Distributed Cloud Firewall & FireNet

AVIATRIX DISTRIBUTED CLOUD FIREWALL

ACE Solutions Architecture Team

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

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.

Related Aviatrix Features

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

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.

Use Cases:

Zero Trust Network Access (Cloud Firewalling

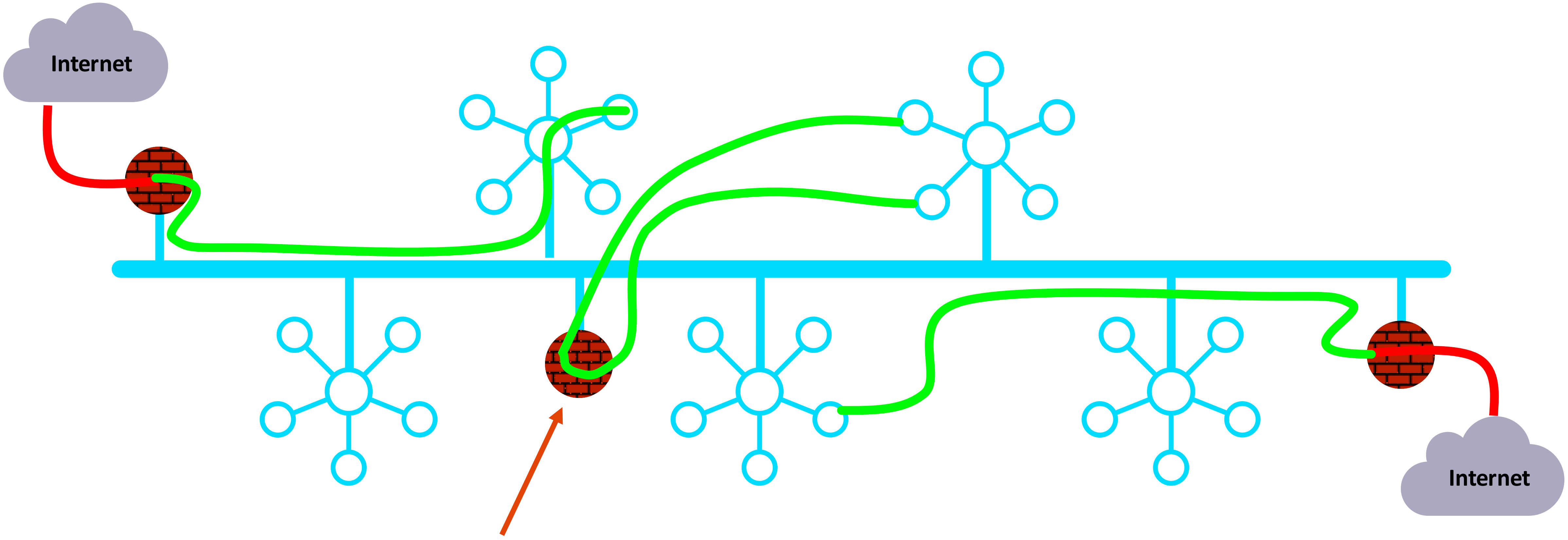
Secure B2B Connectivity

Secure High-Performance Data Connectivity for LLMS

Secure High-Performance Datacenter Edge

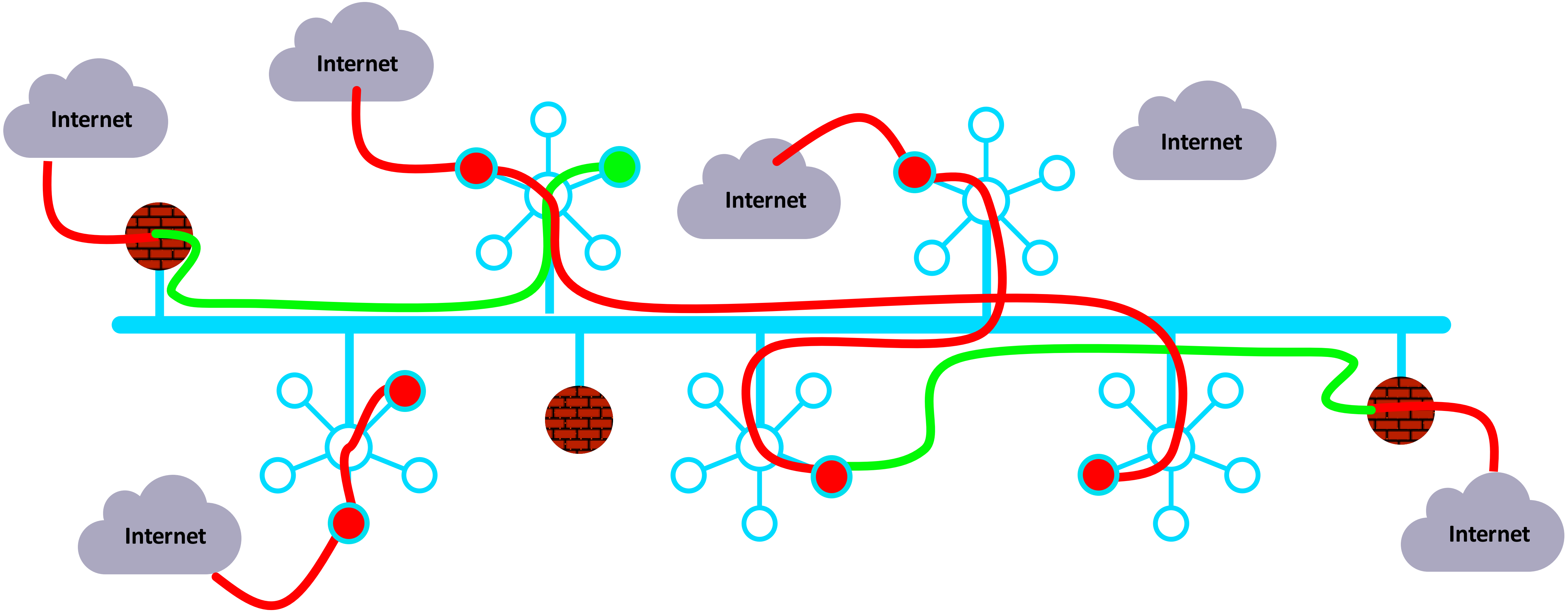
Cloud Visibility and Tooling

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

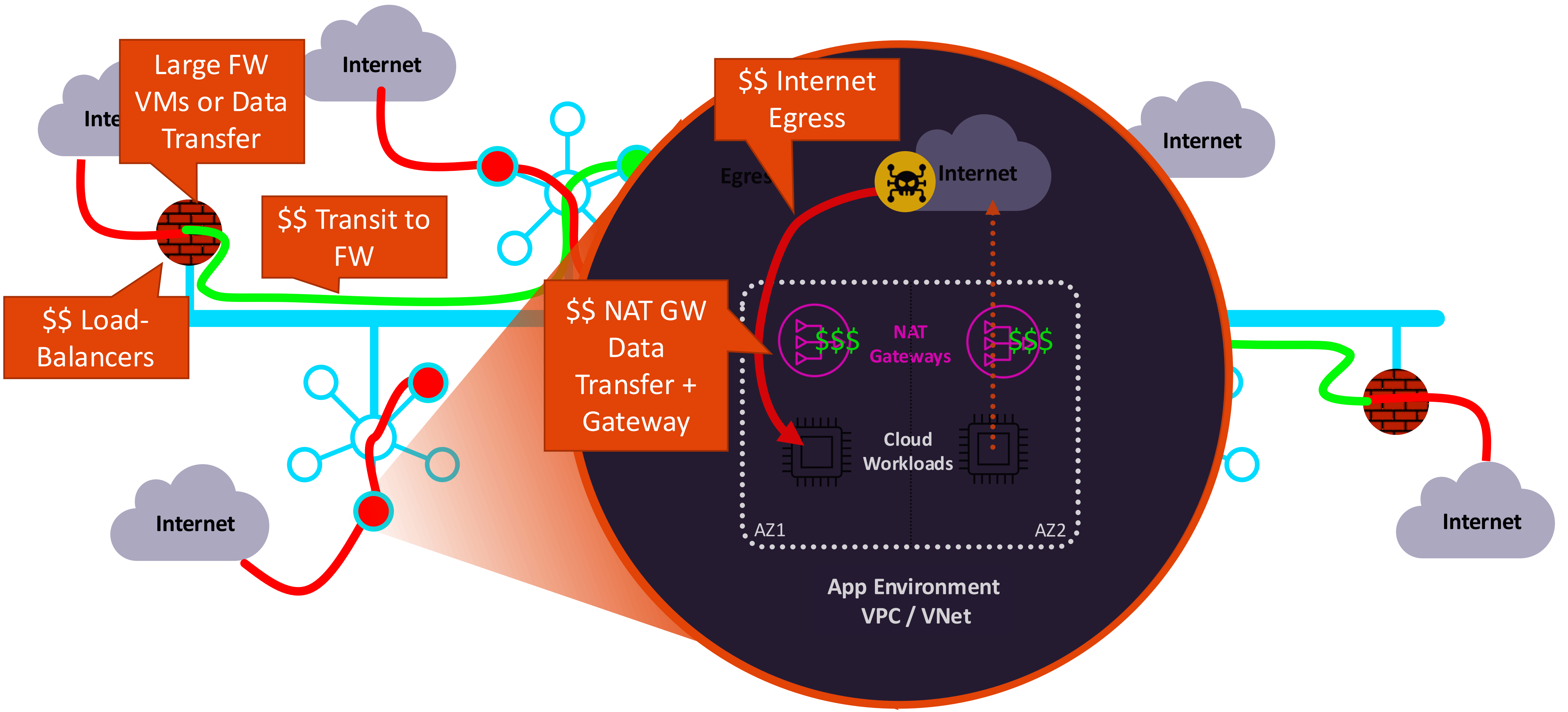


"3rd Party Last Generation Firewalls"

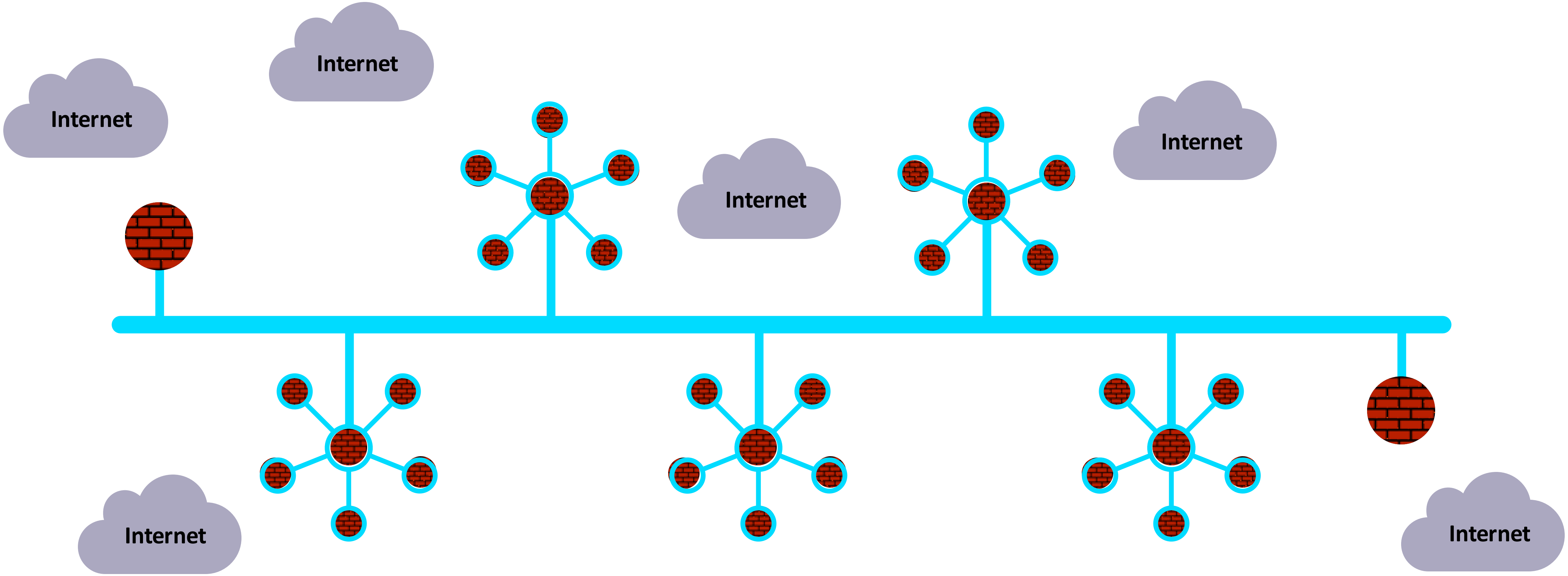
In Reality…


Internet
Internet
Internet
Internet
Internet
Internet
