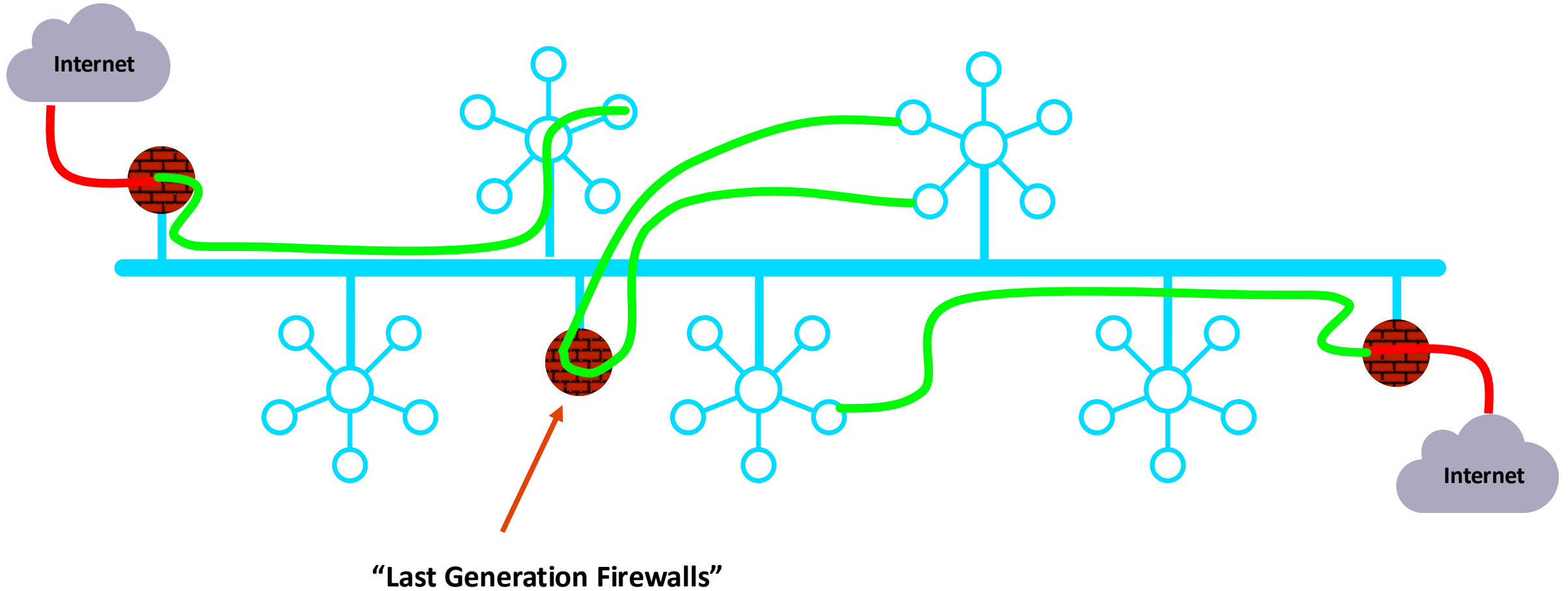




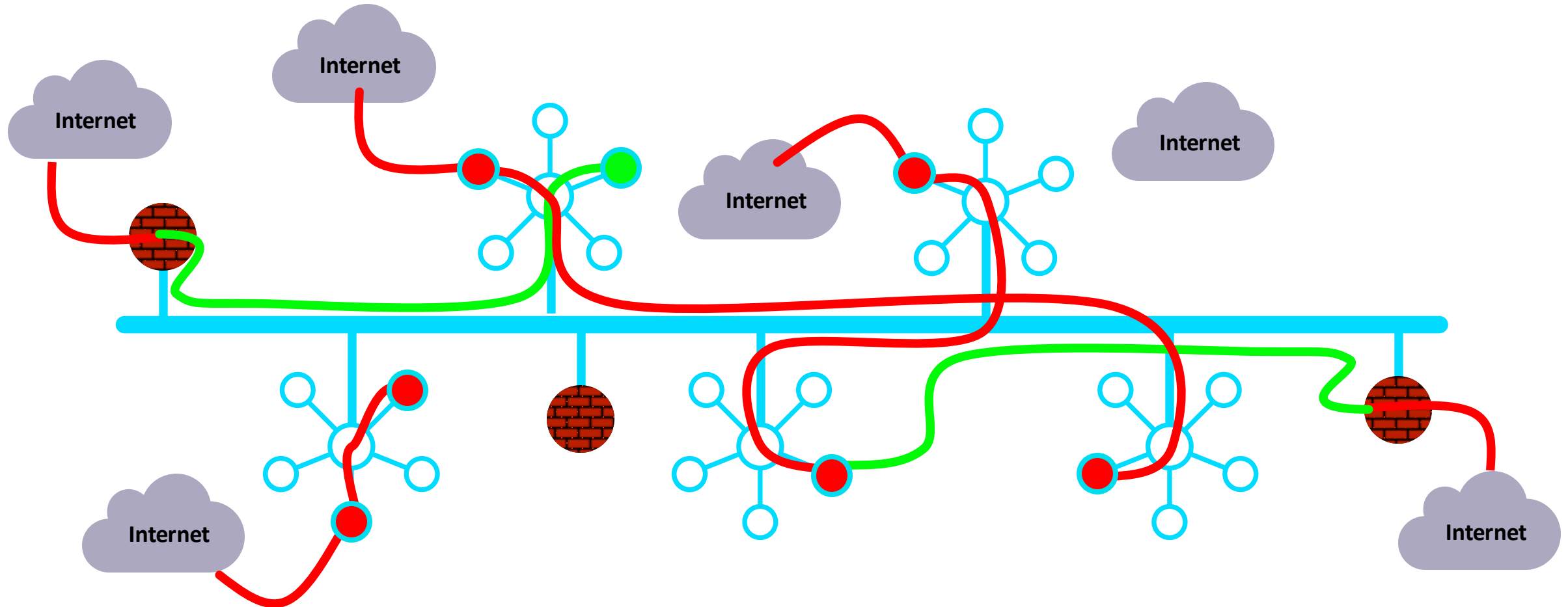
# Distributed Cloud Firewall

ACE Team

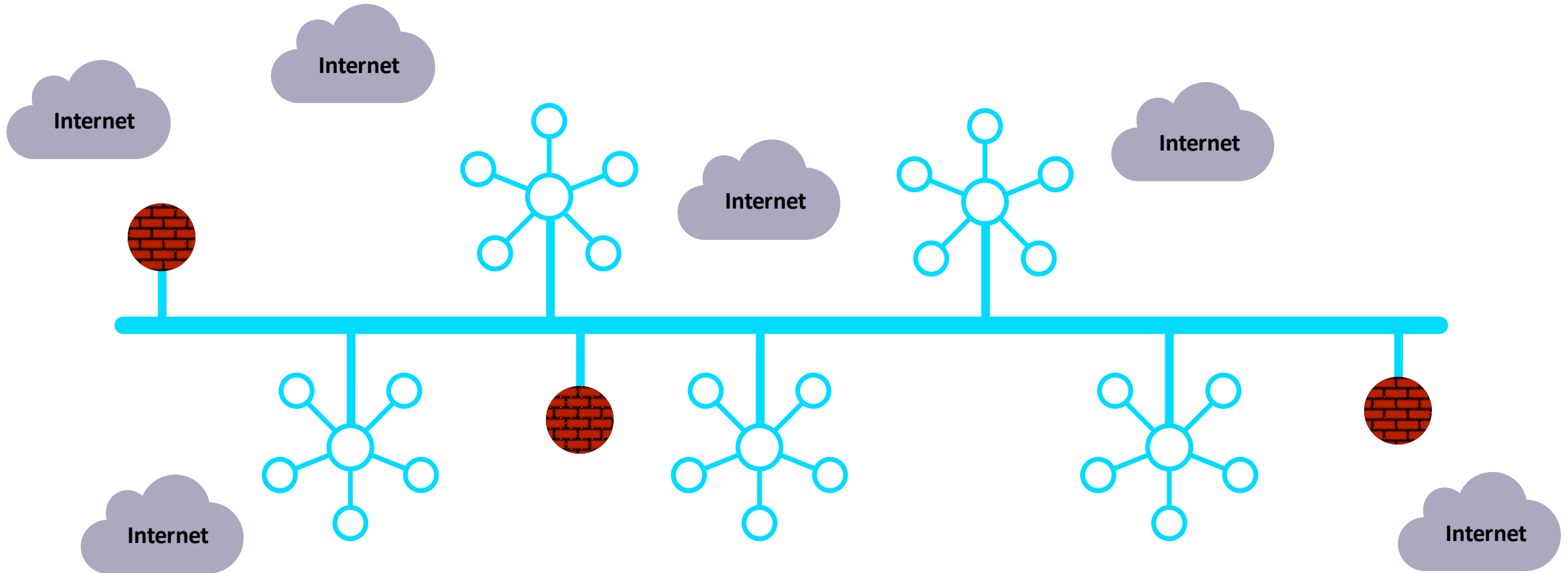
# As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



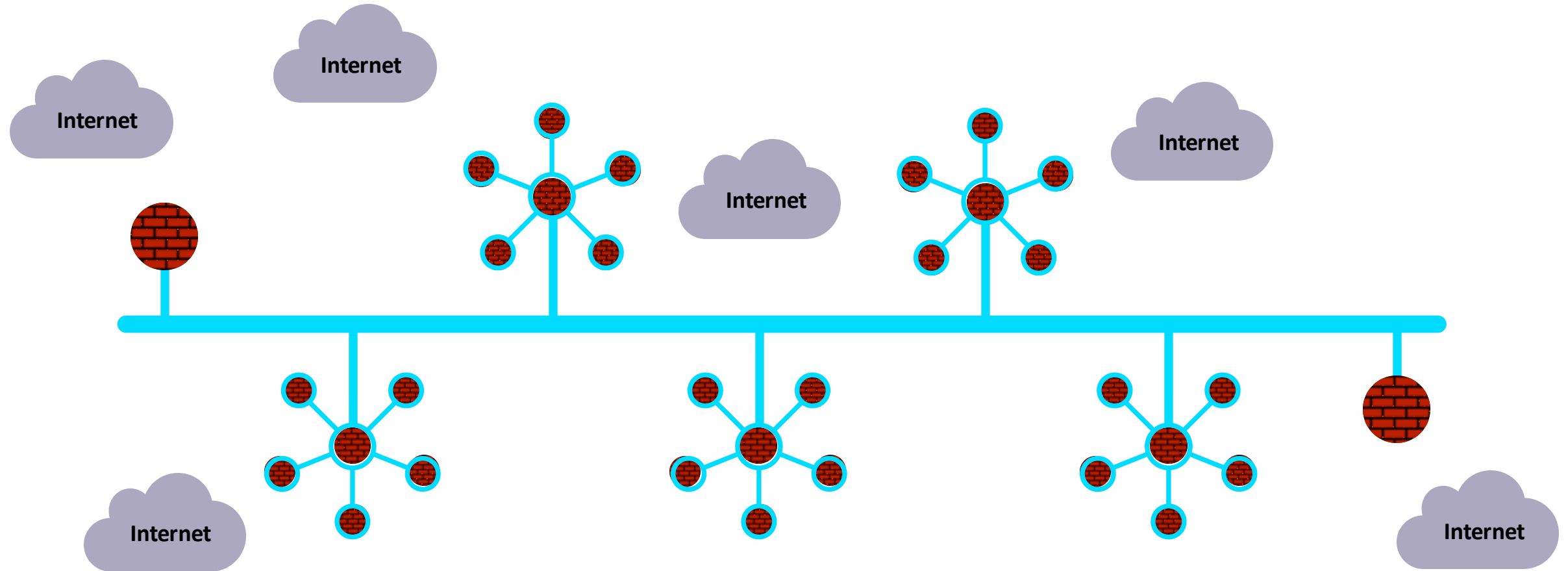
# In Reality...



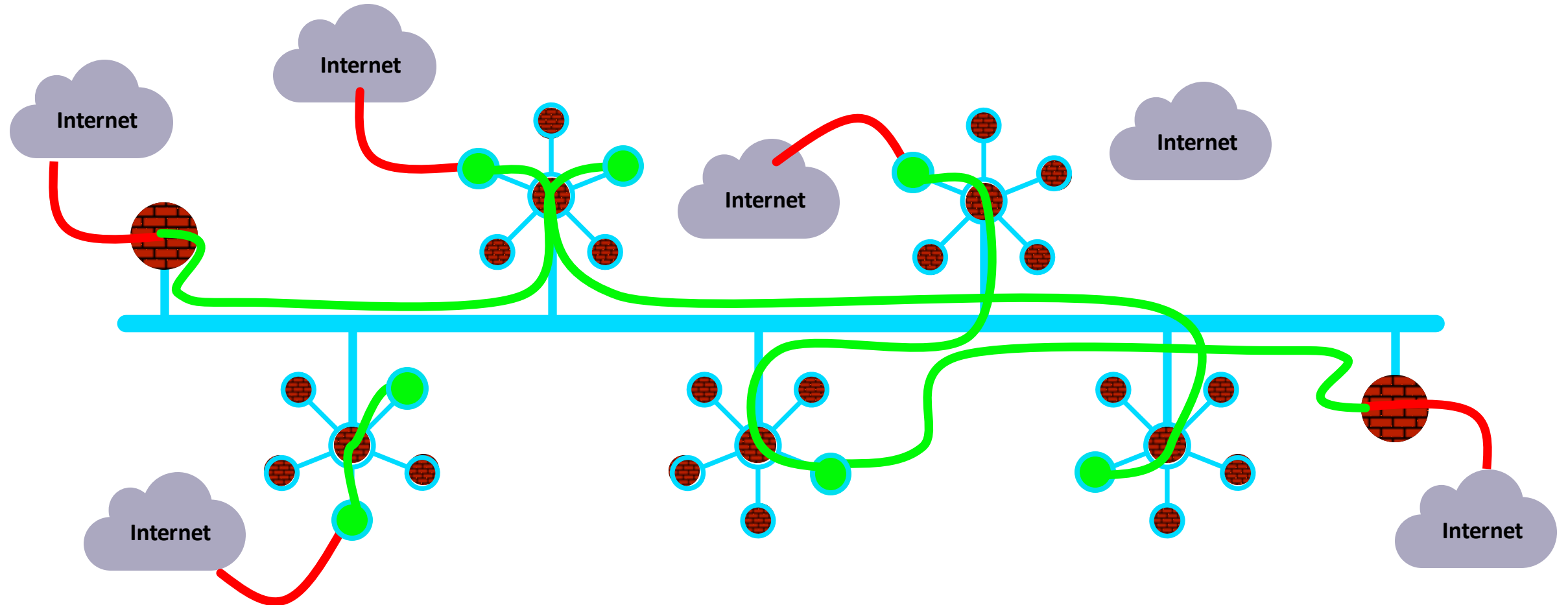
# What If... the architecture was built for cloud



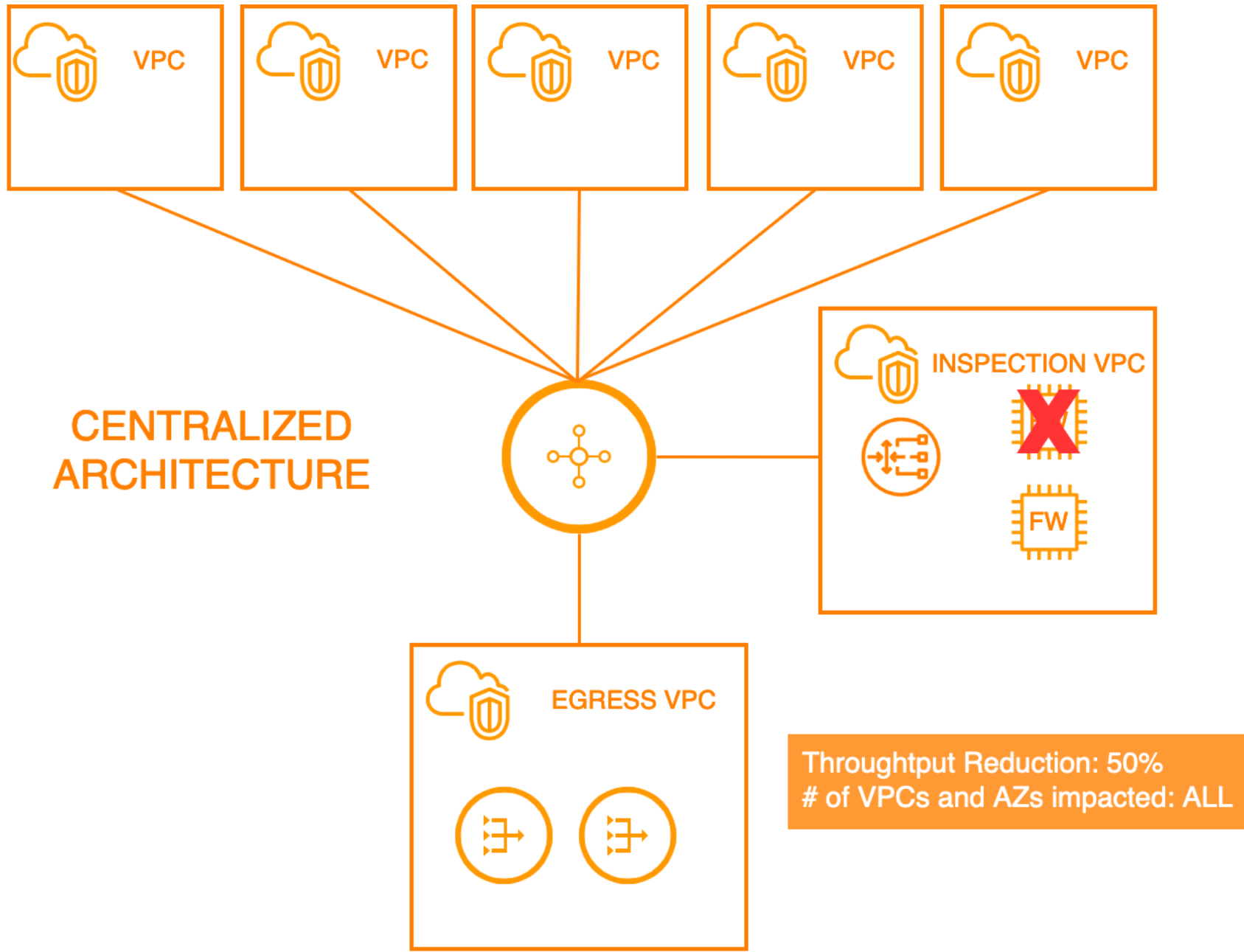
# Firewalling Functions were Embedded in the Cloud Network Everywhere...



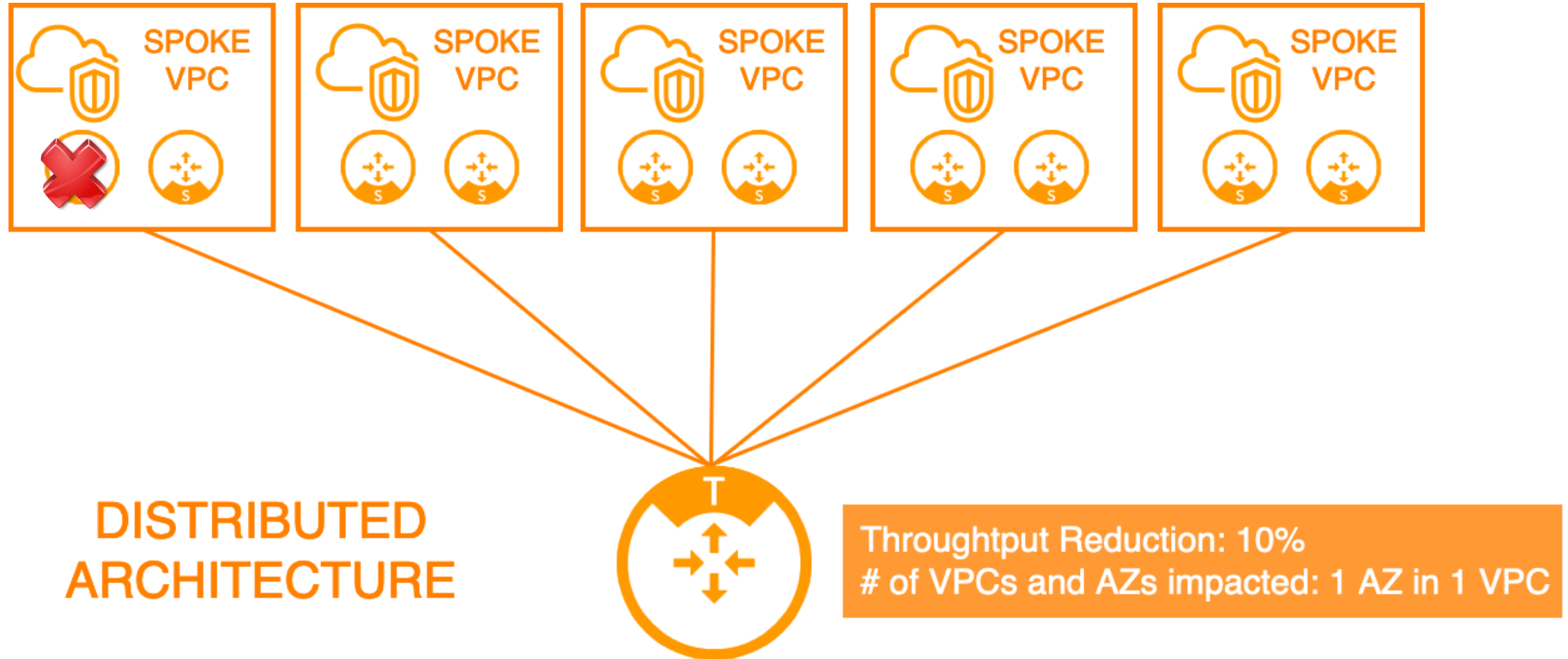
# Distribution of the Security Services into the Spokes



# Impact of Failure – Centralized Architecture



## Impact of Failure – Distributed Architecture





# Centralized Vs Distributed Firewalling Architecture



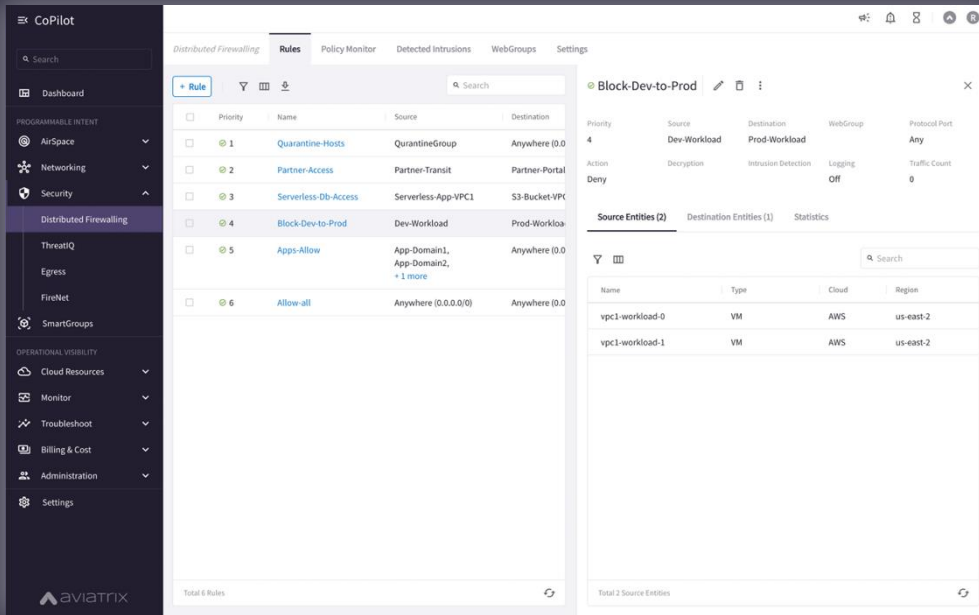
Aspect	Cloud Centralized Firewall Model	Aviatrix Distributed Cloud Firewall
Blast Radius (Fault Tolerance and Resilience)	Single point of failure risks, although mitigated by redundant systems; still, failure can affect entire network traffic.	Enhanced fault tolerance by distributing firewalls, reducing impact of localized failures and increasing overall network resilience.
Performance	Potential latency issues due to traffic bottlenecks through a centralized point; performance can degrade under high load.	Optimized for low latency by distributing firewall capabilities close to application workloads, improving overall network performance.
Cost	Maintaining centralized Firewall architectures is increasingly expensive. Cloud providers and firewall vendors profit from costly data processing charges, oversized VMs, and pricey licenses.	DCF's cloud-native design enables organizations to sidestep the costly data processing fees, oversized virtual machines, and exorbitant licensing often encountered with traditional centralized models.
Deployment Speed	Longer deployment times due to hardware installations and configurations.	Quick deployment and provisioning, leveraging cloud-native tools for rapid scaling and implementation
Noisy Neighbor	Since all network traffic is funneled through a limited set of centralized appliances, high traffic from one tenant or application can degrade the performance of others sharing the same resources	Effectively mitigates the "Noisy Neighbor" issue through its decentralized design

# And, What If Policy Creation Looked Like One Big Firewall...

Centralized Policy Creation



Distributed Enforcement



Aviatrix CoPilot



**SURICATA**  
IDS / IPS



**NSG**  
Micro-Segmentation



**Threat Prevention**



**Advanced NAT**



**Distributed Firewalling**

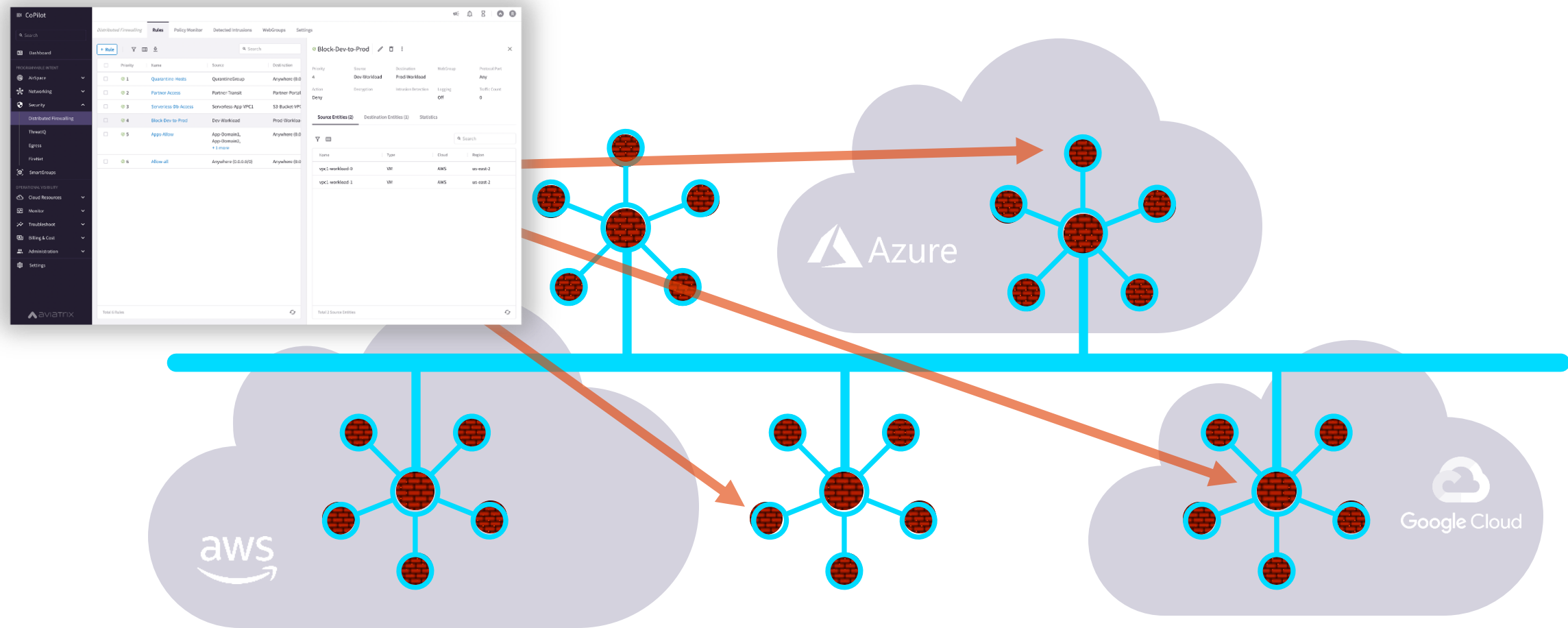


**Decryption**



**URL Filtering**

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



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

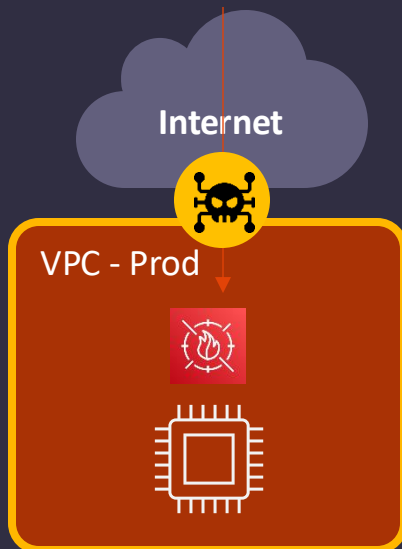
# Firewall The 3 Perimeters

Aviatrix Solution

Easy

## Ingress

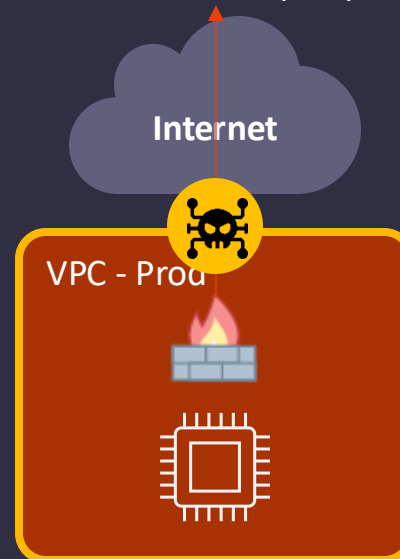
- **Why?** Detect and Block MITRE ATT&CK™ Recon, Initial Access, and Execution Phases. OWASP Top 10
- **Tools:**
  - Cloud-Native WAF and DDoS
  - CloudFlare, Akamai, F5



Easy

## Egress

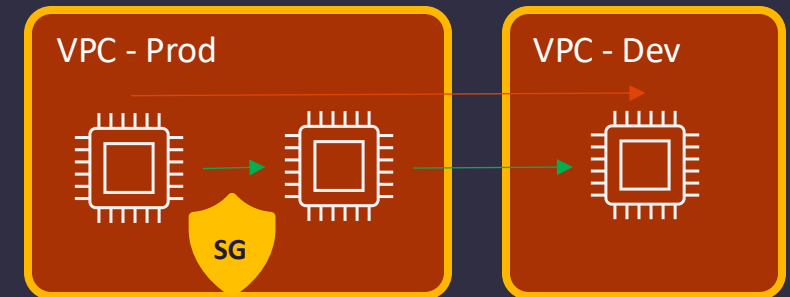
- **Why?** Detect and Block MITRE ATT&CK™ Establish Execution, Command and Control and Data Exfil Phases
- **Tools:**
  - NAT Gateways
  - Network Firewalls
  - URL/FQDN/IDS (IPS)



Moderate

## East-West

- **Why?** Detect and Block MITRE ATT&CK™ Lateral Movement Phase
- **Tools:**
  - Network Firewalls
  - Security Groups
  - Agents
  - L4, Microsegmentation, Zero Trust



# SmartGroups: Definition

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

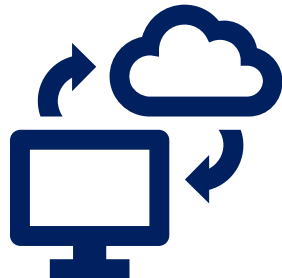
- Source
- Destination

- **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:

- CSP Tag
- Subnets
- VPC/Vnets
- Kubernetes
- Hostnames
- External Connections (S2C)



# Smart Groups Creation



CoPilot

Groups

SmartGroups ExternalGroups WebGroups Settings

+ SmartGroup

Refetch CSP Resources

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

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

Successfully refreshed CSP resources

Auto Dismisses in 4s

Dismiss

Create SmartGroup

Name

BU1

Resource Selection

Preview (3)

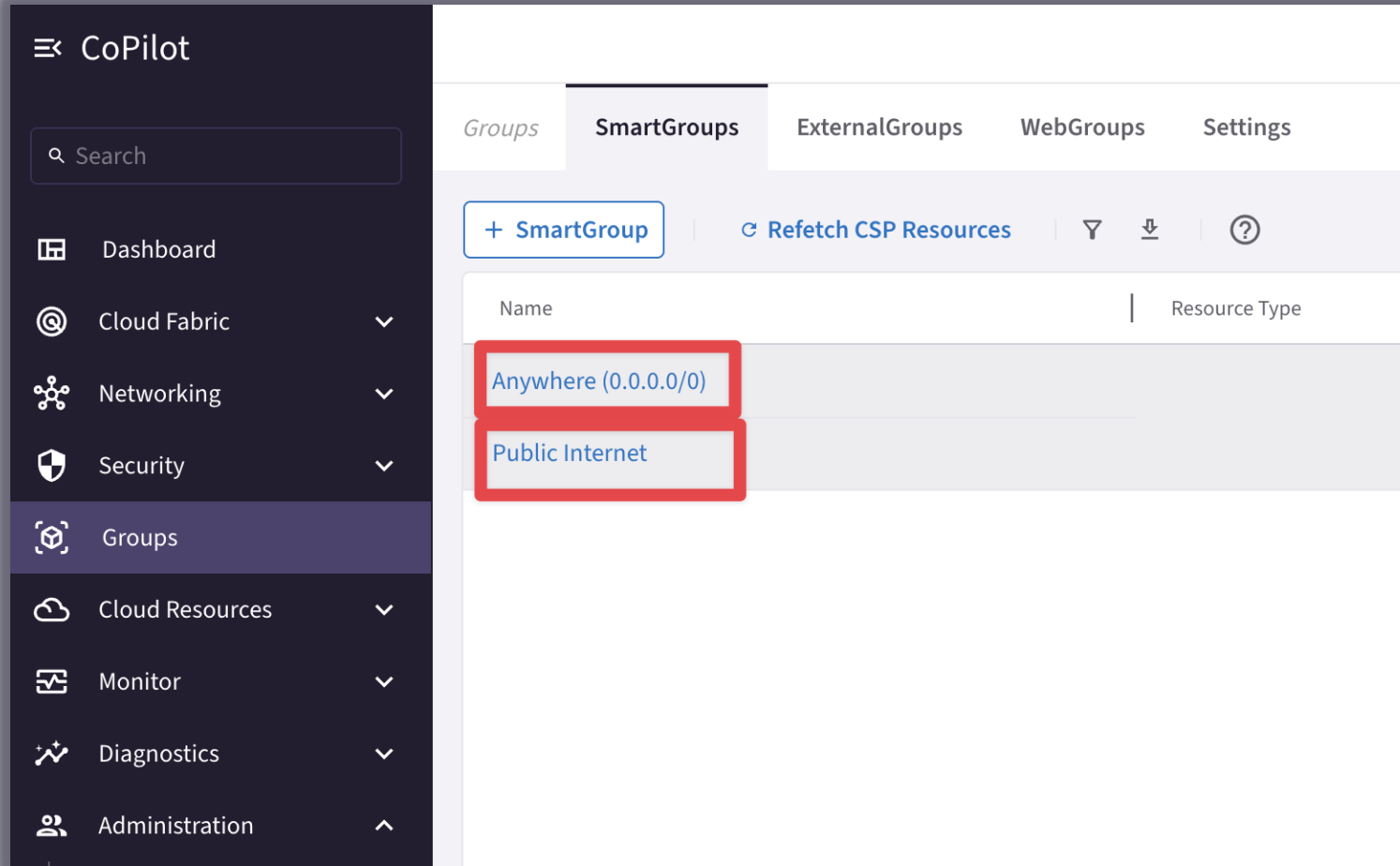
Name	Type	Cloud	Region
accounting-web-dev	VM	AWS	us-east-1
engineering-web-dev	VM	AWS	us-east-2
marketing-web-dev	VM	Azure ARM	northeurope

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



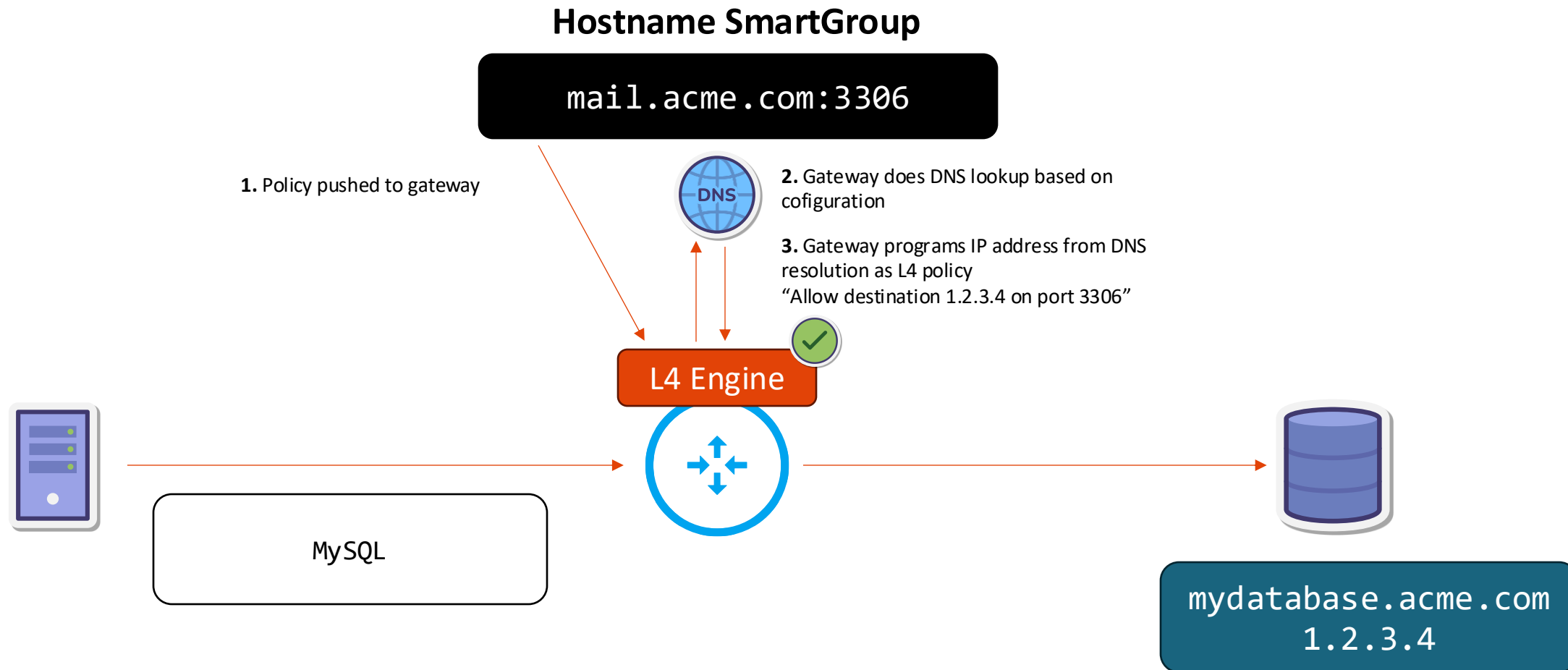
The screenshot shows the AviaTriX CoPilot interface. On the left is a dark sidebar with a menu including Dashboard, Cloud Fabric, Networking, Security, Groups (highlighted), Cloud Resources, Monitor, Diagnostics, and Administration. The main area has tabs for Groups, SmartGroups (selected), ExternalGroups, WebGroups, and Settings. Below the tabs are buttons for '+ SmartGroup', 'Refresh CSP Resources', and filters. A table lists pre-defined SmartGroups:

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)

# Hostname SmartGroups

Enables FQDN-based policies for non-TLS/HTTP Connections





# Configuring a Hostname SmartGroup



## Create a SmartGroup – Not a WebGroup

Create SmartGroup

Name

acme-mailserver

Resource Selection

Preview (1)

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

+ Resource Type

Hostnames

Preview

mail.acme.com

Cancel

Save

## Used as a Destination Group, not a WebGroup

Create Rule

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

Name

Source Groups

Anywhere (0.0.0.0/0)

Destination Groups

acme-mailserver

WebGroups

# Configuring a Hostname DNS



## Groups → Settings

**DNS Server for Hostname Resolution ⓘ**

☐ Gateway's Management DNS Server

☒ Custom DNS Servers

Maximum 2 DNS Servers

Cancel

Save

## Spoke Gateways -> Settings

Gateways

Overview

Transit Gateways

Spoke Gateways

Specialty Gateways

Gateway Management

Settings

< ☰

egress-demo

Details

Instances

Attachments

VPC/VNet Route Tables

Gateway Routes

Interface Stats

Performance

Settings

🔍 Search

▸ Network Address Translation (NAT)

▾ General

**Gateway Management DNS Server ⓘ**


☒ Aviatrix Default DNS Server

☐ Cloud VPC/VNet DNS Server

**Jumbo Frame ⓘ**

☒ On

# 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.

[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.

Distributed Cloud Firewall								
Rules								
Monitor								
Detected Intrusions								
Settings								
<a href="#">+ Rule</a>   <a href="#">Actions</a>   <a href="#">Filter</a>   <a href="#">Grid</a>   <a href="#">Download</a>   <a href="#">Help</a>								
<input type="text" value="Search"/>								
<input type="checkbox"/> Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	
<input type="checkbox"/>	214748... <a href="#">Greenfield-Rule</a>	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0...		Any		Permit	
<input type="checkbox"/>	214748... <a href="#">DefaultDenyAll</a>	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0...		Any		Deny	

# The Greenfield-Rule Structure



Edit Rule: Greenfield-Rule

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

Name  
Greenfield-Rule

Source SmartGroups  
Anywhere (0.0.0.0/0) x

Destination SmartGroups  
Anywhere (0.0.0.0/0) x

WebGroups

Protocol  
Any

Port  
All  
Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

**Rule Behavior** Enforcement ☒ Logging ☐

Action  
Permit

SG Orchestration <sup>ⓘ</sup> ☐ Off

Ensure TLS ☐ Off

TLS Decryption ☐ Off

Intrusion Detection (IDS) ☐ Off

**Rule Priority**

Cancel Save In Drafts

- **Source SmartGroups:** Anywhere(0.0.0.0/0)
- **Destination SmartGroups:** Anywhere(0.0.0.0/0)
- **Protocol:** Any
- **Action:** Permit
- Can be **edited** and **deleted**
- It can be **moved** when new rules are created like any other rules
- If it is the only rule present in the rules base, it is allocated above the implicit deny-all rule

# TLS Decryption: Decryption CA Cert

1. Download the Decryption CA Bundle.
2. Distribute the bundle across all the workloads.

① Decrypt CA Certificates should be trusted by the Source SmartGroup virtual machines when TLS Decryption is enabled for proxy.

Action

Permit



SG Orchestration ⓘ

On

Ensure TLS

Off

TLS Decryption

On

Intrusion Detection (IDS)

Off

Decrypt CA Certificates should be trusted by the **Source SmartGroup** virtual machines when TLS Decryption is enabled for proxy.

Distributed Cloud Firewall Rules Monitor Detected Intrusions Settings

**Security Group (SG) Orchestration** [Preview](#)

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

Orchestration Enabled On

Complete 1 VPC/VNets

[Pause Next Cycle](#)

[View in Topology](#) [Manage](#)

**Decryption CA Certificate**

Certificate

Expires in 10 years (Self-Signed)

[Renew Certificate](#)

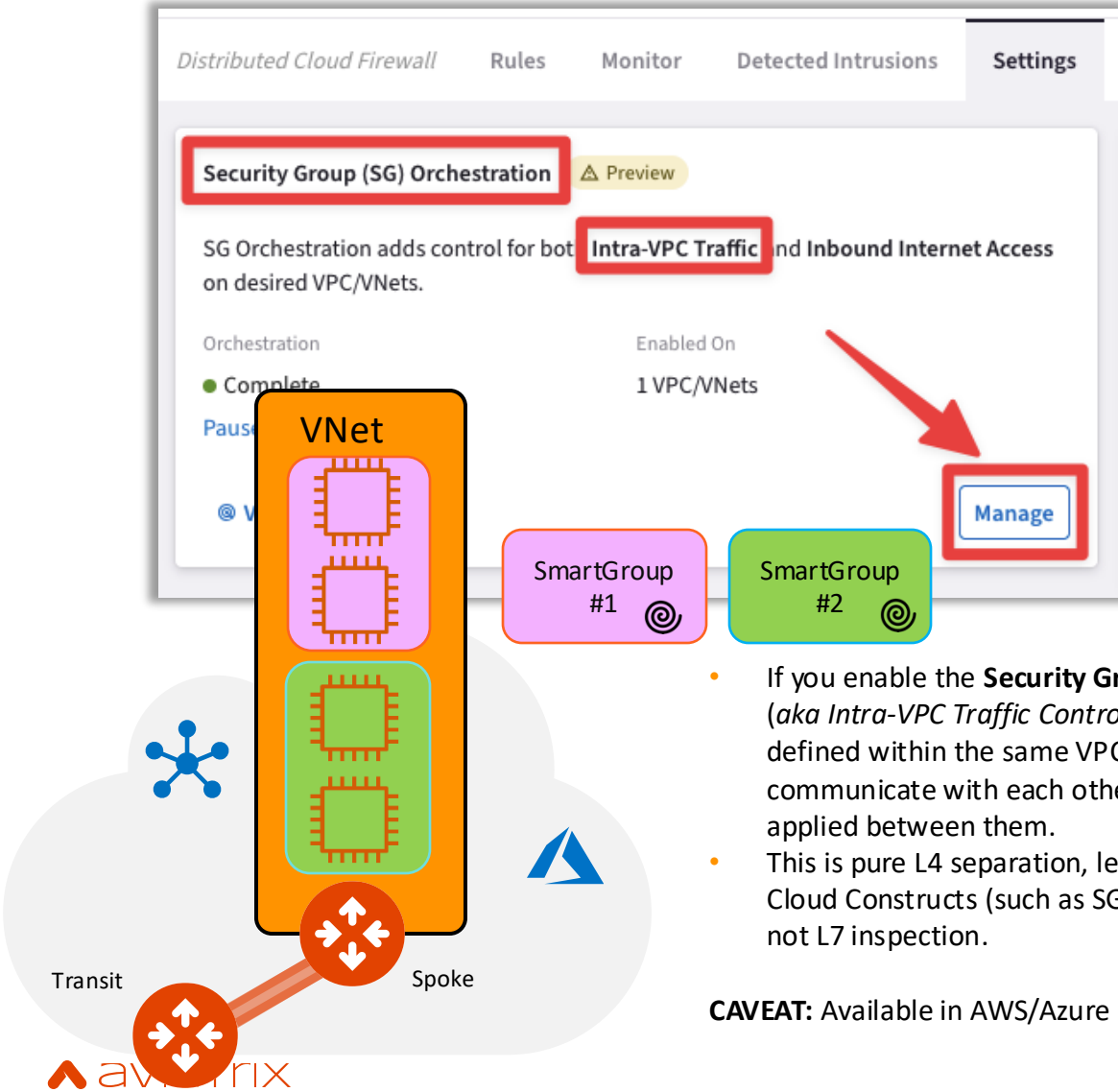
Enforcement Permissive

Trust Bundle default-trustbundle

[Download Certificate](#)

# Security Group (SG) Orchestration: Intra VPC/VNET Traffic Control

## Enable the feature on the relevant VPC/VNet



- If you enable the **Security Group (SG) Orchestration** (aka *Intra-VPC Traffic Control*), the SmartGroups defined within the same VPC/VNet will not be able to communicate with each other, unless an inter rule is applied between them.
- This is pure L4 separation, leveraging the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.

**CAVEAT:** Available in AWS/Azure

### 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 Rule

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

Name  
Allow-HTTPS

Source SmartGroups  
AVX-FRANKFURT-PROD1

Destination SmartGroups  
Public Internet

WebGroups  
Any-Web

Protocol  
TCP

Port  
443

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior

Enforcement ☒ Logging ☐

Action  
Permit

SG Orchestration ☐ Off

Ensure TLS ☐ Off

TLS Decryption ☐ Off

Intrusion Detection (IDS) ☐ Off

Rule Priority

Cancel Save In Drafts

## ☐ 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 Rule

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

Name: Allow-HTTPS

Source SmartGroups: AVX-FRANKFURT-PROD1

Destination SmartGroups: Public Internet

WebGroups: Any-Web

Protocol: TCP, Port: 443

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior: Action: Permit, SG Orchestration: Off, Ensure TLS: Off, TLS Decryption: Off, Intrusion Detection (IDS): Off

Rule Priority:

Enforcement: ☒ Logging: ☒

Cancel Save In Drafts

### Monitor

Auto Refresh ☐ Search All Logs

Timestamp	Rule	Source IP	Destination IP	URL	Protocol	Source Port	Destination Port	Action	Enforced
Mar 25, 2025 5:54:04 PM	default-deny-all	10.2.5.141	10.4.2.10		TCP	44324	3306	Deny	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.2.5.149	10.4.2.10		TCP	57200	3306	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.40	209.85.202.138		TCP	56834	443	Permit	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.40	23.217.72.114		TCP	44650	443	Permit	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.70	209.85.203.102		TCP	57610	443	Permit	On
Mar 25, 2025 5:54:03 PM	default-deny-all	10.1.5.13	10.2.5.163		TCP	56230	443	Deny	On
Mar 25, 2025 5:54:03 PM	allow-internet-https	10.2.2.70	2.18.237.177		TCP	41148	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-k8s-prod-marketing	10.1.5.57	10.2.5.161		TCP	34700	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-internet-https	10.1.5.13	151.101.3.52		TCP	47030	443	Permit	On
Mar 25, 2025 5:54:01 PM	allow-internet-https	10.1.5.47	147.75.40.148		TCP	60574	443	Permit	On

Logging can be turned ON/OFF per rule

Configure Syslog to view the logs