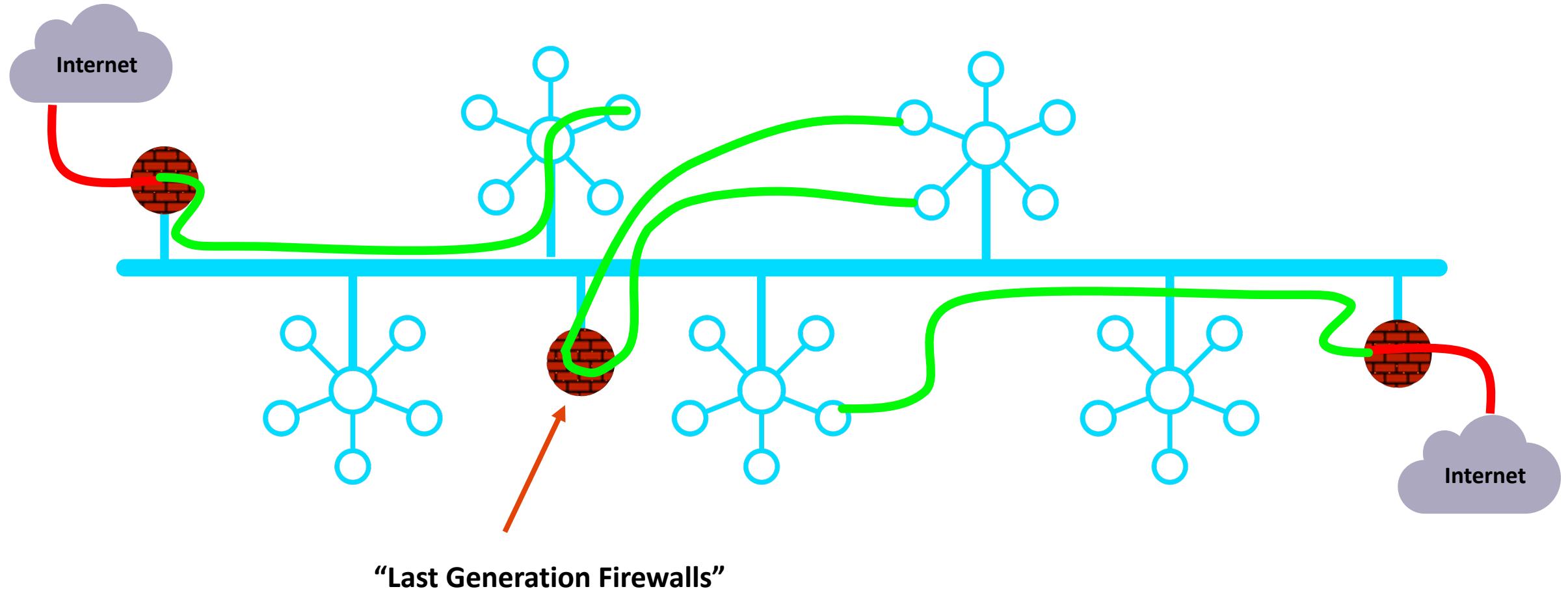




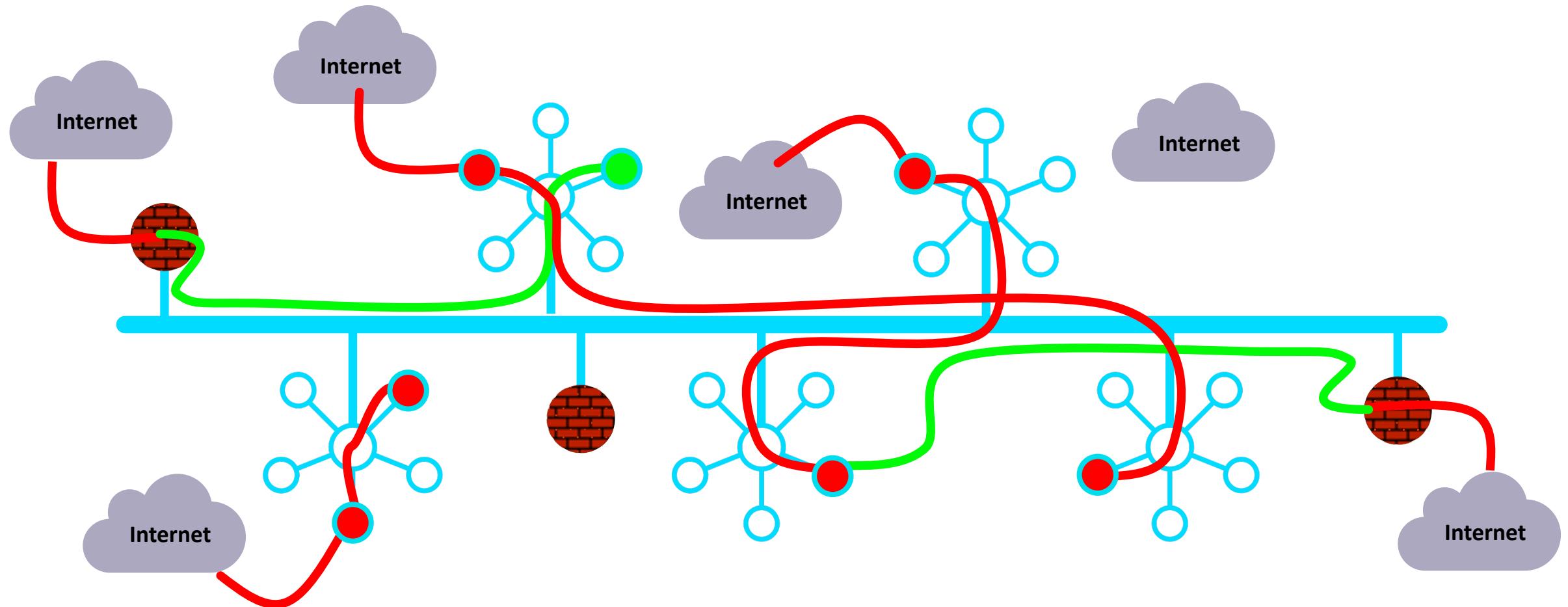
# Distributed Cloud Firewall

ACE Solutions Architecture Team

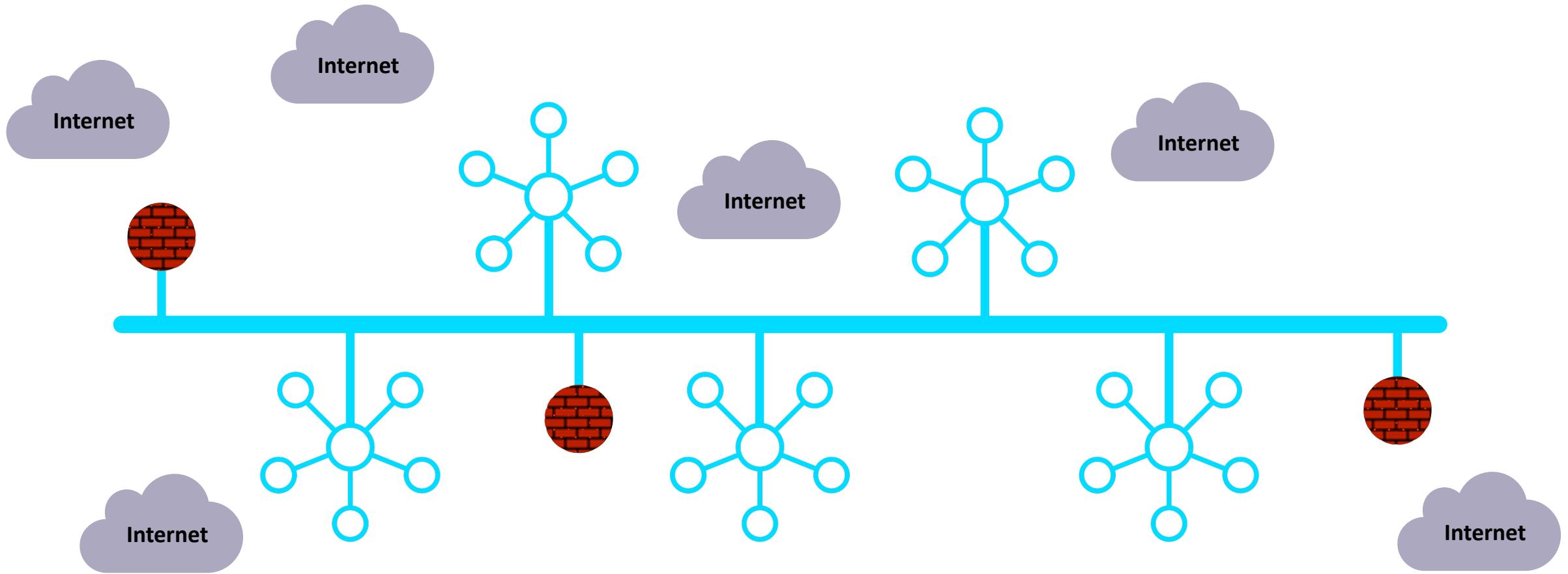
# As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



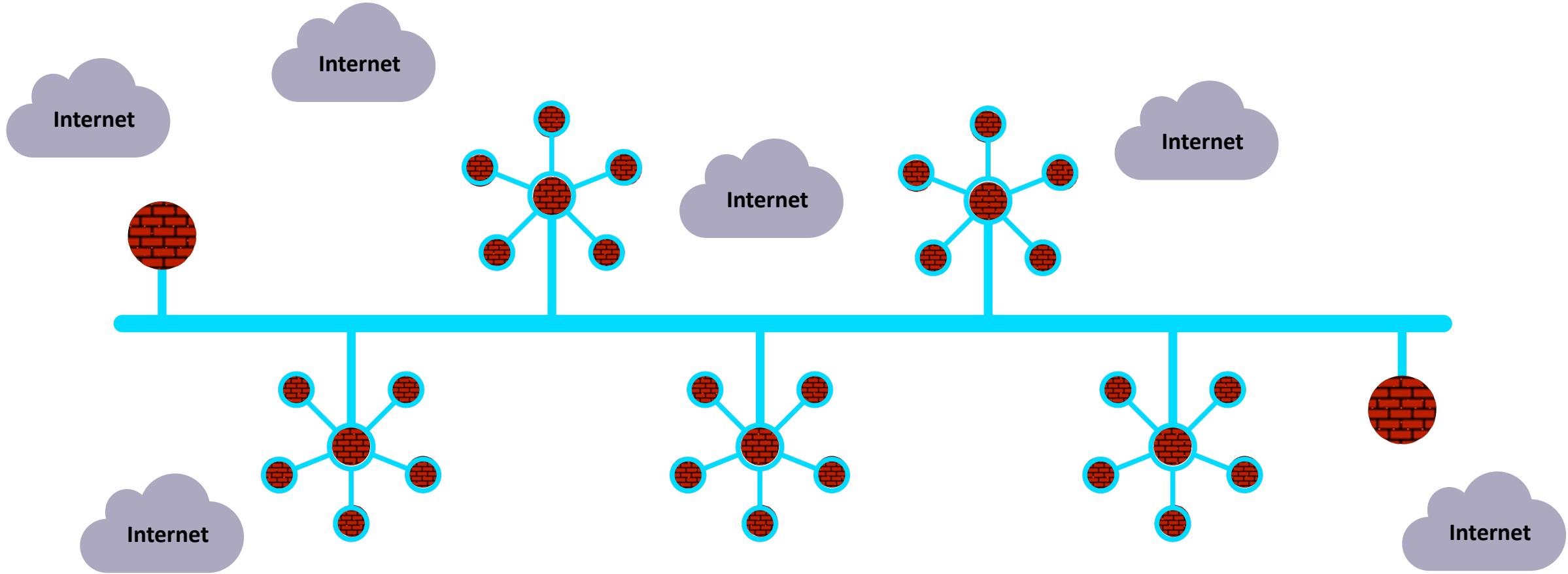
# In Reality...



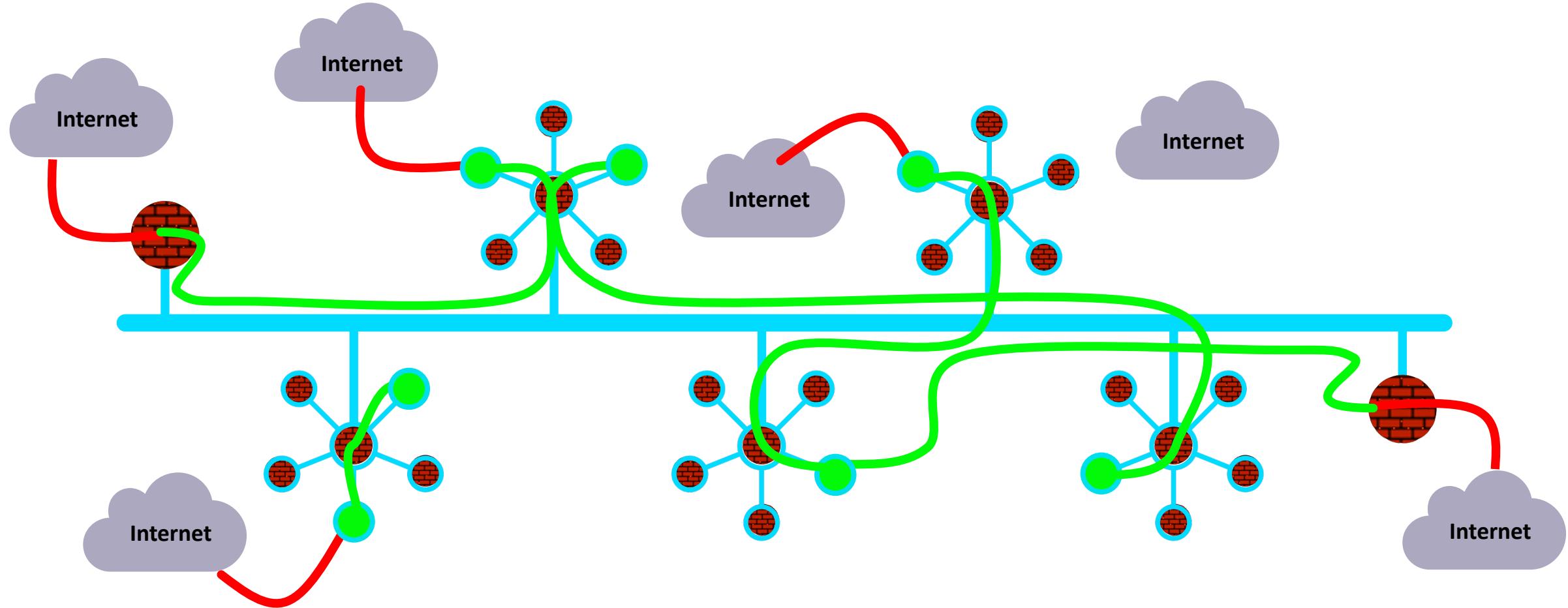
# What If... the architecture was built for cloud



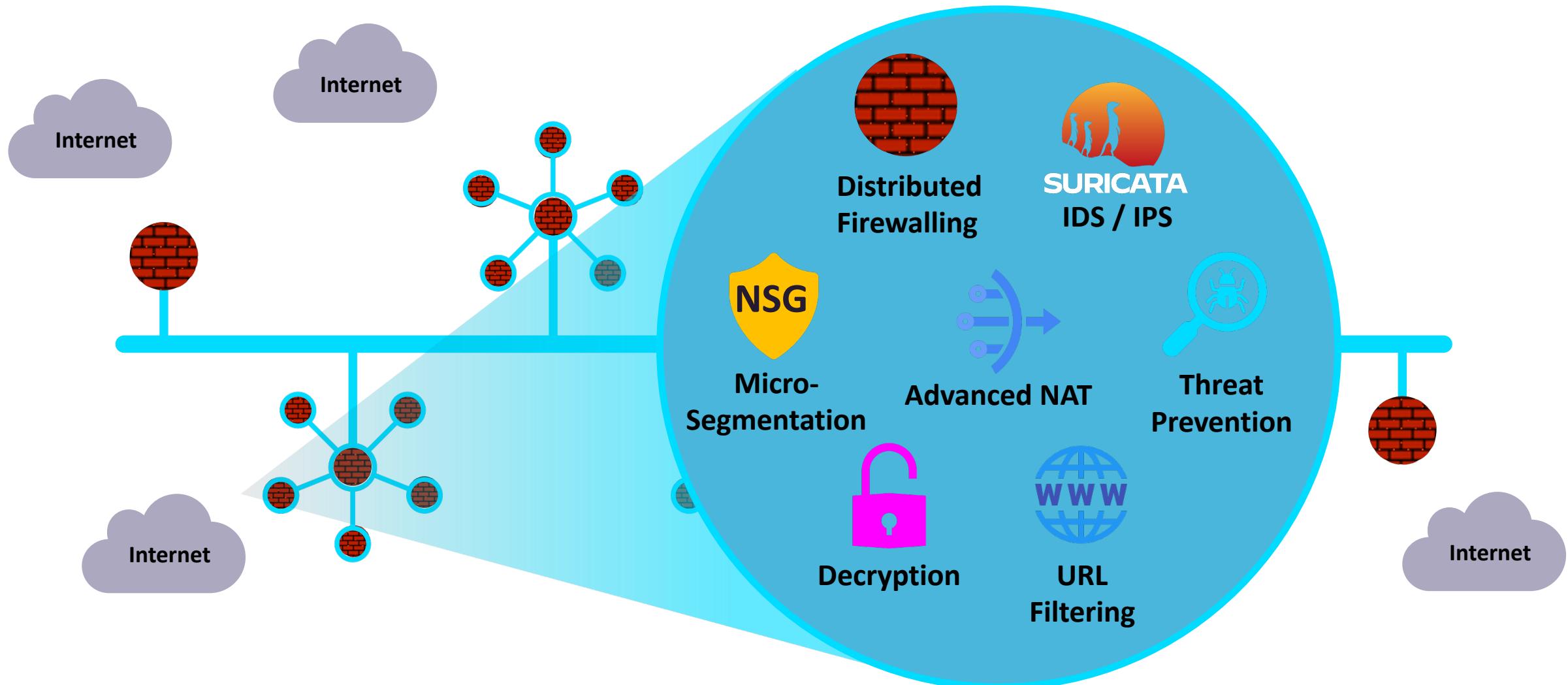
# Firewalling Functions were Embedded in the Cloud Network Everywhere...



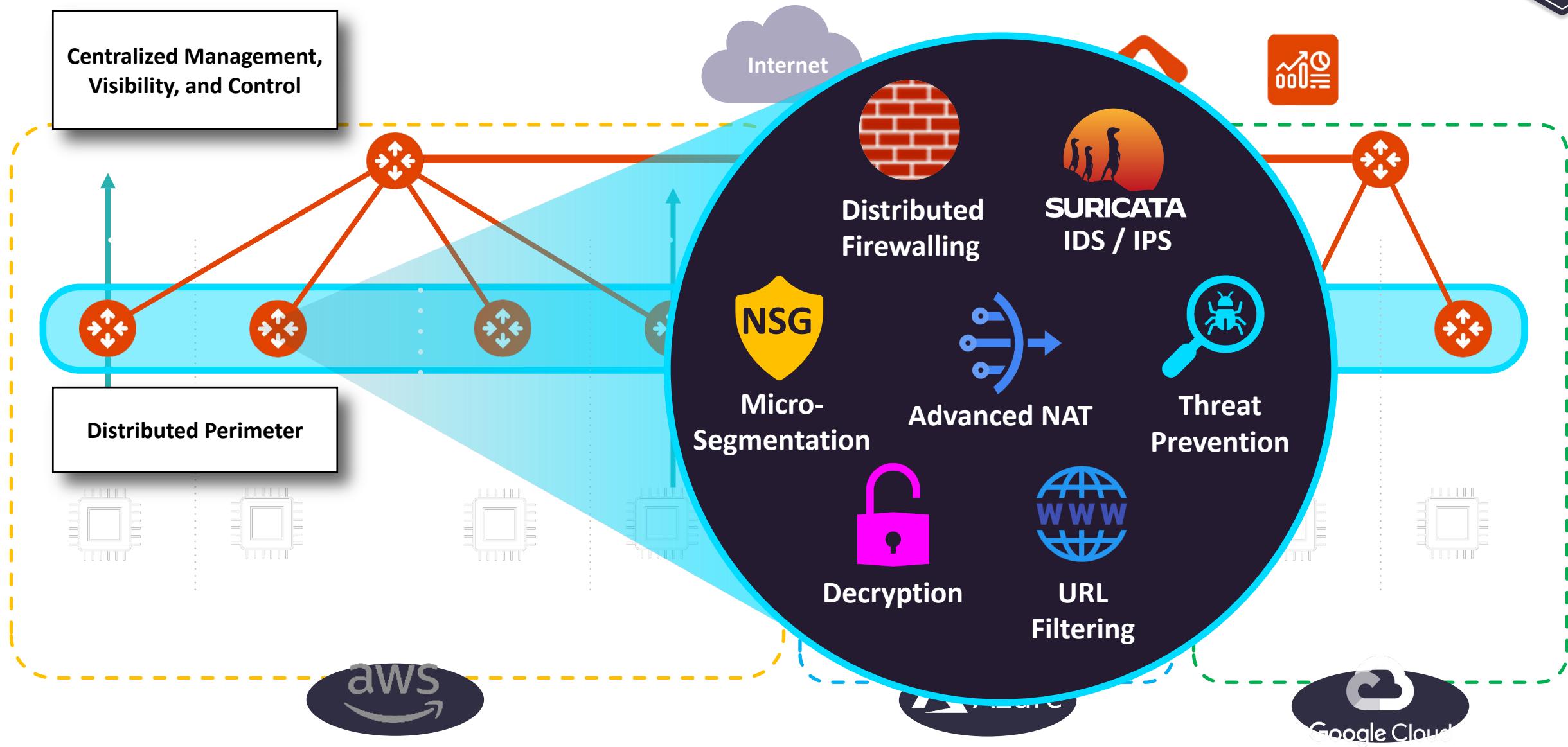
# Distribution of the Security Services into the Spokes



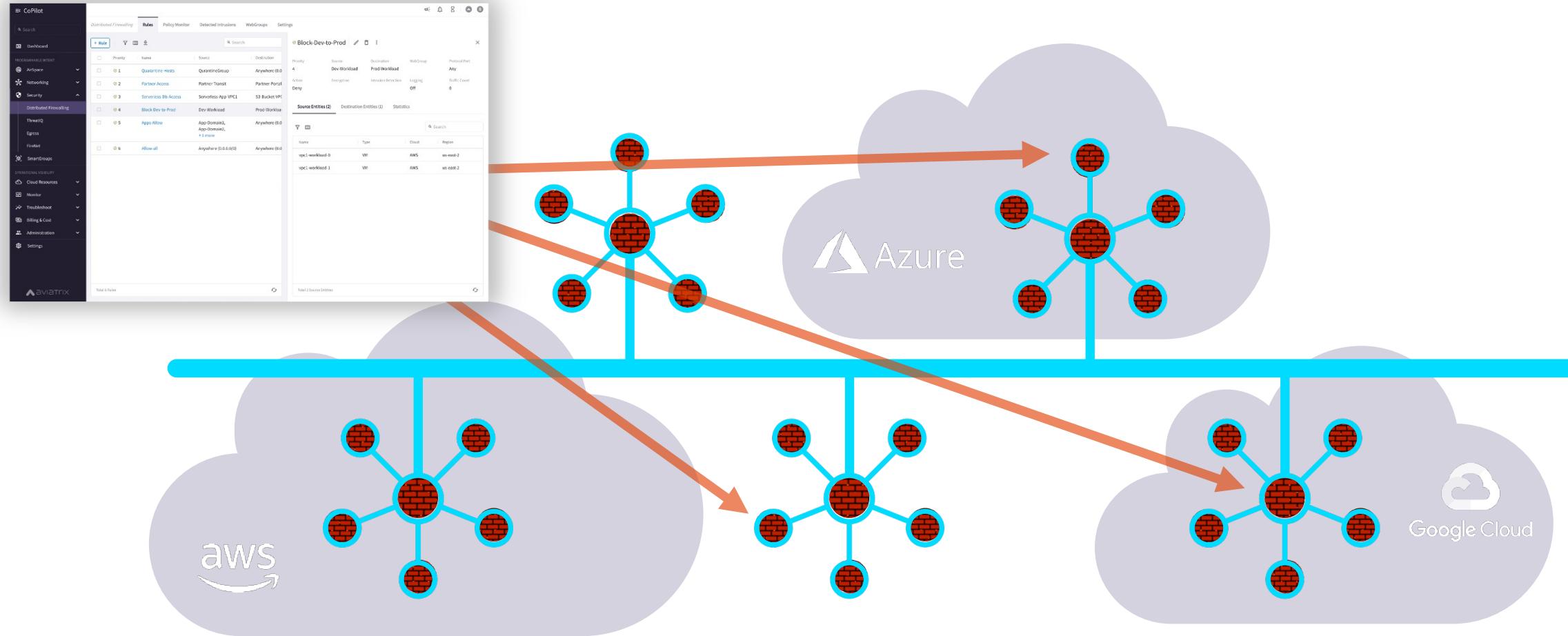
# And, What If it was more than just firewalling...



# Aviatrix Distributed Cloud Firewall



# 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:
  - **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 *three* methods:

- CSP Tags
- Resource Attributes
- CIDR



# SmartGroups: Classification Methods

## CSP Tags (recommended)

- Tags are assigned to:
  - Instance
  - VPC/VNET
  - Subnet
- Tags are {Key, Value} pairs
- Eg: A VM hosting shopping cart application can be tagged with:
  - {Key: Type, Value: Shopping cart app}
  - {Key: Env, Value: Staging}

Instance: i-0380038ff7d66b66f (shopping cart app)

Select an instance above

Details | Security | Networking | Storage | Status checks | Monitoring | **Tags**

Tags	
<input type="text"/>	
Key	Value
Env	Staging
Name	shopping cart app

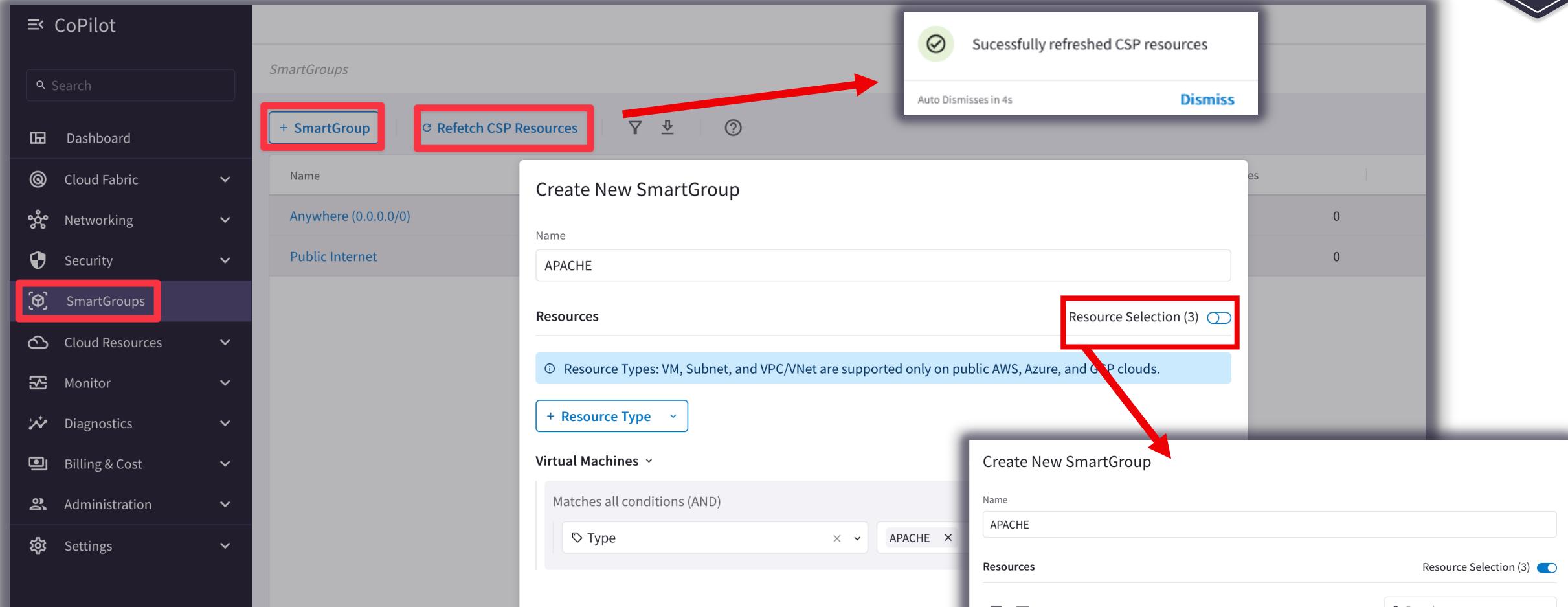
## Resource attribute

- Region Name, Account Name

## IP Prefixes

- CIDR

# SmartGroups Creation



The screenshot shows the Aviatrix CoPilot interface with the 'SmartGroups' menu item highlighted. The 'Create New SmartGroup' dialog is open, showing the name 'APACHE' and three selected resources. A success message at the top right indicates 'Successfully refreshed CSP resources'.

**SmartGroup Creation Steps:**

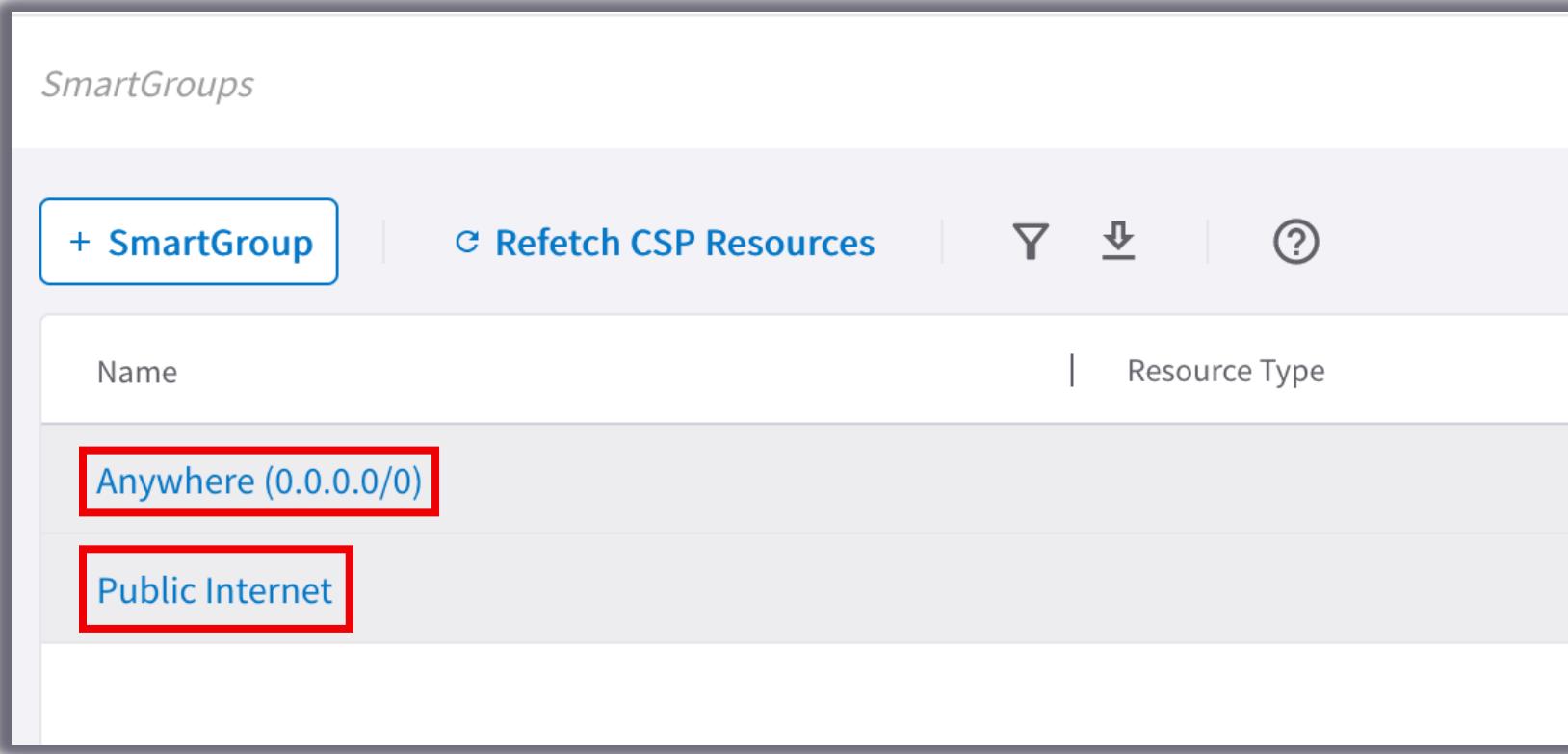
- Click on the '+ SmartGroup' button.
- Click on the 'Resource Selection (3)' toggle switch.

**SmartGroup Details:**

Name	Type	Cloud	Region
PROD1-APACHE	VM	AWS	eu-central-1
PROD2-APACHE	VM	AWS	eu-central-1
prod3-apache	VM	Azure ARM	westeurope

- 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 SmartGroups



The screenshot shows a user interface for managing SmartGroups. The title bar says "SmartGroups". Below it is a toolbar with a "+ SmartGroup" button (which is highlighted with a red border), a "Refetch CSP Resources" button, and other icons for search, sort, and help. The main area has two columns: "Name" and "Resource Type". There are two entries: "Anywhere (0.0.0.0/0)" and "Public Internet", both of which are also highlighted with red borders.

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



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.

[Manage Add-on Features](#) [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.

Distributed Cloud Firewall		Rules	Monitor	Detected Intrusions	WebGroups	Settings	
<a href="#">+ Rule</a>   <a href="#">Actions</a> ▾							
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
<input type="checkbox"/>	21474... <a href="#">Greenfield-Rule</a>	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit

# 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

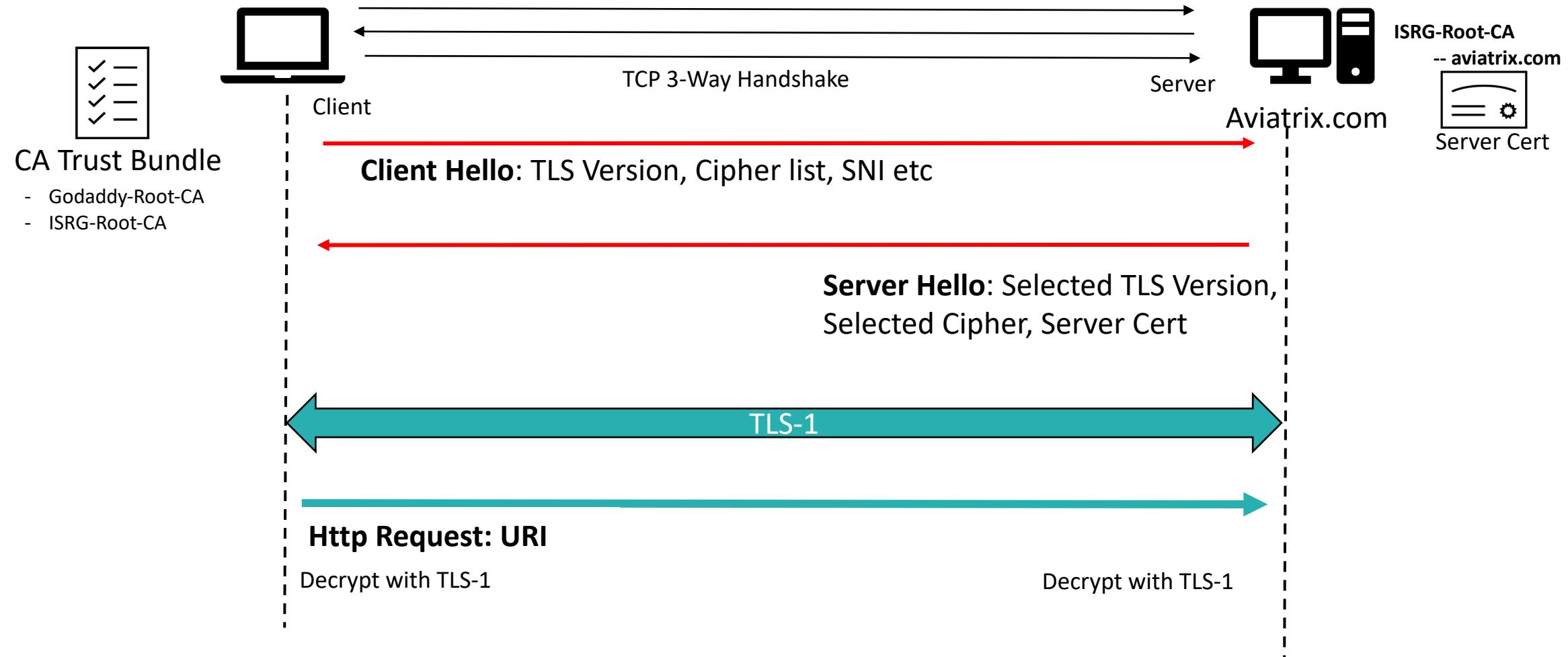
Enforcement  Logging

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

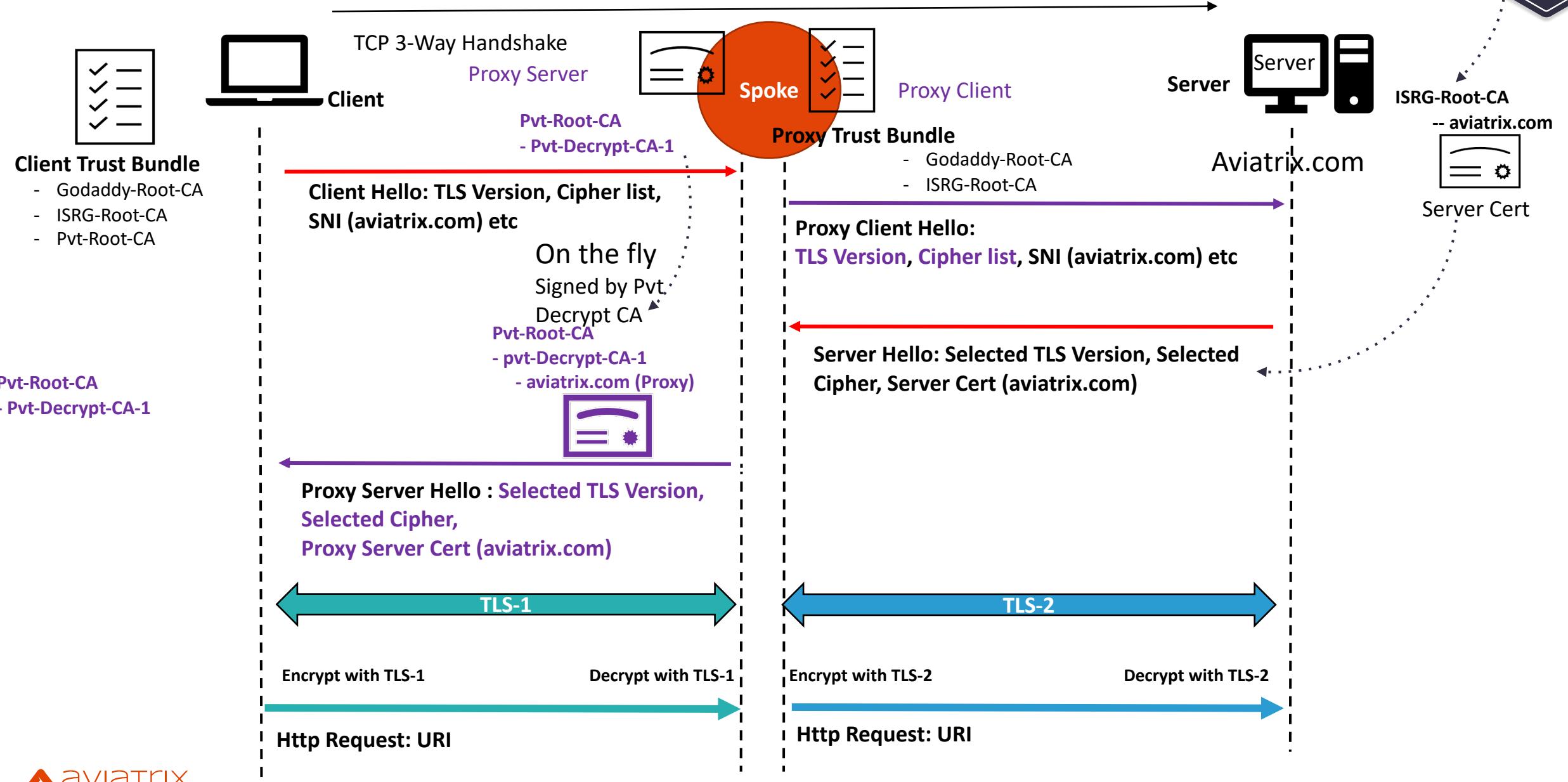
## Decryption CA Cert

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**

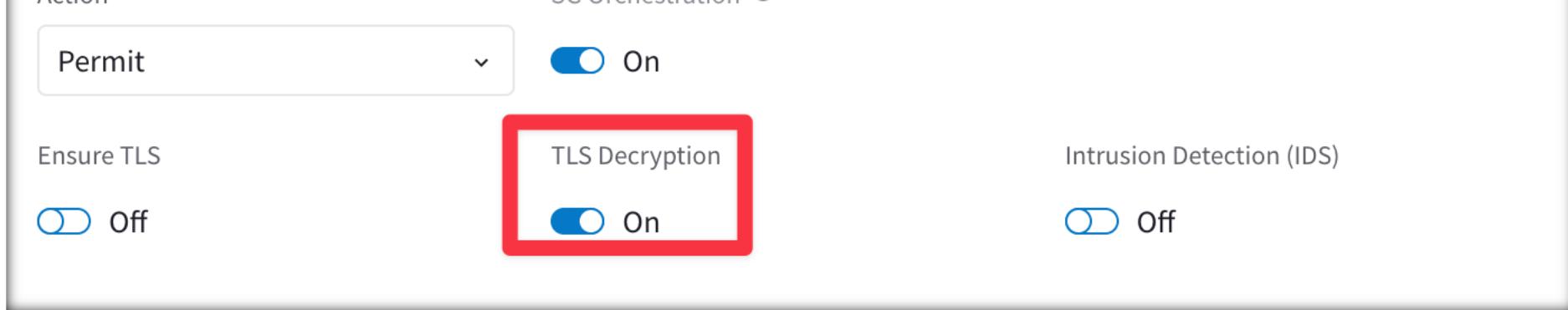
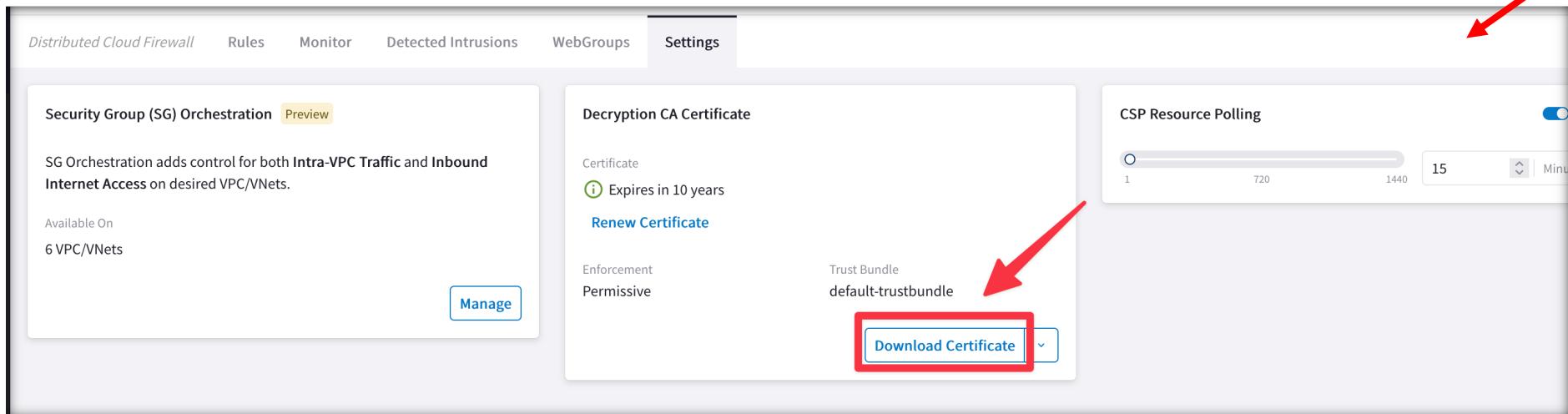
General	Details
<b>Certificate Hierarchy</b>	
ISRG Root X1	
R3	
aviatrix.com	
<b>Certificate Fields</b>	
Certificate	
Version	
Serial Number	
Certificate Signature Algorithm	
Issuer	
Validity	
Subject	
Subject Public Key Info	
<b>Field Value</b>	
CN = aviatrix.com	

# 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.

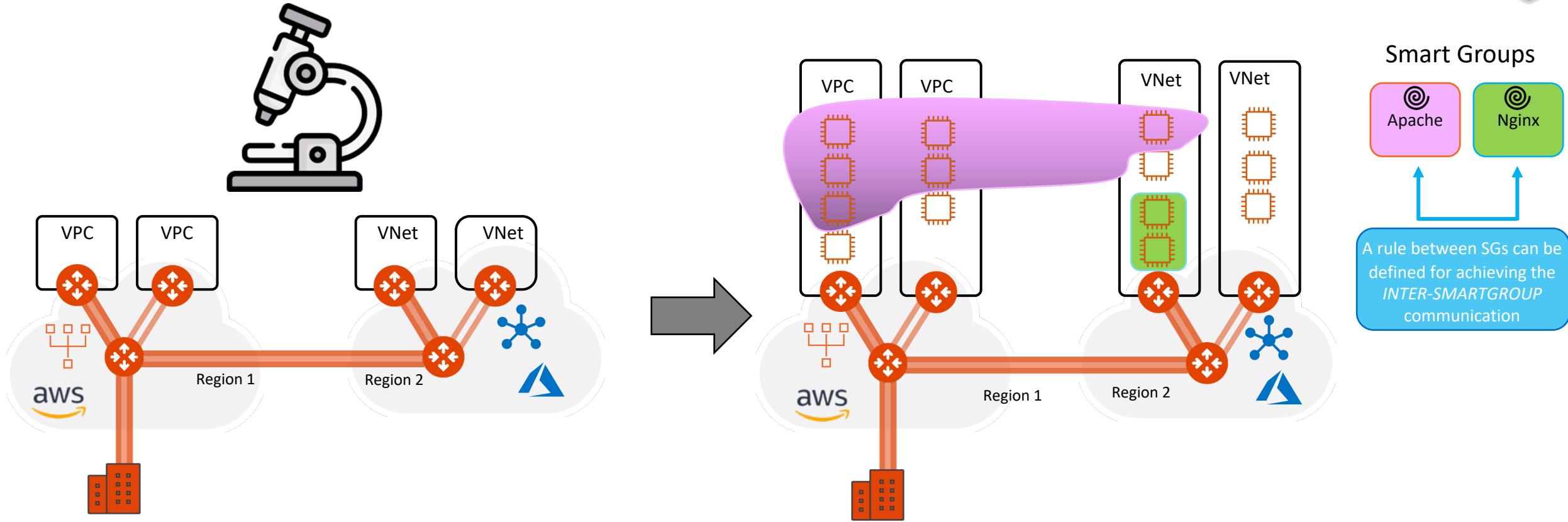



The screenshot shows the 'Settings' tab of the Distributed Cloud Firewall. In the 'Decryption CA Certificate' section, the 'Download Certificate' button is highlighted with a red box and arrow. The 'Trust Bundle' dropdown shows 'default-trustbundle'. Other sections visible include 'Security Group (SG) Orchestration' and 'CSP Resource Polling'.

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

**SmartGroup Apache**

**SmartGroup Nginx**

**SmartGroup Nginx** → **SmartGroup Apache**

**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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: Off

Logging: On

Cancel Save In Drafts

**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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: Off

Logging: On

Cancel Save In Drafts

**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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: Off

Logging: On

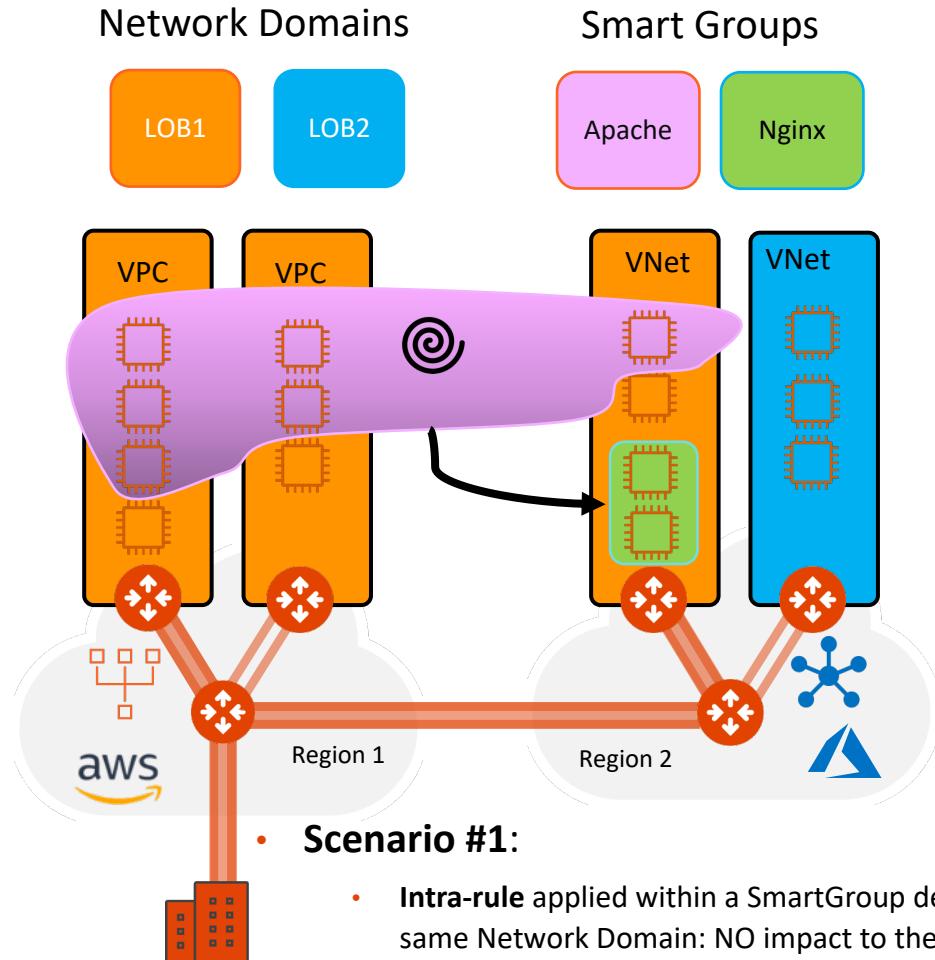
Cancel Save In Drafts

Distributed Cloud Firewall							
Rules		Monitor		Detected Intrusions		WebGroups	
+ Rule	Actions	Y	Y	4 New	1 Modified	Discard	Commit
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
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

20

# Network Segmentation & Distributed Cloud Firewall Rule together

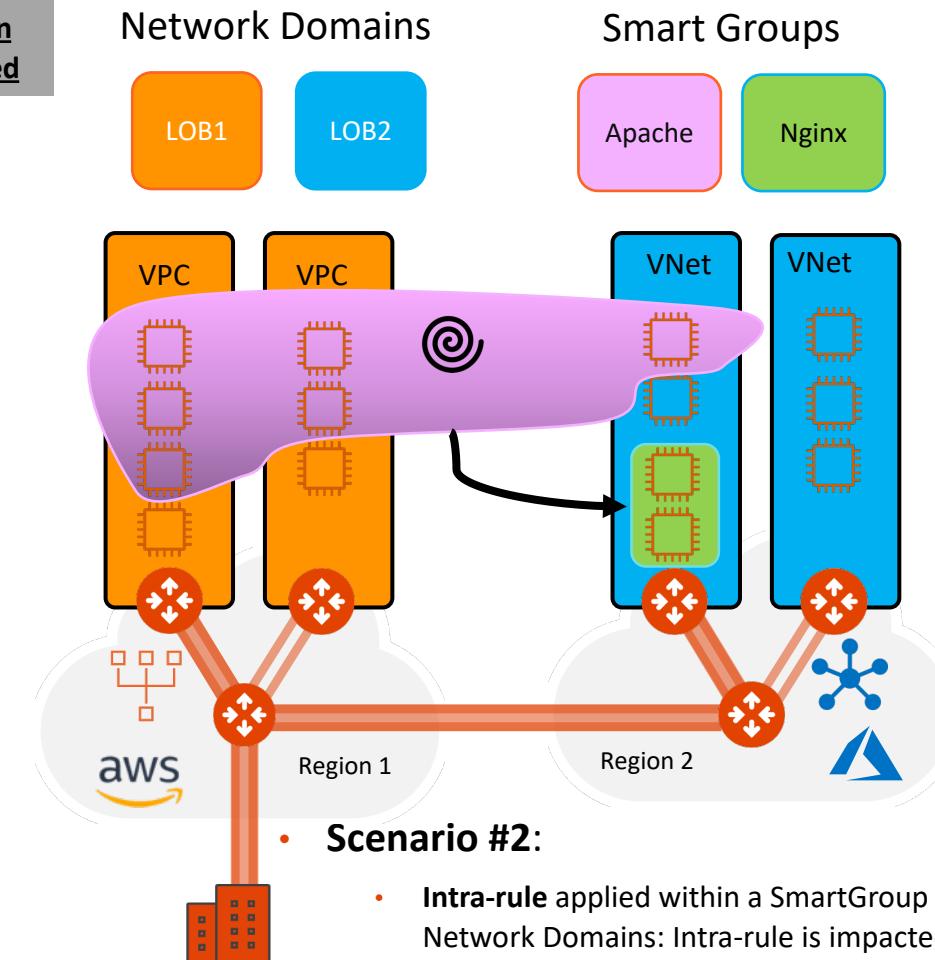


- Scenario #1:

- **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

*Caveat:*

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

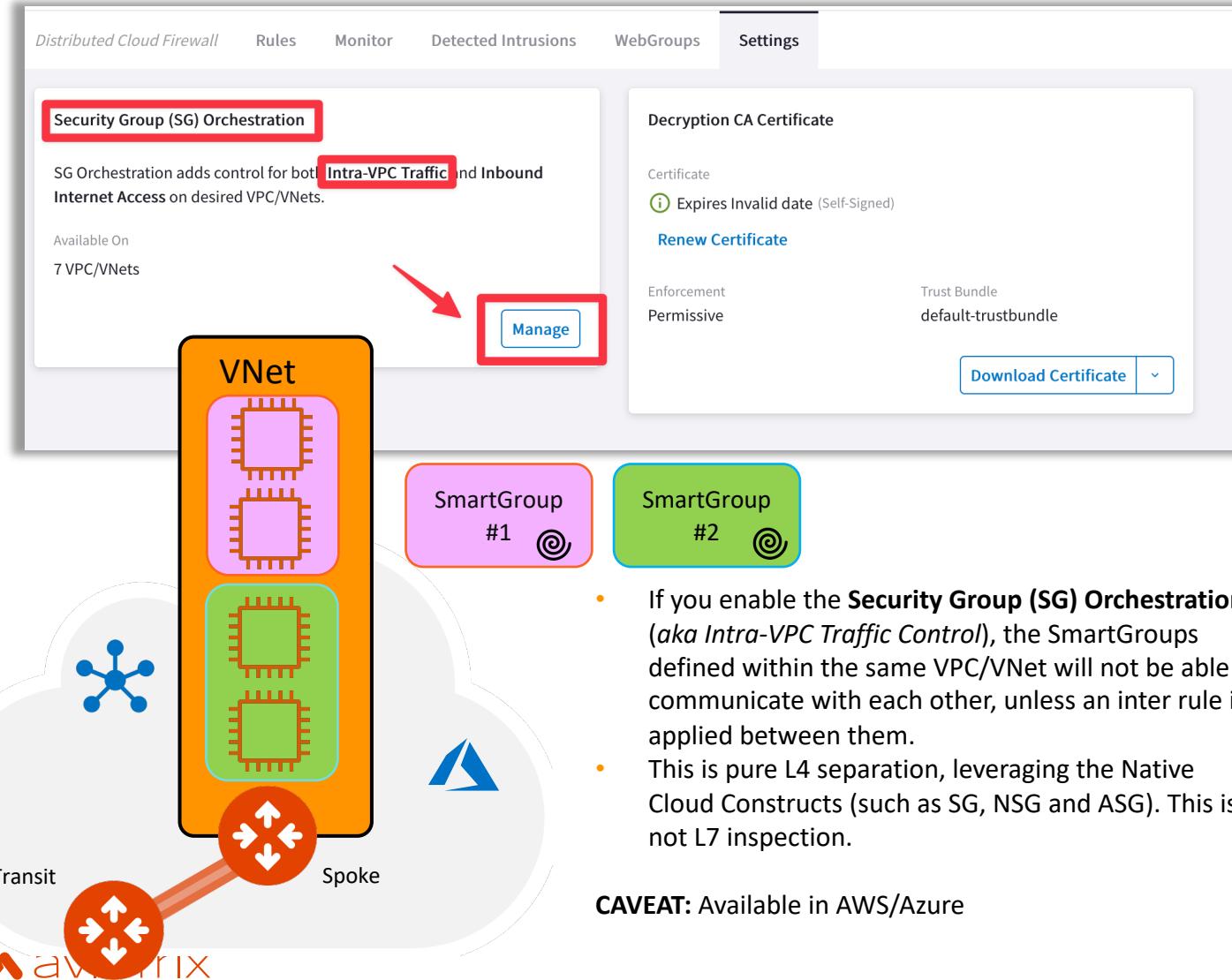


- Scenario #2:

- **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

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

## ☐ Enable the feature on the relevant VPC/VNet



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

**Security Group (SG) Orchestration**

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

Available On 7 VPC/VNets

VNet

SmartGroup #1

SmartGroup #2

Transit Spoke

**CAVEAT:** Available in AWS/Azure

Decryption CA Certificate

Certificate Expires Invalid date (Self-Signed)

**Renew Certificate**

Enforcement **Permissive**

Trust Bundle default-trustbundle

**Download Certificate**

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**.

⚠ 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	<b>Enabled</b>
AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<b>Enabled</b>

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 SG Orchestration: Off

Ensure TLS: Off TLS Decryption: Off

Intrusion Detection (IDS): Off

Enforcement  Logging

Cancel Save In Drafts

Policy Monitor

Auto Refresh  Search

Showing all 20 logs

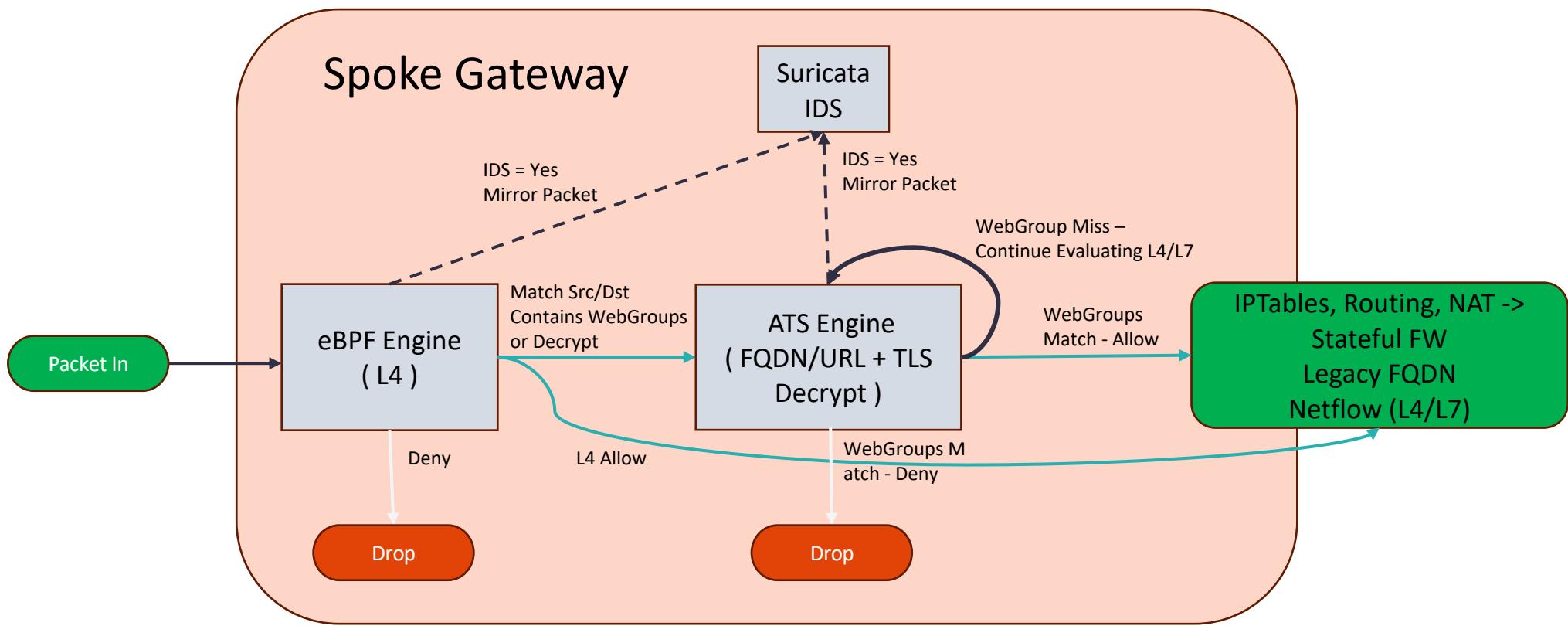
Timestamp	Rule	Source SmartGroup	Destination SmartGroup	Source IP	Destination IP	Protocol	Source Port	Destination Port	Action	Enforcing
2023-04-14 09:16:16.006 PM	intra-ssh-bu1	bu1	bu1	192.168.1.100	10.0.1.100	TCP	22	52106	PERMIT	✓
2023-04-14 09:16:15.824 PM	allow-ssh-myip-bu1	bu1	local-machine	10.0.1.100	31.164.145.177	TCP	22	53342	PERMIT	✓
2023-04-14 09:16:15.584 PM	allow-ssh-myip-bu1	local-machine	bu1	31.164.145.177	10.0.1.100	TCP	53342	22	PERMIT	✓
2023-04-14 09:16:15.461 PM	allow-ssh-myip-bu1	bu1	local-machine	10.0.1.100	31.164.145.177	TCP	22	53342	PERMIT	✓
2023-04-14 09:16:15.378 PM	allow-ssh-myip-bu1	local-machine	bu1	31.164.145.177	10.0.1.100	TCP	53342	22	PERMIT	✓
2023-04-14 09:16:15.349 PM	intra-ssh-bu1	bu1	bu1	10.0.1.100	192.168.1.100	TCP	52106	22	PERMIT	✓
2023-04-14 09:14:50.602 PM	allow-ssh-myip-bu1	local-machine	bu1	31.164.145.177	10.0.1.100	TCP	53342	22	PERMIT	✓

❑ 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)





# 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
Overlapping IPs are supported				x	x
<a href="#">Security Group Orchestration</a> is supported				x (Azure)	x (AWS and Azure)



Next: Lab 10 – Distributed Cloud Firewall