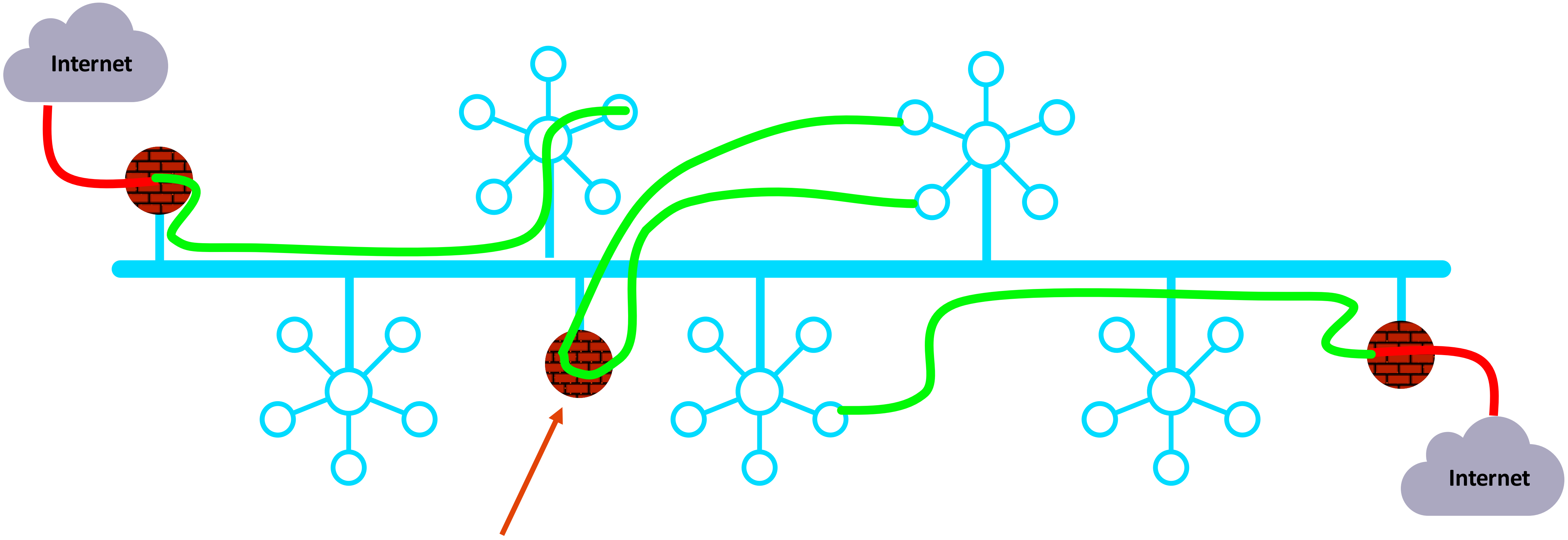
Distributed Cloud Firewall

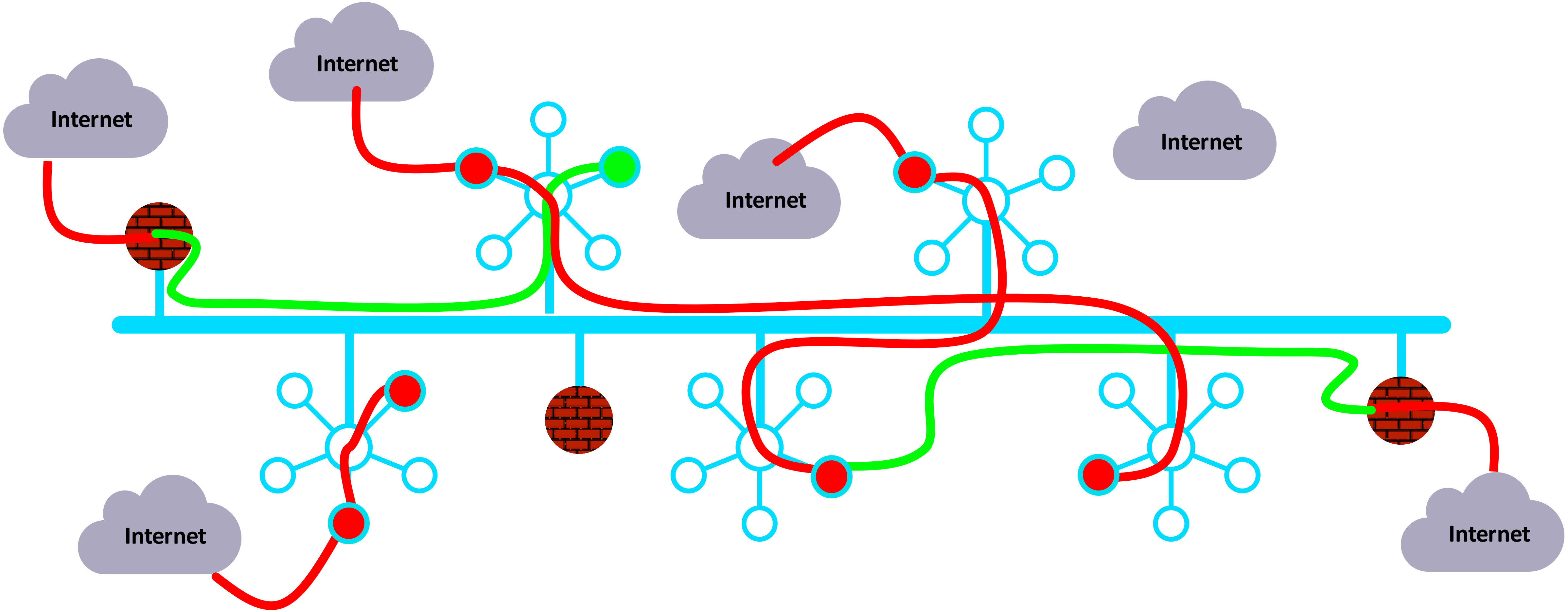
ACE Team

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

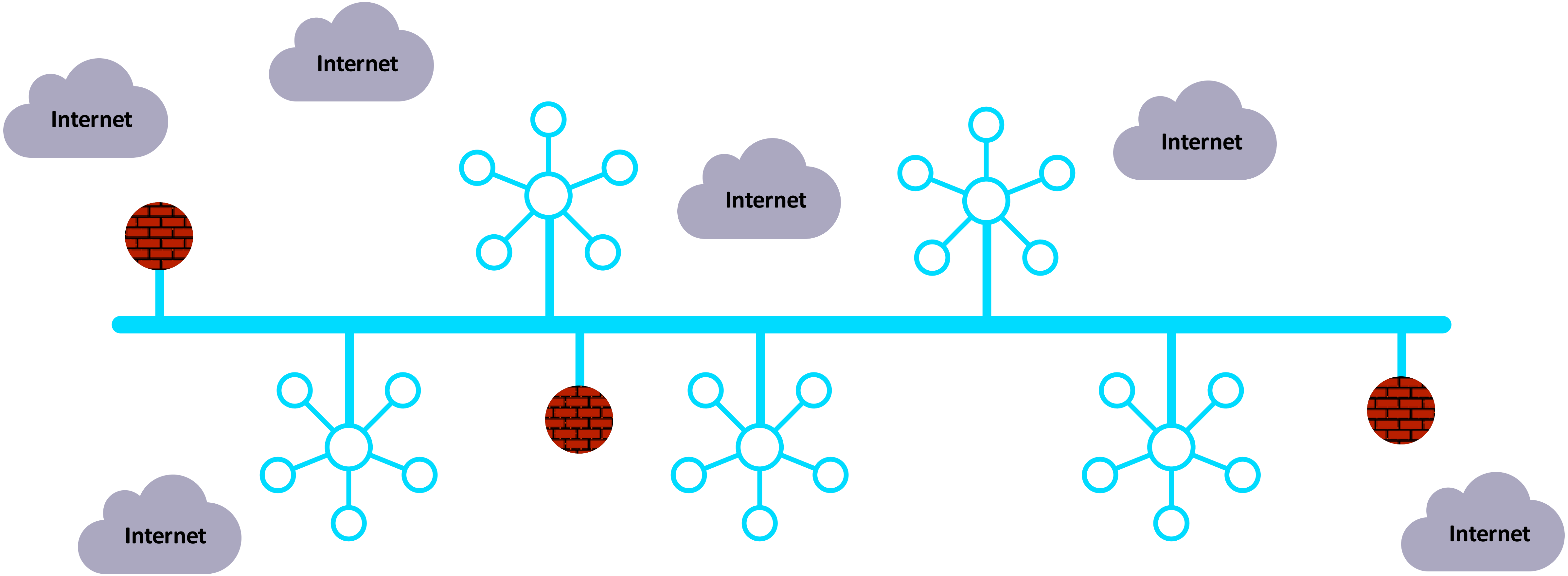


“Last Generation Firewalls”

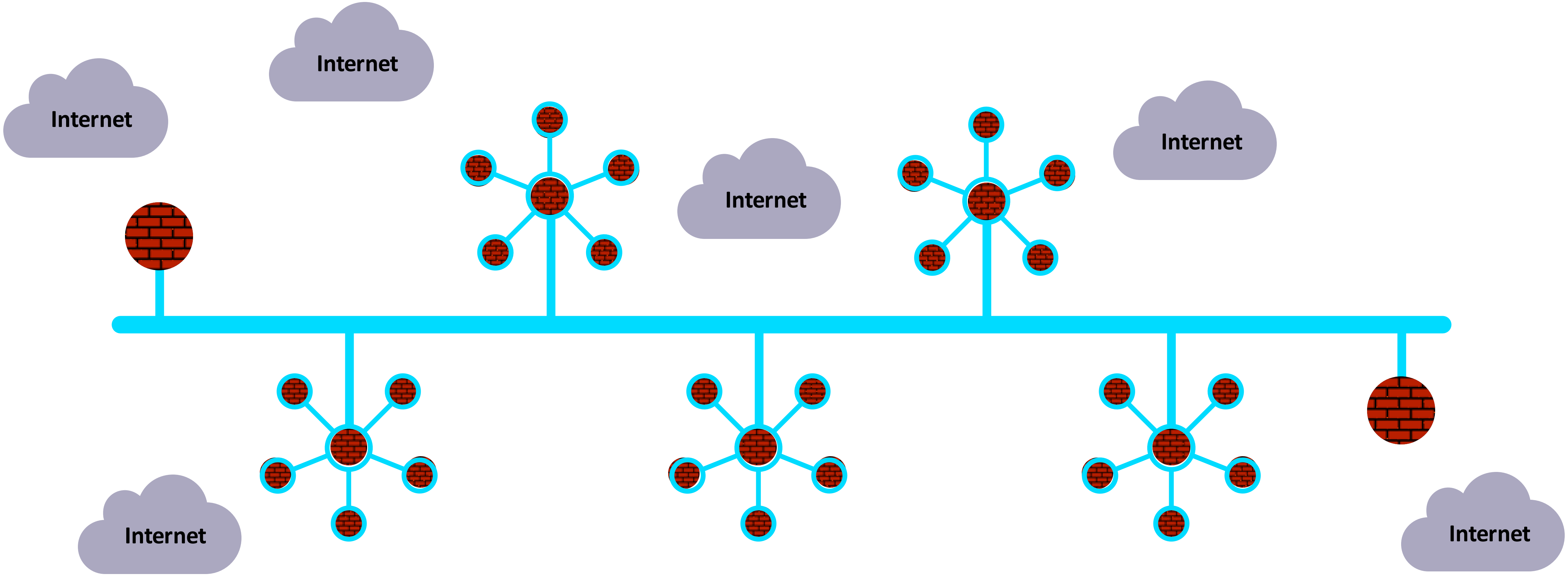
In Reality...


Internet
Internet
Internet
Internet
Internet
Internet
Internet

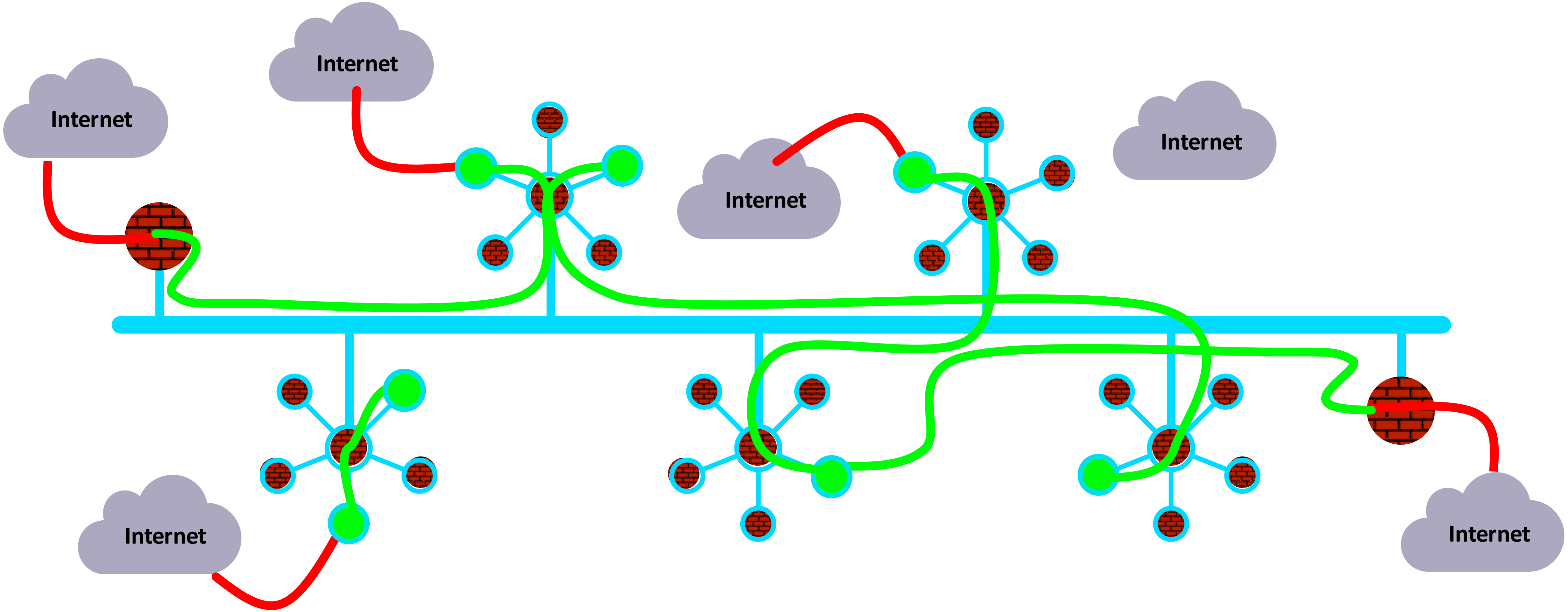
What If… the architecture was built for cloud



