



# Security Close to the Applications

AVIATRIX DISTRIBUTED CLOUD FIREWALL



# NIST Tenets Covered

This module will cover two tenets of NIST Zero-Trust Architecture (ZTA)

1. Security Close to the Applications
2. Global, Dynamic and Centralized Policy Model

## Related Aviatrix Features

- Aviatrix Distributed Cloud Firewall
- Network Segmentation
- Micro-Segmentation
- ThreatIQ / ThreatGuard
- GeoBlocking
- URL Filtering / Internet Egress Traffic Filtering
- Centralized Policy Engine

### Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

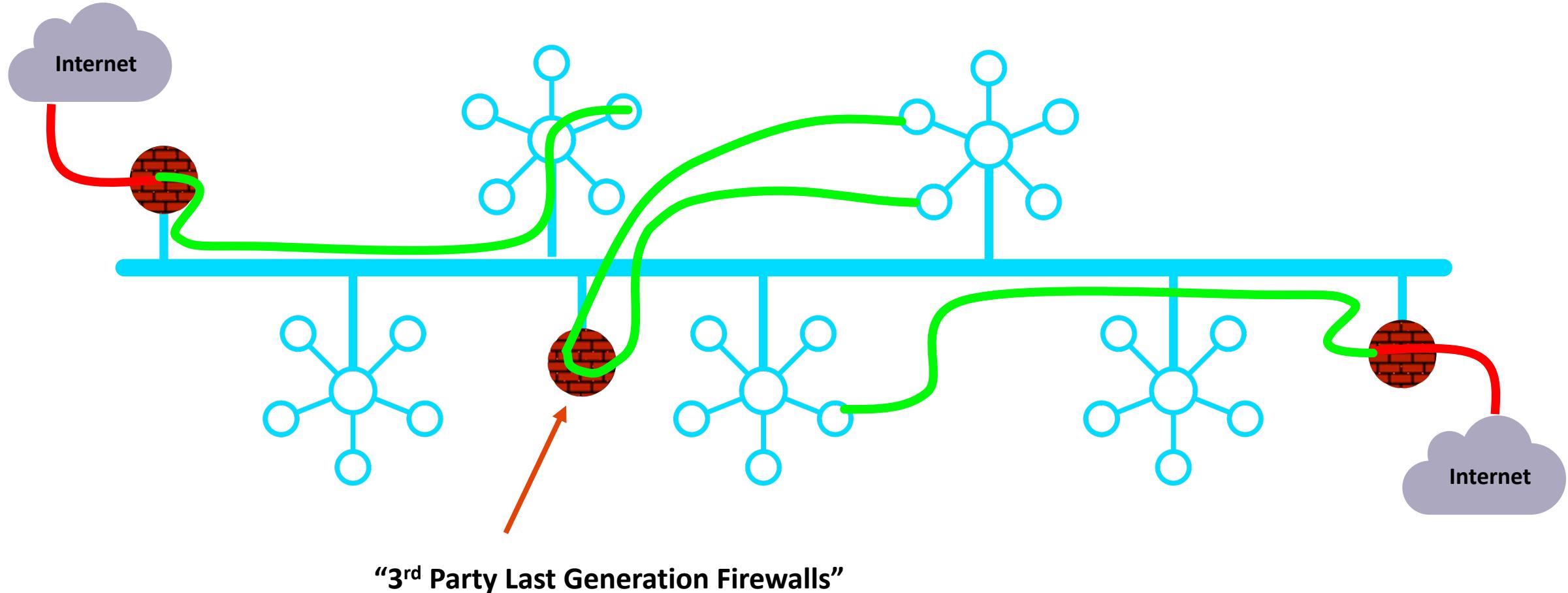
**Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture.**

Workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise networks. This also includes workloads migrating from on-premises data centers to non-enterprise cloud instances.

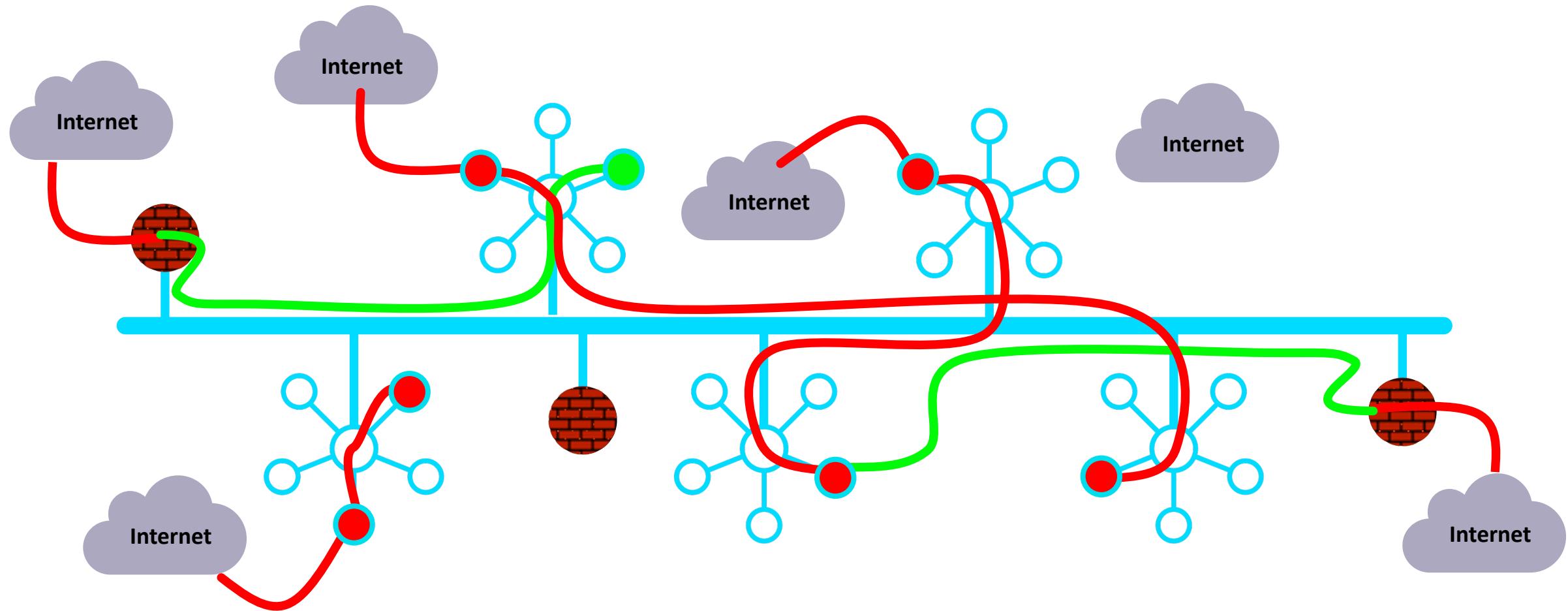
### Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

