

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Architecting Hybrid Multi-Cloud Infrastructures

David Jansen – CCIE #5952
Distinguished Solutions Engineer
BRKDCN-2916

A little bit about David...



Cisco role: Distinguished, Solutions Engineer; Global Solutions Engineering.

Experience: My career @Cisco has spanned half of my life.

Fun fact 1: Written / published 4 books; 6 video series.

Fun fact 2: Enjoy the outdoors, music, working out, running.

Most Importantly: I am here for you!

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2916>



Agenda

- Current Challenges, Issues, Administration and Options
- Key Capabilities
- Connecting Users / Devices / Thing to the Cloud
- Applications behind SD-WAN and Cloud Security
 - Use-Cases
 - Expanding Policy to Public IaaS
 - Security: In & Between the Clouds
- Common Policy
- Visibility / Day2 Operations
- Summary

Session Focus Areas

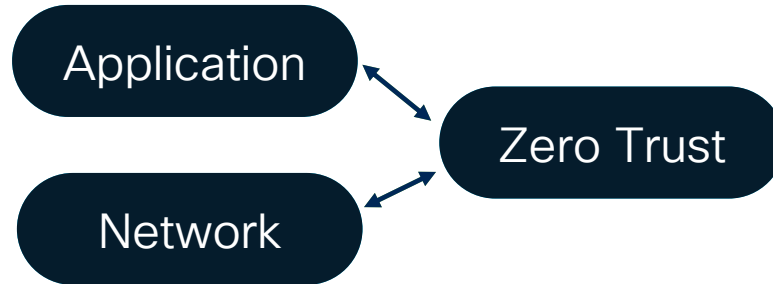
Abstract

Cloud continues to be a major disruptor; 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
- I 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

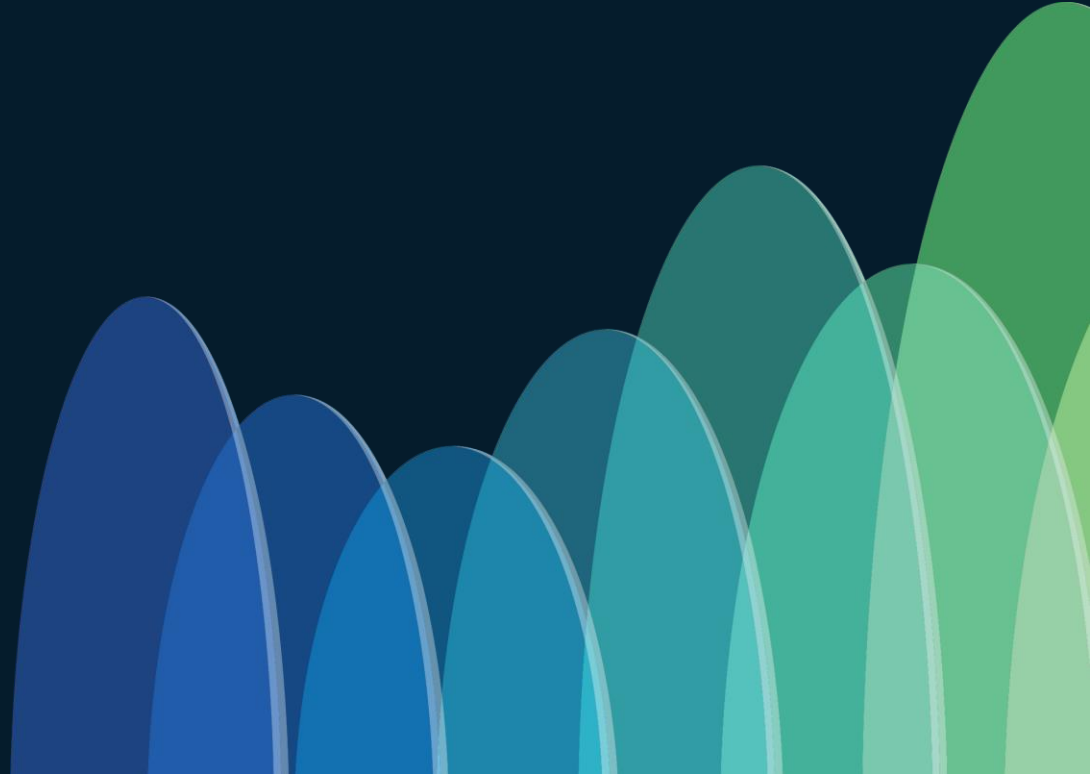
Cloud Terminology Matrix



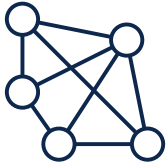
For Your
Reference

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

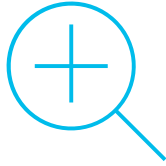
Current Challenges, Issues, Administration and Options



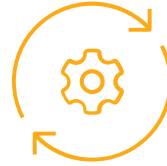
Challenges to solve



Network
connectivity



Operations
and visibility



Automation

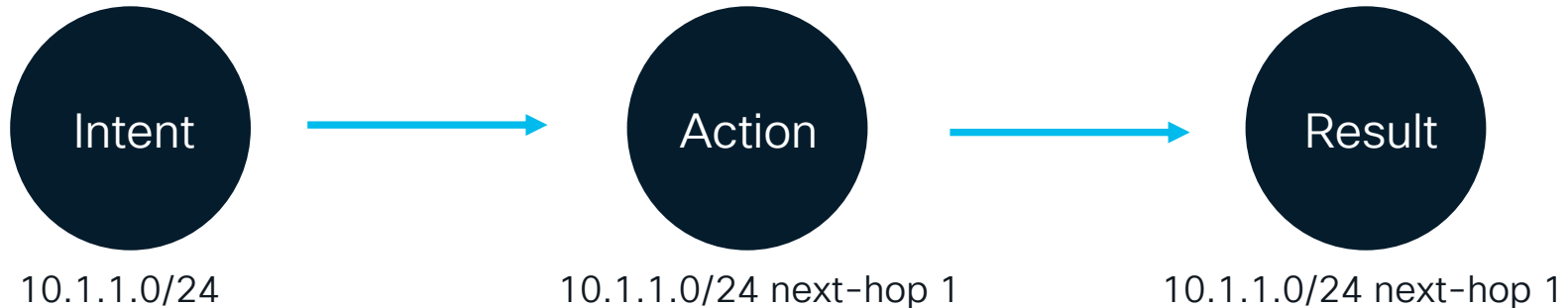


Segmentation
and security

Need For Homogenous Experience Across Heterogenous Cloud Environments

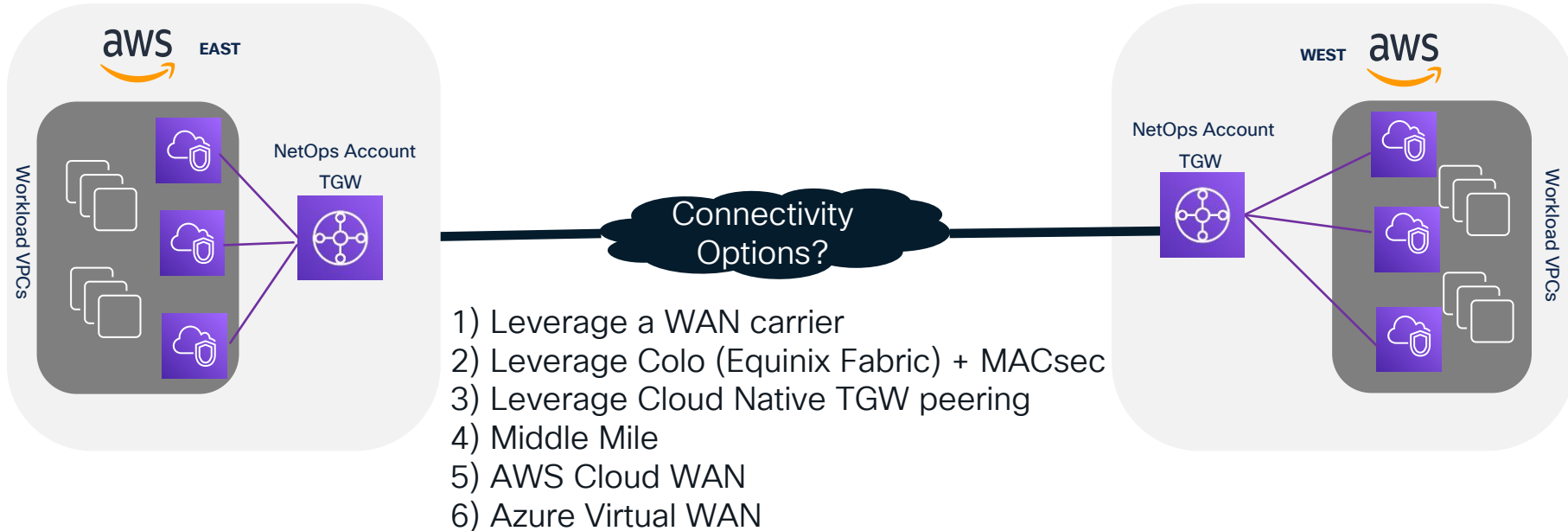
Cloud Native Routing

- **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

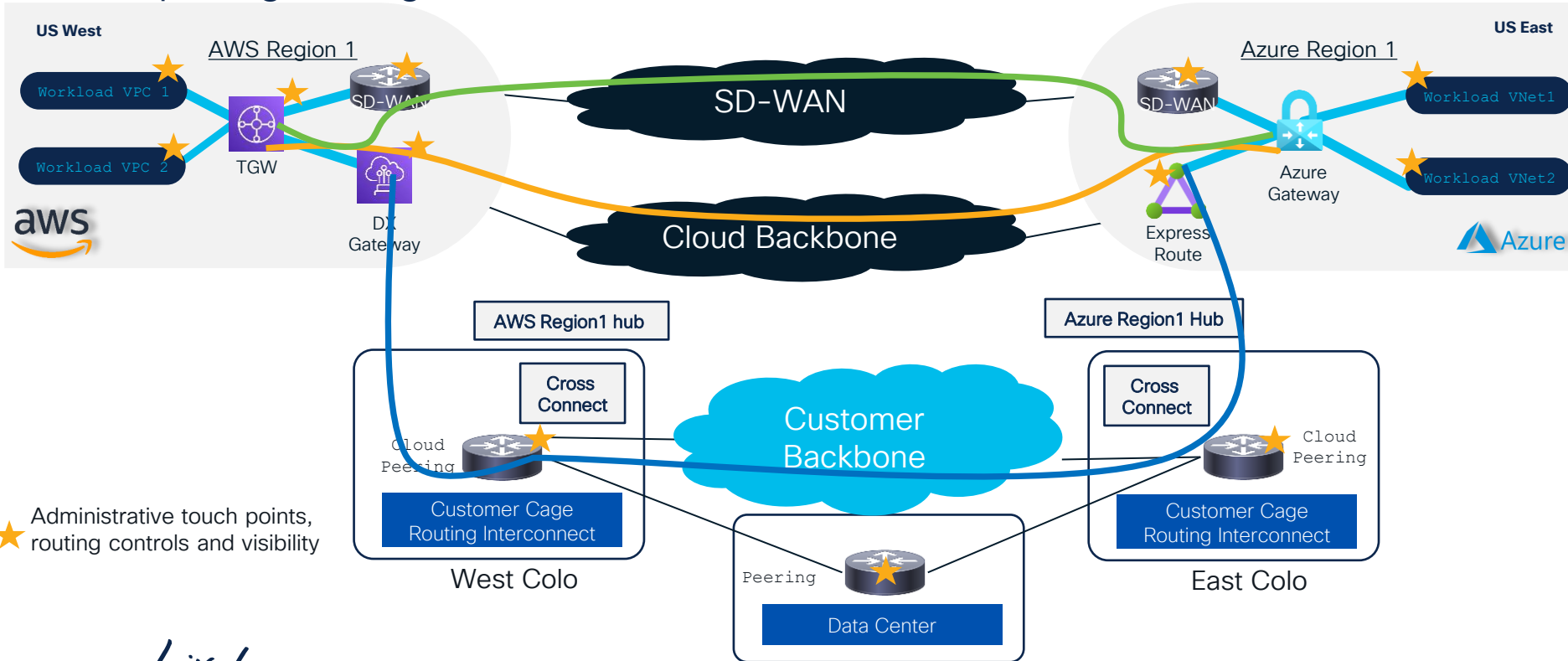
Connectivity Options



Customers are looking to build and create an environment they can switch out of easy (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...

Key Capabilities

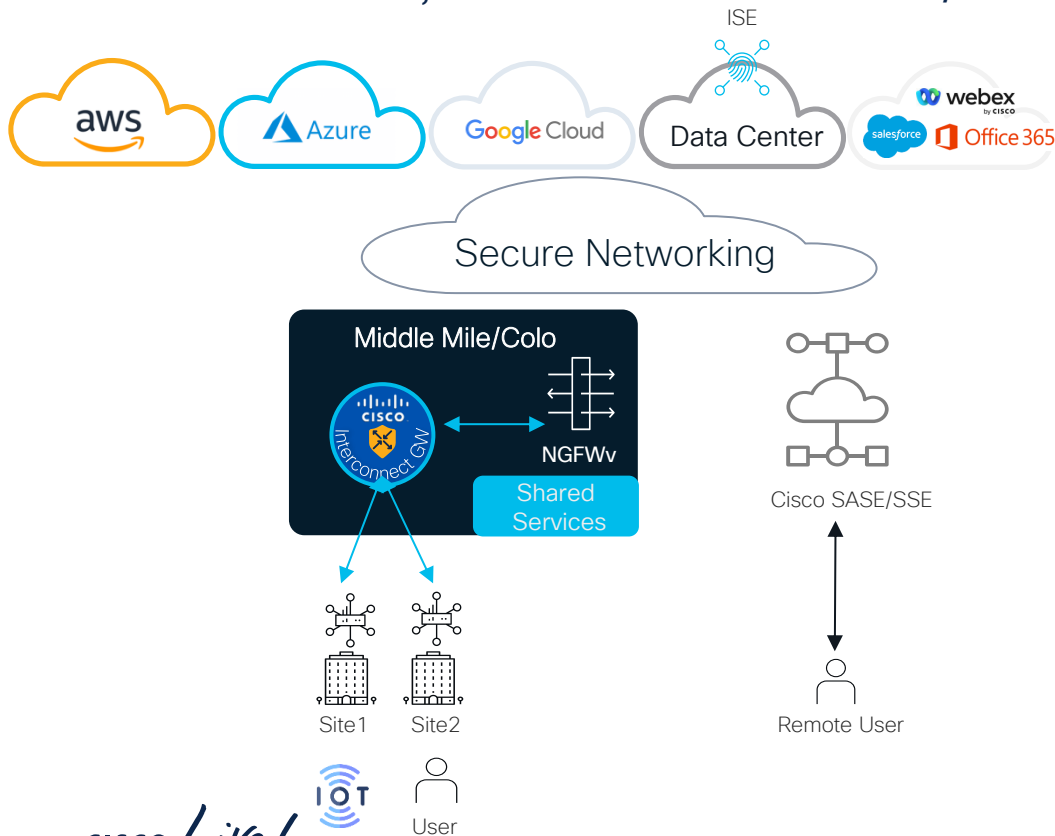


Taxonomy, a few more...

- NGFW: Next Generation Firewall
- ISE: Identify 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
- DLB: Data Loss Prevention
- ZTNA: Zero Trust Network Access

Topology

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

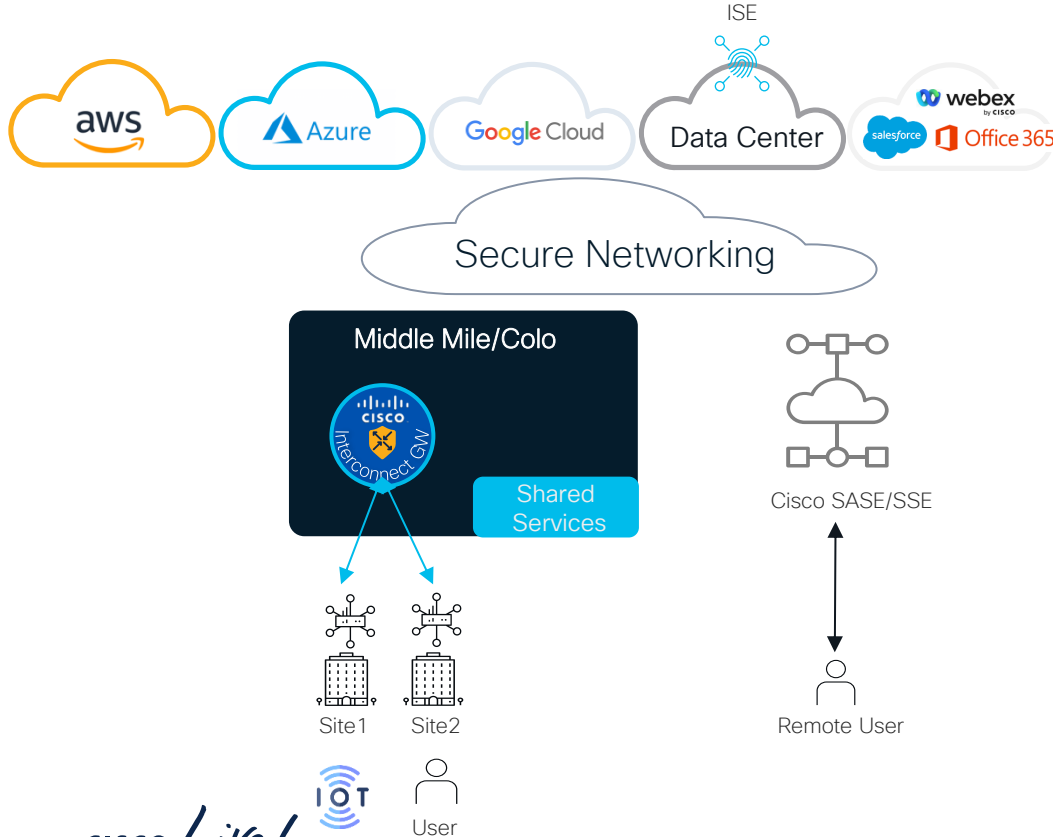


- Secure Networking: End to End Network + Security automation
- End to End Policy, Encryption and Segmentation; ability to carry segmentation
- Policy Enforcement Points
- Ability to do egress enforcement with Catalyst/Meraki SD-WAN
- Ability to provide Remote Users/Site connectivity and security to different destinations. SaaS, Private, and Public applications

Middle Mile:

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

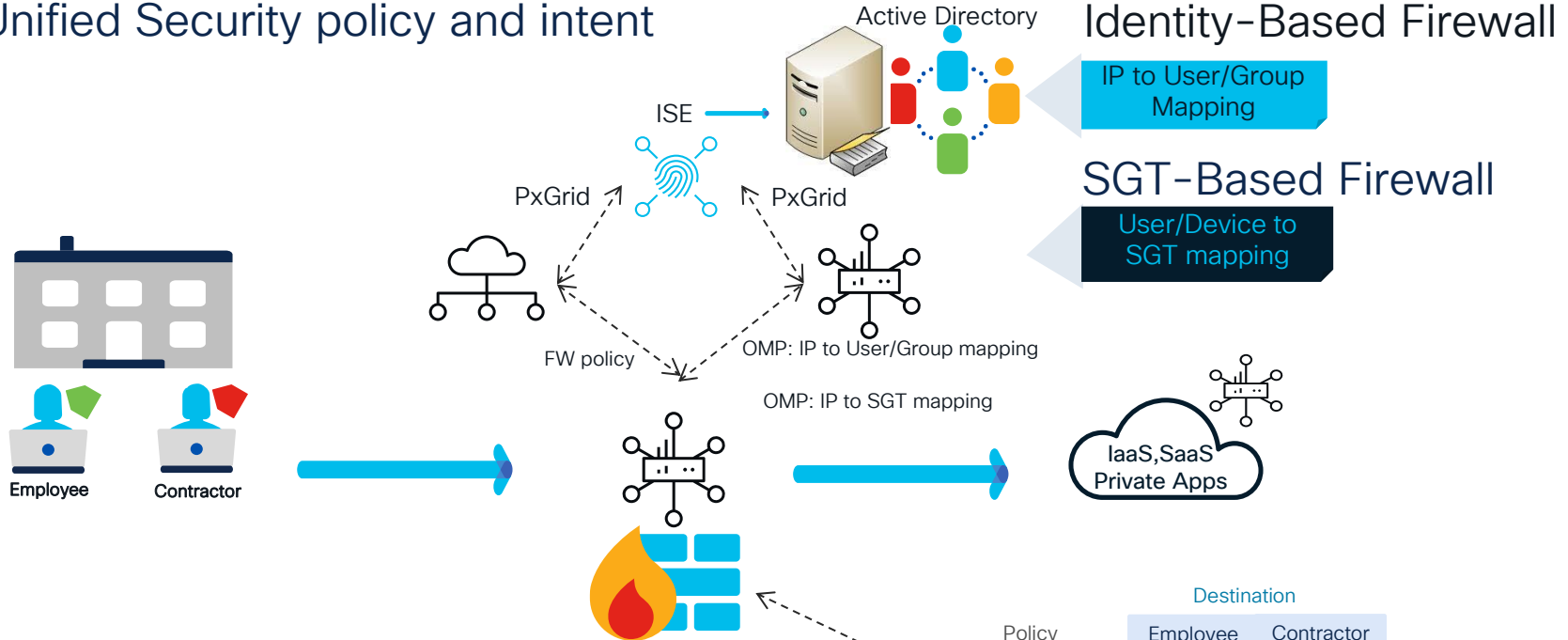
Capabilities: Site/User-to-Cloud



- SD-WAN + Firewall
 - Identity-Based Firewall
 - SGT-Based Firewall
- Ability to carry + Enforce VN/VRF and SGT end to end
- Ability to choose enforcement options
- 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

Capabilities: cEdge Firewall

Unified Security policy and intent



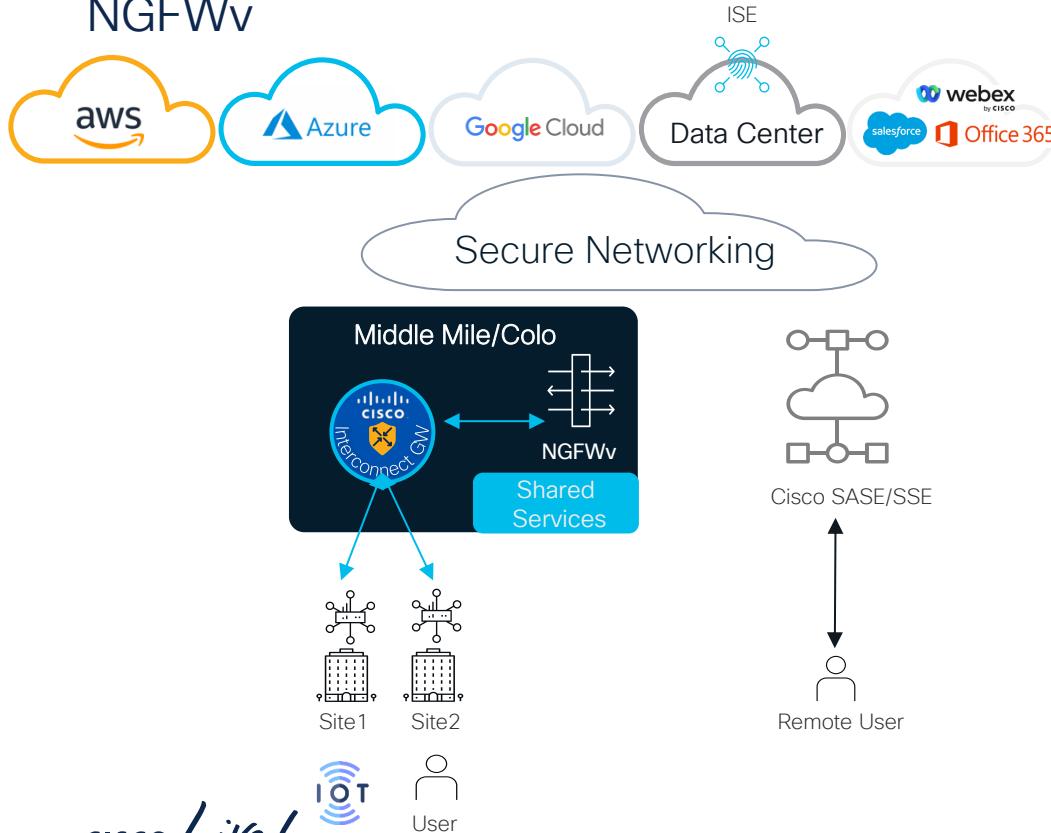
Granular Security Control at User/Group Level

CISCO Live!

