

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Securing High Speed Private Links to Public Cloud Providers

Overview, Designs, and Methods Connecting Securely to Public Cloud Providers

Craig Hill
Distinguished Architect
U.S. Public Sector, CTO Office

@netwrkr95
<https://www.linkedin.com/in/crhill/>

BRKENT-2003

CISCO *Live!*

#CiscoLiveAPJC

Presentation “House Keeping” Items 😊

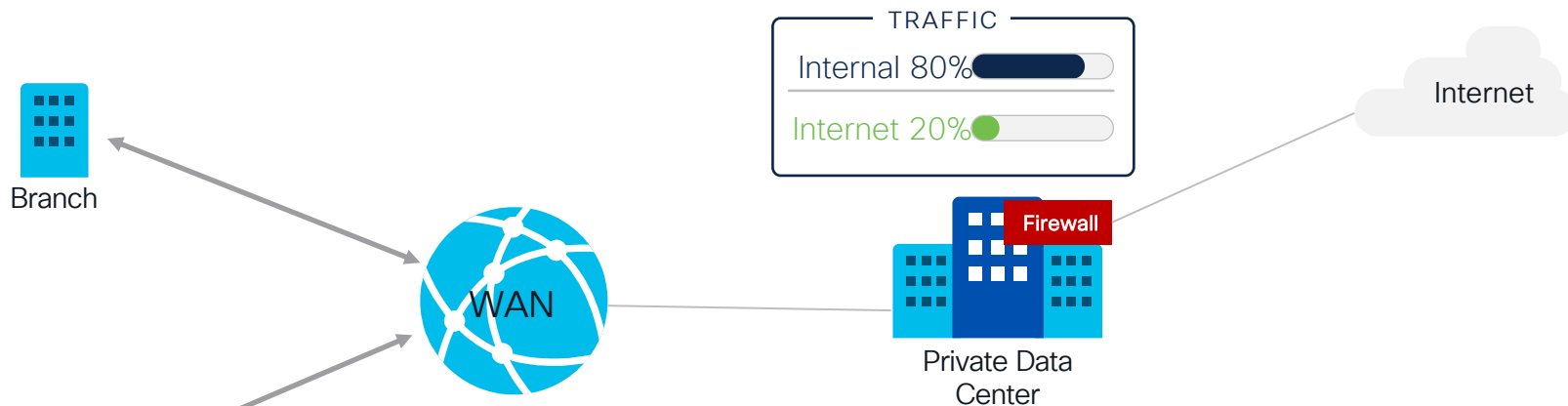
- This is not a product pitch 😊
- This session is focused heavily on secure network design options for connecting private networks securely into the public cloud
- Key customers where this applies? Commercial, enterprise, public sector (government, education), financials, health care
- While several prominent cloud providers will be included in this discussion, the discussion has no preferred cloud provider other than those supporting the intended technology topic

Agenda

- Quick primer – How cloud app hosting has transformed WAN designs
- Connection Option Overview for Public/Private Access into the Cloud
- Securing High Speed Access into the Public Cloud with MACsec
- Configuration Example Reviews – MACsec into Public Cloud
- Extending Enterprise Controlled Encryption into the cloud – Design options, trade-offs, evaluation criteria
- Cloud Network Visibility Options
- Summary & References

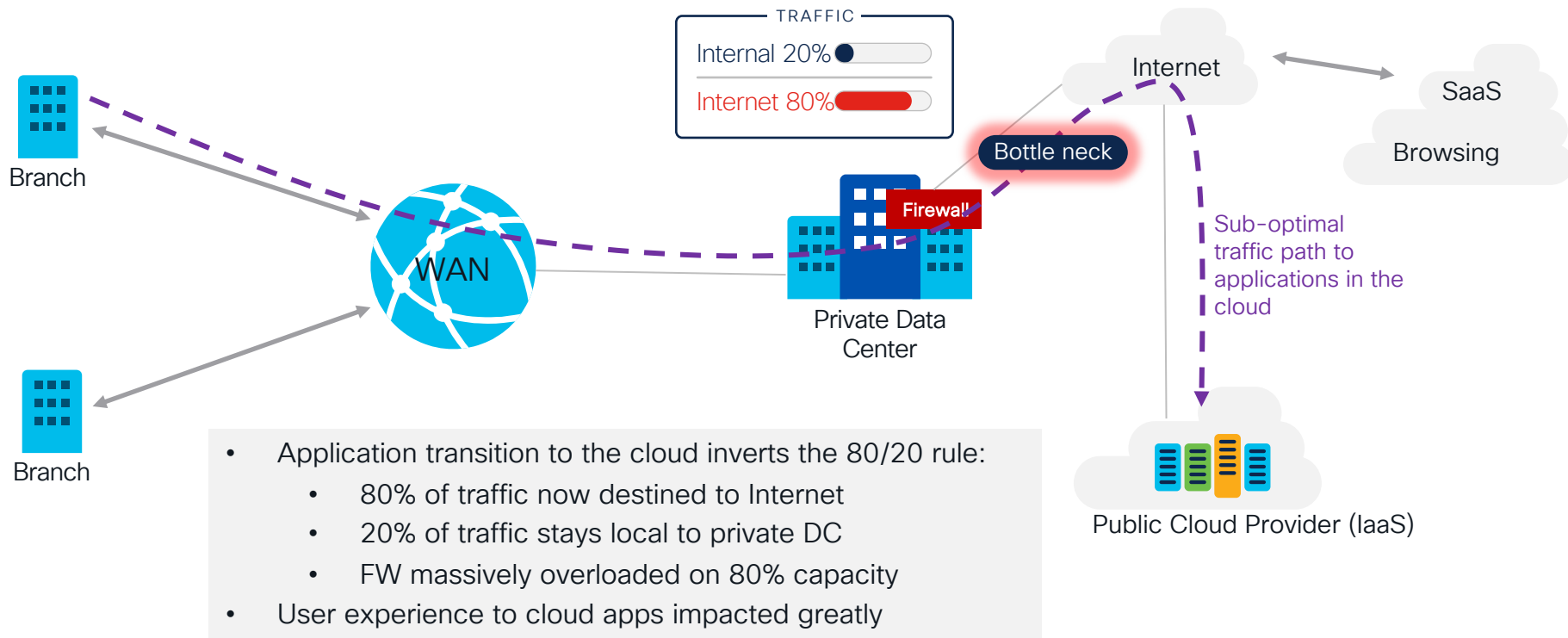
How the WAN is Evolving as Enterprise Applications Transition to the Cloud

Evolution of App Hosting in the Enterprise

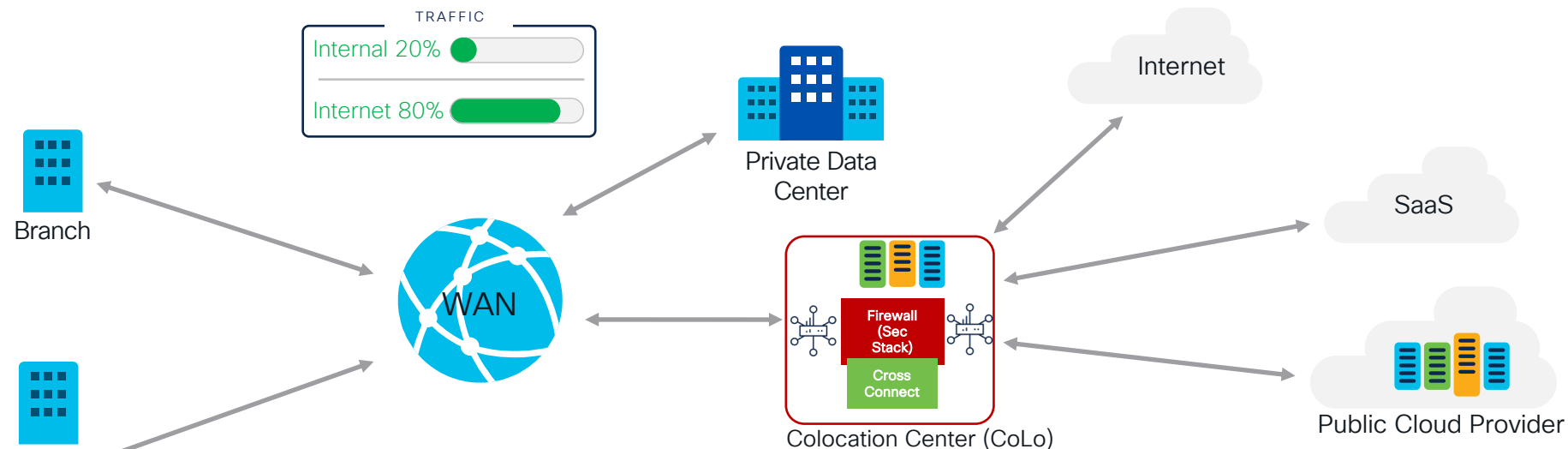


- Common and successful architecture for many years
- Enterprise applications hosted in private data center (DC)
- ~ 80% of branch traffic – destined to private DC applications
- ~ 20% of branch traffic – destined to Internet through the FW
- Aligns with 80/20 rule – apps / internet

Evolution of App Hosting in the Enterprise



The “Cloud Ready Network” Transition Architecture



- The CoLo is the center of the universe for the enterprise WAN
 - Provides X-connect options to public cloud, SaaS, Internet, private peering
 - Supports on-prem DC without being “on-prem” of customer facility
 - Vitally important element for any WAN design and cloud transition strategy
 - Provides platform that is “multi cloud” ready
- Connection options into the public cloud are numerous and pros/cons vary per option

Carrier Neutral / Co-Location Facilities

‘a facility which allows interconnection between multiple telecommunication carriers and/or colocation providers. Network neutral data centers exist all over the world and vary in size and power’

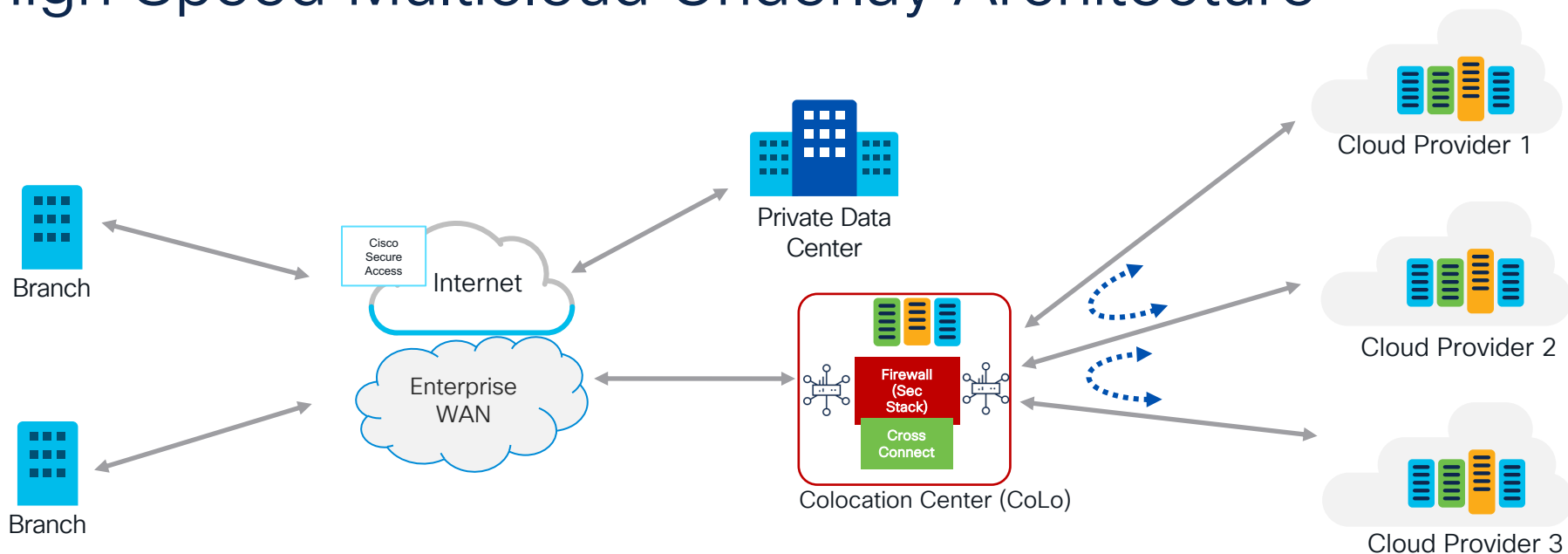
Benefits:

- Access to some of the largest [Cloud Providers](#)
- Carrier Neutral encourages [Competition](#) leading to better pricing & services
- Simpler to switch between suppliers
- Time to connectivity is fast

Examples:



High Speed Multicloud Underlay Architecture

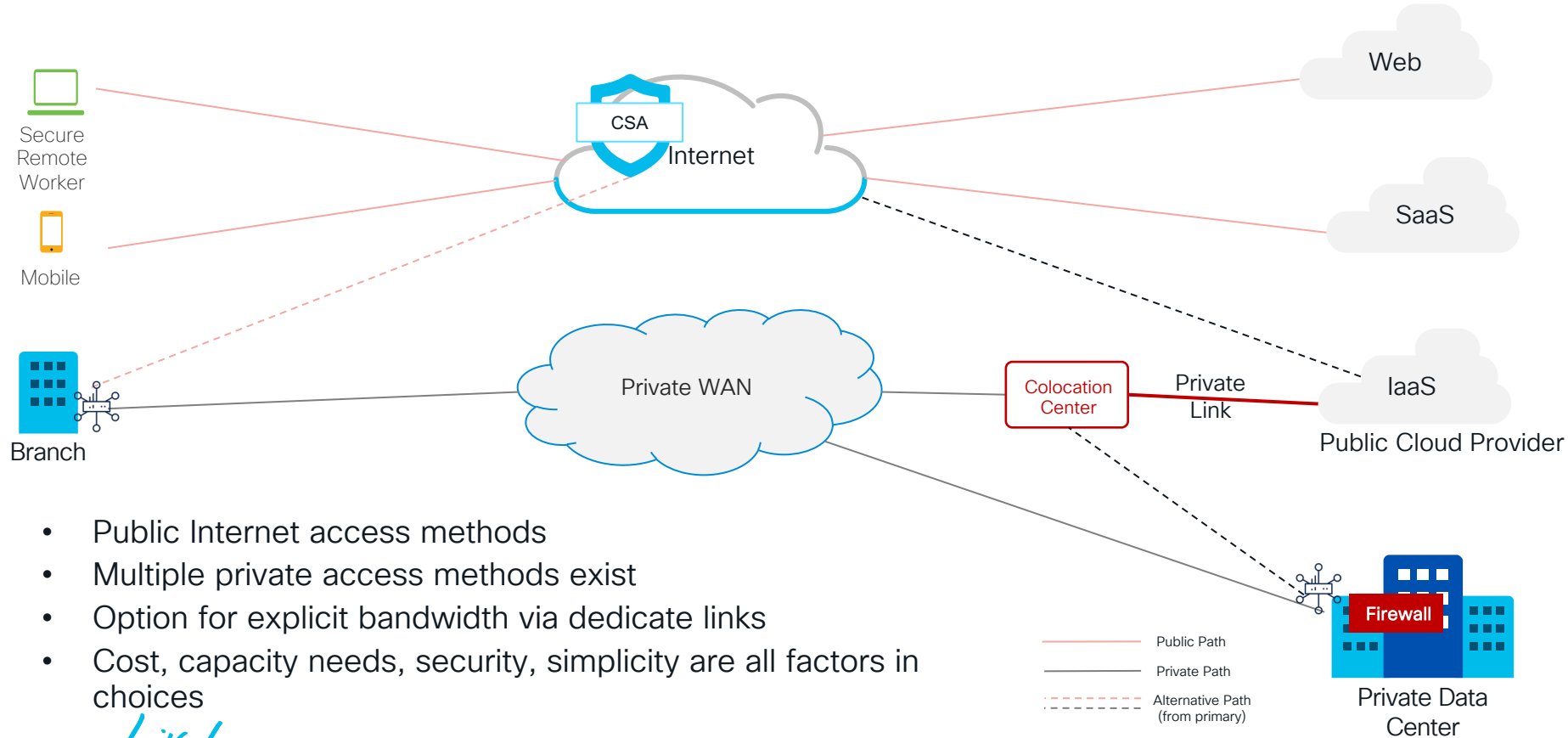


- The CoLo is the center of the universe for Multicloud private link
- Provides multicloud “High Speed underlay” cross-connect between each cloud provider
- Enterprise can establish own security policies for inter-cloud provider comms
- Assumes leveraging cloud provider private link options (AWS DX, Azure ExpressRt, etc)

Options for Connecting to Cloud Providers

Public and Private
Network Access Options

Options for Connecting into the Cloud Providers



- Public Internet access methods
- Multiple private access methods exist
- Option for explicit bandwidth via dedicate links
- Cost, capacity needs, security, simplicity are all factors in choices

Option for Connecting Into the Cloud Providers

“Public Internet” Option

Advantages: Using the Internet?

- Easy access from anywhere into the hosted cloud applications
- Internet ubiquitous from any location
- No need for dedicated private link cost

Challenges: Using the Internet?

- Lack of deterministic transport behavior (loss, latency, jitter)
- Sustained BW requirements available indeterministic
- Impact on user experience for applications needing tighter SLA's

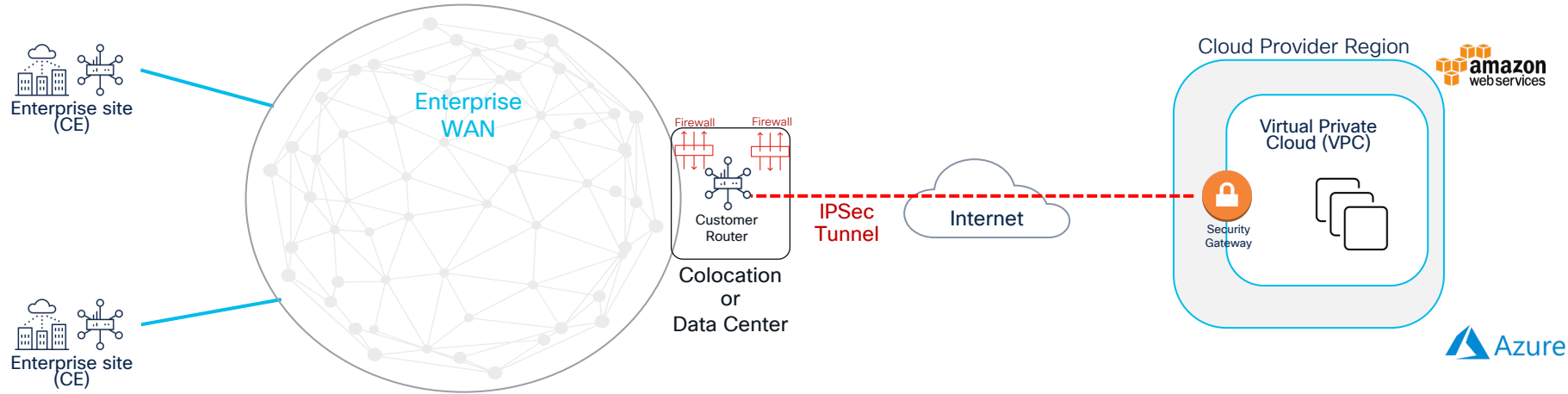
Options for Connecting Into the Cloud Providers

“Private Link” Connection Option

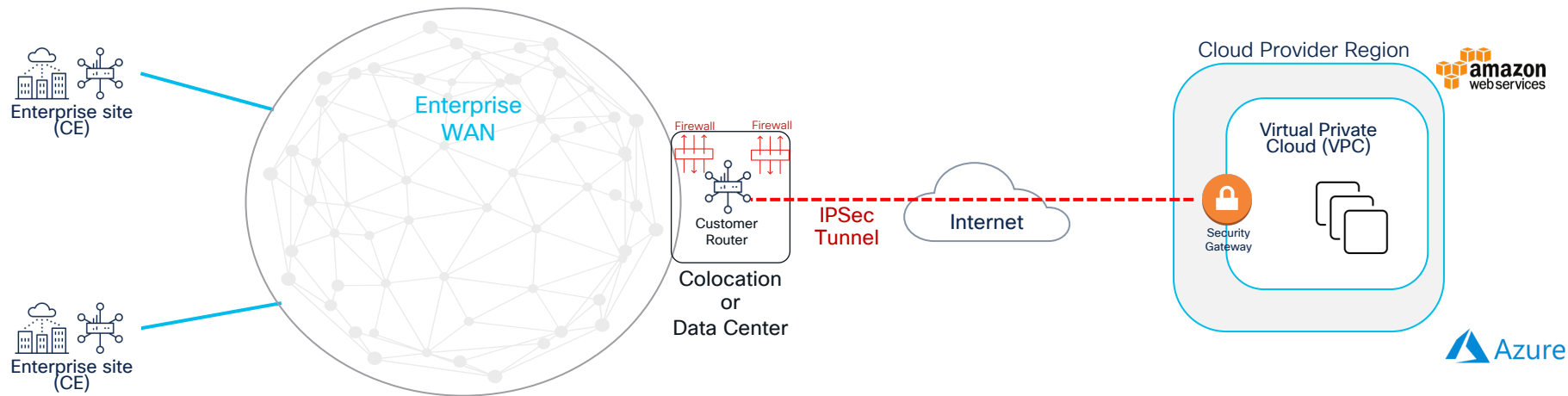
- **Advantages:** Private Links into the Cloud Providers?
 - Shortest path to the applications hosted in the cloud
 - Deterministic transport behavior (loss, latency, jitter) to/from the cloud
 - Isolation from the public internet
 - More tailored IP routing and route control between the cloud and enterprise
- **Challenges:** Private Links into the Cloud Providers?
 - Cost, Security of those links, complexity of setup
- **CoLo Presence:** Private links to CSP + Enterprise-owned router in the CoLo
 - Offers flexible “Cloud On Ramp” access to any XaaS, carrier, cross-connect, ISP peer
 - Multicloud Prep: Sets the table for multi-cloud support (current or future)

Public Cloud Connection Access Options

IPSec VPN Tunnels into the Cloud Provider



IPSec VPN Tunnels into the Cloud Provider



Key Benefits

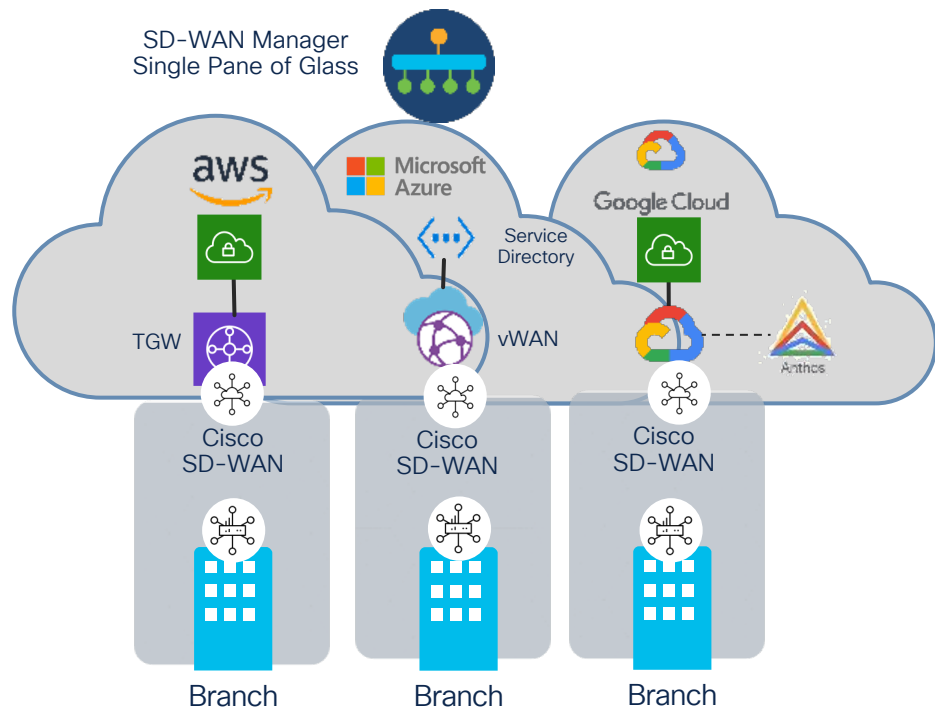
- Simple
- Cost effective (egress data charges still exist)
- Leverages existing security tools
- Can benefit from automation (IaC)

Deployment Targets

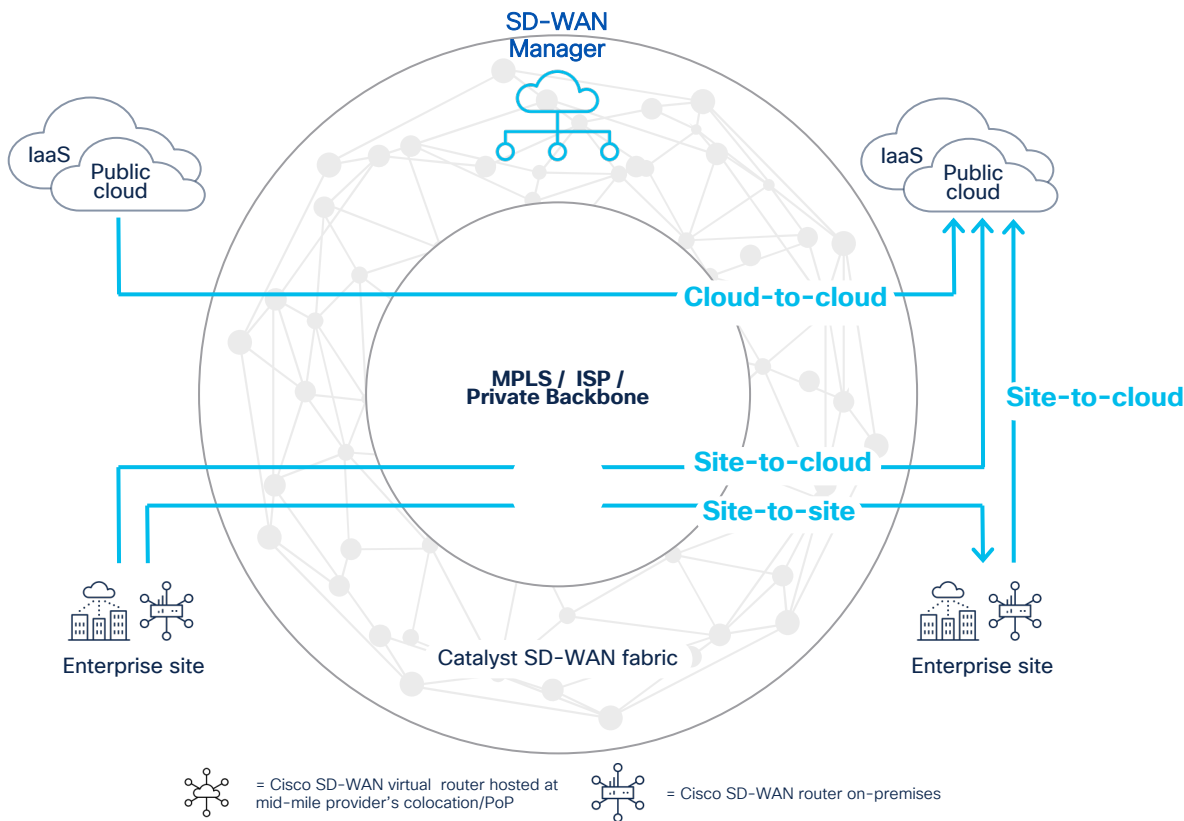
- Targets low-scale connections into the cloud
- High BW and deterministic QoS not needed
- Ideal for lab environments and smaller workloads
- Must always cautious of egress charges



Cloud OnRamp Multicloud



Cisco SD-WAN Cloud OnRamp (IaaS)



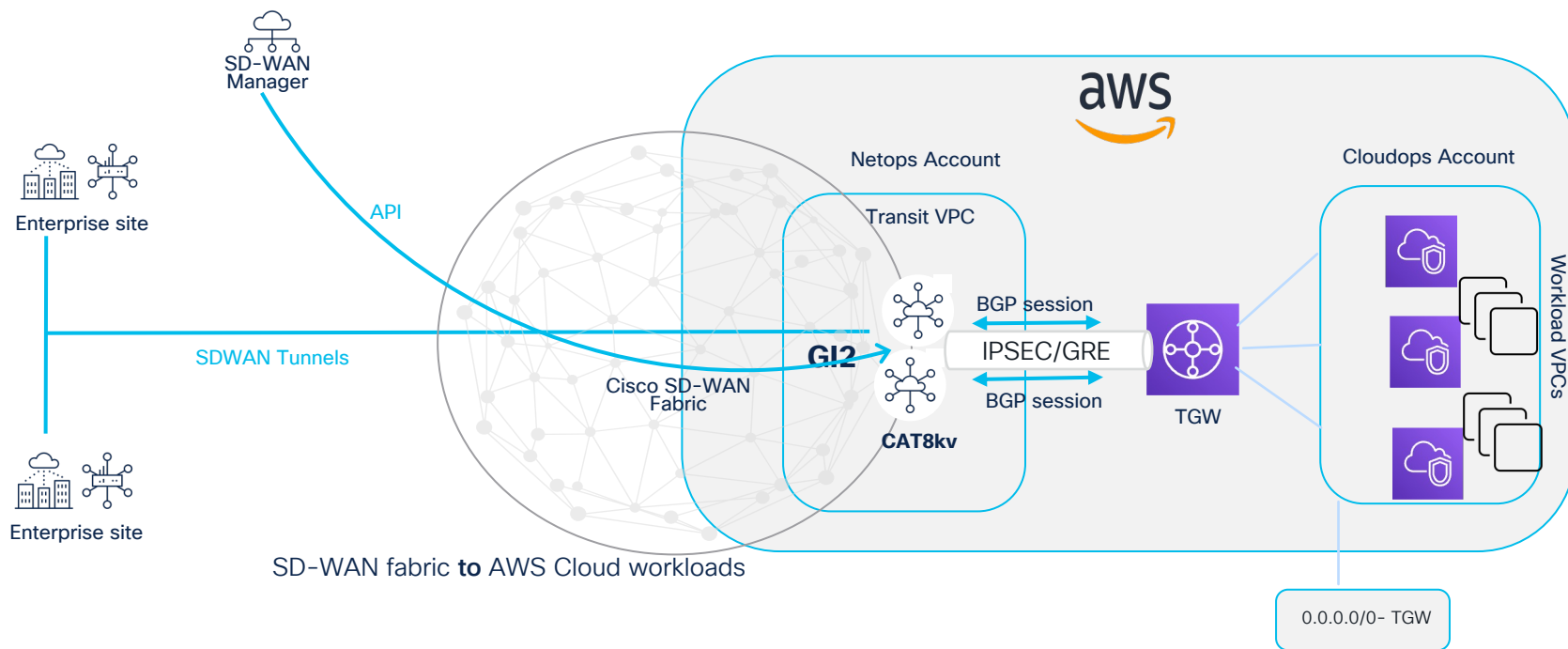
Key Advantages

- Provides a “shrink wrapped” automation solution for extending Cisco SD-WAN into the public cloud providers
- Offers global presence, automation
- Establishes the foundation for:
 - Site to Site
 - Site to Cloud
 - Region to Region
 - Cloud to Cloud (multicloud)
- Offers the ability to leverage the cloud provider global infrastructure as a transport option cloud to cloud

Deployment Targets

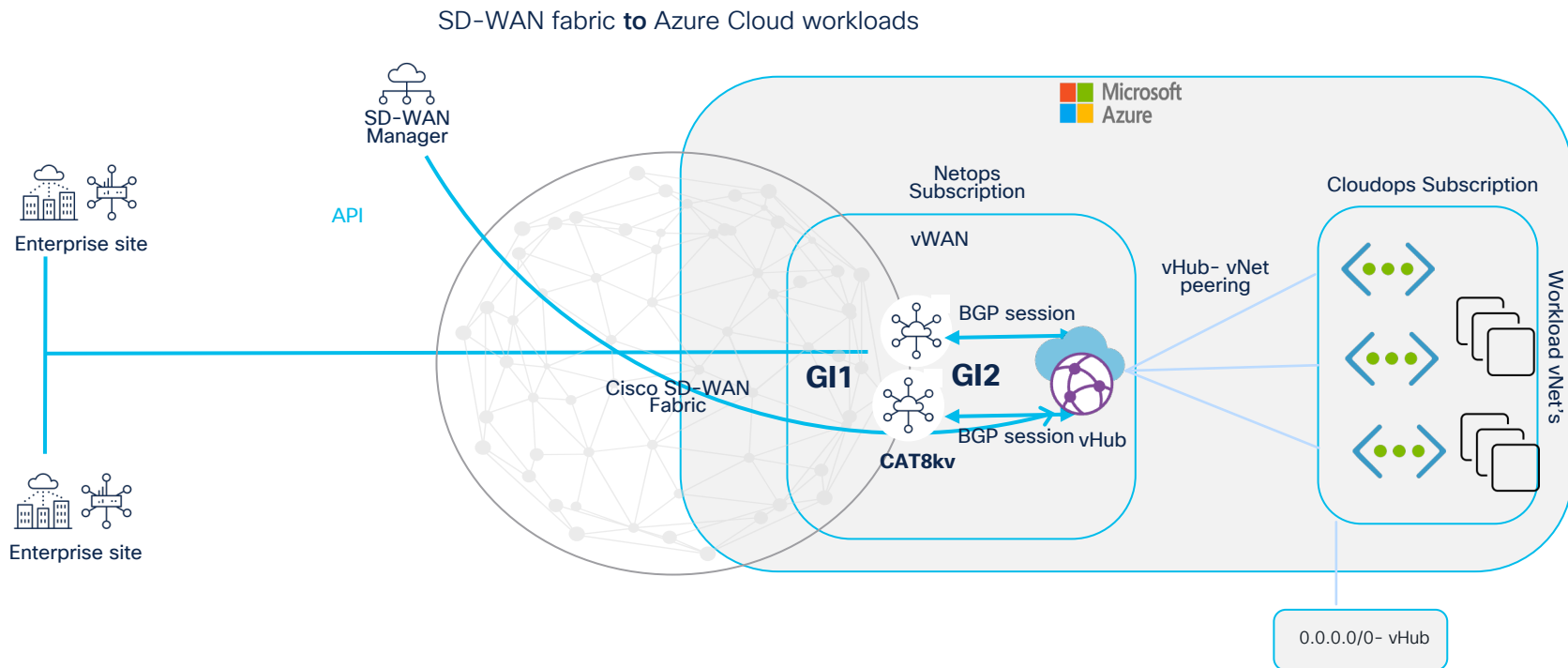
- Already operating and own SD-WAN
- Extends visibility vantage point into the public cloud for network operations
- Automation and (Infra as Code) direction for operations
- Sets table for Multicloud transition

Example: AWS - Site-to-Cloud



- GRE adds 4x the BW improvement using Connect to TGW from Catalyst 8000v
- If needed, Cat8000v can drive to 30Gbps throughput (c5n.18xlarge) @ 1400B packets

Example: Azure - Site-to-Cloud

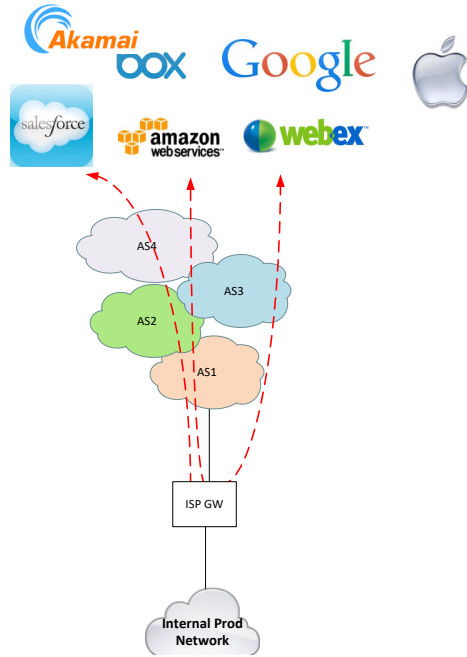
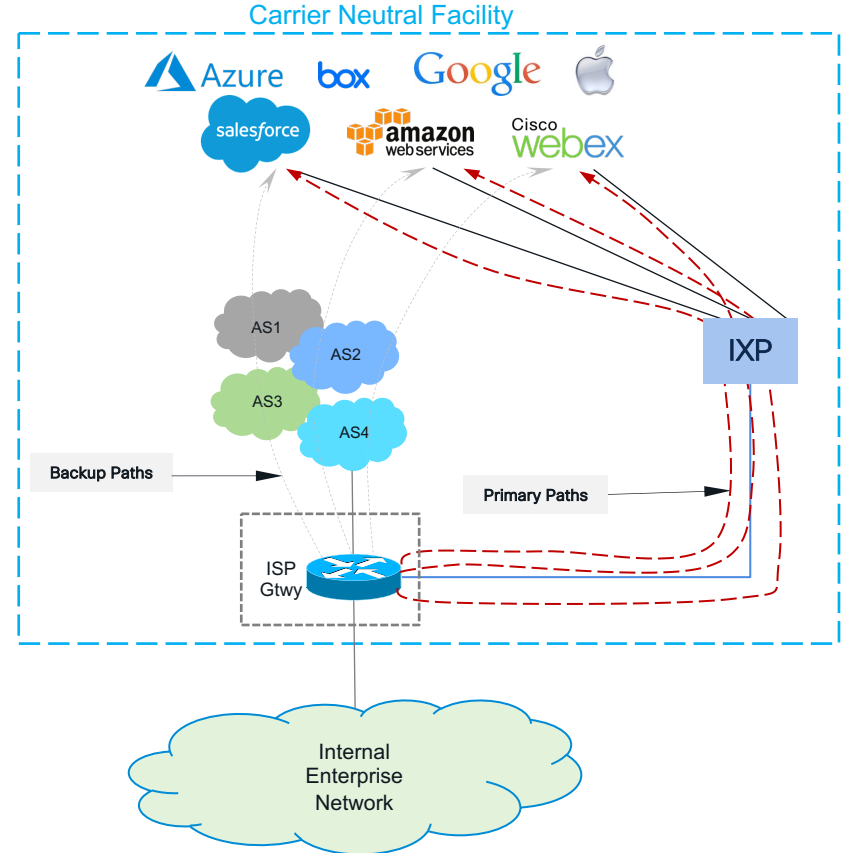


CAT8k Network virtual appliances are hosted in vhub, running BGP to vHub control plane to learn vNet mapping

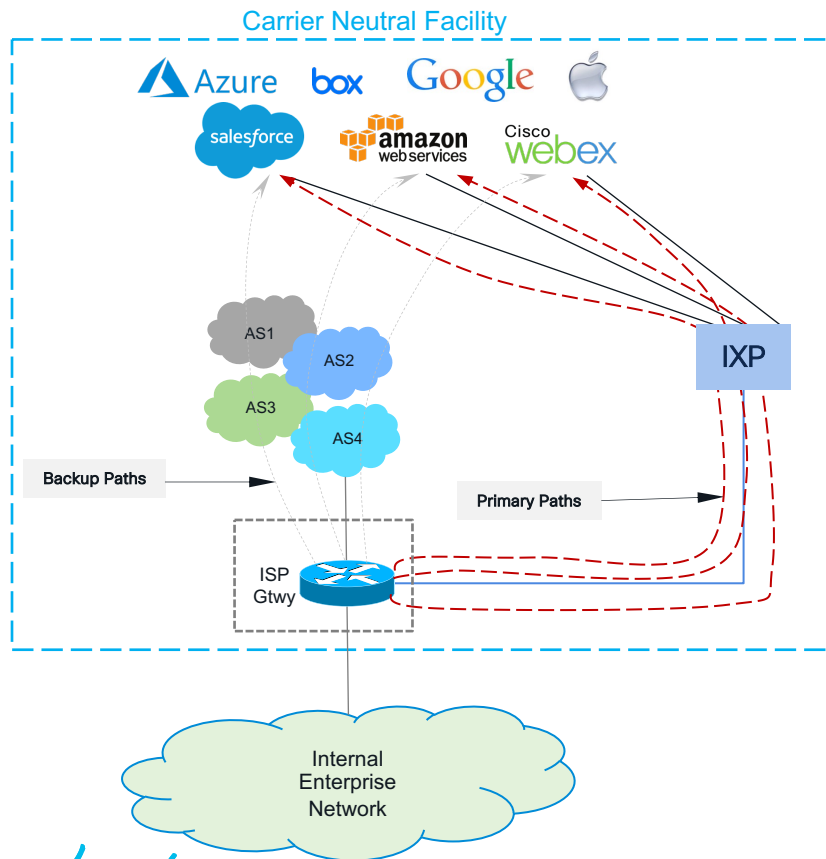
Public Connection to the Cloud

High Speed Peering
Agreements with Cloud
Providers

Customer Use Case – Enterprise to Public Cloud



Enterprise to Public Cloud Peering - Summary



Key Advantages

- Provides a high speed “front door” access to the public cloud
- More cost effective than a private link (backdoor) service
- Ideal if customer has carrier neutral facility presence
- While not SLA based, direct peering provides better assurance of performance
- Can leverage ISP peering for backup

Deployment Targets

- Ideal solution if enterprise already resides in the cloud provider CNF partner site
- Enterprise requires high speed access into the public cloud but does not want the private link cost (i.e., Direct Connect, Express Route)

Cisco Systems, Inc.

Organization	Cisco Systems, Inc.
Also Known As	Cisco
Long Name	
Company Website	http://www.cisco.com
ASN	109
IRR as-set/route-set	AS-CISCO
Route Server URL	
Looking Glass URL	
Network Type	Enterprise
IPv4 Prefixes	100
IPv6 Prefixes	5
Traffic Levels	Not Disclosed
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	☒ Unicast IPv4 ☐ Multicast ☐ IPv6 ☐ Never via route servers
Last Updated	2023-08-10T13:45:41Z
Public Peering Info Updated	2022-04-27T20:57:18
Peering Facility Info Updated	2022-02-25T22:03:24
Contact Info Updated	2022-12-15T15:52:36

Notes	<p>Overview: Cisco Systems (AS109) provides connectivity for Cisco's corporate network and cisco.com based Internet services. Cisco is actively expanding its peering footprint globally across Europe, North America, and Asia Pacific. At this time a selective peering policy has been chosen where Cisco will limit the number of bilateral peers. Cisco will not be peering through exchange route servers.</p> <p>General Terms:</p> <ul style="list-style-type: none"> Peering agreements will be reviewed yearly to ensure traffic requirements are maintained. Cisco reserves the right to modify this policy at any time without notice. Compliance with the terms of this policy does not guarantee a peering relationship with Cisco. This policy is a guideline and Cisco may refuse peering for any reason without disclosure. Peering may be temporarily or permanently disconnected by either party for any reason. Cisco and Requester agree not to abuse the peering relationship. Examples of abusive behavior are, but are not limited to: static routes, default routes, improper filtering, and willfully sending malicious traffic. <p>Guidelines and Requirements:</p> <ul style="list-style-type: none"> Cisco shall maintain accurate contact information and POP residence at peeringdb.com
-------	--

Public Peering Exchange Points

Exchange ⌵	ASN	Speed	RS Peer
IPv4	IPv6		
AMS-IX 80.249.211.50	109 2001:7f8:1::a500:109:1	10G	☐
Equinix Ashburn 206.126.237.85	109 2001:504:0:2::109:1	20G	☐
Equinix Dallas 206.223.118.166	109 2001:504:0:5::109:1	10G	☐
Equinix Dallas 206.223.118.167	109 2001:504:0:5::109:2	10G	☐
Equinix San Jose 206.223.116.53	109 2001:504:0:1::109:1	20G	☐
Equinix Singapore 27.111.228.194	109 2001:de8:4::109:1	10G	☐
Equinix Sydney 45.127.172.226	109 2001:de8:6::109:1	10G	☐
Equinix Tokyo 203.190.230.90	109 2001:de8:5::109:1	10G	☐
LINX LON1 195.66.227.143	109 2001:7f8:4::6d:1	10G	☐

Interconnection Facilities

Facility ⌵	Country
ASN	City
Asia Tone Shanghai 109	China Shanghai
CoreSite - Los Angeles (LA1) One Wilshire 109	United States of America Los Angeles
CoreSite - San Jose (SV1) 109	United States of America San Jose
Equinix AM1/AM2 - Amsterdam, Luitenbergweg 109	Netherlands Amsterdam
Equinix DA1 - Dallas 109	United States of America Dallas
Equinix DC1-DC15, DC21 - Ashburn 109	United States of America Ashburn
Equinix LD8 - London, Docklands 109	United Kingdom London
Equinix NY9 - New York, 111 8th Avenue 109	United States of America New York
Equinix SG1 - Singapore 109	Singapore Singapore

- Where can I peer to cloud SaaS and IaaS providers?
- Who's at the Carrier Neutral Facility?

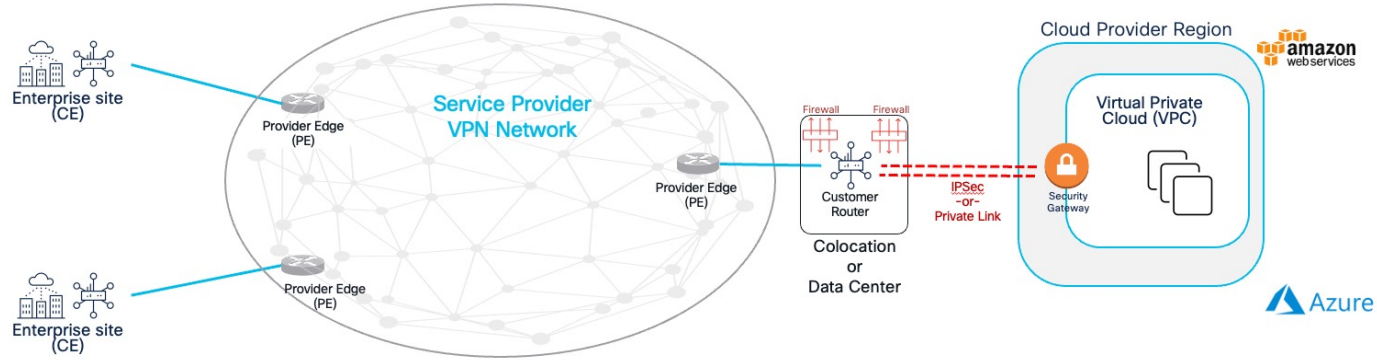
Peeringdb.com

Private Connection to the Cloud

Private Access to Cloud via
Private IP VPN Service

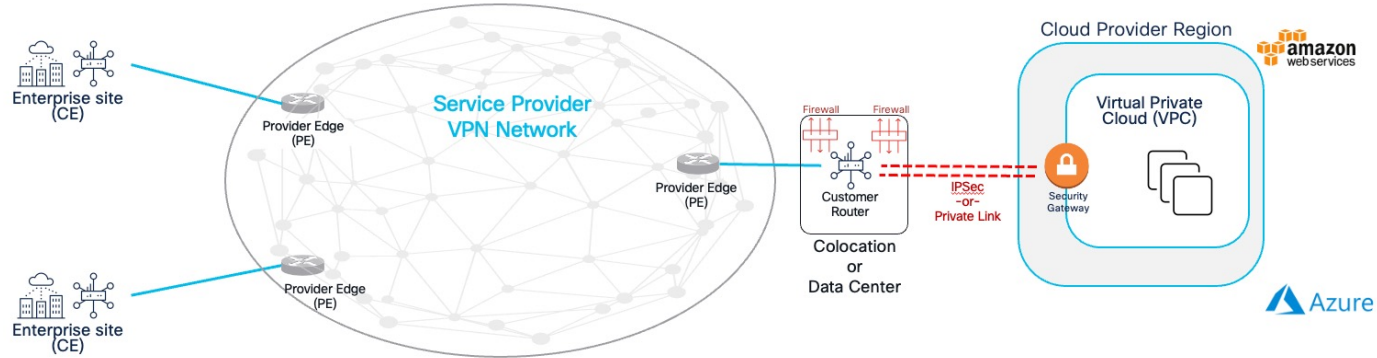
IP VPN Service Connectivity to the Public Cloud

Manual Extension

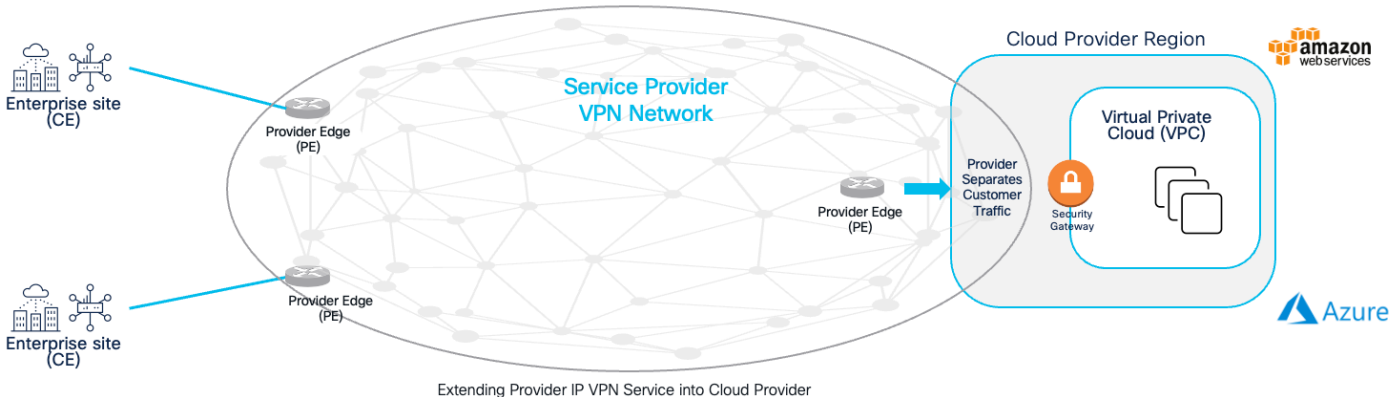


IP VPN Service Connectivity to the Public Cloud

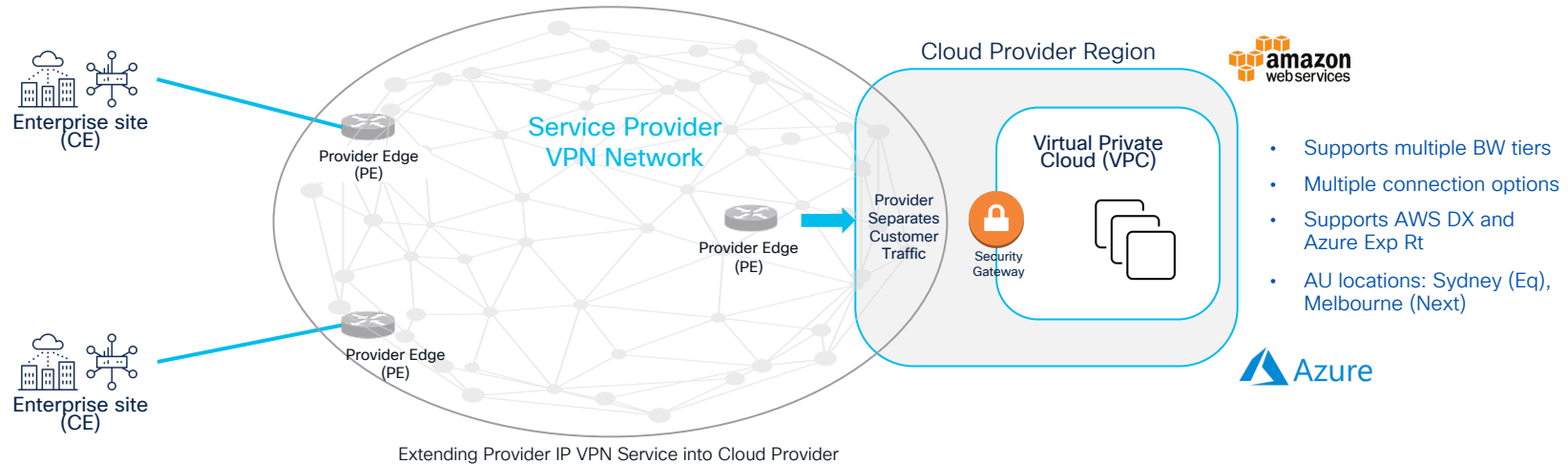
Manual Extension



IP VPN Extension



IP VPN Service Connectivity to the Public Cloud



Key Benefits

- Ideal integration with “SD-WAN Multicloud” overlay
- Leverage existing secure IP VPN transport (if utilized today)
- Leverage existing transport SLA’s in place, to public cloud
- Reduced complexity for connections into public cloud
- AU Provider offerings: Telstra, Optus

CISCO *Live!*

Deployment Targets

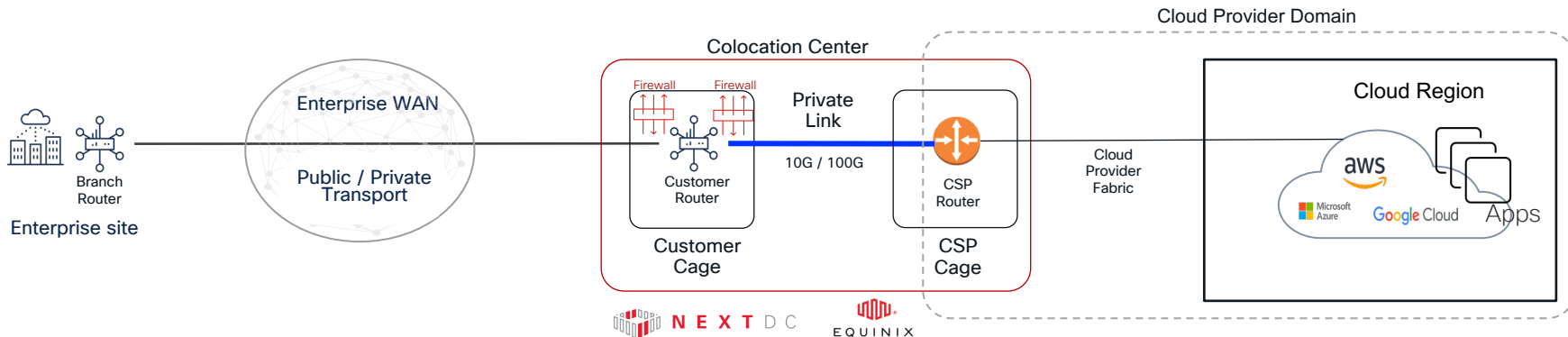
- Optimal option if already leveraging service provider IP VPN service
- Provides SLA based transport service to cloud
- Reduces the manual complexity needed for public cloud connectivity
- **Option: Cisco SD-WAN OnRamp over top**

Private Connection to the Cloud

Private High Speed Direct
Connections to the Cloud
Provider (back door access)

Private Link Service to Public Cloud Provider

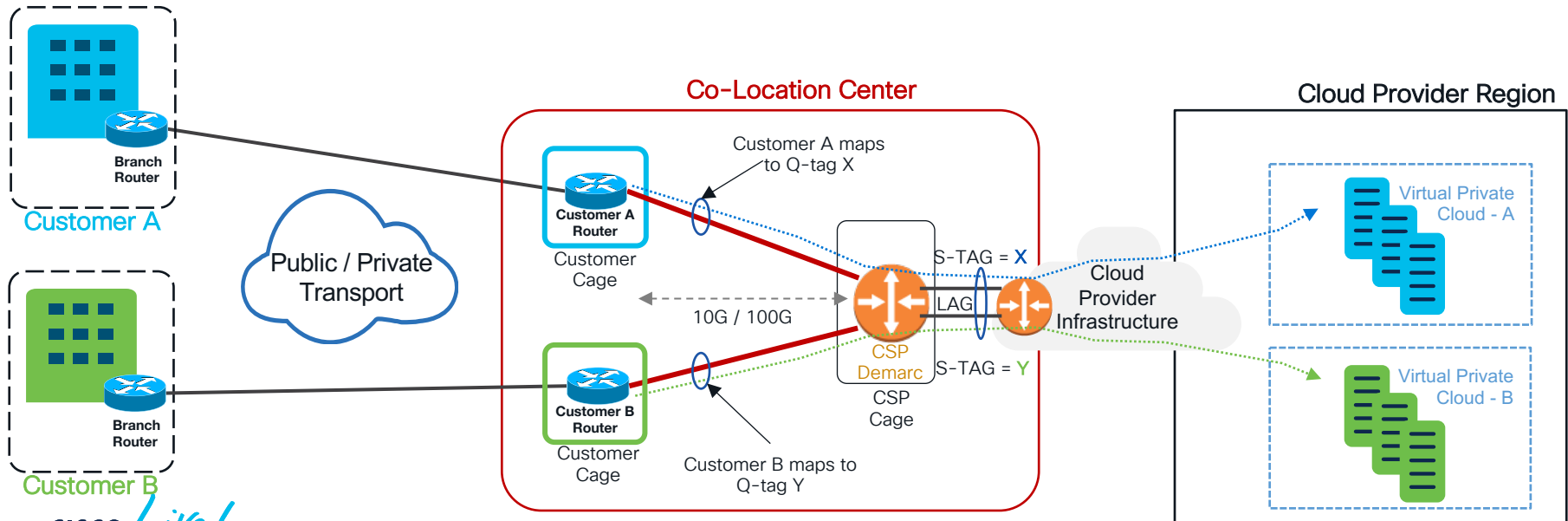
- Offers high speed dedicated (10G, 100G) and (sub-rate) private link options
- Targets those customers wanting dedicated BW and deterministic network behavior into, and from, their cloud hosted workloads
- Dedicated assumes customer has presence (or access into) in CoLo partner space
- CSP provides an extensive list of partners, locations, details of capabilities, redundancy options, and speeds



Private Link Service to Public Cloud Provider

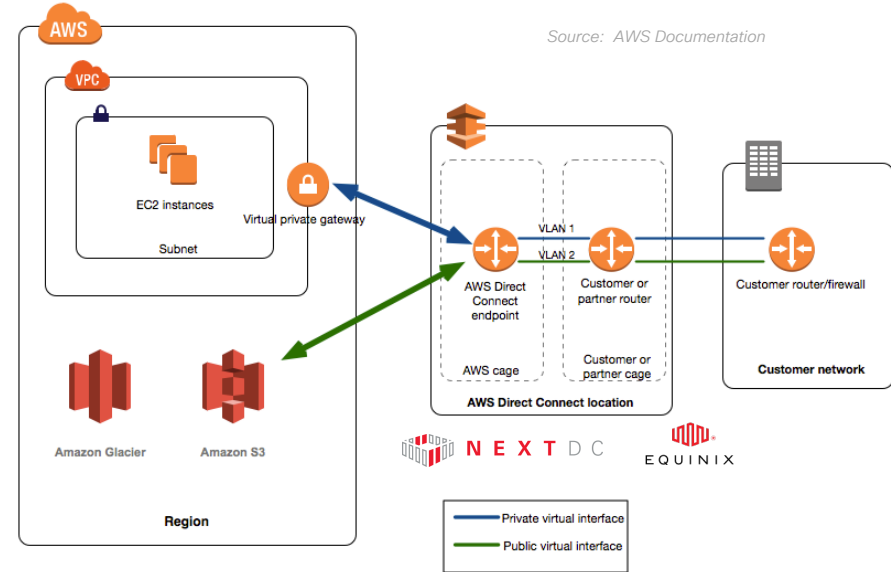
Anatomy of the Service

- CSP separates customer traffic through use of 802.1Q tags through a Virtual Interface (VIF)
- The VIF controls customer (tenant) and access (public / private) to services within the CSP
- Customer traffic remains completely segmented from each tenant



Example: AWS Direct Connect (DX)

- **Dedicated connection** between the enterprise and AWS
- Provides (1) **private peering to VPCs** and (2) **public peering to AWS public services (AWS S3, Glacier)**
 - Sub-interface on corporate DC router for each service
 - BGP peering for route exchange for each service
- 10G and 100G dedicated connections; sub-1G connections available via partners
- Multiple accounts can share a connection
- Multiple connections for redundancy
- BFD for fast failure detection and failover
- Data-in is free, data-out is cheaper (compared to Internet)

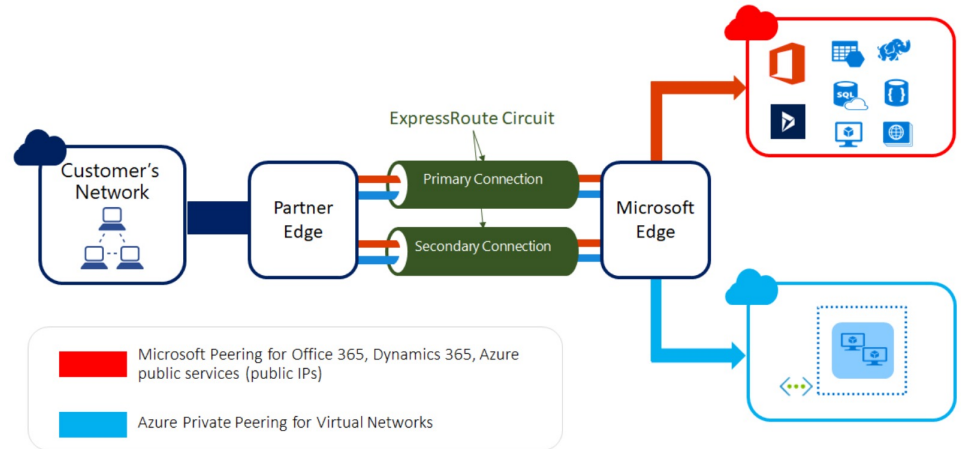


Example: Azure ExpressRoute Direct



- **Dedicated connection** between the enterprise and Azure
- BGP peering for route exchange for each service
- 10G and 100G dedicated connections
- Supports active/active at scale
- Other ExpressRoute connection options exist aligned with SP and connection partners

Source: Azure Documentation



Source: <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models#Direct>

How Do I Secure My High-Speed Private Links into the Public Cloud Providers?

Encrypting ExpressRoute for improved security

MACsec

Let's start with MACsec as this solution can only apply to ExpressRoute Direct. With ExpressRoute Direct, customers establish a layer 2 private connection from their edge to Microsoft Enterprise Edge in Azure. Once you have connectivity at layer 1, your layer2 is setup which allows you to then create logical ExpressRoute circuits on top of that. MACsec or Media Access Control Security, encrypts traffic from the customers edge to the Microsoft Enterprise Edge using a set of secrets which can be kept in Azure Key Vault for safe keeping.

MACsec for Cloud Interconnect overview



MACsec for Cloud Interconnect helps you secure traffic on Cloud Interconnect connections, specifically between your on-premises router and Google's edge routers. MACsec for Cloud Interconnect uses IEEE standard [802.1AE Media Access Control Security \(MACsec\)](#) to encrypt traffic between your on-premises router and Google's edge routers.

MACsec for Cloud Interconnect doesn't provide encryption in transit within Google. For stronger security, we recommend that you use MACsec with other network security protocols, such as IP Security (IPsec) and Transport Layer Security (TLS). For more information about using IPsec to secure your network traffic to Google Cloud, see the [HA VPN over Cloud Interconnect overview](#).

MACsec for Cloud Interconnect is available for 10-Gbps and 100-Gbps circuits. However, to order MACsec for Cloud Interconnect for 10-Gbps circuits, you must contact your account manager.

AWS Direct Connect Announces MACsec Encryption for Dedicated 10Gbps and 100Gbps Connections at Select Locations

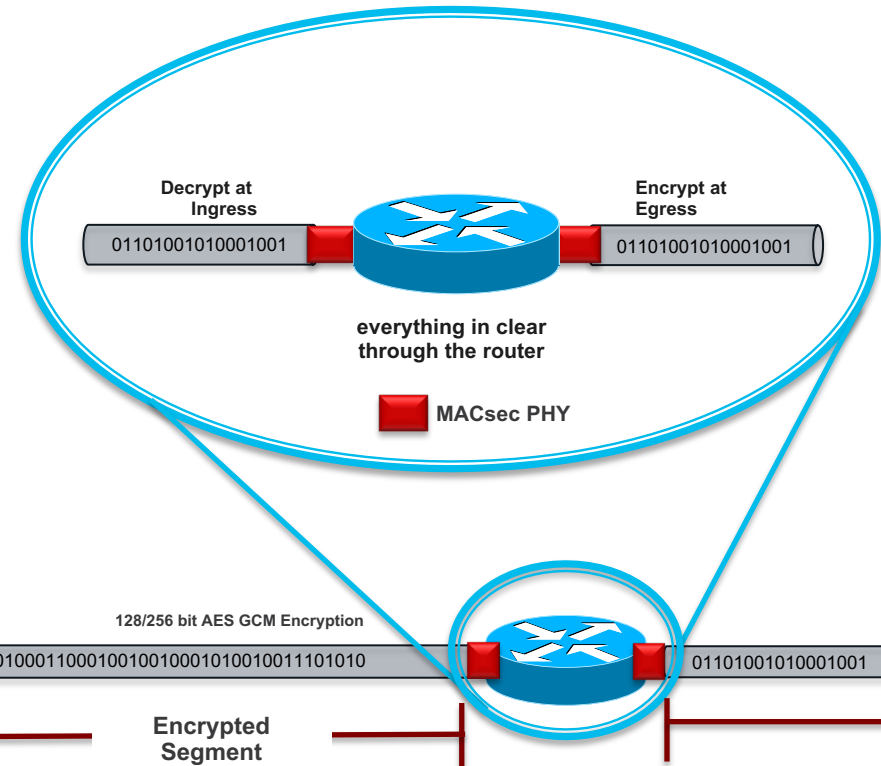
Posted On: Mar 31, 2021

AWS Direct Connect now offers IEEE 802.1AE MAC Security Standard (MACsec) encryption for 10Gbps and 100Gbps Dedicated Connections at select locations to secure your high-speed, private connectivity to the cloud.

What is MAC Security (MACsec)?

Hop-by-Hop Encryption via IEEE 802.1AE

- Hop-by-Hop Encryption model
 - Packets are **encrypted on egress port (MACsec PHY)**
 - Packets are **in the clear through the device**
 - Packets are **decrypted on ingress port (MACsec PHY)**
- Supports 1/10/40G, 100G, and 400G encryption
- Data plane (IEEE 802.1AE) / control plane (IEEE 802.1x-Rev) support PSK or PKI, standards based
- Transparent to Layer-3 (IPv4/v6, SR, MPLS, multicast, routing protocols, etc.)
- Encryption aligns with Link PHY speed (Ethernet)



WAN MACsec: Top Enterprise and SP Use Cases

Use Case	Applicability	Transport
Metro E - Branch Router Back-haul *	Encryption requirements exceed IPSec capabilities, leverage .1Q-tag-in-clear at Hub Site *	E-LINE E-LAN
High Speed Data Center Interconnect (DCI)	Targets 10/ 40/100Gbps DC interconnect links for storage replication and workload movement	E-LINE optical/fiber
MPLS Core / Edge Links Security	Encrypt all PE-P, P-P links inside of an MPLS backbone. Allows transparency of MPLS labels, TE, Segment Routing, etc...	E-LINE optical/fiber
Secure Metro Ethernet Service Offering	Service Provider option for offering “secure” Metro E services to end customers	E-LINE E-LAN
Hybrid MACsec and IPSec Design	Position MACsec in high-speed core, and IPSec for high-volume sites, lower speed	E-LINE/E-LAN/IPSec
Encrypt High Speed Private Link Services into Public Cloud Providers (CSP)	Leverage MACsec to protect 10/100G private link offers into the CSP infrastructure	E-LINE

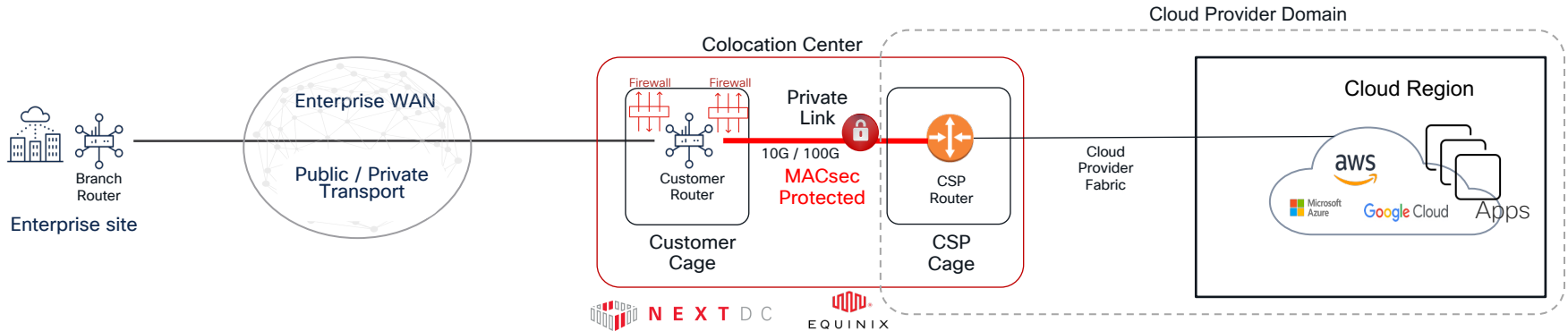
* Requires Cisco WAN MACsec

Securing High Speed Private Links to the Cloud using MACsec

Cloud Provider Secure Private Link Access

Using MACsec Encryption (10/100G)

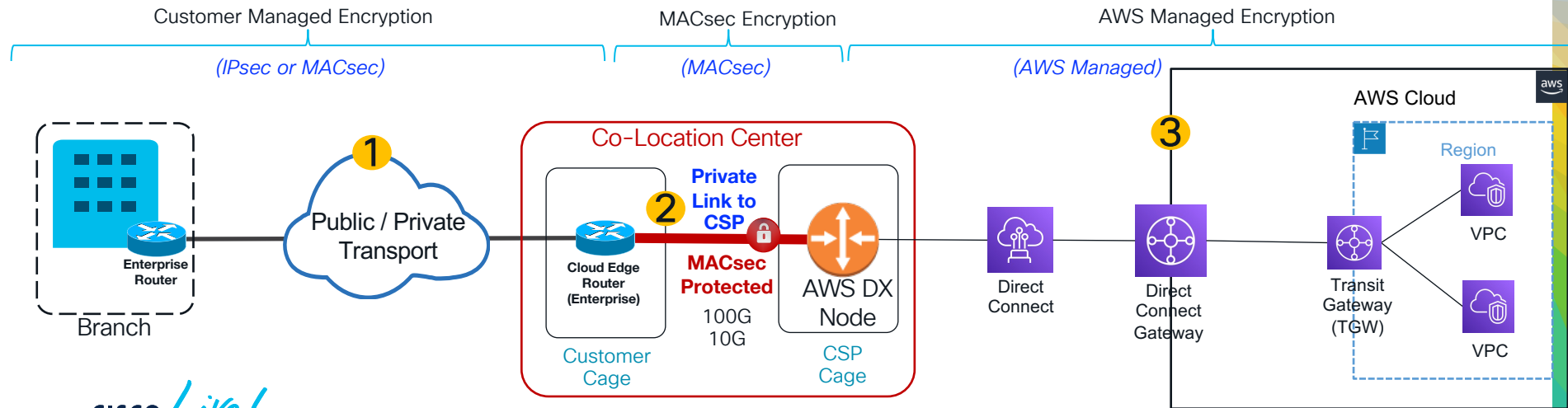
- Options exist from major CSP's to support MACsec to encrypt data from private network to CSP
- Offers high speed (10G, 100G) dedicated private link options (not supported over "hosted")
- Targets those customers wanting dedicated BW and encryption over private link
- Assumes customer has presence (or access into) in CoLo space
- CSP's provide list of partners, locations, details of capabilities and speeds offered with MACsec



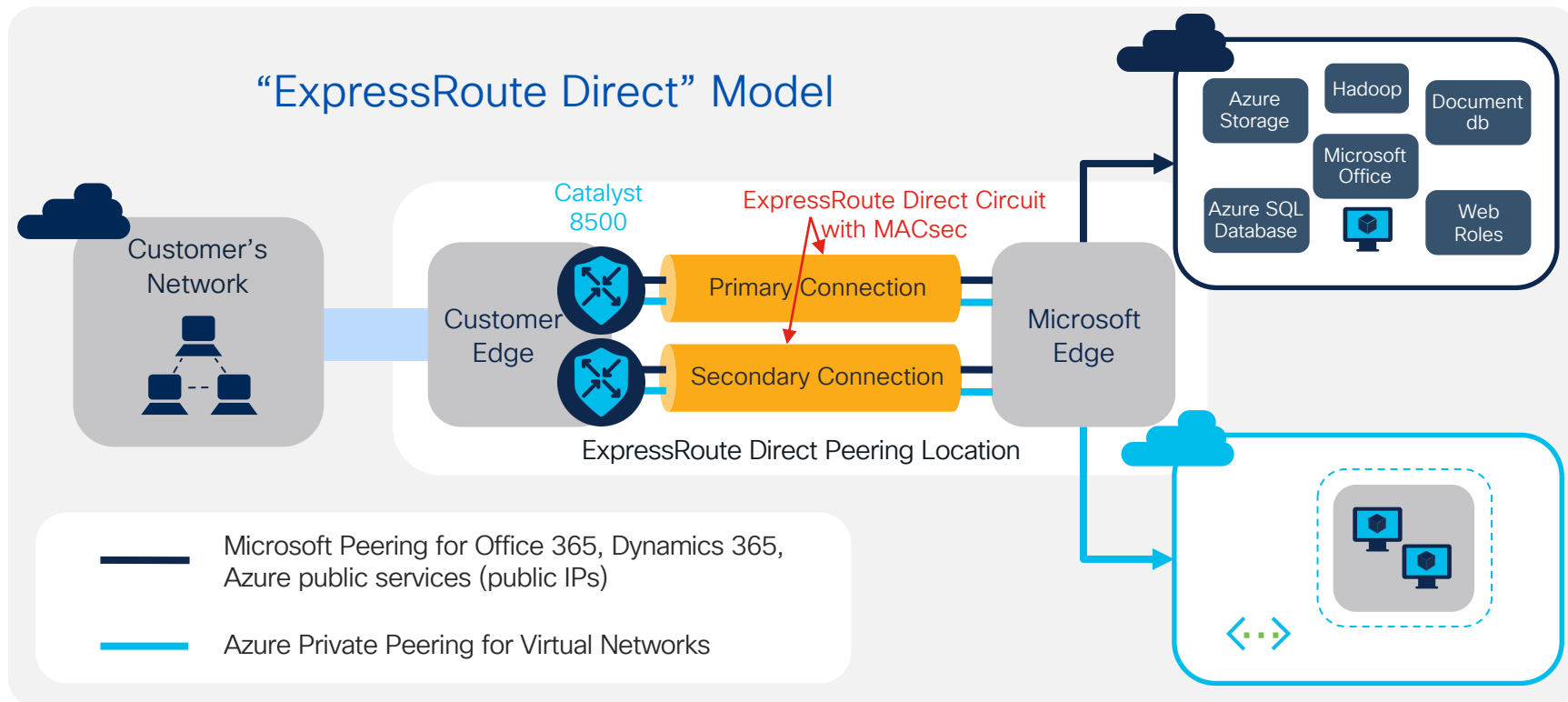
AWS Example: Private Link using MACsec Protection



- 1 Enterprise manages their own encryption into the Colocation Center
- 2 MACsec encryption is used between Customer-owned Edge → AWS DX Node
- 3 CSP (AWS example) provides selected encryption (varies within each CSP) from the DX Node (in CoLo) out to their cloud data center and within their infrastructure



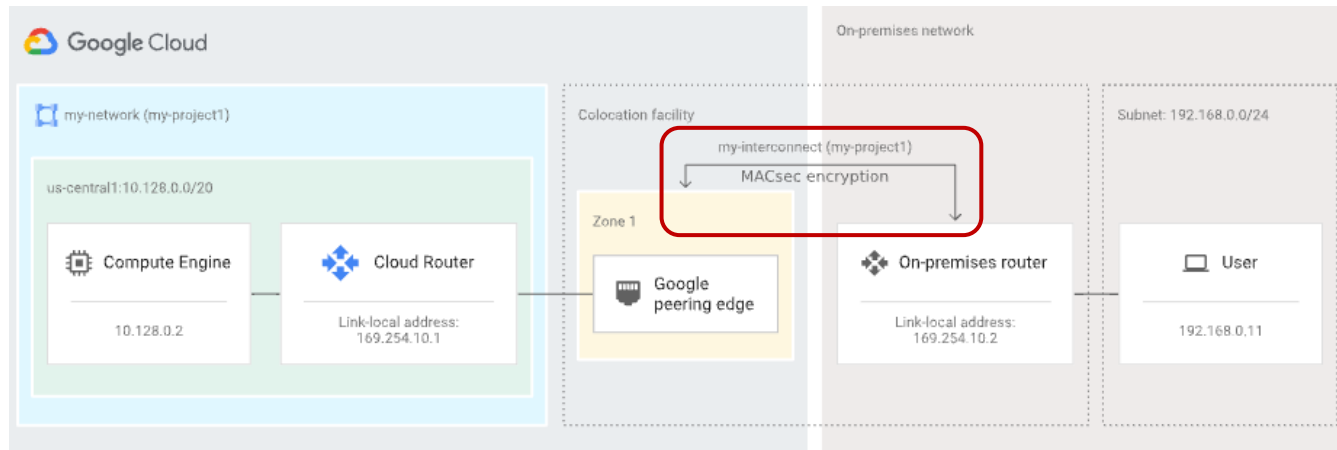
Azure Example: Private Link using MACsec Protection



Google Example: Private Link using MACsec Cloud Interconnect



- Enterprise manages their own encryption into the Colocation facility
- MACsec encryption is used between Customer-owned Edge → Google Peering Edge
- Supports 10Gb and 100Gbps connections
- Multiple options exist for customer residing in colocation (shown) and leverage a partner interconnection between Google peering and partner SP



Example: AWS Direct Connect with MACsec (Asia Pac)

AWS Direct Connect Location.	Also accessible from:	Associated AWS Region	1G	10G	100G
• Equinix HK1, Tsuen Wan N.T., Hong Kong SAR		Asia Pacific (Hong Kong)	✓	✓M	✓M
• Equinix SG2, Singapore		Asia Pacific (Singapore)	✓	✓M	✓M
• Global Switch, Singapore		Asia Pacific (Singapore)	✓	✓M	✓M
• Equinix ME2, Melbourne, Australia	Equinix ME1, Melbourne	Asia Pacific (Melbourne)	✓	✓M	✓M
• Equinix SY3, Sydney, Australia	Equinix SY1 - SY4, Sydney.	Asia Pacific (Sydney)	✓	✓M	✓M
• NEXTDC S2, Sydney, Australia		Asia Pacific (Sydney)	✓	✓M	✓M
• AT Tokyo CC1 Chuo Data Center, Tokyo, Japan		Asia Pacific (Tokyo)	✓	✓M	✓M
• Equinix TY2, Tokyo, Japan	Equinix TY2, TY6 - TY8, Tokyo	Asia Pacific (Tokyo)	✓	✓M	✓M

Link: <https://aws.amazon.com/directconnect/locations/>

M = MACsec

Securing Private Links to the Cloud using MACsec

Configuration Examples
(IOS-XE)

Router Configuration “step” Requirements

MACsec Configurations

1. Key Chain Setup (Pre Shared Key example)
 2. MKA Policy
 3. Interface Configuration
 4. Expected output from “show commands”
-
- Preliminary Port-channel configuration (optional)

AWS Example – MACsec Recommendations

Parameter	Description
CKN length	This is a 64-hexadecimal character (0-9, A-E) string. Use the full length to maximize cross-platform compatibility.
CAK length	This is a 64-hexadecimal character (0-9, A-E) string. Use the full length to maximize cross-platform compatibility.
Cryptographic algorithm	AES_256_CMAC
SAK Cipher Suite	<ul style="list-style-type: none">For 100 Gbps connections: GCM_AES_XPN_256For 10 Gbps connections: GCM_AES_XPN_256 or GCM_AES_256
Key Cipher Suite	16
Confidentiality Offset	0
ICV Indicator	No
SAK Rekey Time	PN Rollover>

Key and MKA Policy Configuration

```
key chain KEY_1 macsec
description MACsec Link to AWS
key 01
  cryptographic-algorithm aes-256-cmac
  key-string 0123456789012345678901234567890123456789012345678901234567890123
  lifetime 00:00:00 Jan 1 2022 infinite
!
mka policy aws-test
  key-server priority 10
  macsec-cipher-suite gcm-aes-xpn-256
  sak-rekey interval 3600
  ssci-based-on-sci
!
```

MACsec 64 hexadecimal
key configuration

MKA Policy with XPN
Cipher configuration,
key-server priority
should be non-zero

Important config to interop
using XPN cipher with remote
end MACsec SCI capabilities

Interface Configuration

```
interface HundredGigE0/1/0
```

```
mtu 9216
```

```
no ip address
```

```
ip mtu 9184
```

```
negotiation auto
```

```
mka policy aws-test
```

```
mka pre-shared-key key-chain KEY_1
```

```
macsec access-control should-secure
```

```
macsec replay-protection window-size 512
```

```
macsec
```

```
channel-group 5
```

```
end
```

IP MTU is MTU minus
32B (MACsec header
overhead)

Attach MACsec Policy
and Key Configuration

Expected Window size
based on remote end
configuration

Enables MACsec on the
interface

Configure port-
channel Member
for Po5

100G MACsec Direct Connect (DX) Verification

```
C8500-12X4QC-2#show mka sessions interface Hu0/1/0
```

Summary of All Currently Active MKA Sessions on Interface HundredGigE0/1/0...

Interface Port-ID	Local-TxSCI Peer-RxSCI	Policy-Name MACsec-Peers	Inherited Status	Key-Server CKN
Hu0/1/0 24	f04a.022a.dec4/0018 a0b4.39b6.e684/0001	aws-test 1	NO Secured	NO 01

MACsec session should
be in Secured state

Correct Key (CKN) and
MACsec Policy should be
applied as per config.

```
C8500-12X4QC-2#
```

100G MACsec DX Verification

```
C8500-12X4QC-2#sh macsec status interface Hu0/1/0
```

Capabilities:

Ciphers Supported: GCM-AES-128 GCM-AES-256 GCM-AES-XPB-128 GCM-AES-XPB-256
Cipher: GCM-AES-XPB-256
Confidentiality Offset: 0
Replay Window: 512
Delay Protect Enable: FALSE
Access Control: should-secure
Include-SCI: TRUE

Correct cipher should be applied as per config.

Transmit SC:

SCI: F04A022ADEC40018

Transmitting: TRUE

Transmit SA:

Next PN: 2

Delay Protect AN/nextPN: NA/0

Receive SC:

SCI: A0B439B6E6840001

Receiving: TRUE

Receive SA:

Next PN: 18

AN: 0

Delay Protect AN/LPN: 0/0

```
C8500-12X4QC-2#
```

Azure ExpressRoute Examples

Azure ExpressRoute Examples

Reference Session (from CLUS 2022):

BRKENT-2809: Untangle Enterprise Direct Cloud Connectivity with Powerful Catalyst 8500 Series Edge Platforms

Link: <https://www.ciscolive.com/on-demand/on-demand-library.html?search=2809#/session/1655479484932001IRuX>

Extending Encryption into the Cloud Provider

Design Options

Extending Enterprise Network Encryption Into the Cloud Provider Infrastructure

Public Access

- Public Internet
- Public Internet Peering Option

Private Link

- **Trusted:** Encryption option for private link service (DX, ExpressRoute) into CSP **meets the security compliance requirements** for the enterprise standards
- **Un-Trusted:** Encryption option for private link service (DX, ExpressRoute) into the CSP **does NOT meet the security compliance requirements** for the enterprise standards
 - To comply, encryption by enterprise is extended further into the cloud providers infrastructure

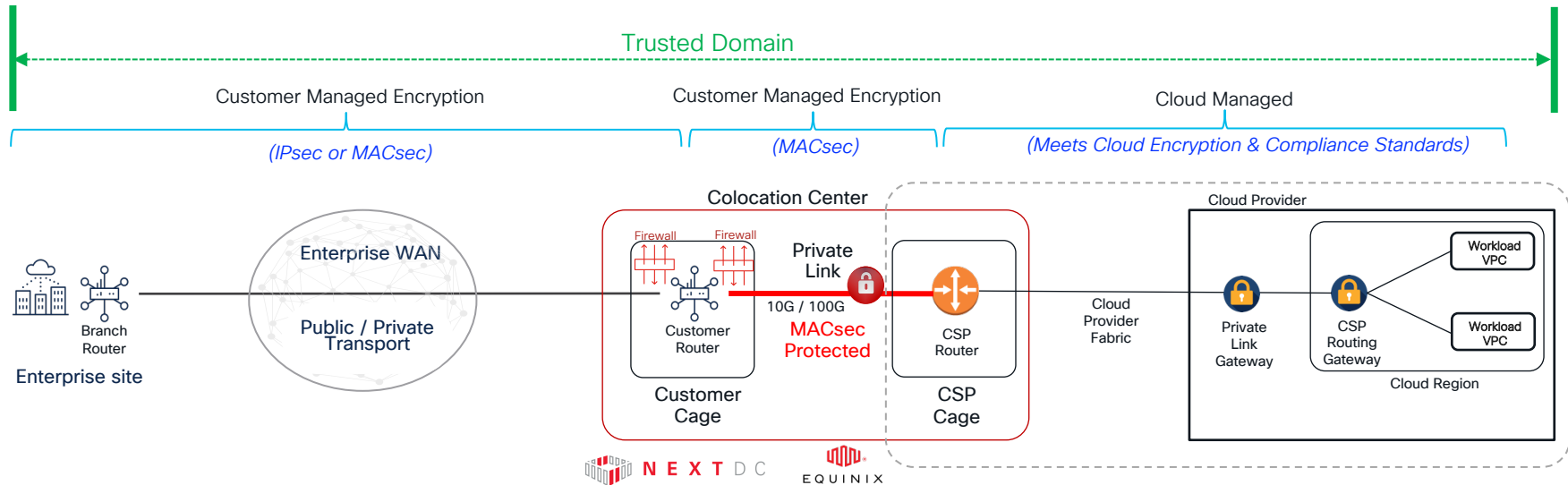
Compliance will vary per Customer based on required business policies and standards

Private Link – Trusted – End to End:

Private Link using MACsec Protection

- Private WAN from the branch encryption options (IPSec, MACsec) controlled by the enterprise
- MACsec leveraged over private link to the cloud provider

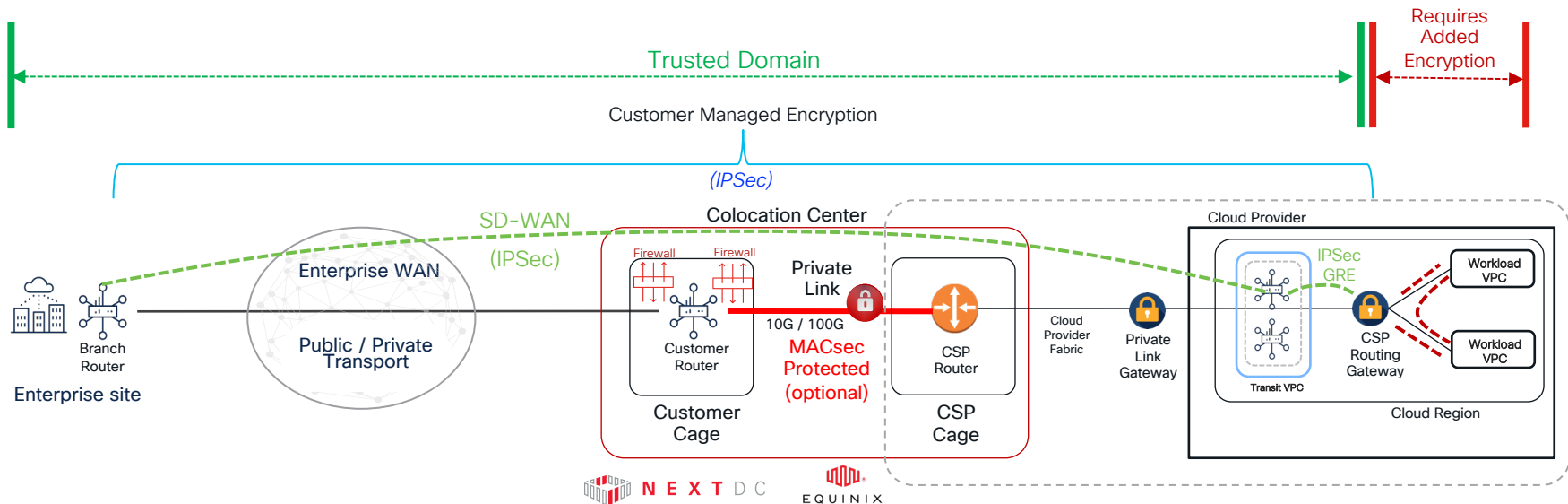
Summary: Cloud provider infrastructure, with MACsec private link encryption, assumed secure that would meet some enterprise/government security and compliance policy requirements



Private Link - Un-Trusted - Option 1: Cisco SD-WAN Multi Cloud (MACsec Optional)

- Private WAN from the branch encryption options (IPSec, MACsec) controlled by the enterprise
- Enterprise controls encryption, via secure SD-WAN fabric, from branch (IPSec/GRE) to Routing Gtwy in CSP
- Routing Gtwy to workload VPC's in clear (by default). Methods to encrypt vary and evolving

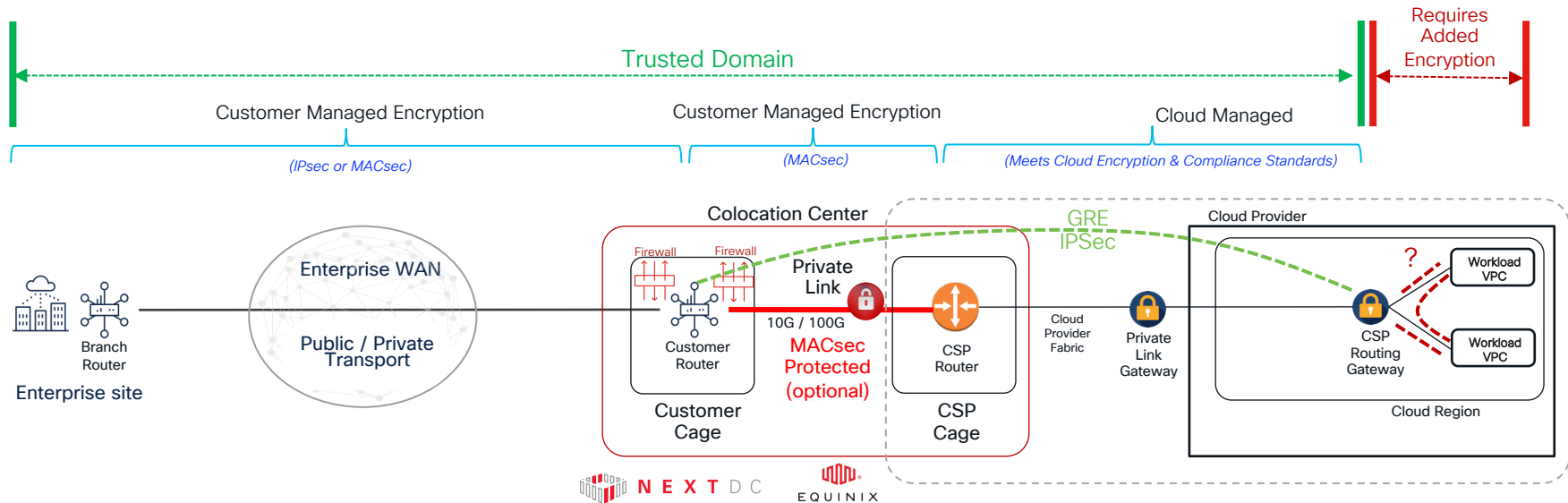
Summary: Enterprise security and compliance policies will dictate “encryption domain”



Private Link - Un-Trusted - Option 2: Encrypted Peering: IPSec + GRE (MACsec Optional)

- Private WAN from the branch encryption options (IPSec, MACsec) controlled by the enterprise
- Encryption controlled by the enterprise from branch, through CoLo, to Routing Gtwy in the CSP
- Routing Gtwy to workload VPC's in clear (by default). Methods to encrypt vary and evolving

Summary: Enterprise security and compliance policies will dictate “encryption domain”



Summary and Caveats

- Important to align enterprise and compliance policies with encryption capabilities into the cloud
- Each cloud provider will vary how they encrypt internally and extend how far
- Requirements for encryption will vary per customer based on these policies
- WAN back-haul within the enterprise, to the CoLo, and extended into the cloud (“Un-Trusted” Option #1 and #2) are all enterprise controlled
- Solutions to encrypt to/between the workload VPC’s continue to evolve

Visibility Options into the Cloud Providers

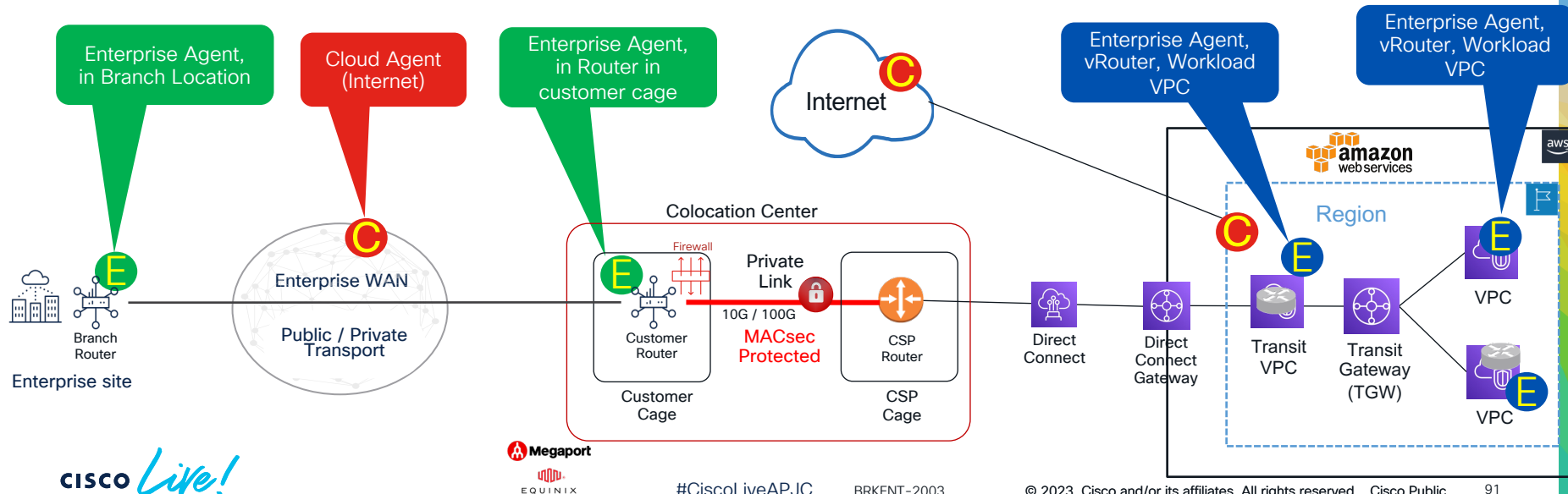
ThousandEyes Visibility End to End

Private/Public Link and Cloud Visibility



- Private link through the CoLo and into the cloud provider presents areas of “dark” visibility
- ThousandEyes offers several advantages for visibility in the WAN and cloud, including:
 - Global Visibility from Branch (last mile) into CoLo, private agents on network devices can extend into private space in the public cloud, and IaaS “native” agents (automated via AWS CloudFormation)

- C** Thousand Eyes – Cloud Agent
- E** Thousand Eyes – ENT Agent
- E** Thousand Eyes – Native AWS – ENT Agent



AWS Network Path Enrichment

What problem is this solving?

- Like the Internet, the public cloud presents blind spots for network operators

What areas were enhanced?

- ThousandEyes worked with the AWS team, who provided enhanced information
- The solution helps customers identify which nodes the traffic is traversing within the AWS network, identify the types of services and report on the performance.

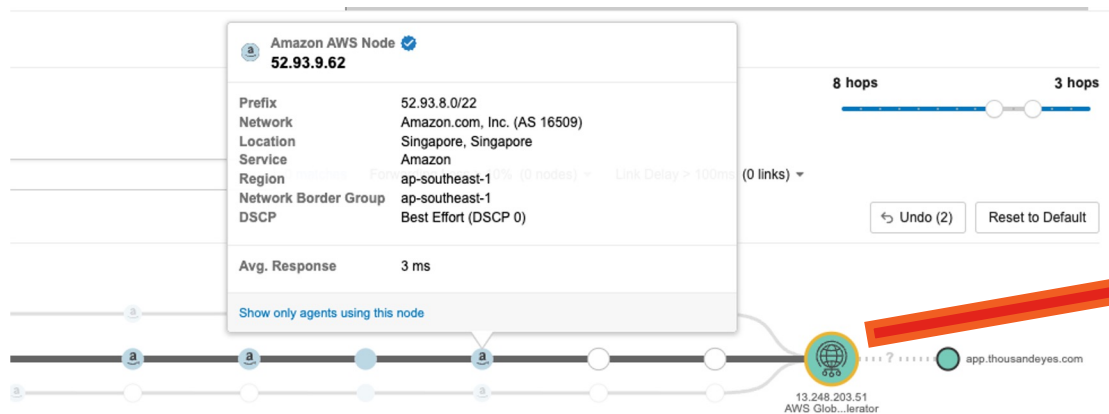
Who does this target?

- Network Operators that want to monitor user traffic to applications that leverage AWS-hosted resources.
- Teams that have resources deployed within AWS to monitor networks and components.

AWS Network Path Enrichment

Extended visibility into AWS networks and services

- Leverage new data sources from our AWS partnership to enrich Path visualization
- Auto-detect “AWS Identified nodes” including region, network border group, and service
- Highlight Global Accelerator nodes with higher than expected response time
- Detailed diagnostic POP comparison including json data that can be shared with AWS Support



Agents with higher than expected response time

	Amazon AWS Global Accelerator ab42238cb7f67e12e.awsglobalaccelerator.com
IP Address	13.248.203.51
Prefix	13.248.128.0/17
Network	Amazon.com, Inc. (AS 16509)
Location	US
Service	Globalaccelerator
Region	GLOBAL
Network Border Group	GLOBAL
Avg. Response	⚠ 160 ms (Expected: 3 ms)

Agents with High Response Times vs Expected From Closest POPs

	Singapore	⚠ 160 ms
POP 1	Singapore, Singapore (SIN2-1)	3 ms
POP 2	Singapore, Singapore (SIN52-2)	3 ms

Cloud Performance Report 2022

CLOUD PERFORMANCE REPORT

2022 Edition

INDUSTRY

How to Monitor API Endpoints from AWS VPCs

By [Sumana Mannem](#) | February 6, 2020 | 10 min read



<https://www.thousandeyes.com/blog/monitor-api-endpoints-aws-vpc>

<https://www.thousandeyes.com/resources/cloud-performance-report-2022>

Summary

Key Takeaway's from the Discussion...

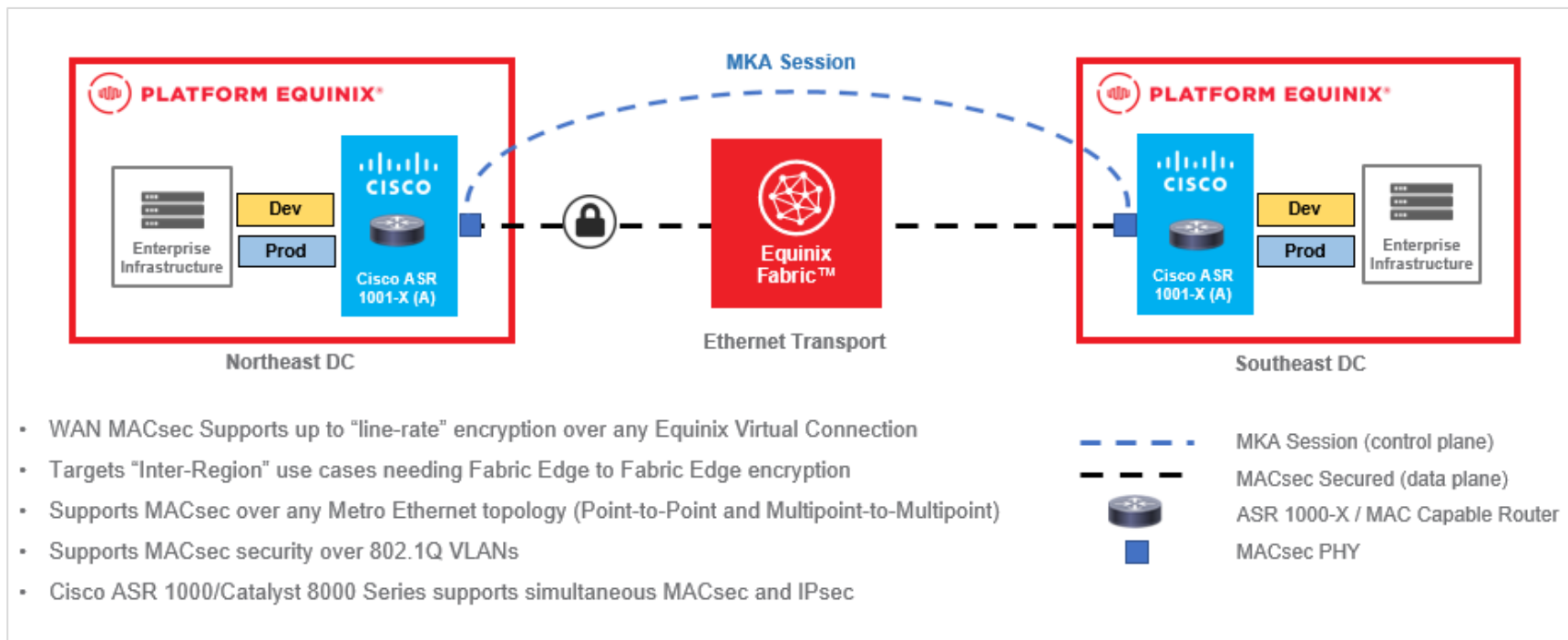
- Evaluate incorporating Co-Location centers into WAN designs to optimize cloud transitions design options
- Evaluate the available cloud connectivity options available that best fit your existing transport today (immediate). Then evaluate best options moving forward that meet the business, Ops team experience, cost, etc.
- Consider encryption (MACsec) for private link protection (up to 100G)
- Evaluate the level of encryption extension needed (compliance requirements) into the cloud to align for the business/agency. Work with cloud provider to understand all options available.
- Enhance your visibility vantage points inside the cloud provider. Consider options like ThousandEyes to provide a view into today's "blind spots"

Useful References

References

- MACsec White Paper (Hill, C., Orr, S.)
 - <https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf>
- Equinix White Paper (Hill, C., Hocker, C., Wiggins, D., Carrara, R.)
 - <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/equinix-fabric-wan-macsec-wp.html>
- Details For Running MACsec over Public Ethernet Transports (Hill, C.)
 - https://github.com/netwrkr95/macsec_eapol_capabilities
- Cloud Ready Networks Paving the Way to Agility, Visibility, and Security (Hill, C., Hocker, C.)
 - <https://www.meritalk.com/articles/cloud-ready-networks-paving-the-way-to-agility-visibility-and-security/>
- Cisco Catalyst 8500 / Microsoft Azure ExpressRoute – Joint Validated Design Guide
 - <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/cisco-catalyst-8500-microsoft-azure.html>
- AWS Direct Connect – MAC Security
 - <https://docs.aws.amazon.com/directconnect/latest/UserGuide/MACsec.html>
- Azure ExpressRoute – Configure MACsec
 - <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-macsec>

Inter Region Testing Example (Cisco + Equinix)



White Paper Link: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/equinix-fabric-wan-macsec-wp.html>

Blog Preview: <https://blogs.cisco.com/government/securing-multiple-data-centers-our-results-using-macsec-over-the-equinix-fabric>



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC