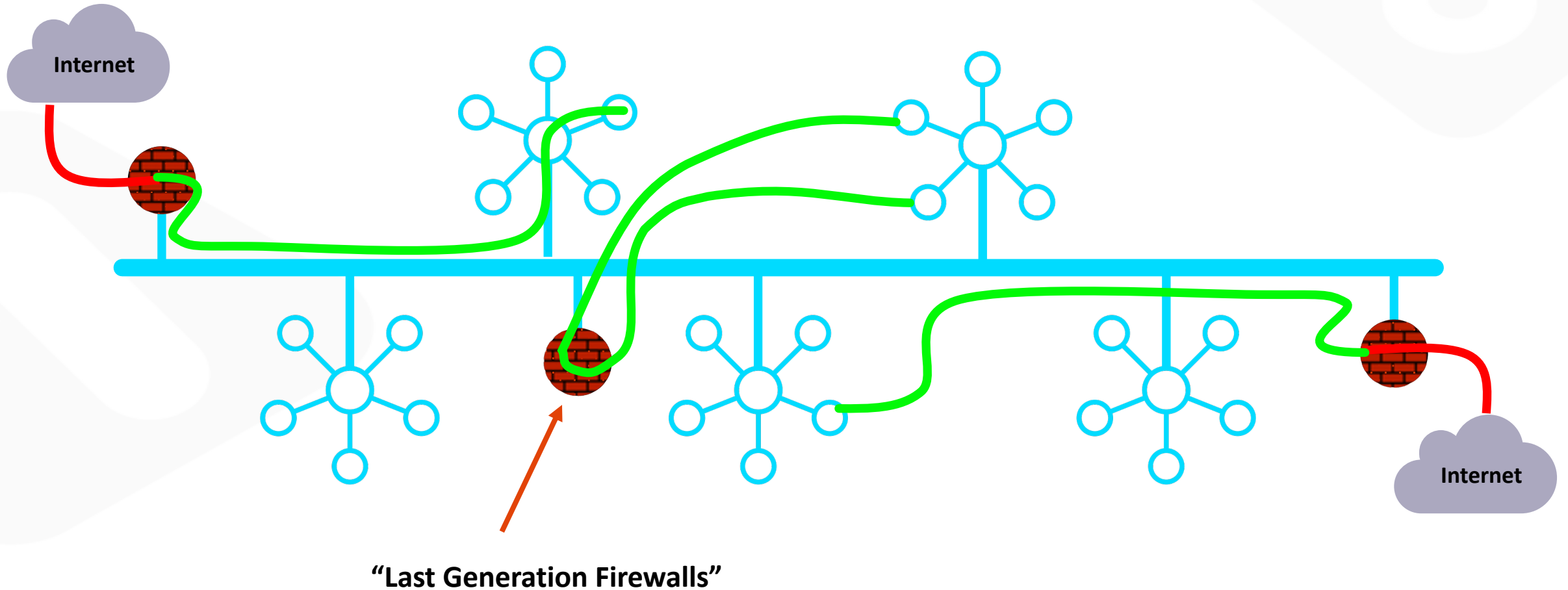


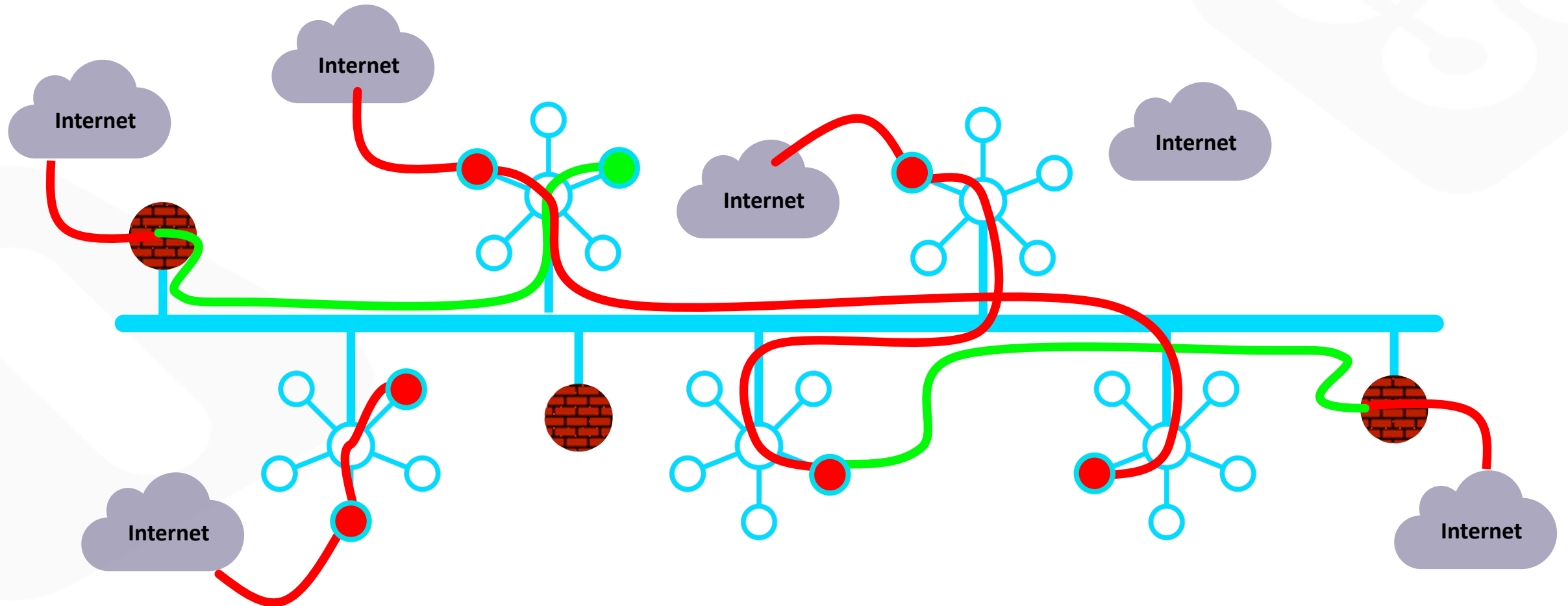


Distributed Cloud Firewall

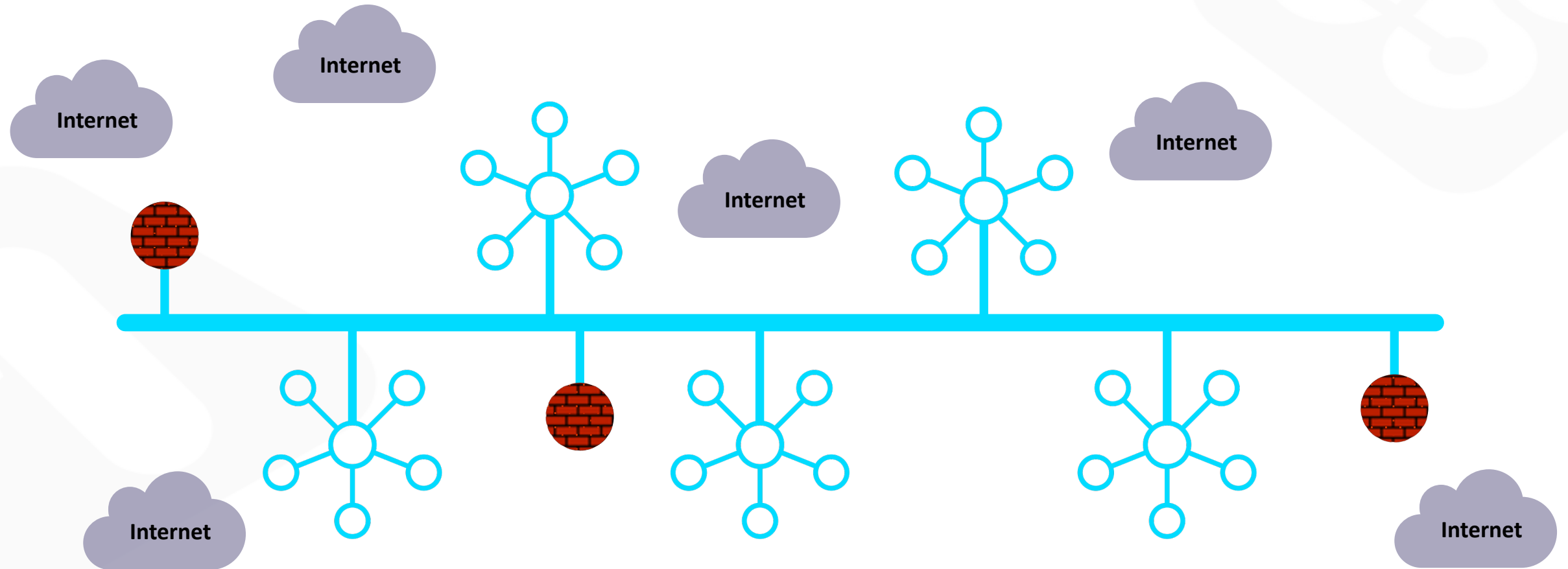
