
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Securing High Speed Private Links to Public Cloud Providers

Overview, Designs, and Methods without Sacrificing Performance

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

Chris Hocker
Solutions Architect
U.S. Federal

BRKENT-2003

Cisco Webex App

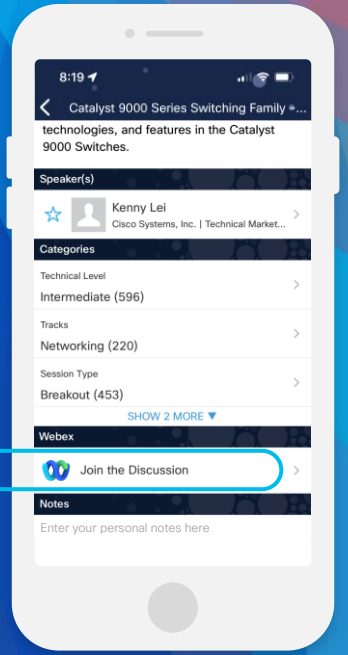
Questions?

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 June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2003

Session Presenters

Craig Hill

Distinguished Architect

US Public Sector – CTO Office

CCIE # 1628

Chris Hocker

Solutions Architect

US Public Sector - Federal

CCIE # 11508

Presentation “House Keeping” Items ☺

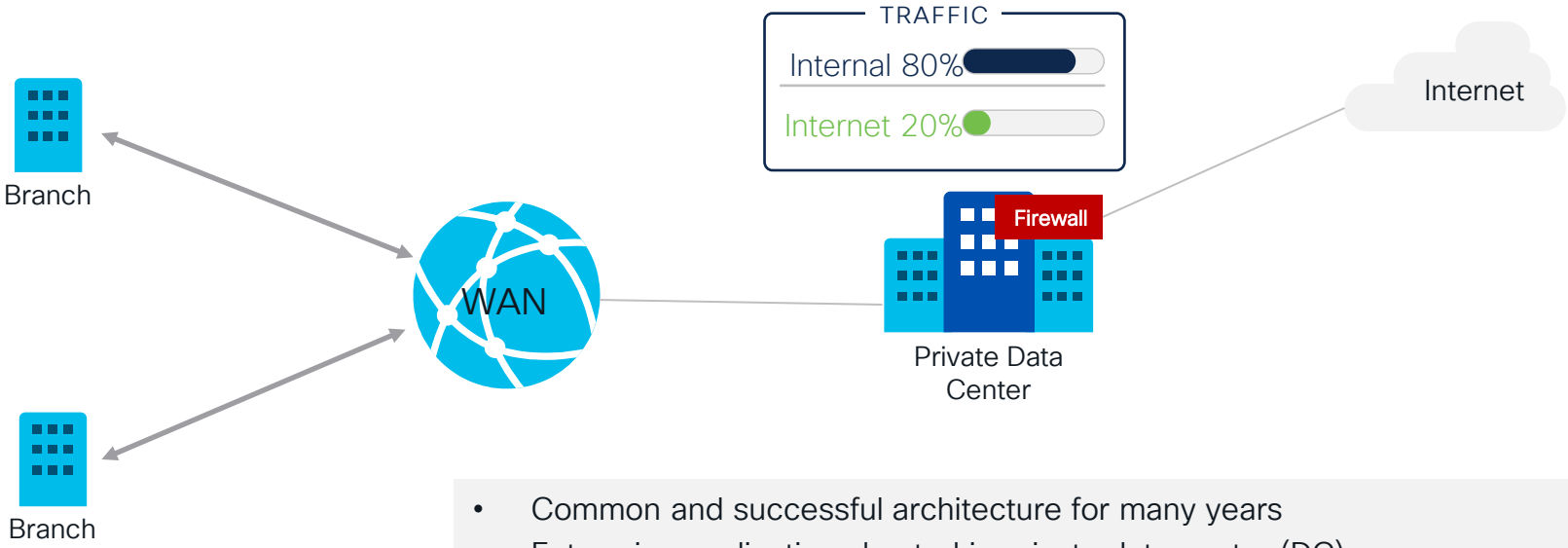
- This is not a product pitch ☺
- This session is focused heavily on secure network design options from customer private networks into the public cloud
- While several prominent cloud providers will be included in this discussion, the discussion has no preferred cloud provider other than those supporting the intended topic

Agenda

- How the transition to the cloud has transformed WAN designs
- Review: Connection Options for Public/Private Access into the Cloud
- “MACsec 101” and Securing High Speed Access into the Cloud
- Configuration Example Reviews
- Design Options for Extending Enterprise Encryption into the cloud
- Inter Region Connection Examples and Cloud Network Visibility
- Summary & References

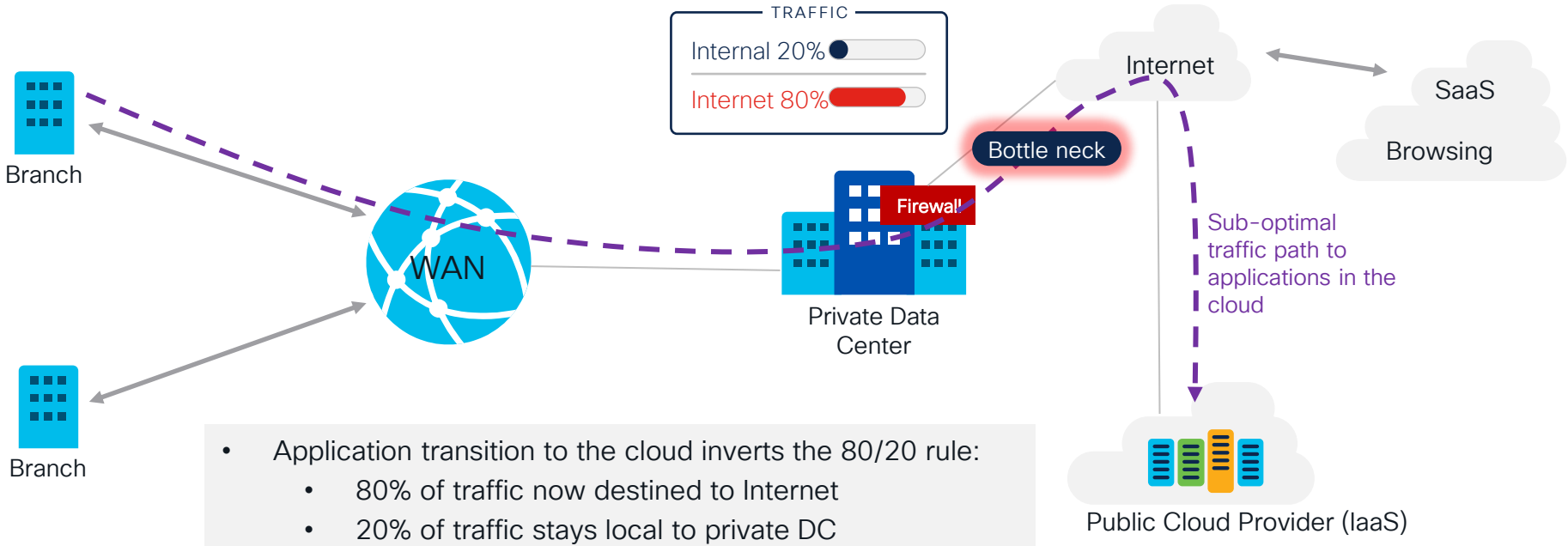
How the WAN is Evolving as Enterprise Applications Transition to the Cloud

Evolution of Applications in the Enterprise



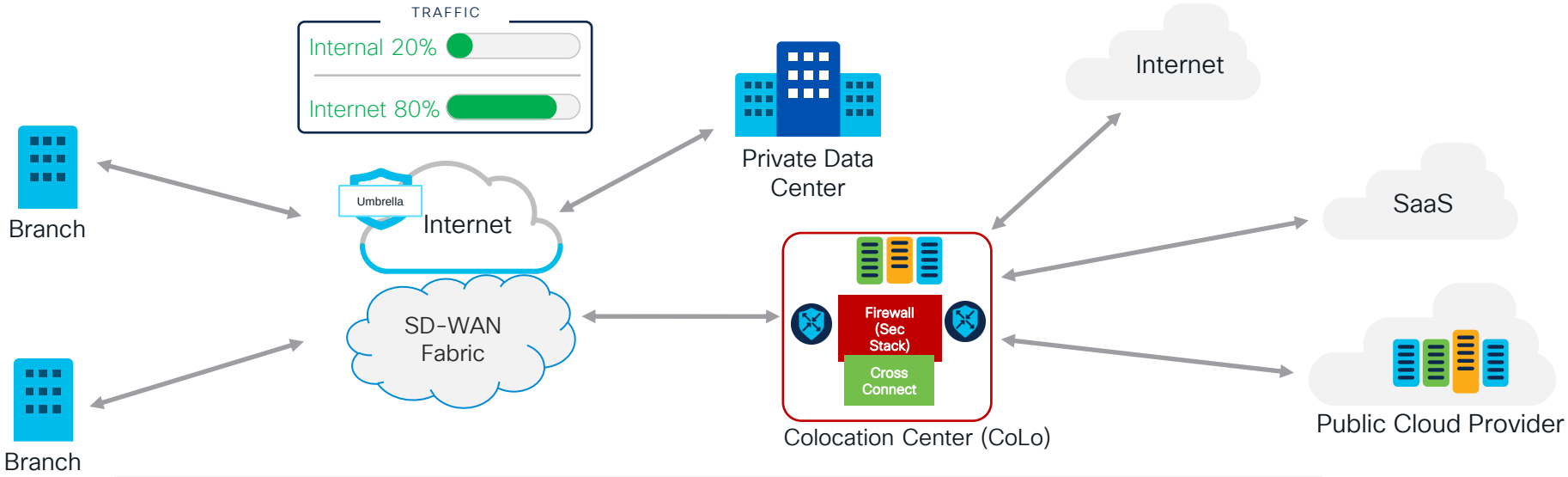
- Common and successful architecture for many years
- Enterprise applications hosted in private data center (DC)
- ~ 80% of branch traffic – destined to private DC applications
- ~ 20% of branch traffic – destined to Internet through the FW
- Aligns with 80/20 rule – apps / internet

Evolution of Applications in the Enterprise



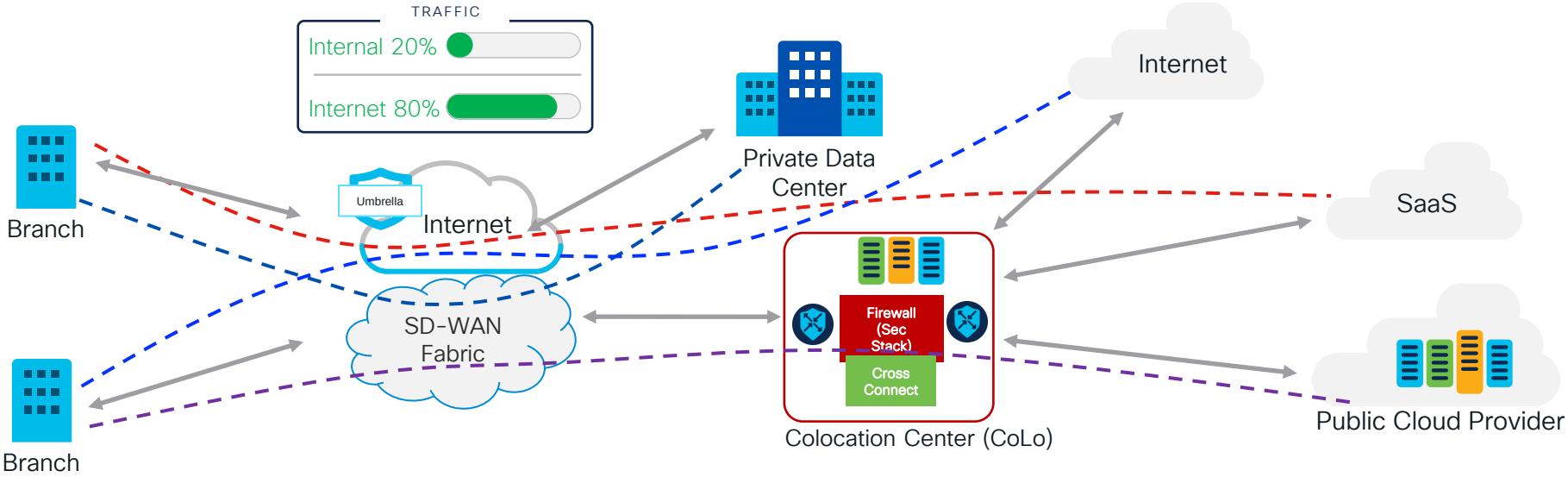
- Application transition to the cloud inverts the 80/20 rule:
  - 80% of traffic now destined to Internet
  - 20% of traffic stays local to private DC
  - FW massively overloaded on 80% capacity
- User experience to cloud apps impacted greatly

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

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:

EQUINIX

NEXTDC

Megaport

When Does Presence in a “CoLo” Best Apply to my WAN Architecture? It Depends... ☺

Highly Desirable

- Enterprise owns and maintains their own WAN
- Desires easy access to largest cloud providers, other XaaS, peering, etc.
- Increasing number of ENT applications and workloads moving/residing in cloud
- Business Apps in cloud demand deterministic network behavior to consumers

“Limited” Need for CoLo

- Enterprise is small and leverages managed WAN service offerings
- Internet is the primary WAN transport for all access for users → applications
- SaaS is primary business application resource
- Internet transport to hosted application is “good enough” (user experience)

When Does Presence in a “CoLo” Best Apply to my WAN Architecture? It Depends... ☺

Highly Desirable

- Enterprise owns and maintains their own WAN
- Desires easy access to largest cloud providers, other XaaS, peering, etc.
- Increasing number of ENT applications and workloads moving/residing in cloud
- Business Apps in cloud demand deterministic network behavior to consumers

Needs deeper evaluation

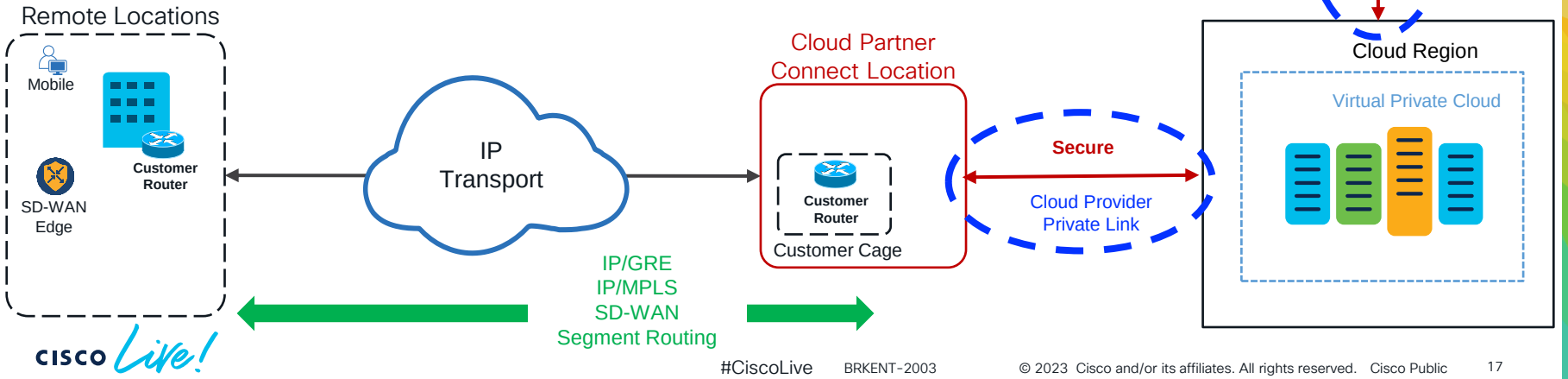
- Enterprise owns and maintains their own WAN
- % Apps hosted in the cloud?
- Pace of transition to cloud?
- % SaaS? % IaaS?
- How is user-to-app experience?

”Limited” Need for CoLo

- Enterprise is small and leverages managed WAN service offerings
- Internet is the primary WAN transport for all access for users → applications
- SaaS is primary business application resource
- Internet transport to hosted application is “good enough” (user experience)

Securing Cloud Service Provider Private Links and Inter-Region Transport

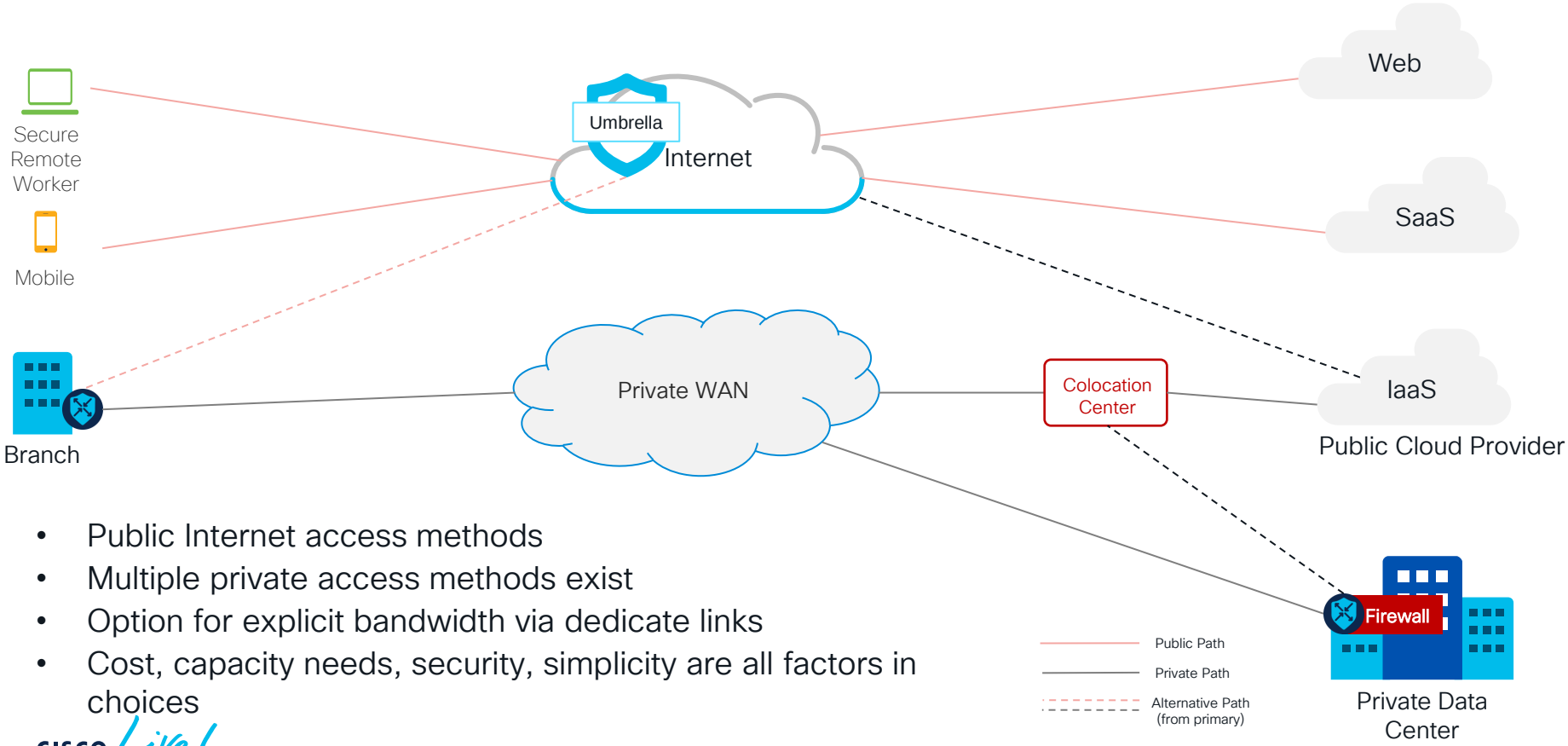
- Cloud Service Provider's (CSP) offering dedicated (10G, 100G) private links
  - Targets those customers wanting dedicated BW and deterministic network behavior into, and from, their cloud hosted workloads
  - How to secure these private links up to 100G?
  - CSP provides an extensive list of partners, locations, details of capabilities, redundancy options, and speeds
- Look deeper at the Inter-Region cloud Interconnect options, pros/cons, and how to apply security



Options for Connecting to Cloud Providers

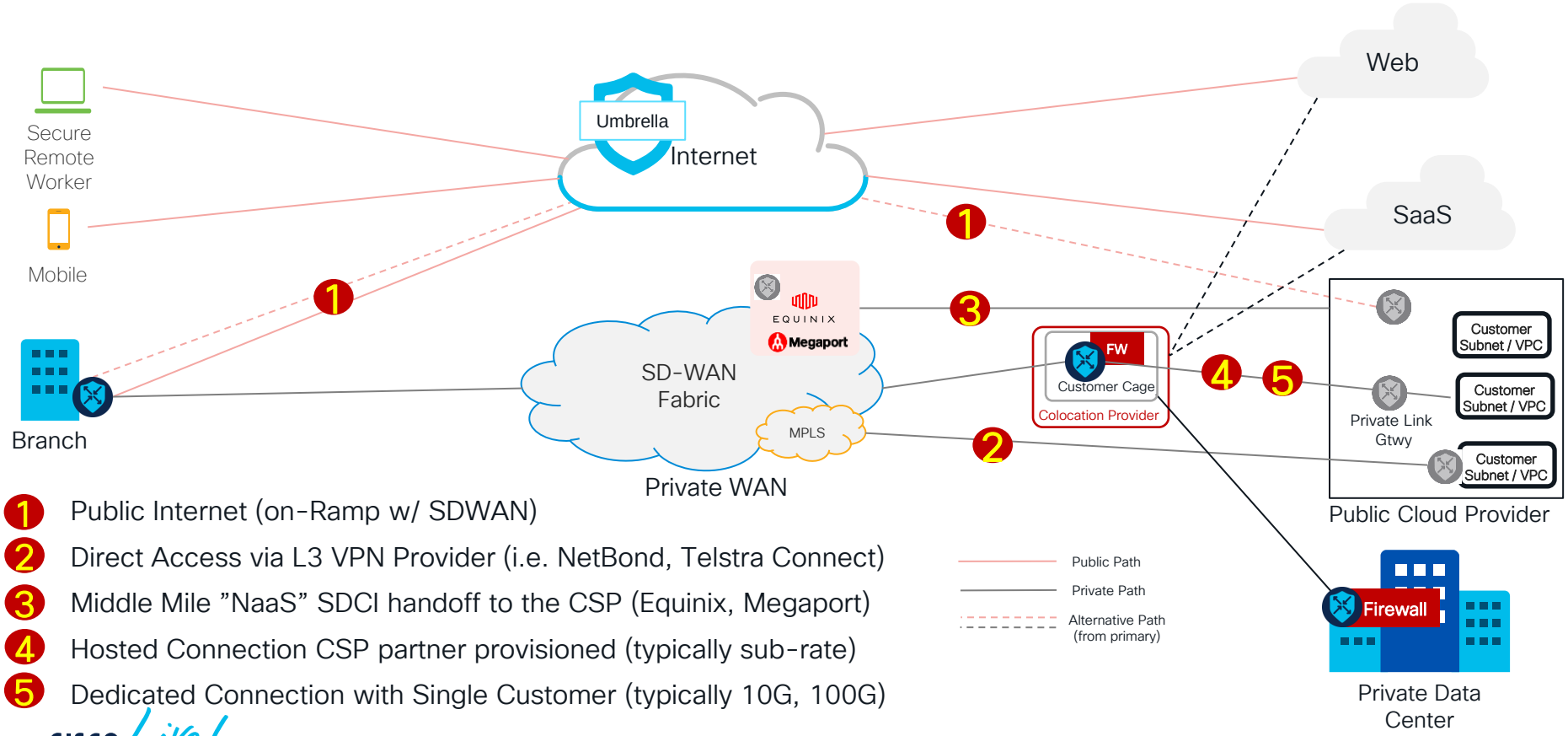
Evaluating Private Link Access

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

Options for Connecting into the Cloud Providers



1. Public Internet (on-Ramp w/ SDWAN)
2. Direct Access via L3 VPN Provider (i.e. NetBond, Telstra Connect)
3. Middle Mile "NaaS" SDCI handoff to the CSP (Equinix, Megaport)
4. Hosted Connection CSP partner provisioned (typically sub-rate)
5. Dedicated Connection with Single Customer (typically 10G, 100G)

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

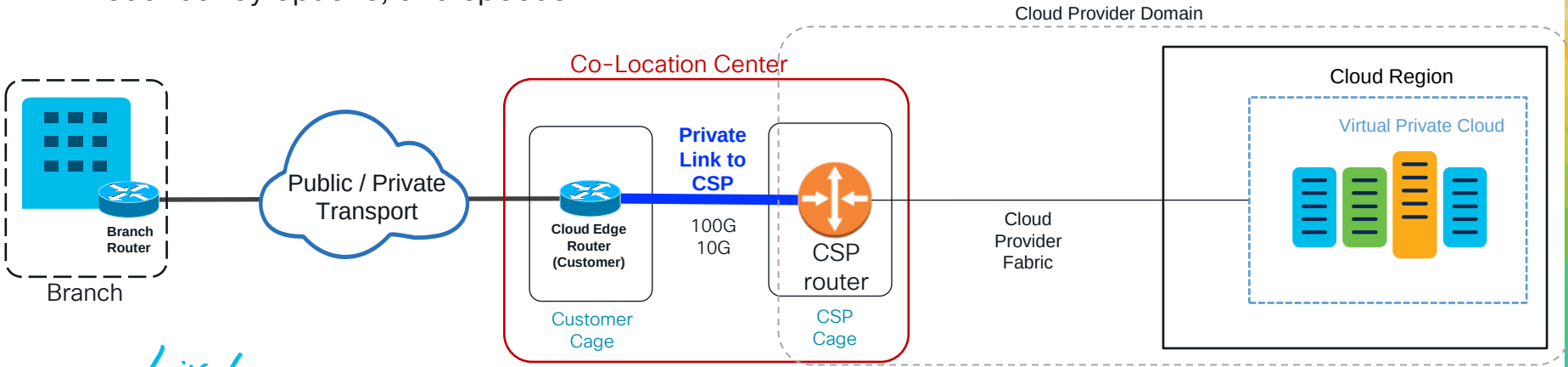
- Challenges: Private Links into the Cloud Providers?
  - Cost, Security of those links, complexity of setup

- 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
  - Multi-cloud Prep: Sets the table for multi-cloud support (current or future)

“Private Link” Support into the Cloud Providers

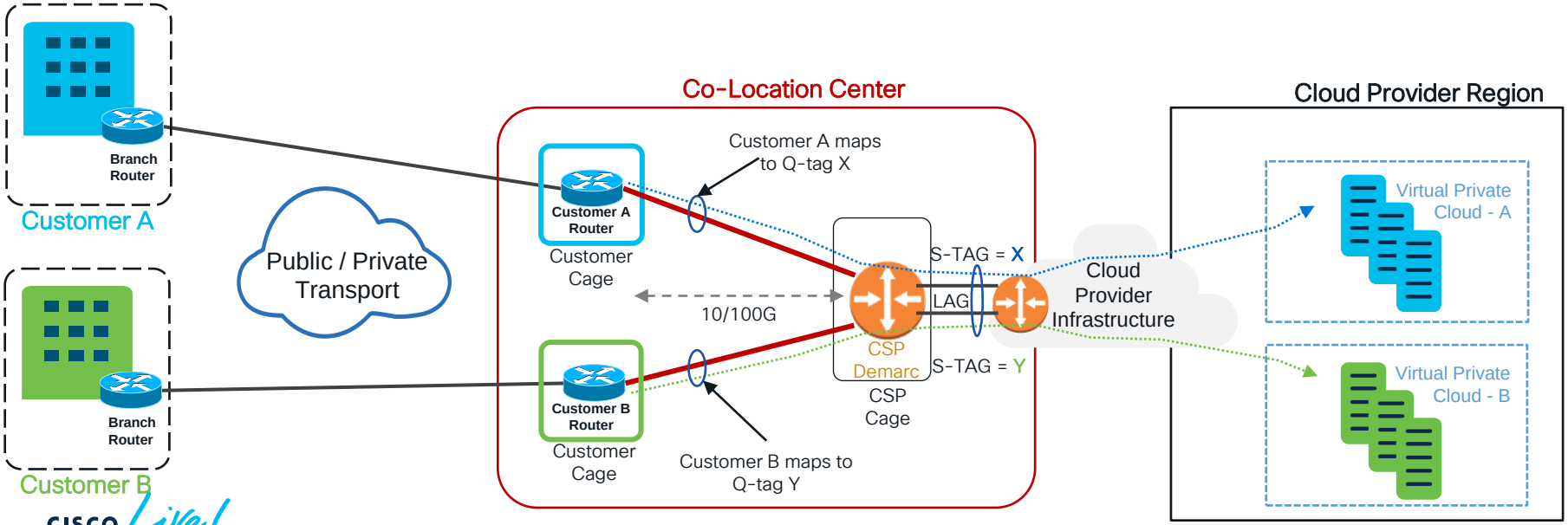
Example: CSP Private Link Offering

- 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



Example: CSP Private Link Offering
Anatomy of the Service

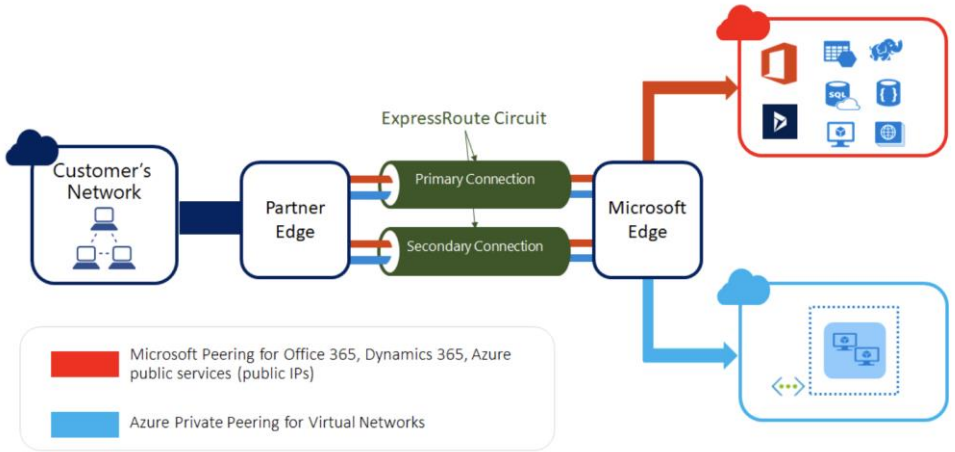
- CSP separates customer traffic through use of 802.1Q tags through a Virtual Interface (VIF)
- The VIF controls customer (tenant) and access (public / private) to services within the CSP
- Customer traffic remains completely segmented from each tenant



Example: Private Link – 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

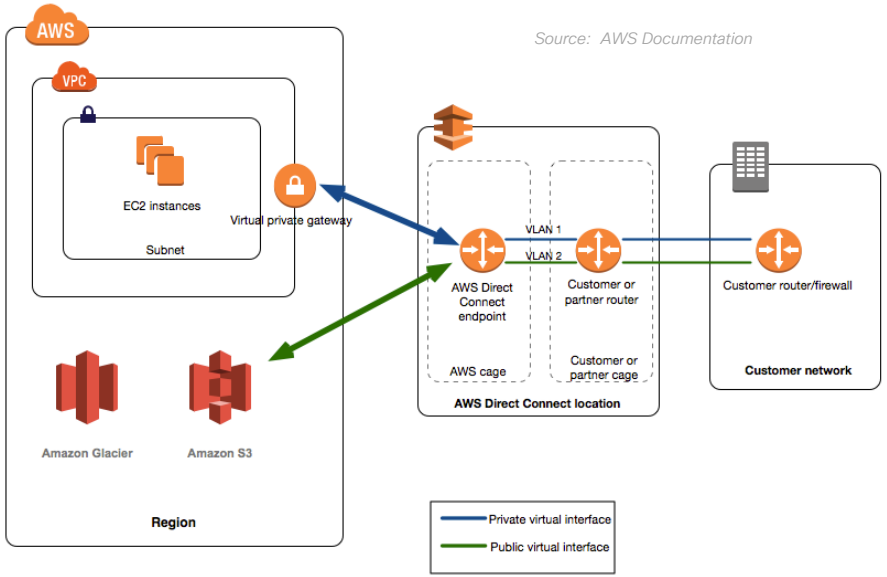
Source: Azure Documentation



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

Example: Private Link – 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)



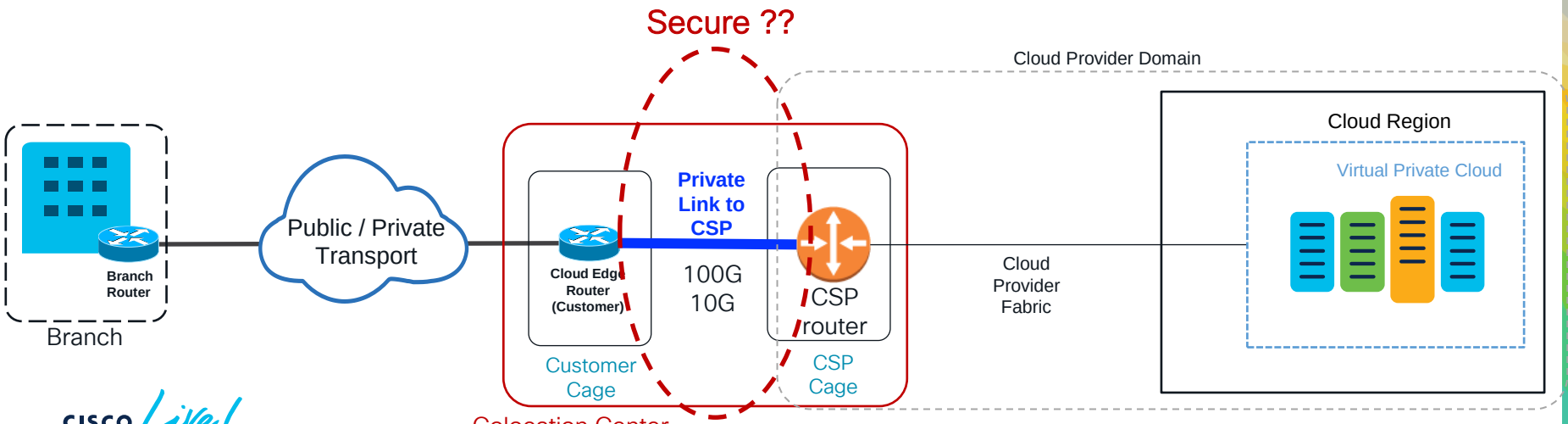
Source: https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

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

CSP Private Link Security

- Offers high speed dedicated (10G, 100G) and (sub-rate) private link options

1. How can I assure the link is protected through the CoLo Providers Infrastructure?
2. Can I provide encryption rates that can support 100G?
3. Is this supported over both “Dedicated” and “Hosted” (sub-rate) offerings?



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.

Encrypting ExpressRoute for improved security

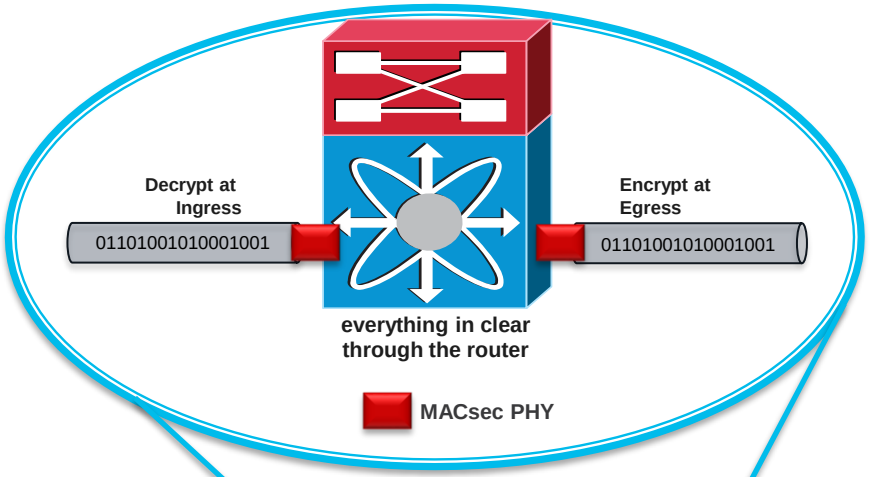
MACsec

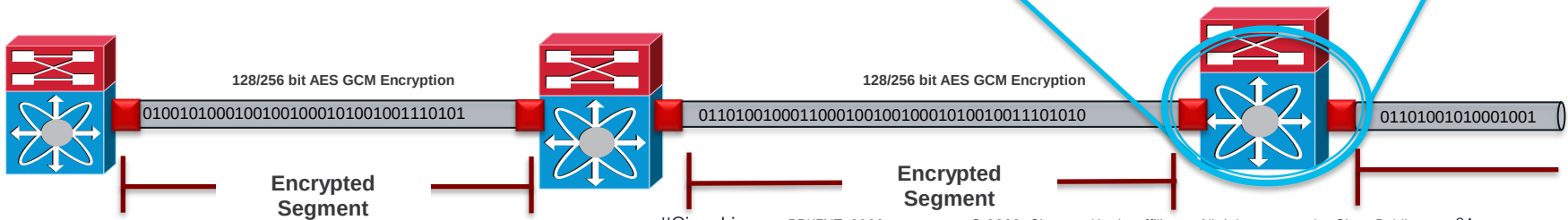
Let's start with MACsec as this solution can only apply to ExpressRoute Direct. With ExpressRoute Direct, customers establish a layer 2 private connection from their edge to Microsoft Enterprise Edge in Azure. Once you have connectivity at layer 1, your layer2 is setup which allows you to then create 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 101”

What is MAC Security (MACsec)?
Hop-by-Hop Encryption via IEEE802.1AE

- 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)

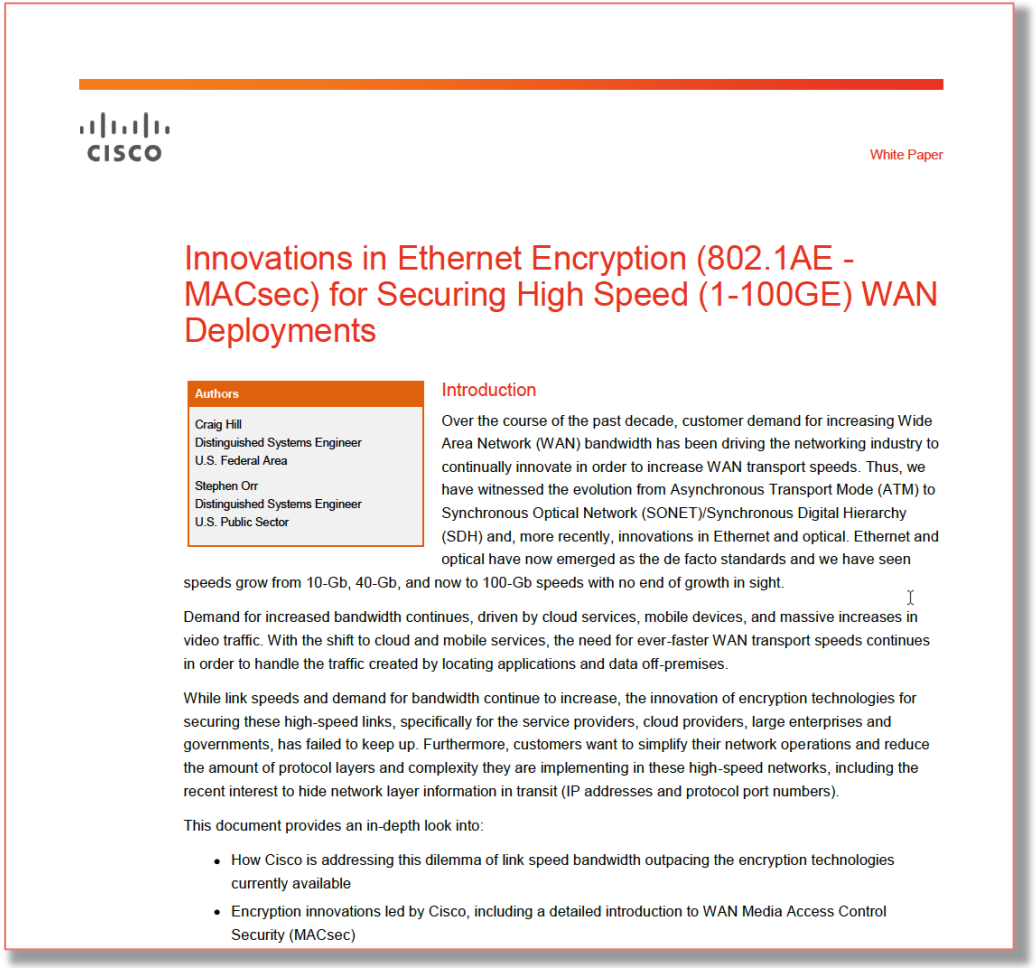




WAN MACsec: Top Enterprise and SP Use Cases

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



White Paper

Innovations in Ethernet Encryption (802.1AE - MACsec) for Securing High Speed (1-100GE) WAN Deployments

Authors

Craig Hill
Distinguished Systems Engineer
U.S. Federal Area

Stephen Orr
Distinguished Systems Engineer
U.S. Public Sector

Introduction

Over the course of the past decade, customer demand for increasing Wide Area Network (WAN) bandwidth has been driving the networking industry to continually innovate in order to increase WAN transport speeds. Thus, we have witnessed the evolution from Asynchronous Transport Mode (ATM) to Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH) and, more recently, innovations in Ethernet and optical. Ethernet and optical have now emerged as the de facto standards and we have seen speeds grow from 10-Gb, 40-Gb, and now to 100-Gb speeds with no end of growth in sight.

Demand for increased bandwidth continues, driven by cloud services, mobile devices, and massive increases in video traffic. With the shift to cloud and mobile services, the need for ever-faster WAN transport speeds continues in order to handle the traffic created by locating applications and data off-premises.

While link speeds and demand for bandwidth continue to increase, the innovation of encryption technologies for securing these high-speed links, specifically for the service providers, cloud providers, large enterprises and governments, has failed to keep up. Furthermore, customers want to simplify their network operations and reduce the amount of protocol layers and complexity they are implementing in these high-speed networks, including the recent interest to hide network layer information in transit (IP addresses and protocol port numbers).

This document provides an in-depth look into:

- How Cisco is addressing this dilemma of link speed bandwidth outpacing the encryption technologies currently available
- Encryption innovations led by Cisco, including a detailed introduction to WAN Media Access Control Security (MACsec)

Previous WAN MACsec Sessions at CLUS (OnDemand)

BRKRST-2309 – Introduction to WAN MACsec

WAN MACsec Blog

WAN MACsec WP over Equinix Fabric

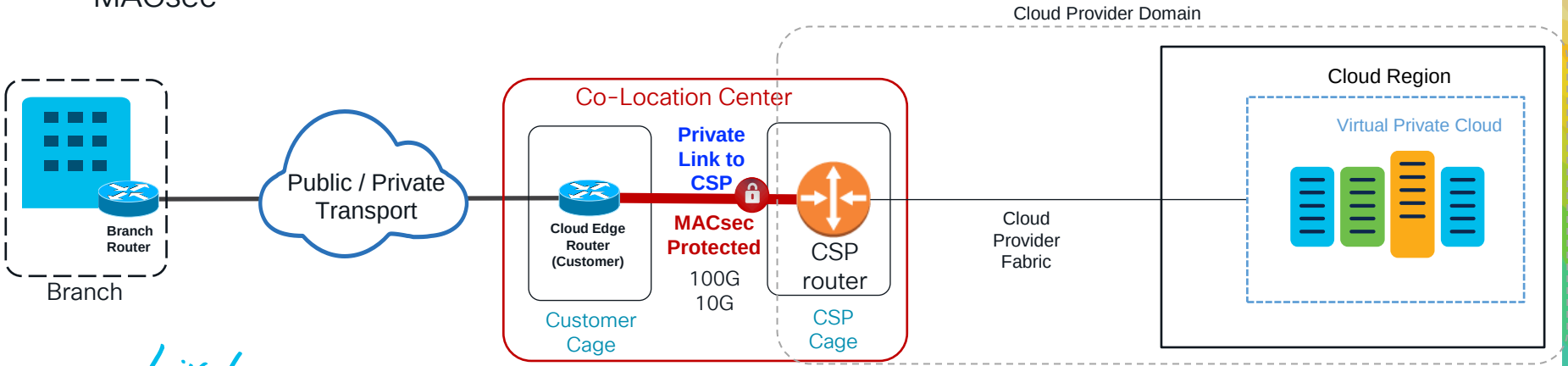
http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

Securing High Speed Private Links to the Cloud using MACsec

cisco Live!

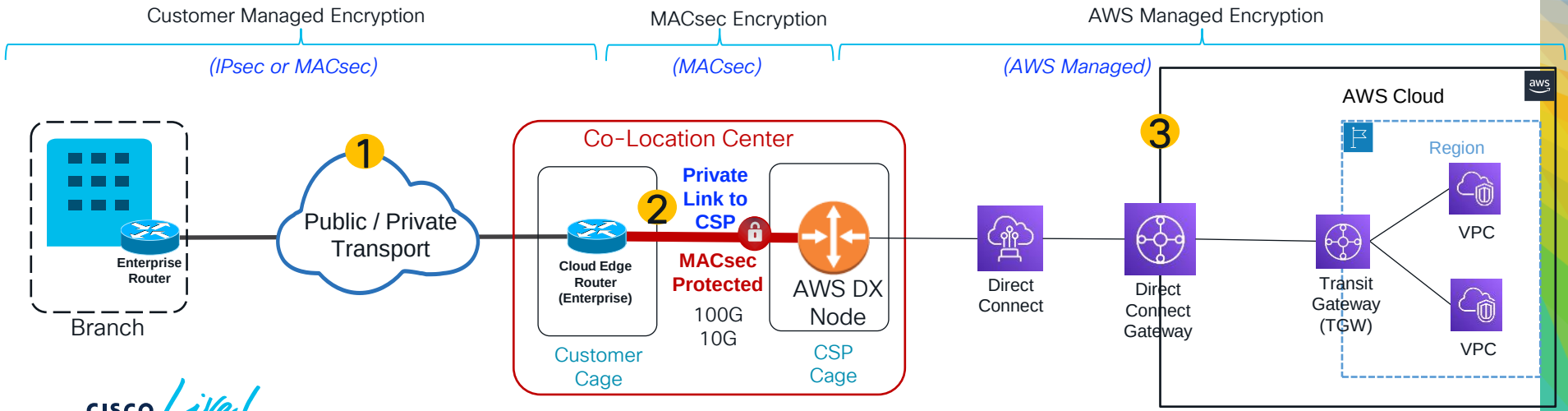
CSP Private Link using MACsec Protection