Source	Destination	
	Employee	Contractor
Employee	Permit All	Deny All
PLC	Permit All	Deny All
Contractor	Deny All	Permit All

Capabilities: Site/User-to-Cloud

NGFWv



- Require Advanced NGFW
- SD-WAN + FW – NGFWv automated to offer secure policy enforcement point (PEP).
- Catalyst SD-WAN Manager Day0/1, and FW manager (SecOps) Day 2+
- Identity + ISE
- Ability to carry VN/VRF and SGT end to end
- Ability to choose enforcement options
- Identity integration with on-prem ISE
- Leverage on-prem ISE Investment

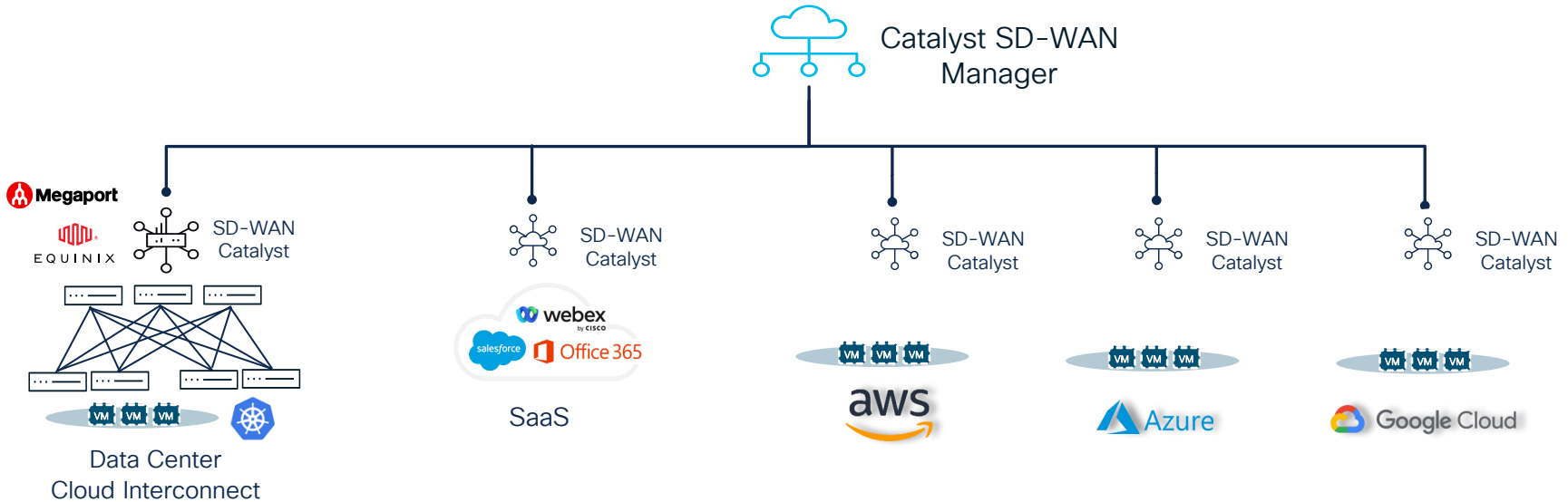
Connecting Users / Devices / Things to the Cloud

Multi-Cloud Networking: Catalyst SD-WAN Manager



Multi-Cloud Networking

Automate connectivity & segmentation with full visibility across hybrid cloud



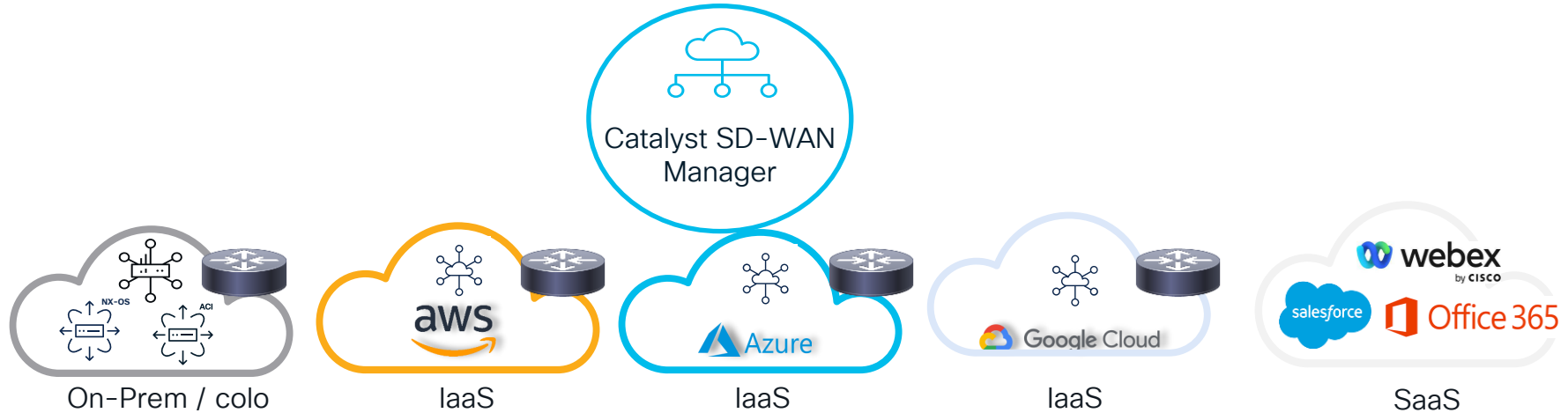
Automated connectivity
and routing

Consistent security and
segmentation

Single Point of Orchestration
Visibility & Troubleshooting

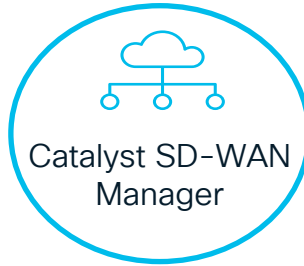
Automated insertion of L4-7
services

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



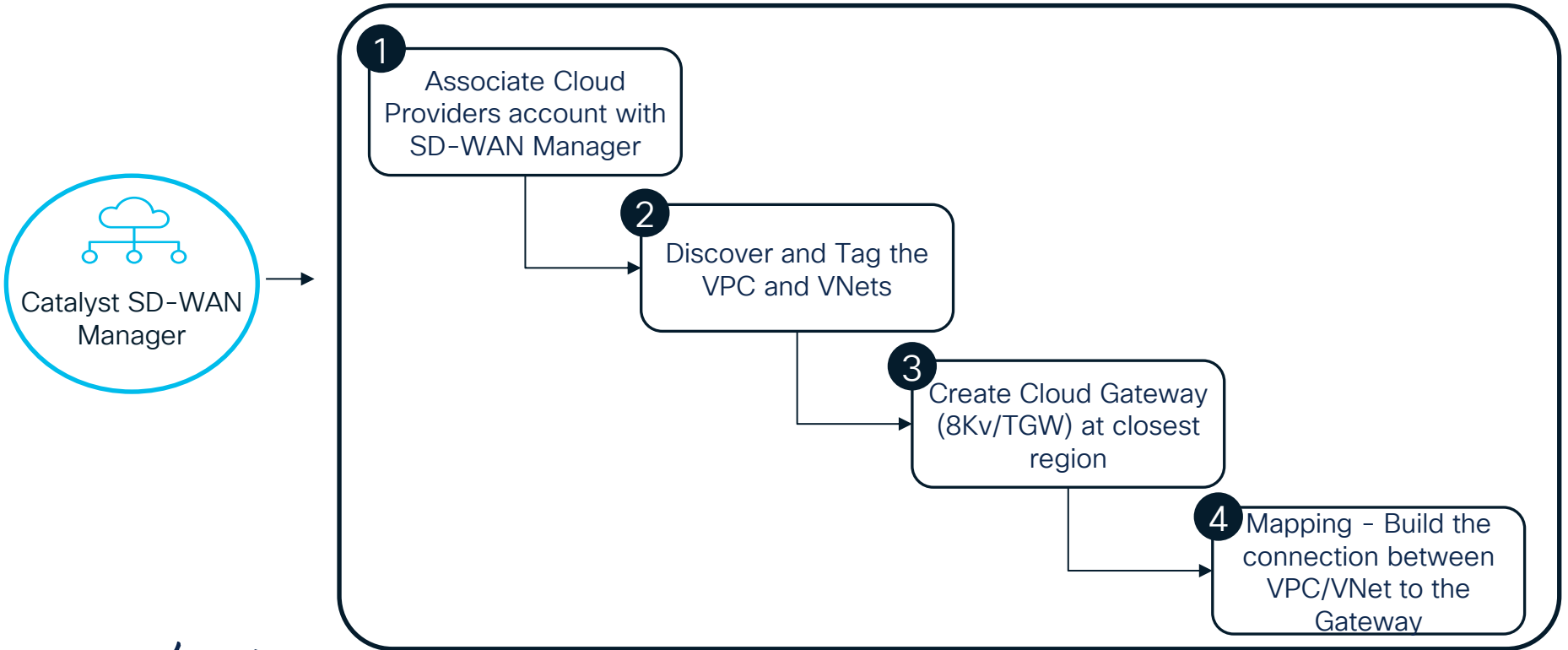
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
le. Firewall

Multi-Cloud Workflow

Secure Connectivity achieved in minutes

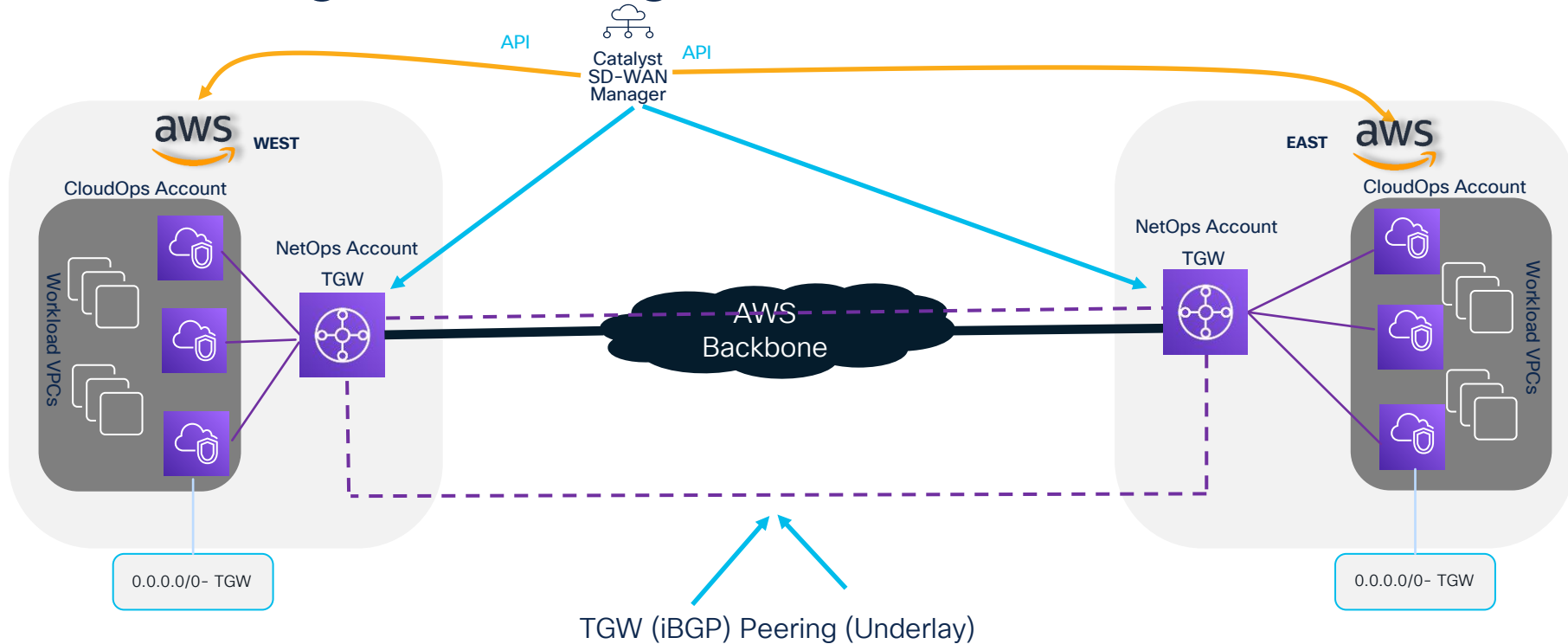


Integration and connectivity to AWS

With TGW



AWS: Region-to-Region

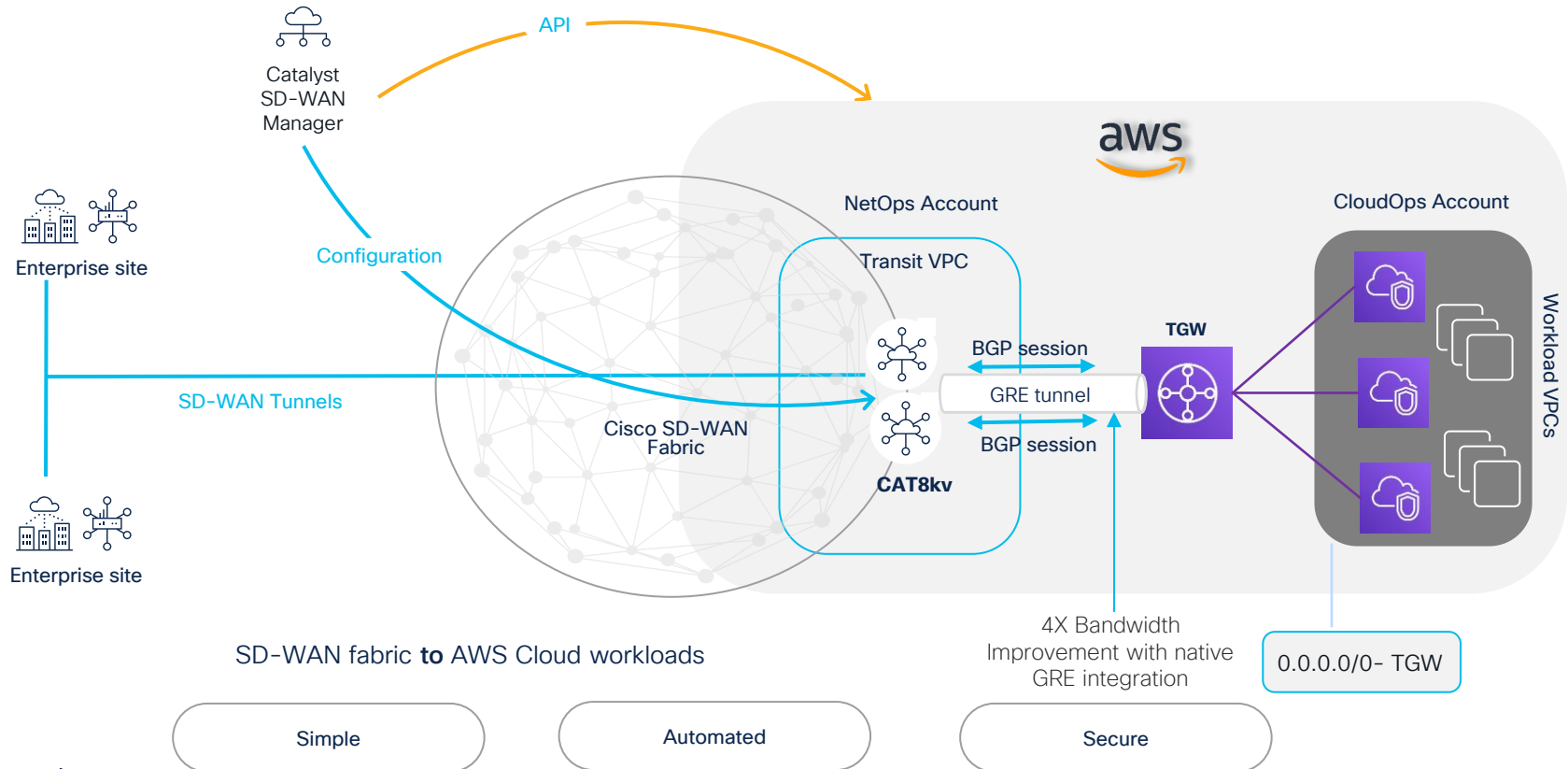


SD-WAN fabric across AWS Cloud global network



AWS: Site-to-Cloud

SD-WAN Native Integration using **GRE** (TGW Connect) between c8kvs within Transit VPC and Transit Gateway

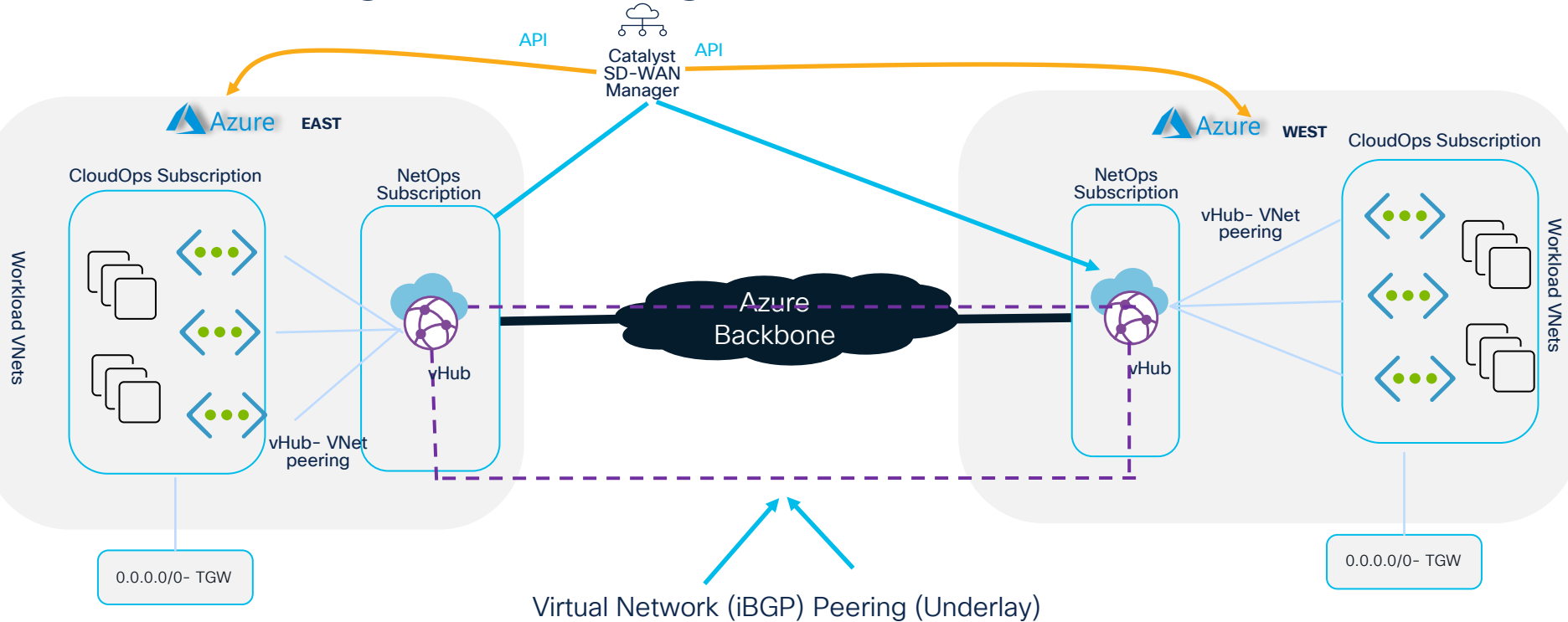


Integration and connectivity to Azure

With vWAN/vHub

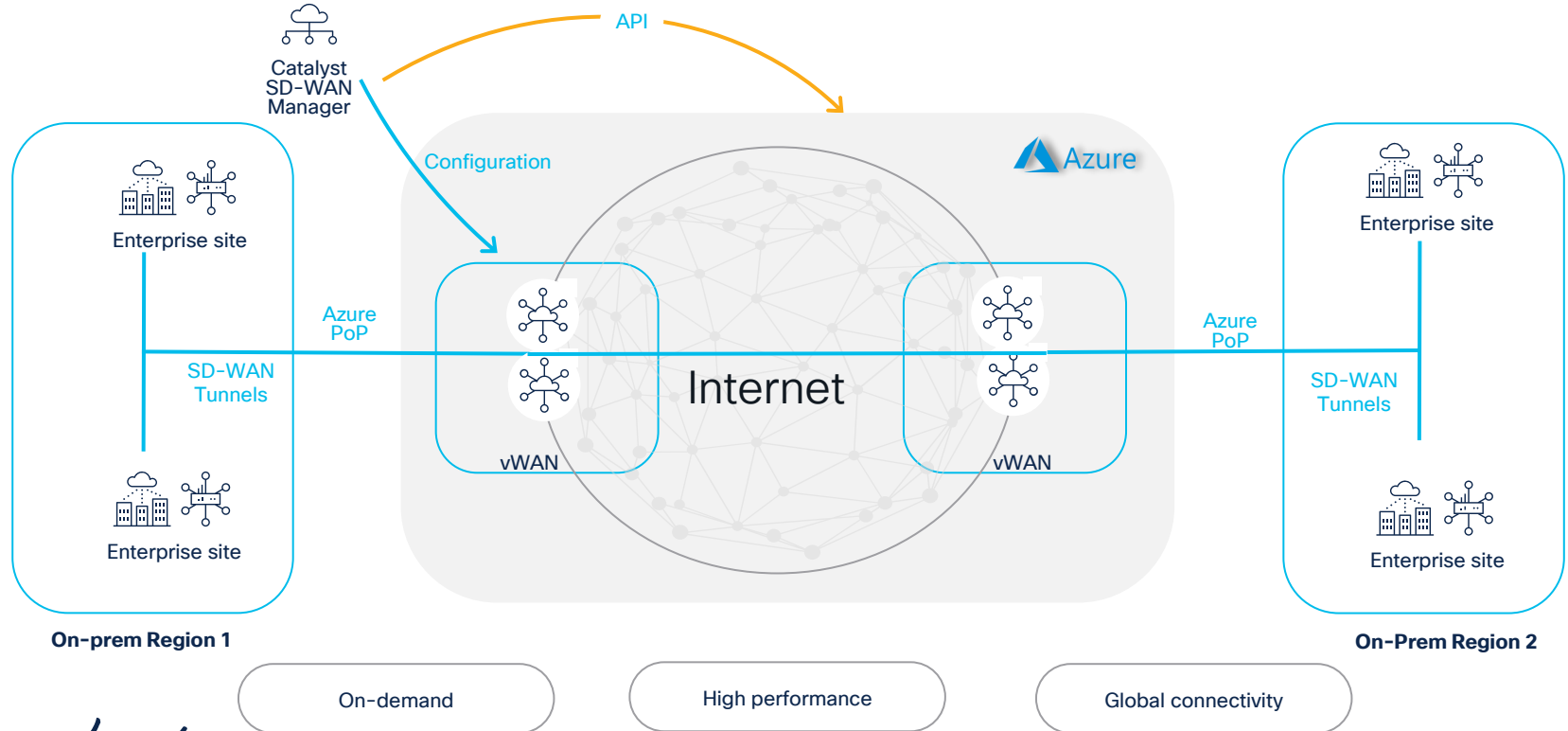


Azure: Region-to-Region

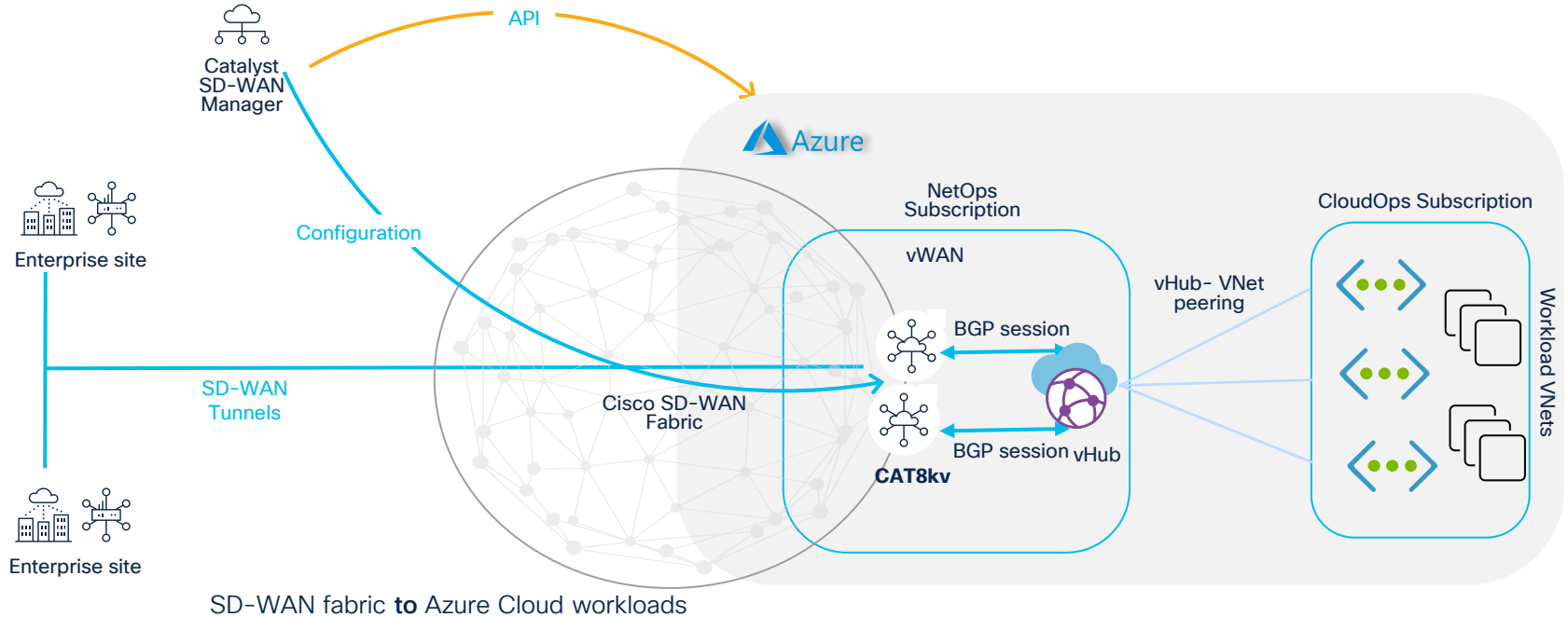


Azure: Site-to-Site

SD-WAN fabric across Azure global network



Azure: Site-to-Cloud

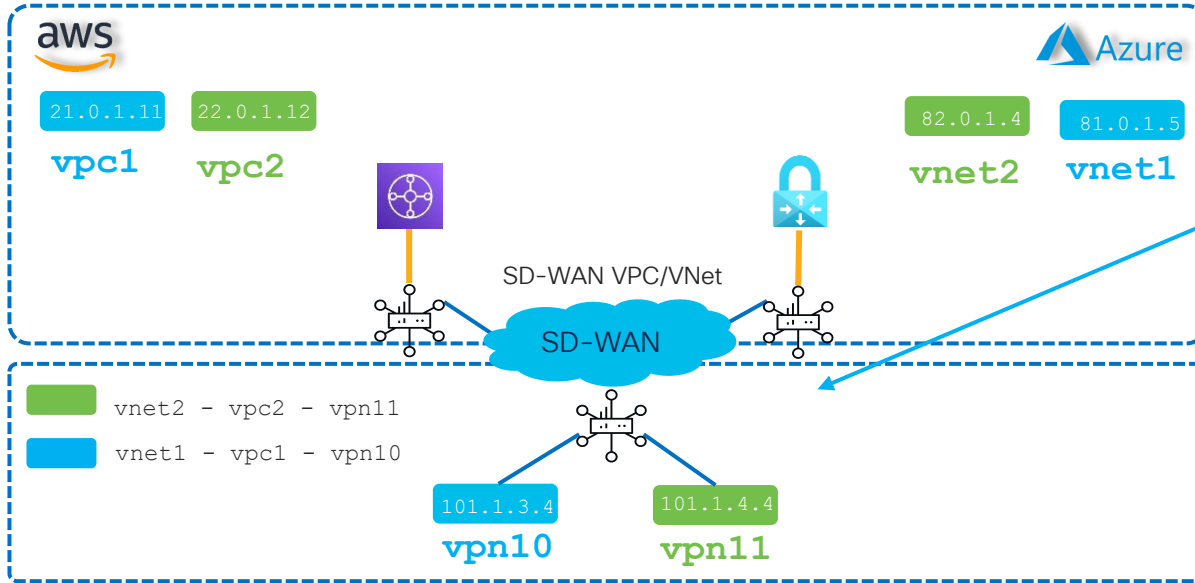
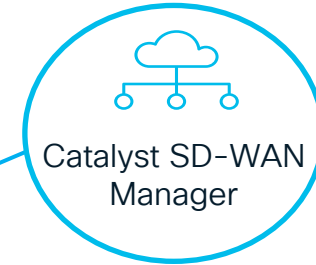