**Access to resources is determined by dynamic policy**—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

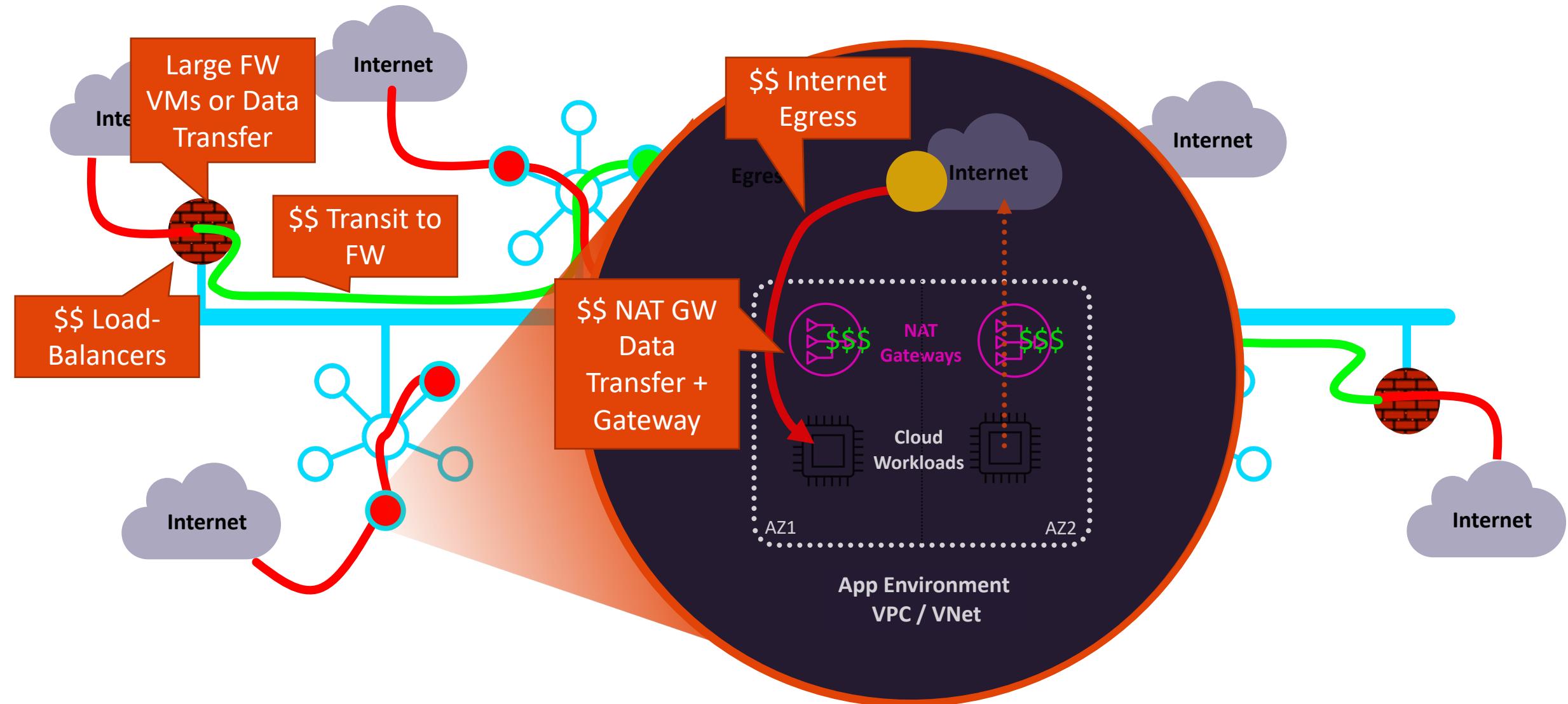
# As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



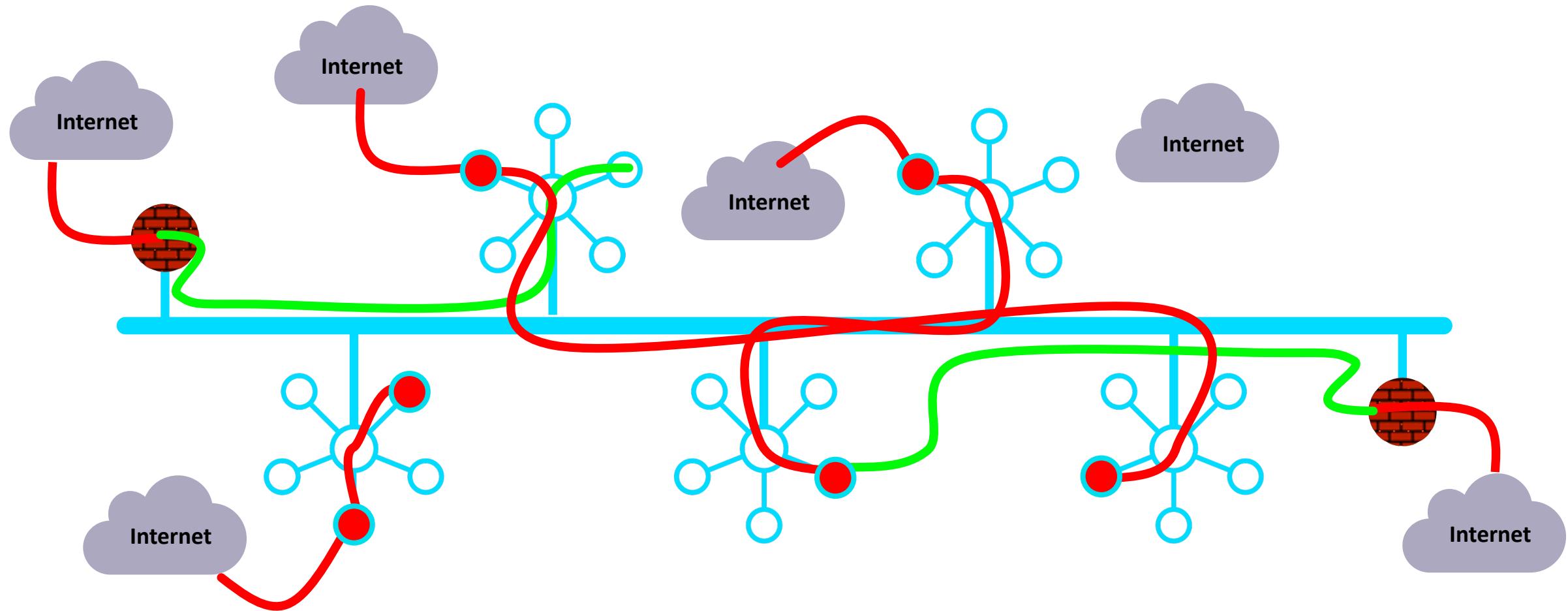
# In Reality...



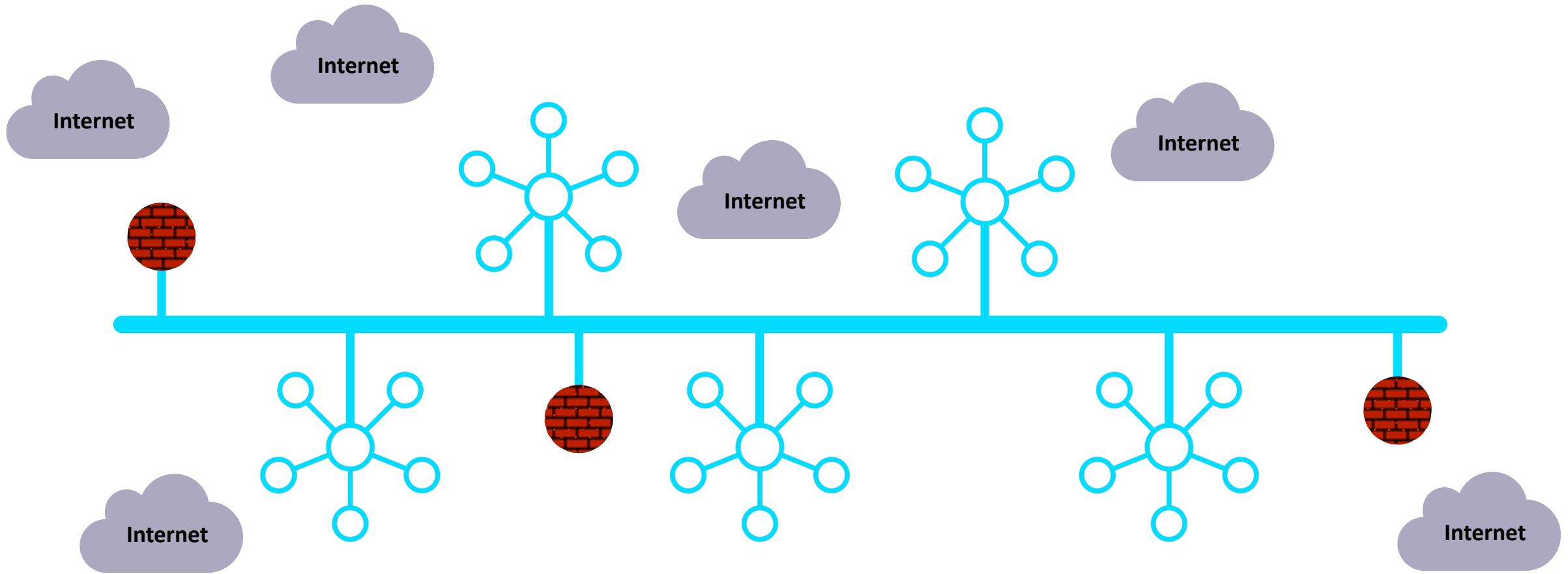
# This is bad! Expensive and Lacks Enterprise-Grade Security



