



Distributed Firewalling

Distributed Firewalling Basics

Distributed Firewalling* enforces policy exactly where needed across the entire network

Characteristics:

- Two components: Smart Groups & Rules
- Leveraging the Aviatrix **Spoke Gateways** as Enforcement points.
- **Orchestrating** the provisioning of **Azure NSGs**, for **Intra-VPC segmentation**

* As of v3.2 of the CoPilot, Micro-Segmentation has been renamed to **Distributed Firewalling**

Smart Group

- **What is a Smart Group?**

A Smart Group identifies a group of resources that have similar policy requirements, that are confined in the same logical container.

- The members of a Smart Group can be classified using *three* methods:

- CSP Tags
- Resource Attributes
- CIDR



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}

Resource attribute

- Region Name, Account Name

IP Prefixes

- CIDR

Instance: i-0380038ff7d66b66f (shopping cart app)

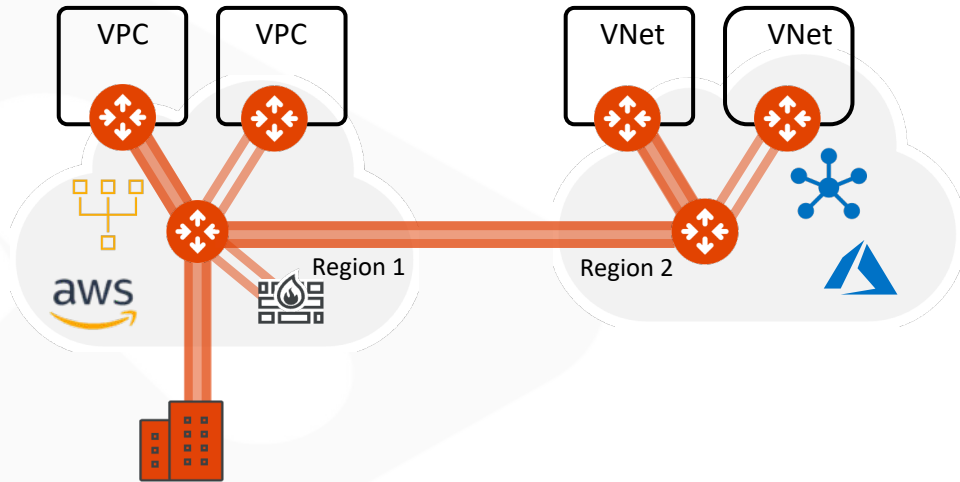
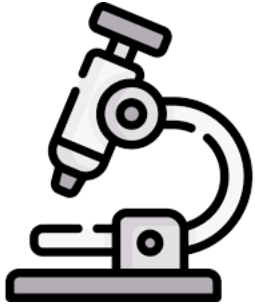
Select an instance above

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

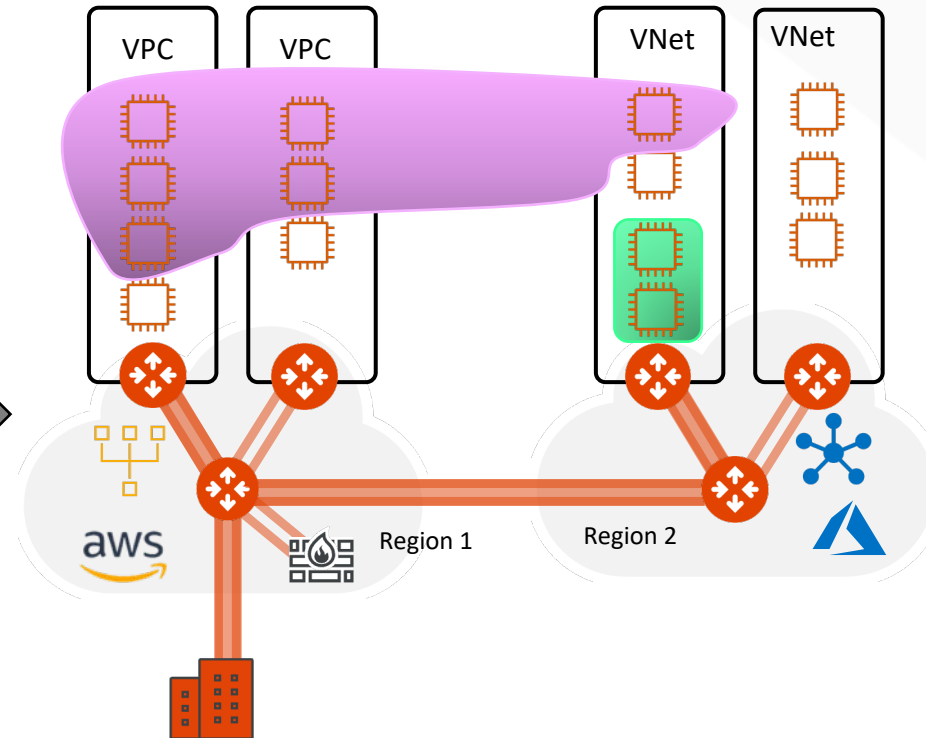
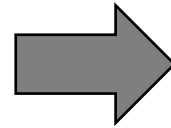
Tags

