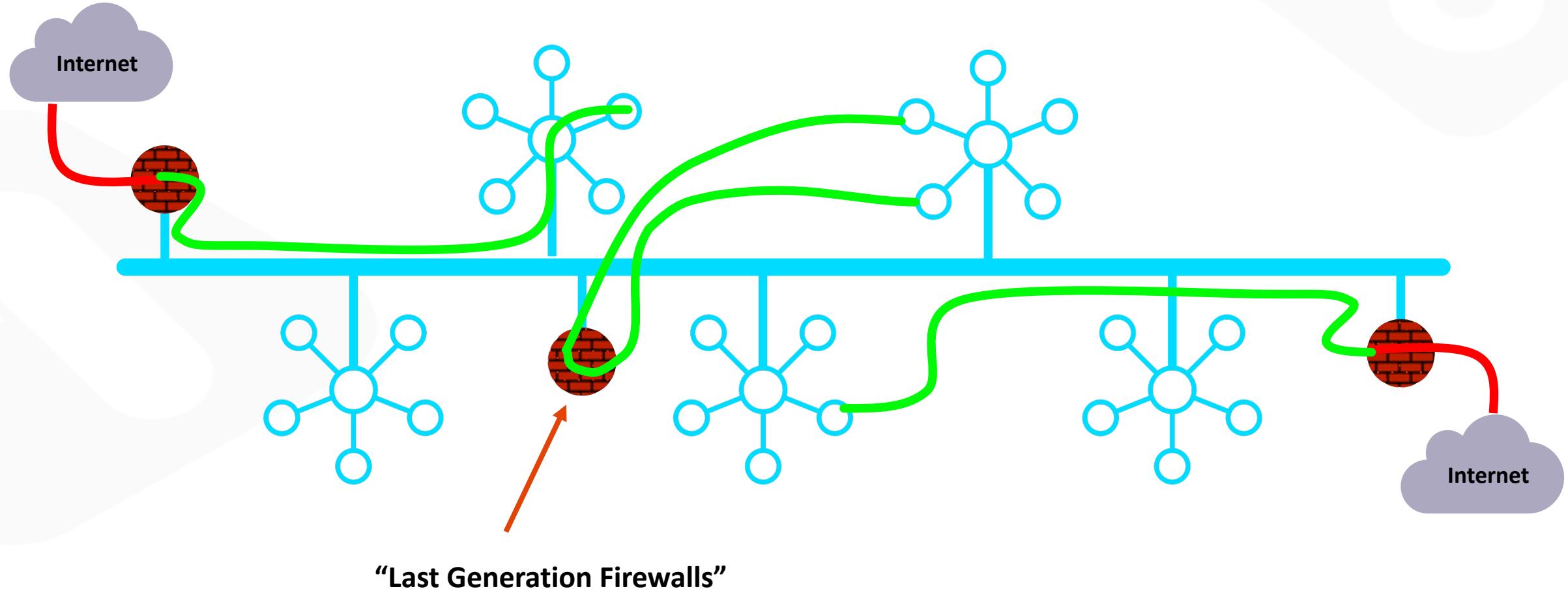


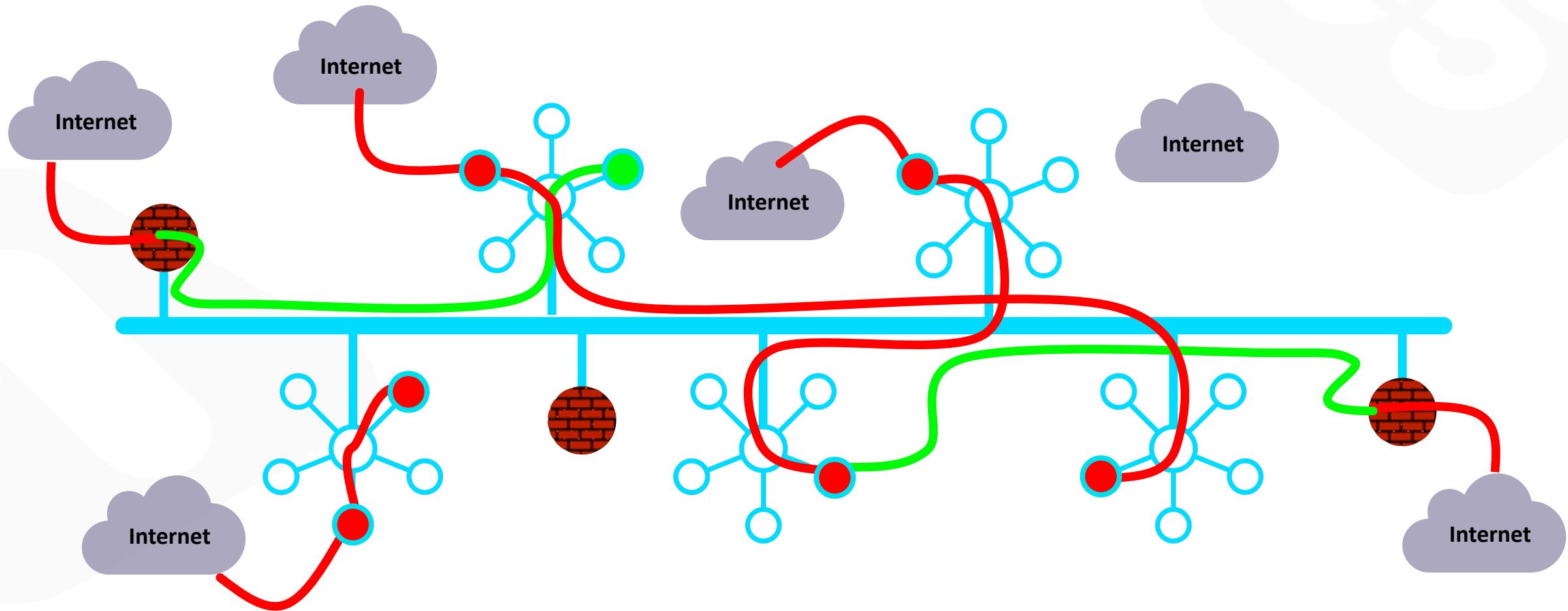


Distributed Cloud Firewall

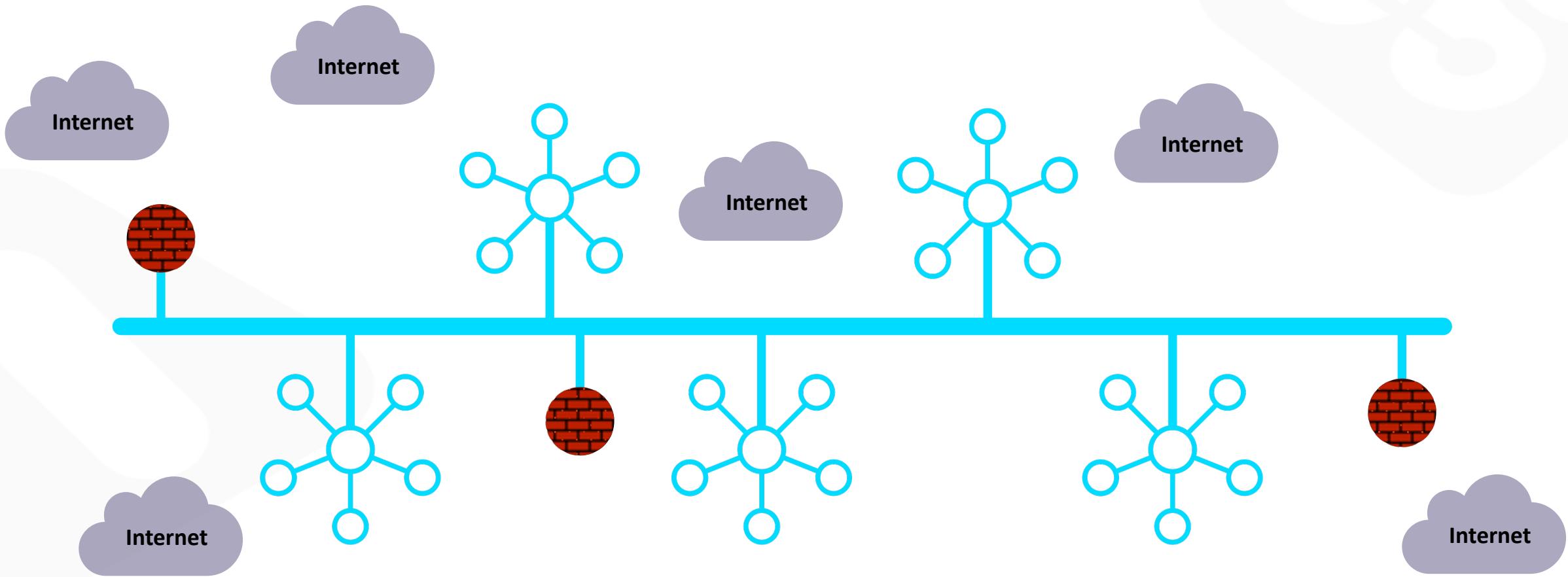