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



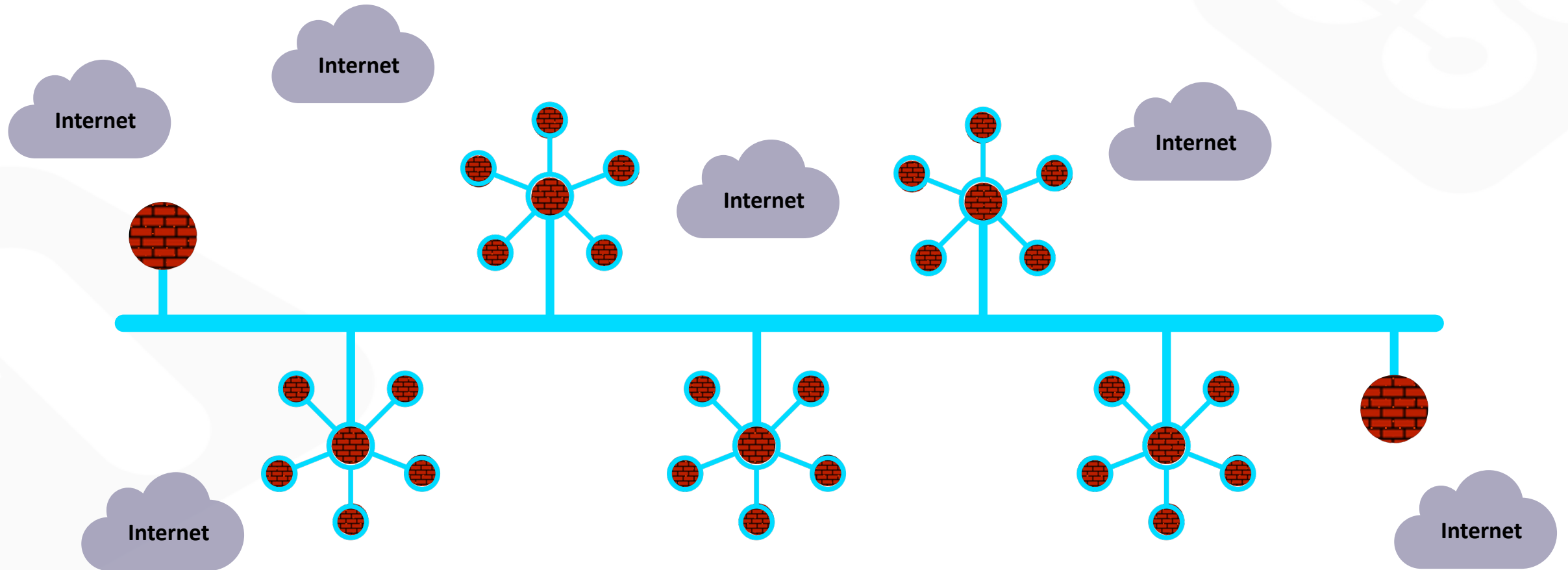
In Reality...



