

Architecting Hybrid Multi-Cloud Infrastructures

cisco Live !

Brenden Buresh, CCIE #2073
Distinguished Solutions Engineer

Session ID: BRKDCN-2916

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://cislive.ciscoevents.com/cislivebot/#BRKDCN-2916>

Agenda

- 01 **Current Challenges, Issues**
- 02 **Key Capabilities**
- 03 **Connecting Users+Devices+Things**
- 04 **Applications behind SD-WAN**
- 05 **Common Policy**
- 06 **Visibility / Day2 Operations**
- 07 **Summary**

Session Focus Areas

Cloud continues to be a major workload placement option; customers have been on the Cloud Journey for several years.

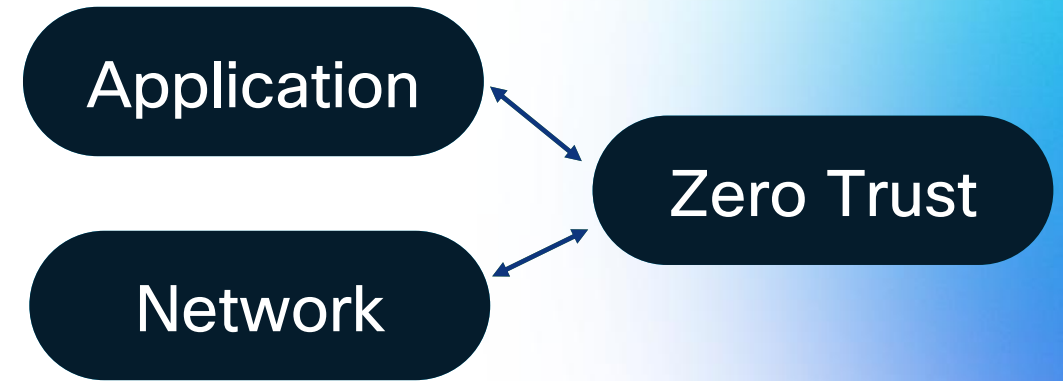
- Architectural trends impacting hybrid and multicloud infrastructures.
- Why private data centers and applications remain critical, even as applications and data move from traditional private data centers to public clouds.

How to:

- Address growing demands of users and applications being everywhere in a secure multi-cloud world.
- Help you optimize and understand traffic flows, operational efficiencies, and visibility in a multi-cloud world.

Goals of today's session

- Explore top challenges and discuss relevant use cases
- Provide a deeper understanding of current Cloud Networking deployment options
- Offer practical guidance on how best to deliver:
 - A consistent Cloud Networking, Segmentation, and Security solution
 - Visibility across entire solutions – including in-region, intra-region and inter-cloud connectivity options visibility



Taxonomy

- Hybrid-Cloud: Public Cloud and Private Cloud
- Multi-Cloud*: Hybrid-Cloud + 2 or more Cloud Providers (CSP)
- East / West Traffic Flows within (intra) across Cloud Regions/Branches
- North / South Traffic Flows across (inter) Clouds and on-prem Data Centers as well as user to app flows

We will be using AWS terminology but applies to other CSPs:

- IGW: Internet Gateway
- DX Gateway: Direct Connect Gateway
- TGW: Transit Gateway
- VPC: Virtual Private Cloud

*Multi-Cloud and Multicloud are used interchangeably in this session

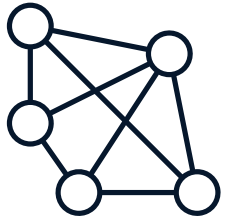
Cloud Terminology Matrix



Area	AWS service	Azure service	GCP Service
Cloud virtual networking	<u>Virtual Private Cloud (VPC)</u>	<u>Virtual Network (VNet)</u>	<u>Virtual Private Cloud (VPC)</u>
NAT gateways	<u>NAT Gateways</u>	<u>Virtual Network NAT</u>	<u>Cloud NAT</u>
Cross-premises connectivity	<u>VPN Gateway</u>	<u>VPN Gateway</u>	<u>Cloud VPN Gateway</u>
DNS management	<u>Route 53</u>	<u>DNS</u>	<u>Cloud DNS</u>
DNS-based routing	<u>Route 53</u>	<u>Traffic Manager</u>	<u>Cloud DNS</u>
Dedicated network	<u>Direct Connect</u>	<u>ExpressRoute</u>	<u>Cloud Interconnect</u>
Load balancing	<u>Network Load Balancer</u>	<u>Load Balancer</u>	<u>Network Load Balancing</u>
Application-level load balancing	<u>Application Load Balancer</u>	<u>Application Gateway</u>	<u>Global Load Balancing</u>
Route table	<u>Custom Route Tables</u>	<u>User Defined Routes</u>	<u>Routes</u>
Private link	<u>PrivateLink</u>	<u>Azure Private Link</u>	<u>Private Service Connect</u>
Private PaaS connectivity	<u>VPC endpoints</u>	<u>Private Endpoint</u>	<u>Private Service Connect</u>
Virtual network peering	<u>VPC Peering</u> <u>Transit Gateway</u>	<u>VNet Peering</u>	<u>VPC Network Peering</u>
Content delivery networks	<u>Cloud Front</u>	<u>Azure CDN</u>	<u>Cloud CDN</u>
Network Monitoring	<u>VPC Flow Logs</u>	<u>Azure Network Watcher</u>	<u>Network Intelligence Center</u>

Current Challenges, Issues, Administration and Options

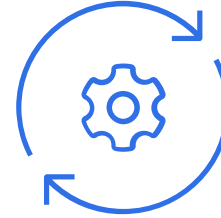
Challenges to solve



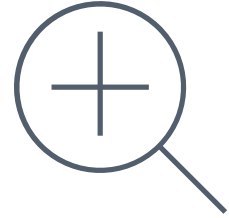
Network
connectivity



Segmentation
and security



Automation



Operations
and visibility

Need For Homogenous Experience Across Heterogenous Cloud Environments

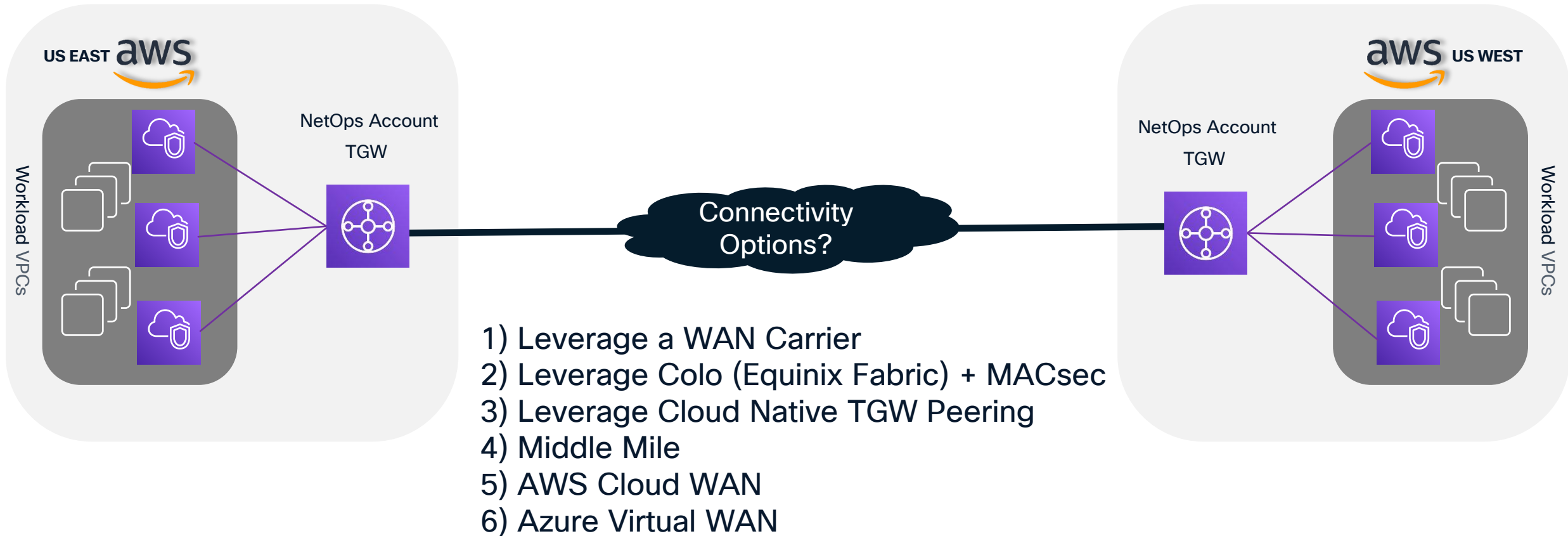
Cloud Native Routing

- **Intent:** Reach 10.1.1.0/24 over all possible paths (ECMP) and path failure(s)
- Think of each cloud as a distributed router
- How do we know about path failures?
- How do we have a backup path?
- ECMP?



Inter-Region Connectivity

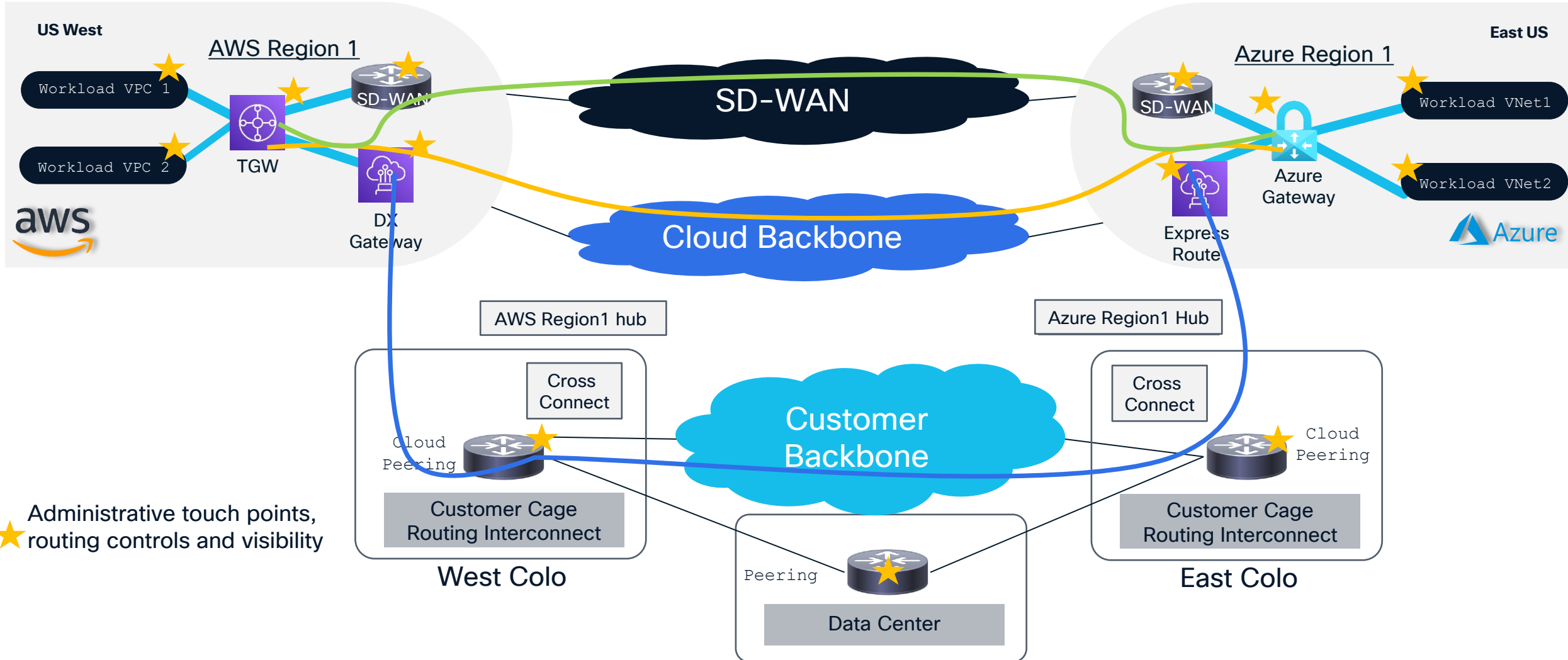
Connectivity Options



Customers are looking to build and create an environment they can switch out easily (options) based on cost / pricing / charges.

Multi-Cloud Connectivity and Routing

Multiple Ingress/Egress



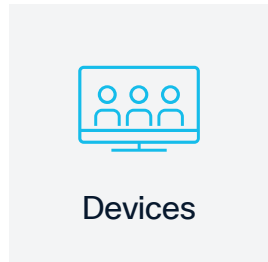
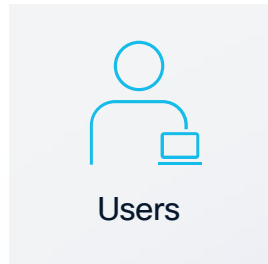
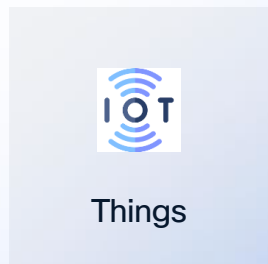
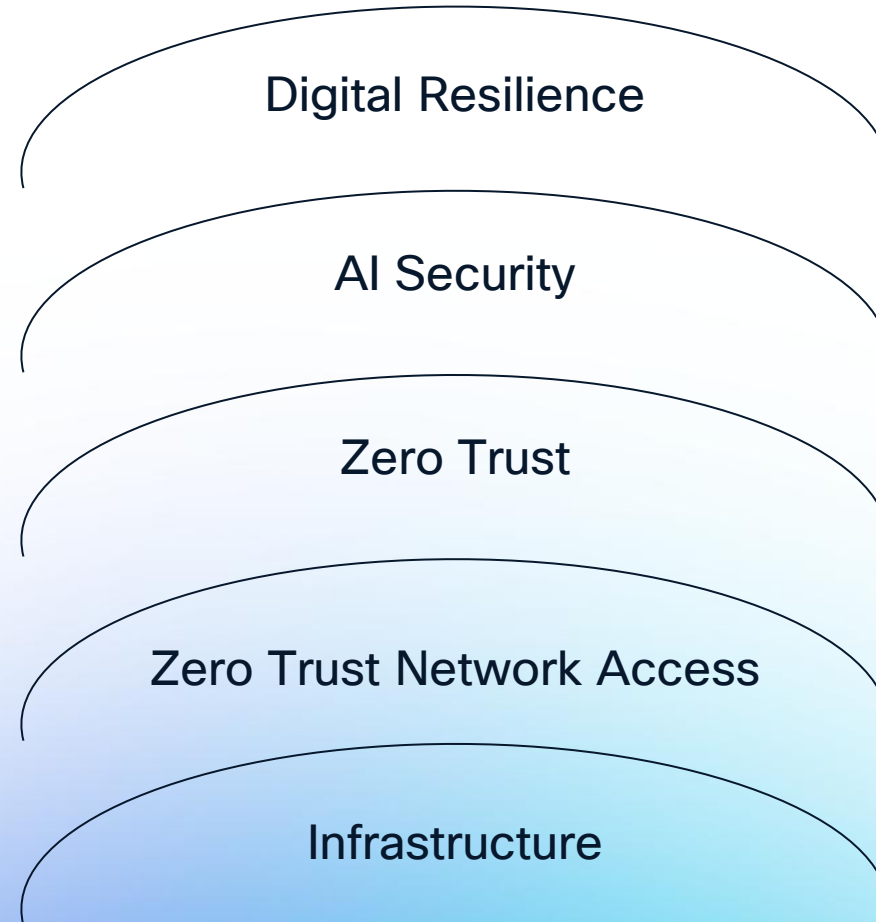
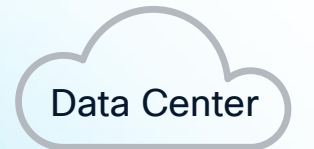
Questions to solve for:

- Which path did the traffic flow?
- Is ECMP possible?
- Failover?
- Path failure detection and re-routing to a new / backup path?
- What about visibility?

Let's take a closer look...

Architecture

Secure Networking



Key Capabilities

Taxonomy, a few more...

NGFW: Next Generation Firewall

ISE: Identity Services Engine

SGT: Security Group Tag

SASE: Secure Access Service Edge

SSE: Security Service Edge

SD-WAN: Software Defined WAN

SDCI: Software Defined Cloud Interconnect

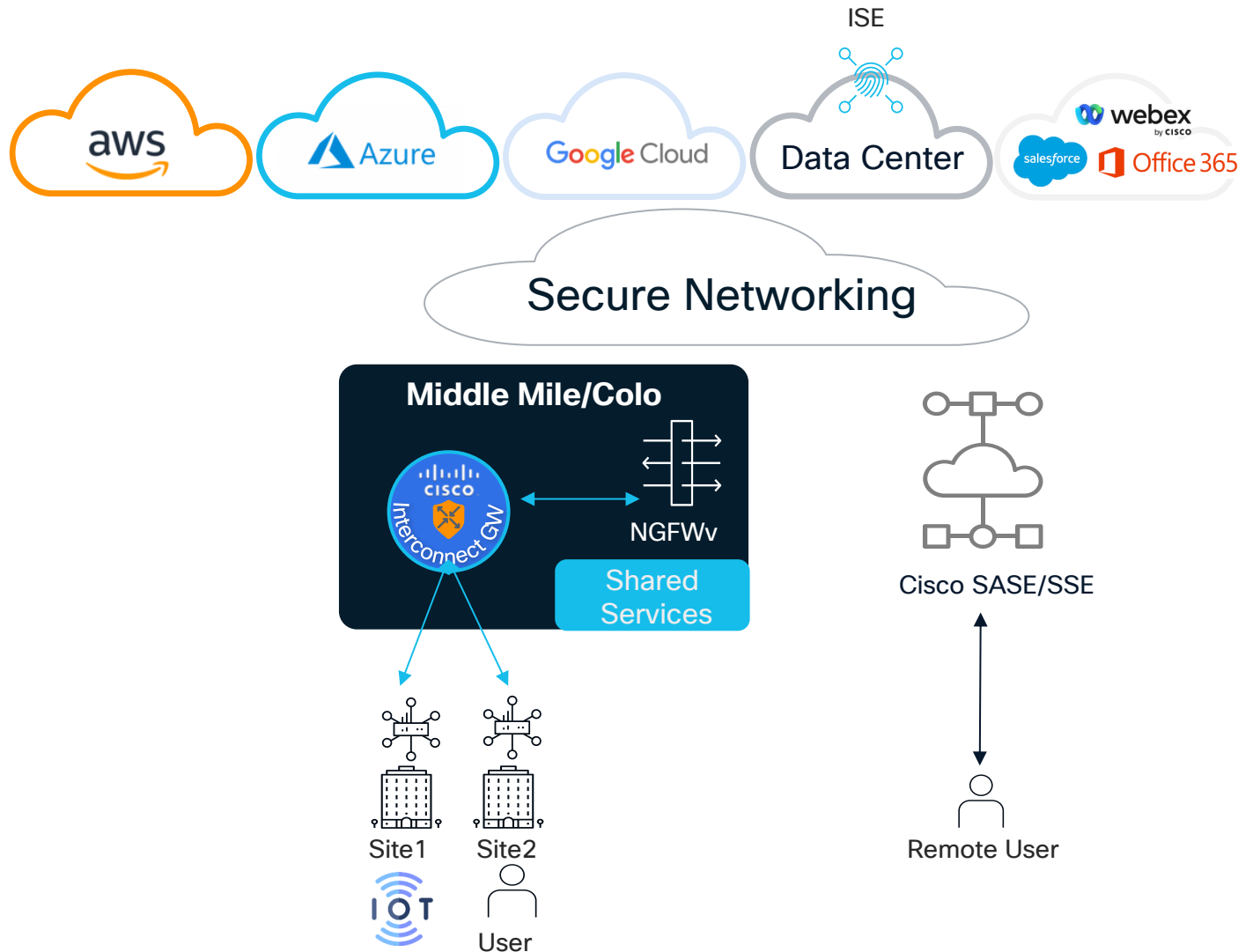
CASB: Cloud Access Security Broker

DLP: Data Loss Prevention

ZTNA: Zero Trust Network Access

Topology

Automate branch, cloud and Data Center/Colo connectivity / security

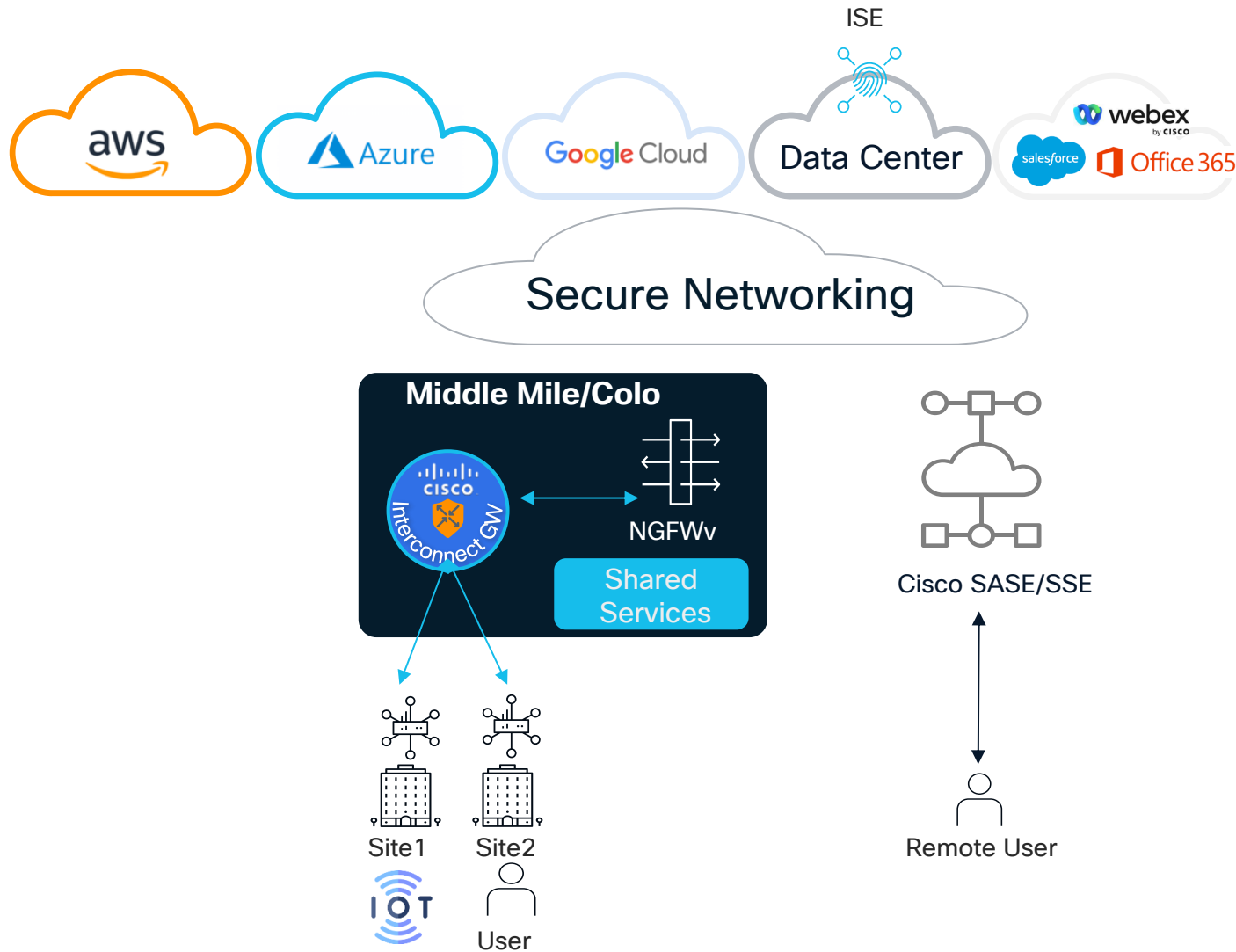


- Secure Remote Users / locations / sites
- IaaS / SaaS / Internet / Private DC
- IoT Use-Cases
- Automation + Management + Visibility
- Segmentation (macro/micro)
- Policy Enforcement Points
- Common Policy

Middle Mile:

- Rely on more Internet Connectivity
- Discrete circuits connecting locations
- Consumption Options
- Optimize Traffic Flows
- Cloud Connectivity
- Remote location + Geo(s)

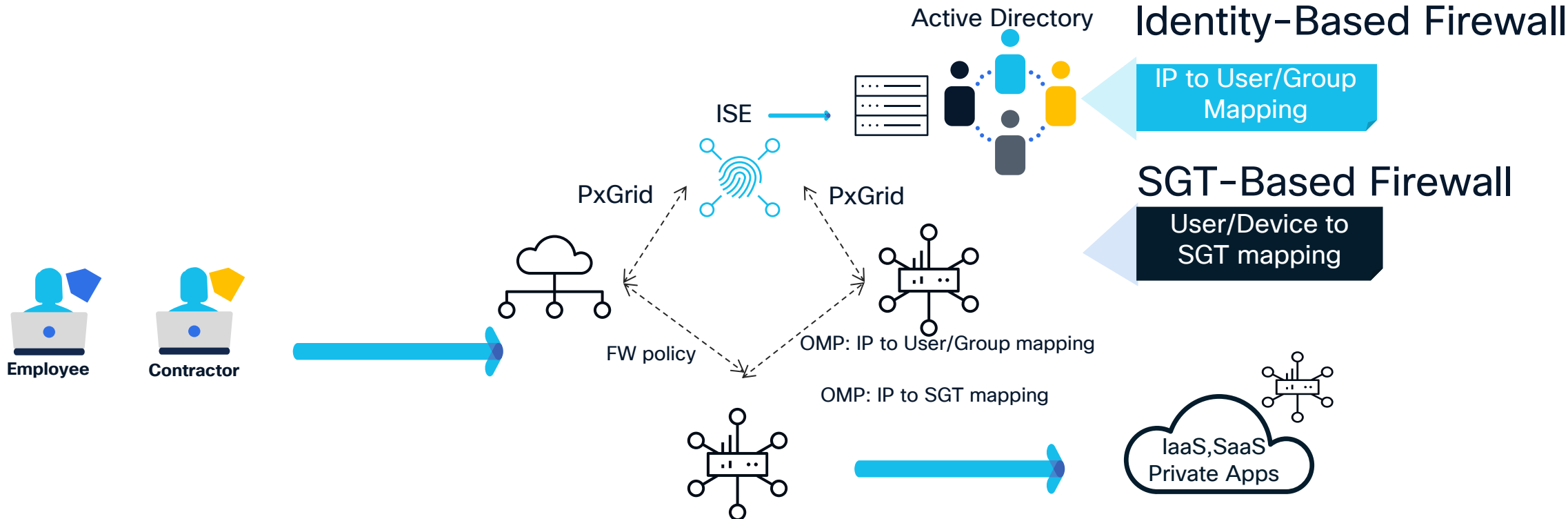
Capabilities: Site/User-to-Cloud



- SD-WAN + Firewall
 - Identity-Based Firewall
 - SGT-Based Firewall
- Stateful Firewall on cEdge
- Deployment Options:
 - **Base Firewall:** L3/L4
 - **Advanced Firewall:** Identity-based Firewall
 - **Advanced NGFW:** SGT-based Firewall
- Leverage on-prem ISE Investment Identity + ISE
- Ability to choose enforcement options
- Ability to carry + Enforce VRF and SGT end to end
- NGFW

Edge Firewall

Unified Security policy and intent



Granular Security Control at User/Group Level

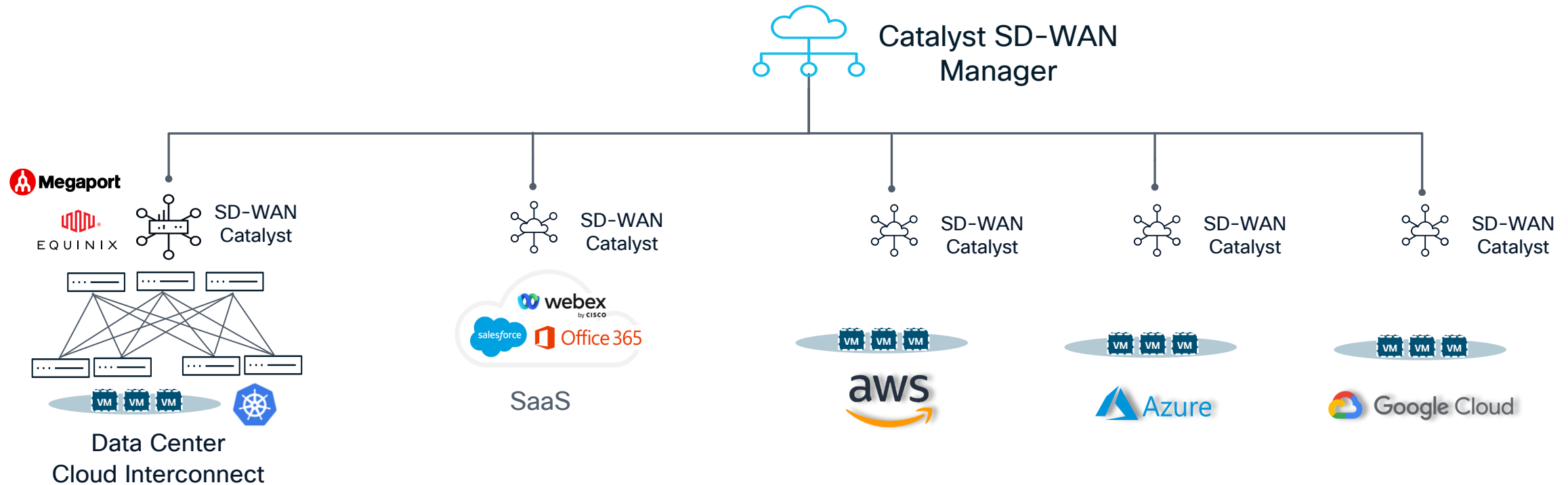
Policy	Destination	
	Employee	Contractor
Employee	Permit All	Deny All
PLC	Permit All	Deny All
Contractor	Deny All	Permit All

Connecting Users / Devices / Things to the Cloud

Multi-Cloud Networking: Catalyst SD-WAN Manager

Multi-Cloud Networking

Automate connectivity & segmentation with full visibility across hybrid cloud



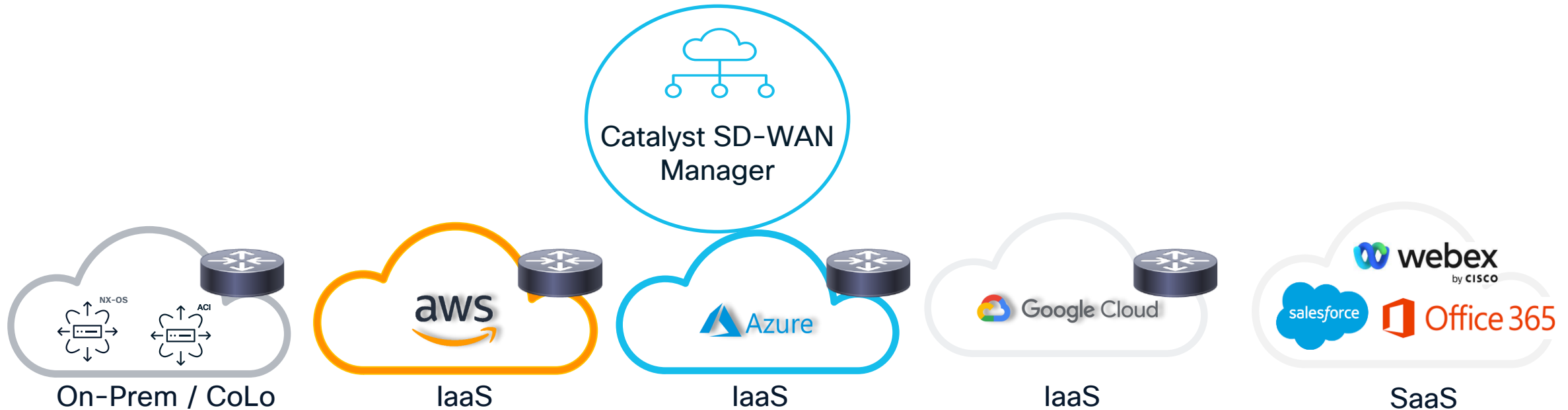
Automated connectivity
and routing

Consistent security and
segmentation

Single Point of Orchestration
Visibility & Troubleshooting

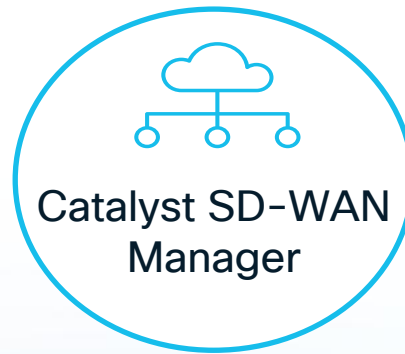
Automated insertion of L4-7
services

Distributed Cloud Networking



- Catalyst SD-WAN Manager is highly resilient / available software defined controller
- Each Cloud is a distributed router
- Leverage SLA probes to monitor Cloud Objects / Path Selection

Personas



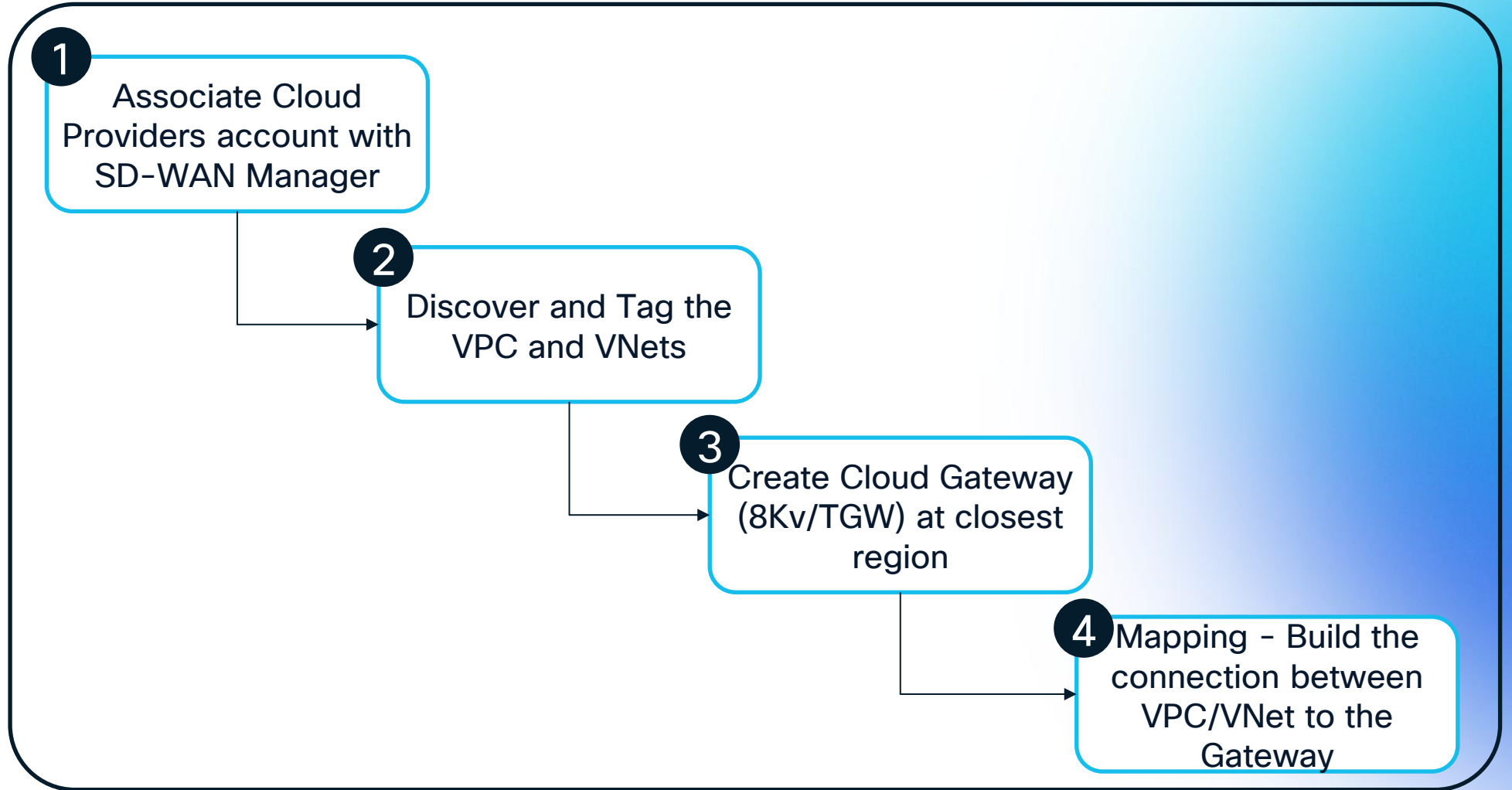
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
le. Firewall

Multi-Cloud Workflow

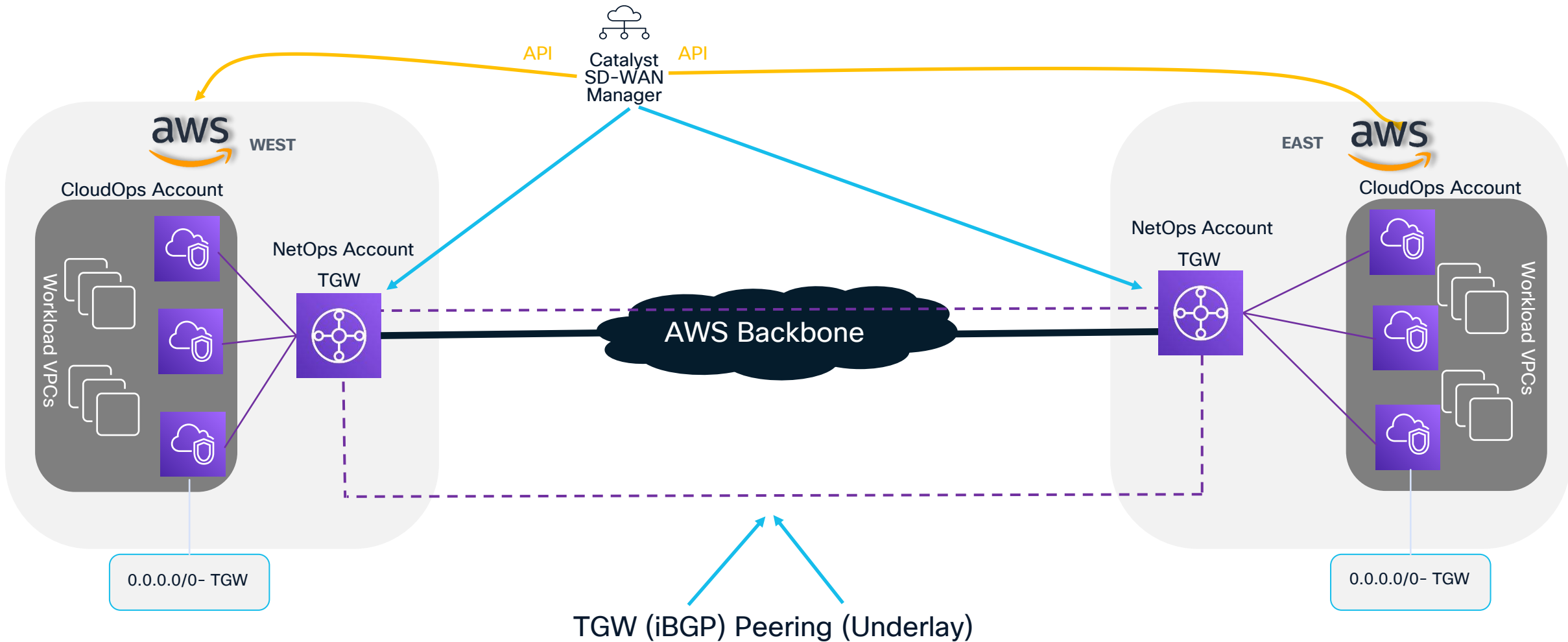
Secure Connectivity
achieved in minutes



Integration and connectivity to AWS

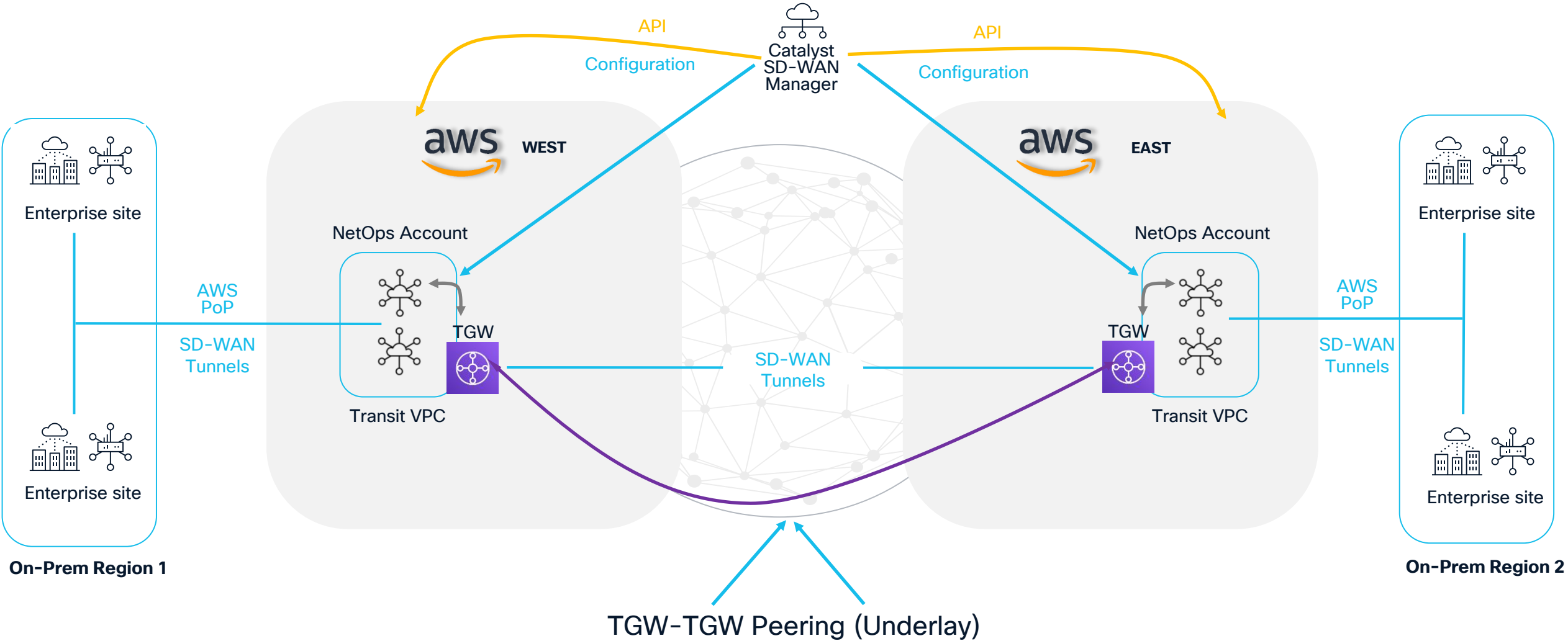
With TGW

AWS: Region-to-Region

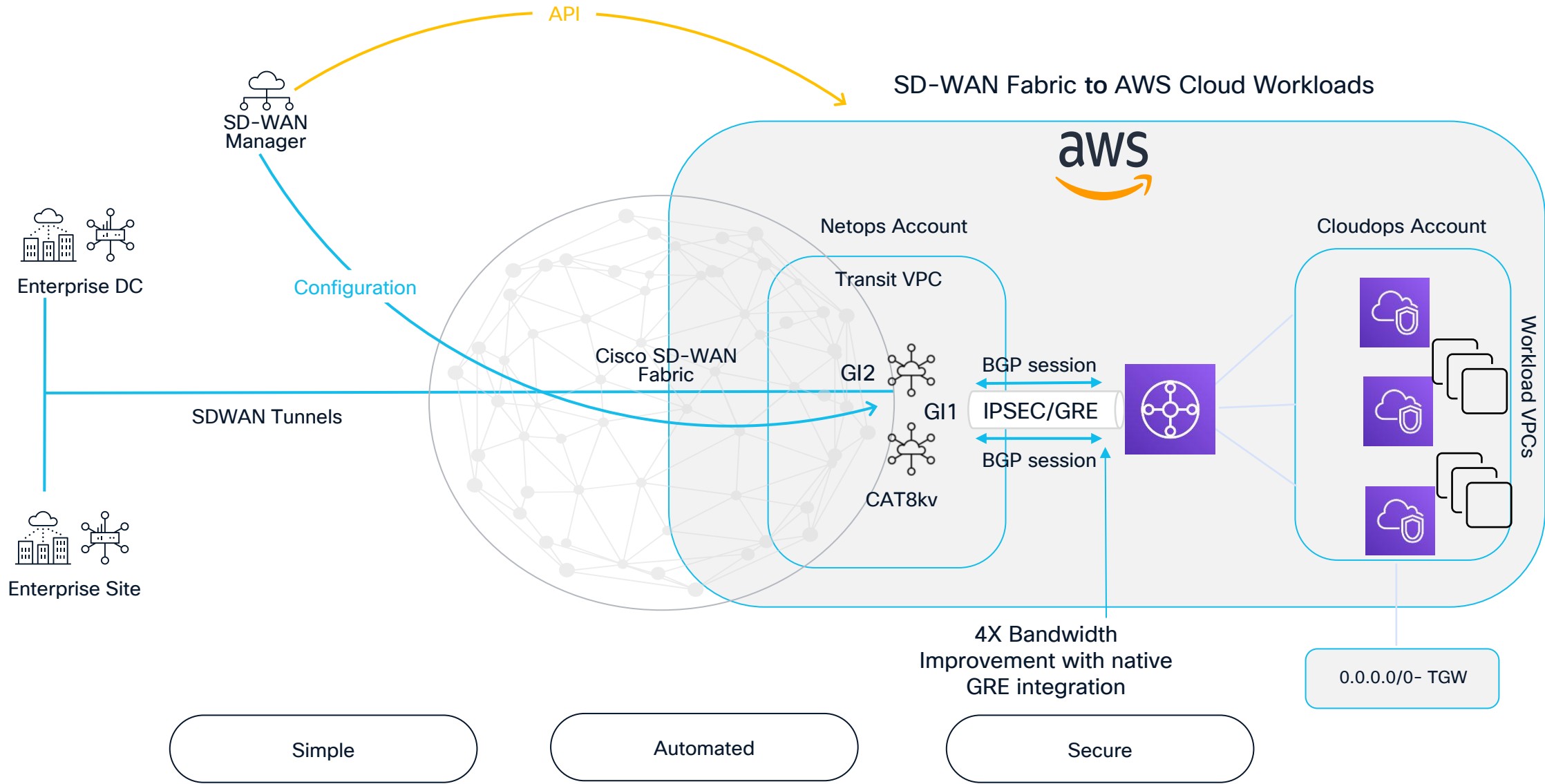


AWS: Site-to-Site

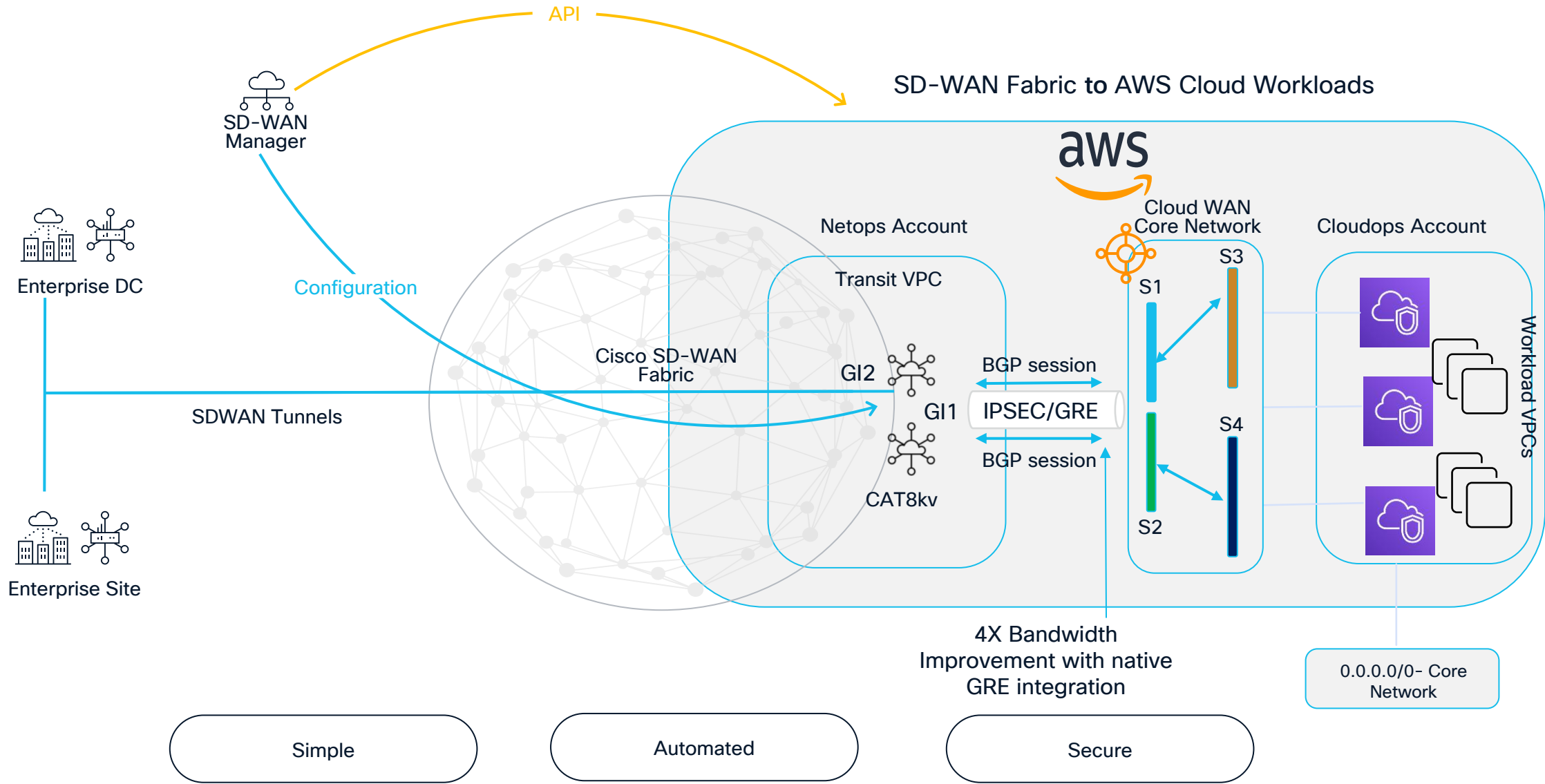
SD-WAN Fabric Across AWS Cloud Global Network



AWS Site to Cloud with TGW



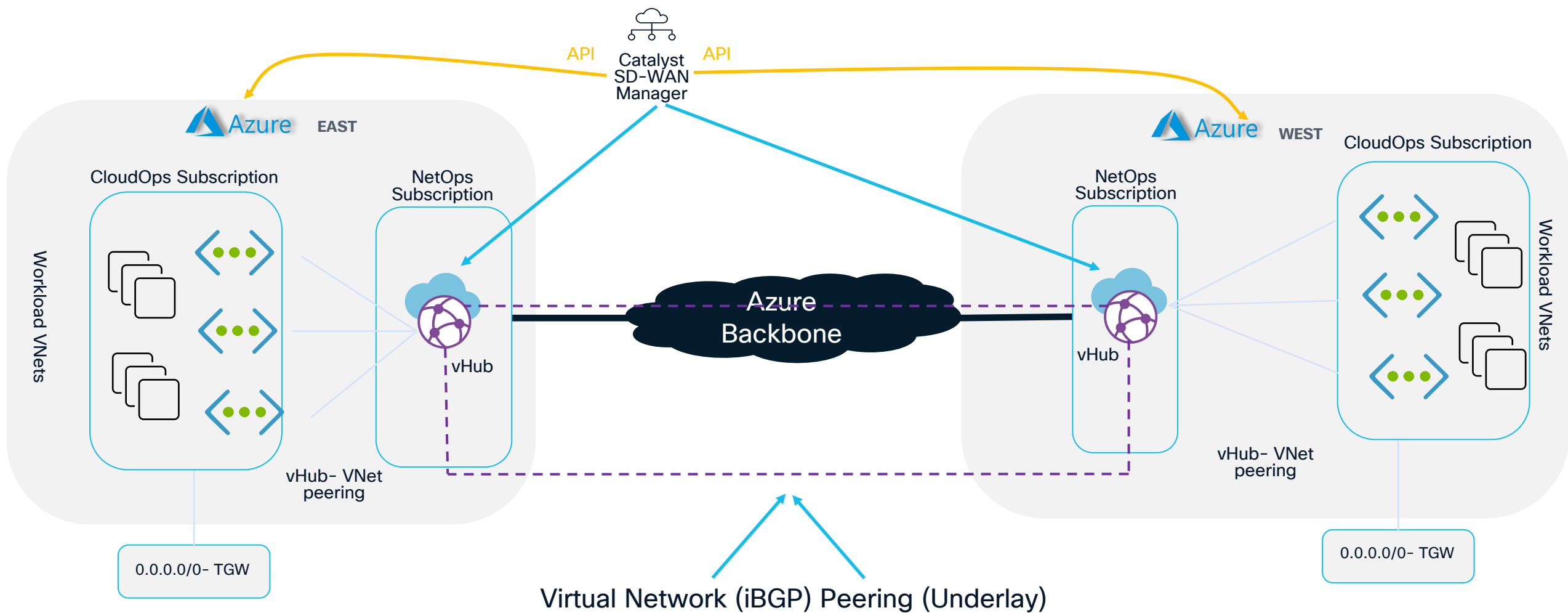
AWS Site to Cloud with Cloud WAN



Integration and Connectivity to Azure

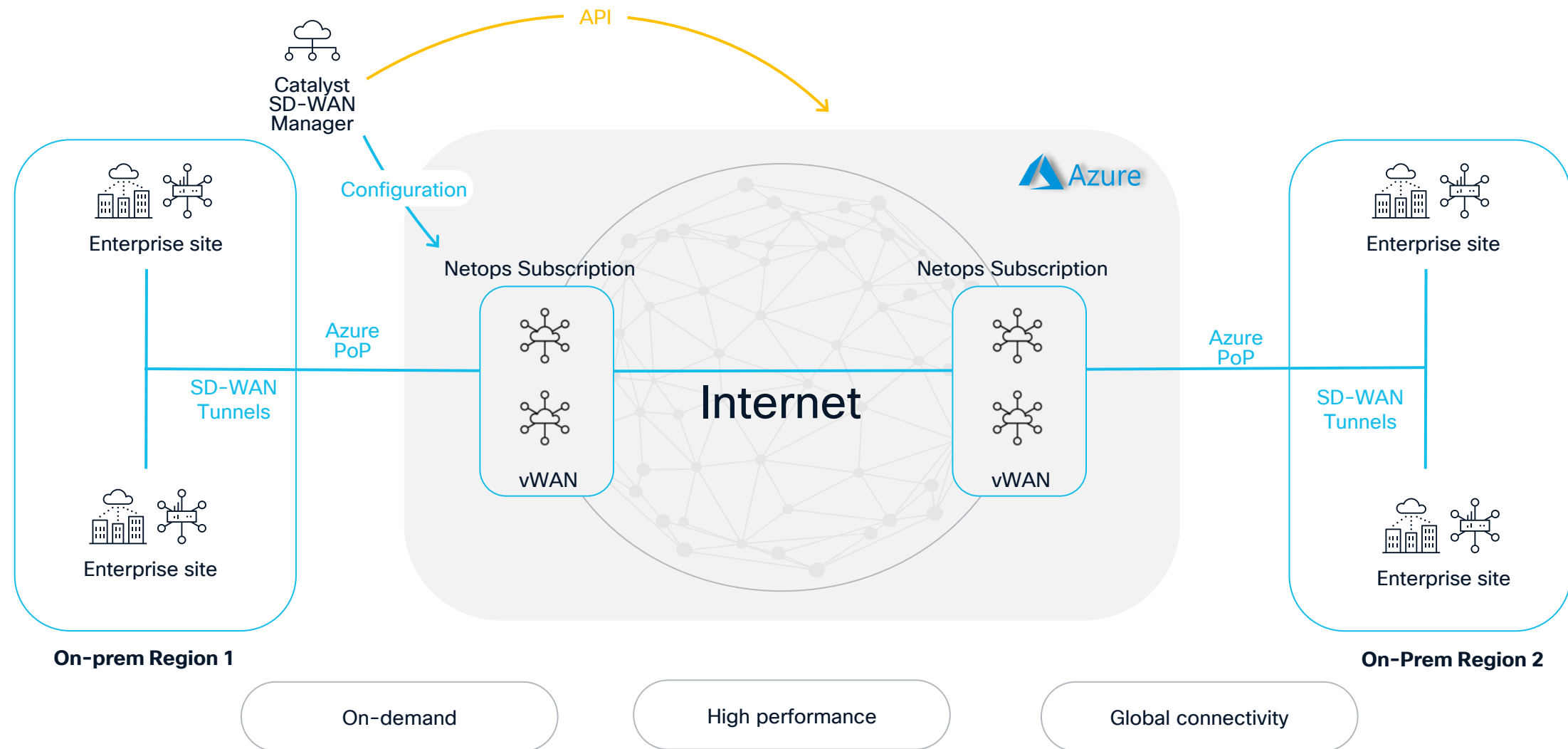
With vWAN/vHub

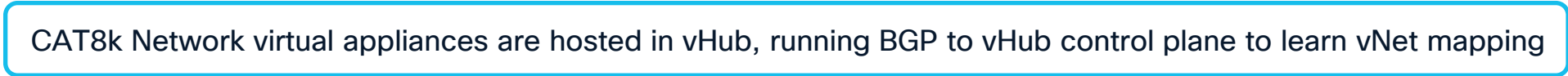
Azure: Region-to-Region



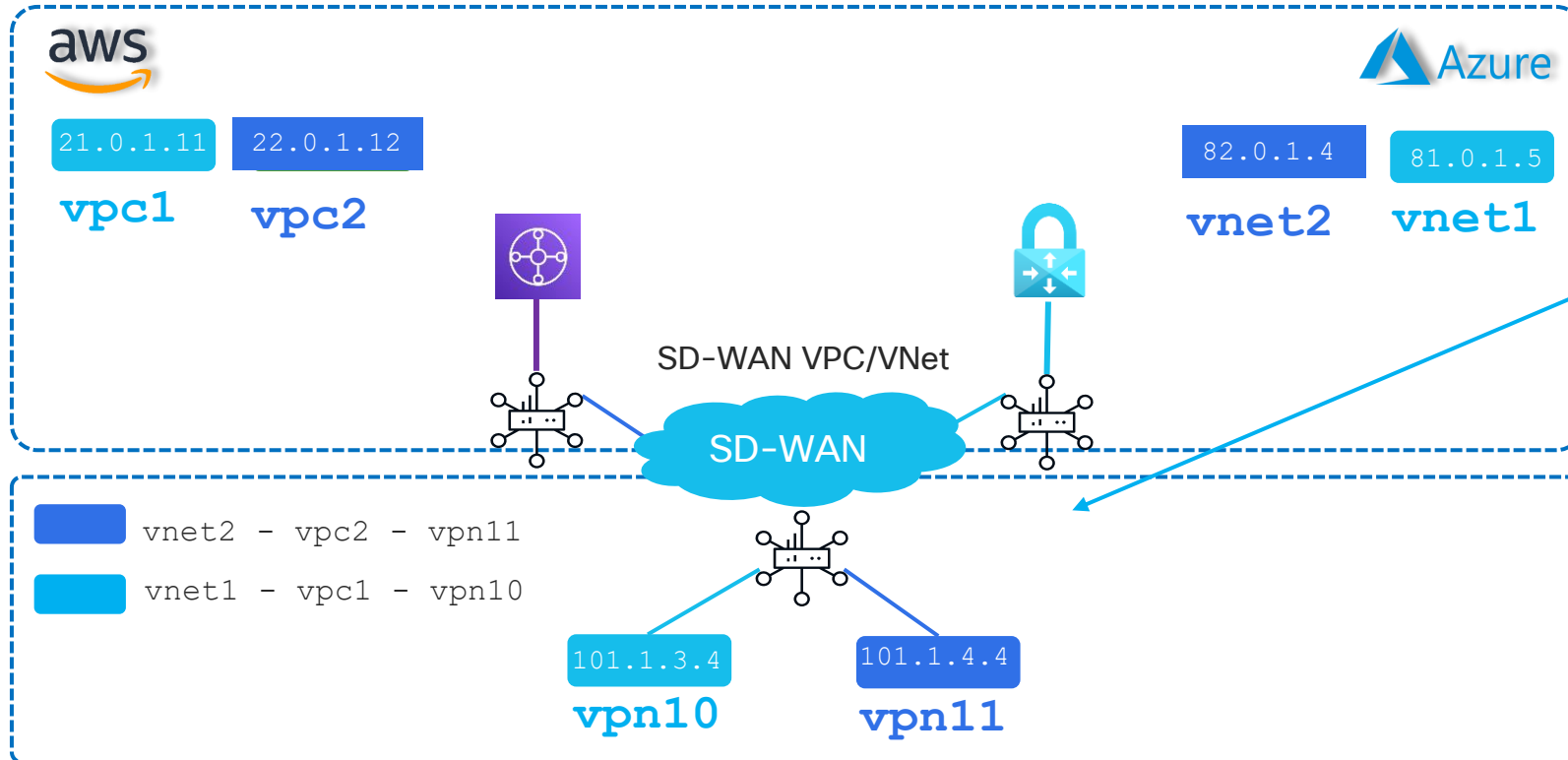
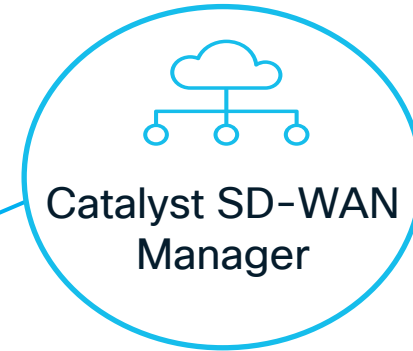
Azure: Site-to-Site

SD-WAN Fabric Across Azure Global Network

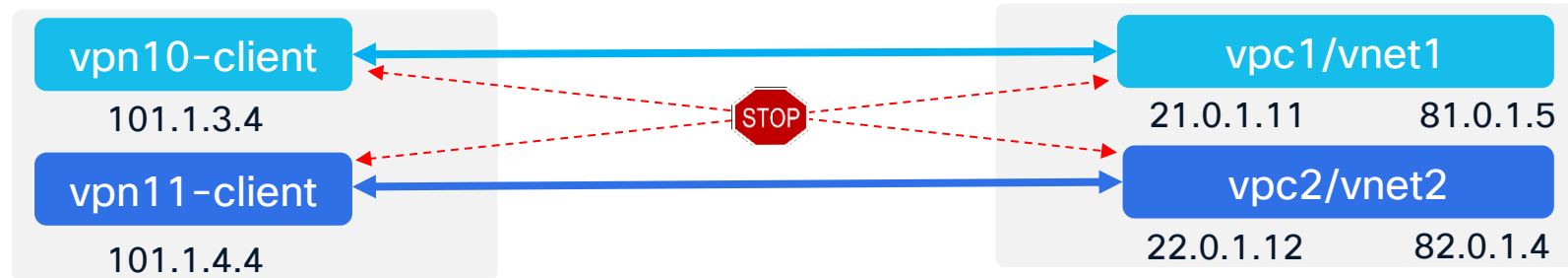




Segmentation with SD-WAN

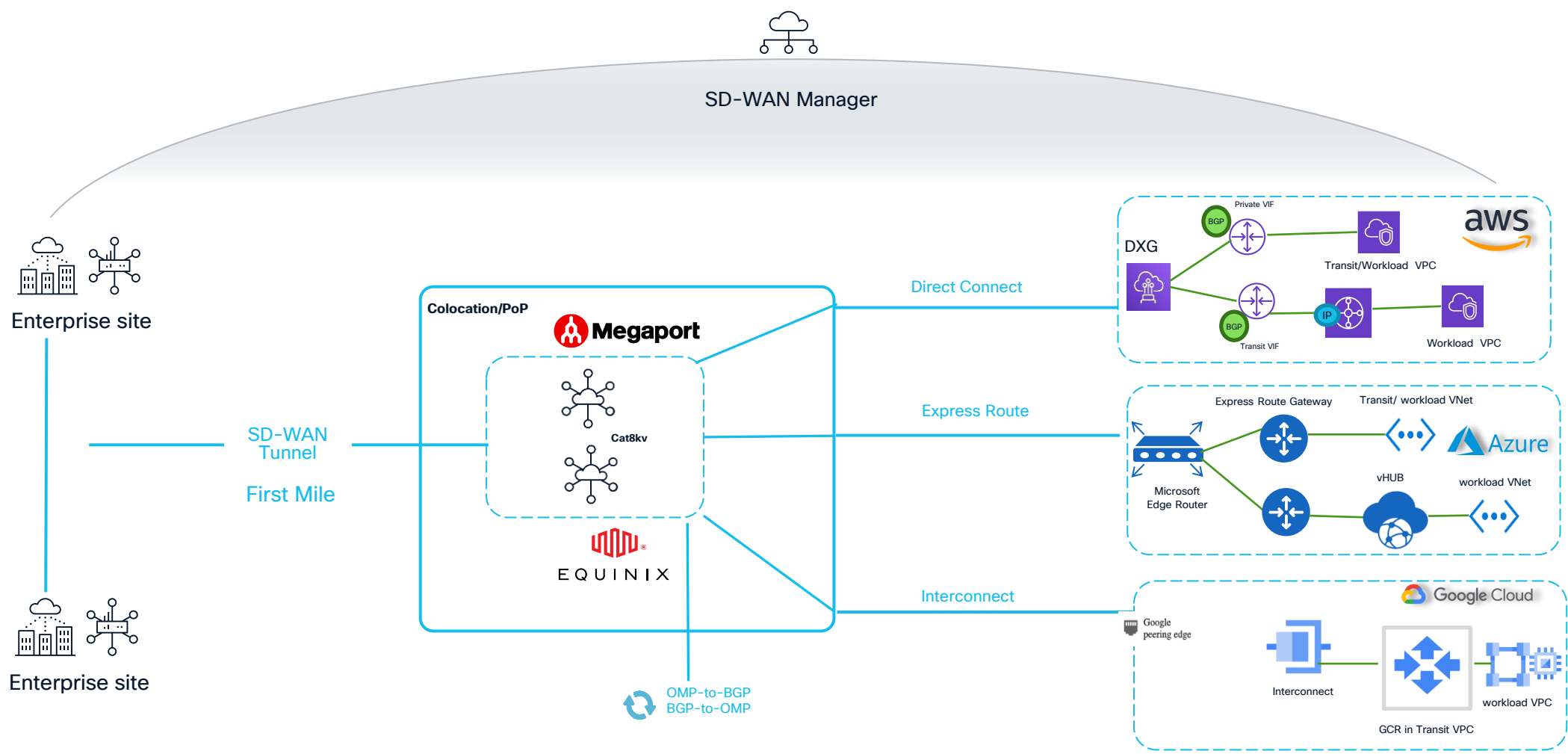


- 1) SDWAN connectivity terminates at the Cat8ks for the different VRFs
- 2) VRF(s) are extended to the TGW/ Cloud WAN extended to the native VPCs



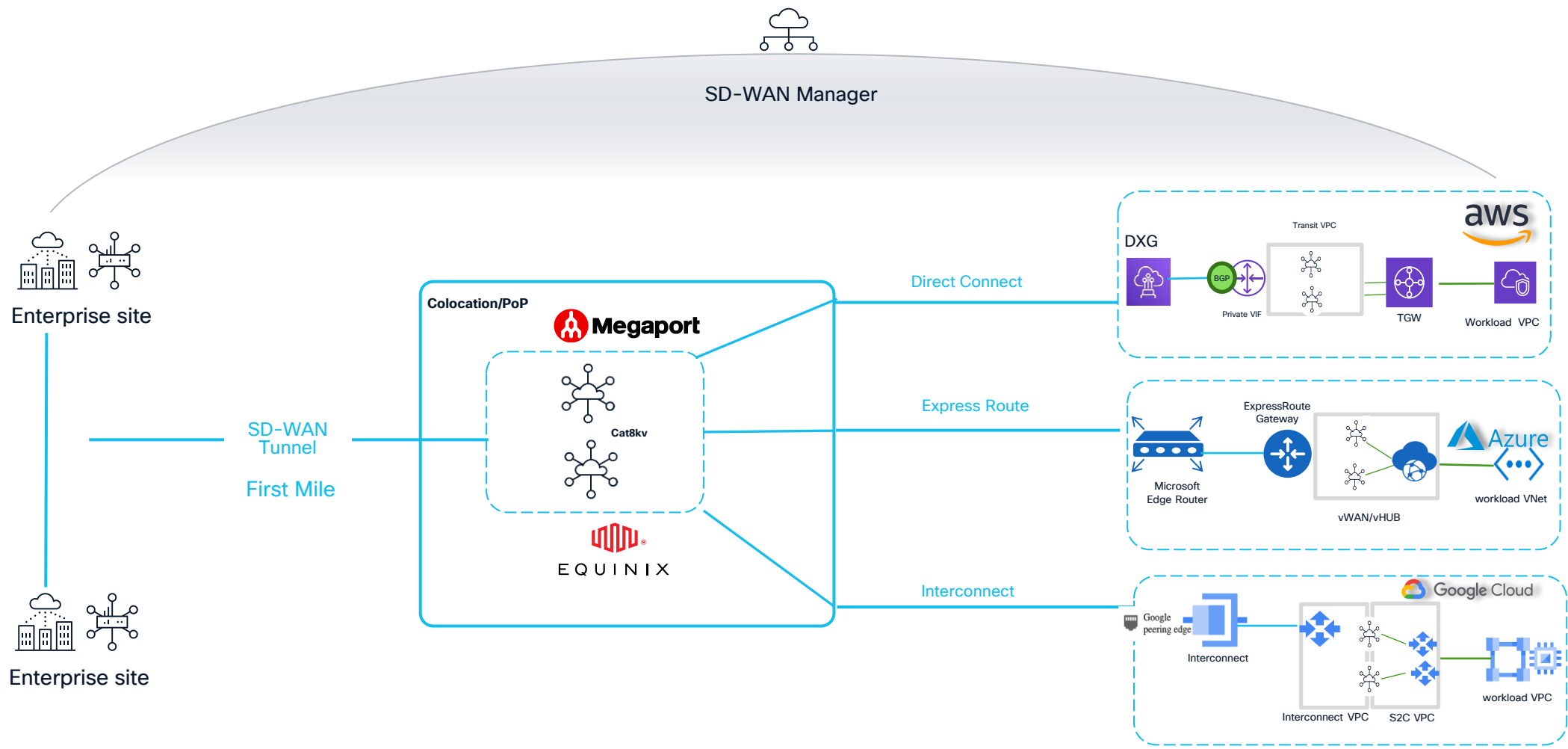
Middle Mile with Megaport & Equinix

Site-to-Multicloud- Megaport or Equinix



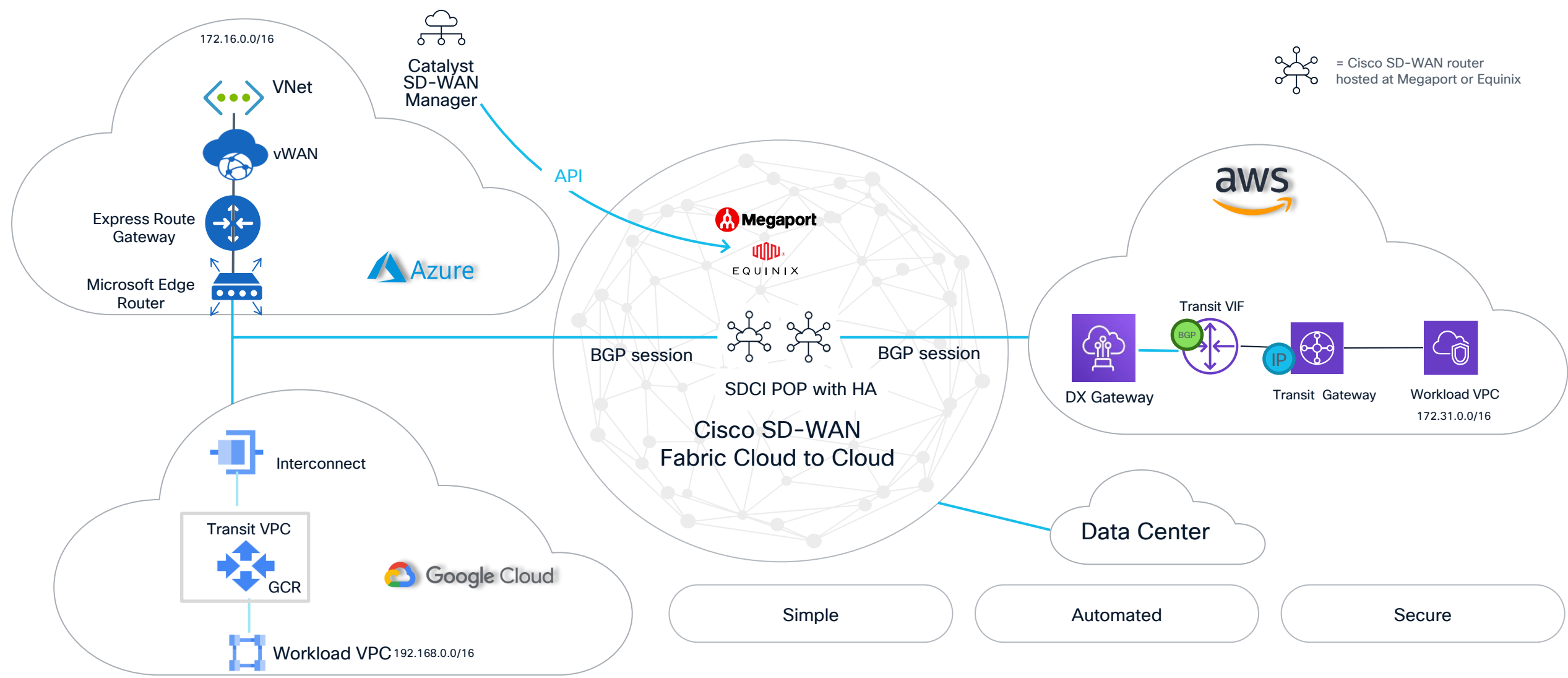
Site-to-Multicloud- Megaport or Equinix

Fully Encrypted



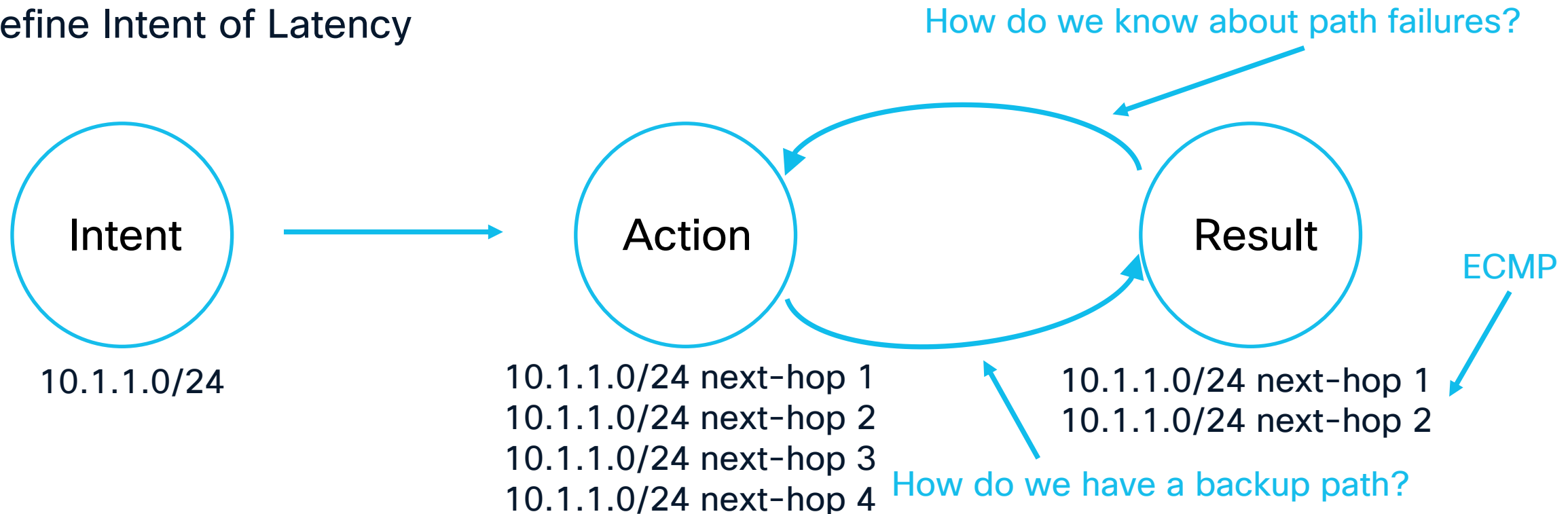
Cloud to Cloud: Private Connect

Megaport/Equinix



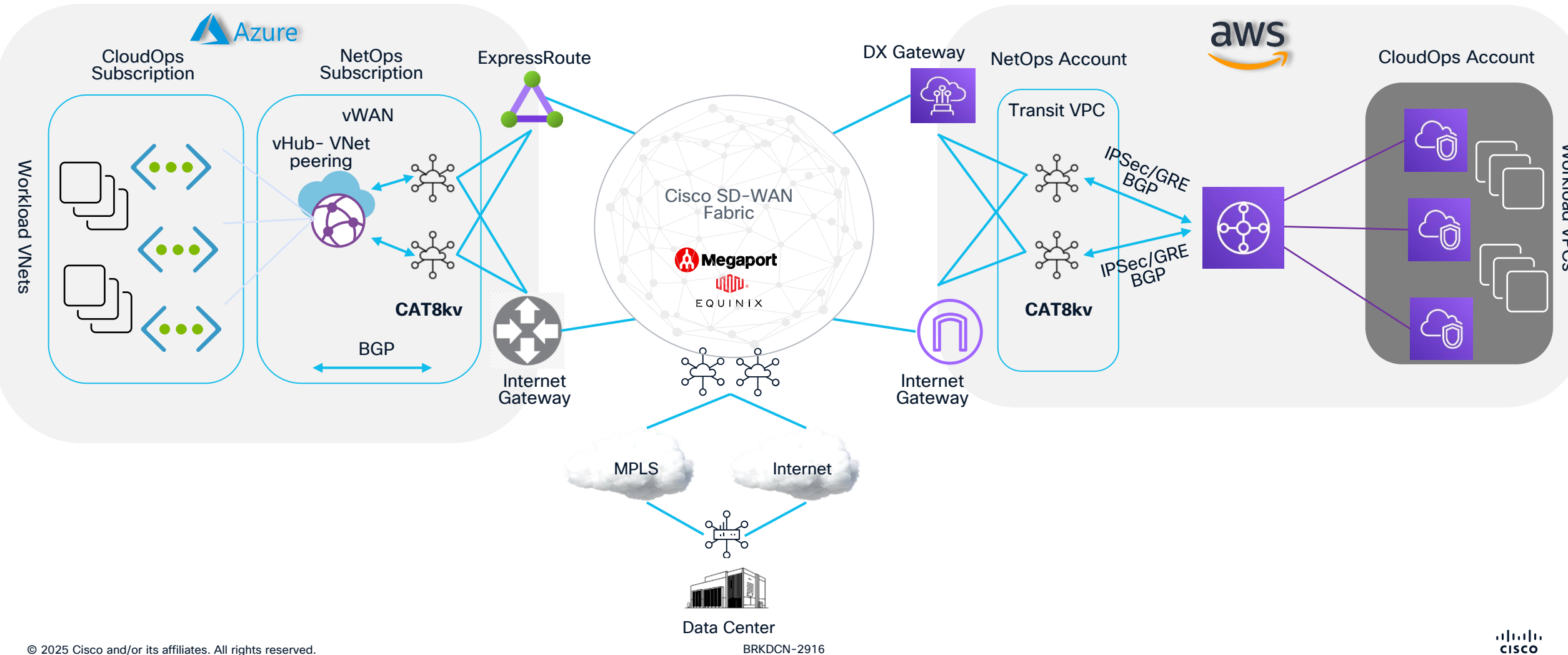
Cloud Networking with SD-WAN Manager

- **Intent:** Reach 10.1.1.0/24 over all possible paths (ECMP) and Path Failure(s)
- Administrator expresses the Routing Intent (NetOps / Cloud NetOps)
- Validation of reachability
- Define Intent of Latency



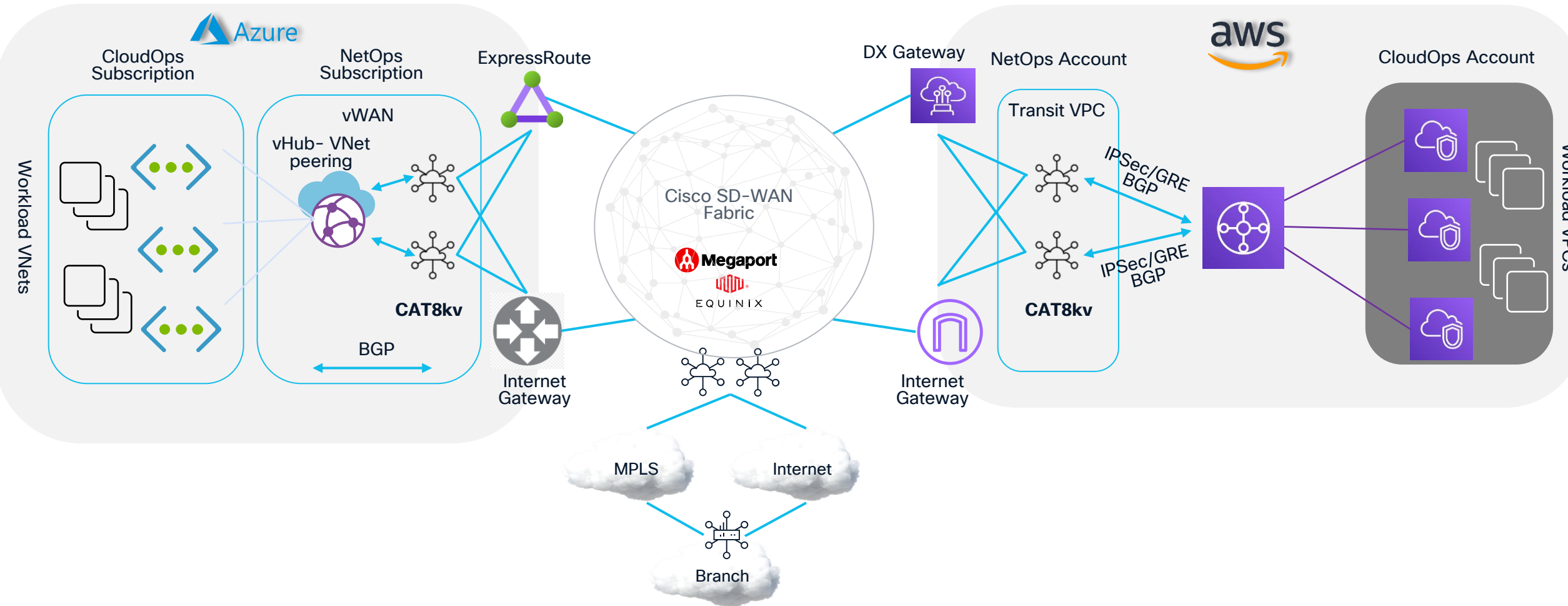
Cloud-to-Cloud

ECMP



Cloud-to-Cloud

ECMP



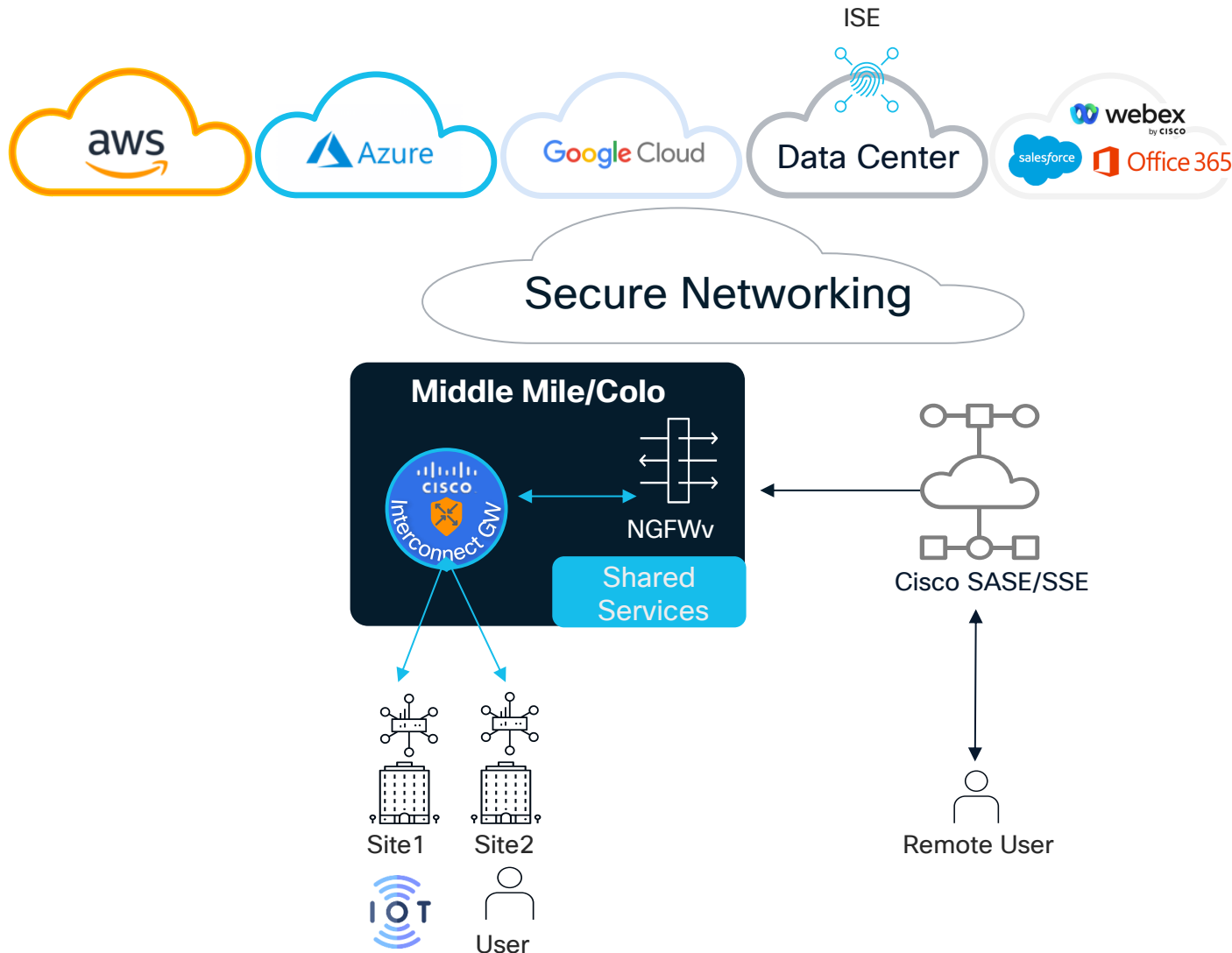
So where is the new perimeter?

I define it as, wherever security controls and capabilities are to protect users/devices, things, applications and data; the security perimeter is **everywhere**.

Applications behind SD-WAN and Cloud Security Stack

Use Case: Site/User-to-Cloud

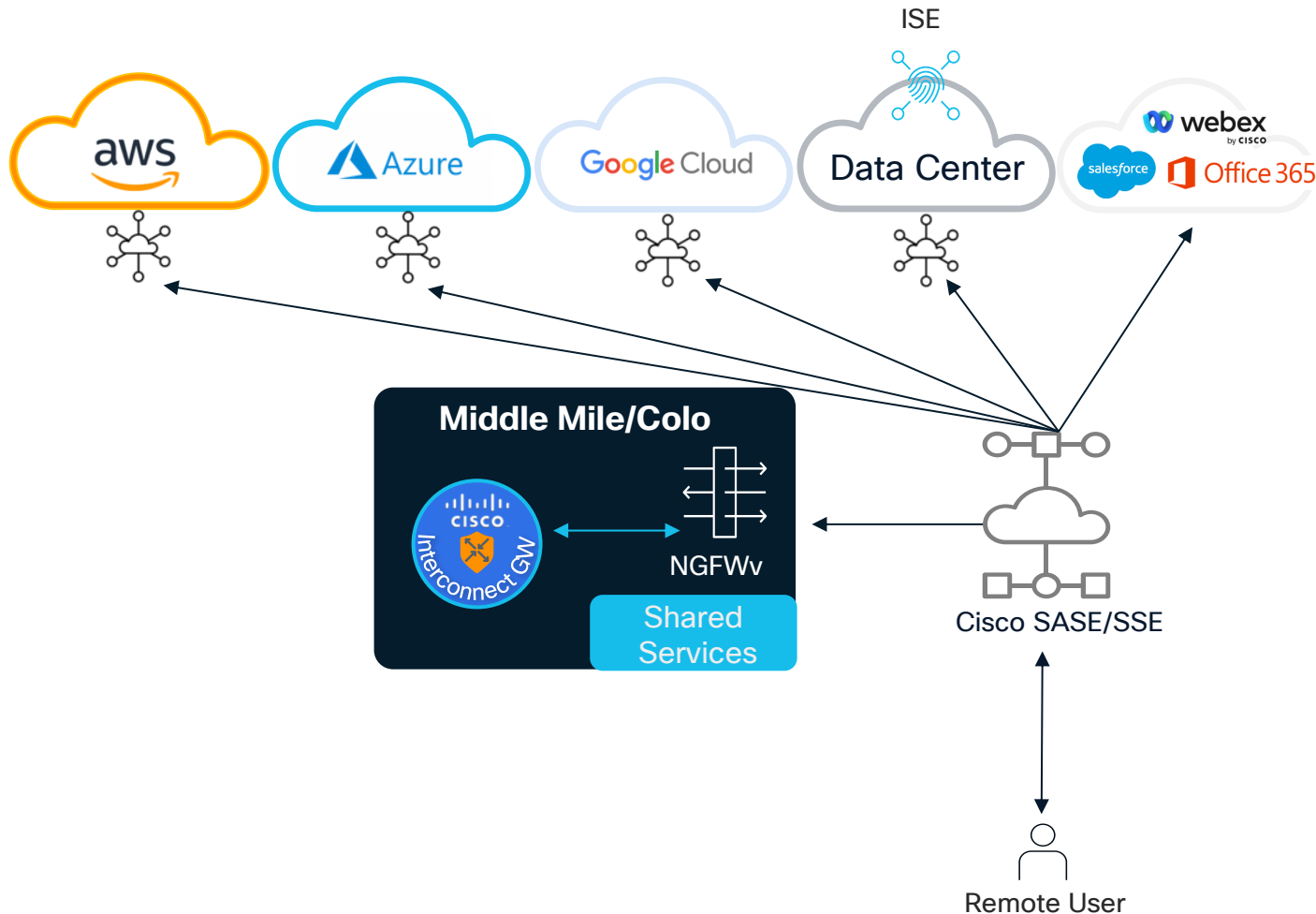
SASE/SSE



- Cloud Security for remote Users / Branch Users and IoT.
- Network automation + SASE/SSE (Secure Web Gateway (SWG), CASB/DLP, ZTNA, FWaaS)
- Capabilities: Ability to carry VRF and SGT end-to-end
- Ability to choose enforcement options
- Identity integration with on-prem ISE
- Selective Application Traffic and Internet Egress routed to SASE/SSE stack
- SASE Bypass/Direct Internet Access (DIA): Getting traffic to the right place- not every application can go through SASE. For example, Office365 no proxy/SWG.
- Least privilege access
- Cisco Security Cloud Control

Use Case: Site/User-to-Cloud

SASE/SSE - Remote User



- **Remote User to Internet**

- Secure Client Web Module for DIA Security (DNS and Web SWG)

- **Remote User to SaaS Application**

- SWG
- DIA w/o Module (i.e. Webex or O365)
- User Experience (i.e. API hook into WebEx Tenant and bypass)
- DLP and CASB Controls (i.e.. upload only)

- **Remote User to Private**

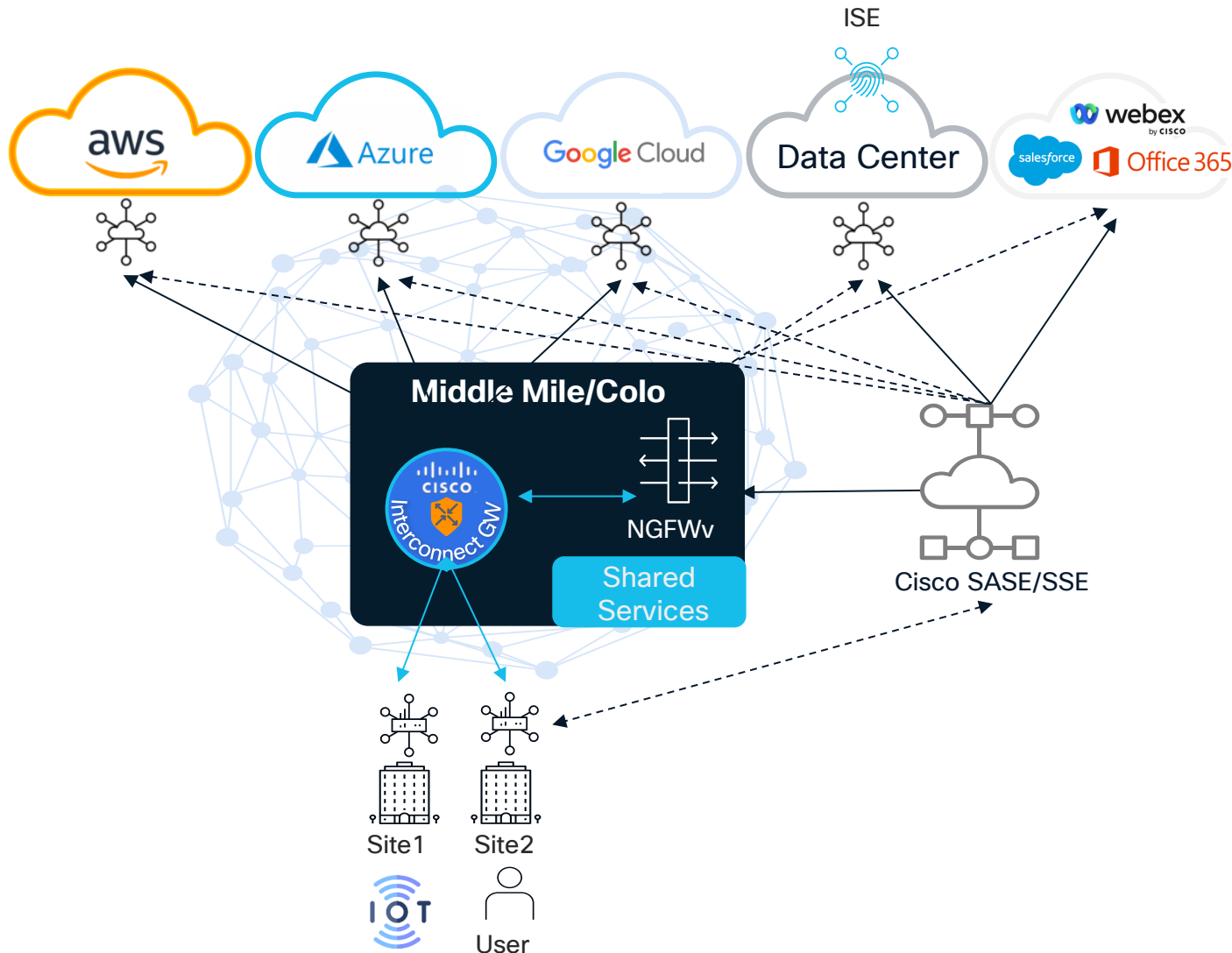
- Application in CSP
- Application in Private DC
- Application Middle Mile Shared- Services. Traffic goes through Secure Access First (FW/Inspection) PEP/IPS/Decryption/ZTNA FW

- **Three Different ways to get traffic into the SSE stack:**

- Secure Client ZTNA module (per app tunneling / posture and auth)
- Secure Client VPN module (traditional RA-VPN)
- Clientless (browser) – unmanaged use-case

Use Case: Site/User-to-Cloud

SASE/SSE – Branch Site



- **Branch User/IoT to Internet/SaaS**

- Catalyst/Meraki SD-WAN Optimized Routing
- SSE Security Controls, Inspection and least-priv access
- SD-WAN Security Capabilities

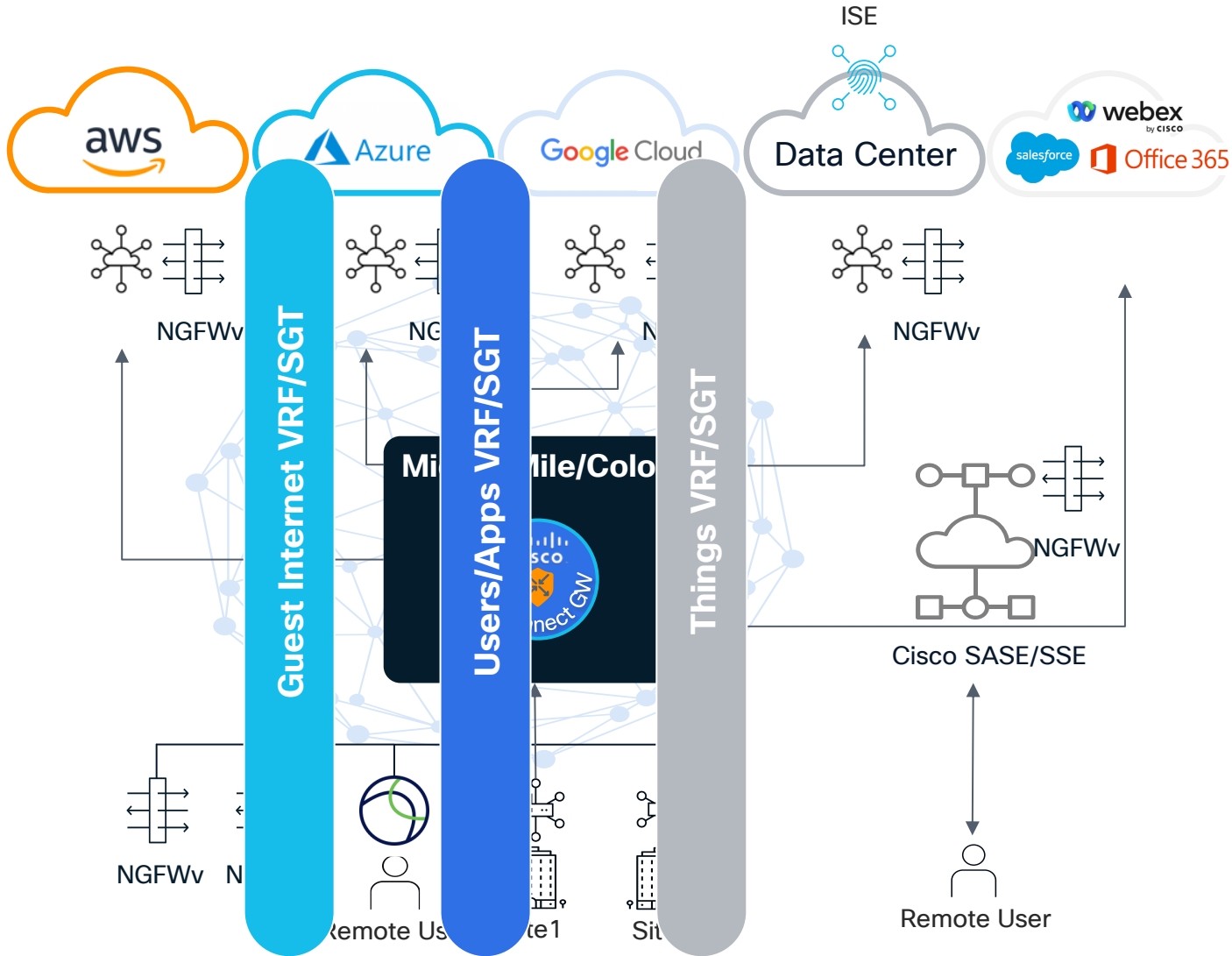
- **Branch User/IoT to Private App**

- Catalyst/Meraki SD-WAN Optimized Routing (i.e.. DC via Middle-mile)
- SSE Security Controls, Inspection and least-priv access
- SD-WAN Security Capabilities

- **Identity Attribute Options:**

- Azure-AD Username (SGT as well)
- SGT Identity
- VPN-ID (Ie. Acquisition/GuestNet)

End to End Segmented Traffic + Enforcement



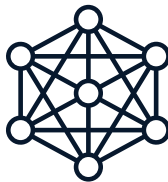
- Keep specific on its own “rail”
- VRF is ability to get traffic to the Firewall
- Micro-segmentation can also be applied
- Use Security Policy to x-connect “rail” to “rail” policy / communication

Resulting in:

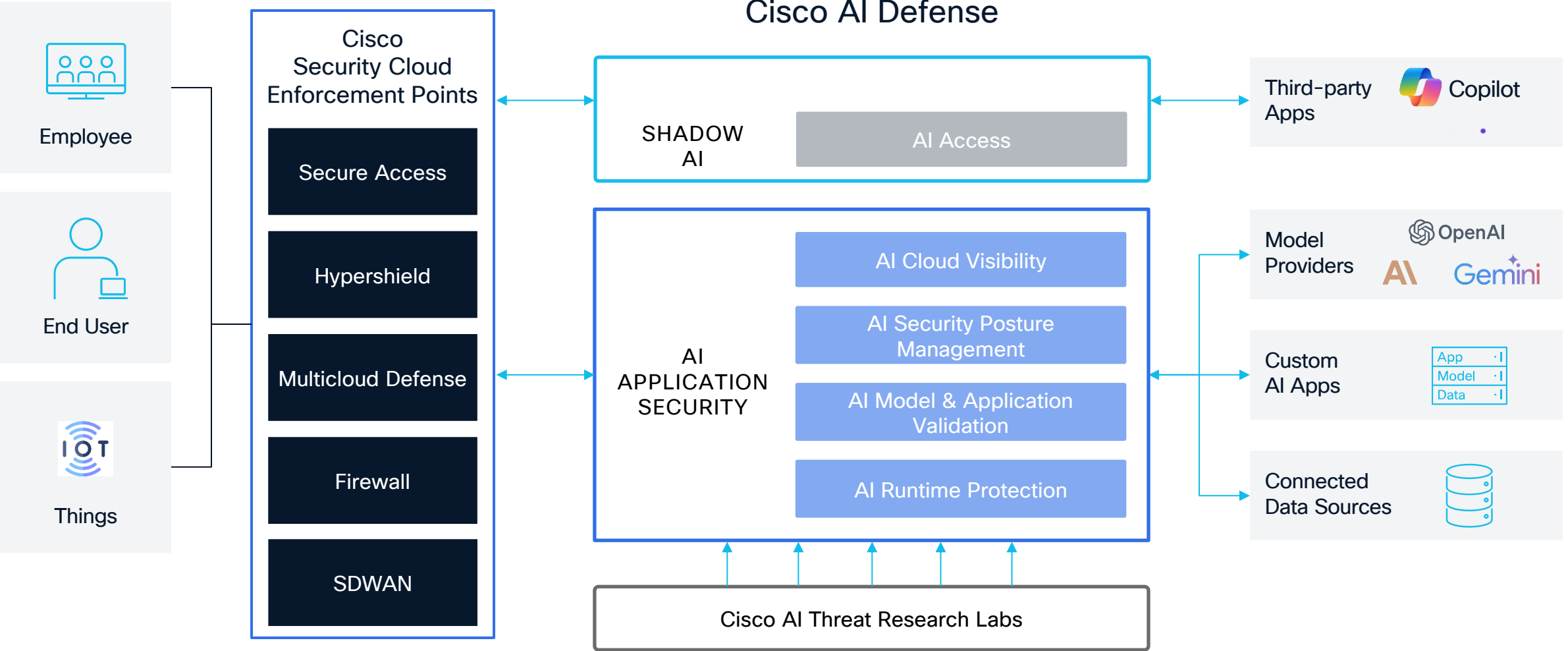
- Security Policies that are aligned user and group vs IP Addresses
- SD-WAN embedded security stack is now aware of user identity and apply policy.
- Identity Firewall capability provides granular access control based on user identity
- ZTNA trust assertion based on user and device context
- Trust based establishment

