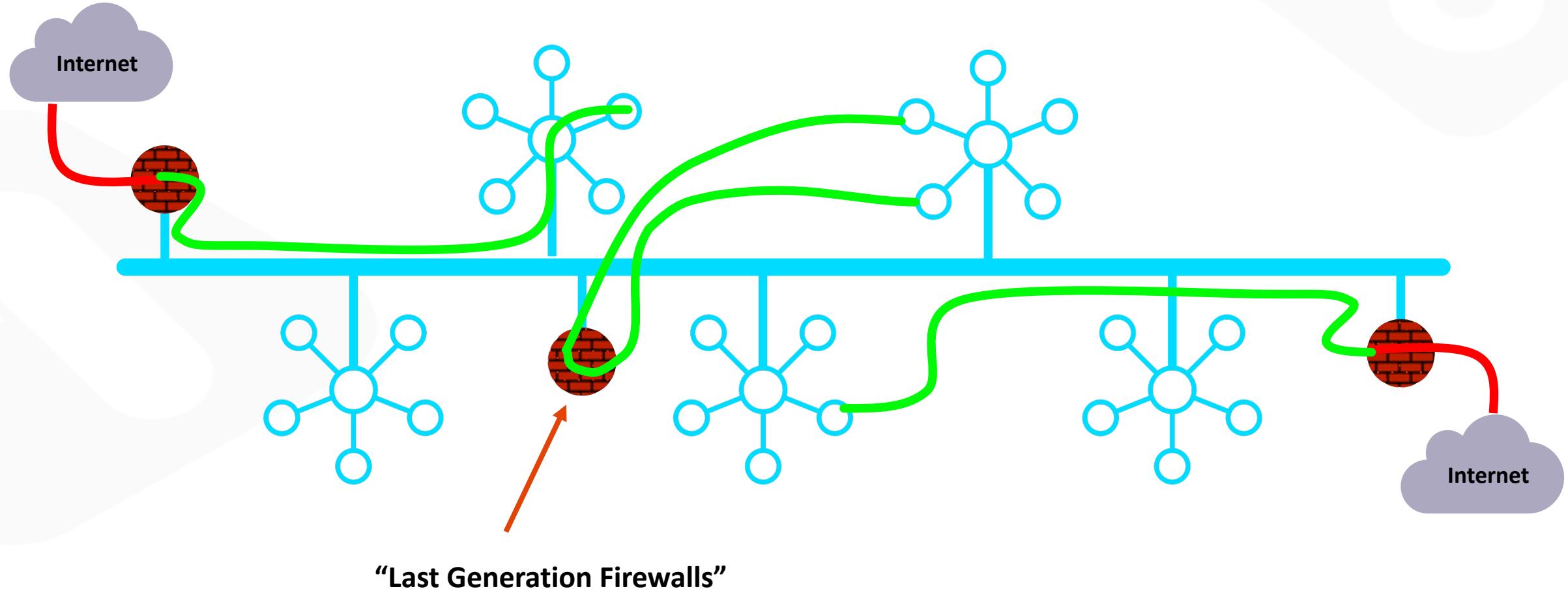


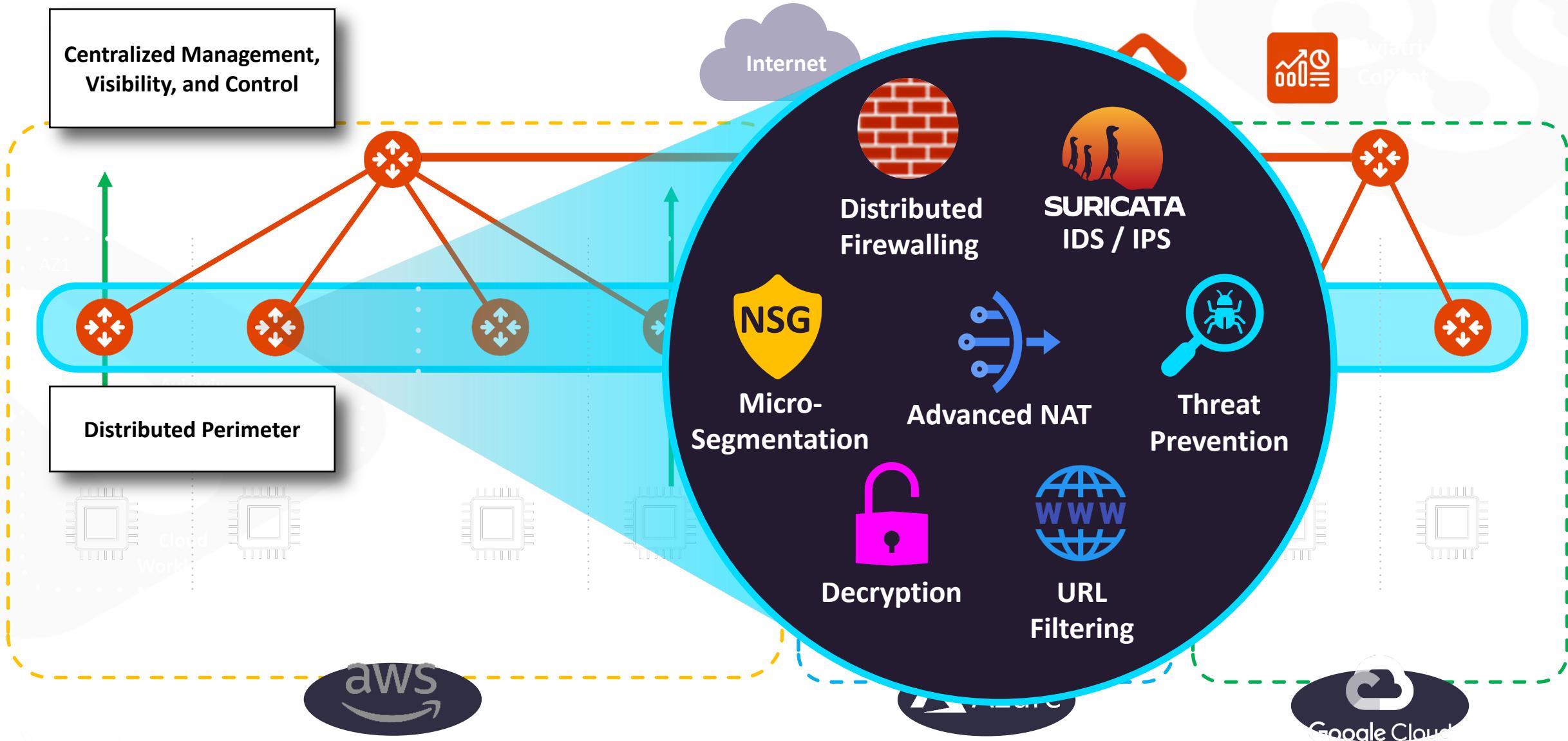


Distributed Cloud Firewall

