



Security Close to the Applications

Aviatrix Distributed Cloud Firewall

Topics Covered

This module will cover two tenants 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

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

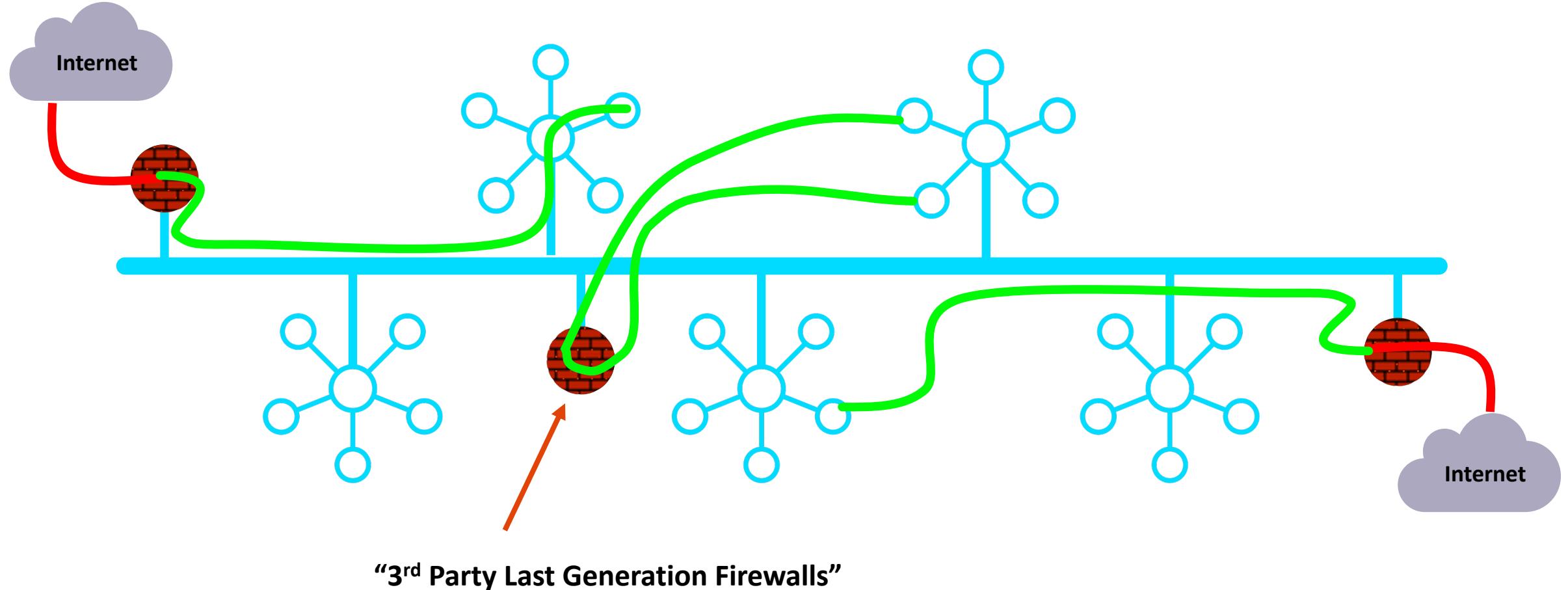
Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture.

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.

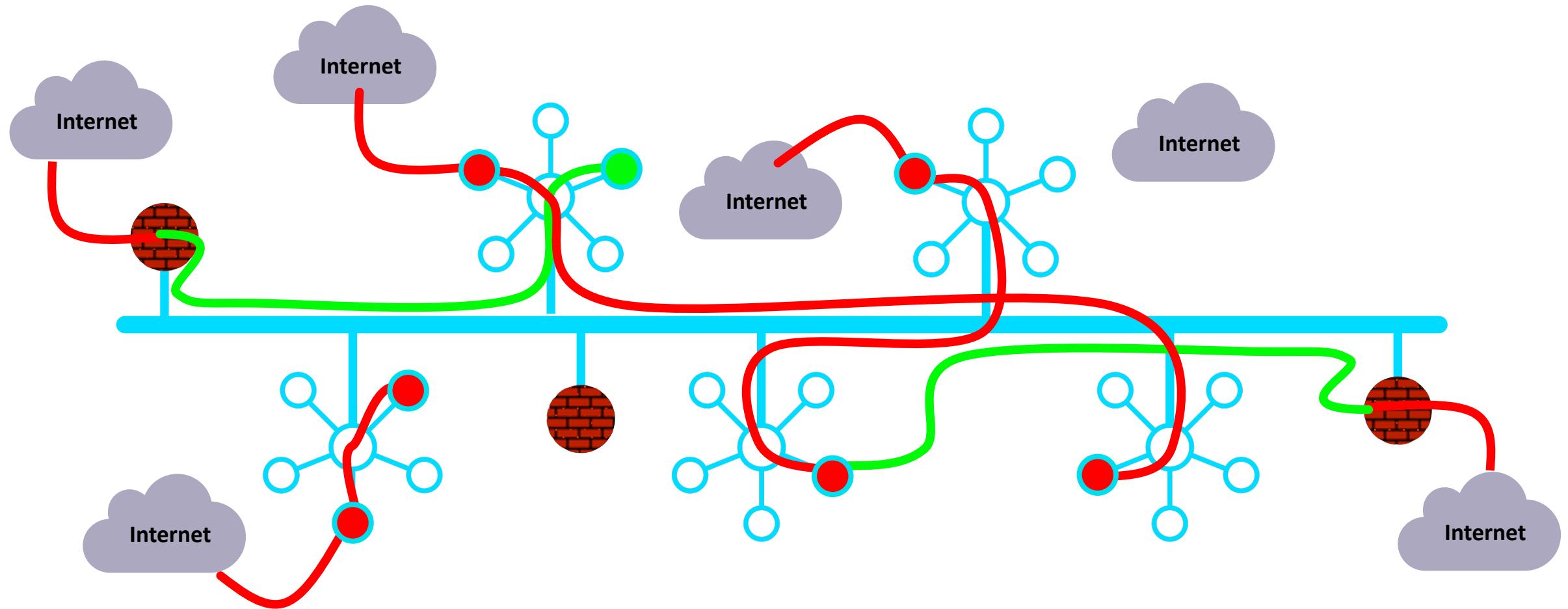
Tenant from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

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.

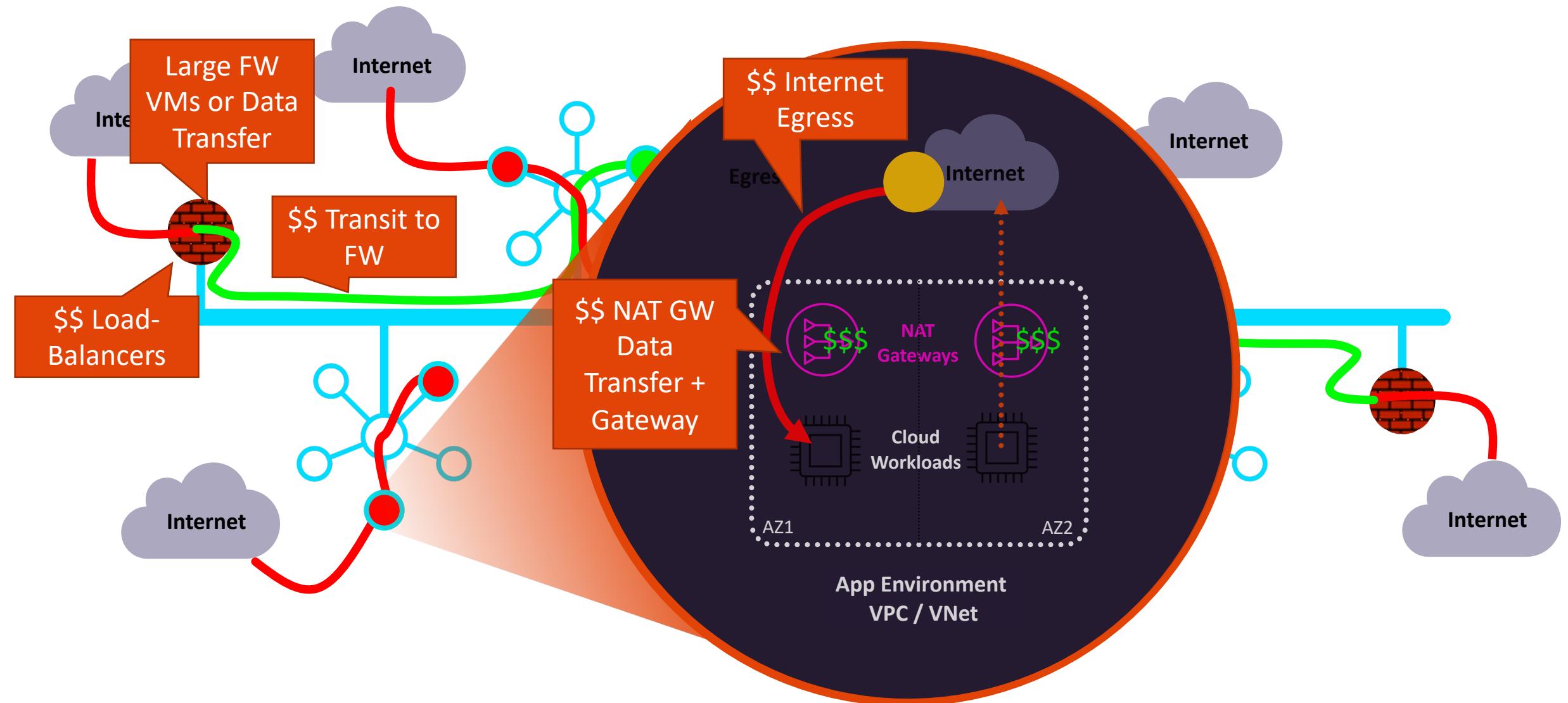
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



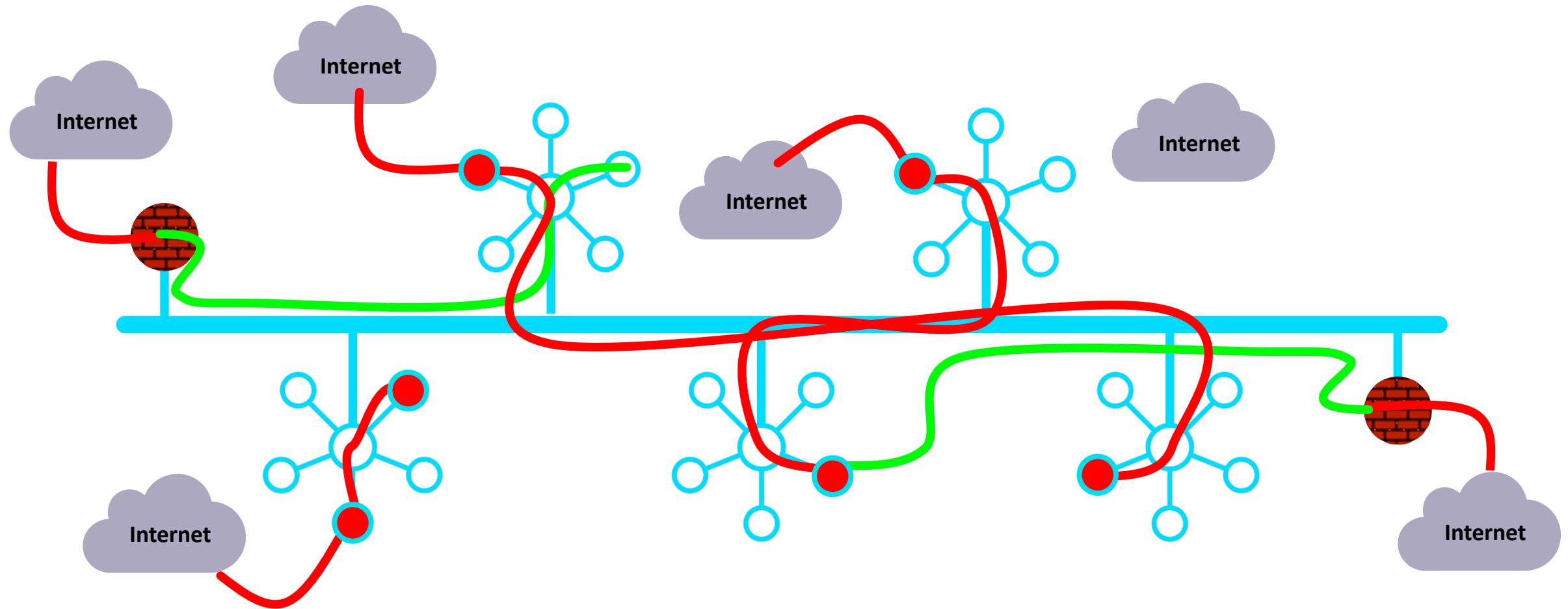
In Reality...



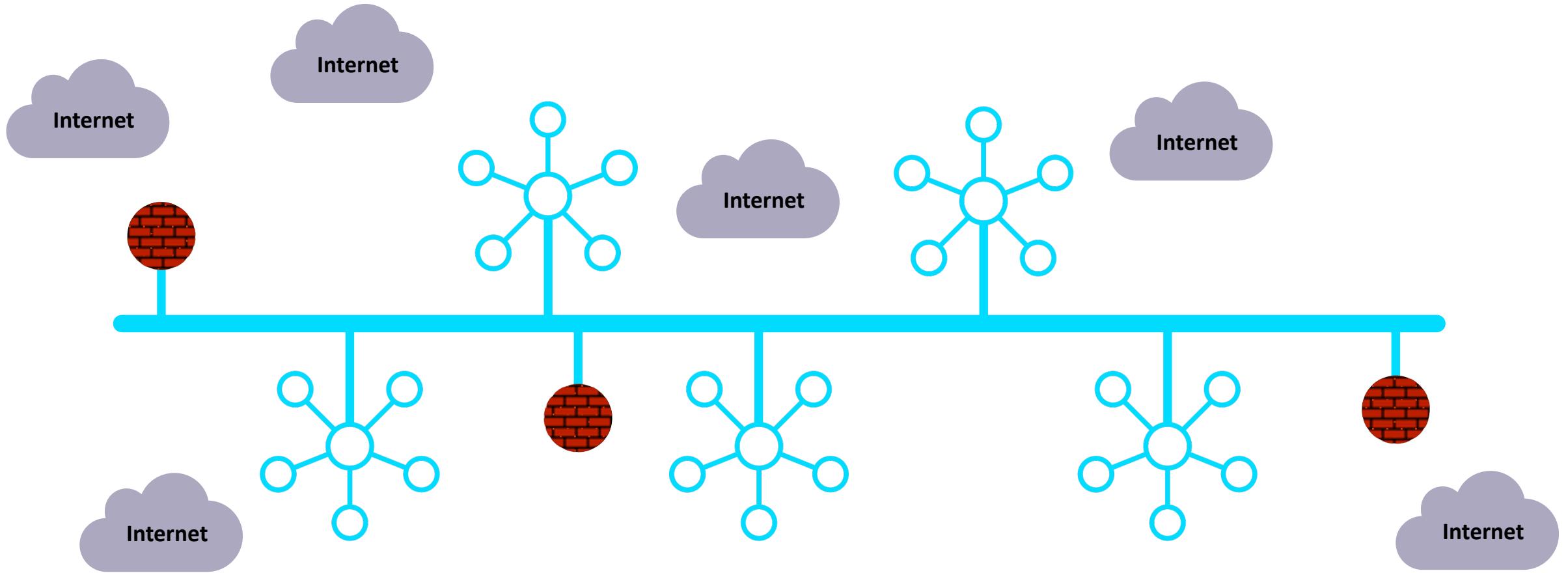
This is bad! Expensive and Lacks Enterprise-Grade Security



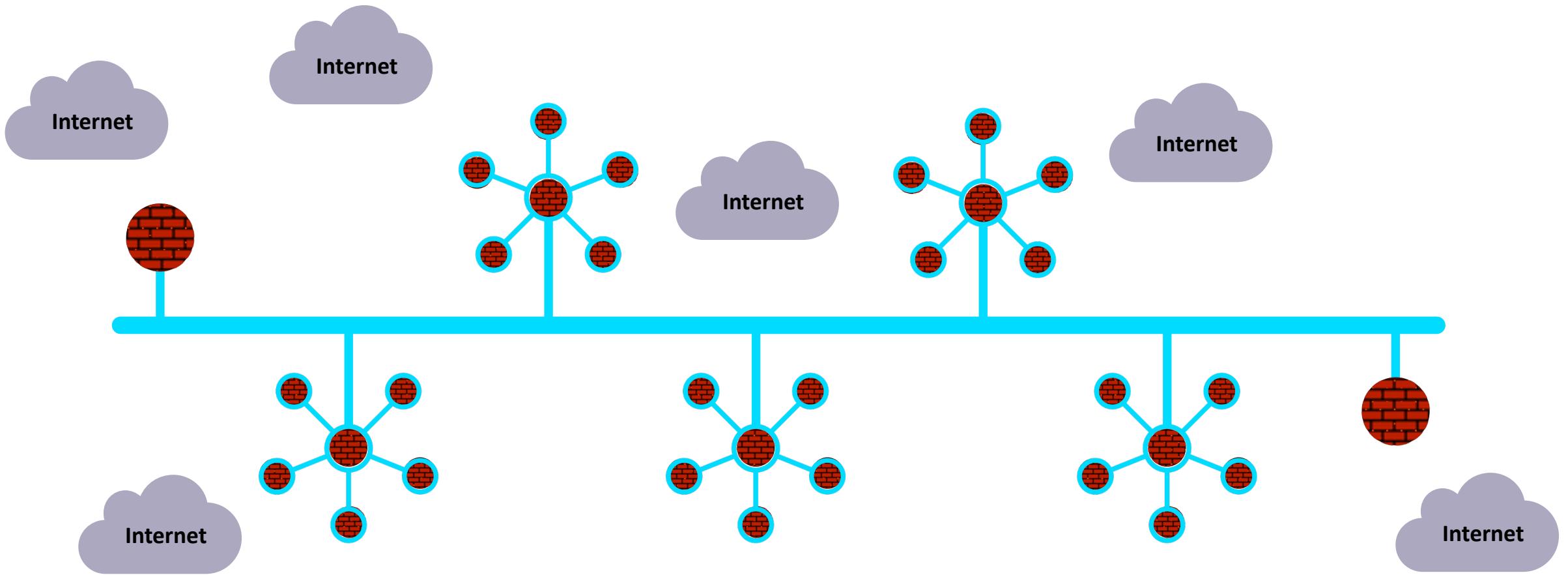
In Reality...



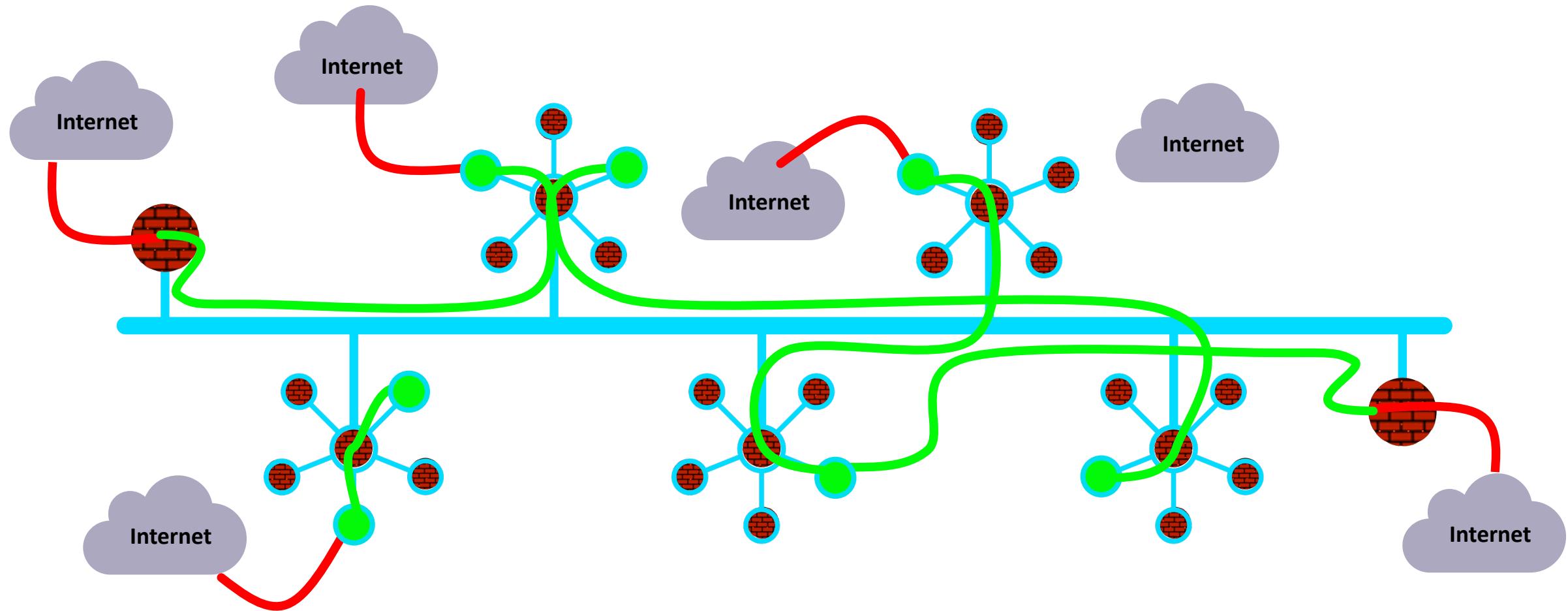
What If...



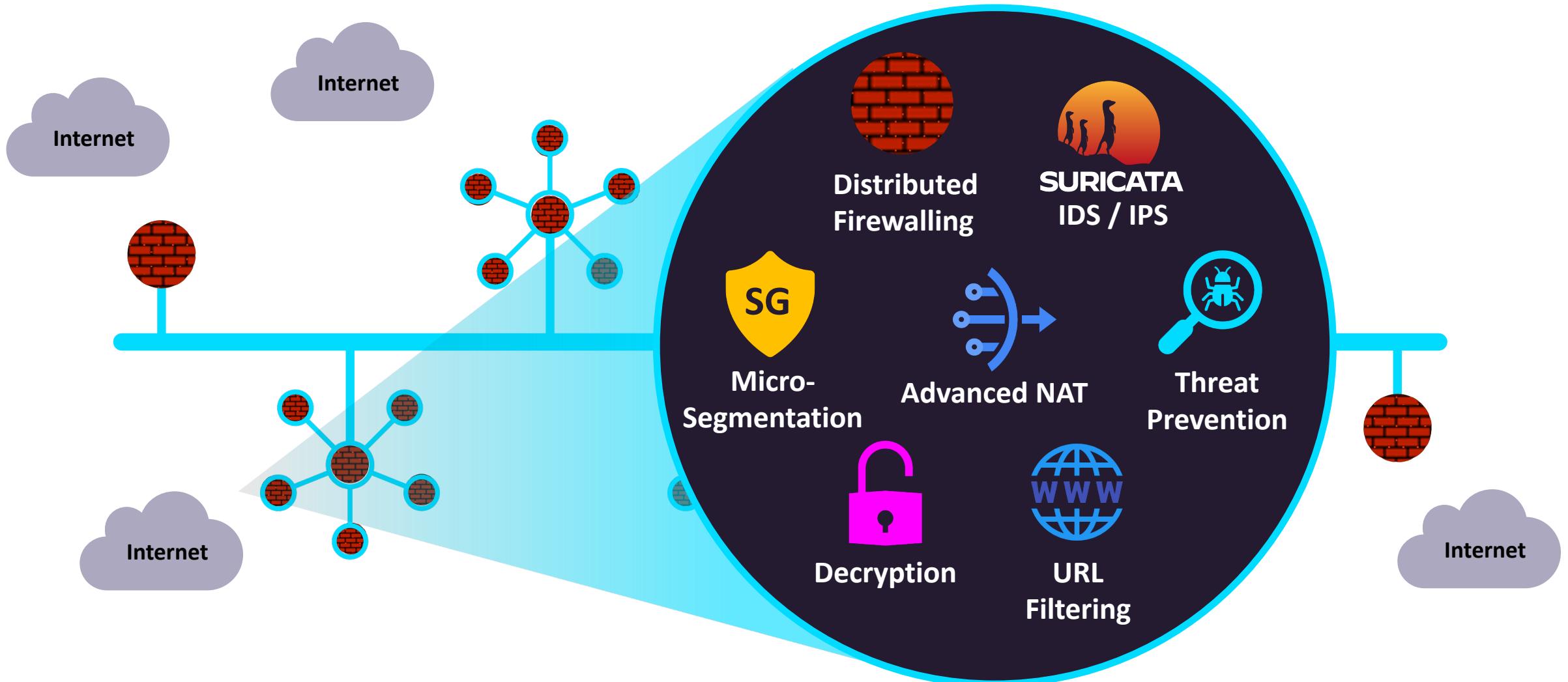
Firewalling Functions were Embedded in the Cloud Network Everywhere...



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 is a dark sidebar with navigation links like Dashboard, AirSpace, Networking, Security, ThreatIQ, Egress, FireNet, and SmartGroups. The main area has tabs for Distributed Firewalling, Rules, Policy Monitor, Detected Intrusions, WebGroups, and Settings. Under Rules, there's a table of rules with columns for Priority, Name, Source, Destination, Action, Decryption, Intrusion Detection, Logging, and Protocol Port. Rule 4 is selected, showing details: Block-Dev-to-Prod, Dev-Workload to Prod-Workload, Any protocol port, Deny action, Decryption off, Intrusion Detection off, Logging off, and Traffic Count 0. Below the table are sections for Source Entities (2) and Destination Entities (1), both listing 'vpc1-workload-0' and 'vpc1-workload-1' respectively. At the bottom, it says 'Total 6 Rules'.

Aviatrix CoPilot

Distributed Enforcement



SURICATA

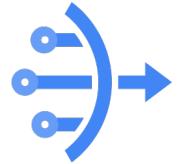
IDS / IPS



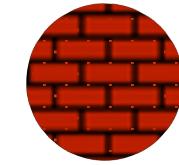
**Micro-
Segmentation**



**Threat
Prevention**



Advanced NAT



**Distributed
Firewalling**

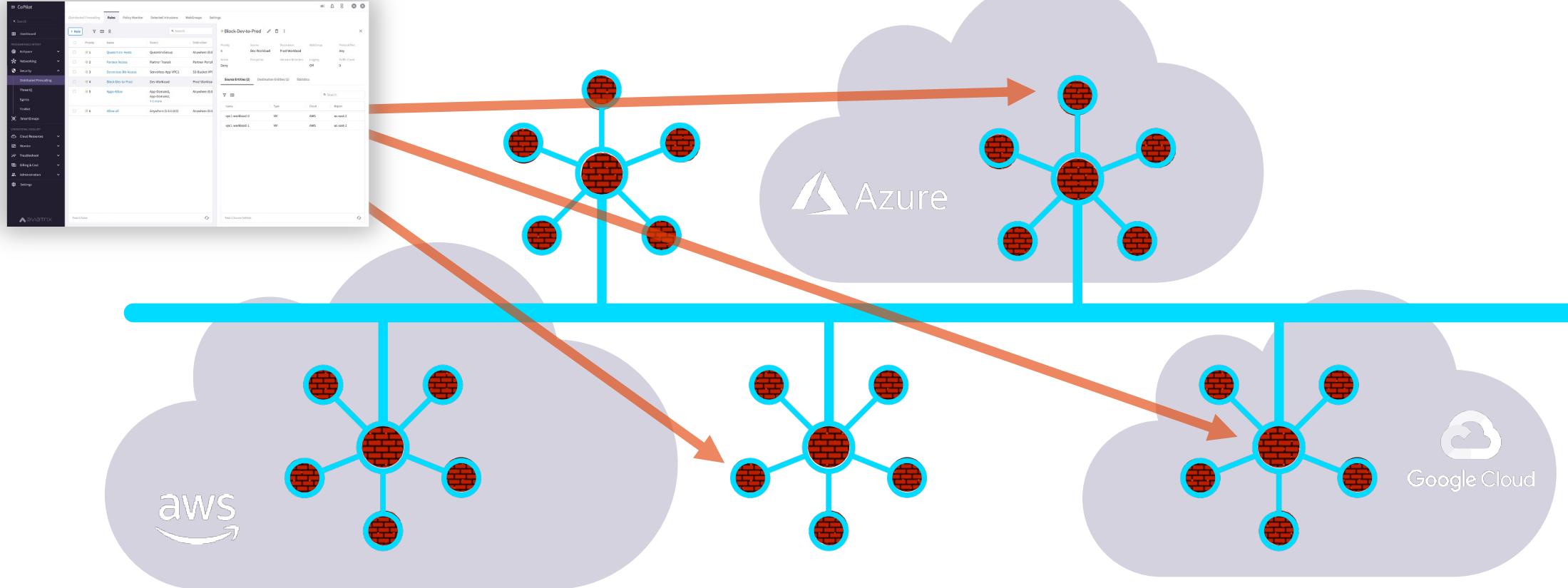


Decryption



**URL
Filtering**

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

The screenshot shows a modal dialog box titled "Distributed Cloud Firewall". Inside the dialog, there is a warning message: "Enabling the Distributed Cloud Firewall **without configured rules will deny all** previously permitted traffic due to its implicit Deny All rule." Below this, another message states: "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." At the bottom of the dialog are two buttons: "Cancel" and "Begin". To the right of the dialog, there is a small illustration of a person in a suit standing next to a briefcase. Below the dialog, a text snippet reads: "Provides granular network security in the cloud, and a centralized policy management across multiple clouds." A large orange arrow points downwards from the "Begin" button towards the "DENY LIST MODEL" section.

The screenshot shows the "Rules" tab of the Distributed Cloud Firewall interface. The table displays a single rule:

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

Protocol
ICMP

Rule Behavior

Action
Deny

SG Orchestration
On

TLS Decryption
Off

Rule Priority

Place Rule
Top

Enforcement Logging

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 ×

Destination SmartGroups

dev ×

WebGroups

Protocol

TCP

Port

80 ×

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

Rule Behavior

Action

Deny

SG Orchestration ○

○ On

TLS Decryption

○ 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		Search
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												
○ ×												
○ ×												

Disabling Distributed Cloud Firewall

Search

Configuration General License Logging Services Private Mode

License Type Universal

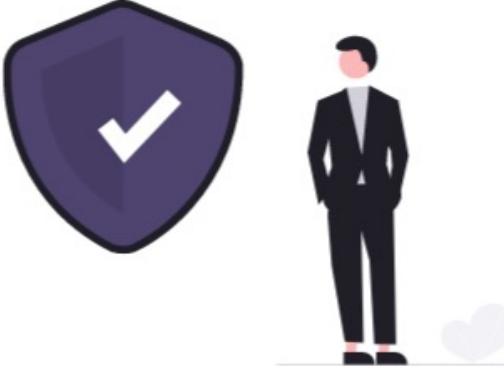
License ID
Lic-1664988

Customer ID
avi.....

Add-on Features

Feature

- Distributed
- CostIQ
- CoPilot AP

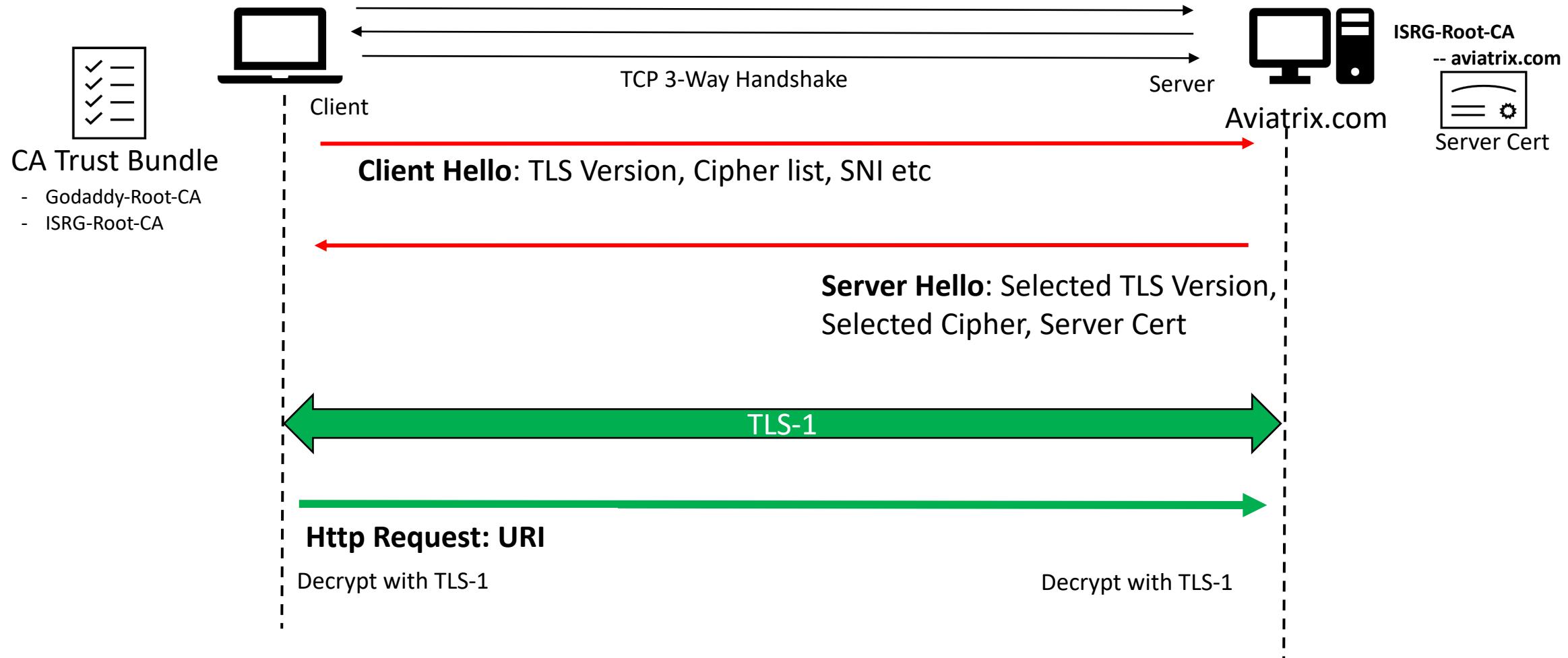
 Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, with a zero-trust architecture and a centralized policy management across multiple clouds.

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

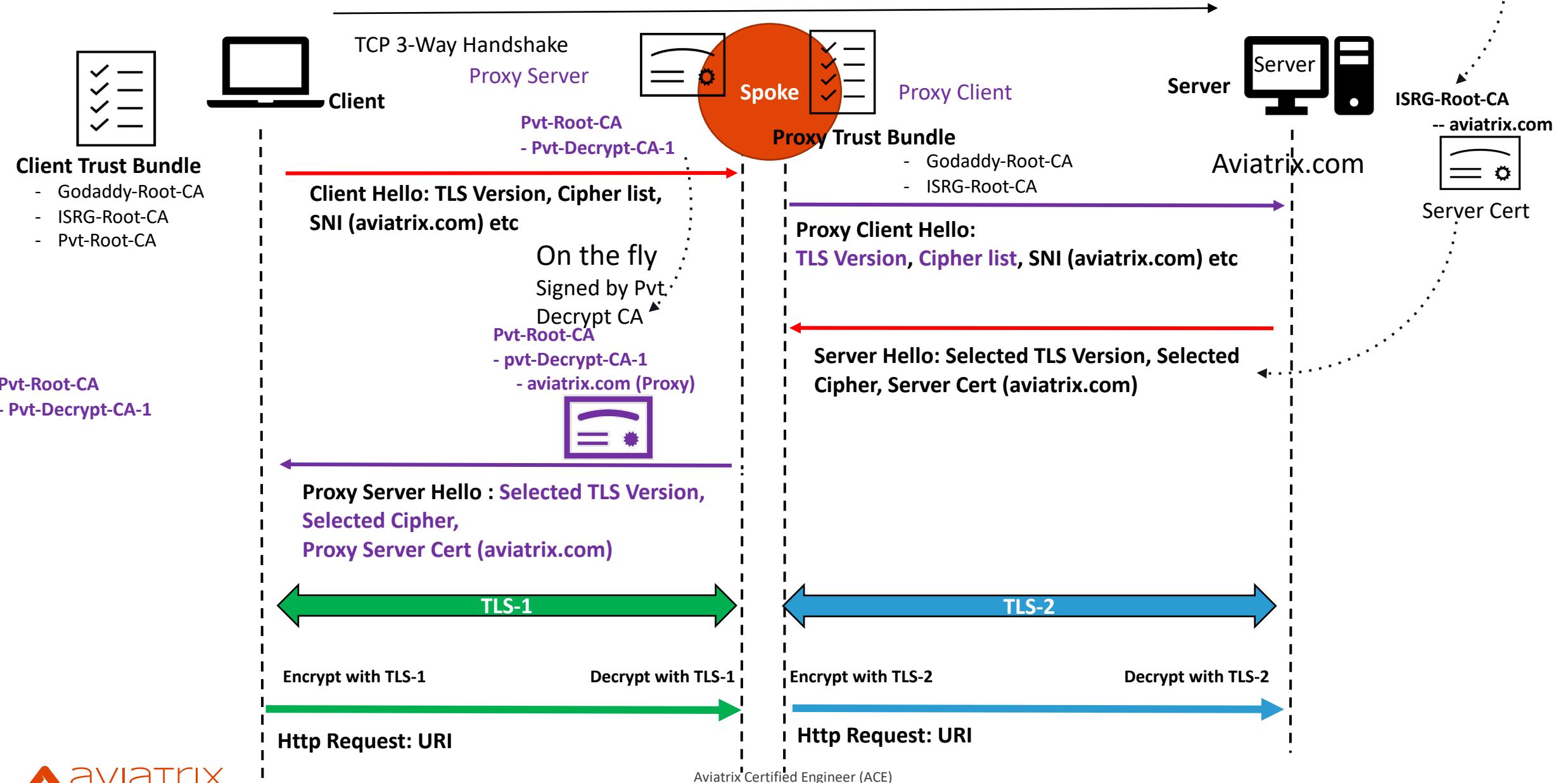
Used by the Client and/or Proxy Gateway to Identify/ Trust the Original Server Cert

Decryption CA Cert

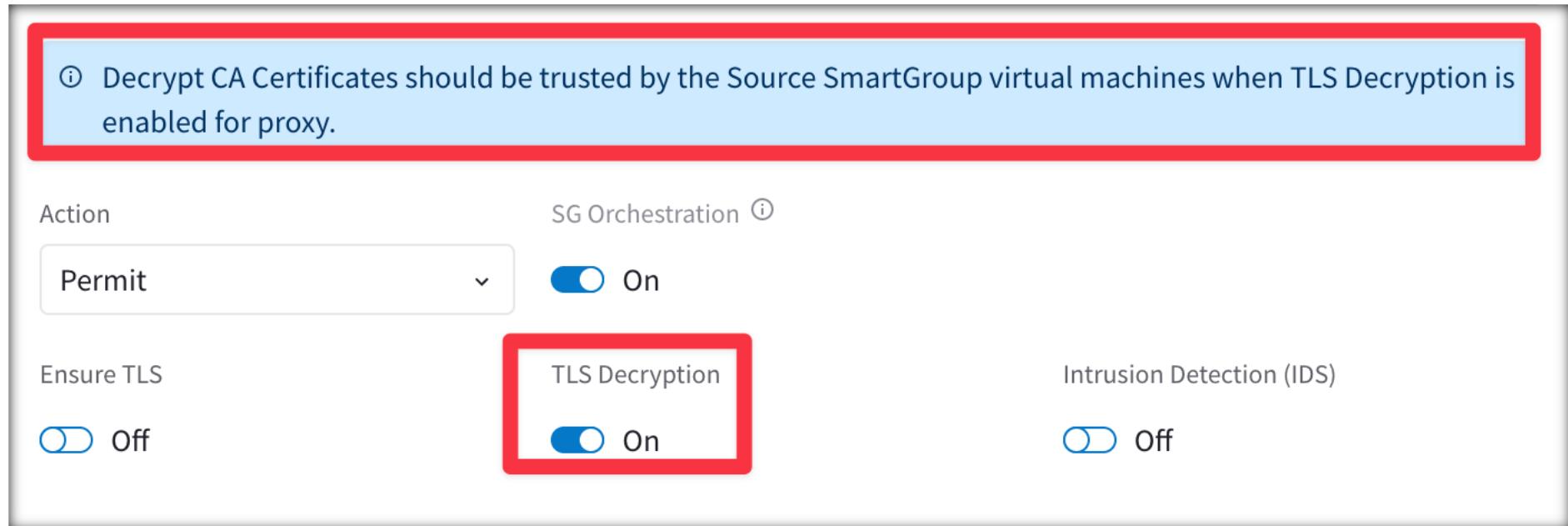
Used by the Decryption/Proxy gateway to generate a new Proxy-Server Cert and Sign it with the Decryption CA Cert

The screenshot shows a 'Certificate Viewer' interface for the domain 'aviatrix.com'. The top navigation bar has tabs for 'General' and 'Details', with 'Details' being the active tab. Below the tabs is a section titled 'Certificate Hierarchy' which shows the chain of trust: 'ISRG Root X1' → 'R3' → 'aviatrix.com'. Under the 'Certificate Fields' section, there are expandable categories: 'Certificate' (Version, Serial Number, Certificate Signature Algorithm, Issuer), 'Validity', 'Subject', and 'Subject Public Key Info'. The 'Field Value' section at the bottom displays the value 'CN = aviatrix.com'.

TLS Decryption: Basic TLS Decryption



TLS Decryption: Decryption CA Cert

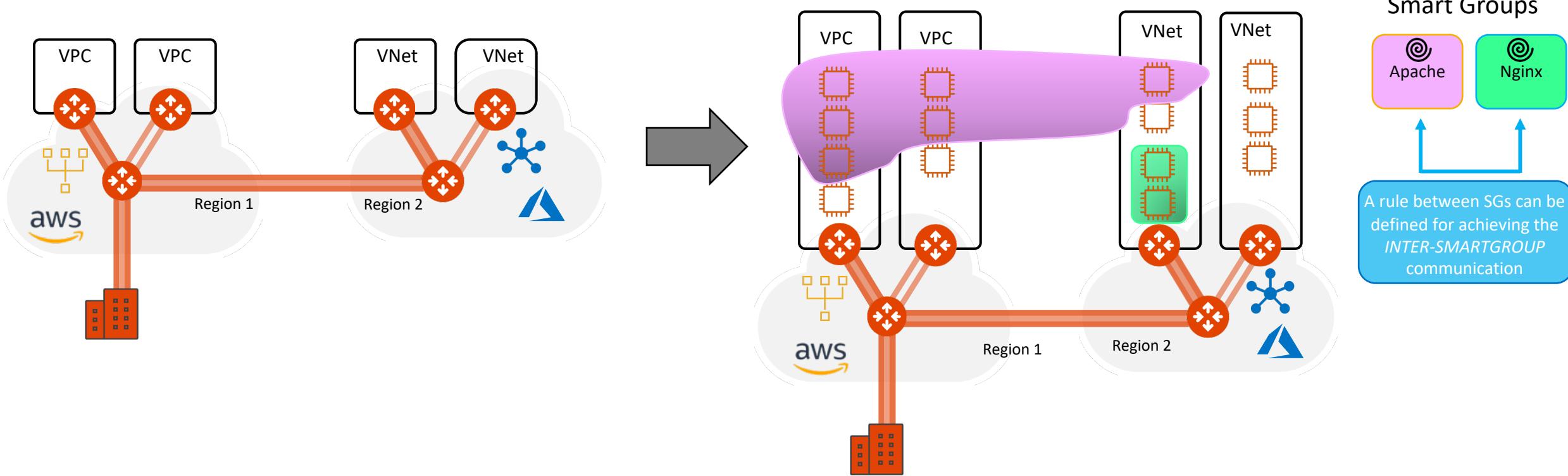


This screenshot shows the "Settings" tab of the "Distributed Cloud Firewall" interface. It includes sections for "Security Group (SG) Orchestration" and "Decryption CA Certificate". The "Decryption CA Certificate" section displays a certificate that expires in 10 years, with a "Renew Certificate" button. Below this is an "Enforcement" dropdown set to "Permissive" and a "Trust Bundle" dropdown set to "default-trustbundle". A red box highlights the "Download Certificate" button, which is also pointed to by a red arrow from the text box on the right.

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

The diagram illustrates the flow of rules between SmartGroups across two regions:

- Region 1:** Contains two VPCs (represented by orange boxes) and a VNet (represented by a large orange box). A purple cloud-like shape covers both VPCs and the VNet.
- Region 2:** Contains a VNet (represented by a large orange box).
- SmartGroup Apache:** Represented by a pink rounded rectangle. It is associated with the VPCs in Region 1 and the VNet in Region 2.
- SmartGroup Nginx:** Represented by a green rounded rectangle. It is associated with the VNet in Region 2.
- SmartGroup Nginx → SmartGroup Apache:** A green arrow points from the Nginx SmartGroup to the Apache SmartGroup, indicating an inter-SmartGroup rule.
- SmartGroup Apache → SmartGroup Apache:** A pink arrow points from the Apache SmartGroup back to itself, indicating an intra-SmartGroup rule.

Create Rule Screenshots:

- SmartGroup Apache (Intra-Rule):** Shows a rule named "INTRACLICMP-APACHE" with Source SmartGroups set to APACHE and Destination SmartGroups set to APACHE. Protocol is ICMP, Action is Permit, SG Orchestration is On, and Enforcement is Off.
- SmartGroup Nginx (Intra-Rule):** Shows a rule named "INTRACLICMP-NGINX" with Source SmartGroups set to NGINX and Destination SmartGroups set to NGINX. Protocol is ICMP, Action is Permit, SG Orchestration is On, and Enforcement is Off.
- SmartGroup Nginx → SmartGroup Apache (Inter-Rule):** Shows a rule named "INTERCLICMP-NGINX-APACHE" with Source SmartGroups set to NGINX and Destination SmartGroups set to APACHE. Protocol is ICMP, Action is Permit, SG Orchestration is On, and Enforcement is Off.

Distributed Cloud Firewall Rules Table:

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	Decryption
1	INTRACLICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
2	INTRACLICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
3	INTERCLICMP-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		

Buttons at the bottom of the rules table:

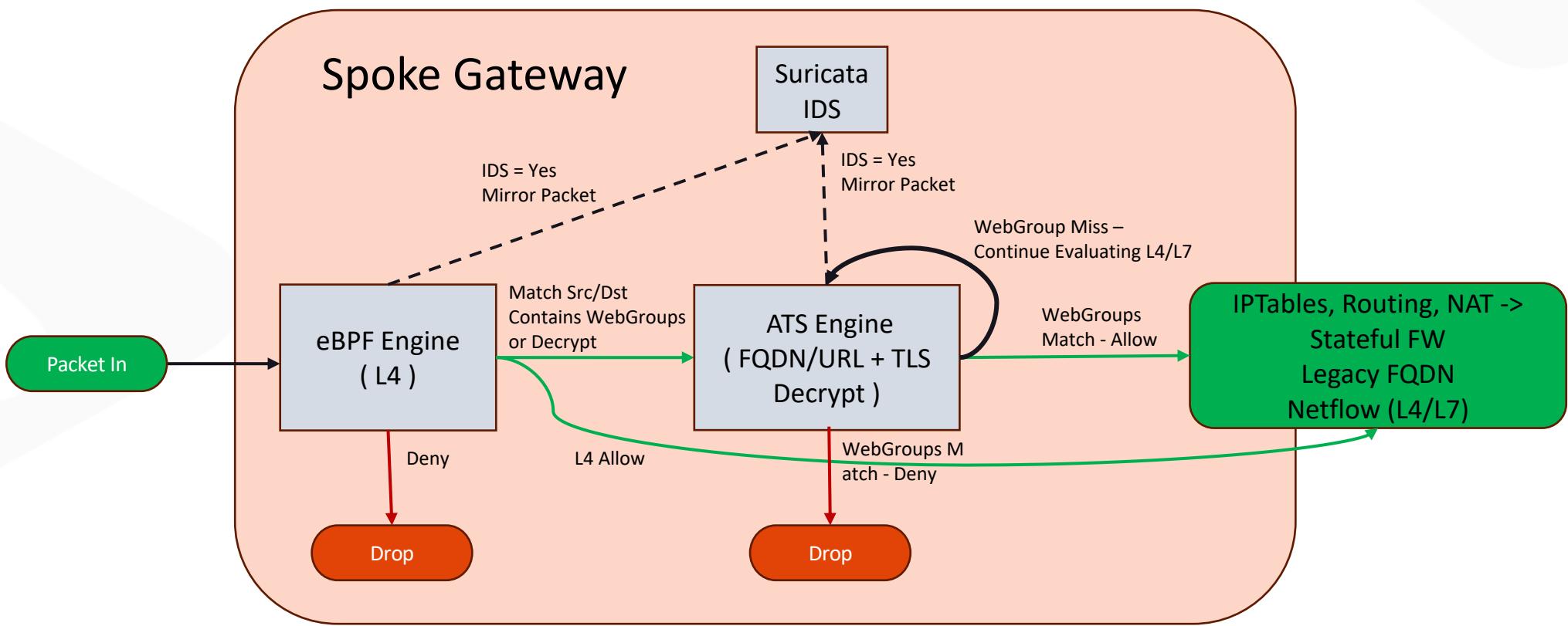
- 4 New
- 1 Modified
- Discard** (Red box)
- Commit** (Blue box)

List of key points:

- 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

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)



3rd Party Firewall Service Insertion (Aviatrix FireNet)

Centralized model

Use as necessary

Aviatrix FireNet For 3rd 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

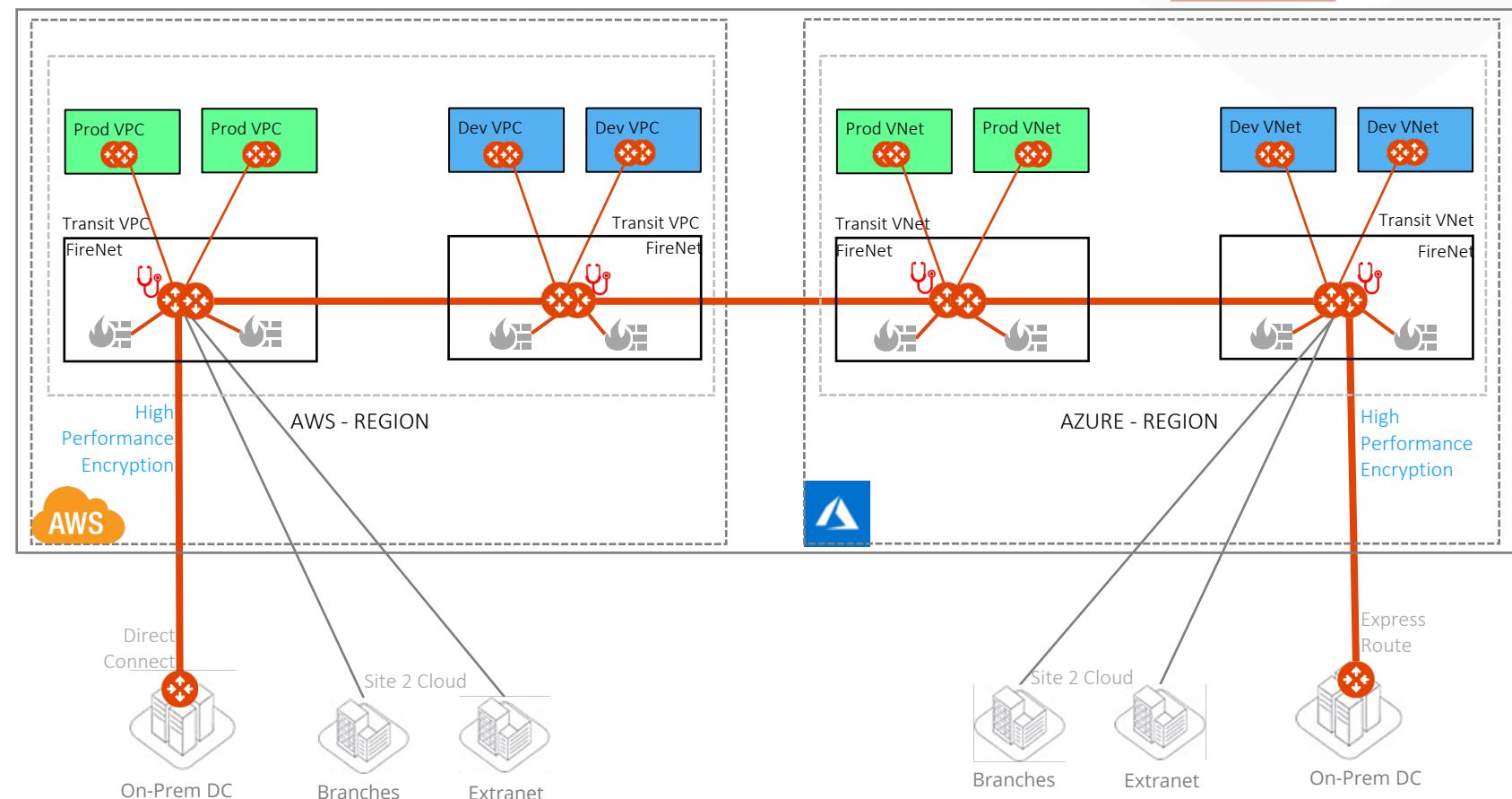


Aviatrix Controller

FORTINET

paloalto
NETWORKS

Bring Your
Own
Appliance





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



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