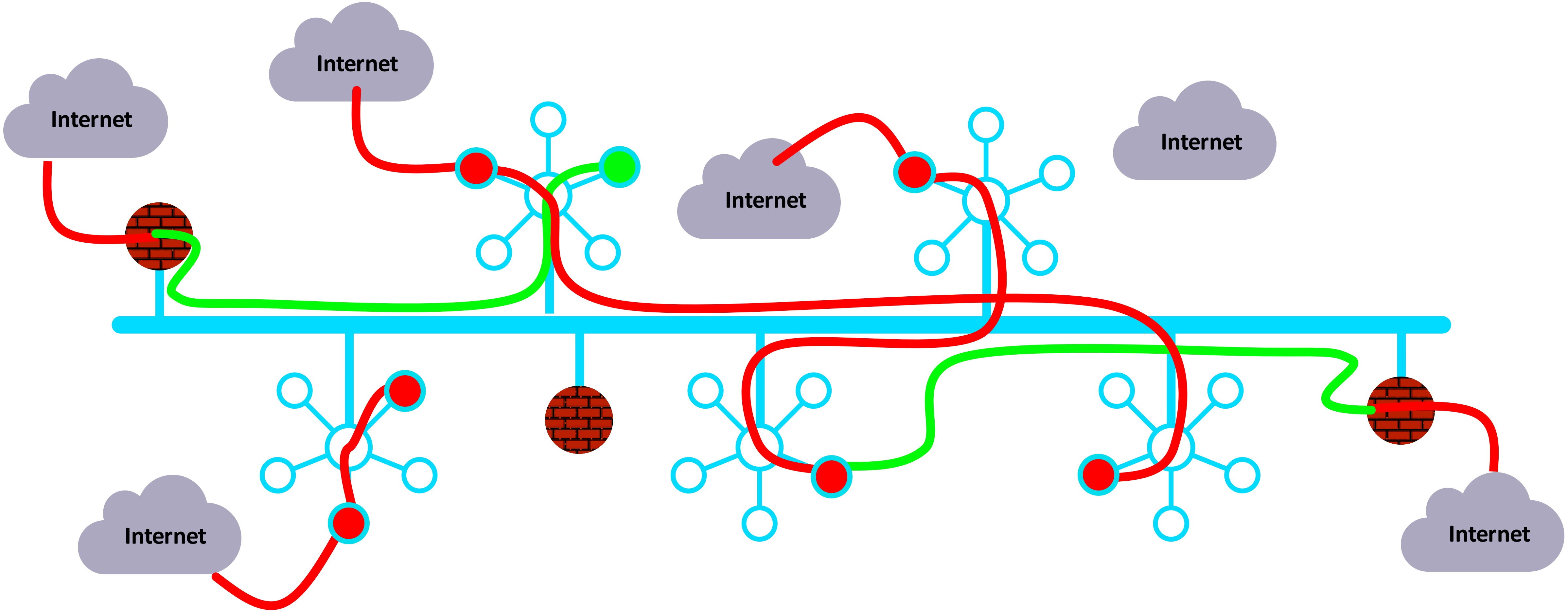
ACE Team

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



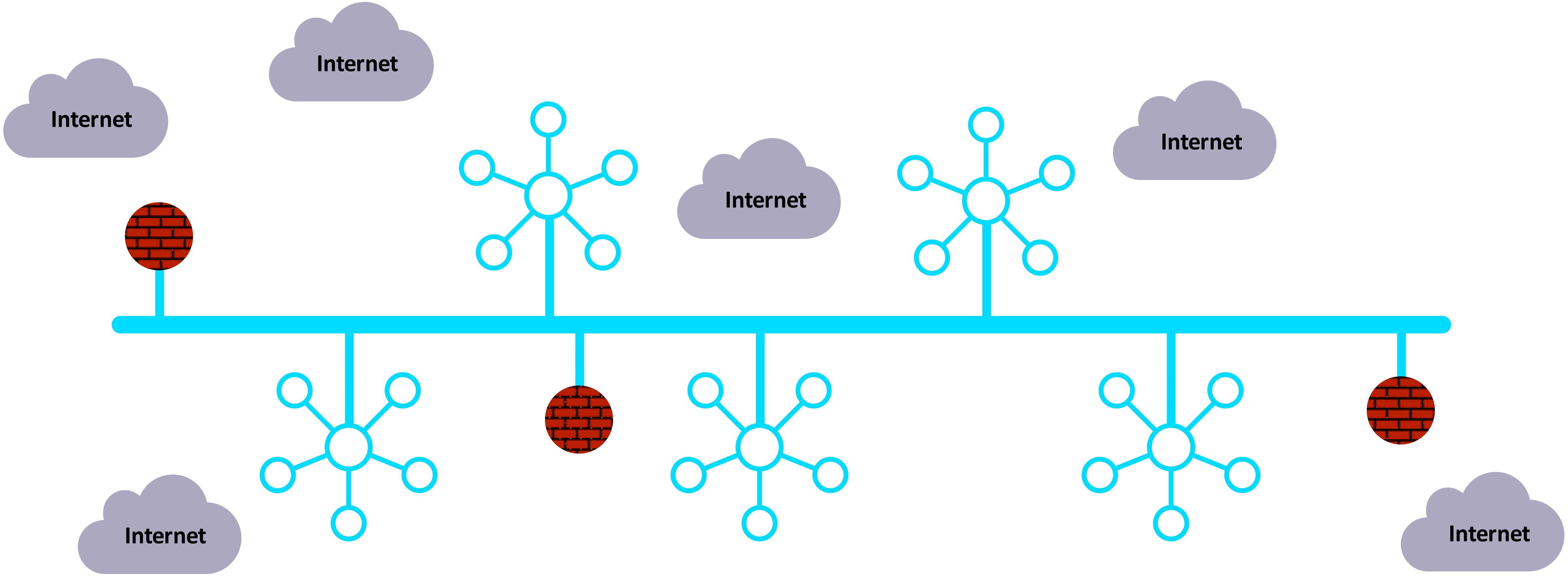
"Last Generation Firewalls"

In Reality…

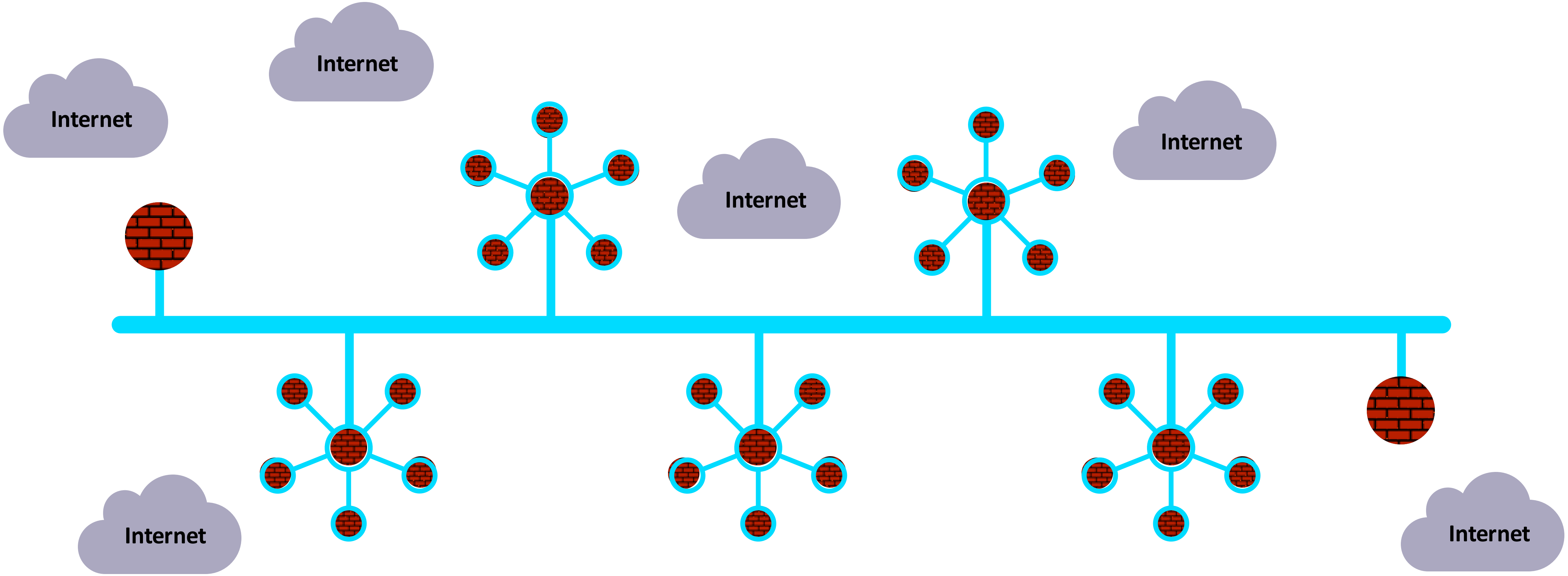


AVIATRIX

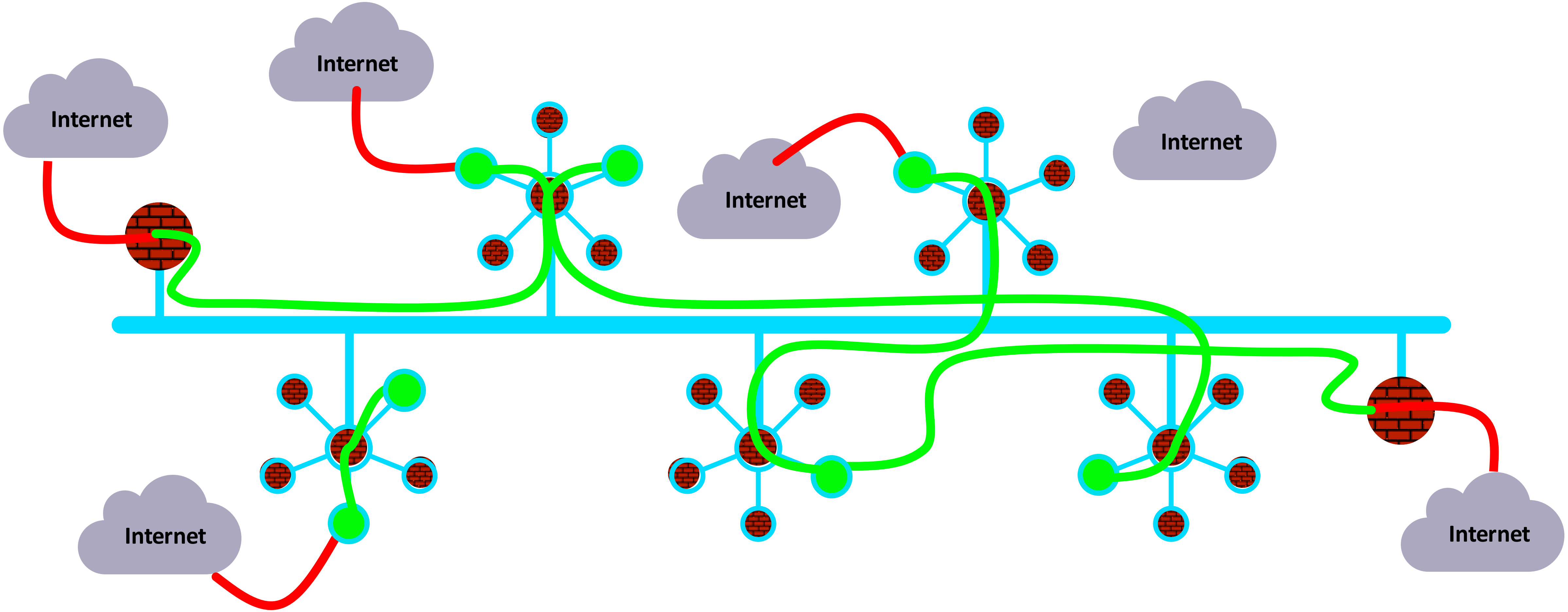
What If… the architecture was built for cloud



