Architecting Hybrid Multi-Cloud Infrastructures

David Jansen - Distinguished Solutions Engineer
CCIE #5952

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!

Webex App

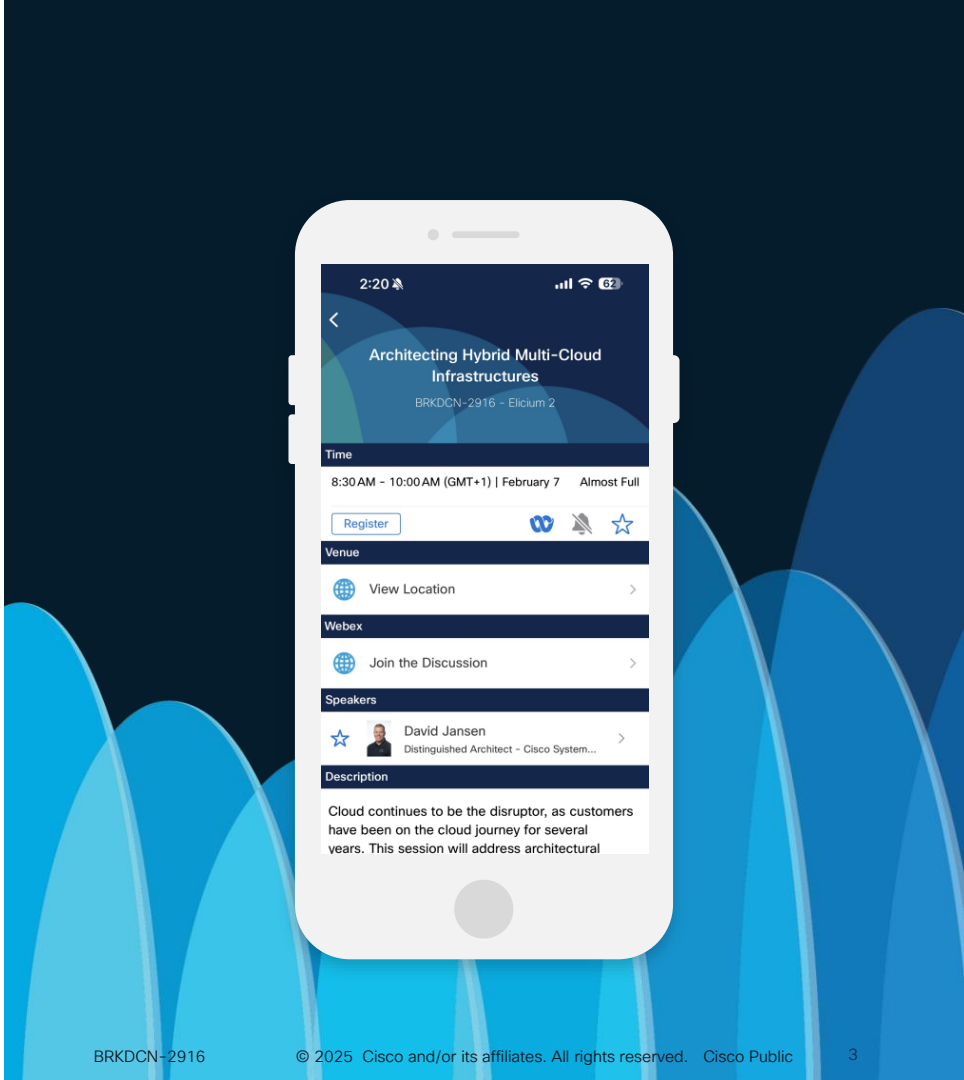
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



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

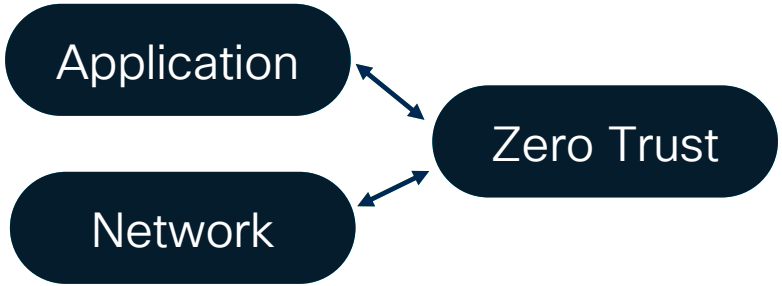
Abstract

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

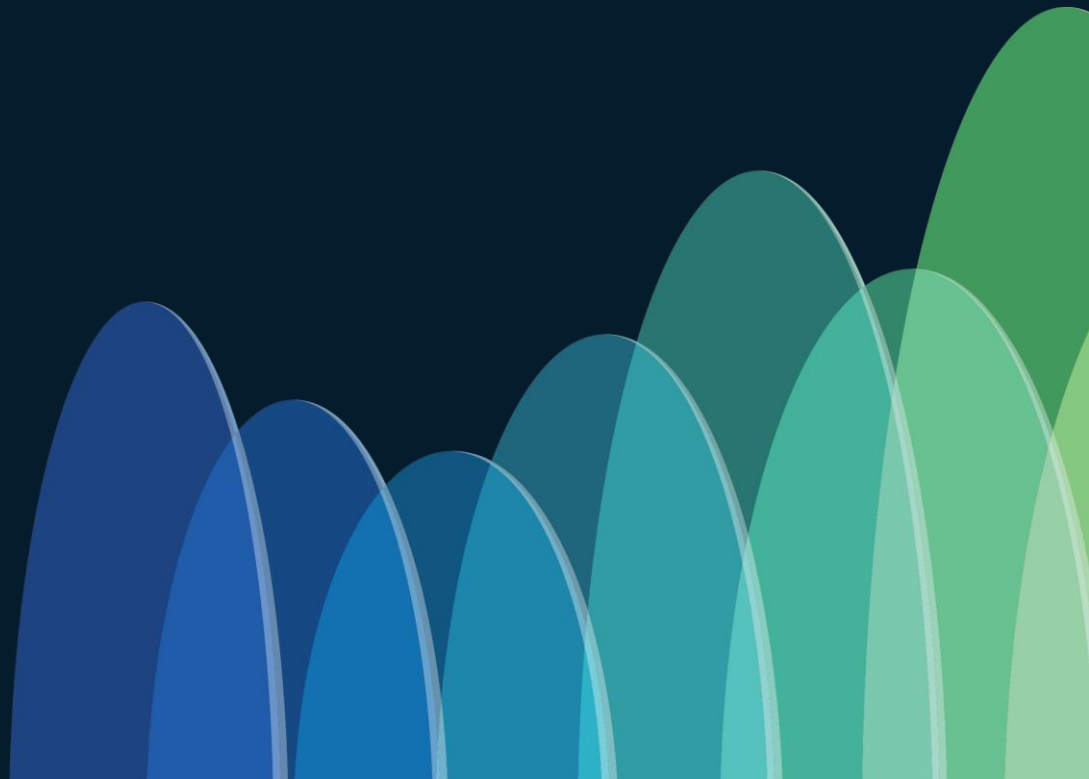
*Multi-Cloud and Multicloud are used interchangeably in this session

Cloud Terminology Matrix

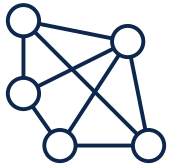
For Your Reference

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



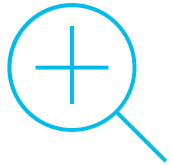
Challenges to solve



Network connectivity

Segmentation and security

Automation

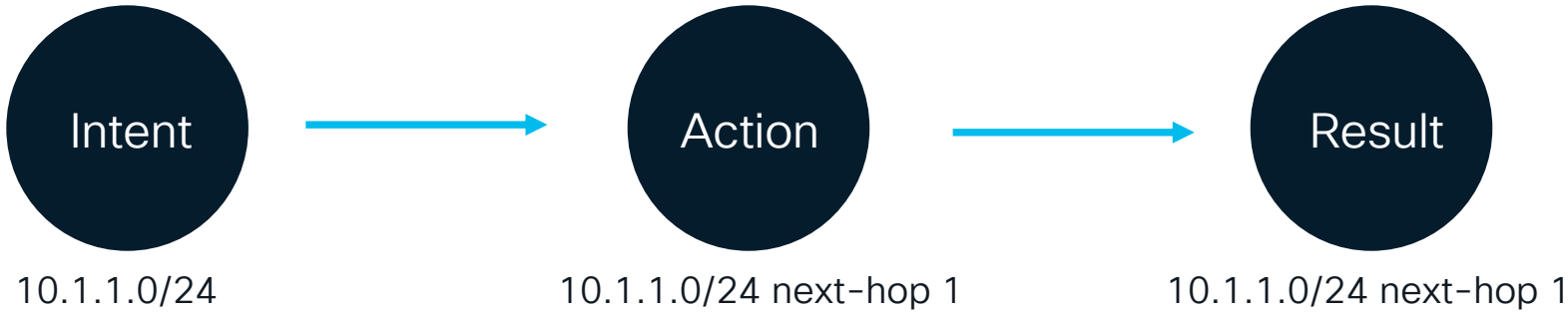


Operations and visibility

Need For Homogenous Experience Across Heterogenous Cloud Environments

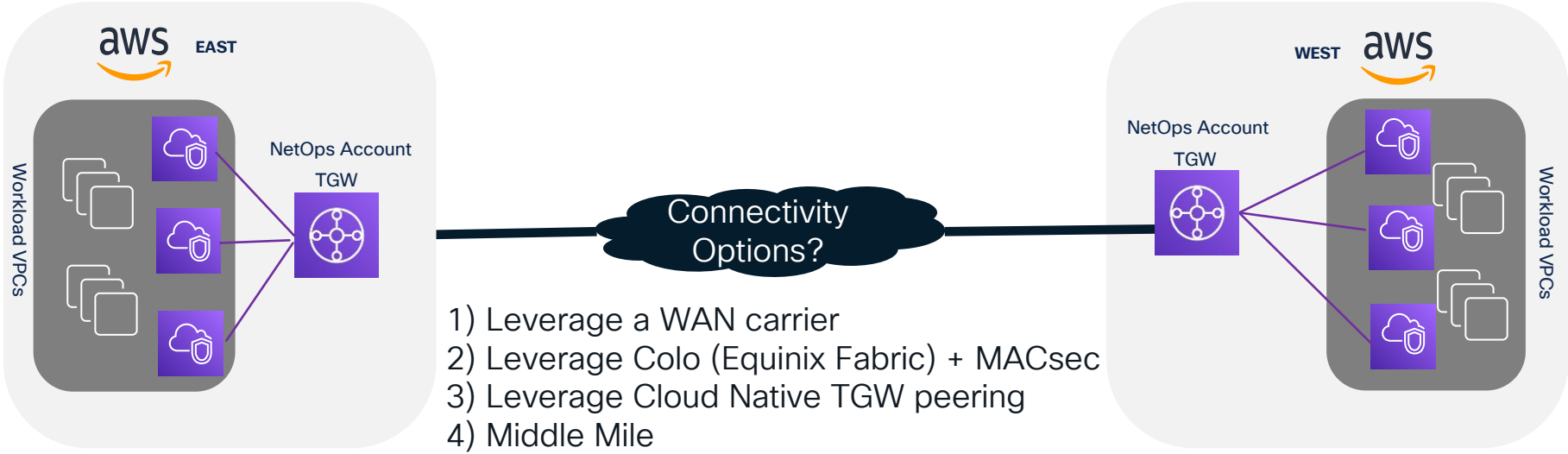
Cloud Native Routing

- 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

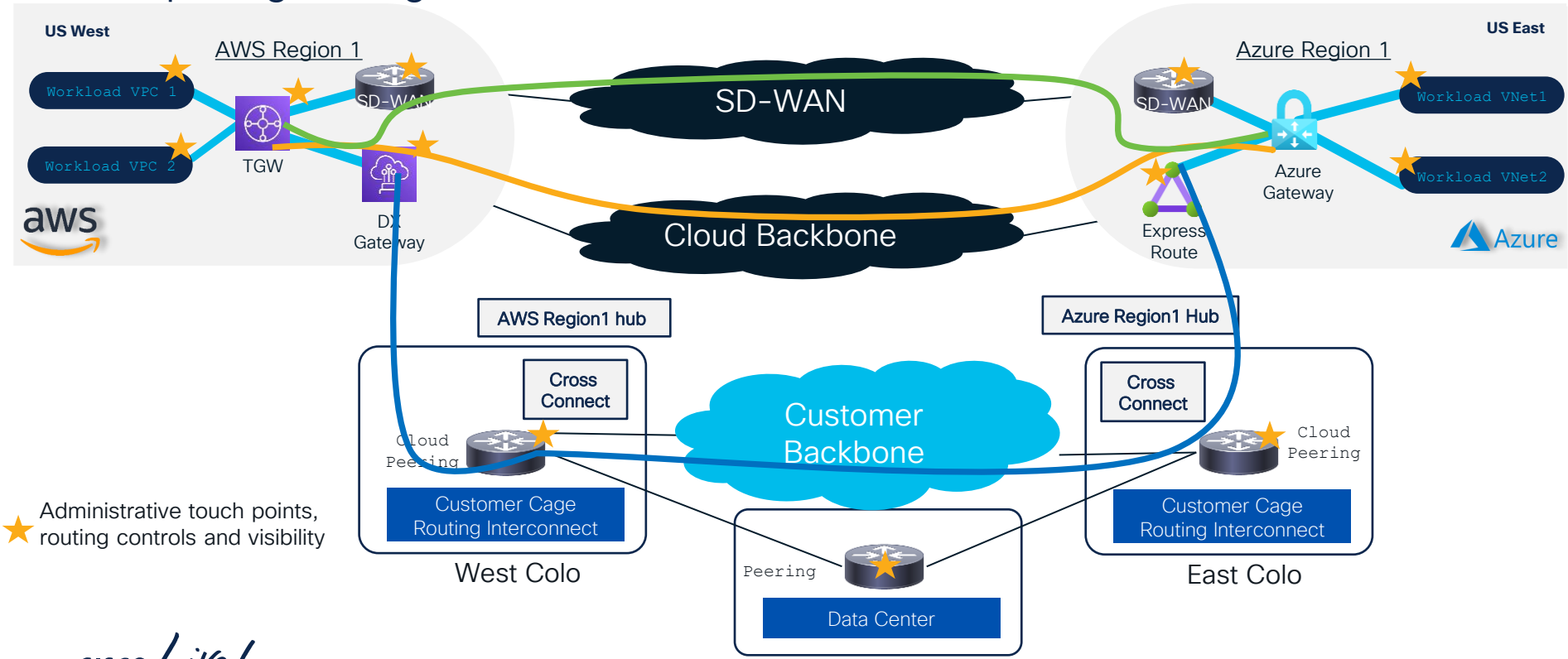


1) Leverage a WAN carrier
2) Leverage Colo (Equinix Fabric) + MACsec
3) Leverage Cloud Native TGW peering
4) Middle Mile
5) AWS Cloud WAN
6) Azure Virtual WAN

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



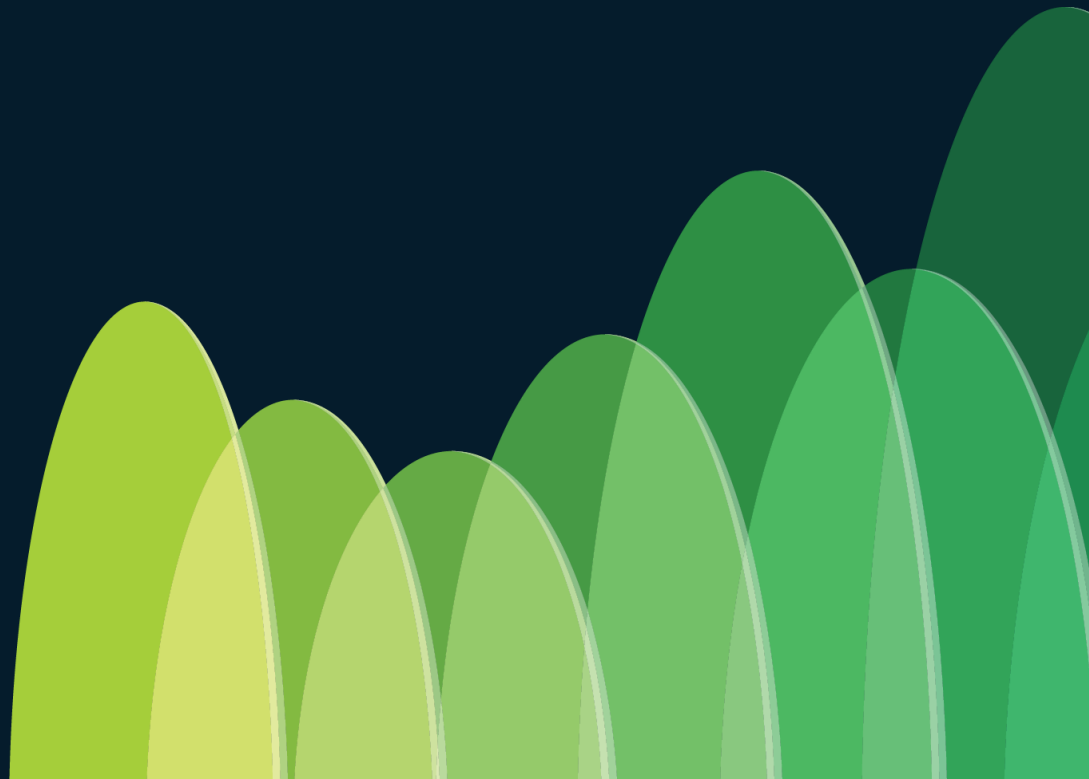
★ Administrative touch points, routing controls and visibility

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

Devices

Users

Things

Digital Resilience

AI Security

Zero Trust

Zero Trust Network Access

Infrastructure

Applications/Data

webex by cisco

salesforce

Office 365

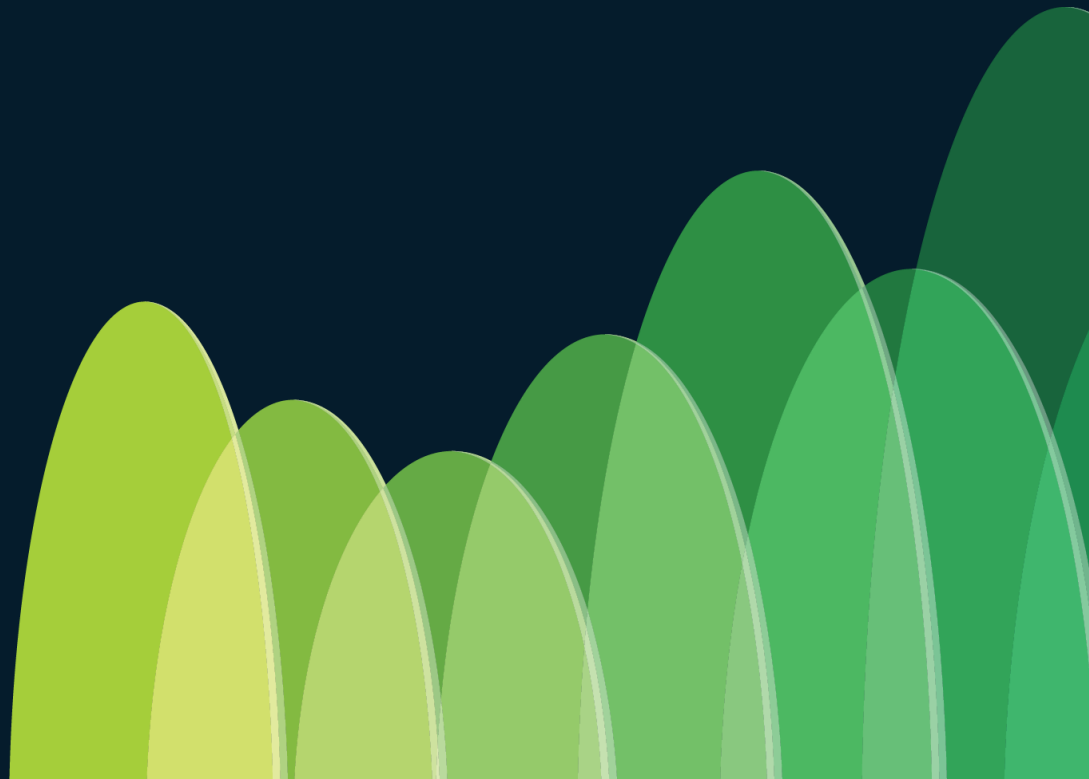
aws

Google Cloud

Azure

Data Center

Key Capabilities

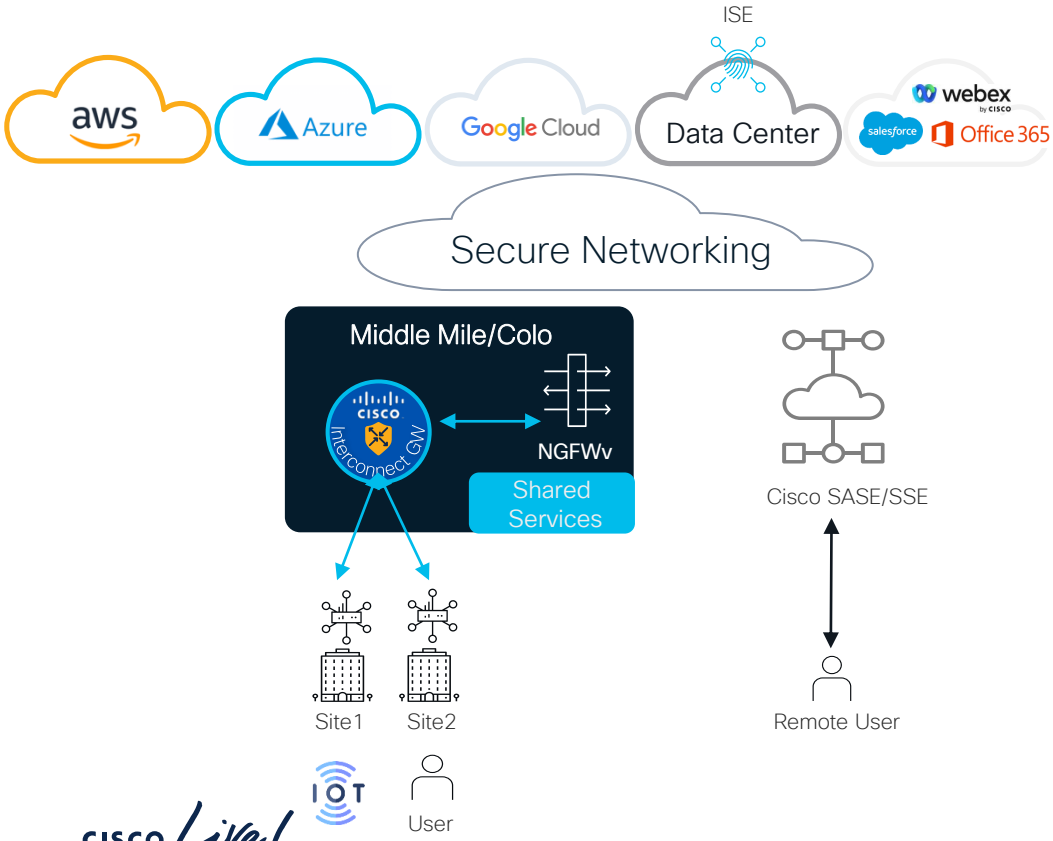


Taxonomy, a few more...

- 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

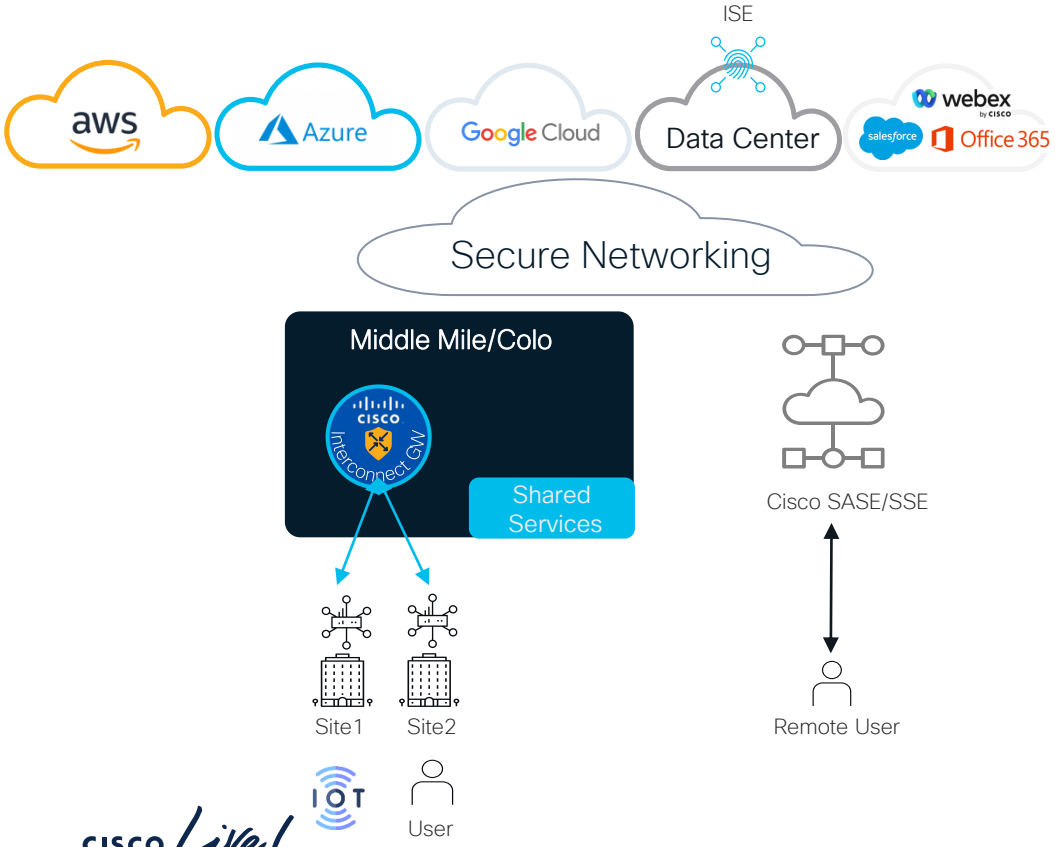


- Secure Remote Users / locations / sites
- IaaS / Saas / Internet / Private DC
- IoT Use-Cases
- Automation + Management + Visibility
- Segmentation (macro/micro)
- Policy Enforcement Points
- Common Policy

Middle Mile:

