

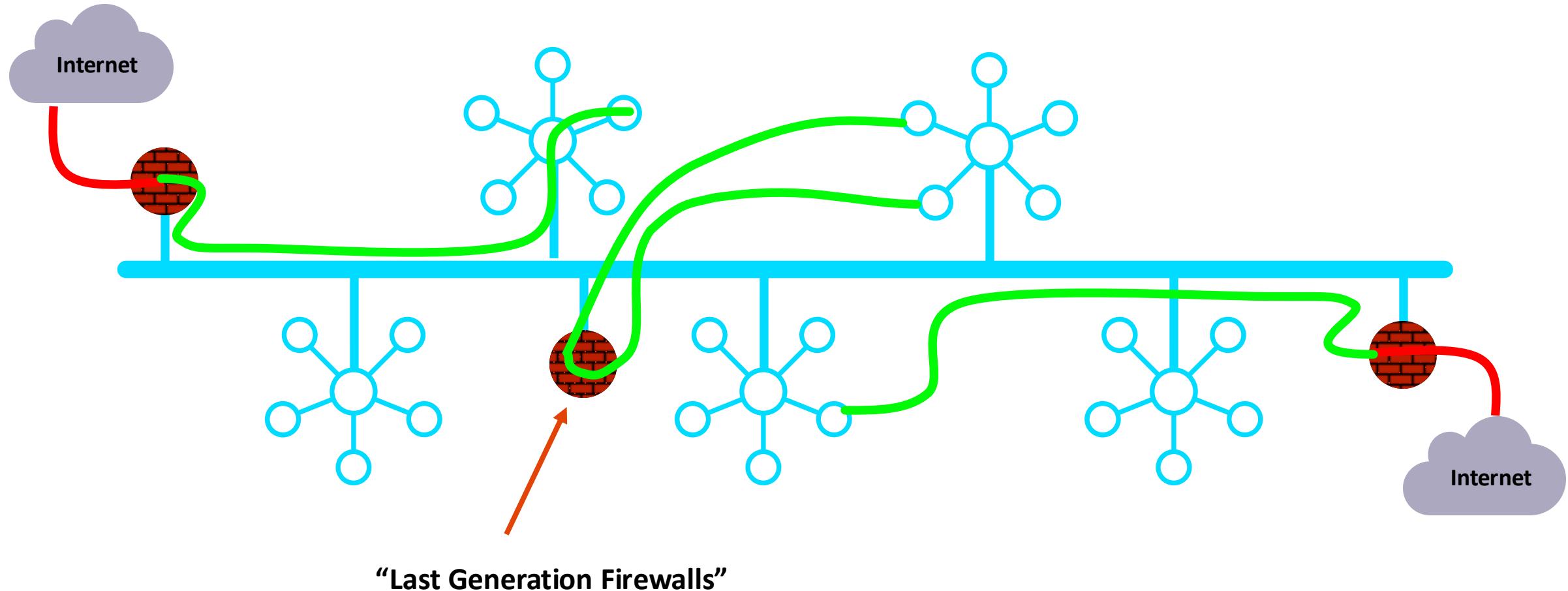


Distributed Cloud Firewall

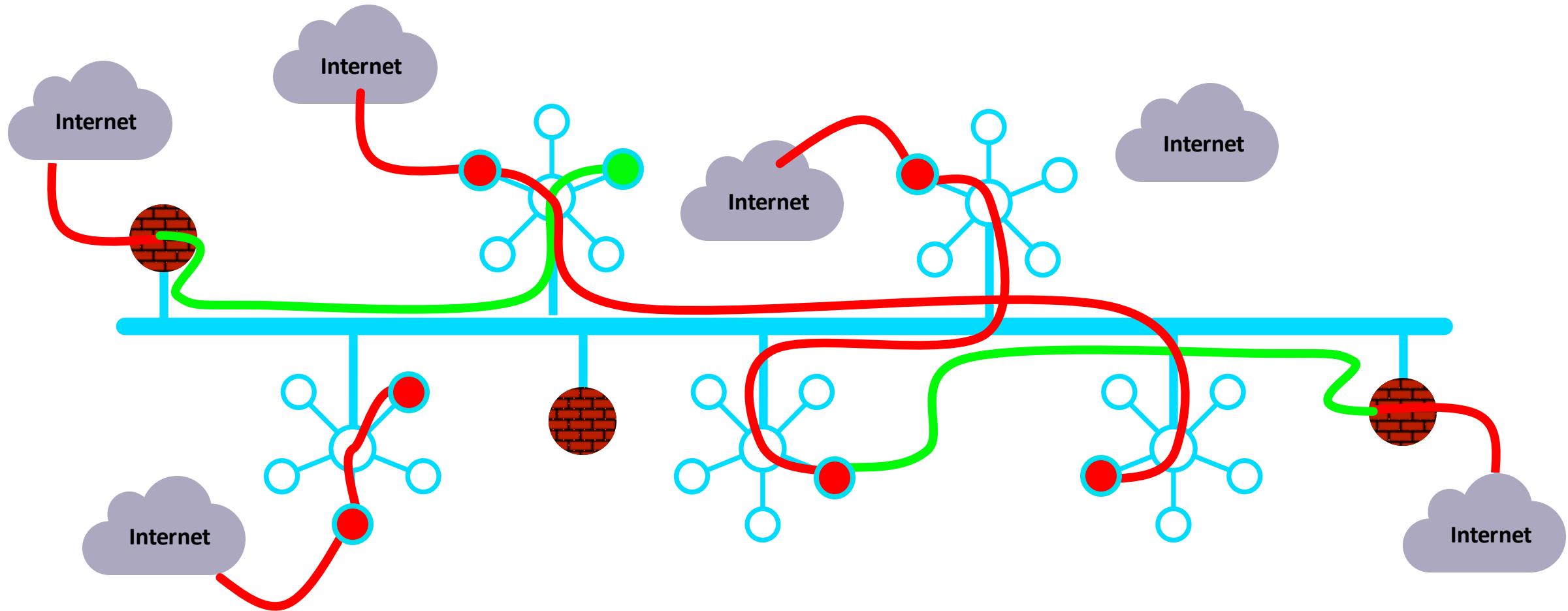
ACE Team



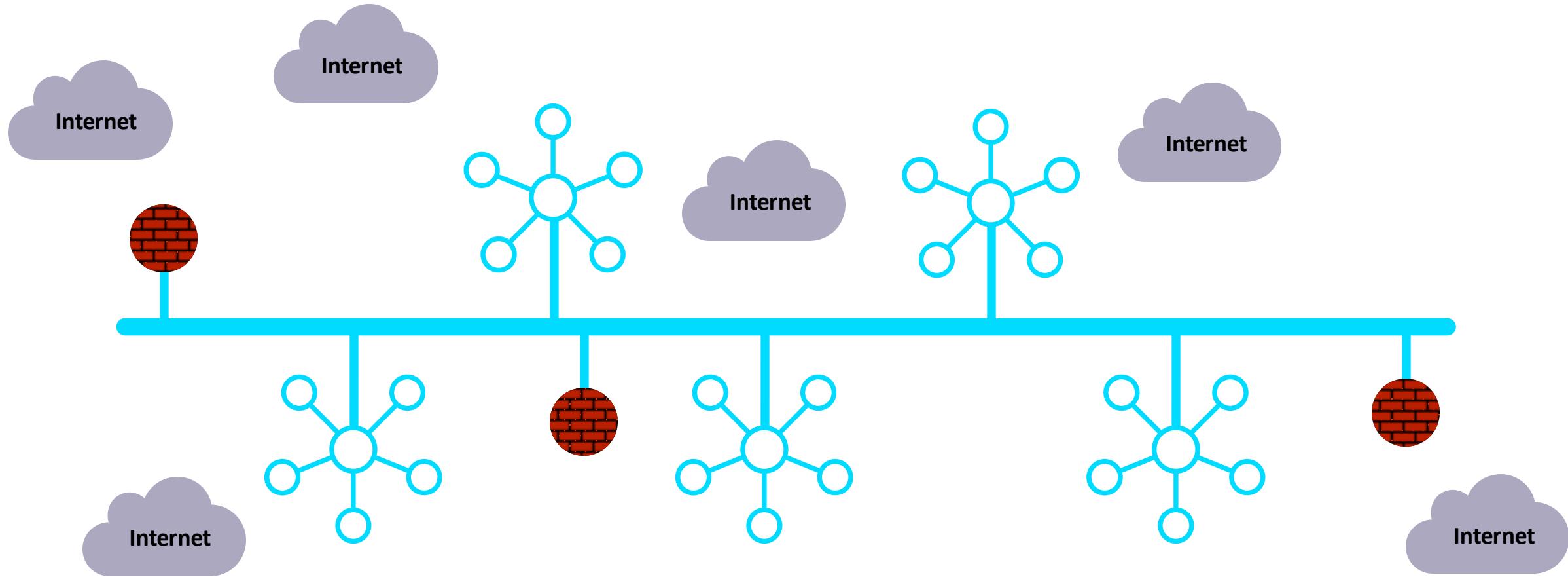
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



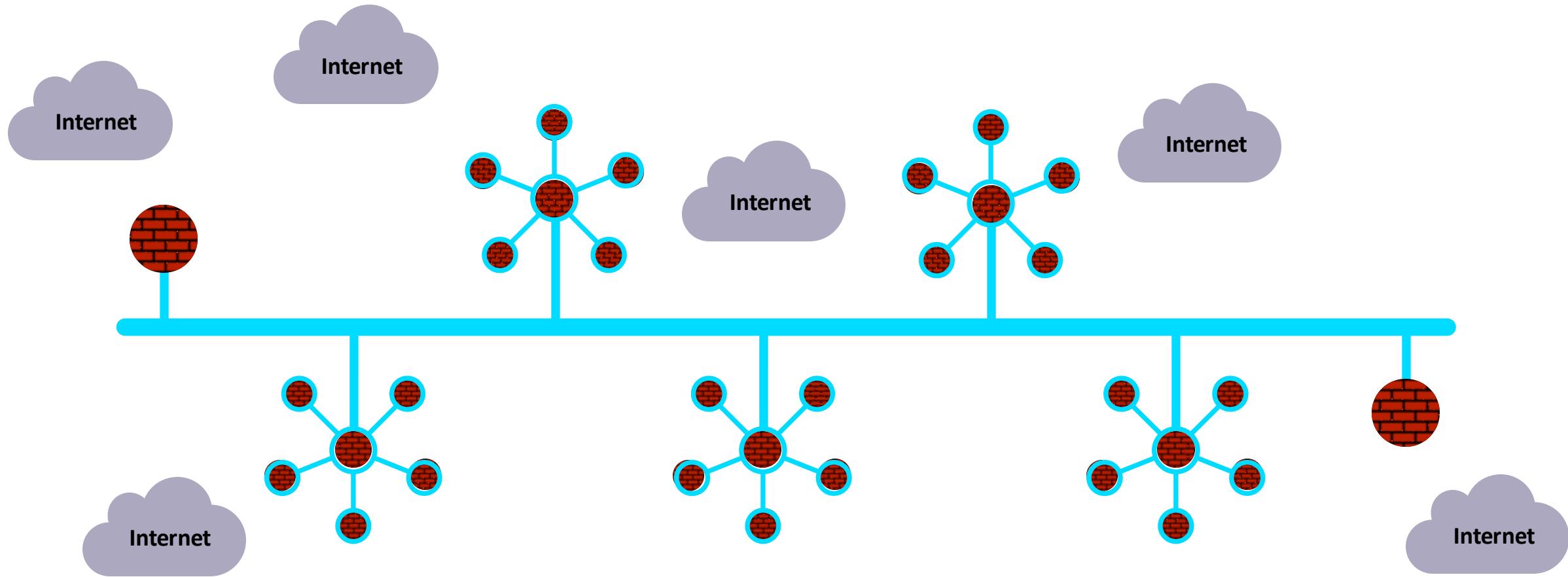
In Reality...



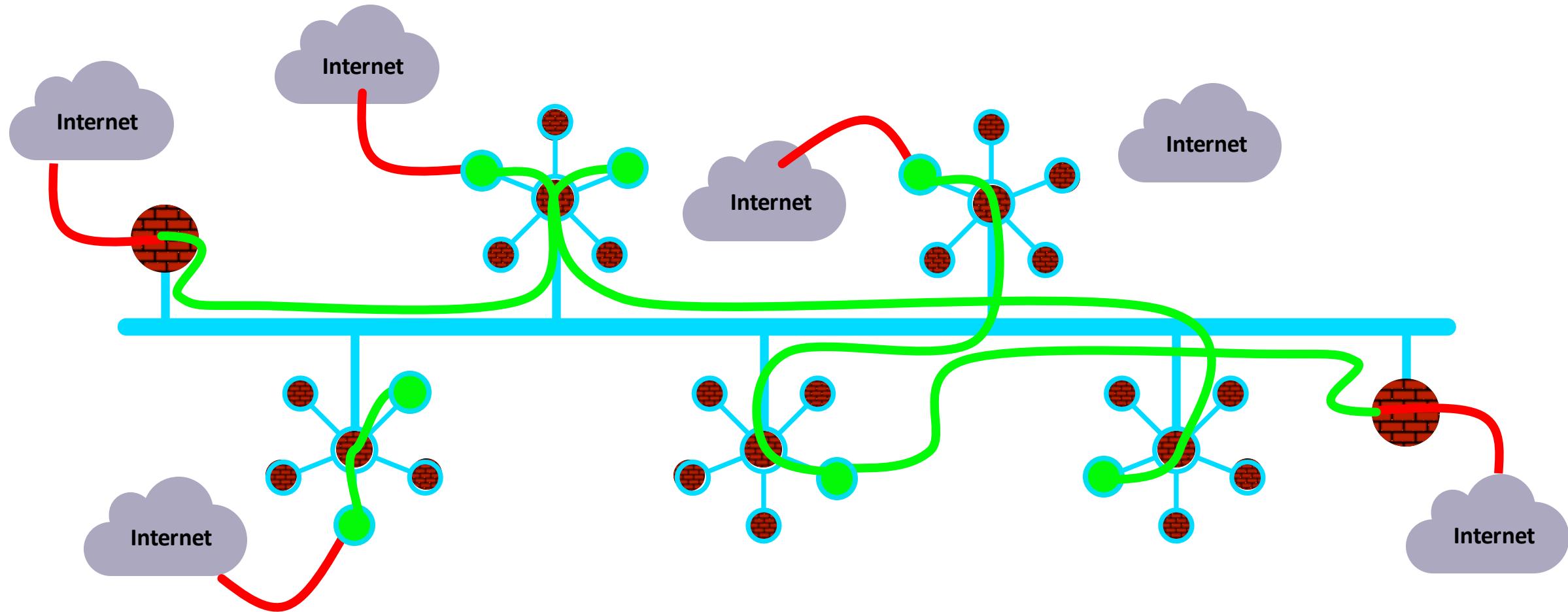
What If... the architecture was built for cloud



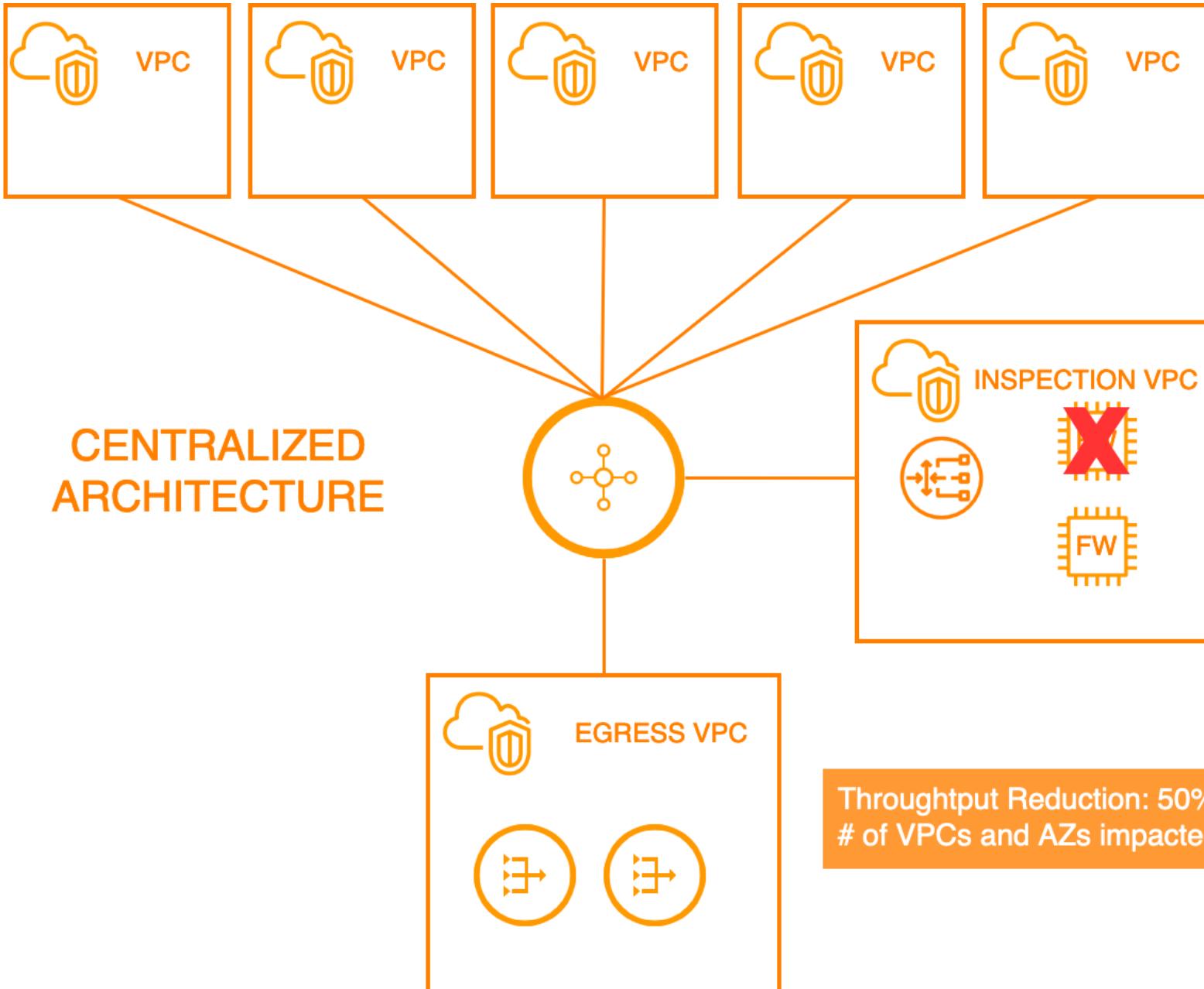
Firewalling Functions were Embedded in the Cloud Network Everywhere...



Distribution of the Security Services into the Spokes



Impact of Failure – Centralized Architecture



Impact of Failure – Distributed Architecture

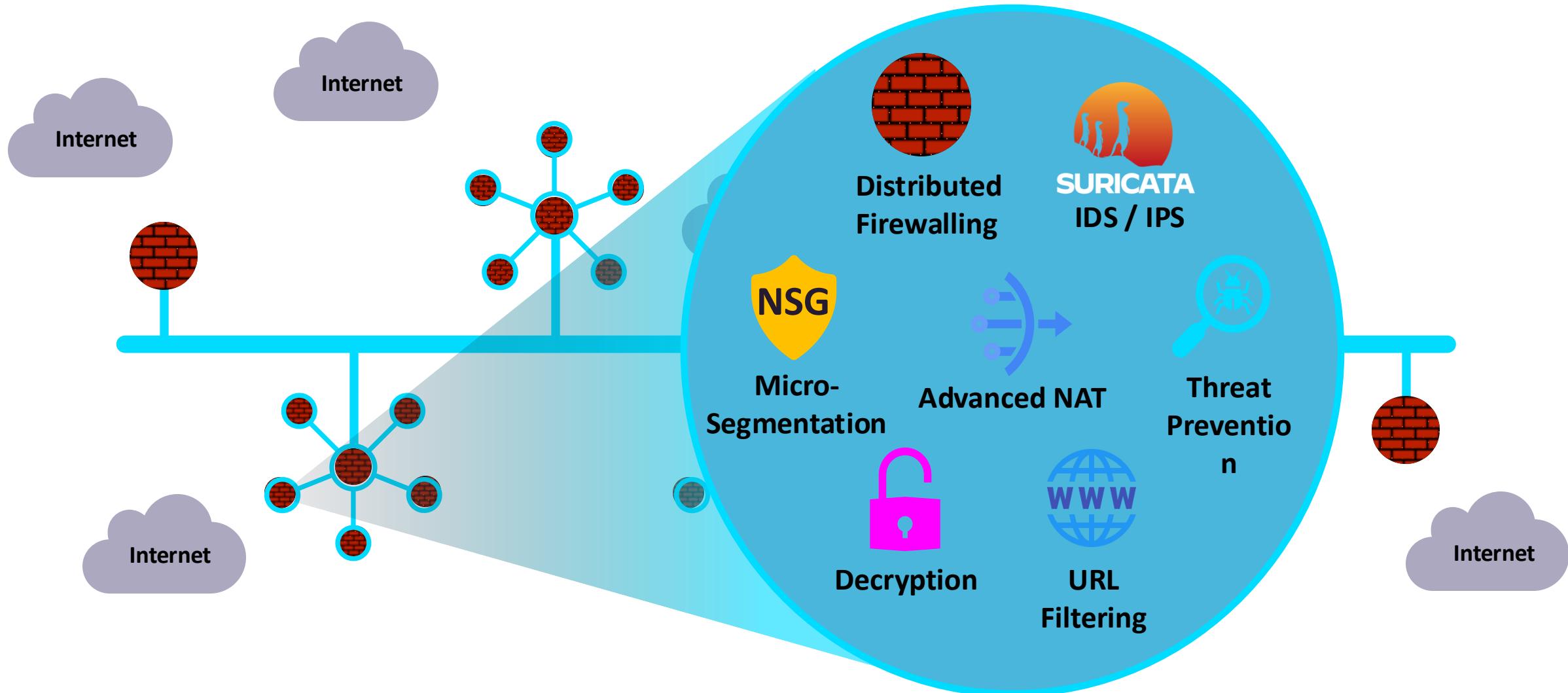


DISTRIBUTED
ARCHITECTURE

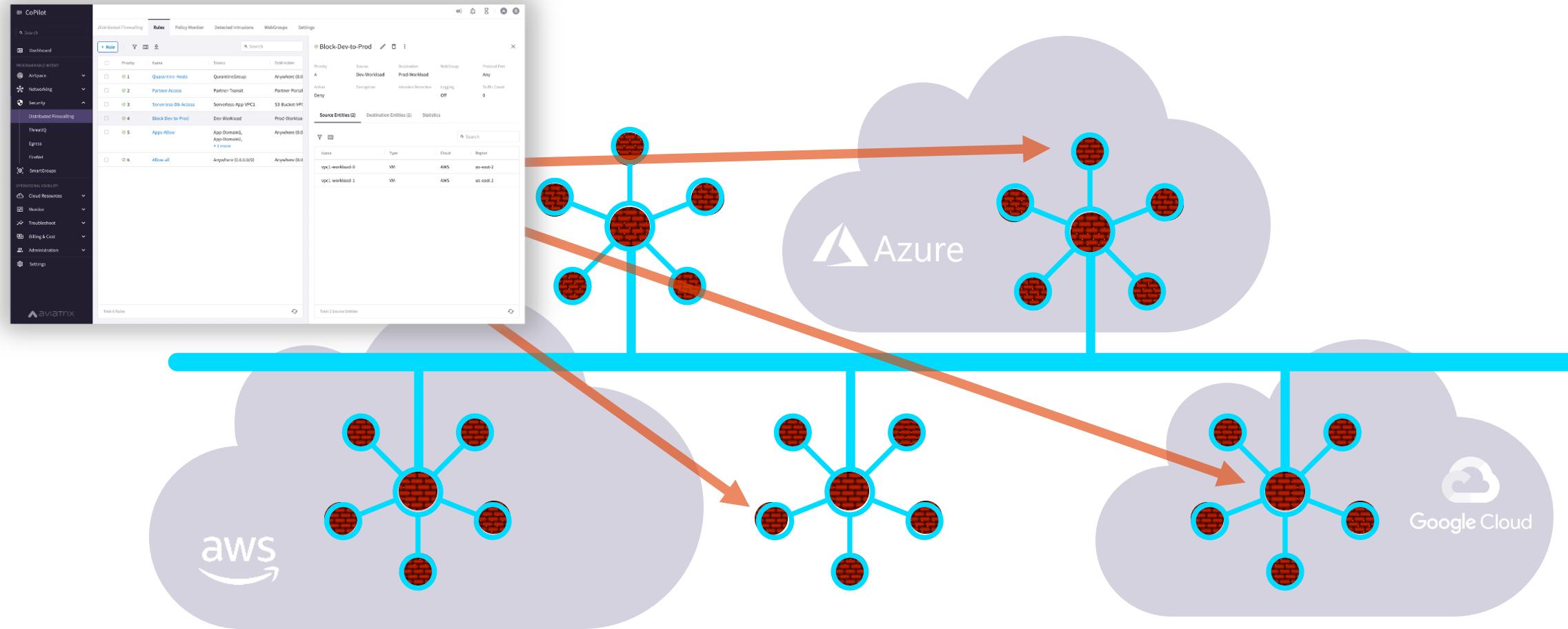


Throughput Reduction: 10%
of VPCs and AZs impacted: 1 AZ in 1 VPC

And, What If it was more than just firewalling...



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



Where and How Policies Are Enforced Is Abstracted...

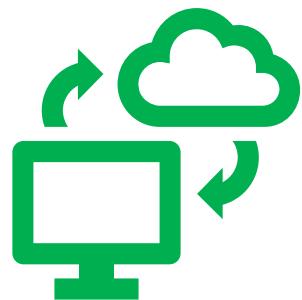
SmartGroups: Definition

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

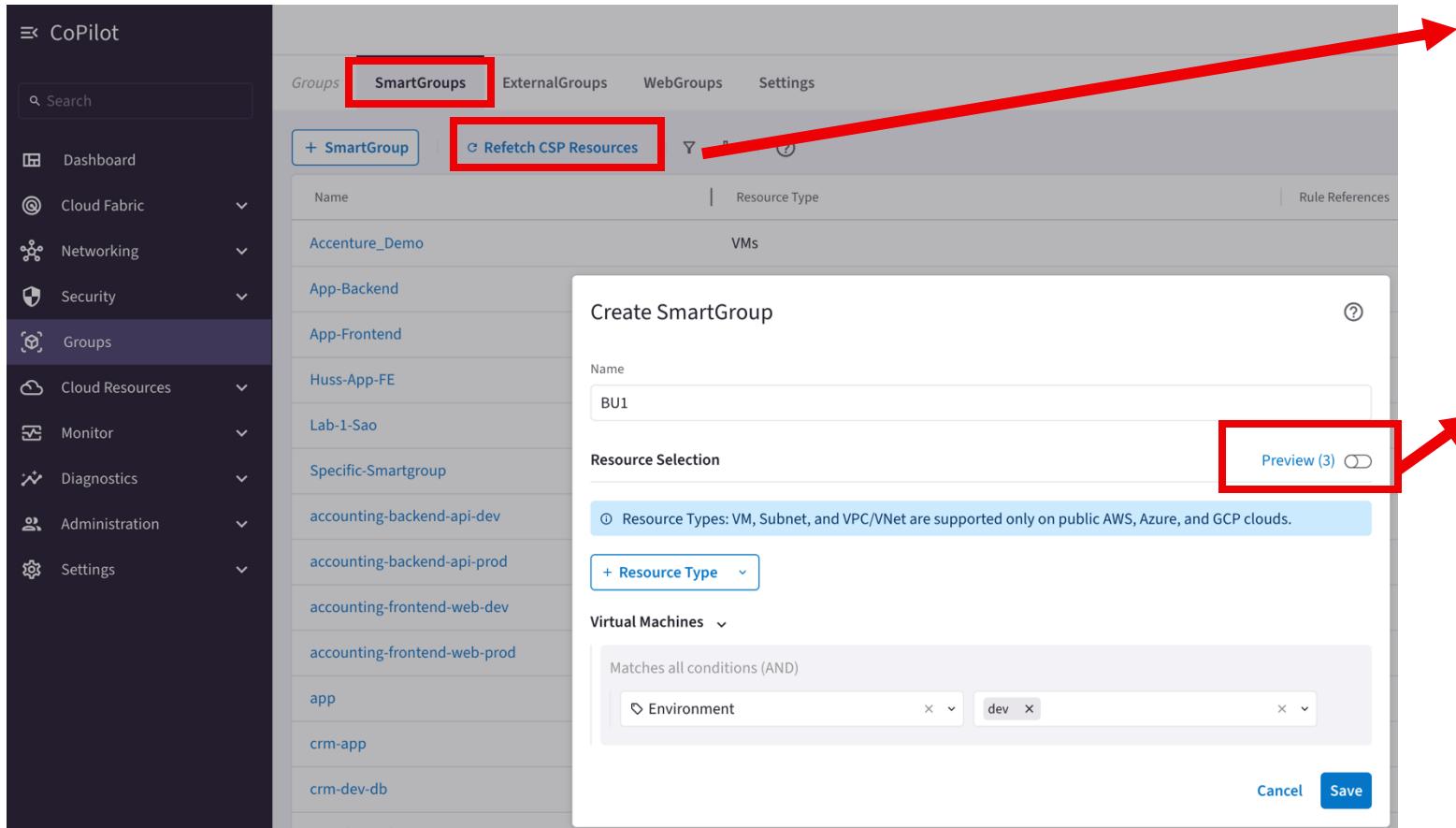
A SmartGroup identifies a group of resources that have similar policy requirements and are associated to the same *logical container*.

- The members of a SmartGroup can be classified using *different* methods:

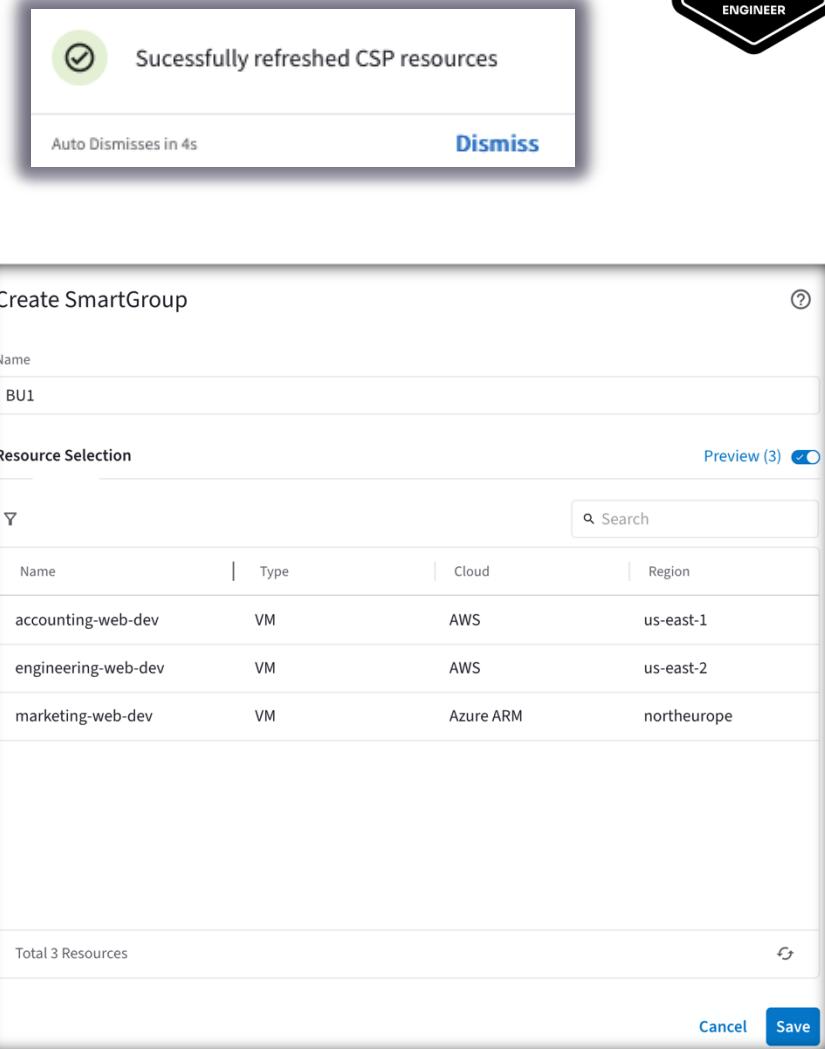
- CSP Tag
- Subnets
- VPC/Vnets
- Kubernetes
- Hostnames
- External Connections (S2C)



Smart Groups Creation



The screenshot shows the CoPilot interface with the 'Groups' tab selected. In the center, a 'Create SmartGroup' dialog is open, showing the name 'BU1' and a resource selection section. A red box highlights the 'Create SmartGroup' button and the 'Refetch CSP Resources' button. A red arrow points from the 'Create SmartGroup' dialog to a success message box on the right.



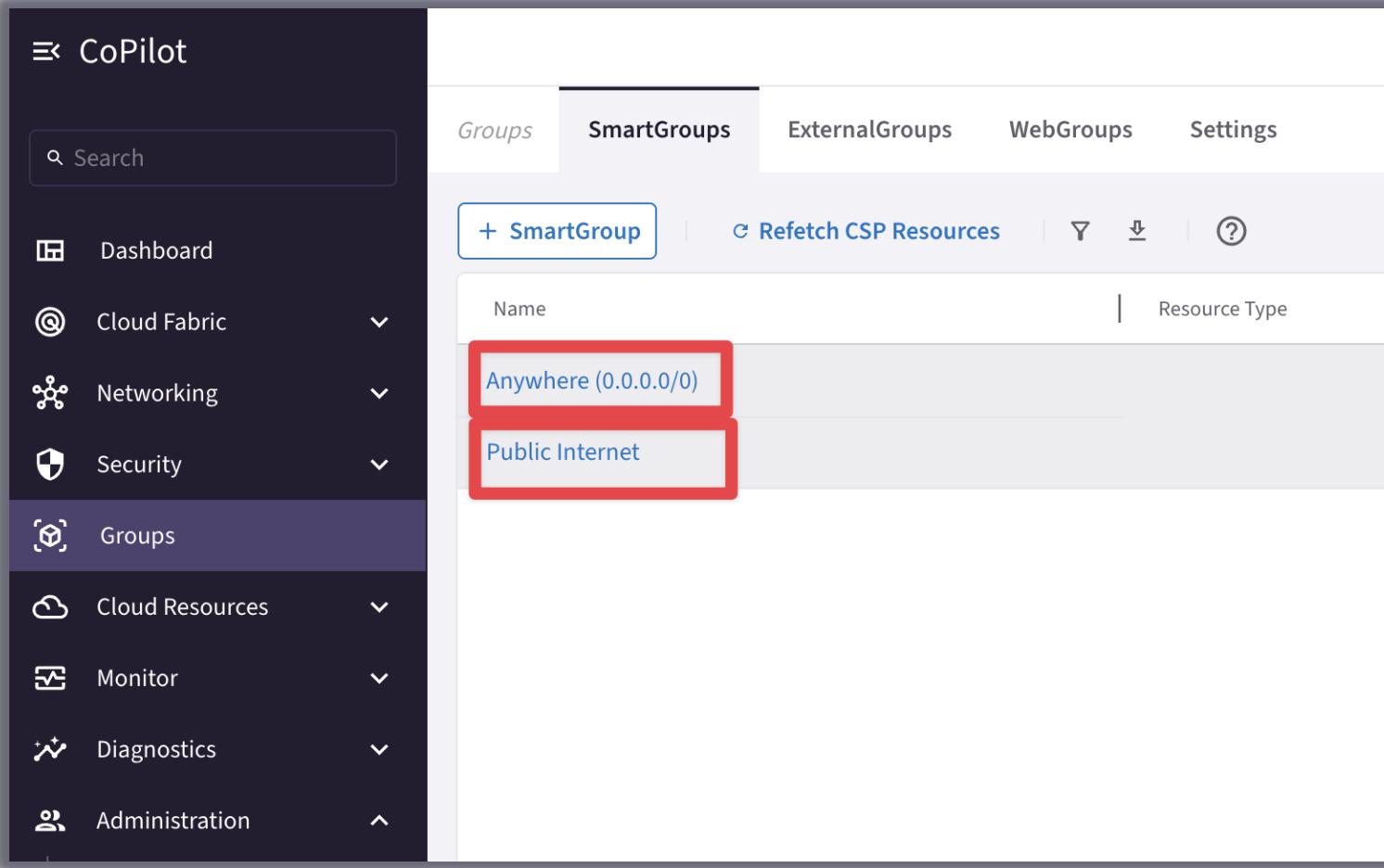
The screenshot shows the 'Create SmartGroup' dialog with the name 'BU1'. Under 'Resource Selection', there is a table of resources:

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

A red box highlights the 'Preview (3)' button. To the right, a success message box says 'Successfully refreshed CSP resources' with a 'Dismiss' button.

- 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

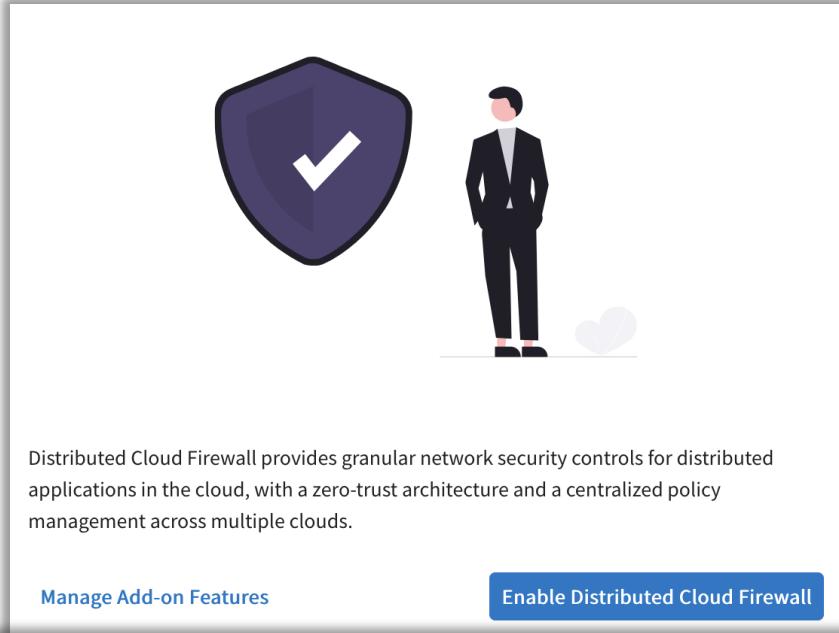


The screenshot shows the CoPilot interface with the 'SmartGroups' tab selected. Two pre-defined smart groups are listed: 'Anywhere (0.0.0.0/0)' and 'Public Internet'. Both entries are highlighted with a red rectangular box.

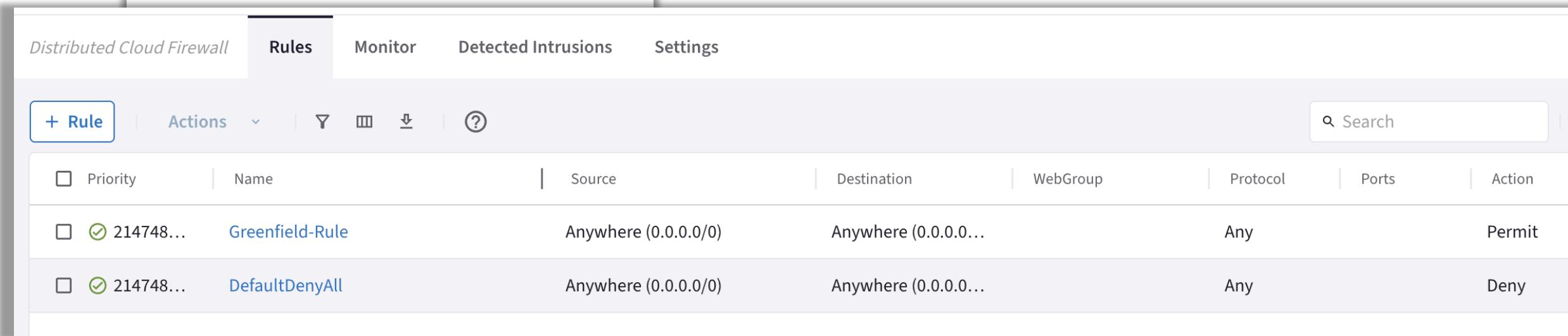
Name	Resource Type
Anywhere (0.0.0.0/0)	
Public Internet	

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

Enabling Distributed Cloud Firewall



- 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
<input type="checkbox"/>	214748... Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit
<input type="checkbox"/>	214748... DefaultDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		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

Action
Permit

SG Orchestration
Off

Ensure TLS
Off

TLS Decryption
Off

Intrusion Detection (IDS)
Off

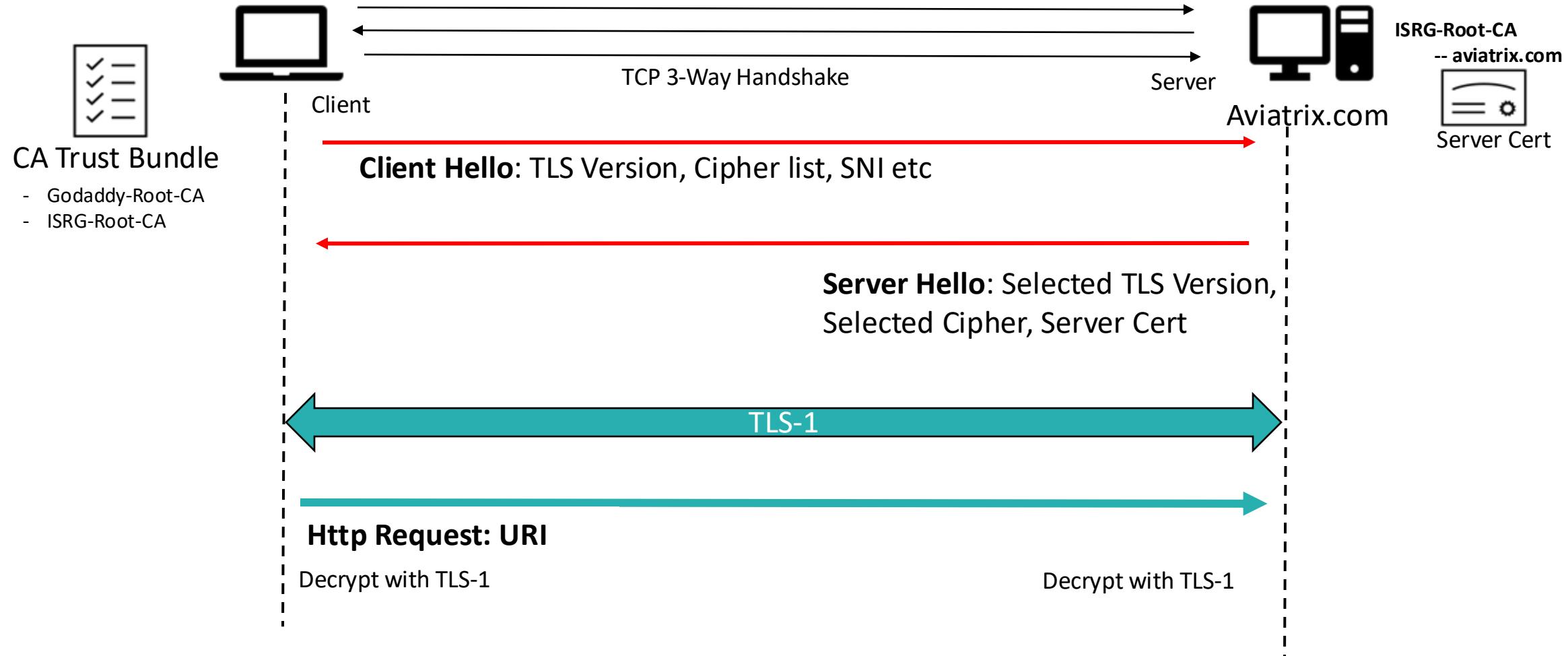
Rule Priority

Enforcement Logging

Cancel **Save In Drafts**

- **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

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

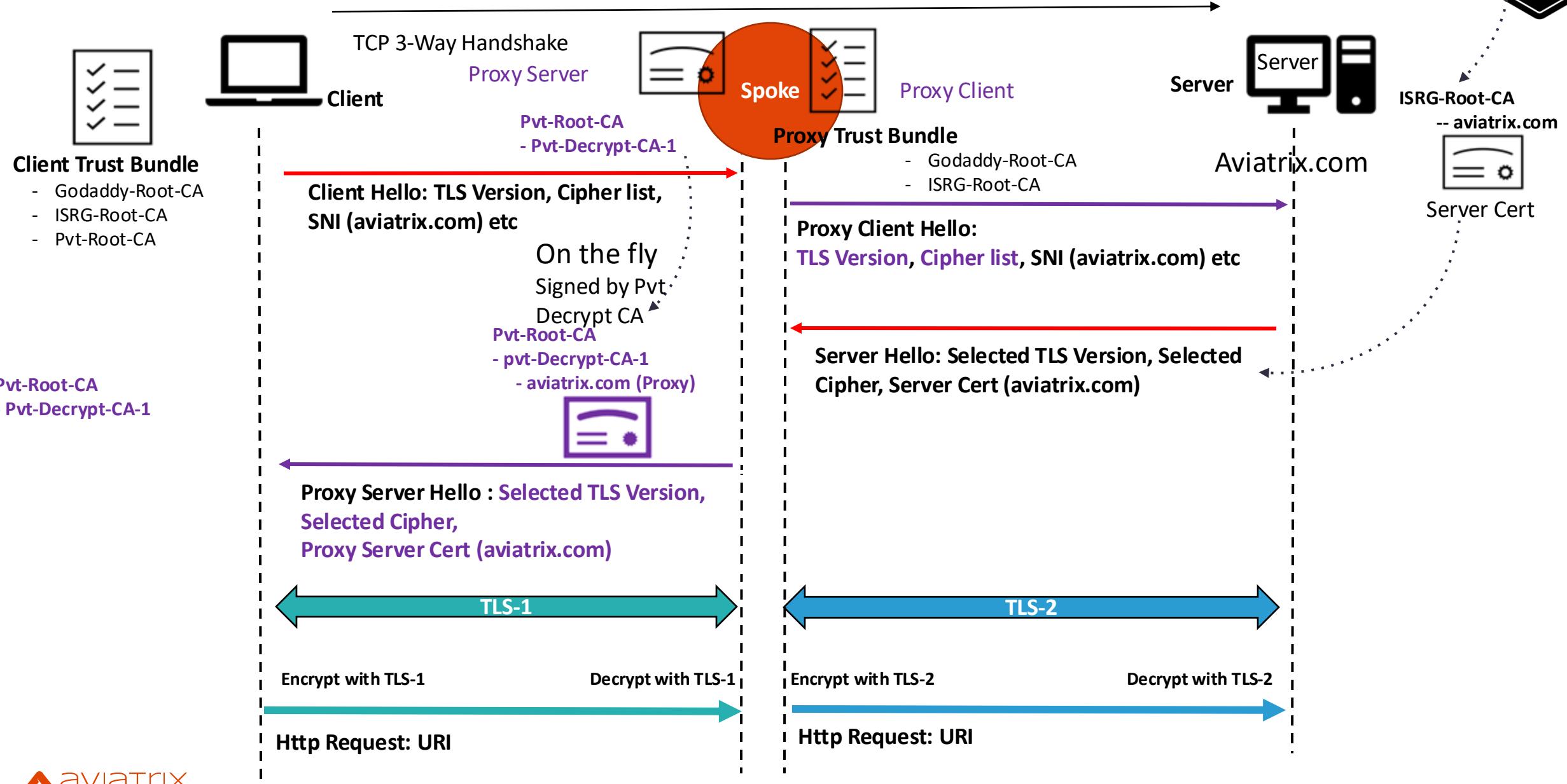
▼ Subject Public Key Info

Field Value

CN = aviatrix.com

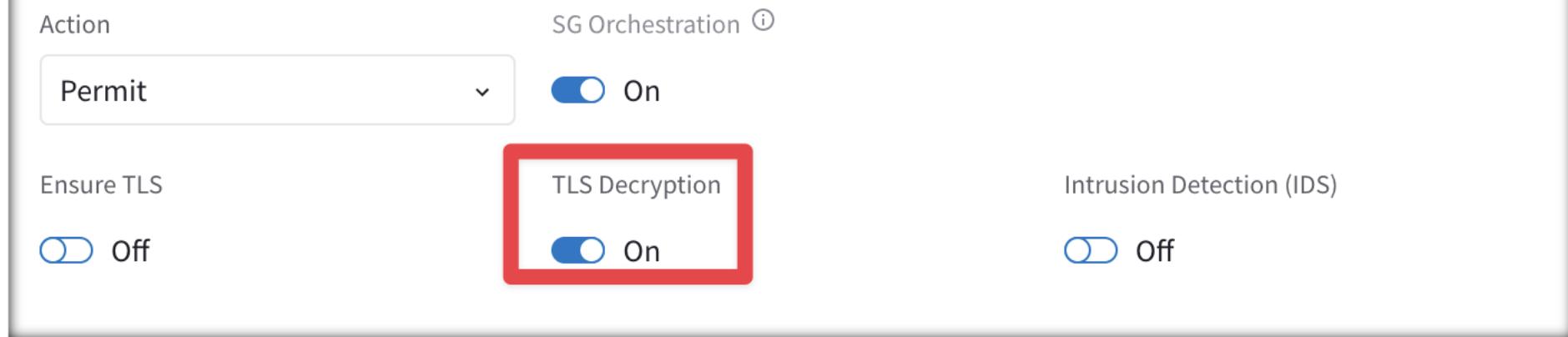


TLS Decryption: Basic TLS Decryption



TLS Decryption: Decryption CA Cert

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

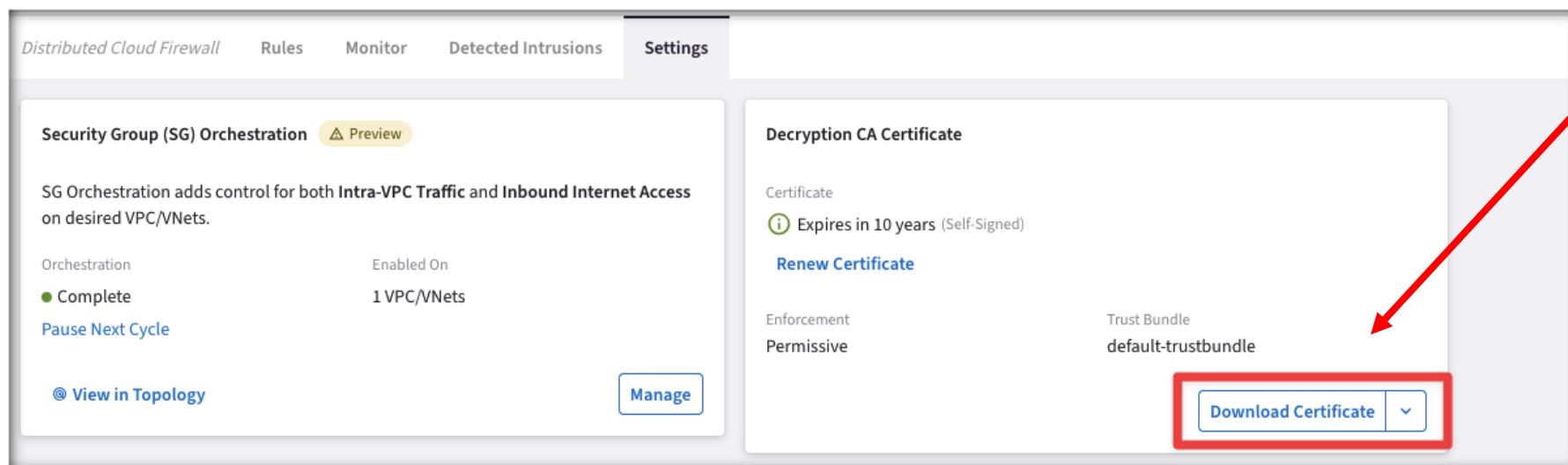


Action: Permit, SG Orchestration: On

Ensure TLS: Off

TLS Decryption: On (highlighted with a red box)

Intrusion Detection (IDS): Off



Distributed Cloud Firewall, Rules, Monitor, Detected Intrusions, Settings

Security Group (SG) Orchestration: Preview

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

Orchestration: Complete, Enabled On: 1 VPC/VNets

@ View in Topology, Manage

Decryption CA Certificate:

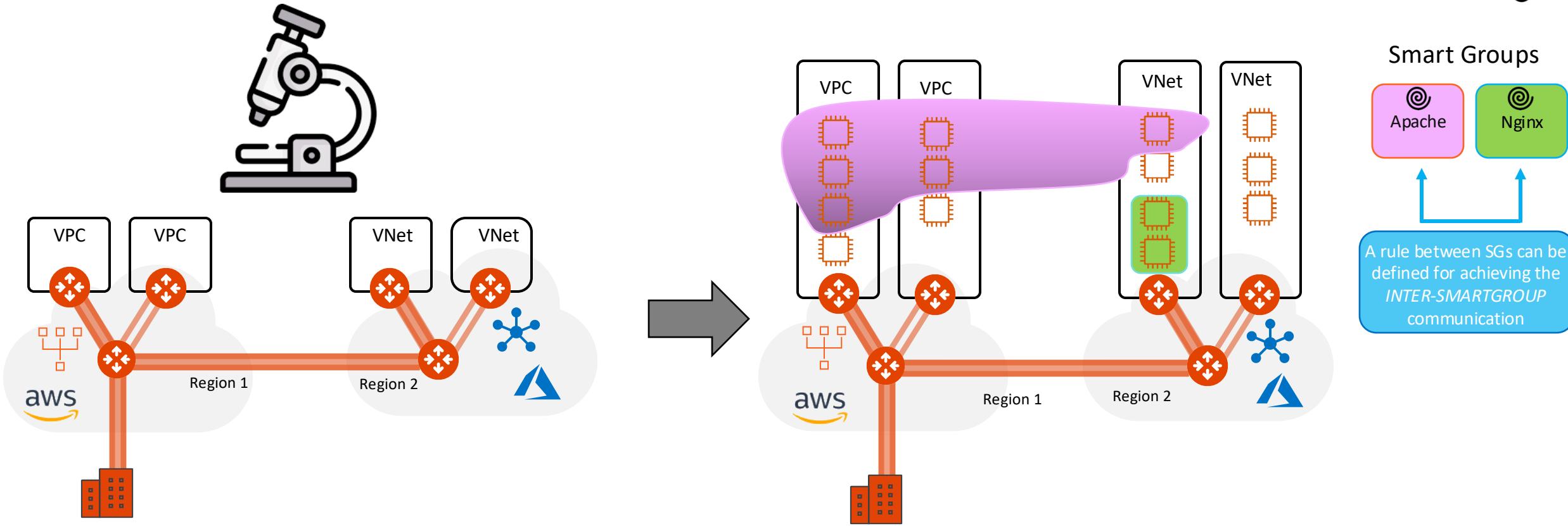
- Certificate: Expires in 10 years (Self-Signed)
- Renew Certificate
- Enforcement: Permissive
- Trust Bundle: default-trustbundle

Download Certificate (highlighted with a red box)

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-Segmentation: SmartGroups, Intra-Rules and Inter-Rules



Diagram Overview: The diagram illustrates a multi-region cloud architecture. On the left, two VPCs (Region 1) are connected to a central VNet (Region 2). A pink oval highlights the internal traffic between the VPCs, labeled "intra". Three green boxes represent SmartGroups: "SmartGroup Apache" (orange), "SmartGroup Nginx" (green), and "SmartGroup NGINX" (blue). Arrows indicate "intra" traffic between SmartGroups within a VPC and "inter" traffic between different SmartGroups across VPCs.

Create Rule Screenshots:

- SmartGroup Apache (Intra Rule):** Shows a rule named "INTRAL-ICMP-APACHE" from APACHE to APACHE via ICMP, with "Permit" action and SG Orchestration turned on.
- SmartGroup Nginx (Intra Rule):** Shows a rule named "INTRAL-ICMP-NGINX" from NGINX to NGINX via ICMP, with "Permit" action and SG Orchestration turned on.
- SmartGroup NGINX (Inter Rule):** Shows a rule named "INTERL-ICMP-NGINX-APACHE" from NGINX to APACHE via ICMP, with "Permit" action and SG Orchestration turned on.

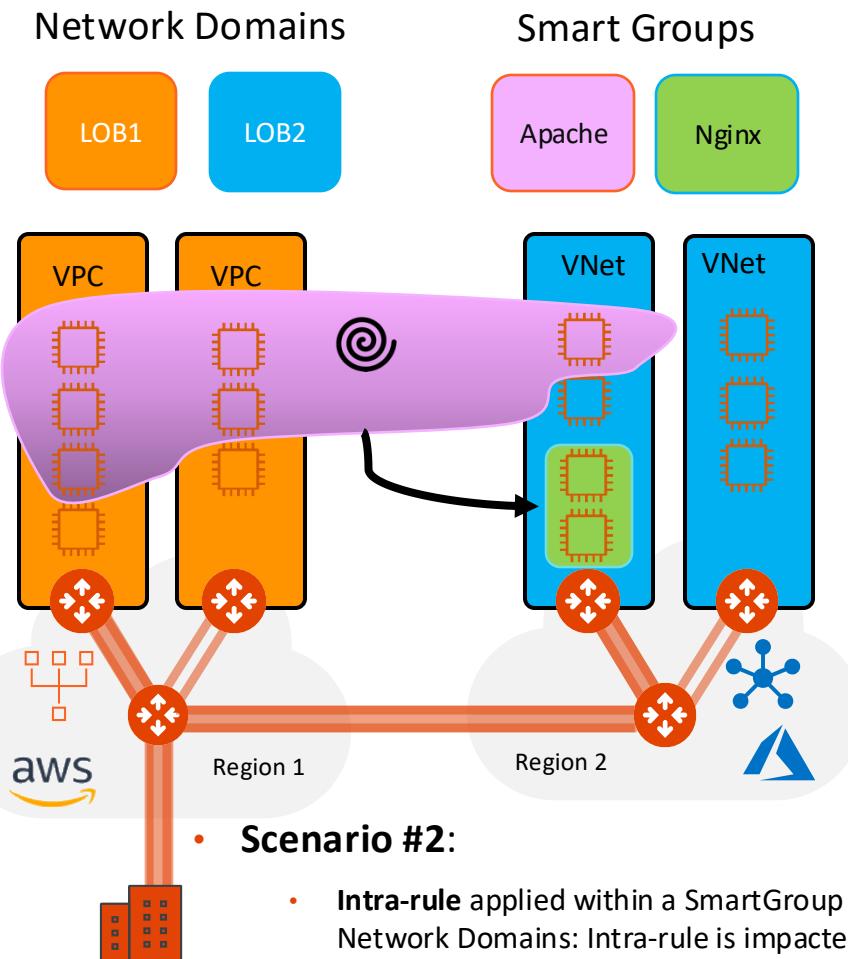
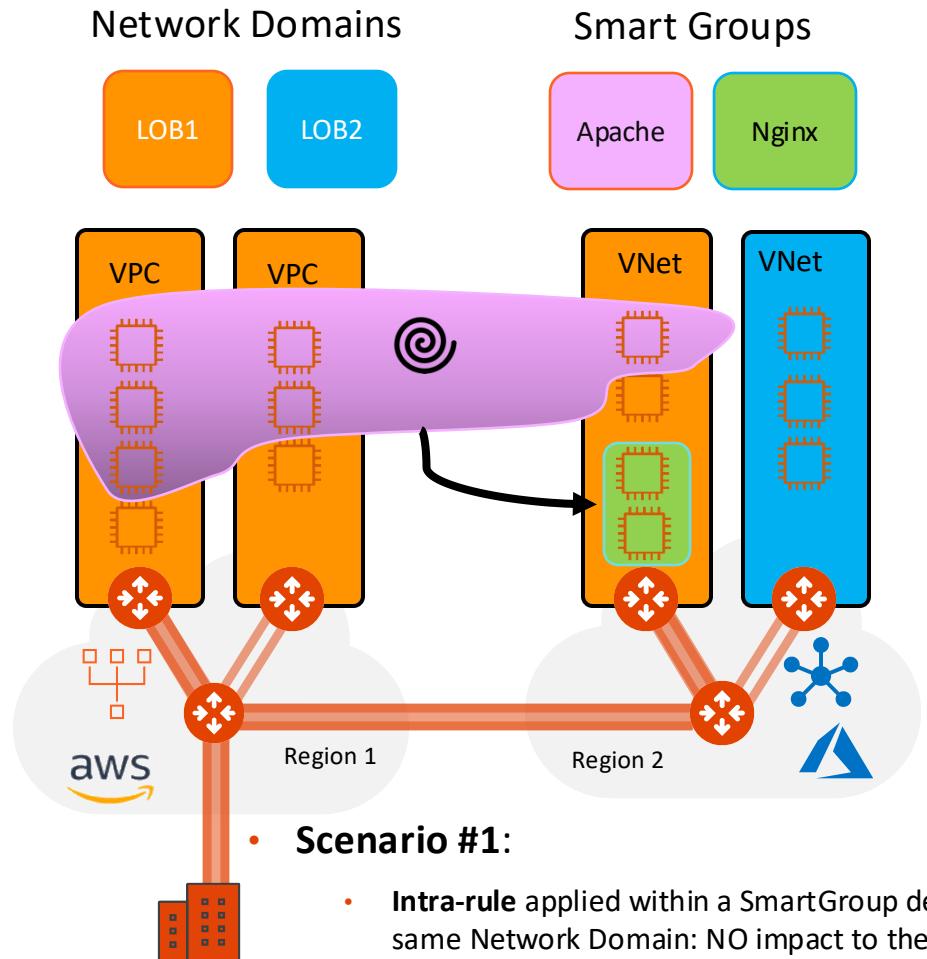
Distributed Cloud Firewall UI: The screenshot shows the DCF interface with a table of rules. A red arrow points to the "Commit" button at the top right of the table header. The table lists the following rules:

Priority	Name	Source	Destination	Protocol	Action	SG Orchestr...	Decryption
1	INTRAL-ICMP-APACHE	APACHE	APACHE	ICMP	Permit	On	
2	INTRAL-ICMP-NGINX	NGINX	NGINX	ICMP	Permit	On	
3	INTERL-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		

List of Key Points:

- 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

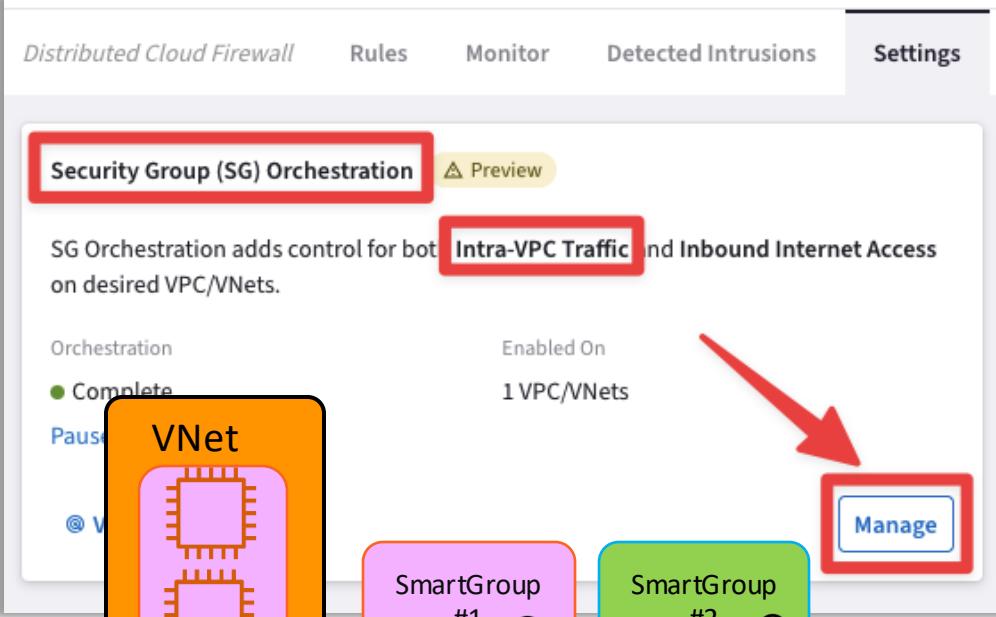


Caveat:

- 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

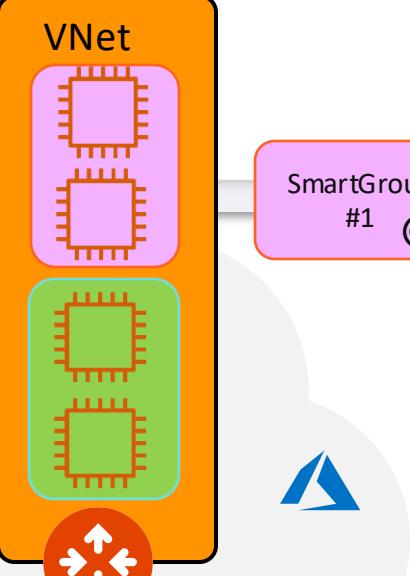
☐ Enable the feature on the relevant VPC/VNet



Orchestration

- Complete
- Pause
- ⋮ View

VNet



Enabled On
1 VPC/VNets

SmartGroup #1 ⚡

SmartGroup #2 ⚡

Manage

- 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

 aviatrix

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.

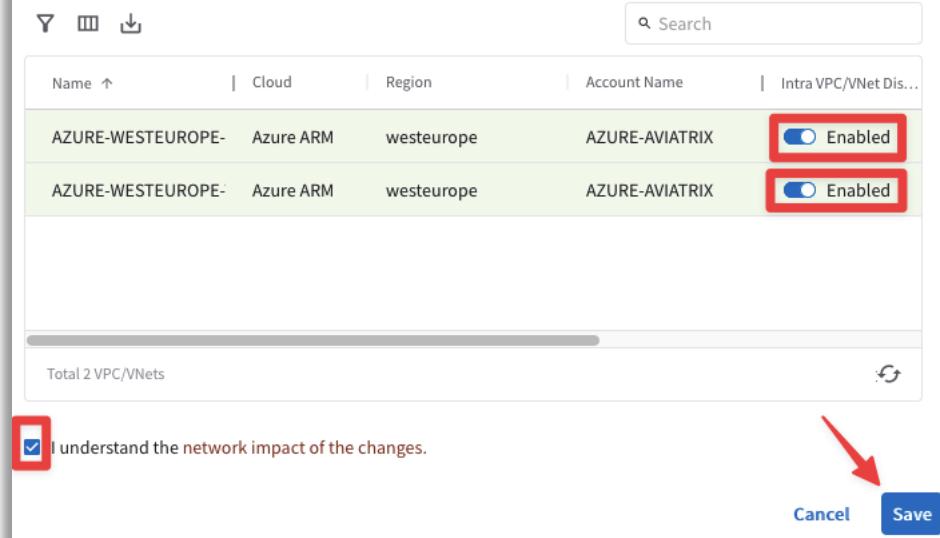
VPC/VNETs have to be enabled to support Intra VPC/VNet Distributed Firewalling.

Name	Cloud	Region	Account Name	Intra VPC/VNet Dis...
AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled
AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled

Total 2 VPC/VNets

I understand the **network impact** of the changes.

Cancel **Save**



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

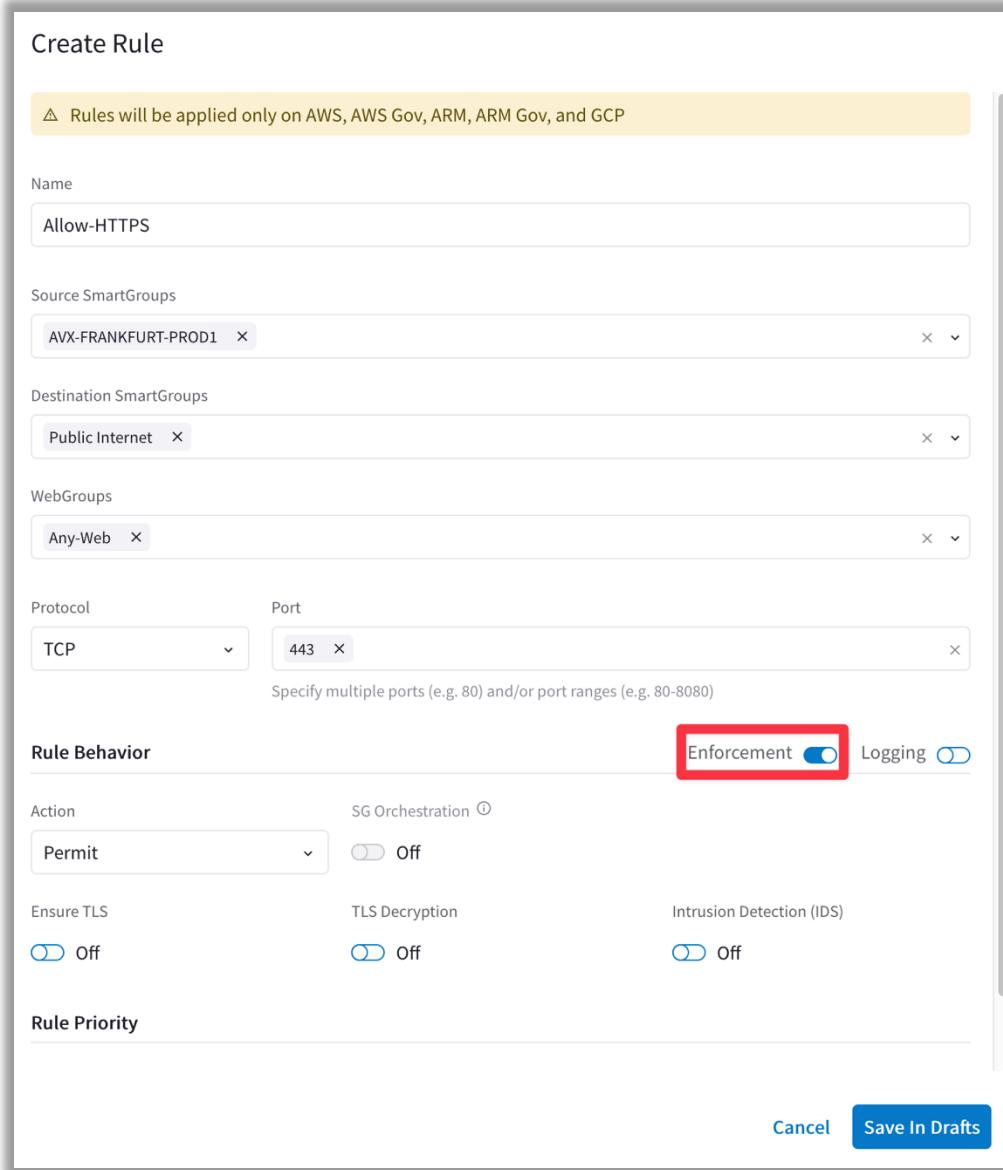
Rule Behavior: Enforcement Logging

Action: Permit SG Orchestration Off

Ensure TLS: Off TLS Decryption: Off Intrusion Detection (IDS): Off

Rule Priority

Cancel Save In Drafts



□ 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 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	
Action	Permit
Ensure TLS	Off
Rule Priority	
<input checked="" type="checkbox"/> Enforcement <input checked="" type="checkbox"/> Logging	
<input checked="" type="checkbox"/> SG Orchestration <small>①</small>	
<input checked="" type="checkbox"/> TLS Decryption	
<input checked="" type="checkbox"/> Intrusion Detection (IDS)	
<input checked="" type="checkbox"/> Save In Drafts	

Monitor

Auto Refresh

Search All Logs

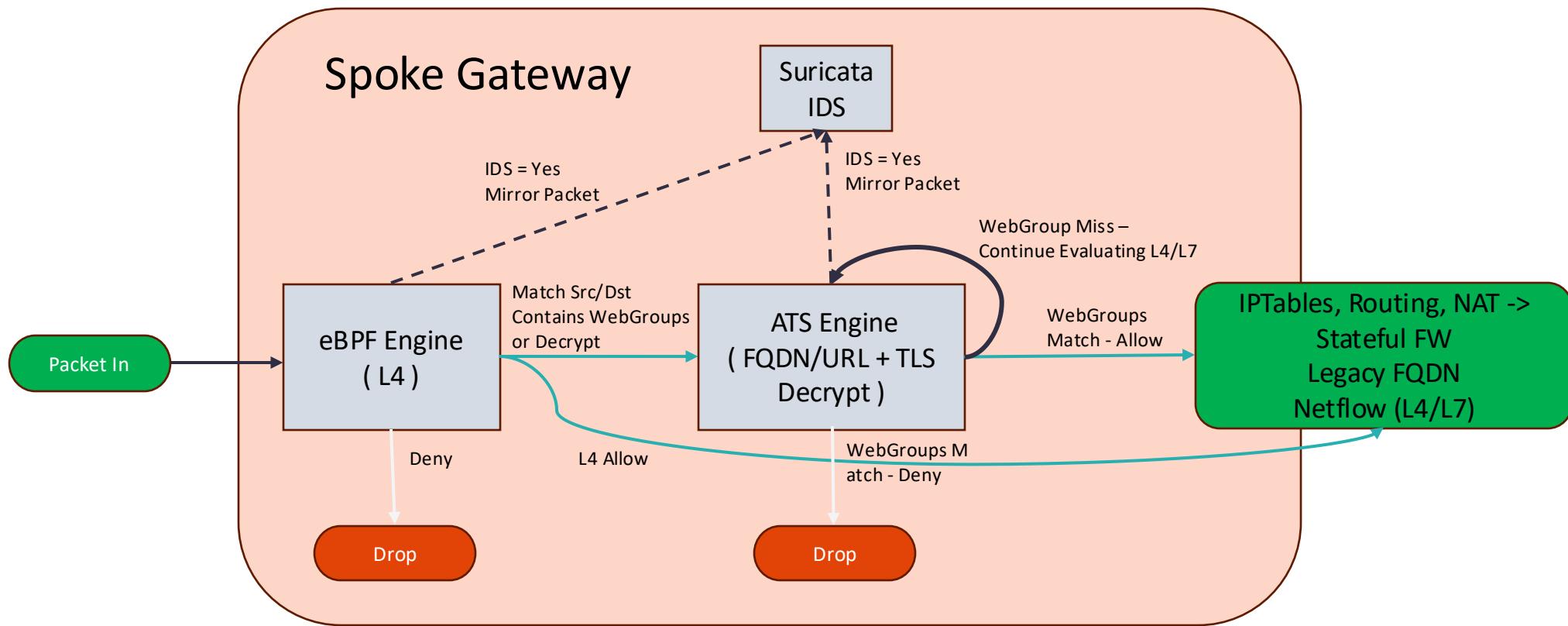
Timestamp	Rule	Source IP	Destination IP	URL	Protocol	Source Port	Destination Port	Action	Enforced
Mar 25, 2025 5:54:04 PM	default-deny-all	10.2.5.141	10.4.2.10		TCP	44324	3306	Deny	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.2.5.149	10.4.2.10		TCP	57200	3306	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https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