AI Applications

Cisco Security Cloud Control

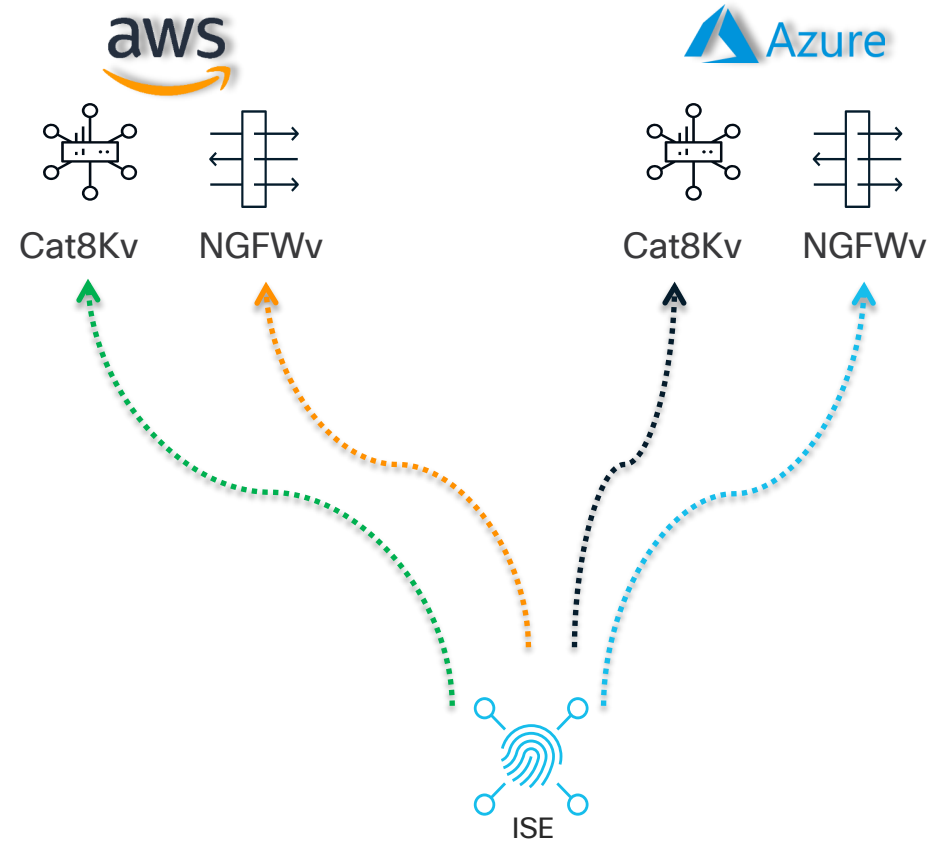


Security Cloud Control



Extending Policy to Public IaaS

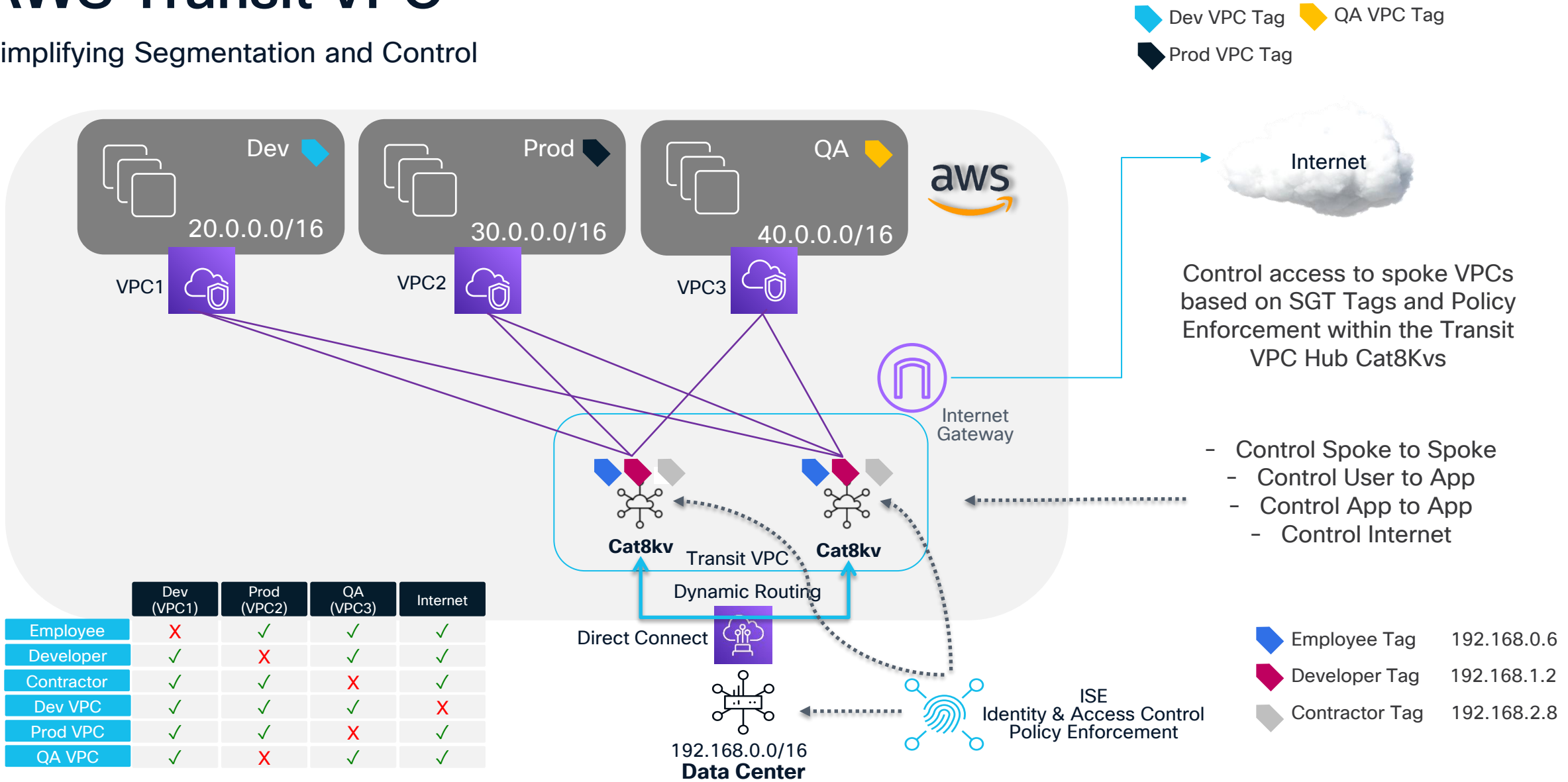
Enabling Group-Based Policies



Leveraging SGTs and ISE controls on the Cat8Kv/NGFWv within the cloud transit environments.

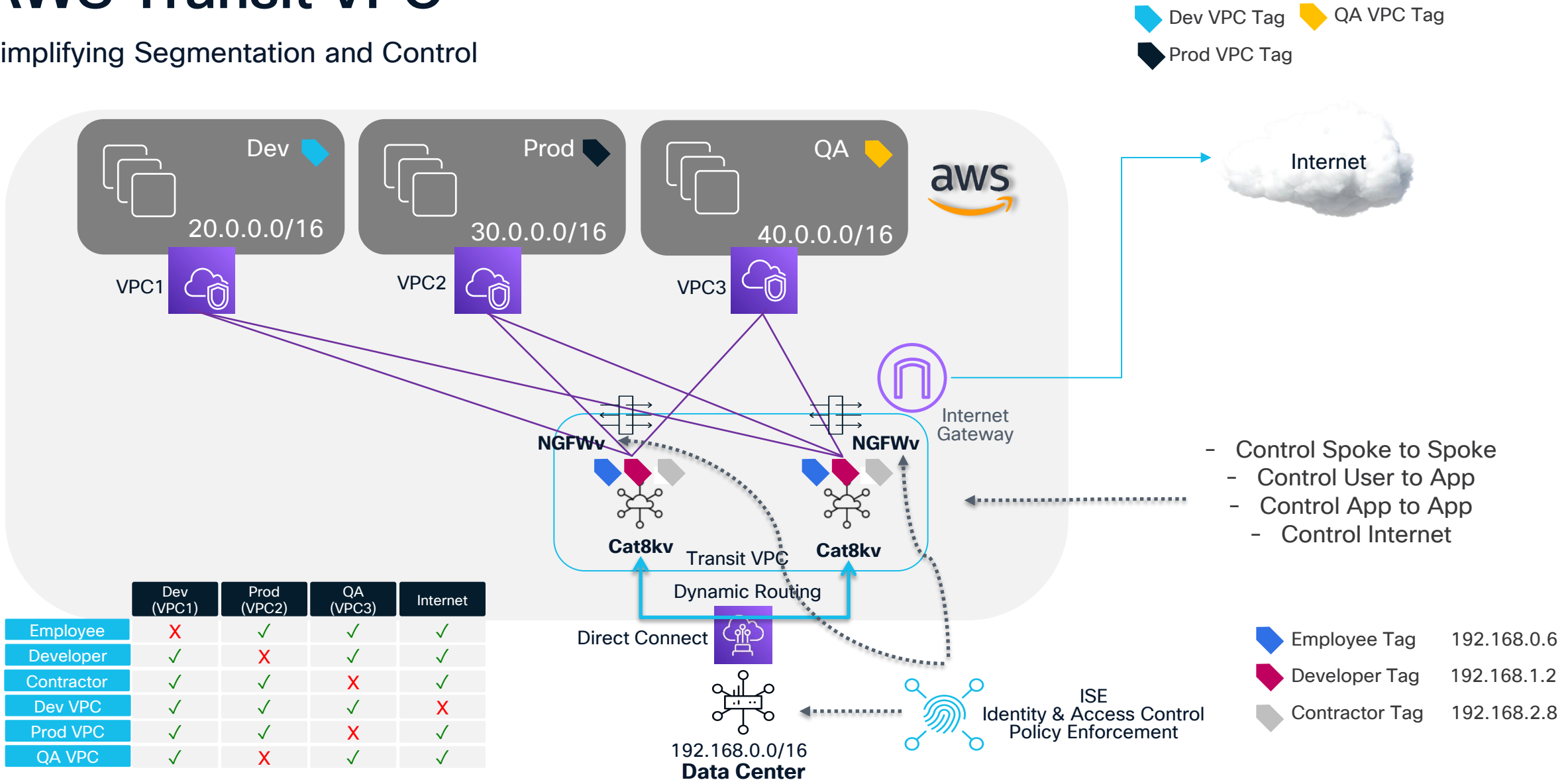
AWS Transit VPC

Simplifying Segmentation and Control



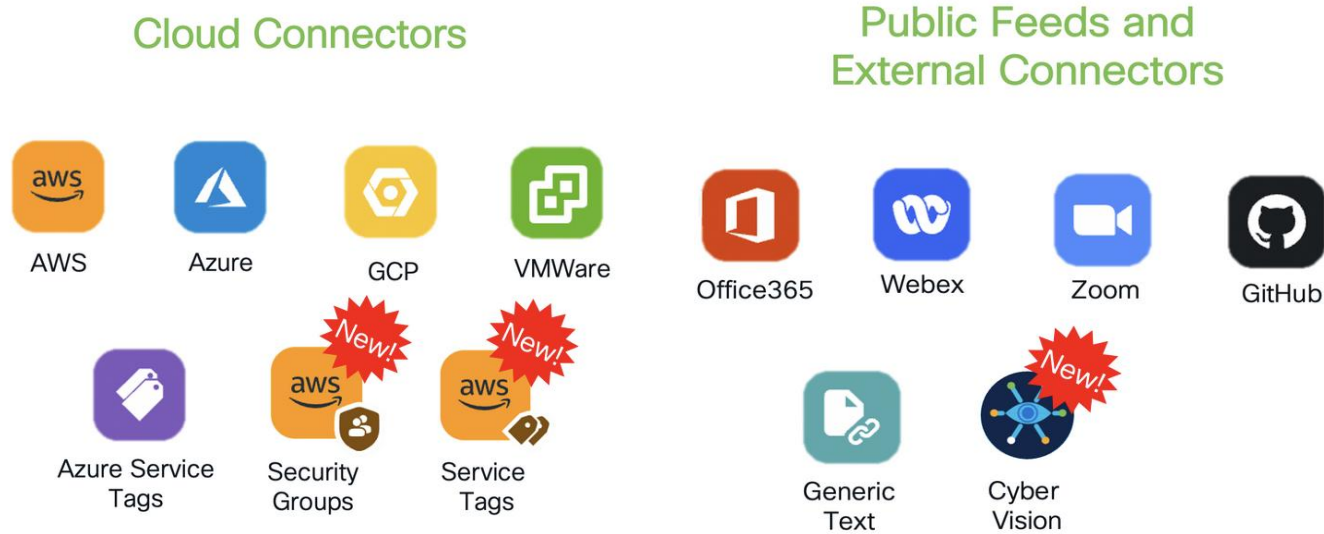
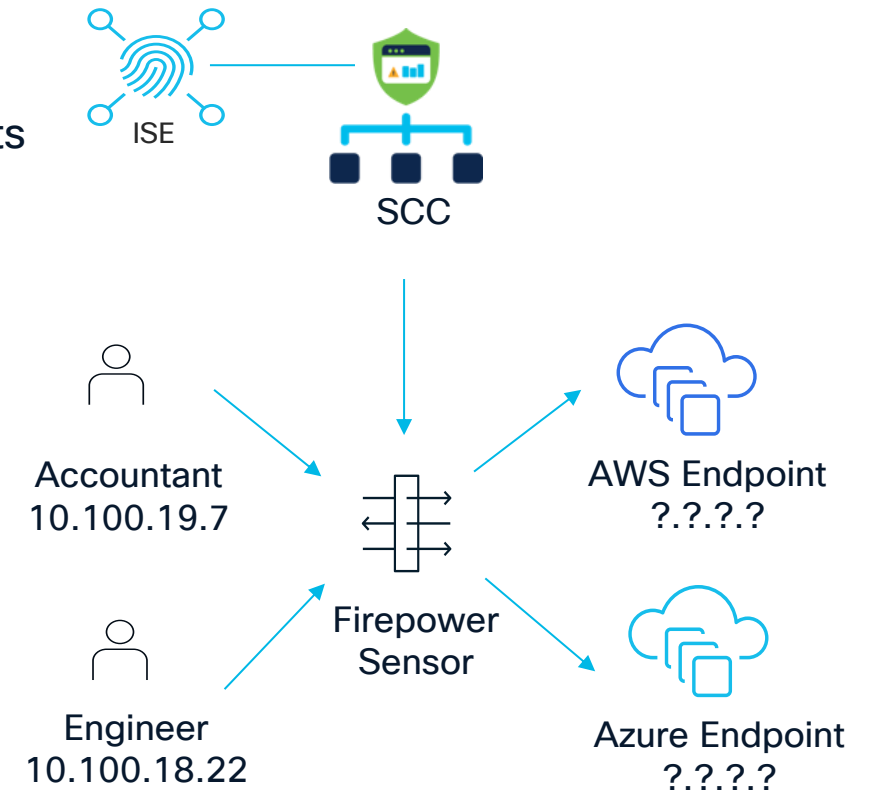
AWS Transit VPC

Simplifying Segmentation and Control



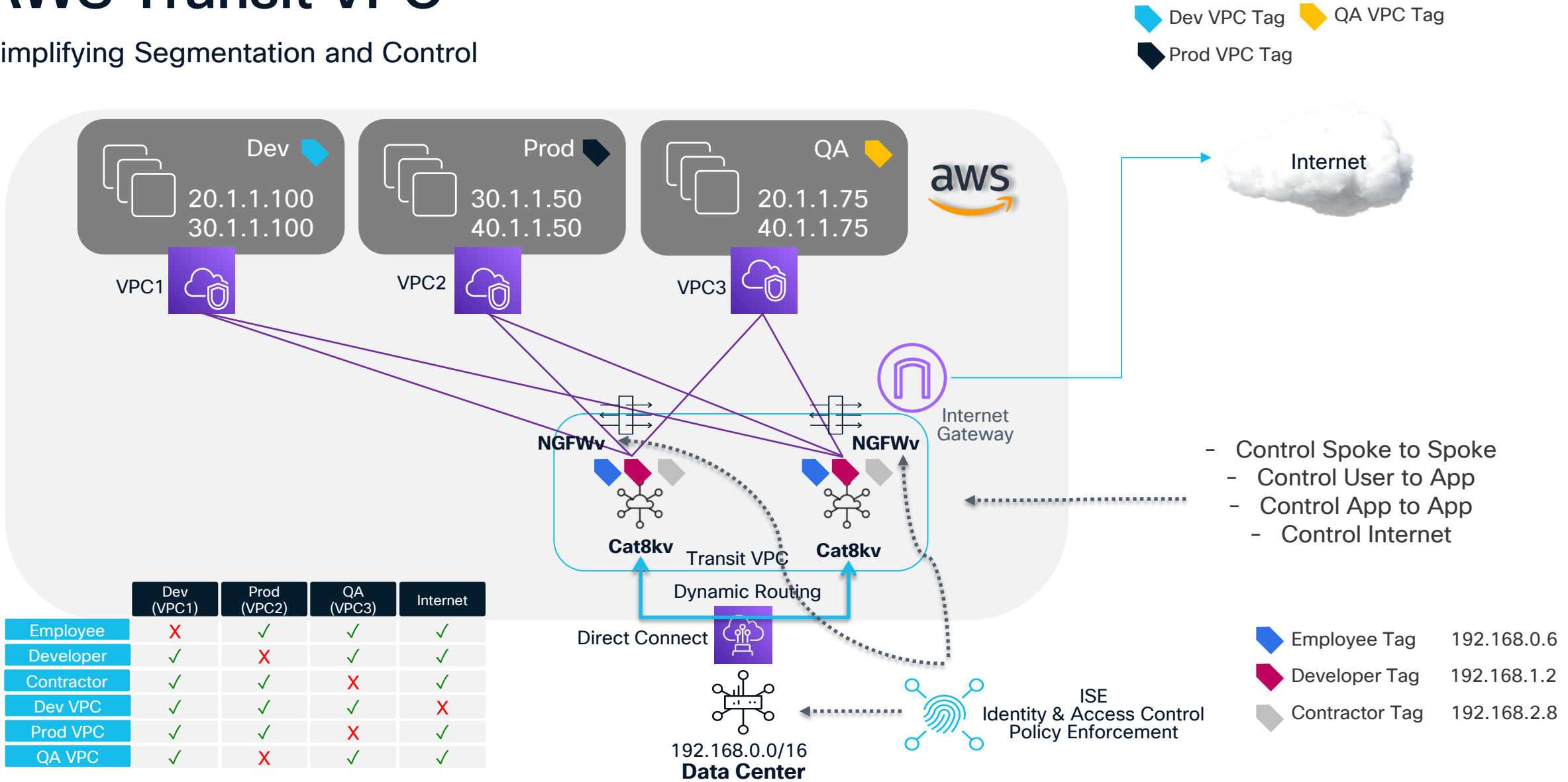
Cisco Secure Dynamic Attributes Connector

- Instead of manually defining the IP/Group mapping
- Gather attributes from dynamically changing cloud environments
- Subscribe to and pull dynamic IP feeds
- Ability to assign multiple IP addresses to multiple dynamic Firewall objects



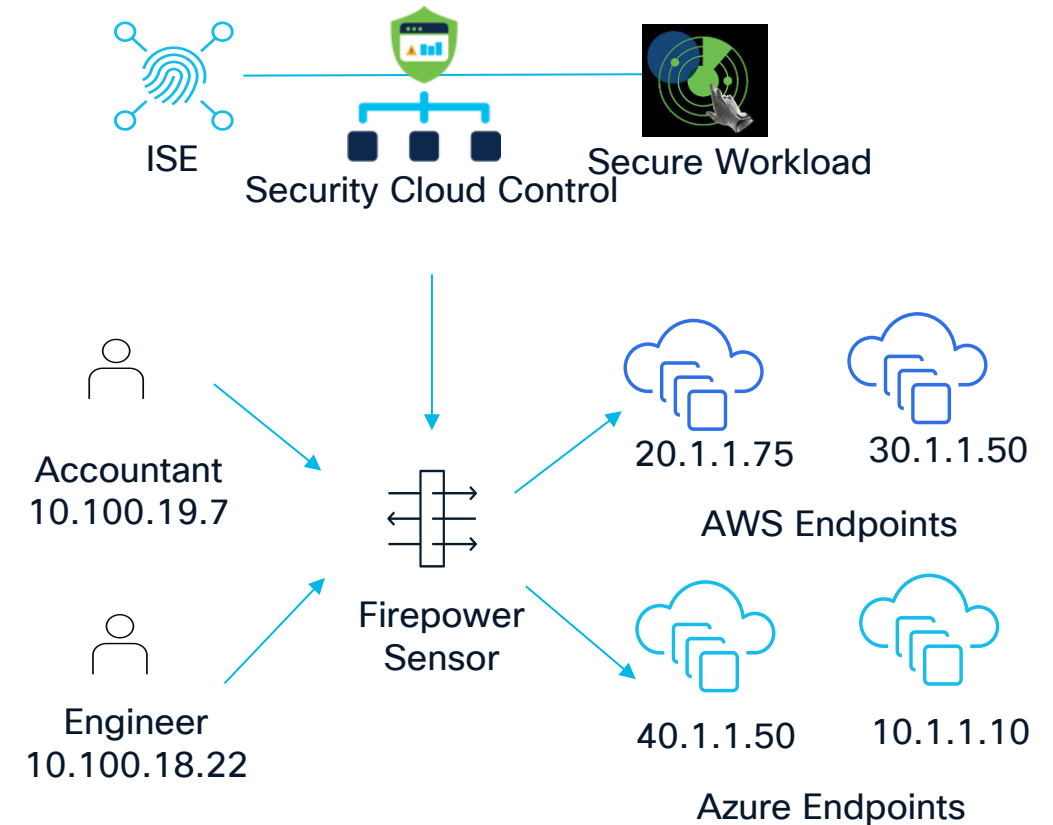
AWS Transit VPC

Simplifying Segmentation and Control



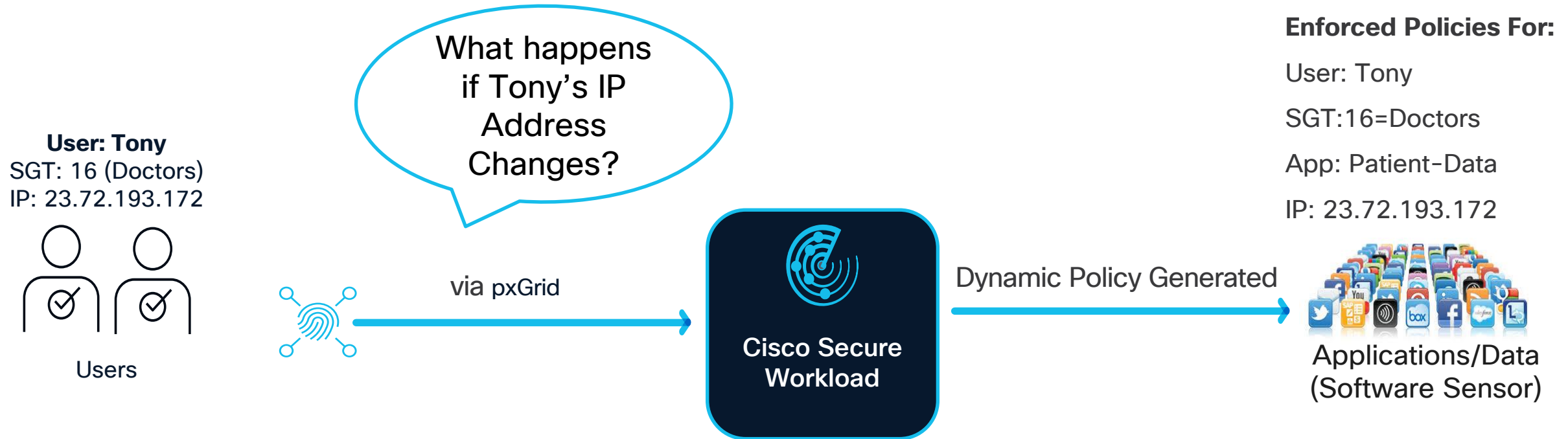
Cisco Secure Workload

- Segmentation policies enforcement at workloads
- Virtual Machines, Containers and Bare Metal
- Private and Public IaaS
- Prevent East / West lateral Movement
- Dynamic Policy
- Policy Enforcement
- Policy Visibility



Secure Workload with ISE

ISE Provides Identity to Secure Workload



- 1) The sensor endpoint is sending Telemetry data
- 2) The endpoint also authenticates with ISE which notifies our identity repository via pxGrid.
- 3) Secure Workload merges the two streams and outputs dynamically generated policy.