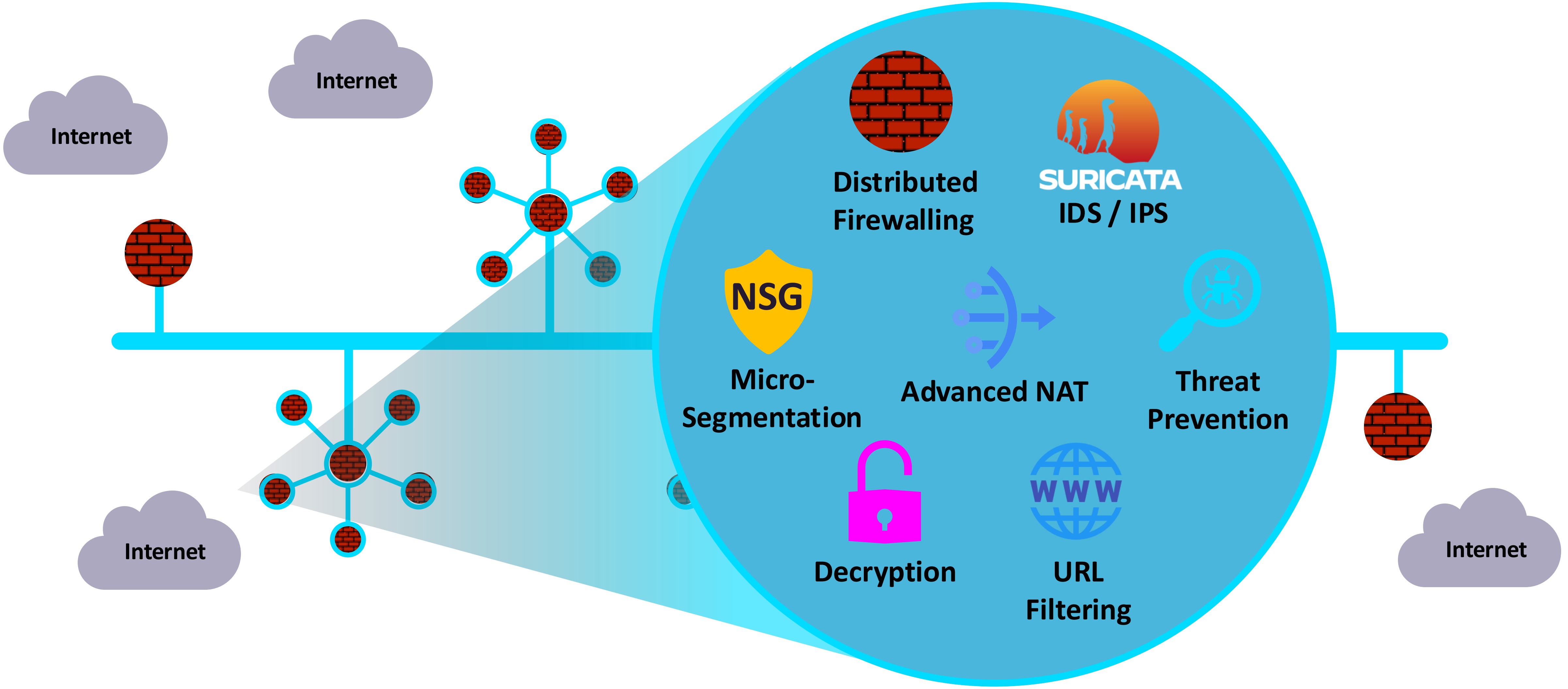
Firewalling Functions were Embedded in the Cloud Network Everywhere…



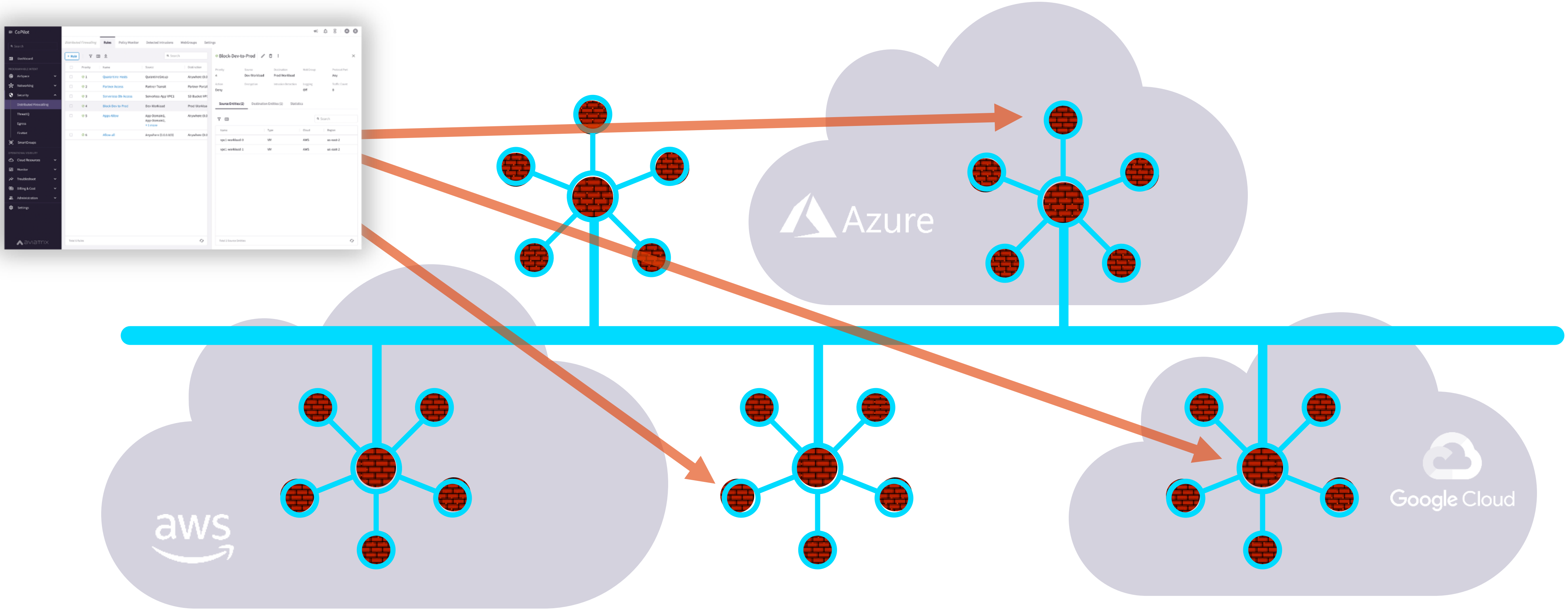
Centrally Managed, with Distributed Inspection & Enforcement…



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	QuarantineGroup	Anywhere (0.0
2	Partner Access	Partner Transit	Partner Portal
3	Serverless Db Access	Serverless App VPC1	S3 Bucket VPC
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	Encryption	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

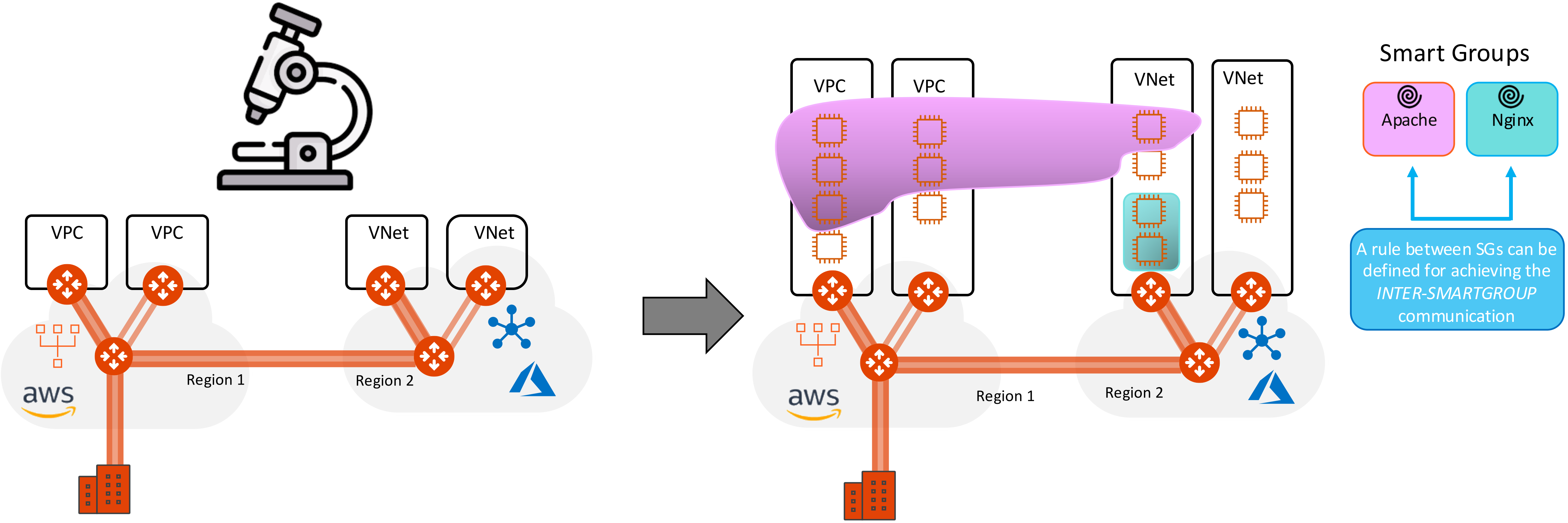
- A firewall rule consists of two important initial elements (i.e. *L3 info*):
  - **Source**
  - **Destination**

- **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:
  - Virtual Machines
  - Subnets
  - VPC/Vnets
  - Kubernetes
  - Hostnames
  - External Connections (S2C)

