

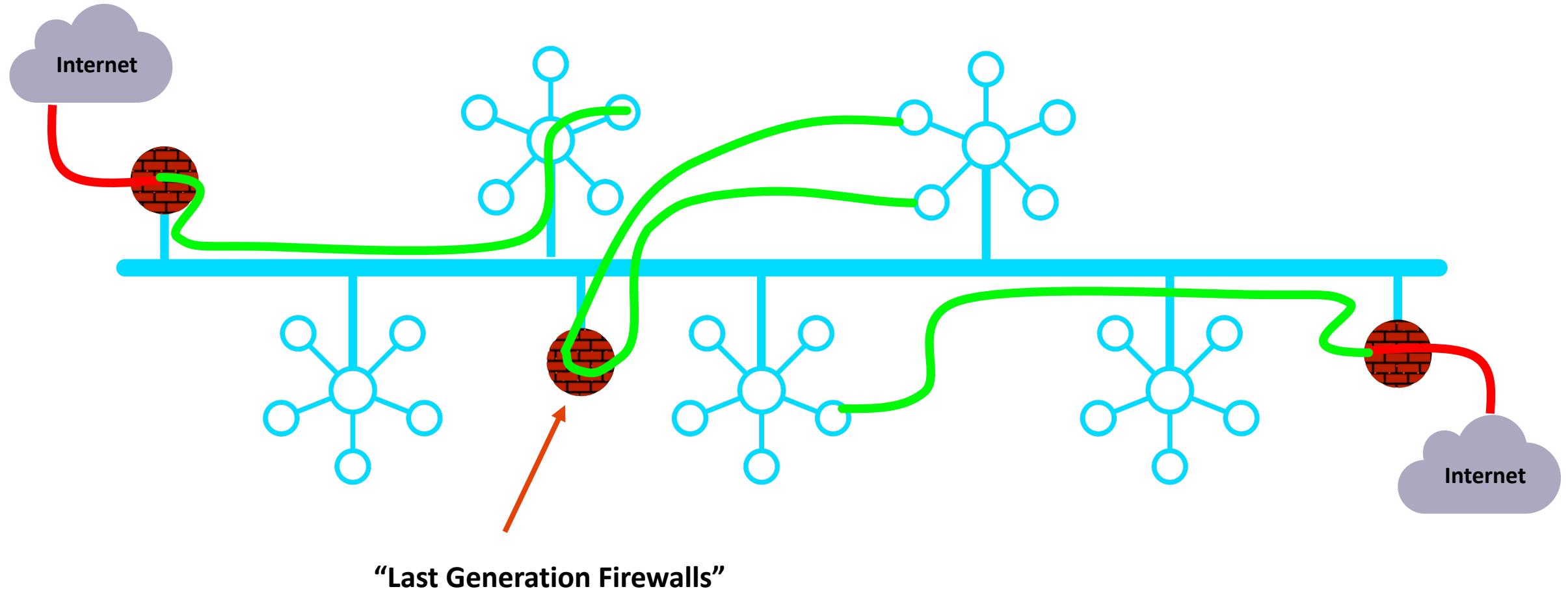


# Distributed Cloud Firewall

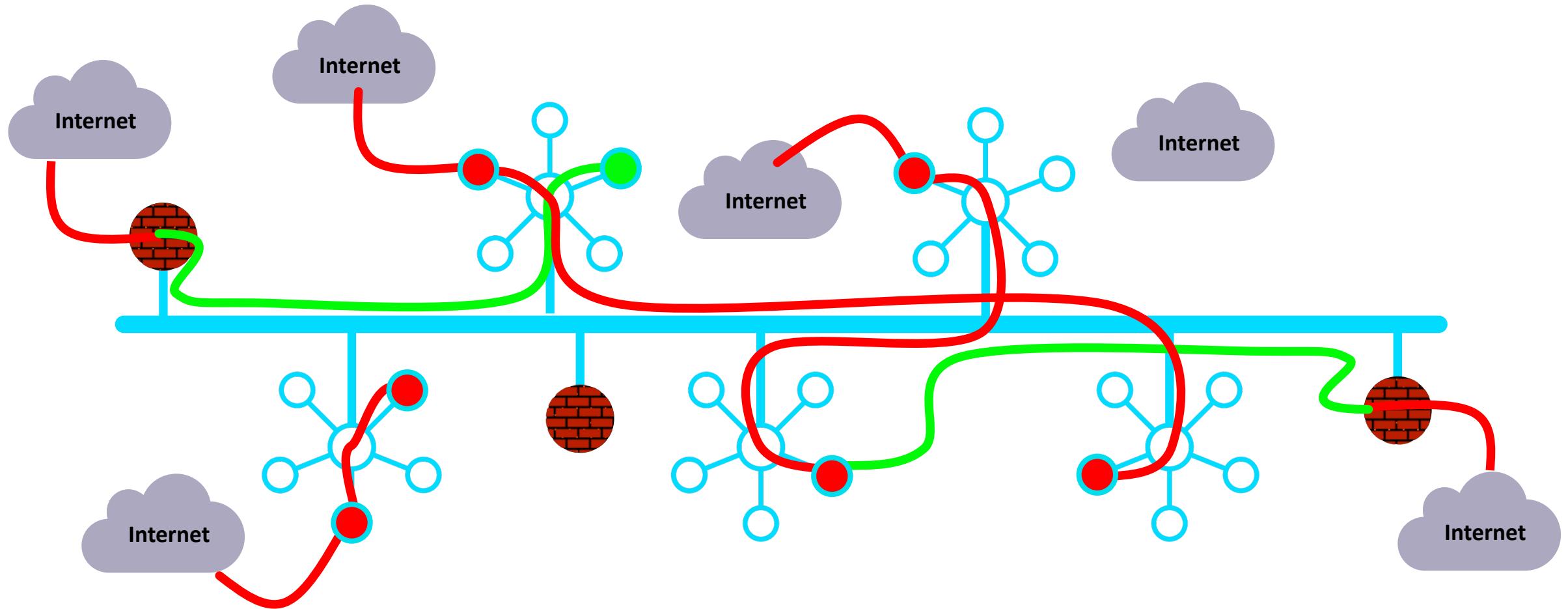
ACE Solutions Architecture Team



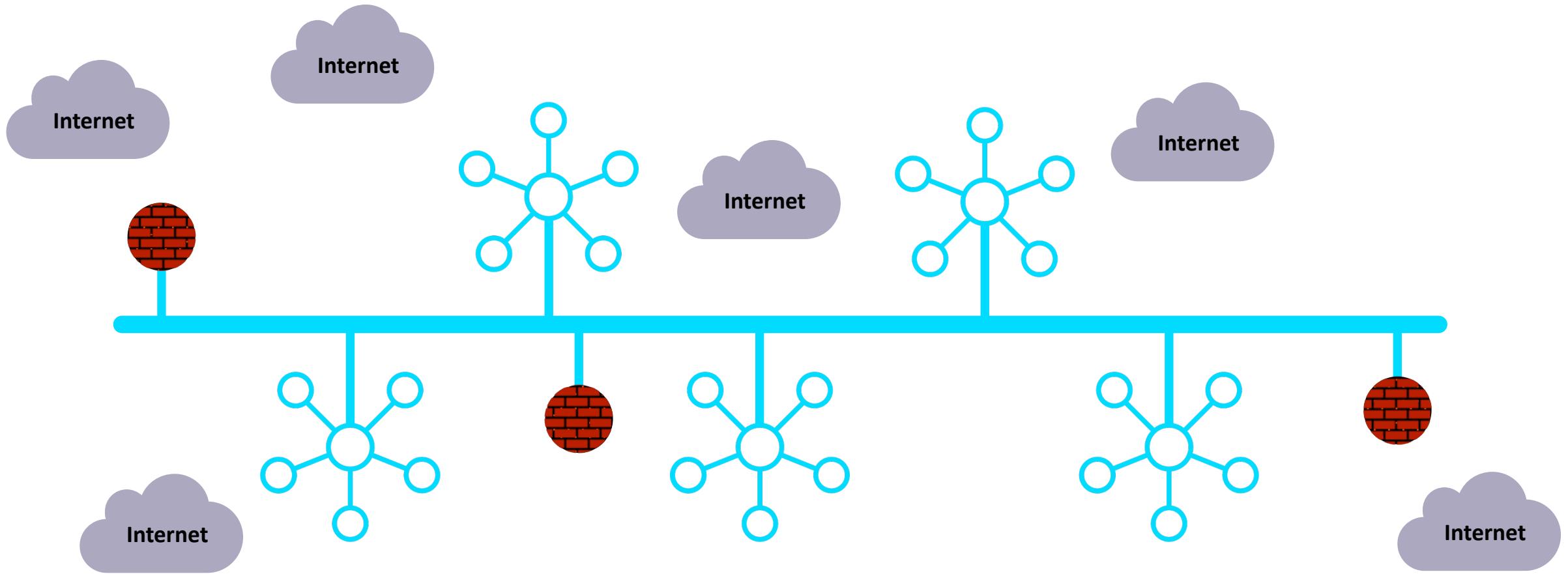
# As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