- 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

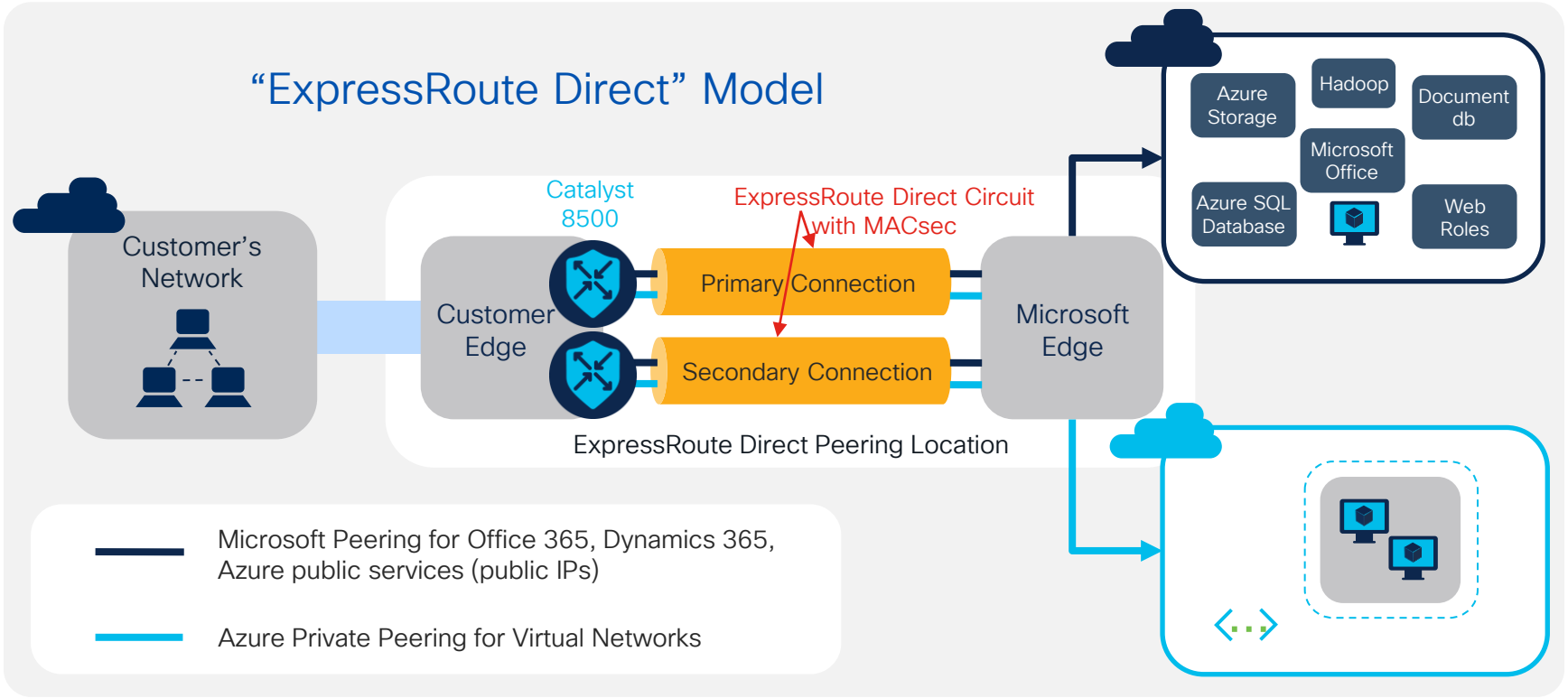


AWS Example: Private Link using MACsec Protection

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



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 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	• For 100 Gbps connections: GCM_AES_XPN_256 • For 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

Reference slide

```
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
!
```

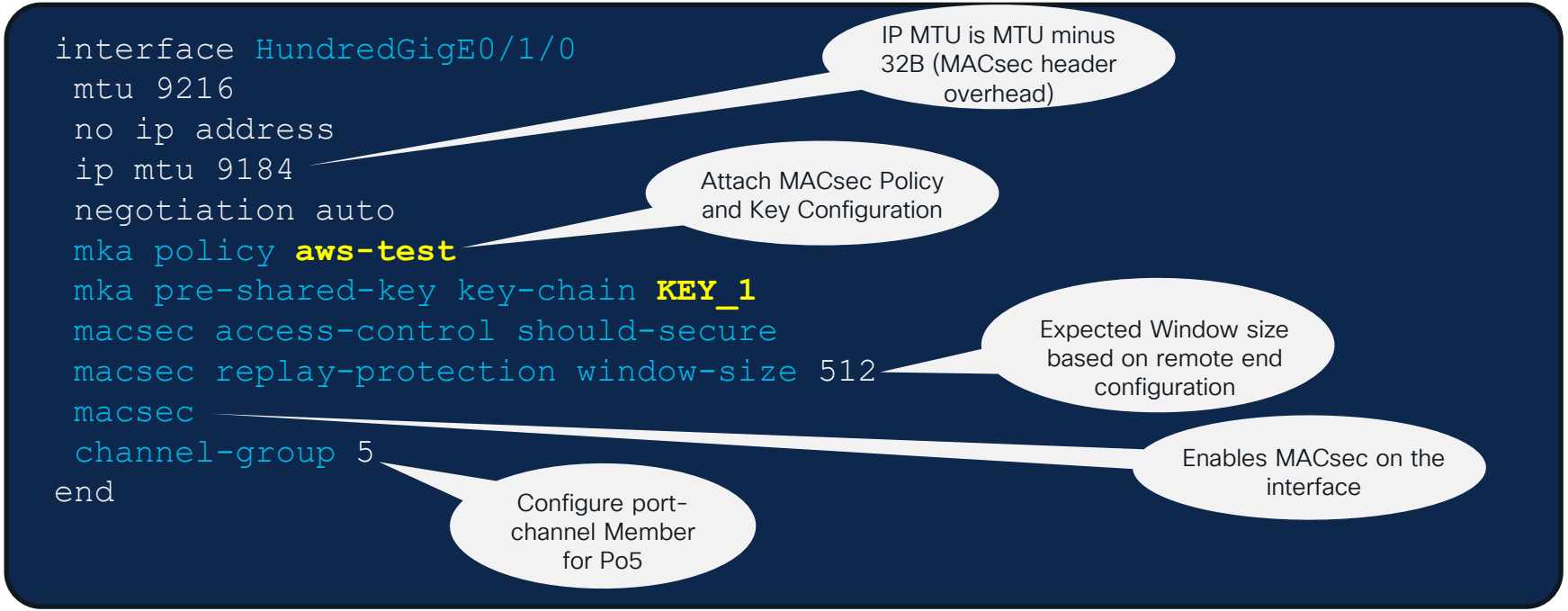
MACsec 64 hexadecimal key configuration

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

Reference slide



100G MACsec Direct Connect (DX) Verification

Reference slide

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

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

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

C8500-12X4QC-2#
```

MACsec session should be in Secured state

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

100G MACsec DX Verification

Reference slide

```
C8500-12X4QC-2#sh macsec status interface Hu0/1/0
 Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
  Cipher:                   GCM-AES-XPN-256
  Confidentiality Offset:   0
  Replay Window:            512
  Delay Protect Enable:     FALSE
  Access Control:           should-secure
  Include-SCI:              TRUE


 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#
```

Correct cipher should be applied as per config.

Azure ExpressRoute Examples

Azure ExpressRoute Examples

Reference Session:

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/1655479484932001lRuX

Extending Encryption into the Cloud Provider

Design Options

Extending Enterprise Network Encryption Into the CSP

Public Access

- Public Internet
- Public Internet Peering Option

Private Link

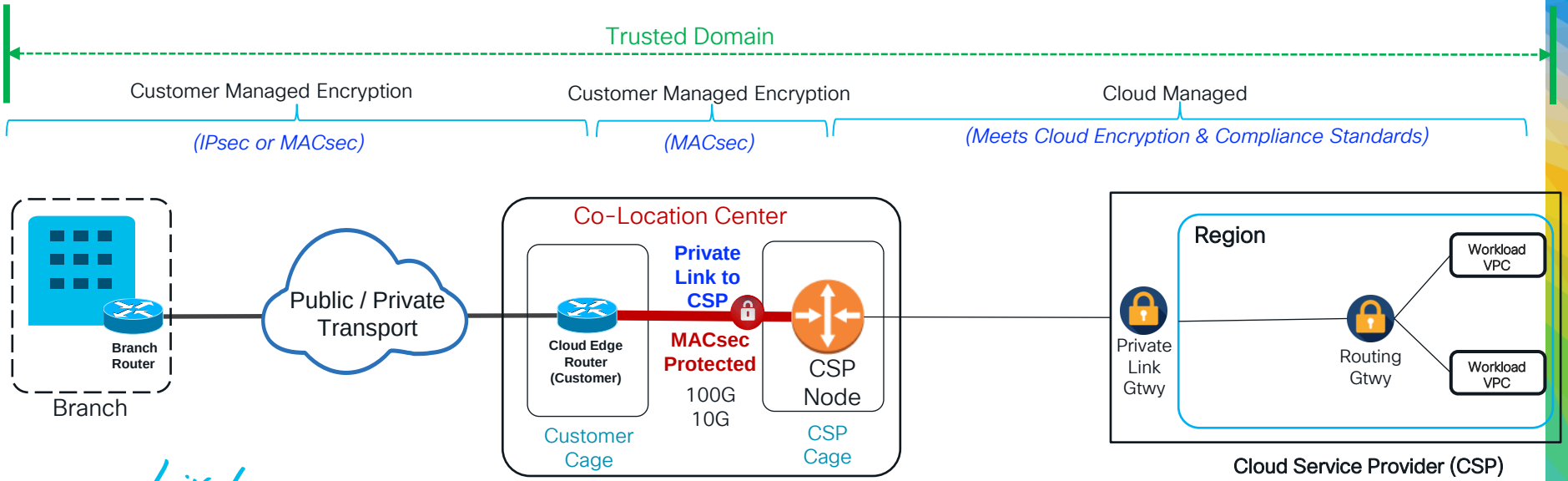
- Trusted: Encryption option for private link service (DX, ExpressRoute) into CSP meets the security compliance requirements for the enterprise standards
- Un-Trusted: Encryption option for private link service (DX, ExpressRoute) into the CSP does NOT meet the security compliance requirements for the 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

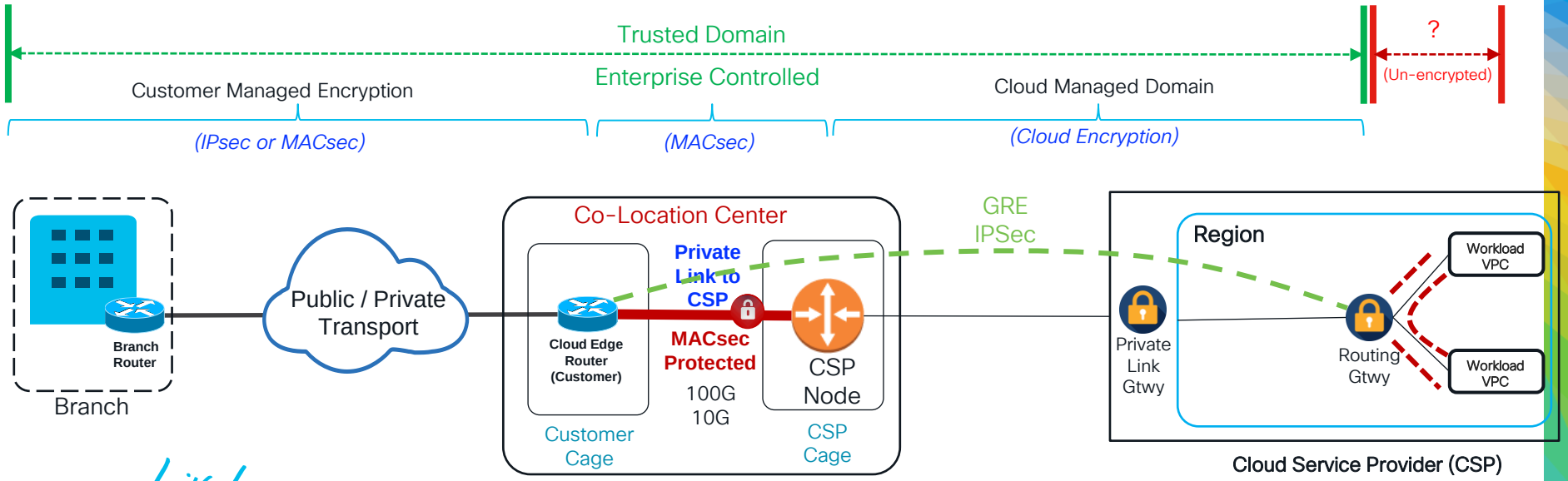
Summary: Cloud provider infrastructure, with MACsec private link encryption, assumed secure that would meet some enterprise/government security and compliance policy requirements



Private Link – Un-Trusted – Option 1:
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

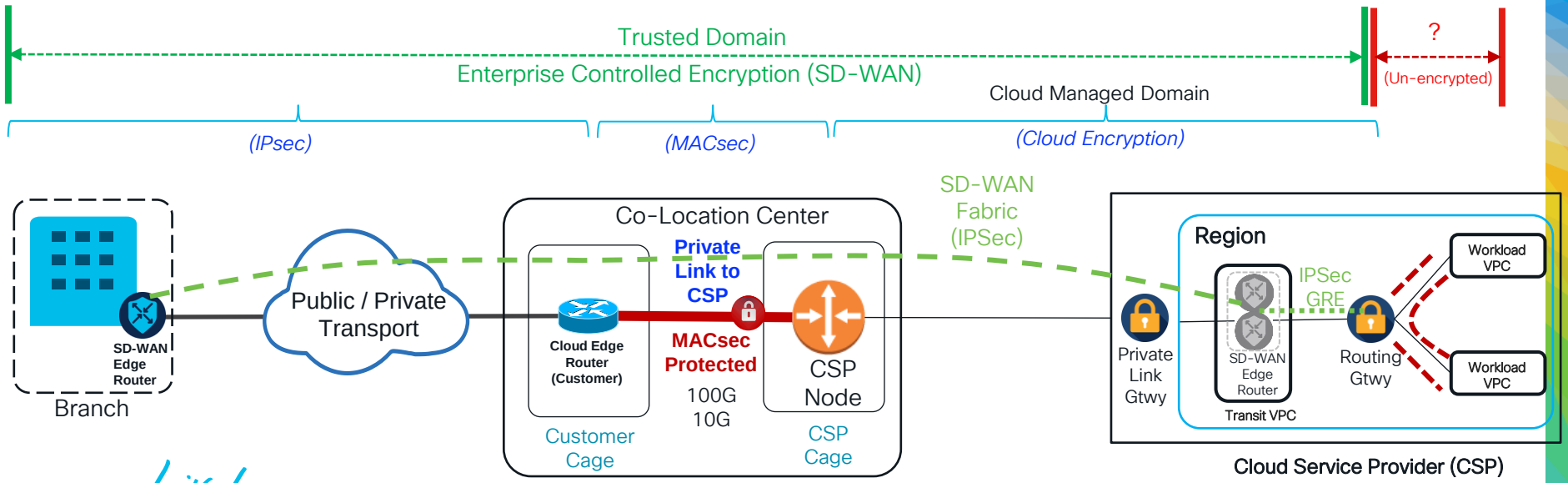
Summary: Enterprise security and compliance policies will dictate "encryption domain"



Private Link – Un-Trusted – Option 2:
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"

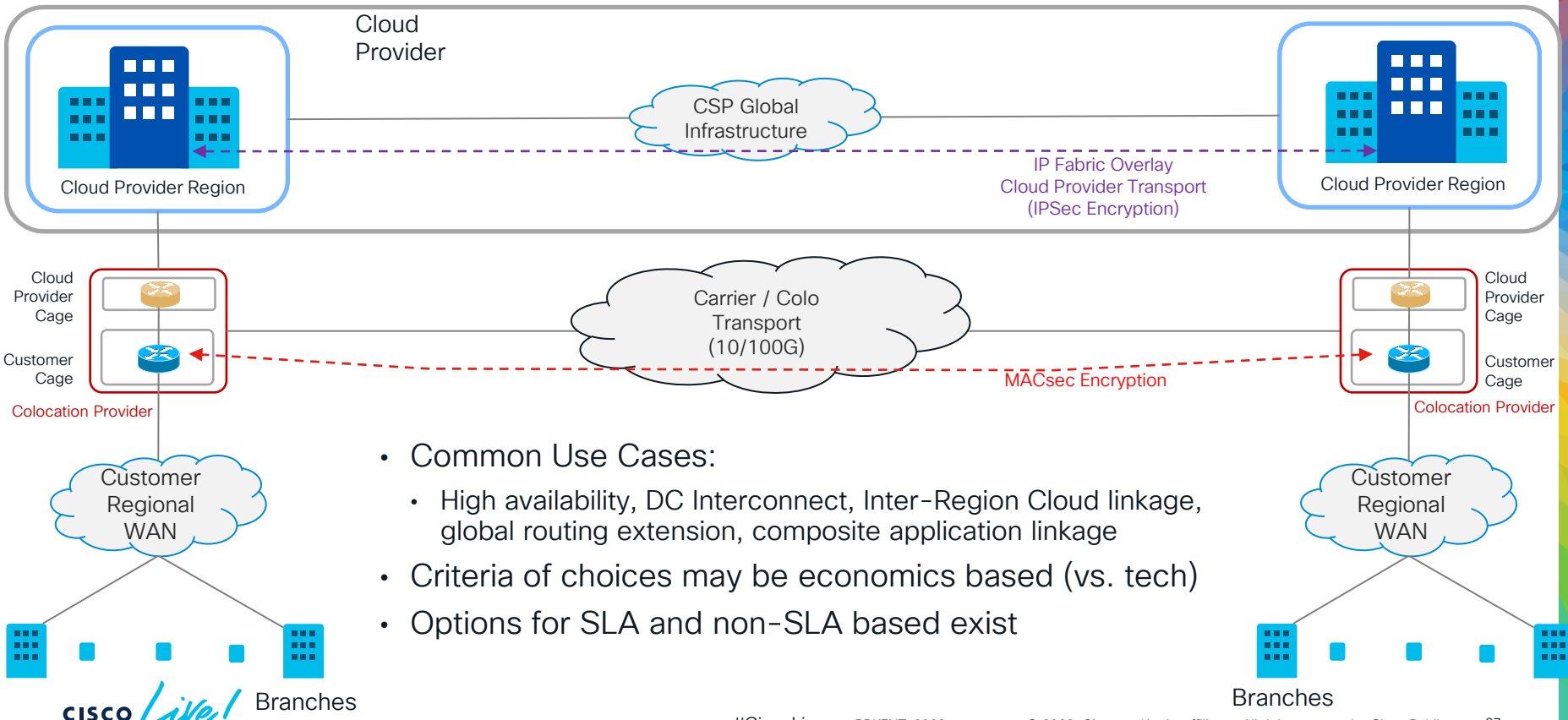


Summary and Caveats

- 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

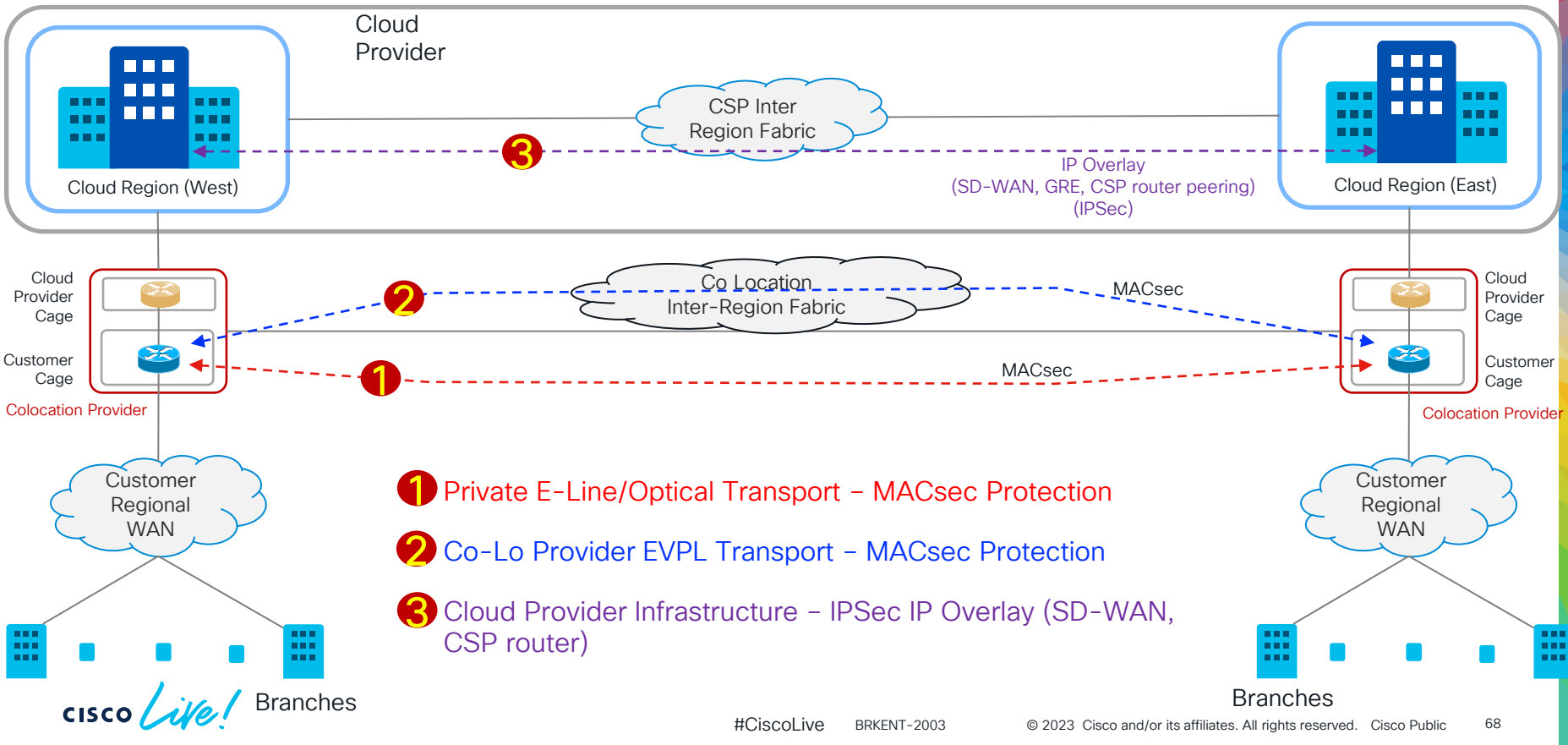
Securing Inter-Region Interconnections

Securing High Speed Inter Region Interconnections



- Common Use Cases:
  - High availability, DC Interconnect, Inter-Region Cloud linkage, global routing extension, composite application linkage
- Criteria of choices may be economics based (vs. tech)
- Options for SLA and non-SLA based exist

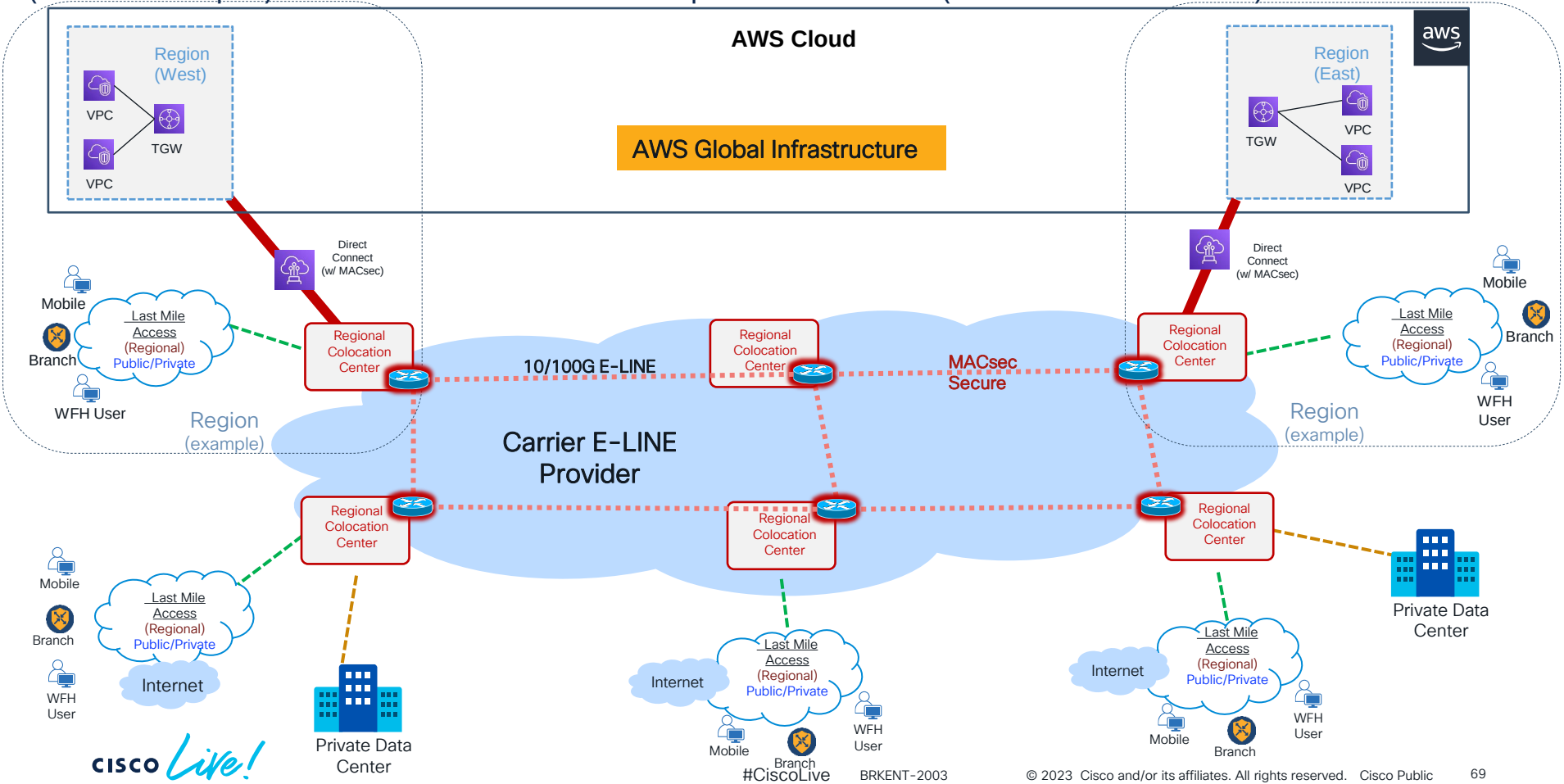
Securing High Speed Inter Region Interconnections



1. Private E-Line/Optical Transport – MACsec Protection
2. Co-Lo Provider EVPL Transport – MACsec Protection
3. Cloud Provider Infrastructure – IPSec IP Overlay (SD-WAN, CSP router)

Example 1: Global WAN – Regional Interconnect

(AWS Example): Dedicated E-LINE Transport via Carrier (MACsec Protected)



Example 1: Global WAN – Regional Interconnect

Example: Dedicated E-LINE Transport via Carrier (MACsec Protected)

PROS

- Provides a guaranteed Service Level Agreement (SLA), per circuit, between each regional location
- Full 100G non-blocking circuit between regions
- No performance impact for encrypting the link at 100G using MACsec for encryption

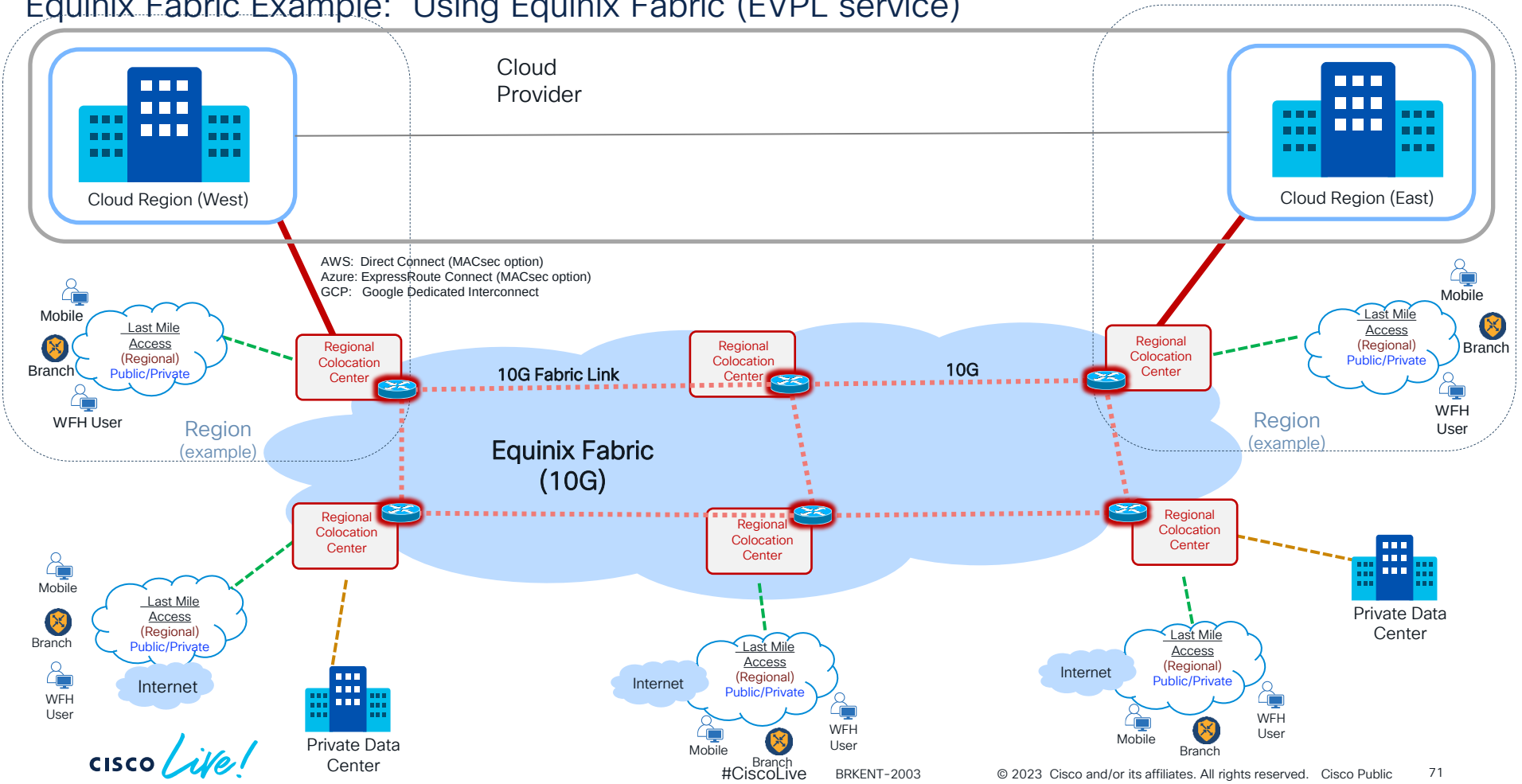
CONS

- Cost - Requires dedicated transport circuits between colocation centers ($$$ costly)
- Cost per traffic patterns - Egress charges will apply for any traffic “from” cloud provider (traffic patterns will dictate this)

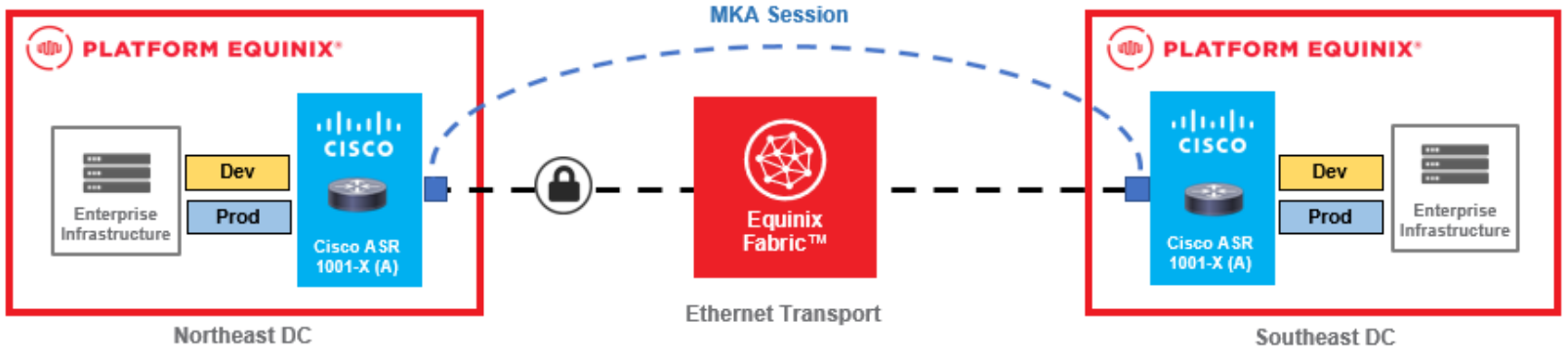
Example 2: Global WAN – Regional Interconnect

WAN MACsec Router

Equinix Fabric Example: Using Equinix Fabric (EVPL service)



Inter Region Testing Example (Cisco + Equinix)



- WAN MACsec Supports up to "line-rate" encryption over any Equinix Virtual Connection
- Targets "Inter-Region" use cases needing Fabric Edge to Fabric Edge encryption
- Supports MACsec over any Metro Ethernet topology (Point-to-Point and Multipoint-to-Multipoint)
- Supports MACsec security over 802.1Q VLANs
- Cisco ASR 1000/Catalyst 8000 Series supports simultaneous MACsec and IPsec

MKA Session (control plane)
MACsec Secured (data plane)
ASR 1000-X / MAC Capable Router
MACsec PHY

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

Example 2: Global WAN – Regional Interconnect
Equinix Fabric Example: Using Equinix Fabric (EVPL service)

PROS

- Provides an easy access to regional interconnect transport if already using Equinix services
- Simple turn up if already leveraging Equinix cage space
- Leverages Cisco WAN MACsec capabilities (see white paper) for encryption over the Equinix fabric

CONS

- Limited to 10 Gb max throughput
- For applications requiring extreme predictable behavior (latency, jitter, packet loss) operator should understand transport capabilities with application requirements
- Advanced Cisco MACsec capabilities (802.1Q tag-in-clear, EAPoL tuning) are required for MACsec encryption over the Equinix Fabric

Example 3: Inter Region Transit Architecture with Cisco SD-WAN

Modern Transit Architecture with Cisco Cloud OnRamp for Azure Virtual WAN White Paper

Back to Url

Updated: November 22, 2021

Bias-Free Language

Table of Contents

Table of Contents

Phase 1: Evolution to the Mode...

Phase 2: Cloud OnRamp for Ia...

Phase 3: Modern Transit Archit...

Summary

Save Download Print

Today, digital transformation and cloud migration are the top priorities for most organizations. The question is not whether to migrate to the cl oud but when. IT teams have started realizing the benefits of moving workloads to the cloud, such as agility, scalability, and reduced costs an d time to bring up new services. Some applications have moved to the cloud, while others are still residing in the data center. This has resulte d in a hybrid cloud world, in which users accessing these applications are largely unchanged. They are still accessing applications from branc hes, campus hubs, and now from home as well.

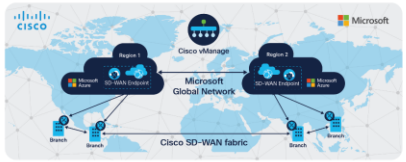


Figure 1.

Modern transit connectivity using Cisco SD-WAN Cloud OnRamp for Azure Virtual WAN

cisco Products and Services Solutions Support Learn Partners

Solutions / Design Zone / Design Zone for WAN and Branch/Remote Sites / Design Guides /

Cisco SD-WAN Cloud onRamp for Multicloud using Google Cloud Platform

July 12, 2022

2 Comments

Networking

Cisco SD-WAN with AWS Cloud WAN for an on-demand global cloud network

Nitisha Bhatia

SD-WAN is now a foundational part of the cloud journey for organizations adopting Infrastructure-as-a-Service for on-demand application availability. But that journey needs to continue ever-evolving. The option of manually stitching the connectivity from branch to cloud or region-by-region is no longer efficient or scalable.

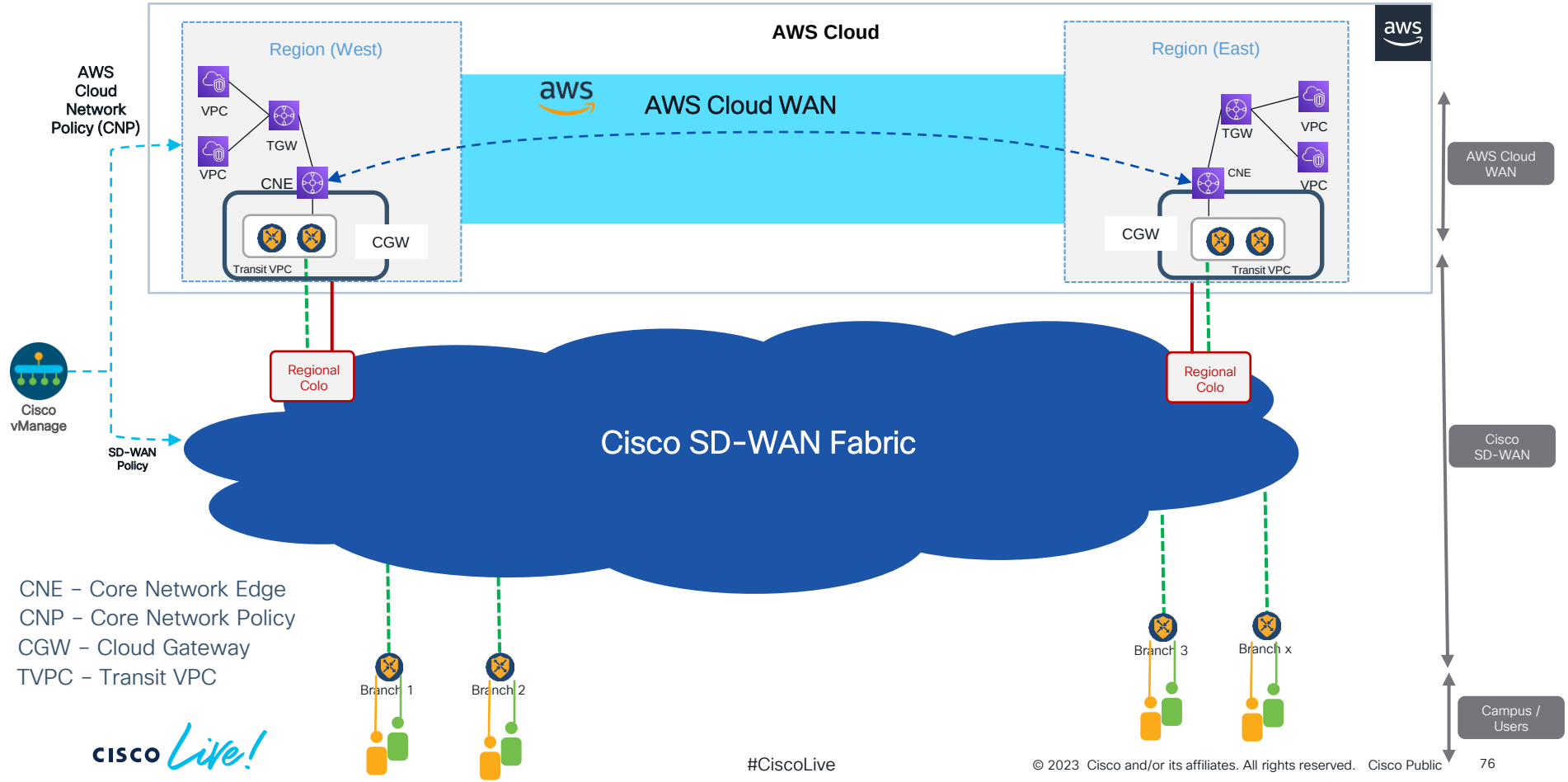
Keeping pace with this evolving reality, Cisco became the first vendor in the industry to natively integrate SD-WAN with major cloud service providers, automating site-to-cloud connectivity and creating a uniform network configuration and policy management experience for enterprise IT. And over the past several years, Cisco and AWS have been innovating to simplify and accelerate the cloud journey for their large joint customer base in order to achieve a truly optimized global network fabric.

Continuing this innovation, Cisco and AWS are now working closely on integrating Cisco SD-WAN with AWS Cloud WAN to connect multi-region as well as cloud-to-on-premises workloads together. Using the Cisco SD-WAN powered by Viptela solution, customers can leverage Cisco SD-WAN vManage for a single-portal experience, end-to-end visibility and assurance, and secure connectivity across their AWS cloud regions.

Contributing Author: **Steve Wood, Principal Engineer – Technical Marketing – SD-WAN**

Example 3: Global WAN – Regional Interconnect

Example: Using AWS Global Infrastructure



CNE – Core Network Edge
CNP – Core Network Policy
CGW – Cloud Gateway
TVPC – Transit VPC

Example 3: Global WAN – Regional Interconnect
Example: Using Cloud Provider Global WAN Infrastructure

PROS

- Provides a simple transport option when the source/destination between cloud regions are the same cloud provider
- Integrates well into WAN solutions used for extending transport into the cloud provider (i.e., SD-WAN)
- Cisco SD-WAN provides a tight integration into cloud providers
- Cisco SD-WAN integrates all API's needed, simplifying the provisioning

CONS

- No predictable bandwidth throughput
- Not as applicable if multiple cloud providers are required for certain composite applications that span multiple cloud
- Not applicable for those applications requiring predictable latency / packet-loss / Jitter, there are No SLA's offered for the transport

Reference: BRKENT-2283 – 4 Steps to Unify Multi-Cloud Connectivity with Cisco SD-WAN

Visibility Options into the Cloud Providers

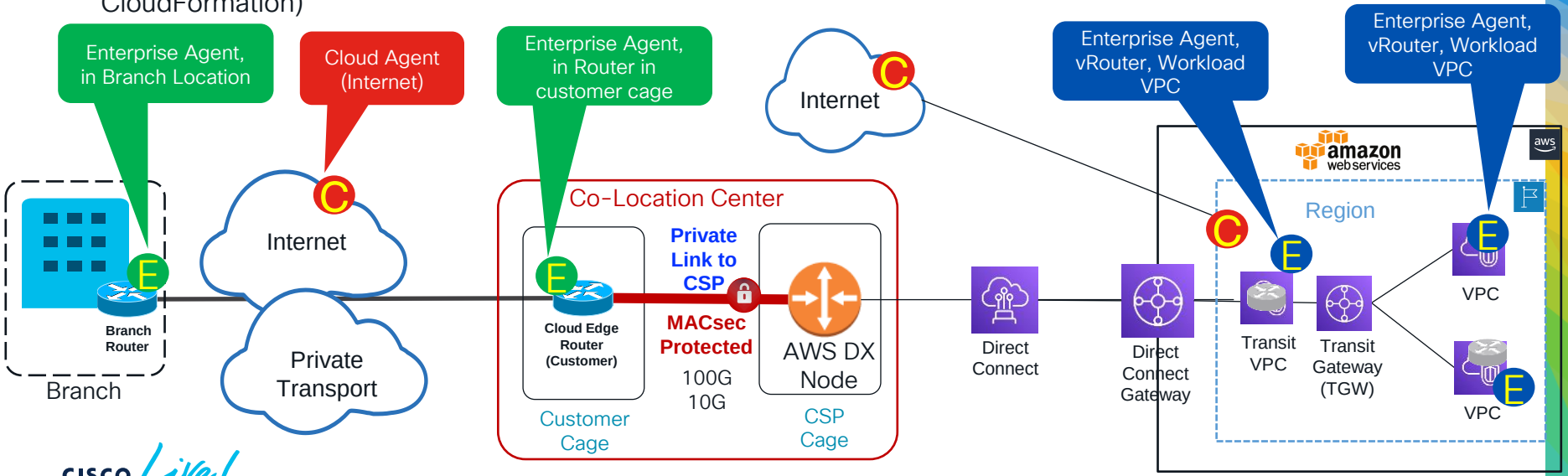
ThousandEyes Visibility Example:
Private and Public Link Visibility into the Cloud Service Provider

- 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



Cloud Performance Report 2022

Thousand Eyes

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
- Evaluate the available cloud connectivity options available and how they best optimize your users access to the applications in the cloud
- Leverage MACsec encryption for private link protection at high speeds (100G)
- Leverage the working config examples provided in this session
- Evaluate the level of encryption extension needed into the cloud to meet compliance requirements for the enterprise
- Evaluate ThousandEyes visibility that relate to networking in public clouds

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

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

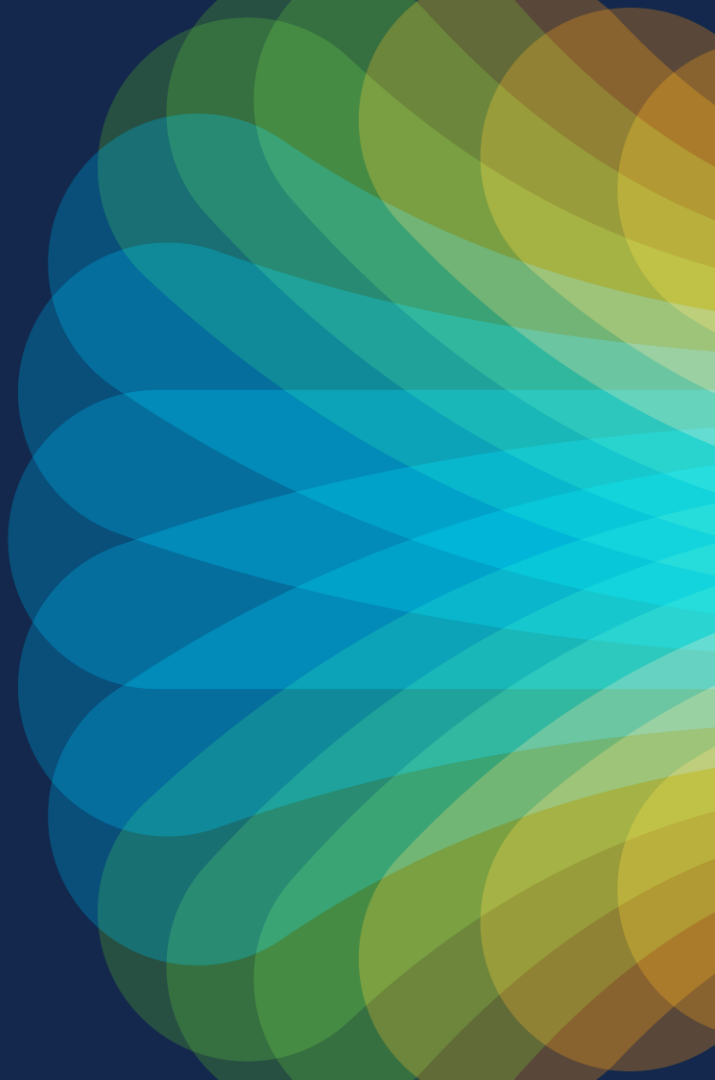
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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 www.CiscoLive.com/on-demand

The bridge to possible

Thank you



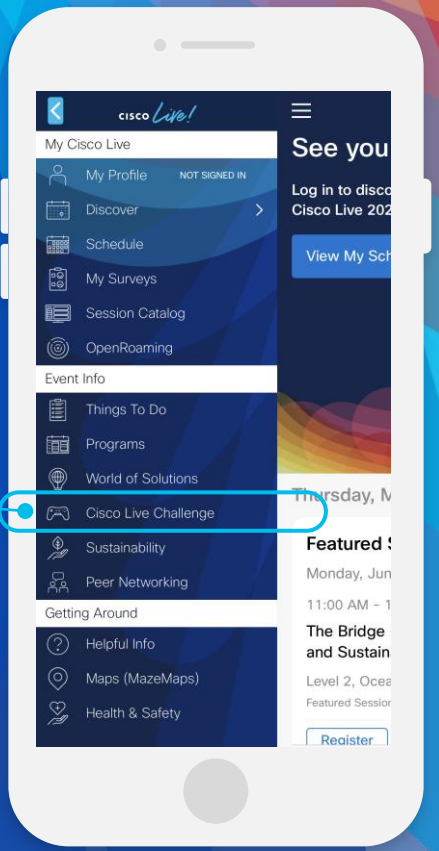
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!


cisco Live!
Let's go
#CiscoLive