Distributed Firewalling: Intra-rule vs. Inter-rule

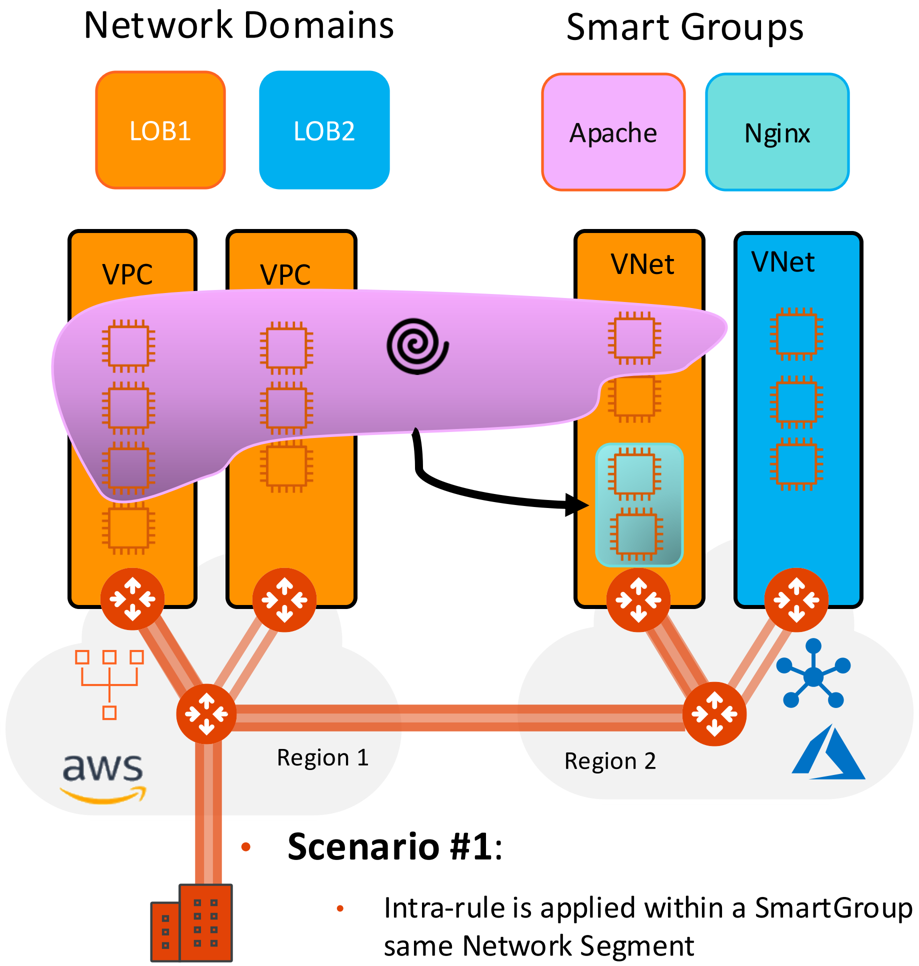


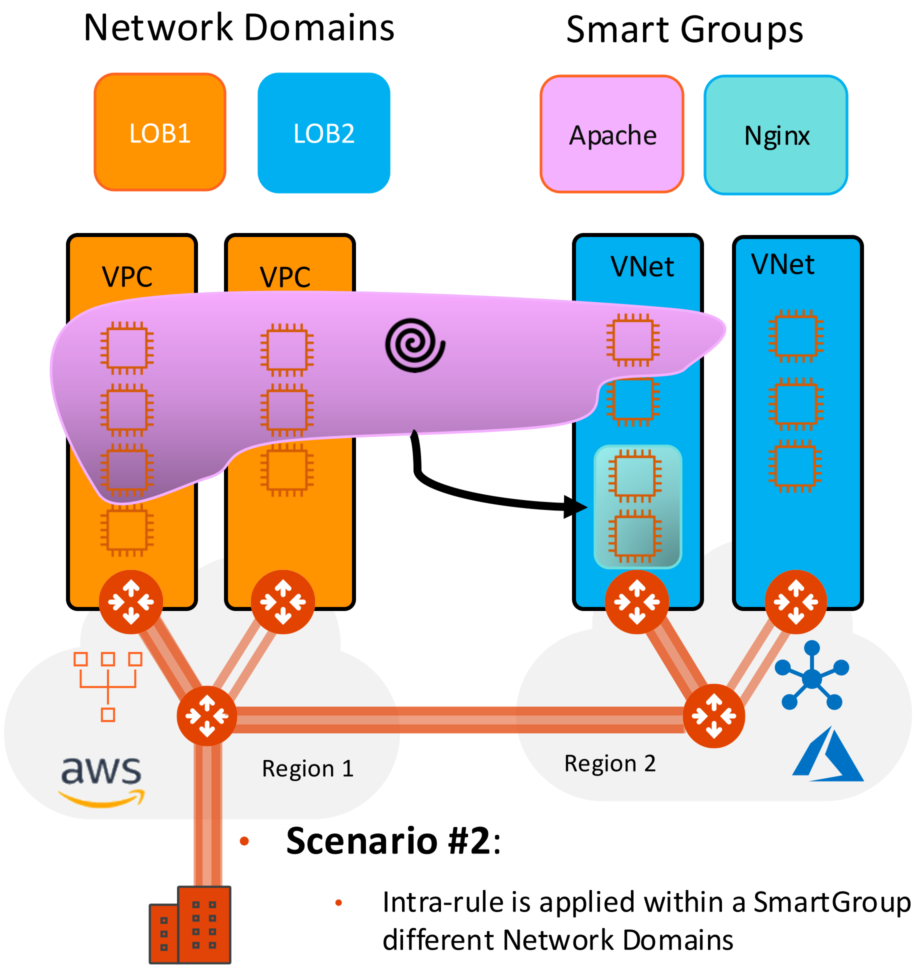
A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

- **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.

Network Segmentation & Distributed Cloud Firewall Rule





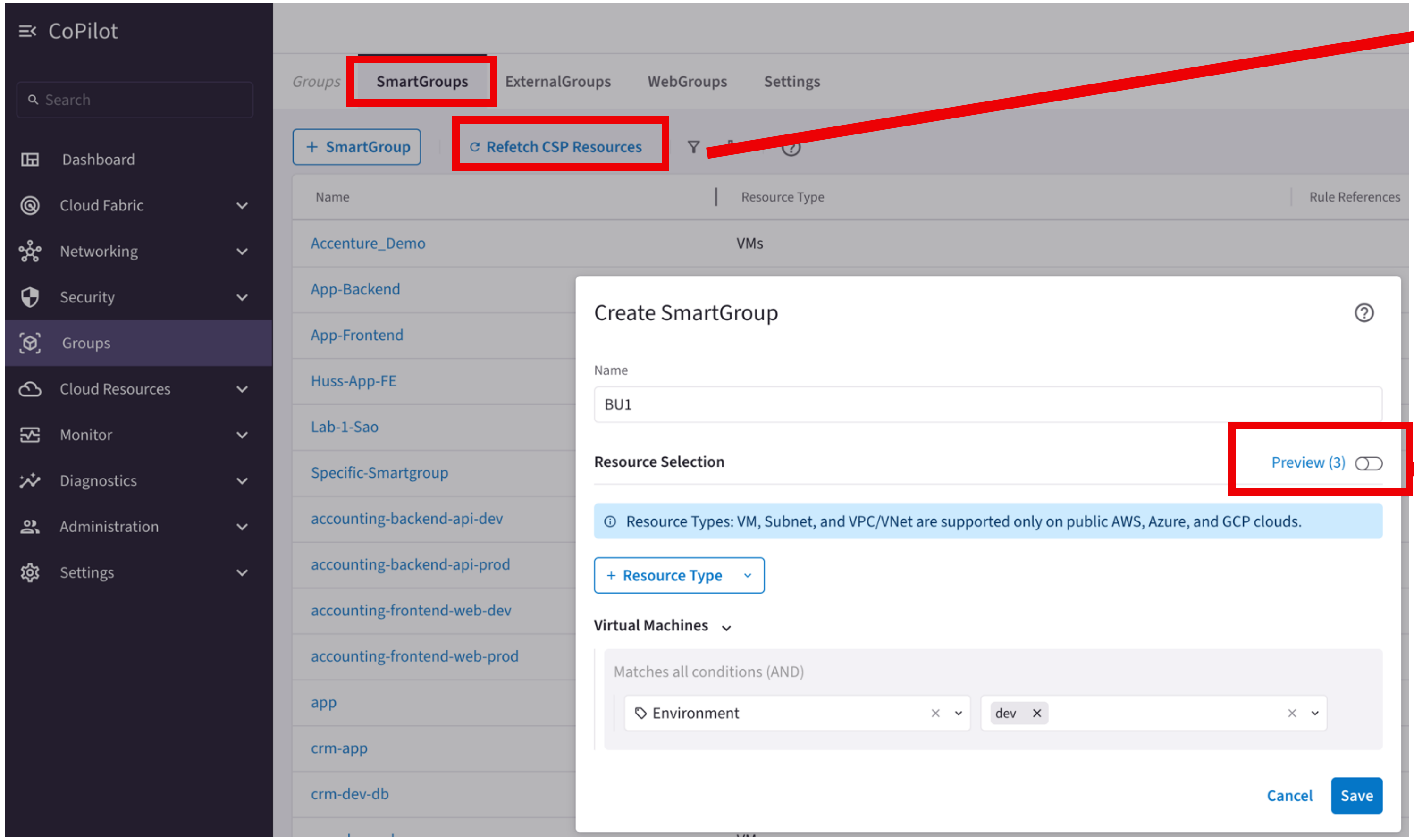
- **Scenario #1**:
  - Intra-rule is applied within a SmartGroup defined in the same Network Segment
  - Inter-rule is applied between SmartGroups within the same network Domain

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

Caveat:

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

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.

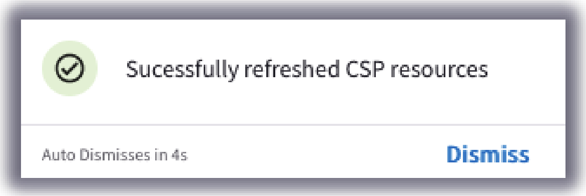
+ Resource Type

Virtual Machines

Matches all conditions (AND)

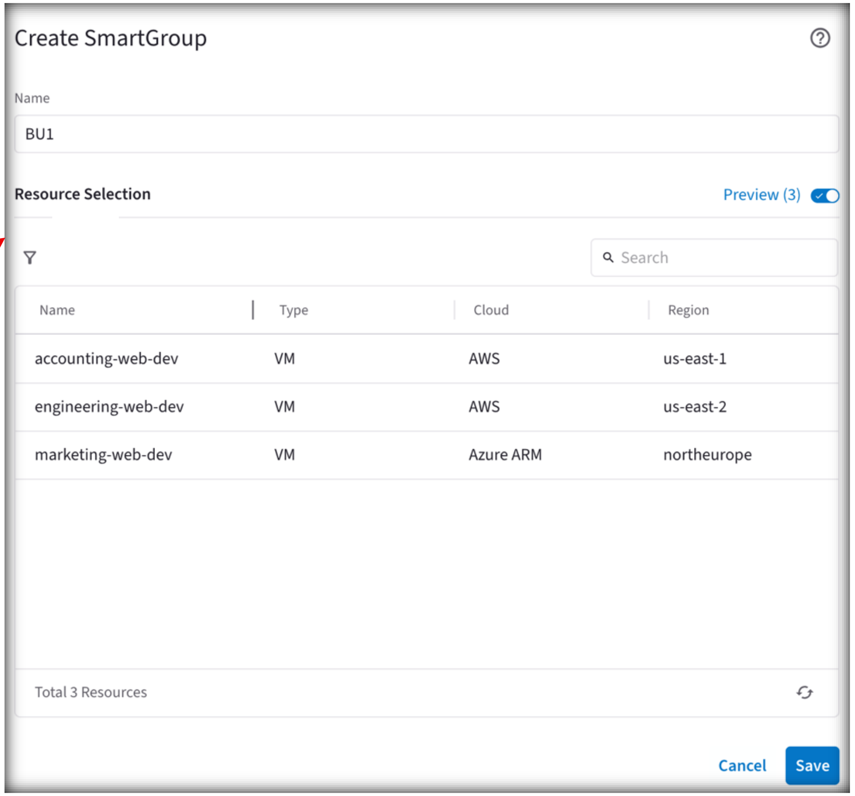
Environment — dev

Cancel Save



Sucessfully refreshed CSP resources

Auto Dismisses in 4s — Dismiss



Create SmartGroup

Name: BU1

Resource Selection — Preview (3)

Search

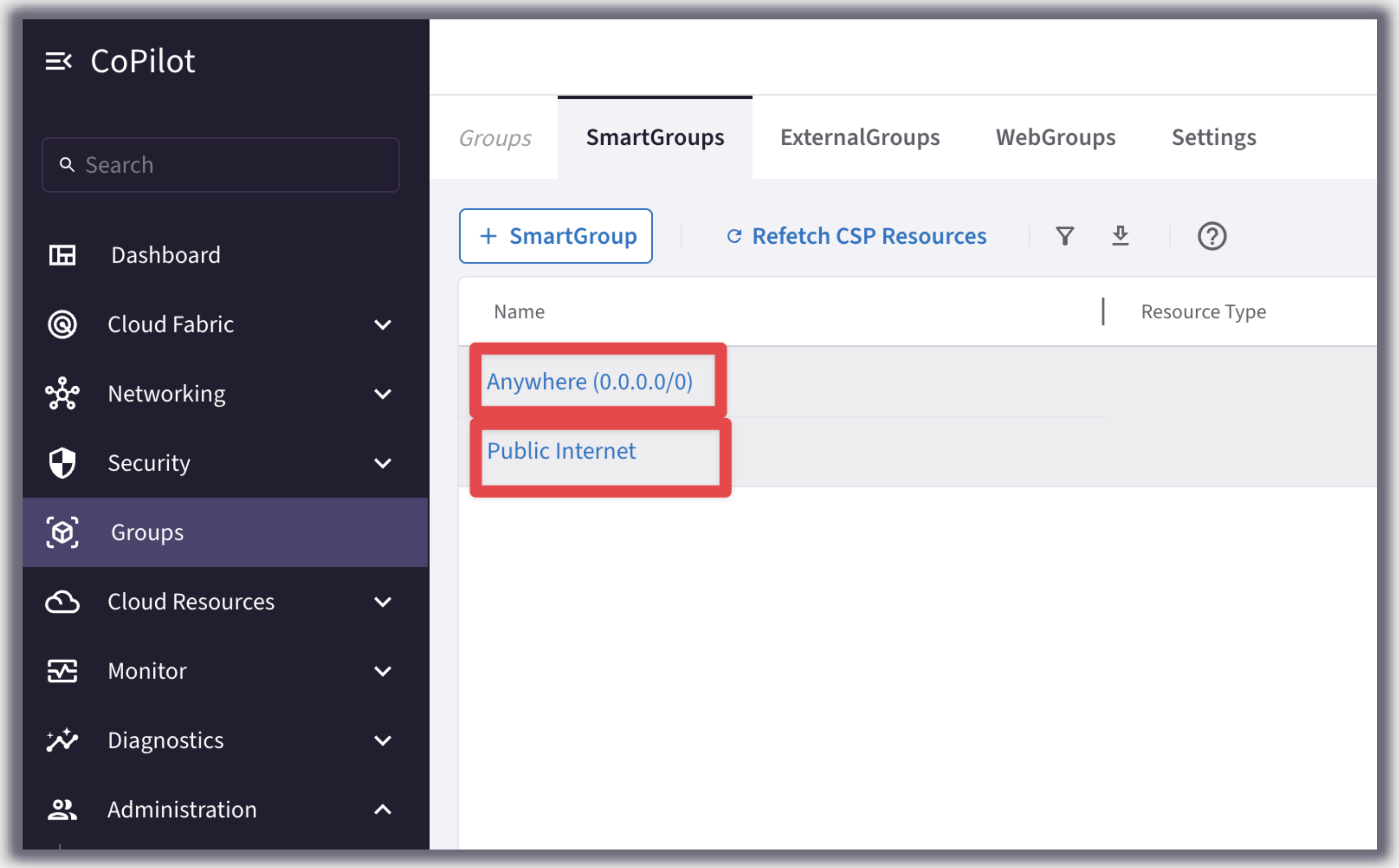
Name	Type	Cloud	Region
accounting-web-dev	VM	AWS	us-east-1
engineering-web-dev	VM	AWS	us-east-2
marketing-web-dev	VM	Azure ARM	northeurope

Total 3 Resources

Cancel Save

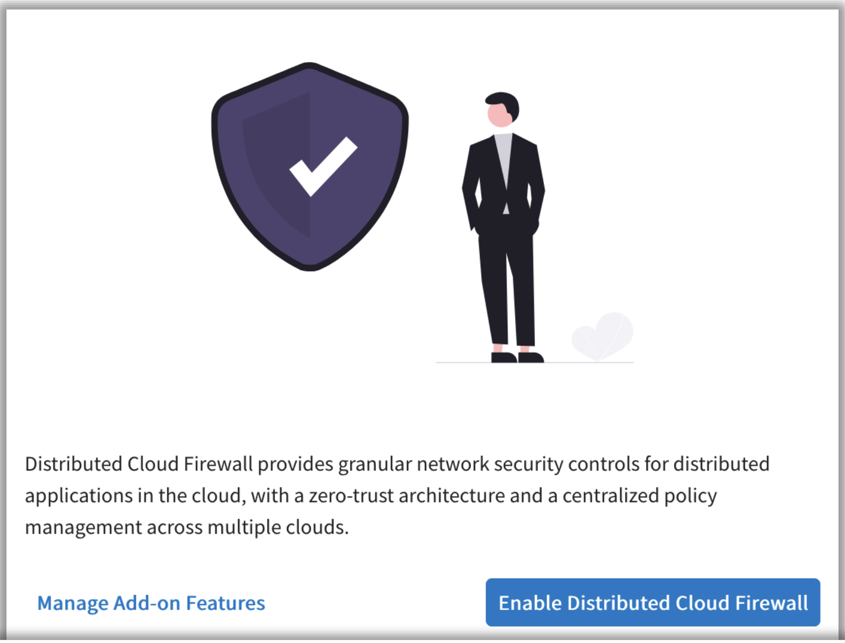
- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

Pre-defined Smart Groups



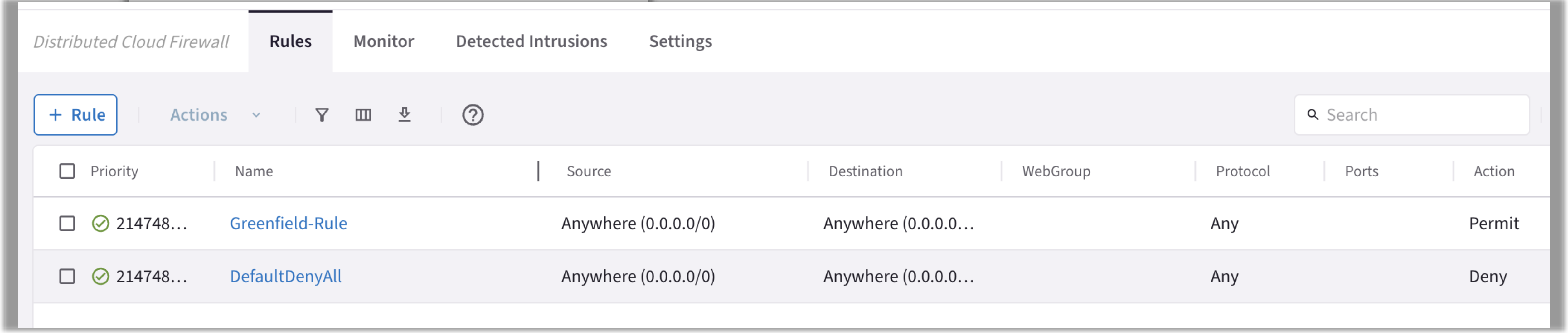
- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

Enabling Distributed Cloud Firewall



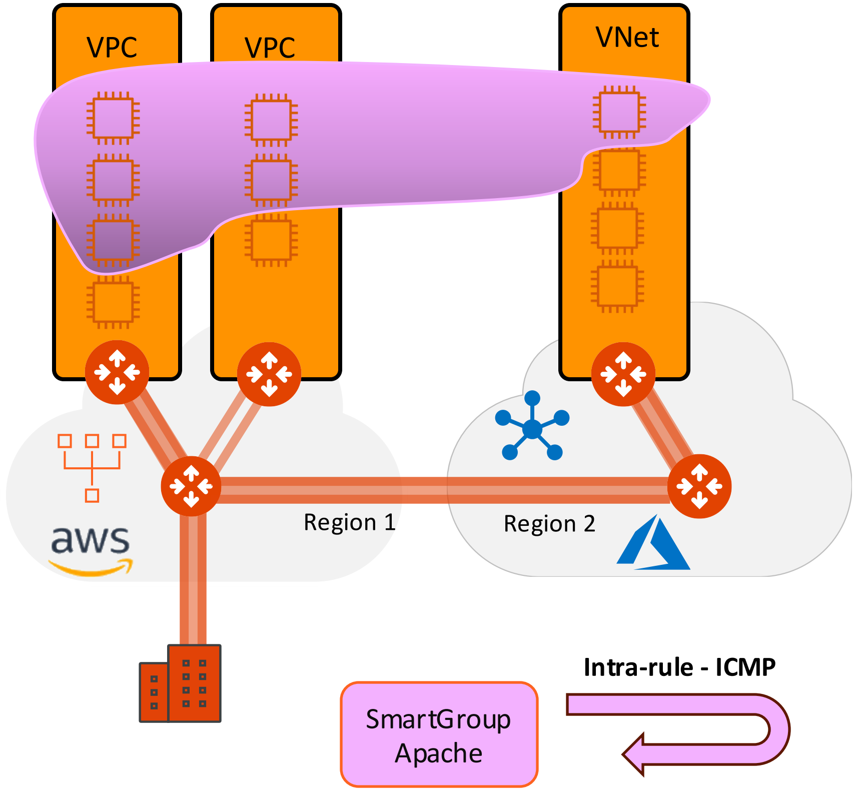
Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

- 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.



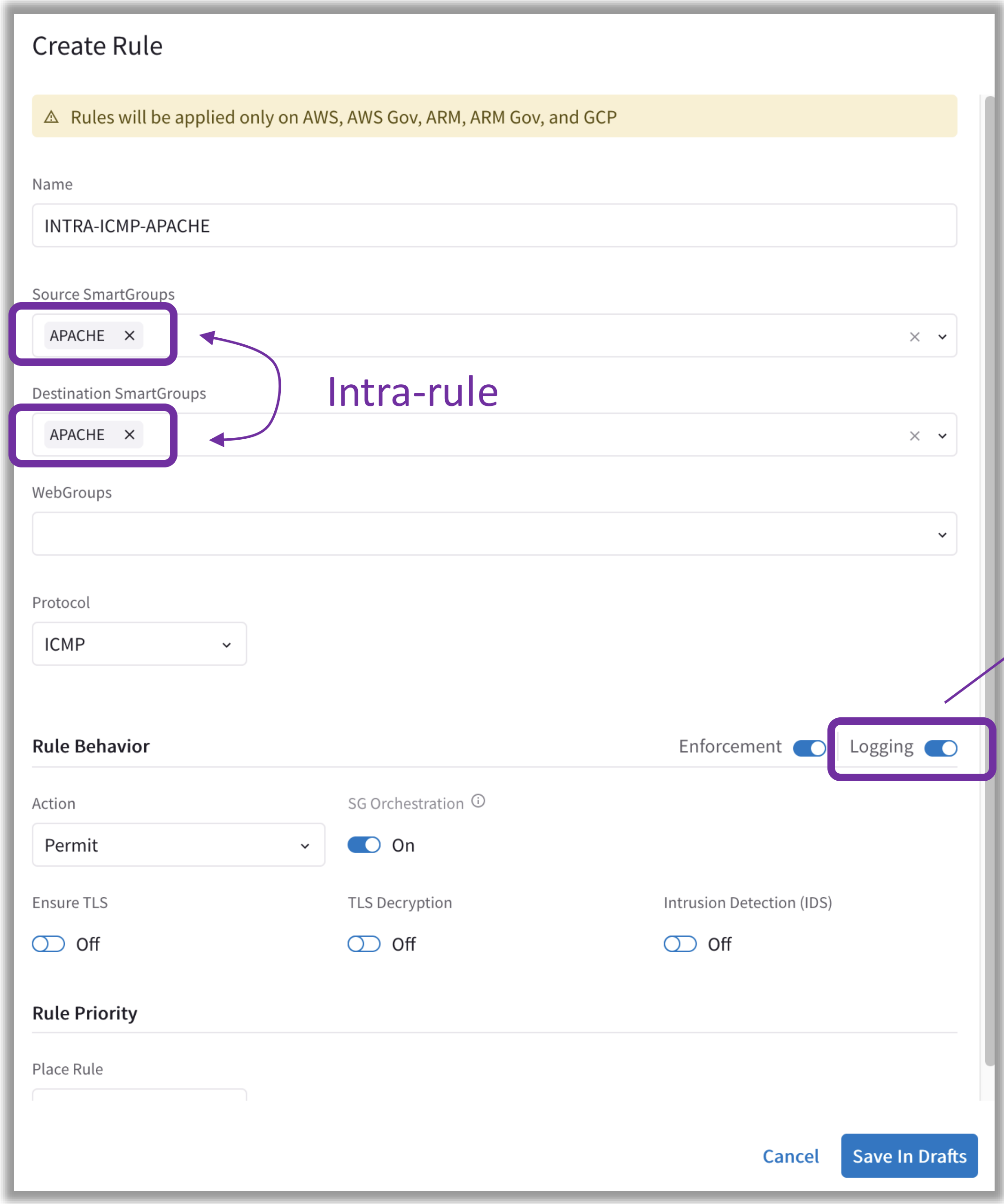
□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
□	✓ 214748…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0…		Any		Permit
□	✓ 214748…	DefaultDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0…		Any		Deny

Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (1)



Scenario #1

- ❑ **Create a DCF rule for the APACHE SmartGroup with the following requirements:**
  - Permit ICMP traffic internally
  - Enable the Logging feature



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: On — Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