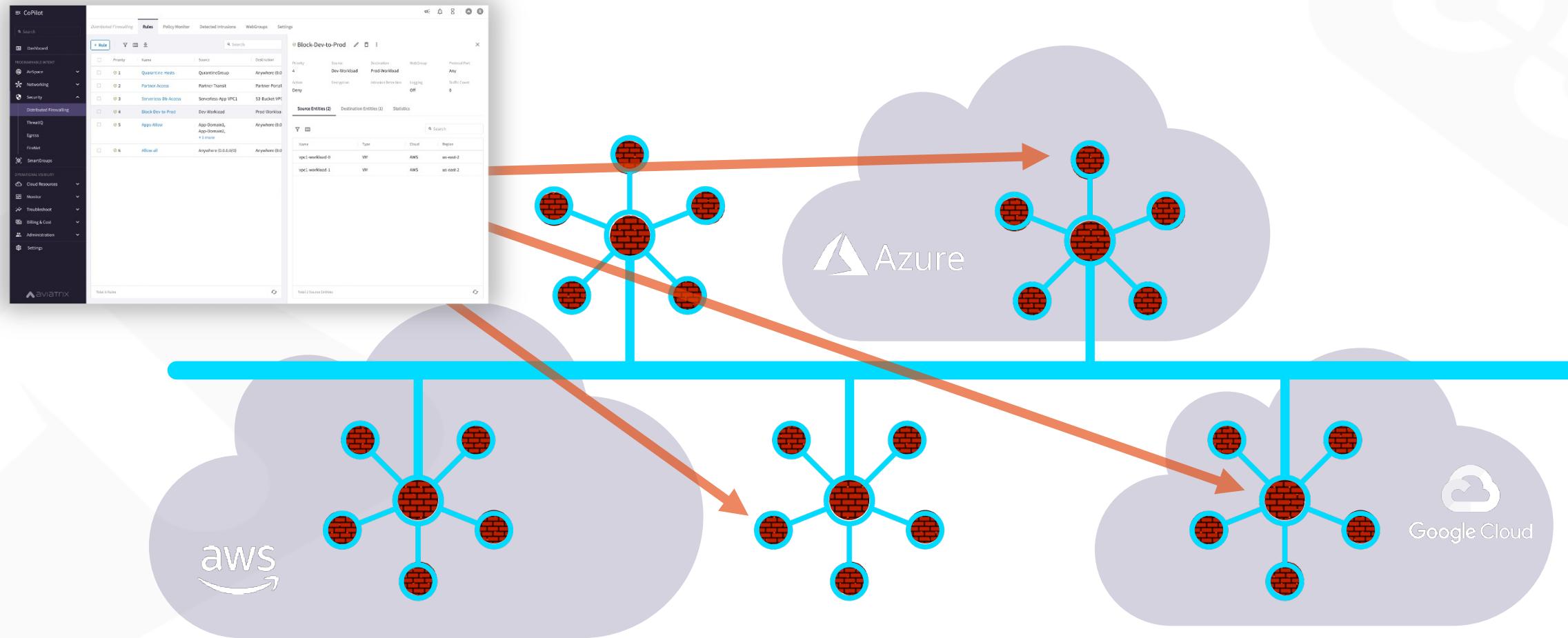
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