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

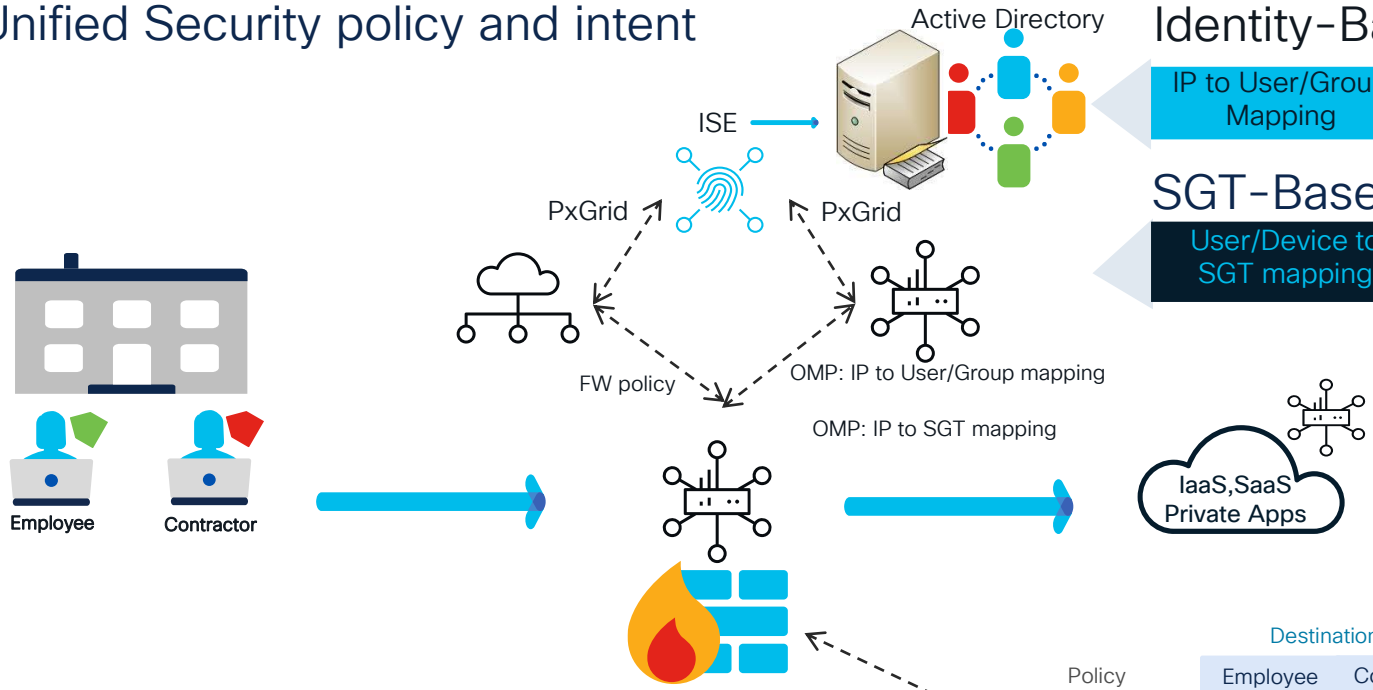
Capabilities: Site/User-to-Cloud



- SD-WAN + Firewall
  - Identity-Based Firewall
  - SGT-Based Firewall
- Ability to carry + Enforce 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



Identity-Based Firewall

IP to User/Group Mapping

SGT-Based Firewall

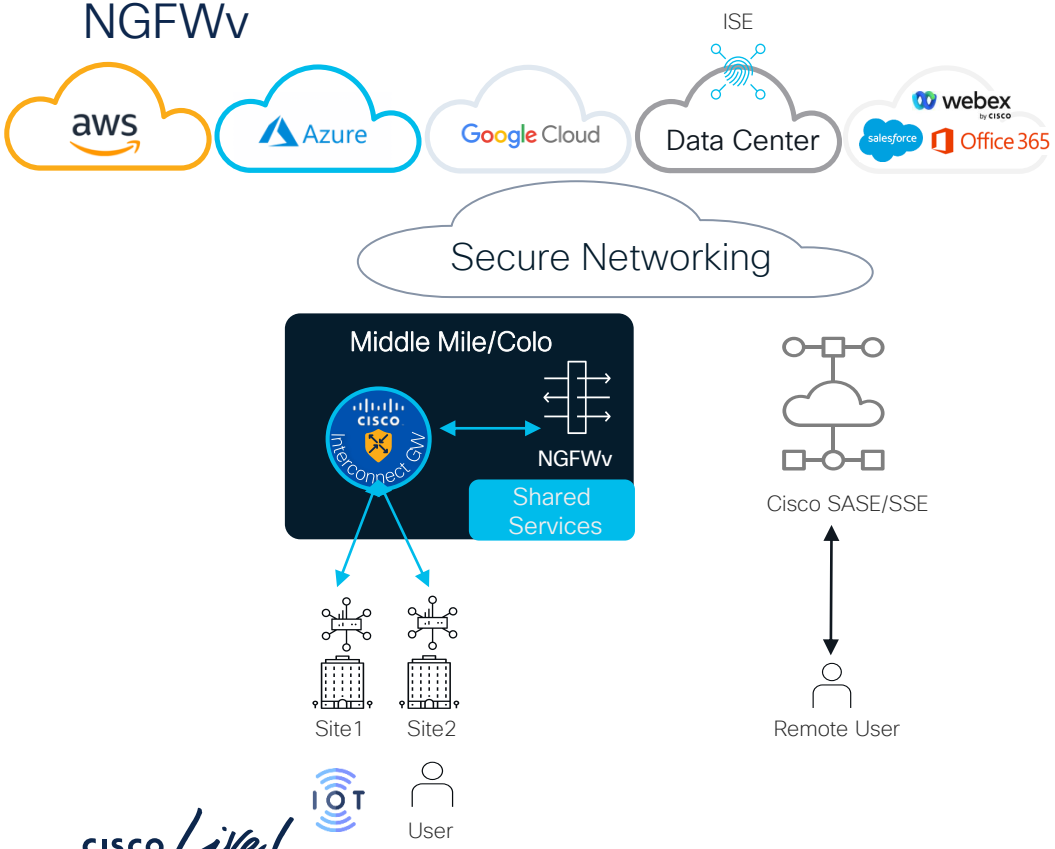
User/Device to SGT mapping

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

Granular Security Control at User/Group Level

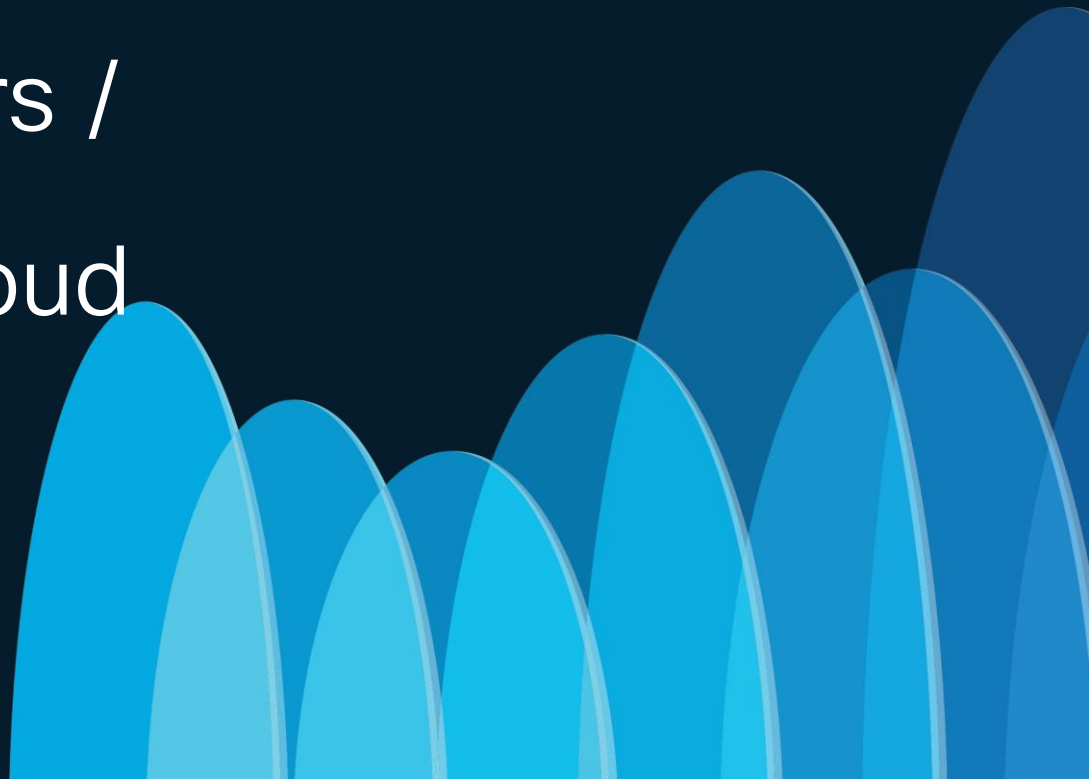
Capabilities: Site/User-to-Cloud

NGFWv



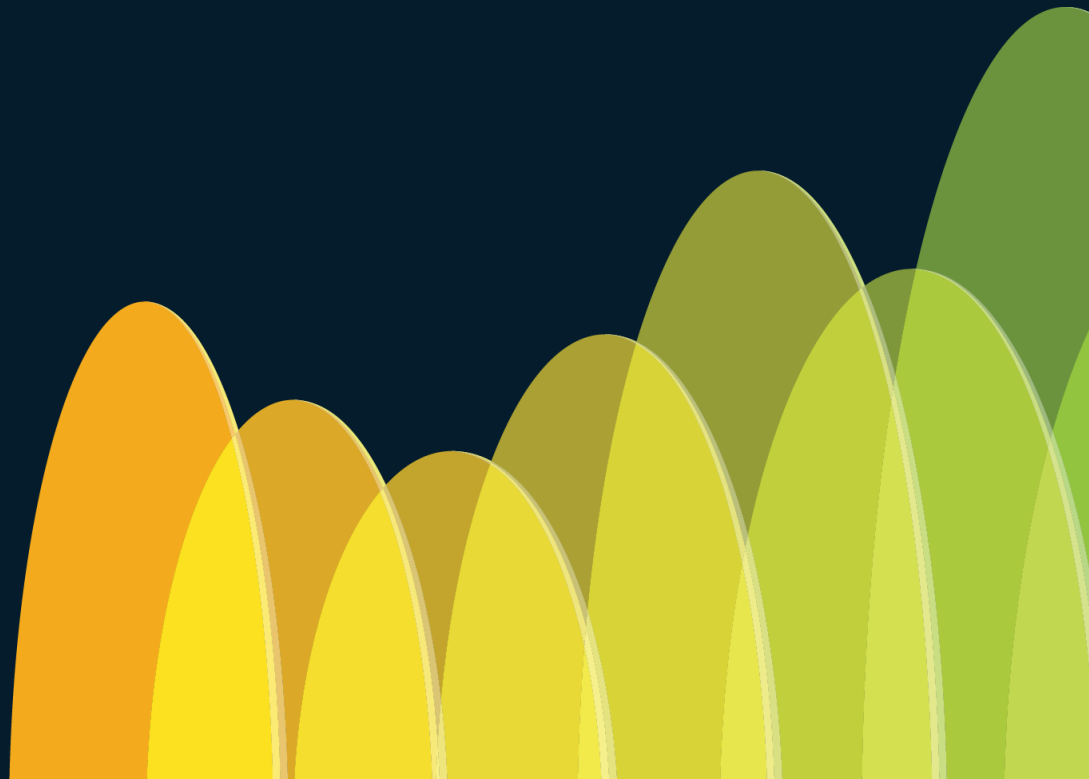
- Require Advanced NGFW
- SD-WAN + FW – NGFWv automated to offer secure policy enforcement point (PEP).
- Catalyst SD-WAN Manager Day0/1, and FW manager (SecOps) Day 2+
- Identity + ISE
- Ability to carry VRF and SGT end to end
- Ability to choose enforcement options
- Identity integration with on-prem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

Connecting Users / Devices / Things to the Cloud



cisco Live!

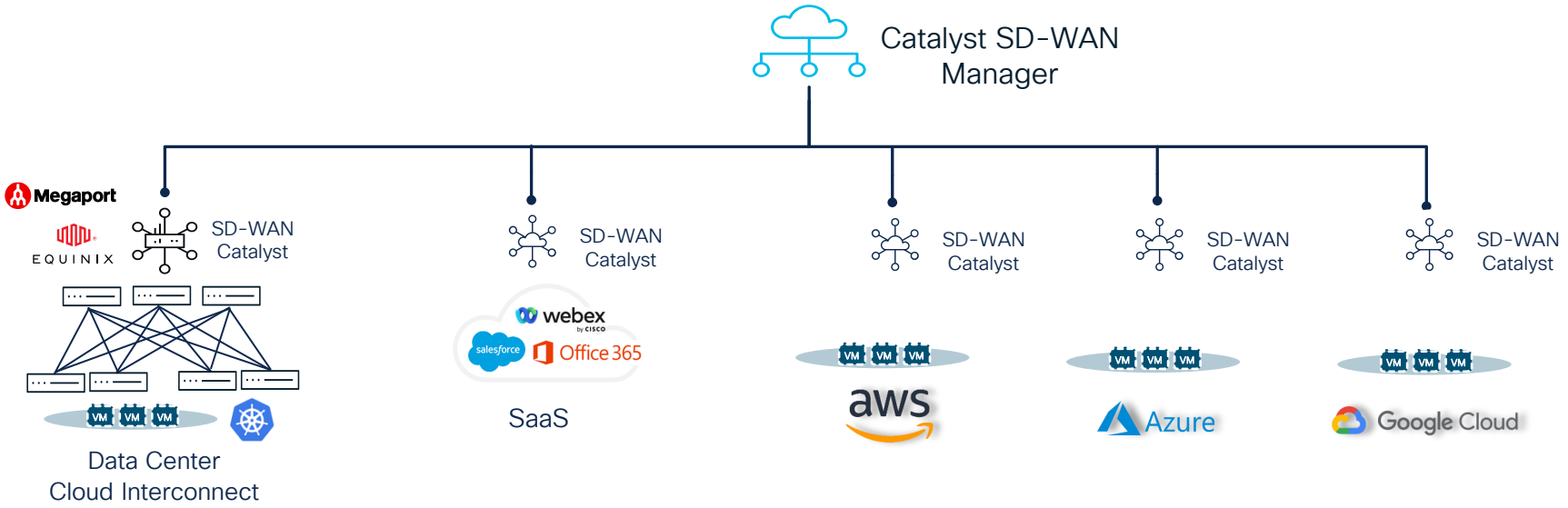
Multi-Cloud Networking: Catalyst SD-WAN Manager



cisco Live!

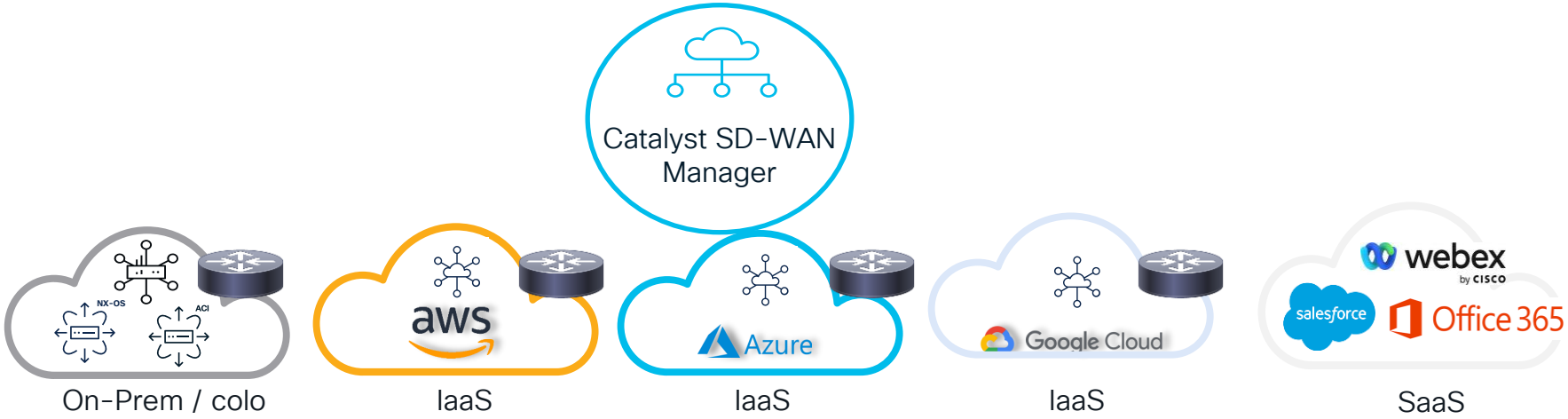
Multi-Cloud Networking

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

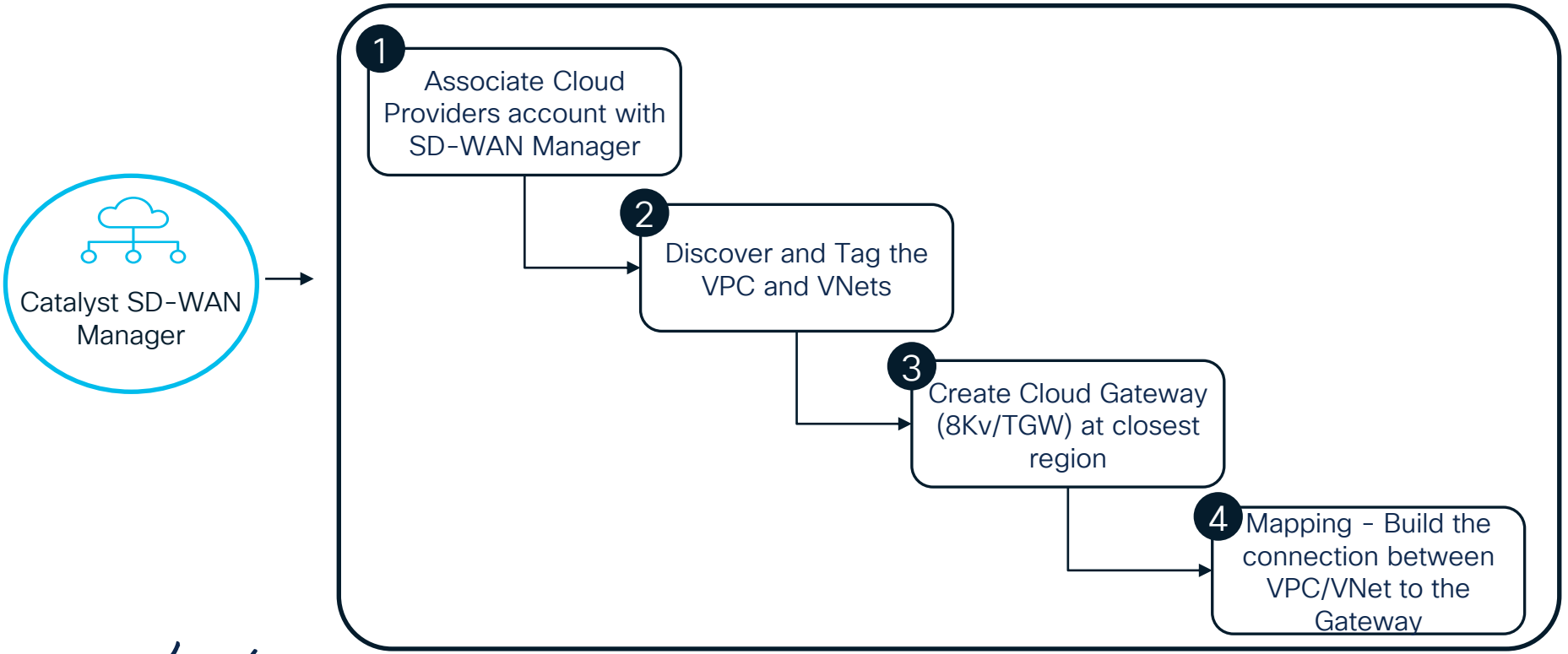
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
Ie. Firewall

Multi-Cloud Workflow

Secure Connectivity achieved in minutes

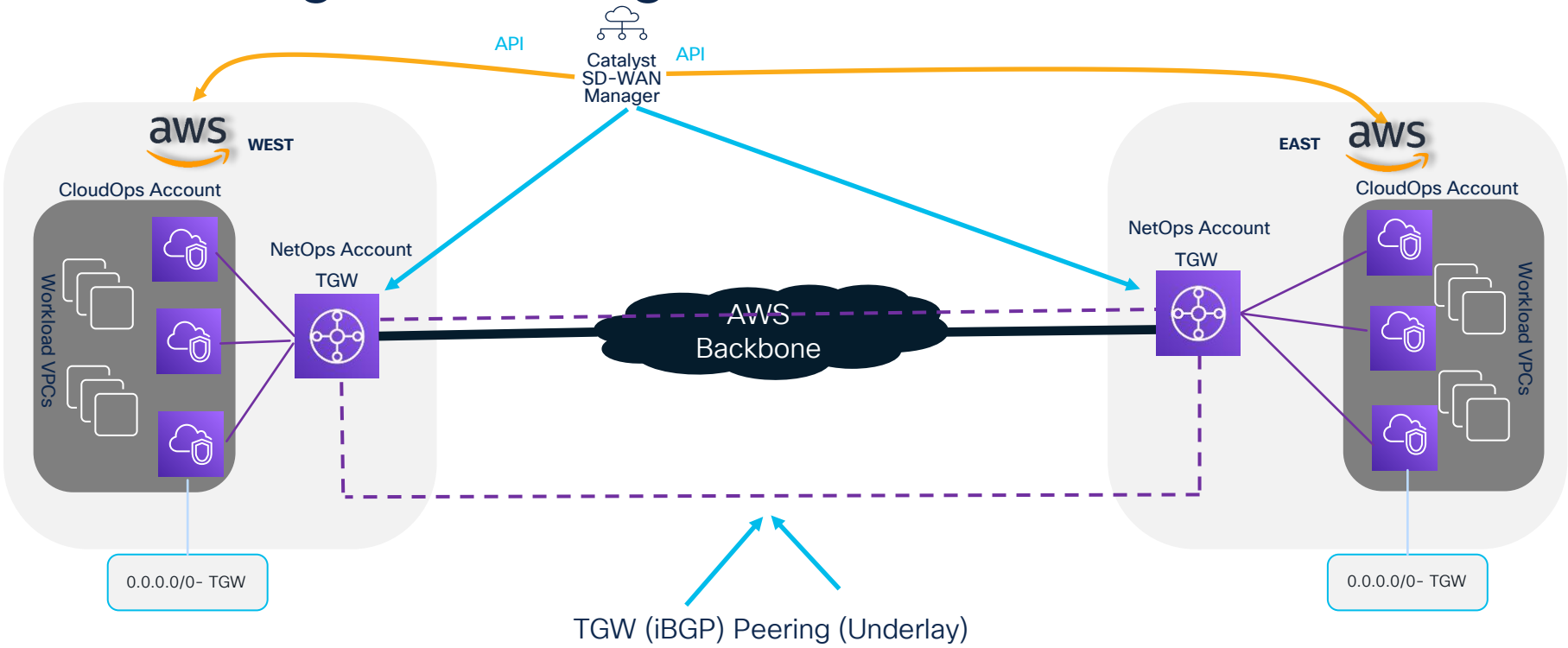


Integration and connectivity to AWS

With TGW

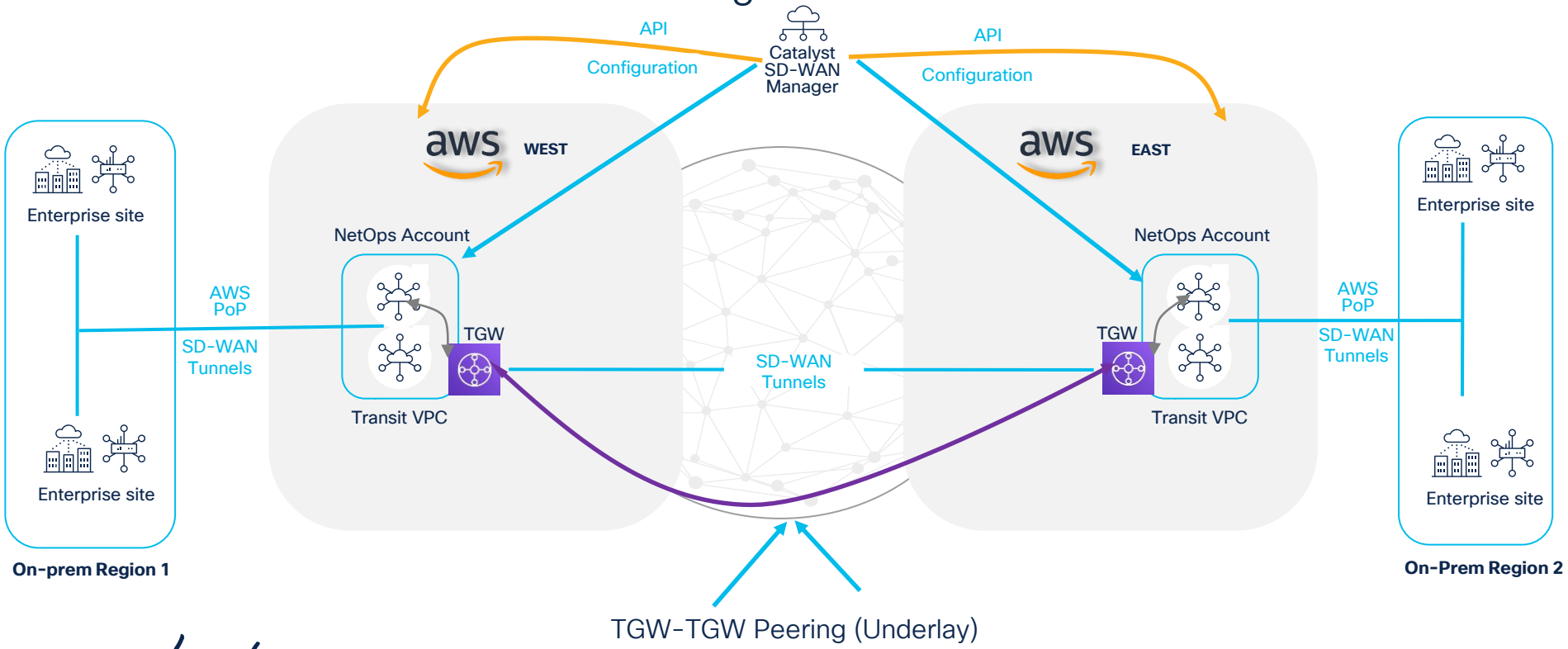
cisco Live!

