

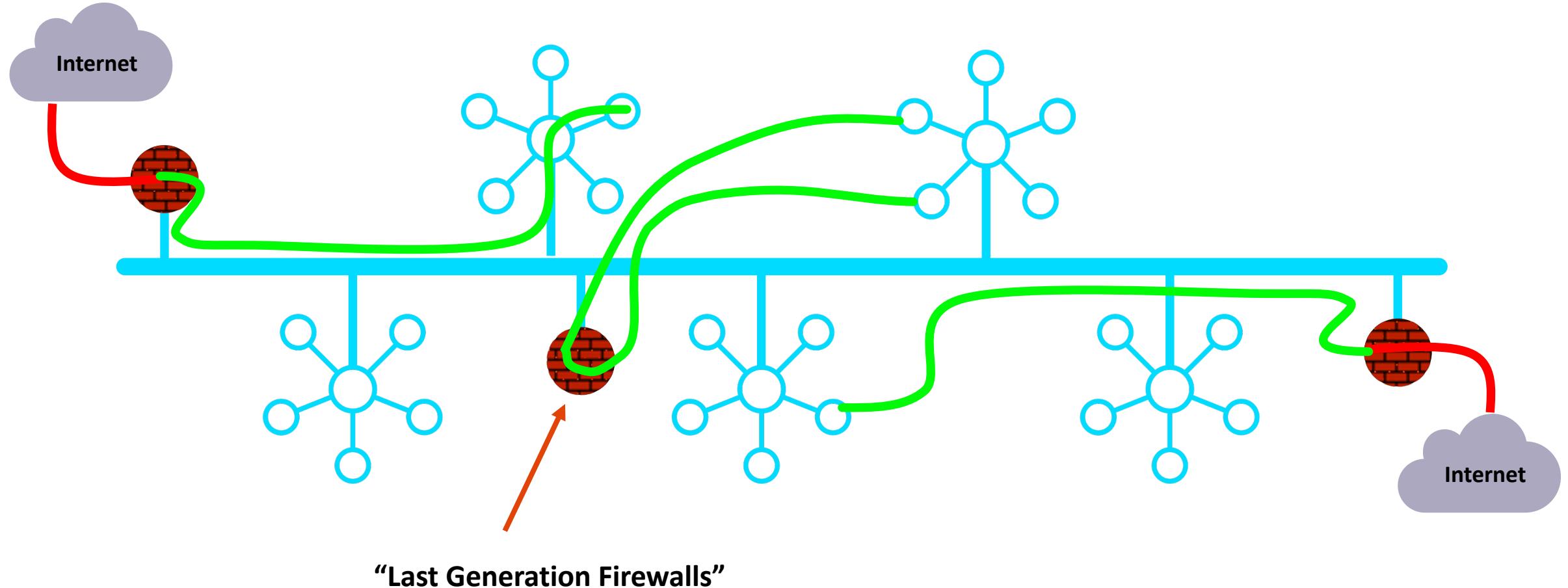


▲ aviatrix

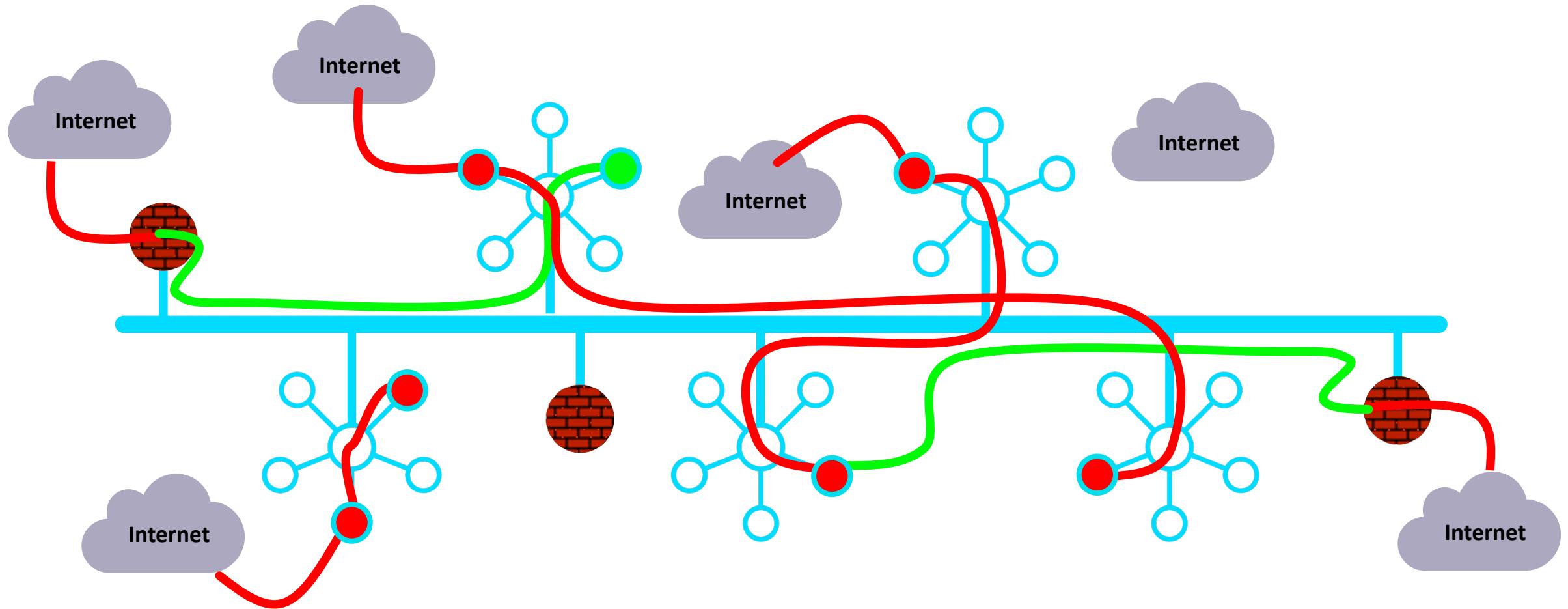


## Distributed Cloud Firewall

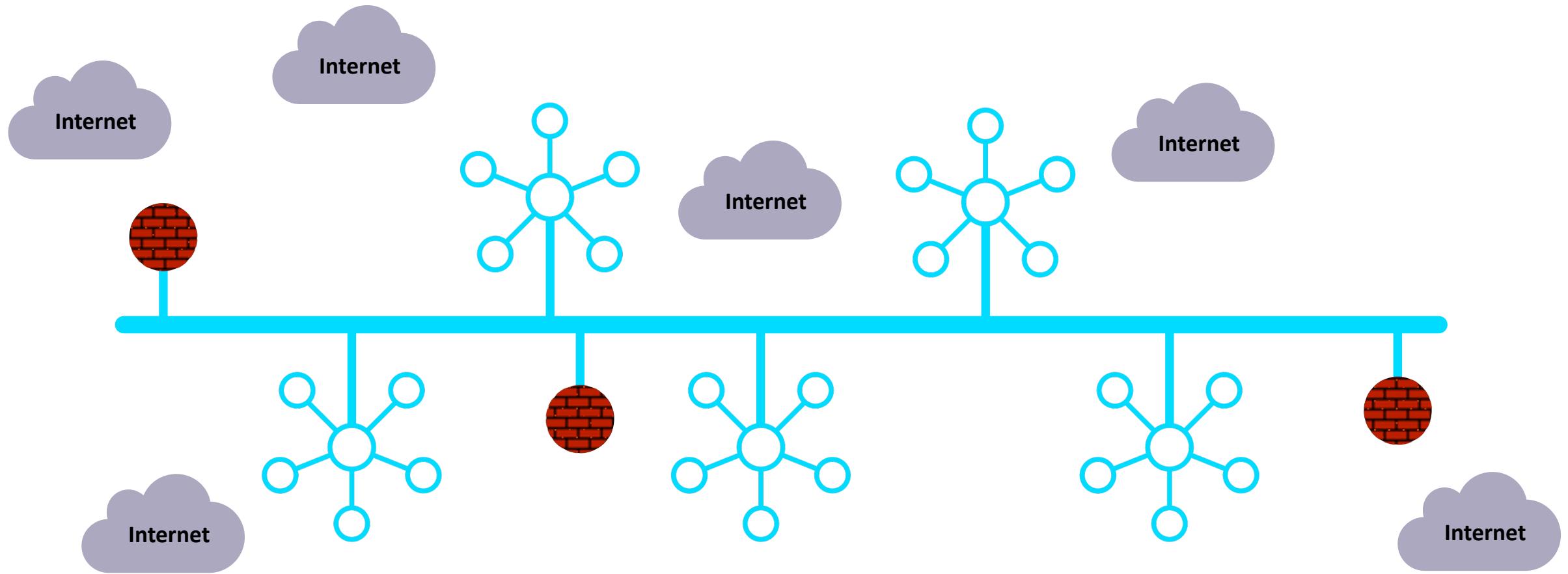
# As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