Internet

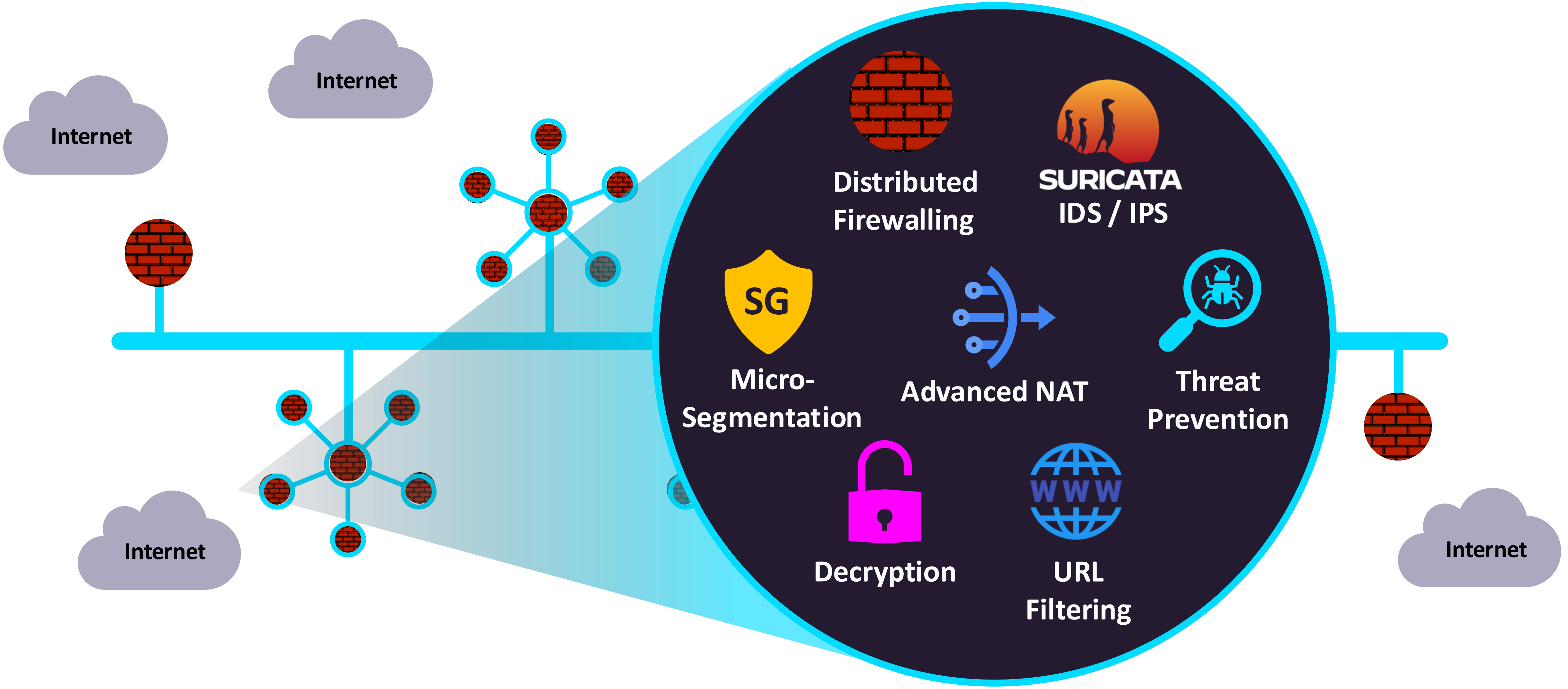
This is bad! Expensive and Lacks Enterprise-Grade Security