AWS: Region-to-Region



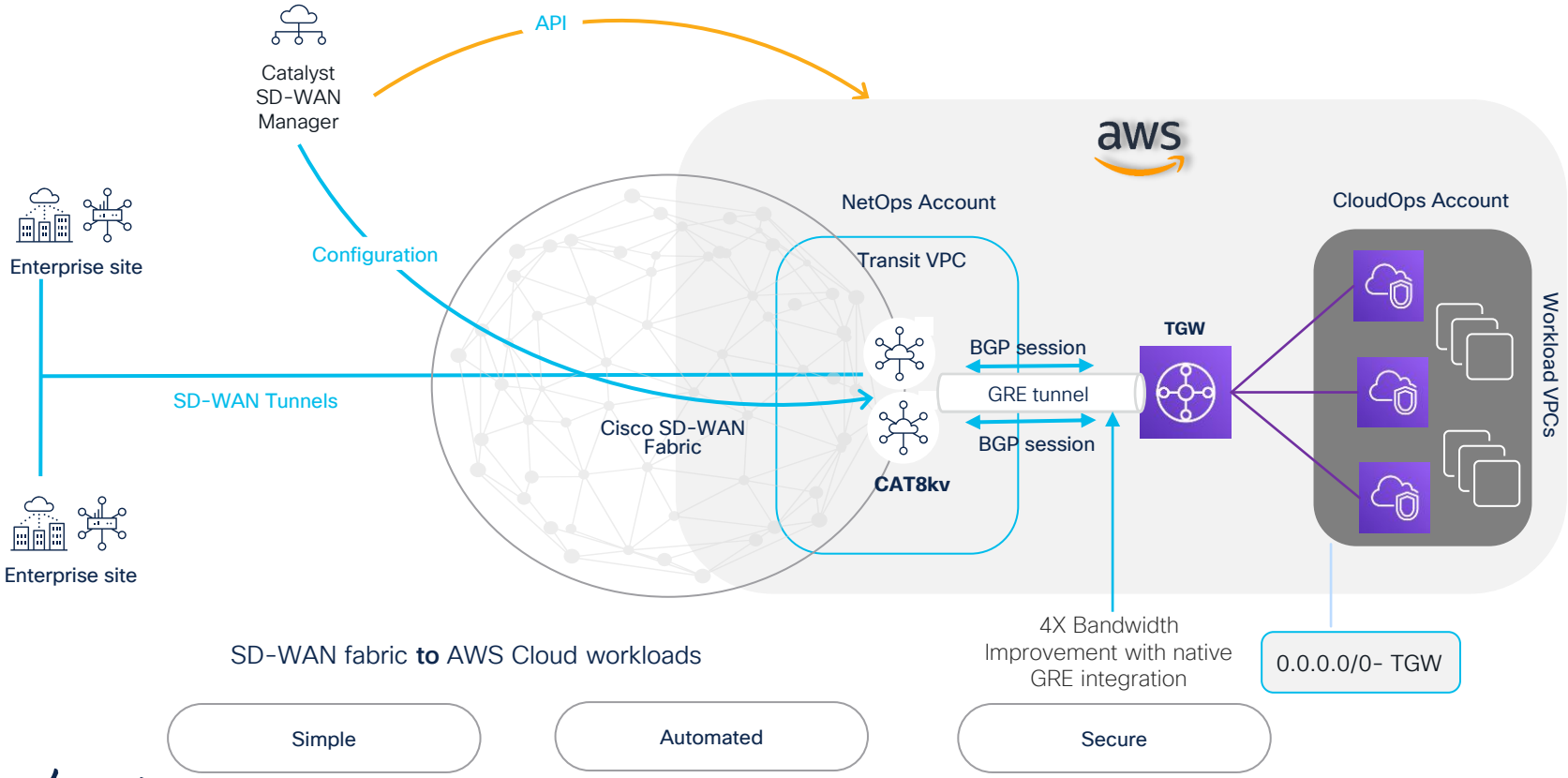
AWS: Site-to-Site

SD-WAN fabric across AWS Cloud global network



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

AWS: Site-to-Cloud



SD-WAN fabric **to** AWS Cloud workloads

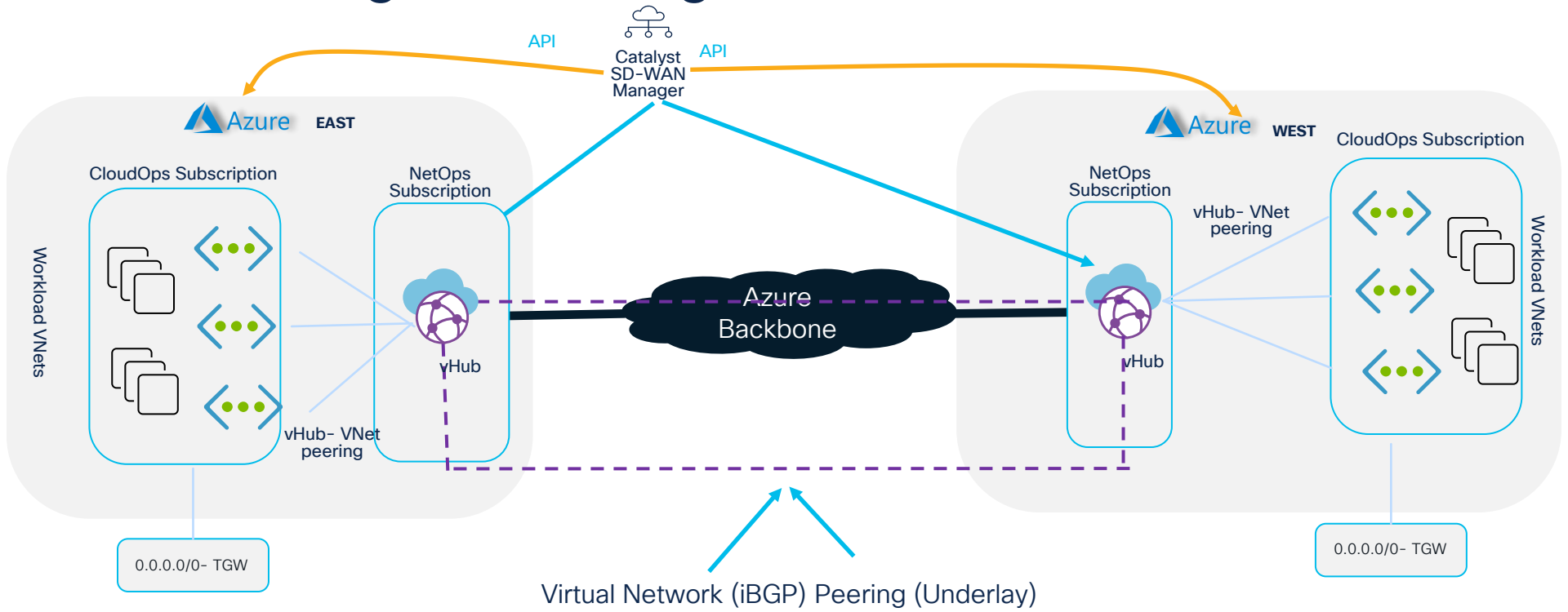
Simple | Automated | Secure

Integration and connectivity to Azure

With vWAN/vHub

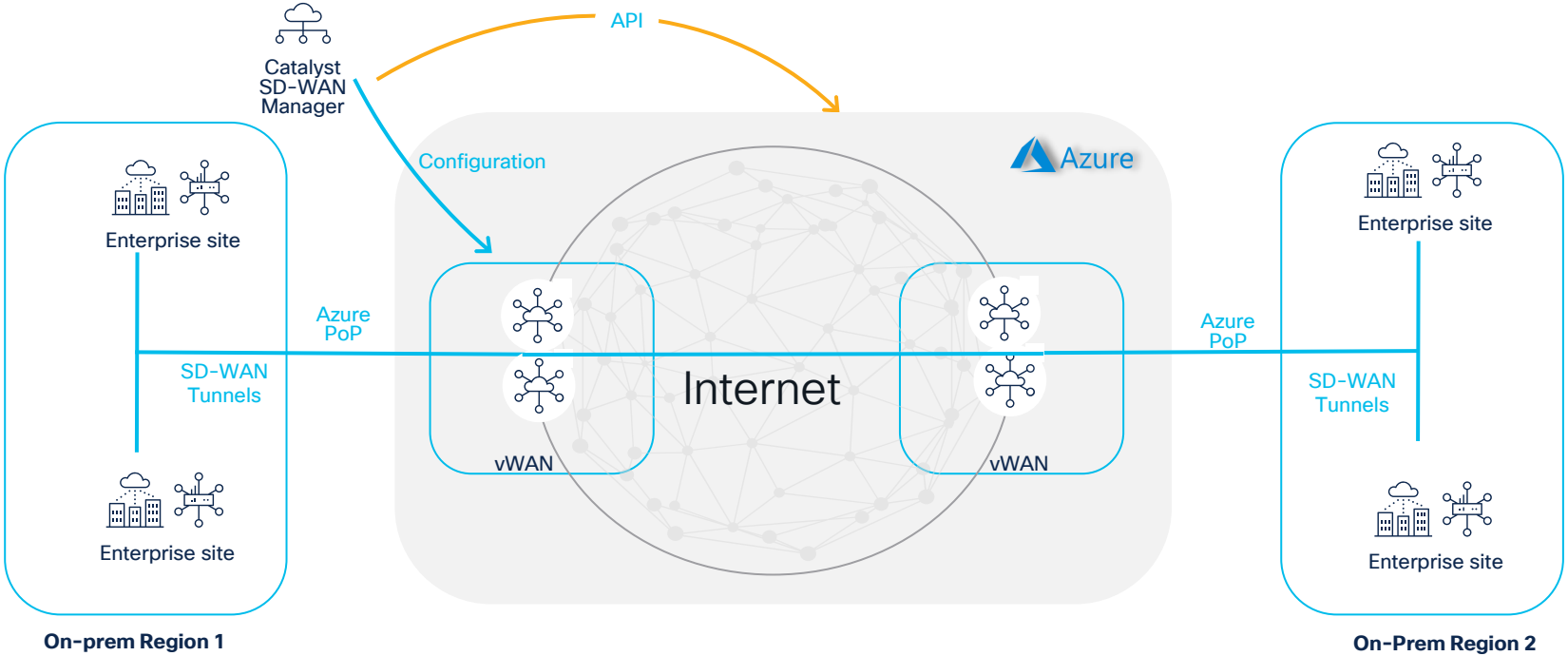
cisco Live!

Azure: Region-to-Region

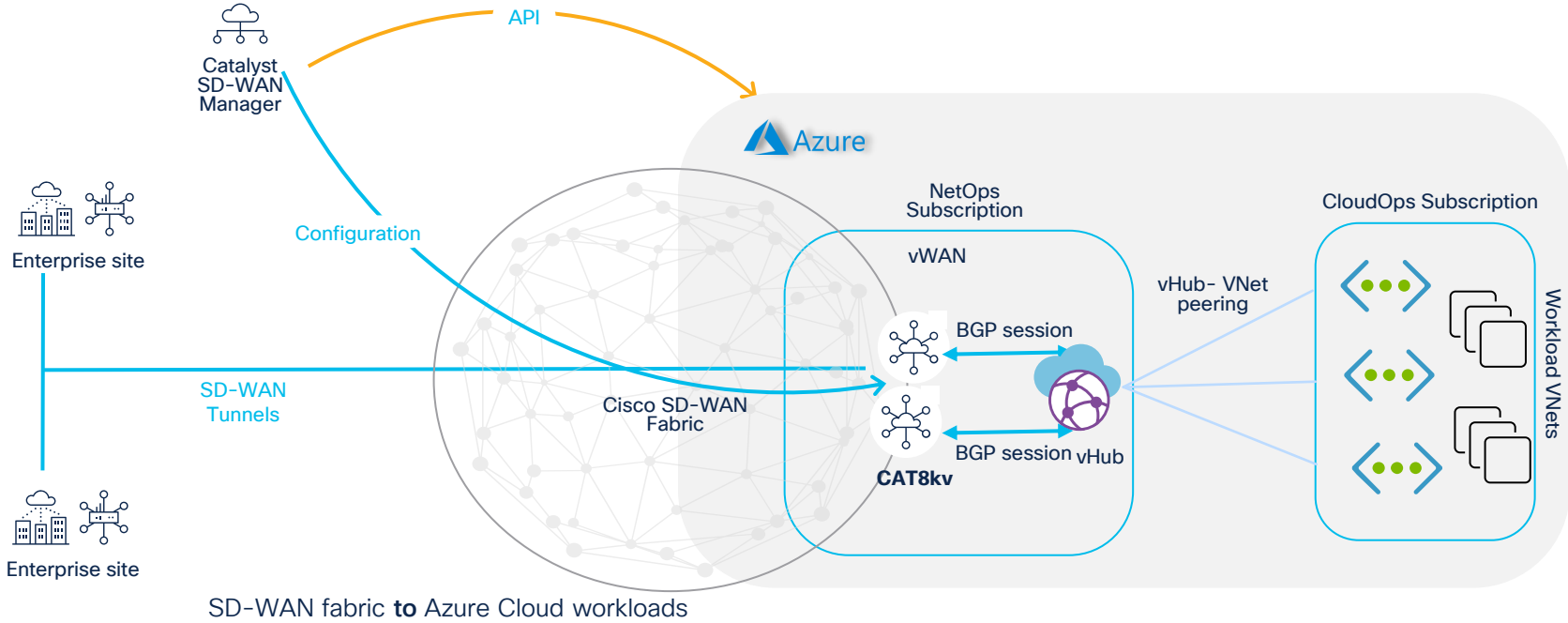


Azure: Site-to-Site

SD-WAN fabric across Azure global network



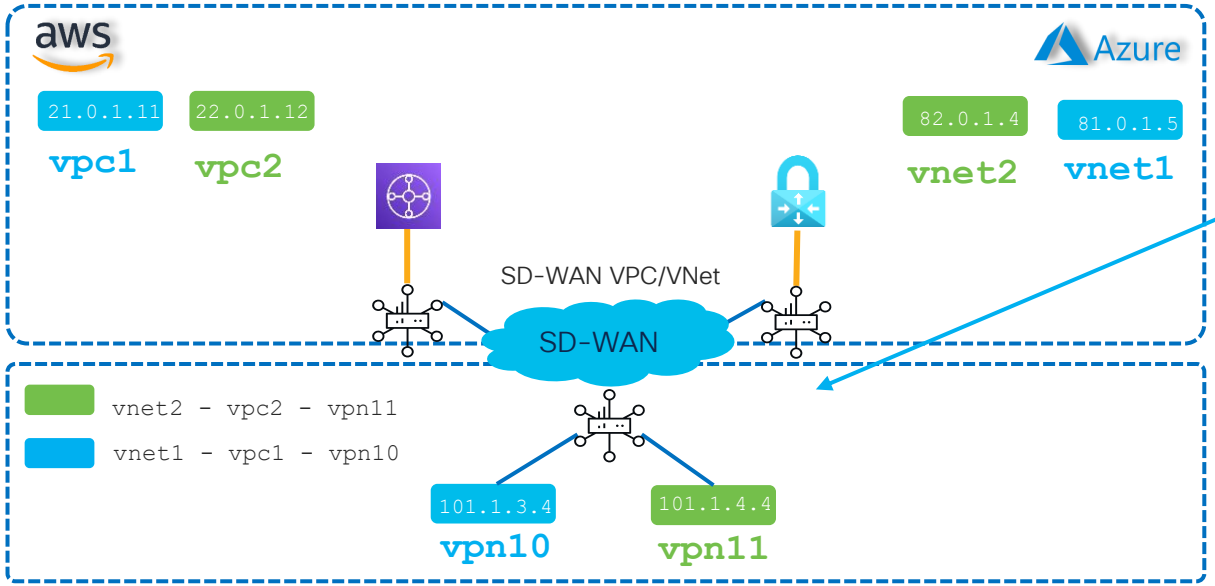
Azure: Site-to-Cloud



SD-WAN fabric **to** Azure Cloud workloads

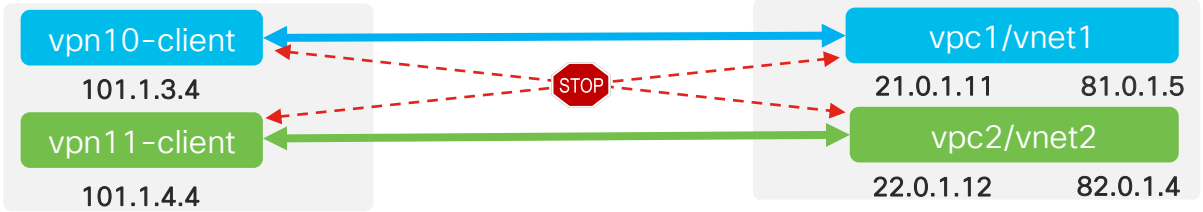
Simple | Automated | Secure

Segmentation with SD-WAN

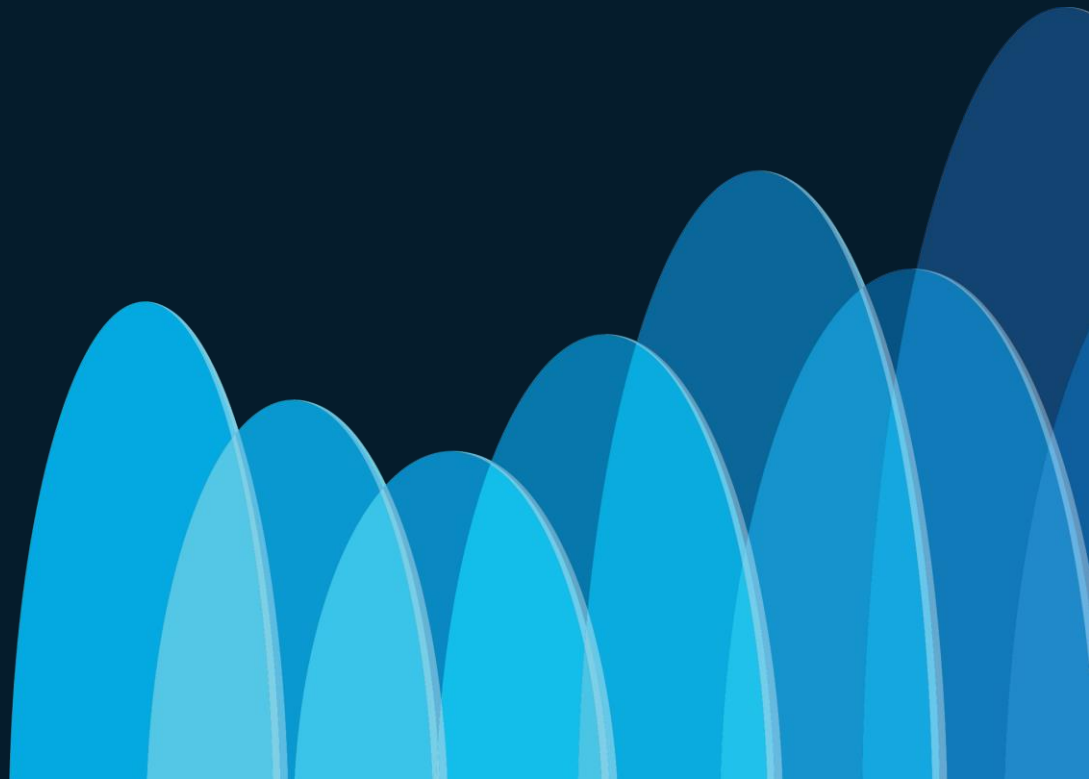


1) SDWAN connectivity terminates at the Cat8ks for the different VRFs

2) VRF(s) are extended to the TGW/ Cloud WAN extended to the native VPCs

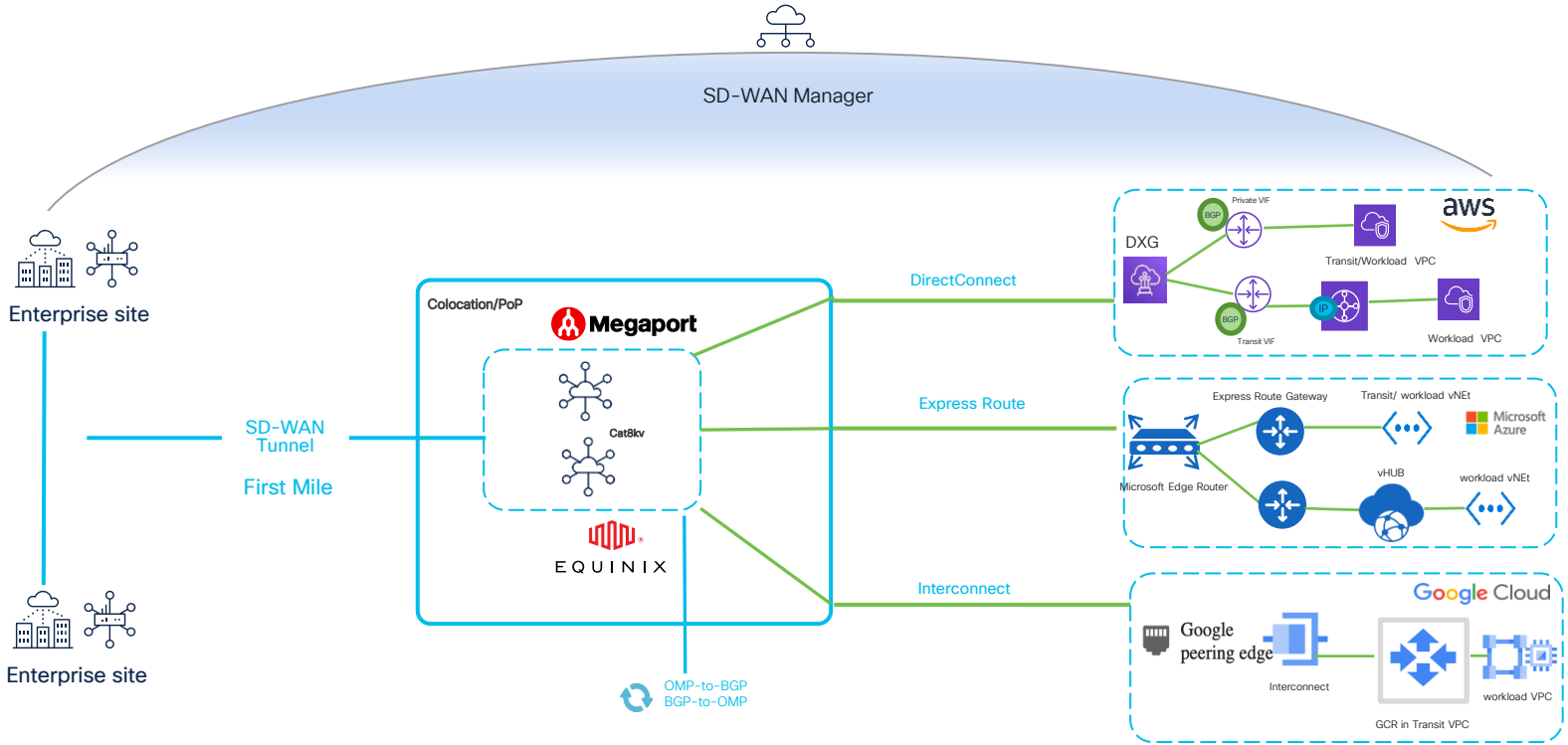


Middle Mile w/ Megaport & Equinix



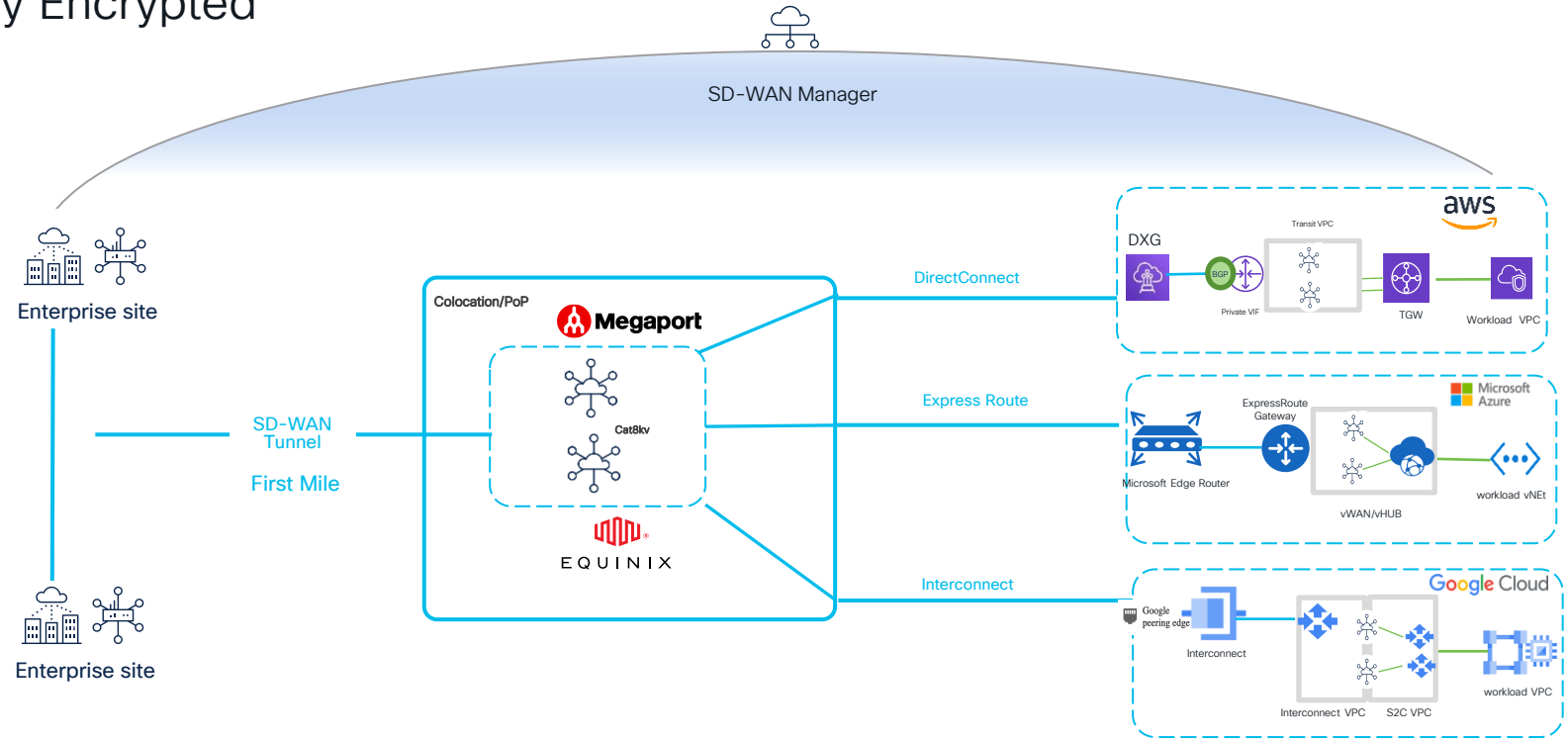
cisco Live!