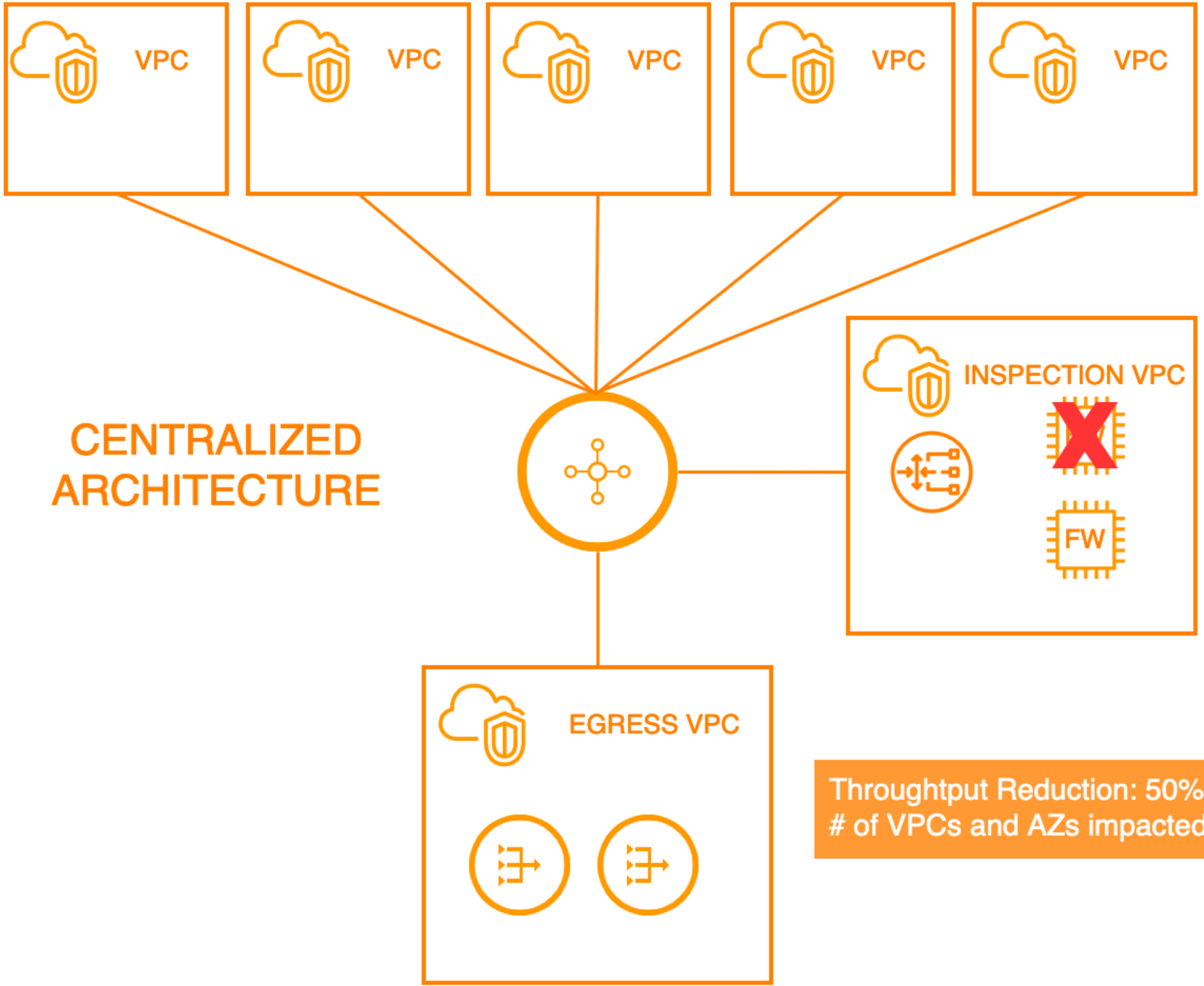
Firewalling Functions were Embedded in the Cloud Network Everywhere…



Distribution of the Security Services into the Spokes

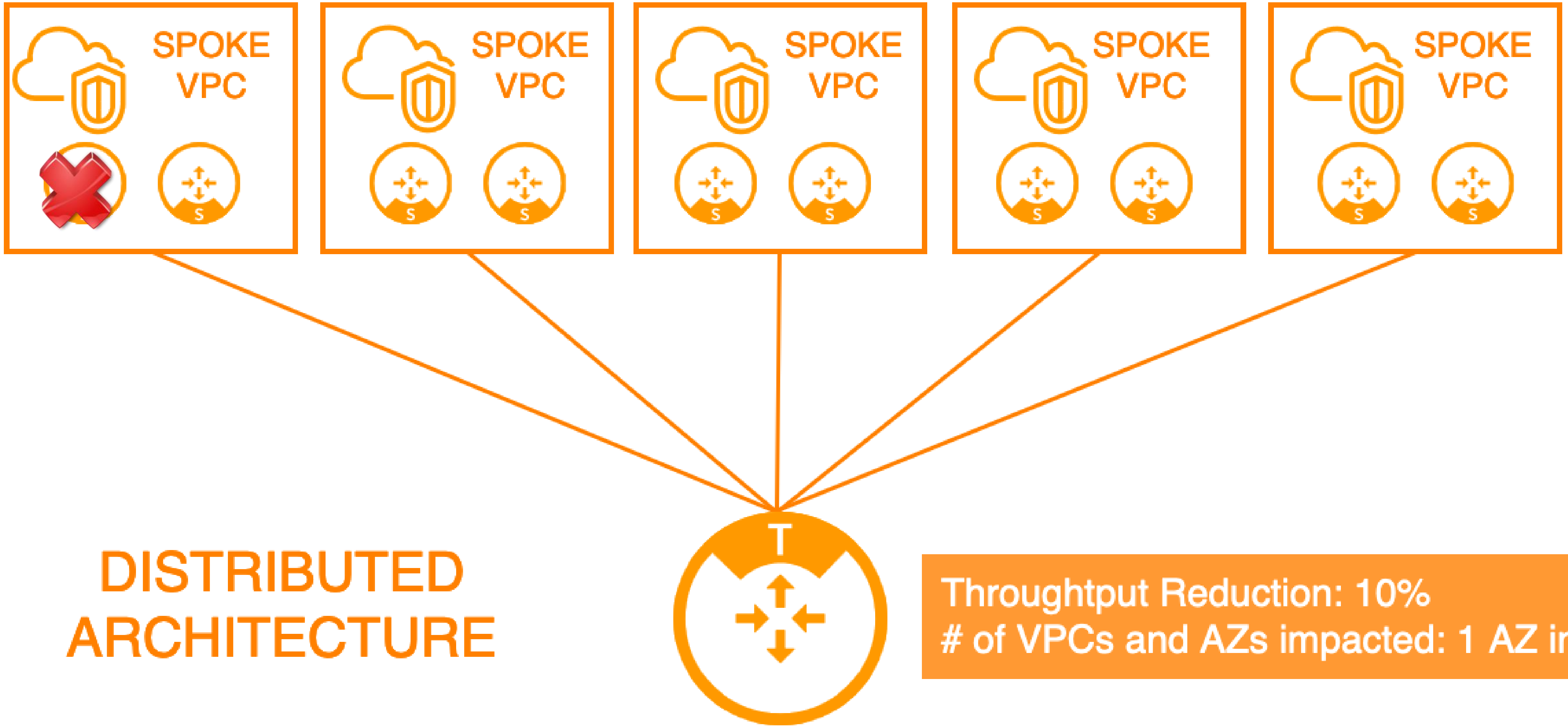


Impact of Failure – Centralized Architecture



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

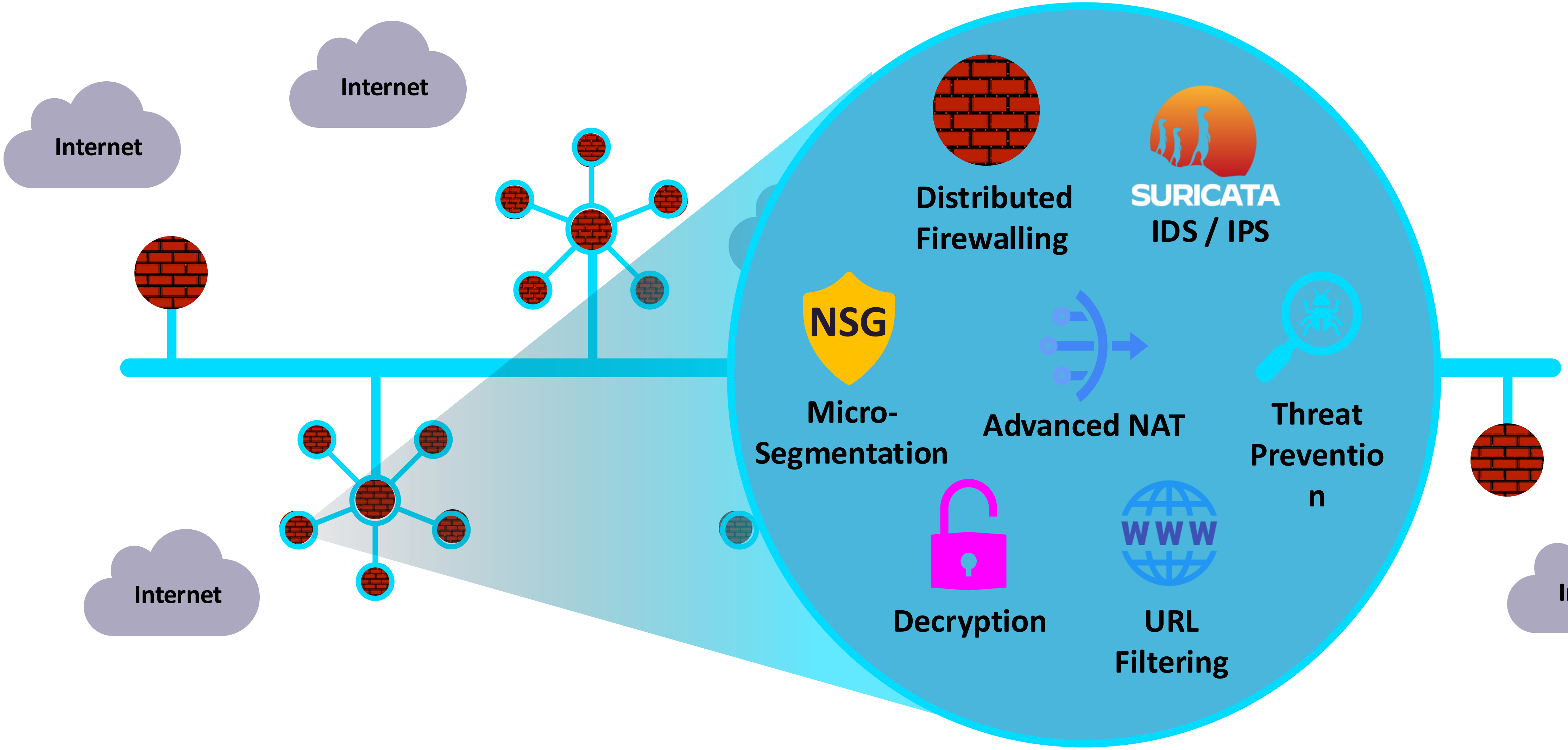
Impact of Failure – Distributed Architecture



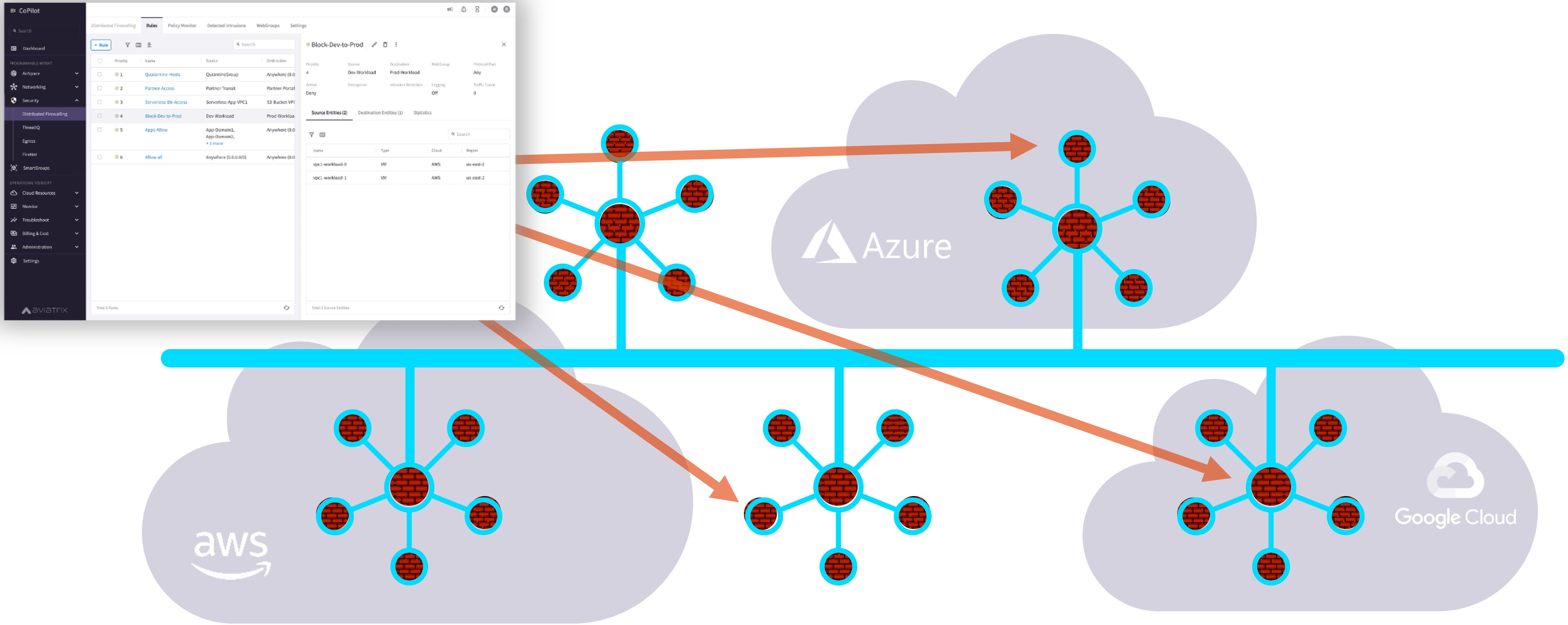
DISTRIBUTED ARCHITECTURE

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

And, What If it was more than just firewalling…



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



□	Priority	Name	Source	Destination
□	1	Quarantine-Hosts	QurantineGroup	Anywhere (0.0
□	2	Partner-Access	Partner-Transit	Partner-Portal
□	3	Serverless-Db-Access	Serverless-App-VPC1	S3-Bucket-VP
□	4	Block-Dev-to-Prod	Dev-Workload	Prod-Workloa
□	5	Apps-Allow	App-Domain1, App-Domain2, + 1 more	Anywhere (0.0
□	6	Allow-all	Anywhere (0.0.0.0/0)	Anywhere (0.0

