aviatrix

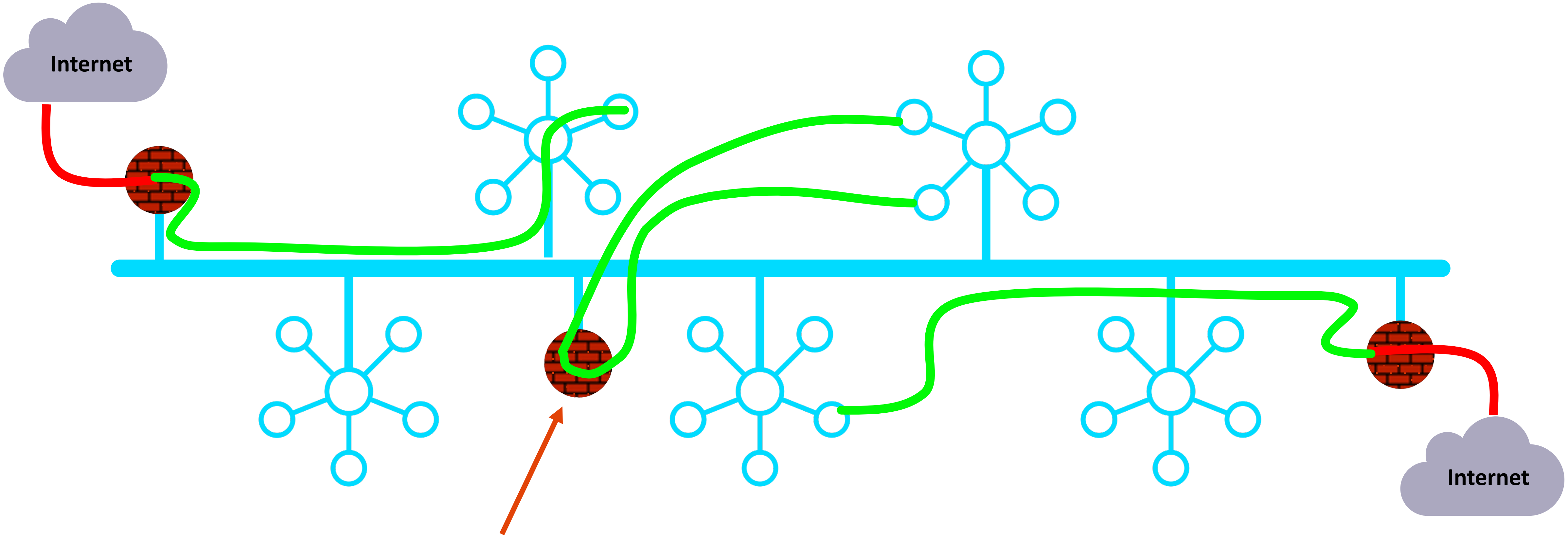
ACE

Aviatrix Certified Engineer

Distributed Cloud Firewall

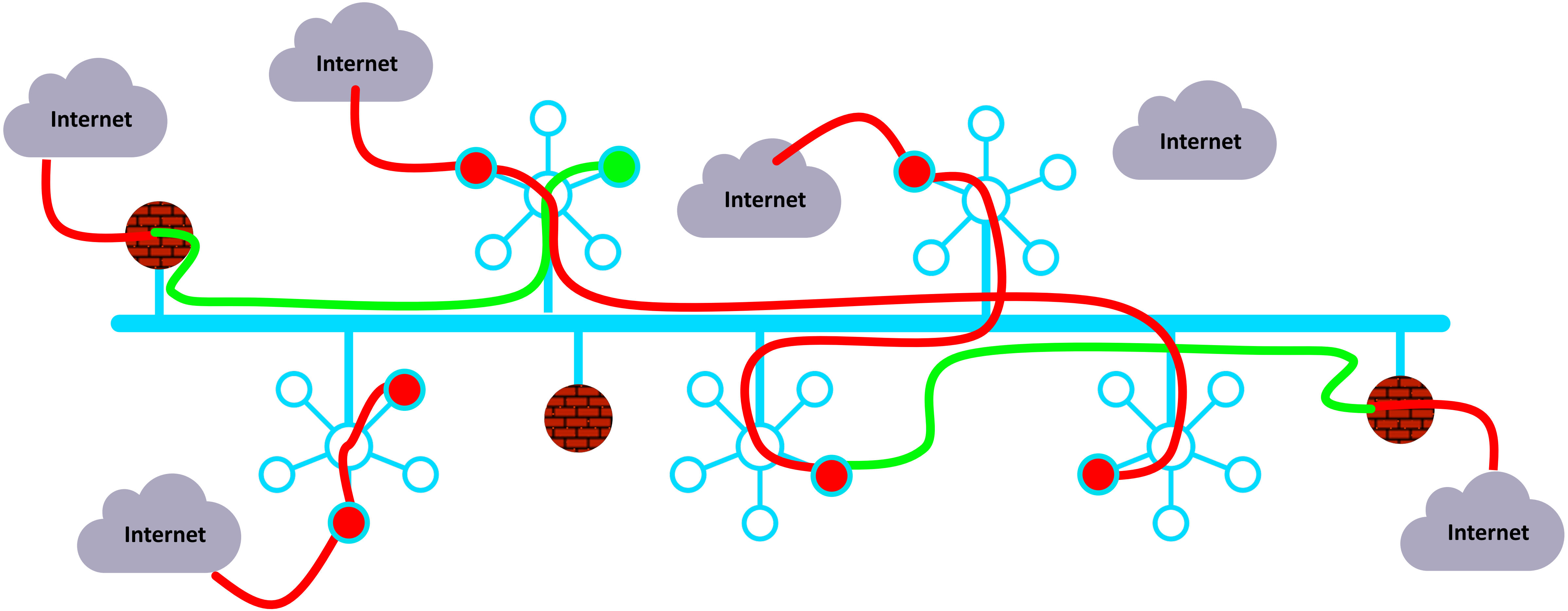
ACE Solutions Architecture Team

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

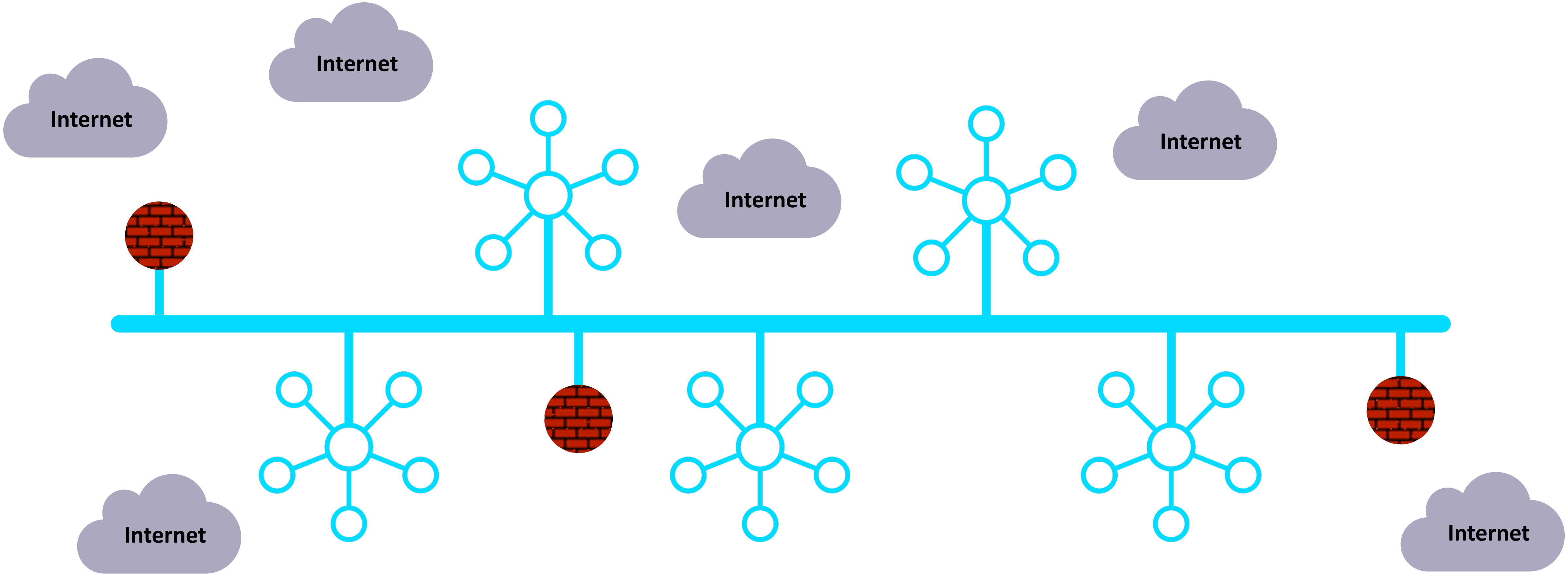


“Last Generation Firewalls”

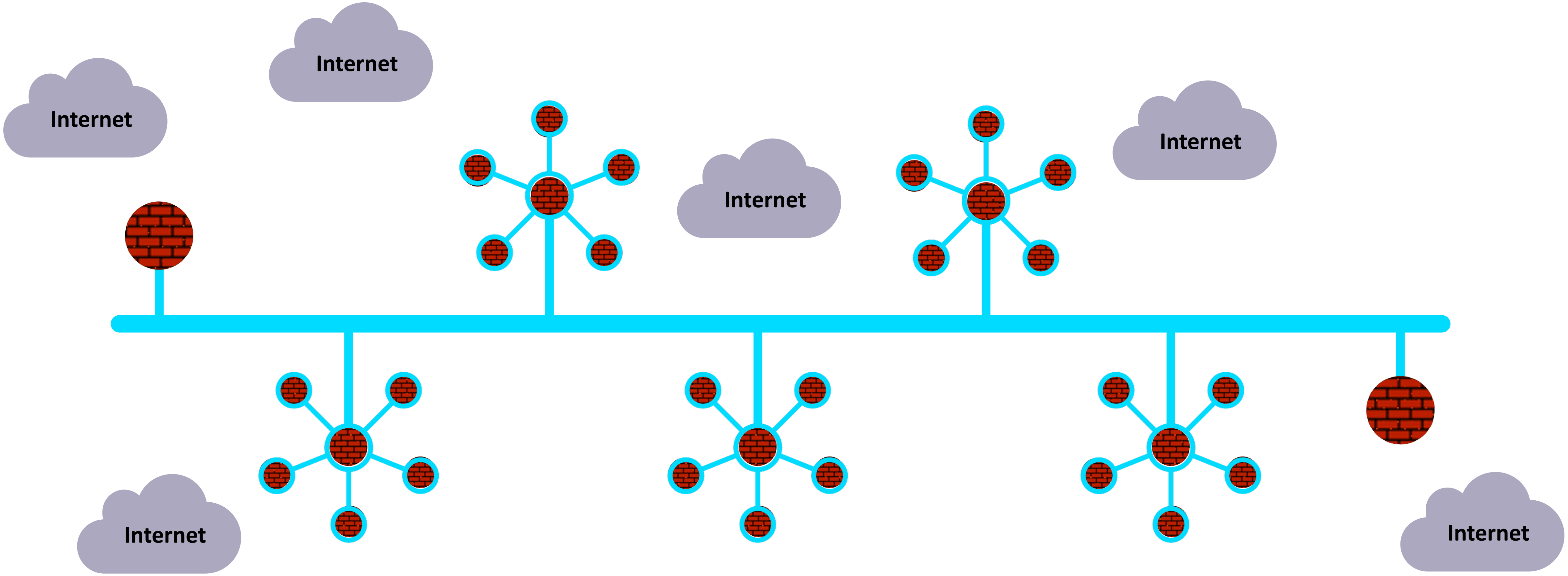
In Reality…



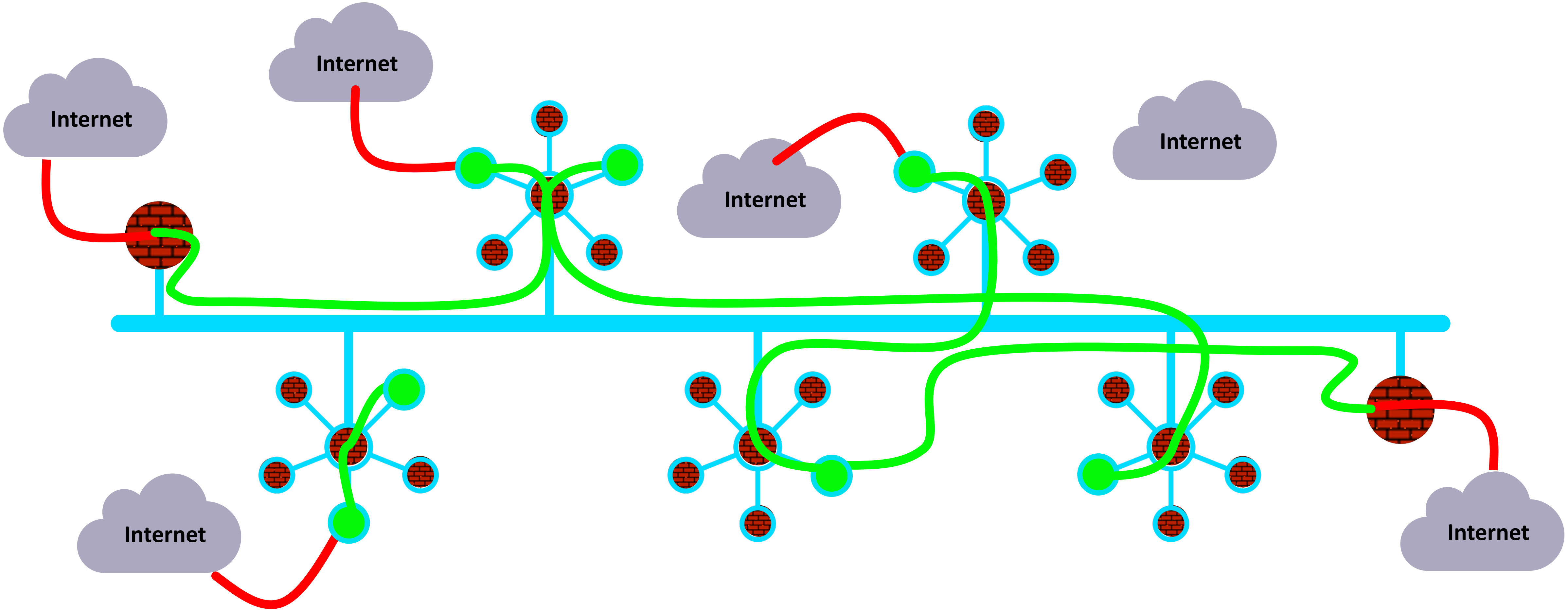
What If… the architecture was built for cloud



Firewalling Functions were Embedded in the Cloud Network Everywhere…

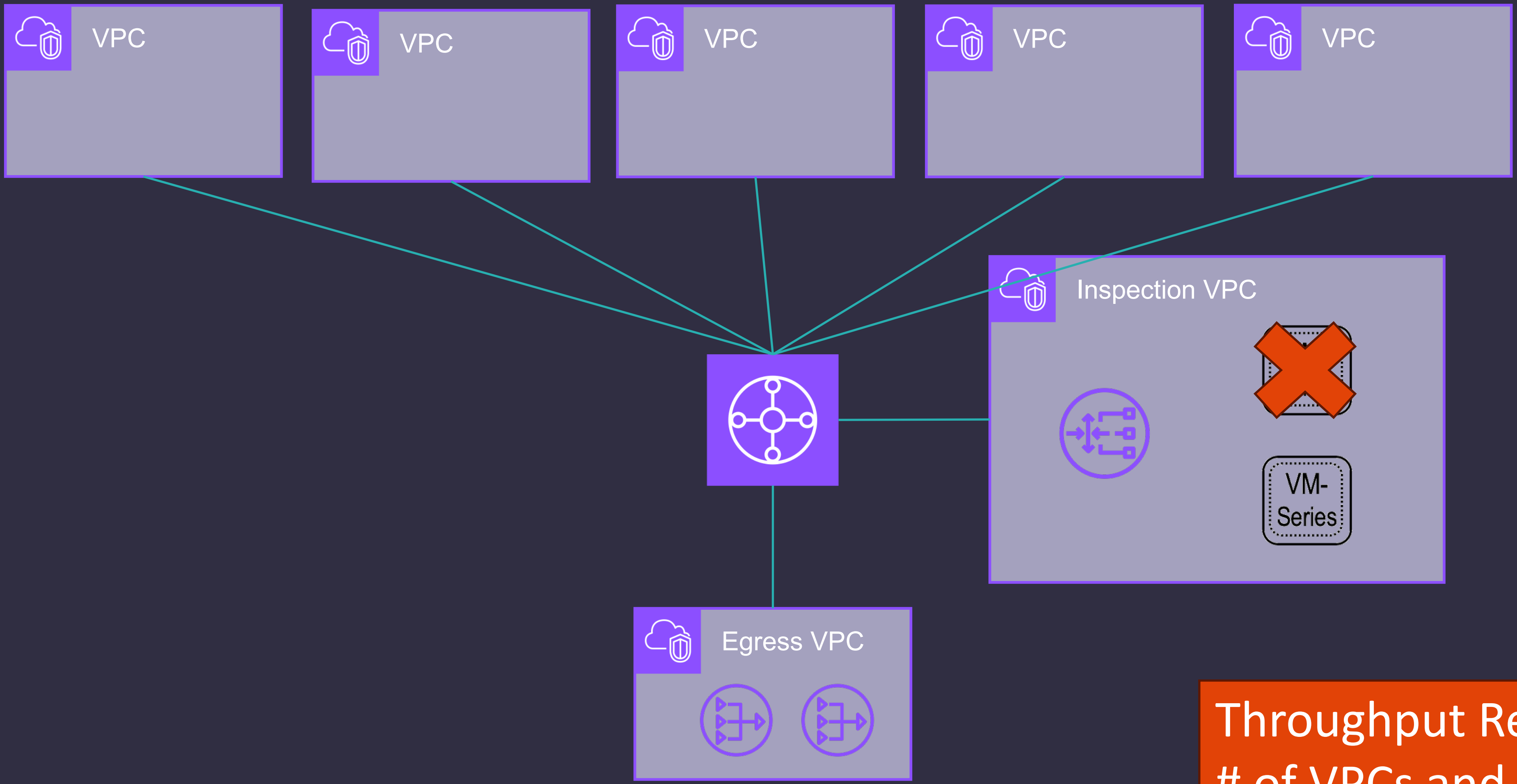


Distribution of the Security Services into the Spokes



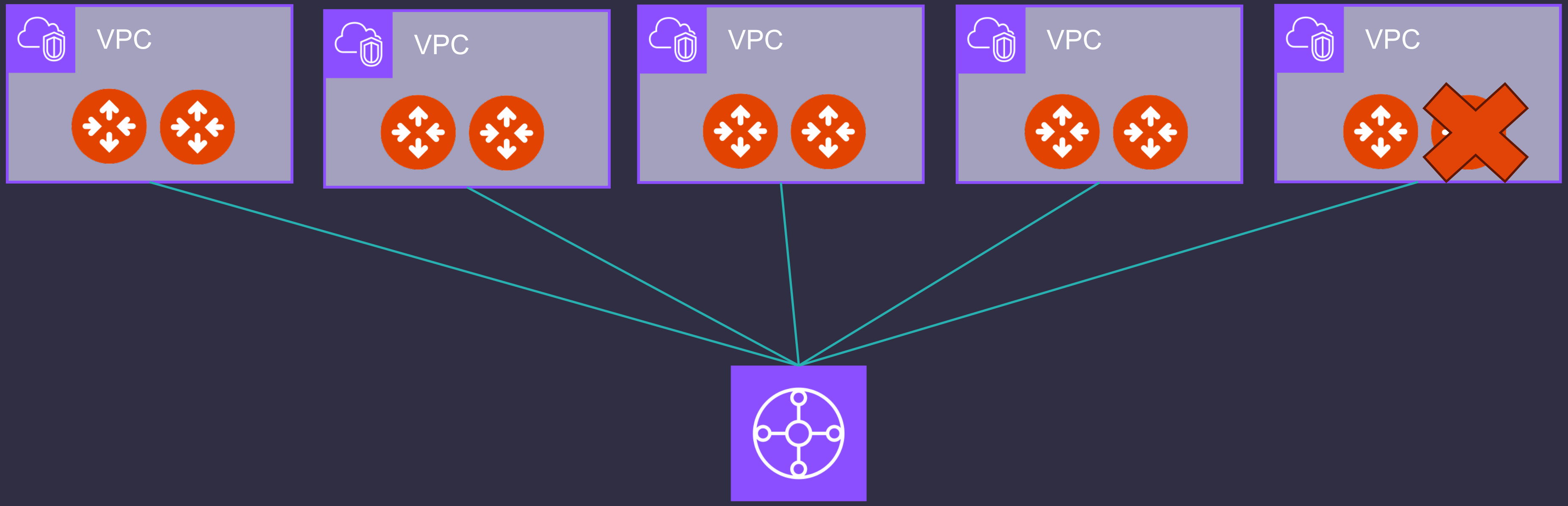
How companies are navigating the network security is an obstacle course in 2024

Impact of Failure – Centralized Architecture



Throughput Reduction: 50%
# of VPCs and AZs Impacted: ALL

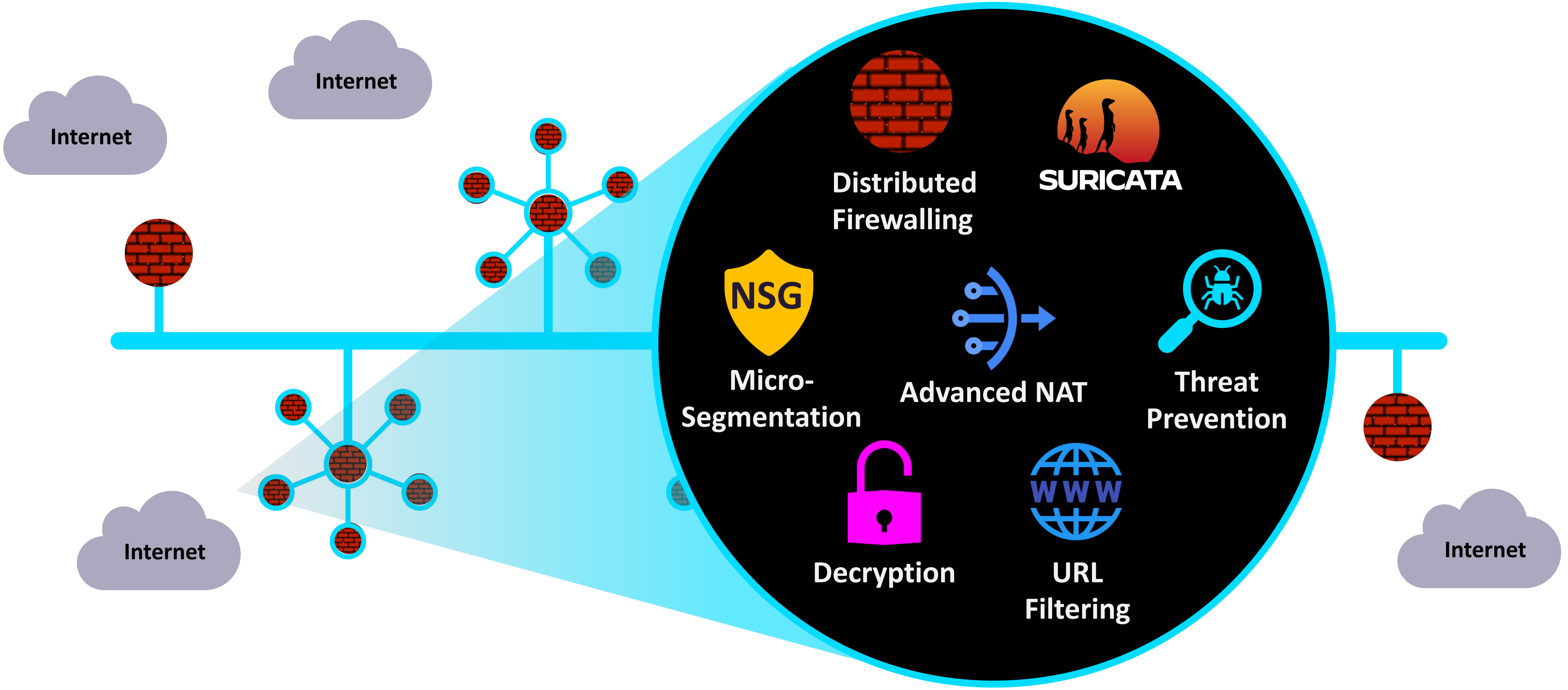
Impact of Failure – Distributed Architecture



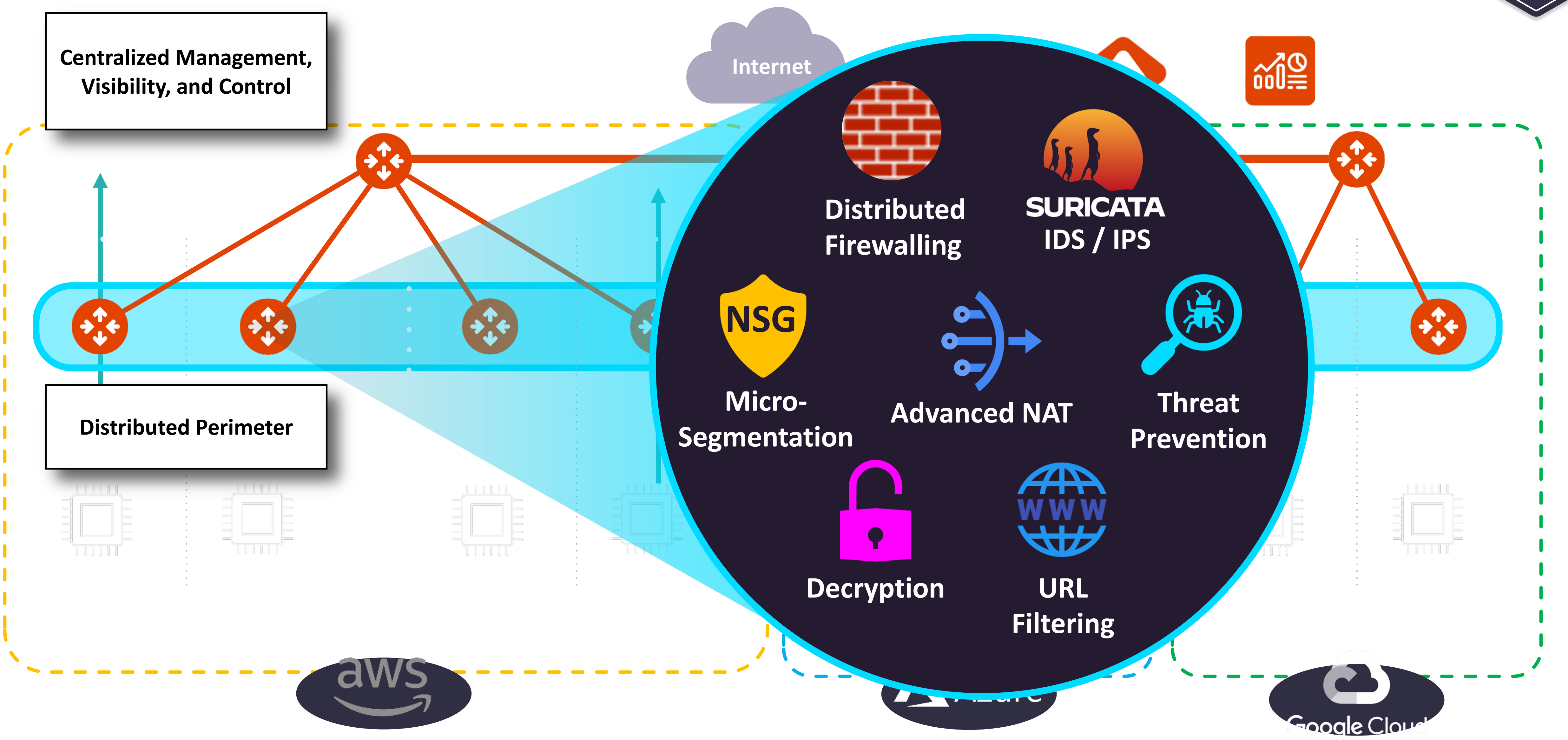
Throughput Reduction: 10%

# of VPCs and AZs Impacted: 1 AZ in 1 VPC

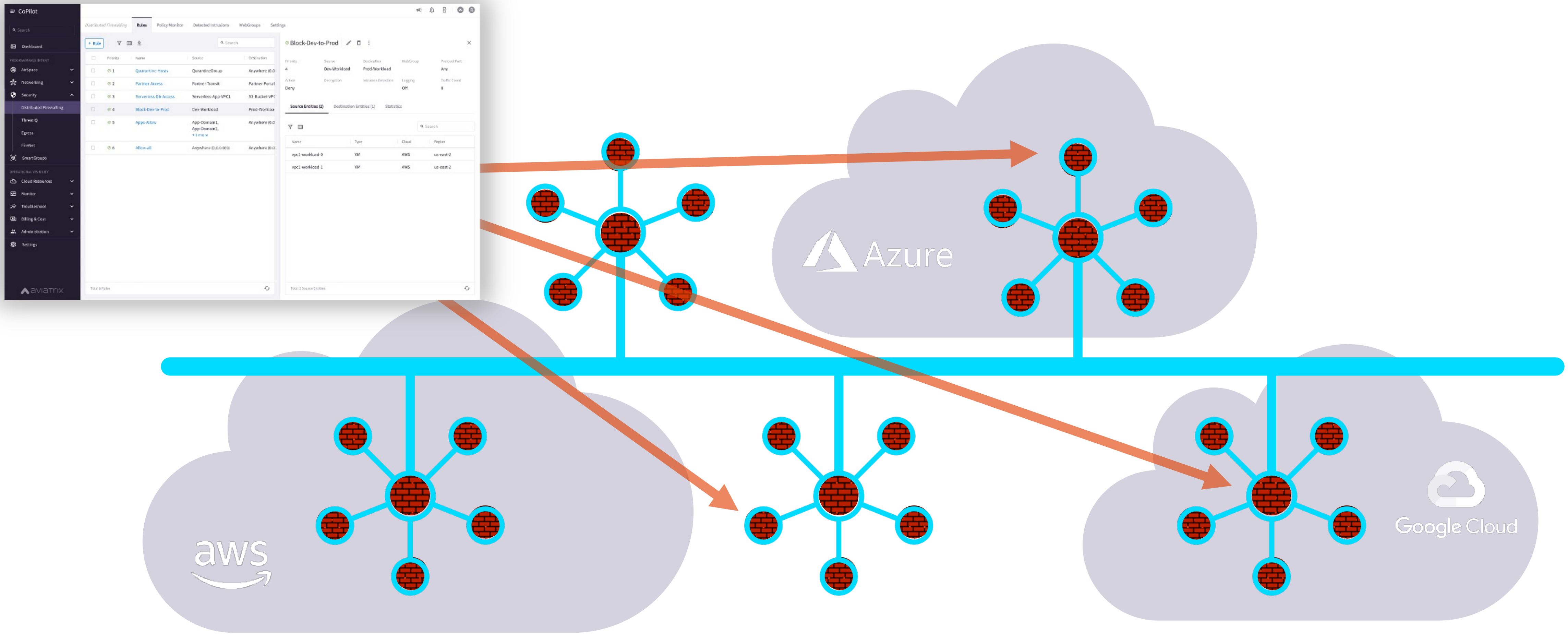
And, What If it was more than just firewalling…



Aviatrix Distributed Cloud Firewall



Policy Creation Looked Like One Big Firewall … A Distributed Cloud Firewall…



Priority	Name	Source	Destination
1	Quarantine-Hosts	QurantineGroup	Anywhere (0.0
2	Partner-Access	Partner-Transit	Partner-Portal
3	Serverless-Db-Access	Serverless-App-VPC1	S3-Bucket-VP
4	Block-Dev-to-Prod	Dev-Workload	Prod-Workloa
5	Apps-Allow	App-Domain1, App-Domain2, + 1 more	Anywhere (0.0
6	Allow-all	Anywhere (0.0.0.0/0)	Anywhere (0.0

Total 6 Rules

Block-Dev-to-Prod

Priority	Source	Destination	WebGroup	Protocol Port
4	Dev-Workload	Prod-Workload		Any

Action	Decryption	Intrusion Detection	Logging	Traffic Count
Deny			Off	0

Source Entities (2) Destination Entities (1) Statistics

Name	Type	Cloud	Region
vpc1-workload-0	VM	AWS	us-east-2
vpc1-workload-1	VM	AWS	us-east-2

Total 2 Source Entities

Where and How Policies Are Enforced Is Abstracted…

SmartGroups: Definition

- A firewall rule consists of two important initial elements:
  - **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 *three* methods:
  - CSP Tags
  - Resource Attributes
  - CIDR

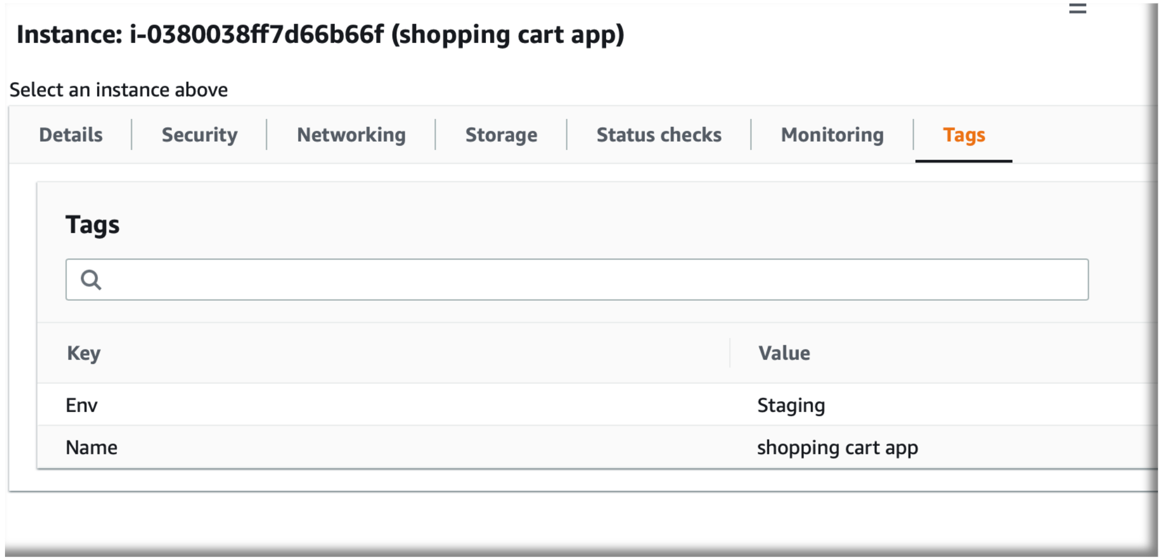
SmartGroups: Classification Methods

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

Tags

Key	Value
Env	Staging
Name	shopping cart app

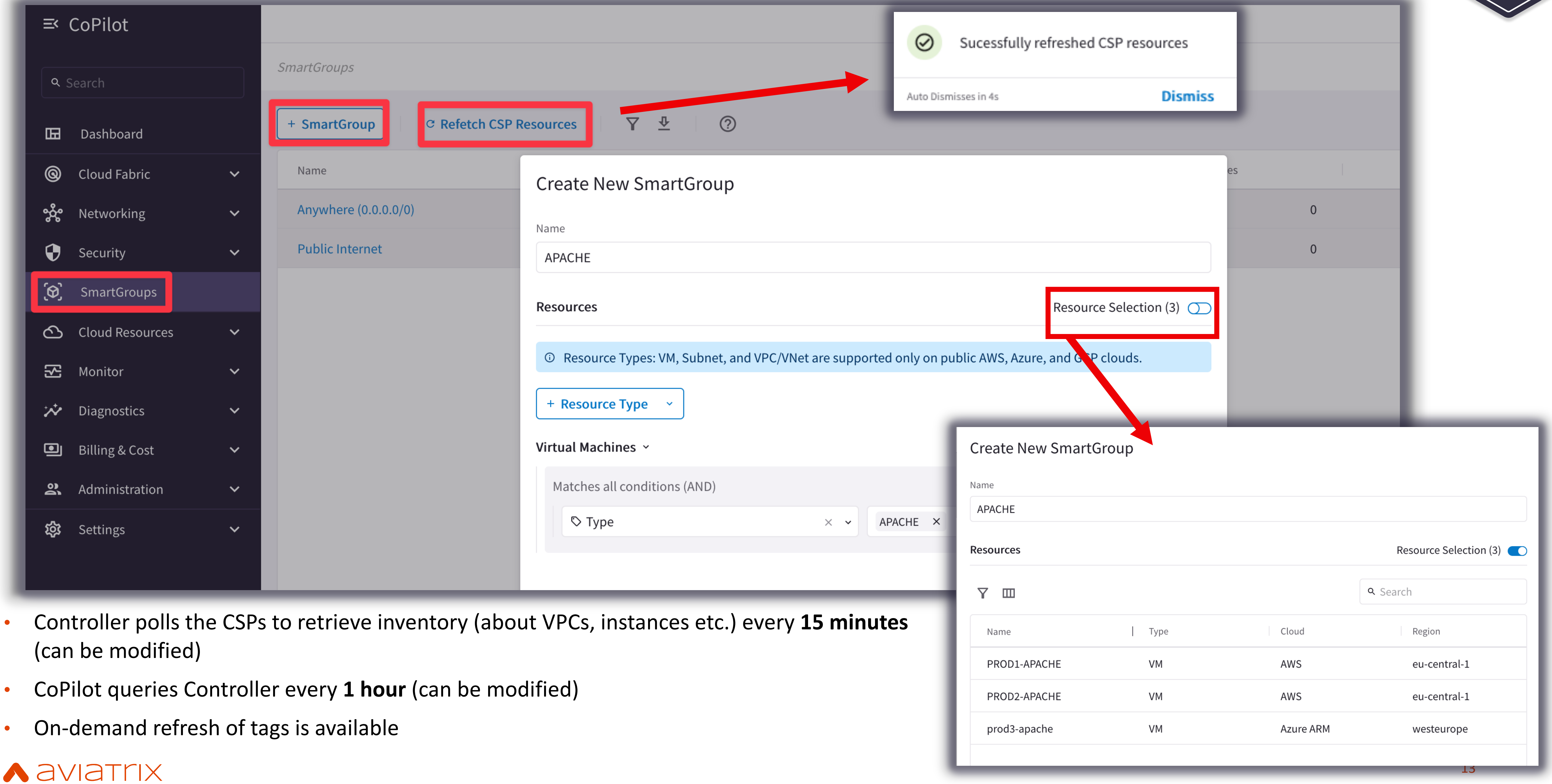
Resource attribute

- Region Name, Account Name

IP Prefixes

- CIDR

SmartGroups Creation



Sucessfully refreshed CSP resources

Auto Dismisses in 4s   Dismiss

Name	es
Anywhere (0.0.0.0/0)	0
Public Internet	0

Create New SmartGroup

Name: APACHE

Resources — Resource Selection (3)

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

Virtual Machines

Matches all conditions (AND)

Type: APACHE

Create New SmartGroup

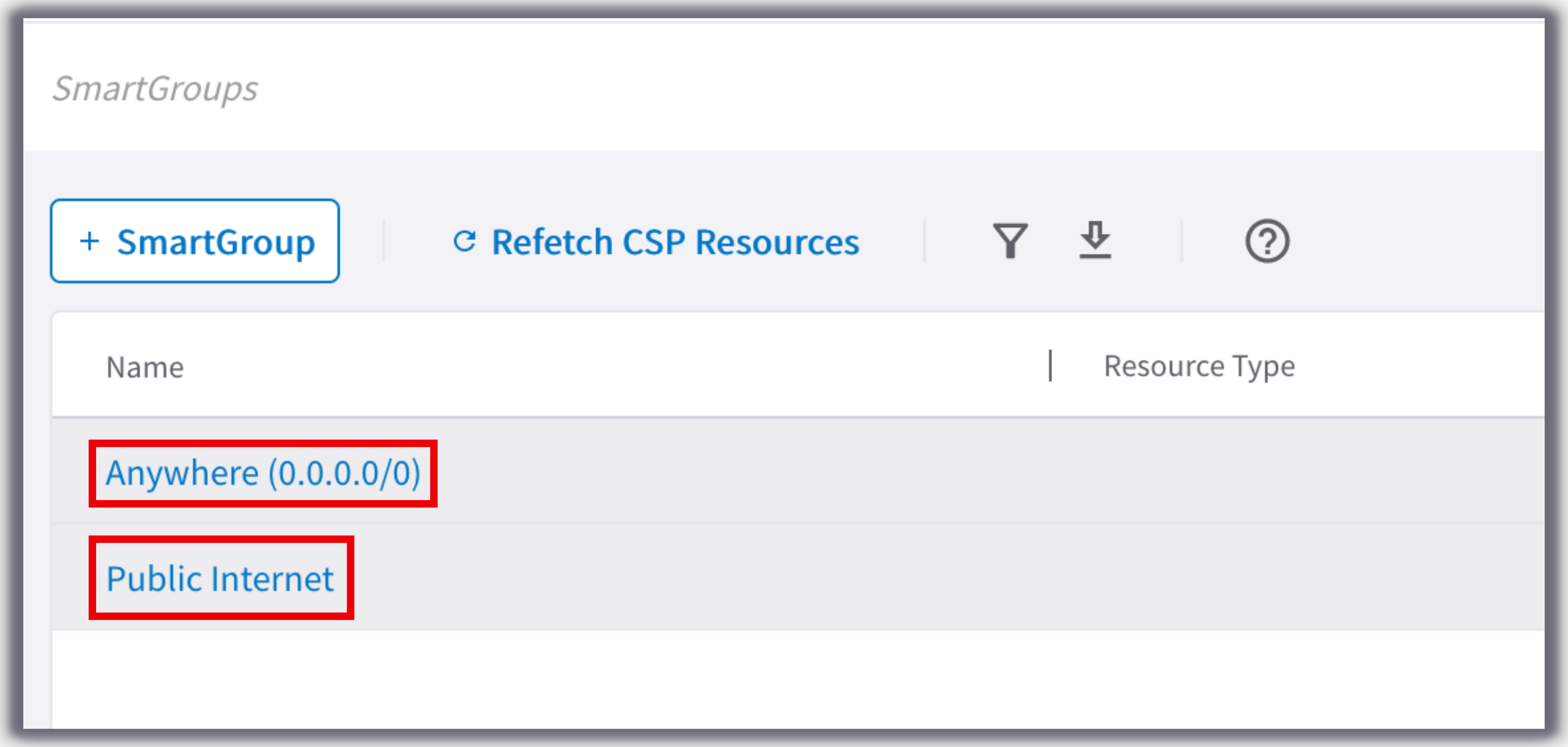
Name: APACHE

Resources — Resource Selection (3)

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 SmartGroups

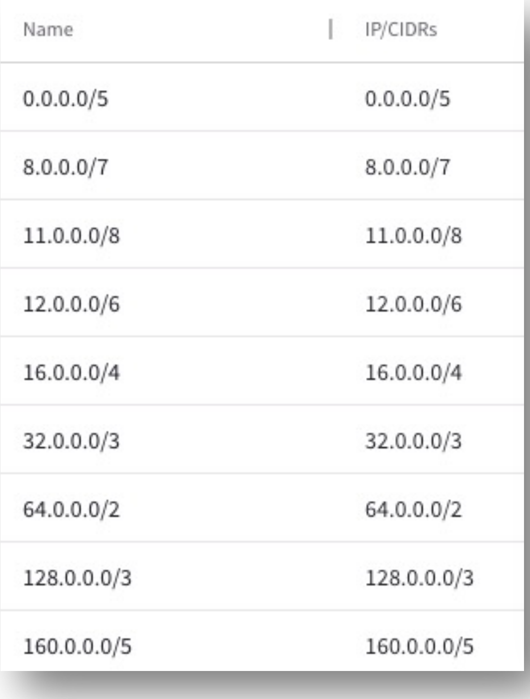
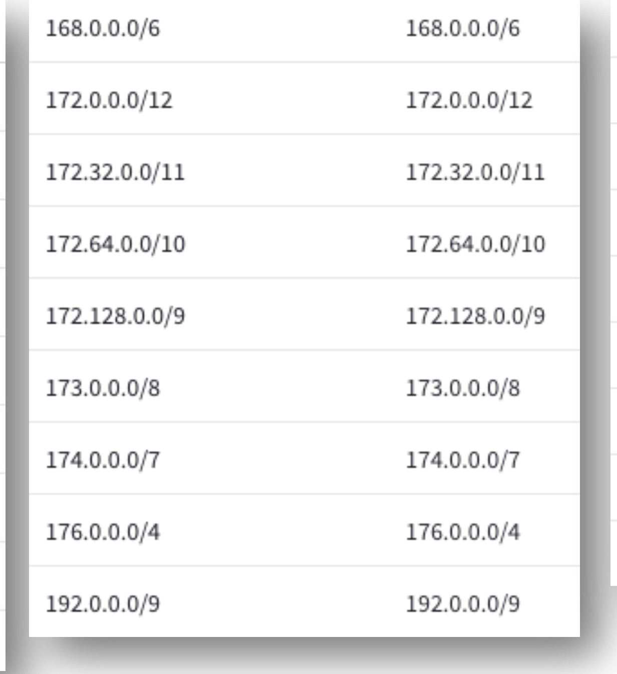
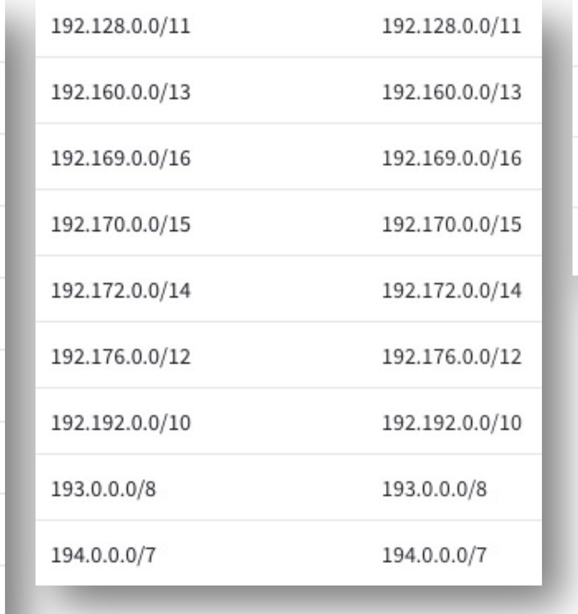
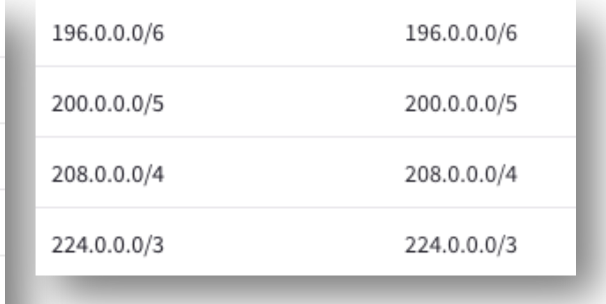


SmartGroups

Name	Resource Type
Anywhere (0.0.0.0/0)	
Public Internet	

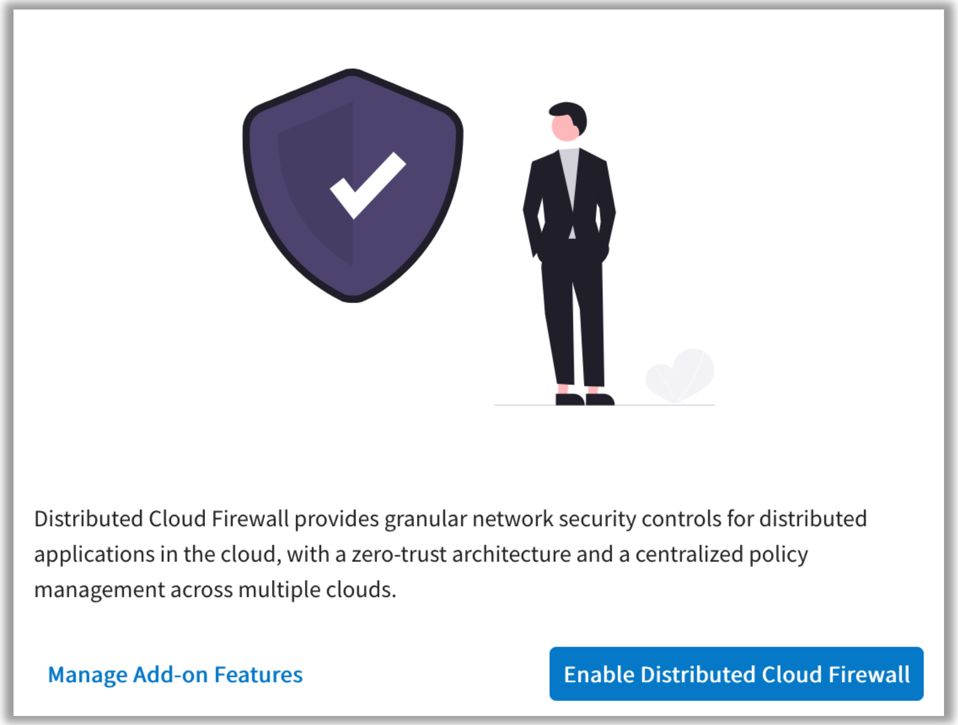
- **Anywhere (0.0.0.0/0)** → 0.0.0.0/0 (Type: CIDR)
- **Public Internet** → 31 Public Internet Summary Routes (Type: CIDR)

“Public Internet Summary” CIDRs

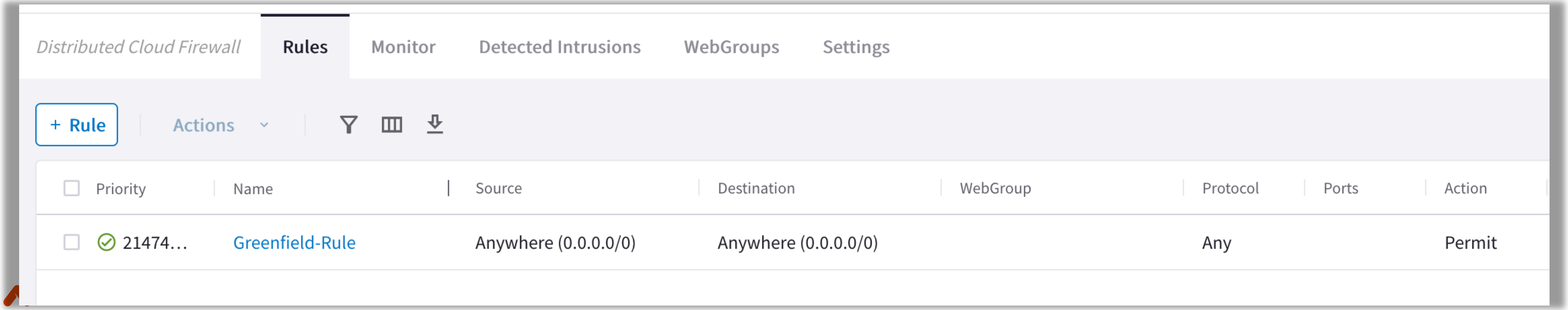
Name	IP/CIDRs
0.0.0.0/5	0.0.0.0/5
8.0.0.0/7	8.0.0.0/7
11.0.0.0/8	11.0.0.0/8
12.0.0.0/6	12.0.0.0/6
16.0.0.0/4	16.0.0.0/4
32.0.0.0/3	32.0.0.0/3
64.0.0.0/2	64.0.0.0/2
128.0.0.0/3	128.0.0.0/3
160.0.0.0/5	160.0.0.0/5
168.0.0.0/6	168.0.0.0/6
172.0.0.0/12	172.0.0.0/12
172.32.0.0/11	172.32.0.0/11
172.64.0.0/10	172.64.0.0/10
172.128.0.0/9	172.128.0.0/9
173.0.0.0/8	173.0.0.0/8
174.0.0.0/7	174.0.0.0/7
176.0.0.0/4	176.0.0.0/4
192.0.0.0/9	192.0.0.0/9
192.128.0.0/11	192.128.0.0/11
192.160.0.0/13	192.160.0.0/13
192.169.0.0/16	192.169.0.0/16
192.170.0.0/15	192.170.0.0/15
192.172.0.0/14	192.172.0.0/14
192.176.0.0/12	192.176.0.0/12
192.192.0.0/10	192.192.0.0/10
193.0.0.0/8	193.0.0.0/8
194.0.0.0/7	194.0.0.0/7
196.0.0.0/6	196.0.0.0/6
200.0.0.0/5	200.0.0.0/5
208.0.0.0/4	208.0.0.0/4
224.0.0.0/3	224.0.0.0/3

Enabling Distributed Cloud Firewall



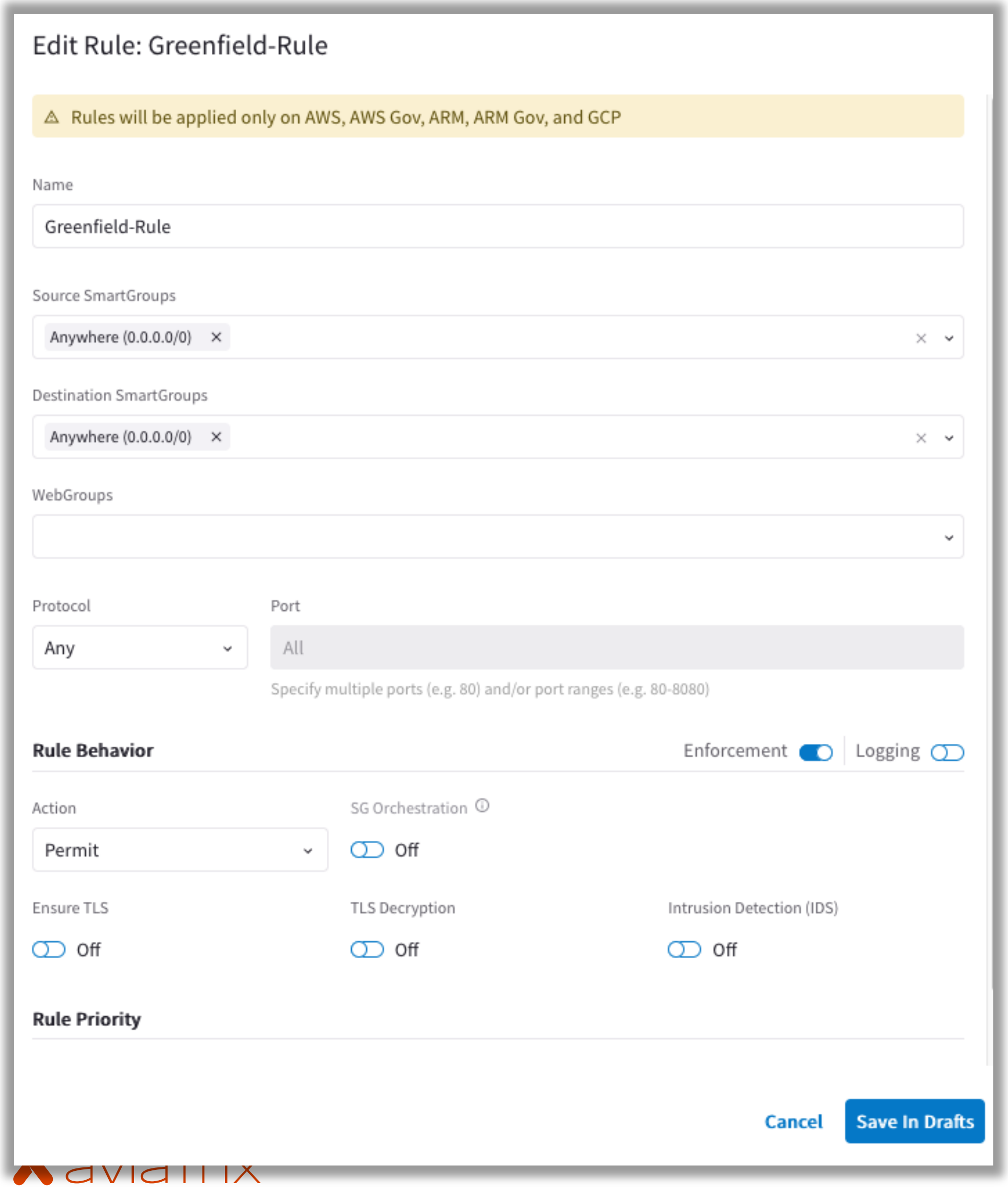
Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

- 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.



☐	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
☐	✓ 21474…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit

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)

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: On · Logging: Off

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

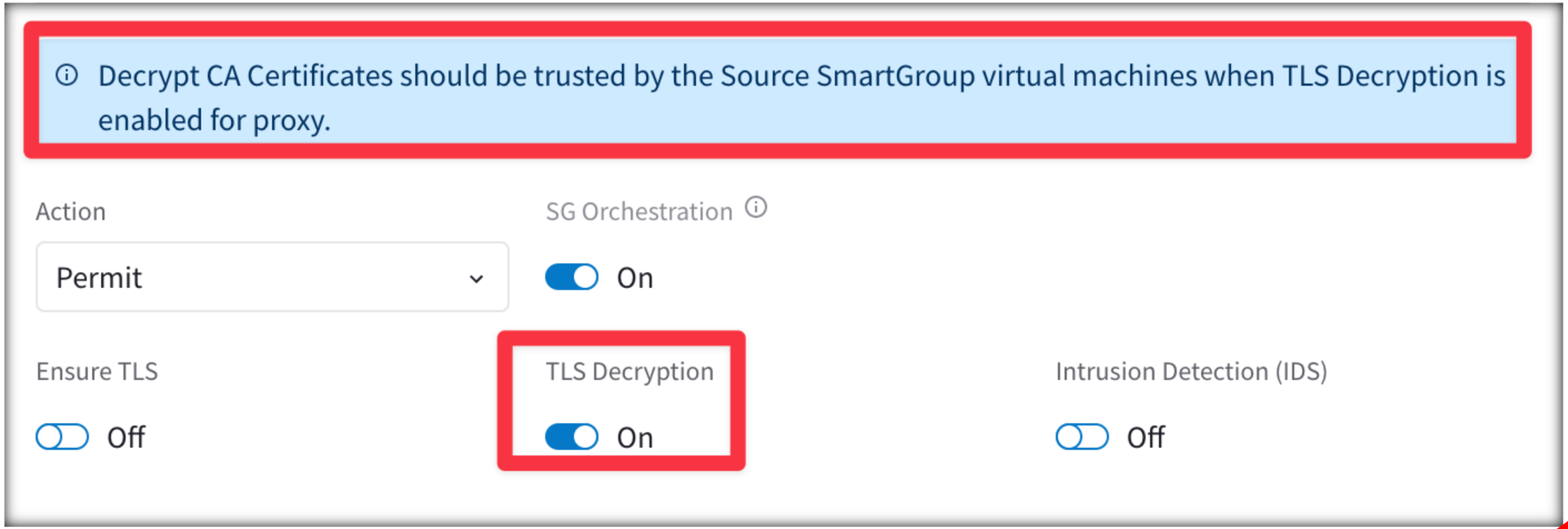
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

- **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



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

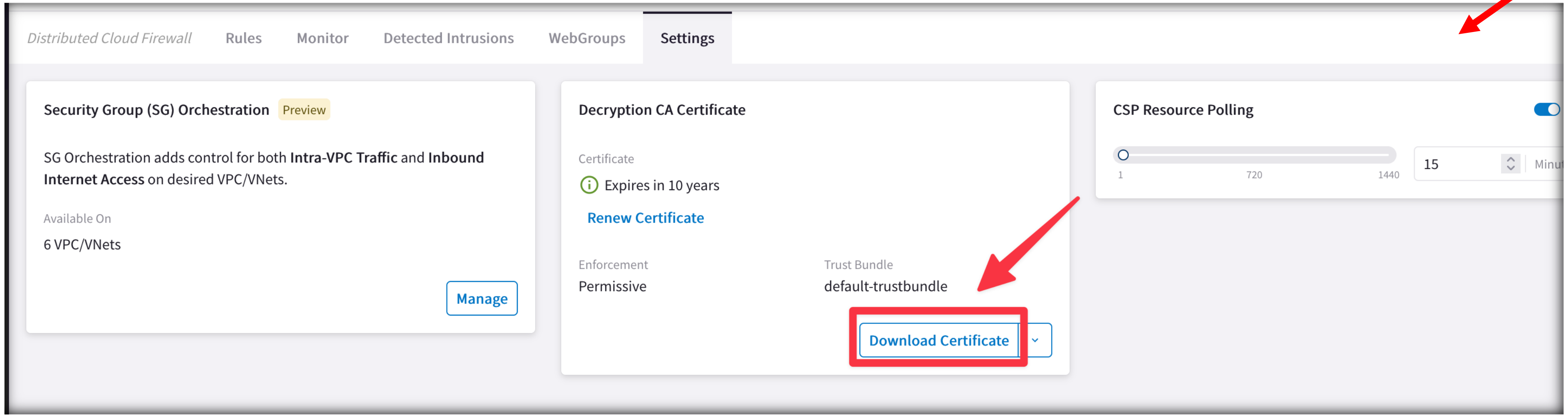
Action: Permit

SG Orchestration ⓘ: On

Ensure TLS: Off

TLS Decryption: On

Intrusion Detection (IDS): Off



Security Group (SG) Orchestration Preview

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

Available On: 6 VPC/VNets

Decryption CA Certificate

Certificate: ⓘ Expires in 10 years

Enforcement: Permissive

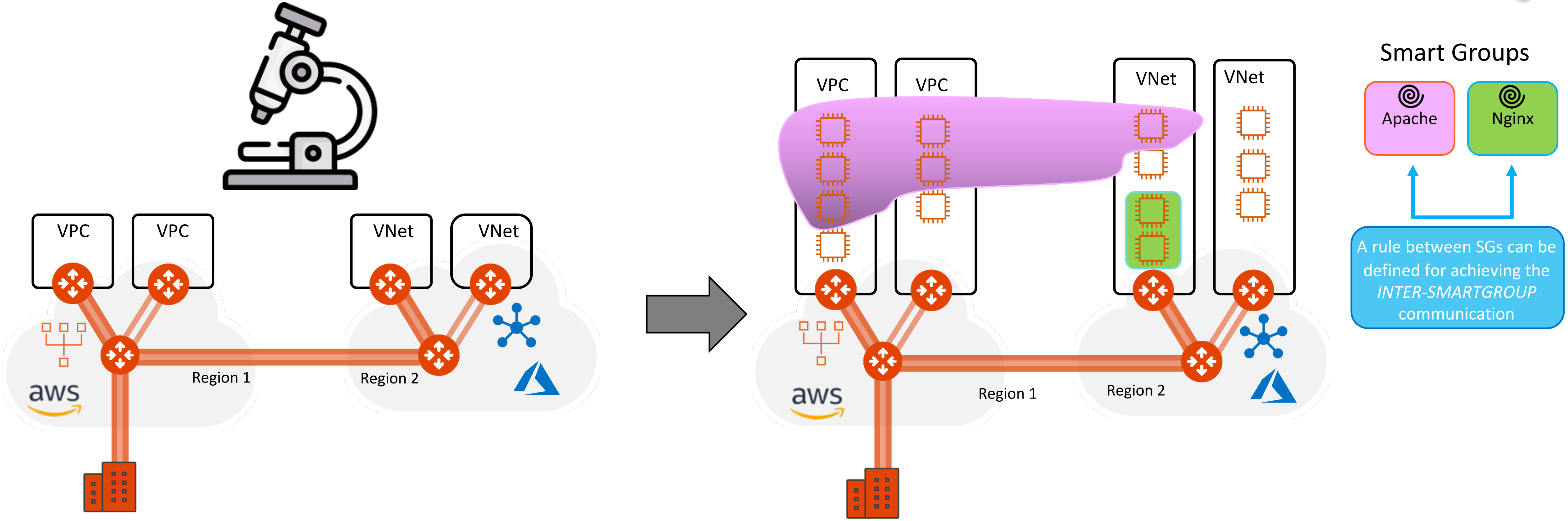
Trust Bundle: default-trustbundle

CSP Resource Polling

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

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

Distributed Cloud Firewall Rule Types: Intra-rule vs. Inter-rule

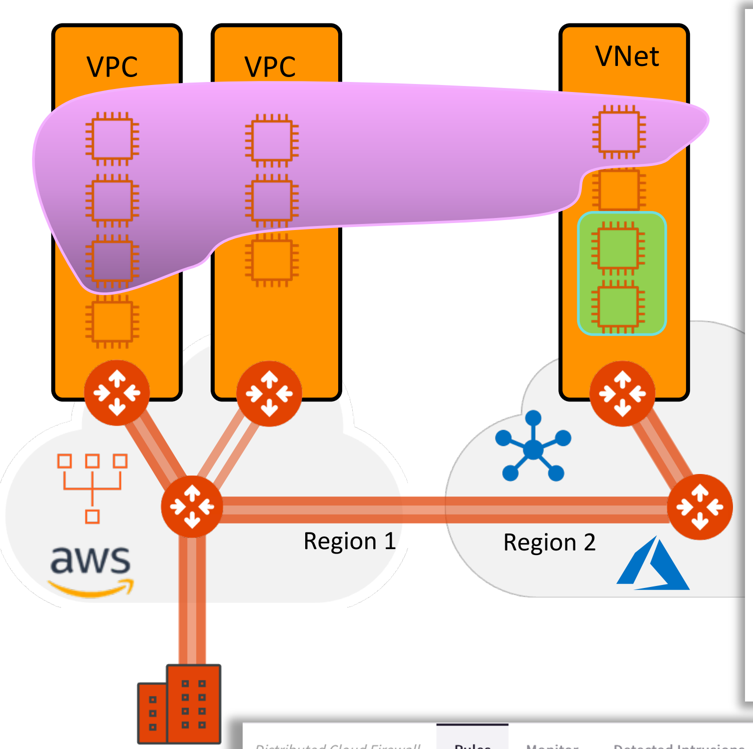


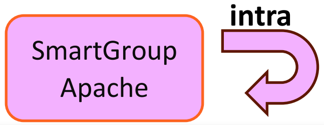
A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

- **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

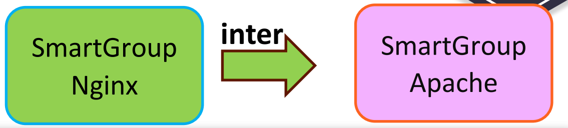
- **INTER-RULE:** is defined among Smart Groups, for dictating what kind of traffic is allowed/prohibited among two or more Smart Groups.

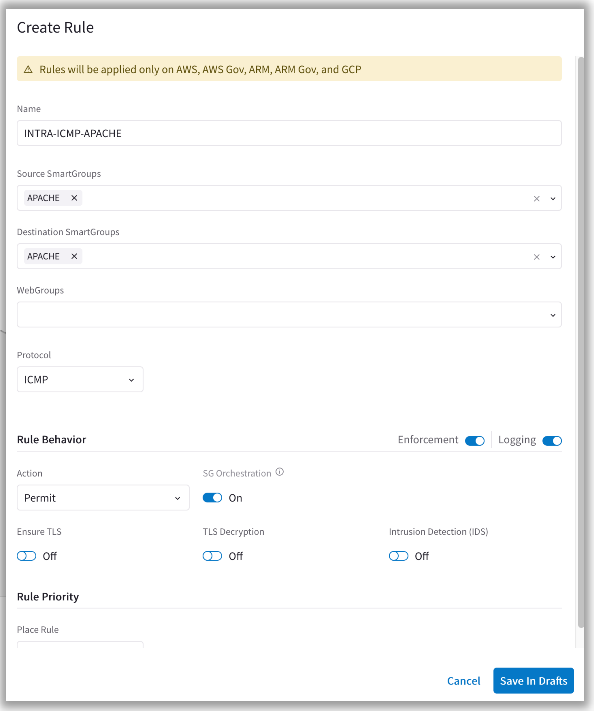
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules





SmartGroup Nginx
intra





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 ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement: On — Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

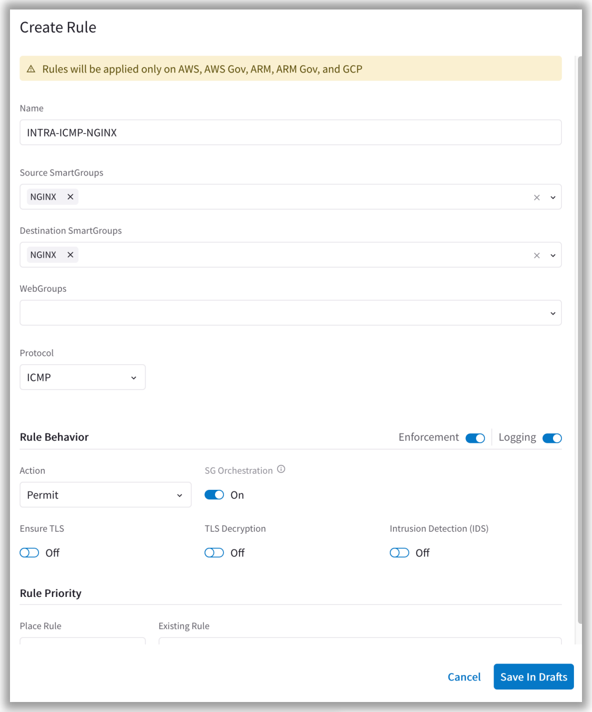
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

Cancel | Save In Drafts



Create Rule

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

Name: INTRA-ICMP-NGINX

Source SmartGroups: NGINX ×

Destination SmartGroups: NGINX ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement: On — Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

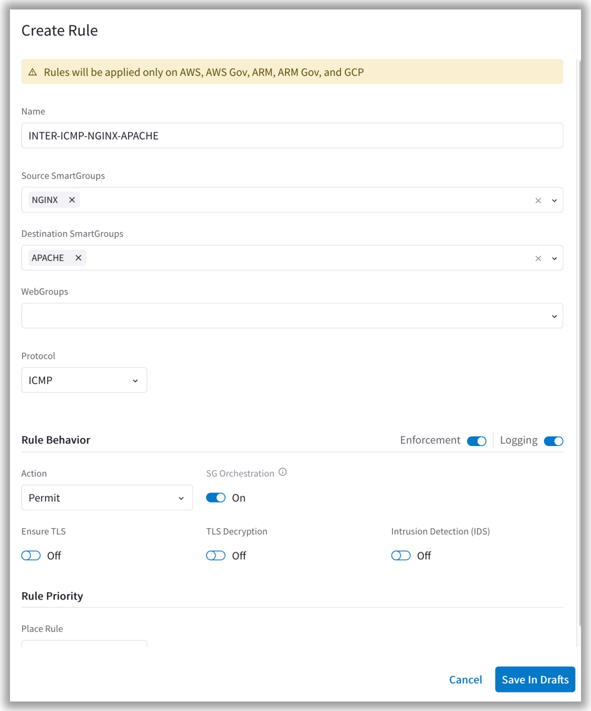
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule | Existing Rule

Cancel | Save In Drafts



Create Rule

⚠ 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 ×

WebGroups:

Protocol: ICMP

Rule Behavior — Enforcement: On — Logging: On

Action: Permit

SG Orchestration: On

Ensure TLS: Off

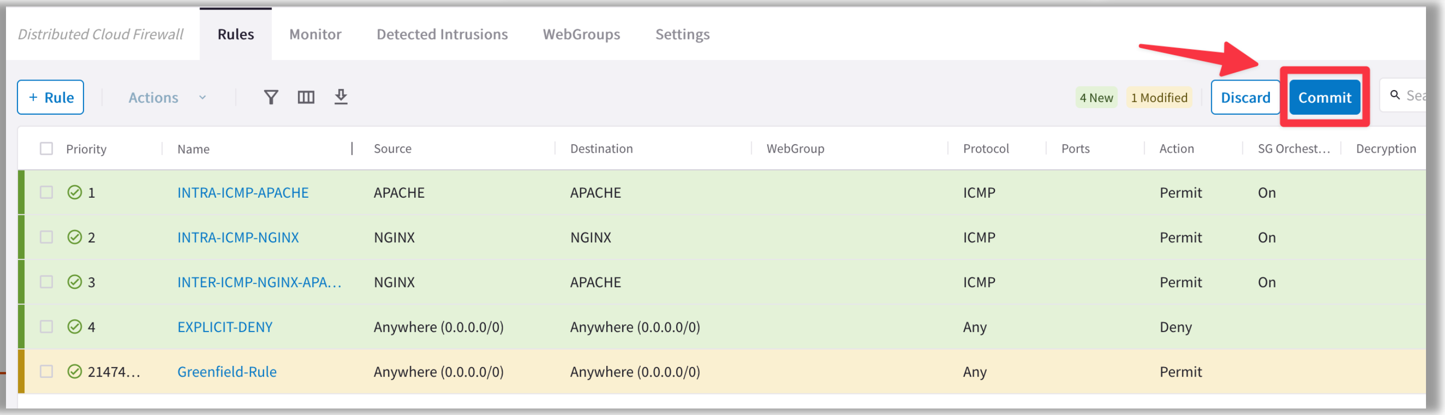
TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

Place Rule

Cancel | Save In Drafts



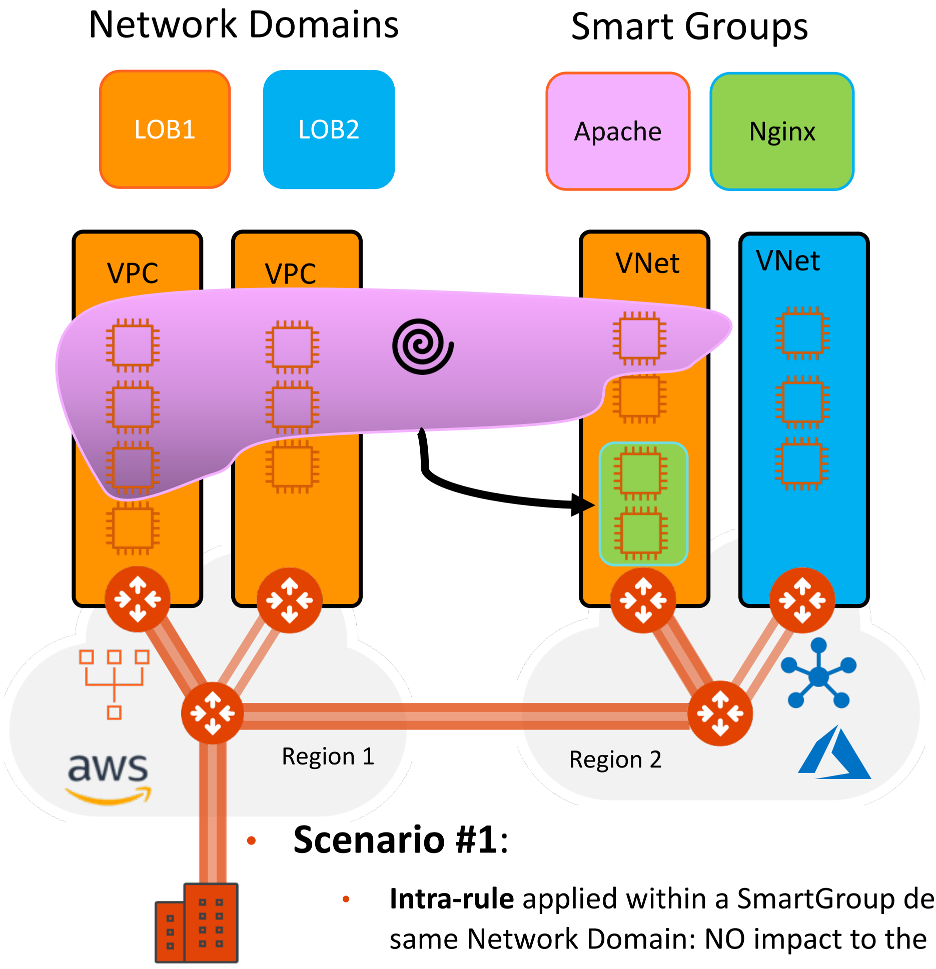
Distributed Cloud Firewall | Rules | Monitor | Detected Intrusions | WebGroups | Settings

+ Rule | Actions | 4 New | 1 Modified | Discard | Commit | Sea

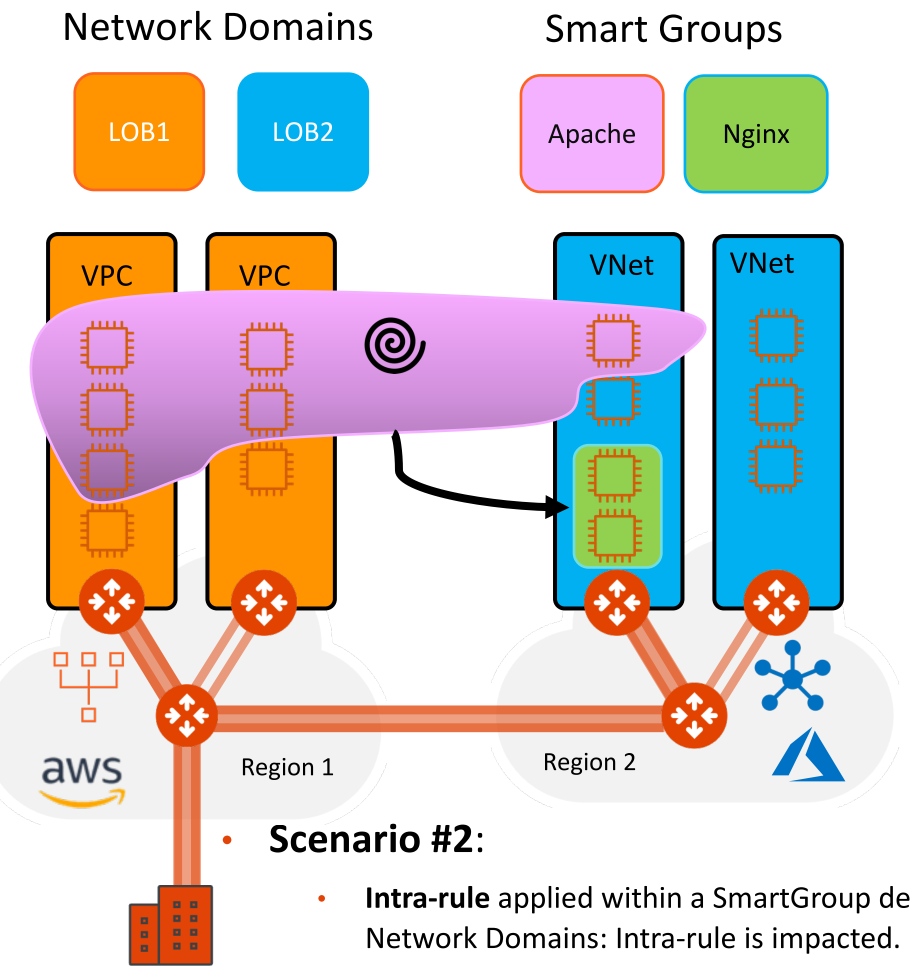
□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchest…	Decryption
□	✓ 1	INTRA-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
□	✓ 2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
□	✓ 3	INTER-ICMP-NGINX-APA…	NGINX	APACHE		ICMP		Permit	On	
□	✓ 4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere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

- **Micro-Segmentation**: 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

Network Segmentation & Distributed Cloud Firewall Rule together



NO connection policy is applied



- **Scenario #1**:
  - **Intra-rule** applied within a SmartGroup defined within the same Network Domain: NO impact to the rule
  - **Inter-rule** applied between SmartGroups defined within the same Network Domains: NO impact to the rule

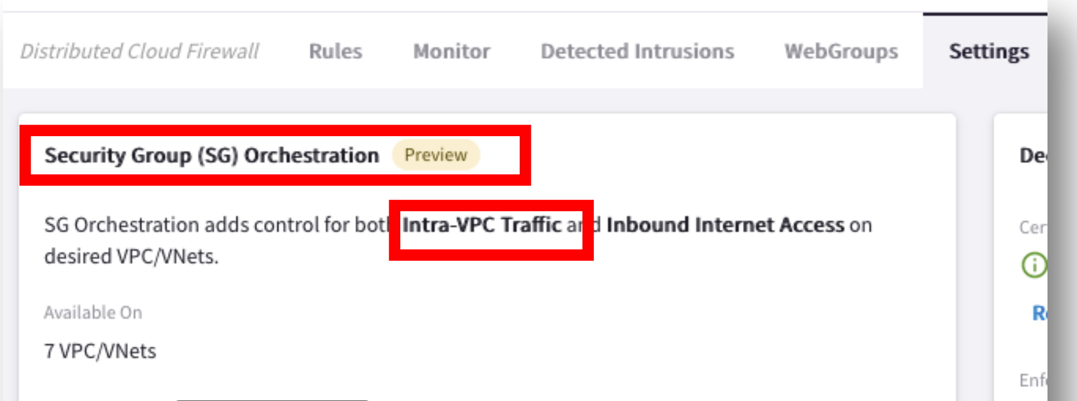
- **Scenario #2**:
  - **Intra-rule** applied within a SmartGroup defined across two Network Domains: Intra-rule is impacted.
  - **Inter-rule** is applied between SmartGroups defined across two different Network Domains: Inter-rule is impacted

Caveat:

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

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

❑ Enable the feature on the relevant VPC/VNet



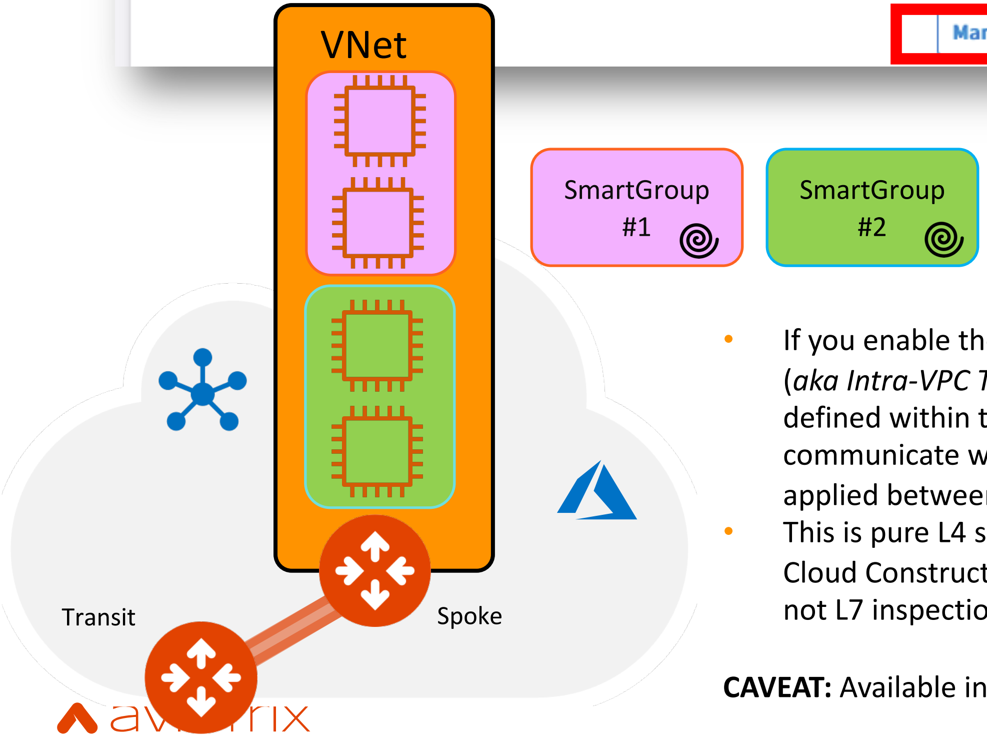
Security Group (SG) Orchestration Preview

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

Available On

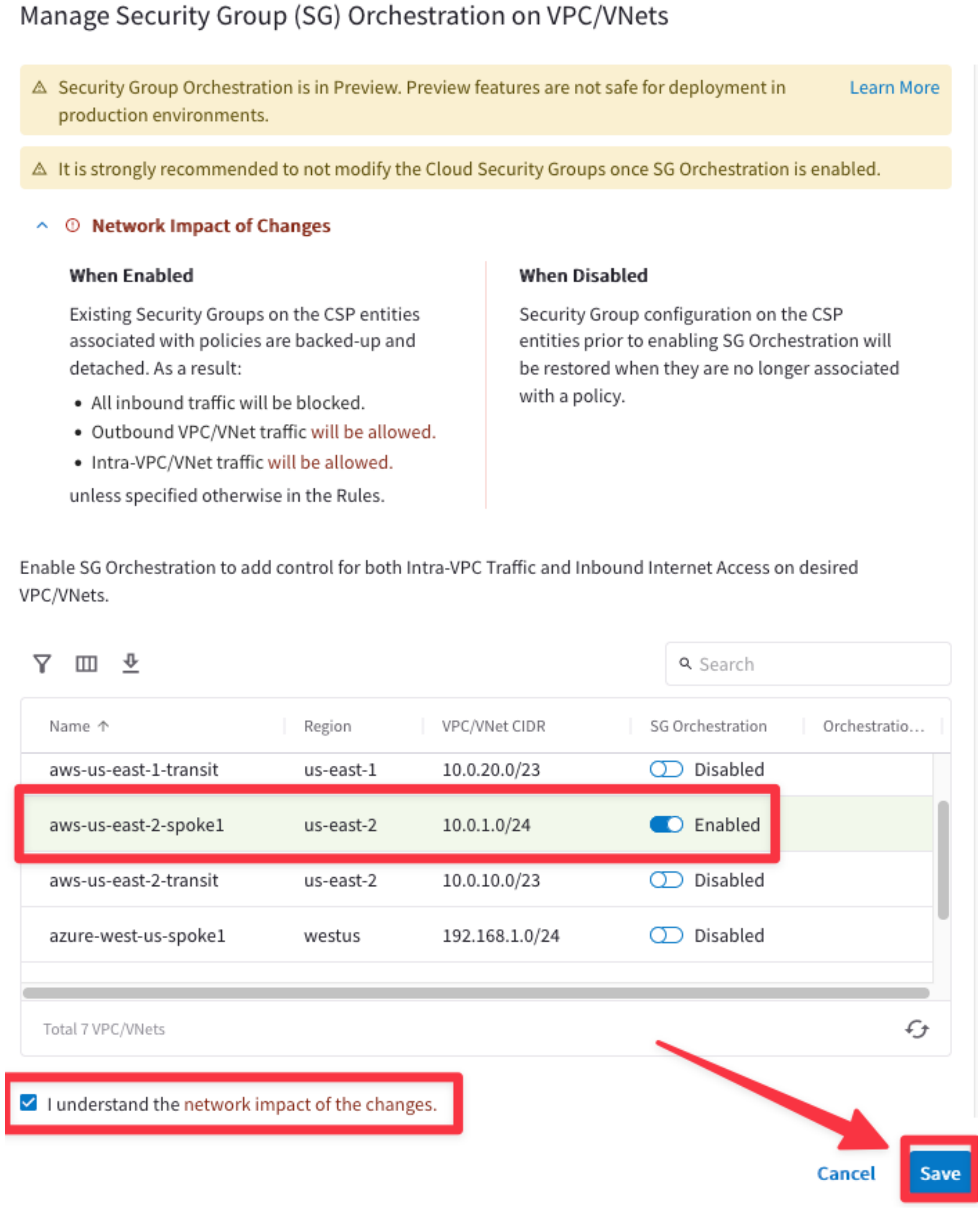
7 VPC/VNets

Manage



- 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 Security Group (SG) Orchestration on VPC/VNets

⚠ Security Group Orchestration is in Preview. Preview features are not safe for deployment in production environments. Learn More

⚠ It is strongly recommended to not modify the Cloud Security Groups once SG Orchestration is enabled.

ⓘ **Network Impact of Changes**

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.
- Outbound VPC/VNet traffic will be allowed.
- Intra-VPC/VNet traffic will be allowed.

unless specified otherwise in the Rules.

When Disabled

Security Group configuration on the CSP entities prior to enabling SG Orchestration will be restored when they are no longer associated with a policy.

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

Search

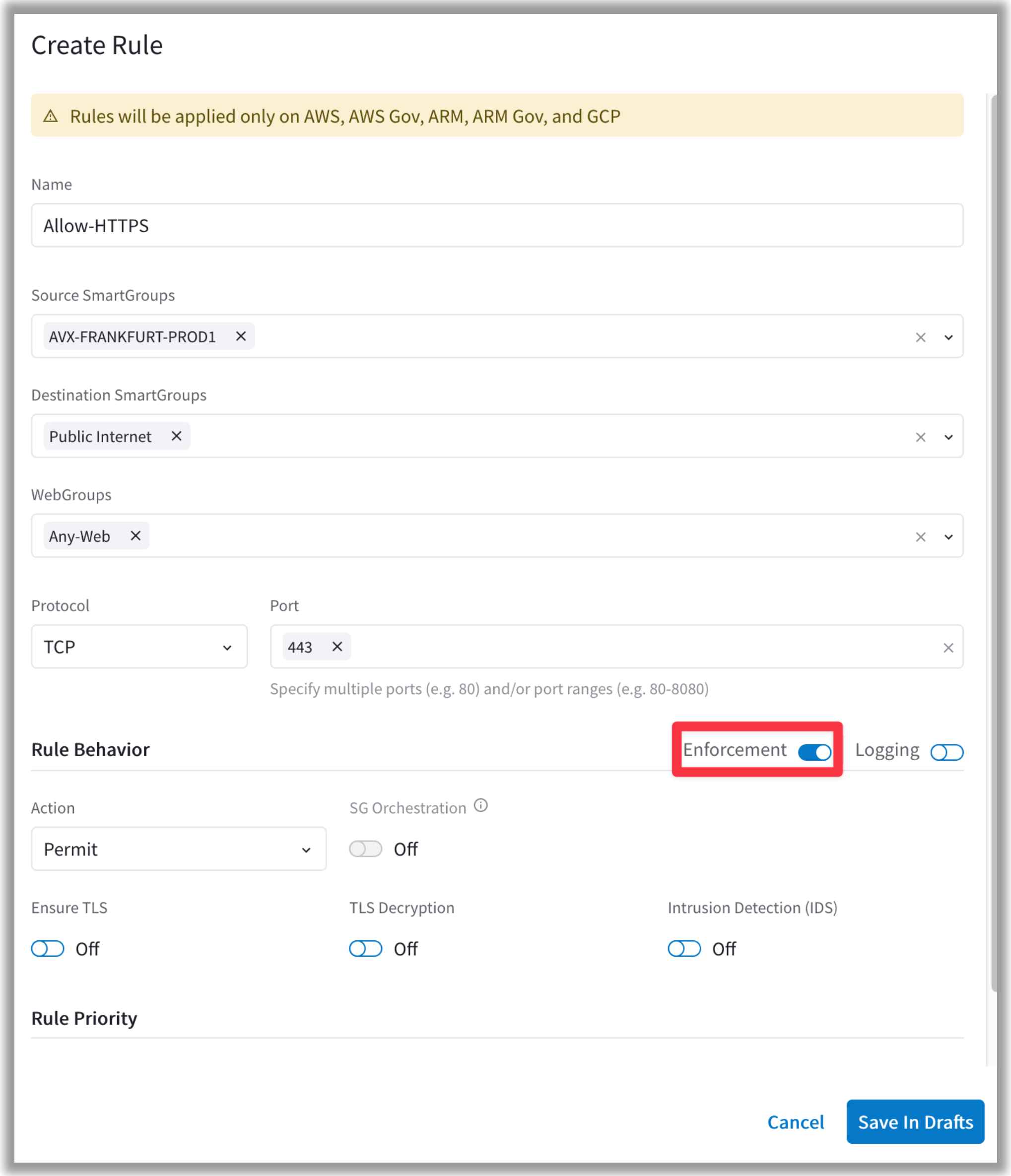
Name ↑	Region	VPC/VNet CIDR	SG Orchestration	Orchestratio...
aws-us-east-1-transit	us-east-1	10.0.20.0/23	○ Disabled	
aws-us-east-2-spoke1	us-east-2	10.0.1.0/24	● Enabled	
aws-us-east-2-transit	us-east-2	10.0.10.0/23	○ Disabled	
azure-west-us-spoke1	westus	192.168.1.0/24	○ Disabled	

Total 7 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: On

Logging: Off

Action: Permit

SG Orchestration: Off

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority

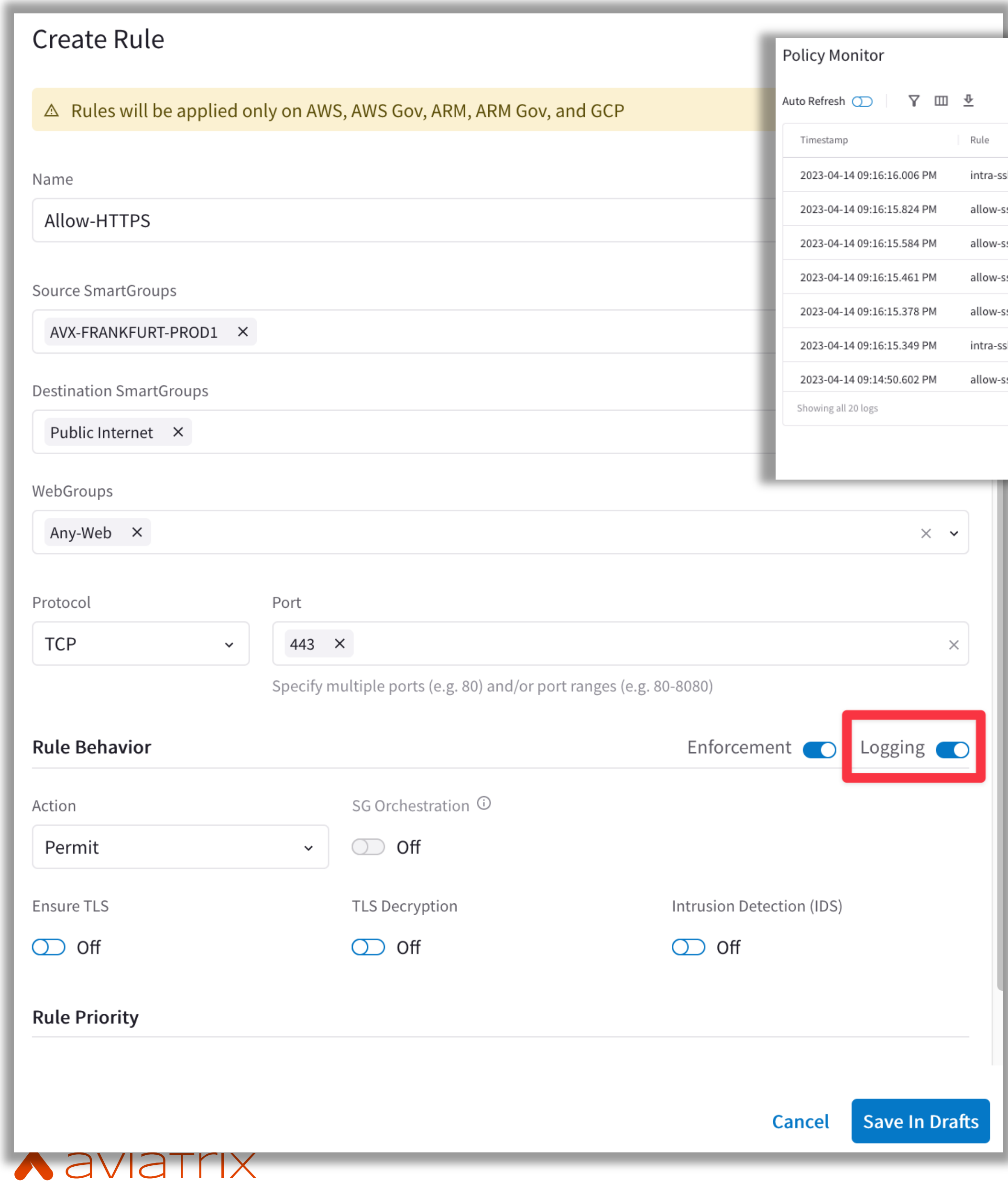
❑ Enforcement ON

- 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

Enforcement: On

Logging: On

Action: Permit

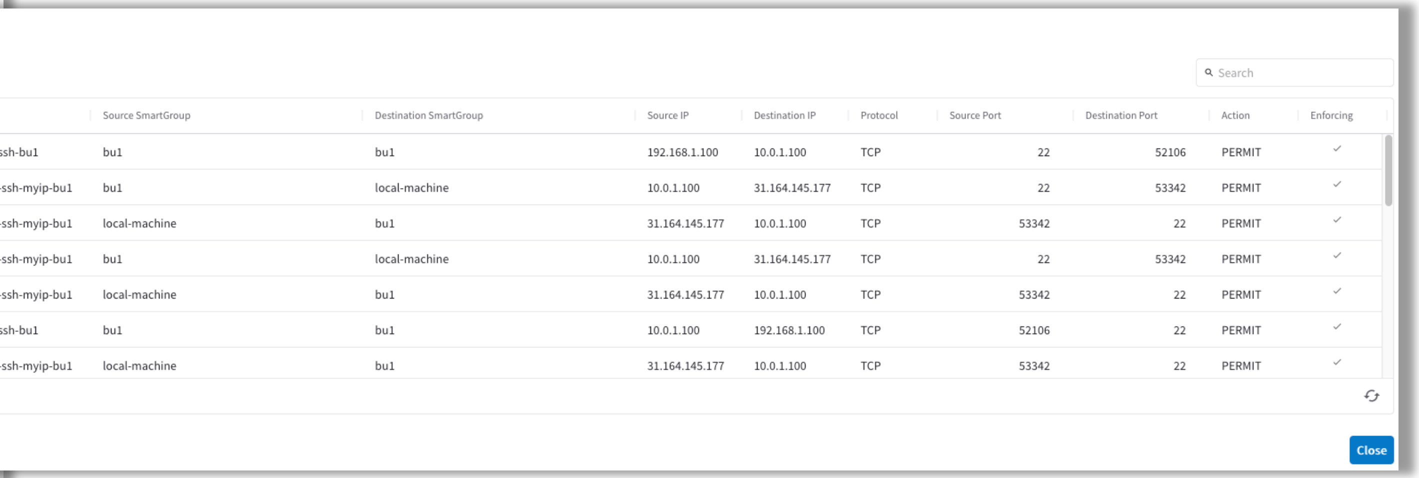
SG Orchestration: Off

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority



Policy Monitor

Auto Refresh: Off

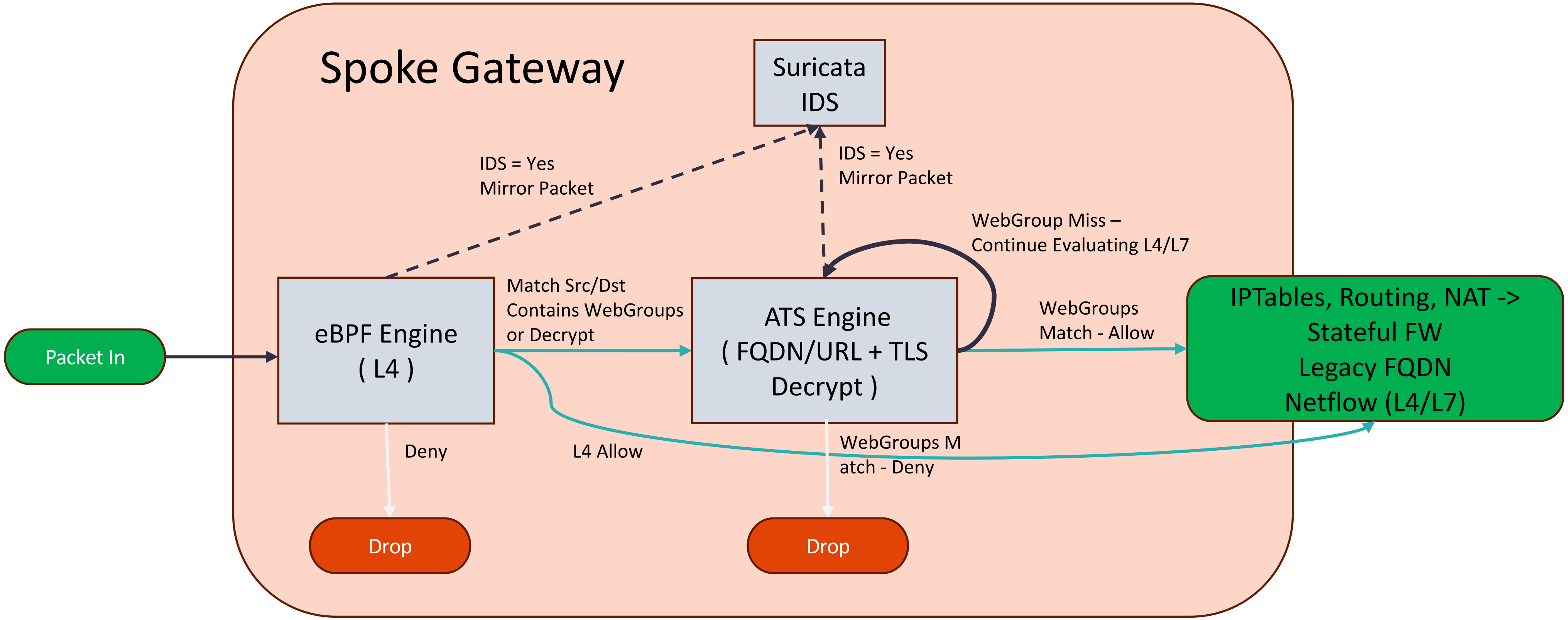
Timestamp	Rule	Source SmartGroup	Destination SmartGroup	Source IP	Destination IP	Protocol	Source Port	Destination Port	Action	Enforcing
2023-04-14 09:16:16.006 PM	intra-ssh-bu1	bu1	bu1	192.168.1.100	10.0.1.100	TCP	22	52106	PERMIT	✓
2023-04-14 09:16:15.824 PM	allow-ssh-myip-bu1	bu1	local-machine	10.0.1.100	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

- **Logging can be turned ON/OFF per rule**
- **Configure Syslog to view the logs**

DFW Engines At-a-Glance

- **eBPF** (extended Berkeley Packet Filter) Engine (L4) → Stateful Firewall Rule (forwarding path)
- WebProxy **ATS** (Apache Traffic Server) Engine (L7) → it is triggered whether WebGroups or TLS Decryption are required
- **Suricata** Engine (DPI) → Signature of the payload (only in IDS mode at the moment)



Supported Capabilities

Capability	6.7	6.8	6.9	7.0	7.1
Distributed Cloud Firewall is supported in the following cloud providers:	AWS, Azure	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP	AWS, AWS GovCloud, Azure, Azure Government, and GCP
You can configure up to 500 SmartGroups	x	x	x	x	x
You can have up to 3000 CIDRs per SmartGroup	x	x	x	x	x
Number of rules per policy	64	2000	2000	2000	2000
Number of port ranges	1	64	64	64	64
Overlapping IPs are supported				x	x
Security Group Orchestration is supported				x (Azure)	x (AWS and Azure)

https://docs.aviatrix.com/documentation/latest/network-security/secure-networking-configuring.html?expand=true#supported-capabilities aviatrix

ACE

Aviatrix Certified Engineer

Next: Lab 10 – Distributed Cloud Firewall