Aviatrix Distributed Cloud Firewall



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



Where and How Policies Are Enforced Is Abstracted...

SmartGroup: Definition

- A firewall rule consists of two important initial elements:

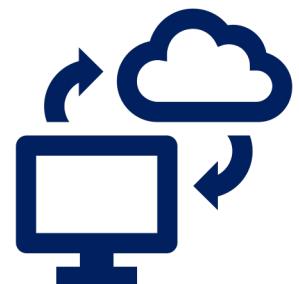
- **Source**
 - **Destination**

- **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. On the left, the navigation bar includes 'CoPilot' and a search bar, followed by a list of categories: Dashboard, Cloud Fabric, Networking, Security, SmartGroups (highlighted with a red box), Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The 'SmartGroups' section contains two buttons: '+ SmartGroup' and 'Refetch CSP Resources' (also highlighted with a red box). A large central window displays the 'Create New SmartGroup' dialog. The 'Name' field is set to 'APACHE'. Under the 'Resources' section, there is a 'Resource Selection (3)' button (also highlighted with a red box). A note below states: 'Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.' At the bottom of the dialog, there is a 'Virtual Machines' dropdown set to 'Matches all conditions (AND)' and a 'Type' filter set to 'APACHE'. To the right of the dialog, a success message box says 'Successfully refreshed CSP resources' with a 'Dismiss' button. Below the dialog, a preview window shows the list of selected resources: PROD1-APACHE, PROD2-APACHE, and prod3-apache.

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

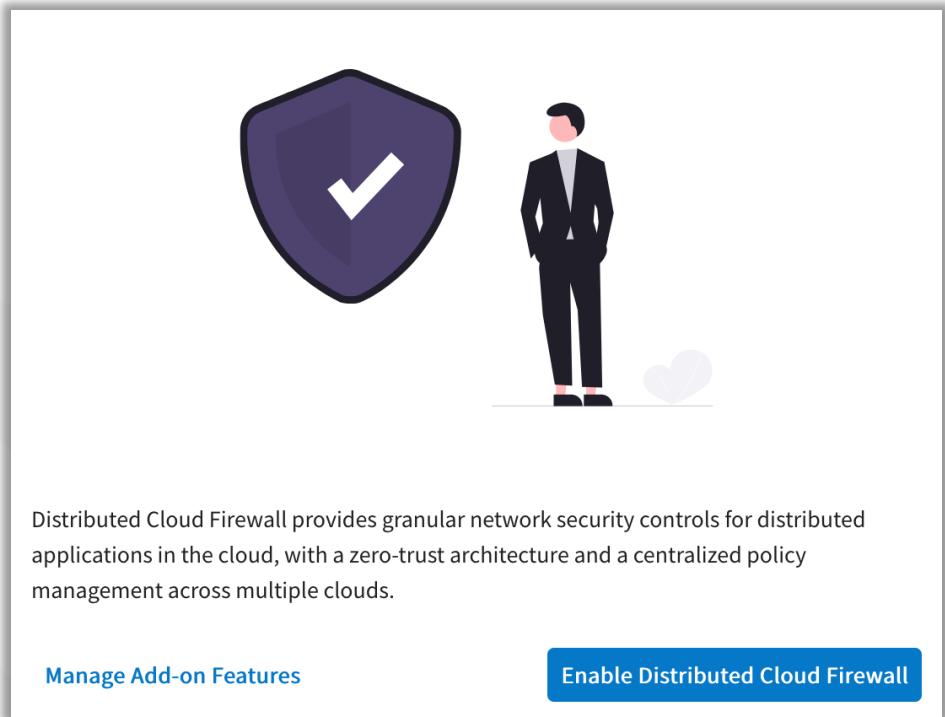
Pre-defined SmartGroups

The screenshot shows a user interface for managing SmartGroups. At the top left, it says "SmartGroups". Below the title are several buttons: "+ SmartGroup" (highlighted with a red border), "⟳ Refetch CSP Resources", a refresh icon, a download icon, and a help icon. 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 highlighted with red boxes.