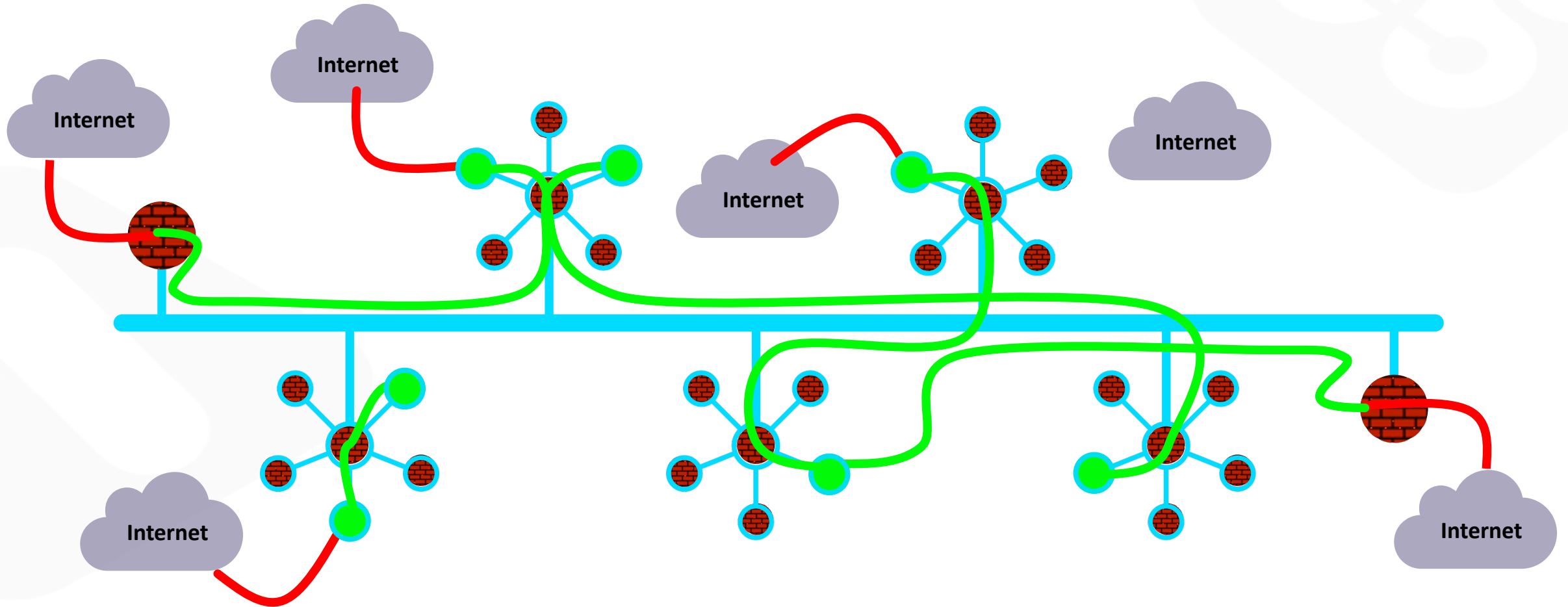
What If... the architecture was built for cloud



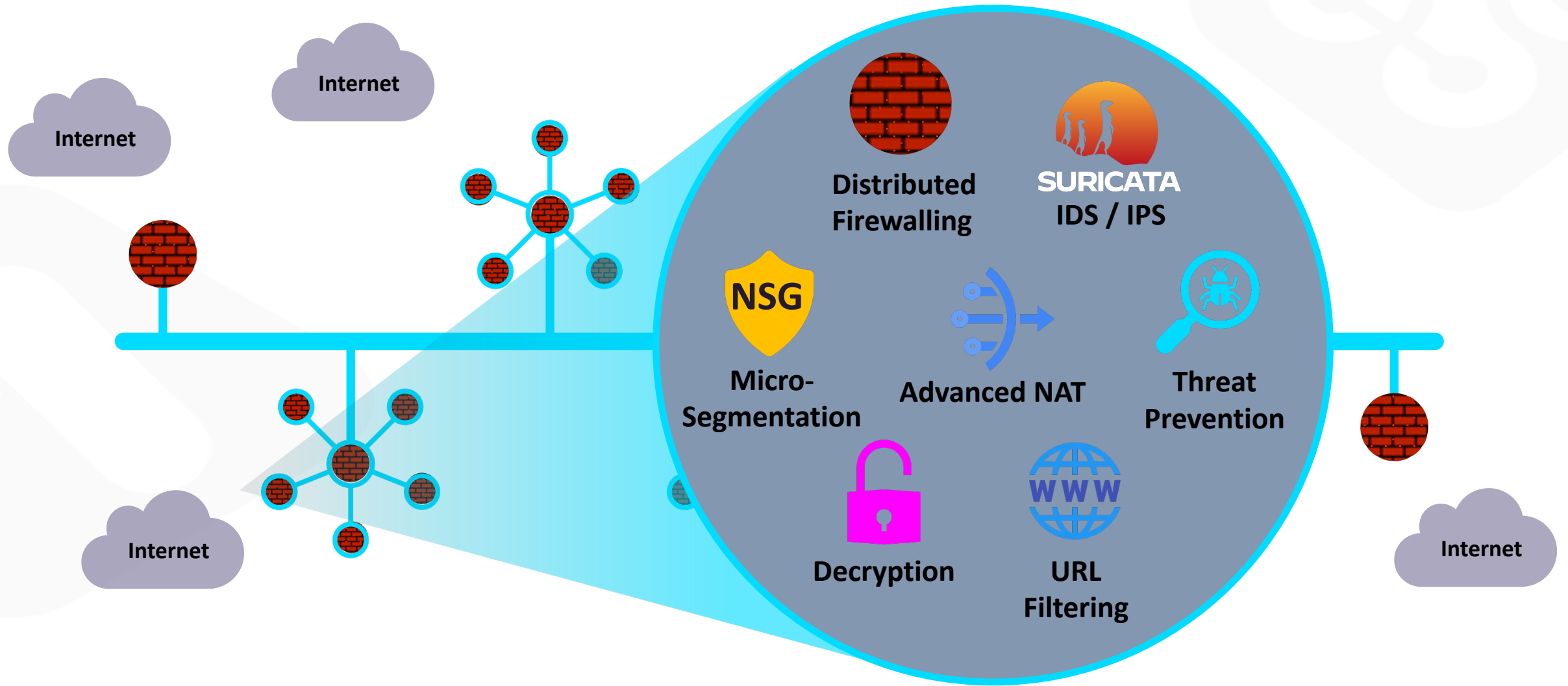
Firewalling Functions were Embedded in the Cloud Network Everywhere...



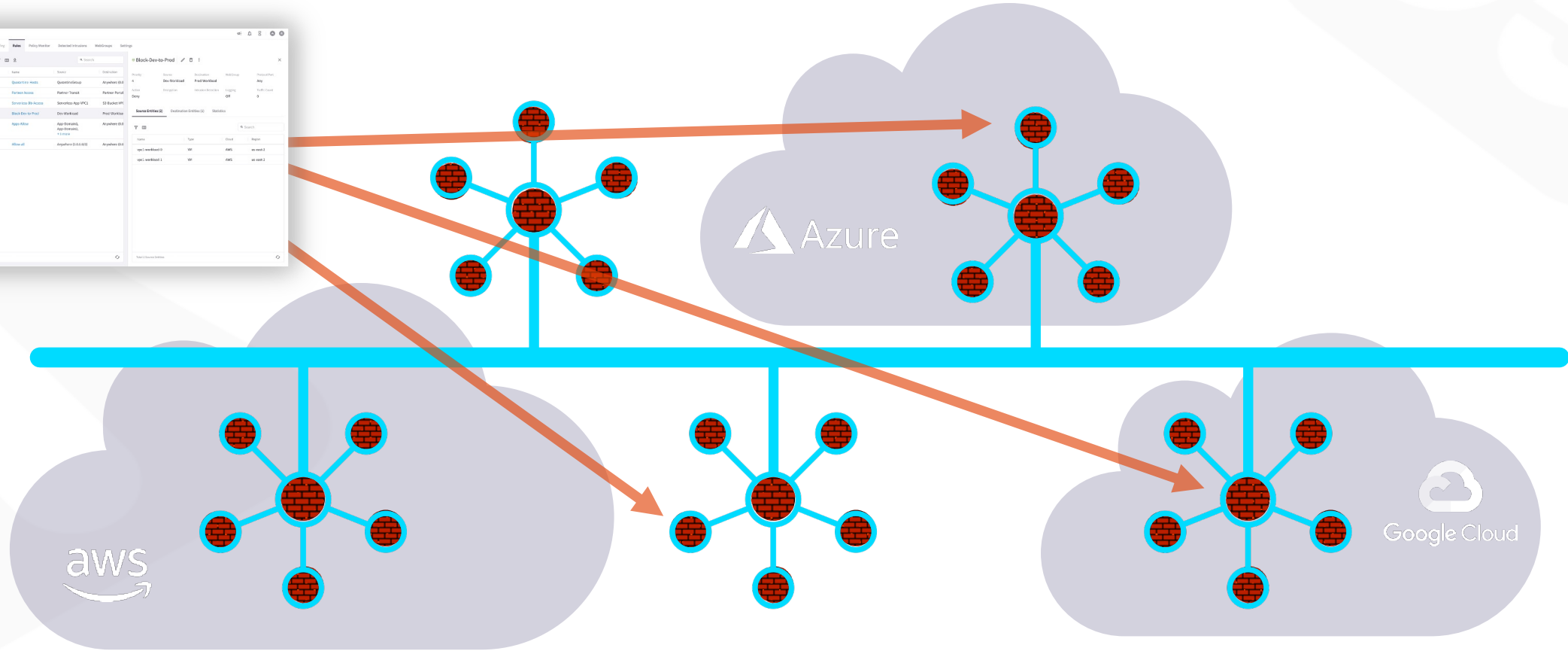
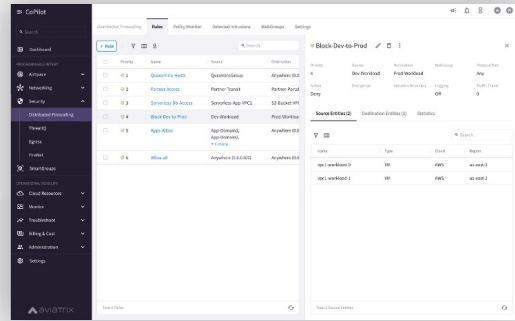
Centrally Managed, with Distributed Inspection & Enforcement...



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...

Distributed Firewalling & Micro-Segmentation Basics

Distributed Firewalling and Micro-Segmentation enforce policy exactly where needed across the entire network

Characteristics:

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

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)

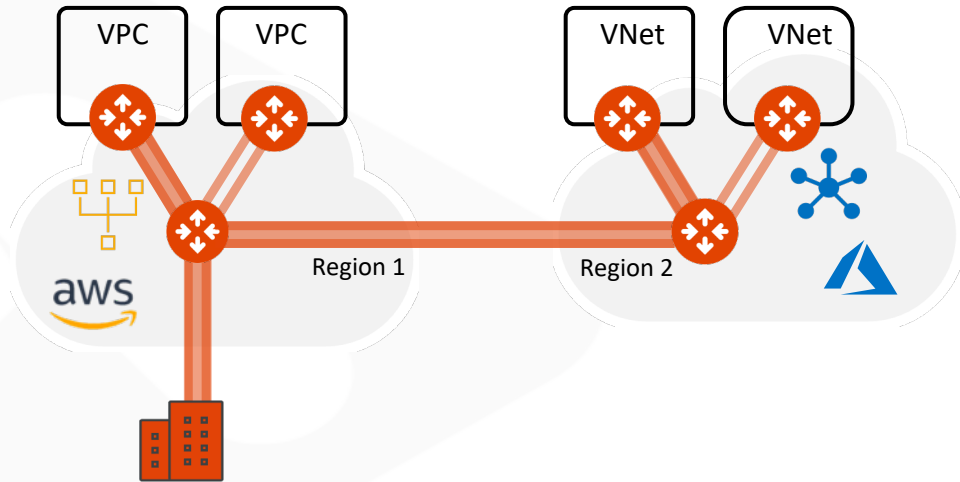
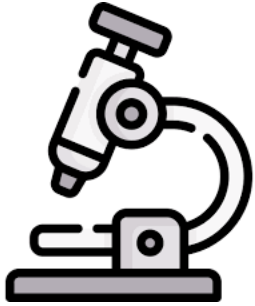
Select an instance above

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

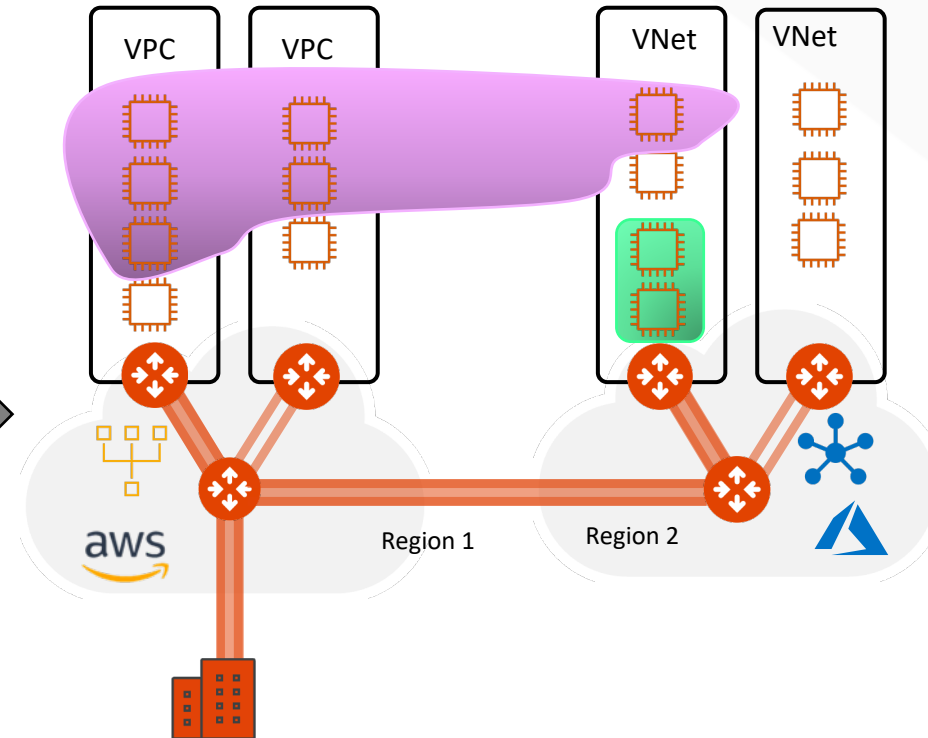
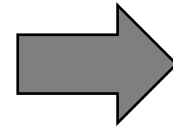
Tags

Key	Value
Env	Staging
Name	shopping cart app

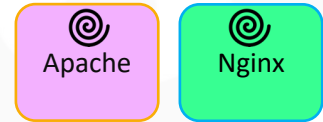
Distributed Firewalling: Intra-rule vs. Inter-rule



- **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



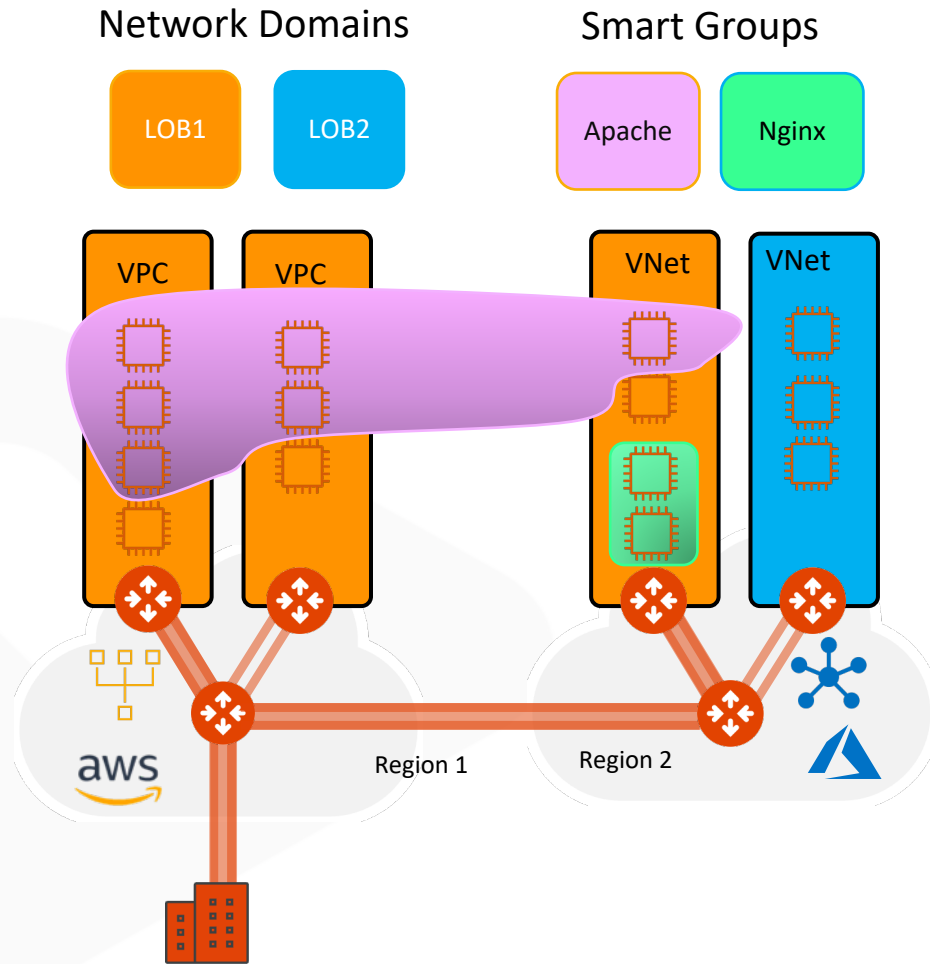
Smart Groups



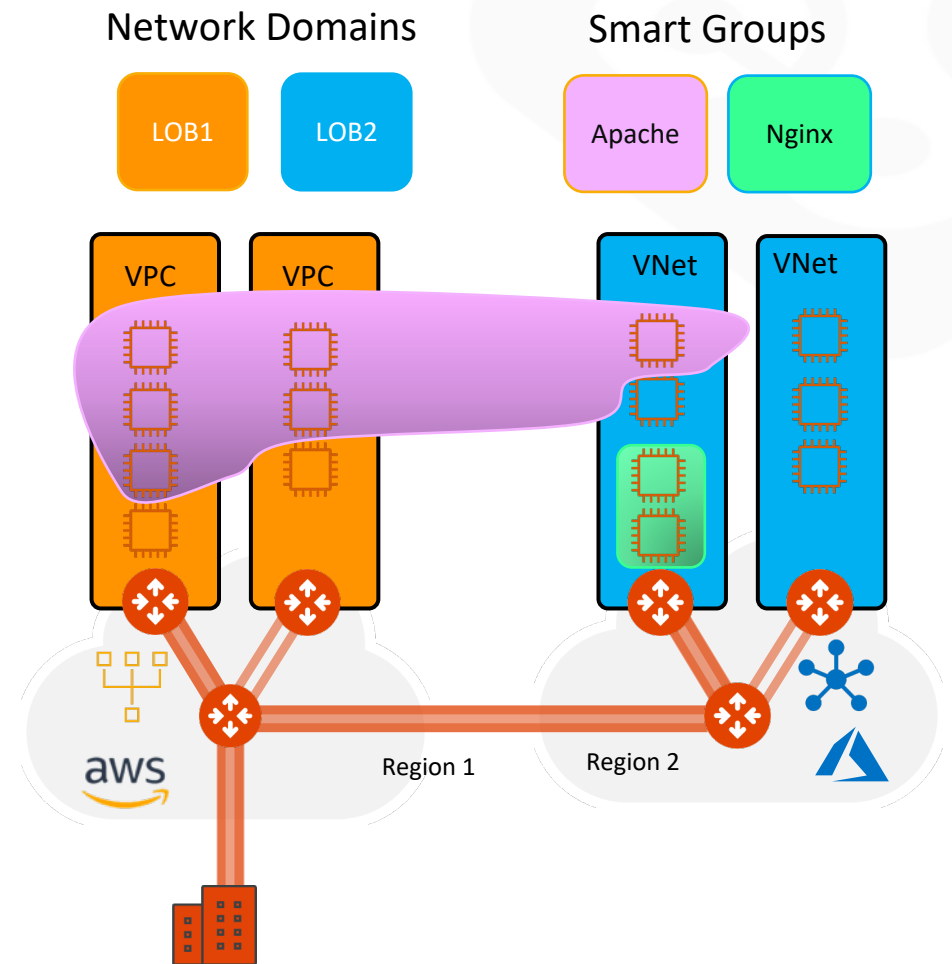
A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

- **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 takes precedence over the extent of a Smart Group

Smart Groups Creation

The screenshot shows the CoPilot interface with a sidebar on the left containing navigation options: Dashboard, Programmable Intent (AirSpace, Networking, Security, SmartGroups), and Operational Visibility (Cloud Resources, Monitor, Troubleshoot, Billing & Cost, Administration, Settings). The 'SmartGroups' option is highlighted. The main panel displays the 'SmartGroups' section with buttons for '+ SmartGroup' and 'Refresh CSP Resources'. A red arrow points from the 'Refresh CSP Resources' button to a notification box that says 'Successfully refreshed CSP resources'. Another red arrow points from the 'Resource Selection (2)' toggle in the 'Create New SmartGroup' dialog to a detailed view of the dialog.

Create New SmartGroup

Name: APACHE-FLEET-SERVERS

Resources

Resource Selection (2) ☒

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)

Type APACHE

- 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

This detailed view of the 'Create New SmartGroup' dialog shows the 'Resources' section with a table of selected resources. The table has columns for Name, Type, Cloud, and Region. Two resources are listed: PROD1-APACHE and PROD2-APACHE, both of type VM on AWS in the eu-central-1 region.

Create New SmartGroup

Name: APACHE-FLEET-SERVERS




Resources

Resource Selection (2) ☒

Name	Type	Cloud	Region
PROD1-APACHE	VM	AWS	eu-central-1
PROD2-APACHE	VM	AWS	eu-central-1

Pre-defined Smart Groups


SmartGroups

[+ SmartGroup](#) | [Refresh CSP Resources](#) |   

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)

Enable 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.

[Manage Add-on Features](#) [Enable 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.



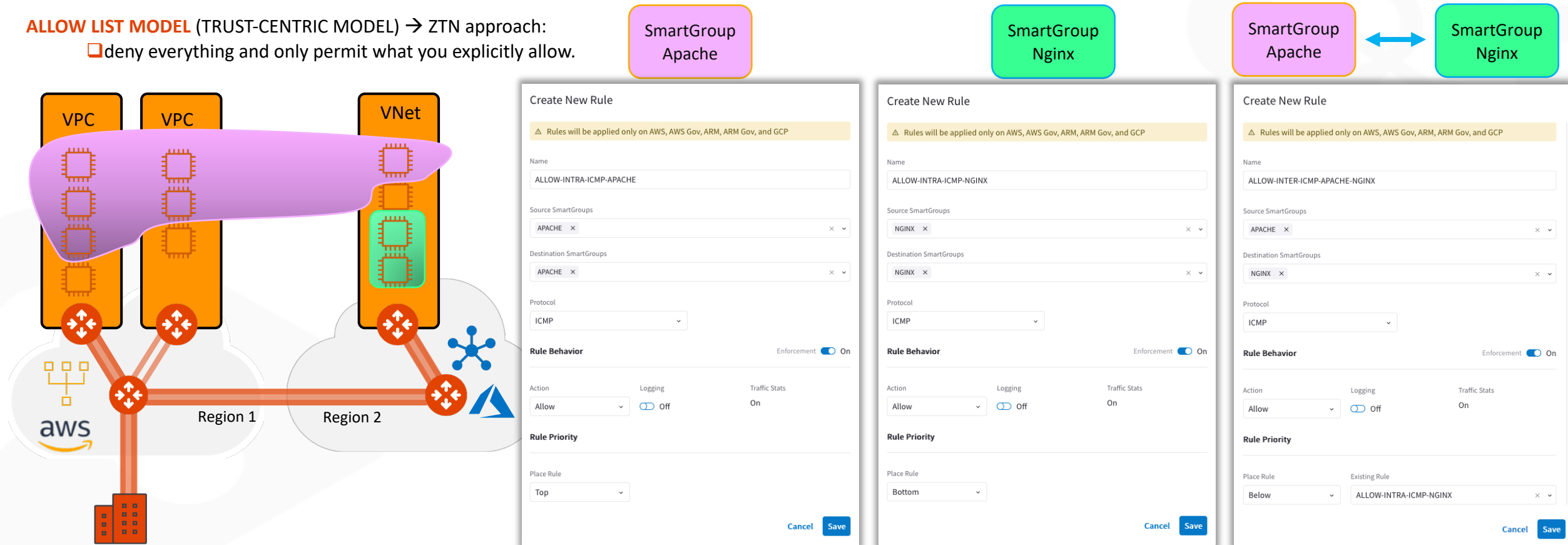
DENY LIST MODEL (THREAT-CENTRIC MODEL):

☐ allow all data to flow, except for exactly what you say should be stopped.

Distributed Cloud Firewall								
Rules								
Monitor								
Detected Intrusions								
WebGroups								
Settings								
<div>+ Rule Actions Filter Grid Download</div>								
<input type="checkbox"/> 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	

Distributed Firewalling Rules on Smart Groups

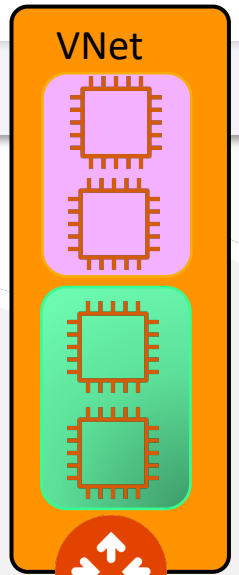
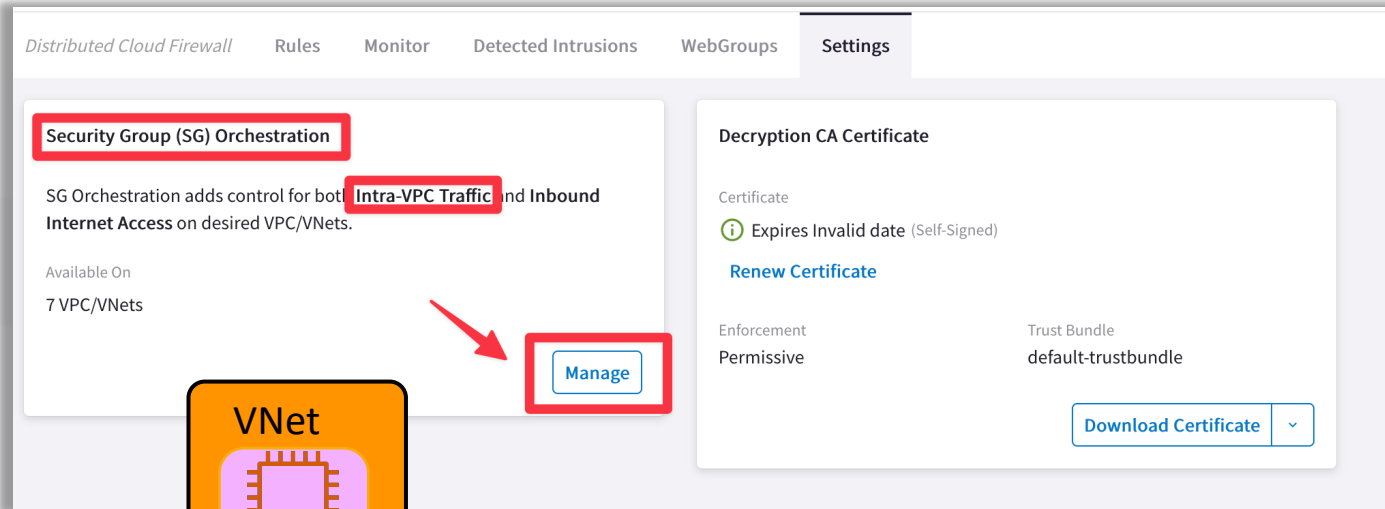
ALLOW LIST MODEL (TRUST-CENTRIC MODEL) → ZTN approach:
❑ deny everything and only permit what you explicitly allow.



- 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)

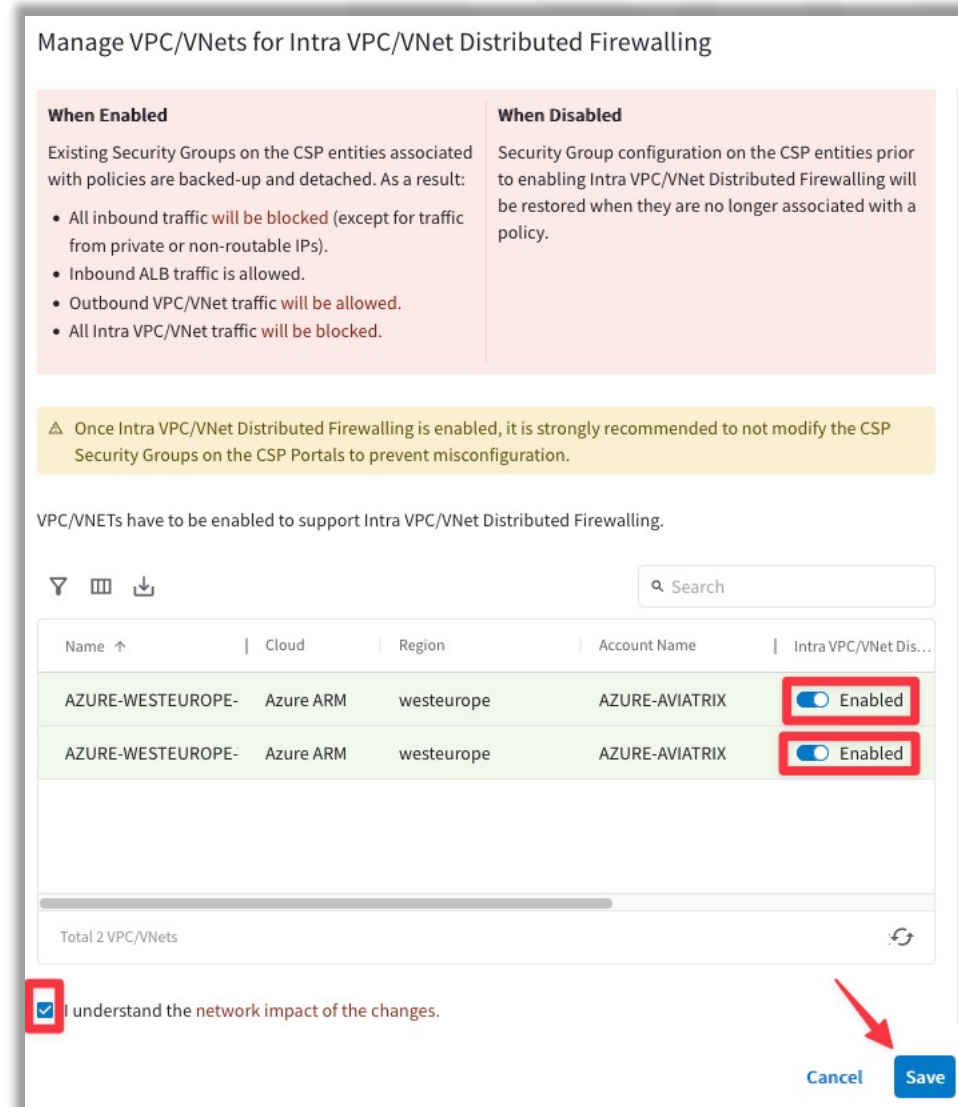
❑ Enable the feature on the concerned VNets



SmartGroup
#1

SmartGroup
#2

- If you enable the *Intra-VPC Traffic control*, the Smart Groups will not be able to communicate to each other, unless an *inter-rule* is applied.



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 x

Destination SmartGroups
NGINX-FLEET-SERVERS x

Protocol
TCP

Port
443 x

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



Next: Lab 10 – Distributed Cloud Firewall