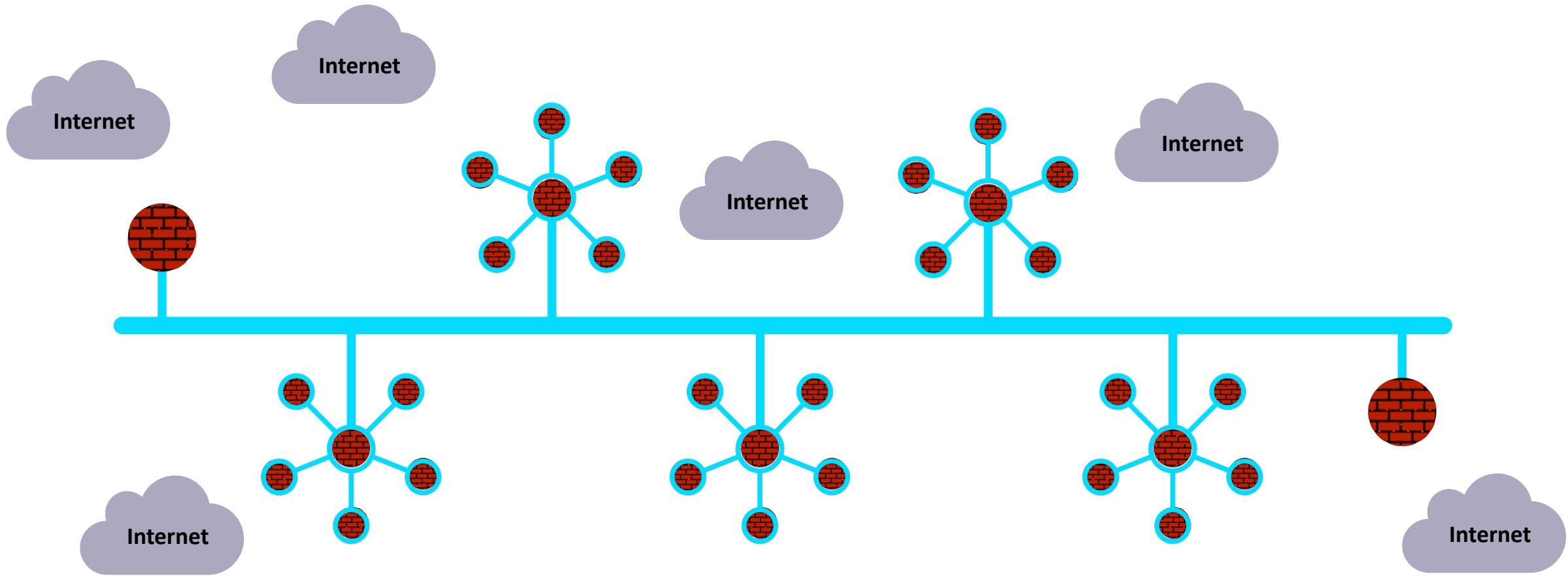
# In Reality...



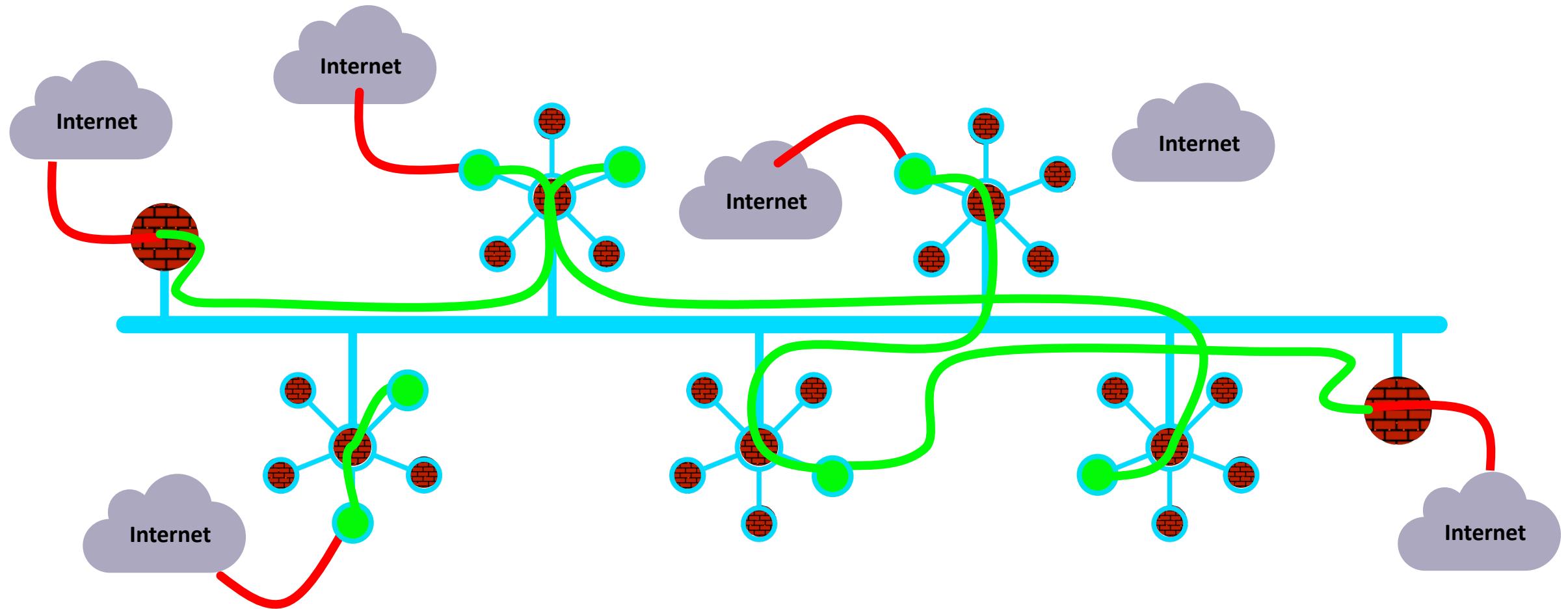
# What If... the architecture was built for cloud



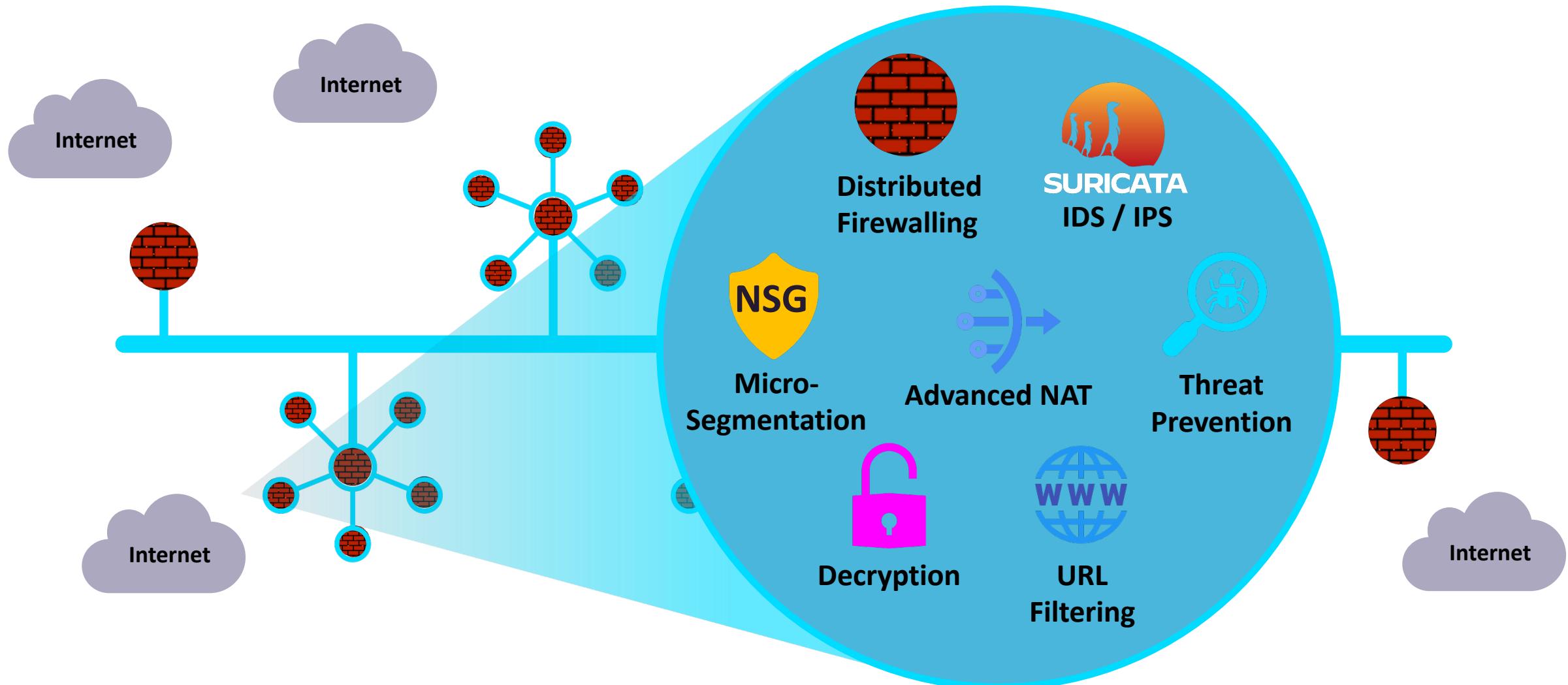
# Firewalling Functions were Embedded in the Cloud Network Everywhere...



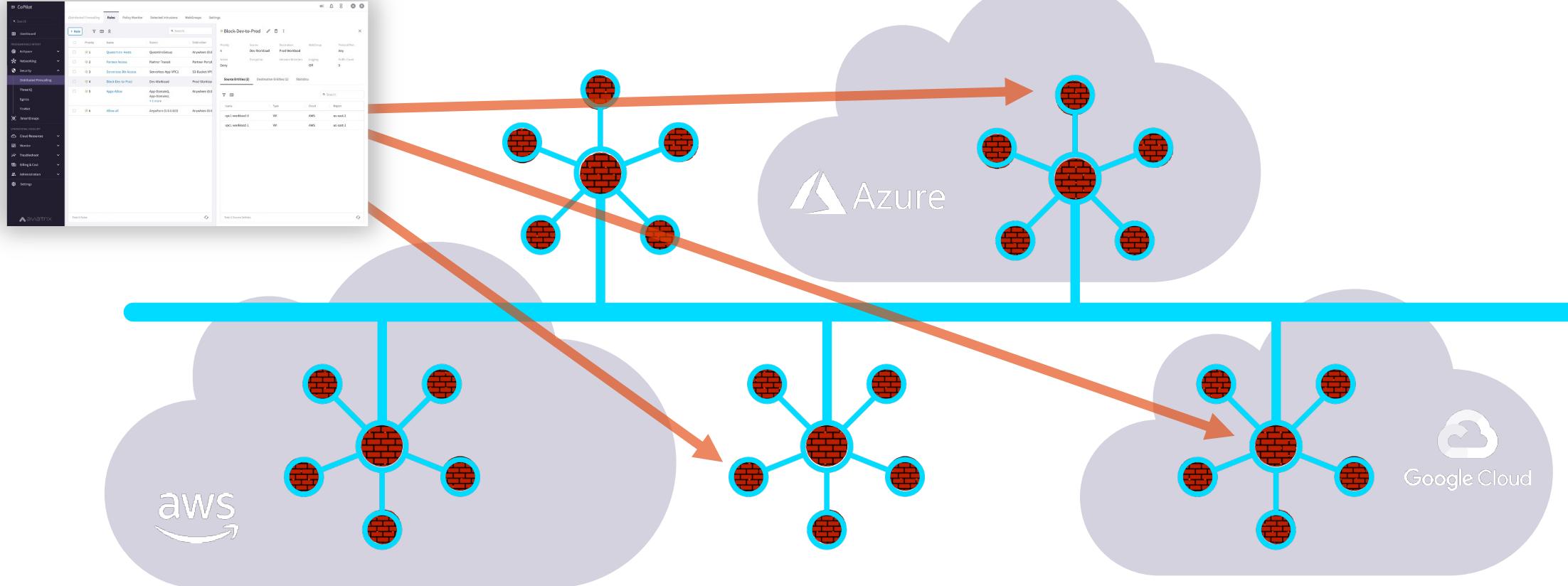
# Centrally Managed, with Distributed Inspection & Enforcement...



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



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



**Where and How Policies Are Enforced Is Abstracted...**

# 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}

Instance: i-0380038ff7d66b66f (shopping cart app)

Select an instance above

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

### Tags



#### Key

Env

#### Value

Staging

#### Name

shopping cart app

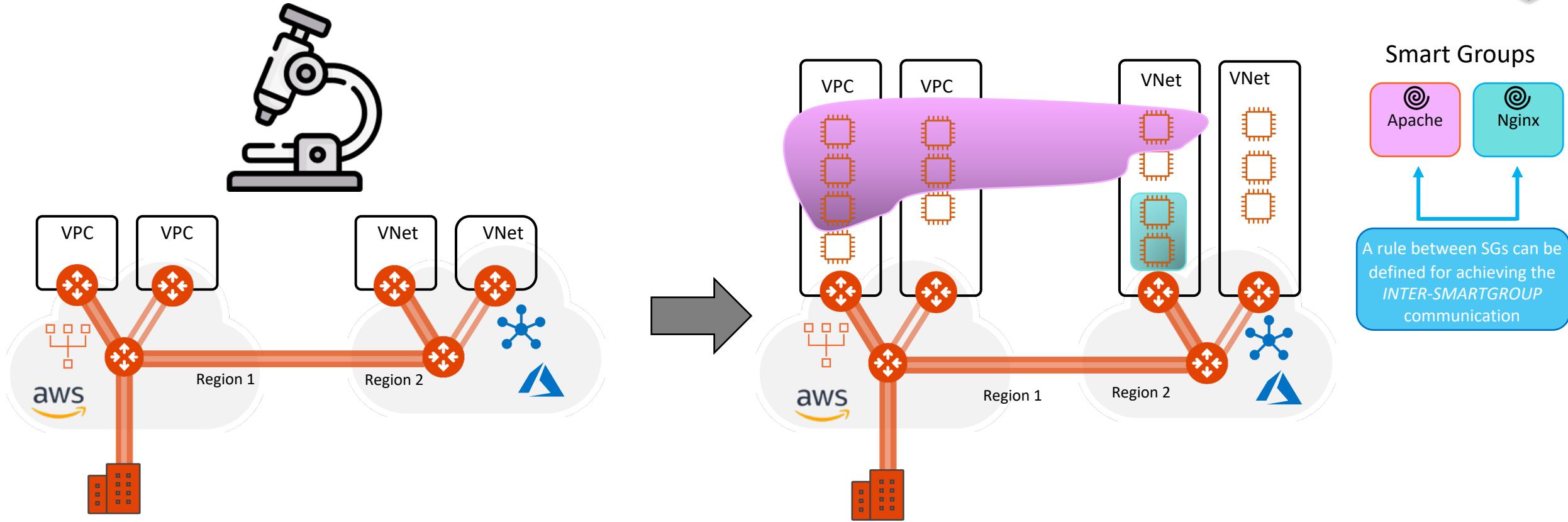
## Resource attribute

- Region Name, Account Name

## IP Prefixes

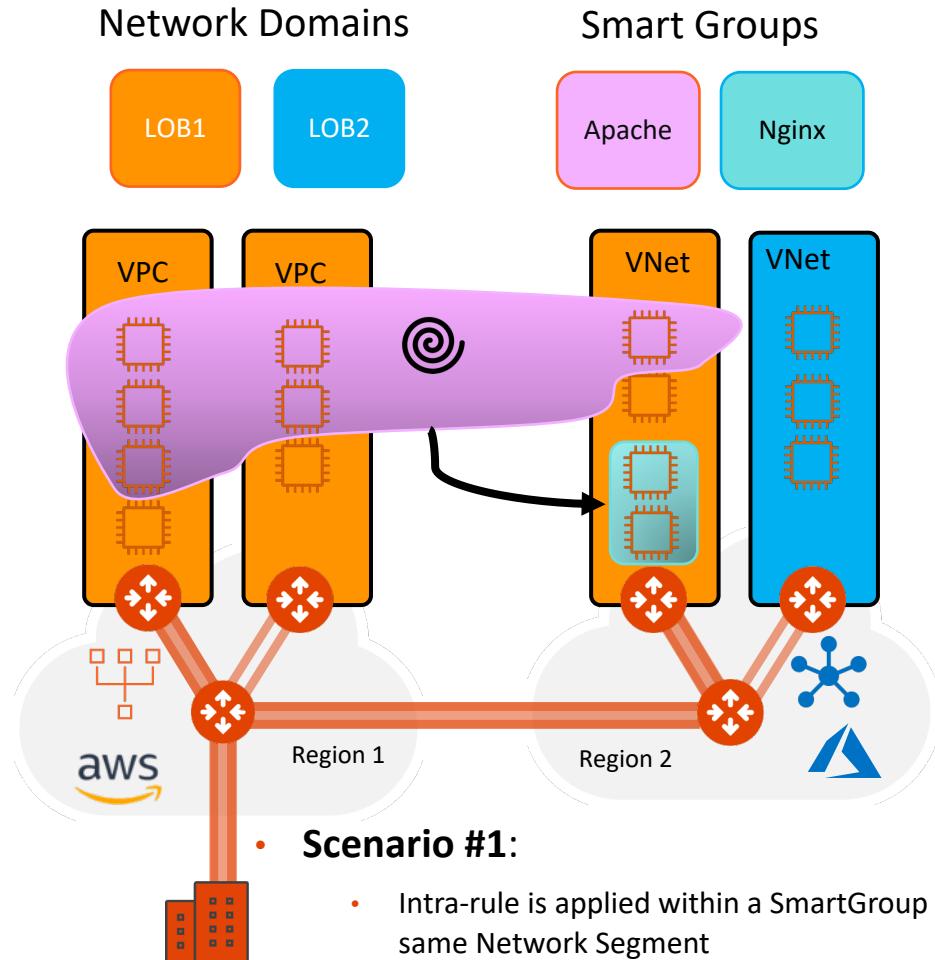
- CIDR

# 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
- **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

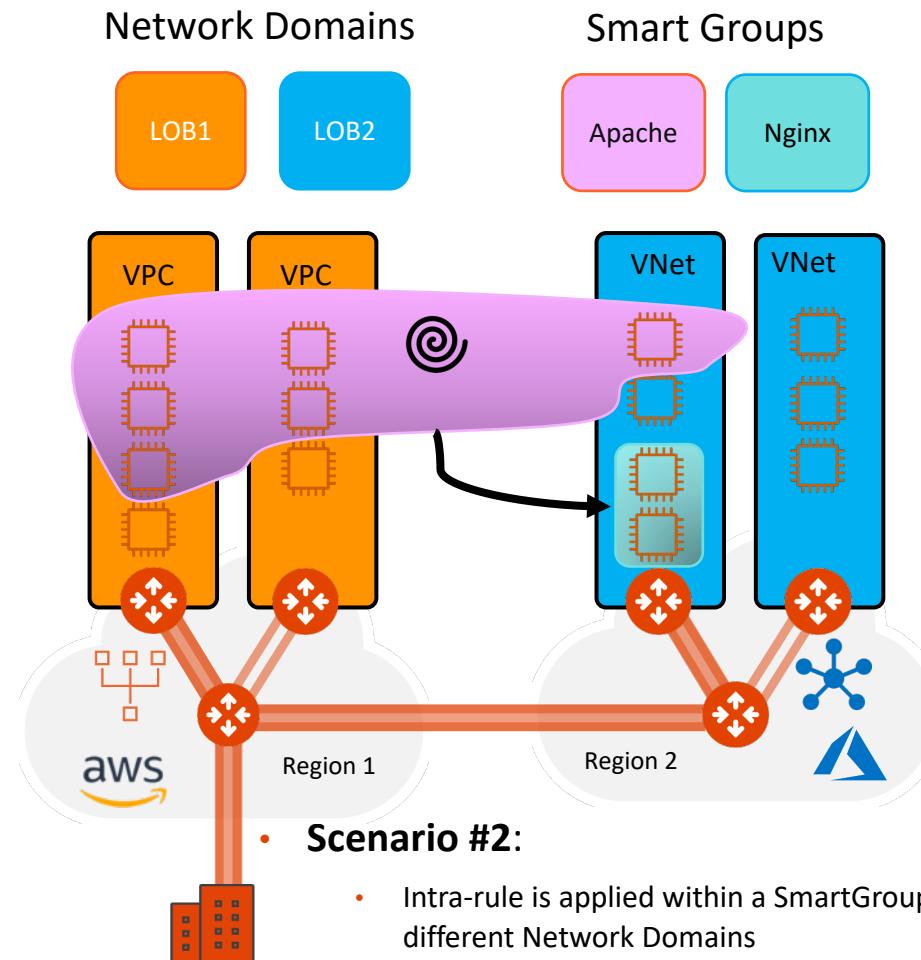


- **Scenario #1:**

- Intra-rule is applied within a SmartGroup defined in the same Network Segment
- Inter-rule is applied between SmartGroups within the same network Domain

*Caveat:*

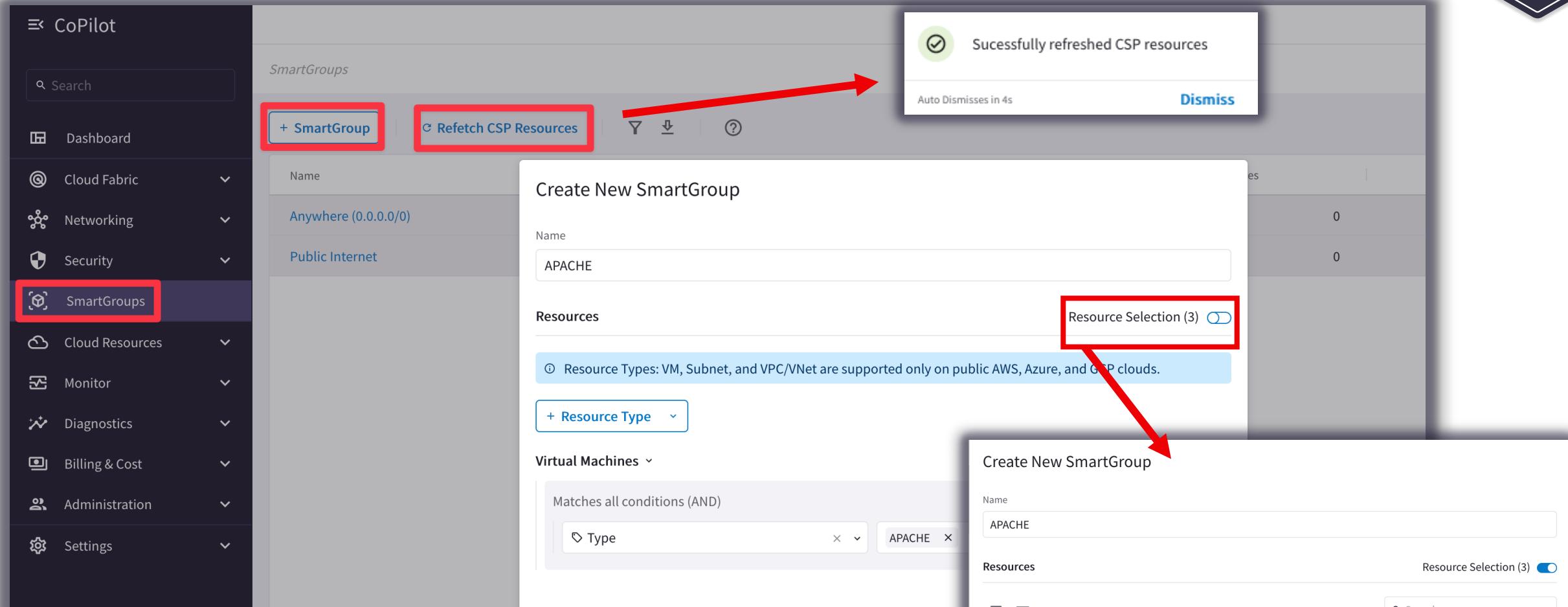
- Network Segmentation and Distributed Firewalling are **NOT** mutually exclusive!
- Network Segmentation takes **precedence** over the extent of a SmartGroup



- **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

# Smart Groups Creation



The screenshot shows the Aviatrix CoPilot interface with the 'SmartGroups' tab selected in the sidebar. A red box highlights the '+ SmartGroup' button. Another red box highlights the 'Refetch CSP Resources' button. A red arrow points from the top right towards a success message: 'Successfully refreshed CSP resources' with a dismiss button. A red box highlights the 'Resource Selection (3)' toggle switch in the 'Create New SmartGroup' dialog. A red arrow points from this dialog to a second 'Create New SmartGroup' dialog where the same resource selection is shown.

**Create New SmartGroup**

- Name: APACHE
- Resources: Resource Selection (3) (Toggle switch)
- Info: Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.
- Add Resource Type: + Resource Type
- Virtual Machines: Matches all conditions (AND)
  - Type: APACHE

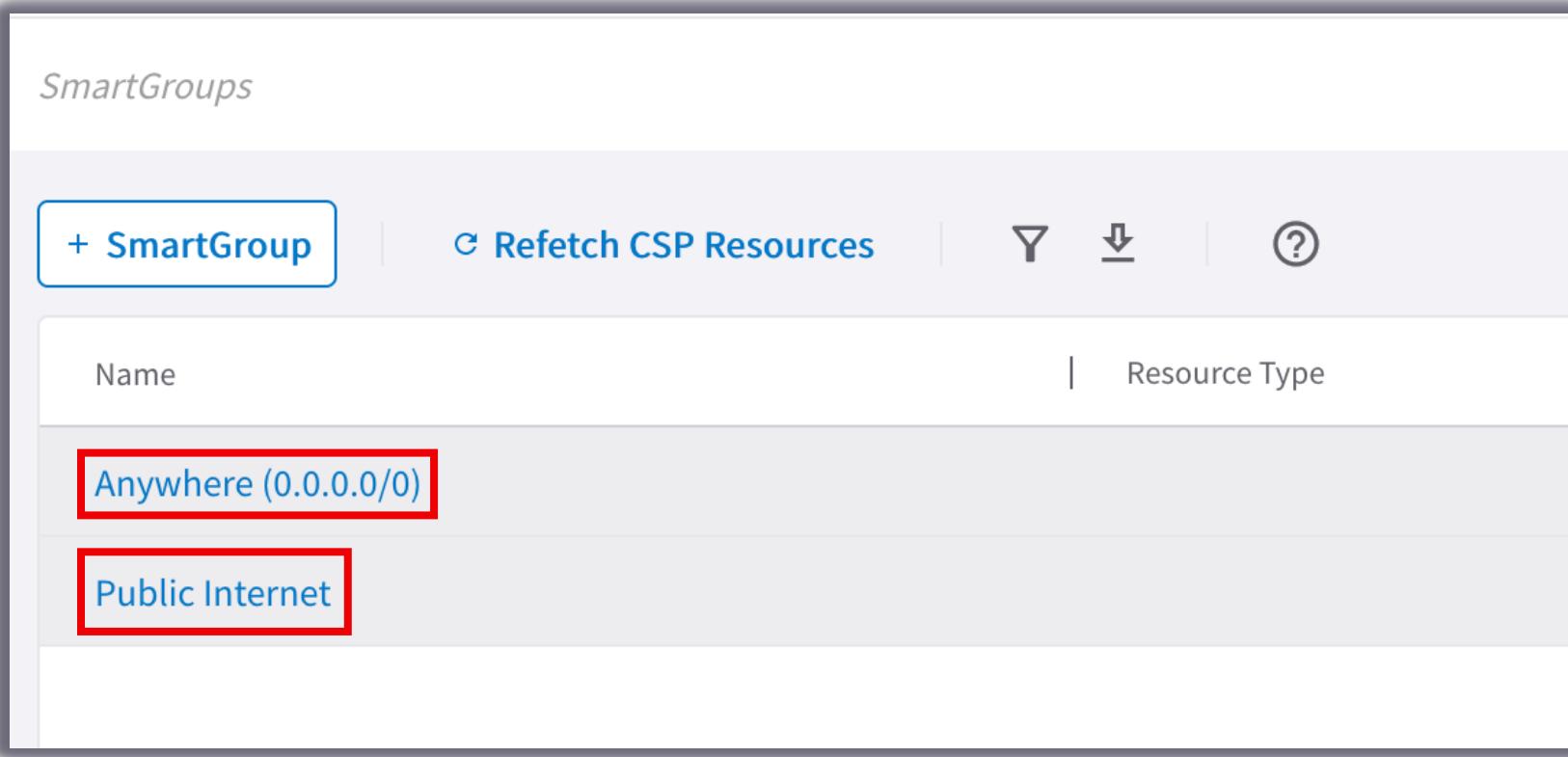
**Create New SmartGroup**

- Name: APACHE
- Resources: Resource Selection (3) (Toggle switch)
- Table:
 

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 Smart Groups

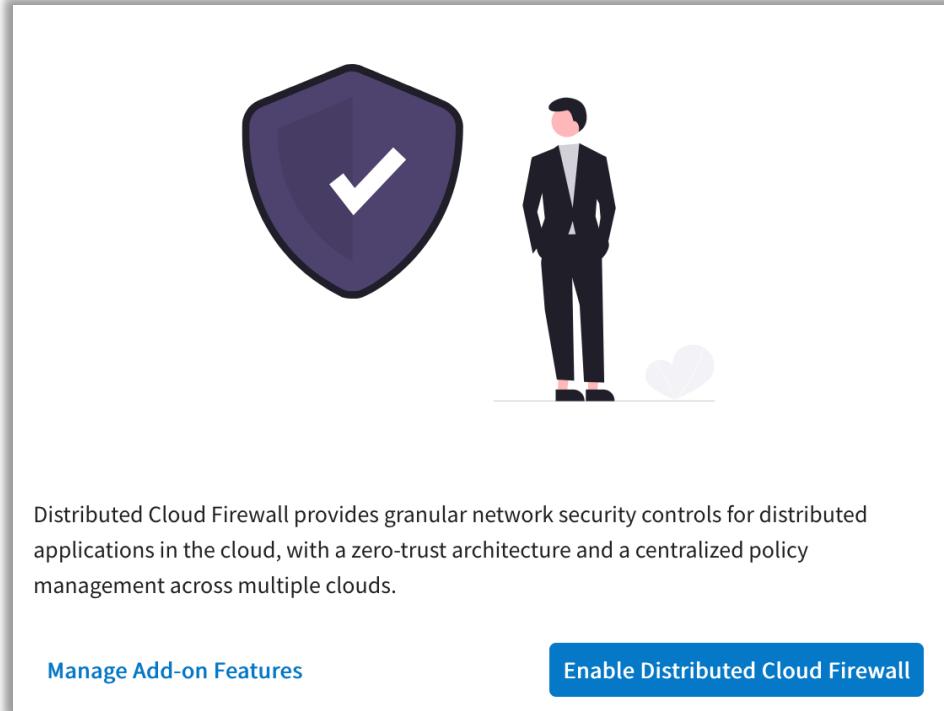


The screenshot shows a user interface for managing Smart Groups. At the top left is the title "SmartGroups". Below it is a toolbar with a "SmartGroup" button (highlighted with a red border), a "Refetch CSP Resources" button, and other icons for search, sort, and help. The main area has two columns: "Name"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

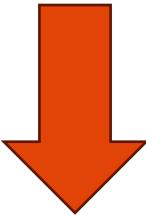
Name	Resource Type
Anywhere (0.0.0.0/0)	
Public Internet	

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

# Enabling Distributed Cloud Firewall

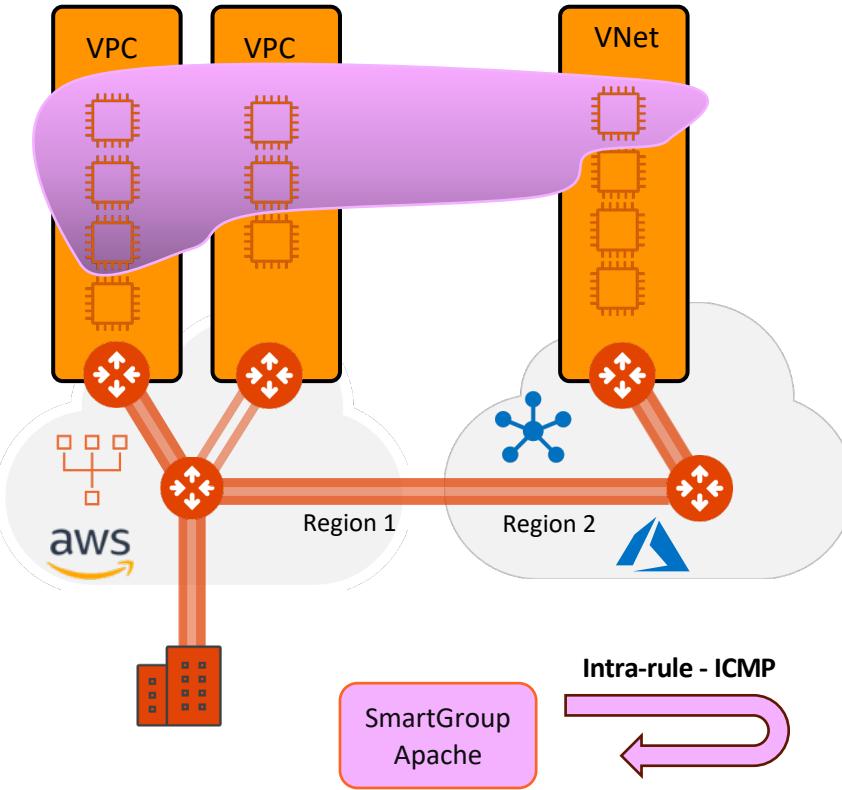


- Enabling the Distributed Cloud Firewall without configured rules will deny all previously permitted traffic due to its implicit Deny All rule.
- To maintain consistency, a **Greenfield Rule** will be created to allow traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.



Distributed Cloud Firewall		Rules	Monitor	Detected Intrusions	WebGroups	Settings	
<a href="#">+ Rule</a>	<a href="#">Actions</a> <a href="#">▼</a>	<a href="#">Y</a> <a href="#">☰</a> <a href="#">▼</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

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



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

**Intra-rule**

WebGroups: [empty]

Rule Behavior

Action: Permit

SG Orchestration: On

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Enforcement:  Logging:

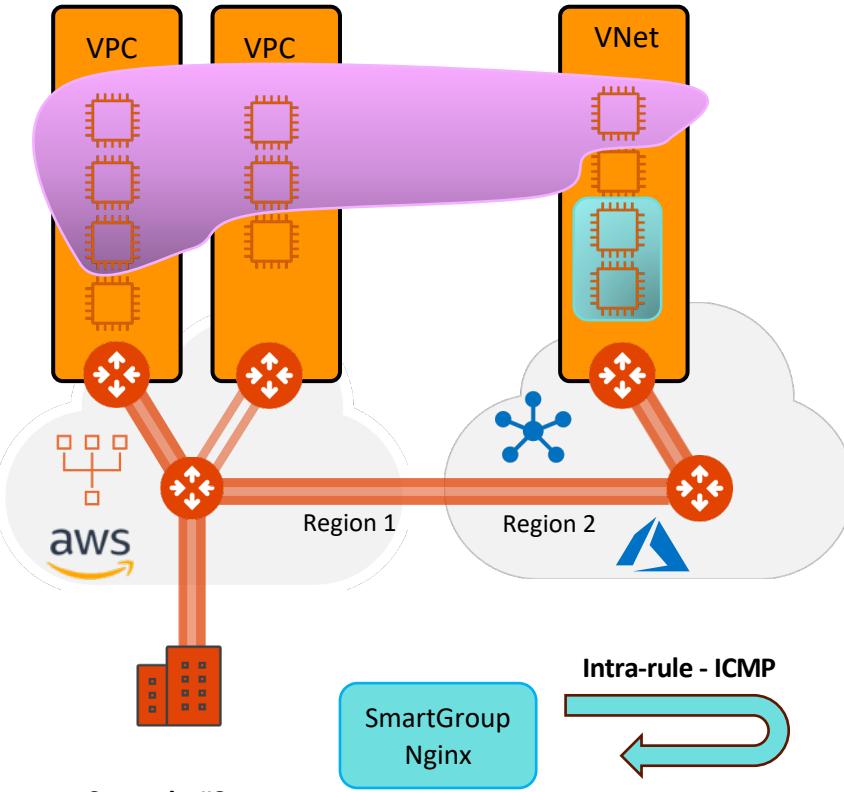
Rule Priority

Place Rule: [empty]

Cancel Save In Drafts

**Monitoring**

# Micro-Segmentation: SmartGroups, Intra-Rules and Inter-Rules (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 (highlighted with a teal border)

Destination SmartGroups: NGINX (highlighted with a teal border)

Protocol: ICMP

**Intra-rule**

Rule Behavior

Action: Permit (highlighted with a teal border)

SG Orchestration: On (highlighted with a teal border)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Enforcement:  Logging (highlighted with a teal border)

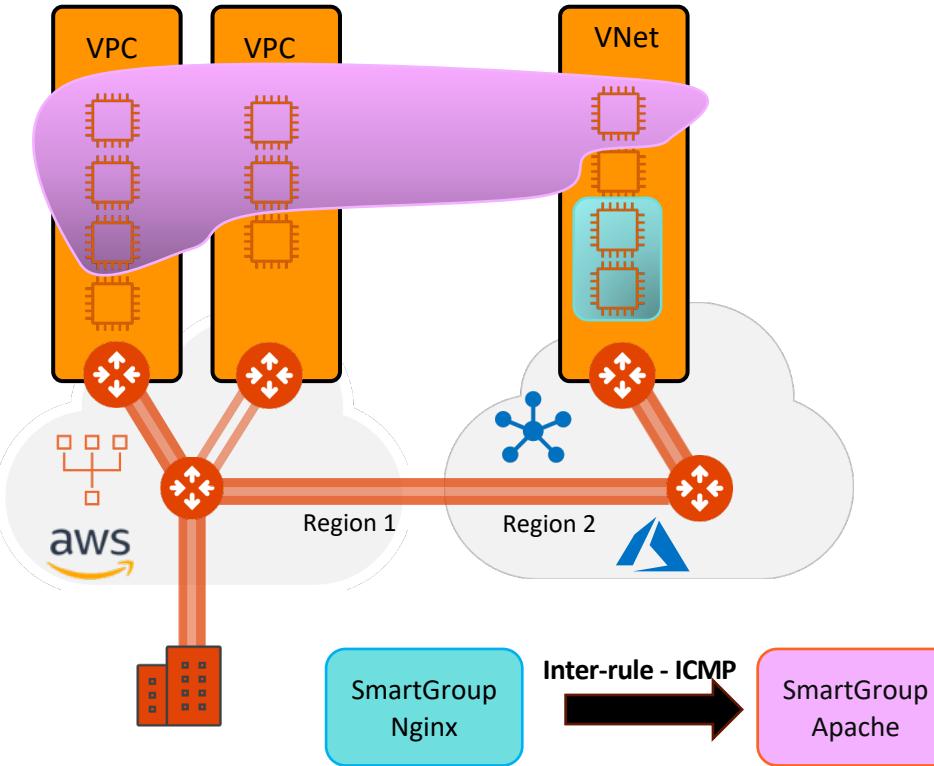
Rule Priority

Place Rule: Existing Rule

Cancel Save In Drafts

Monitoring

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



Create Rule
Cancel
Save In Drafts

⚠ 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

Rule Behavior:

- Action: Permit
- SG Orchestration: On
- Ensure TLS: Off
- TLS Decryption: Off
- Intrusion Detection (IDS): Off

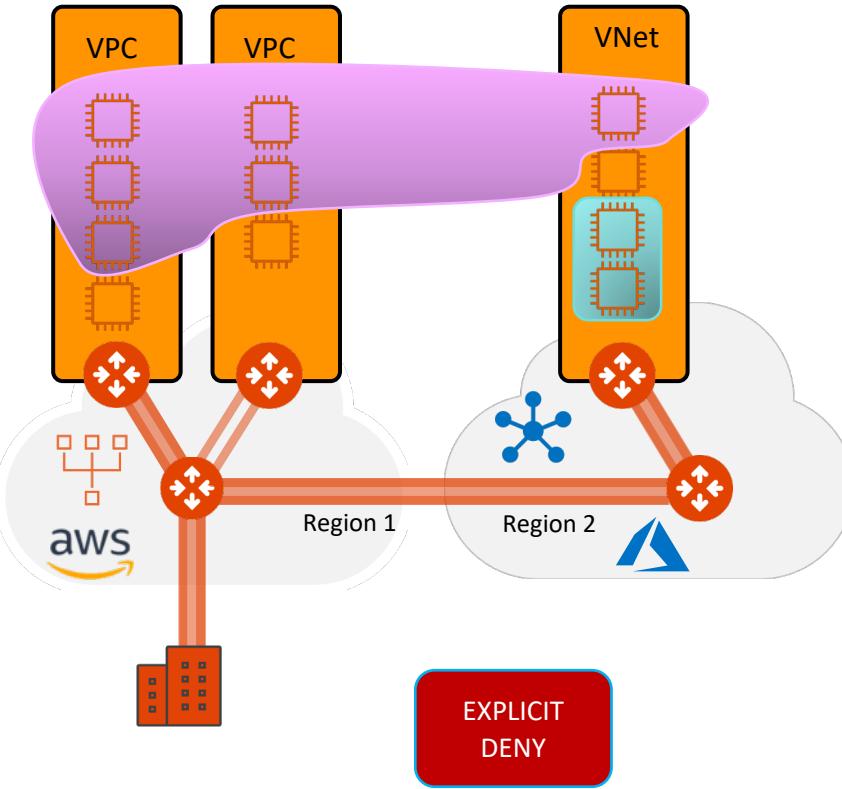
Enforcement:  Logging:

Rule Priority: Place Rule

**Inter-rule**

**Monitoring**

# Micro-Segmentation: SmartGroups, Intra-Rules and Inter-Rules (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

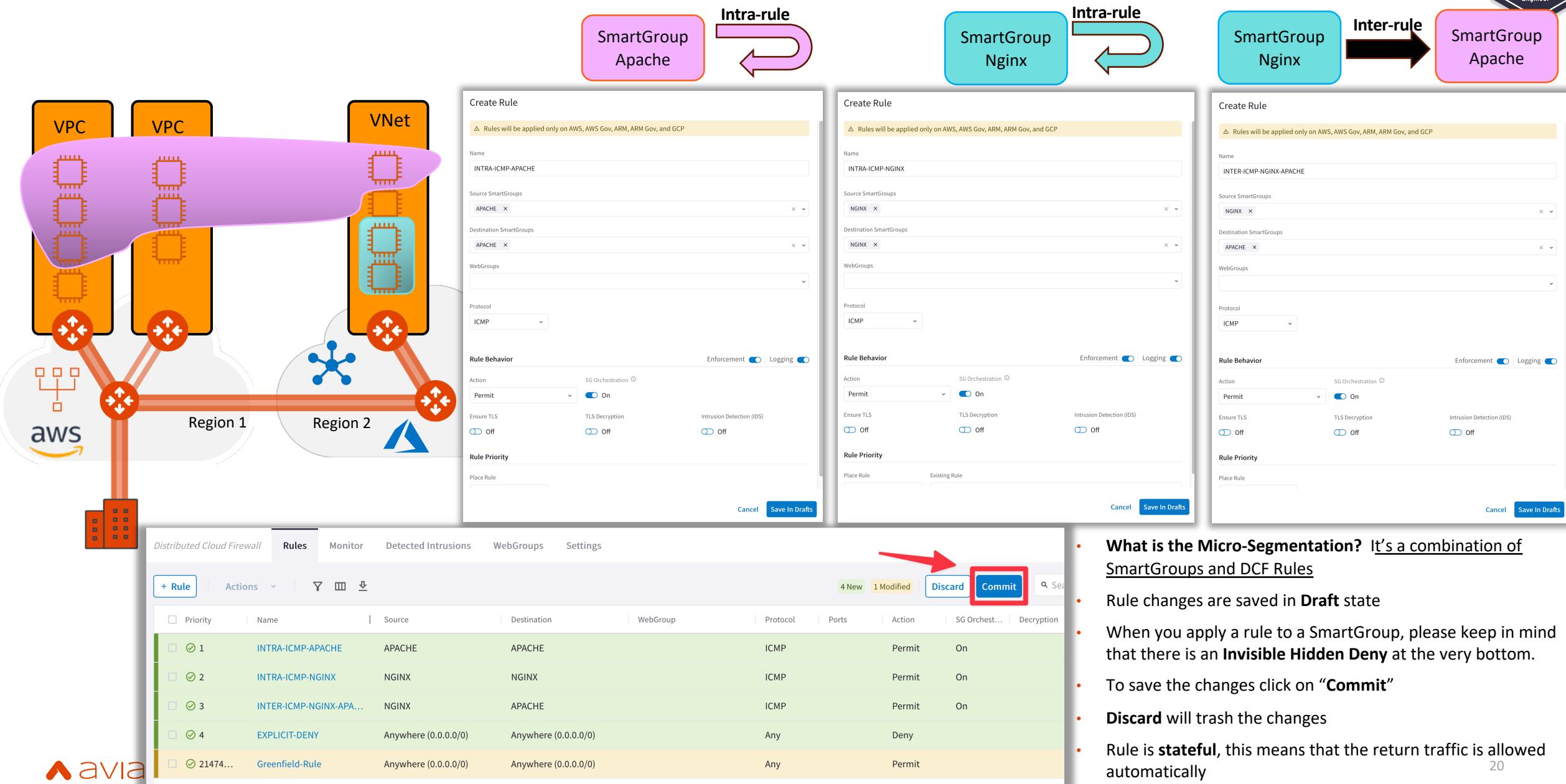
Rule Priority: Place Rule: Existing Rule: Above   Greenfield-Rule  

Monitoring  

Rule Position  

Cancel Save In Drafts

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



The diagram illustrates a Micro-Segmentation architecture across two regions, Region 1 and Region 2. It shows two VPCs connected via a VNet. Three SmartGroups are defined: SmartGroup Apache (orange), SmartGroup Nginx (blue), and SmartGroup Nginx (orange). Each SmartGroup has an Intra-rule (allowing communication between its members) and an Inter-rule (allowing communication from one group to another).

The Aviatrix Distributed Cloud Firewall interface shows the rule creation and management process:

- Create Rule (SmartGroup Apache):** 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. Enforcement: Off. Logging: On. Rule Priority: Place Rule.
- Create Rule (SmartGroup Nginx):** 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. Enforcement: Off. Logging: Off. Rule Priority: Existing Rule.
- Create Rule (SmartGroup Nginx to SmartGroup Apache):** 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. Enforcement: Off. Logging: Off. Rule Priority: Place Rule.

The interface also shows a table of rules:

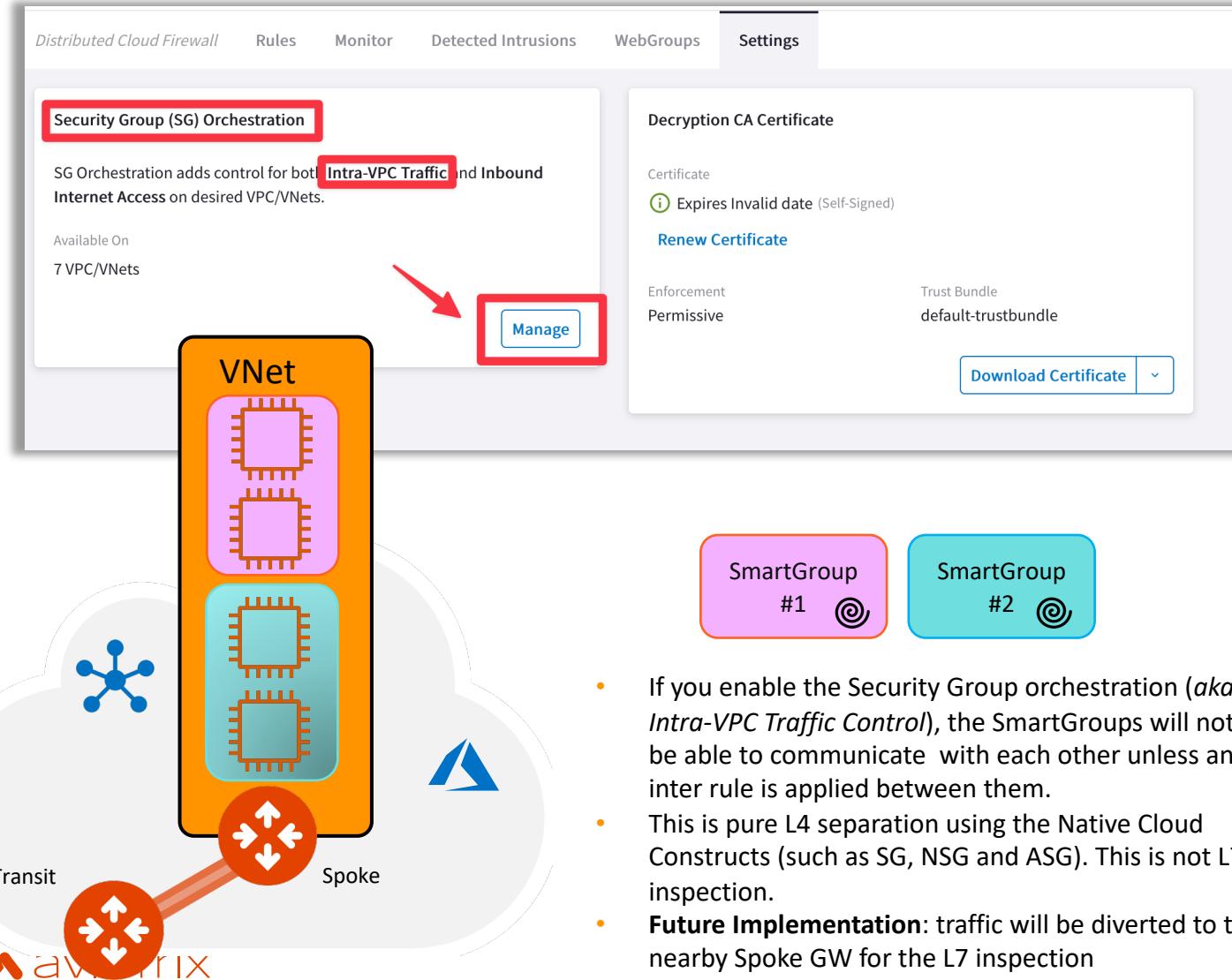
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	Decryption
1	INTRA-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
3	INTER-ICMP-NGINX-APA...	NGINX	APACHE		ICMP		Permit	On	
4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)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

A red arrow points to the **Commit** button, which is highlighted with a red box. Another red arrow points to the **Discard** button, which is also highlighted with a red box.

- 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



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

Available On 7 VPC/VNets

**Manage**

**VNet**

SmartGroup #1

SmartGroup #2

- 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.

**Save**

**Cancel**

# 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 X

Destination SmartGroups  
APACHE X

WebGroups

Protocol  
ICMP

Rule Behavior

Action  
Permit ▼ SG Orchestration ①

Enforcement On Logging On

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

Rule Priority

Place Rule

Cancel Save In Drafts

## □ 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 X

Destination SmartGroups

APACHE X

WebGroups

Protocol

ICMP

Rule Behavior

Enforcement

Logging

Action

SG Orchestration ?

On

Ensure TLS

TLS Decryption

Off

Off

Rule Priority

Place Rule

Cancel

Save In Drafts

- ☐ **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 (default is five days).**

Policy Monitor

Auto Refresh

Y W +

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



# Tools for troubleshooting Distributed Cloud Firewall

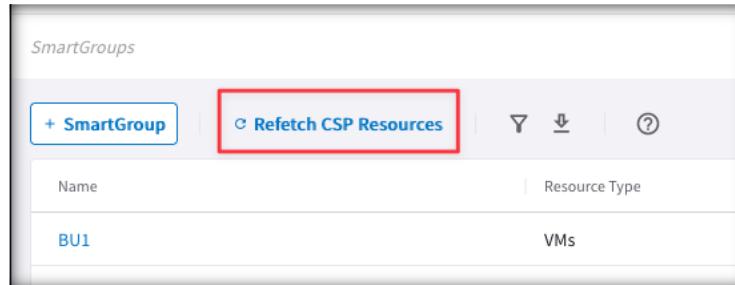
# Creation of the SmartGroup: the right matching criteria dilemma

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

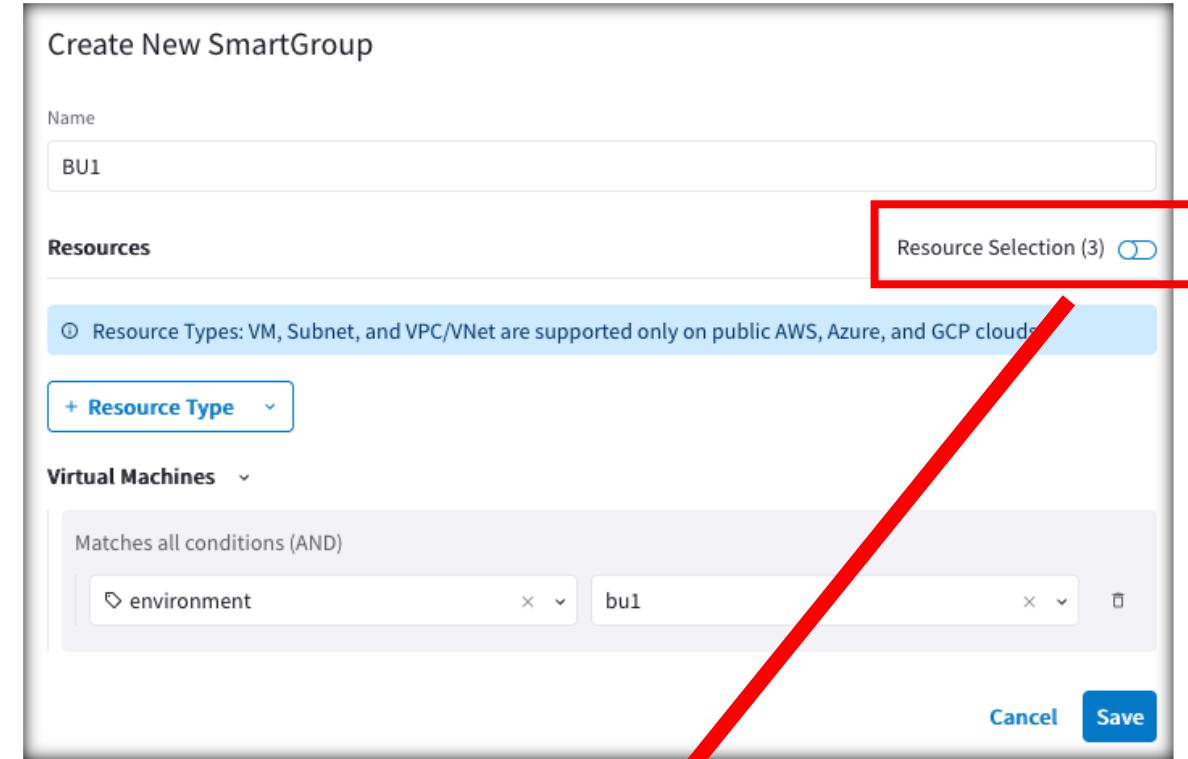
- Classification based on the **CSP Tags**
- Classification based on the **Resource Properties** (i.e. Name, Region or Account Name)
- Classification based on the **IPs/CIDRs**

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

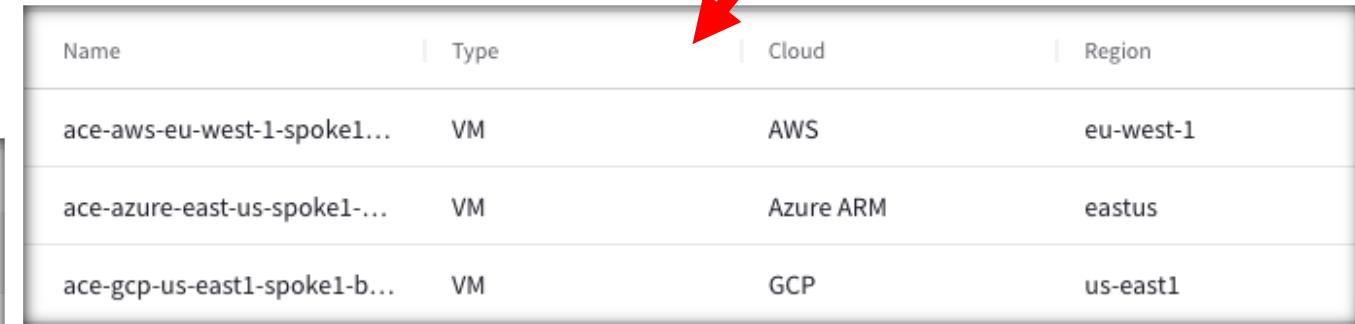
3) Use the On-Demand **Refetch CSP Resources** button to retrieve the most recent inventory



The screenshot shows the Aviatrix SmartGroups interface. At the top, there's a button labeled '+ SmartGroup'. Below it, a button labeled 'Refetch CSP Resources' is highlighted with a red box. The main area displays a table with columns: Name, Resource Type, Cloud, and Region. One row is visible: 'BU1' under Name, 'VMs' under Resource Type, 'AWS' under Cloud, and 'eu-west-1' under Region.



The screenshot shows the 'Create New SmartGroup' dialog. The 'Name' field contains 'BU1'. In the 'Resources' section, a 'Resource Selection (3)' button is highlighted with a red box. Below it, a note says 'Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds'. A 'Virtual Machines' section shows a condition 'Matches all conditions (AND)' with two filters: 'environment' and 'bu1'. At the bottom are 'Cancel' and 'Save' buttons.



The screenshot shows a table of resources. The columns are: Name, Type, Cloud, and Region. The 'Cloud' column header is highlighted with a red arrow. The data rows are:

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

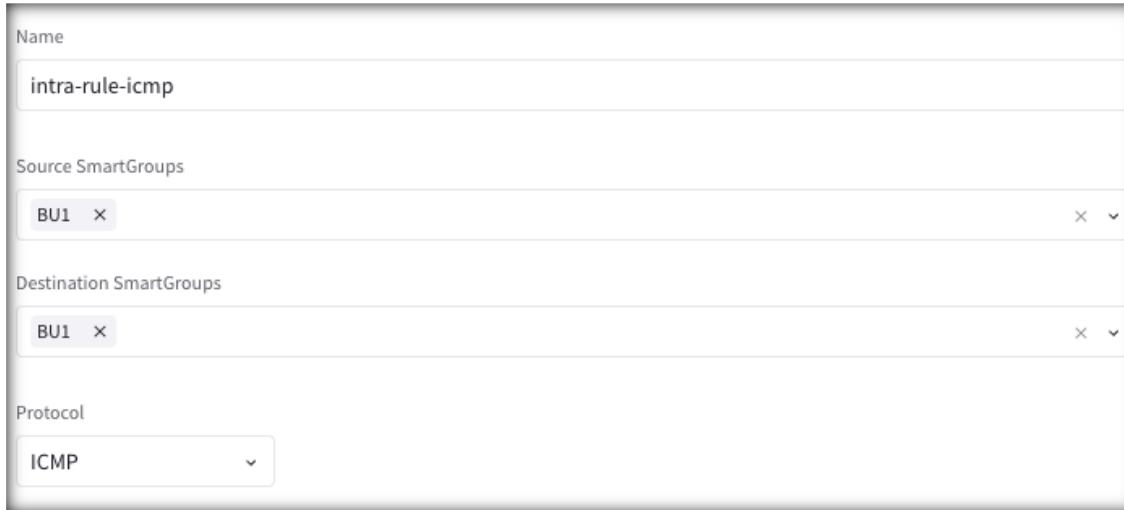
- ❑ Source Smart Group and Destination Smart Group must be the same

Name  
intra-rule-icmp

Source SmartGroups  
BU1

Destination SmartGroups  
BU1

Protocol  
ICMP



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

- ❑ Source Smart Group and Destination Smart Group must differ

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.



Next:

Lab 8 Distributed Cloud Firewall