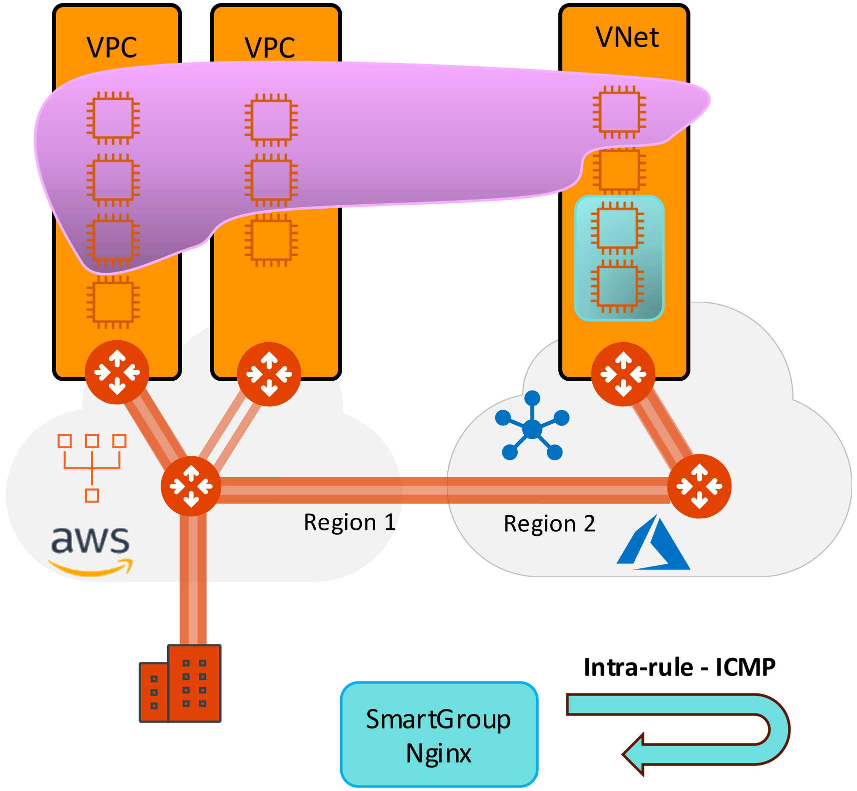
Place Rule

Cancel | Save In Drafts

Intra-rule

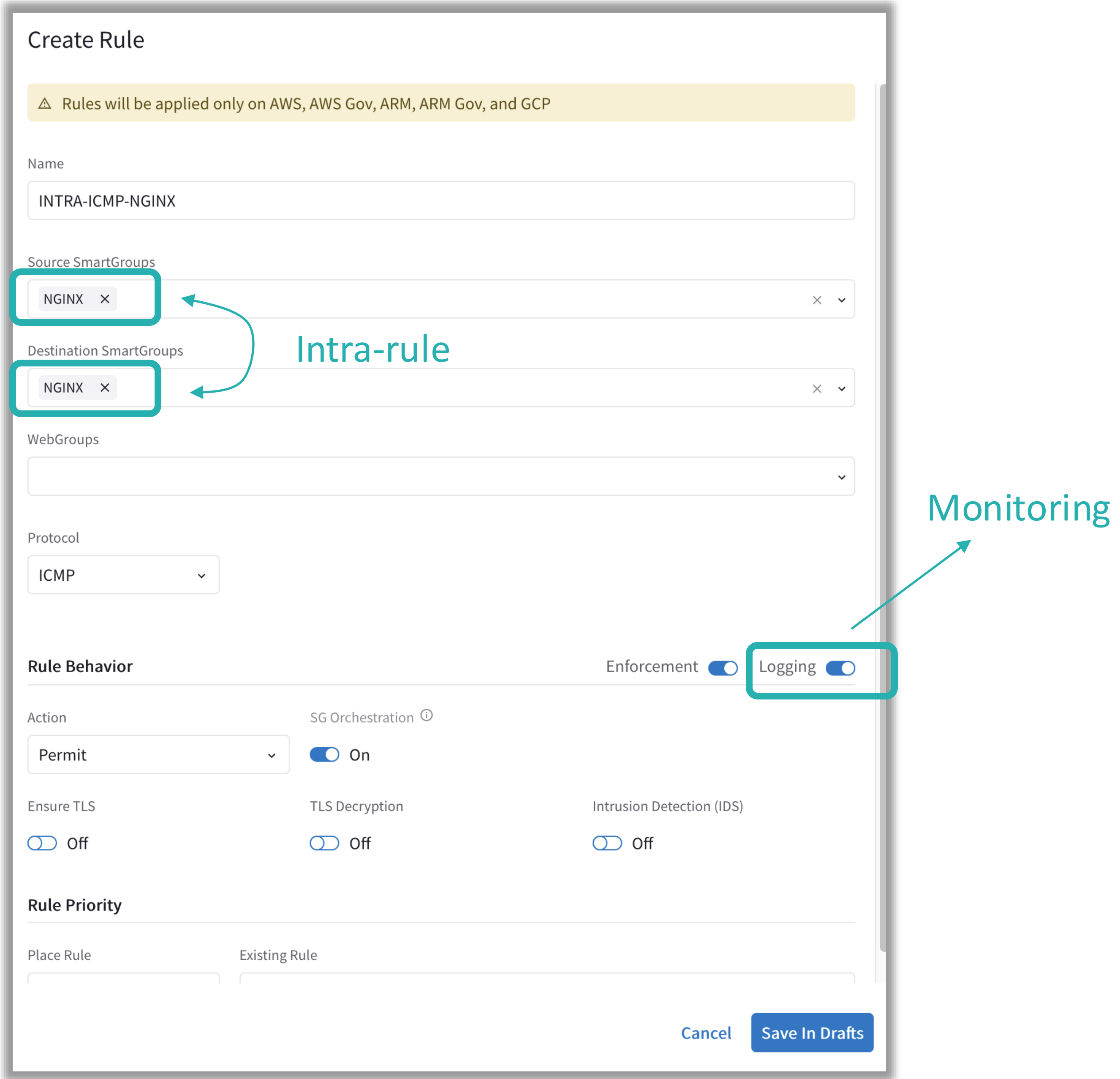
Monitoring

Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (2)



Scenario #2

- **Create a DCF rule for the NGINX SmartGroup with the following requirements:**
  - Permit ICMP traffic internally
  - Enable the Logging feature



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: On

Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

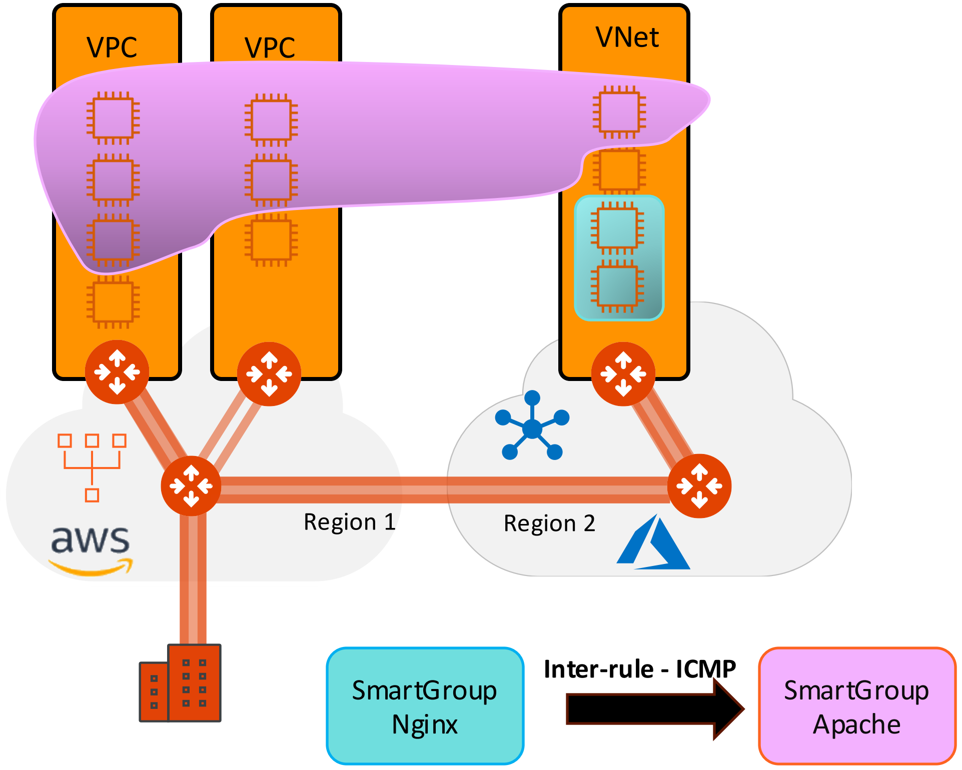
Intrusion Detection (IDS): Off

Rule Priority

Place Rule

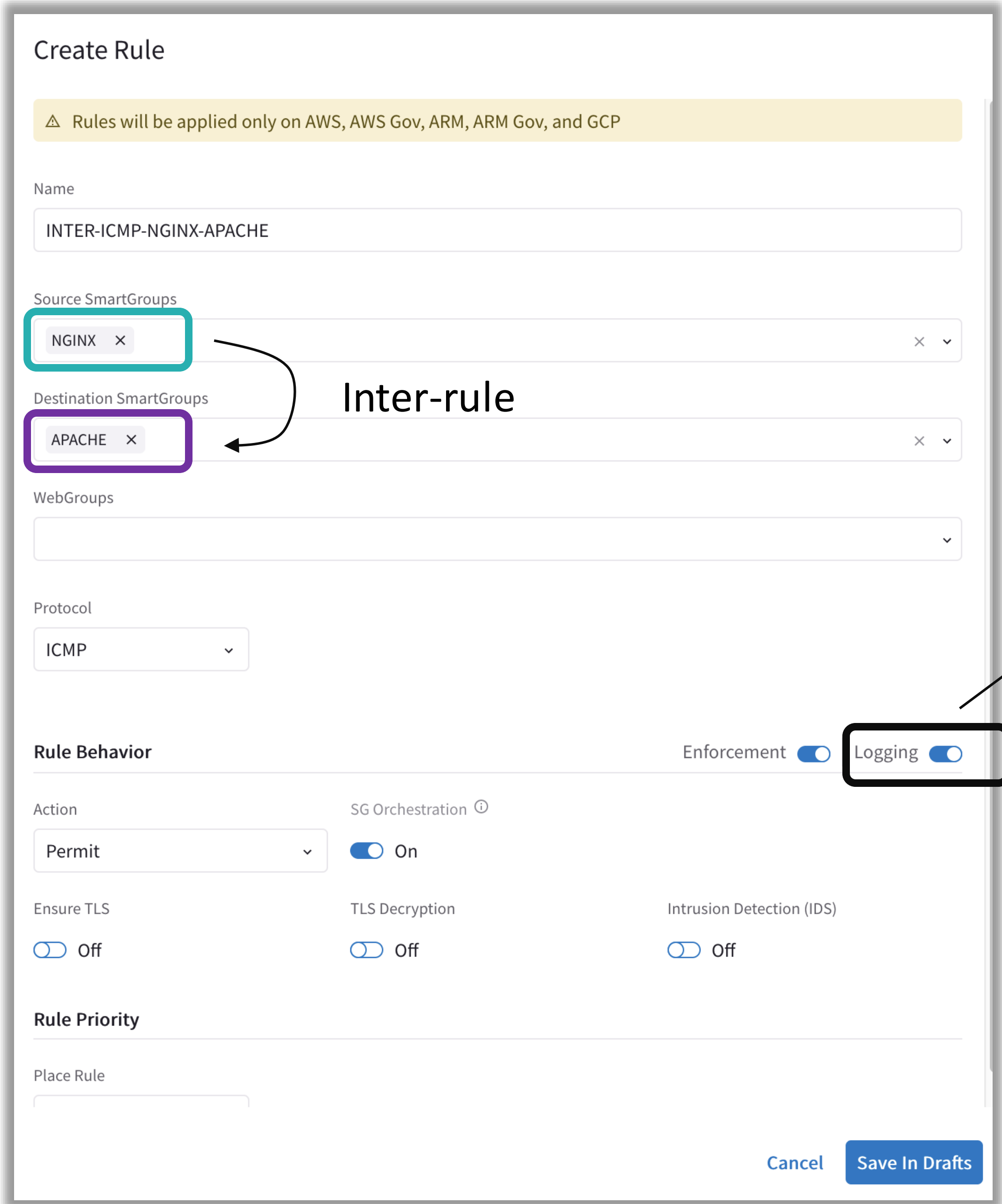
Existing Rule

Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (3)



Scenario #3

- **Create a DCF rule from the NGINX SmartGroup towards the APACHE SmartGroup, solely, not the inverse (NO bidirectional!), with the following requirements:**
  - Allow ICMP traffic between the two SGs
  - Enable the Logging feature



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: On — Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

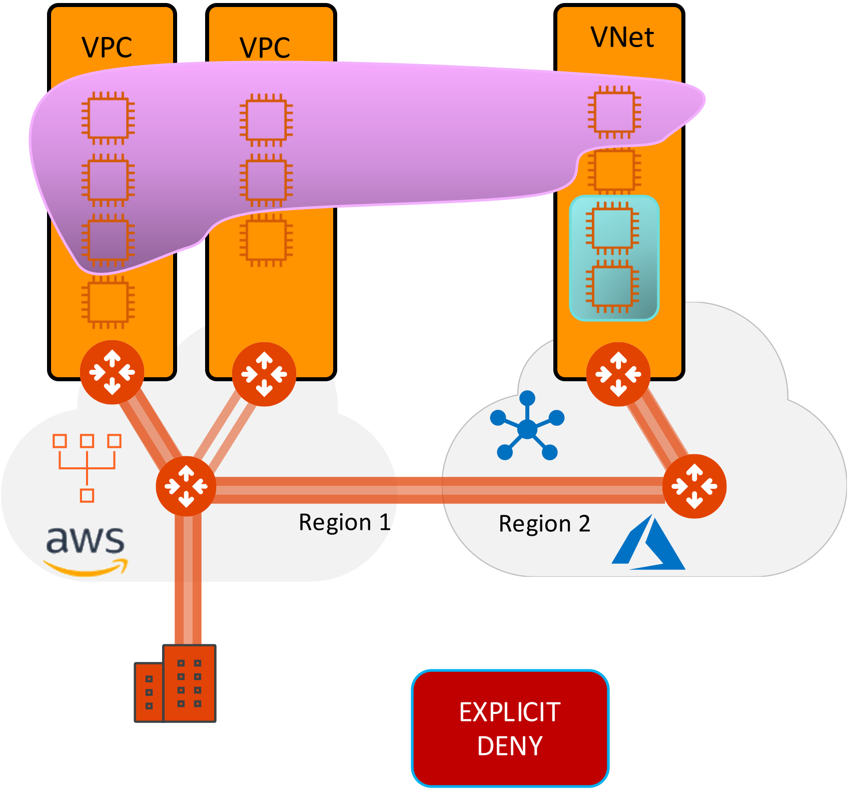
Rule Priority

Place Rule

Inter-rule

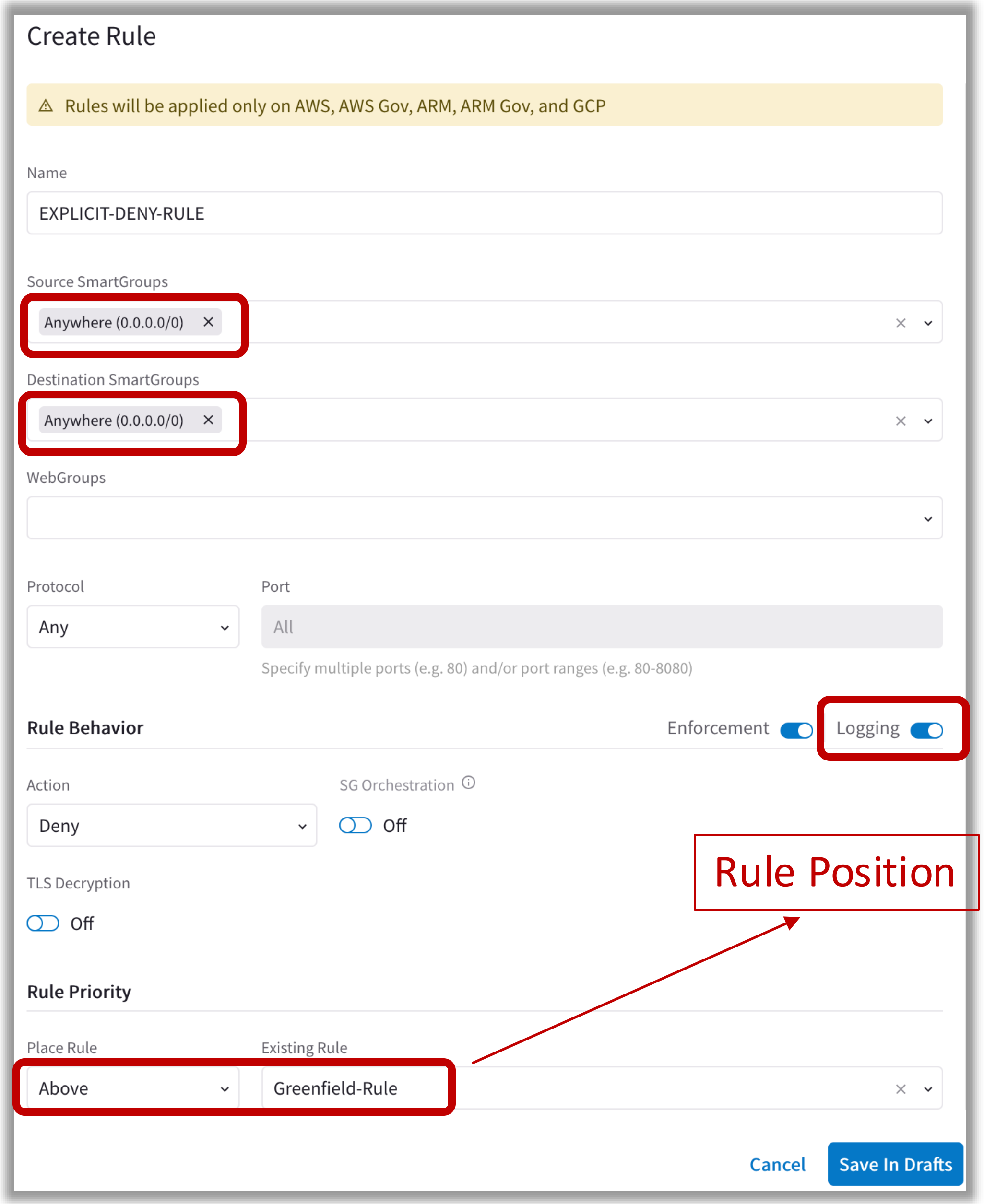
Monitoring

Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (4)



Scenario #4

- ❑ **Create a DCF rule that explicitly deny any kind of traffic based on the following requirements:**
  - Insert the rule below the previous created rules and above the Greenfield-Rule
  - Enable the Logging feature



Create Rule

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

Name: EXPLICIT-DENY-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 ● Logging ●

Action: Deny

SG Orchestration ⓘ: Off

TLS Decryption: Off

Rule Priority

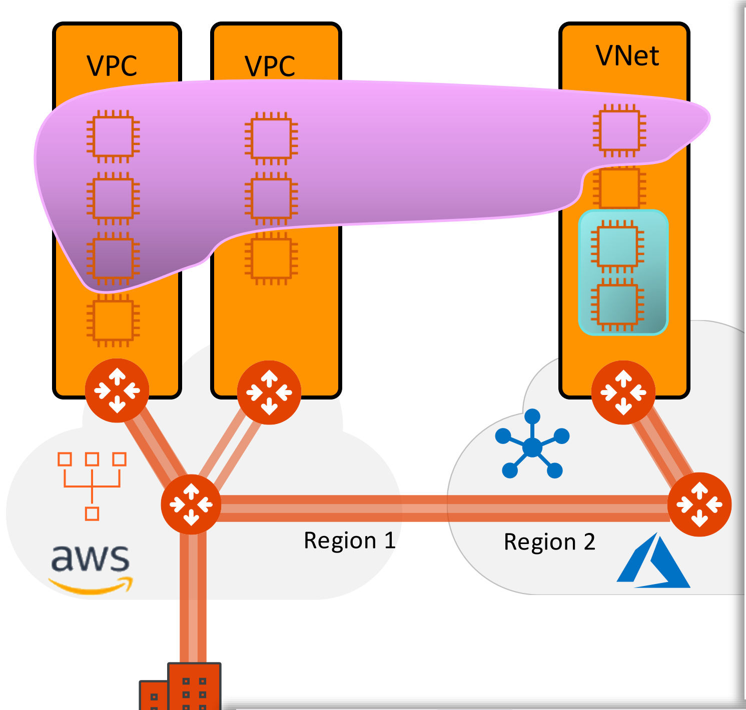
Place Rule: Above

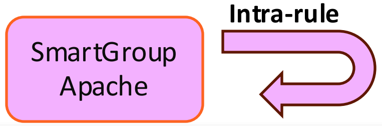
Existing Rule: Greenfield-Rule

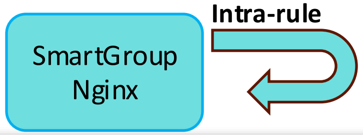
Monitoring

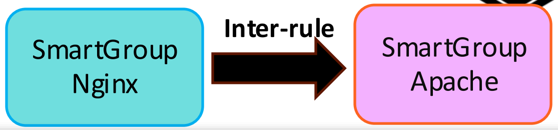
Rule Position

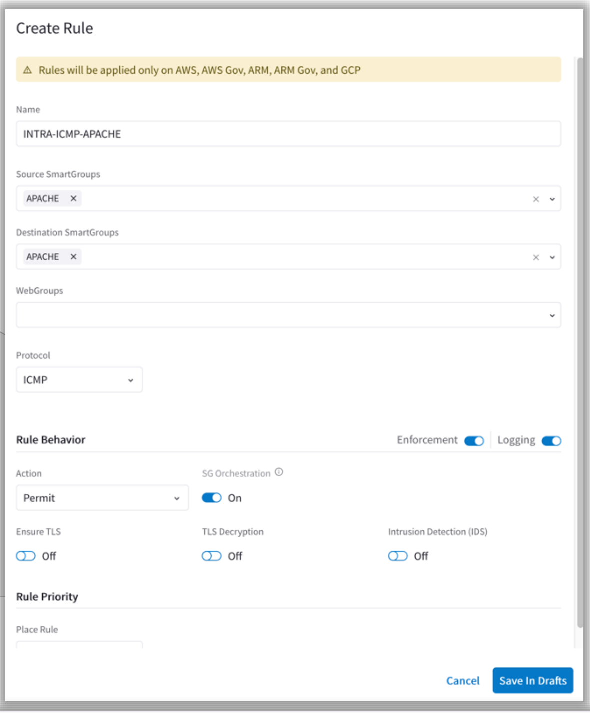
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (5)










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

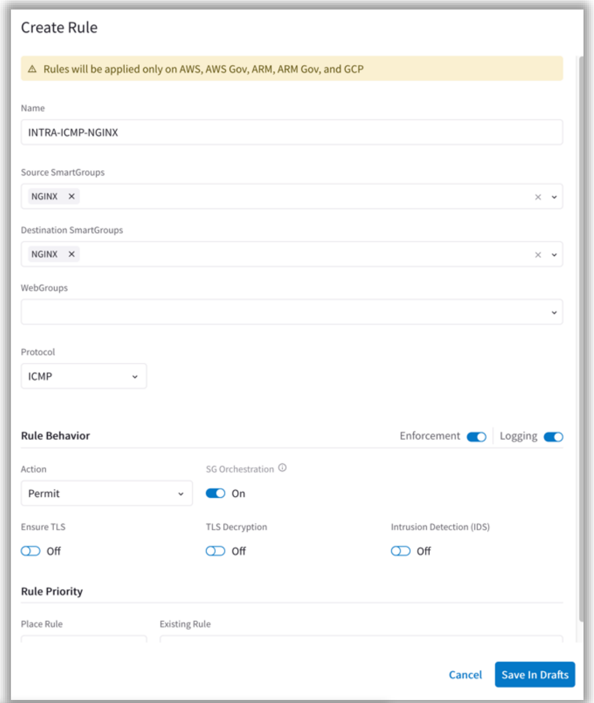
Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule


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

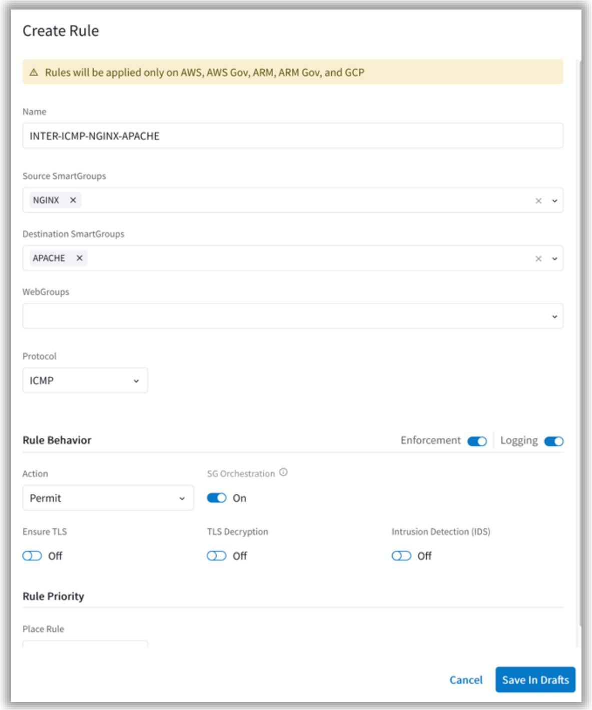
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

Existing Rule


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

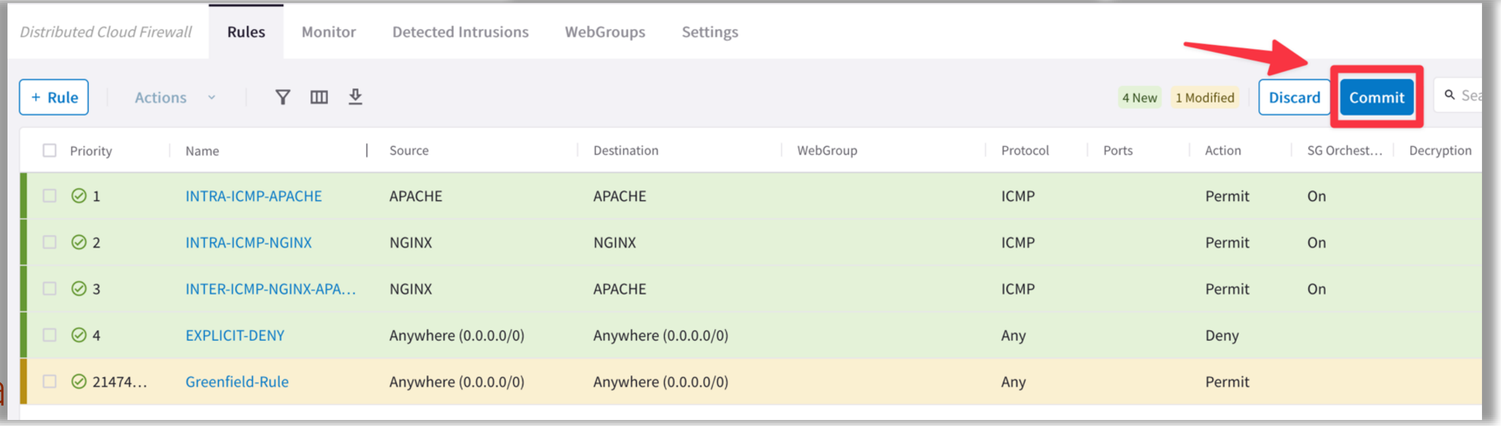
Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

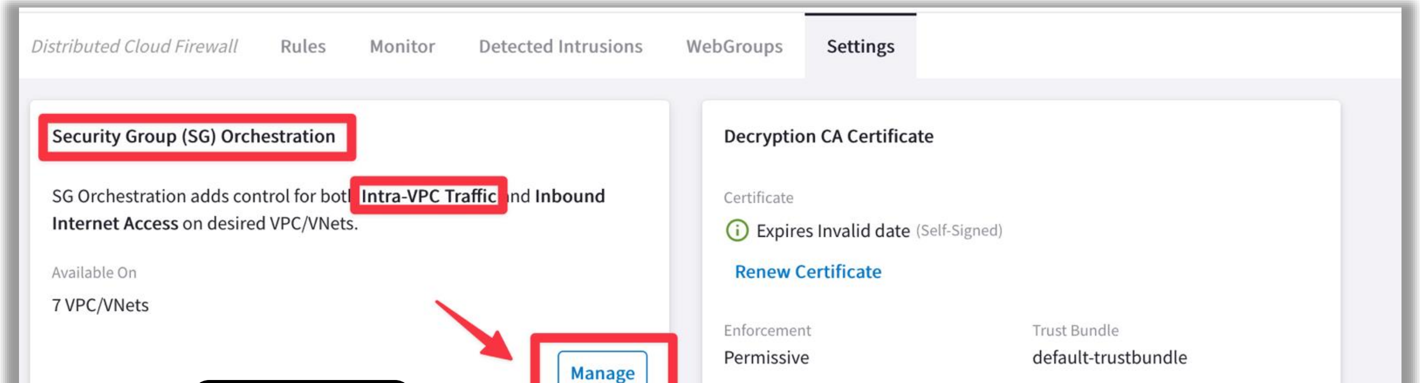


Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchest...	Decryption
1	INTRA-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
3	INTER-ICMP-NGINX-APA...	NGINX	APACHE		ICMP		Permit	On	
4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)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

- **What is the Micro-Segmentation?** It's a 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

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

❑ Enable the feature on the relevant VNets



Security Group (SG) Orchestration

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

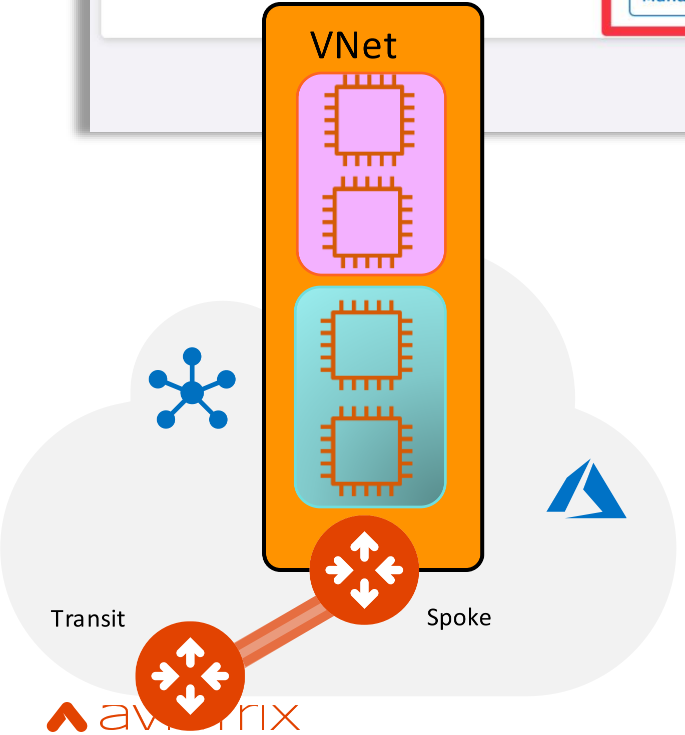
Available On: 7 VPC/VNets

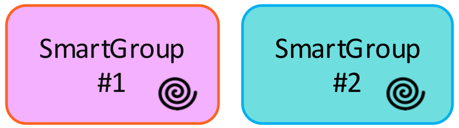
Decryption CA Certificate

Certificate: Expires Invalid date (Self-Signed)

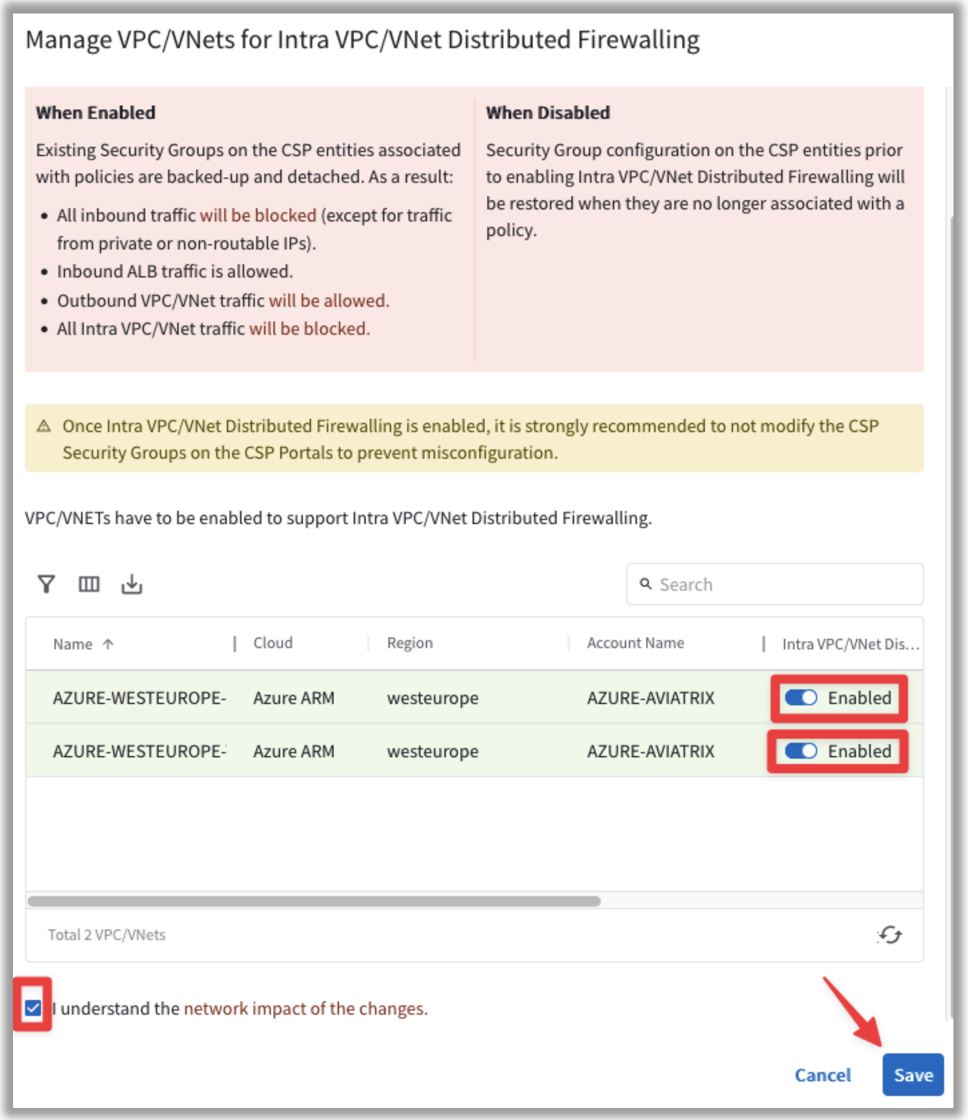
Enforcement: Permissive

Trust Bundle: default-trustbundle





- 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.

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.

AVIATRIX ACE ★★★ OPERATIONS SPECIALTY

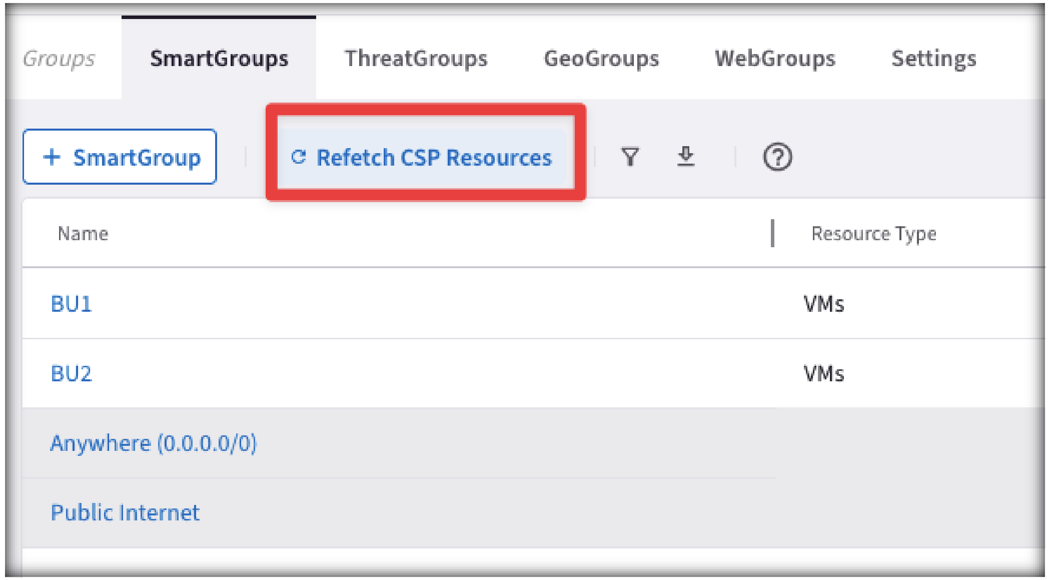
Tools for troubleshooting Distributed Cloud Firewall

Creation of the SmartGroup: the right matching criteria dilemma

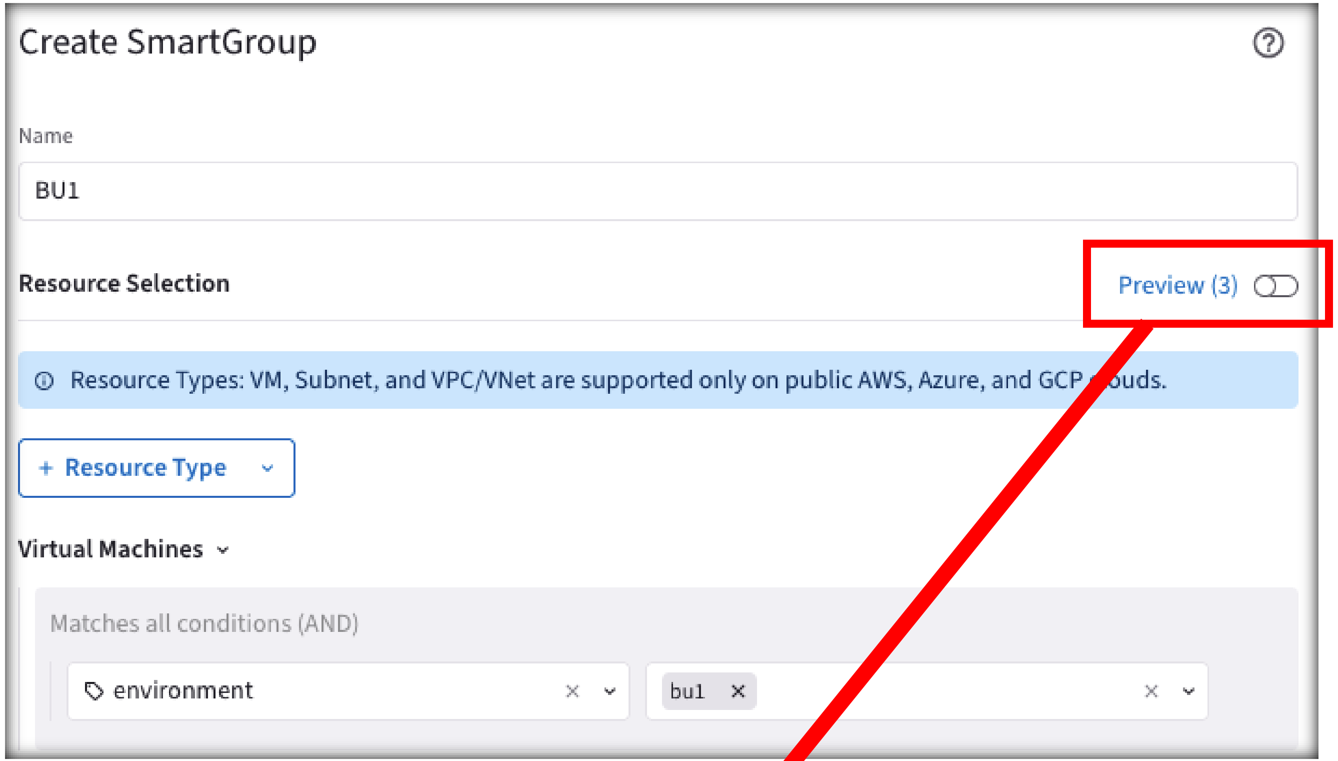
1) Choose the right matching criteria for resources that you want to see assigned to a specific SmartGroup:

2) Use the **Preview Resources** toggle switch to verify the selected resources that have been mapped to the Smart Group

3) Use the On-Demand **Refetch CSP Resources** button to retrieve the most recent inventory



Name	Resource Type
BU1	VMs
BU2	VMs
Anywhere (0.0.0.0/0)	
Public Internet	



Create SmartGroup

Name: BU1

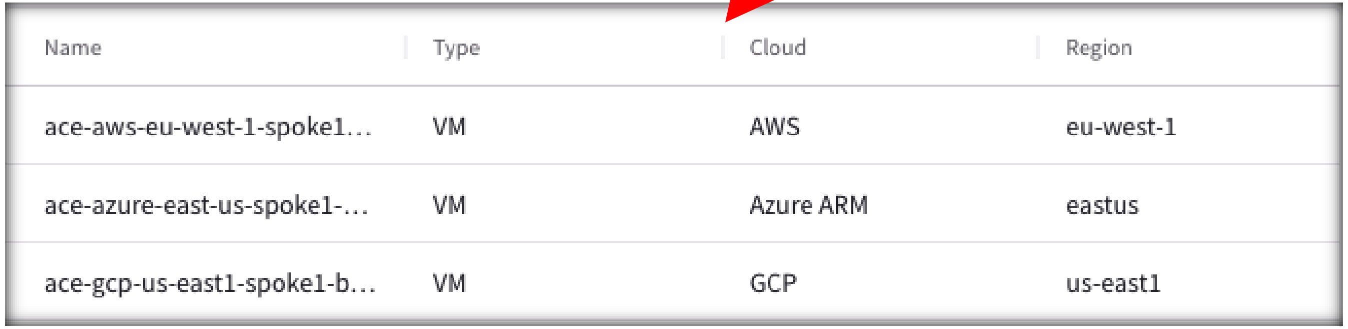
Resource Selection

Preview (3)

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

Matches all conditions (AND)

environment — bu1



Name	Type	Cloud	Region
ace-aws-eu-west-1-spoke1…	VM	AWS	eu-west-1
ace-azure-east-us-spoke1-…	VM	Azure ARM	eastus
ace-gcp-us-east1-spoke1-b…	VM	GCP	us-east1

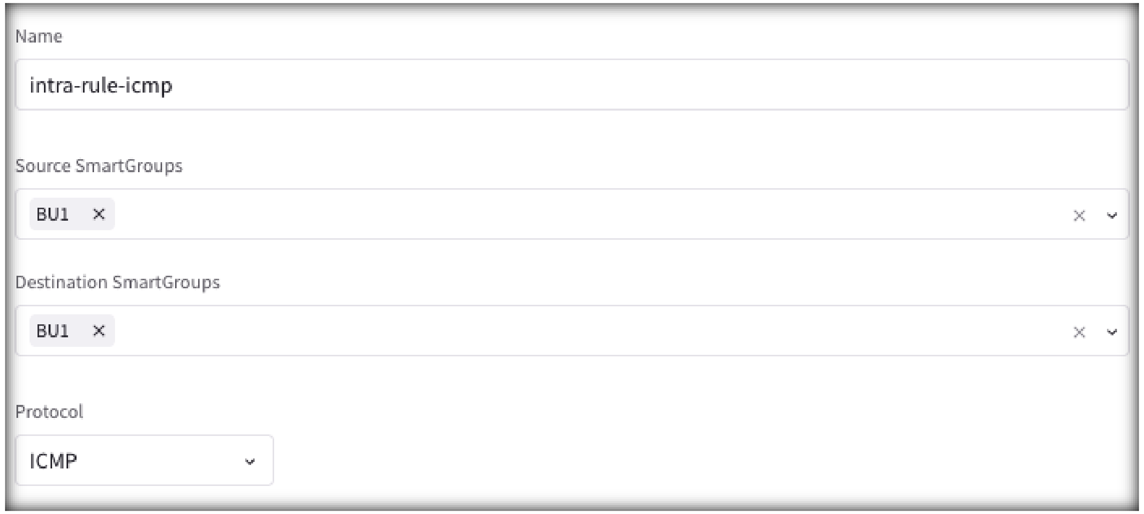
Creation of the Rules: intra-rule vs. inter-rule

1) **Intra-rule** will affect the traffic WITHIN a Smart Group

- ❑ Source Smart Group and Destination Smart Group must be the same

2) **Inter-rule** will affect the traffic BETWEEN SmartGroups

- ❑ Source Smart Group and Destination Smart Group must differ

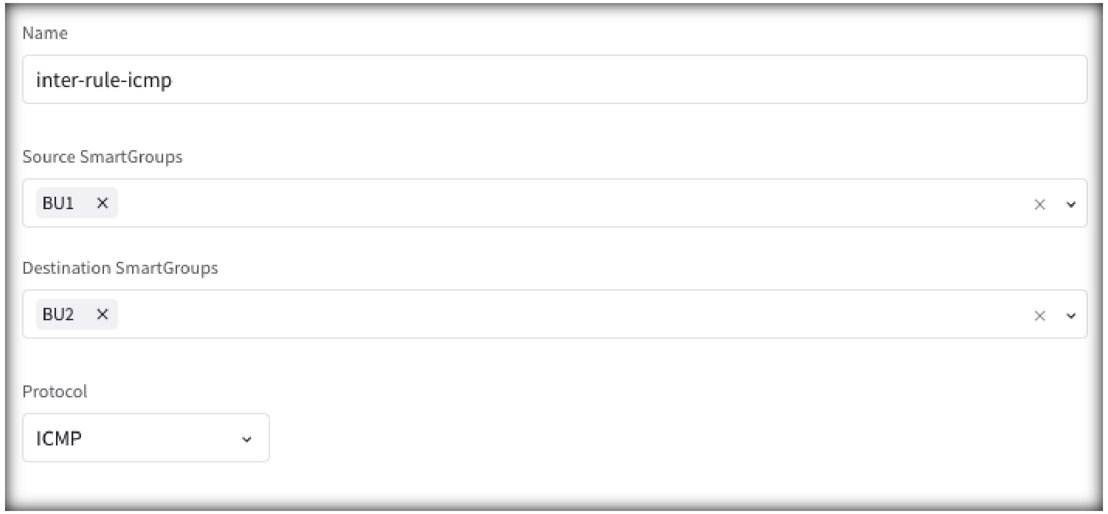


Name: intra-rule-icmp

Source SmartGroups: BU1 ×

Destination SmartGroups: BU1 ×

Protocol: ICMP



Name: inter-rule-icmp

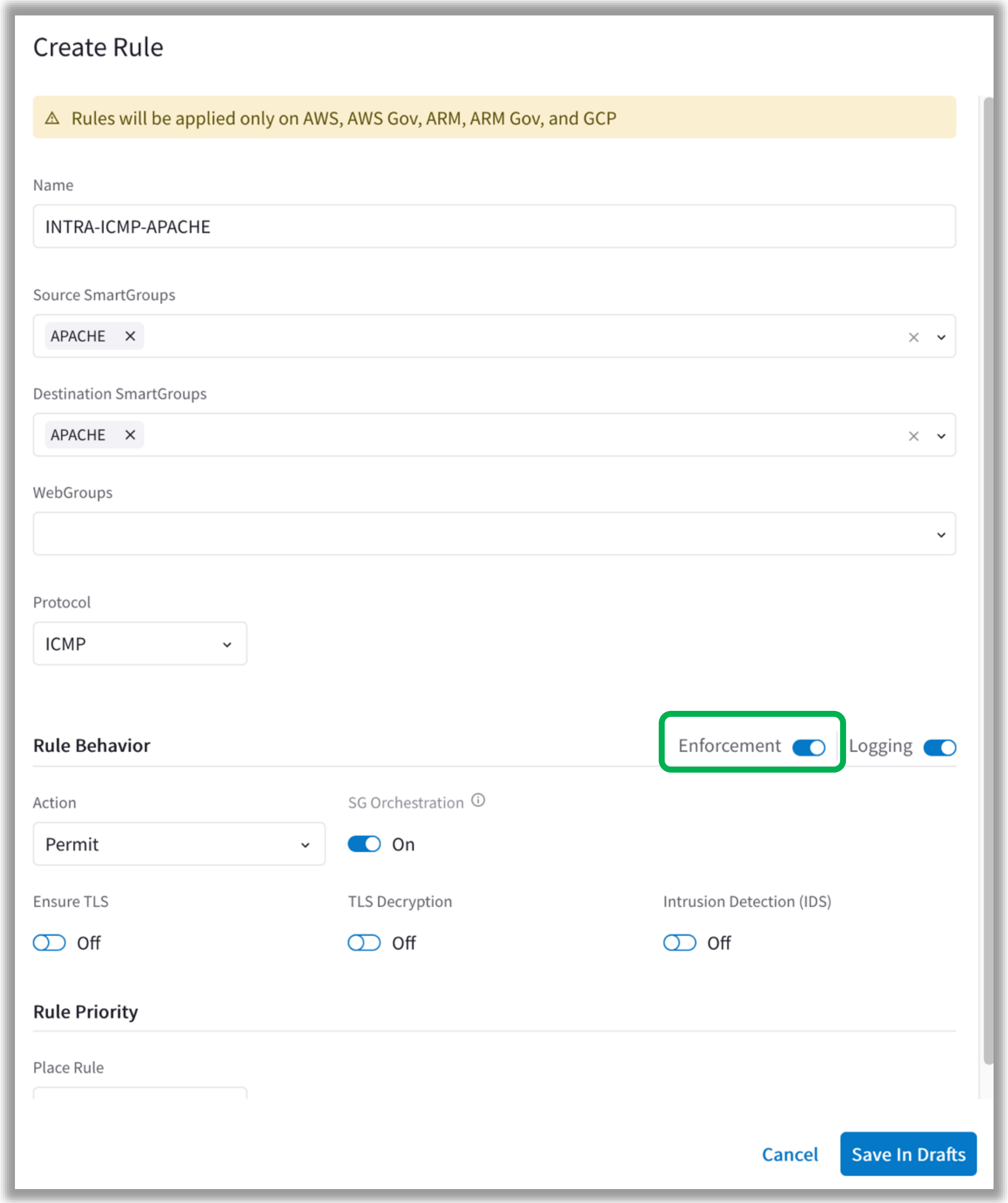
Source SmartGroups: BU1 ×

Destination SmartGroups: BU2 ×

Protocol: ICMP

CAVEAT – The Invisible Implicit Deny: as soon as a Rule is committed (either intra-rule or inter-rule) a hidden deny is applied at the bottom of your Rules list. The implicit deny is really an “invisible deny”; you won’t see a “deny any” line automagically added! Since you don’t see it, it’s easy to forget about. Forgetting about the implicit deny is the #1 reason for Distributed Firewalling Rule not giving you the desired results.

Rule Enforcement



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: On, Logging: On

Action: Permit

SG Orchestration ⓘ: On

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

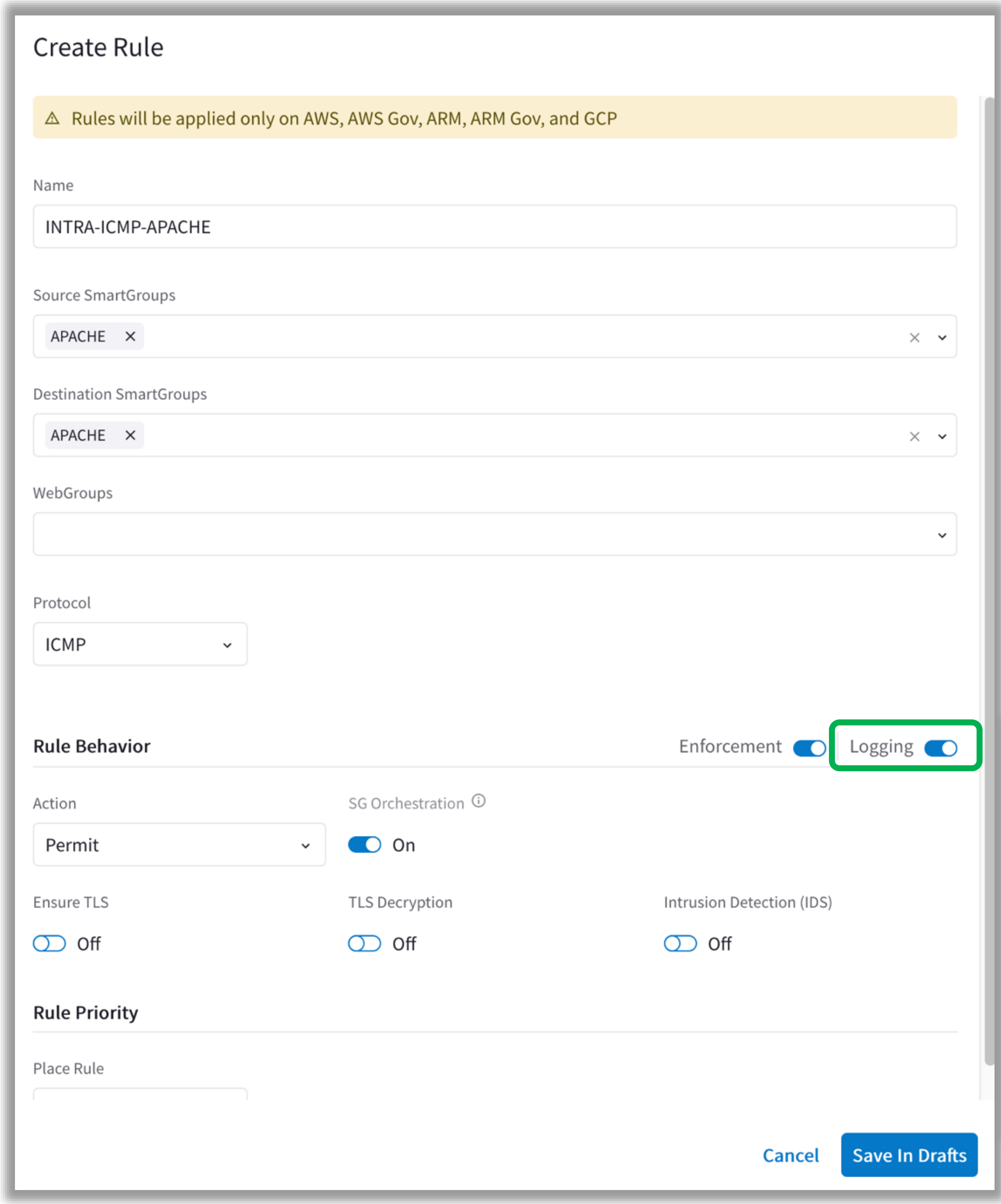
❑ Enforcement ON (enabled by default)

- 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: INTRA-ICMP-APACHE

Source SmartGroups: APACHE ✕

Destination SmartGroups: APACHE ✕

WebGroups:

Protocol: ICMP

Rule Behavior Enforcement ● Logging ●

Action: Permit

SG Orchestration ⓘ: On

Ensure TLS: Off

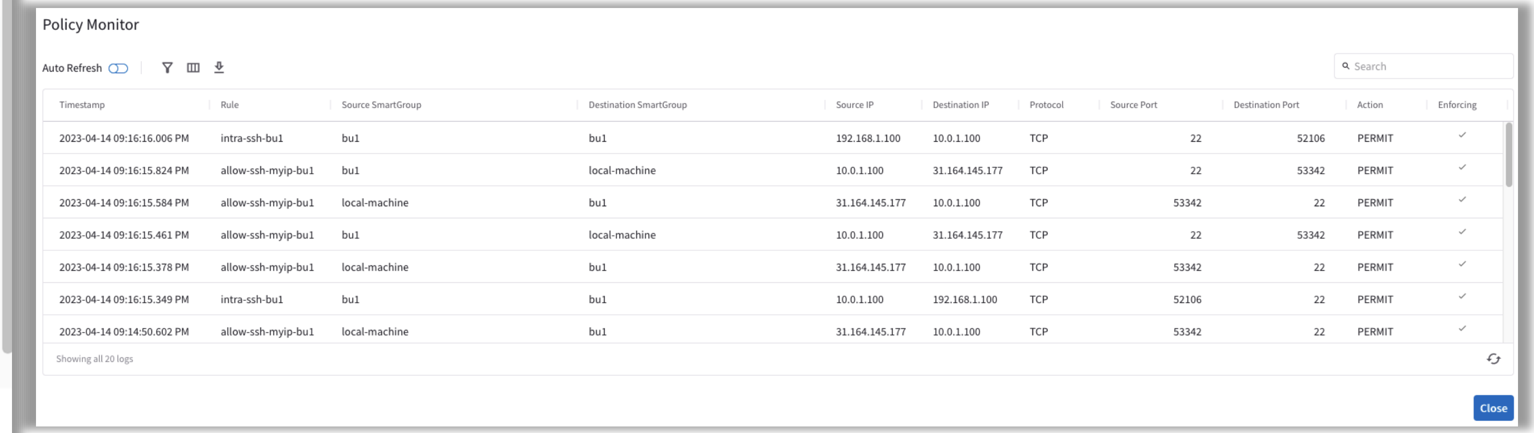
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

- Logging can be turned ON/OFF per rule
- Configure Syslog to view the logs
- To configure how many days to keep your Distributed Cloud Firewall logs, in CoPilot navigate to Settings > Resources > Disk Utilization and scroll down to Distributed Cloud Firewall Logs. Use the slider to select the number of days to retain your logs (<u>default is five days</u>).



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

Next:

Lab 8 Distributed Cloud Firewall