Key	Value
Env	Staging
Name	shopping cart app

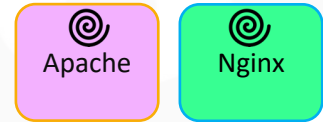
Distributed Firewalling: Intra-rule vs. Inter-rule



- **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



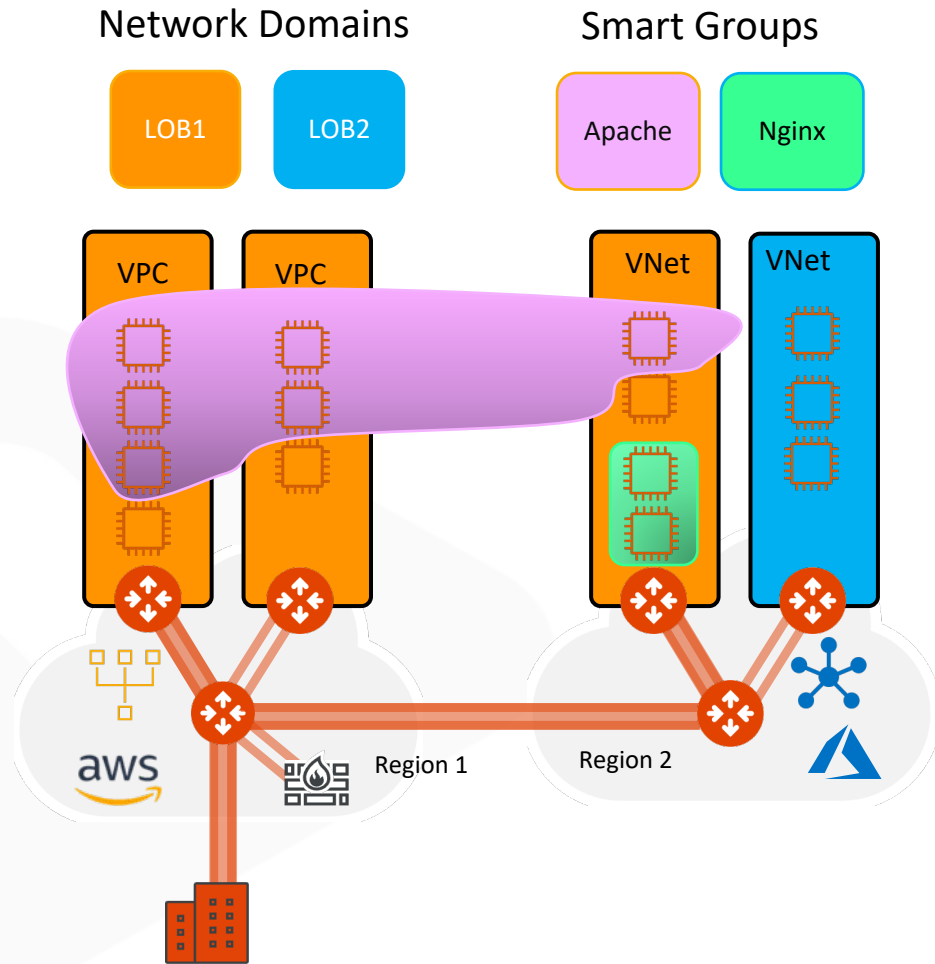
Smart Groups



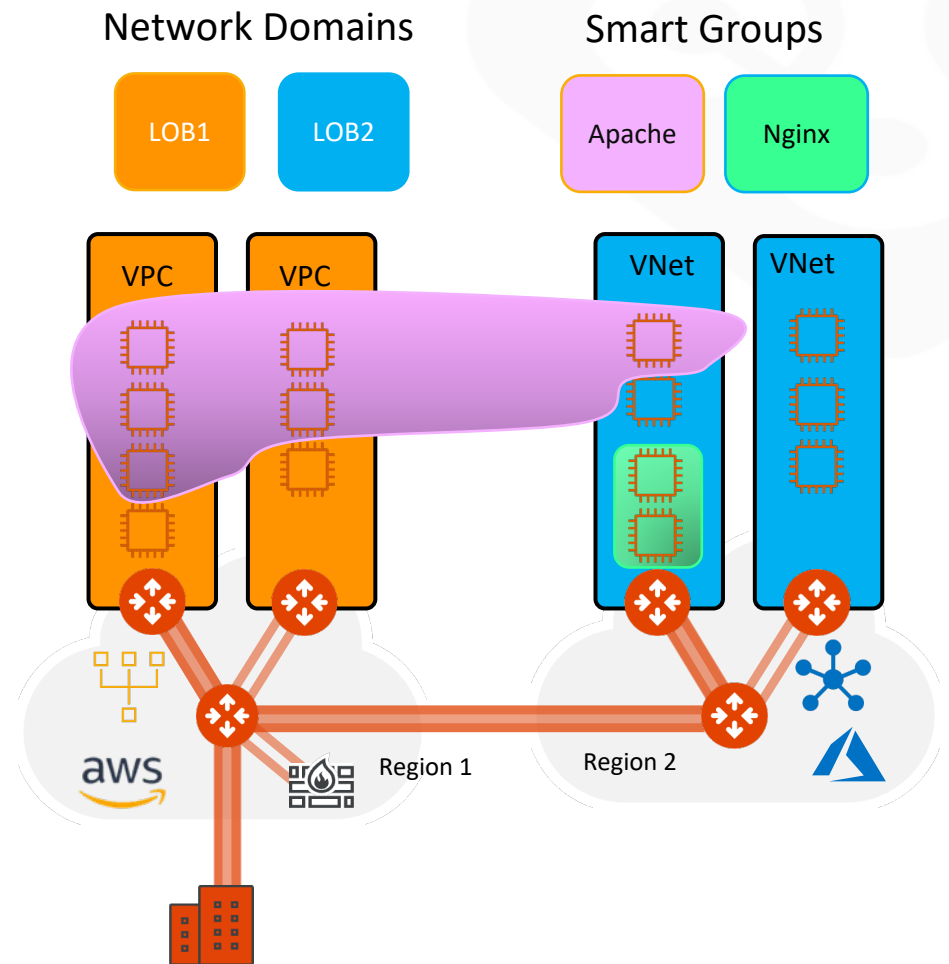
A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

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

Network Segmentation & Distributed Firewalling Together



- **Scenario #1:** Smart Group defined within a Network Segment
- Network Segmentation and Distributed Firewalling are NOT mutually exclusive



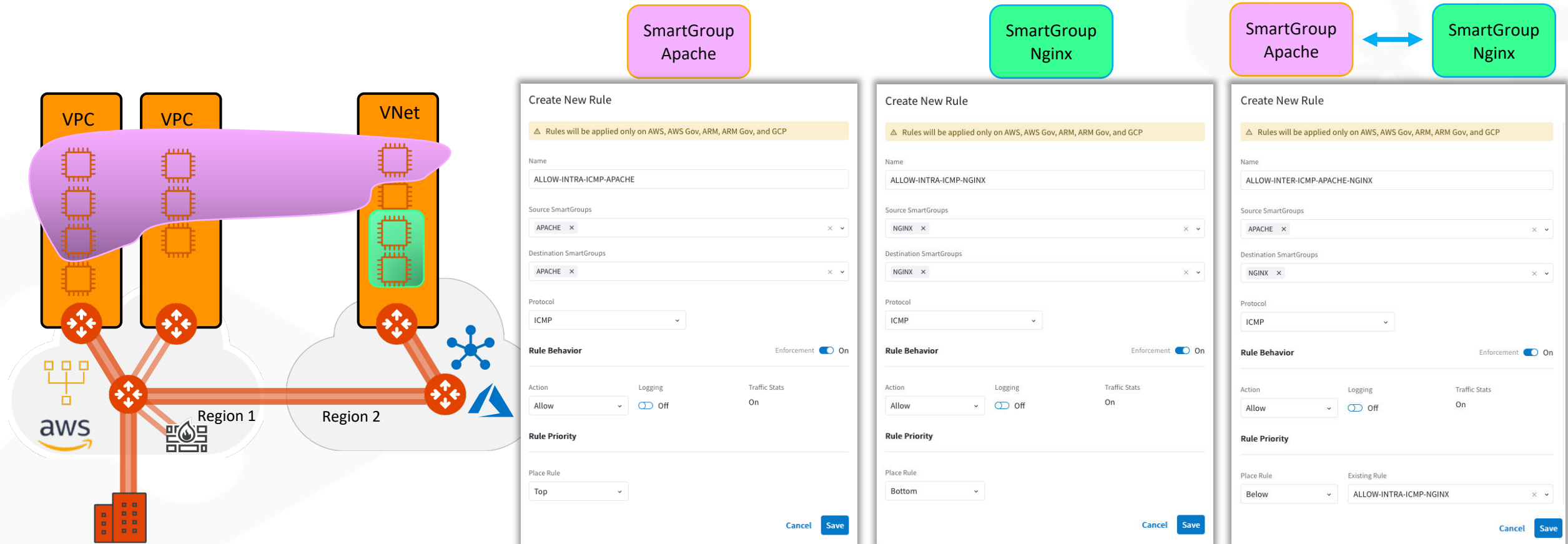
- **Scenario #2:** Smart Group stretched between two Network Domains
- Network Segmentation has precedence on the extent of a Smart Group

Smart Groups Creation

The screenshot illustrates the CoPilot interface for creating Smart Groups. The sidebar on the left contains navigation options: Dashboard, AirSpace, Networking, Security, SmartGroups, Cloud Resources, Monitor, Troubleshoot, Billing & Cost, Administration, and Settings. The main area shows the 'SmartGroups' section with buttons for '+ SmartGroup' and 'Refresh CSP Resources'. A modal window titled 'Create New SmartGroup' is open, showing fields for Name (APACHE-FLEET-SERVERS), Resources (Resource Selection (2)), and Virtual Machines (Matches all conditions (AND) with Type APACHE). A success message 'Successfully refreshed CSP resources' is displayed at the top right.

- 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

Distributed Firewalling Rules on Smart Groups



Distributed Firewalling

Rules | Detected Intrusions | Settings

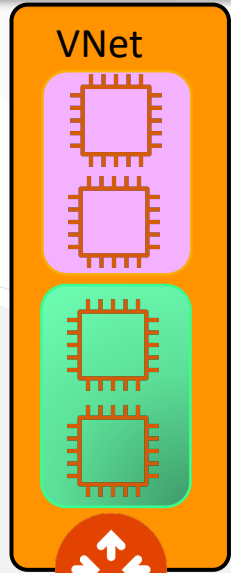
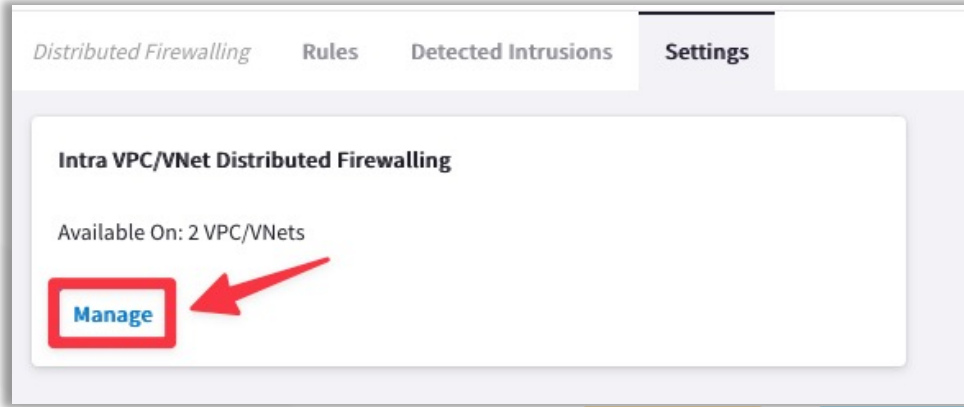
+ Rule | Actions | Policy Monitor | Search

Priority	Name	Source	Destination	Action	Protocol	Ports	Logging	Traffic Count	Enforcement
0	• ALLOW-INTRA-ICMP-APACHE	APACHE	APACHE	Allow	ICMP		Off	0	On
1	• ALLOW-INTRA-ICMP-NGINX	NGINX	NGINX	Allow	ICMP		Off	0	On
2	• ALLOW-INTER-ICMP-APACHE-NGINX	APACHE	NGINX	Allow	ICMP		Off	0	On
3	• DENY-CATCH-ALL	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)	Deny	Any		Off	0	On

- 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

Intra VPC/VNET Distributed Firewalling (on Azure)

❑ Enable the feature on the concerned VNets



SmartGroup
#1

SmartGroup
#2

- If you enable the *Intra-VNet Distributed Firewalling* in Azure, the SmartGroups will not be able to communicate to each other, unless a *rule* is applied.

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.

🔍 Search

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.

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 ☒ ☐ ☐ ☐

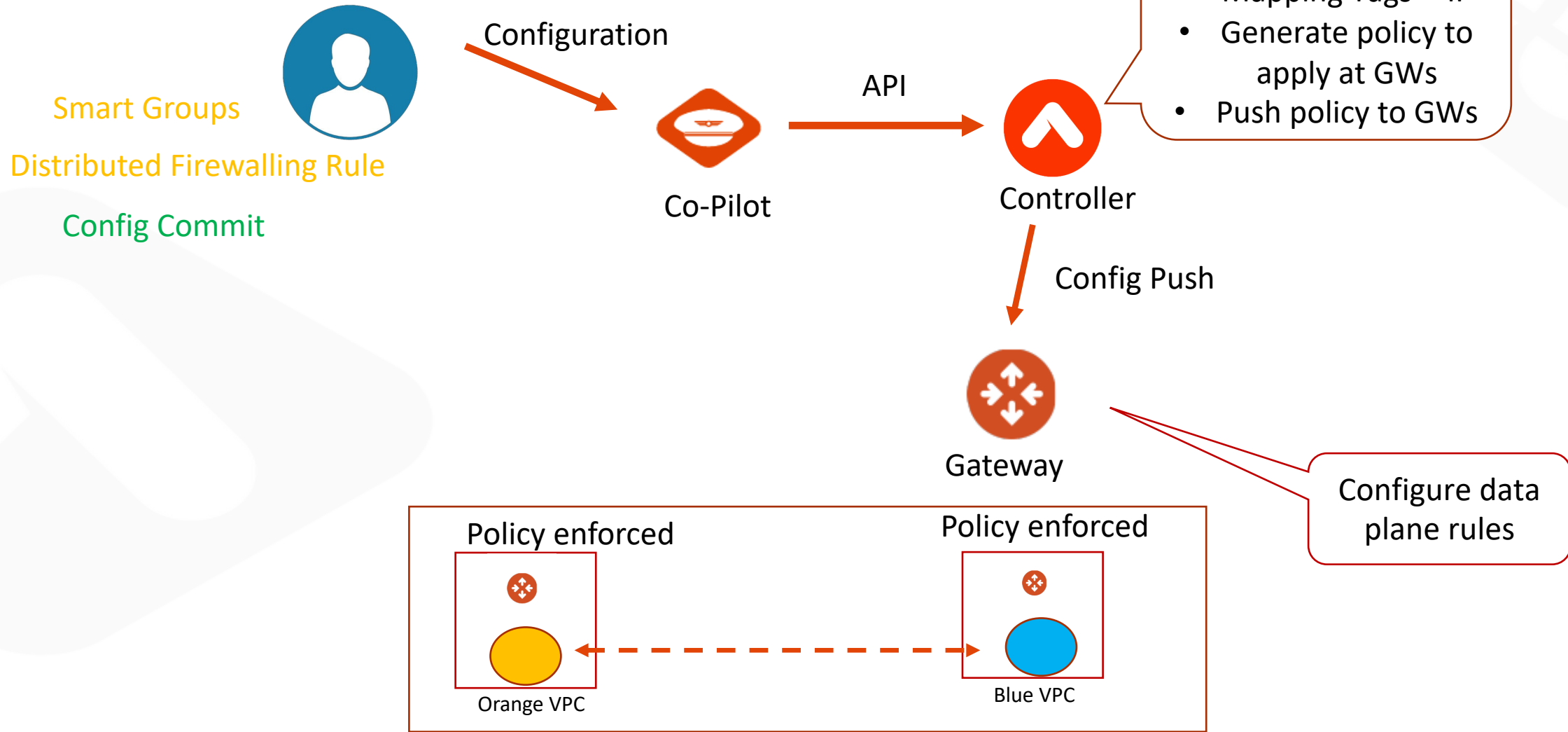
Search

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

Architecture





Next: Lab 10 – Distributed Firewalling