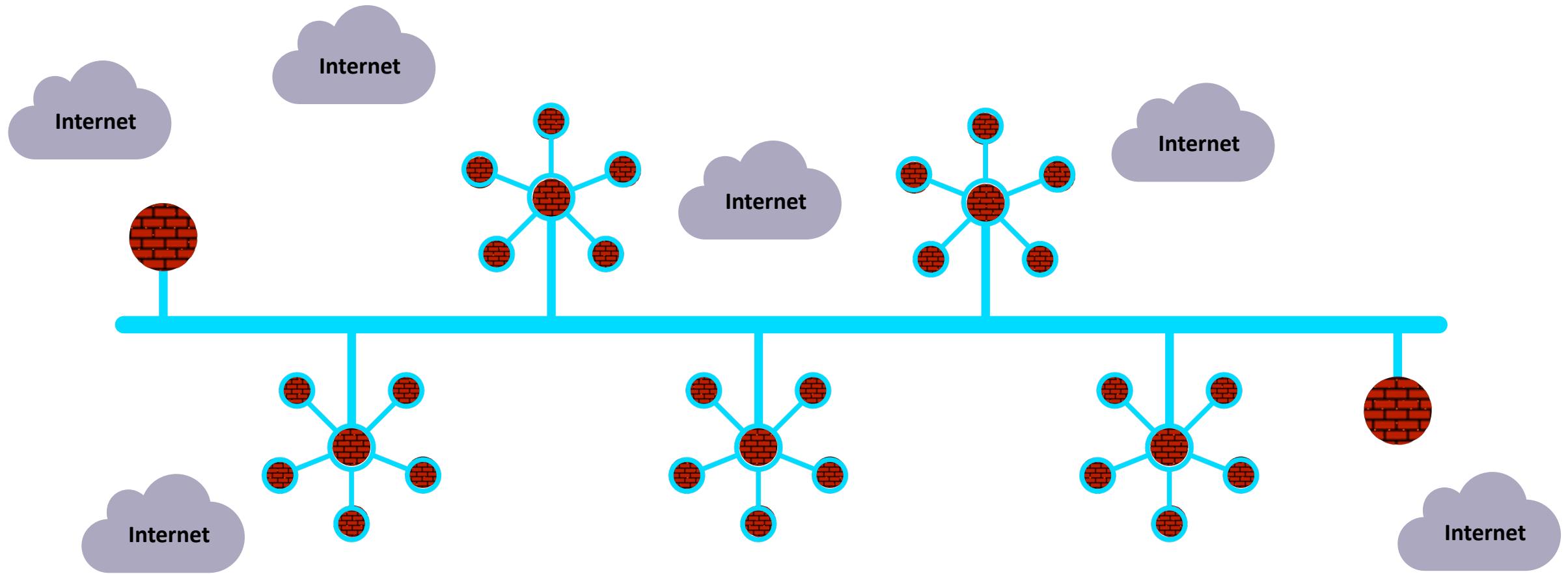
# In Reality...



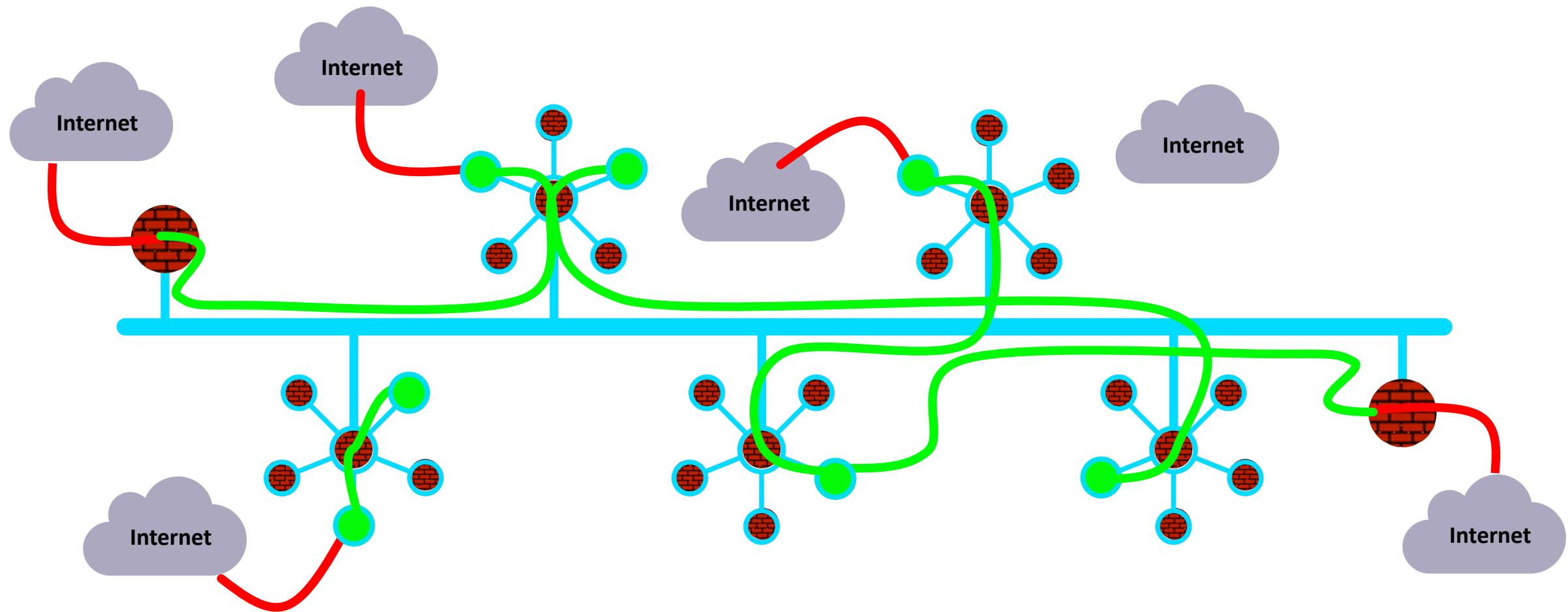
# What If... the architecture was built for cloud



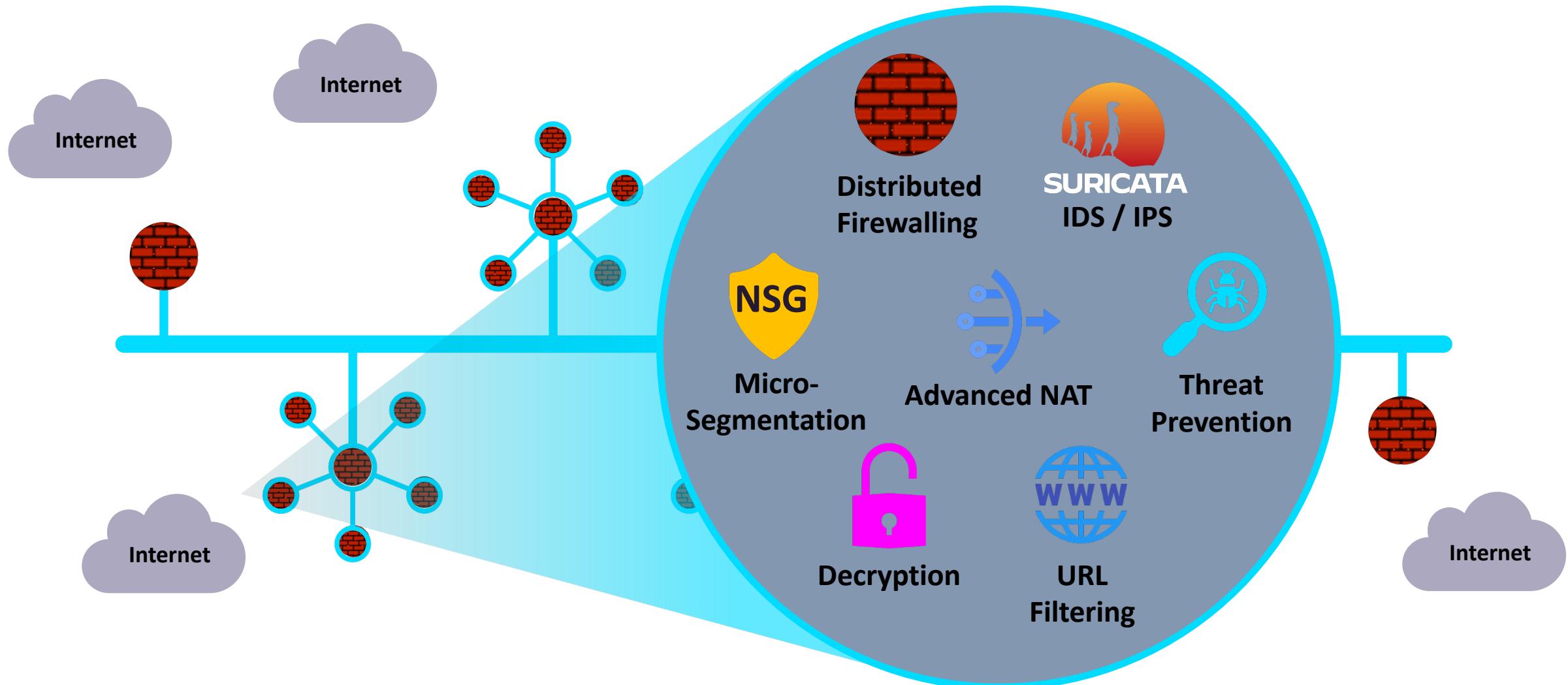
# Firewalling Functions were Embedded in the Cloud Network Everywhere...



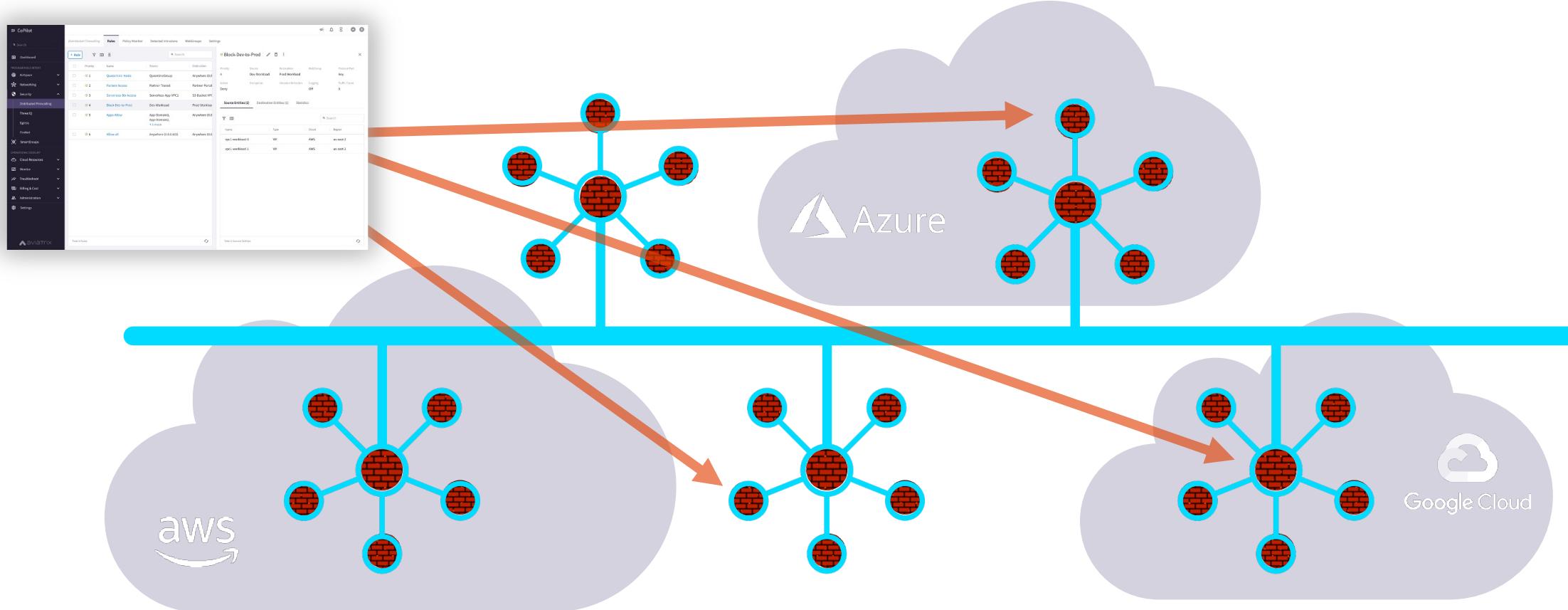
Centrally Managed, with Distributed Inspection & Enforcement...



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

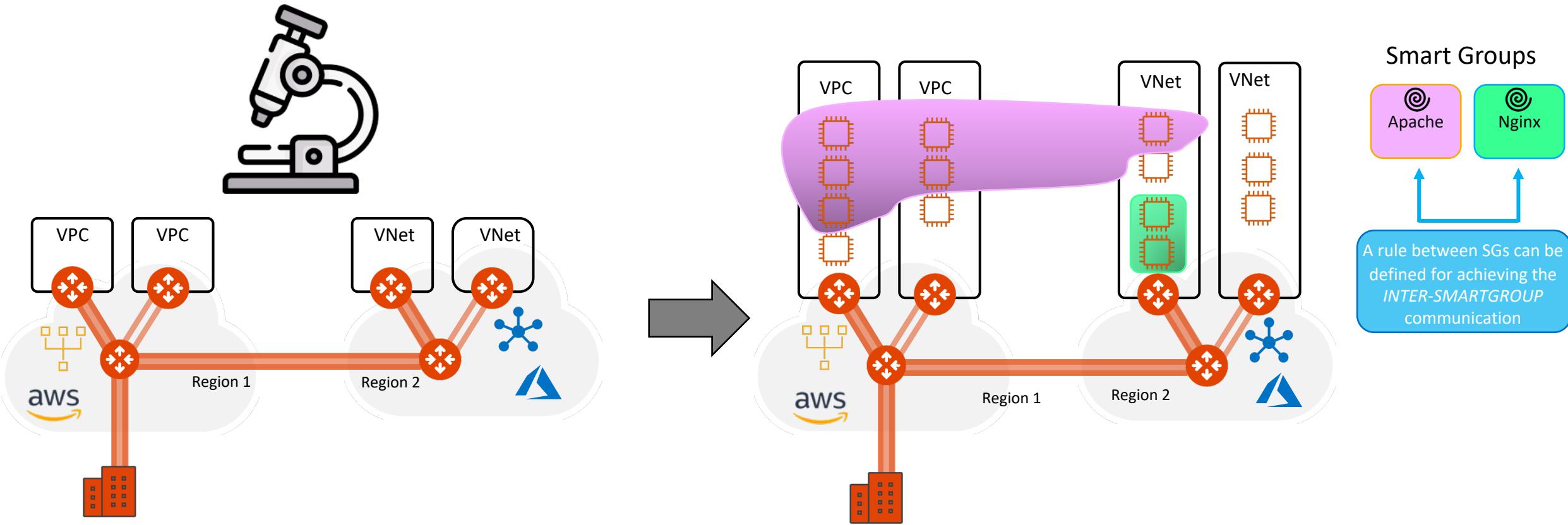
## Resource attribute

- Region Name, Account Name

## IP Prefixes

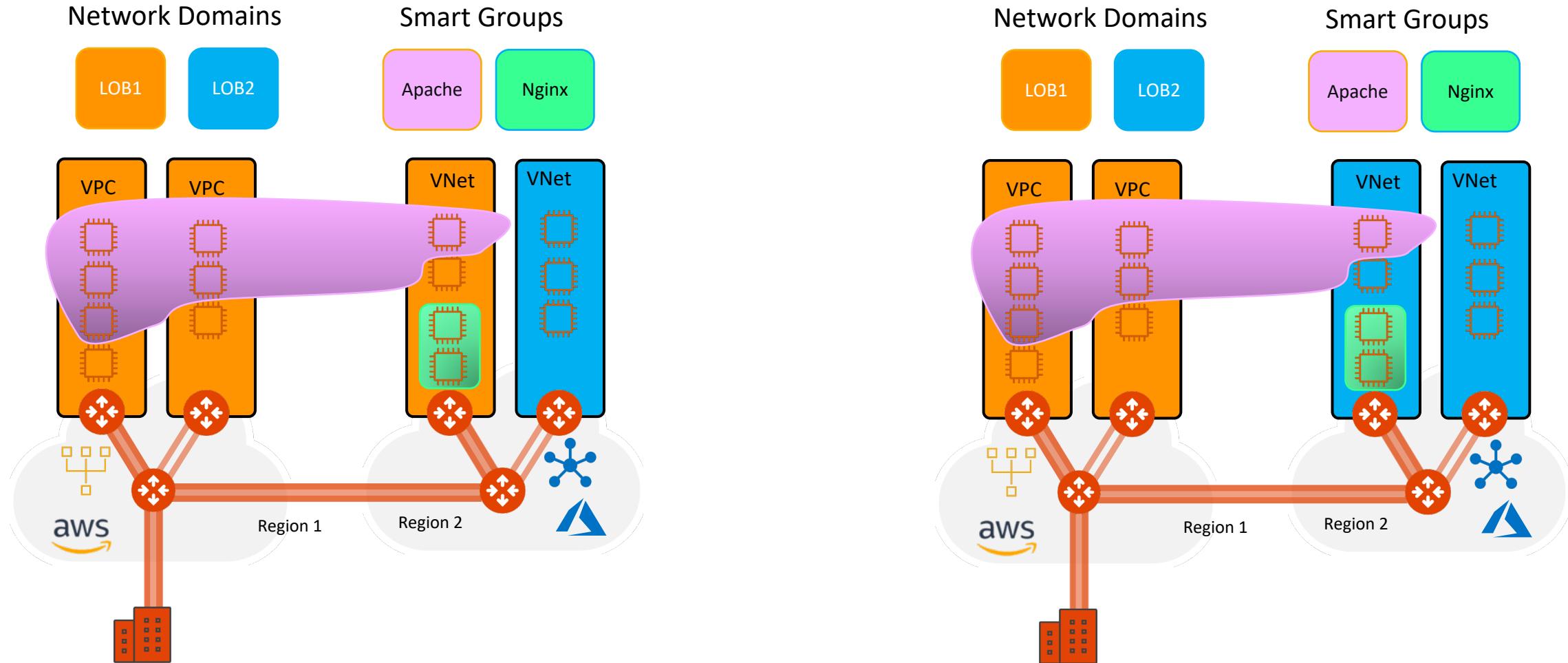
- CIDR

# 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 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 takes precedence over the extent of a Smart Group

# Smart Groups Creation

The screenshot shows the CoPilot interface with the 'SmartGroups' feature highlighted. The sidebar has a 'SmartGroups' button with a red box around it. The main area shows a 'Create New SmartGroup' dialog with a name 'APACHE' and a 'Resource Selection (3)' section. A red arrow points from the sidebar's 'SmartGroups' button to this dialog. Another red arrow points from the 'Resource Selection (3)' toggle in the dialog to the resource list below.

• 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

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

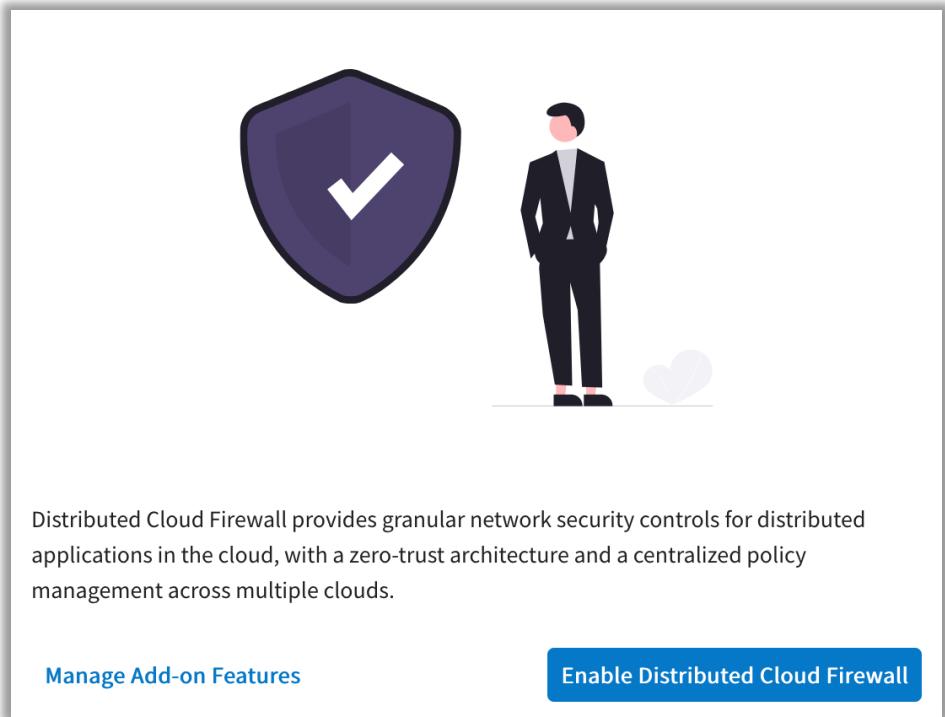
# Pre-defined Smart Groups

The screenshot shows a user interface for managing Smart Groups. At the top, there's a header with the text "SmartGroups". Below the header are several buttons and links: "+ SmartGroup" (highlighted with a red border), "⟳ Refetch CSP Resources", a refresh icon, a download icon, and a help icon. The main area is a table with two columns: "Name" and "Resource Type". There are two rows in the table. The first row contains the text "Anywhere (0.0.0.0/0)" in the "Name" column and is highlighted with a red border. The second row contains the text "Public Internet" in the "Name" column and is also highlighted with a red border. The "Resource Type" column is empty for both rows.

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

# Aviatrix DCF: Intra and inter SmartGroups Rules

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

The diagram illustrates the Aviatrix DCF architecture. It shows two regions, Region 1 and Region 2, each containing VPCs and a VNet. A purple cloud highlights the connection between the VNet of Region 1 and the VNet of Region 2. SmartGroups (Apache and Nginx) are defined in each region, and rules are created to permit traffic between them.

The process involves creating three rules:

- SmartGroup Apache → SmartGroup Nginx:** Rule name: INTRA-ICMP-APACHE. Source SmartGroup: APACHE. Destination SmartGroup: APACHE. Protocol: ICMP. Action: Permit. SG Orchestration: On. Enforcement: Off. Logging: On.
- SmartGroup Nginx → SmartGroup Apache:** Rule name: INTRA-ICMP-NGINX. Source SmartGroup: NGINX. Destination SmartGroup: NGINX. Protocol: ICMP. Action: Permit. SG Orchestration: On. Enforcement: Off. Logging: On.
- SmartGroup Nginx → SmartGroup Apache:** Rule name: INTER-ICMP-NGINX-APACHE. Source SmartGroups: NGINX. Destination SmartGroups: APACHE. Protocol: ICMP. Action: Permit. SG Orchestration: On. Enforcement: Off. Logging: On.

In the Aviatrix DCF UI, the 'Commit' button is highlighted with a red box and arrow, indicating where changes are saved.

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		

- 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)

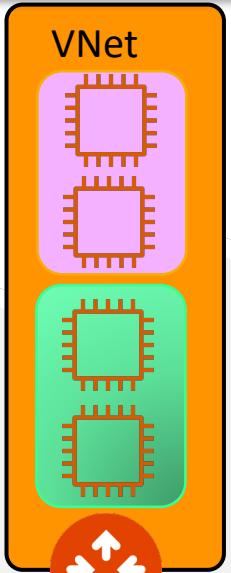
## ☐ Enable the feature on the concerned VNets

Distributed Firewalling    Rules    Detected Intrusions    Settings

Intra VPC/VNet Distributed Firewalling

Available On: 2 VPC/VNets

Manage



- 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.

Name	Cloud	Region	Account Name	Intra VPC/VNet Dis...
AZURE-WESTEUROPE-	Azure ARM	westeurope	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled
AZURE-WESTEUROPE-	Azure ARM	westeurope	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

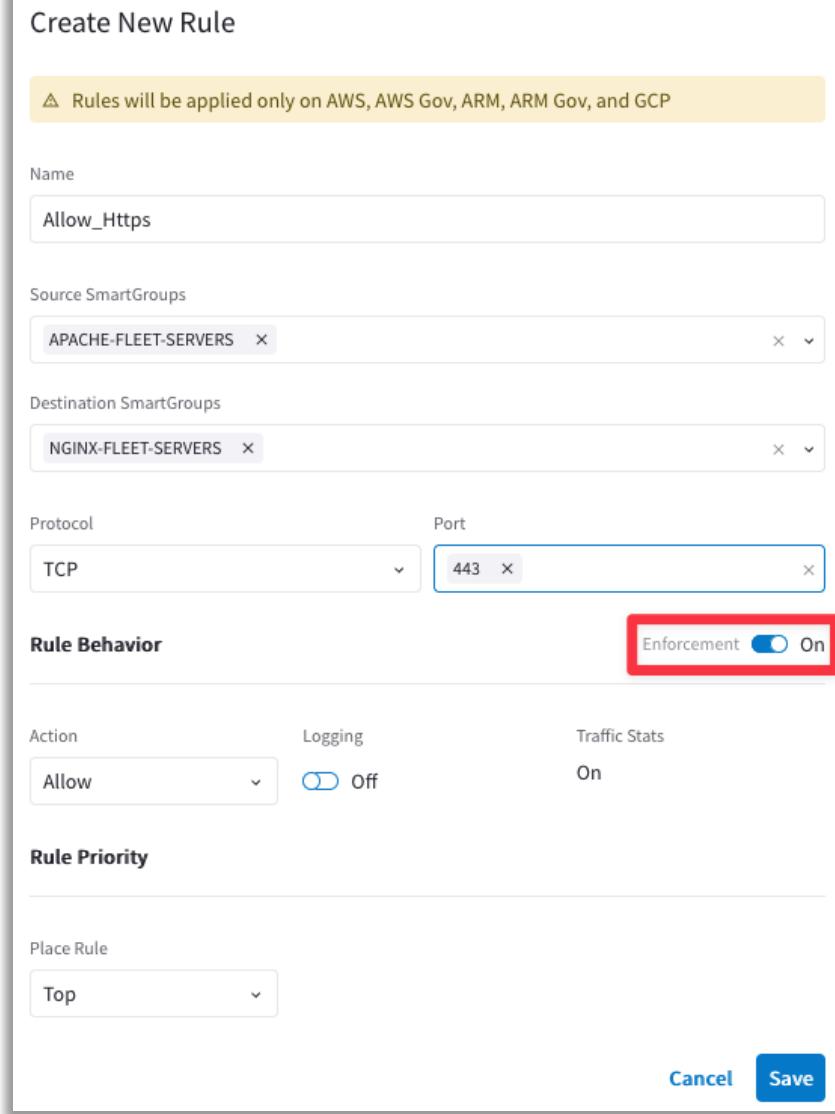
Protocol: TCP, Port: 443

Rule Behavior: Enforcement  On (highlighted with a red box)

Action: Allow, Logging: Off, Traffic Stats: On

Rule Priority: Place Rule

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 X

Destination SmartGroups

NGINX-FLEET-SERVERS X

Protocol

Port

TCP ▼ 443 X X

Rule Behavior

Enforcement On

Action

Logging



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 ✖

## Tools for troubleshooting Distributed Cloud Firewall

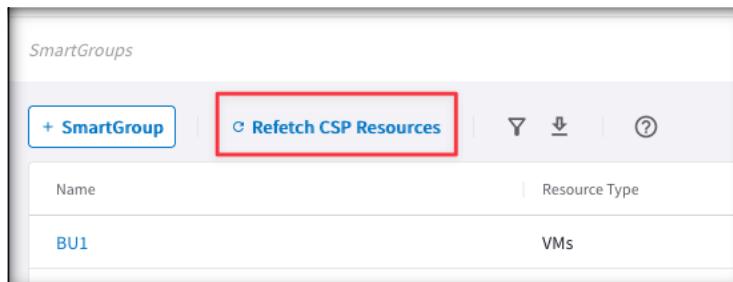
# Creation of the SmartGroup: the right matching criteria dilemma

- 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 'Create New SmartGroup' dialog box. It has a 'Name' field containing 'BU1' and a 'Resources' section. A red box highlights the 'Resource Selection (3)' toggle switch. Below it is a note about supported resource types: 'Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.' A red arrow points from the 'Refetch CSP Resources' button on the dashboard to this note. The 'Virtual Machines' section shows a condition 'Matches all conditions (AND)' with filters 'environment' and 'bu1'. At the bottom are 'Cancel' and 'Save' buttons.

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