May not access employee data

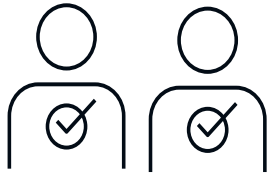


May access patient records

Secure Client (Any Connect)

Enterprise Policy Discovery

User: Steven
SGT: 20 (Doctors)
IP: 23.72.193.172



Users



Secure Client
(IPFIX)

via pxGrid



Dynamic Policy Generated



Applications/Data
(Software Sensor)

Enforced Policies For:

User: Tony

SGT:20=Doctors

App: Patient-Data

IP: 23.72.193.172

- 1) Secure Client Network Visibility Module (NVM) streams IPFIX to Secure Workload
- 2) The endpoint also authenticates with ISE which notifies our identity repository via pxGrid.
- 3) Secure Workload merges the two streams and outputs dynamically generated policy



May not access employee data



May access patient records

Security: In & Between the Clouds

Personas



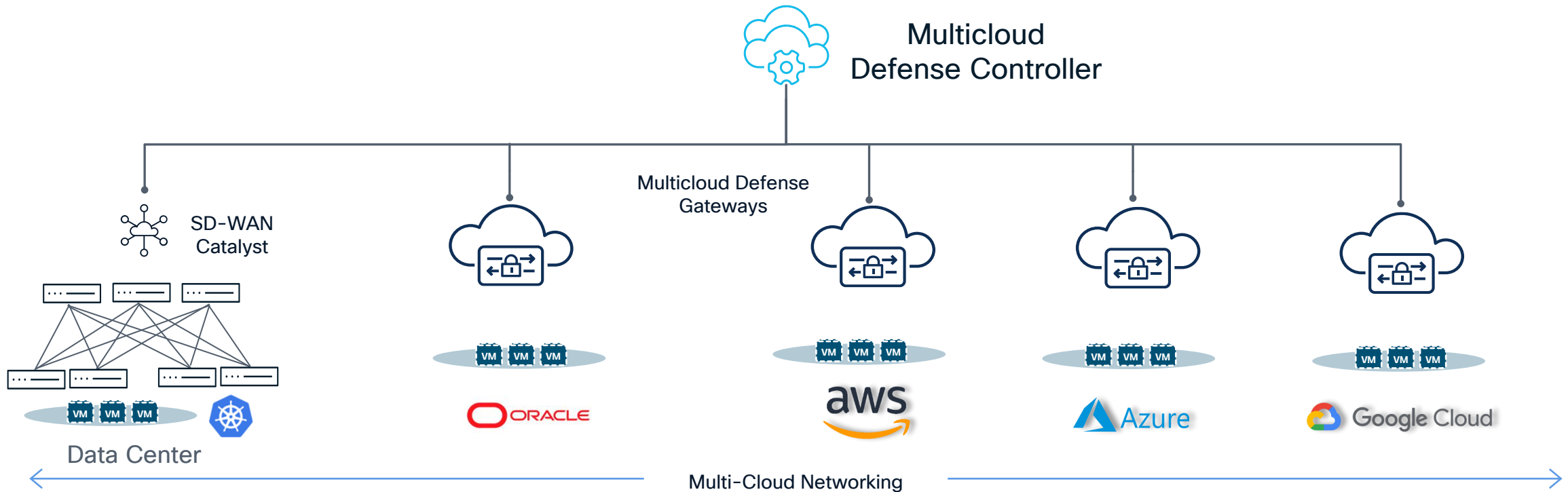
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
le. Firewall

Multicloud Defense

Cloud networking, automation, and cloud-native network security controls



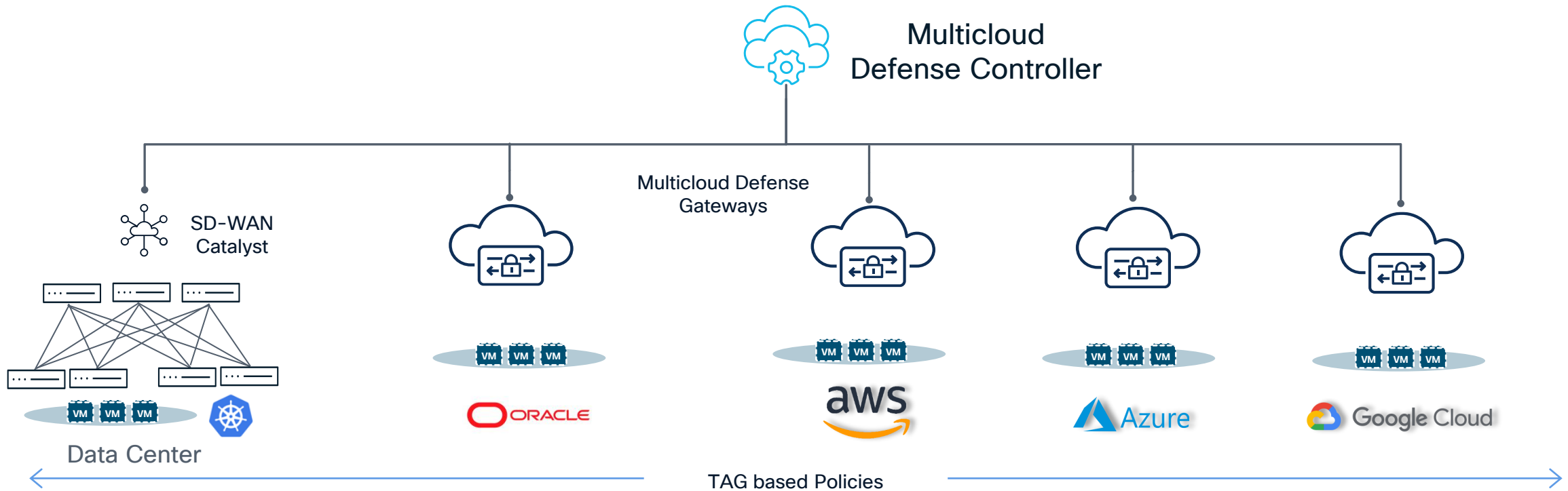
Dynamic Classification &
Security Automation

Unified Security Policy

Segmentation (East/West)
Ingress/Egress Protection

Auto-Scaling

Dynamic Unified Security Policy



Dynamic Multicloud Policy

Construct Mappings



Multicloud Defense Gateways



Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP



Egress Gateway

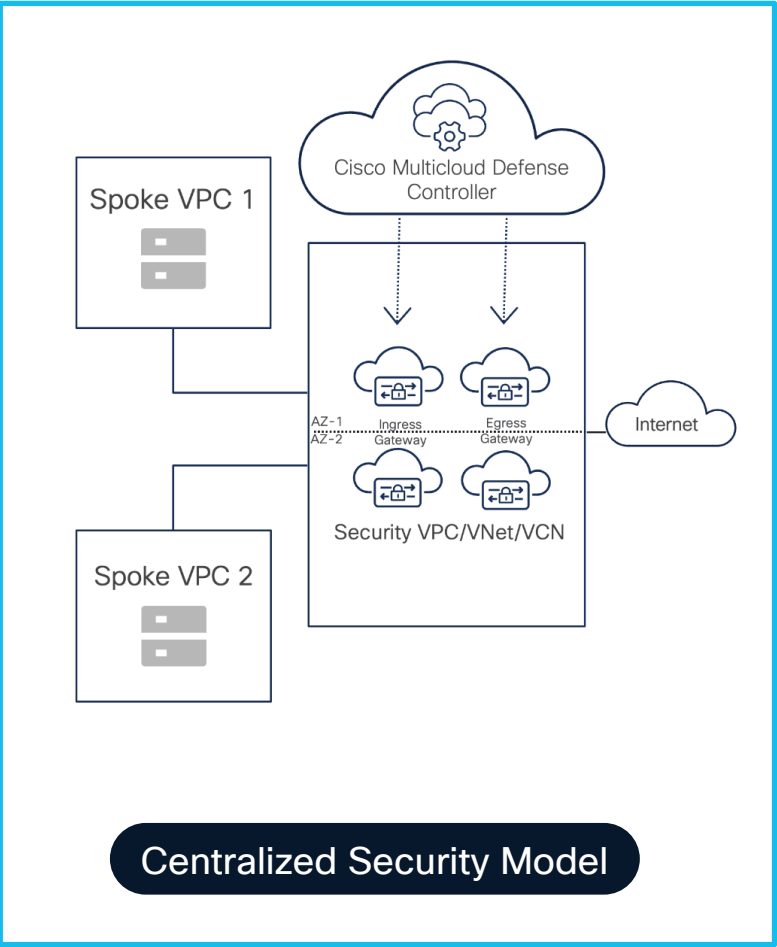
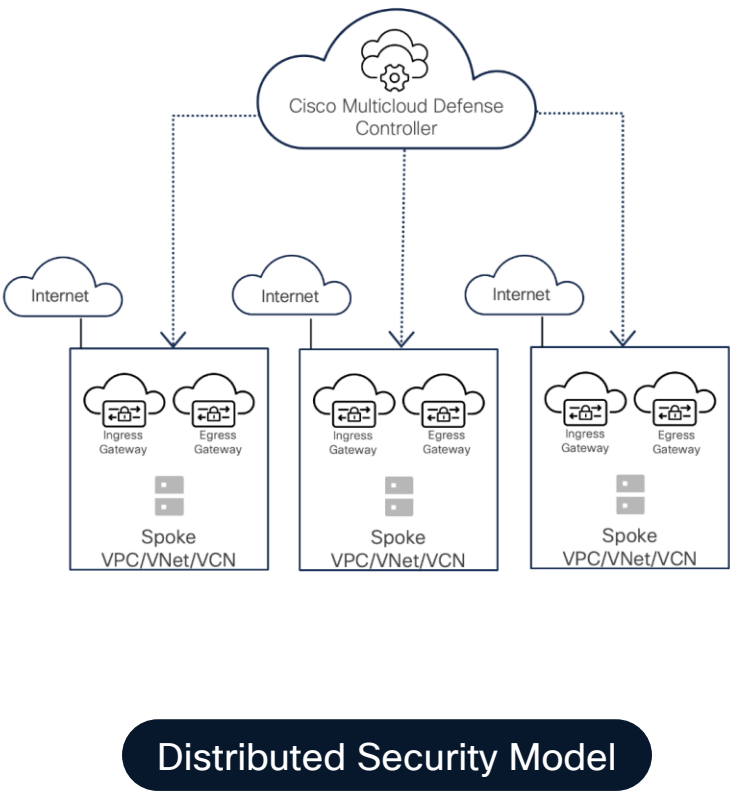
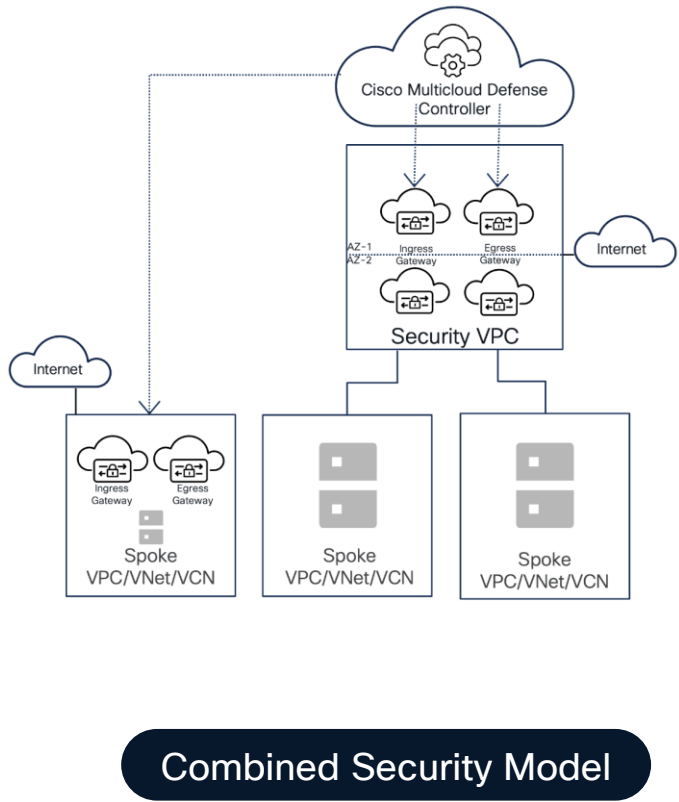
Egress

URL filtering
Forward proxy
TLS decrypt
FQDN filtering
FQDN-based firewall policy
DLP
IDS / IPS
Antivirus

East/West

FQDN filtering
IPS / IDS
Antivirus
Segmentation
FQDN-based firewall policy
TLS decrypt

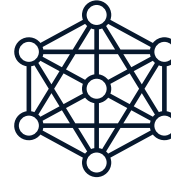
Security Models



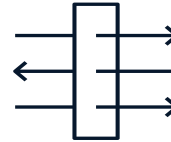
What is New?

Centralized Gateway Model

- Ability to add FTDv Gateway
- FTD Feature Set + Capabilities
- Common-Policy
- On-prem management for Cloud Security



Security Cloud Control



FTDv Firewall

SDWAN

Secure
Firewall

Multicloud
Defense

Hypershield

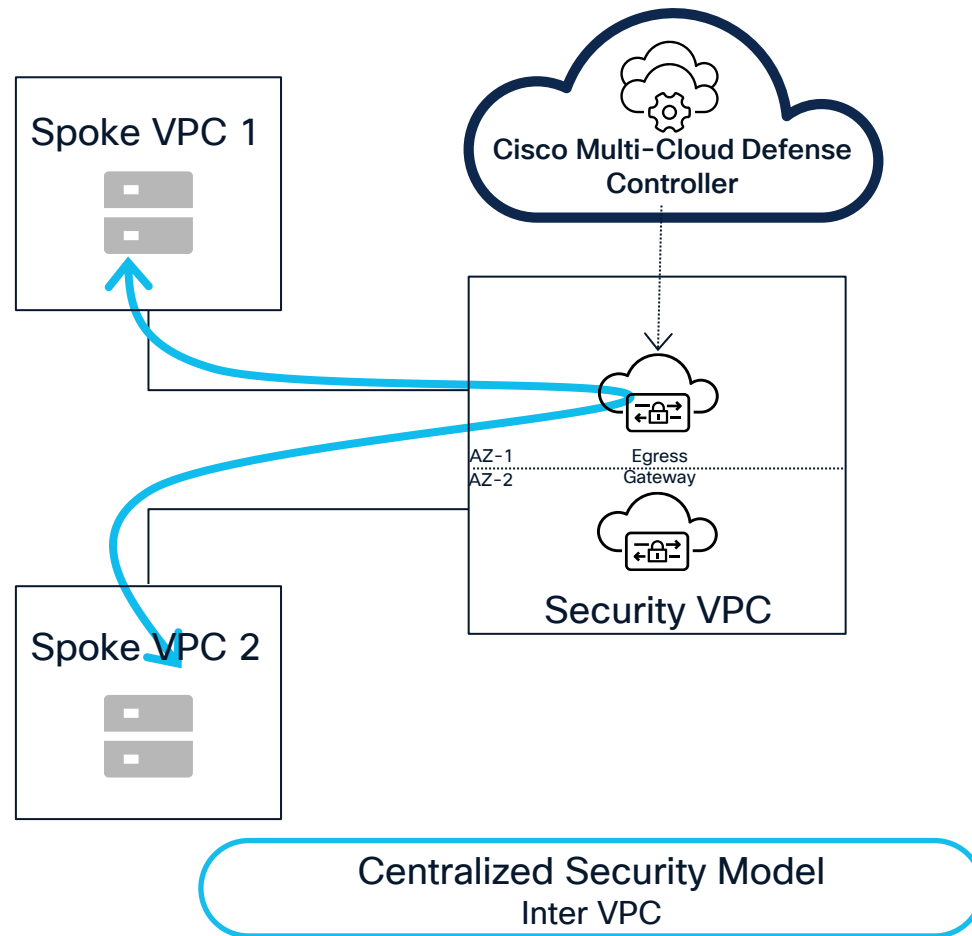
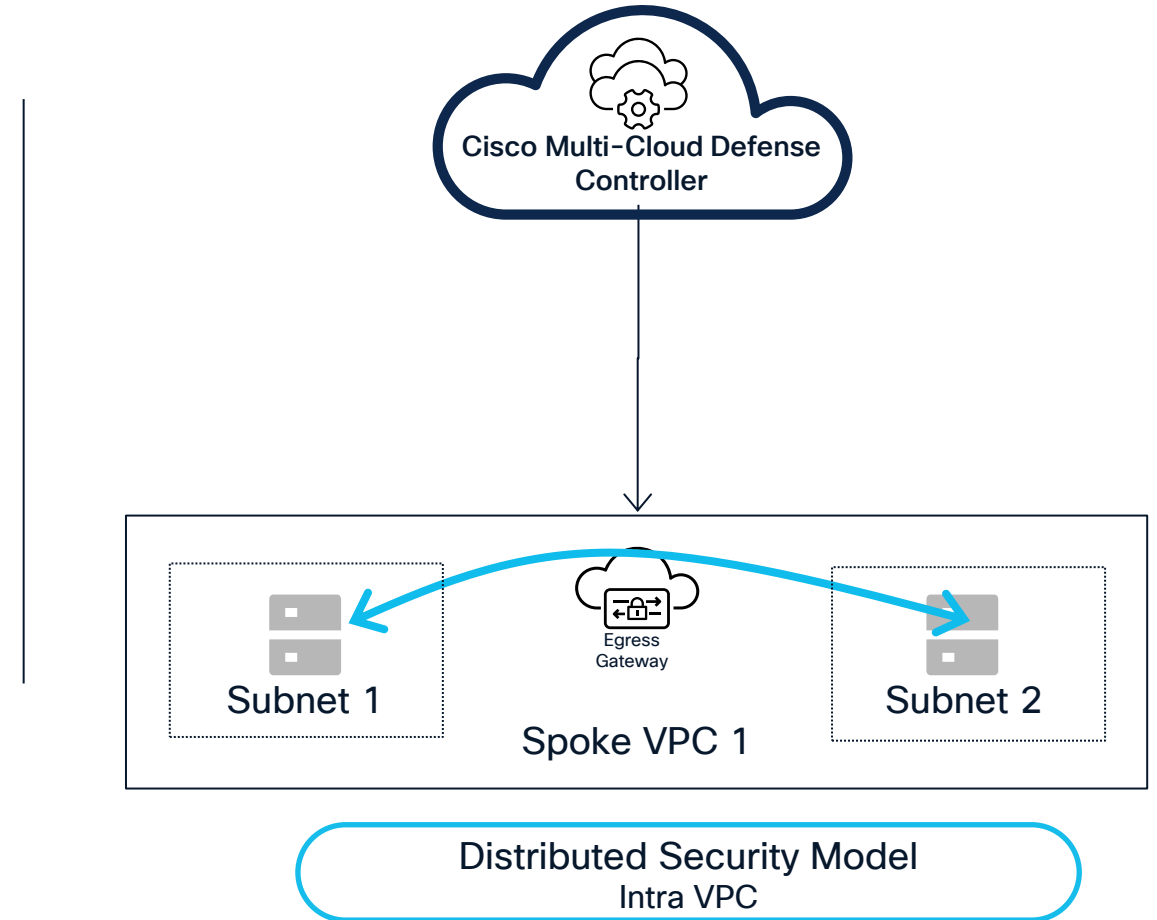
Secure
Workload

Secure
Access

AI Defense

Segmentation

Use Case

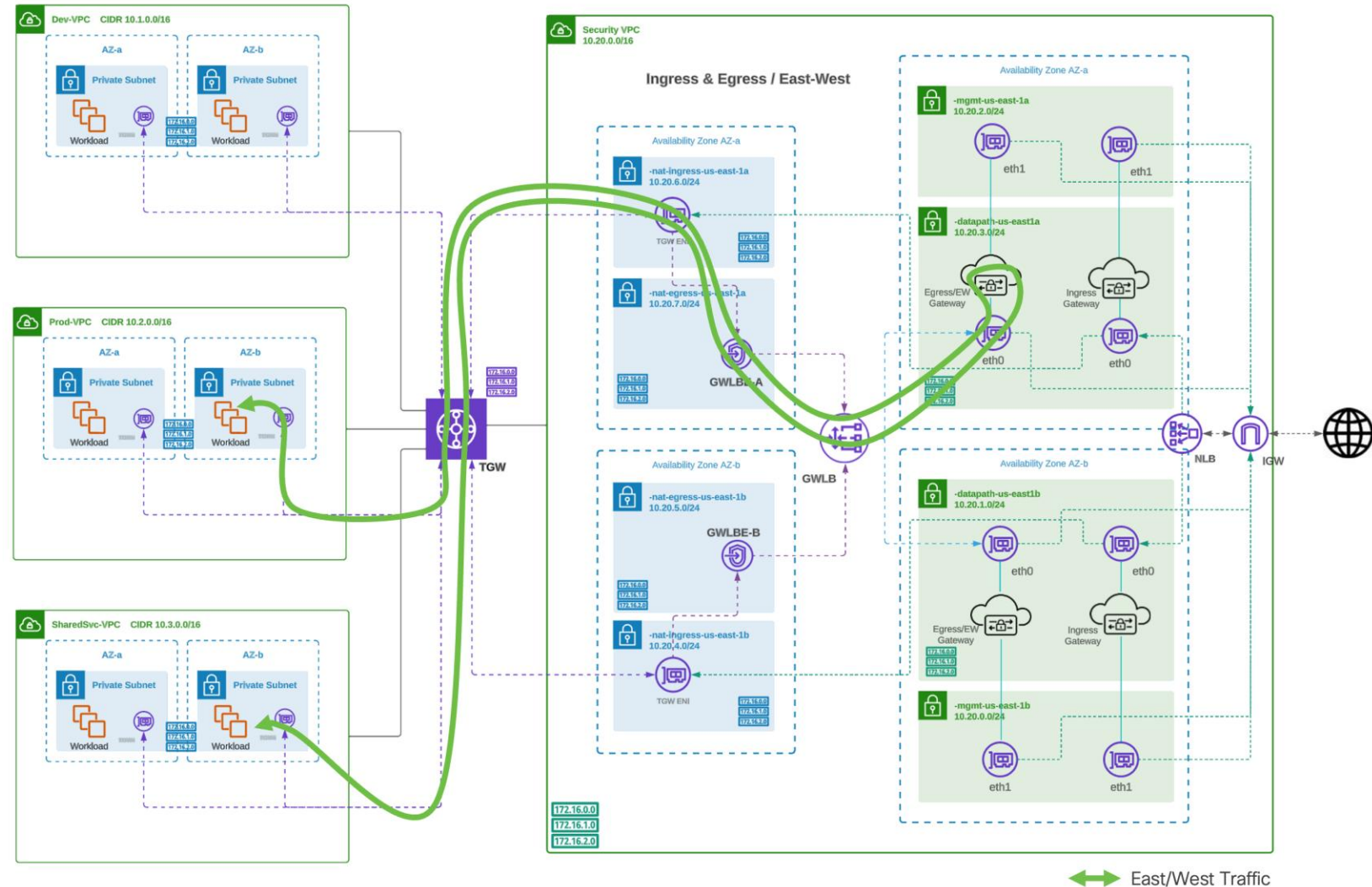


AWS Centralized

East-West Traffic Inspection (Inter-VPC)

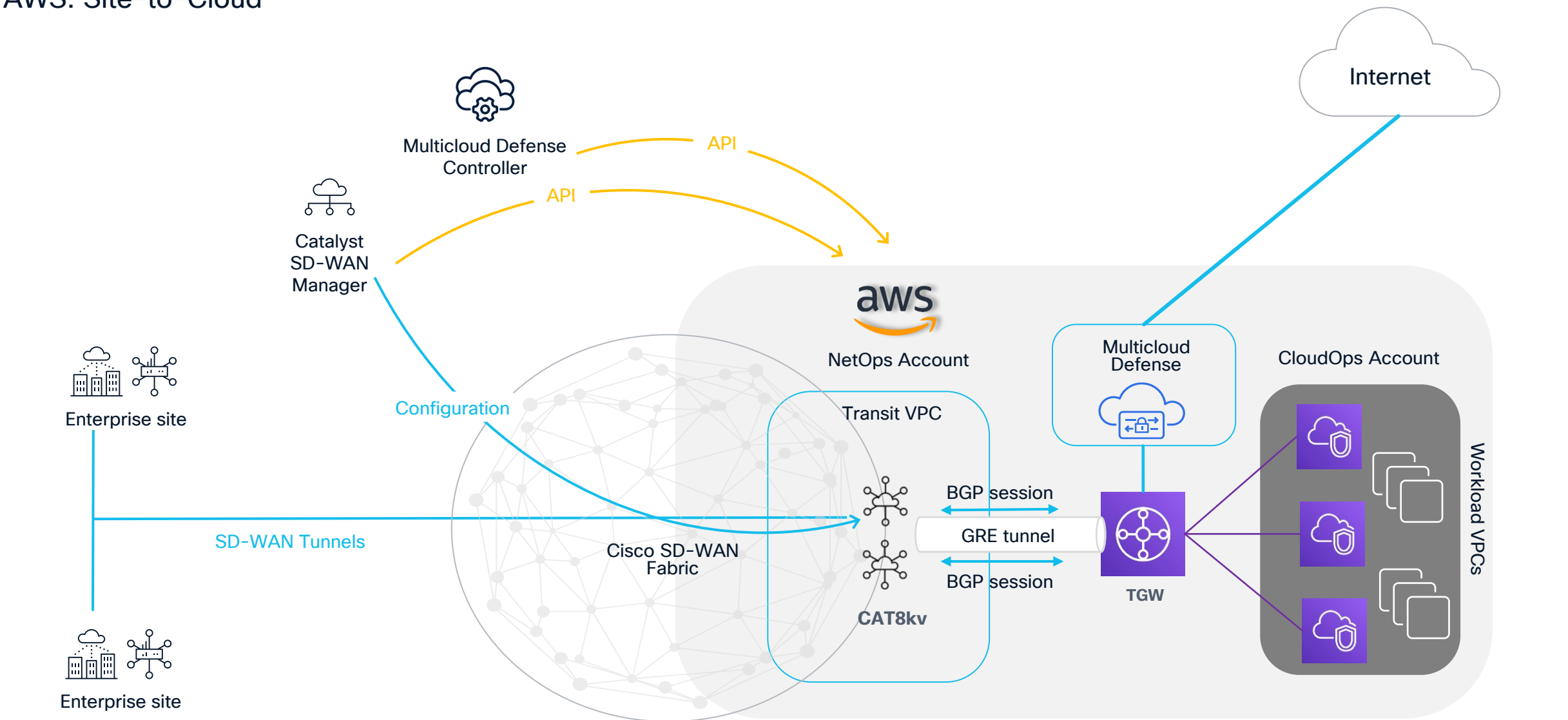
Controller simplifies orchestration

- Security VPC
- Multicloud Defense Gateways
 - Deployment
 - Insertion
 - Autoscaling
- AWS Transit Gateway
 - New or existing TGW
 - TGW attachment
- Traffic engineering (routing)
 - VPC subnet routing to TGW
- AWS Gateway Load Balancer for scalability



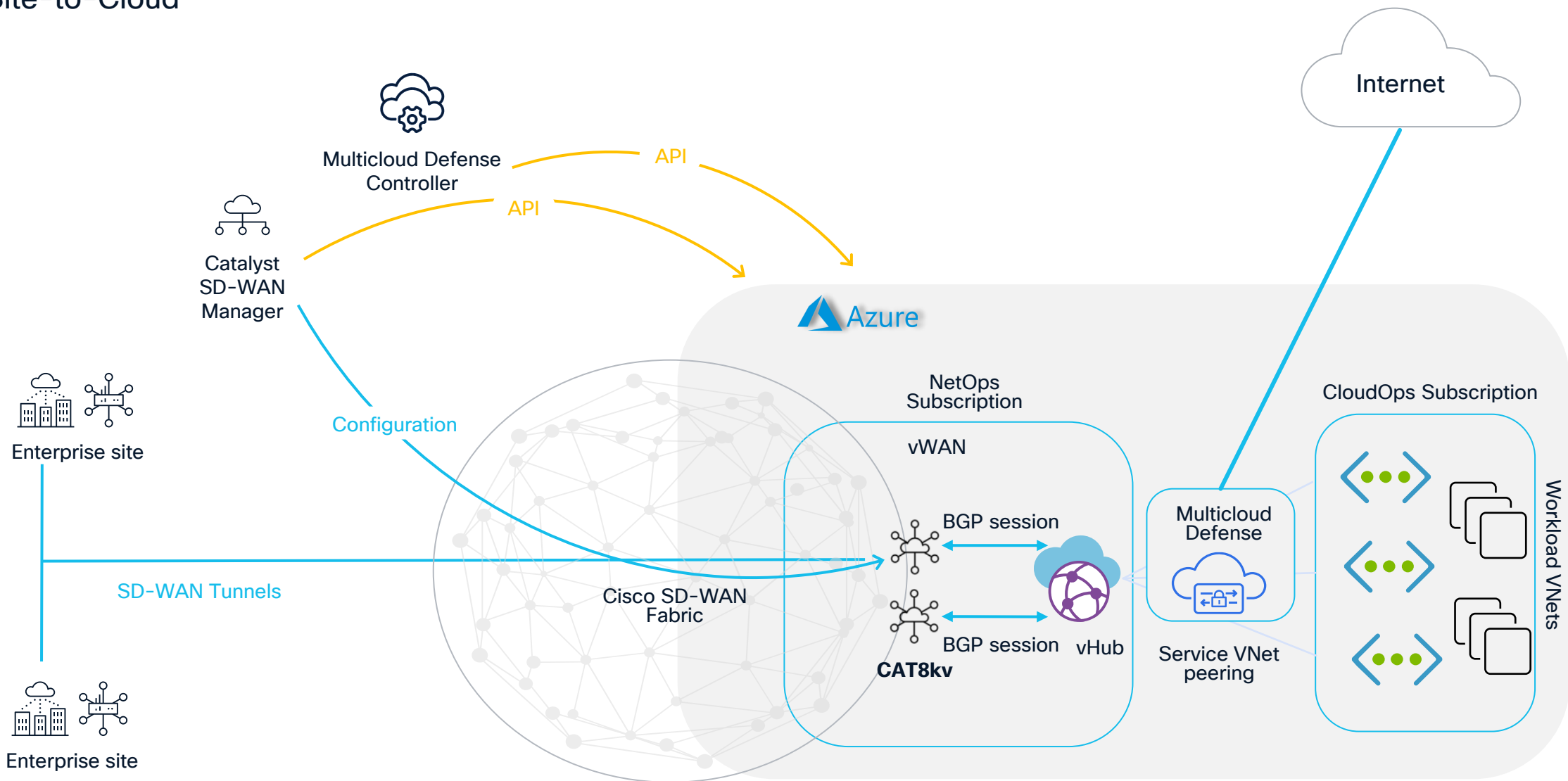
SDWAN + Multi-Cloud Defense

AWS: Site-to-Cloud

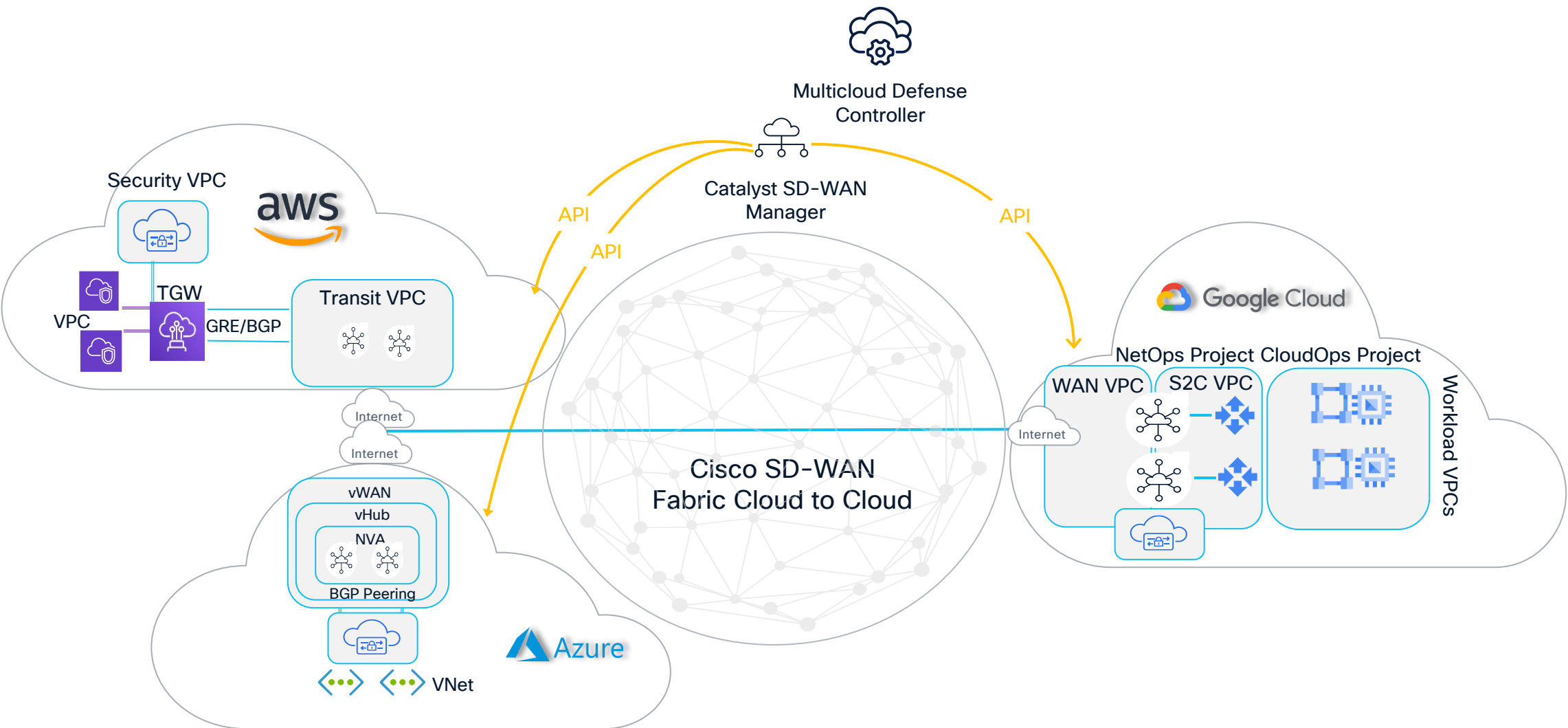


SDWAN + Multi-Cloud Defense

Azure: Site-to-Cloud

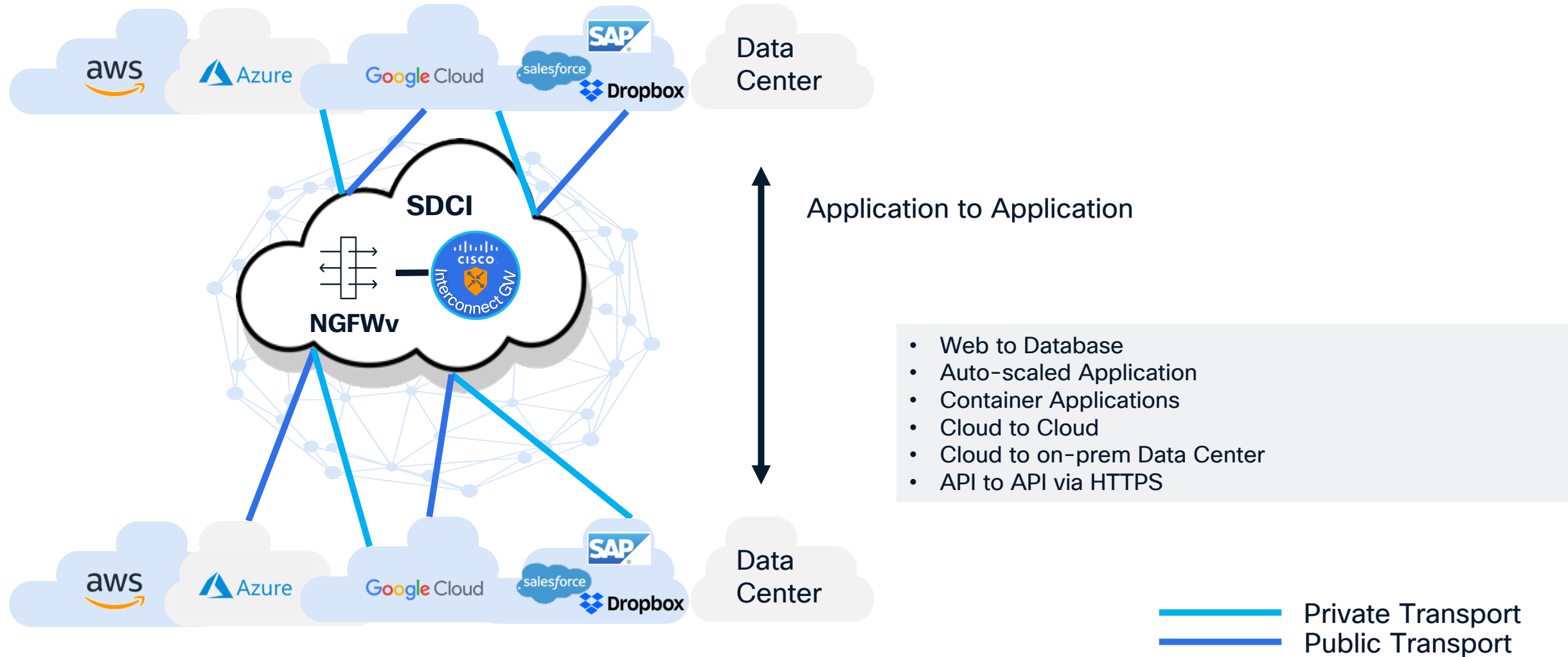


Security Stack Insertion in the Cloud



Transparently secures Application-to-Applications

SD-WAN + NGFWv + MCD

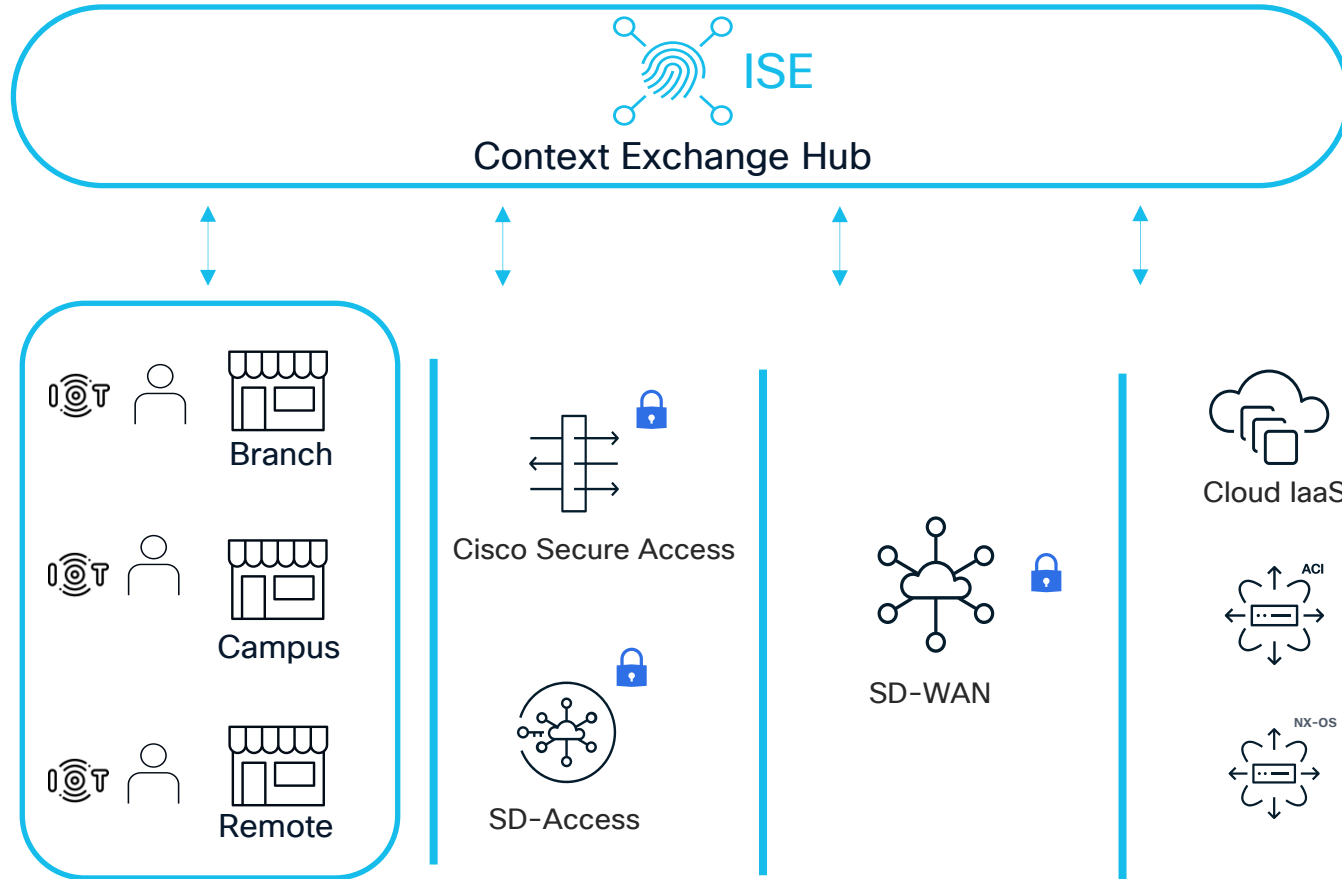


Common Policy

We talked about...



Common Policy



 Policy Enforcement Points:
Consistent Policies



Build context in its local domain and store it as standard security group tags (SGT).



Share context everywhere, across networking and security domains.



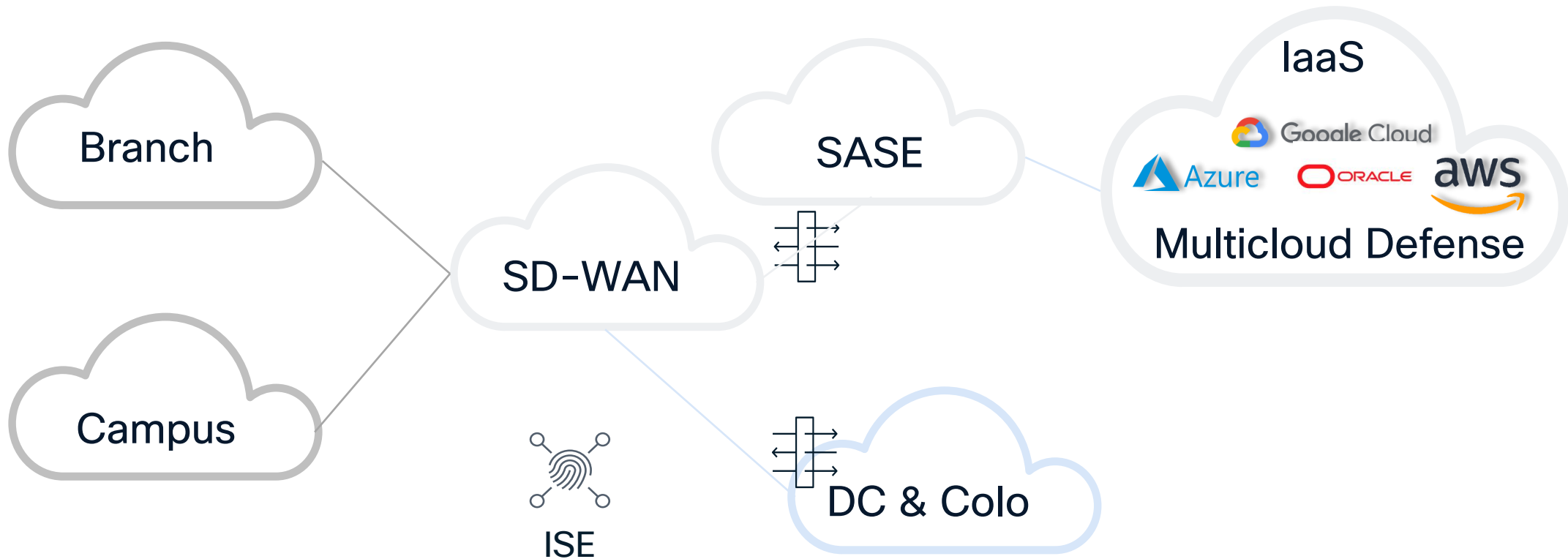
Enforce consistent SGT-based policies; enable simple and unified policy experience.



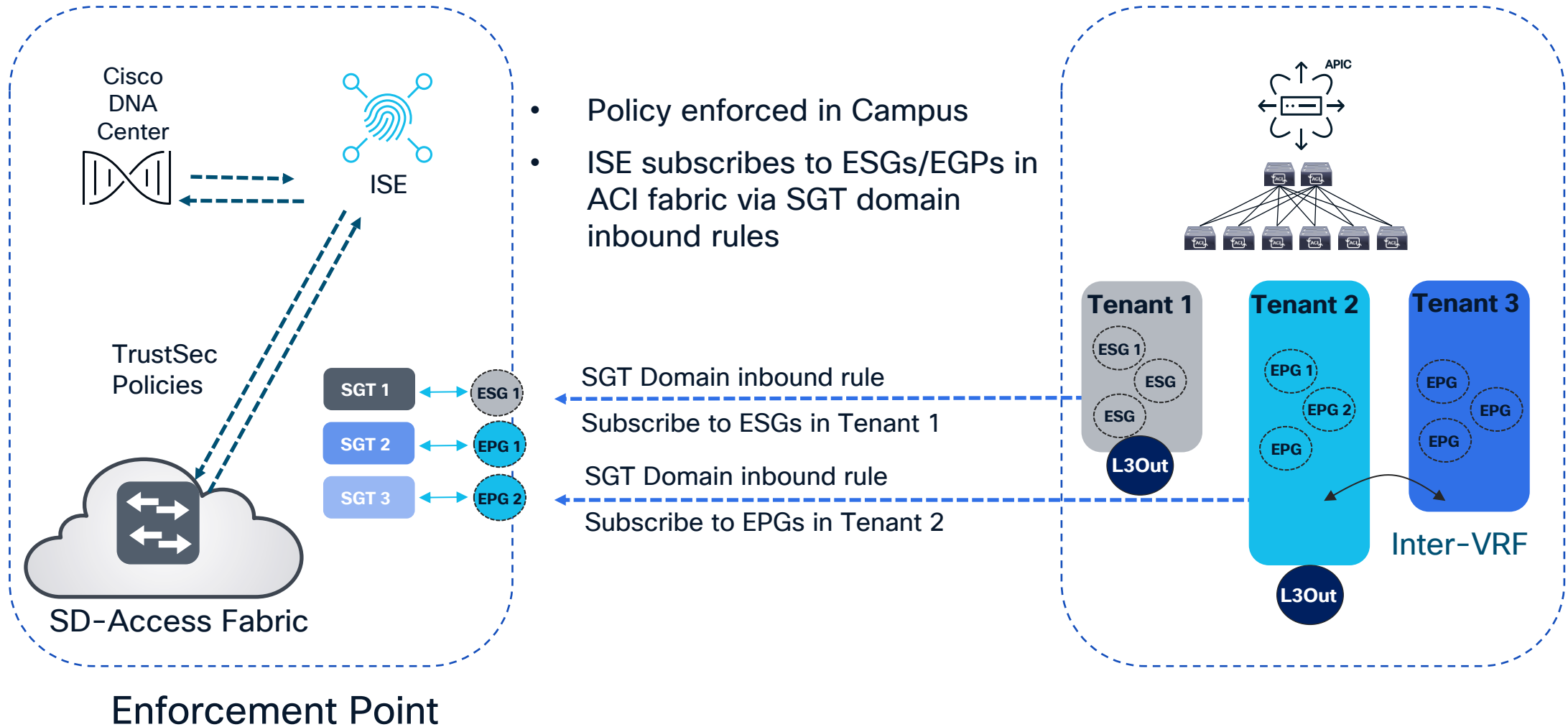
- Context-aware policies for on-prem app and cloud workloads for multiple enforcement points
- Leveraging existing investments in ISE, Catalyst & Nexus Switching & Catalyst Center