Total 6 Rules

Block-Dev-to-Prod

Priority	Source	Destination	WebGroup	Protocol Port
4	Dev-Workload	Prod-Workload		Any

Action	Decryption	Intrusion Detection	Logging	Traffic Count
Deny			Off	0

Source Entities (2) | Destination Entities (1) | Statistics

Name	Type	Cloud	Region
vpc1-workload-0	VM	AWS	us-east-2
vpc1-workload-1	VM	AWS	us-east-2

Total 2 Source Entities

Where and How Policies Are Enforced Is Abstracted…

SmartGroups: Definition

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

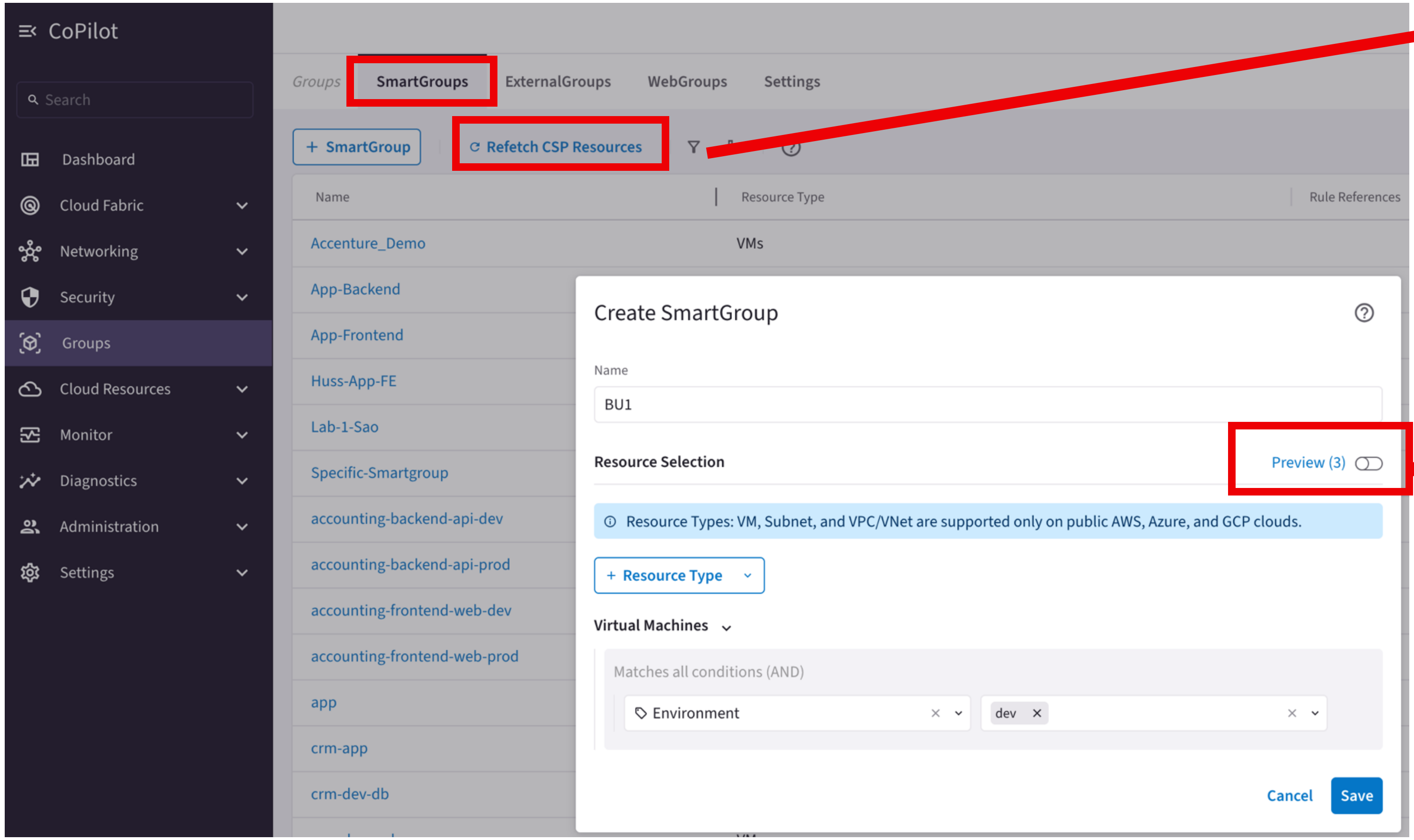
- **What is a SmartGroup?**

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



Name	Resource Type	Rule References
Accenture_Demo	VMs	
App-Backend		
App-Frontend		
Huss-App-FE		
Lab-1-Sao		
Specific-Smartgroup		
accounting-backend-api-dev		
accounting-backend-api-prod		
accounting-frontend-web-dev		
accounting-frontend-web-prod		
app		
crm-app		
crm-dev-db		

Create SmartGroup

Name: BU1

Resource Selection — Preview (3)

Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.

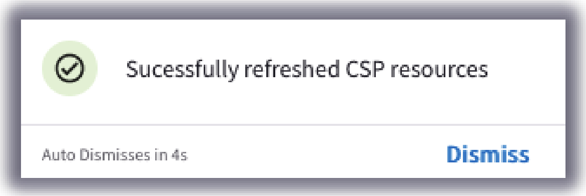
+ Resource Type

Virtual Machines

Matches all conditions (AND)

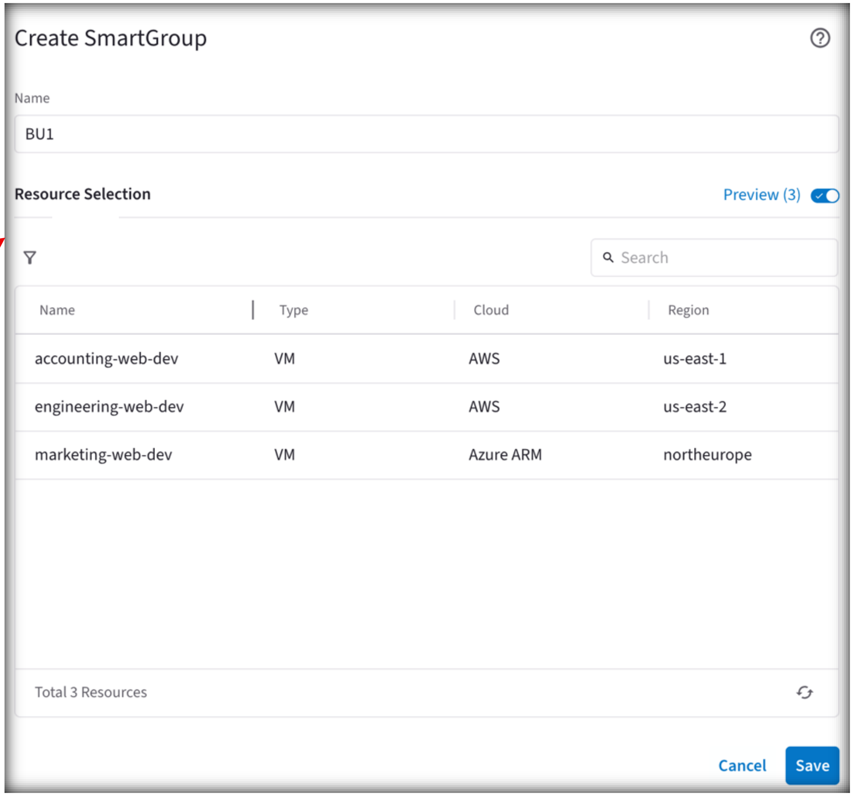
Environment — dev

Cancel Save



Sucessfully refreshed CSP resources

Auto Dismisses in 4s — Dismiss



Create SmartGroup

Name: BU1

Resource Selection — Preview (3)

Search

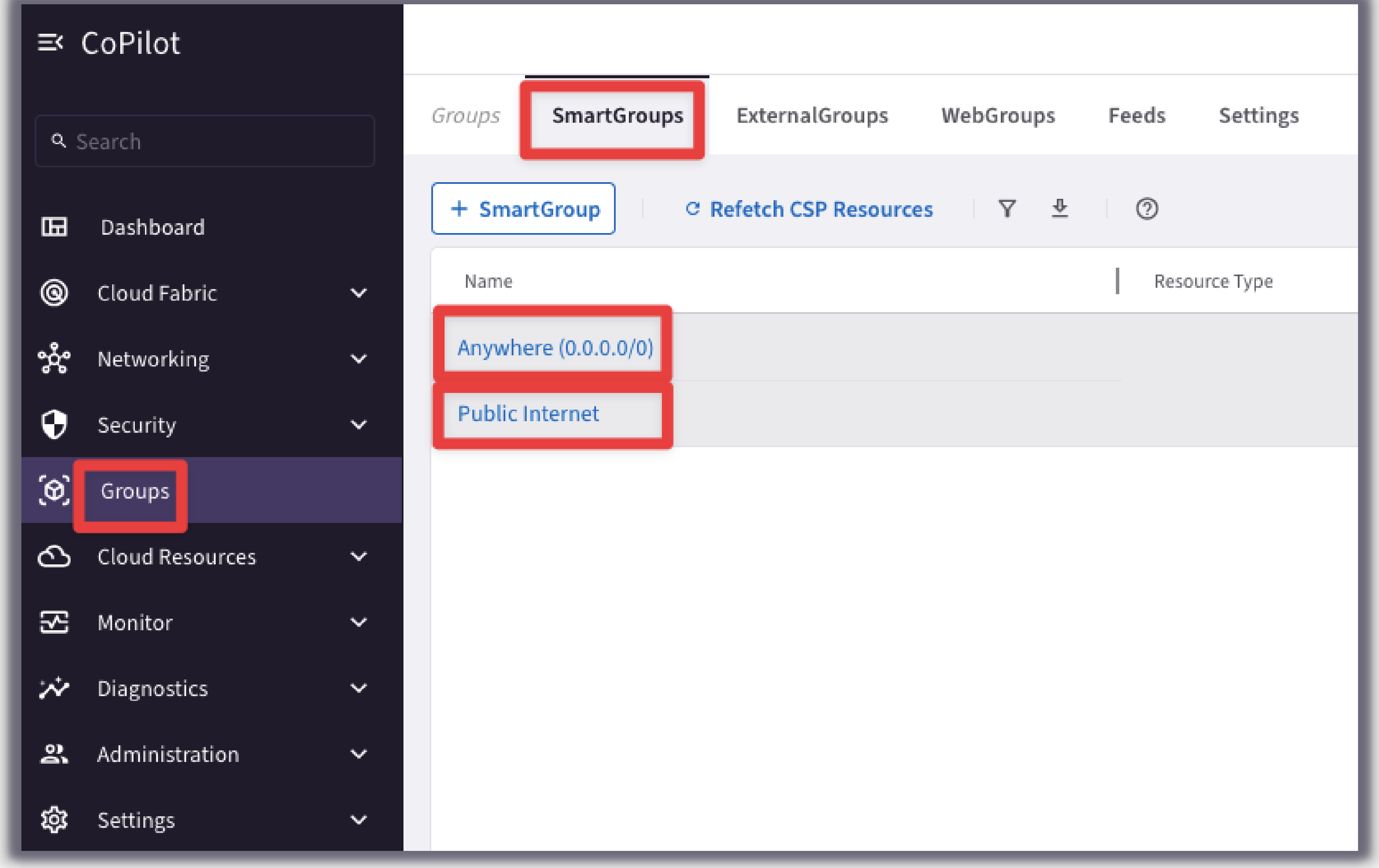
Name	Type	Cloud	Region
accounting-web-dev	VM	AWS	us-east-1
engineering-web-dev	VM	AWS	us-east-2
marketing-web-dev	VM	Azure ARM	northeurope

Total 3 Resources

Cancel Save

- 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

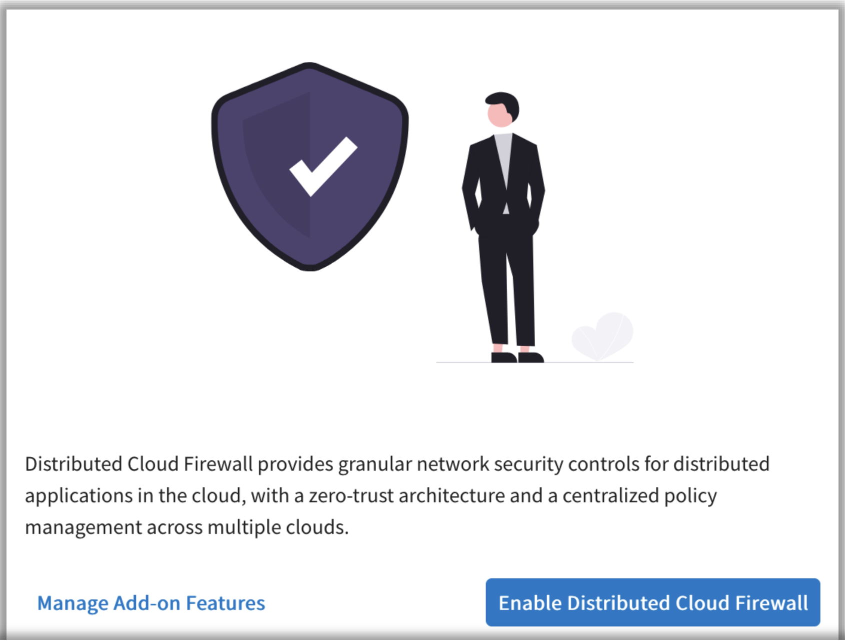


Anywhere (0.0.0.0/0)