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.



DENY LIST MODEL (THREAT-CENTRIC MODEL):

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

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

The Greenfield-Rule

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

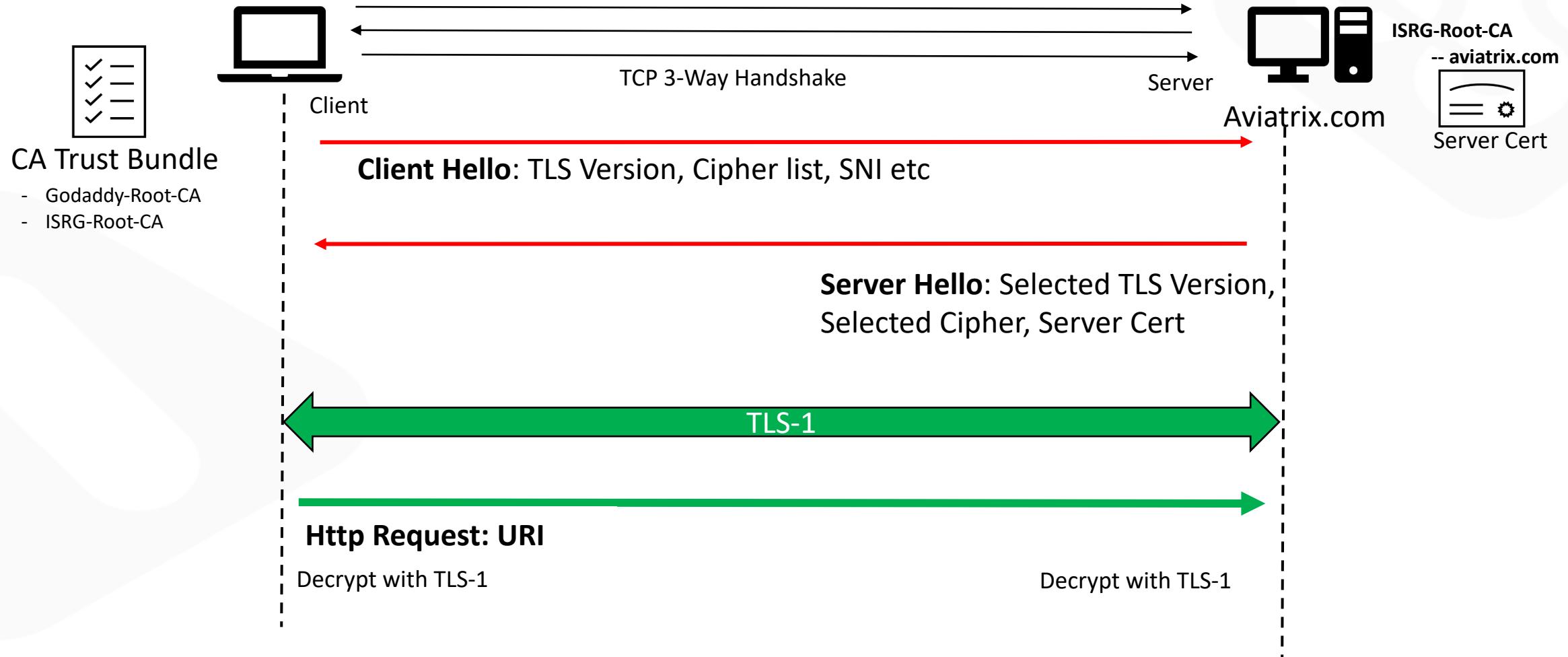