Site-to-Multicloud- Megaport or Equinix

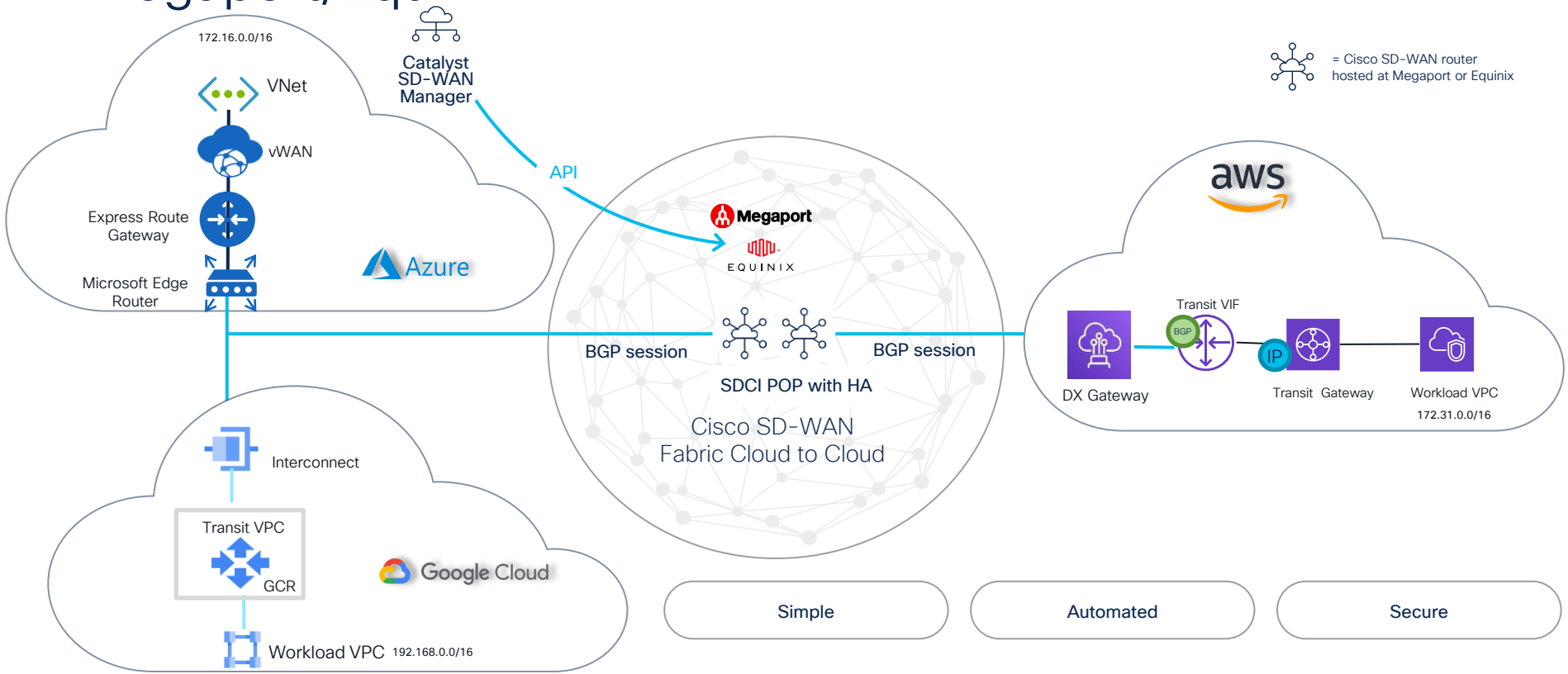


Site-to-Multicloud- Megaport or Equinix

Fully Encrypted

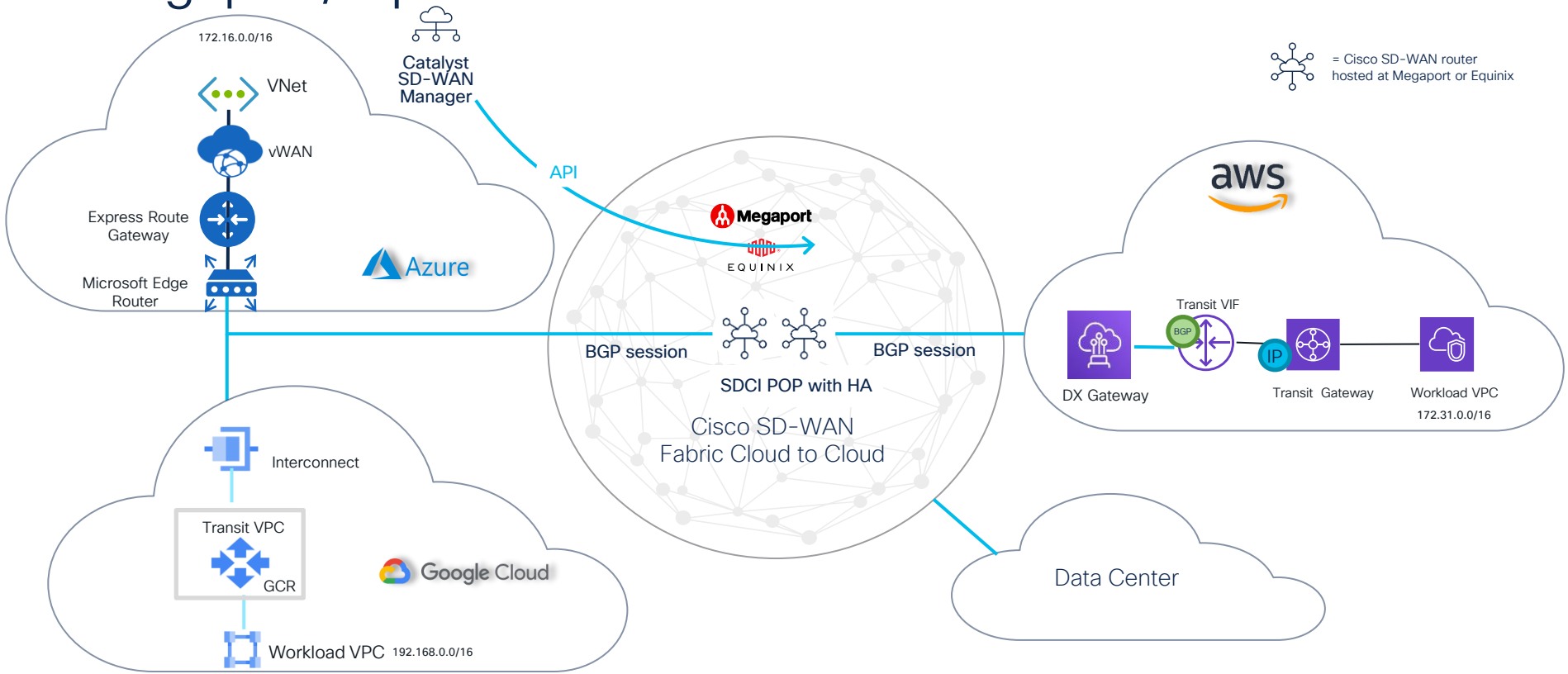


Cloud to Cloud: Private Connect
Megaport/Equinix



Automated with Cisco Catalyst SD-WAN Manager

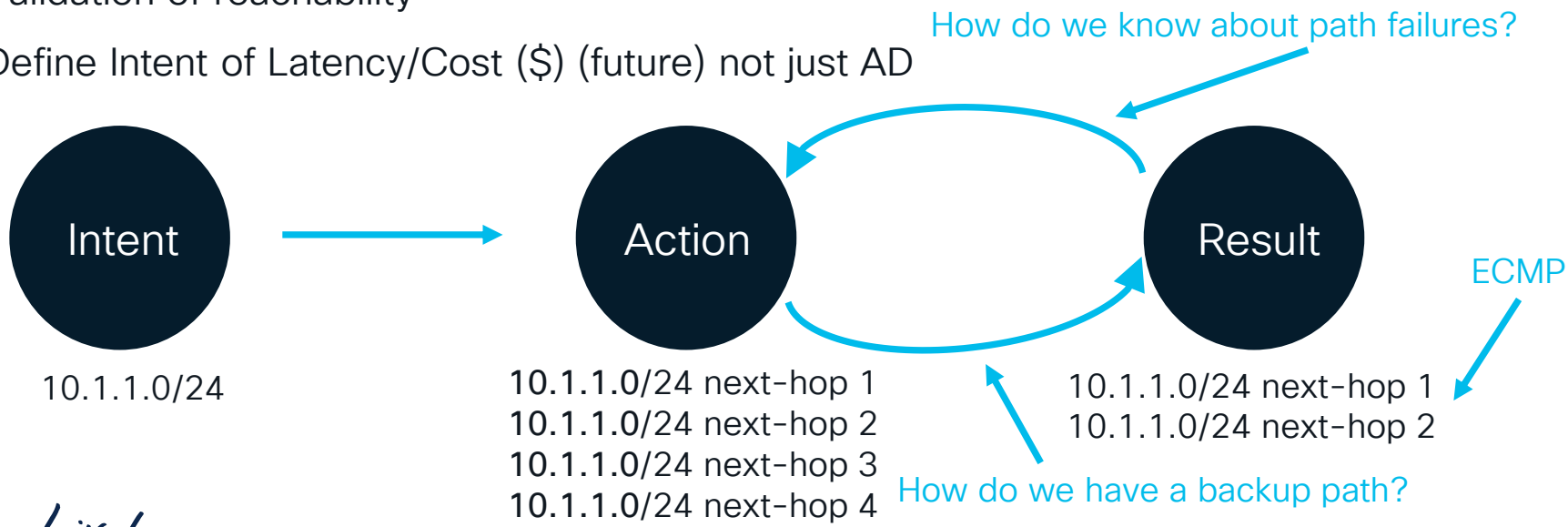
Cloud to Cloud: Private Connect
Megaport/Equinix



Automated with Cisco Catalyst SD-WAN Manager

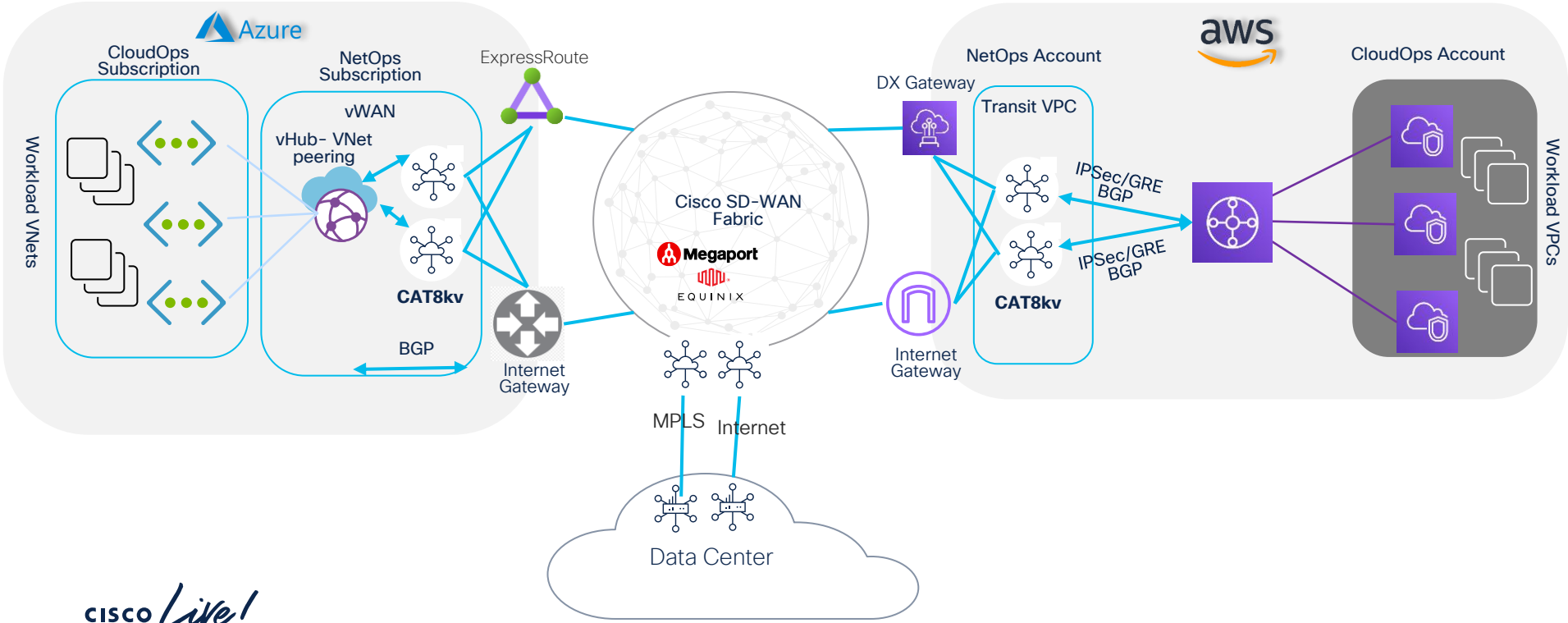
Cloud Networking with SD-WAN Manager

- 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



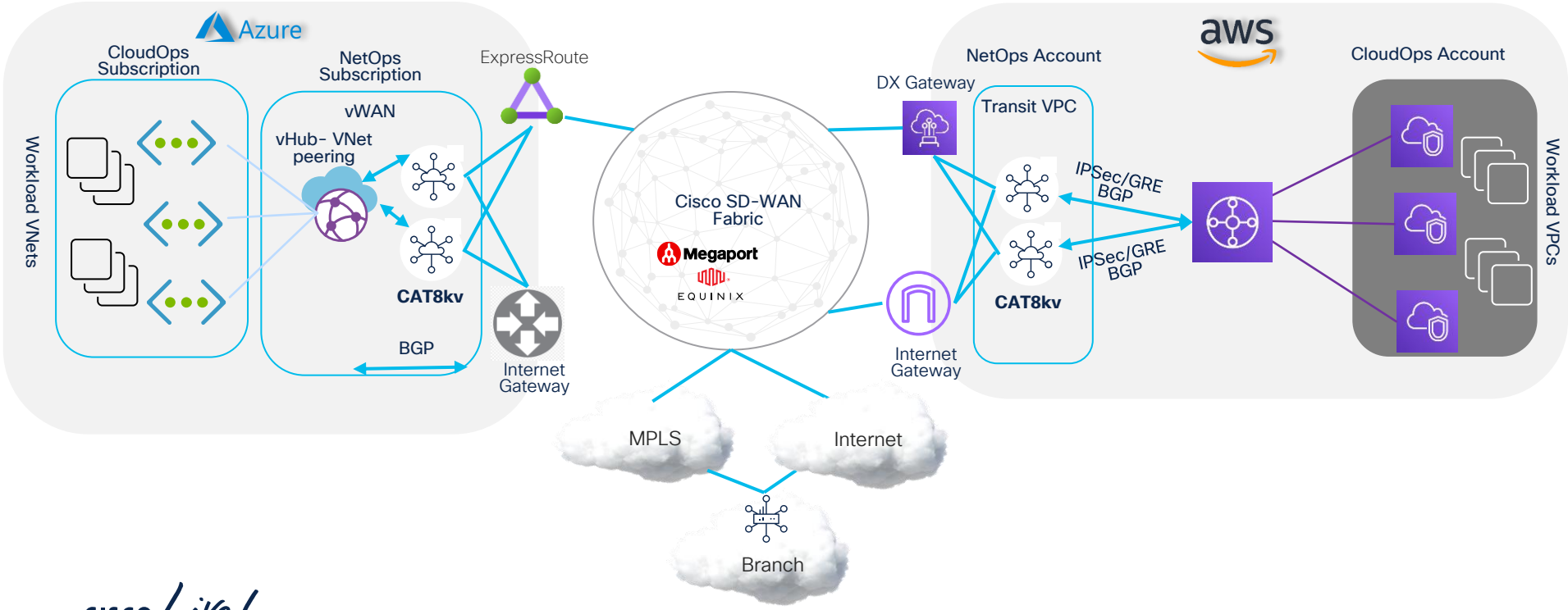
Cloud-to-Cloud

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.

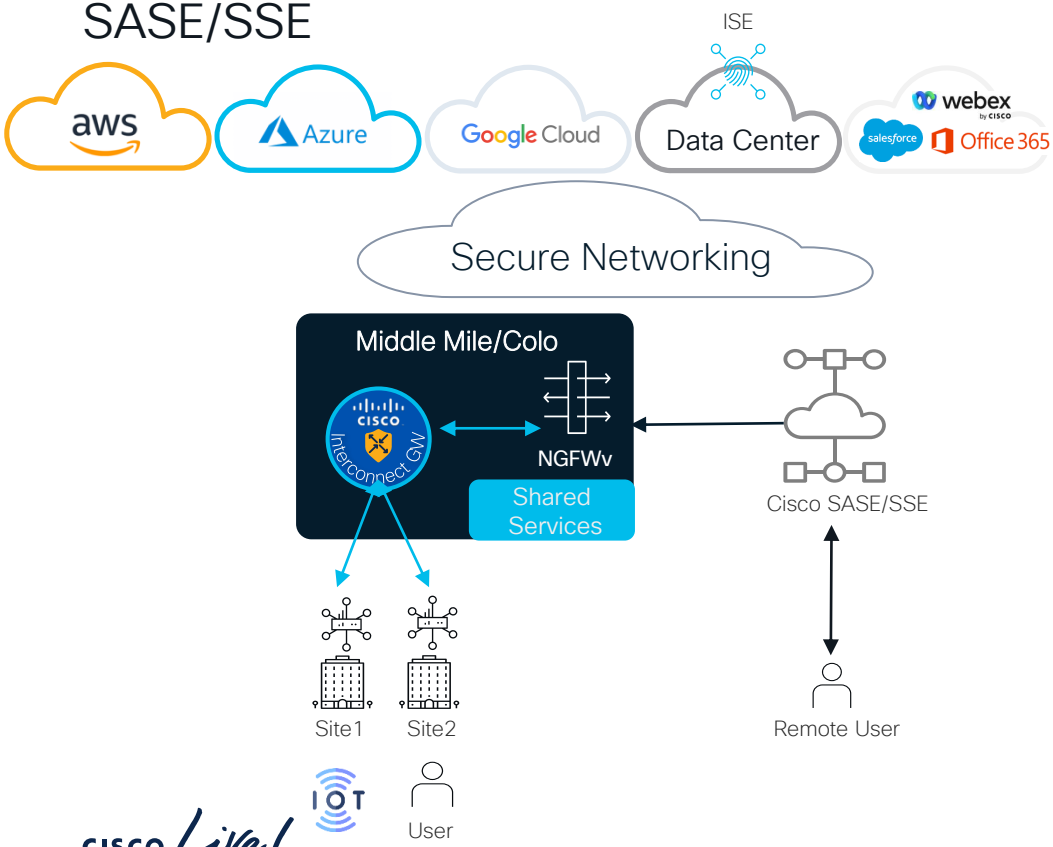
Applications behind SDWAN and Cloud Security Stack

cisco Live!

Use-Cases

Use Case: Site/User-to-Cloud

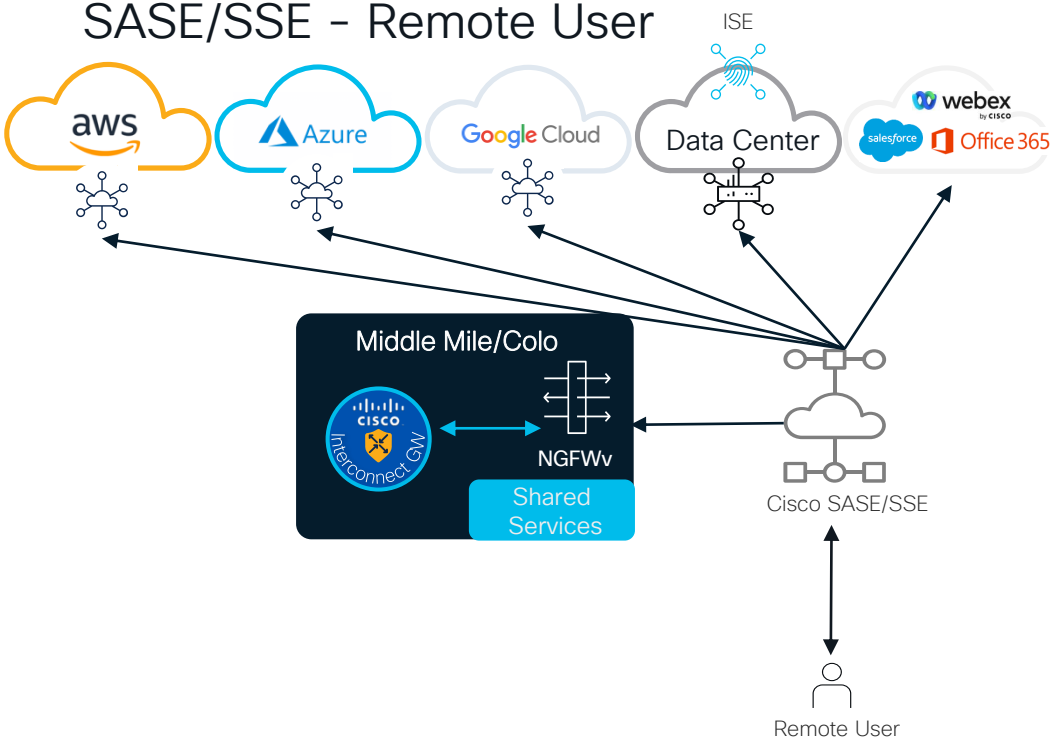
SASE/SSE



- 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 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

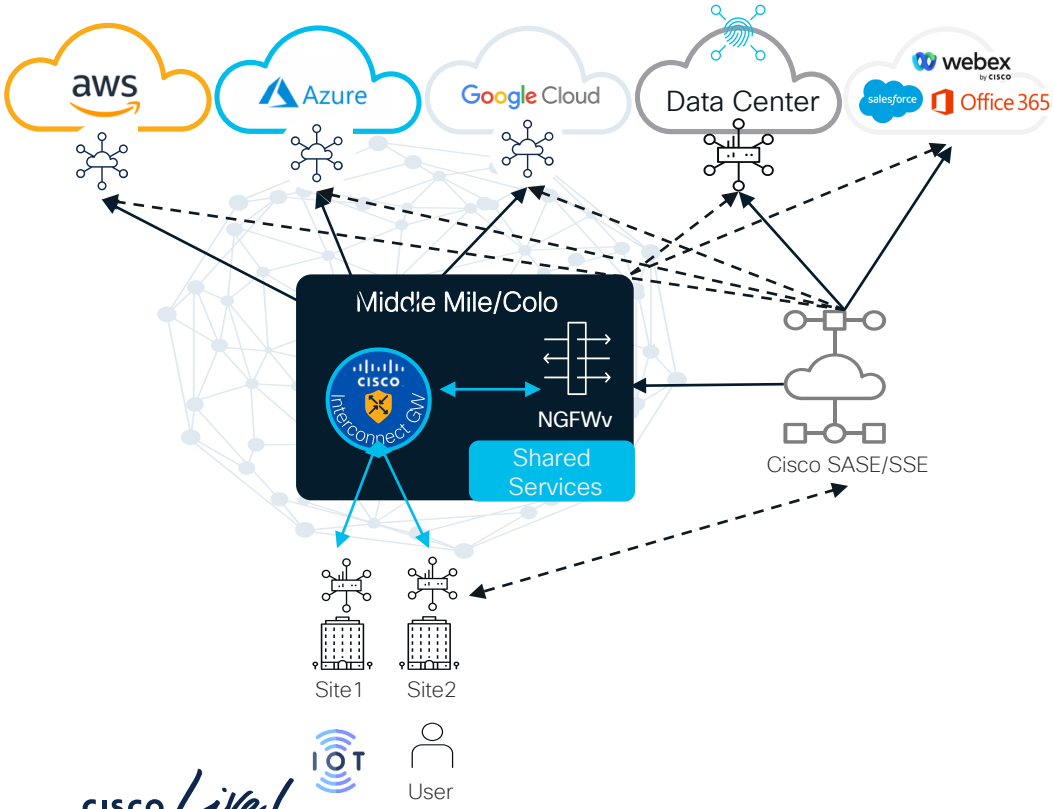
SASE/SSE - Remote User



- **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

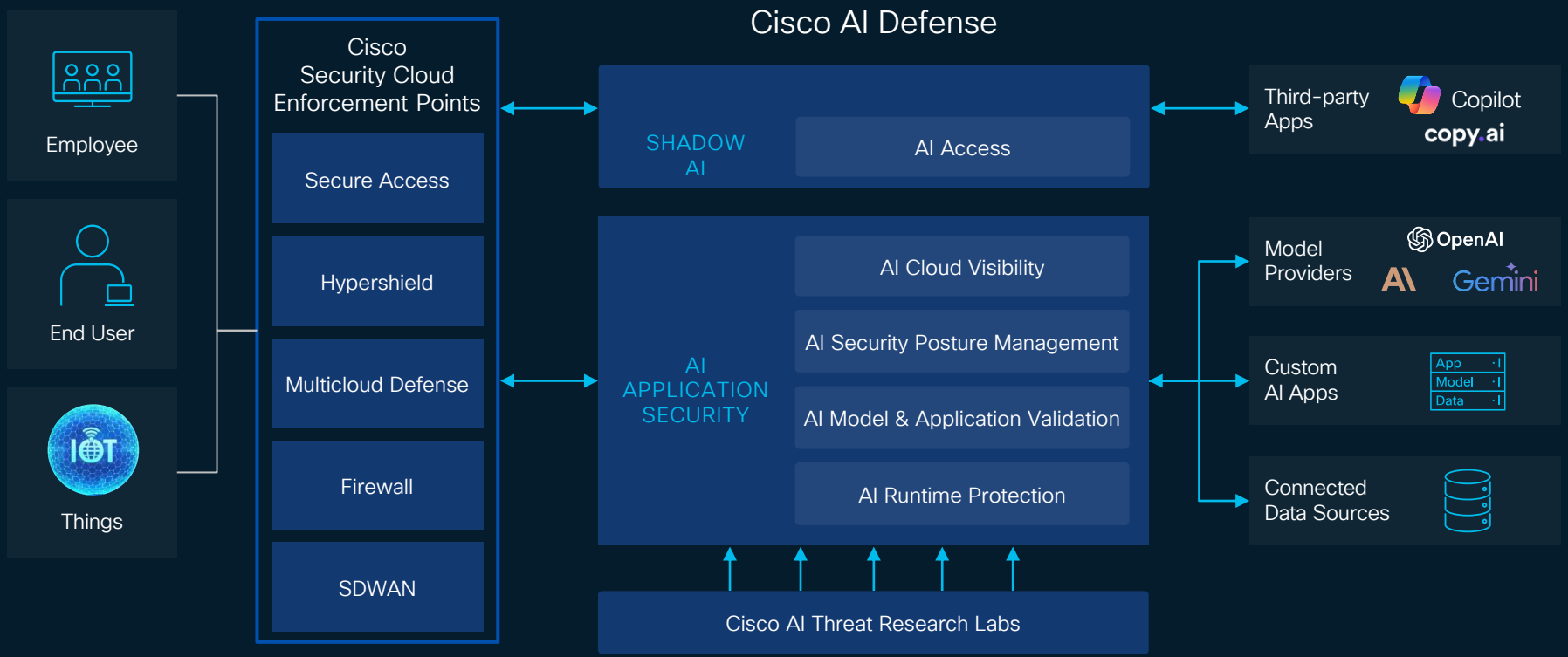
Use Case: Site/User-to-Cloud

SASE/SSE - Branch User/IoT ISE

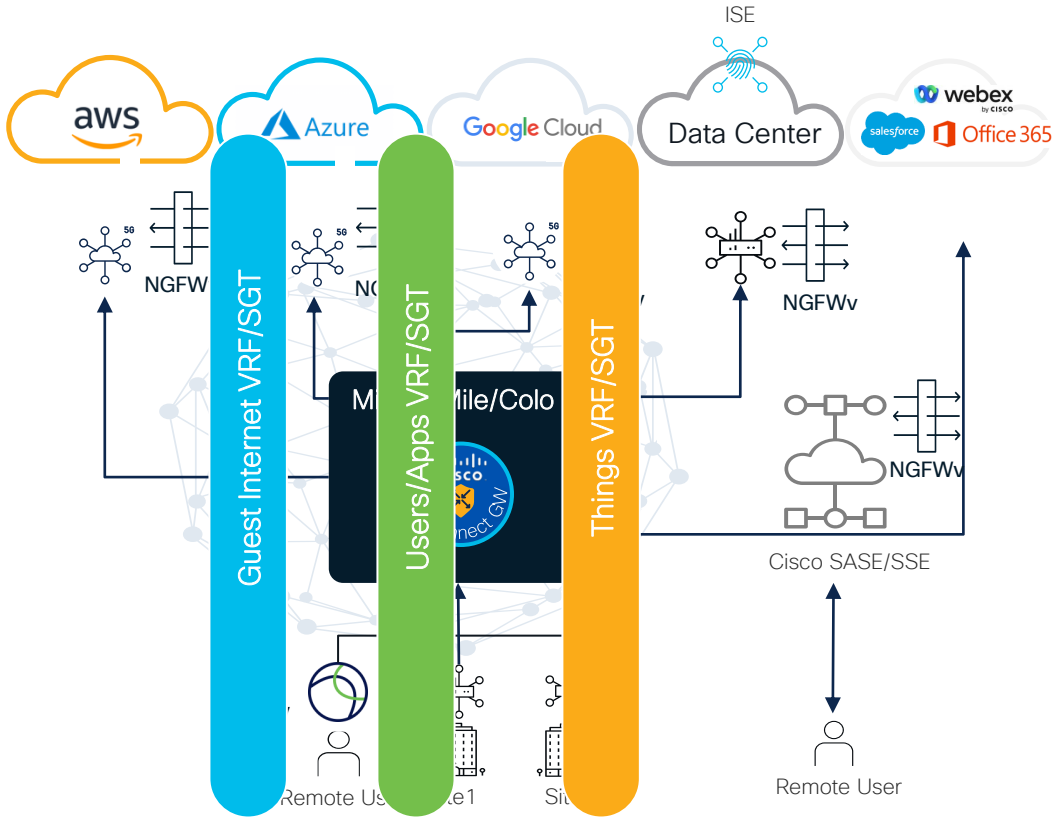


- **Branch User/IoT to Internet/SaaS**
  - Catalyst/Meraki SD-WAN Optimized Routing
  - SSE Security Controls, Inspection and least-priv access
  - SD-WAN Security Capabilities
- **Branch User/IoT to Private App**
  - Catalyst/Meraki SD-WAN Optimized Routing (ie. DC via Middle-mile)
  - SSE Security 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)

Security Cloud Control



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

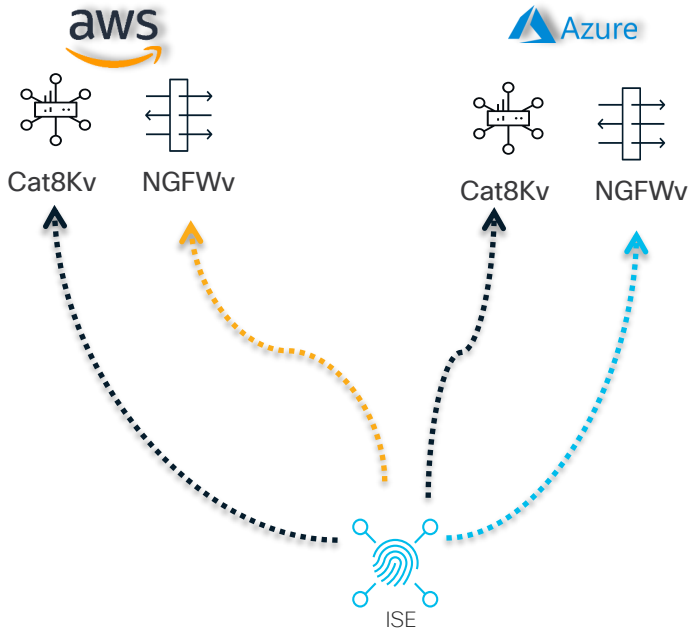
Resulting in:

- 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

Extending Policy to Public IaaS

cisco Live!