Public Internet

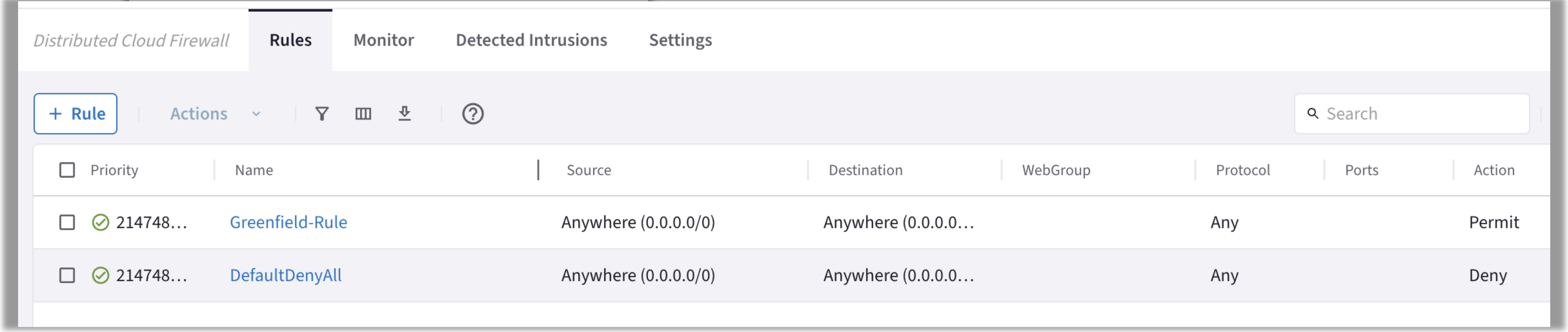
- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

Enabling Distributed Cloud Firewall



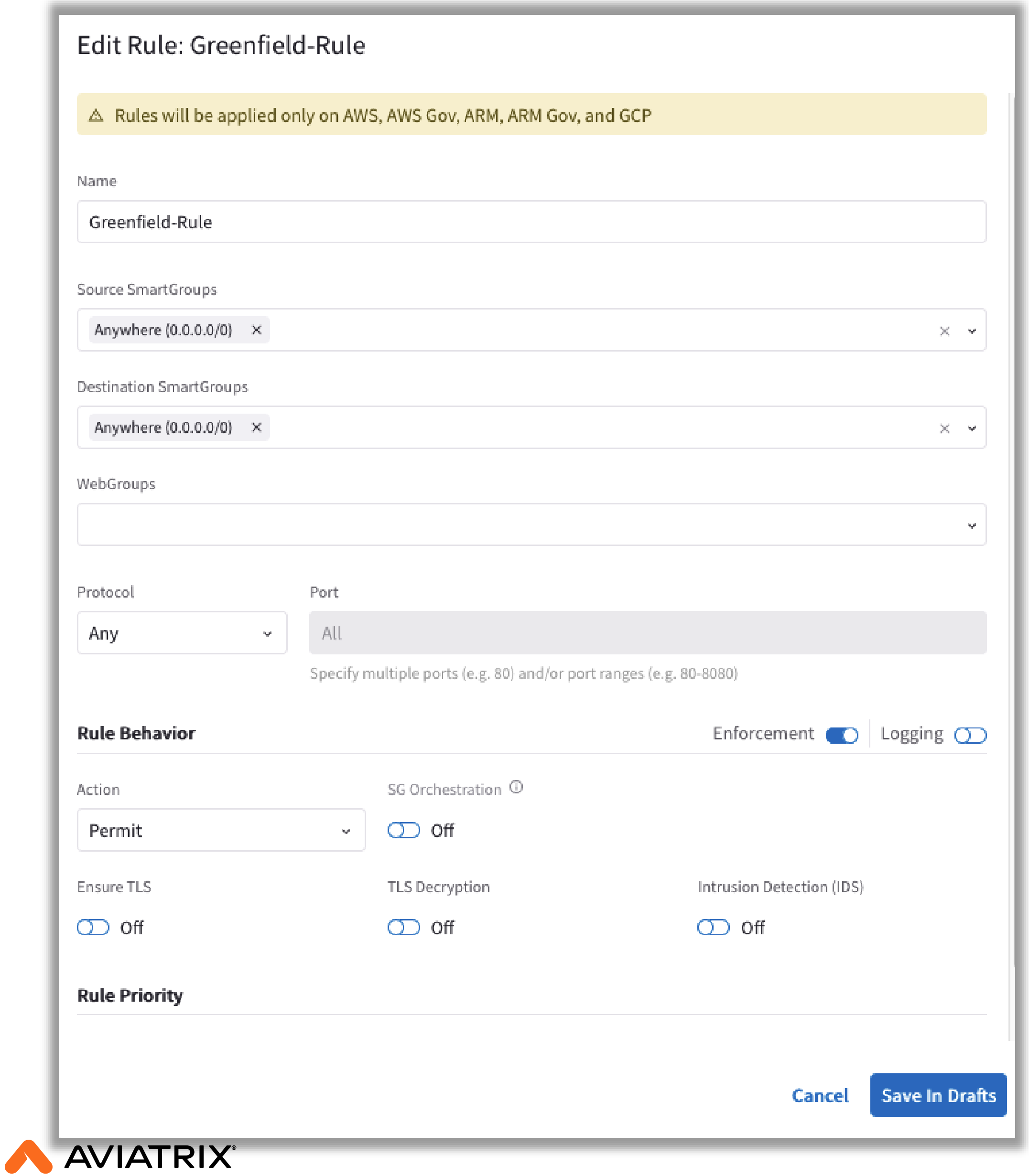
Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

- 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.



□	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



Edit Rule: Greenfield-Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: Greenfield-Rule

Source SmartGroups: Anywhere (0.0.0.0/0)

Destination SmartGroups: Anywhere (0.0.0.0/0)

WebGroups:

Protocol: Any

Port: All

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement: On

Logging: Off

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

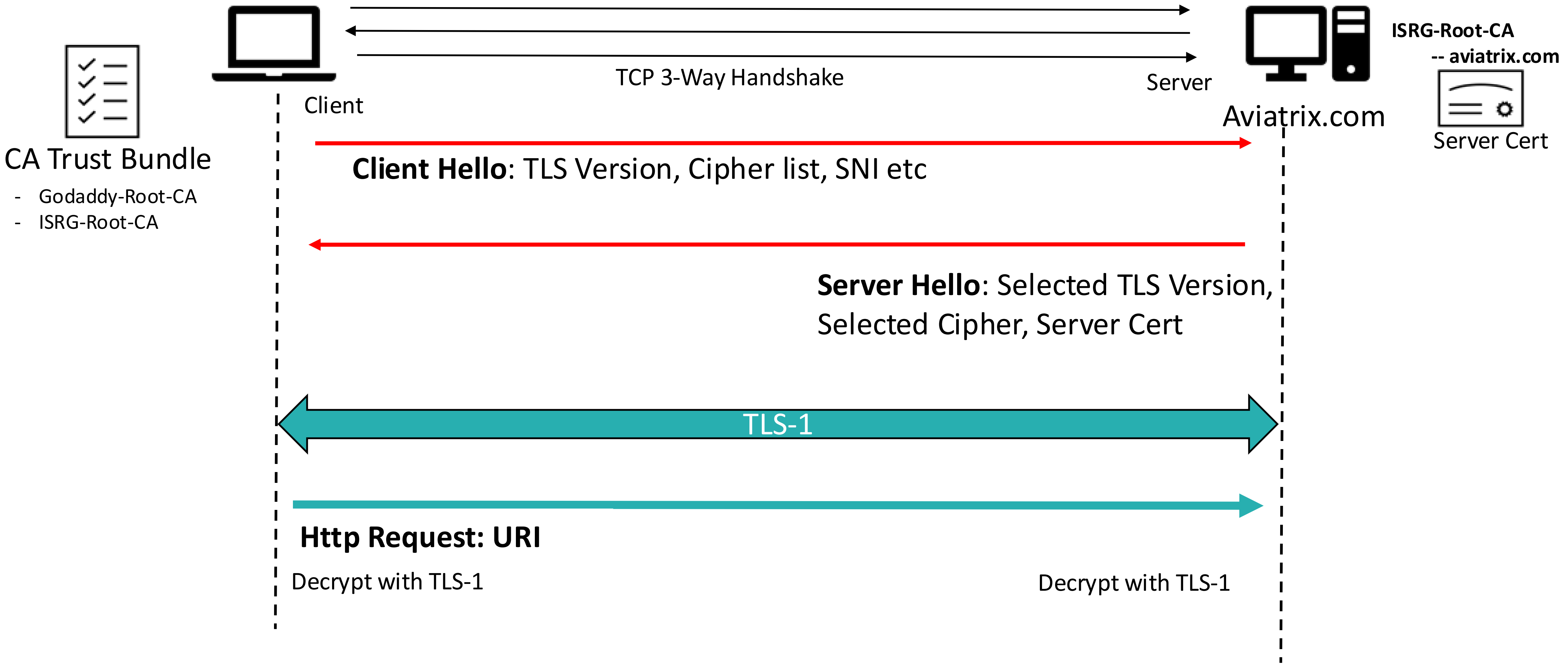
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

- **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



CA Trust Bundle

- Godaddy-Root-CA
- ISRG-Root-CA

Client

TCP 3-Way Handshake

Server

Aviatrix.com

ISRG-Root-CA
-- aviatrix.com

Server Cert

Client Hello: TLS Version, Cipher list, SNI etc

Server Hello: Selected TLS Version, Selected Cipher, Server Cert

TLS-1

Http Request: URI

Decrypt with TLS-1

Decrypt with TLS-1

TLS Decryption: PKI/ KMS and Trust Bundle

Certificate Hierarchy

- Root
  - Intermediate
    - Server Cert (Leaf Cert)

Certificate Fields

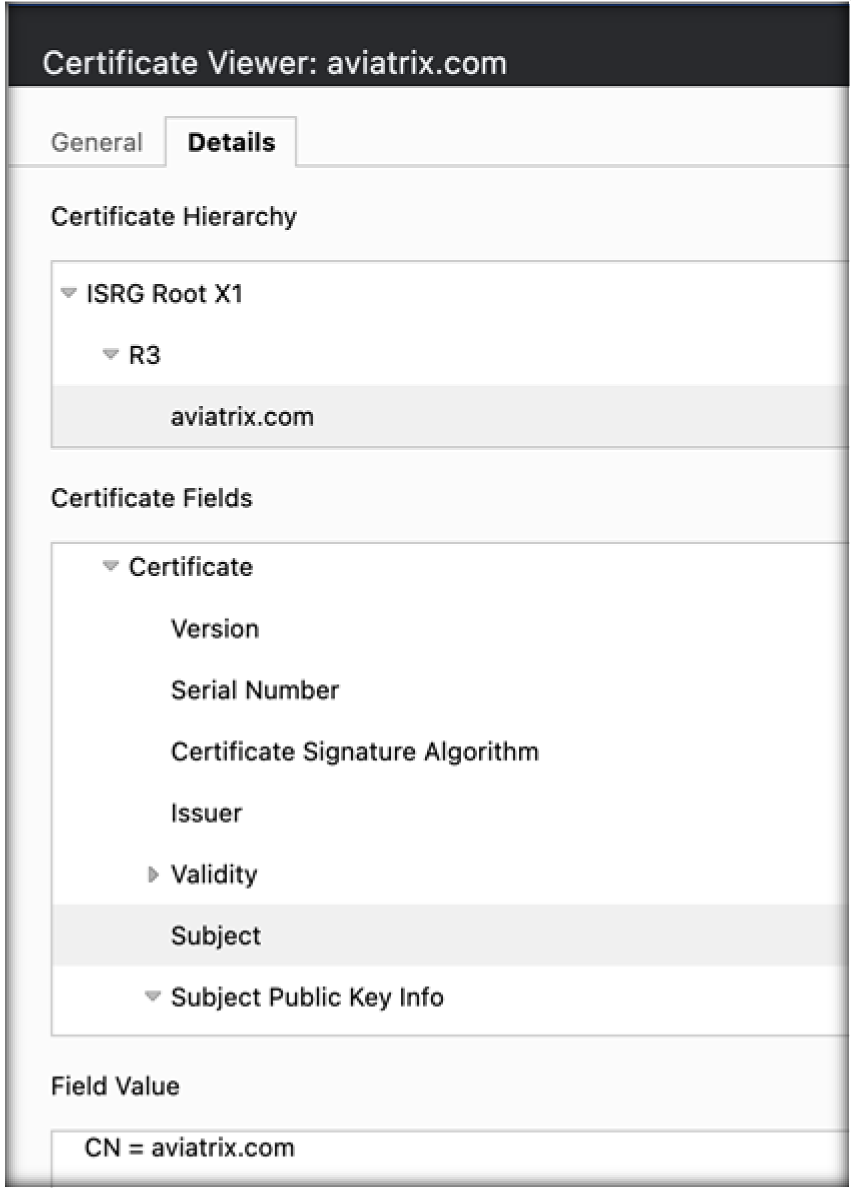
- Issuer
- Validity
- Subject

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



Certificate Viewer: aviatrix.com

General | **Details**

Certificate Hierarchy

- ISRG Root X1
  - R3
    - aviatrix.com

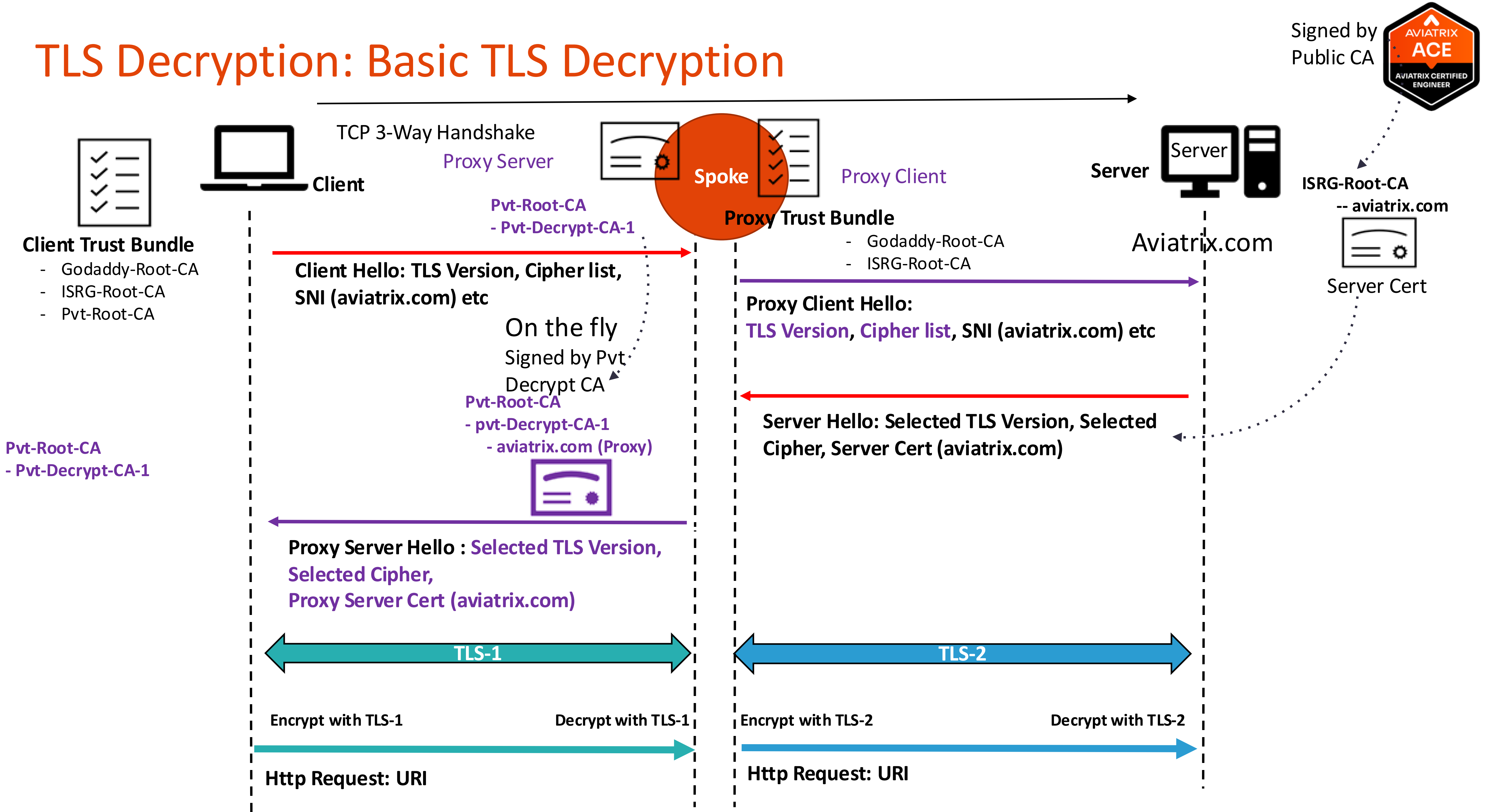
Certificate Fields

- Certificate
  - Version
  - Serial Number
  - Certificate Signature Algorithm
  - Issuer
  - Validity
  - Subject
  - Subject Public Key Info

Field Value

CN = aviatrix.com

TLS Decryption: Basic TLS Decryption



Signed by Public CA

TCP 3-Way Handshake

Client

Proxy Server

Spoke

Proxy Client

Server

Server

Client Trust Bundle
- Godaddy-Root-CA
- ISRG-Root-CA
- Pvt-Root-CA

Pvt-Root-CA
- Pvt-Decrypt-CA-1

Proxy Trust Bundle
- Godaddy-Root-CA
- ISRG-Root-CA

Aviatrix.com

ISRG-Root-CA
-- aviatrix.com

Server Cert

Client Hello: TLS Version, Cipher list, SNI (aviatrix.com) etc

Proxy Client Hello: TLS Version, Cipher list, SNI (aviatrix.com) etc

On the fly Signed by Pvt Decrypt CA

Pvt-Root-CA
- pvt-Decrypt-CA-1
- aviatrix.com (Proxy)

Server Hello: Selected TLS Version, Selected Cipher, Server Cert (aviatrix.com)

Pvt-Root-CA
- Pvt-Decrypt-CA-1

Proxy Server Hello : Selected TLS Version, Selected Cipher, Proxy Server Cert (aviatrix.com)

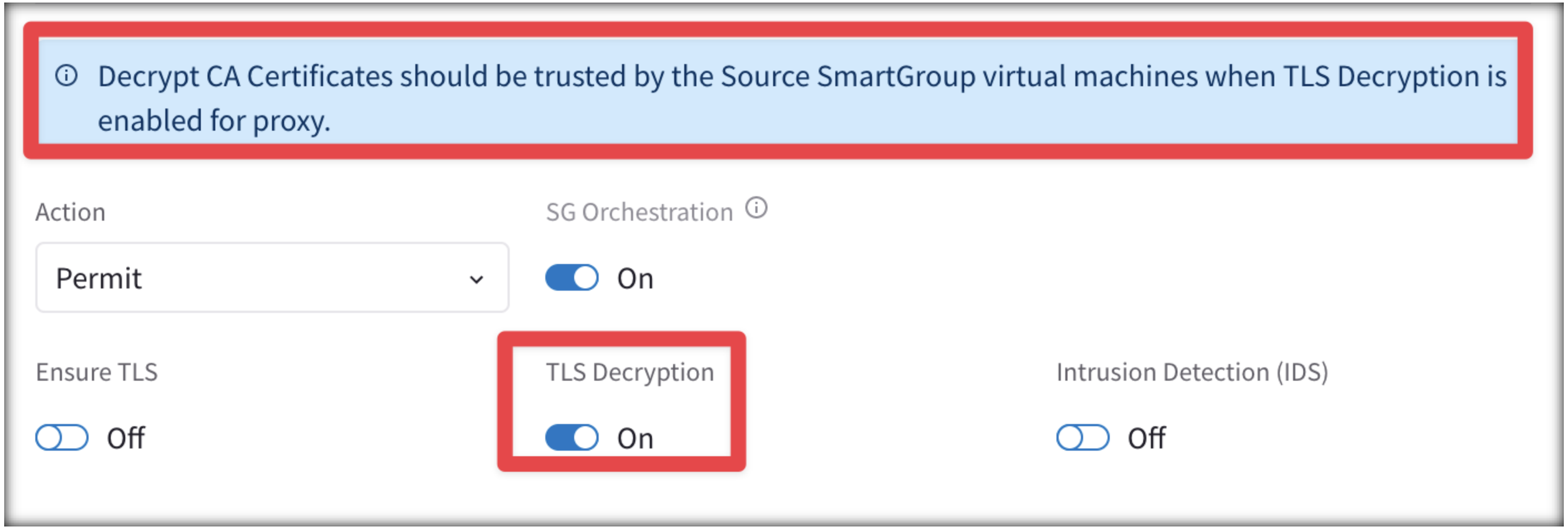
Encrypt with TLS-1 **Decrypt with TLS-1**

Encrypt with TLS-2 **Decrypt with TLS-2**

Http Request: URI

Http Request: URI

TLS Decryption: Decryption CA Cert



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

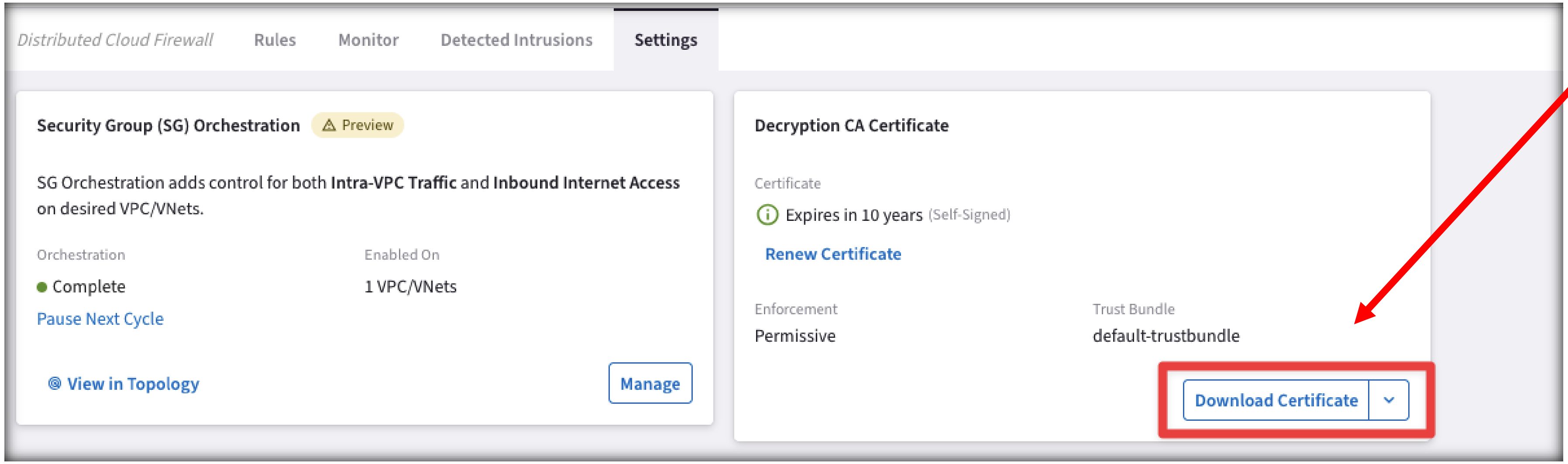
Action: Permit

SG Orchestration ⓘ: On

Ensure TLS: Off

TLS Decryption: On

Intrusion Detection (IDS): Off



Security Group (SG) Orchestration ⚠ Preview

SG Orchestration adds control for both **Intra-VPC Traffic** and **Inbound Internet Access** on desired VPC/VNets.

Orchestration	Enabled On
● Complete	1 VPC/VNets

Decryption CA Certificate

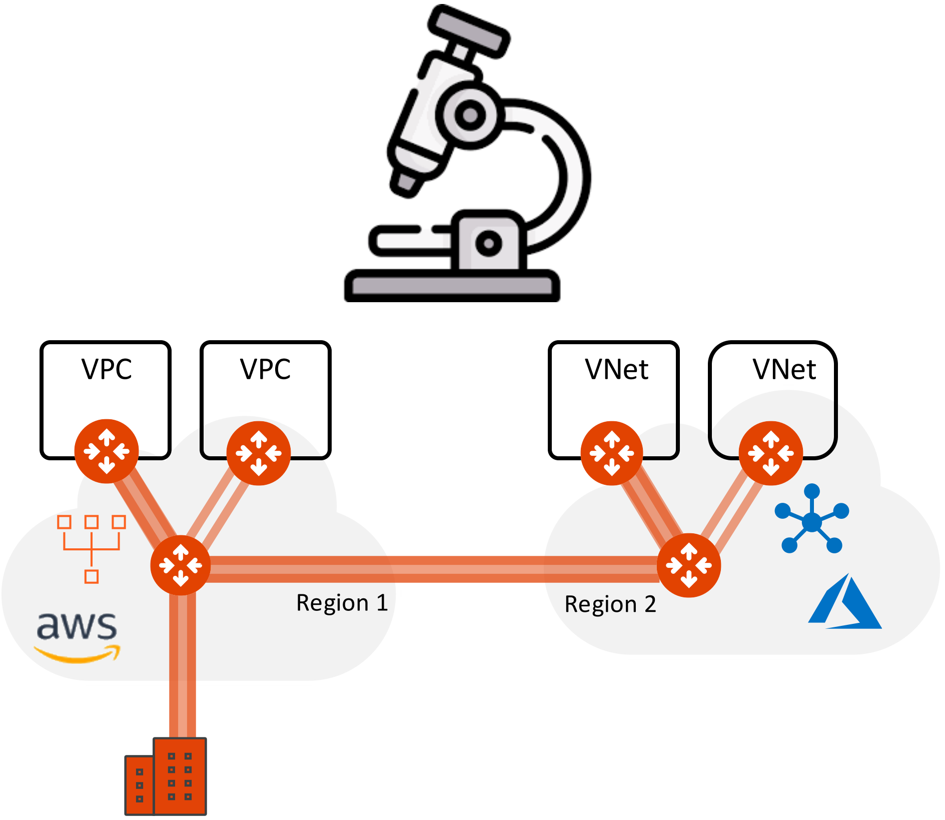
Certificate: ⓘ Expires in 10 years (Self-Signed)

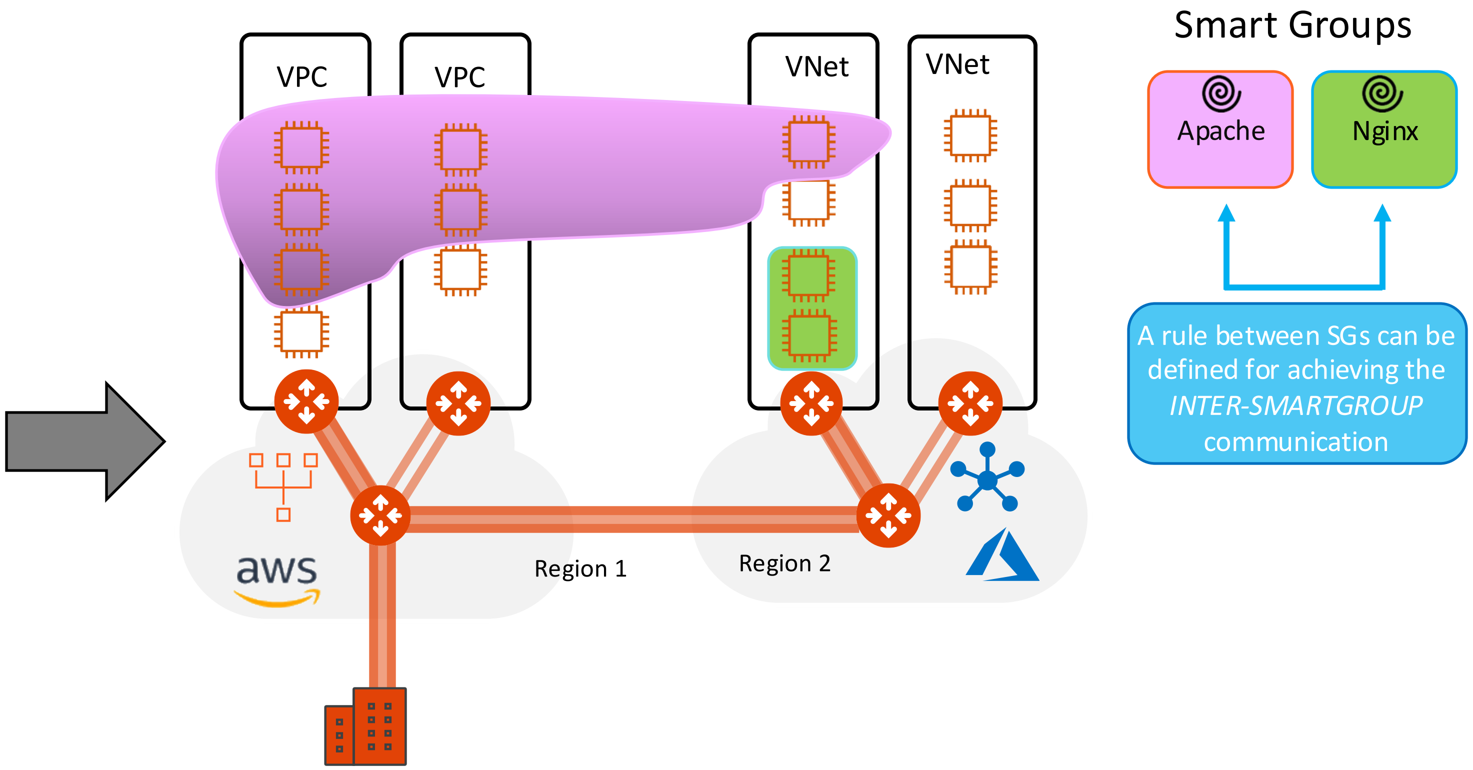
Enforcement	Trust Bundle
Permissive	default-trustbundle

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



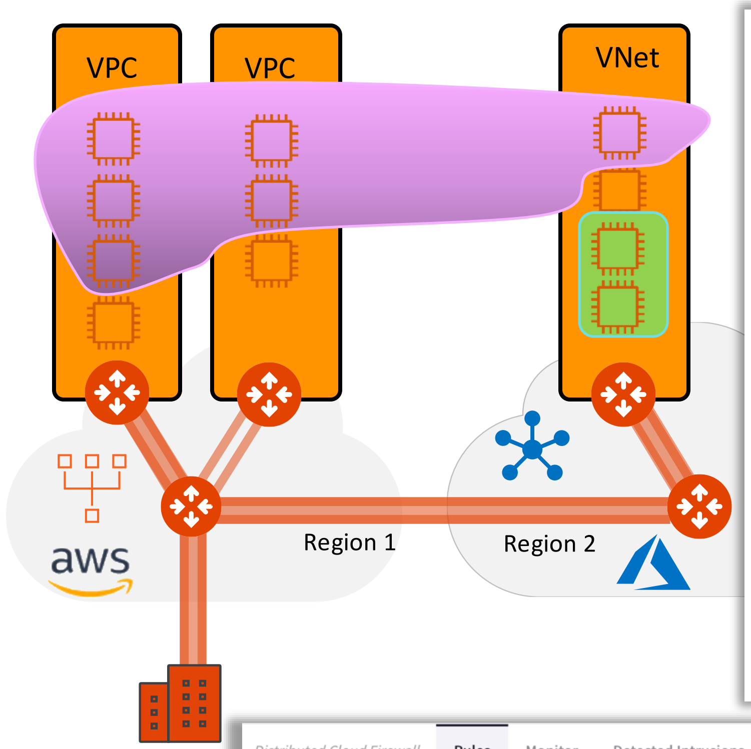


A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

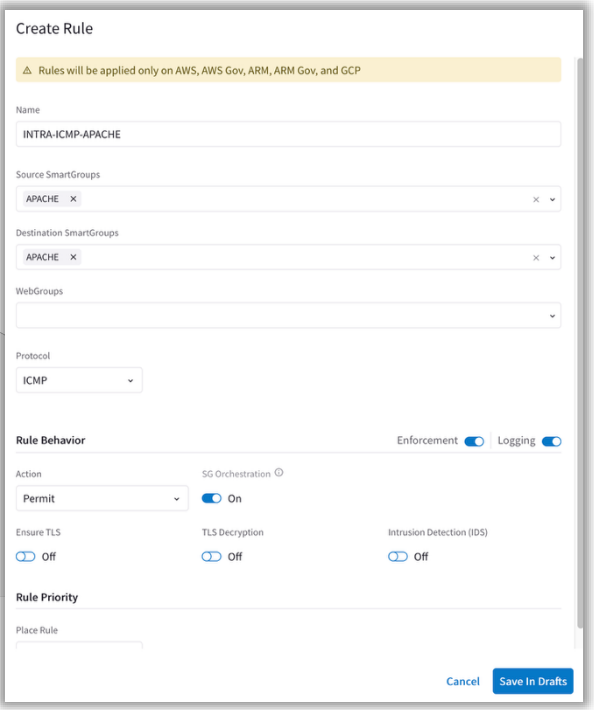
- **INTRA-RULE**: is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

- **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



SmartGroup Apache – intra



Create Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: INTRA-ICMP-APACHE

Source SmartGroups: APACHE ×

Destination SmartGroups: APACHE ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement ● | Logging ●

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

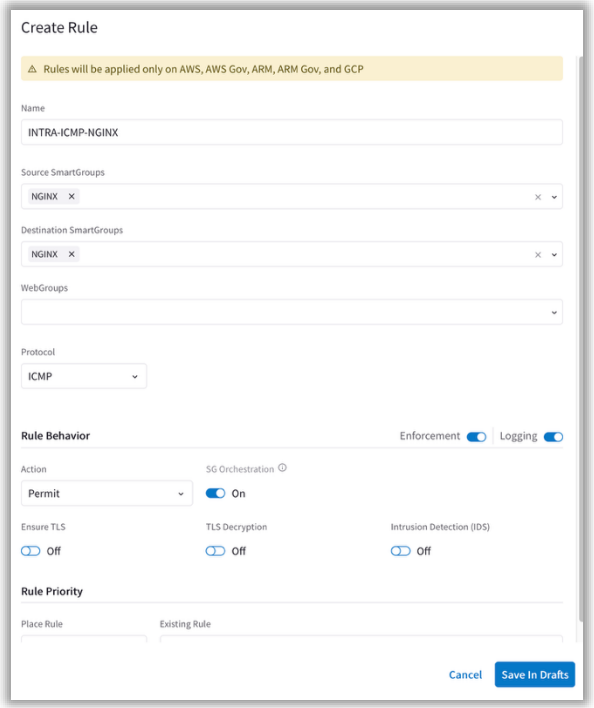
Intrusion Detection (IDS): Off

Rule Priority

Place Rule

Cancel | Save In Drafts

SmartGroup Nginx – intra



Create Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: INTRA-ICMP-NGINX

Source SmartGroups: NGINX ×

Destination SmartGroups: NGINX ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement ● | Logging ●

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

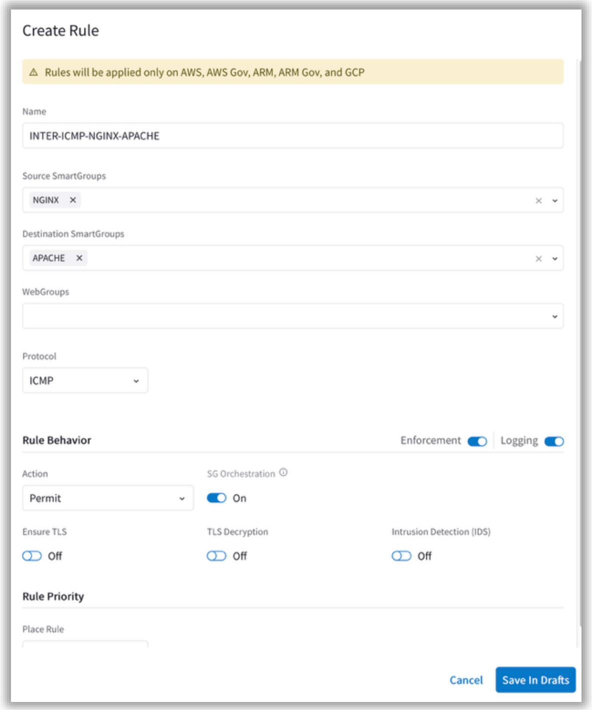
Intrusion Detection (IDS): Off

Rule Priority

Place Rule | Existing Rule

Cancel | Save In Drafts

SmartGroup Nginx – inter → SmartGroup Apache



Create Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: INTER-ICMP-NGINX-APACHE

Source SmartGroups: NGINX ×

Destination SmartGroups: APACHE ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement ● | Logging ●

Action: Permit

SG Orchestration: On

Ensure TLS: Off

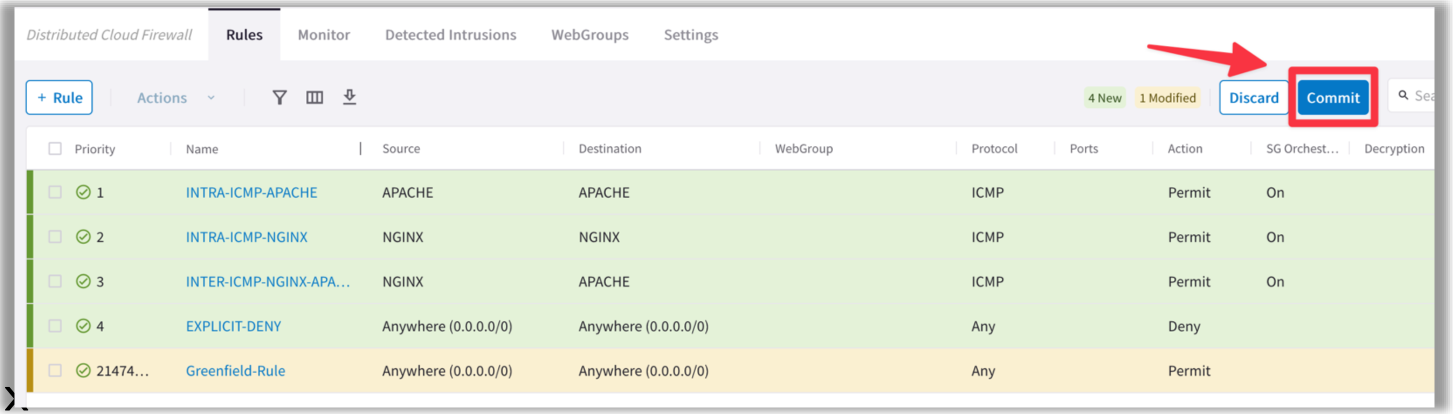
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

Cancel | Save In Drafts



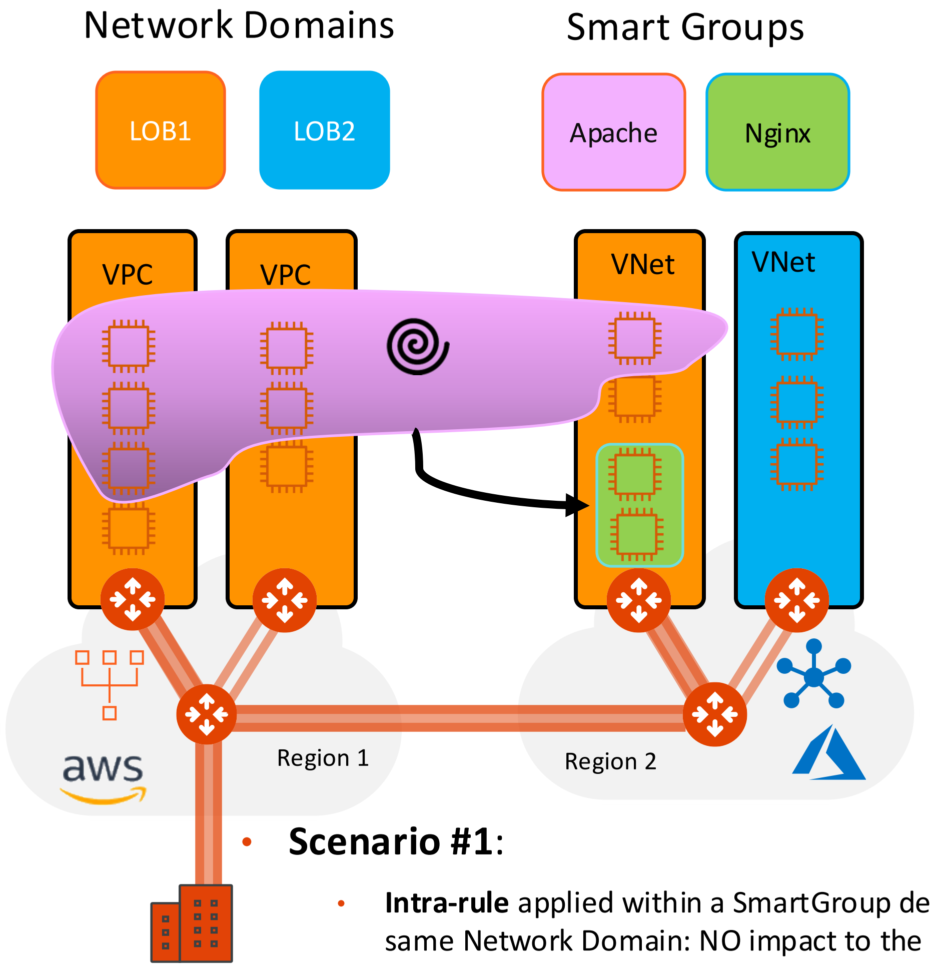
Distributed Cloud Firewall | **Rules** | Monitor | Detected Intrusions | WebGroups | Settings

+ Rule | Actions | 4 New | 1 Modified | Discard | Commit

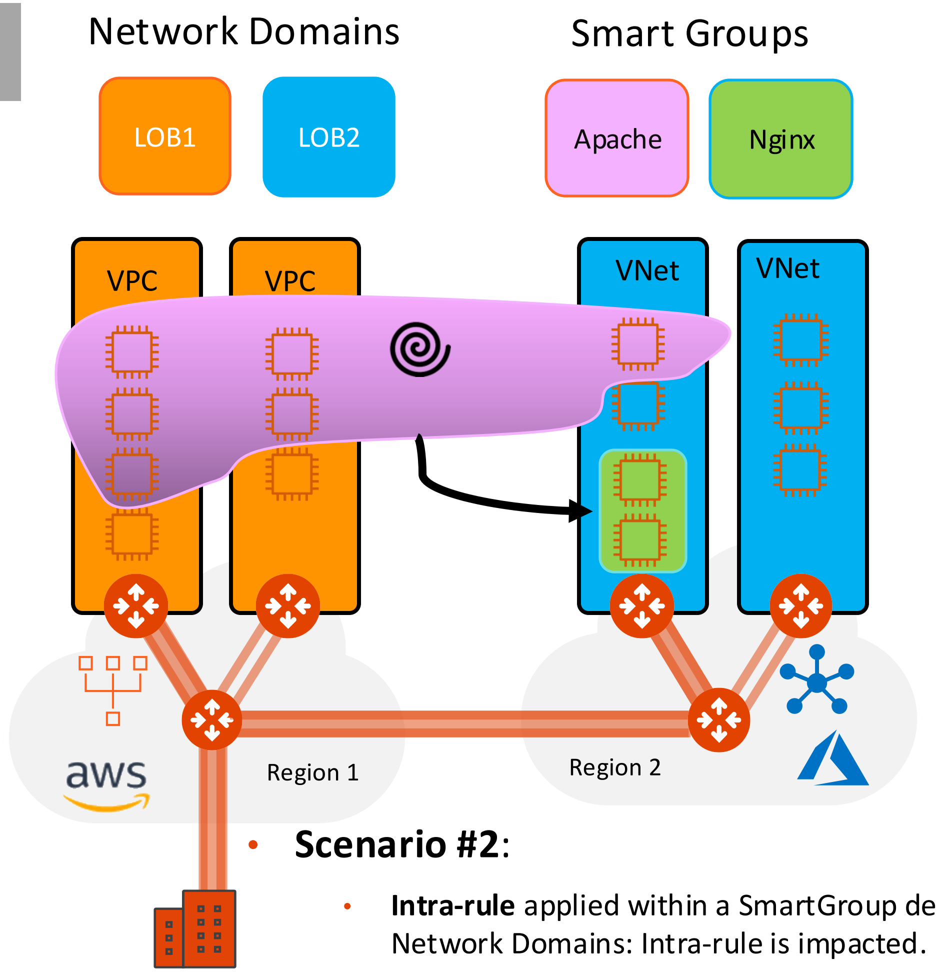
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchest...	Decryption
✓ 1	INTRA-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
✓ 2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
✓ 3	INTER-ICMP-NGINX-APA...	NGINX	APACHE		ICMP		Permit	On	
✓ 4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Deny		
✓ 21474...	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit		

- **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

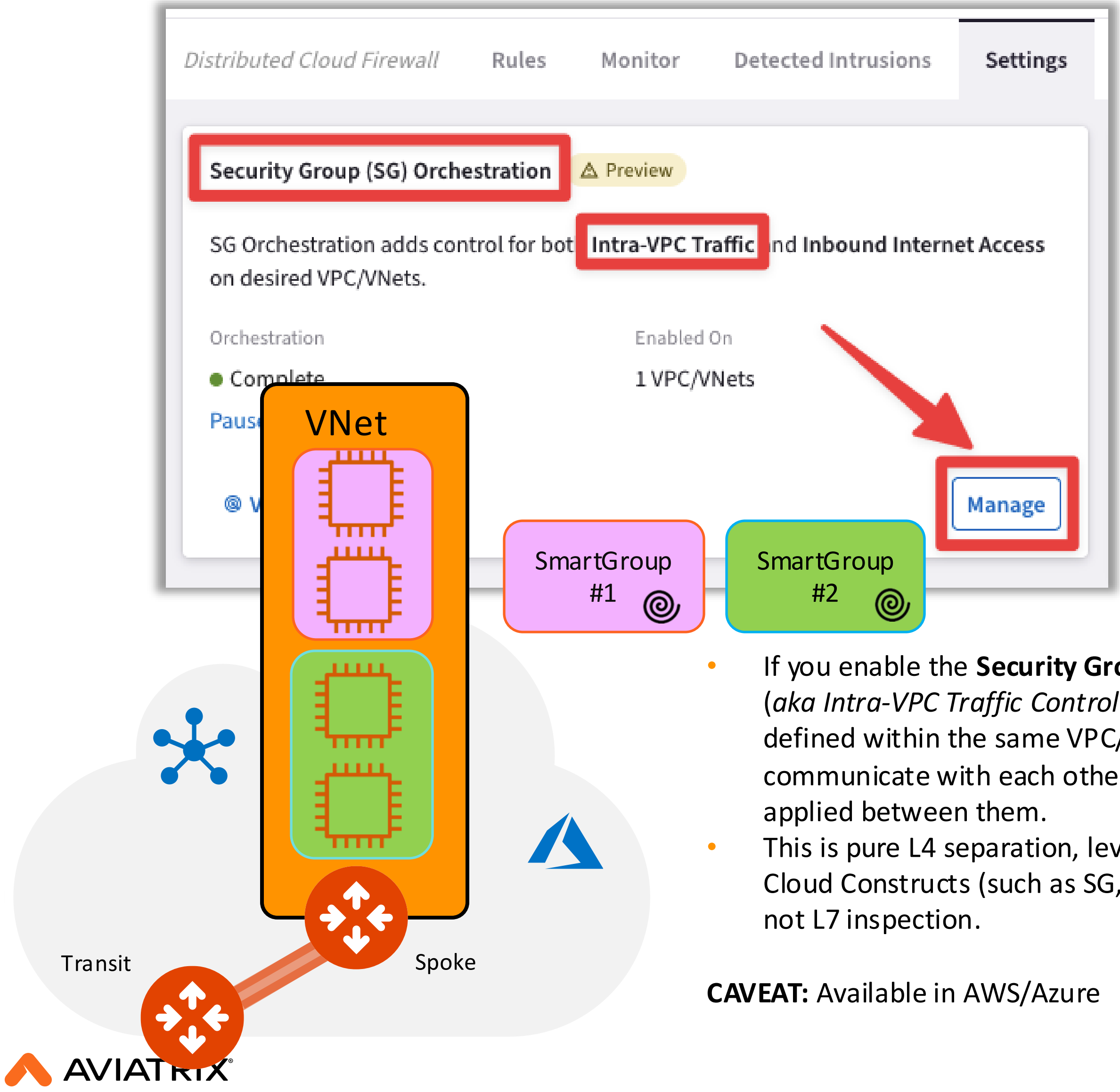
- **Scenario #2**:
  - **Intra-rule** applied within a SmartGroup defined across two Network Domains: Intra-rule is impacted.
  - **Inter-rule** is applied between SmartGroups defined across two different Network Domains: Inter-rule is impacted

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



Security Group (SG) Orchestration

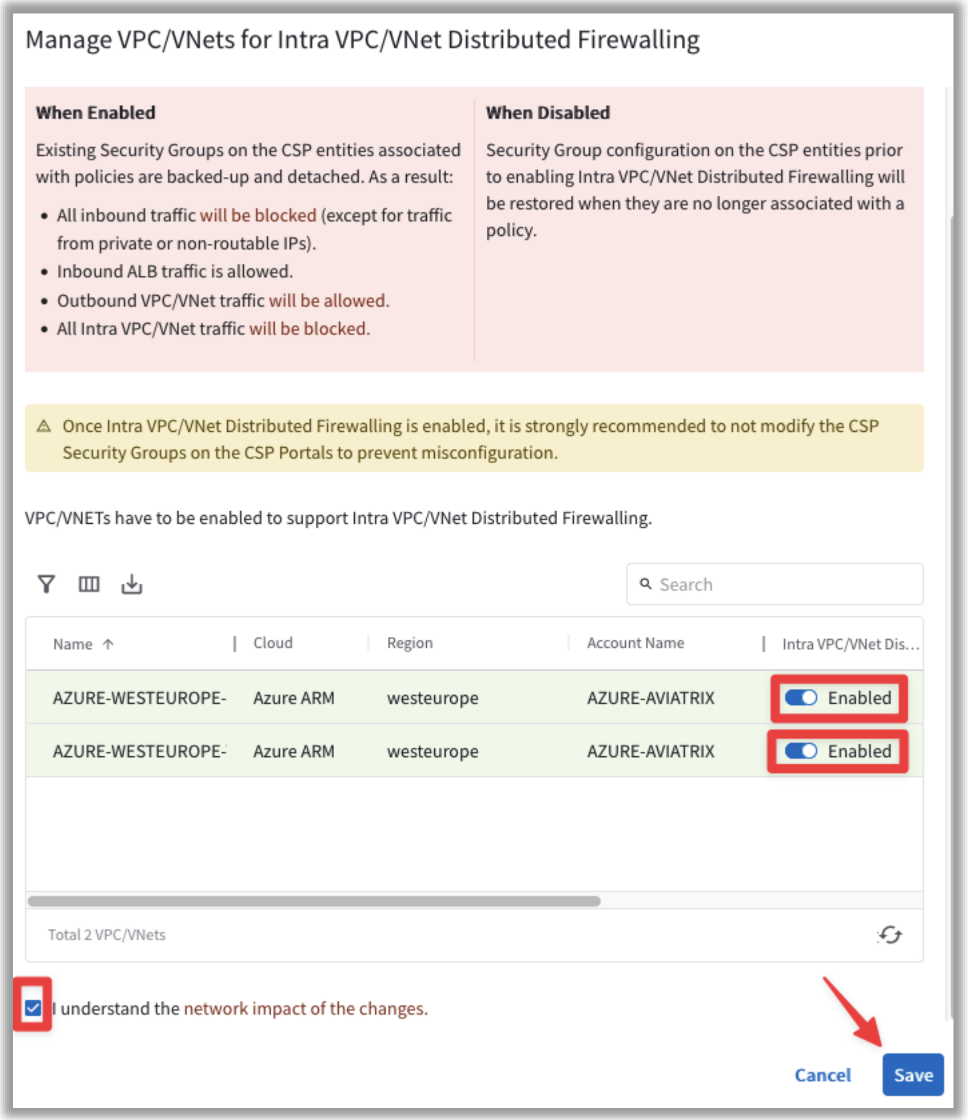
SG Orchestration adds control for bot **Intra-VPC Traffic** nd **Inbound Internet Access** on desired VPC/VNets.

Orchestration	Enabled On
● Complete	1 VPC/VNets

Paus

- 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



Manage VPC/VNets for Intra VPC/VNet Distributed Firewalling

When Enabled

Existing Security Groups on the CSP entities associated with policies are backed-up and detached. As a result:

- All inbound traffic will be blocked (except for traffic from private or non-routable IPs).
- Inbound ALB traffic is allowed.
- Outbound VPC/VNet traffic will be allowed.
- All Intra VPC/VNet traffic will be blocked.

When Disabled

Security Group configuration on the CSP entities prior to enabling Intra VPC/VNet Distributed Firewalling will be restored when they are no longer associated with a policy.

⚠ Once Intra VPC/VNet Distributed Firewalling is enabled, it is strongly recommended to not modify the CSP Security Groups on the CSP Portals to prevent misconfiguration.

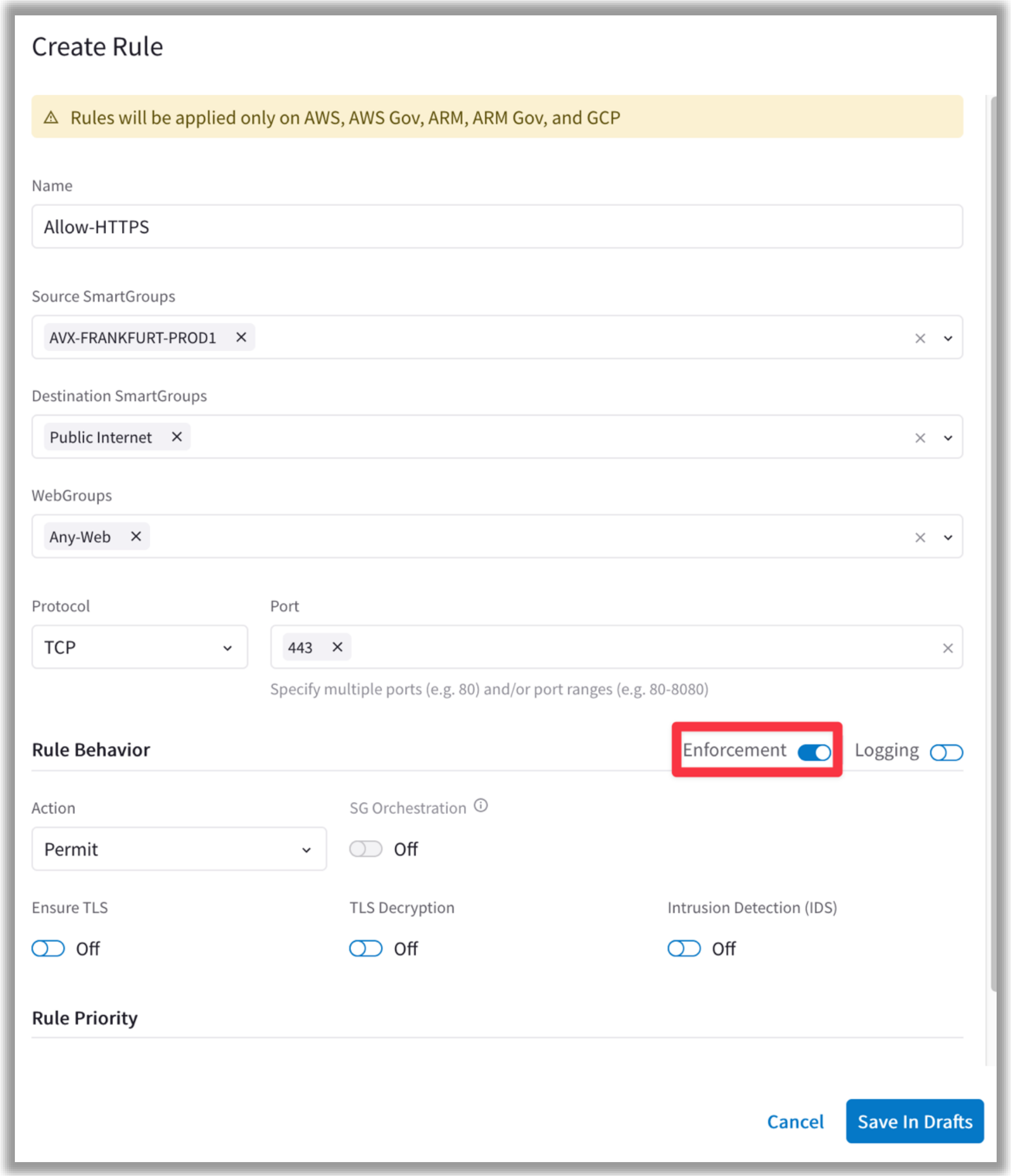
VPC/VNETs have to be enabled to support Intra VPC/VNet Distributed Firewalling.

Name ↑	Cloud	Region	Account Name	Intra VPC/VNet Dis...
AZURE-WESTEUROPE-	Azure ARM	westeurope	AZURE-AVIATRIX	Enabled
AZURE-WESTEUROPE-	Azure ARM	westeurope	AZURE-AVIATRIX	Enabled

Total 2 VPC/VNets

☑ I understand the network impact of the changes.

Rule Enforcement



Create Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: Allow-HTTPS

Source SmartGroups: AVX-FRANKFURT-PROD1 ✕

Destination SmartGroups: Public Internet ✕

WebGroups: Any-Web ✕

Protocol: TCP

Port: 443 ✕

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior Enforcement ● Logging ○

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

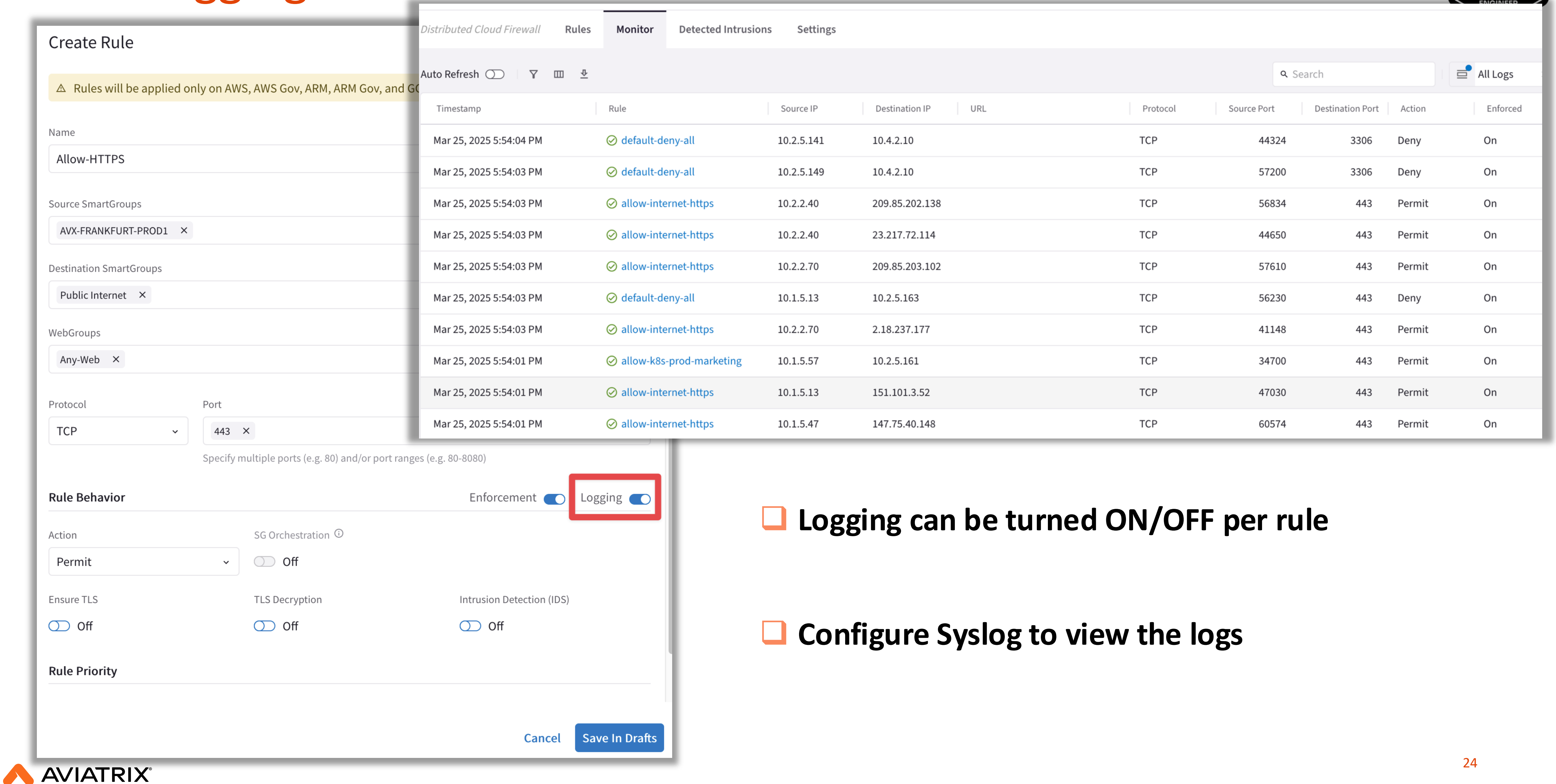
❑ Enforcement ON

- 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



Create Rule

⚠ Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GC

Name: Allow-HTTPS

Source SmartGroups: AVX-FRANKFURT-PROD1 ✕

Destination SmartGroups: Public Internet ✕

WebGroups: Any-Web ✕

Protocol: TCP

Port: 443 ✕

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement: On

Logging: On

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

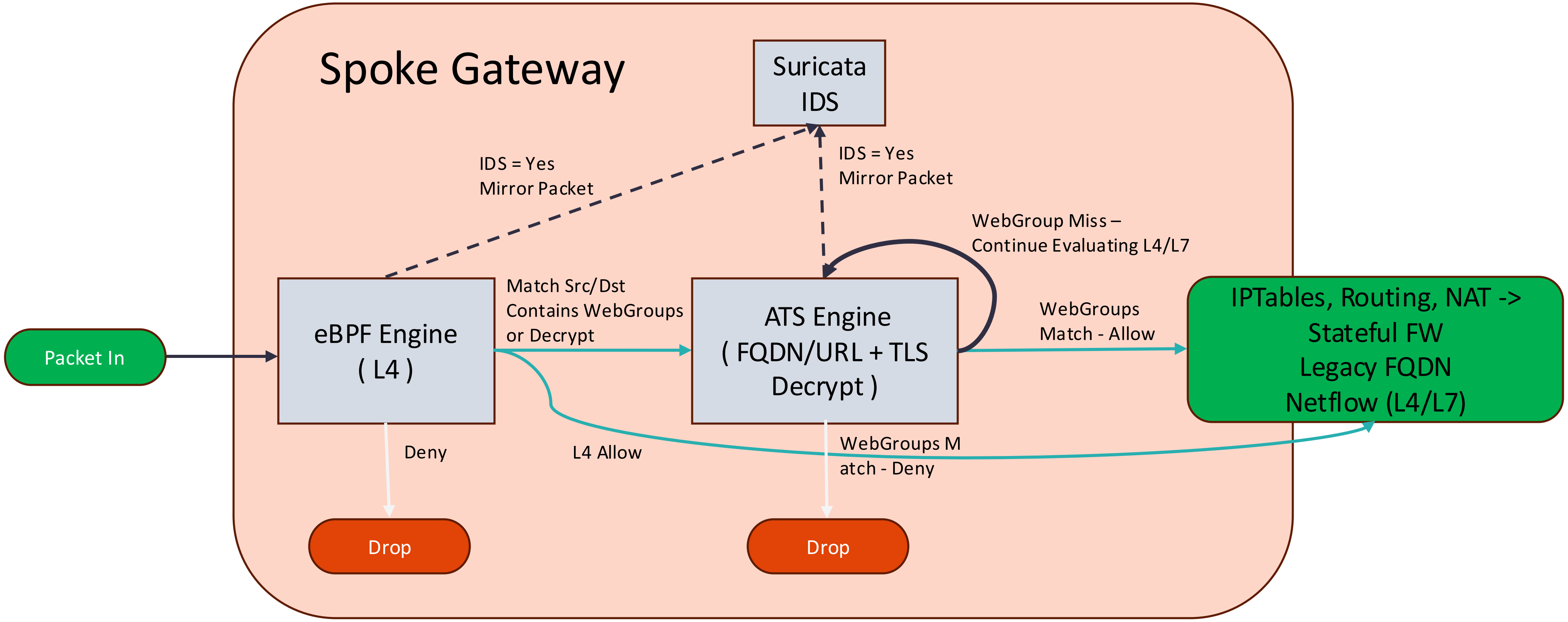
Rule Priority

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 (only in IDS mode at the moment)



Next: Lab 11 – Distributed Cloud Firewall