Enforcement Logging

Rule Priority

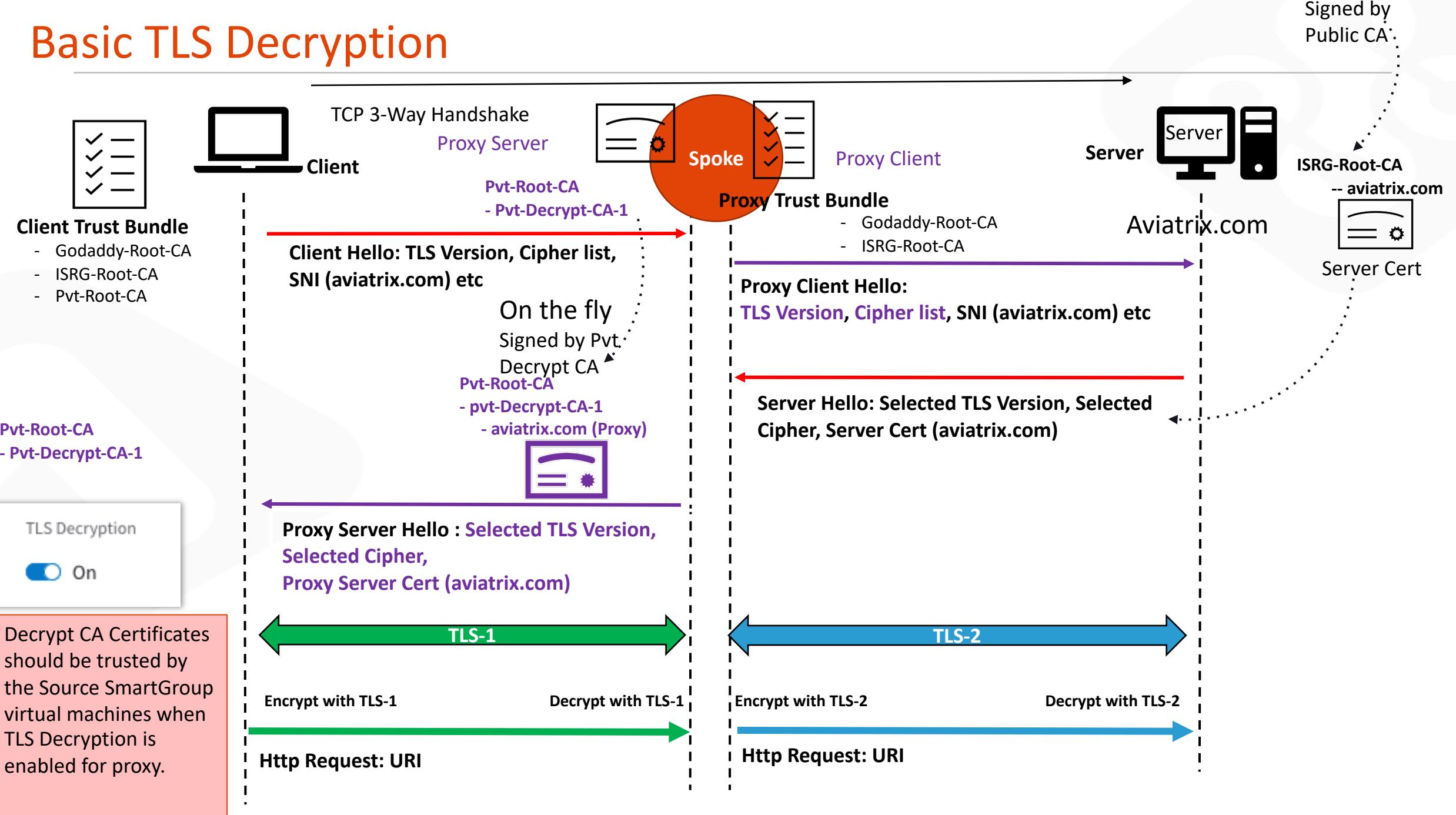
Cancel

- **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
- Customer would get an easy click button to create a greenfield rule, because by product design Zero trust is enforced with Deny-all at the end

Basic TLS Connection

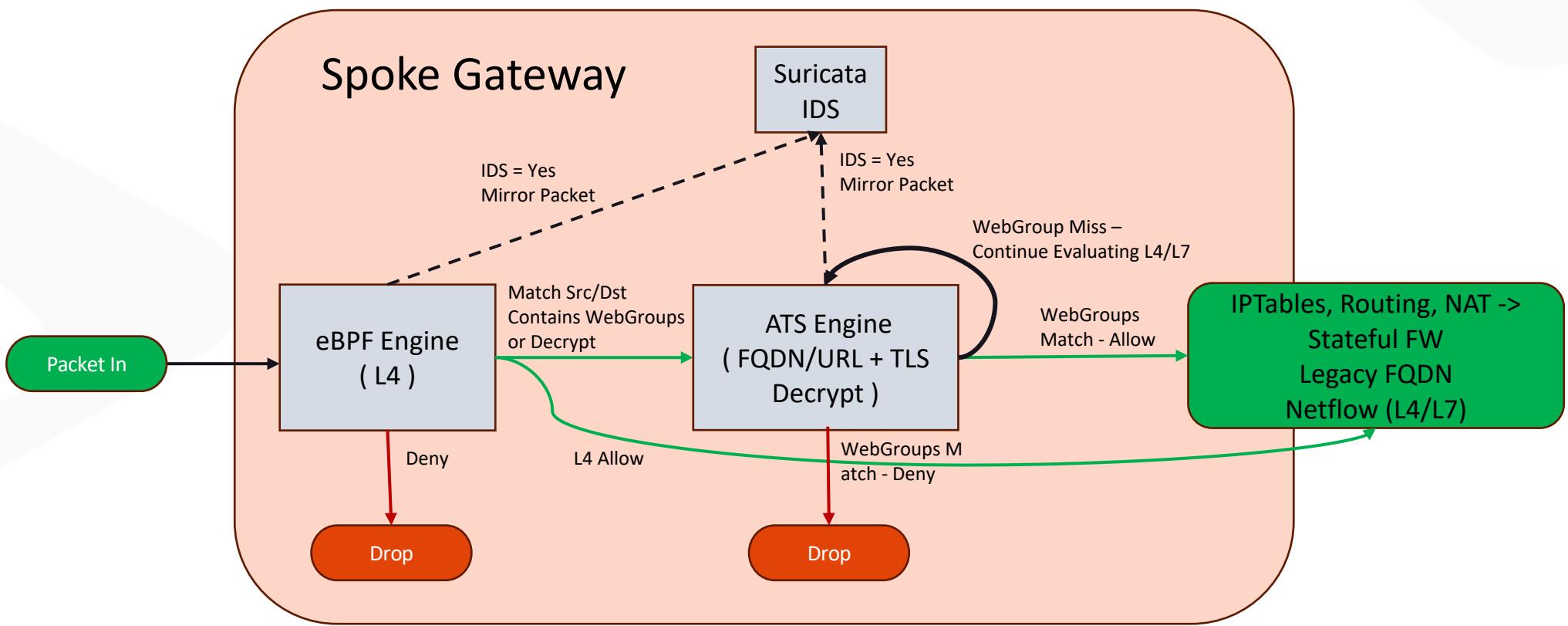


Basic TLS Decryption

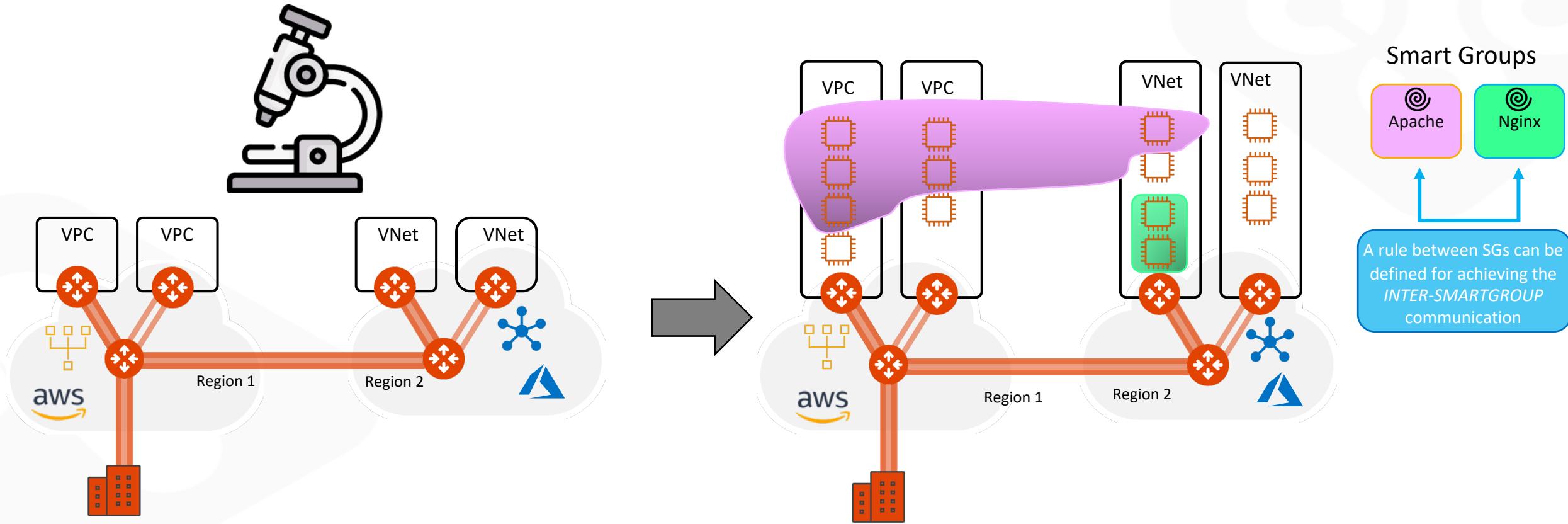


DFW Engines At-a-Glance

- **eBPF** (extended Berkeley Packet Filter) Engine (L4)
- WebProxy **ATS** (Apache Traffic Server) Engine (L7)
- **Suricata** Engine (DPI)



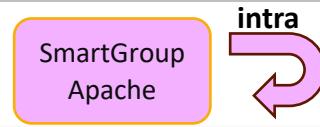
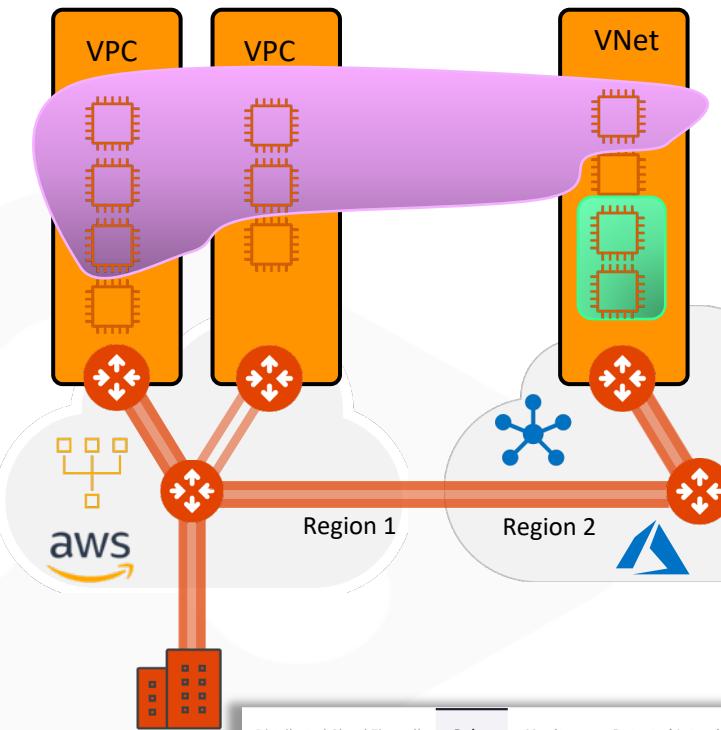
Distributed Cloud Firewall Rule Types: Intra-rule vs. Inter-rule



- **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.

Aviatrix DCF: Intra and Inter Rules - Examples

ALLOW LIST MODEL (TRUST-CENTRIC MODEL) → ZTN approach:
Deny everything and only permit what you explicitly allow.



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: On

Logging: On

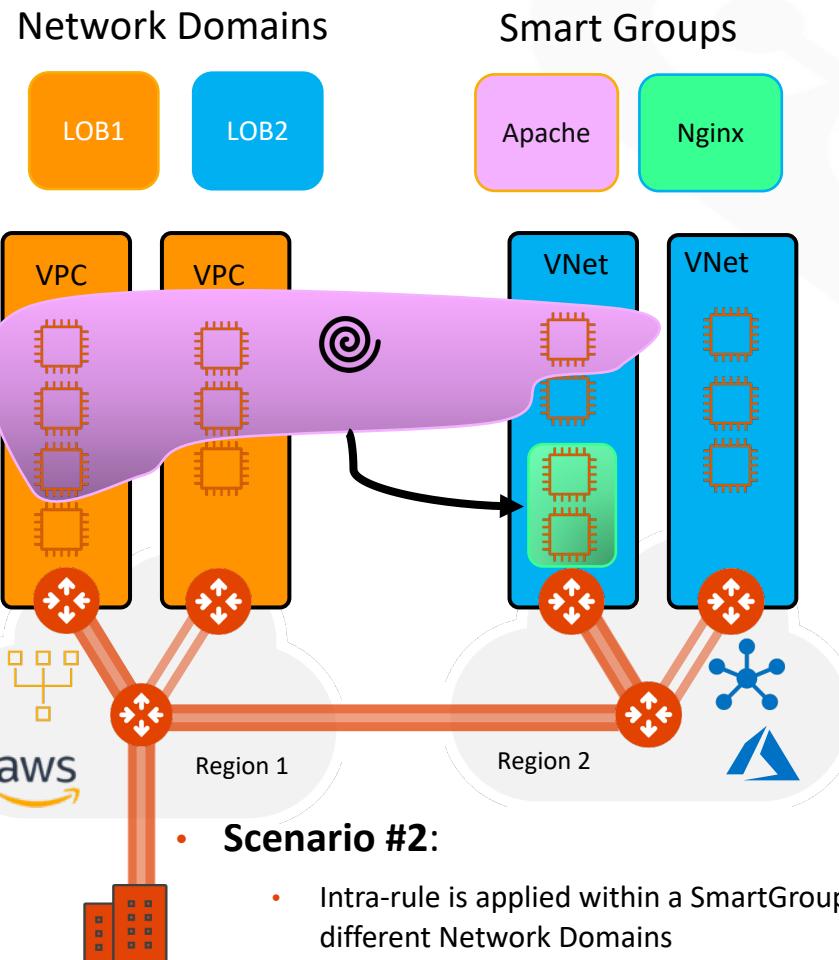
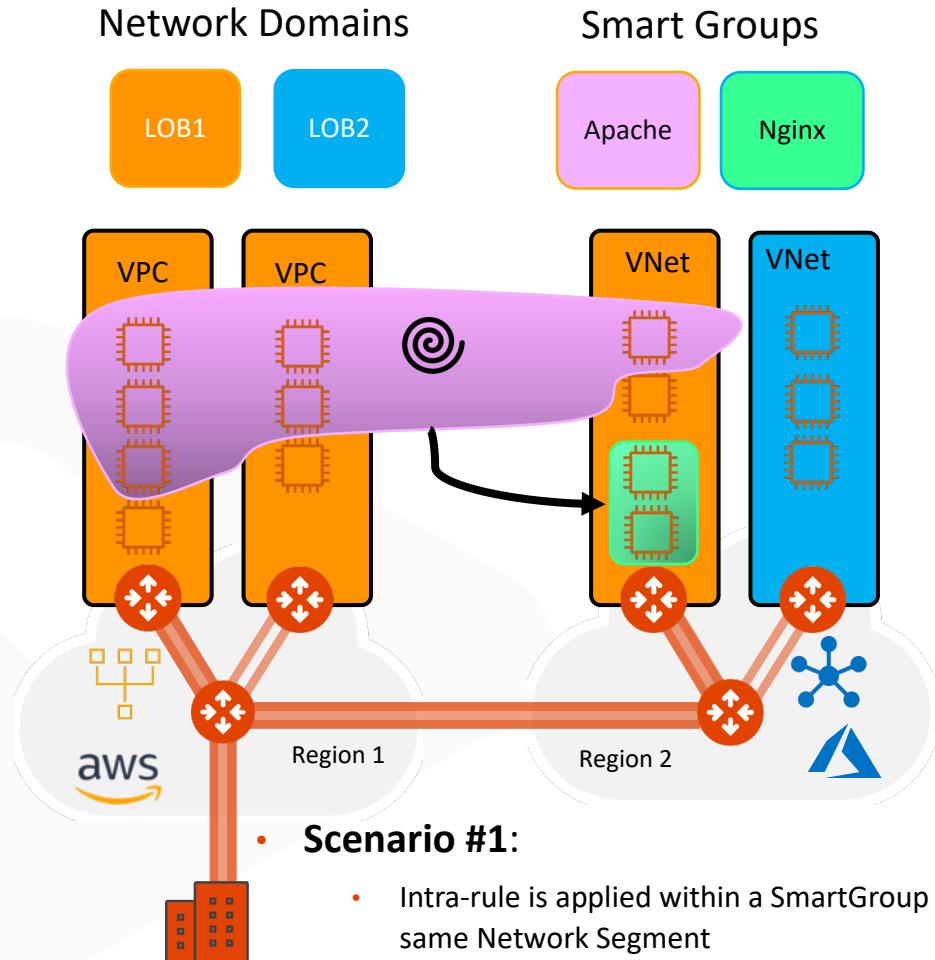
Cancel Save In Drafts

Distributed Cloud Firewall

Rules							
Actions		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
2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit
3	INTER-ICMP-NGINX-APA...	NGINX	APACHE		ICMP		Permit
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

- 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



Caveat:

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

Intra VPC/VNet Distributed Firewalling (available on AWS/Azure)

☐ Enable the feature on the relevant VPC/VNet

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

Available On
7 VPC/VNets

Manage

VNet

SmartGroup #1

SmartGroup #2

Transit

Spoke

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 orchestration (*aka Intra-VPC Traffic Control*), the SmartGroups will not be able to communicate with each other unless an inter rule is applied between them.
- This is pure L4 separation using the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.
- Future Implementation:** traffic will be diverted to the nearby Spoke GW for the L7 inspection

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	<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 New Rule

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

Name
Allow_Https

Source SmartGroups
APACHE-FLEET-SERVERS

Destination SmartGroups
NGINX-FLEET-SERVERS

Protocol
TCP Port
443

Rule Behavior
Enforcement On

Action
Allow Logging
 Off Traffic Stats
On

Rule Priority
Place Rule
Top

Cancel Save

□ 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 New Rule

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

Name
Allow_Https

Source SmartGroups
APACHE-FLEET-SERVERS

Destination SmartGroups
NGINX-FLEET-SERVERS

Protocol TCP Port 443

Rule Behavior Enforcement On

Action Allow Logging **On** Traffic Stats On

Rule Priority

Place Rule Top

Cancel **Save**

❑ Logging can be turned ON/OFF per rule

❑ Configure Syslog to view the logs

Policy Monitor

Auto Refresh |

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	✓

Showing all 20 logs

Close



Next: Lab 10 – Distributed Cloud Firewall