Firewalling Functions were Embedded in the Cloud Network Everywhere…

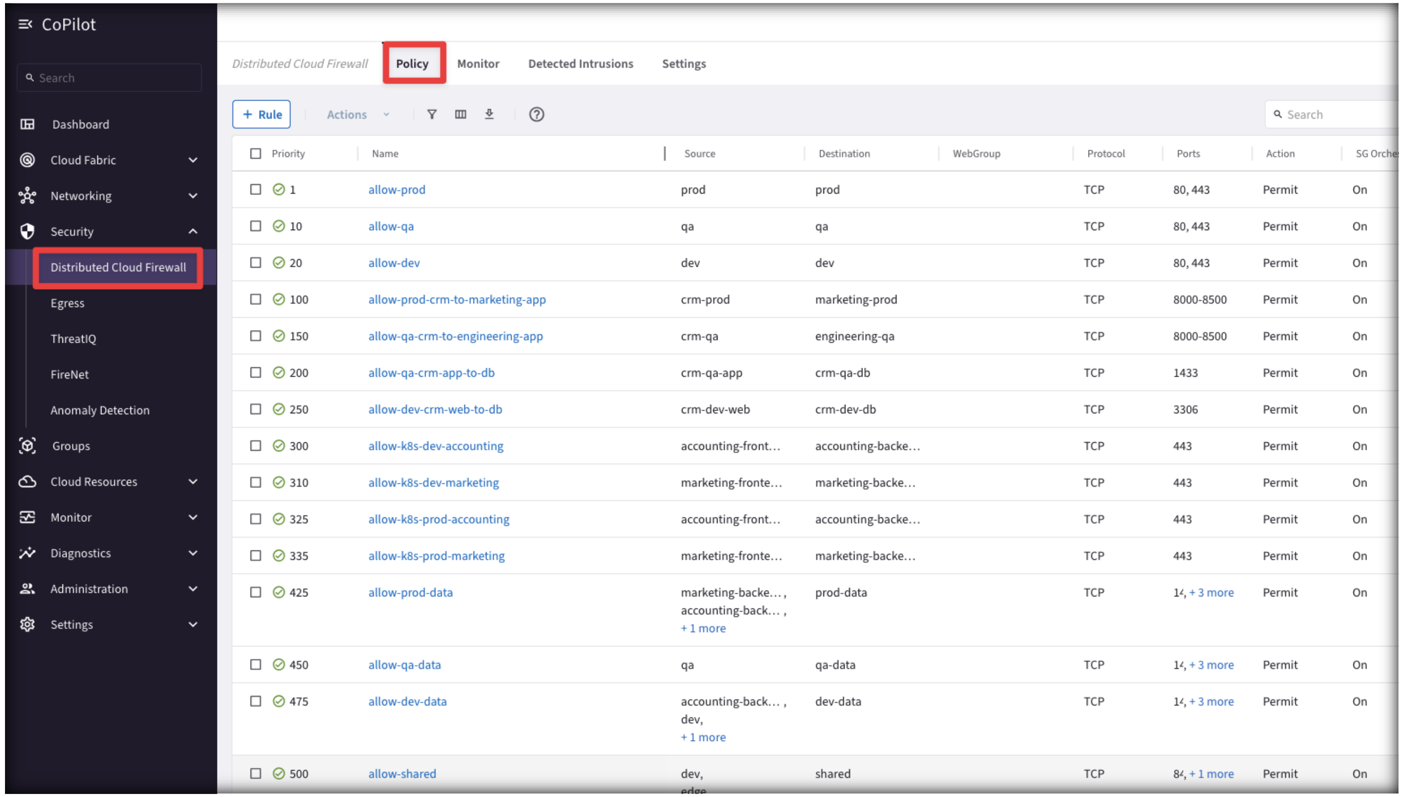


And, What If it was more than just firewalling…



And, What If Policy Creation Looked Like One Big Firewall…

Centralized Policy Creation → Distributed Enforcement



☐ Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orche
☐ ✓ 1	allow-prod	prod	prod		TCP	80, 443	Permit	On
☐ ✓ 10	allow-qa	qa	qa		TCP	80, 443	Permit	On
☐ ✓ 20	allow-dev	dev	dev		TCP	80, 443	Permit	On
☐ ✓ 100	allow-prod-crm-to-marketing-app	crm-prod	marketing-prod		TCP	8000-8500	Permit	On
☐ ✓ 150	allow-qa-crm-to-engineering-app	crm-qa	engineering-qa		TCP	8000-8500	Permit	On
☐ ✓ 200	allow-qa-crm-app-to-db	crm-qa-app	crm-qa-db		TCP	1433	Permit	On
☐ ✓ 250	allow-dev-crm-web-to-db	crm-dev-web	crm-dev-db		TCP	3306	Permit	On
☐ ✓ 300	allow-k8s-dev-accounting	accounting-front…	accounting-backe…		TCP	443	Permit	On
☐ ✓ 310	allow-k8s-dev-marketing	marketing-fronte…	marketing-backe…		TCP	443	Permit	On
☐ ✓ 325	allow-k8s-prod-accounting	accounting-front…	accounting-backe…		TCP	443	Permit	On
☐ ✓ 335	allow-k8s-prod-marketing	marketing-fronte…	marketing-backe…		TCP	443	Permit	On
☐ ✓ 425	allow-prod-data	marketing-backe… , accounting-back… , + 1 more	prod-data		TCP	14, + 3 more	Permit	On
☐ ✓ 450	allow-qa-data	qa	qa-data		TCP	14, + 3 more	Permit	On
☐ ✓ 475	allow-dev-data	accounting-back… , dev, + 1 more	dev-data		TCP	14, + 3 more	Permit	On
☐ ✓ 500	allow-shared	dev, edge	shared		TCP	84, + 1 more	Permit	On

IDS / IPS

NSG

Micro-Segmentation

Threat Prevention

WWW

Distributed Firewalling

URL Filtering

Decryption

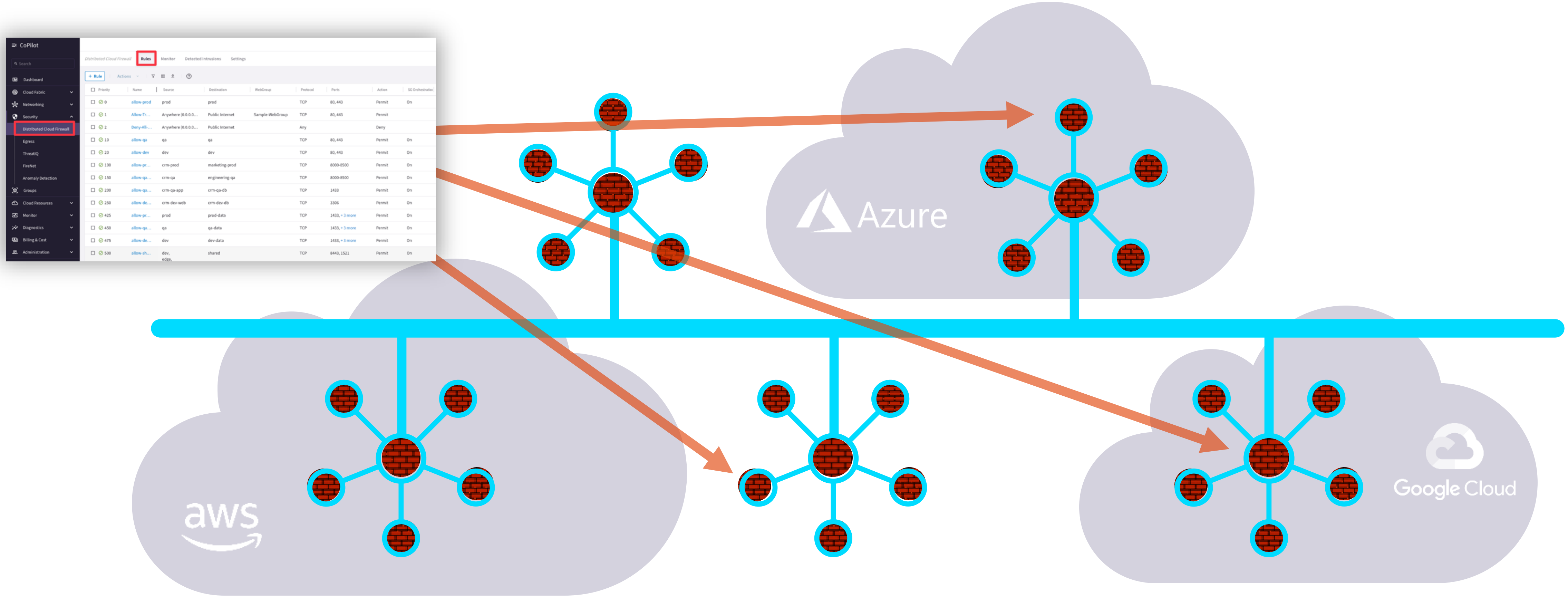
Advanced NAT

Aviatrix CoPilot

Aviatrix Spoke & Secure Edge

aviatrix

A Distributed Cloud Firewall…



☐	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestratio
☐	✓ 0	allow-prod	prod	prod		TCP	80, 443	Permit	On
☐	✓ 1	Allow-Tr…	Anywhere (0.0.0.0…	Public Internet	Sample-WebGroup	TCP	80, 443	Permit	
☐	✓ 2	Deny-All-…	Anywhere (0.0.0.0…	Public Internet		Any		Deny	
☐	✓ 10	allow-qa	qa	qa		TCP	80, 443	Permit	On
☐	✓ 20	allow-dev	dev	dev		TCP	80, 443	Permit	On
☐	✓ 100	allow-pr…	crm-prod	marketing-prod		TCP	8000-8500	Permit	On
☐	✓ 150	allow-qa…	crm-qa	engineering-qa		TCP	8000-8500	Permit	On
☐	✓ 200	allow-qa…	crm-qa-app	crm-qa-db		TCP	1433	Permit	On
☐	✓ 250	allow-de…	crm-dev-web	crm-dev-db		TCP	3306	Permit	On
☐	✓ 425	allow-pr…	prod	prod-data		TCP	1433, + 3 more	Permit	On
☐	✓ 450	allow-qa…	qa	qa-data		TCP	1433, + 3 more	Permit	On
☐	✓ 475	allow-de…	dev	dev-data		TCP	1433, + 3 more	Permit	On
☐	✓ 500	allow-sh…	dev, edge,	shared		TCP	8443, 1521	Permit	On

Where and How Policies Are Enforced Is Abstracted…

AVIATRIX

ACE

SECURITY

SPECIALTY

3rd Party Firewall Service Insertion (Aviatrix FireNet)

Centralized model

Use as necessary

Aviatrix FireNet For 3rd Party FW Service Insertion/Chaining

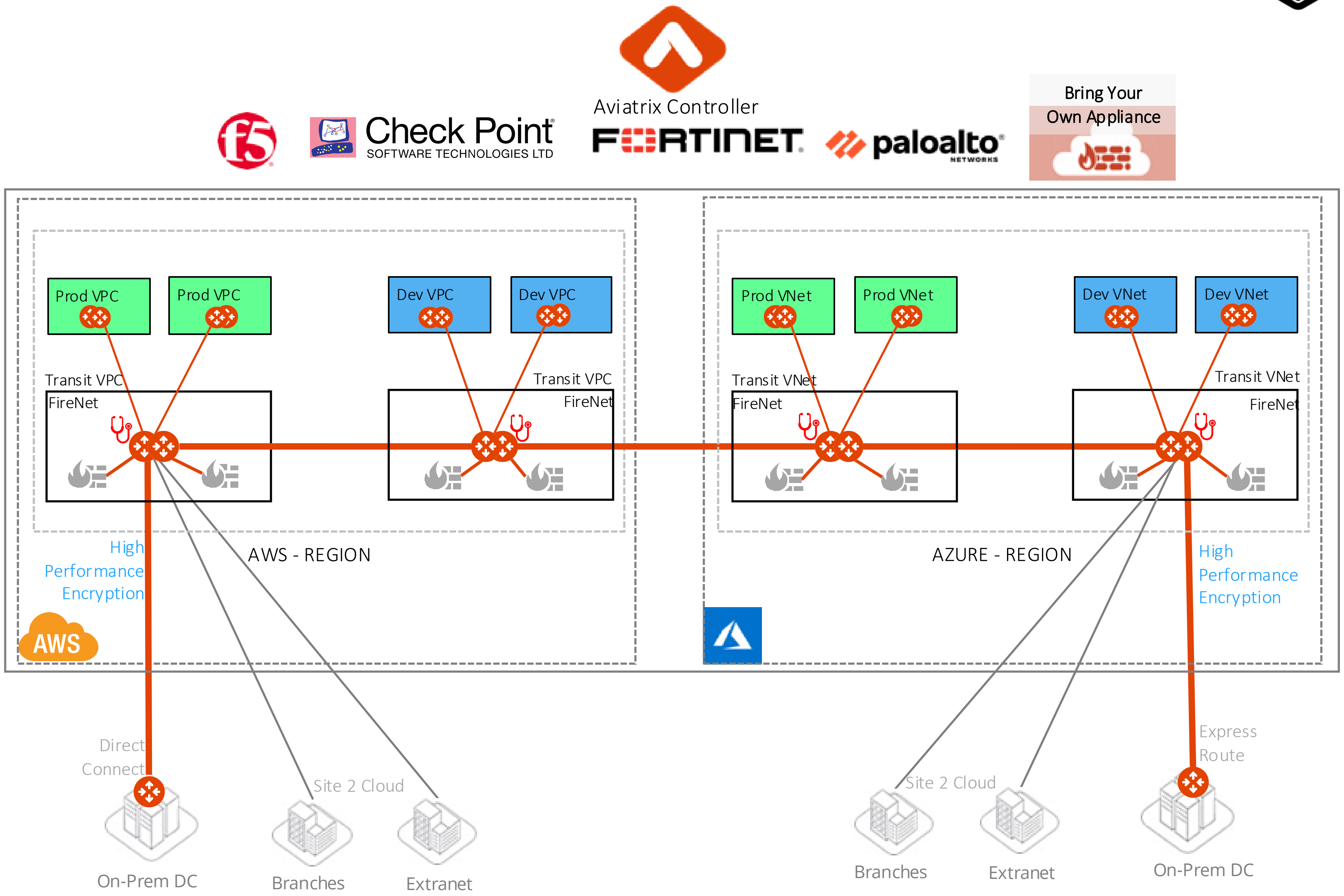
Firewall Service Insertion
- E-W / Egress / Ingress / all traffic
- High Performance Encryption (HPE)
- Active / Active – Across AZs
- No IPsec / No BGP / No SNAT required

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
ACE
SECURITY
SPECIALTY

Next: Micro-Segmentation