Simple

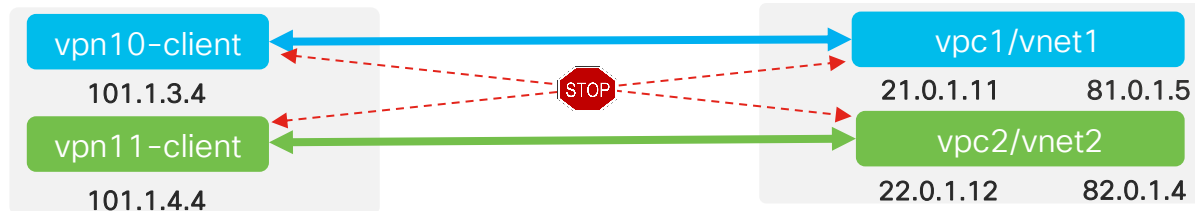
Automated

Secure

Segmentation with SD-WAN

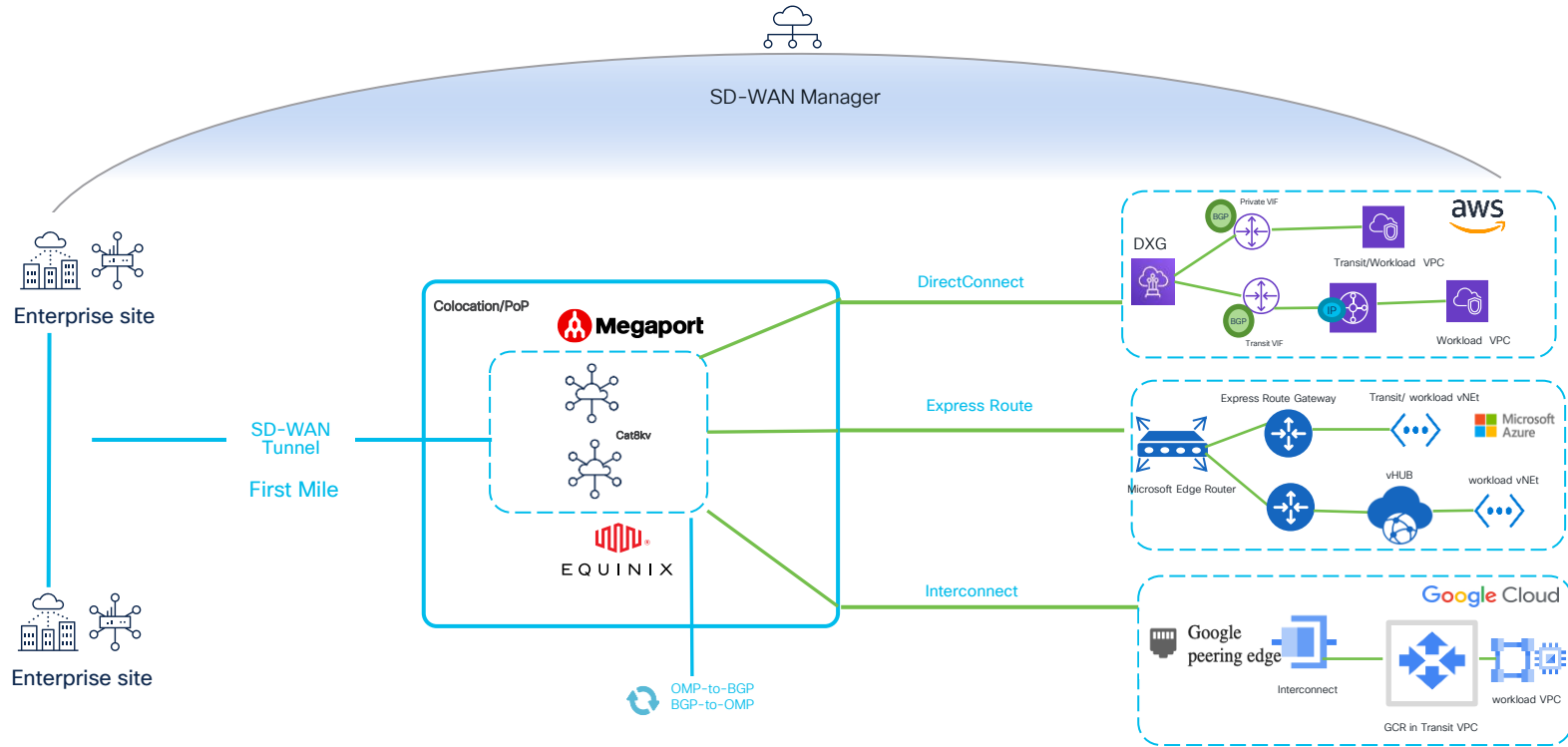


- 1) SDWAN connectivity terminates at the Cat8ks for the different VRFs
- 2) VRF(s) are extended to the TGW/ Cloud WAN extended to the native VPCs



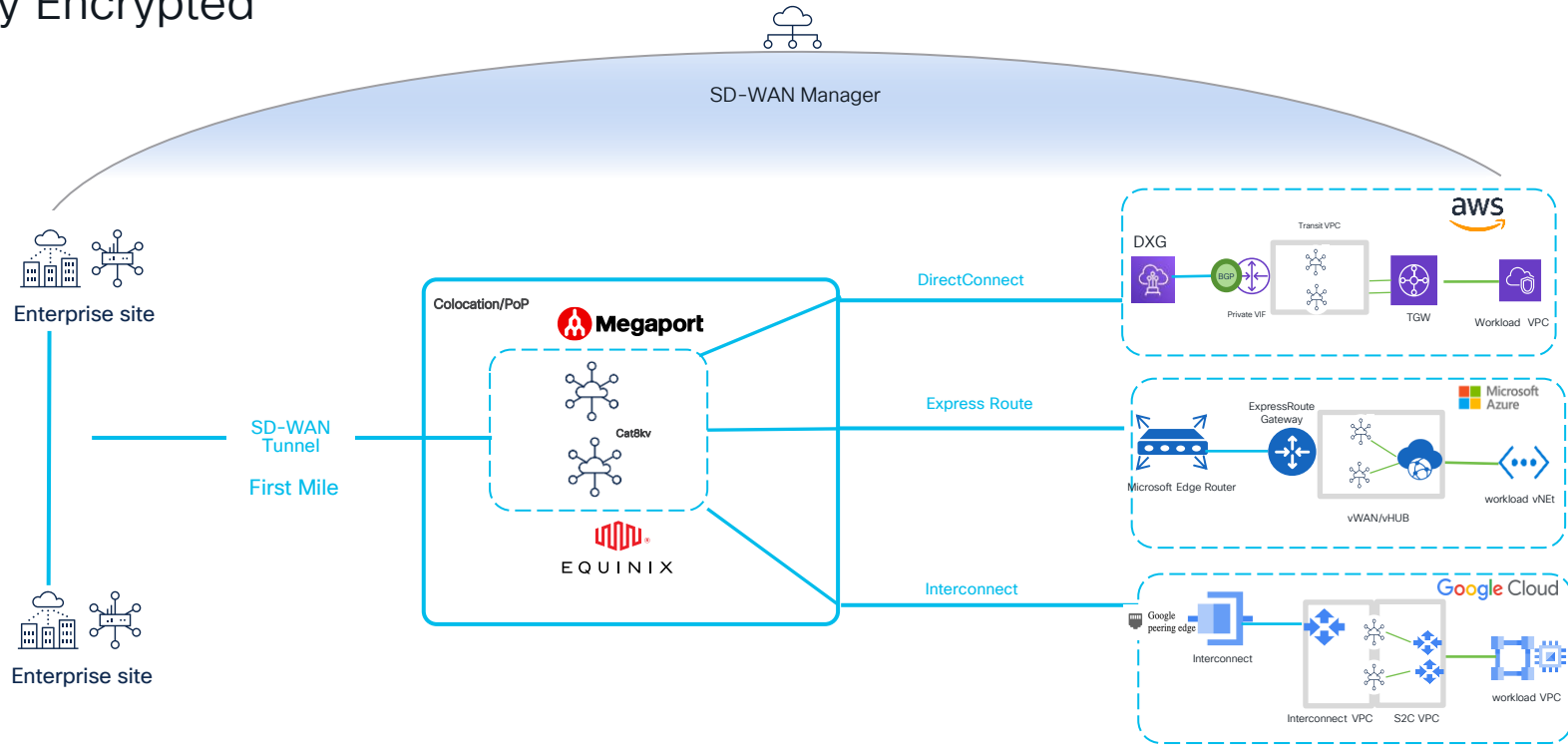
Middle Mile w/ Megaport & Equinix

Site-to-Multicloud- Megaport or Equinix

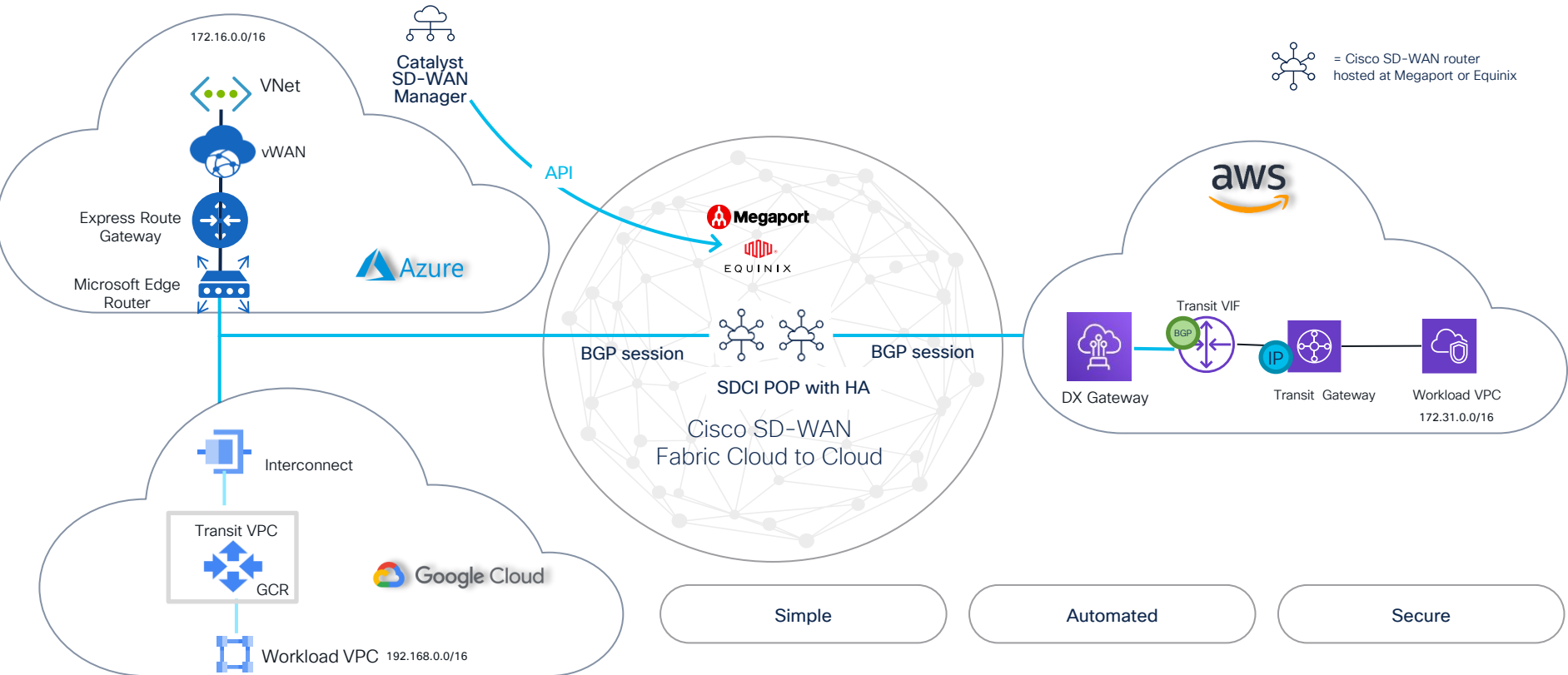


Site-to-Multicloud- Megaport or Equinix

Fully Encrypted



Cloud to Cloud: Private Connect Megaport/Equinix

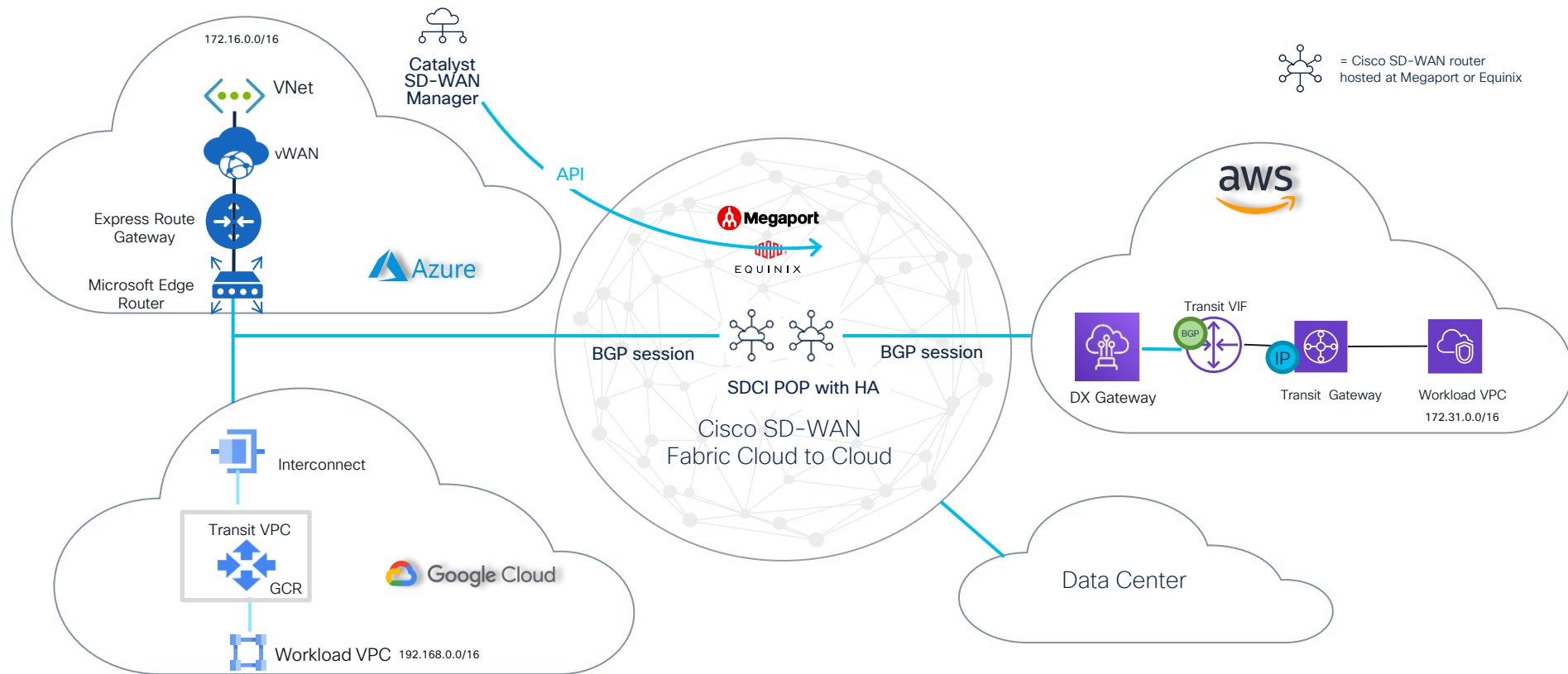


- Simple
- Automated
- Secure

Automated with Cisco Catalyst SD-WAN Manager



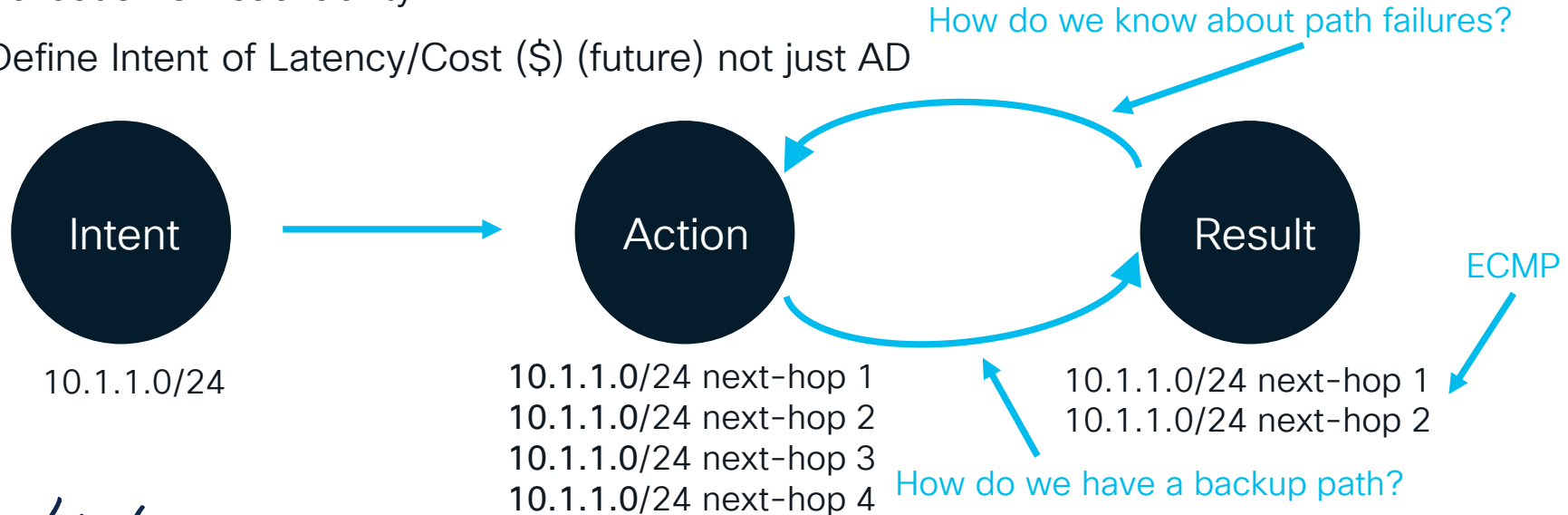
Cloud to Cloud: Private Connect Megaport/Equinix



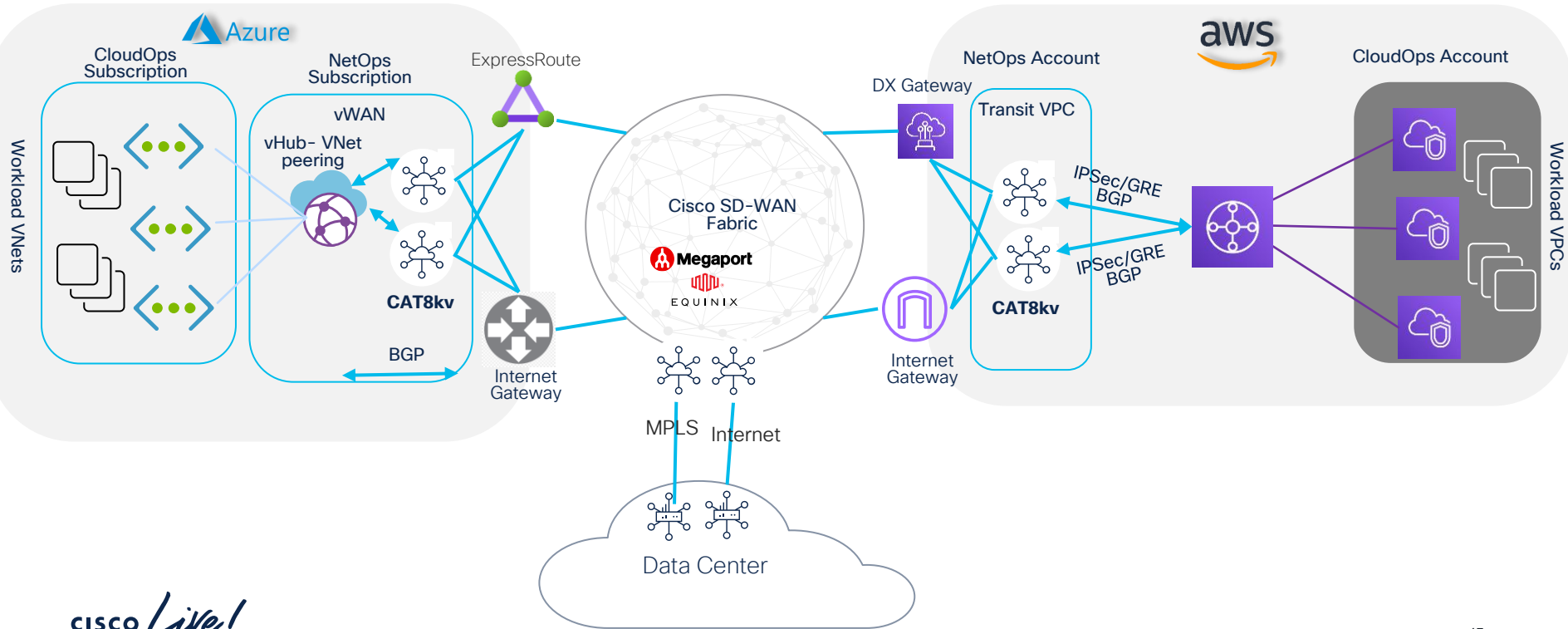
Automated with Cisco Catalyst SD-WAN Manager

Cloud Networking with SD-WAN Manager

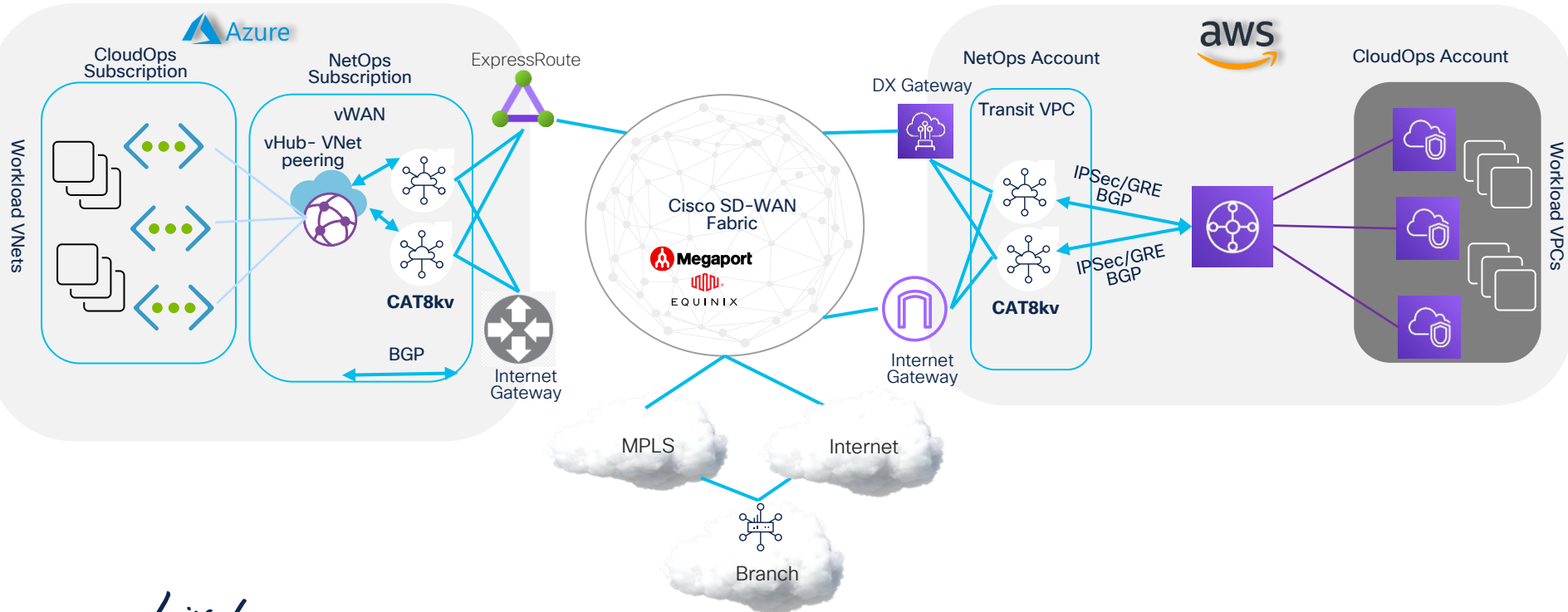
- **Intent:** Reach 10.1.1.0/24 over all possible paths (ECMP) and Path Failure(s)
- Administrator expresses the Routing Intent (NetOps / Cloud NetOps)
- Validation of reachability
- Define Intent of Latency/Cost (\$) (future) not just AD



Cloud-to-Cloud ECMP



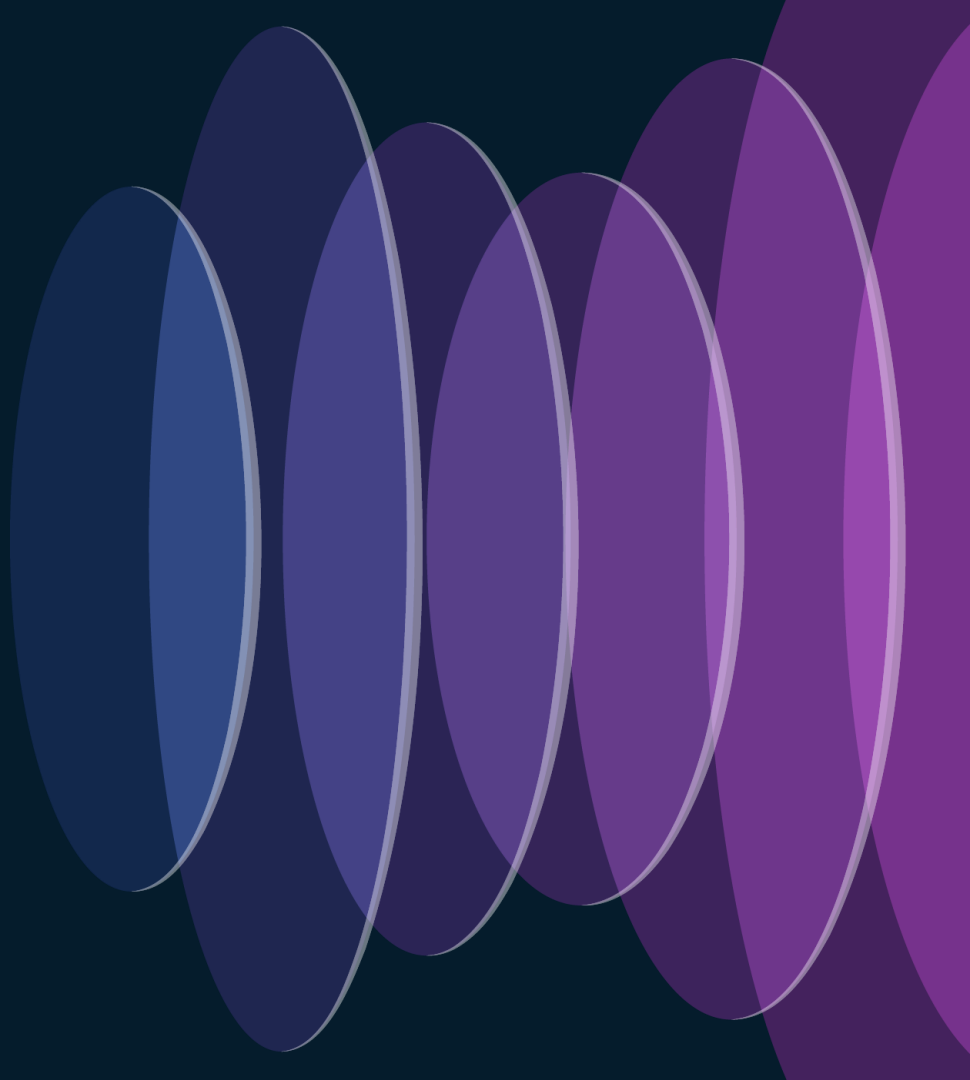
Cloud-to-Cloud ECMP



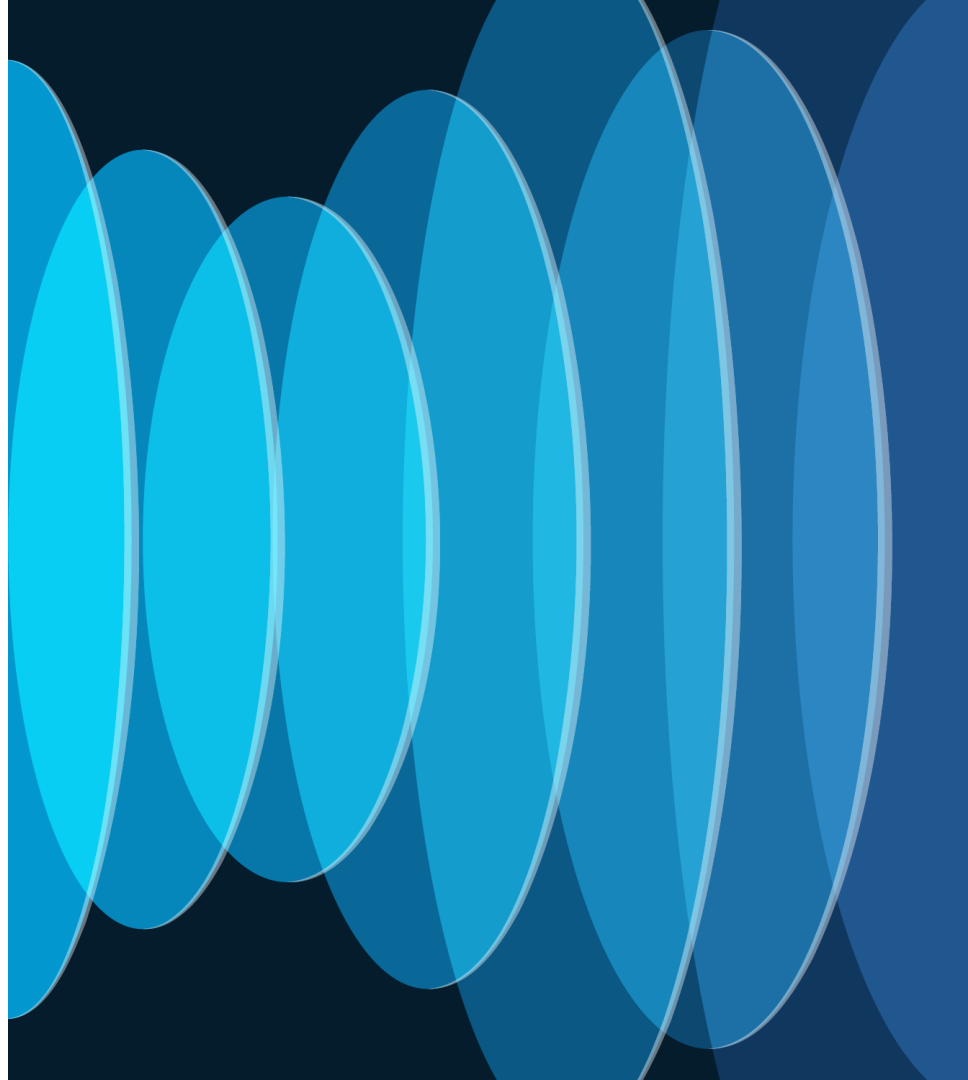
So where is the new perimeter?

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 SDWAN and Cloud Security Stack

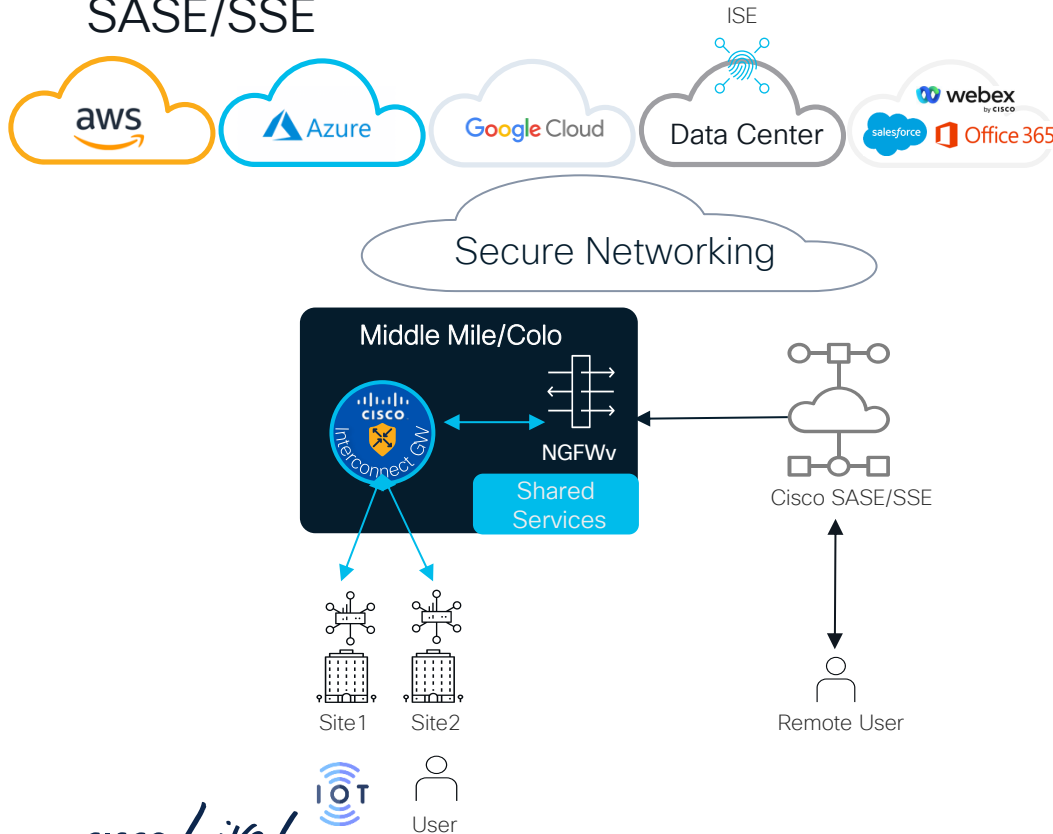


Use-Cases



Use Case: Site/User-to-Cloud

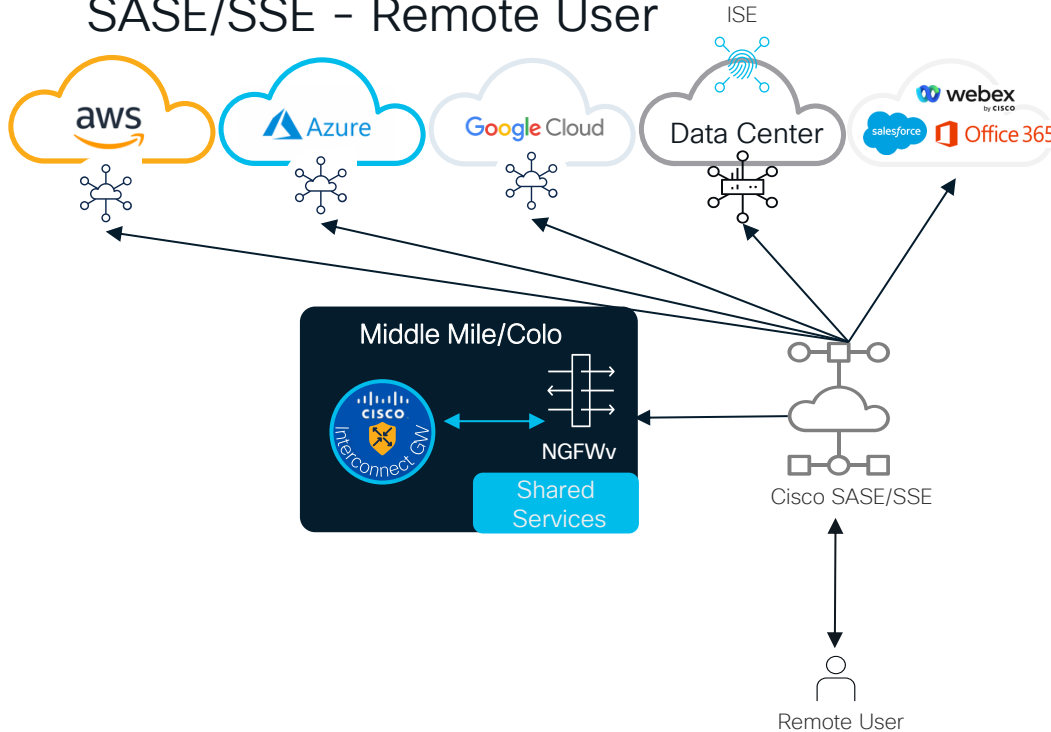
SASE/SSE



- 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 VN/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 the right traffic to the right place- not every application can go through SASE. For example, Office365 no proxy/SWG.
- Least privilege access

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 (ie Webex or O365)
- User Experience (ie API hook into WebEx Tenant and bypass)
- DLP and CASB Controls (ie. upload only)

• Remote User to Private

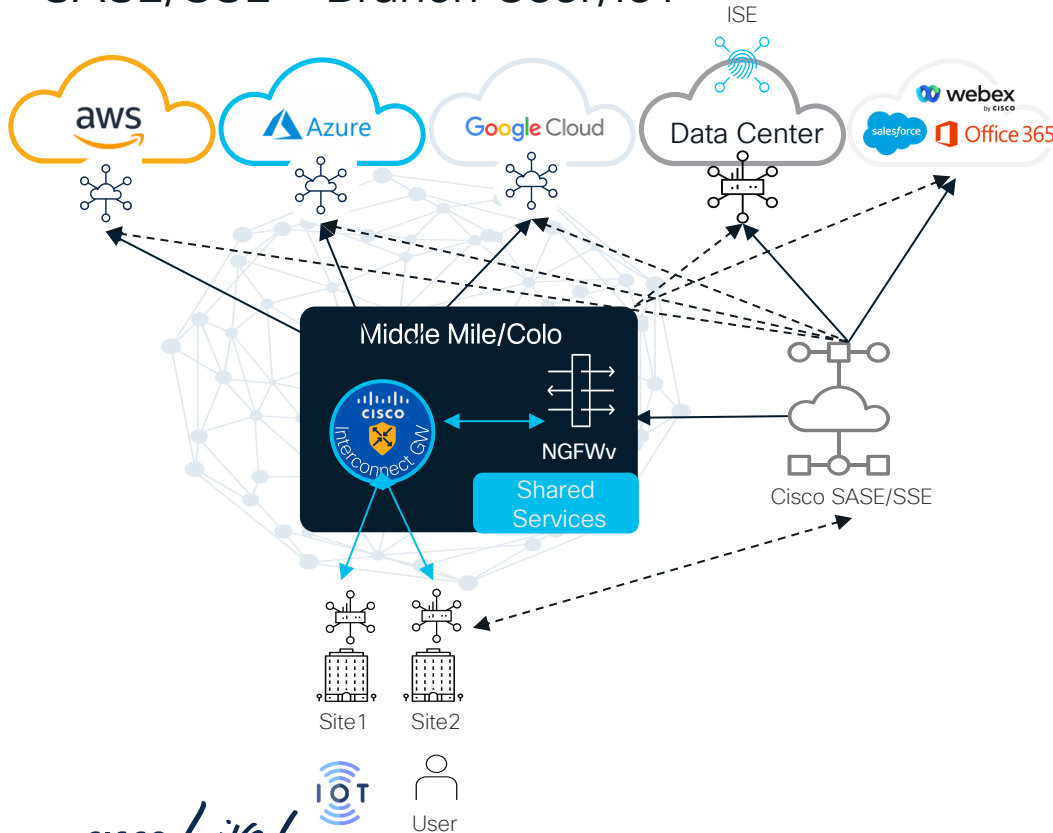
- Application in CSP
- Application in Private DC
- Application Middle Mile Shared- Services. Traffic goes through Secure Access First (FW/Inspection) PEP/IPS/Decryption/ZTNA FW

• 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

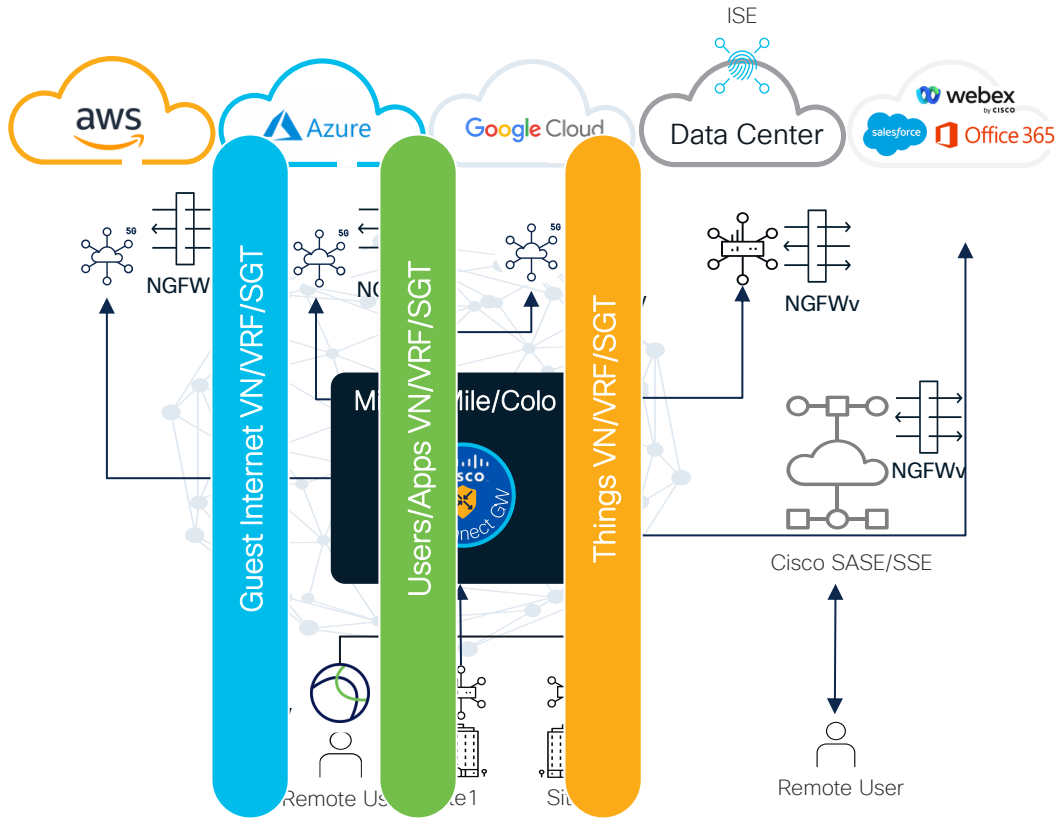
Use Case: Site/User-to-Cloud

SASE/SSE - Branch User/IoT



- **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 (ie. 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”
- VN/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

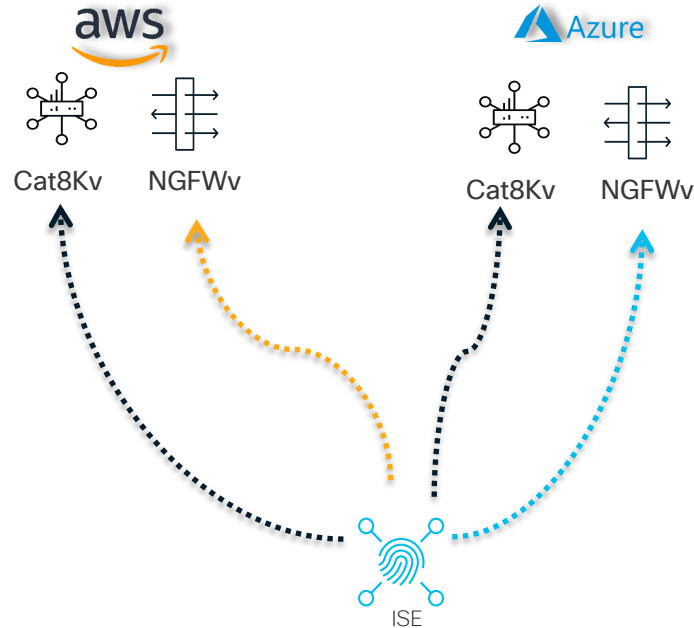
Resulting in:

- 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

Extending Policy to Public IaaS



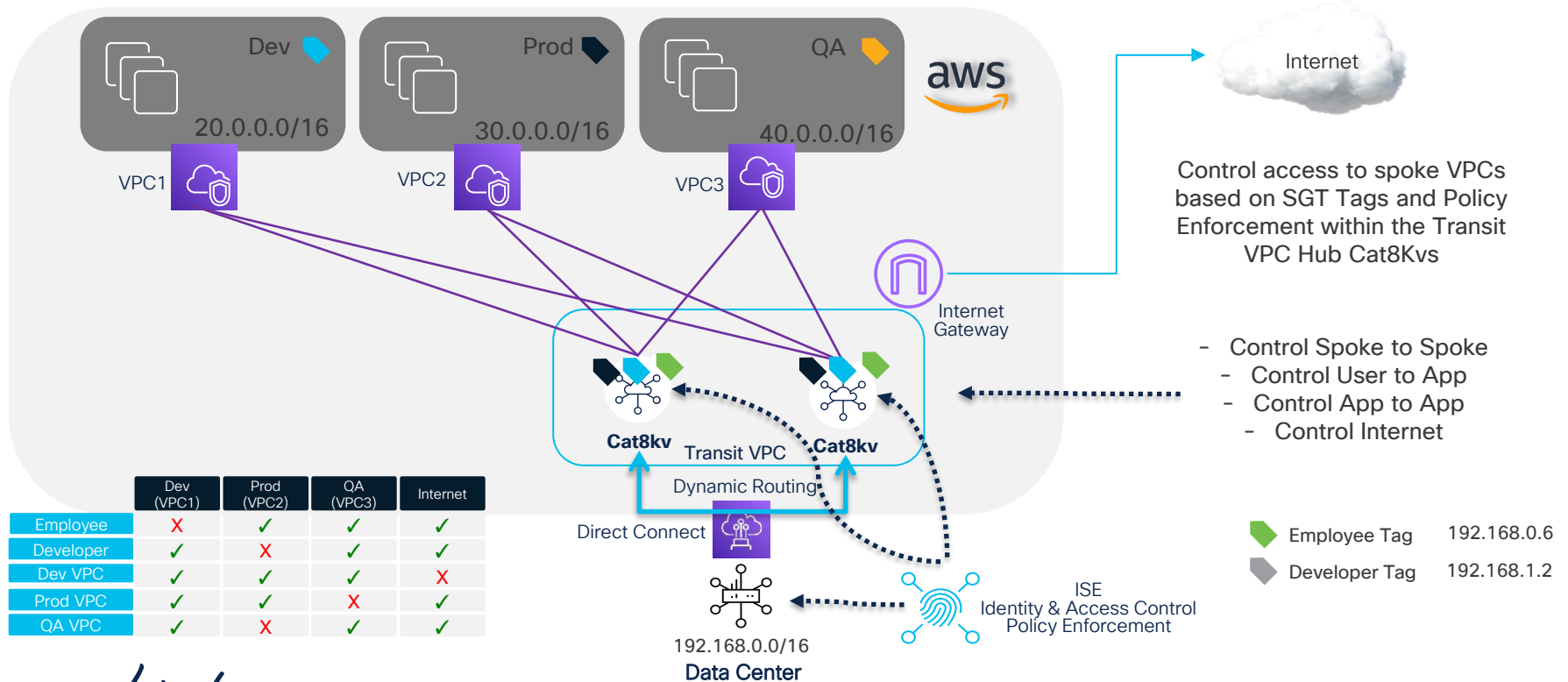
Enabling Group-based Policies



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

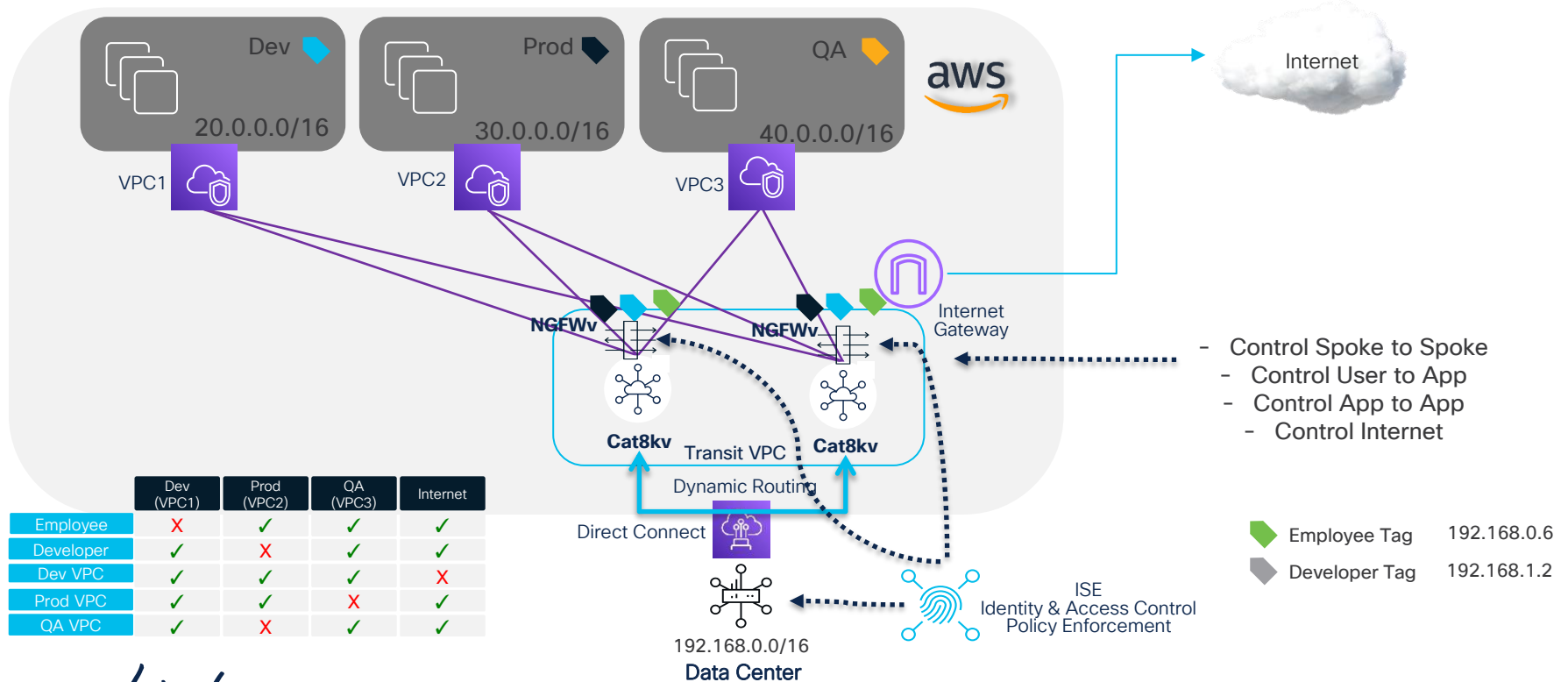
AWS Transit VPC

Simplifying Segmentation and Control



AWS Transit VPC

Simplifying Segmentation and Control



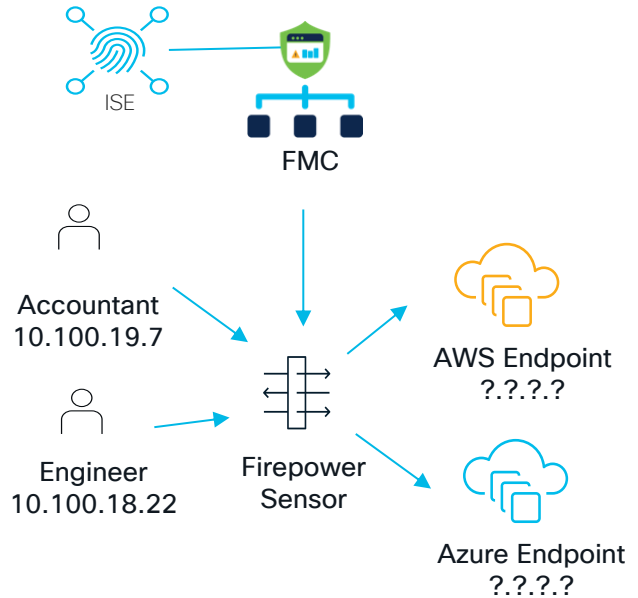
Cisco Secure Dynamic Attributes Connector

- Natively in Firewall Management Center (FMC)
- 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

Cloud Connectors

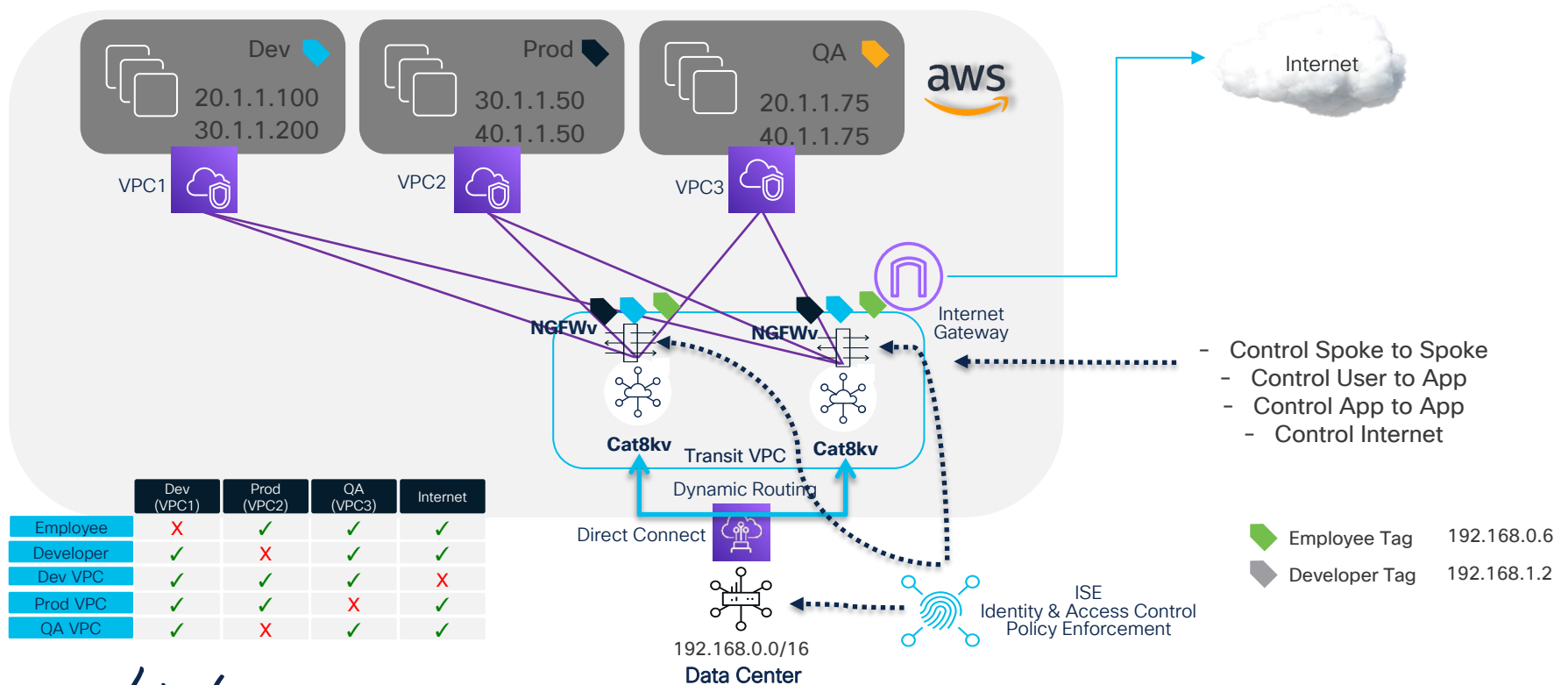


Public Connectors



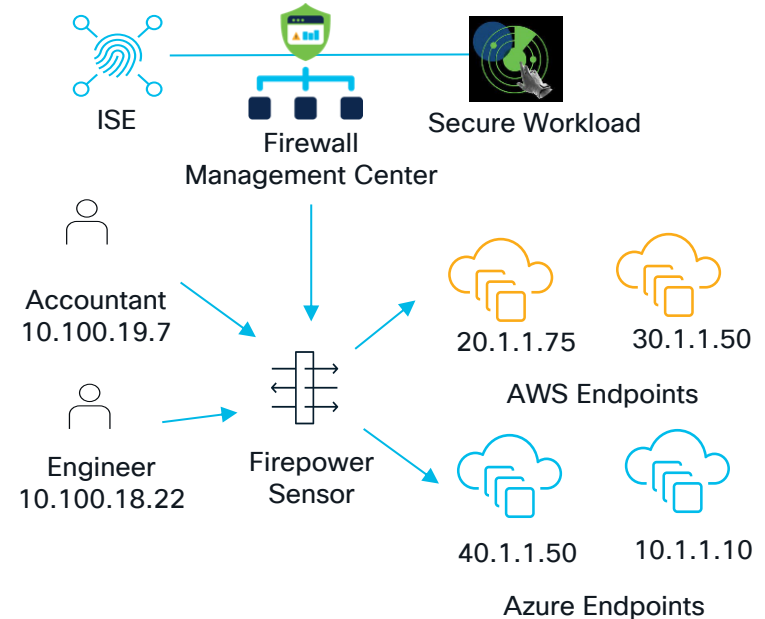
AWS Transit VPC

Simplifying Segmentation and Control



Cisco Secure Workload

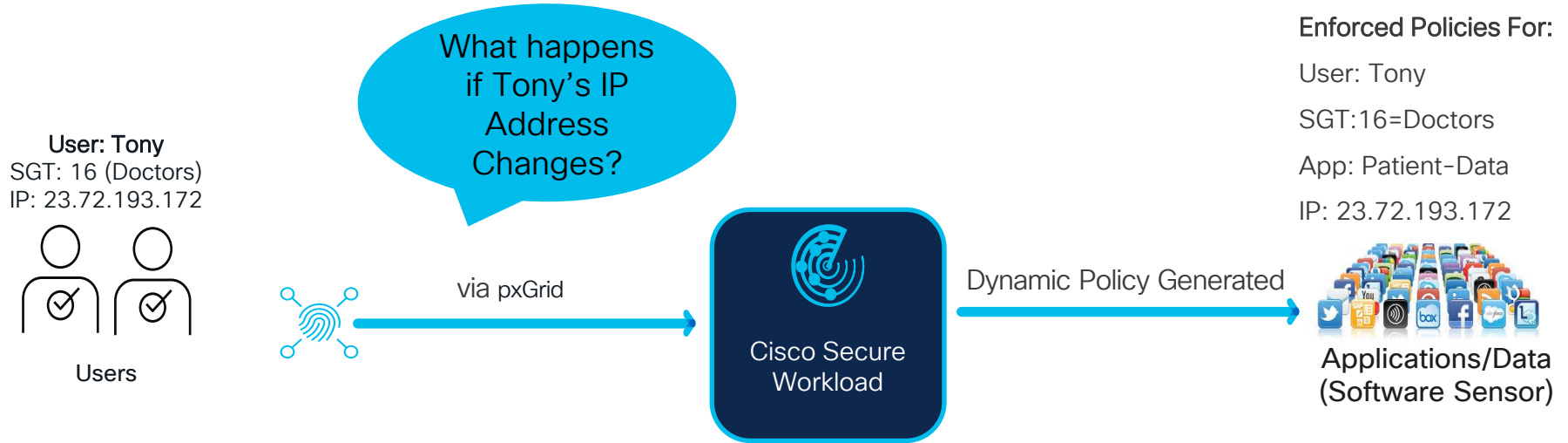
- Segmentation policies enforcement at workloads
- Virtual Machines, Containers and Bare Metal
- Private and Public IaaS
- Prevent East / West lateral Movement
- Dynamic Policy
- Policy Enforcement
- Policy Visibility



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

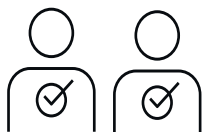


May access patient records

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

Enforced Policies For:

User: Tony

SGT:20=Doctors

App: Patient-Data

IP: 23.72.193.172



Applications/Data
(Software Sensor)

- 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

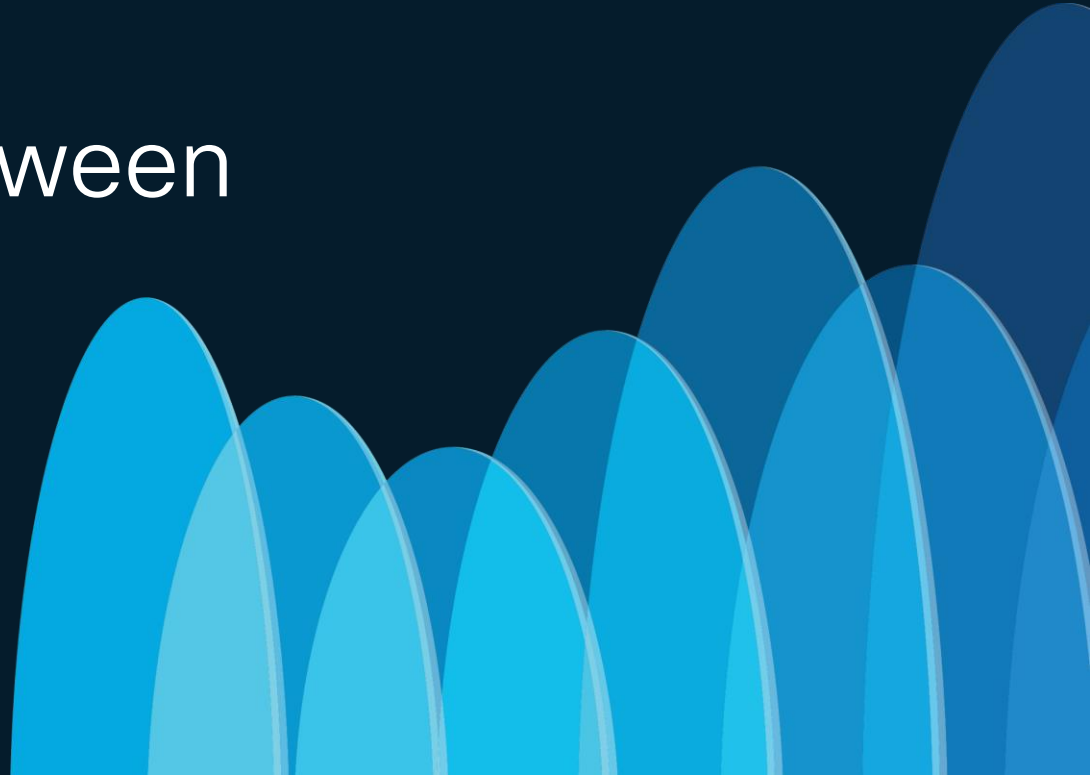


May not access employee data

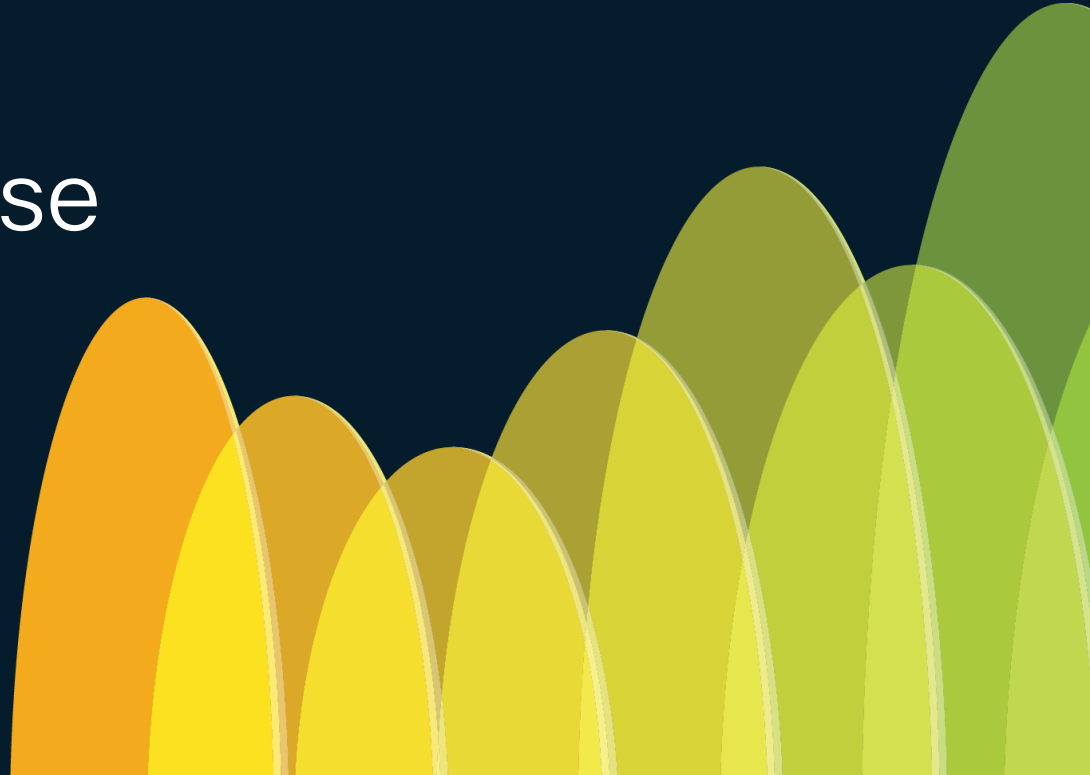


May access patient records

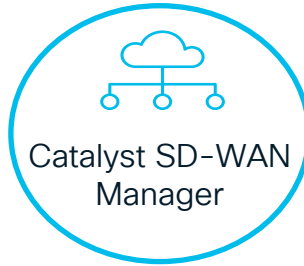
Security: In & Between the Clouds



Multicloud Defense



Personas



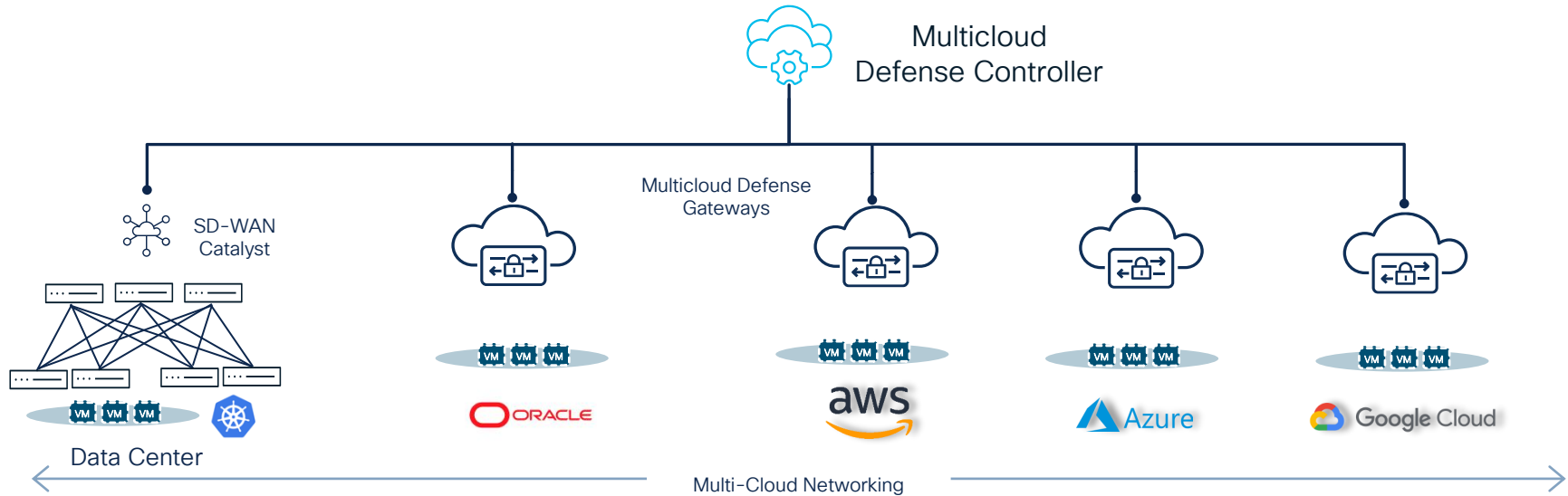
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
le. Firewall

Multicloud Defense

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



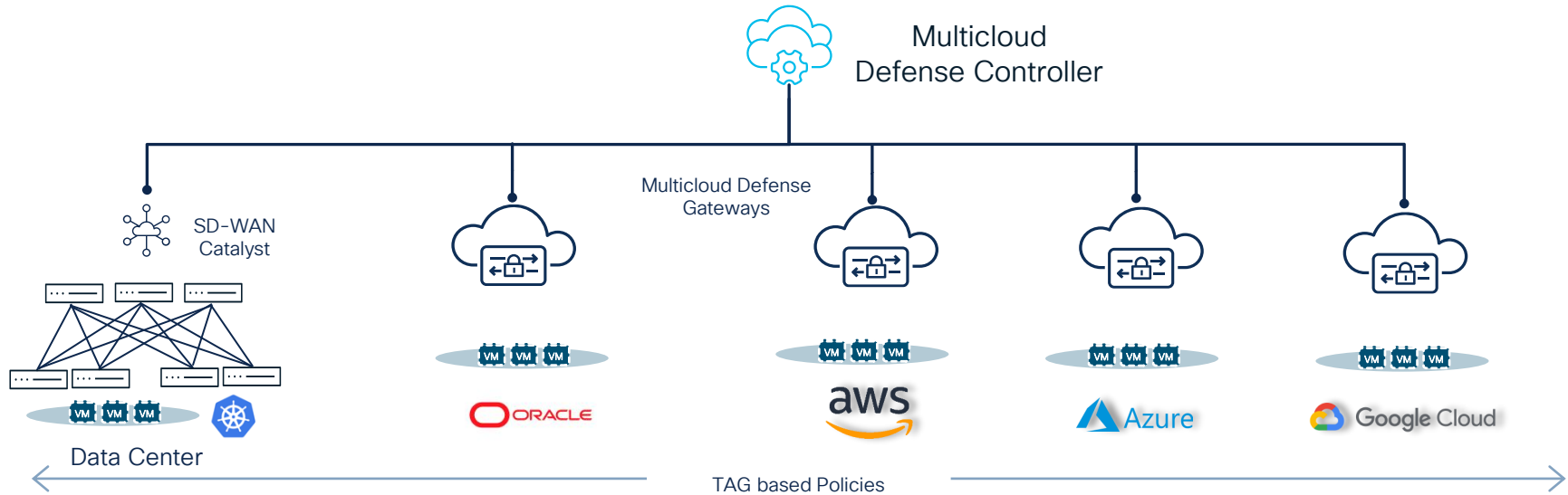
Dynamic Classification &
Security Automation

Unified Security Policy

Segmentation (East/West)
Ingress/Egress Protection

Auto-Scaling

Dynamic Unified Security Policy



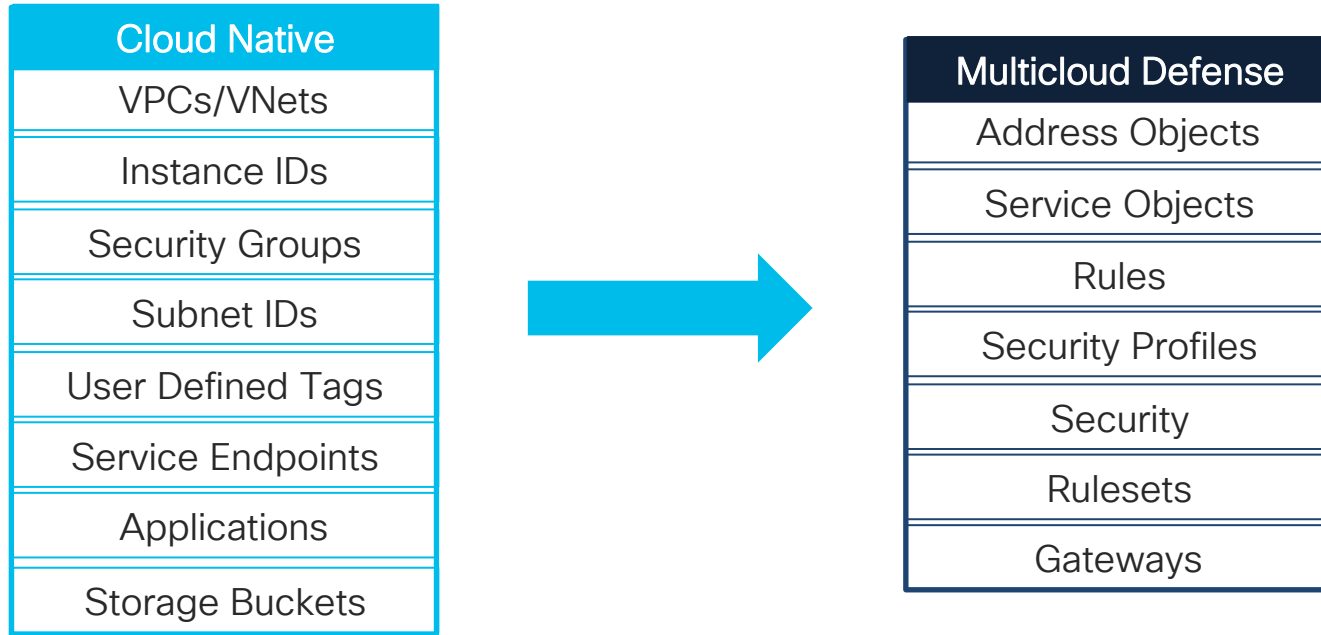
Learn tags in real-time

Unified TAG-based Security Policies

Auto-Scaling

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

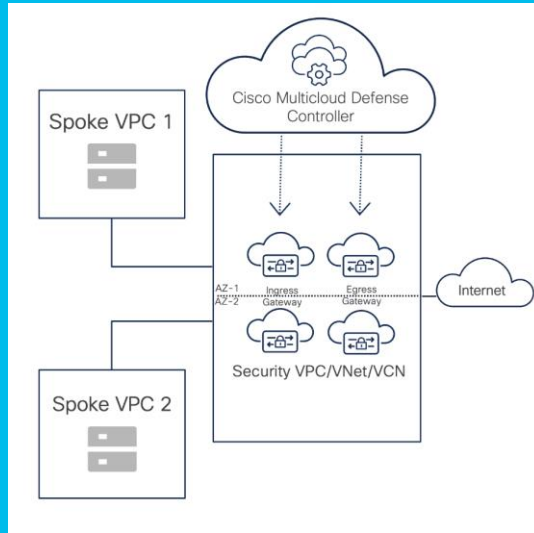
Egress

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

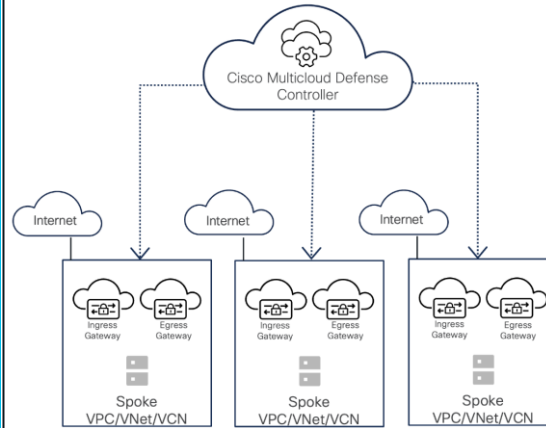
East/West

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

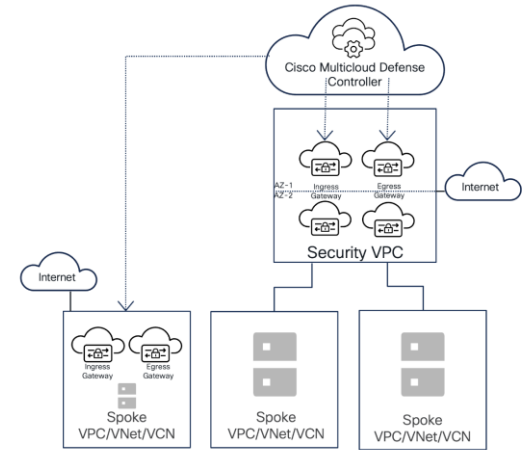
Security Models



Centralized Security Model



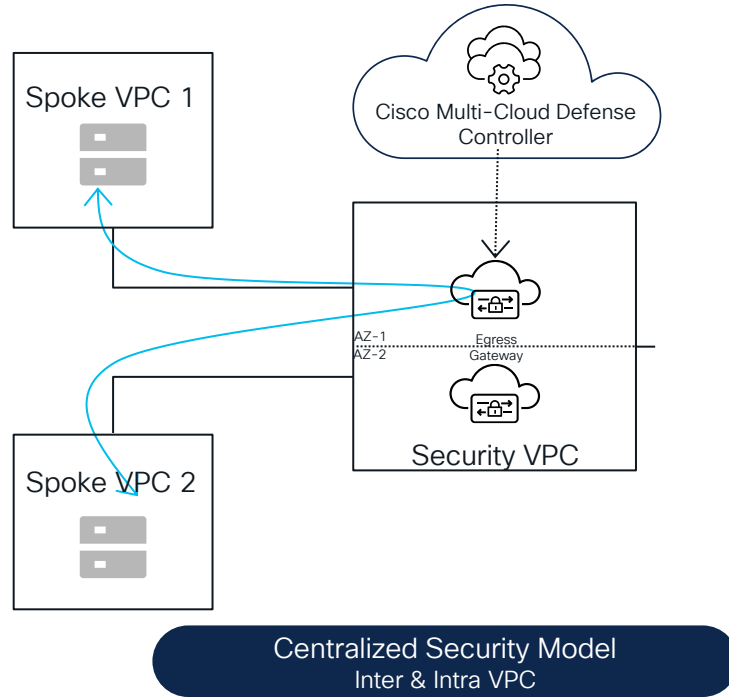
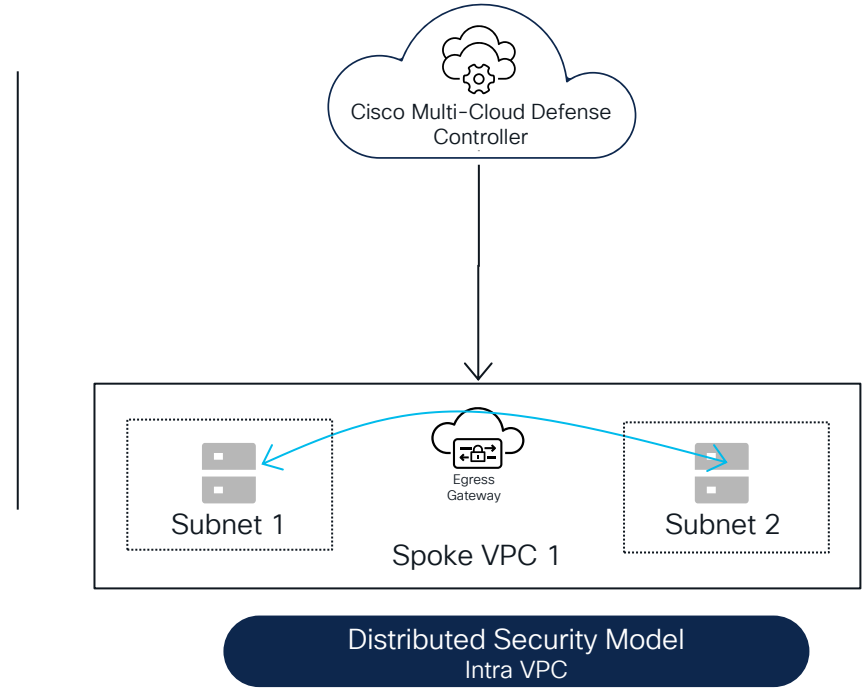
Distributed Security Model



Combined Security Model

Segmentation

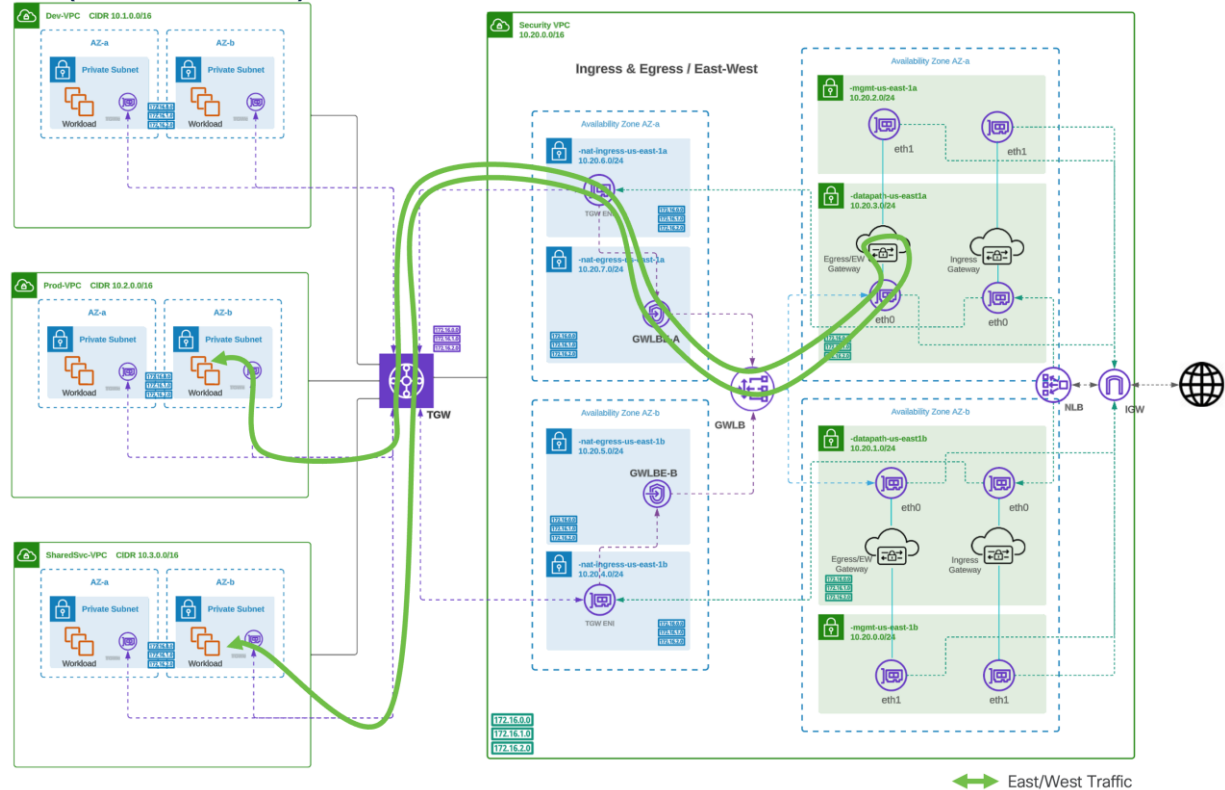
Use-case



AWS Centralized East-West Traffic Inspection (Inter-VPC)

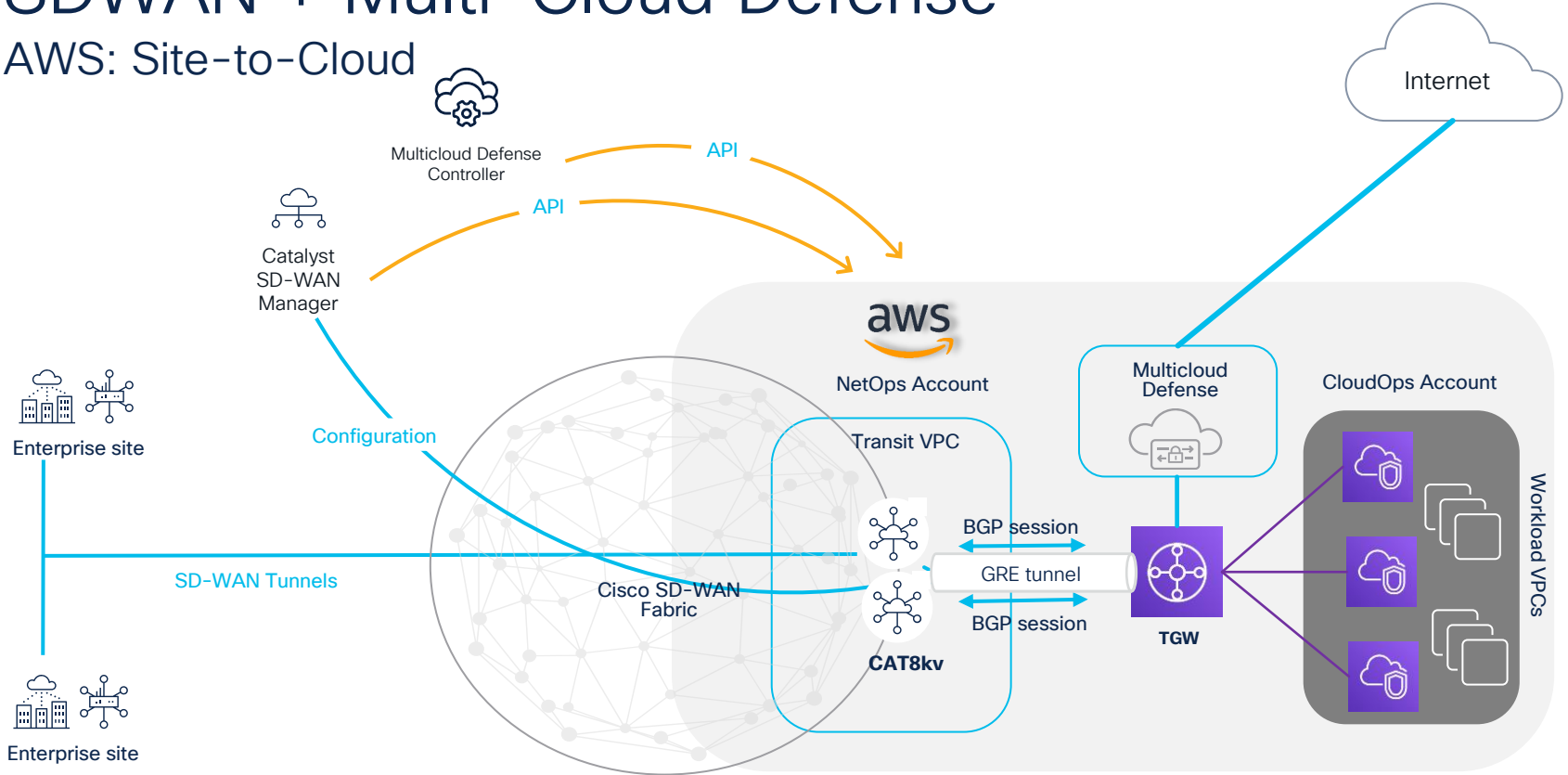
Controller simplifies
orchestration

- 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



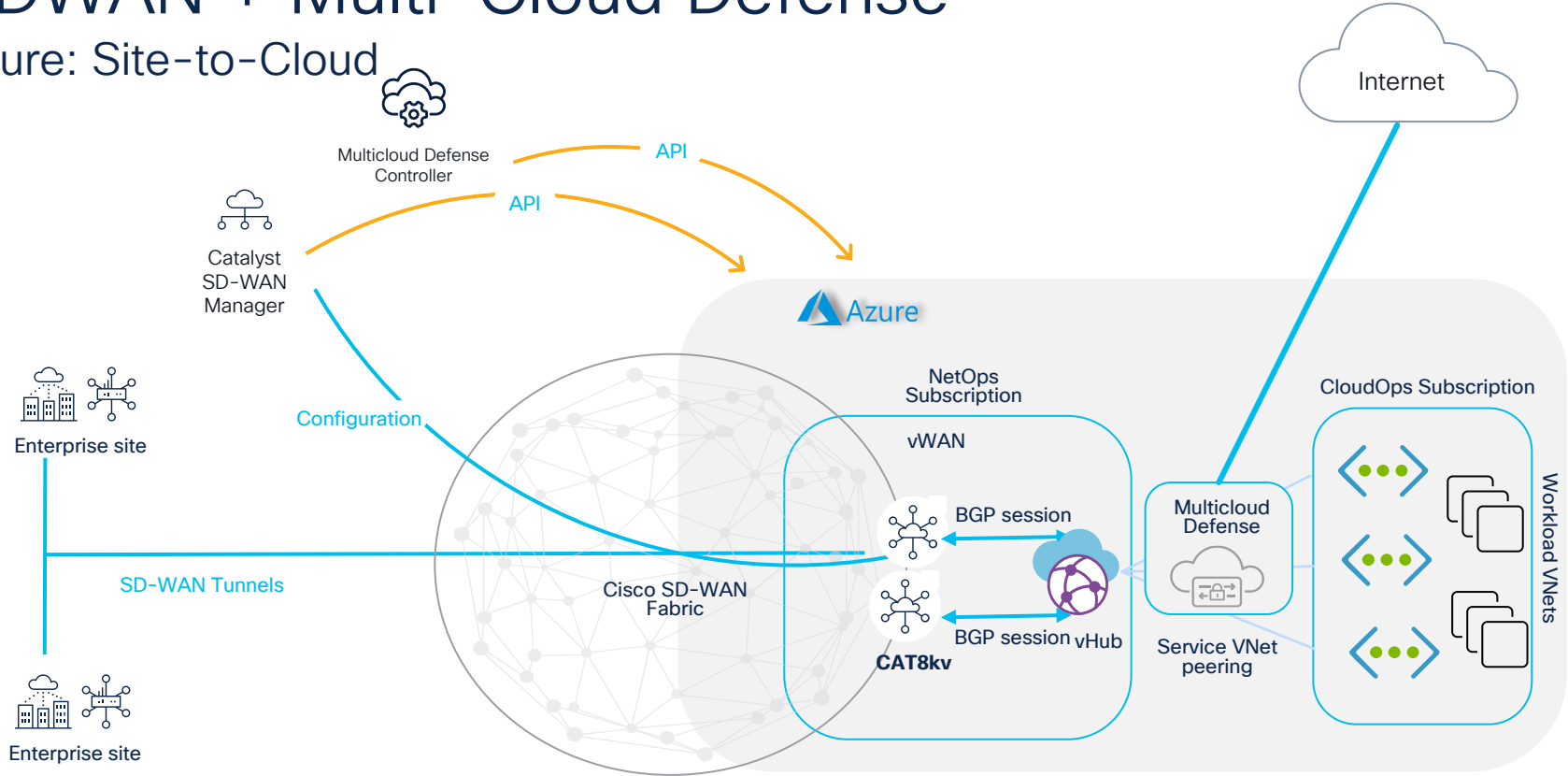
SDWAN + Multi-Cloud Defense

AWS: Site-to-Cloud

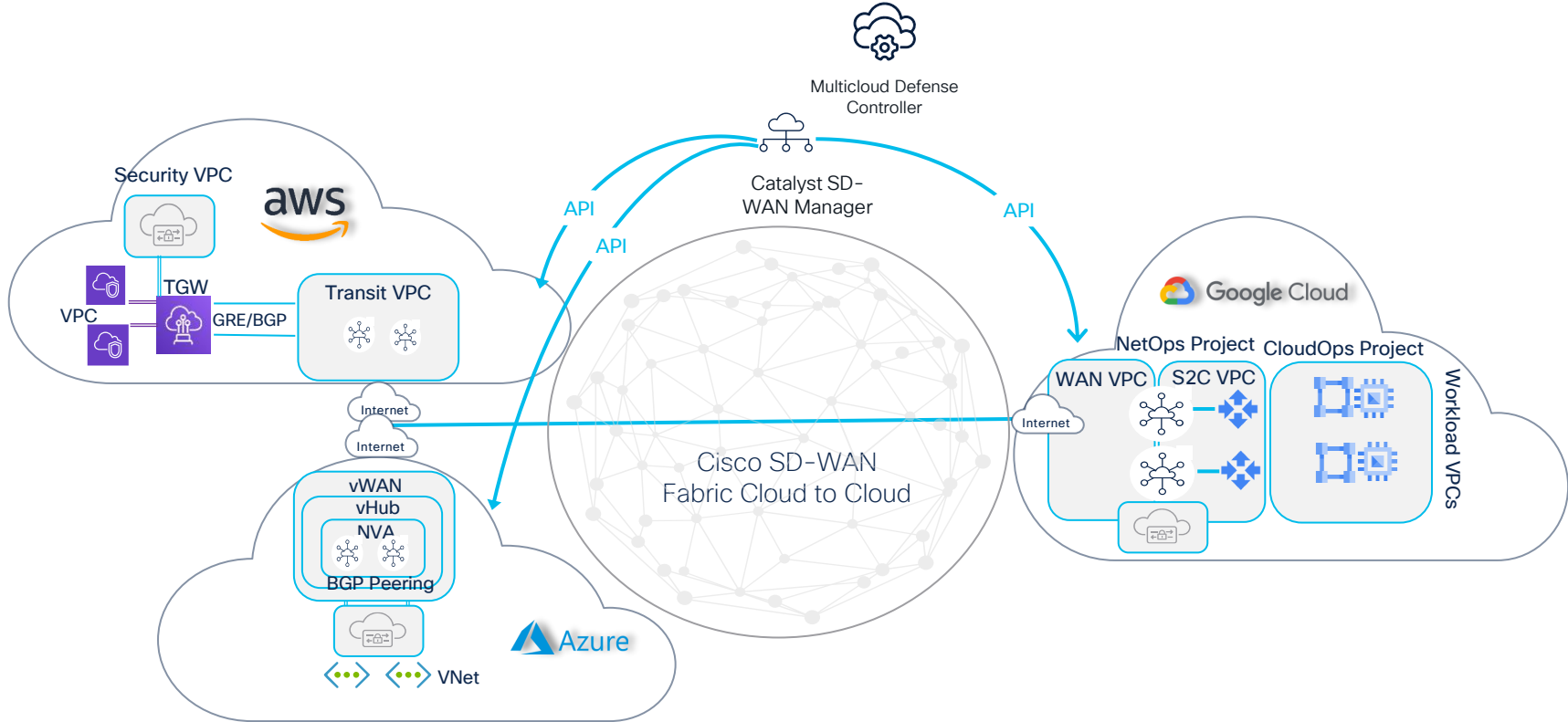


SDWAN + Multi-Cloud Defense

Azure: Site-to-Cloud

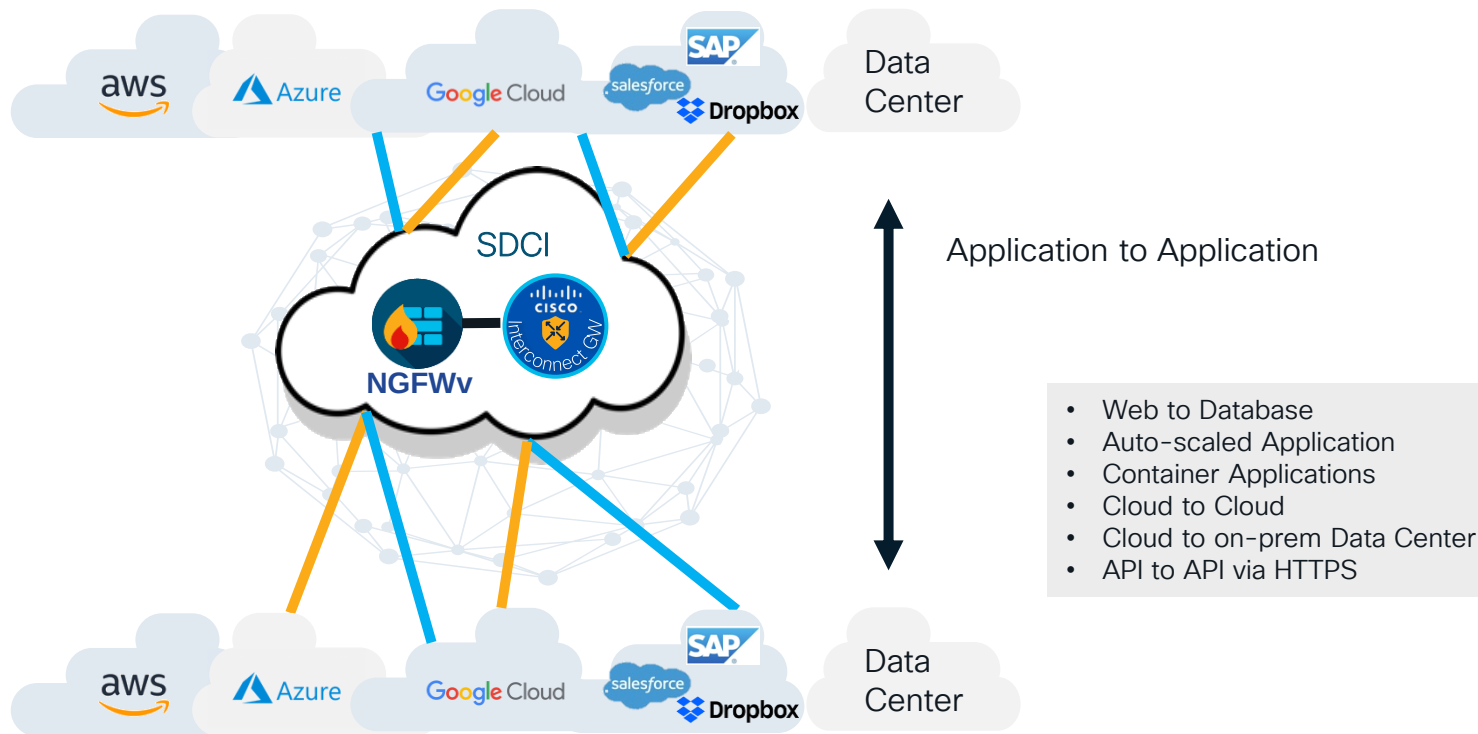


Security Stack Insertion in the Cloud



Transparently secures Application-to-Applications

SDWAN + NGFWv + MCD

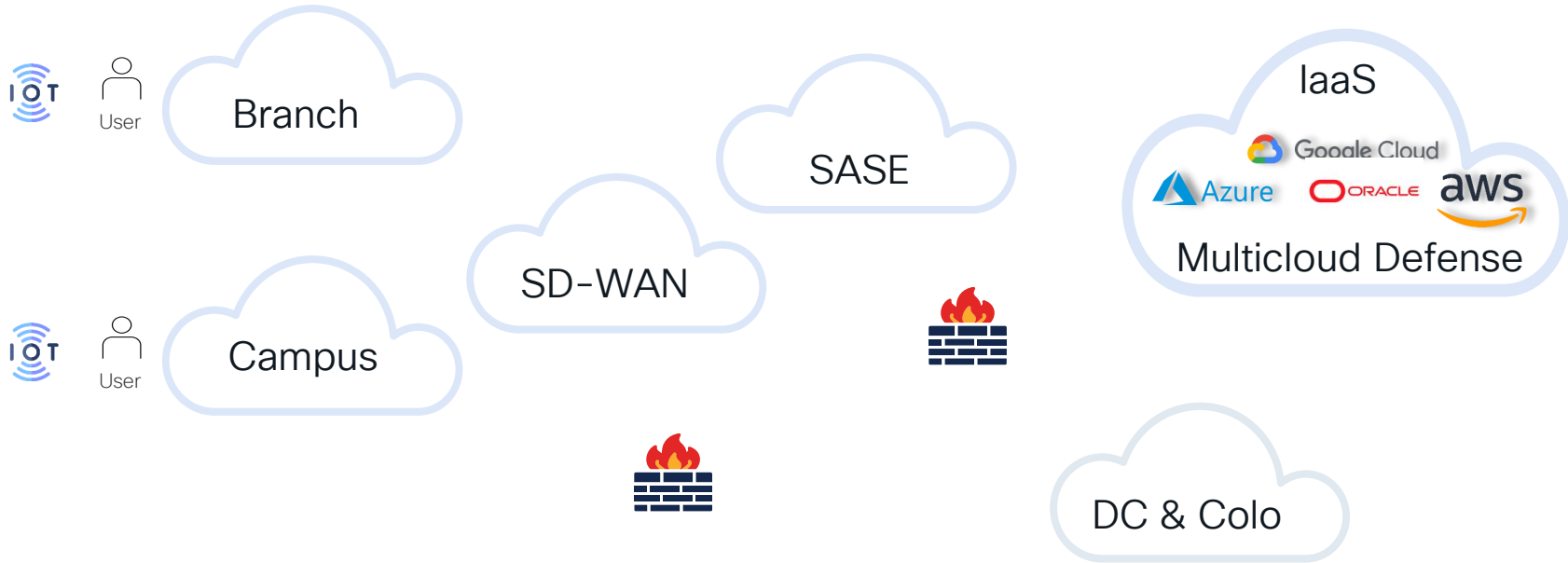


- Web to Database
- Auto-scaled Application
- Container Applications
- Cloud to Cloud
- Cloud to on-prem Data Center
- API to API via HTTPS

Common Policy



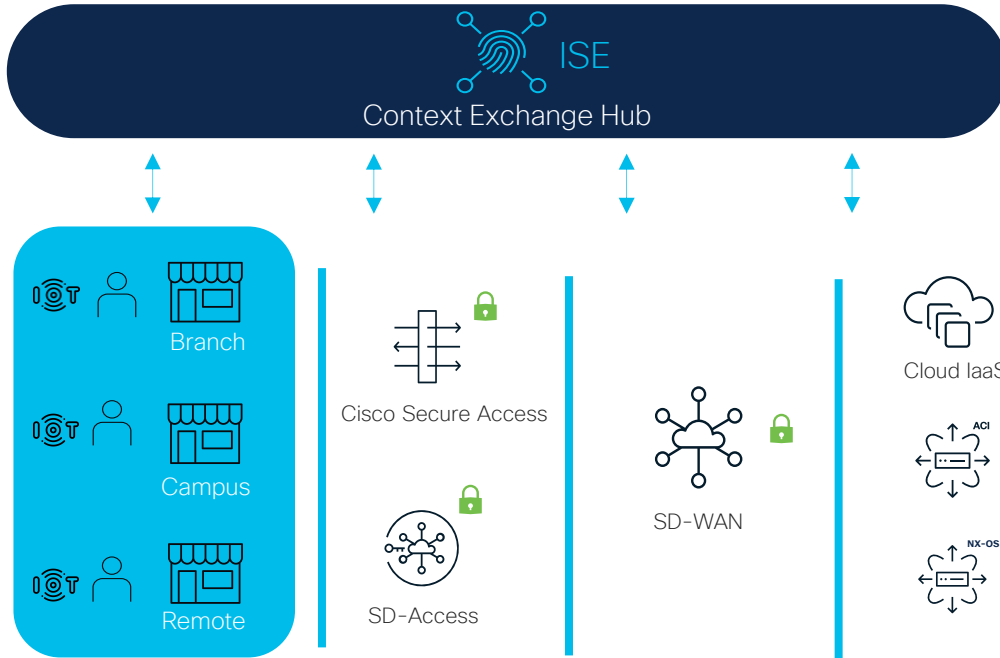
We talked about...



How do we bring all of this together?



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.



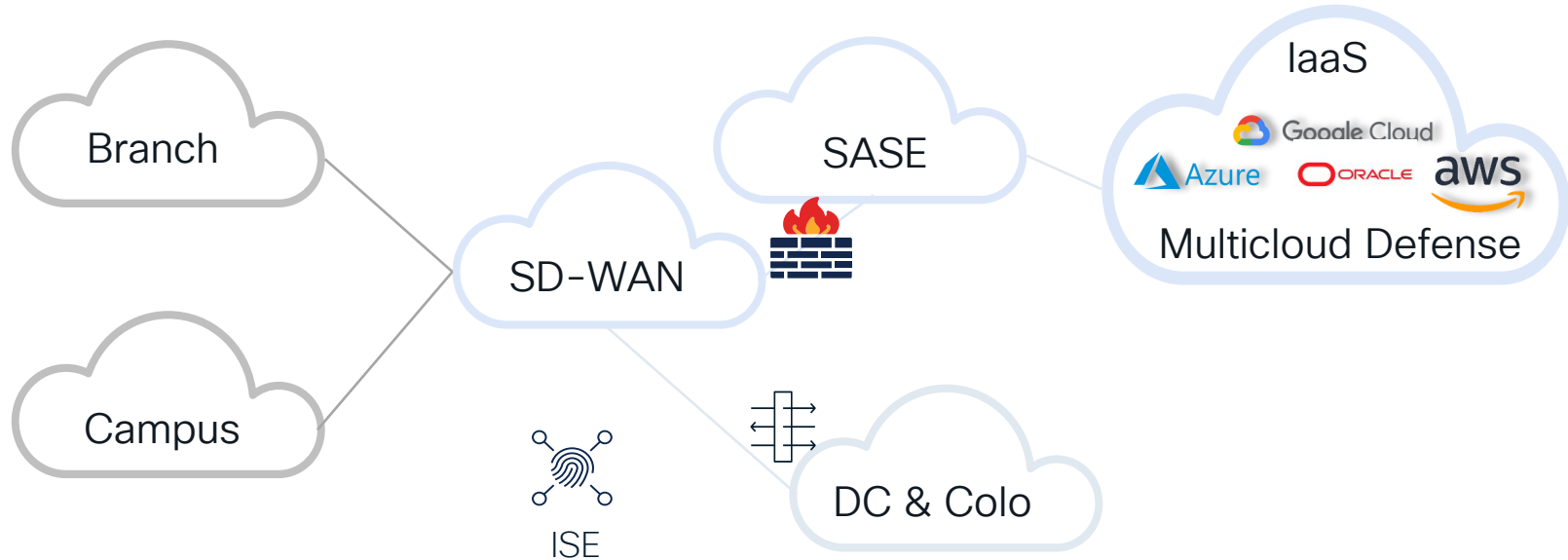
Enforce consistent SGT-based policies; enable simple and unified policy experience.



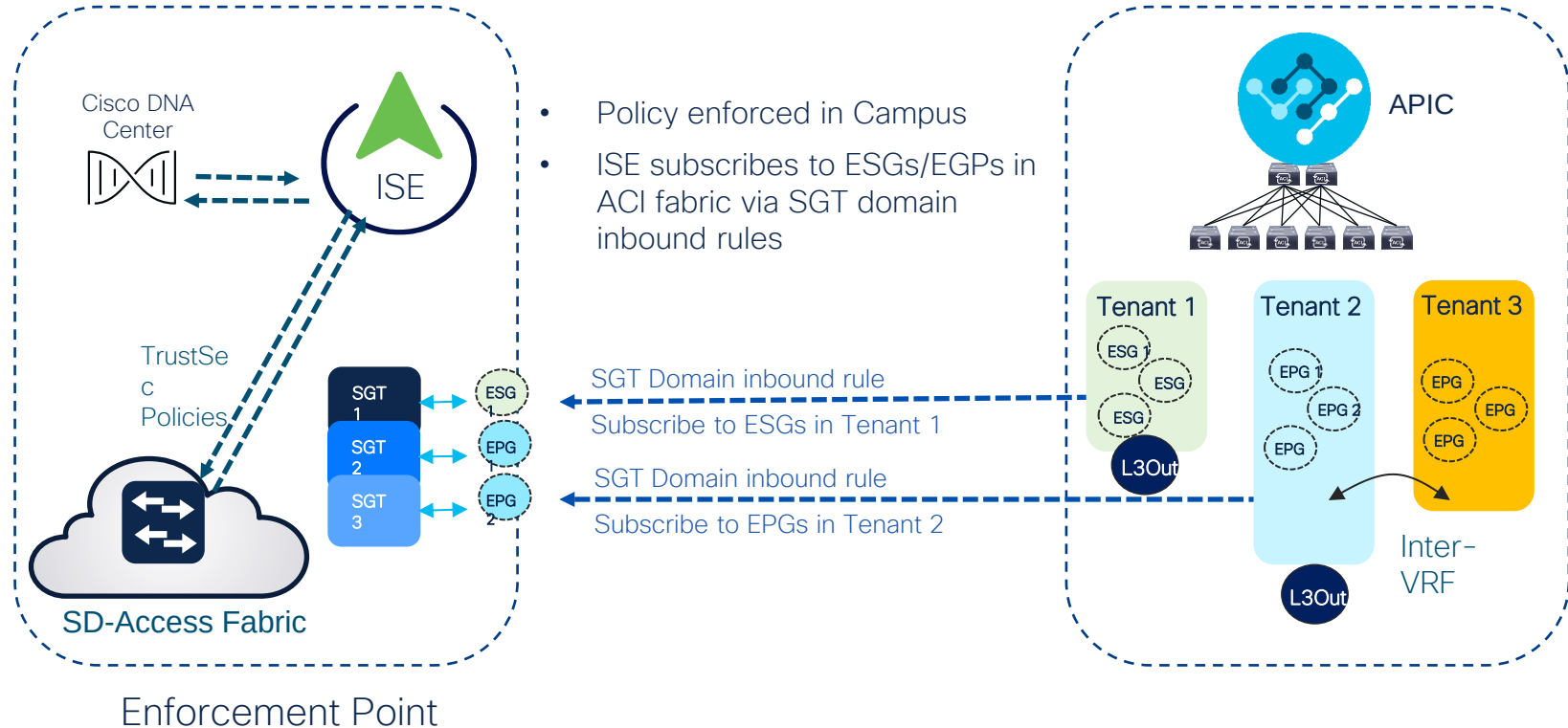
Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

Common Policy

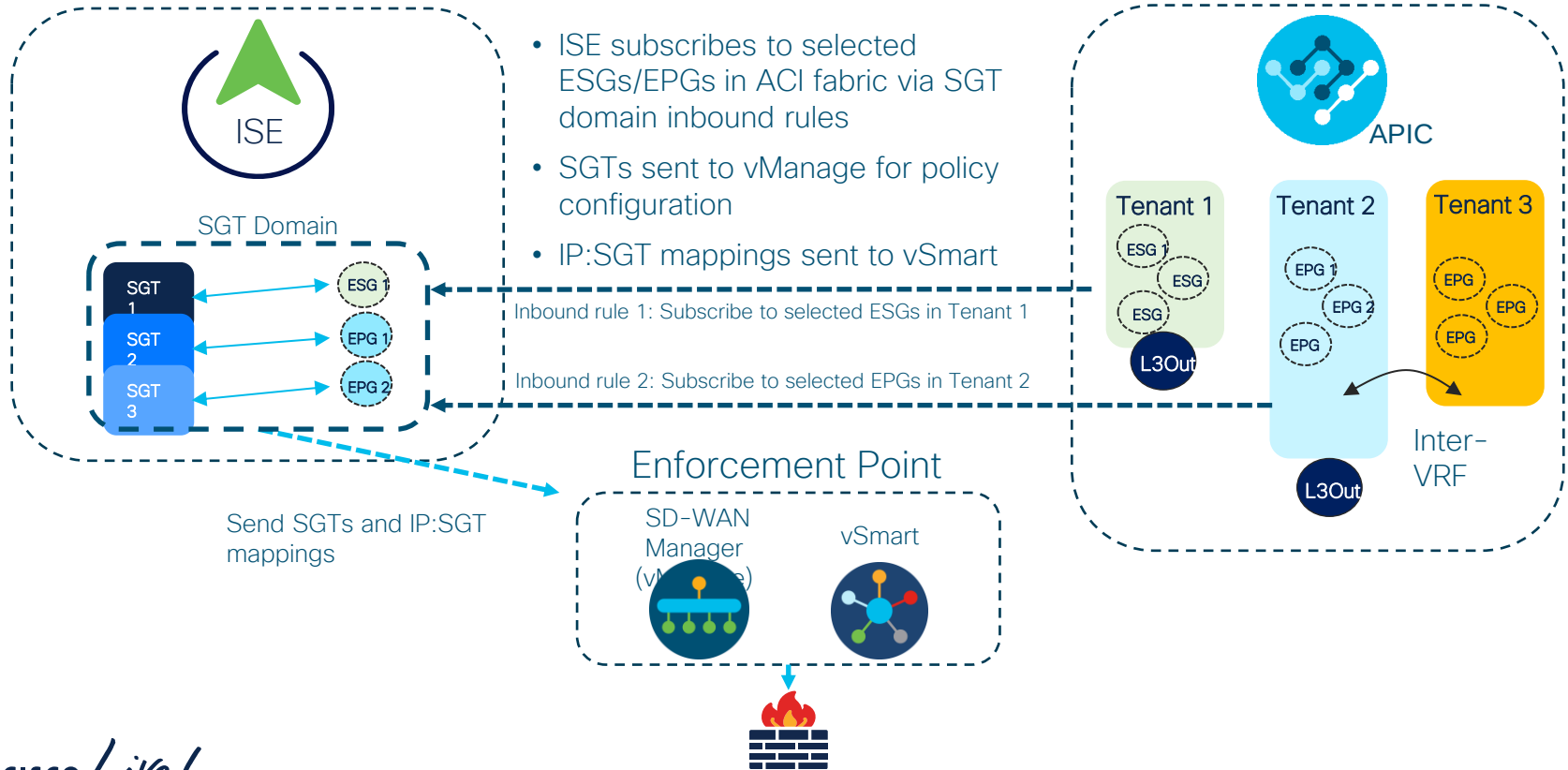
Use Cases



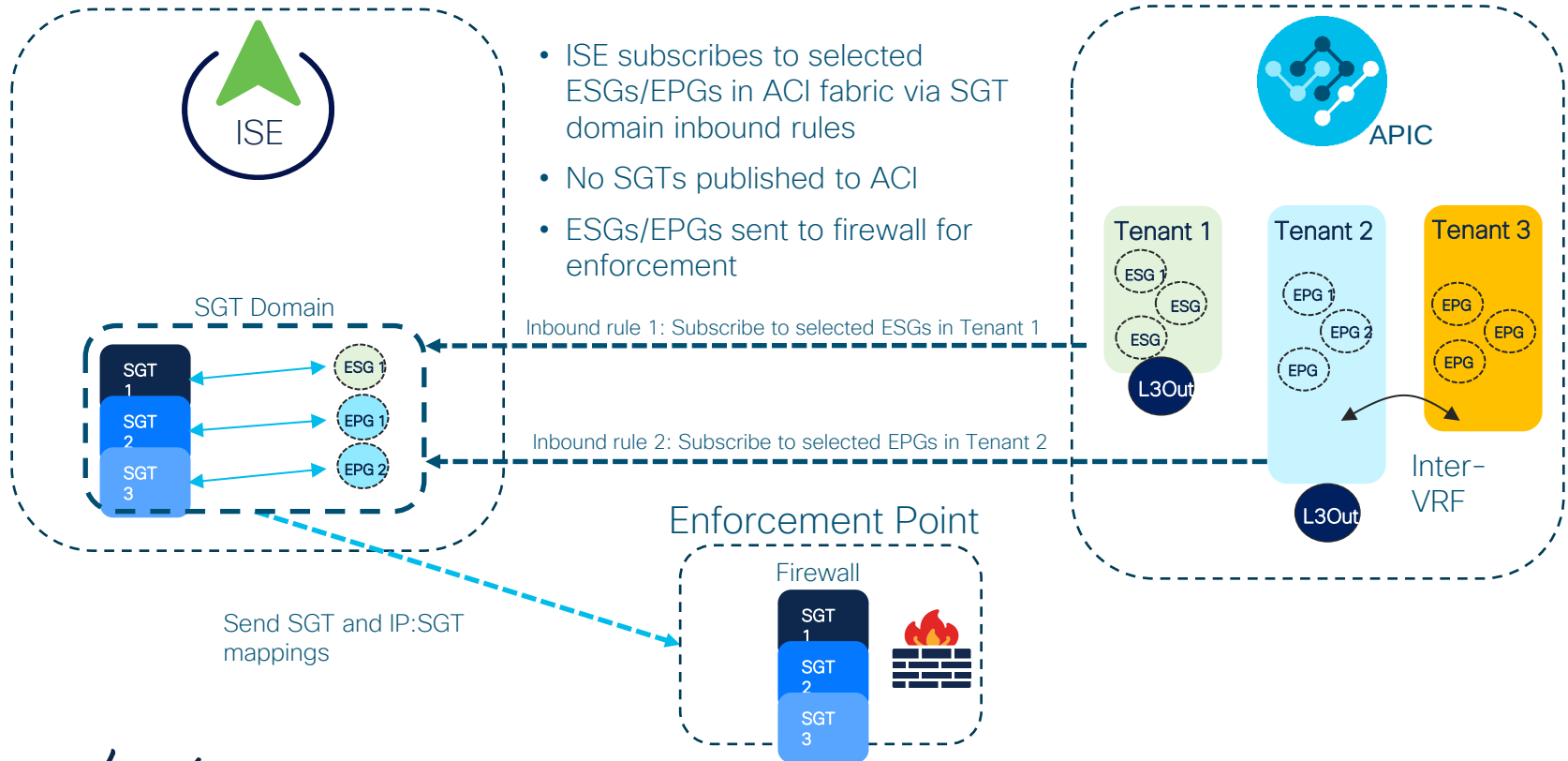
Use Case: Policy Enforcement in Campus



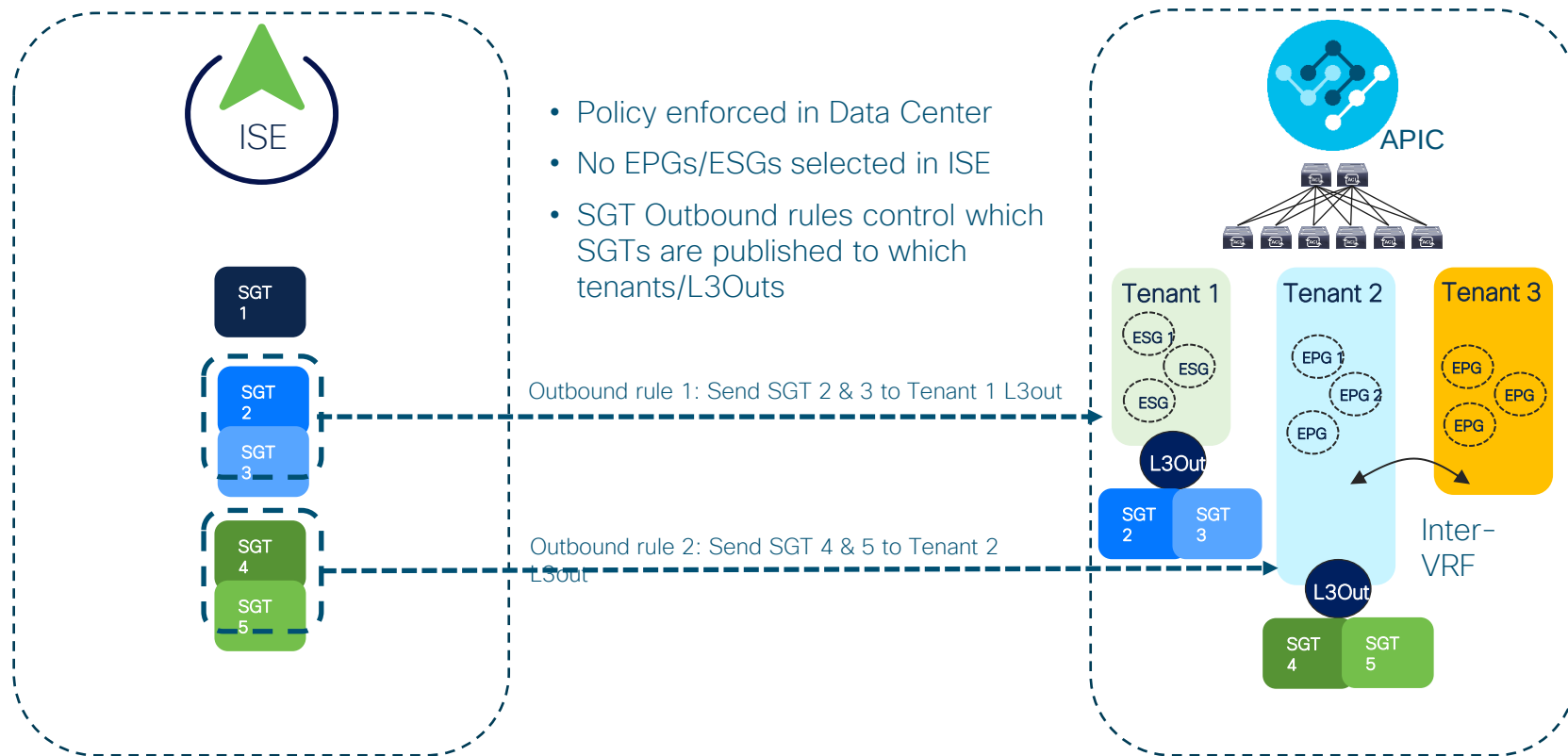
Use Case: Policy Enforcement in SDWAN



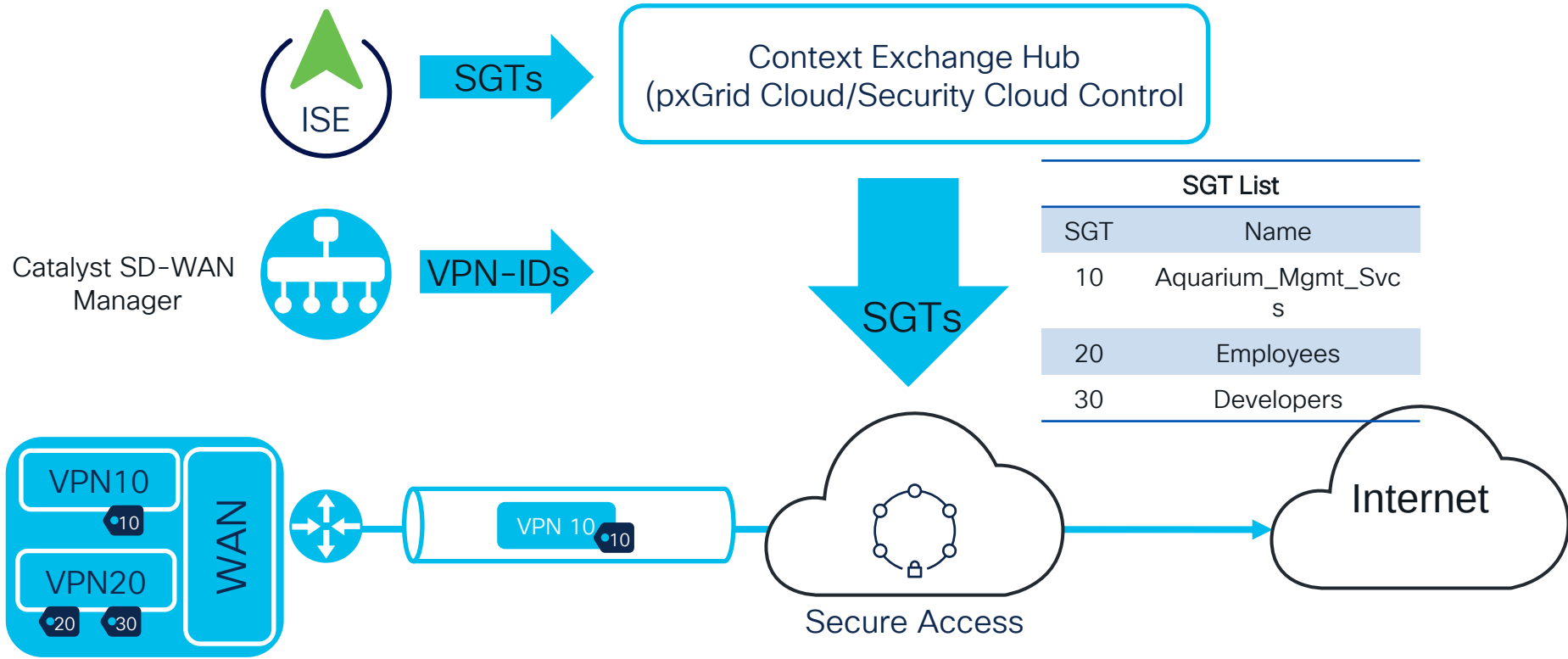
Use Case: Policy Enforcement in Firewall



Use Case: Policy Enforcement in Data Center



ISE / SDWAN / Secure Access Integration



Common Policy

Bringing it all together

Micro-Segmentation

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



Service Chaining

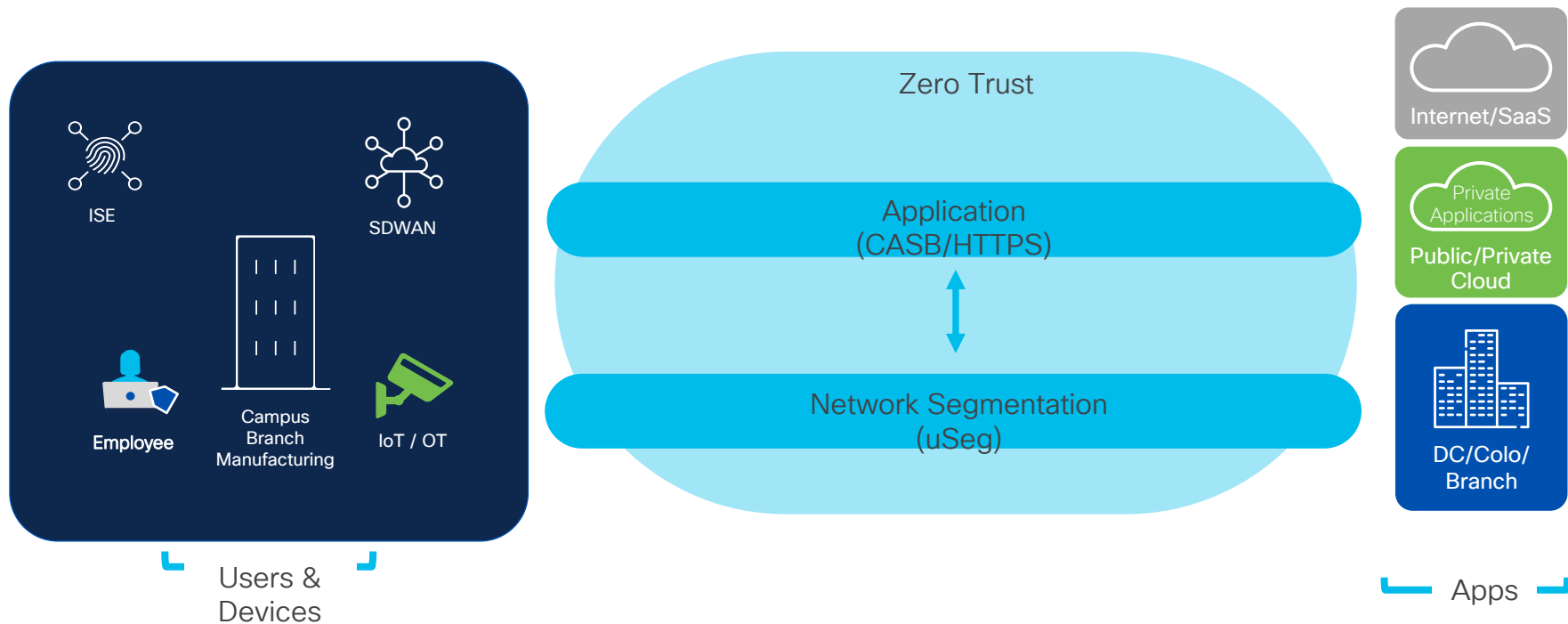
- VXLAN GPO can be used to insert network services into a packet flow based on specific policy criteria.



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

Common Policy Enables Full-Stack Zero Trust

Application and Network



Visibility



Visibility: AWS Inter Region

Thousand Eyes: Dallas, TX to Ashburn, VA

Path Visualization

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) ▾**

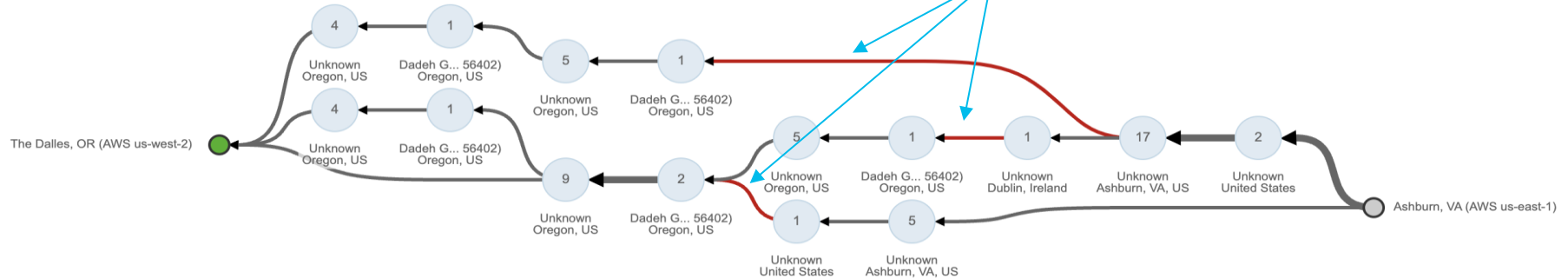
Selecting: Click a node or link Info (1) ▾

3 hops 1 hop

Highlight nodes that match all / any

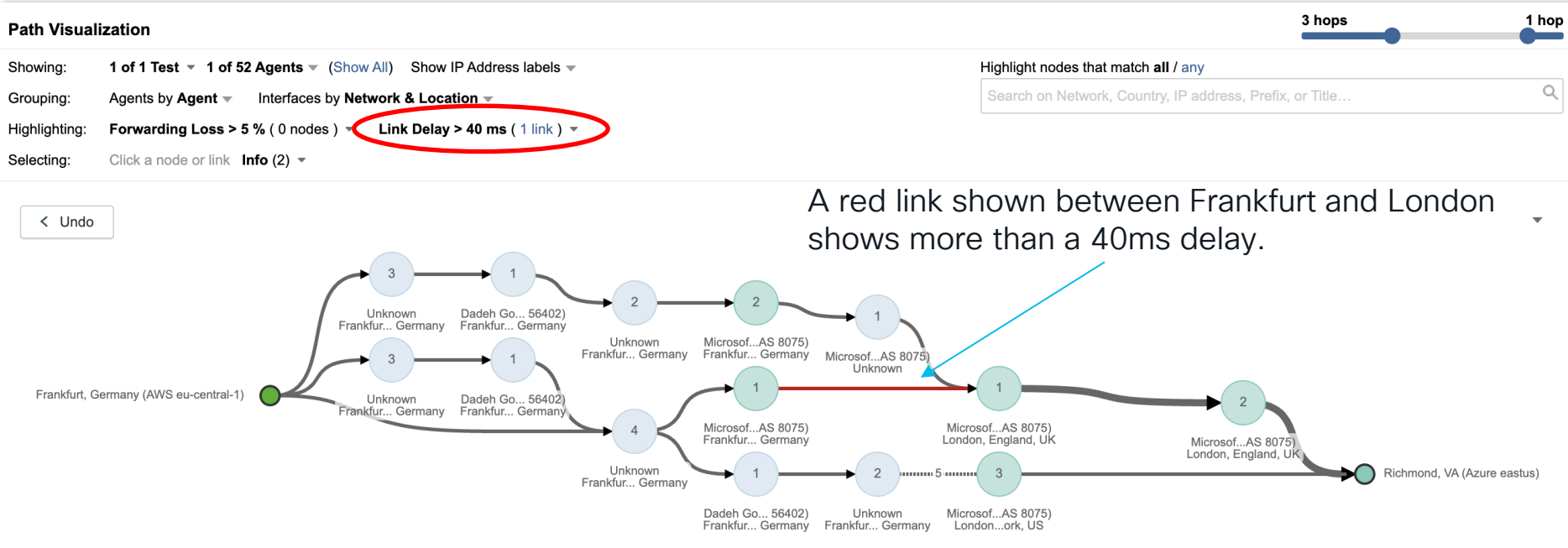
Search on Network, Country, IP address, Prefix, or Title...

< Undo



Visibility: AWS/Azure Inter Cloud

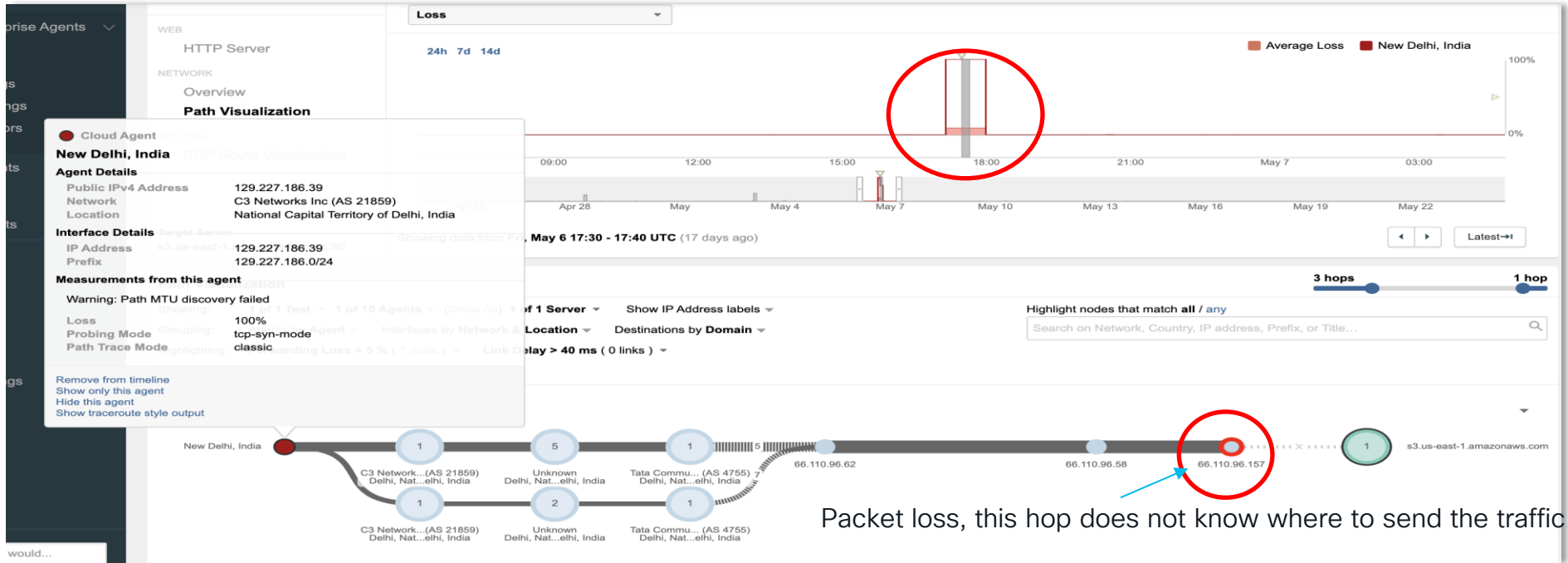
Thousand Eyes – Frankfurt, Germany AWS to Richmond, VA US Azure



- 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

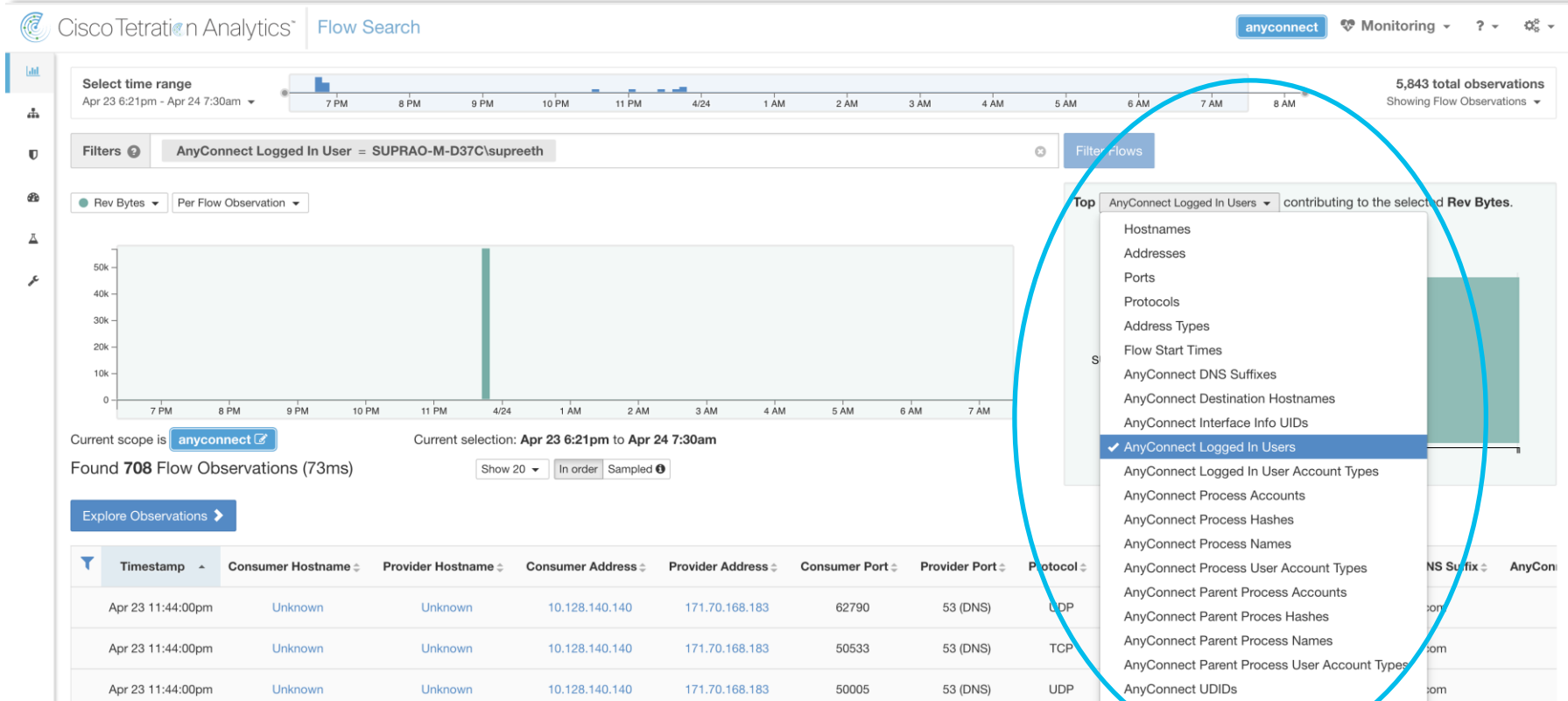
Visibility: AWS/Azure Inter Cloud

Thousand Eyes - End user perspective from New Delhi to S3 Service



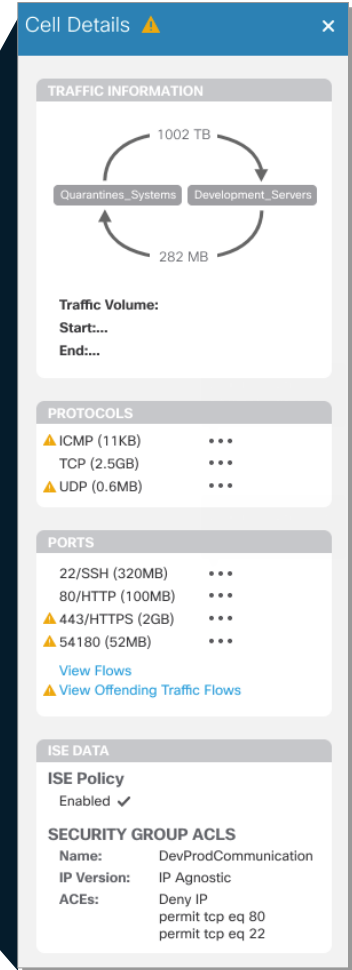
Depicted above is the loss of service, source of loss and time of outage.

Secure Workload Flow Search

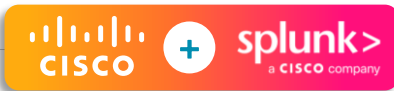


Secure Network Analytics

Trusted ISE Policy - Near Real Time Network Telemetry



Digital Resilience: Hybrid Multi-Cloud



1 Get data in: On-board data to Splunk Data Platform

- Technical add-ons (TAs), Open Telemetry, API endpoints
- Infrastructure and Application Metrics, Events, Logs, Traces
- Microservice and Cloud via gRPC, eBPF

2 Connect your data: Join disparate systems and domains

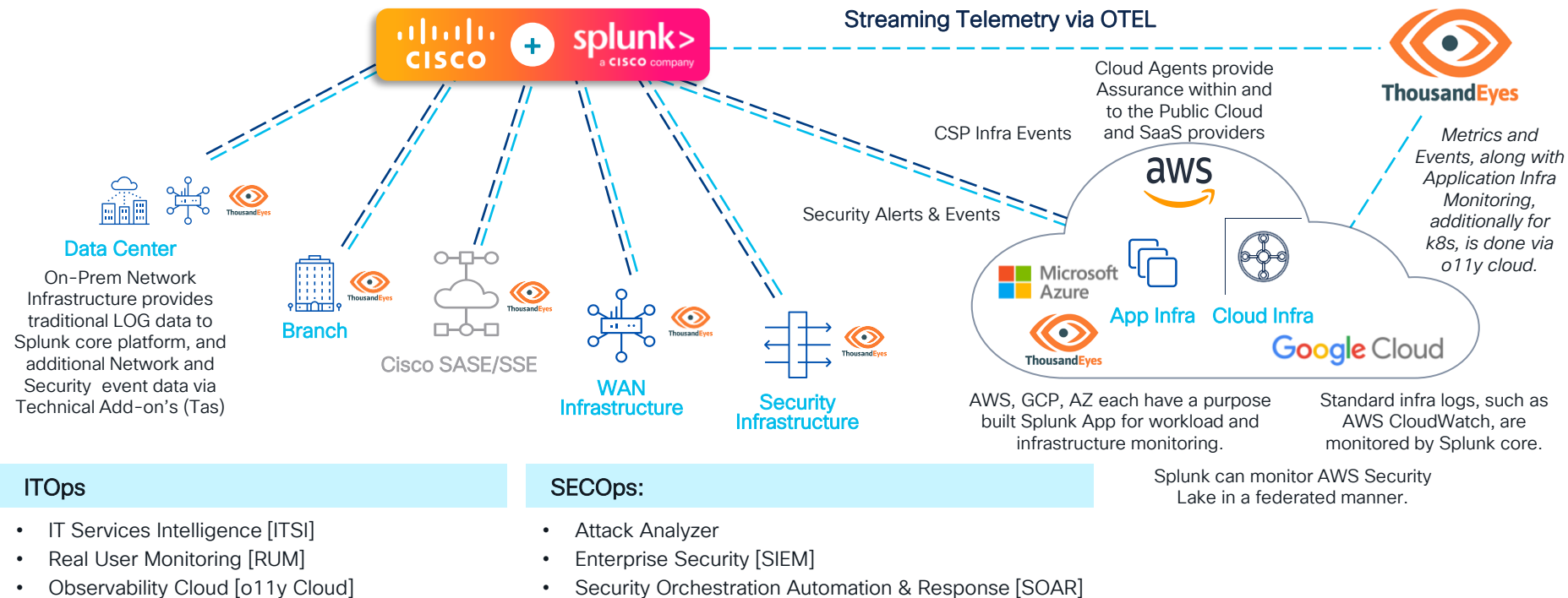
- Performance Monitoring, Incident Management, Insights
- Machine Learning to analyze, eliminate noise / duplication
- Prioritize what is significant and impactful

3 Protect your environment:

- Prevent disruption with greater visibility
- Remediate faster with AI/ML and Automation

Enables both SECOps and ITOps with shared context

Providing End to End Threat Intelligence and Observability for Multi-Cloud



Assurance and Security events and alerts, portfolio to provide coordinated, distributed, enforcement in response.

Finally, what About Infrastructure as Code?

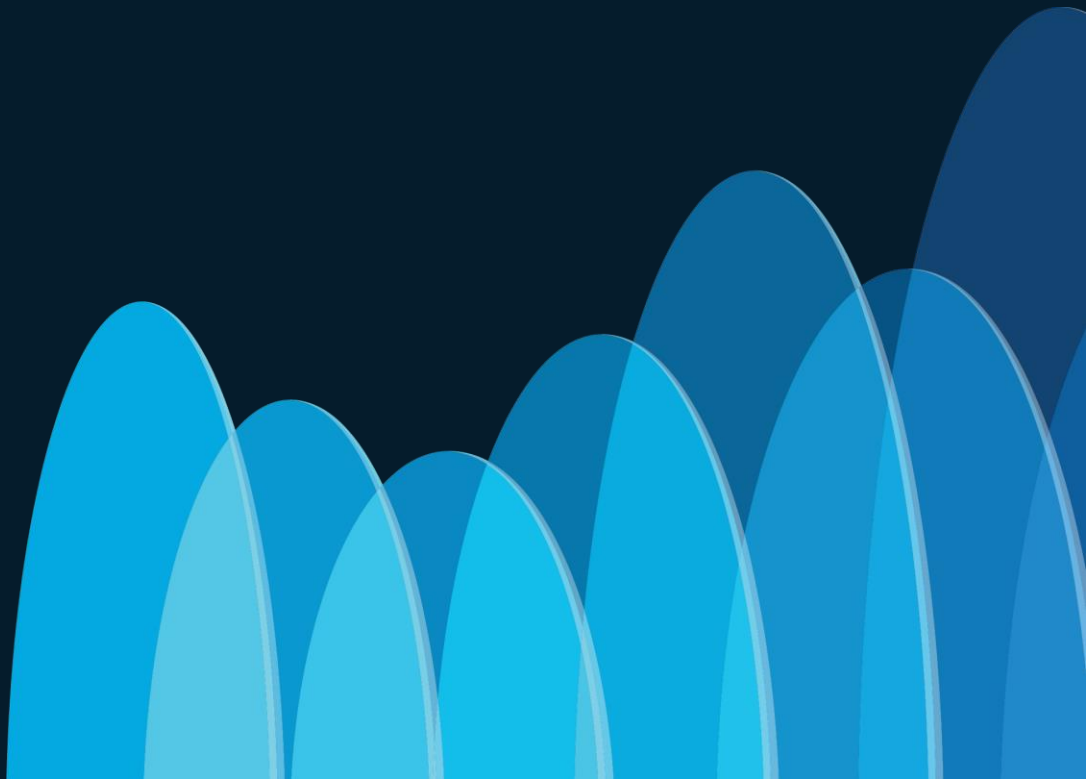


<https://registry.terraform.io/namespaces/CiscoDevNet>

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



Summary



Summary

- This is about customers expanding to the cloud not Migrating to the Cloud.
- Simplified network operations for Multi-Cloud
- Security controls and capabilities are to protect users/devices, things, applications, and data.
- Ability to define dynamic classification (source and destination), define policy and enforcement
- Policy + Network Visibility

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC