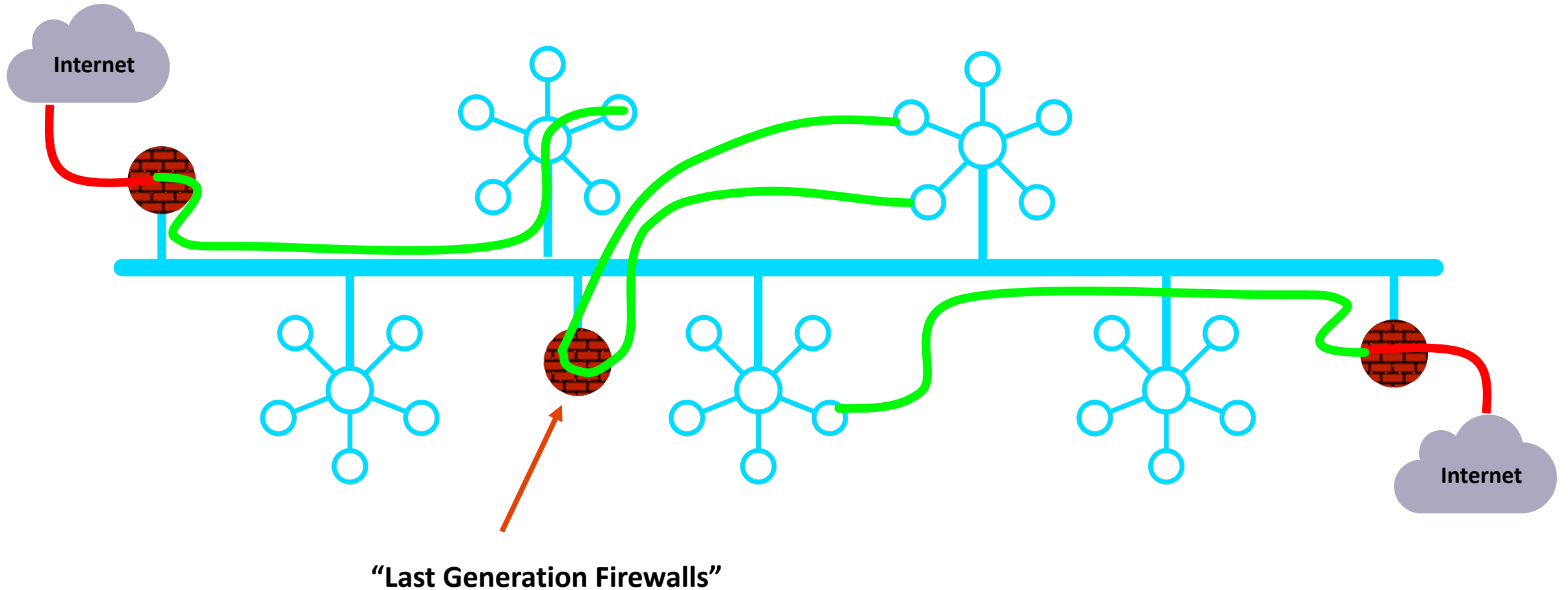


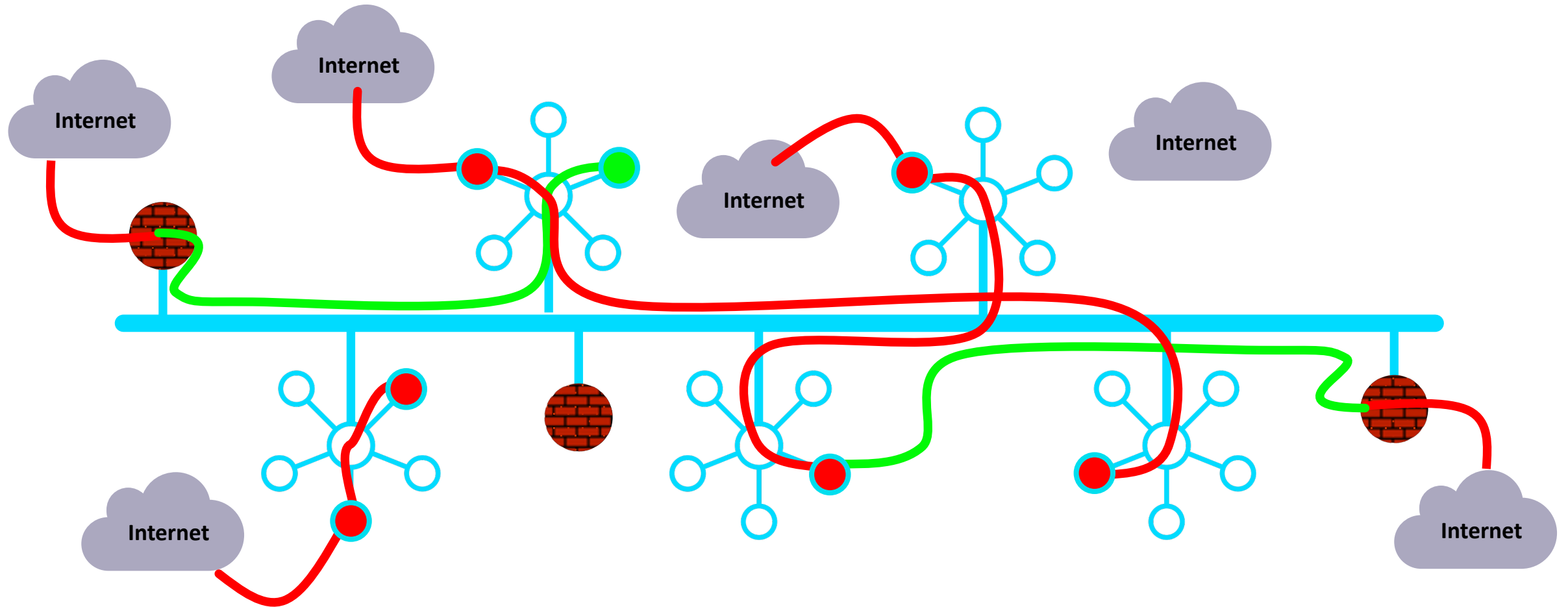


Distributed Cloud Firewall

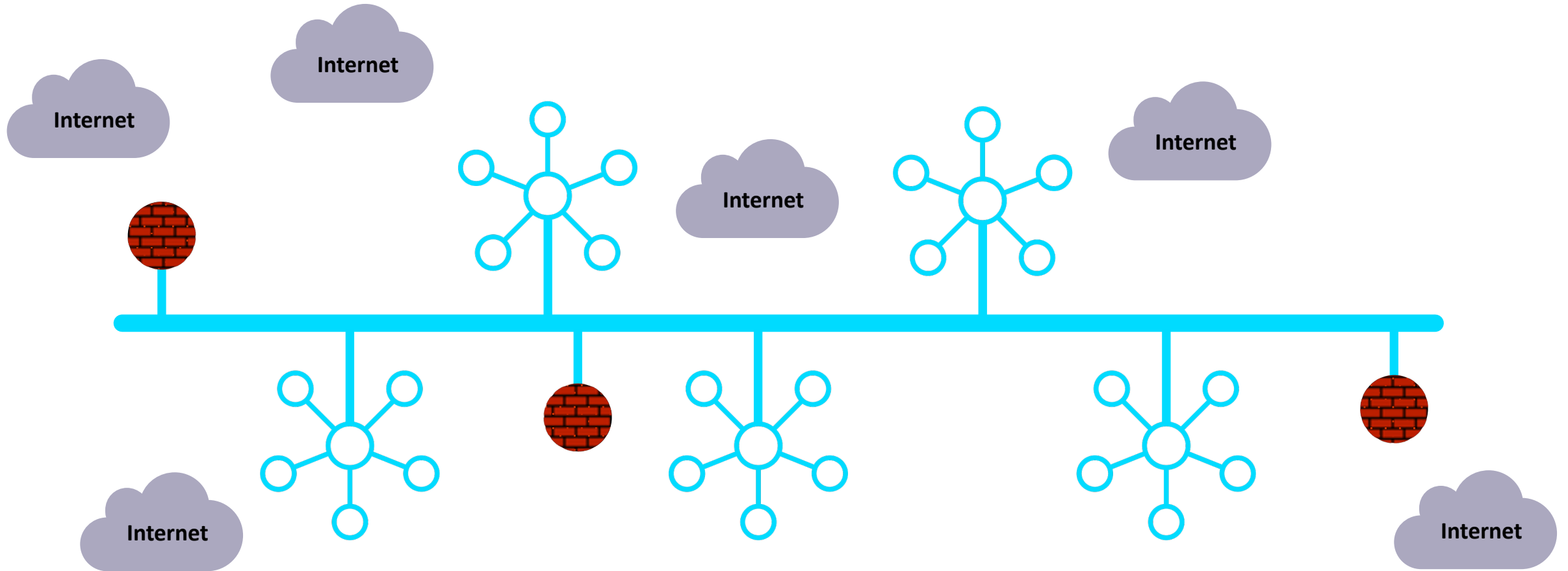
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



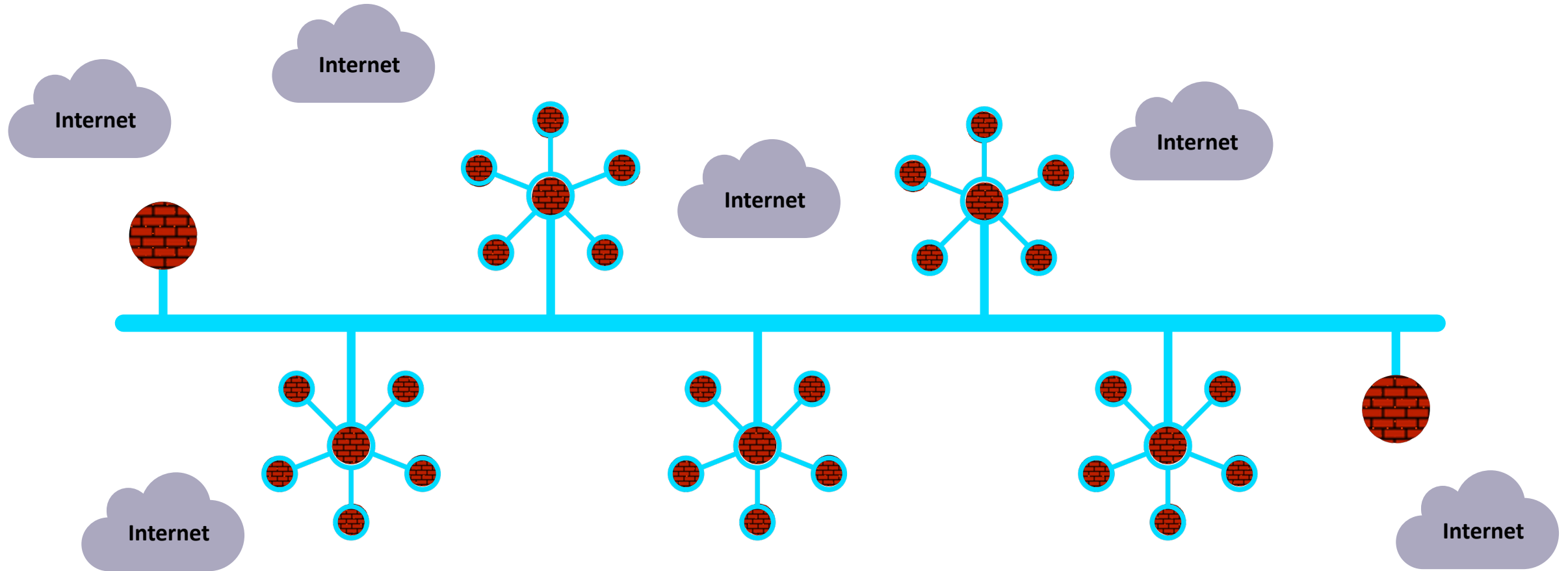
In Reality...



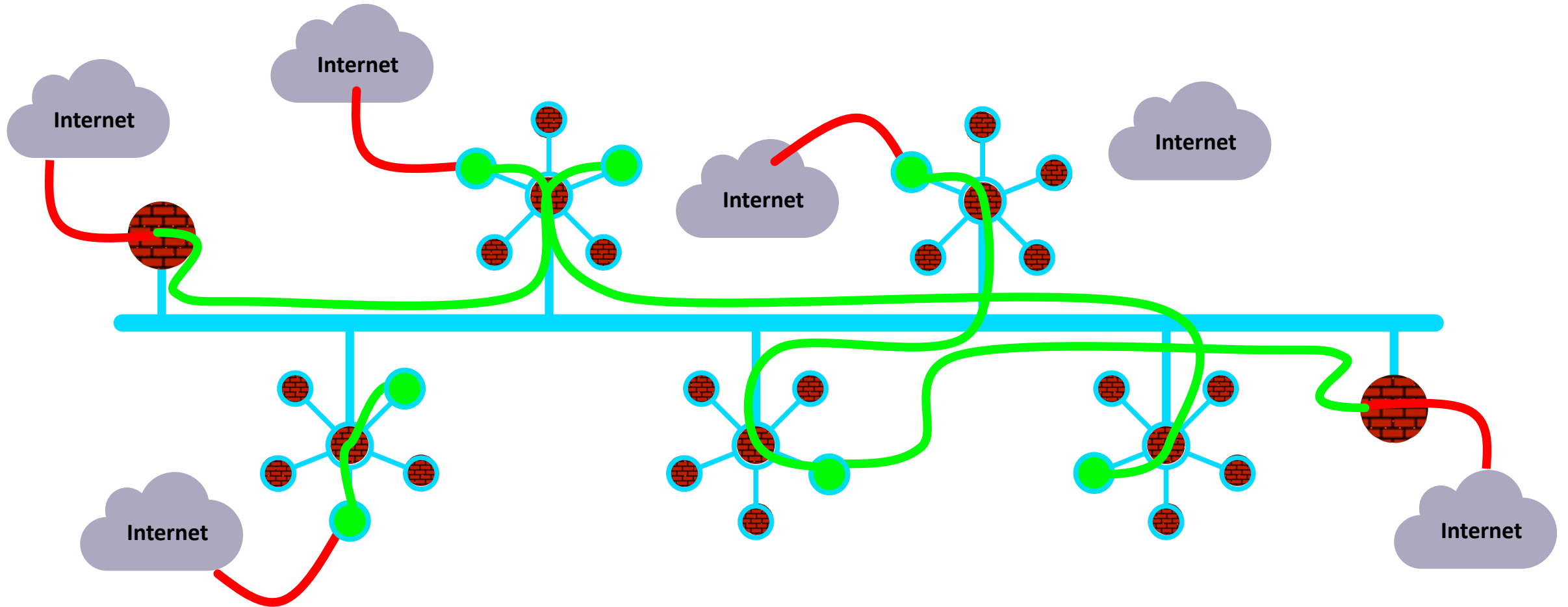
What If... the architecture was built for cloud



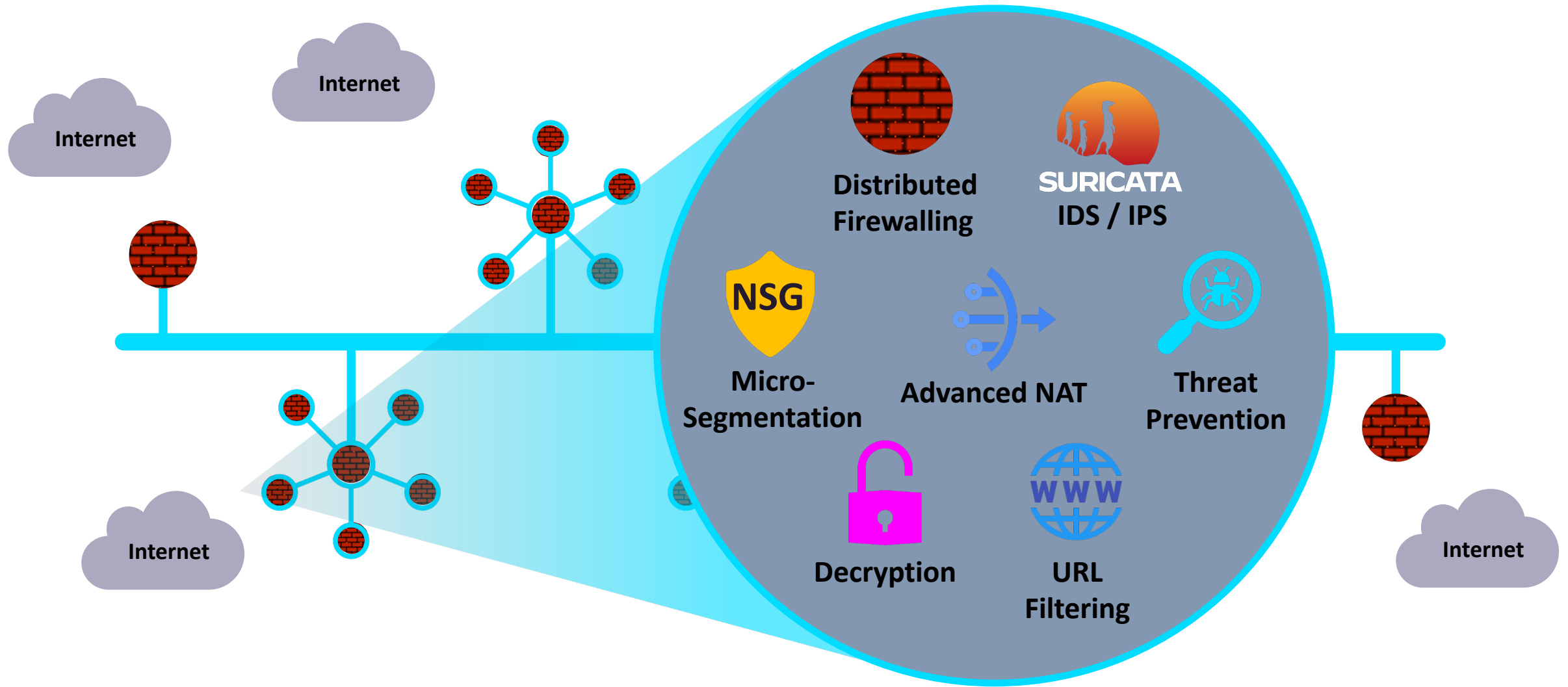
Firewalling Functions were Embedded in the Cloud Network Everywhere...



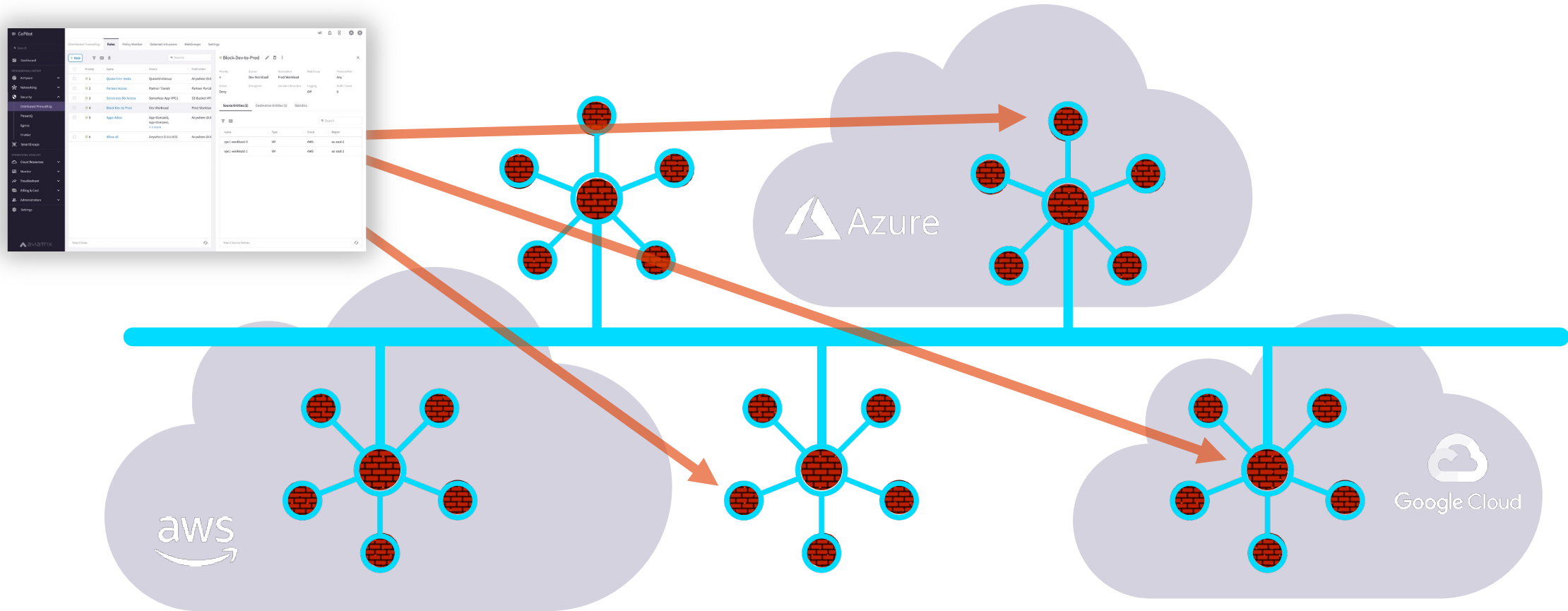
Centrally Managed, with Distributed Inspection & Enforcement...



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}

Resource attribute

- Region Name, Account Name

IP Prefixes

- CIDR

Instance: i-0380038ff7d66b66f (shopping cart app)

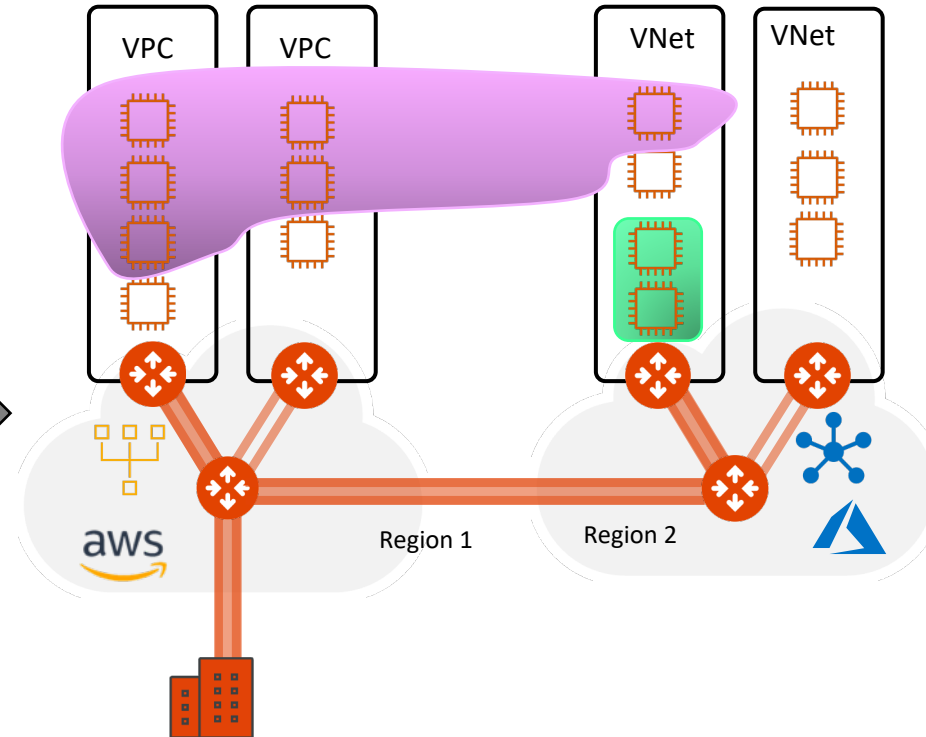
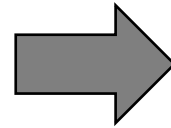
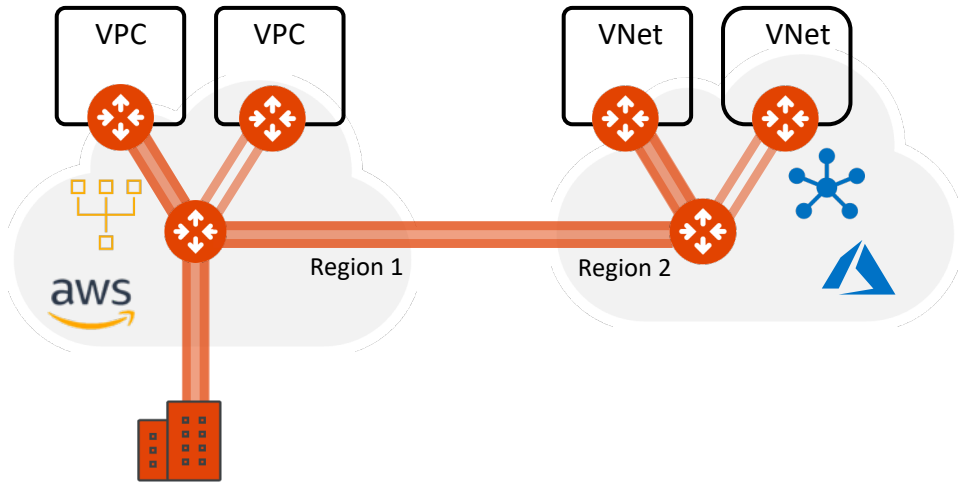
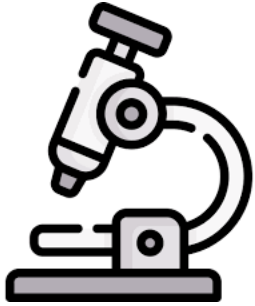
Select an instance above

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

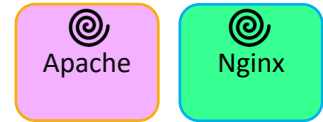
Tags

Key	Value
Env	Staging
Name	shopping cart app

Distributed Firewalling: Intra-rule vs. Inter-rule



Smart Groups

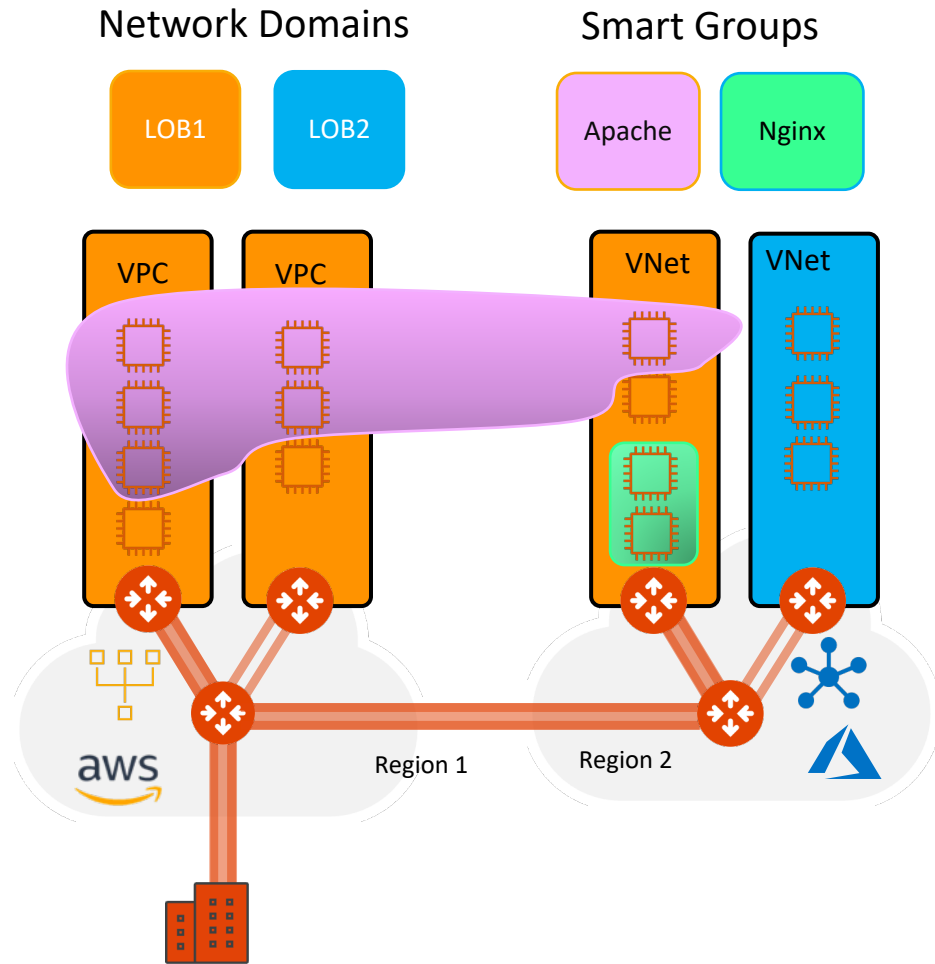


A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

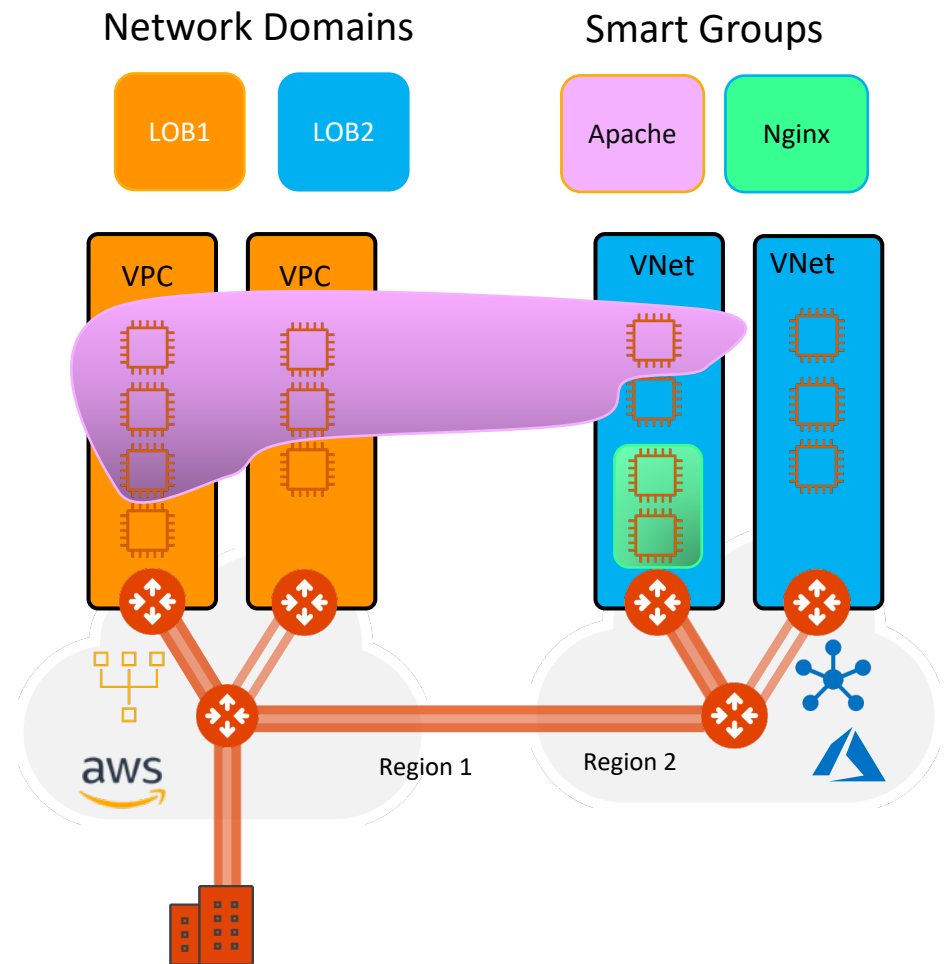
- **INTRA-RULE:** is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

- **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 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 illustrates the process of creating and managing Smart Groups in the AviaTrix CoPilot interface. The sidebar on the left provides navigation to various system components, with 'SmartGroups' highlighted. The main panel shows the 'SmartGroups' management area, where users can create new groups or refresh CSP resources. A modal window for creating a new SmartGroup is shown, with fields for Name, Resources, and Virtual Machines. A success message indicates that CSP resources have been successfully refreshed. A red arrow points from the 'Refetch CSP Resources' button to the success message, and another red arrow points from the 'Resource Selection (2)' toggle to a detailed view of the resource selection table.

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

Create New SmartGroup

Name: APACHE-FLEET-SERVERS

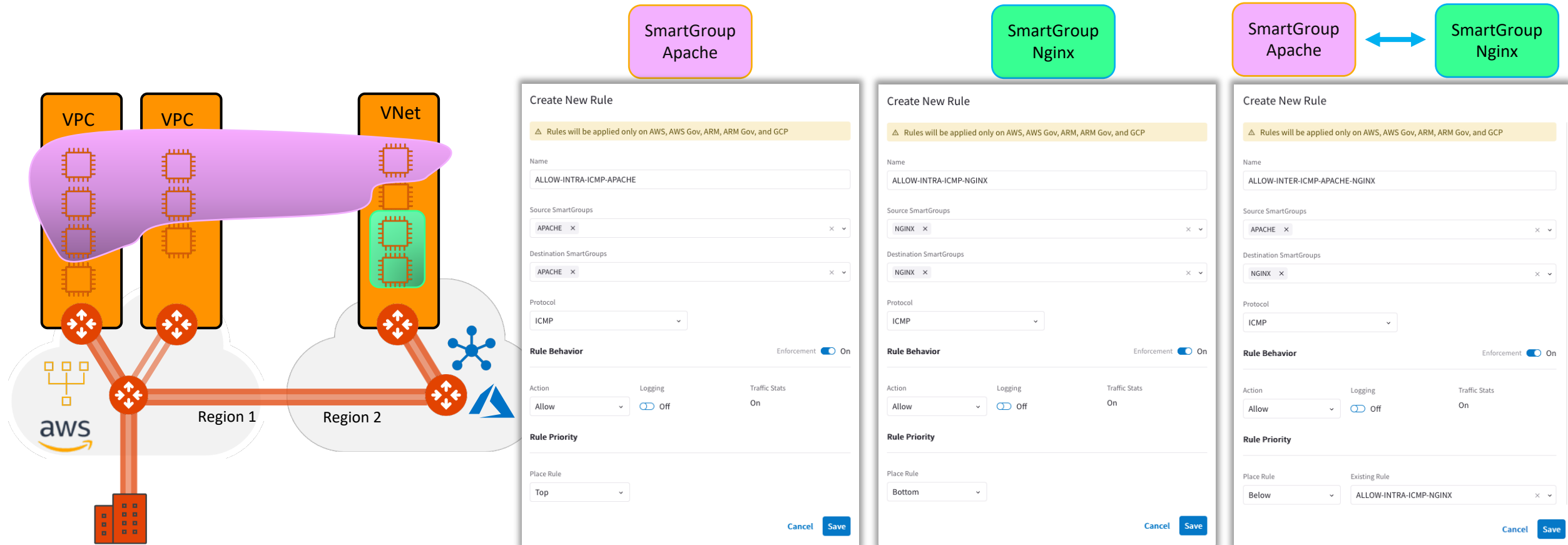
Resources

Resource Selection (2) ☒

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

- 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

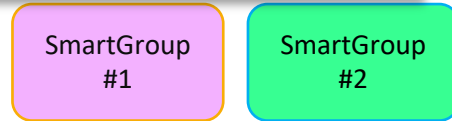
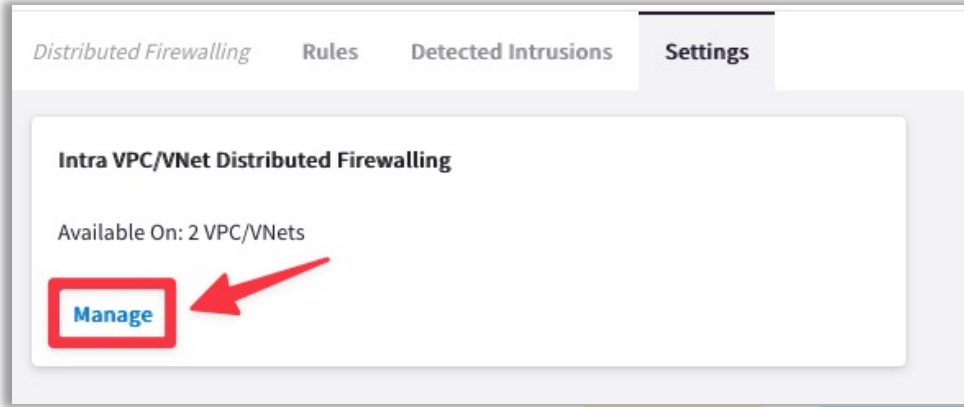
4 New Discard Commit Search

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	

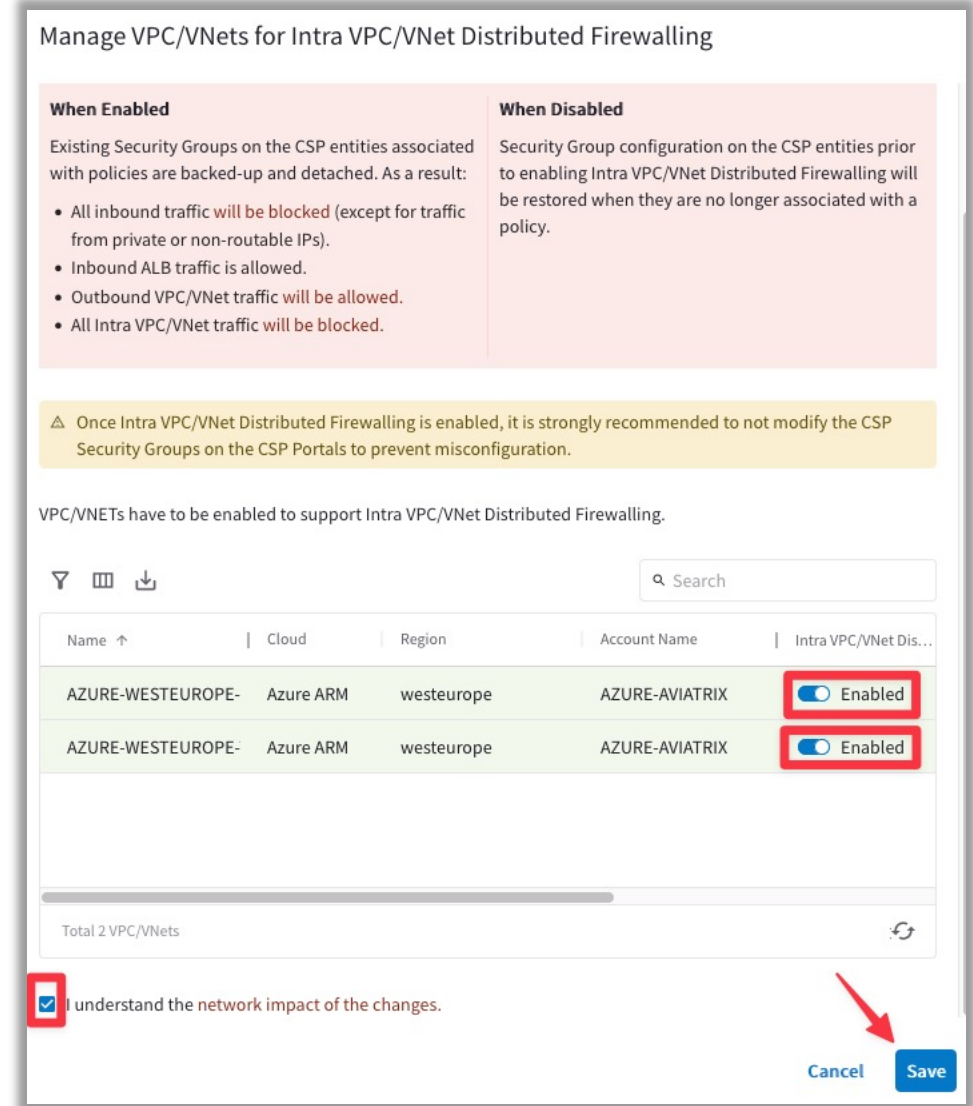
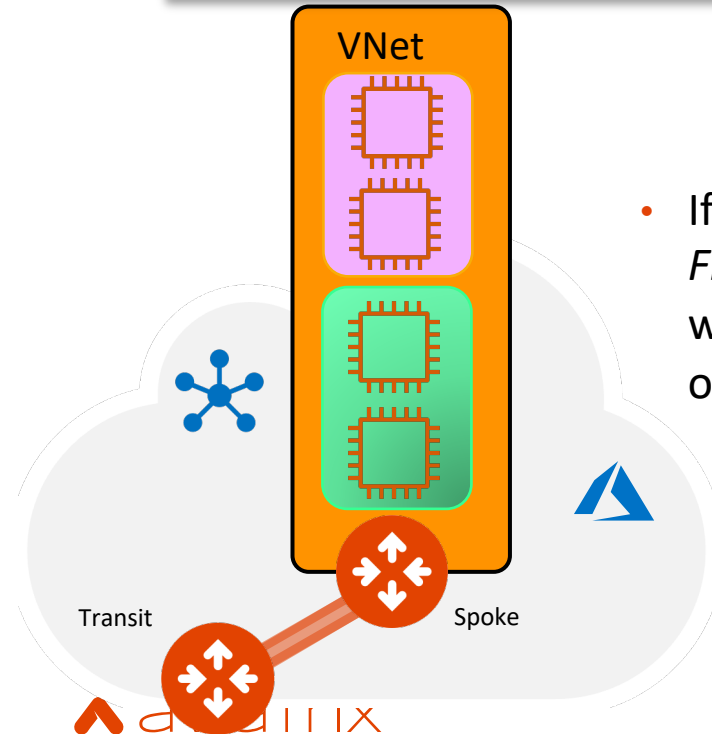
- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on “**Commit**”
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return traffic is allowed automatically

Intra VPC/VNET Distributed Firewalling (on Azure)

❑ Enable the feature on the concerned VNets



- 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.



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

Tools for troubleshooting Distributed Cloud Firewall

Creation of the Smart Group: the right matching criteria dilemma

- 1) Choose the right matching criteria for resources that you want to see assigned to a specific Smart Group:
 - ❑ 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

Create New SmartGroup

Name
BU1

Resources
Resource Selection (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 bu1

Cancel Save

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

SmartGroups

+ SmartGroup Refetch CSP Resources

Name	Resource Type
BU1	VMs

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

The screenshot shows the configuration for an intra-rule. The 'Name' field is 'intra-rule-icmp'. Both the 'Source SmartGroups' and 'Destination SmartGroups' fields contain 'BU1'. The 'Protocol' dropdown is set to 'ICMP'.

2) **Inter-rule** will affect the traffic BETWEEN Smart Groups

- ❑ Source Smart Group and Destination Smart Group must differ

The screenshot shows the configuration for an inter-rule. The 'Name' field is 'inter-rule-icmp'. The 'Source SmartGroups' field contains 'BU1' and the 'Destination SmartGroups' field contains 'BU2'. The 'Protocol' dropdown is set to 'ICMP'.

- ❑ **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 automatically 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