Common Policy

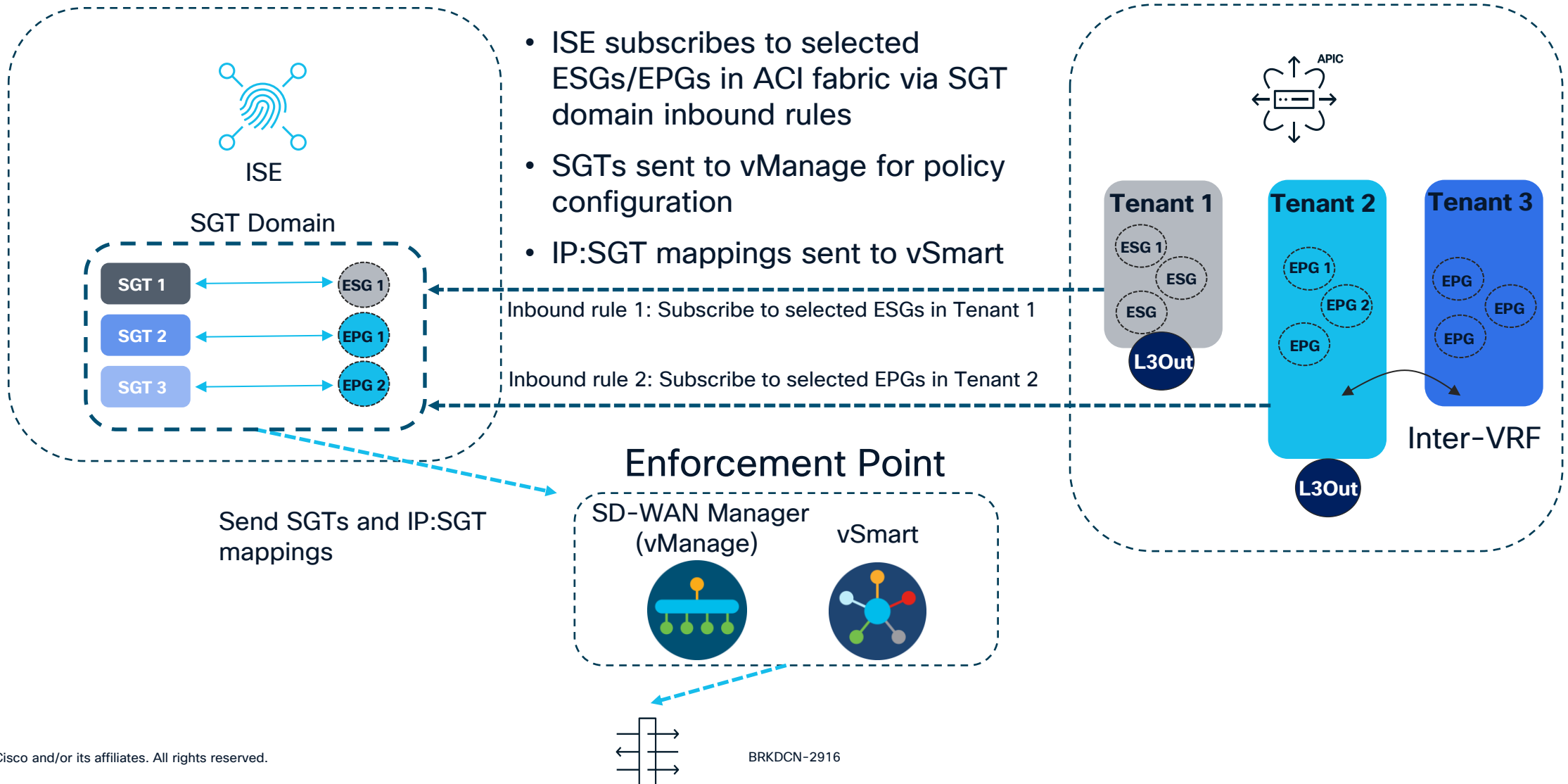
Use Cases



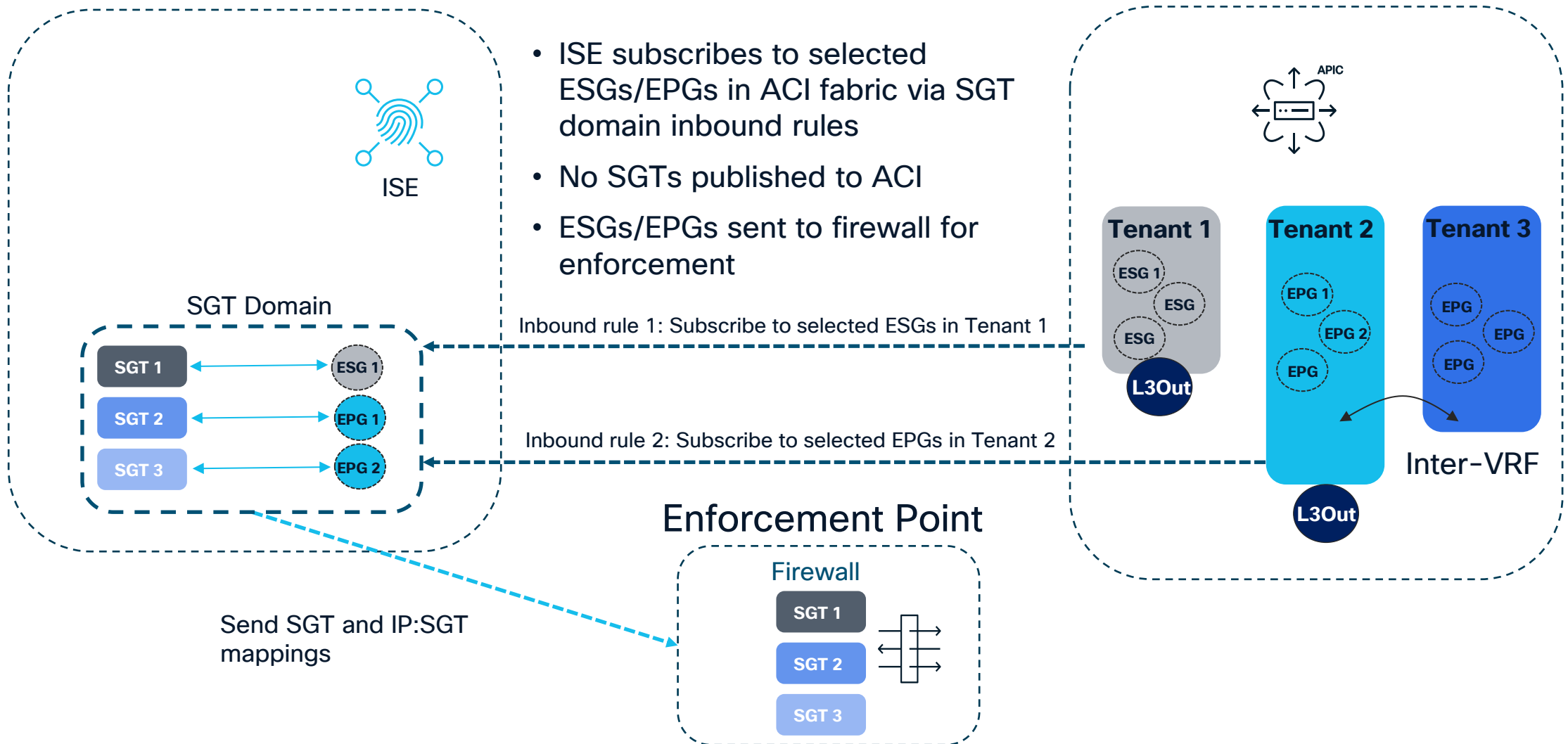
Use Case: Policy Enforcement in Campus



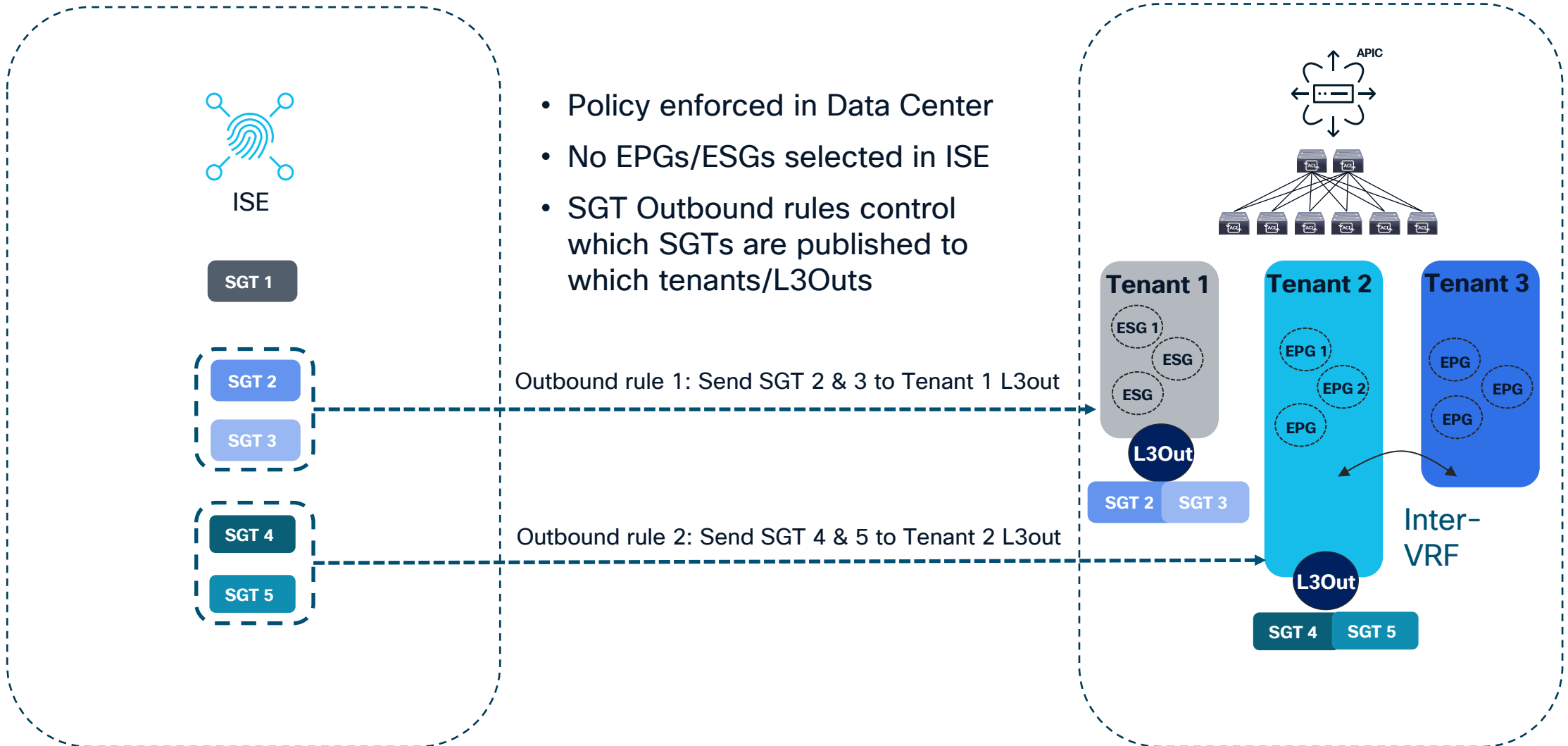
Use Case: Policy Enforcement in SD-WAN



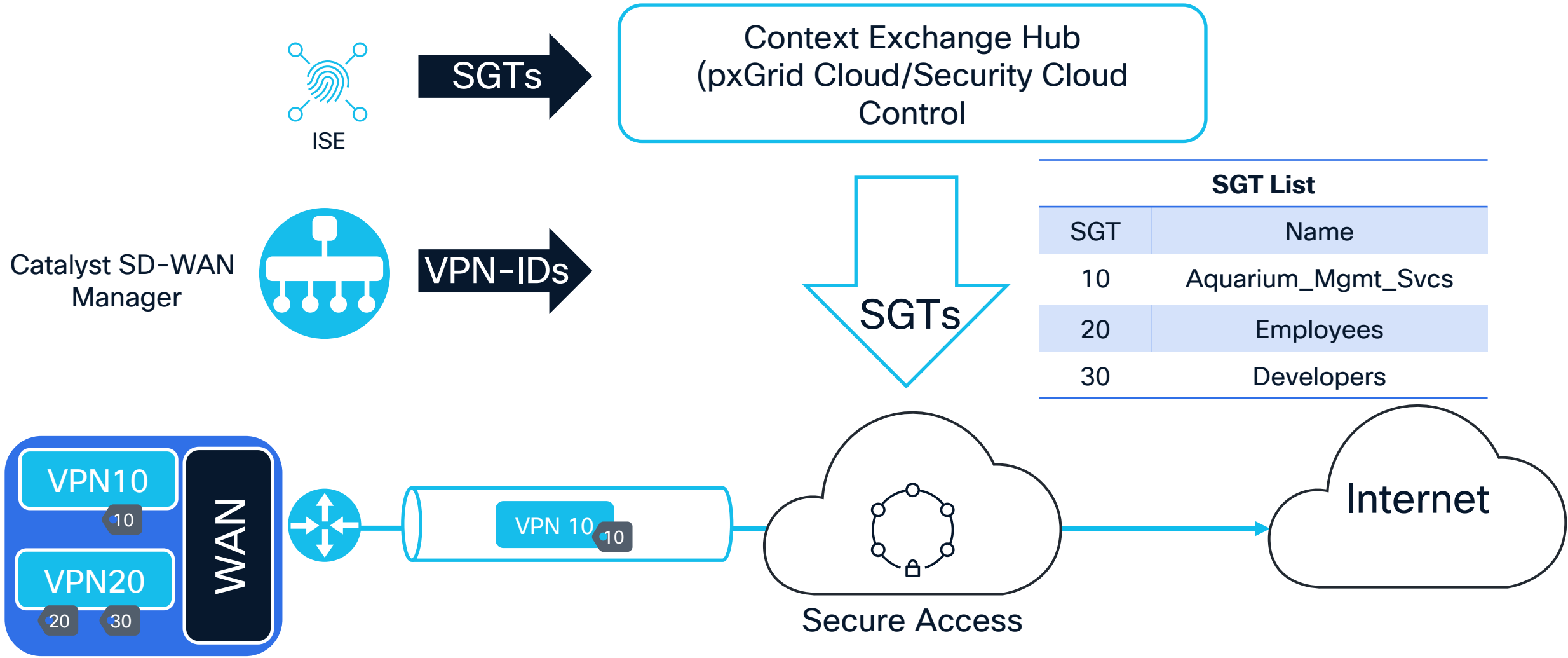
Use Case: Policy Enforcement in Firewall



Use Case: Policy Enforcement in Data Center



ISE / SD-WAN / Secure Access Integration



Common Policy

Bringing it all Together

Micro-Segmentation

- VXLAN GPO allows the user to define policies for micro-segmentation.



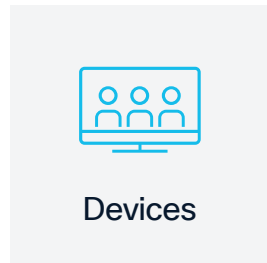
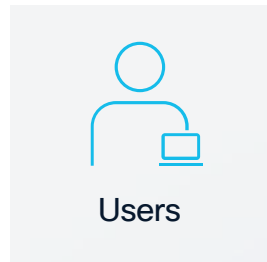
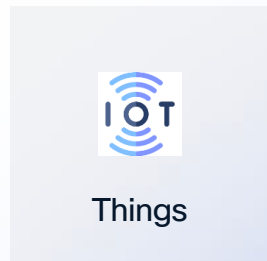
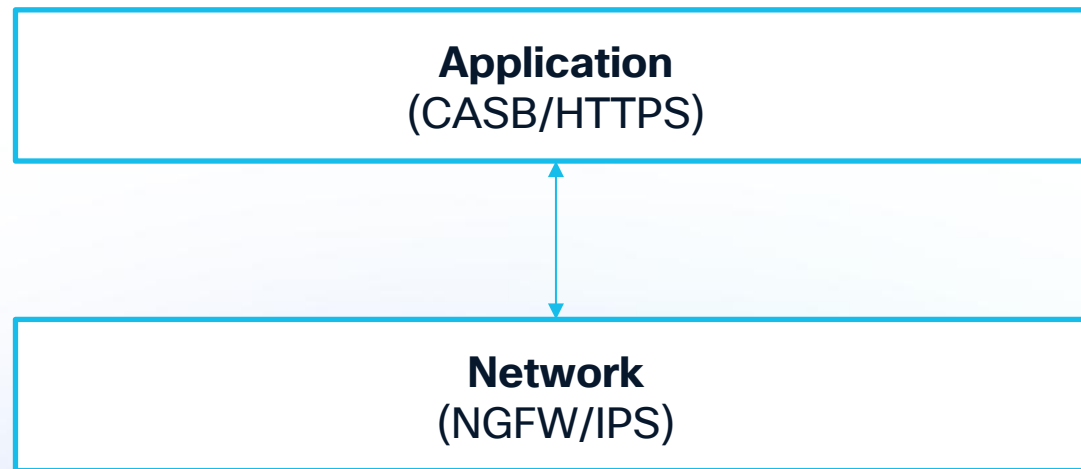
Service Chaining

- VXLAN GPO can be used to insert network services into a packet flow based on specific policy criteria.



Inside each use case is the ability to apply policy for Micro-Segmentation and/or Service-Chaining

Hybrid ZTNA



Visibility

Visibility: AWS Inter Region

Path Visualization

3 hops

1 hop

Showing: 1 of 1 Test ▾ 1 of 12 Agents ▾ (Show All) Show IP Address labels ▾

Grouping: Agents by Agent ▾ Interfaces by Network & Location ▾

Highlighting: Forwarding Loss > 5 % (0 nodes) ▾ **Link Delay > 40 ms (3 links) ▾**

Selecting: Click a node or link Info (1) ▾

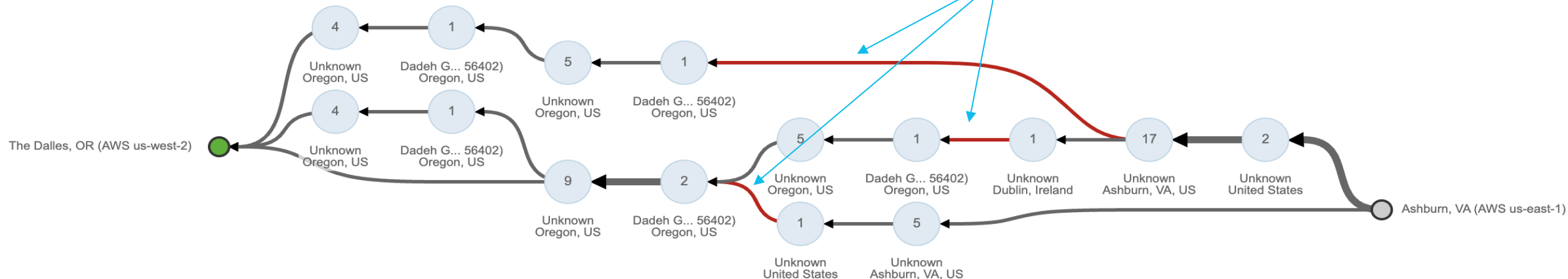
Highlight nodes that match all / any

Search on Network, Country, IP address, Prefix, or Title...

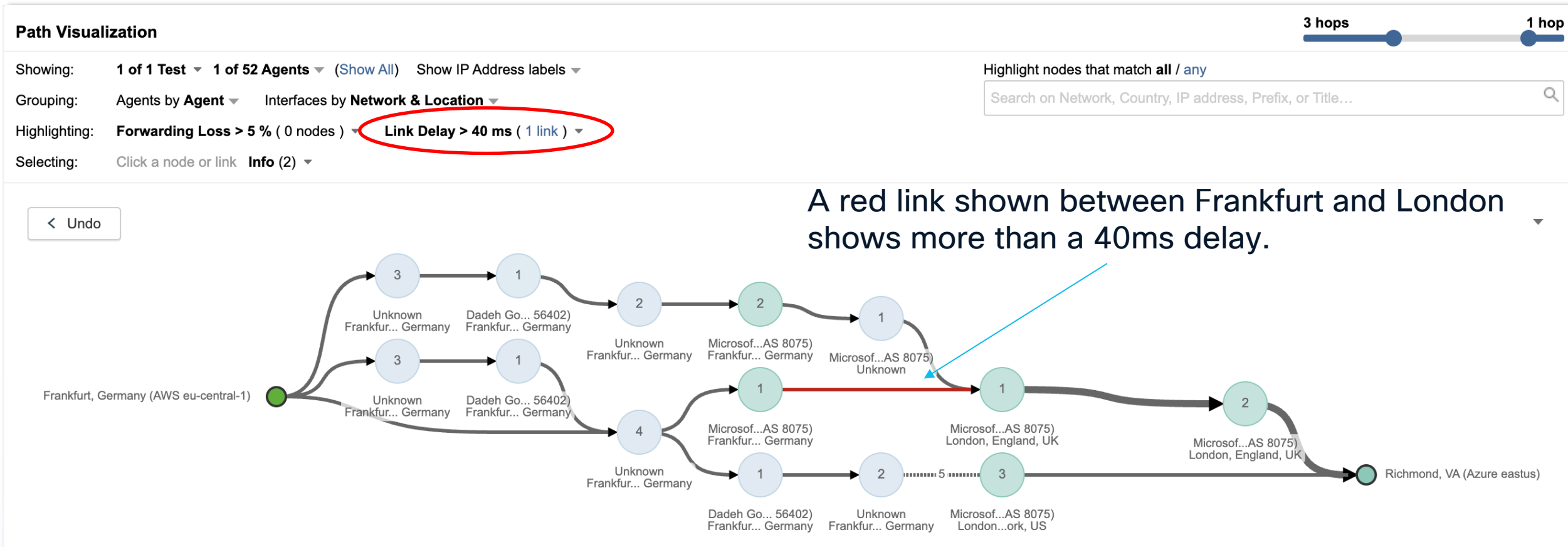


< Undo

The red links show greater than 40 ms latency.

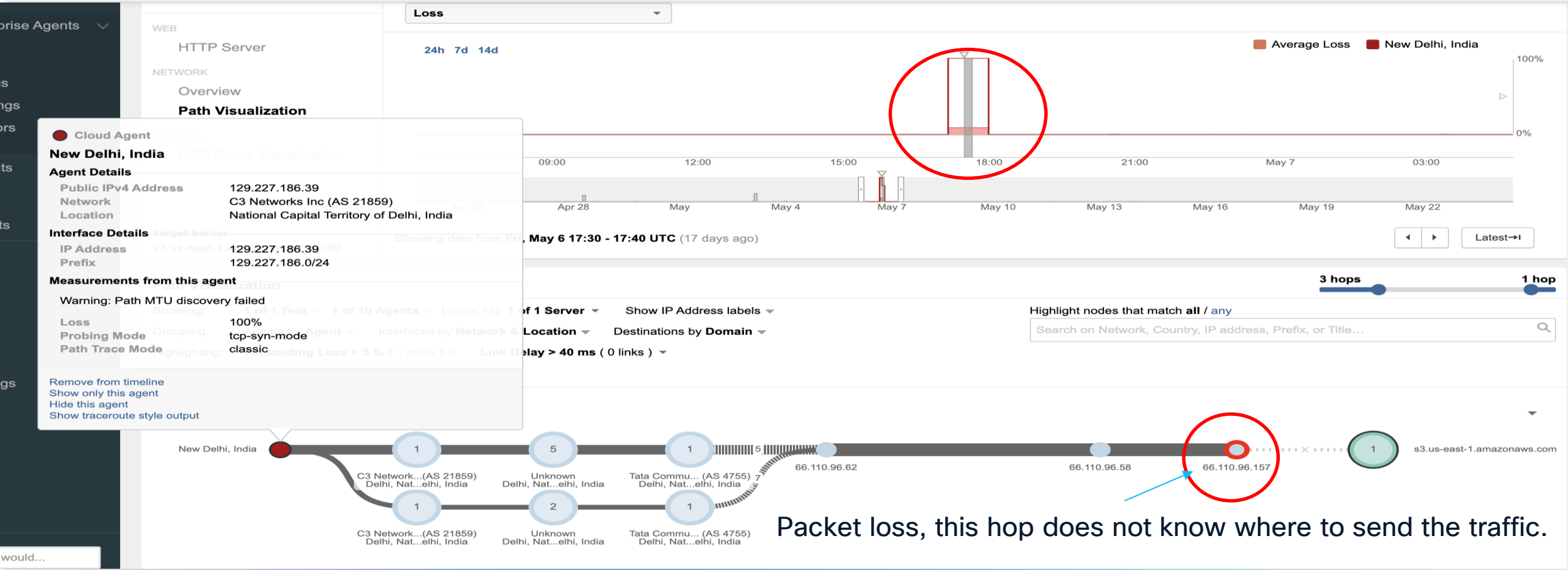


Visibility: AWS/Azure Inter Cloud



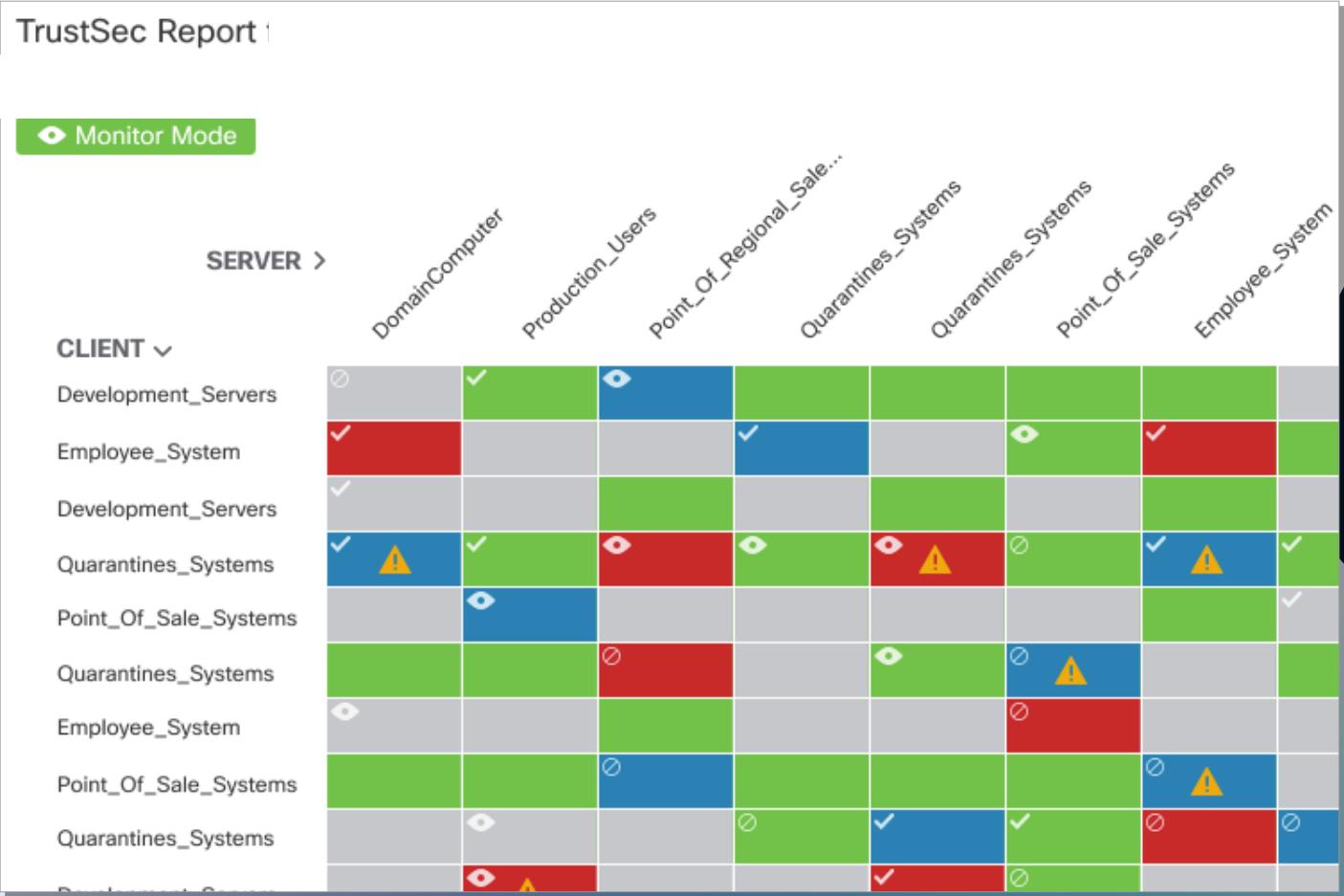
- Provider-to-provider path analysis w/ direct peering relationships.
- Traffic from AWS through an intermediate provider but still gets on the Azure backbone before leaving Frankfurt

Visibility: AWS/Azure Inter Cloud



Depicted above is the loss of service, source of loss and time of outage.

Secure Network Analytics



Cell Details ⚠️

TRAFFIC INFORMATION

1002 TB

Quarantines_Systems

Development_Servers

282 MB

Traffic Volume:
Start: ...
End: ...

PROTOCOLS

⚠️ ICMP (11KB)

...

TCP (2.5GB)

...

⚠️ UDP (0.6MB)

...

PORTS

22/SSH (320MB)

...

80/HTTP (100MB)

...

⚠️ 443/HTTPS (2GB)

...

⚠️ 54180 (52MB)

...

[View Flows](#)
[View Offending Traffic Flows](#)

ISE DATA

ISE Policy

Enabled ✓

SECURITY GROUP ACLS

Name:

DevProdCommunication

IP Version:

IP Agnostic

ACEs:

Deny IP
permit tcp eq 80
permit tcp eq 22

Digital Resilience



1 Foundational Visibility

2 Guided Insights

3 Proactive Response



Digital Resilience: Proactive intelligence, predictive recommendations, and automated remediation for Infrastructure, Security and Applications.

Finally, What About Infrastructure as Code?



<https://registry.terraform.io/namespaces/CiscoDevNet>

<https://galaxy.ansible.com/cisco>



Summary

Outcomes

- 1 As users / devices / things / applications and data are everywhere; common policy simplifies and automates for the customers Enterprise
- 2 Security Cloud Control extend security perimeter and enforcement
- 3 Common Policy to simplify policies for users / devices / things + on-prem app and cloud workloads for multiple enforcement points
- 4 Digital resilience allows security detections, investigations and remediation to become much faster; reducing the customer impact

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: bburesh@cisco.com

Thank you

CISCO Live !