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



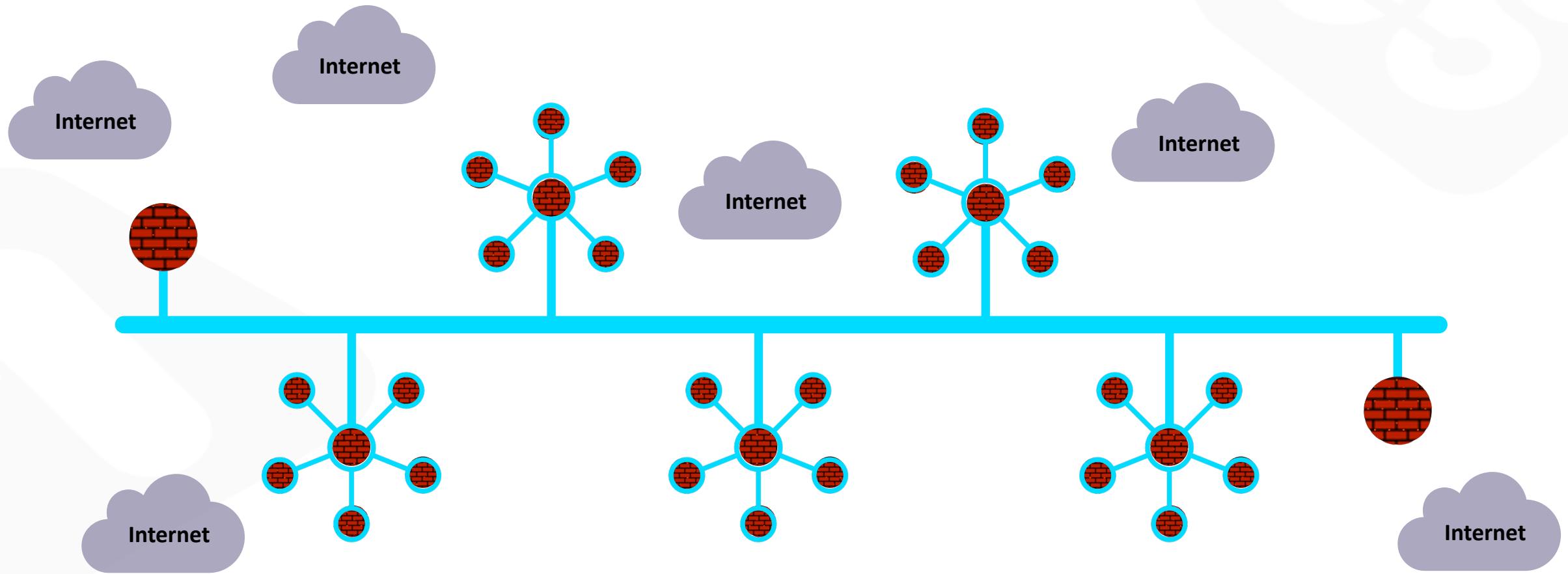
In Reality...



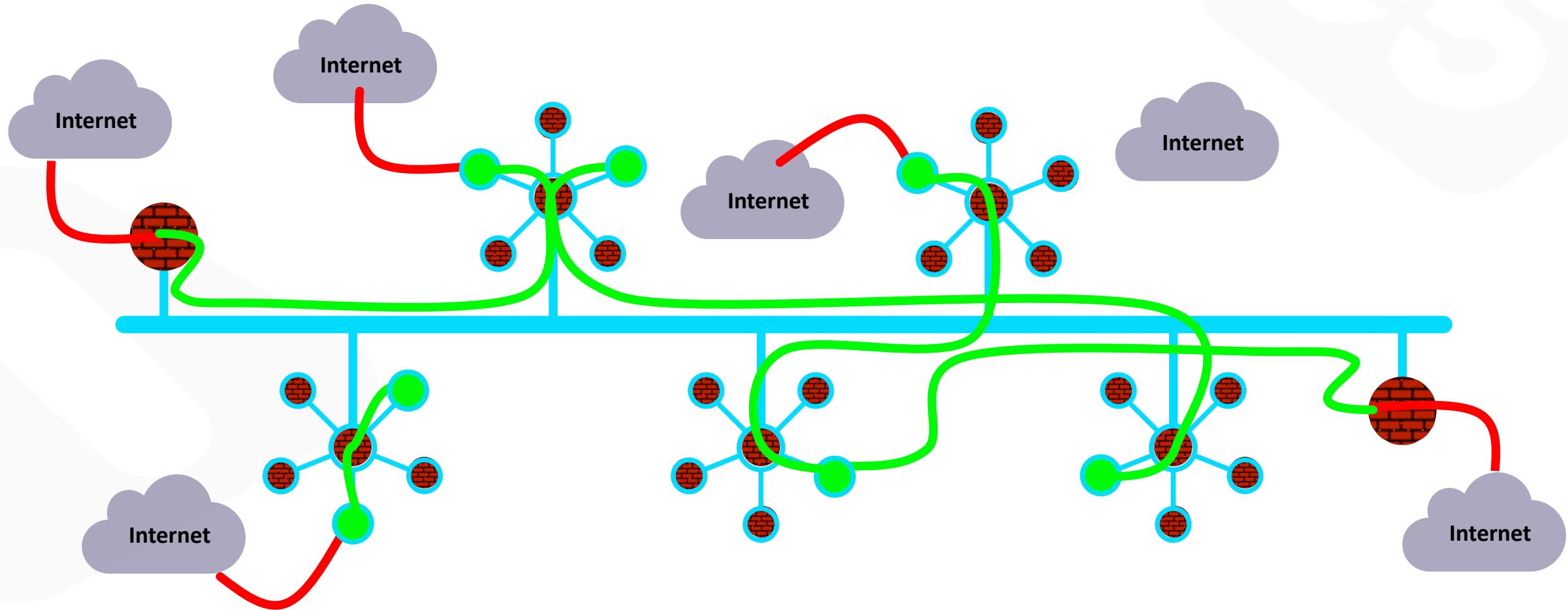
What If... the architecture was built for cloud



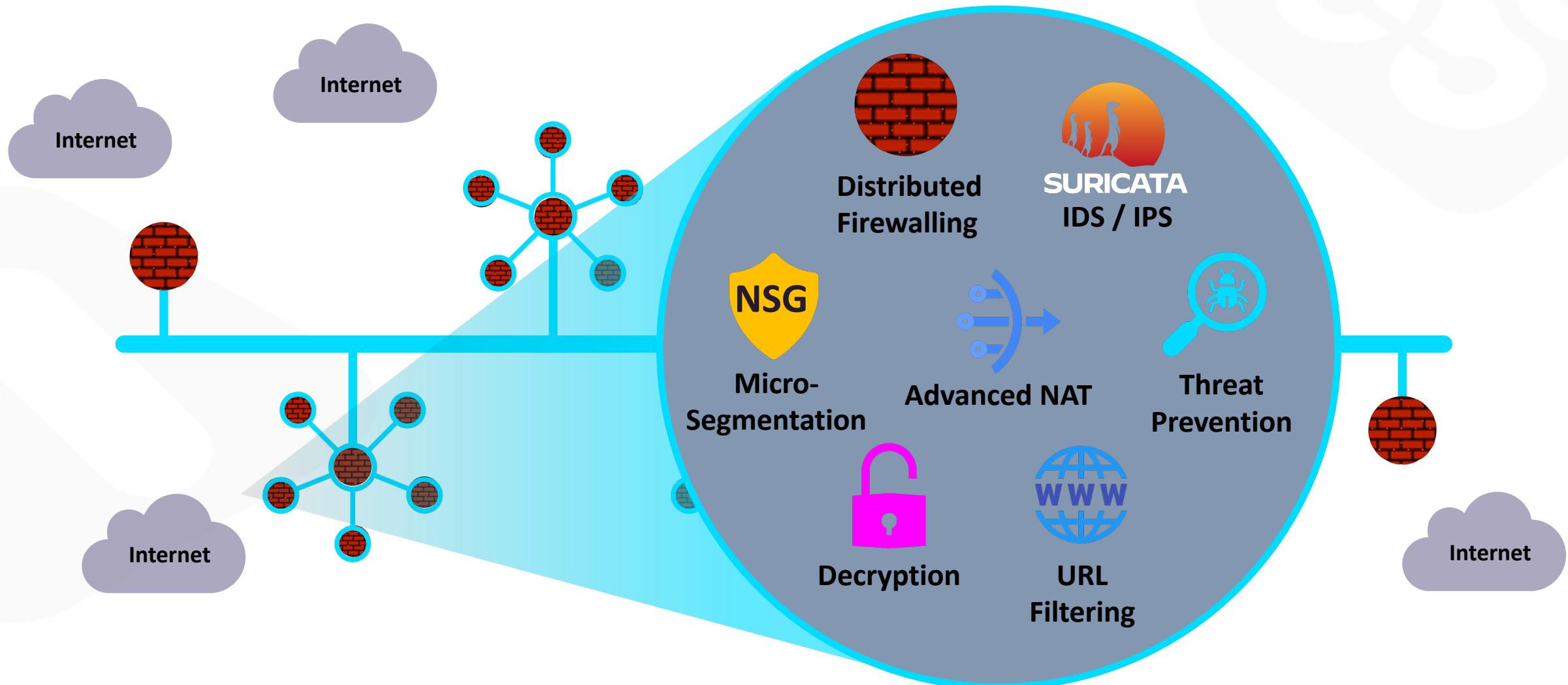
Firewalling Functions were Embedded in the Cloud Network Everywhere...



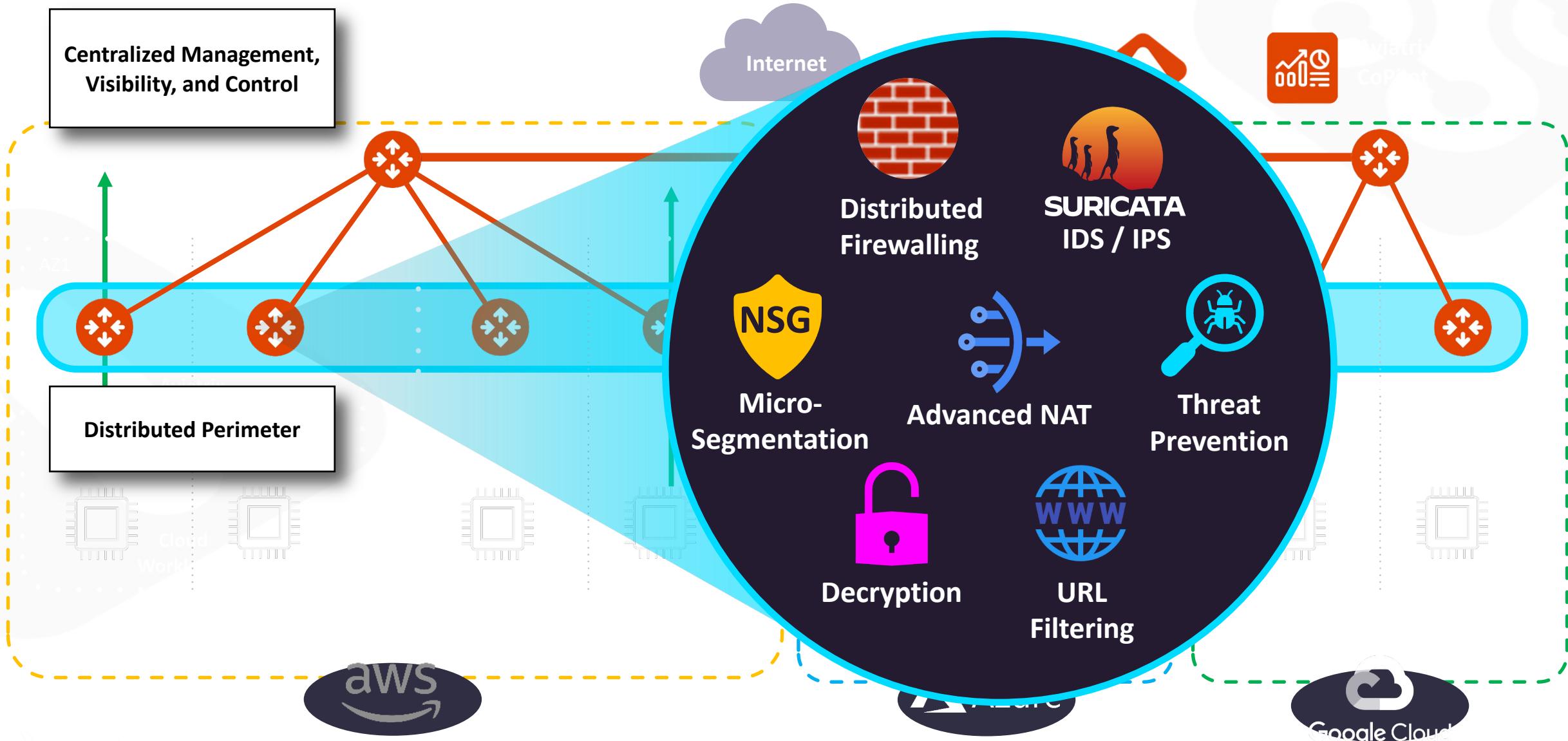
Distribution of the Security Services into the Spokes



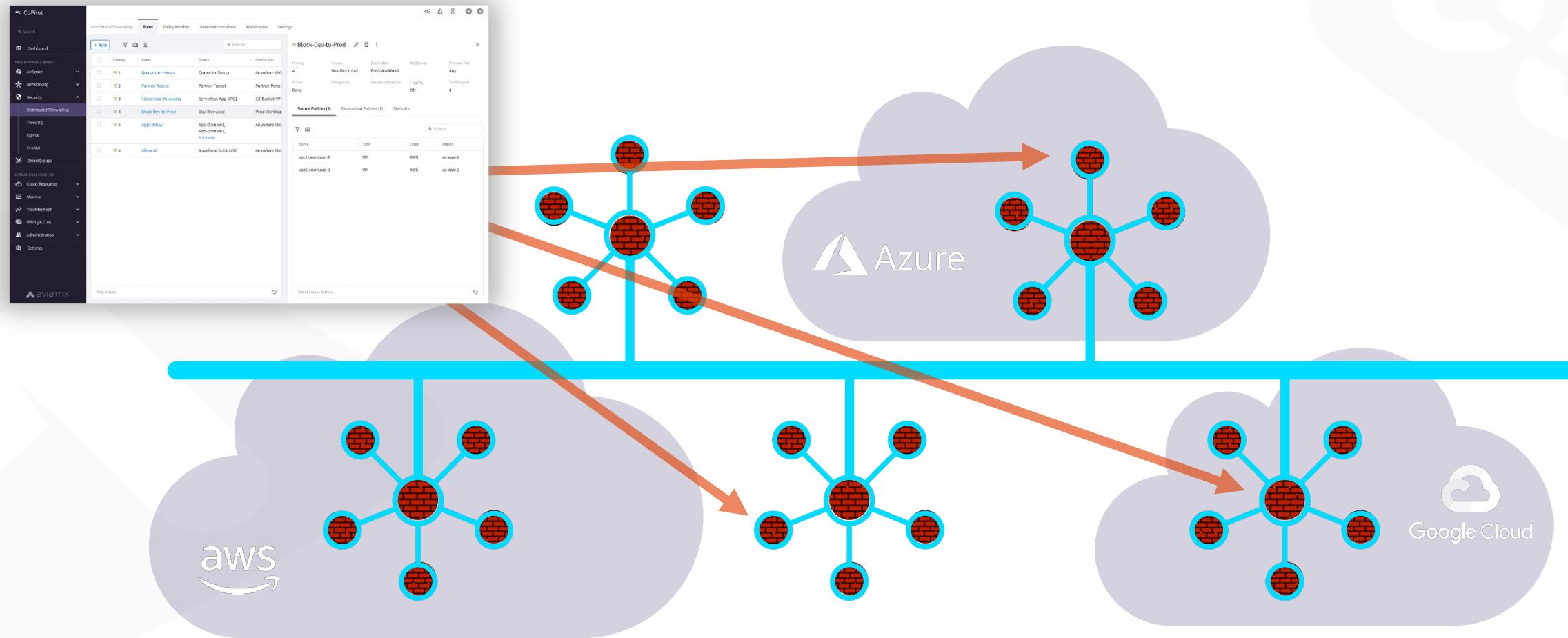
And, What If it was more than just firewalling...



Aviatrix Distributed Cloud Firewall



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



Where and How Policies Are Enforced Is Abstracted...

SmartGroup: 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

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

SmartGroups Creation

The screenshot shows the Aviatrix CoPilot interface. On the left, the navigation bar includes 'CoPilot' and a search bar, followed by a list of categories: Dashboard, Cloud Fabric, Networking, Security, SmartGroups (highlighted with a red box), Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The 'SmartGroups' section contains two buttons: '+ SmartGroup' and 'Refetch CSP Resources' (also highlighted with a red box). A large central window displays the 'Create New SmartGroup' dialog. The 'Name' field is set to 'APACHE'. Under the 'Resources' section, there is a 'Resource Selection (3)' button (also highlighted with a red box). A note below states: 'Resource Types: VM, Subnet, and VPC/VNet are supported only on public AWS, Azure, and GCP clouds.' At the bottom of the dialog, there is a 'Virtual Machines' dropdown set to 'Matches all conditions (AND)' and a 'Type' filter set to 'APACHE'. To the right of the dialog, a success message box says 'Successfully refreshed CSP resources' with a 'Dismiss' button. Below the dialog, a preview window shows the list of selected resources: PROD1-APACHE, PROD2-APACHE, and prod3-apache.

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

The screenshot shows a user interface for managing SmartGroups. At the top, there's a header with the title "SmartGroups". Below the header are several buttons: "+ SmartGroup" (highlighted with a red border), "⟳ Refetch CSP Resources", a refresh icon, a download icon, and a help icon. The main area has two columns: "Name" and "Resource Type". There are two entries listed:

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



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 WebGroups Settings

+ Rule Actions Actions Filter Sort Download

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

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

Action
Permit

SG Orchestration ⓘ
Off

Ensure TLS
Off

TLS Decryption
Off

Intrusion Detection (IDS)
Off

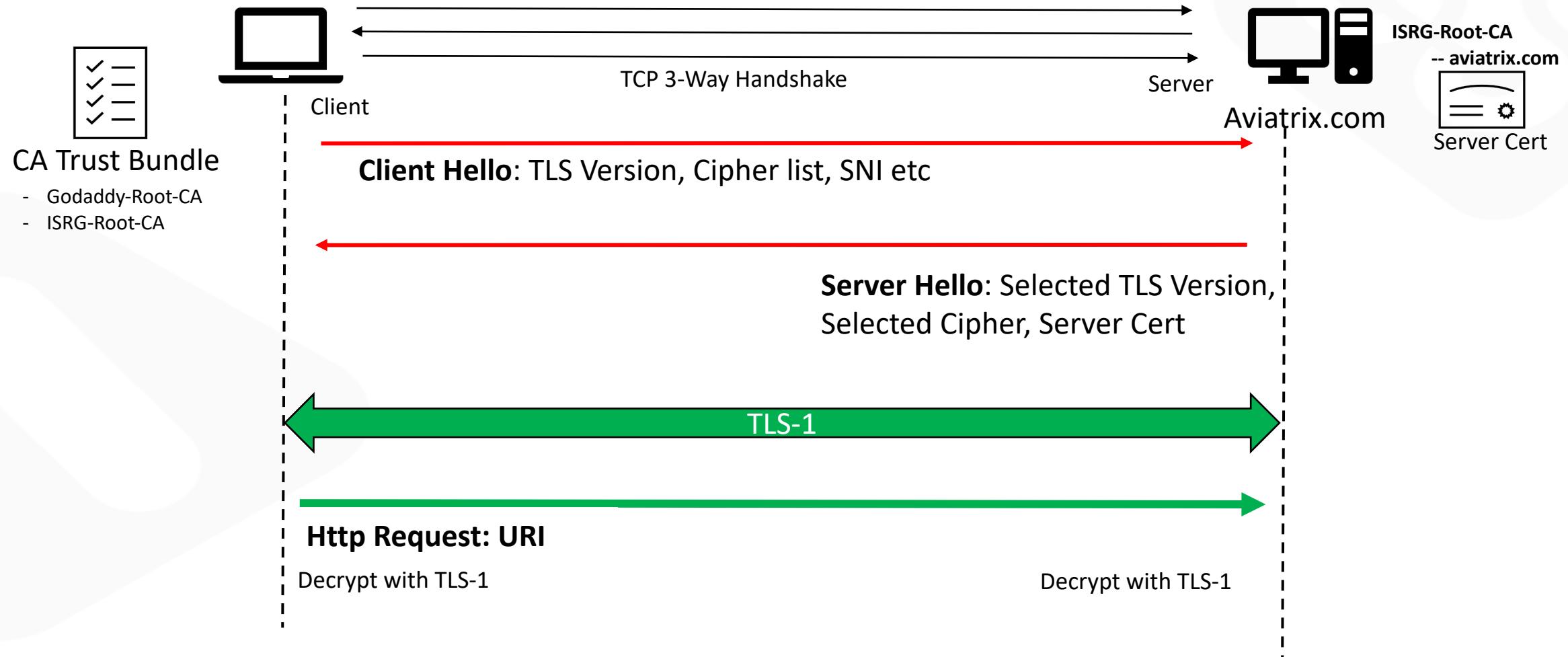
Enforcement Logging

Rule Priority

Cancel

- **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: Basic TLS Connection



TLS Decryption: PKI/ KMS and Trust Bundle

Certificate Hierarchy

- Root
 - Intermediate
 - Server Cert (Leaf Cert)

Certificate Fields

- Issuer
- Validity
- Subject

Trusted Root CA Bundle

Used by the Client and/or Proxy Gateway to Identify/ Trust the Original Server Cert

Decryption CA Cert

Used by the Decryption/Proxy gateway to generate a new Proxy-Server Cert and Sign it with the Decryption CA Cert

The screenshot shows a 'Certificate Viewer' interface for the domain 'aviatrix.com'. The top navigation bar has tabs for 'General' and 'Details', with 'Details' being the active tab. Below the tabs is a section titled 'Certificate Hierarchy' which displays a tree structure of certificates:

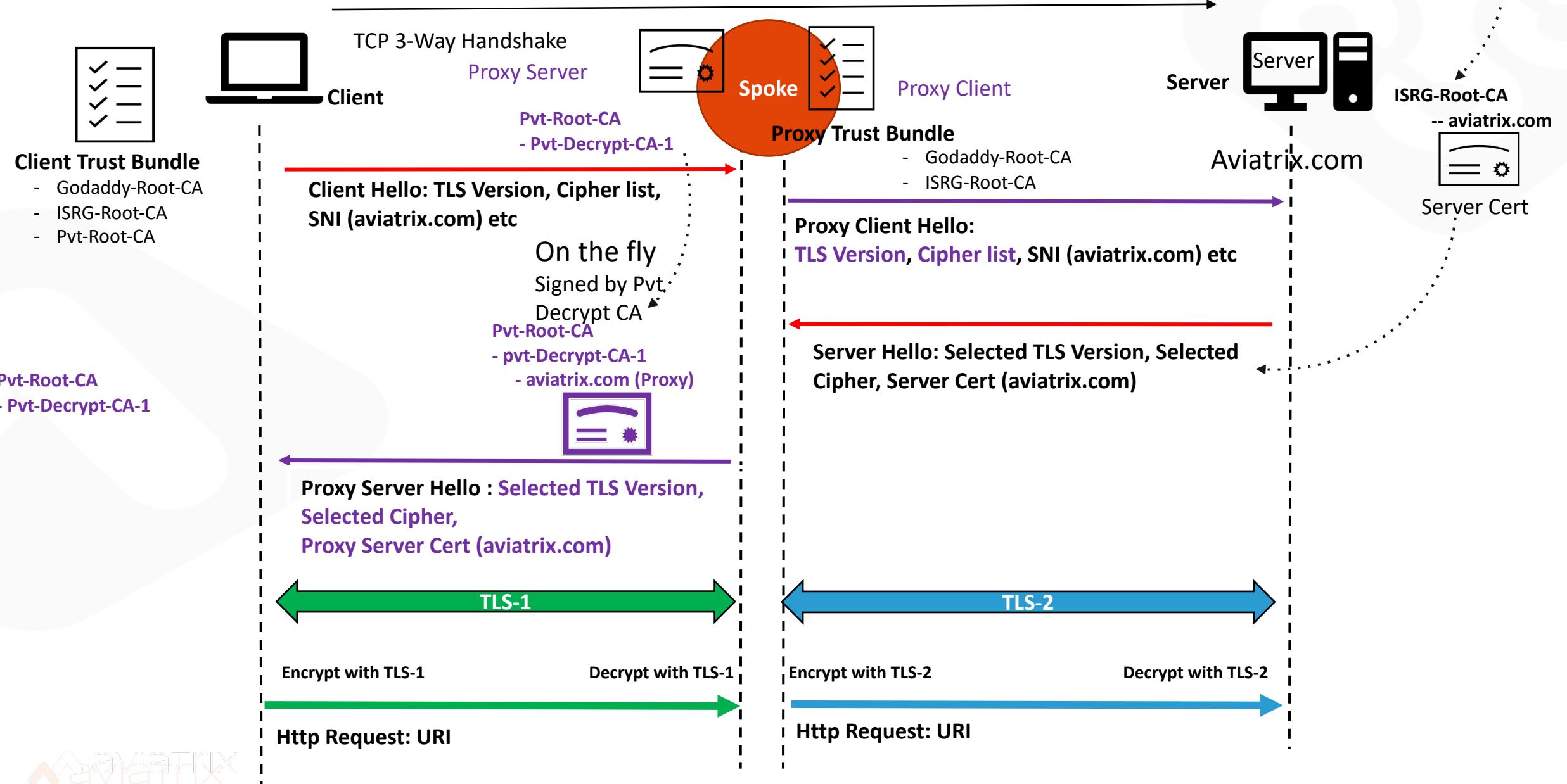
- ISRG Root X1
 - R3
 - aviatrix.com

Under the 'Details' tab, there is a section titled 'Certificate Fields' containing the following fields:

- Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
- Validity
- Subject
- Subject Public Key Info
 - CN = aviatrix.com

At the bottom of the 'Details' tab, there is a section titled 'Field Value' which contains the value 'CN = aviatrix.com'.

TLS Decryption: Basic TLS Decryption



TLS Decryption: Decryption CA Cert

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

The screenshot shows the SG Orchestration interface with the following configuration:

- Action: Permit
- SG Orchestration: On
- Ensure TLS: Off
- TLS Decryption: On (highlighted with a red box)
- Intrusion Detection (IDS): Off

A red arrow points from the "TLS Decryption: On" setting in the top interface to the "Download Certificate" button in the bottom interface.

The screenshot shows the Settings interface with the following configuration:

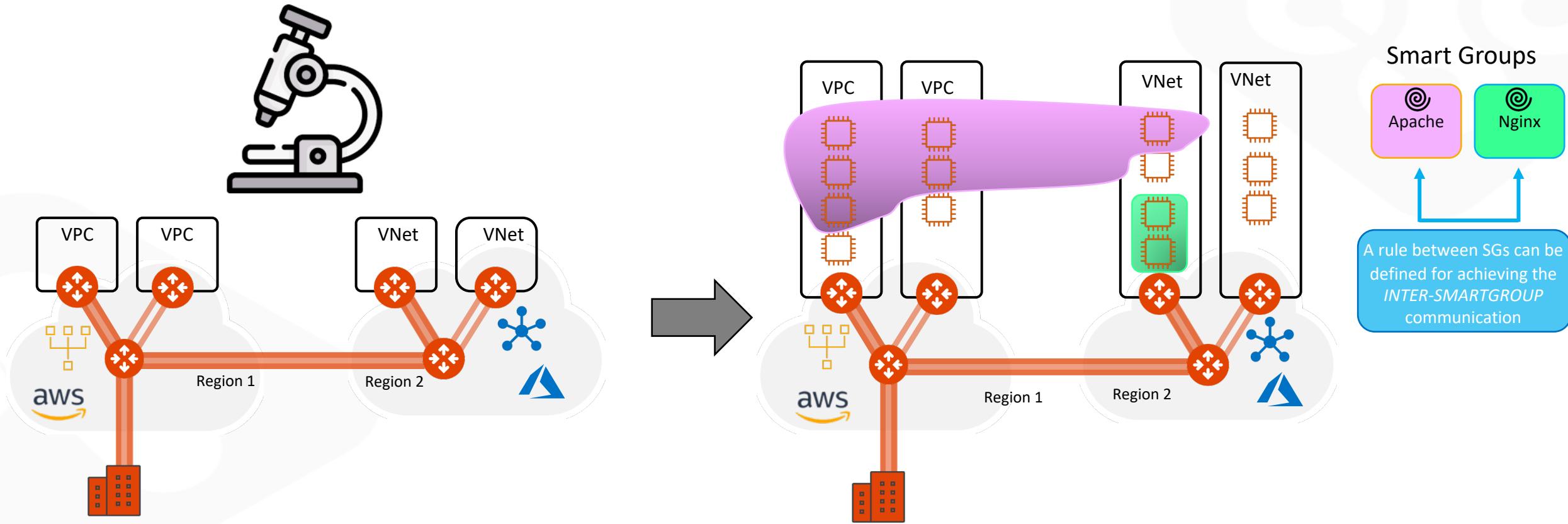
- Security Group (SG) Orchestration: Preview
- Decryption CA Certificate:
 - Certificate: Expires in 10 years
 - Renew Certificate
 - Enforcement: Permissive
 - Trust Bundle: default-trustbundle
 - Download Certificate (highlighted with a red box)
- CSP Resource Polling: On (with a slider set to 15 minutes)

A red box highlights the text: "Decrypt CA Certificates should be trusted by the Source SmartGroup virtual machines when TLS Decryption is enabled for proxy." A red arrow points from this text to the "Download Certificate" button in the bottom interface.

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



- **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-Segmentation: SmartGroups, Intra-Rules and Inter-Rules

The diagram illustrates a cloud network architecture with two regions, Region 1 and Region 2. Each region contains a VNet (Virtual Network) with multiple VPCs. A central fabric connects the VPCs between regions. The network is segmented into SmartGroups: Apache (orange) and Nginx (green). Intra-region traffic is shown with pink arrows, while inter-region traffic is shown with green arrows.

Intra Rules:

- SmartGroup Apache (Region 1):** A pink arrow labeled "intra" points from the SmartGroup Apache icon to a "Create Rule" dialog for "INTRACLIENT-ICMP-APACHE". The rule permits ICMP traffic from APACHE to APACHE.
- SmartGroup Nginx (Region 1):** A green arrow labeled "intra" points from the SmartGroup Nginx icon to a "Create Rule" dialog for "INTRACLIENT-ICMP-NGINX". The rule permits ICMP traffic from NGINX to NGINX.

Inter Rules:

- SmartGroup Nginx (Region 1) to SmartGroup Apache (Region 2):** A green arrow labeled "inter" points from the SmartGroup Nginx icon to a "Create Rule" dialog for "INTER-ICMP-NGINX-APACHE". The rule permits ICMP traffic from NGINX to APACHE.
- SmartGroup Apache (Region 2) to SmartGroup Nginx (Region 1):** A pink arrow labeled "inter" points from the SmartGroup Apache icon to a "Create Rule" dialog for "INTER-ICMP-APACHE-NGINX". The rule permits ICMP traffic from APACHE to NGINX.

Distributed Cloud Firewall UI:

The screenshot shows the "Rules" tab of the Distributed Cloud Firewall interface. It displays a list of rules with columns for Priority, Name, Source, Destination, WebGroup, Protocol, Ports, Action, SG Orchestration, and Decryption. The rules listed are:

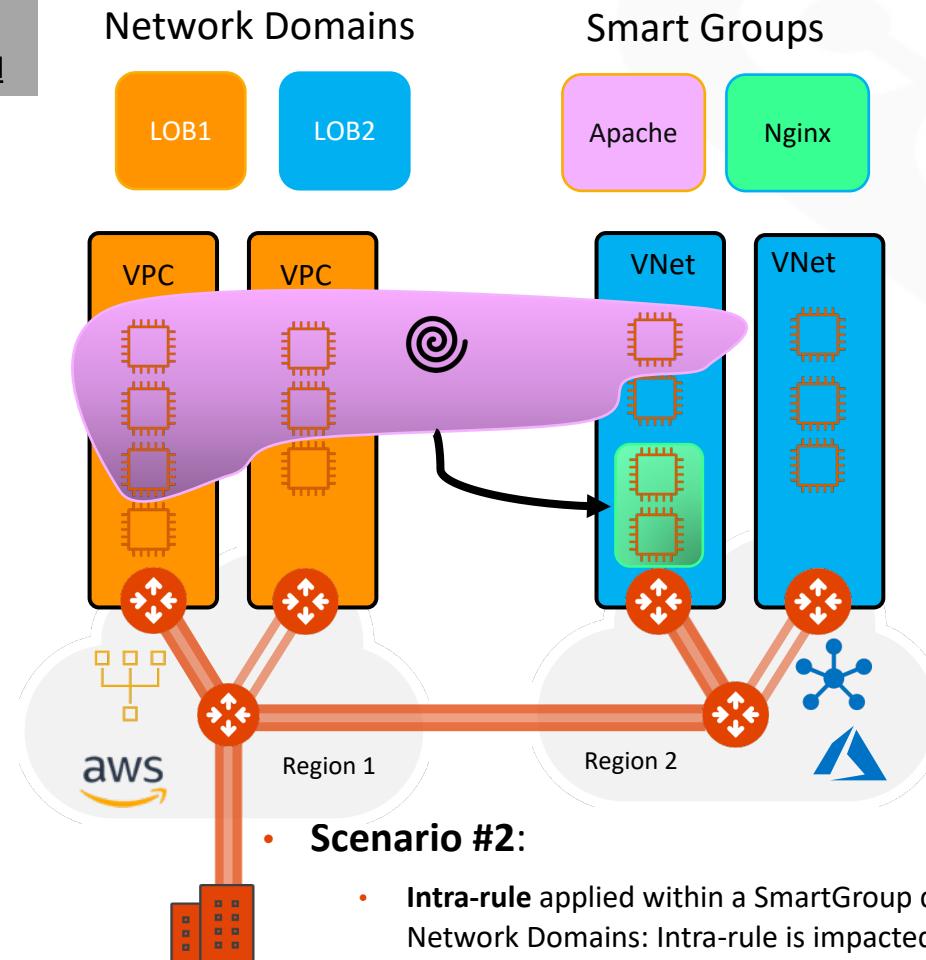
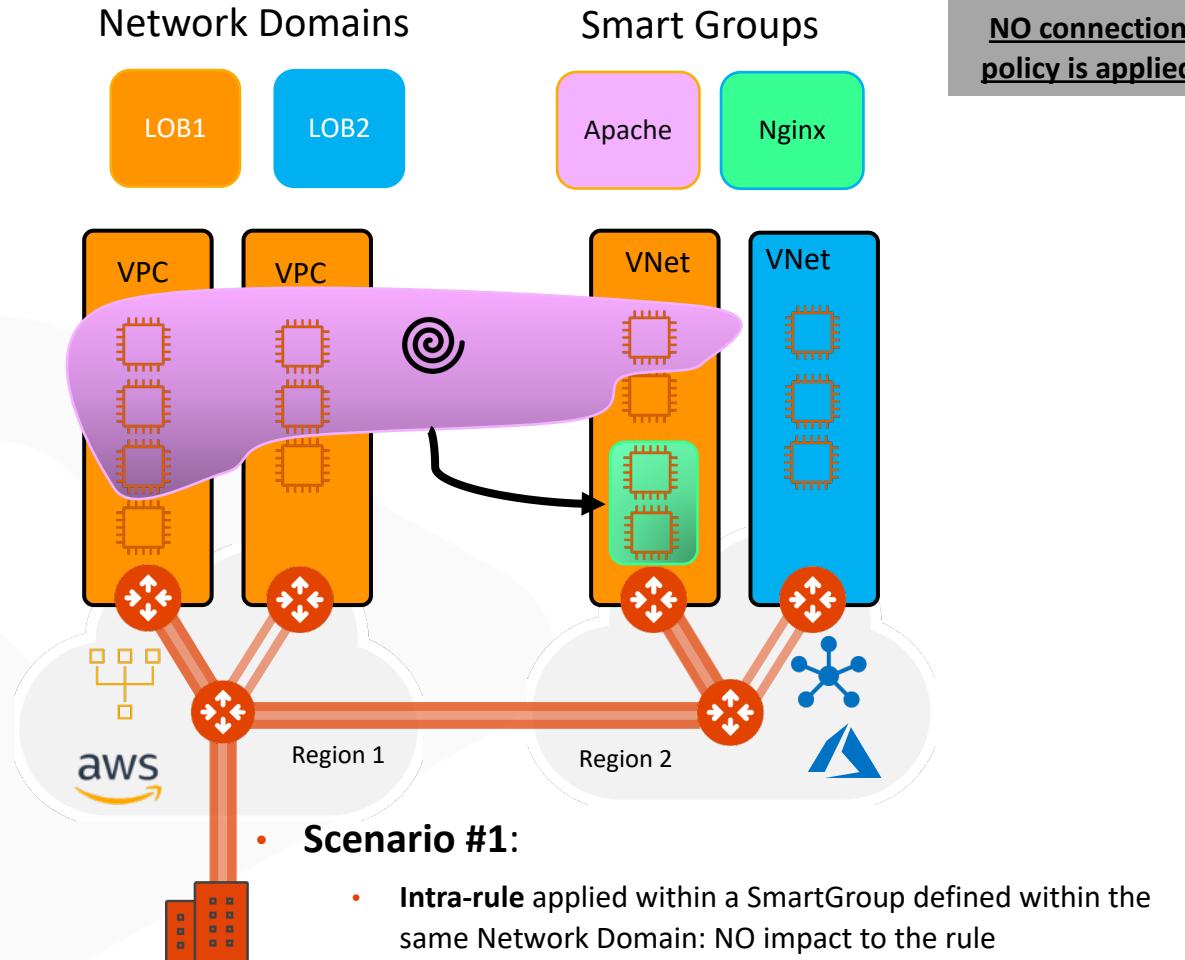
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	Decryption
1	INTRACLIENT-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
2	INTRACLIENT-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
3	INTER-ICMP-NGINX-APACHE	NGINX	APACHE		ICMP		Permit	On	
4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Deny		
21474...	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit		

A red arrow points to the "Commit" button at the bottom right of the rules table, which is highlighted with a red box.

List of Key Points:

- 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



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

The diagram shows a central **VNet** icon containing two pink and two green network card icons. Below it, a **Transit** icon and a **Spoke** icon are connected by a red line. A blue cloud icon is also present. On the left, a white box labeled **Security Group (SG) Orchestration** contains the text: "SG Orchestration adds control for both Intra-VPC Traffic and Inbound Internet Access on desired VPC/VNets." It also states "Available On 7 VPC/VNets". A red arrow points from this box to a **Manage** button in a separate window.

Decryption CA Certificate

- Certificate: Expires Invalid date (Self-Signed)
- [Renew Certificate](#)

Enforcement: Permissive
Trust Bundle: default-trustbundle
[Download Certificate](#)

SmartGroup #1 (purple) and **SmartGroup #2** (cyan) are shown below the main VNet icon.

- 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**.

⚠ 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	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled
AZURE-WESTEUROPE-	Azure ARM	westeuropa	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

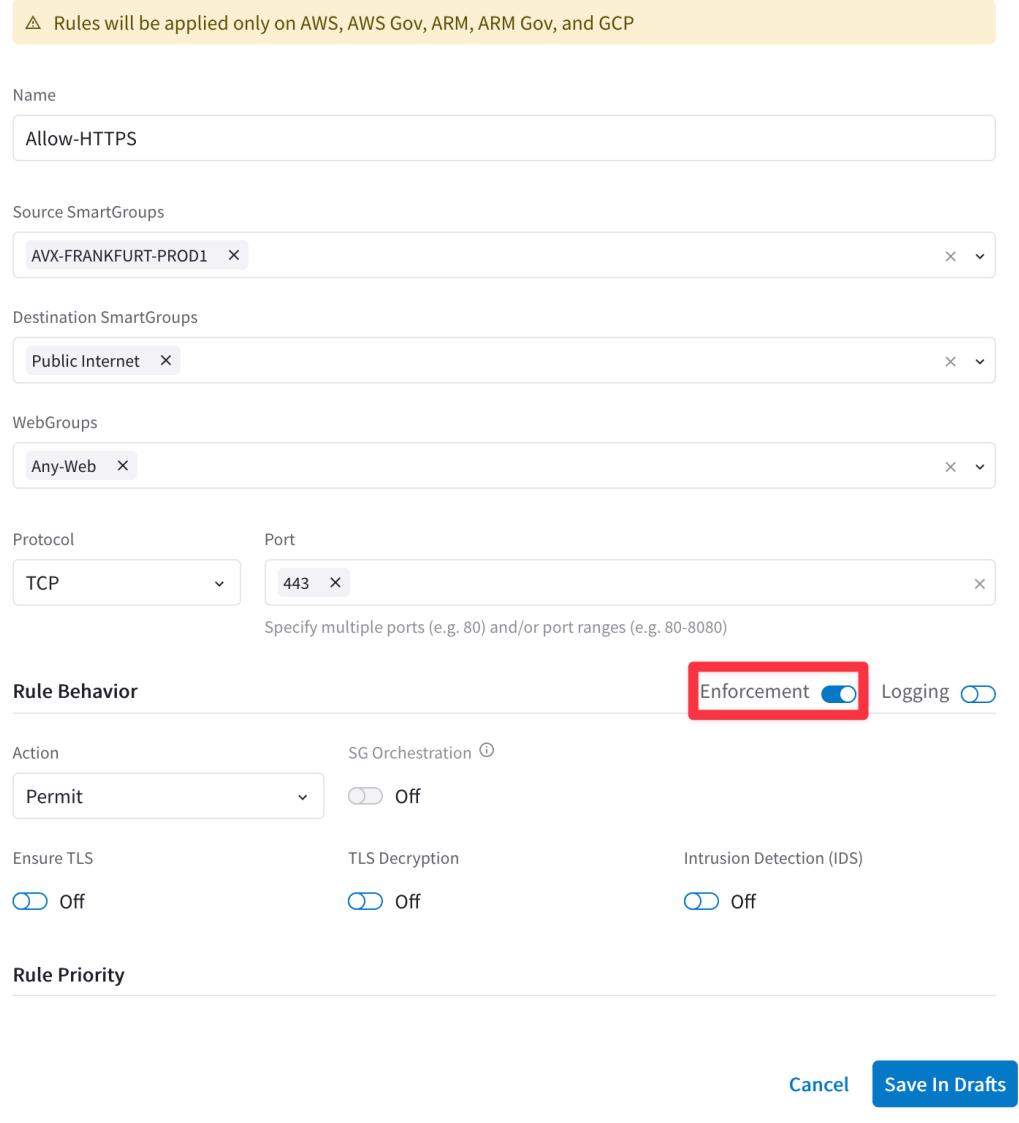
Action Permit SG Orchestration Off

Ensure TLS Off TLS Decryption Off Intrusion Detection (IDS) Off

Rule Priority

Enforcement Logging

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 X

Close

Destination SmartGroups

Public Internet X

WebGroups

Any-Web X

Protocol

TCP X

Port

443 X

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

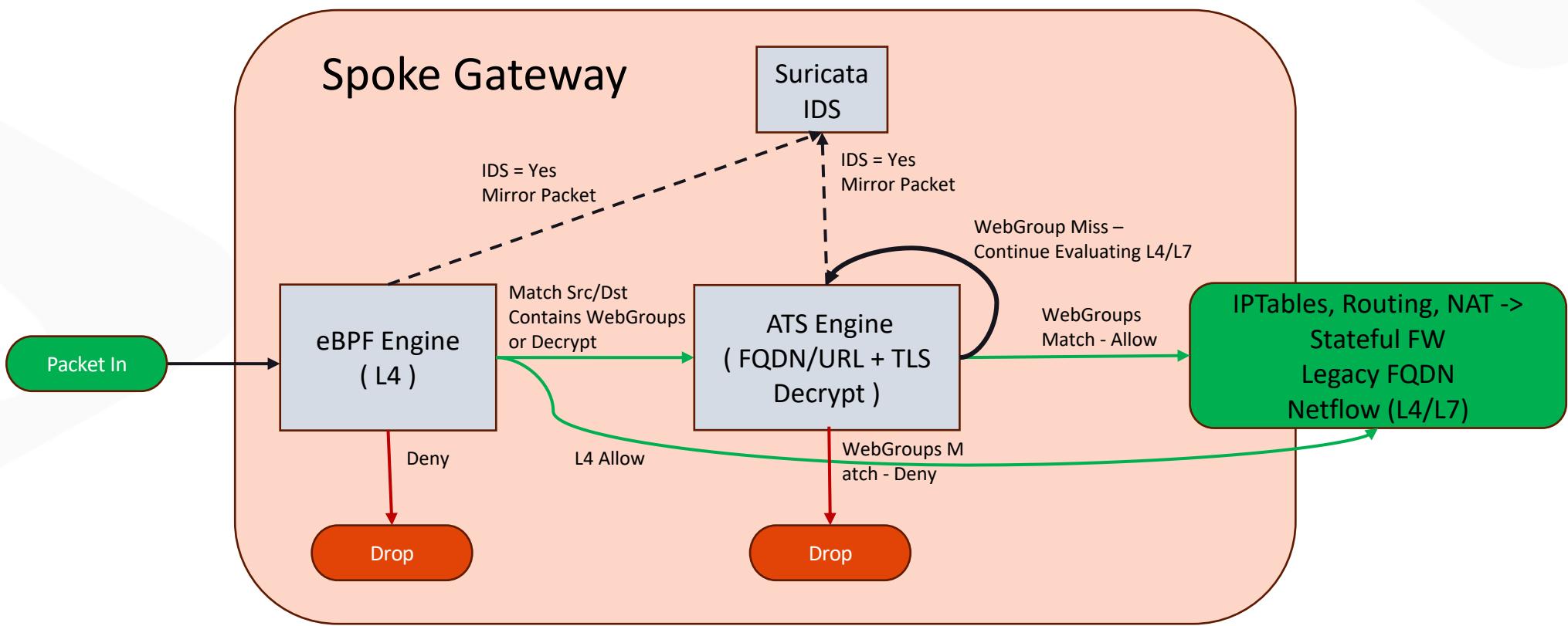
Policy Monitor												
Timestamp	Rule	Source SmartGroup	Destination SmartGroup	Source IP	Destination IP	Protocol	Source Port	Destination Port	Action	Enforcing		
2023-04-14 09:16:16.006 PM	intra-ssh-bu1	bu1	bu1	192.168.1.100	10.0.1.100	TCP	22	52106	PERMIT	✓		
2023-04-14 09:16:15.824 PM	allow-ssh-myip-bu1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

❑ 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)



Next: Lab 10 – Distributed Cloud Firewall