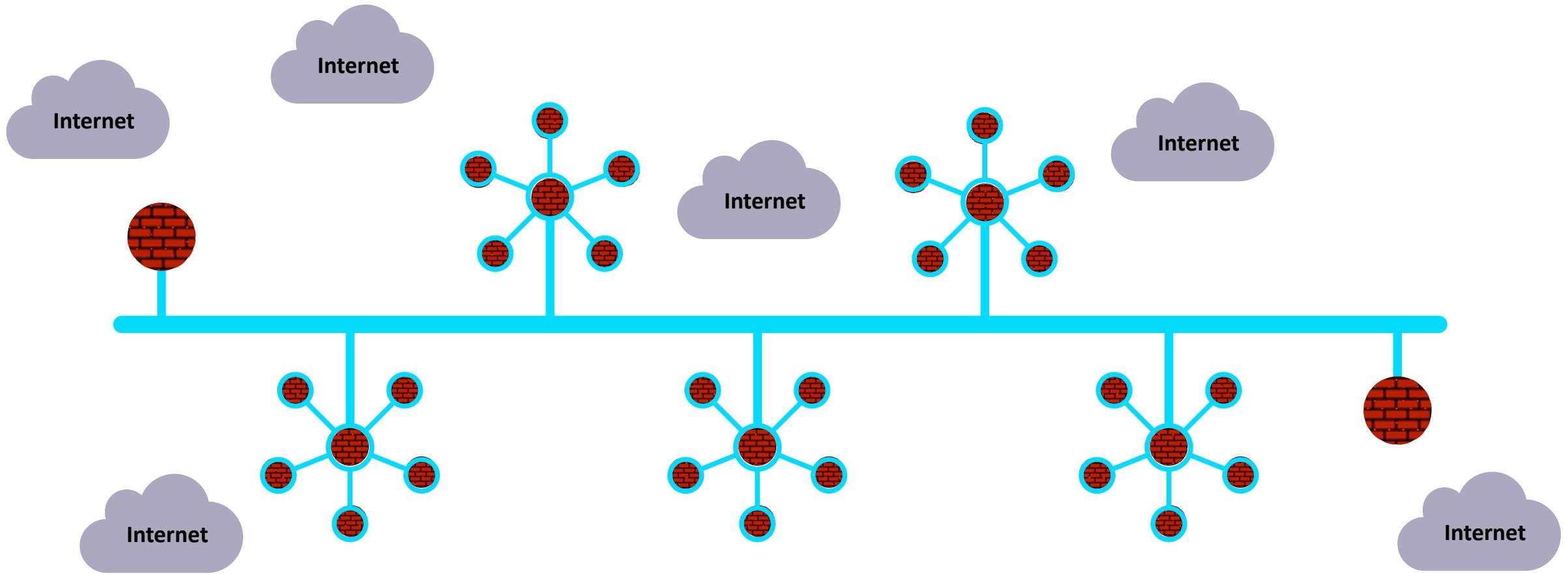
# In Reality...



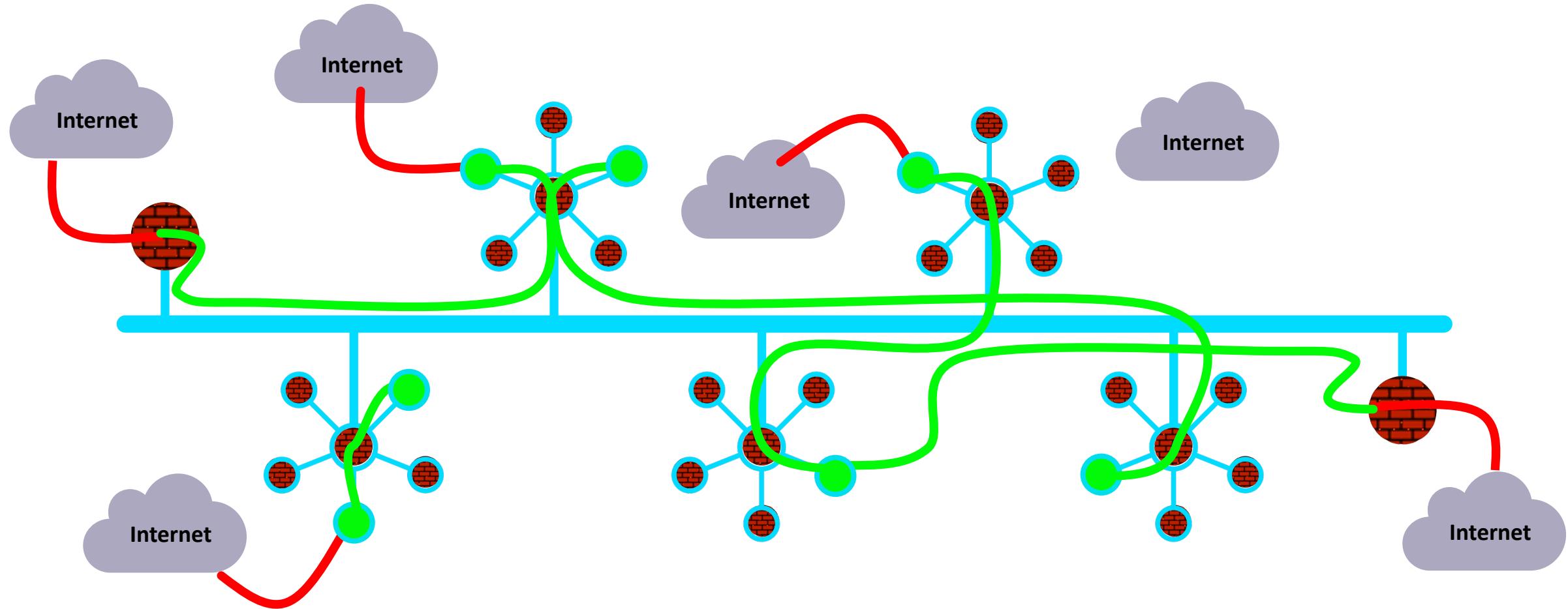
# What If...



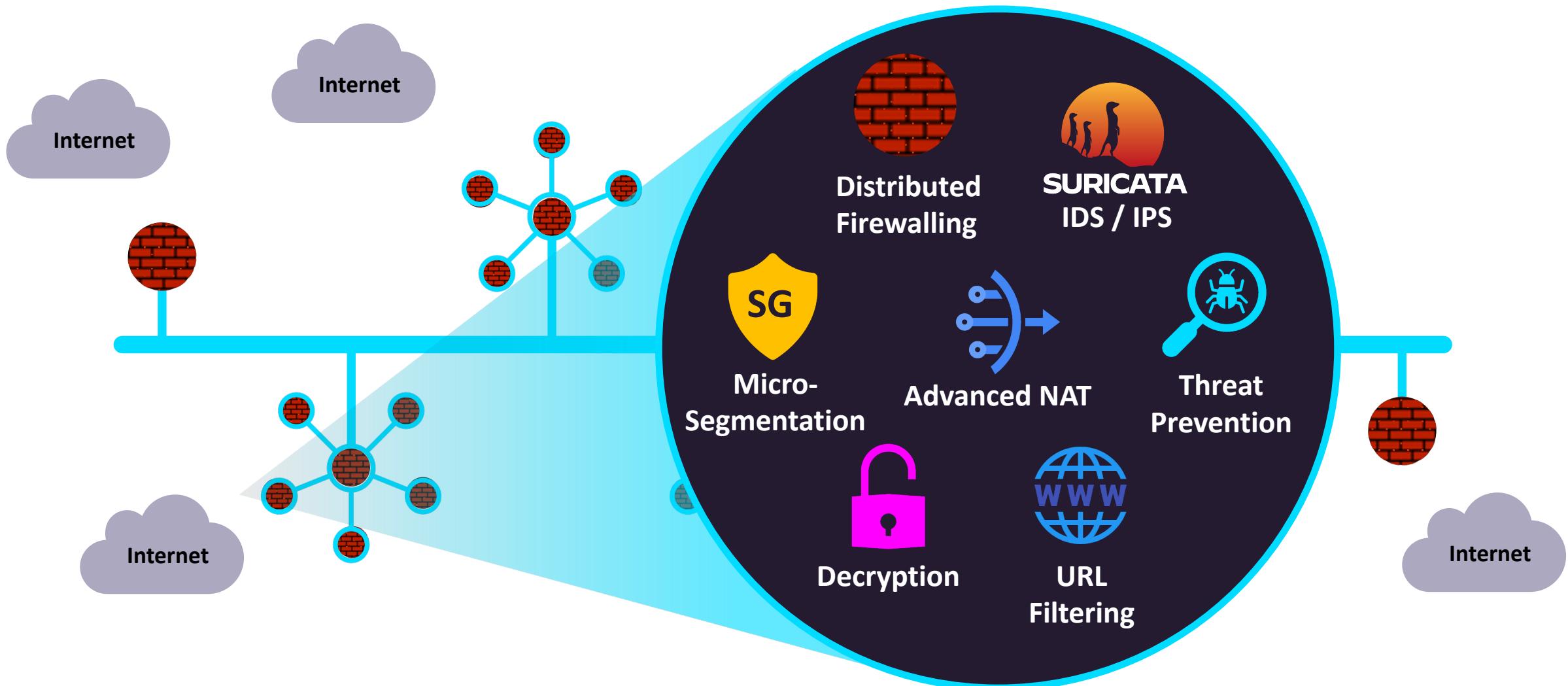
# Firewalling Functions were Embedded in the Cloud Network Everywhere...



# Centrally Managed, with Distributed Inspection & Enforcement...

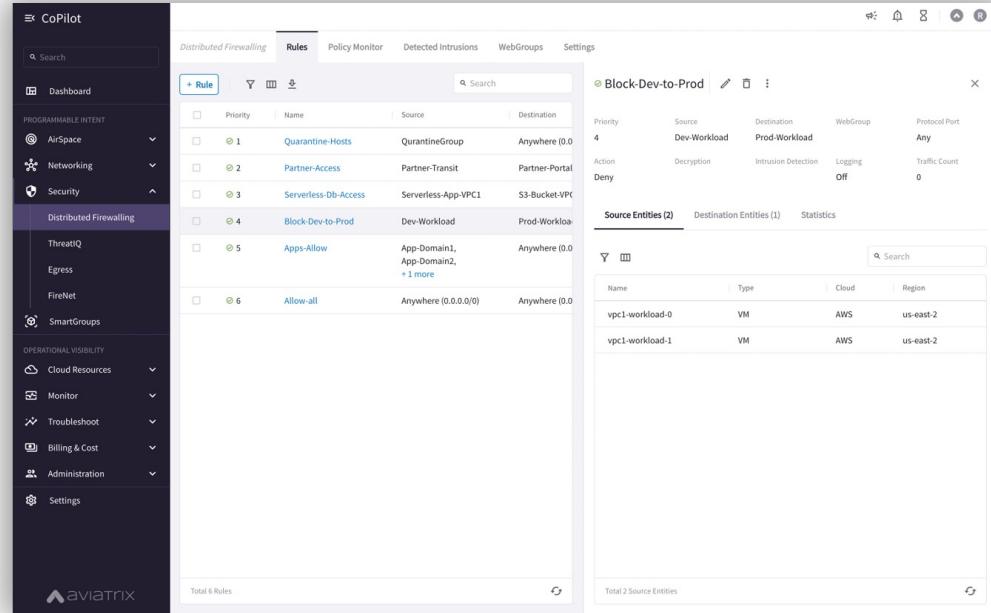


# And, What If it was more than just firewalling...



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

## Centralized Policy Creation



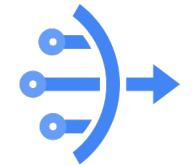
The screenshot shows the Aviatrix CoPilot web interface. On the left, a sidebar menu includes options like Dashboard, AirSpace, Networking, Security, Distributed Firewalling (selected), ThreatIQ, Egress, FireNet, and SmartGroups. The main panel displays a 'Rules' tab with a table of six firewall rules. Rule 4, titled 'Block-Dev-to-Prod', is selected and expanded, showing details such as priority (4), source (Dev-Workload), destination (Prod-Workload), protocol (Any), action (Deny), decryption (On), intrusion detection (On), logging (Off), and traffic count (0). Below the rule table, there are sections for 'Source Entities (2)' and 'Destination Entities (1)'. At the bottom, it says 'Total 6 Rules'.

Aviatrix CoPilot

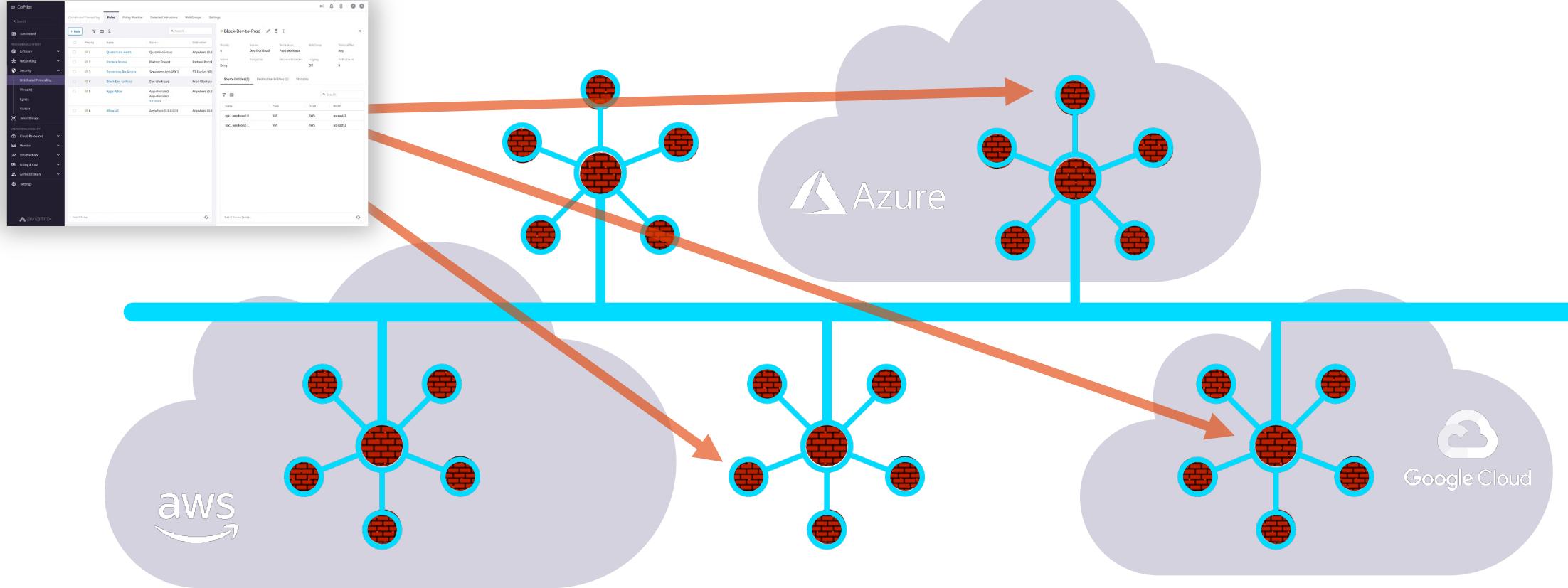
## Distributed Enforcement



**Micro-Segmentation**



# A Distributed Cloud Firewall...



Where and How Policies Are Enforced Is Abstracted...



# Enabling Aviatrix Distributed Cloud Firewall (DCF)

## Global Policy – Distributed Enforcement

# Enable Distributed Cloud Firewall

CoPilot

Search

- Dashboard
- Cloud Fabric
- Networking
- Security
- Distributed Cloud Firewall
- Egress
- ThreatIQ
- FireNet
- Anomaly Detection
- SmartGroups
- Cloud Resources
- Monitor

Distributed Cloud Firewall      Rules      Monitor      Detected Intrusions      WebGroups      Settings

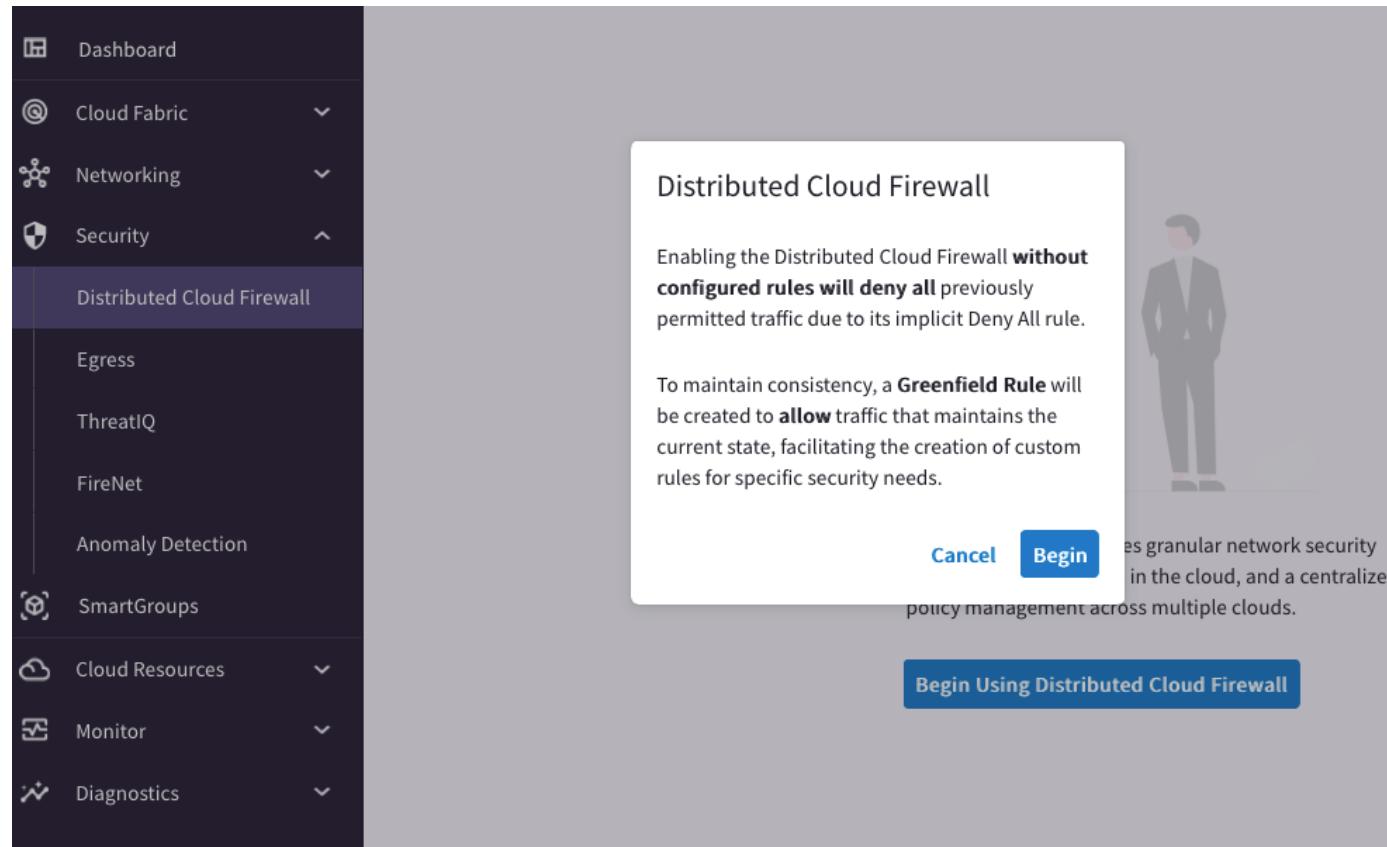


Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

[Manage Add-on Features](#)      [Enable Distributed Cloud Firewall](#)

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.

# Enable Distributed Cloud Firewall



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.

**Cancel** **Begin**

Enables granular network security in the cloud, and a centralized policy management across multiple clouds.

**Begin Using Distributed Cloud Firewall**

Distributed Cloud Firewall		Rules	Monitor	Detected Intrusions	WebGroups	Settings				
+ Rule	Actions									
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	Decryption	IDS
2147483646	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit			

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

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

# Global Policy Rule Creation and Enforcement

Create Rule

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

Name: Deny-ICMP

Source SmartGroups: prod

Destination SmartGroups: dev

WebGroups: (empty)

Protocol: ICMP

**Rule Behavior**

Action: Deny

SG Orchestration: On

TLS Decryption: Off

**Rule Priority**

Place Rule: Top

Buttons: Cancel, Save In Drafts

- **Enforcement ON**
  - The policy is enforced in the Data Plane
- **Enforcement OFF**
  - The policy is NOT enforced in the Data Plane
  - The option provides a *Watch/Test* mode
  - Watch what traffic hits the deny rule before enforcing the rule in the Data Plane.
- **Security Group Orchestration**
  - Provides both Intra VPC/VNET traffic and Inbound Internet Access Control

# Rule Logging

Edit Rule: Deny-HTTP

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

Name

Deny-HTTP

Source SmartGroups

- prod X

Destination SmartGroups

- dev X

WebGroups

- 

Protocol Port

TCP 80 X

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

Rule Behavior

Action SG Orchestration

Deny On

TLS Decryption

Off Off

Rule Priority

Place Rule

Top ▼

**Cancel** **Save In Drafts**

☐ Logging can be turned ON/OFF per rule

☐ Aviatrix CoPilot Syslog/Netflow captures all logs

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	✓		

# Disabling Distributed Cloud Firewall

Configuration General License Logging Services Private Mode

License Type Universal

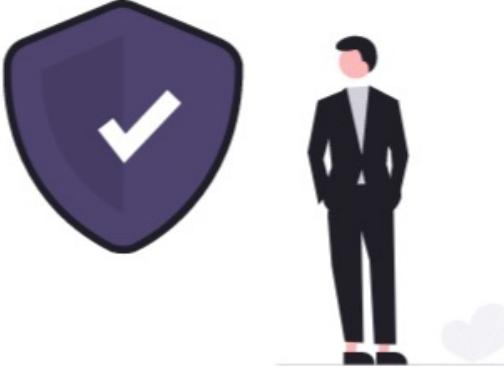
License ID  
Lic-1664988

Customer ID  
avi.....

Add-on Features

Feature

- Distributed Cloud Firewall
- CostIQ
- CoPilot API



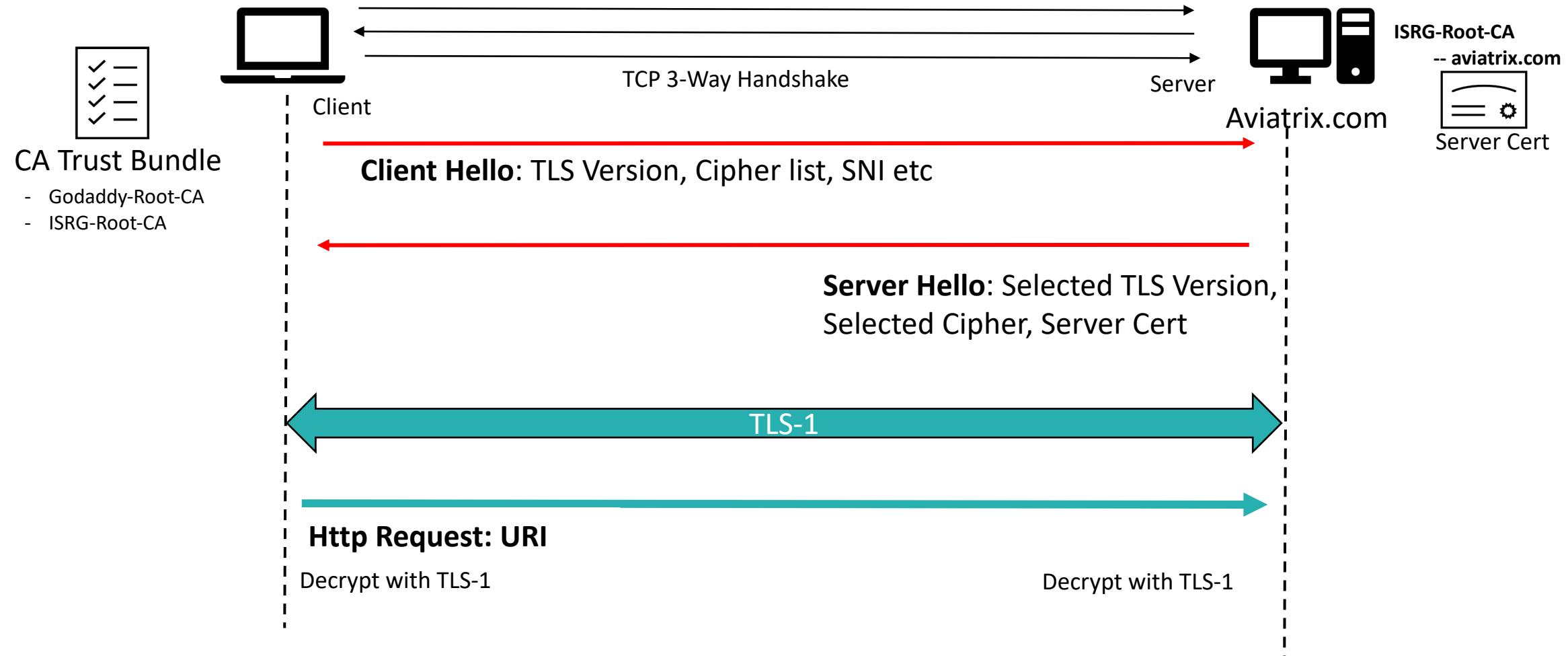
Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

**Disabling Distributed Cloud Firewall will remove all existing policies.**

I understand that all policies will be removed and my instances may no longer be secured.

**Cancel** **Disable Distributed Cloud Firewall**

# 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 includes tabs for 'General' and 'Details'. The main content area is divided into sections: 'Certificate Hierarchy' and 'Certificate Fields'.

**Certificate Hierarchy:** This section displays the certificate chain:

- ISRG Root X1
  - R3
    - aviatrix.com

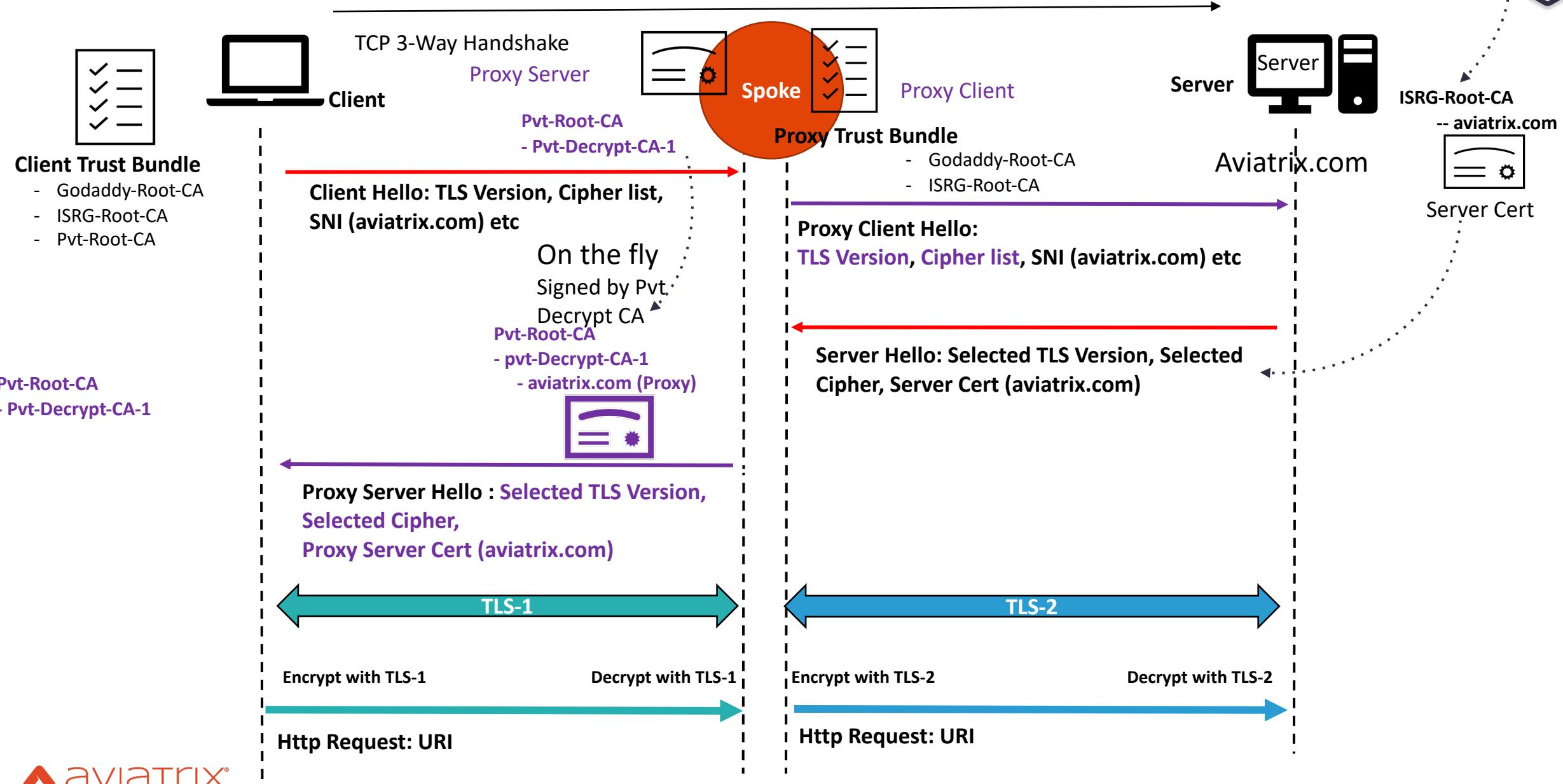
**Certificate Fields:** This section lists the fields of the certificate:

- Certificate:** Version, Serial Number, Certificate Signature Algorithm, Issuer.
- Validity:**
- Subject:**
- Subject Public Key Info:**

**Field Value:** The value for the 'Subject' field is listed as `CN = aviatrix.com`.

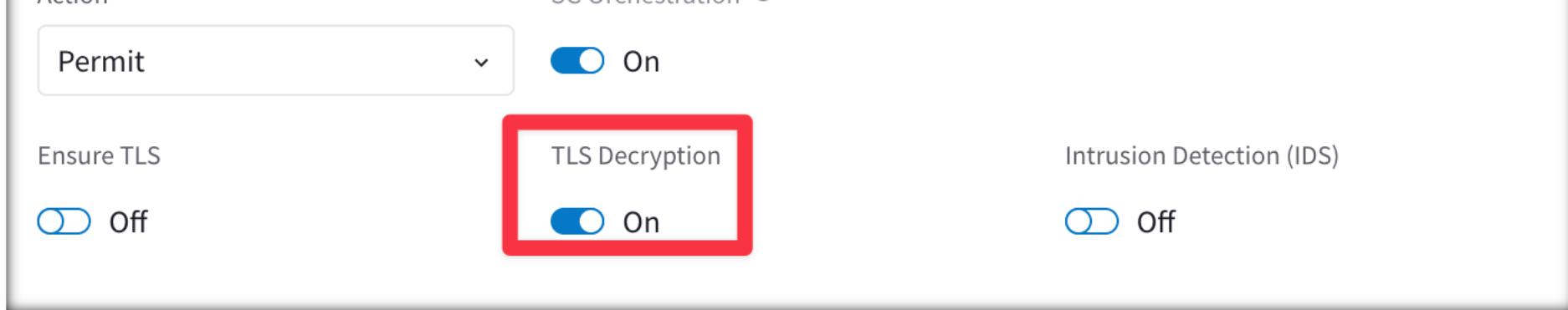
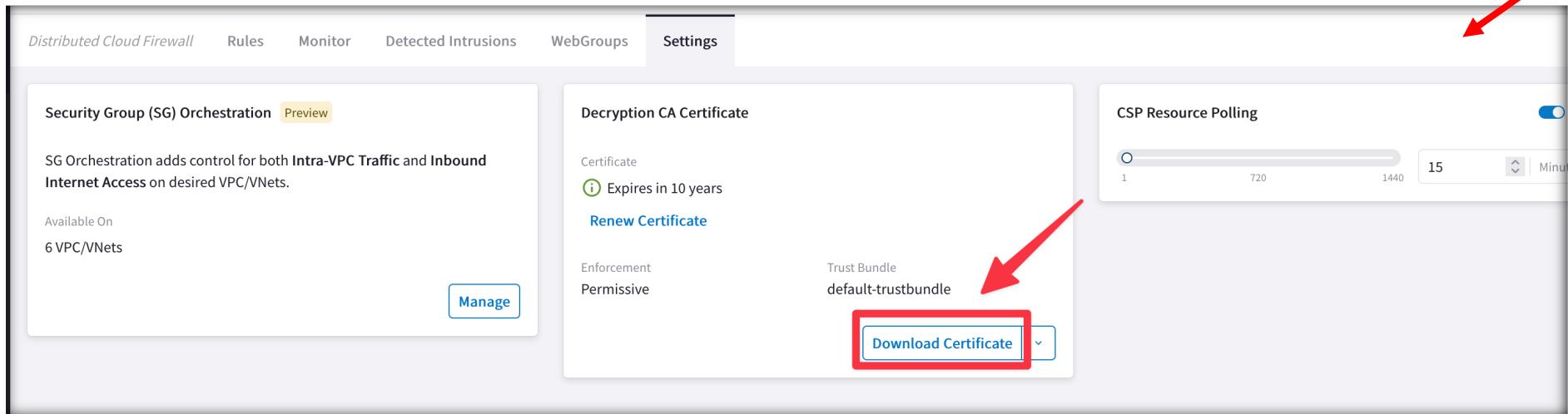


# TLS Decryption: Basic TLS Decryption



# TLS Decryption: Decryption CA Cert

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

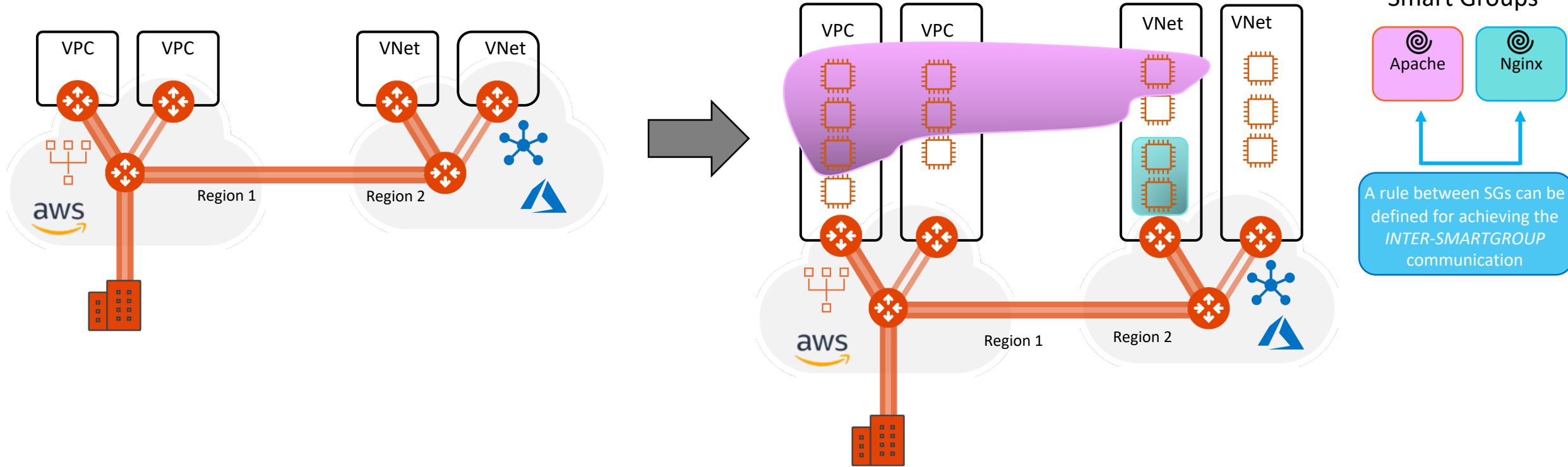



The screenshot shows the "Settings" tab of the "Distributed Cloud Firewall" interface. The "Security Group (SG) Orchestration" section indicates it adds control for Intra-VPC Traffic and Inbound Internet Access. It shows 6 VPC/VNets available and a "Manage" button. The "Decryption CA Certificate" section shows a certificate that expires in 10 years, with a "Renew Certificate" button. The "CSP Resource Polling" section has its toggle turned "On" and a slider set to 15 minutes. The "Trust Bundle" dropdown is set to "default-trustbundle" and the "Download Certificate" button is highlighted with a red box. A red arrow points from the top note about trusting the CA certificate to this "Download Certificate" button.

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

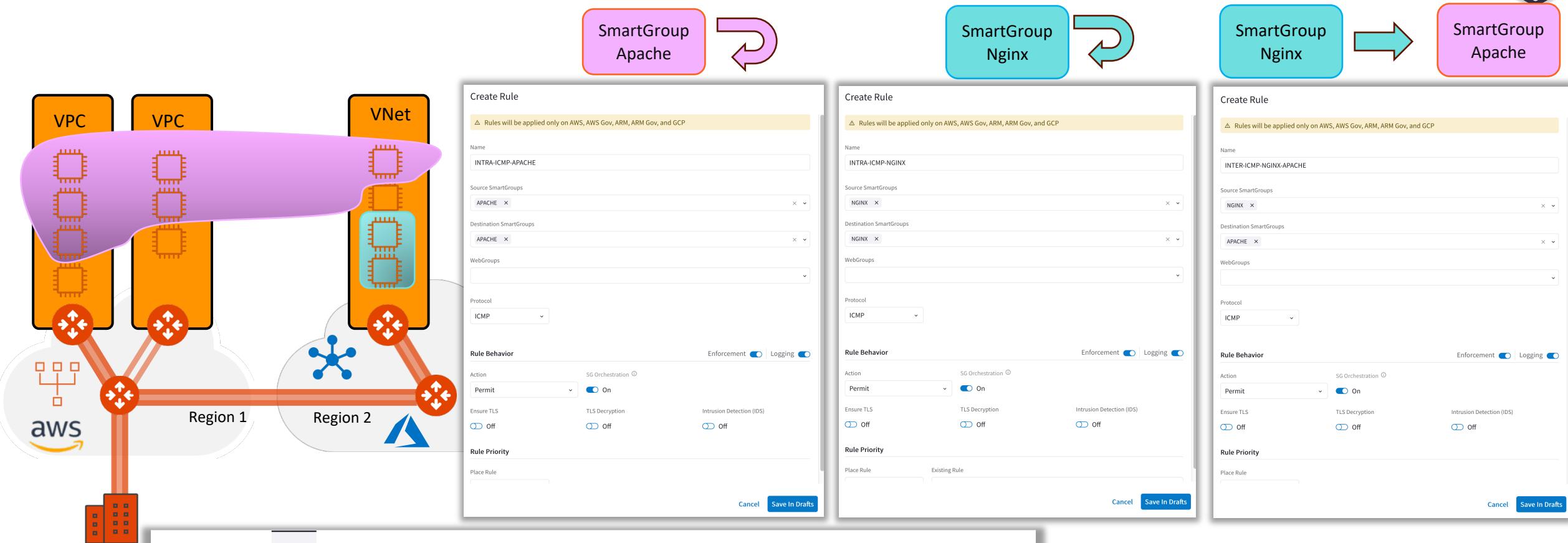
Decrypt CA Certificates should be trusted by the **Source SmartGroup** virtual machines when TLS Decryption is enabled for proxy.

# Aviatrix DCF: Intra and Inter SmartGroups Rules



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

# Aviatrix DCF: Intra and inter SmartGroups Rules



SmartGroup  
Apache

SmartGroup  
Nginx

SmartGroup  
Nginx

SmartGroup  
Apache

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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: Off

Logging: On

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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: Off

Logging: Off

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

Protocol: ICMP

Action: Permit (SG Orchestration On)

Ensure TLS: Off

TLS Decryption: Off

Intrusion Detection (IDS): Off

Rule Priority: Place Rule

Enforcement: On

Logging: On

Cancel Save In Drafts

Distributed Cloud Firewall    Rules    Monitor    Detected Intrusions    WebGroups    Settings

+ Rule    Actions    ▾

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	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		

4 New    1 Modified    Discard    Commit

- 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

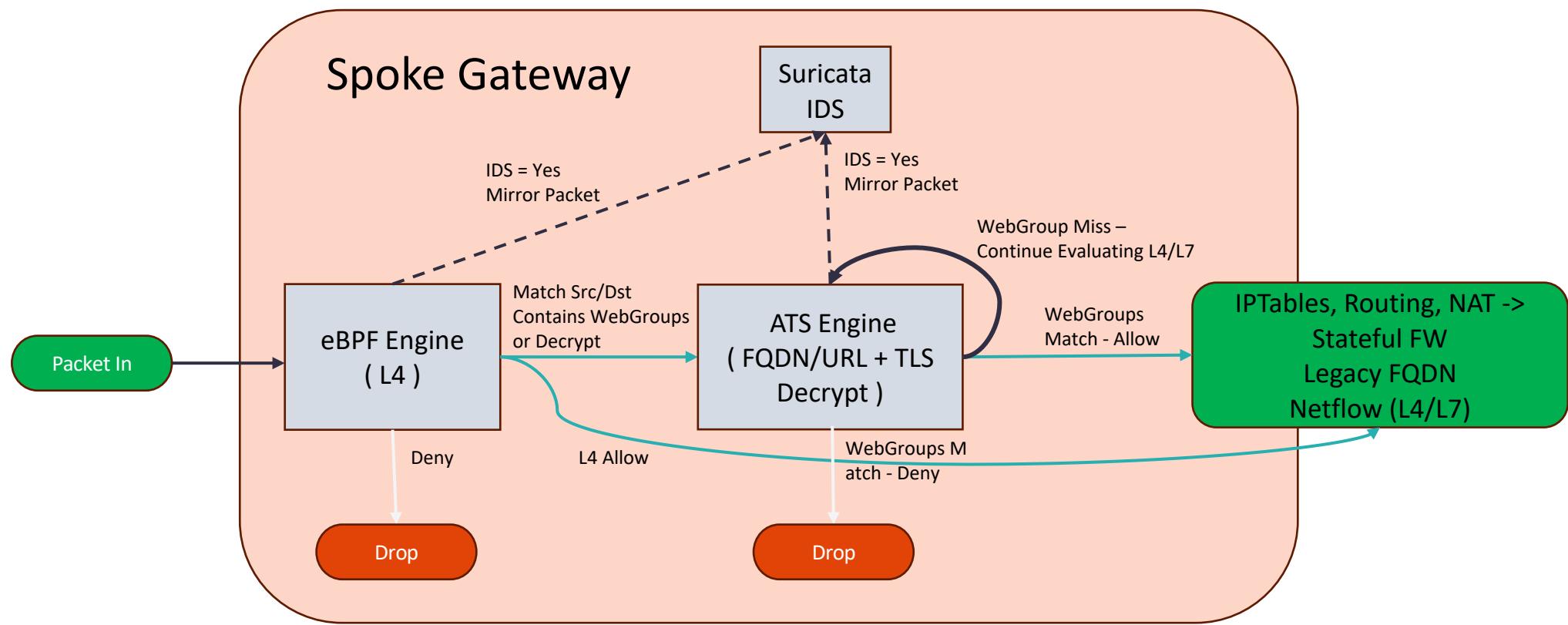


avia

24

# 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
<u><a href="#">Security Group</a></u> <u><a href="#">Orchestration</a></u> is supported				x (Azure)	x (AWS and Azure)



## 3<sup>rd</sup> Party Firewall Service Insertion (Aviatrix FireNet)

Centralized model

Use as necessary

# Aviatrix FireNet For 3<sup>rd</sup> Party FW Service Insertion/Chaining

## Firewall Service Insertion

- E-W / Egress / Ingress / all traffic
- High Performance Encryption (HPE)
- Active / Active – Across AZs
- No IPsec / No BGP / No SNAT required

## Automated Control and Management

- Repeatable architecture across regions/clouds
- Centralized firewall deployment
- Vendor API integration
- UDR and VPC Route propagation

## Improved Failure Detection and Failover

- Health Check monitoring

## Forwarding Algorithm Options

- Intelligent traffic steering and firewalling based on traffic type
- 5-tuple and 2-tuple

## Firewall Bootstrap Support

- Firewall zero-touch deployment capability in Azure and AWS



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

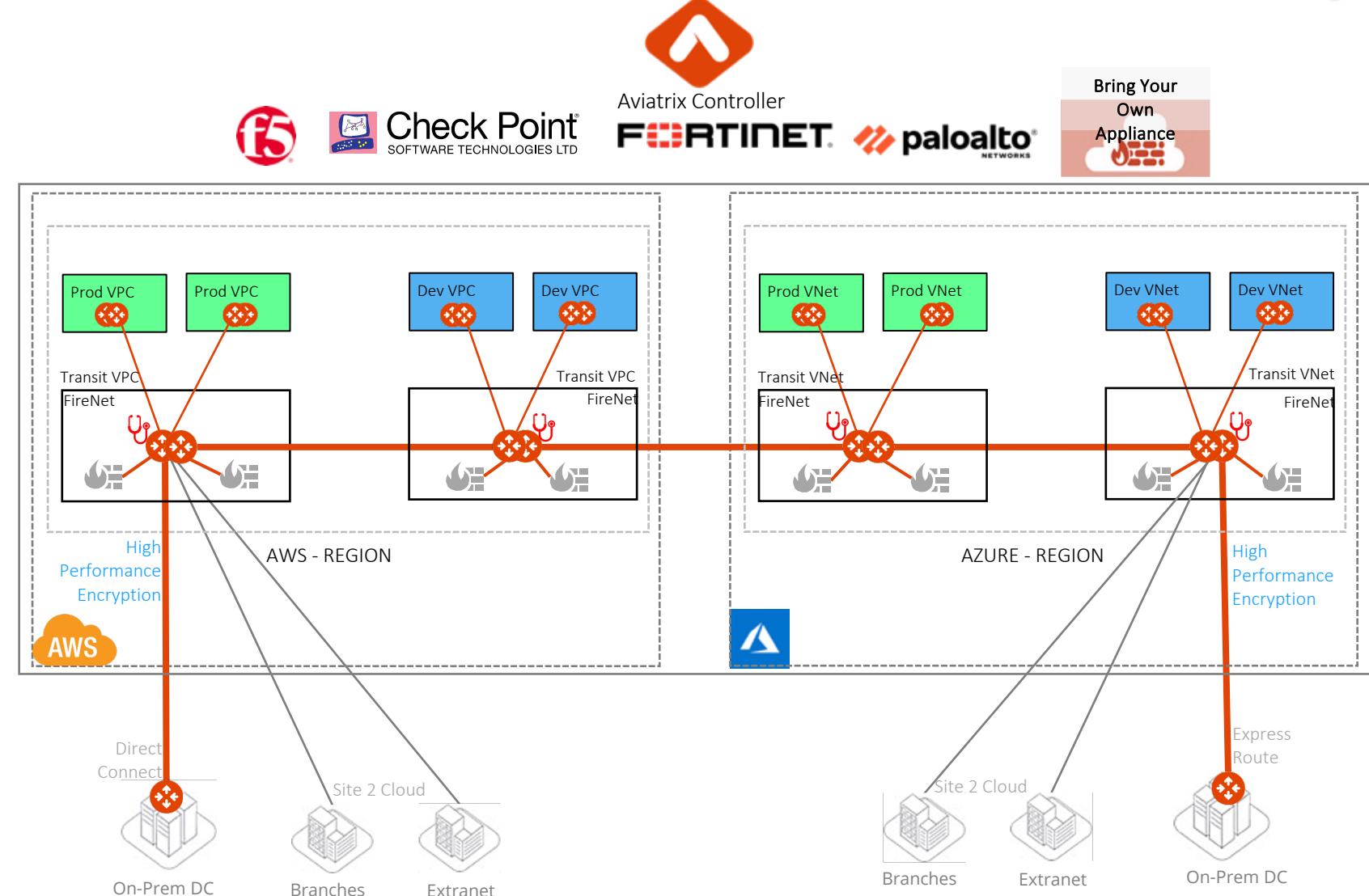


Aviatrix Controller

FORTINET

paloalto<sup>®</sup>  
NETWORKS

Bring Your  
Own  
Appliance





Aviatrix Certified Engineer (ACE)  
<https://aviatrix.com/ACE>



COMMUNITY  
<https://community.aviatrix.com>