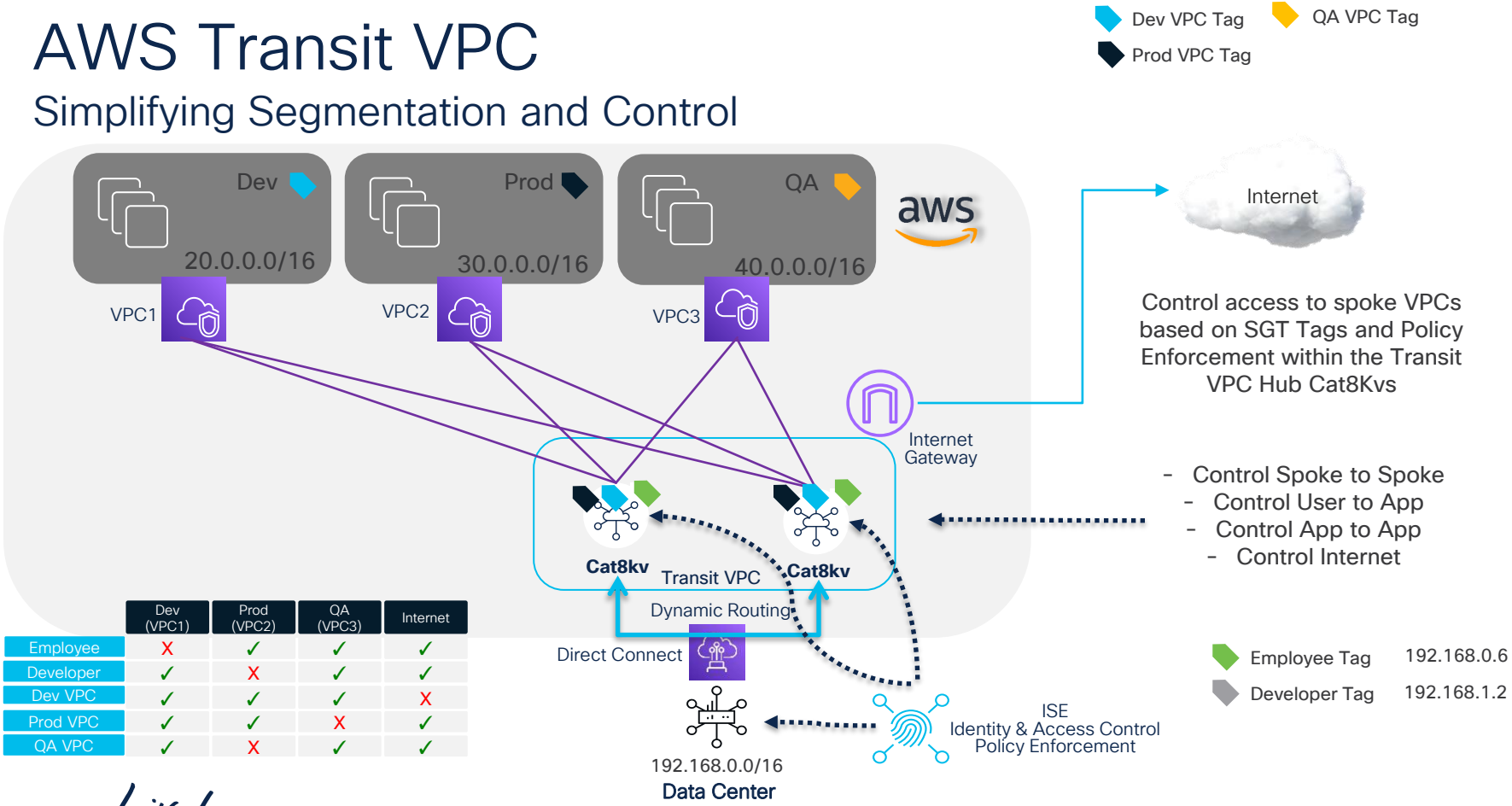
Enabling Group-based Policies



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

AWS Transit VPC

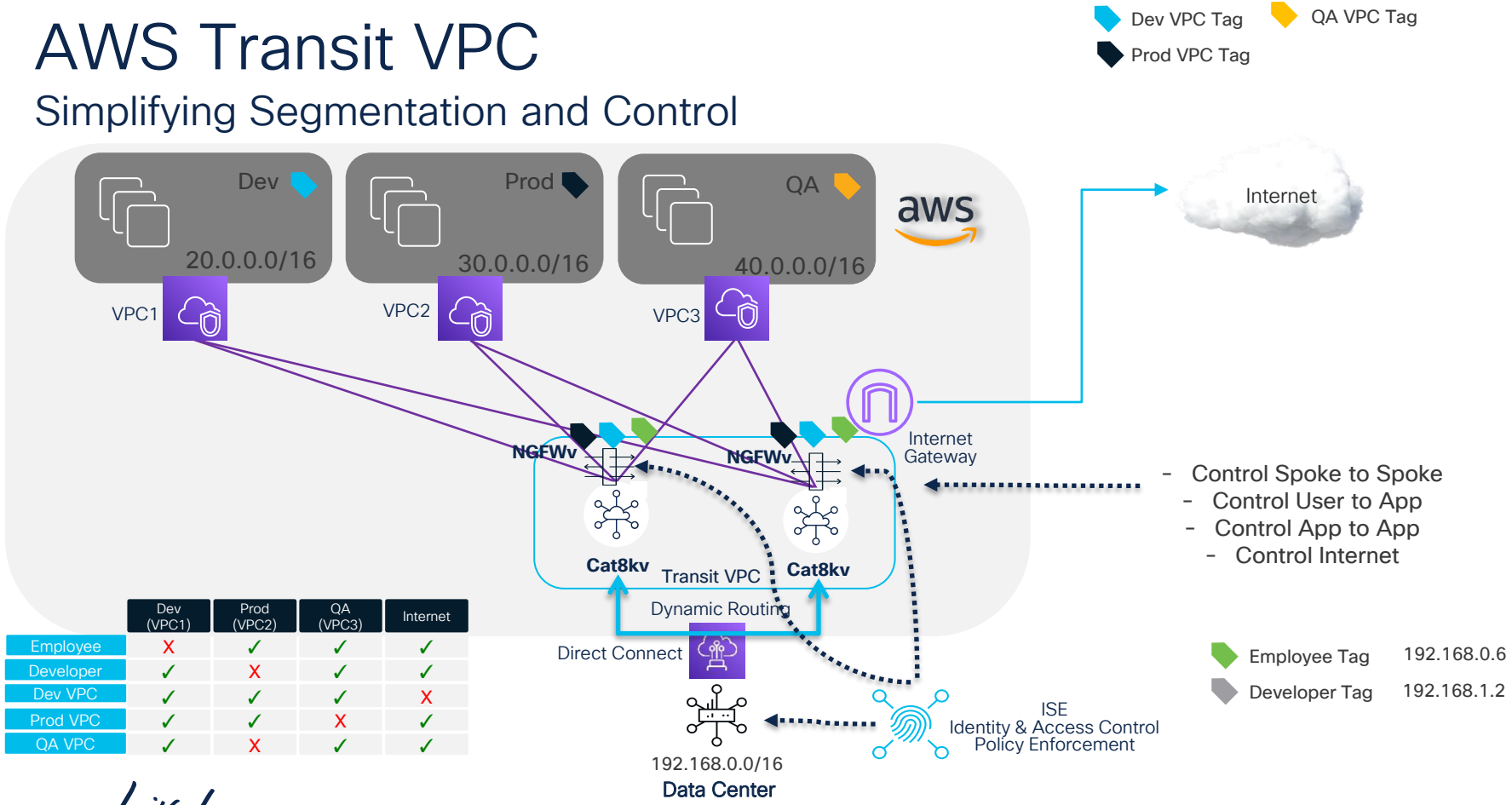
Simplifying Segmentation and Control



	Dev (VPC1)	Prod (VPC2)	QA (VPC3)	Internet
Employee	X	✓	✓	✓
Developer	✓	X	✓	✓
Dev VPC	✓	✓	✓	X
Prod VPC	✓	✓	X	✓
QA VPC	✓	X	✓	✓

AWS Transit VPC

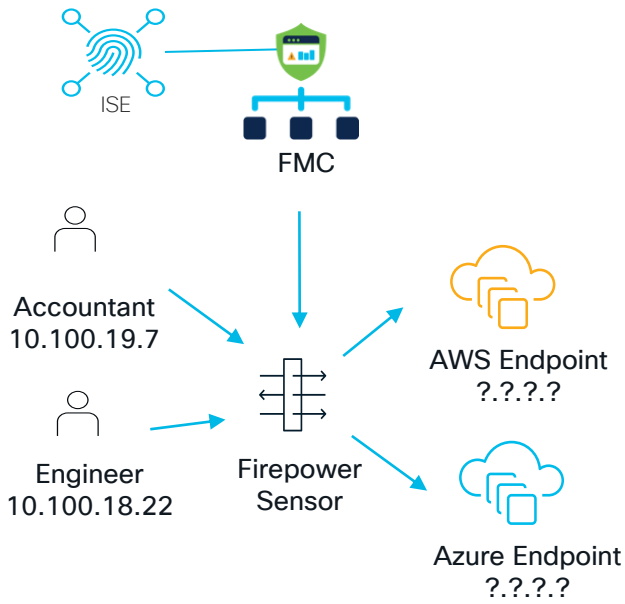
Simplifying Segmentation and Control



	Dev (VPC1)	Prod (VPC2)	QA (VPC3)	Internet
Employee	X	✓	✓	✓
Developer	✓	X	✓	✓
Dev VPC	✓	✓	✓	X
Prod VPC	✓	✓	X	✓
QA VPC	✓	X	✓	✓

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

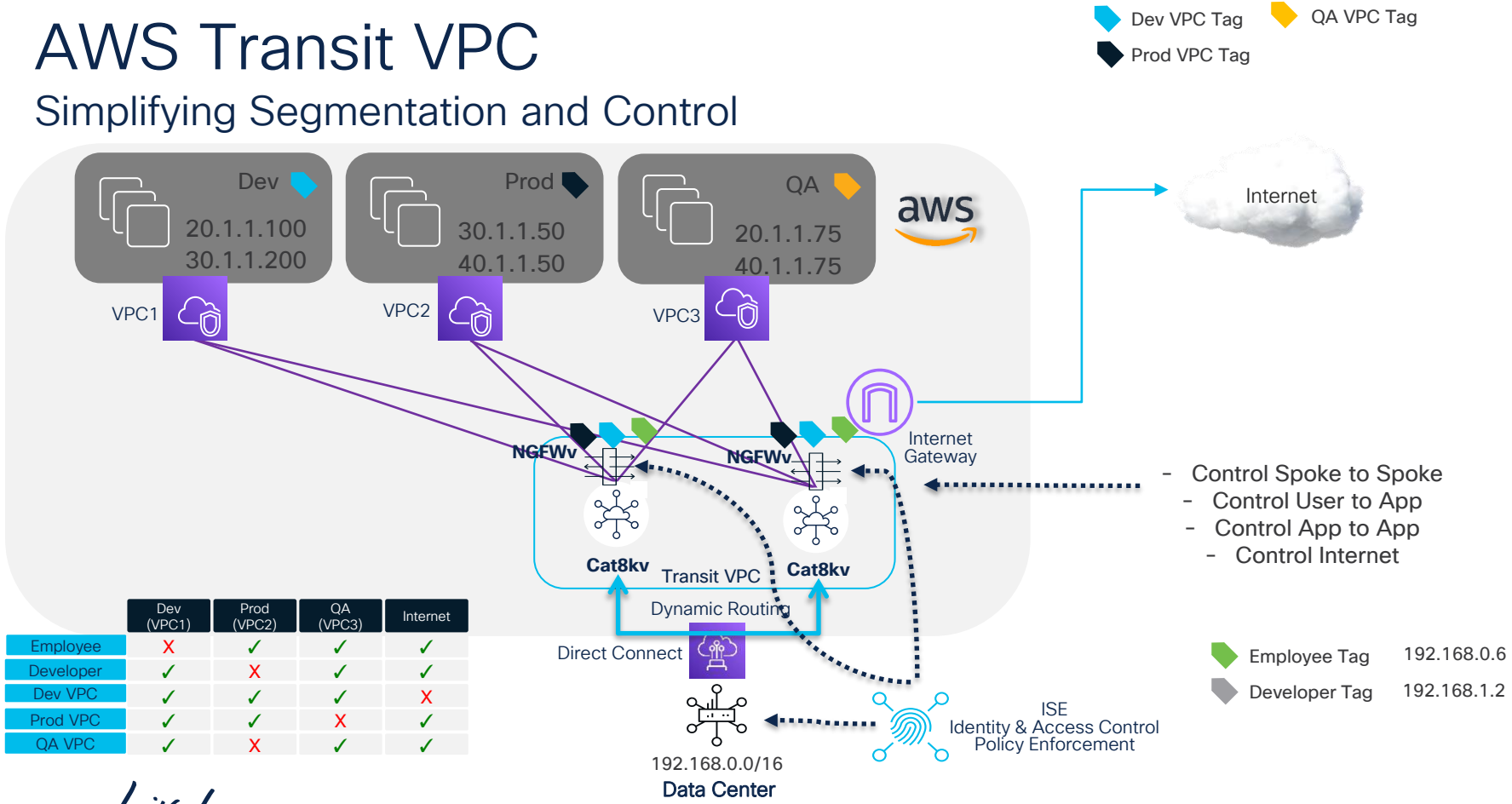
aws Azure Google Cloud vmware

Public Connectors

Office 365 webex by cisco zoom

AWS Transit VPC

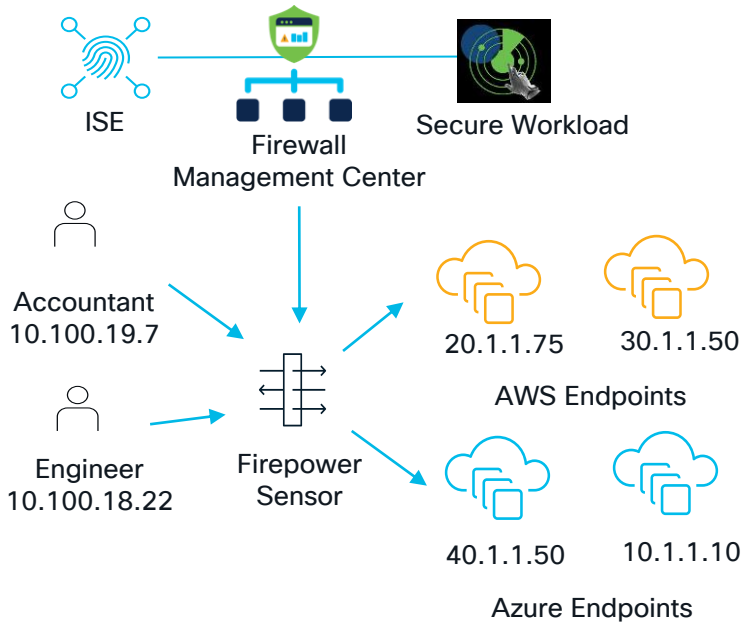
Simplifying Segmentation and Control



	Dev (VPC1)	Prod (VPC2)	QA (VPC3)	Internet
Employee	X	✓	✓	✓
Developer	✓	X	✓	✓
Dev VPC	✓	✓	✓	X
Prod VPC	✓	✓	X	✓
QA VPC	✓	X	✓	✓

Cisco Secure Workload

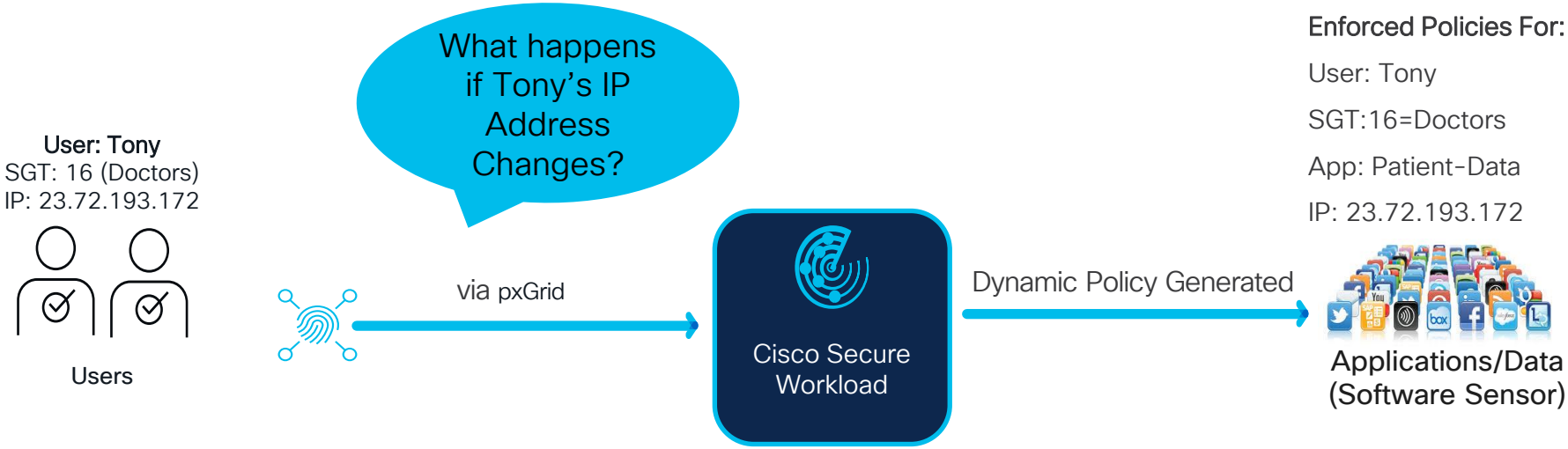
- Segmentation policies enforcement at workloads
- Virtual Machines, Containers and Bare Metal
- Private and Public IaaS
- Prevent East / West lateral Movement
- Dynamic Policy
- Policy Enforcement
- Policy Visibility



Secure Workload with ISE

cisco Live!

ISE Provides Identity to Secure Workload



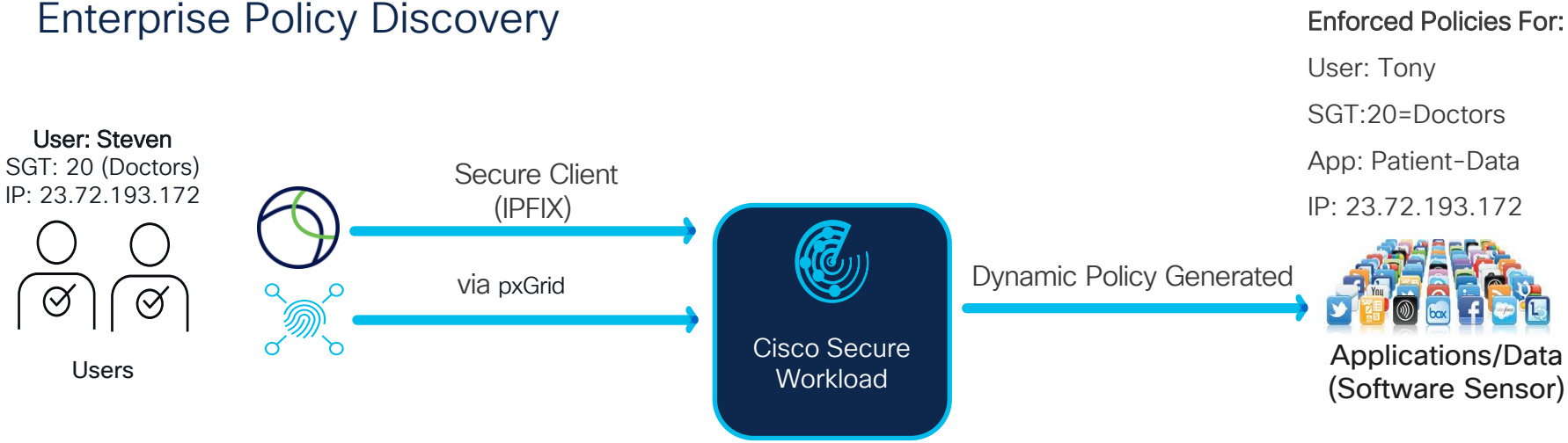
1) The sensor endpoint is sending Telemetry data
2) The endpoint also authenticates with ISE which notifies our identity repository via pxGrid.
3) Secure Workload merges the two streams and outputs dynamically generated policy.

May not access employee data

May access patient records

Secure Client (Any Connect)

Enterprise Policy Discovery

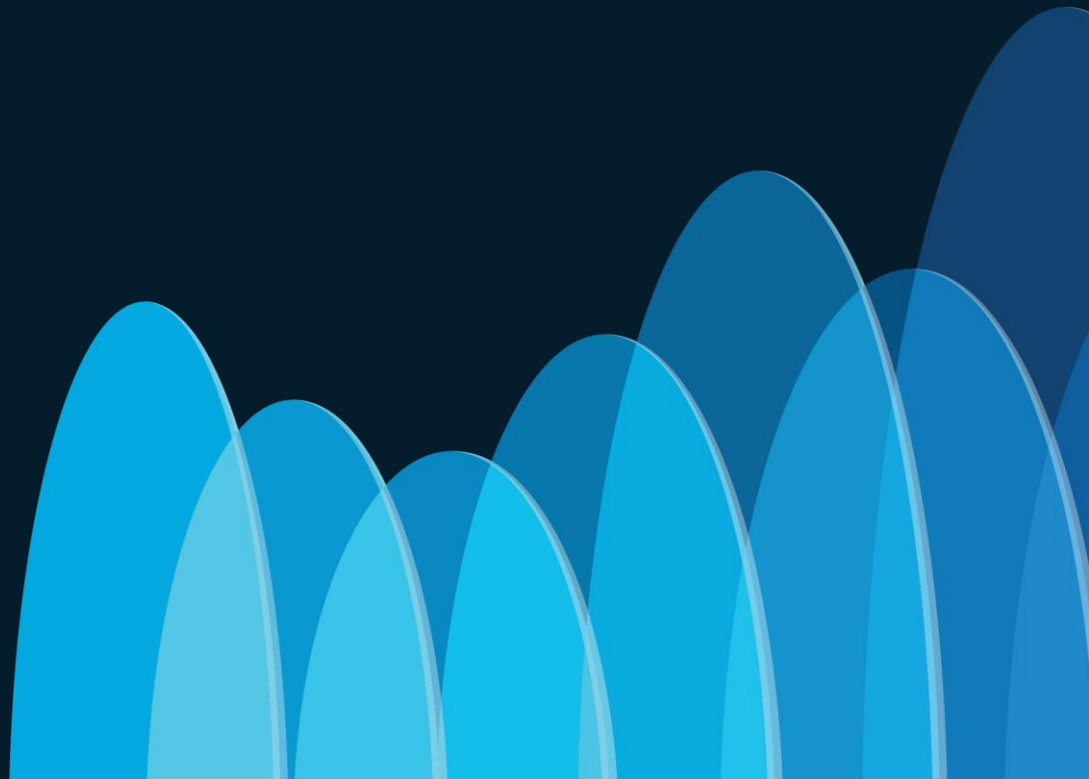


1) Secure Client Network Visibility Module (NVM) streams IPFIX to Secure Workload
2) The endpoint also authenticates with ISE which notifies our identity repository via pxGrid.
3) Secure Workload merges the two streams and outputs dynamically generated policy

May not access employee data

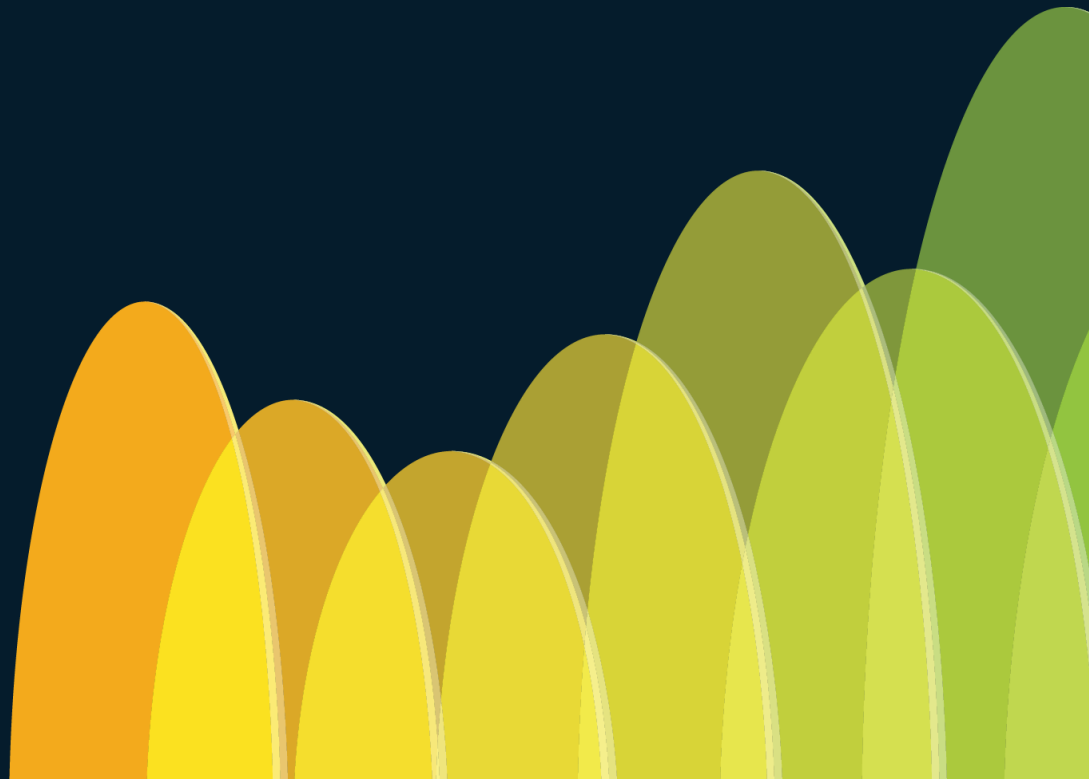
May access patient records

Security: In & Between the Clouds



cisco Live!

Multicloud Defense



cisco Live!

Personas

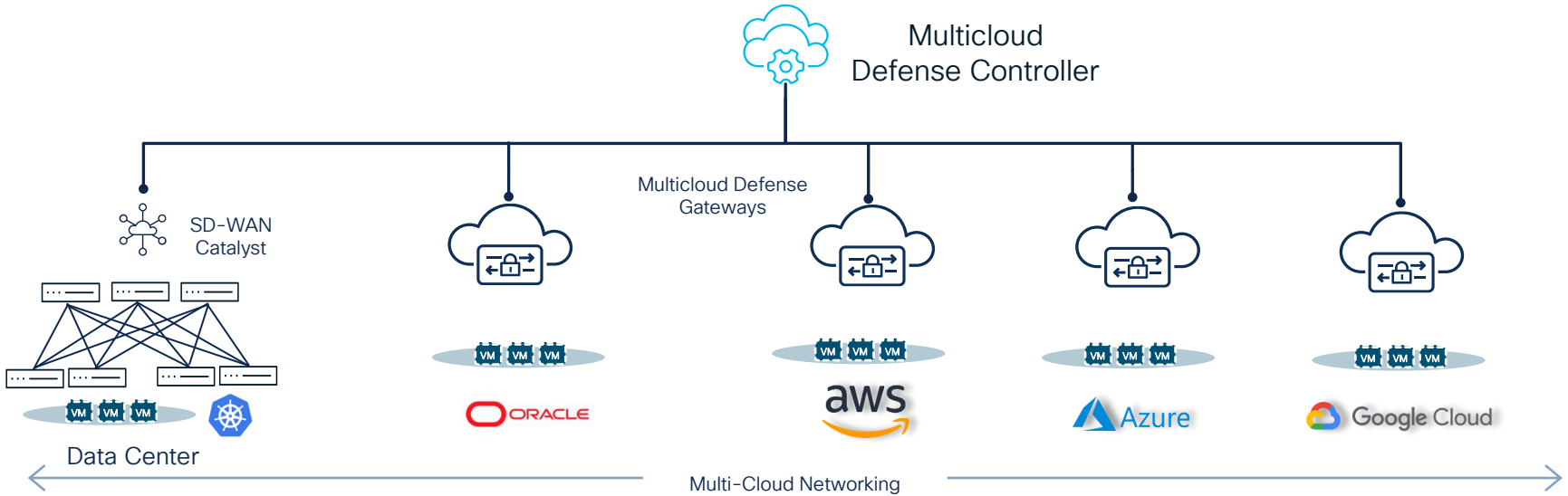
NetCloudOps
Account

CloudOps
Account

NetSecOps
Account
Ie. Firewall

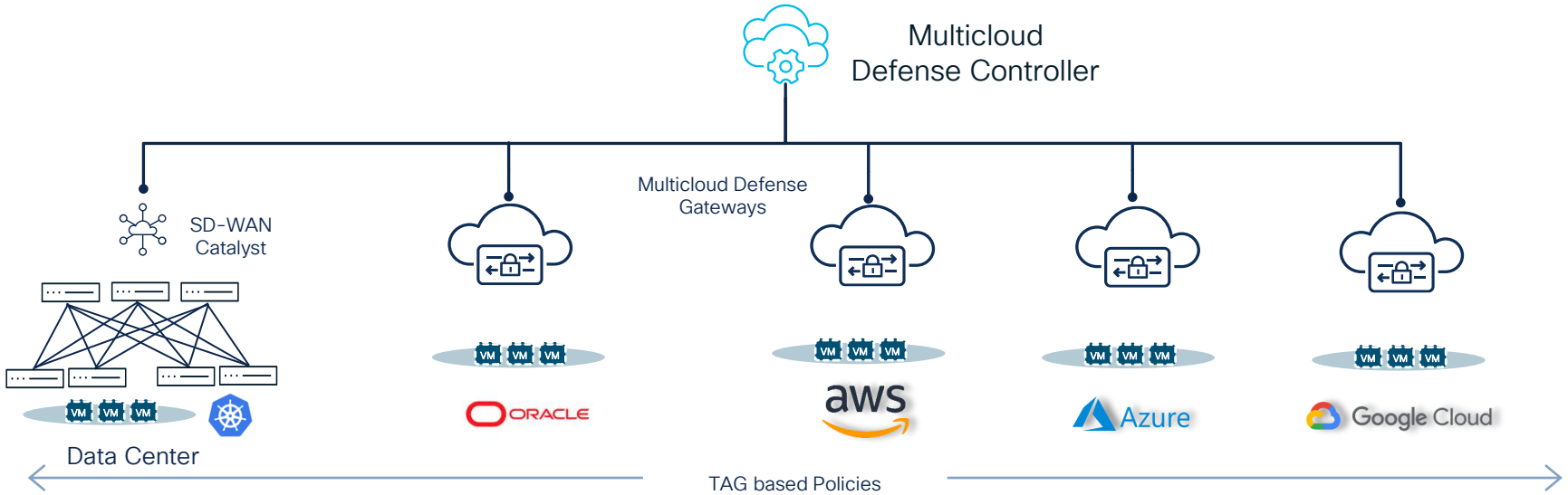
Multicloud Defense

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



Dynamic Classification & Security Automation | Unified Security Policy | Segmentation (East/West) Ingress/Egress Protection | Auto-Scaling

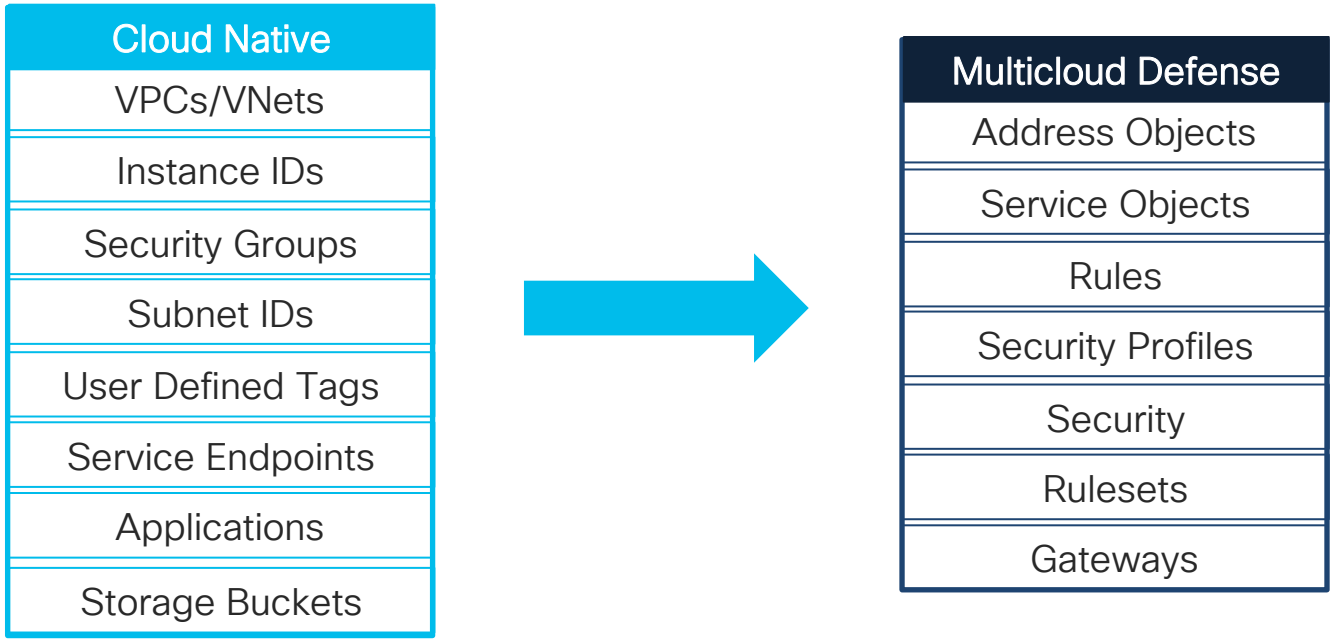
Dynamic Unified Security Policy



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

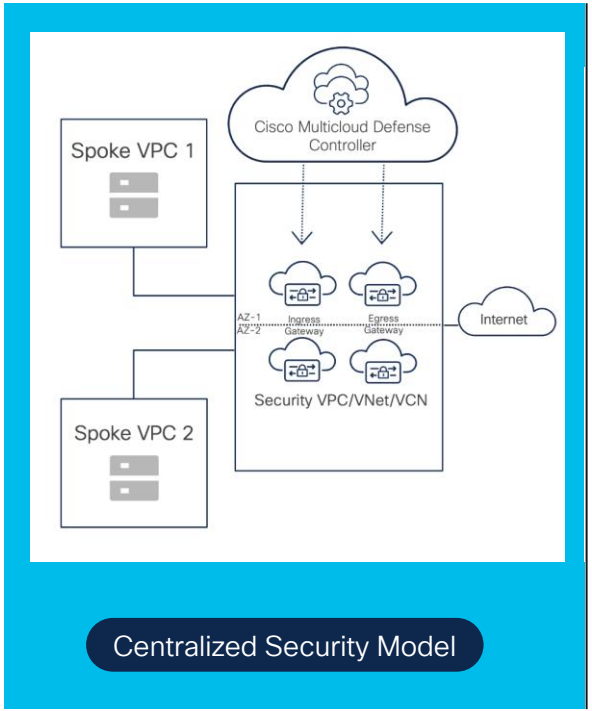
Egress

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

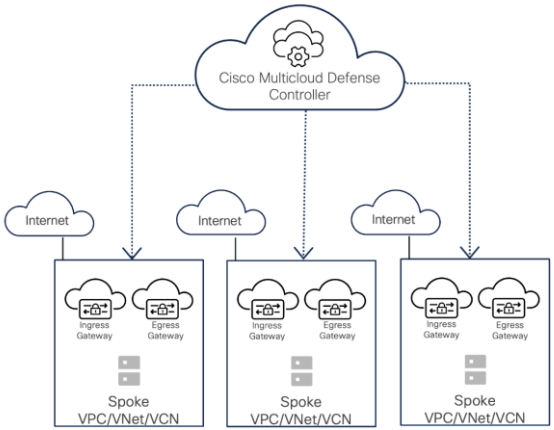
East/West

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

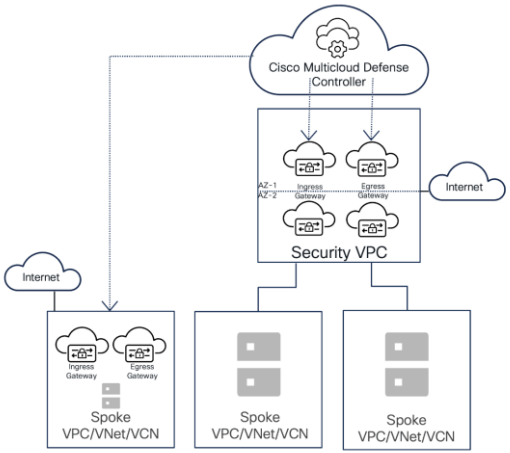
Security Models



Centralized Security Model



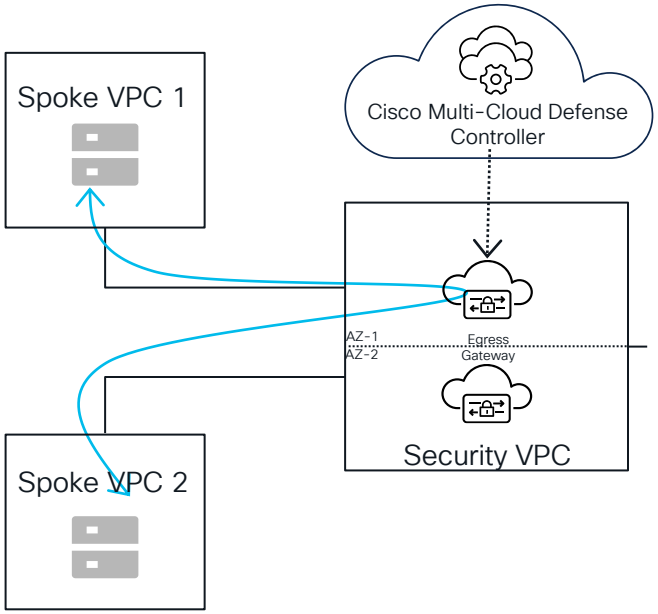
Distributed Security Model



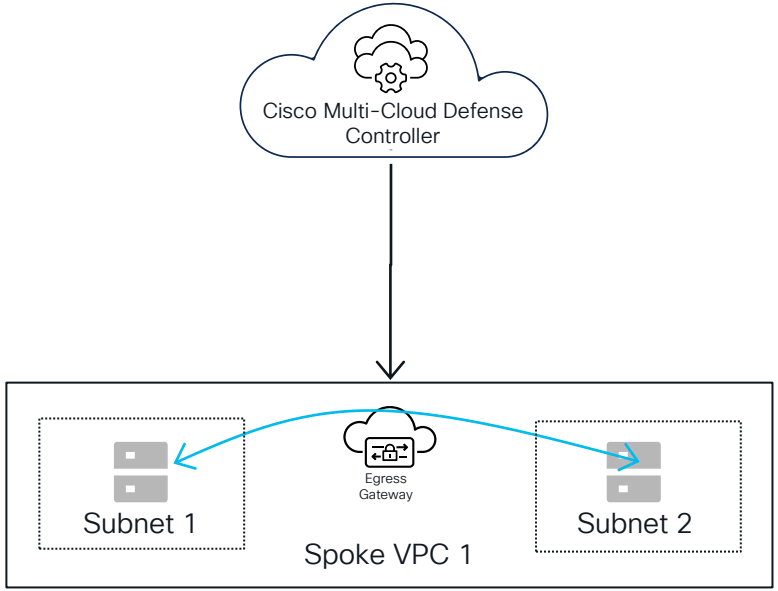
Combined Security Model

Segmentation

Use-case



Centralized Security Model
Inter VPC



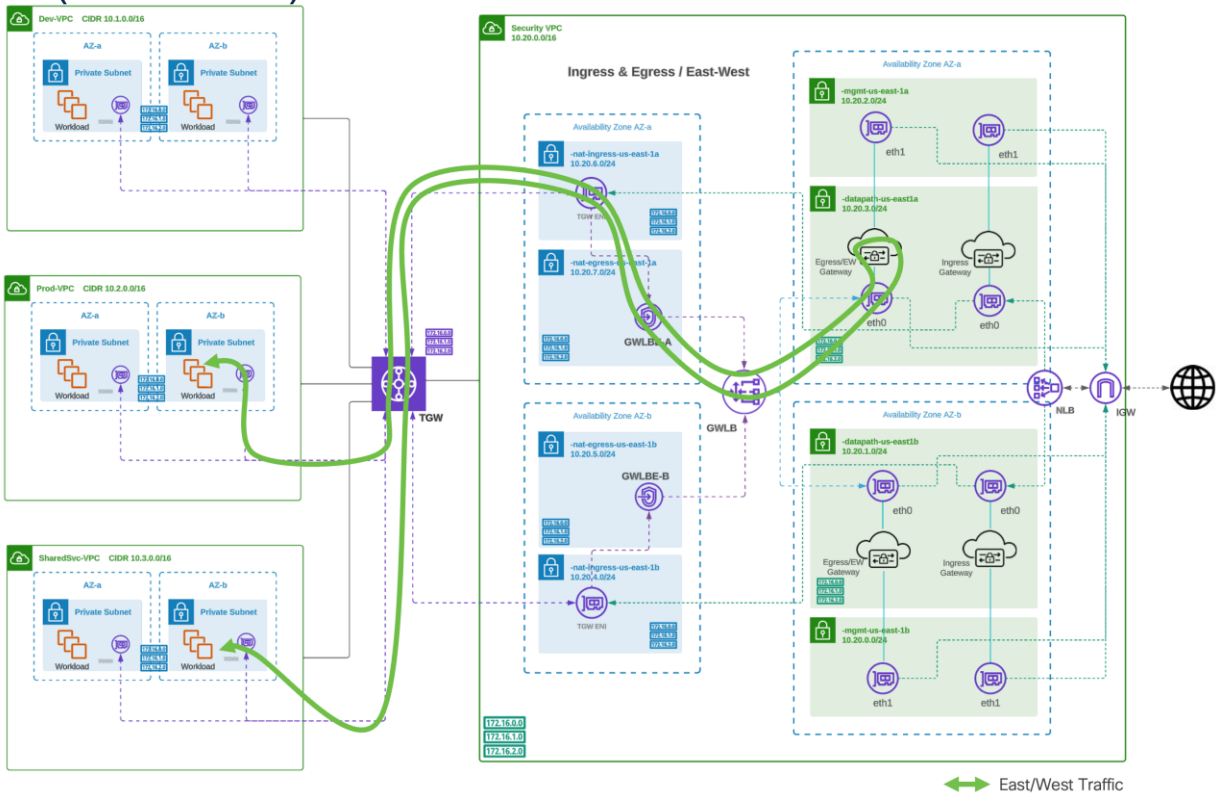
Distributed Security Model
Intra VPC

AWS Centralized

East-West Traffic Inspection (Inter-VPC)

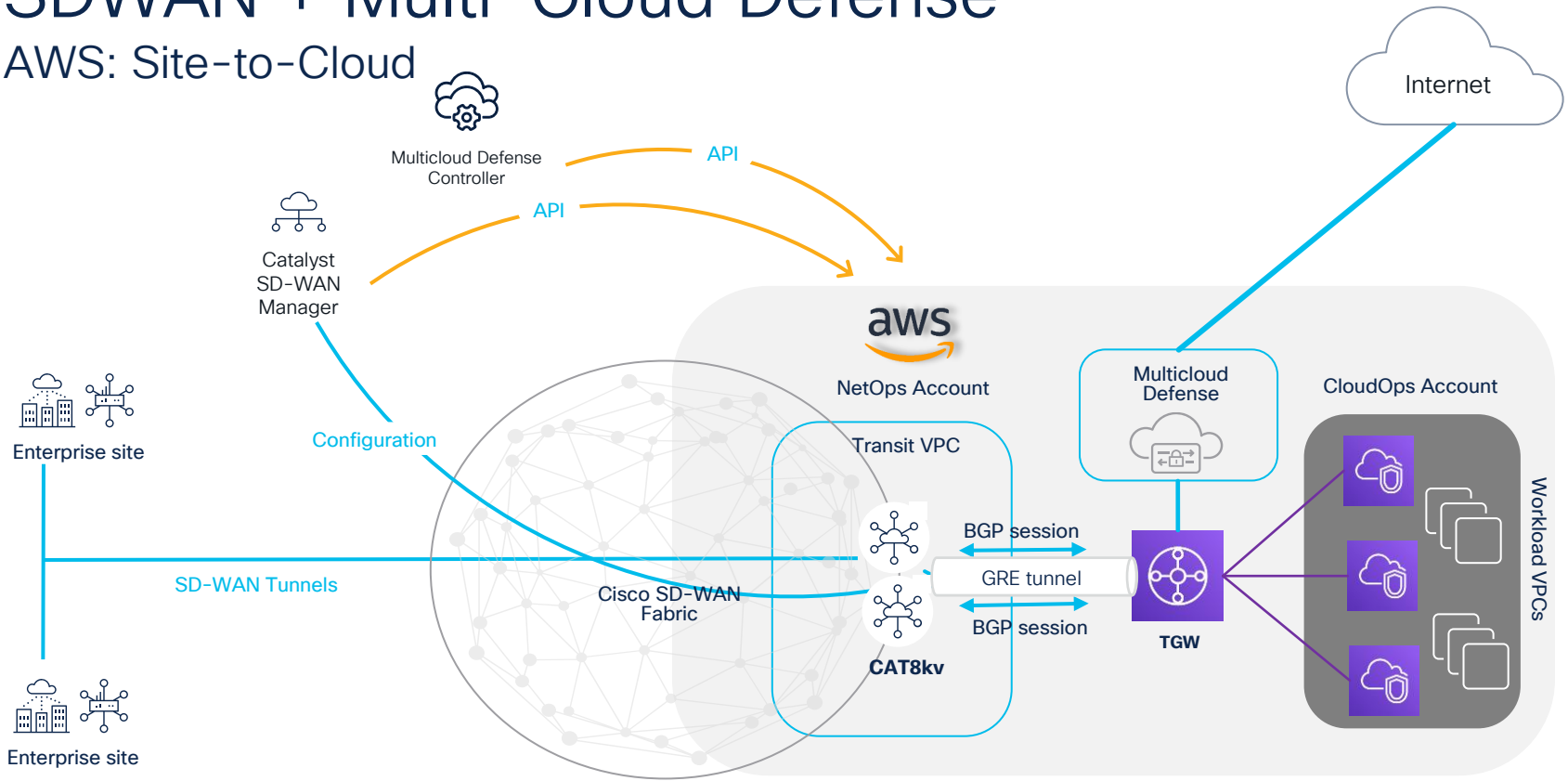
Controller simplifies orchestration

- 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



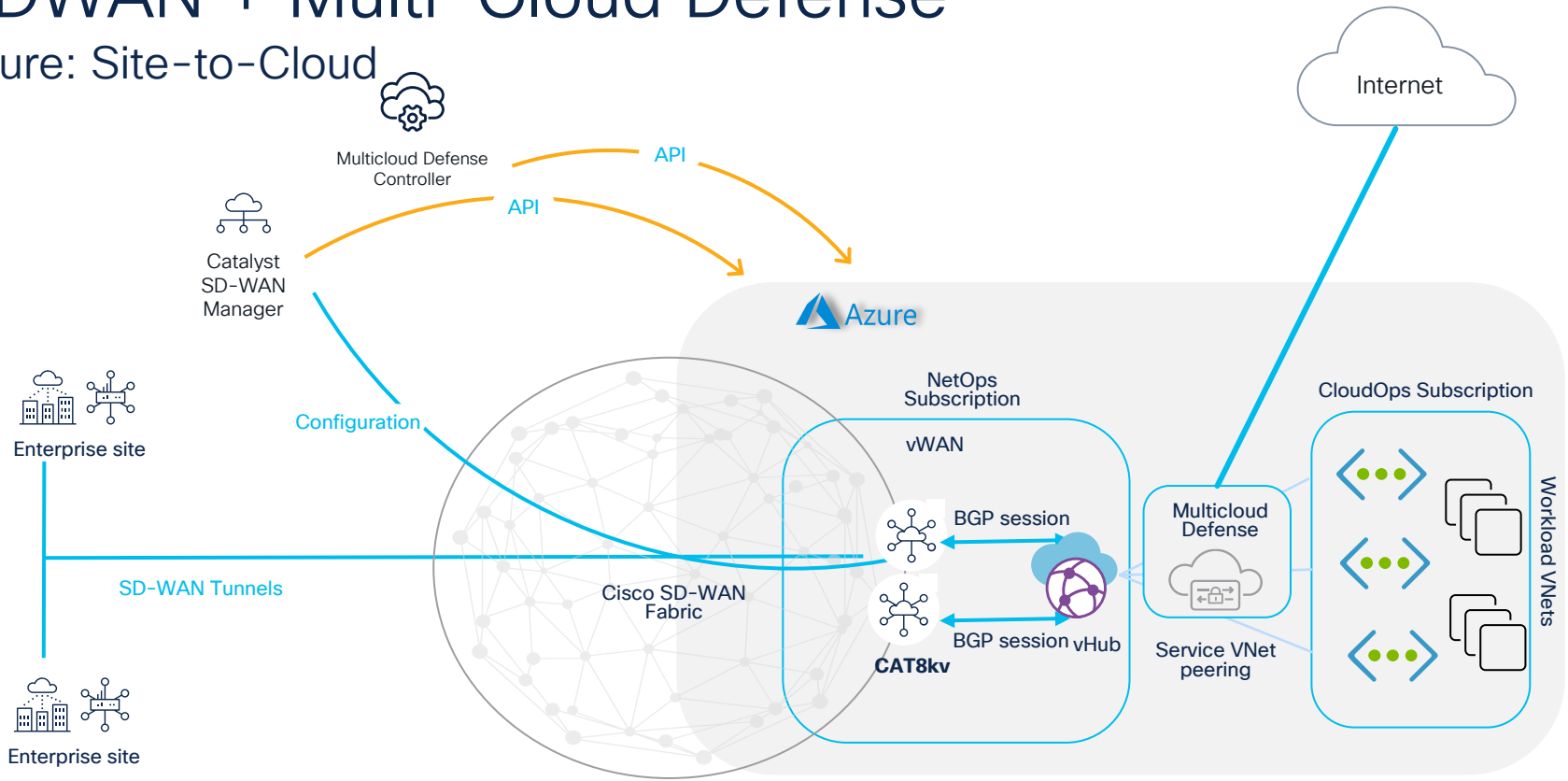
SDWAN + Multi-Cloud Defense

AWS: Site-to-Cloud

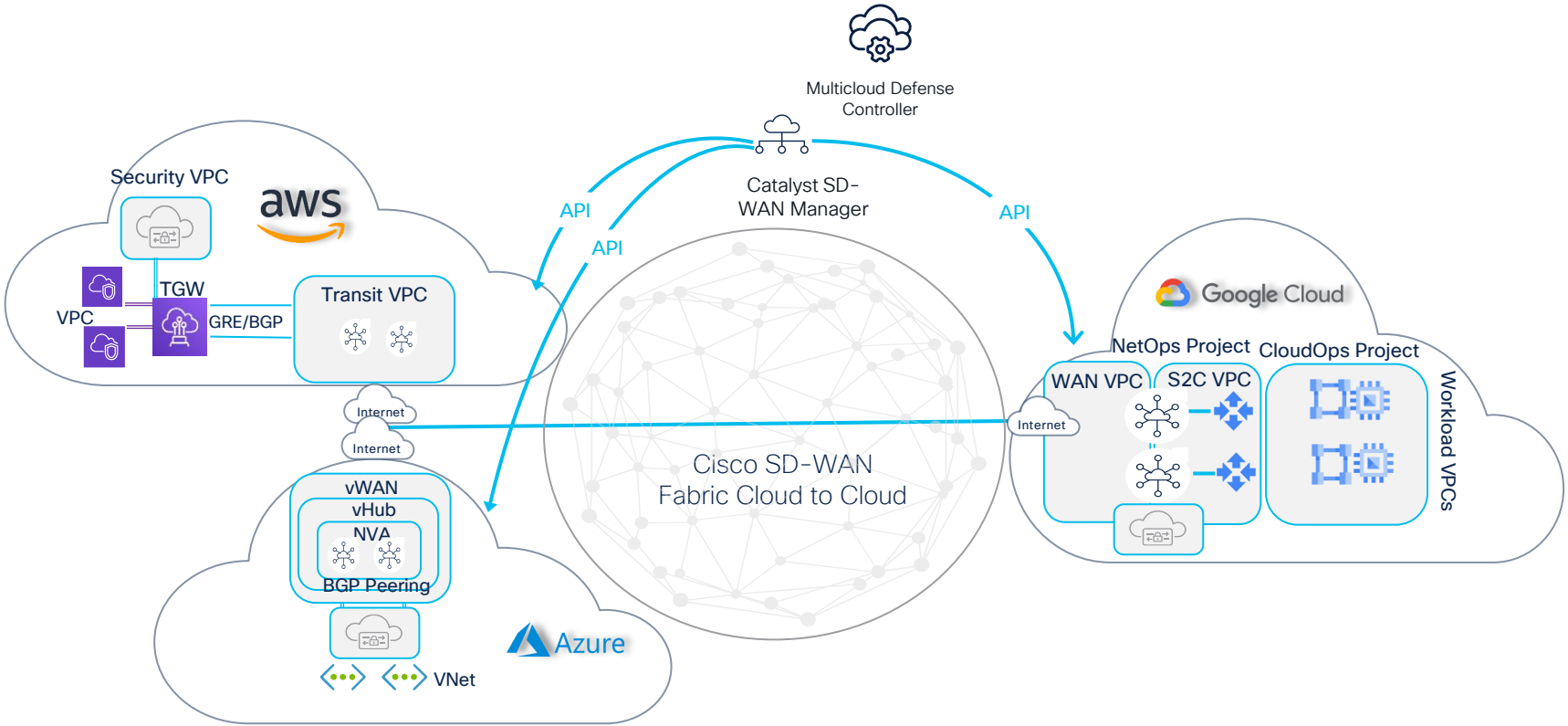


SDWAN + Multi-Cloud Defense

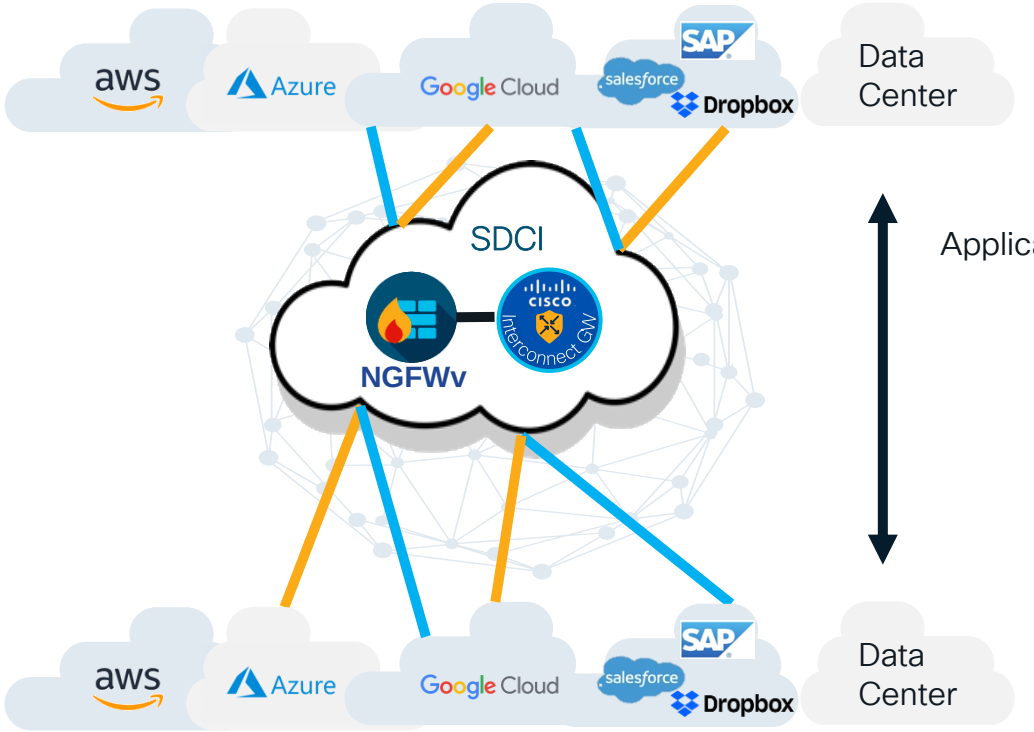
Azure: Site-to-Cloud



Security Stack Insertion in the Cloud



Transparently secures Application-to-Applications
SDWAN + NGFWv + MCD

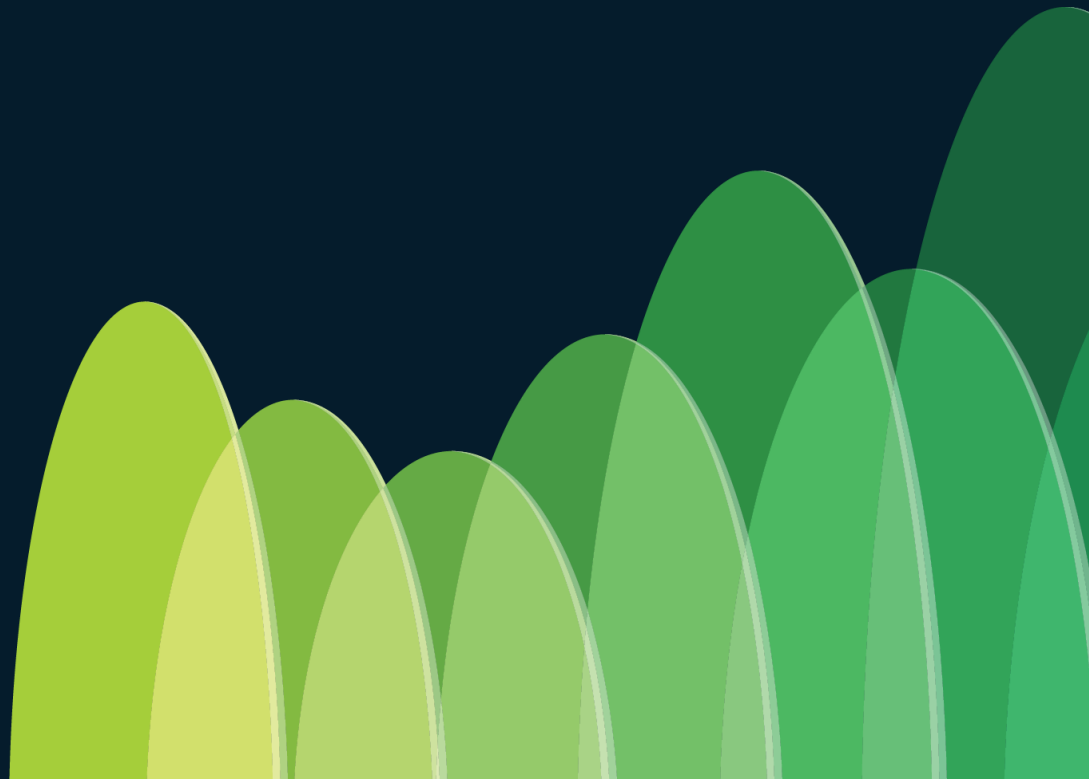


Application to Application

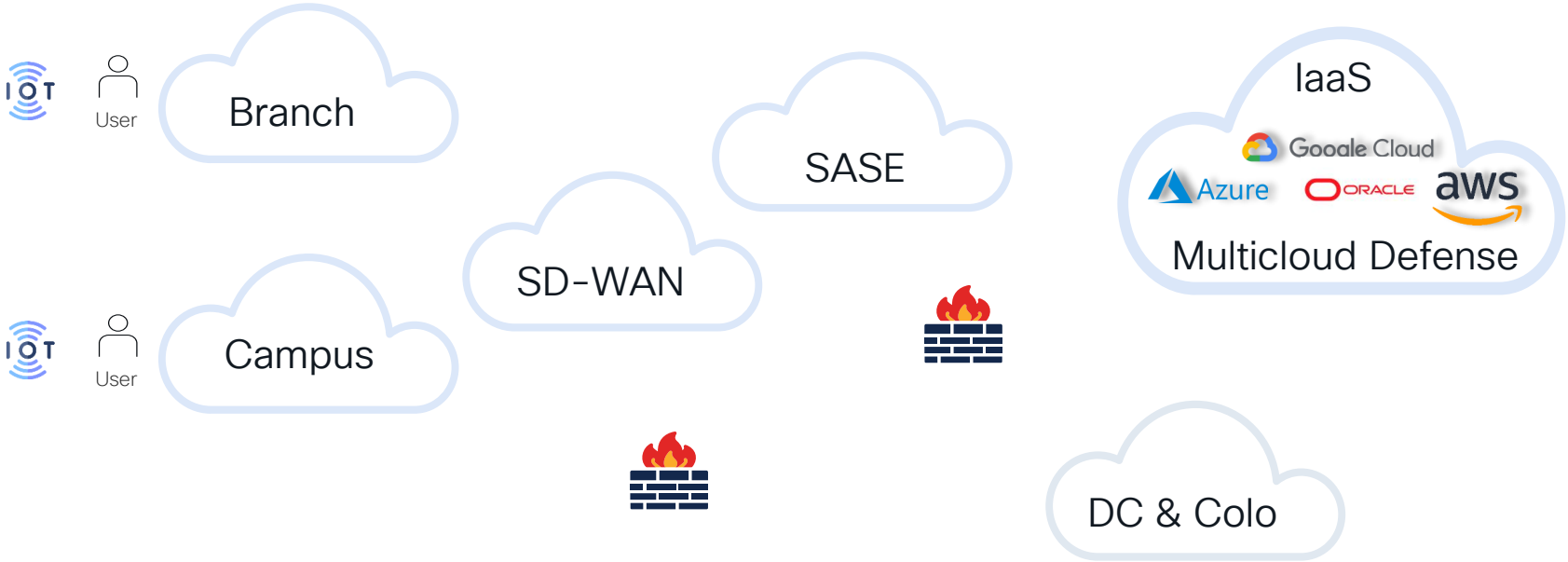
- Web to Database
- Auto-scaled Application
- Container Applications
- Cloud to Cloud
- Cloud to on-prem Data Center
- API to API via HTTPS

Private Transport
Public Transport

Common Policy

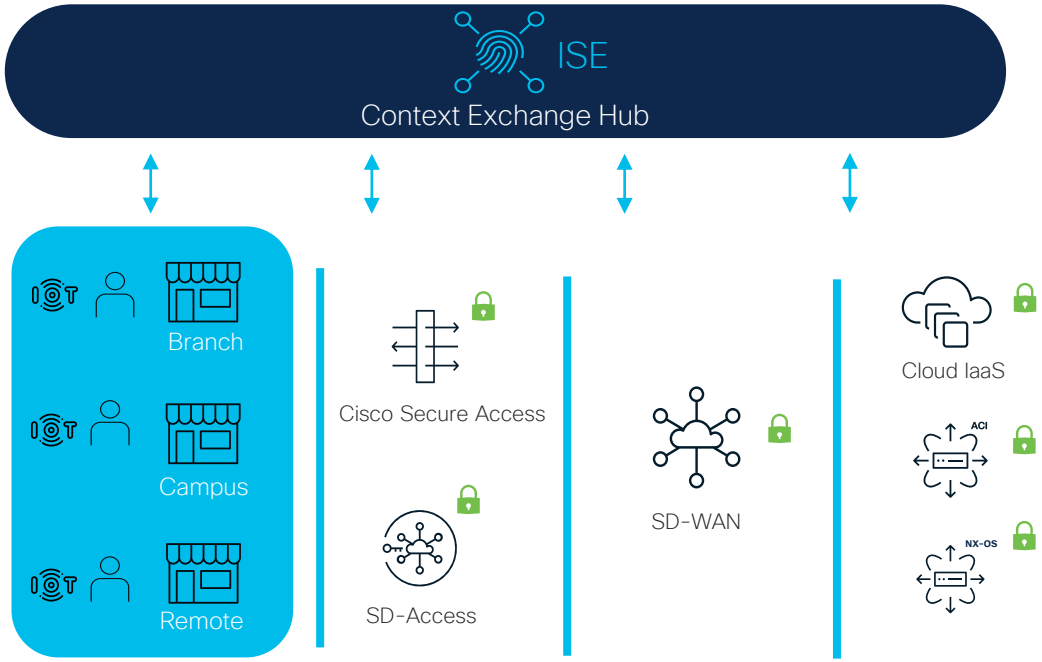


We talked about...



How do we bring all of this together?

Common Policy



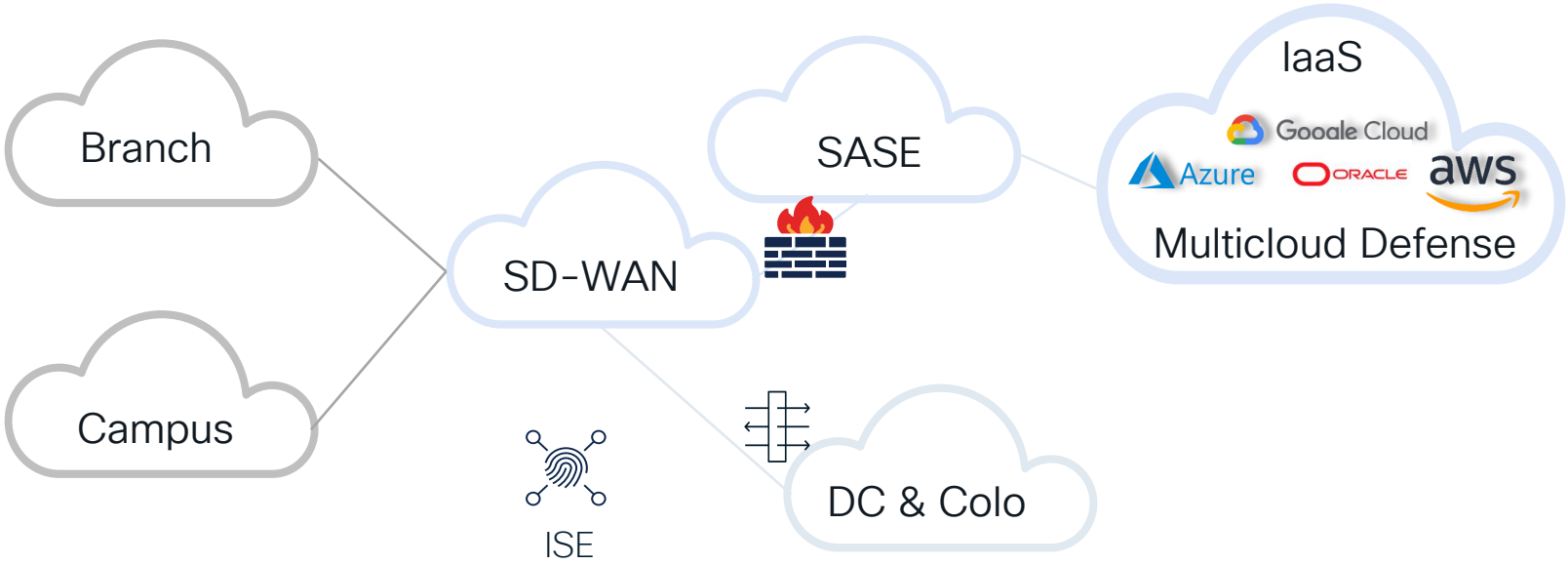
Policy Enforcement Points:
Consistent Policies

- 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.

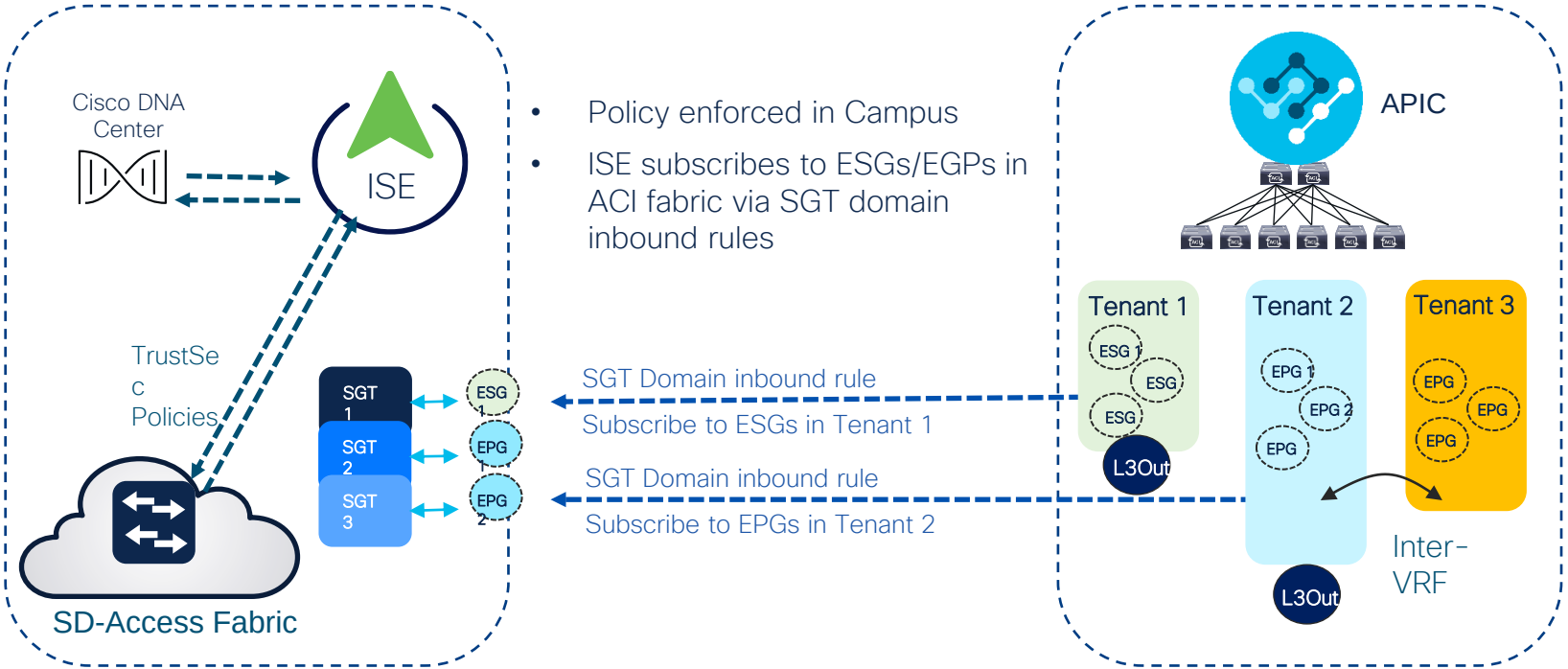
Context-aware policies for on-prem app and cloud workloads for multiple enforcement points

Common Policy

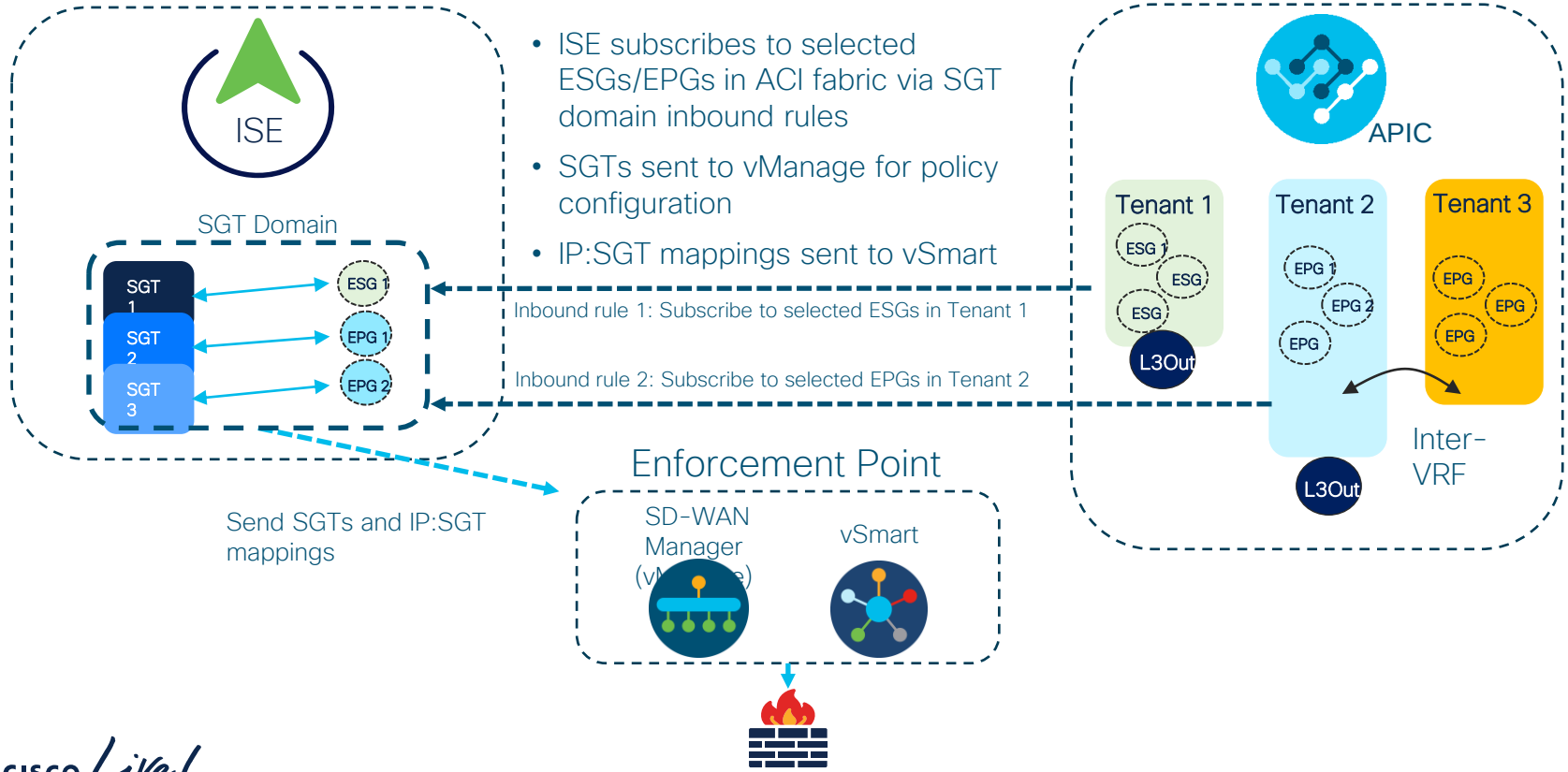
Use Cases



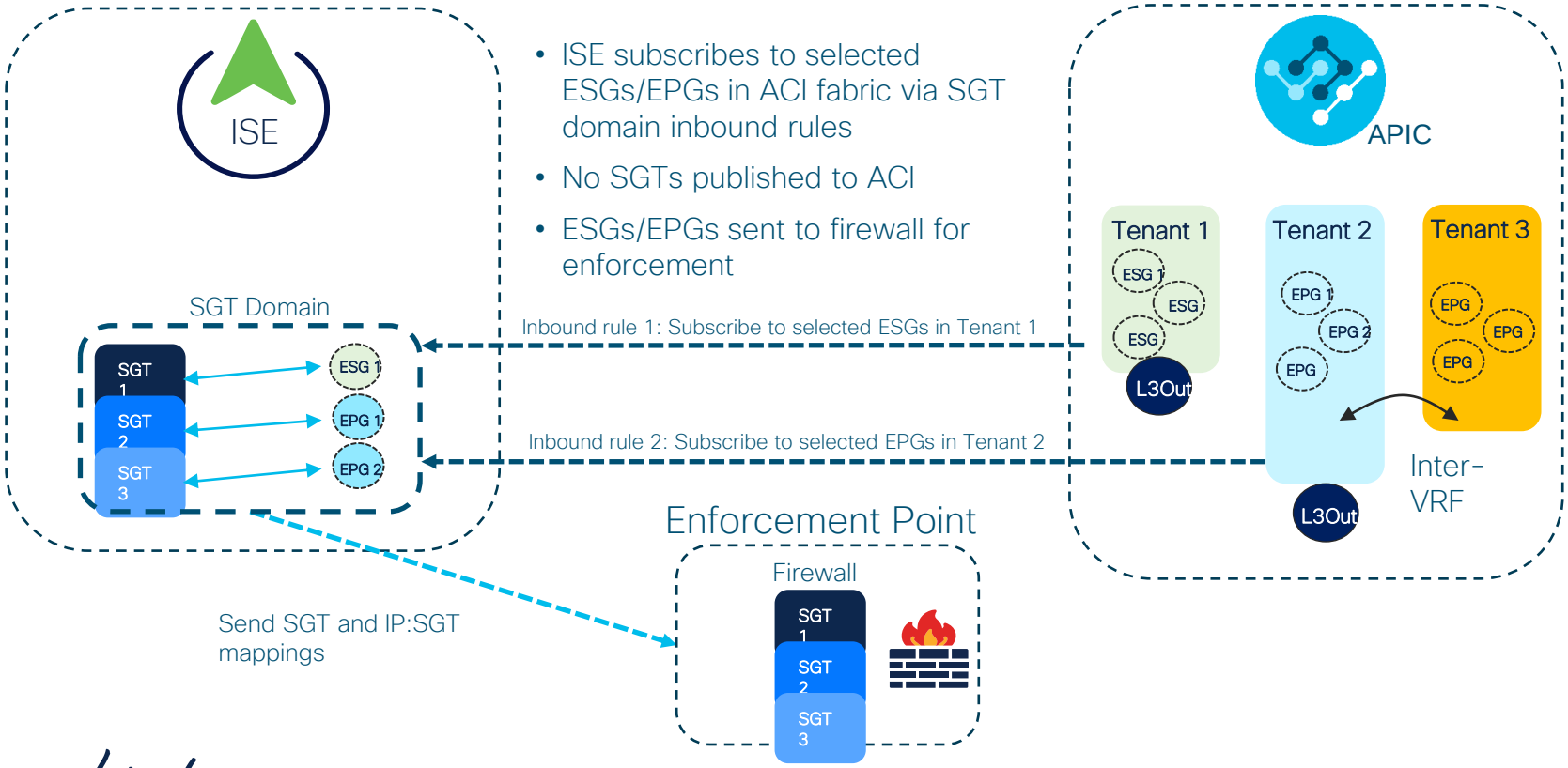
Use Case: Policy Enforcement in Campus



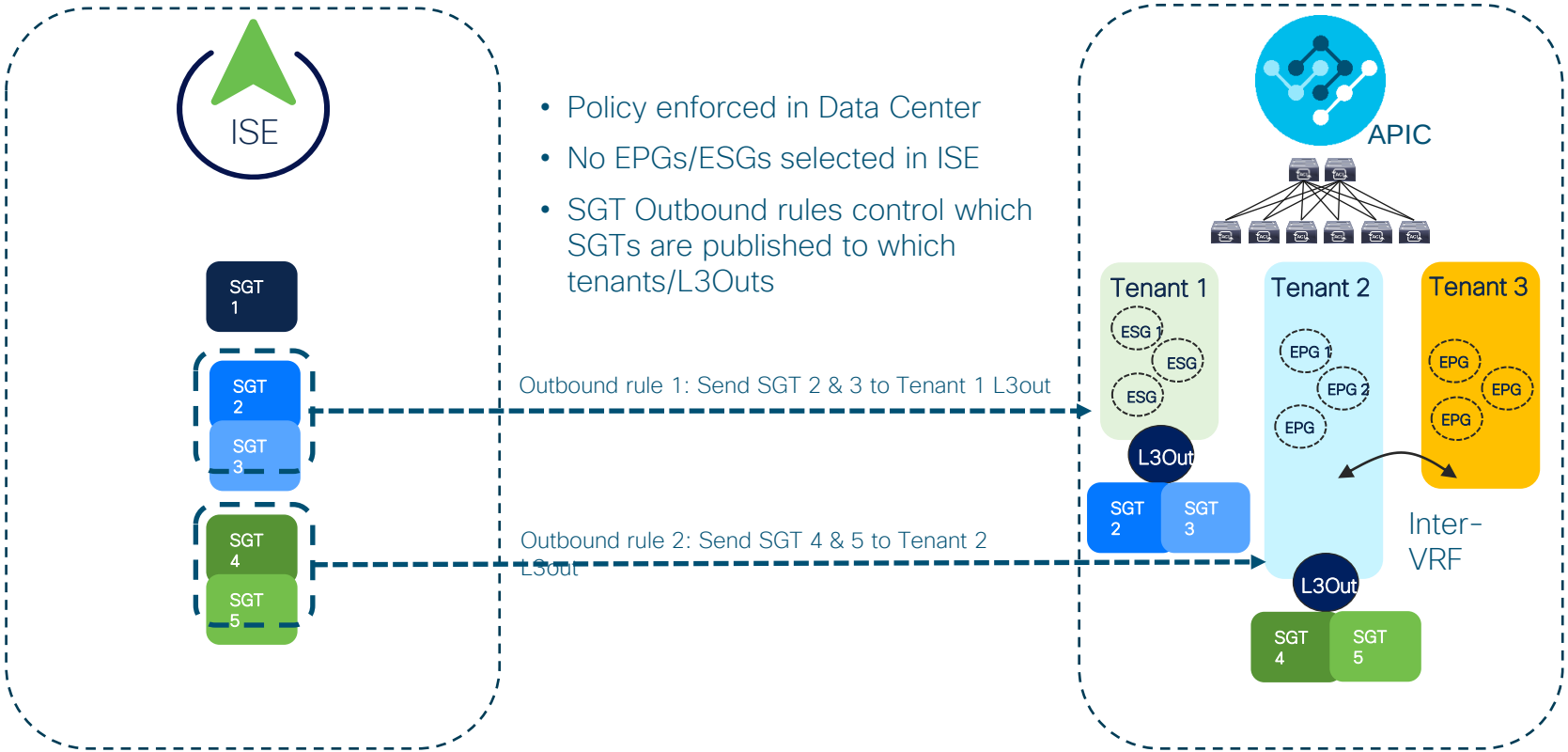
Use Case: Policy Enforcement in SDWAN



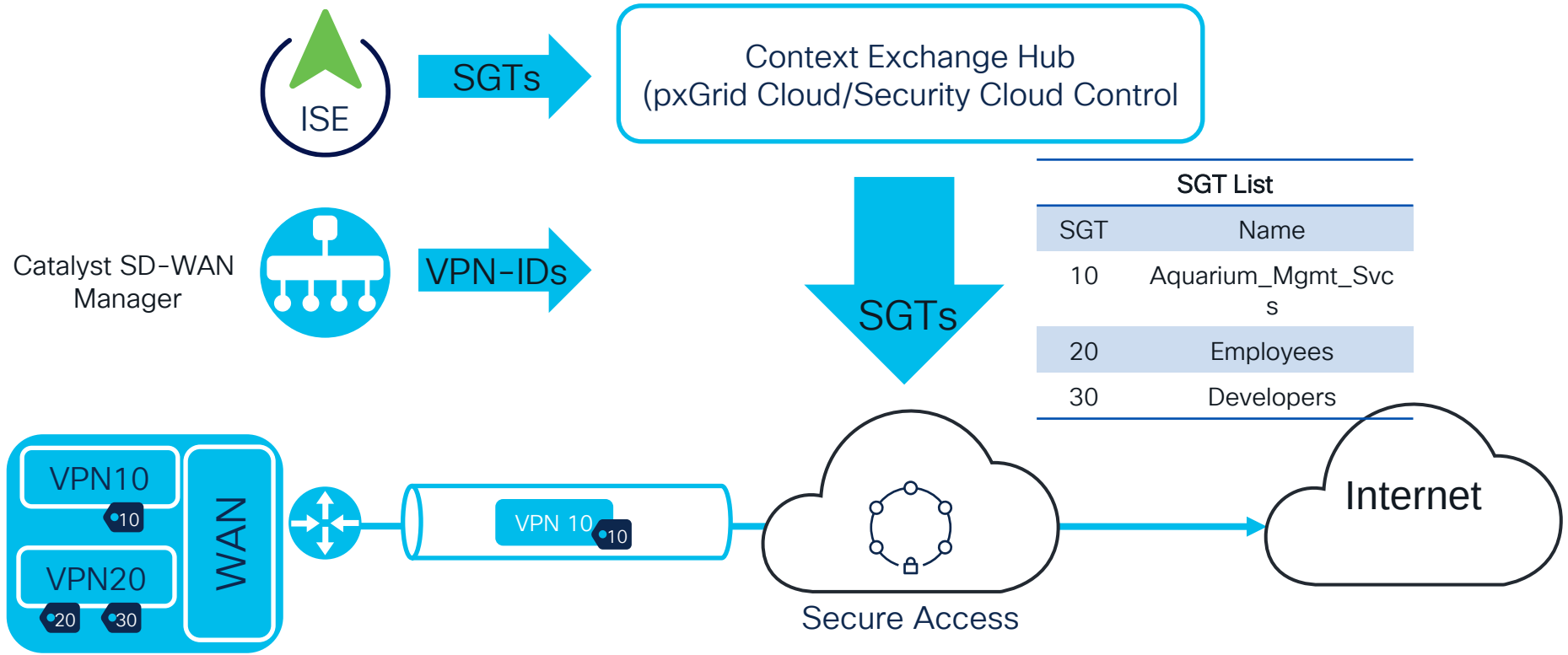
Use Case: Policy Enforcement in Firewall



Use Case: Policy Enforcement in Data Center



ISE / SDWAN / Secure Access Integration

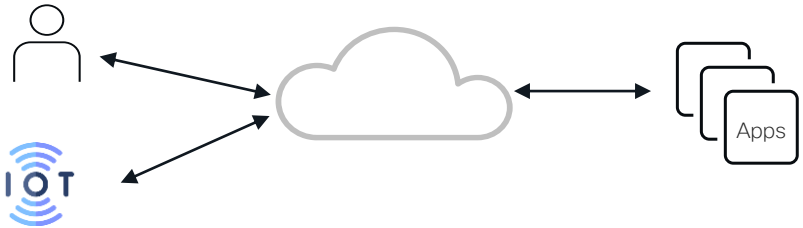


Common Policy

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.

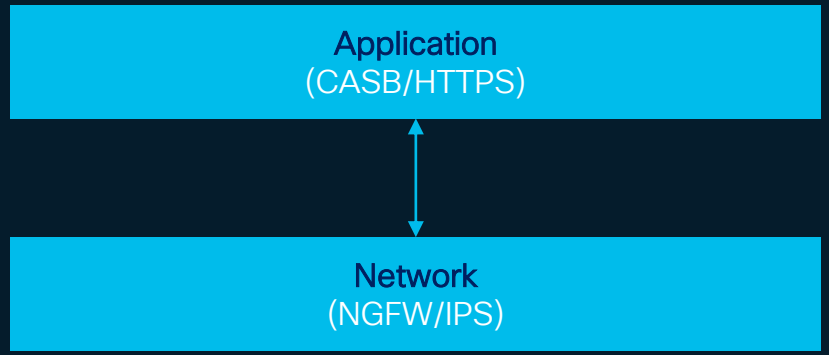
Inside each use case is the ability to apply policy for Micro-Segmentation and/or Service-Chaining

Full Stack Zero Trust

Devices

Users

Things



Applications/Data

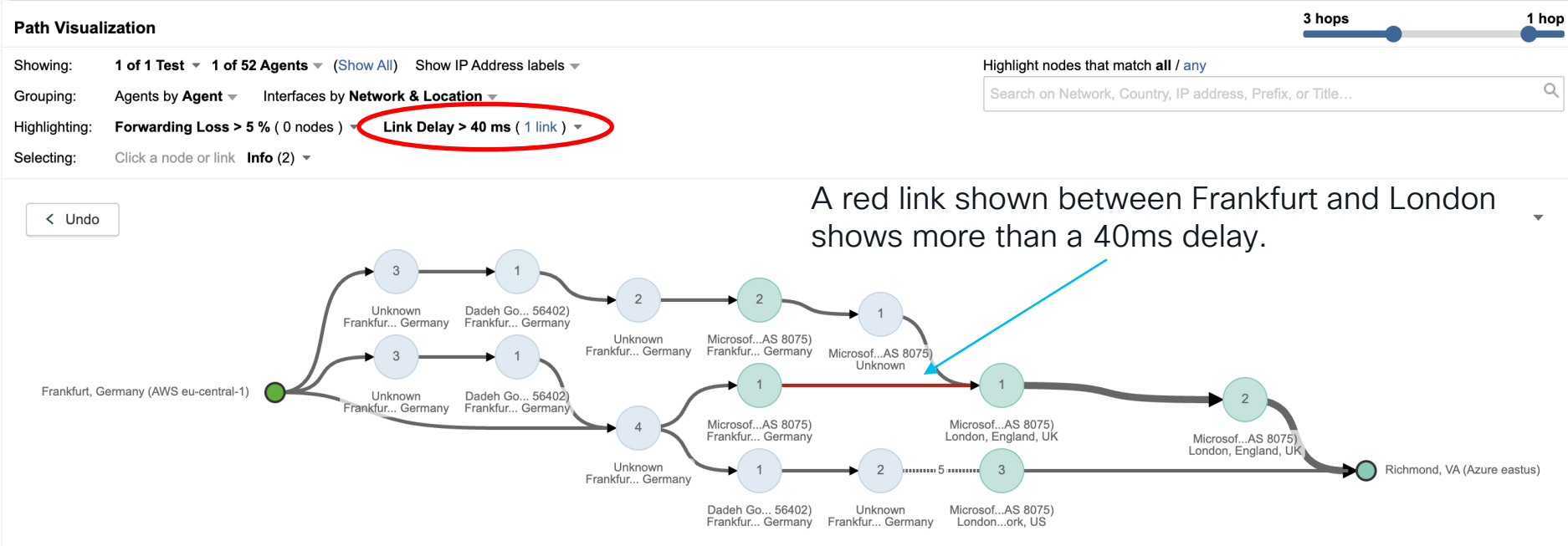
Visibility

Visibility: AWS Inter Region

Thousand Eyes: Dallas, TX to Ashburn, VA

Visibility: AWS/Azure Inter Cloud

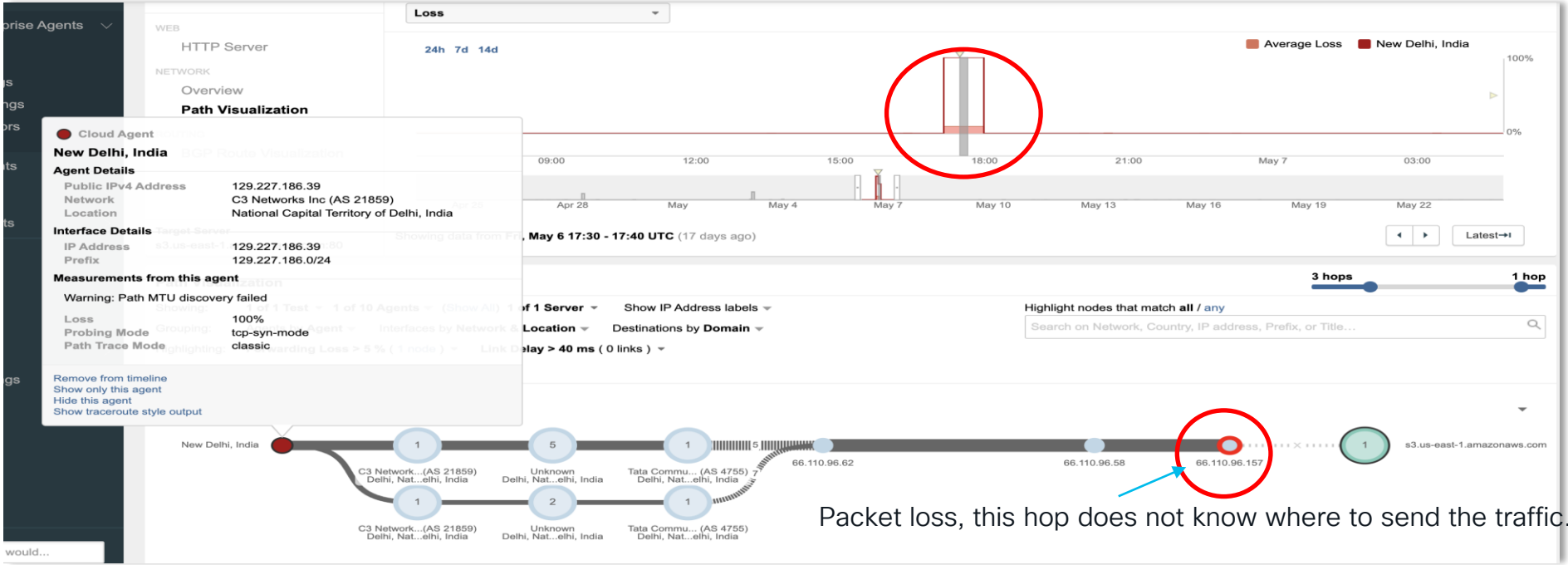
Thousand Eyes – Frankfurt, Germany AWS to Richmond, VA US Azure



- 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

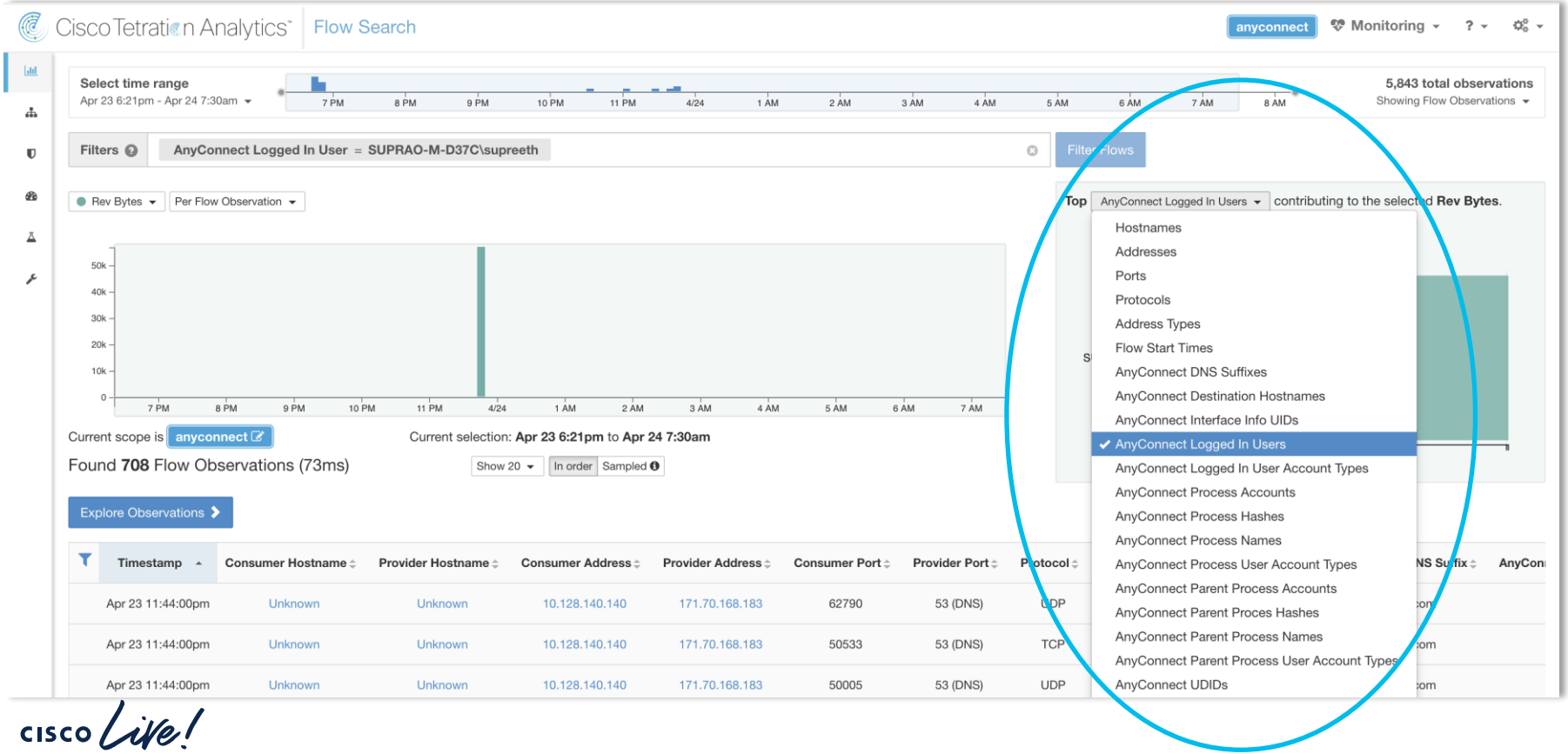
Thousand Eyes – End user perspective from New Delhi to S3 Service



Packet loss, this hop does not know where to send the traffic.

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

Secure Workload Flow Search



cisco Live!

Secure Network Analytics

Trusted ISE Policy - Near Real Time Network Telemetry

cisco Live!

Digital Resilience

1. Foundational Visibility
2. Guided Insights
3. Proactive Response

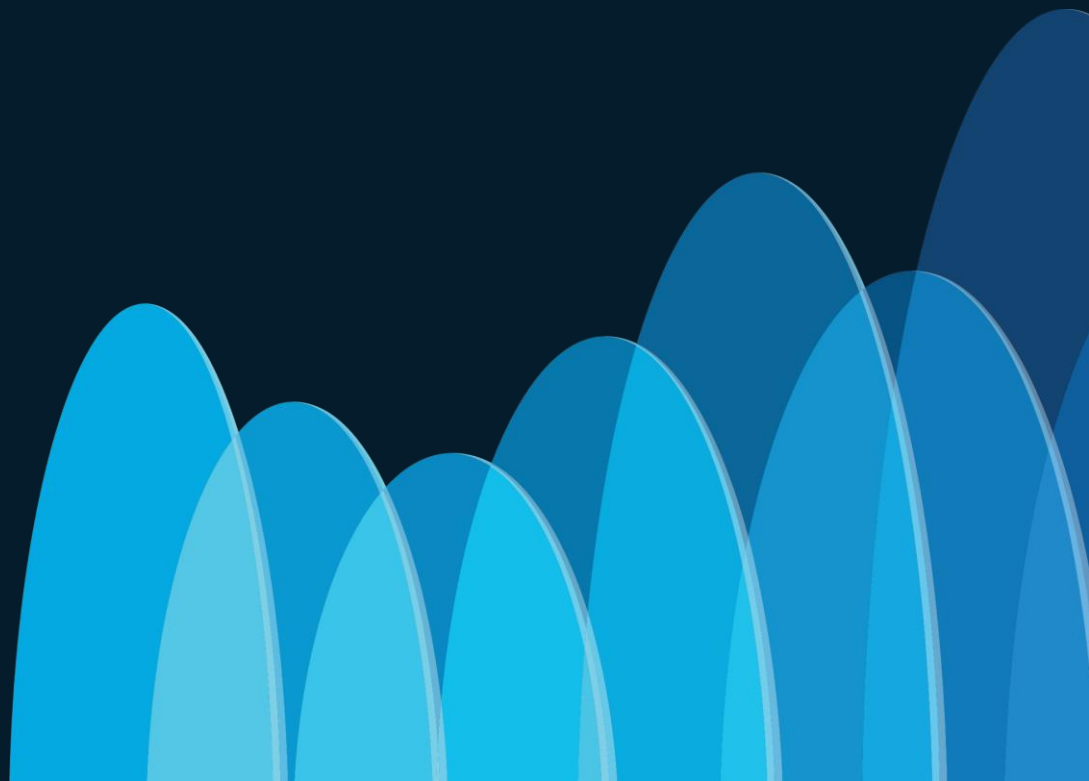
Digital Resilience: Proactive intelligence, predictive recommendations, and automated remediation for Infrastructure, Security and Applications.

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

Webex App

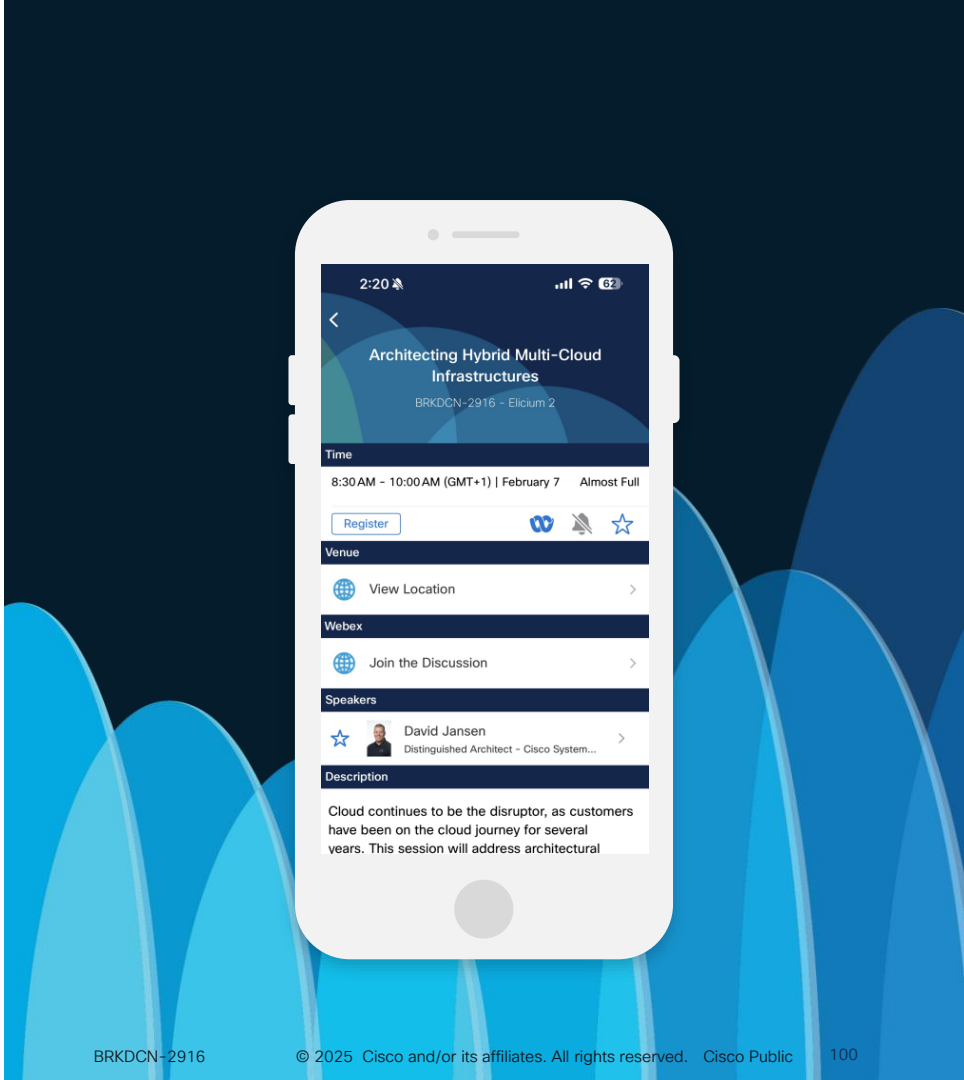
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

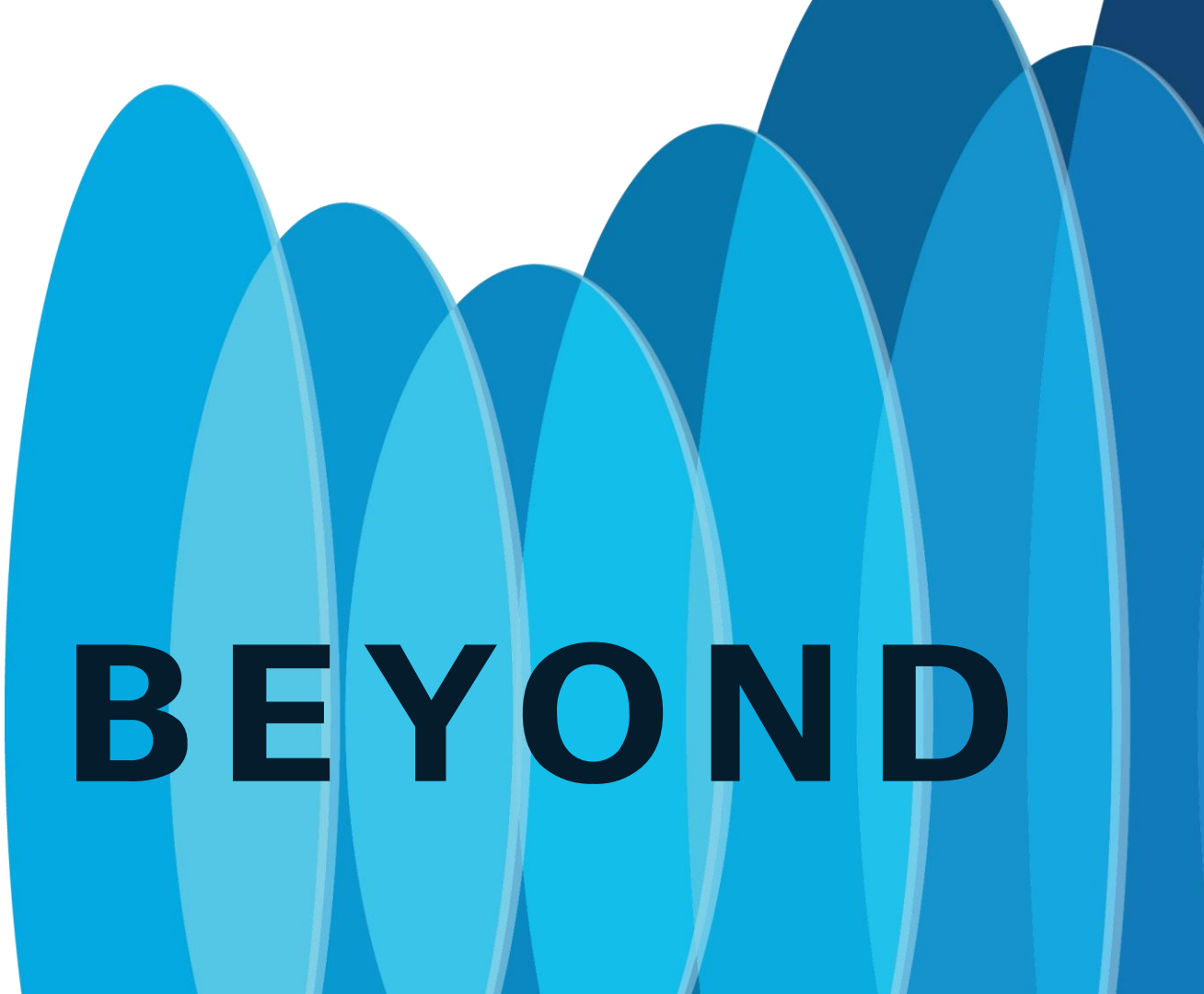
Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND