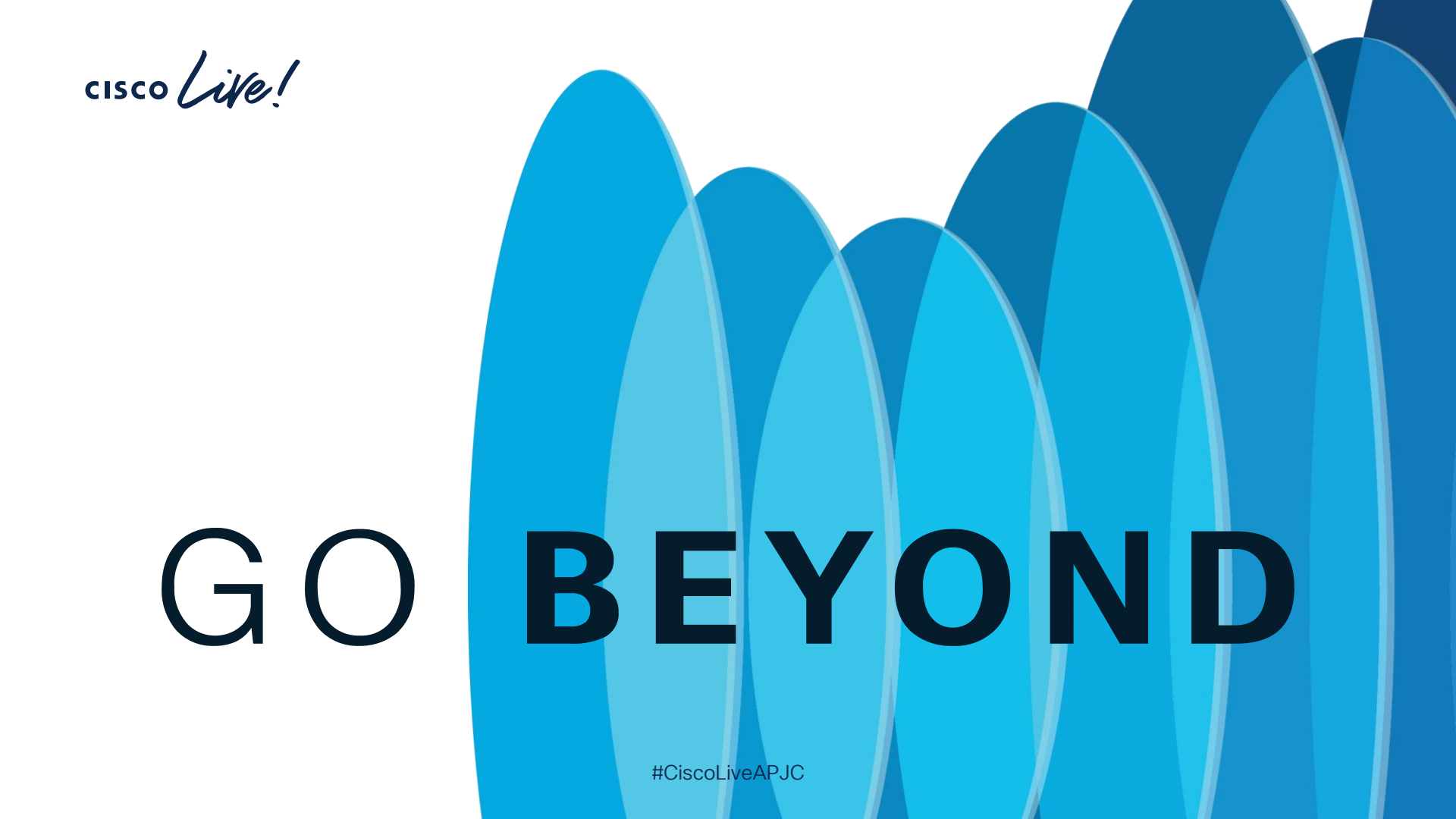

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Securing High Speed Private Link to Public Cloud Providers

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

Craig Hill
Distinguished Solution Engineer
U.S. Public Sector, CTO Office
CCIE #1628
@netwrkr95
https://www.linkedin.com/in/crhill/

BRKNWT-2126

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

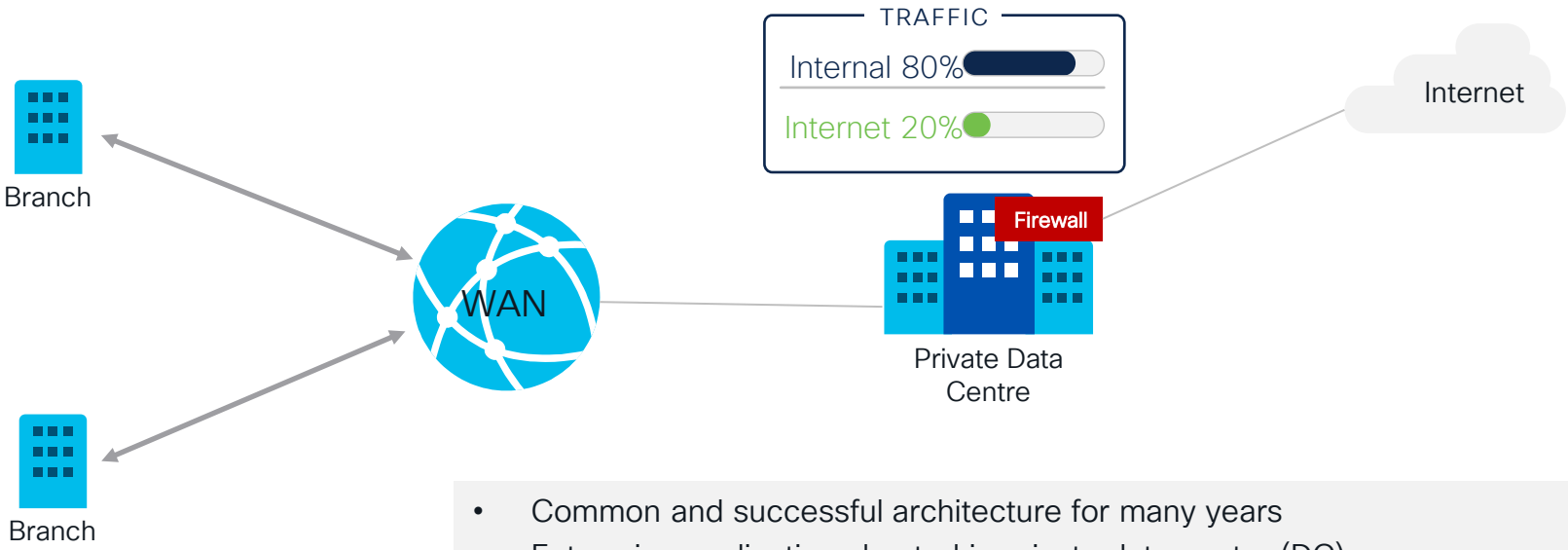
Agenda

- 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
- Advanced Encryption with Quantum Resistance
- Summary and references

WAN Evolution with Application Transition to the Cloud

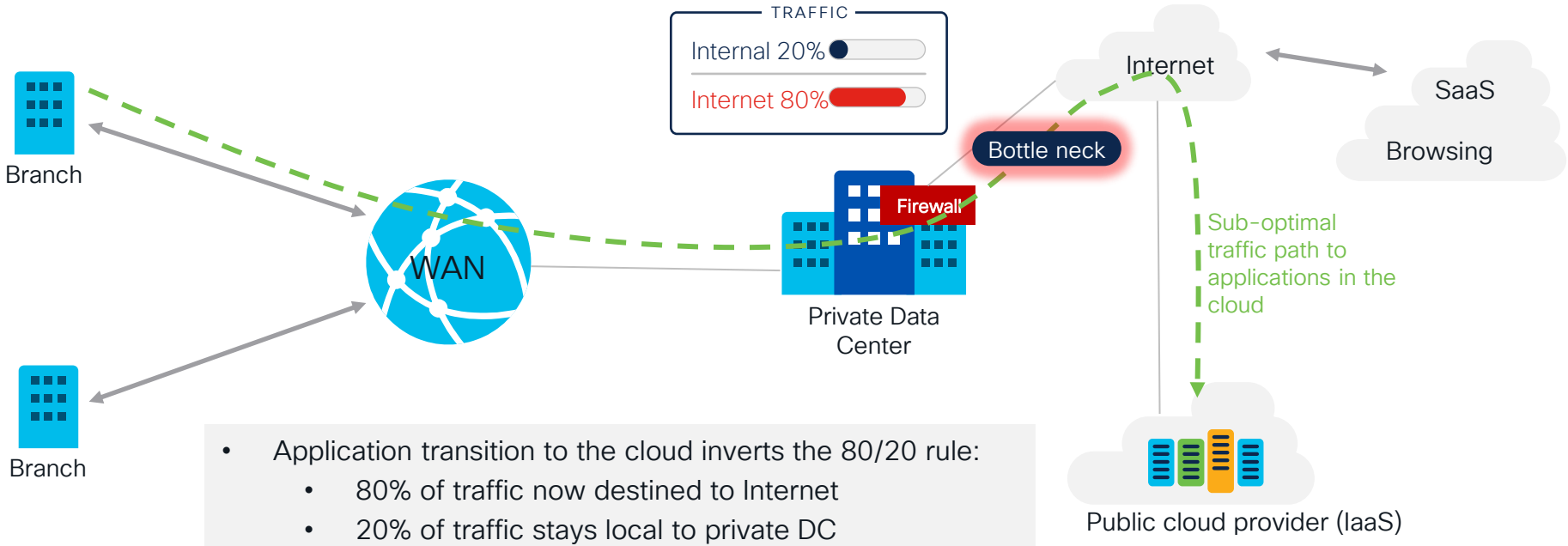
cisco Live!

Evolution of app hosting in the enterprise



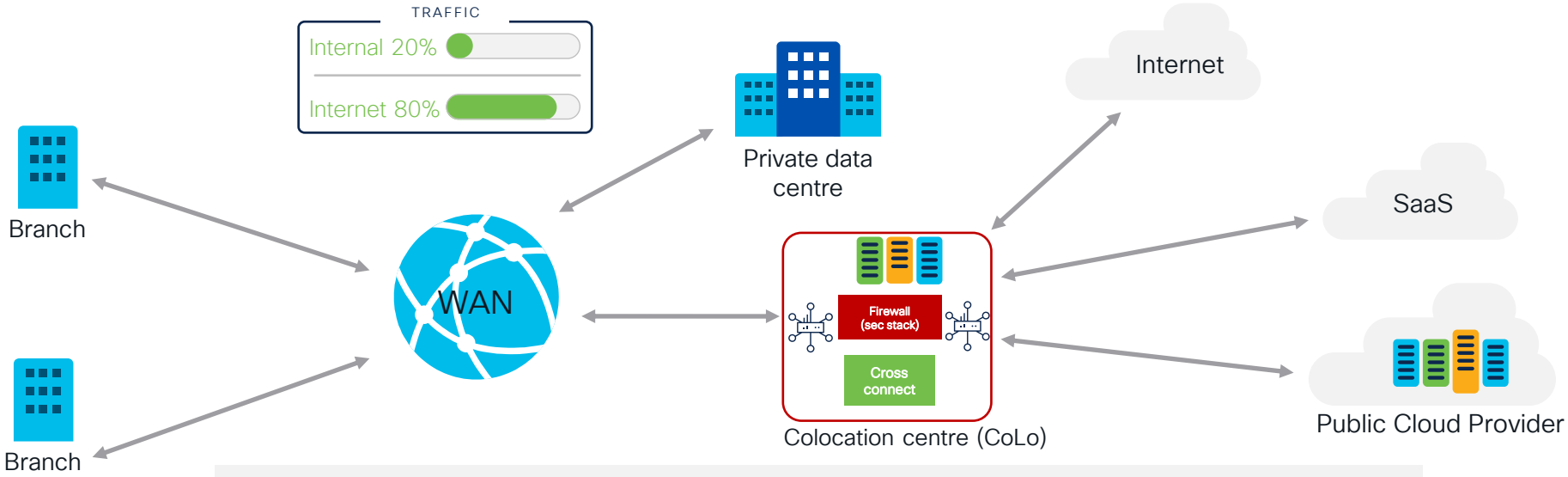
- Common and successful architecture for many years
- Enterprise applications hosted in private data centre (DC)
- ~ 80% of branch traffic – destined to private DC applications
- ~ 20% of branch traffic – destined to Internet through the FW
- Aligns with 80/20 rule – apps / internet

Evolution of app hosting in the enterprise



- 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

Carrier neutral / co-location facilities

A “CoLo” is a facility which allows interconnection between multiple telecommunication carriers and/or colocation providers around the globe, vary in service and connectivity offerings, and vary in size and power.

Benefits:

- Access to the largest cloud providers globally
- Carrier neutral encourages competition leading to better pricing and services
- Time to connectivity is accelerated
- Provides private data center hosting services

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 behaviour 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

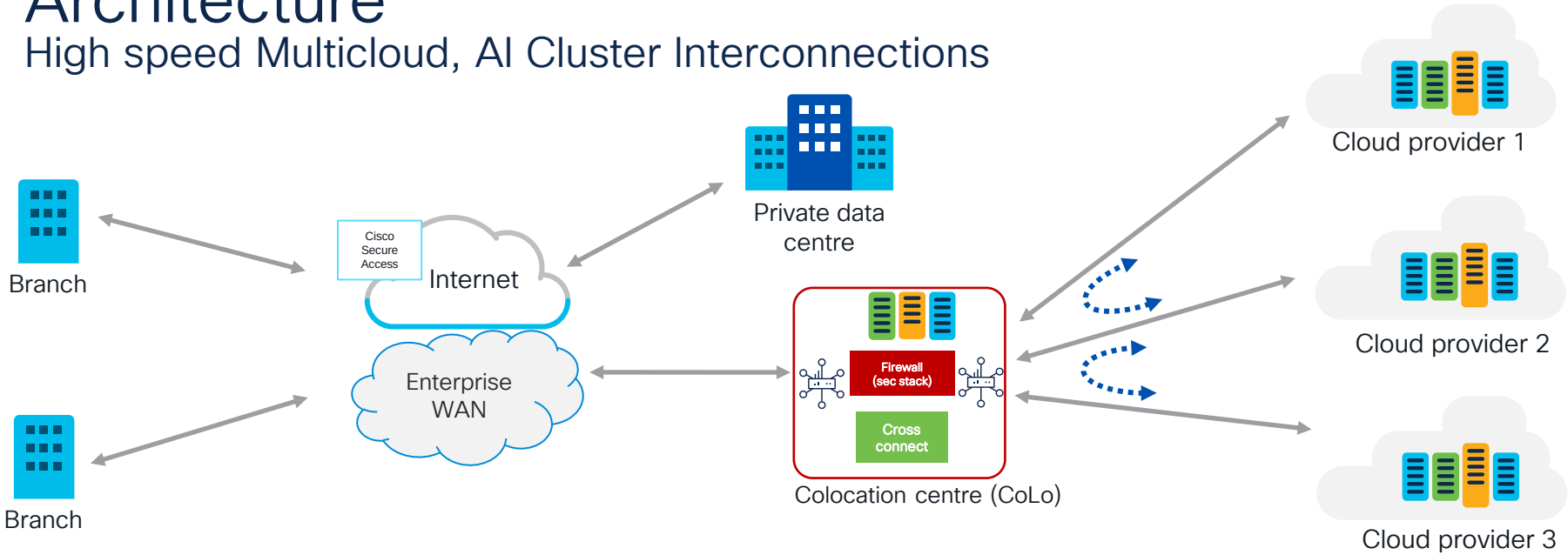
- Enterprise owns and maintains their own WAN?
- % Apps hosted in the cloud?
- Pace of transition to cloud?
- % SaaS? % IaaS?
- Sensitivity of application to latency for best user-to-app experience?

“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)

Evolving Use Cases for the CoLo Centric Architecture

High speed Multicloud, AI Cluster Interconnections



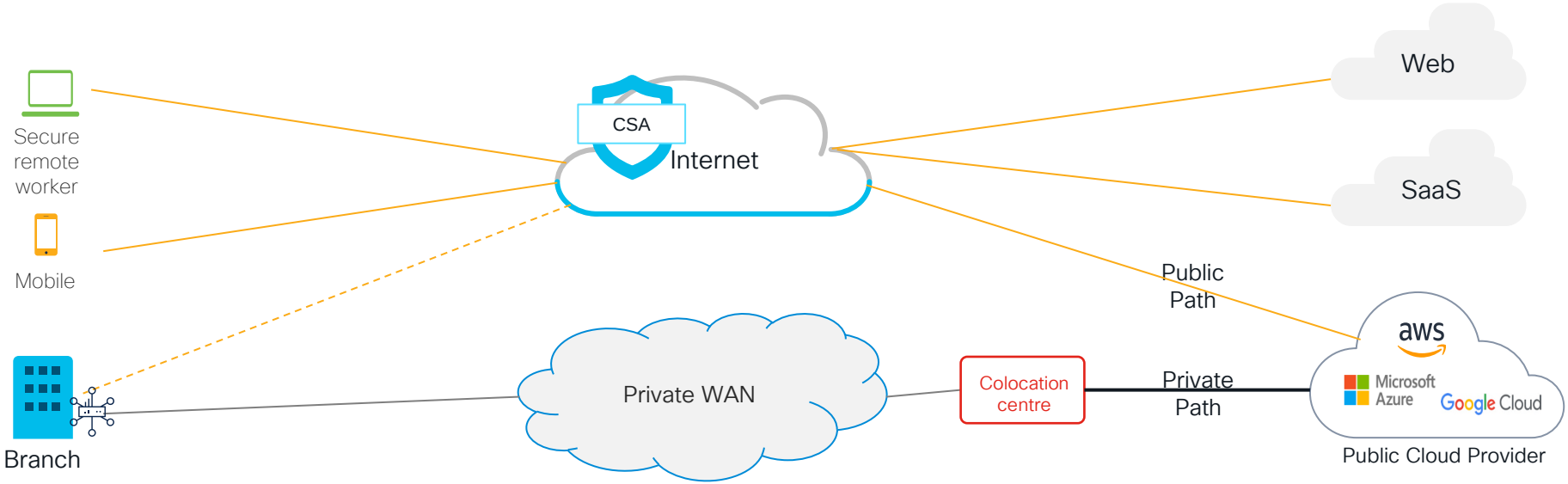
- The CoLo is the centre of the universe for multicloud private link
- Targets customers wanting “high speed underlay” between each cloud provider (multicloud)
- Enterprise can establish own security policies for inter-cloud provider comms
- Early discussion usage for when AI clusters are distributed across geo locations

Options for Connecting to Cloud Providers

Public and Private Network Access Options

cisco Live!

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

Public path
Private path
Alternative path (from primary)

Option for connecting into the cloud providers
"Public Internet" (i.e., Front Door 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 behaviour (loss, latency, jitter)
- Sustained BW requirements available indeterministic
- Impact on user experience for applications needing tighter SLAs

Options for connecting into the cloud providers
"Private Link" (i.e., Back Door 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

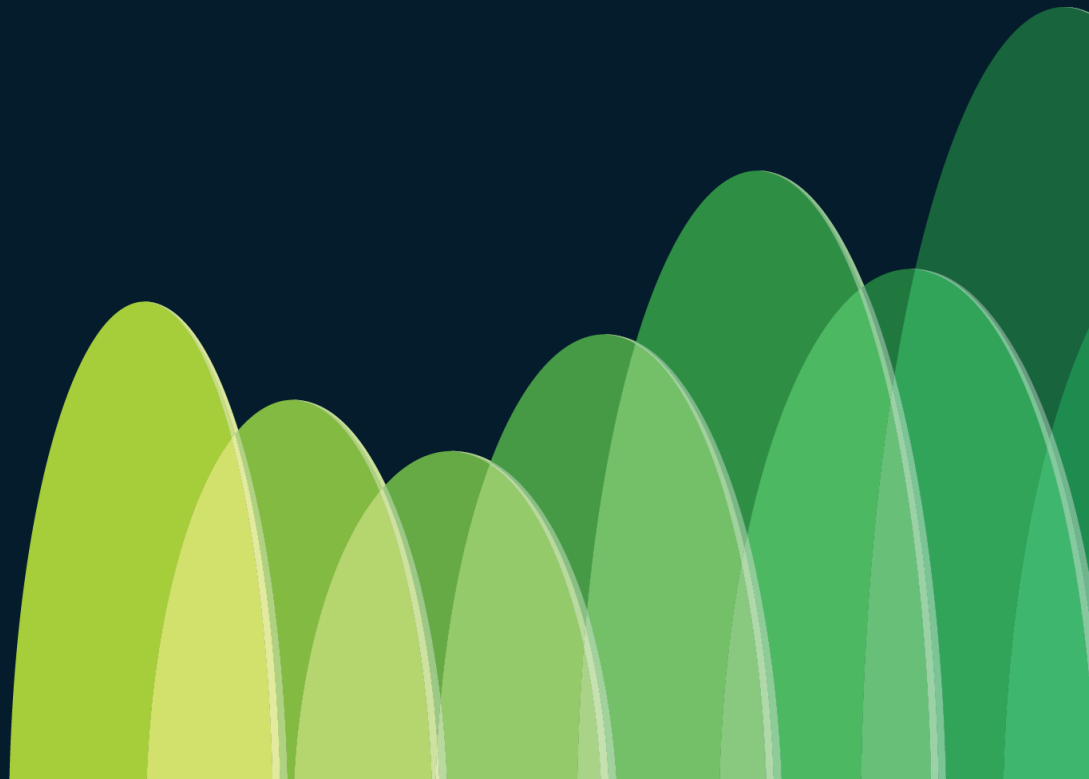
Challenges: Private links into the Cloud Providers?

- Cost, Security of those links, complexity of setup

CoLo Presence: Private links to CSP + Enterprise presence and control

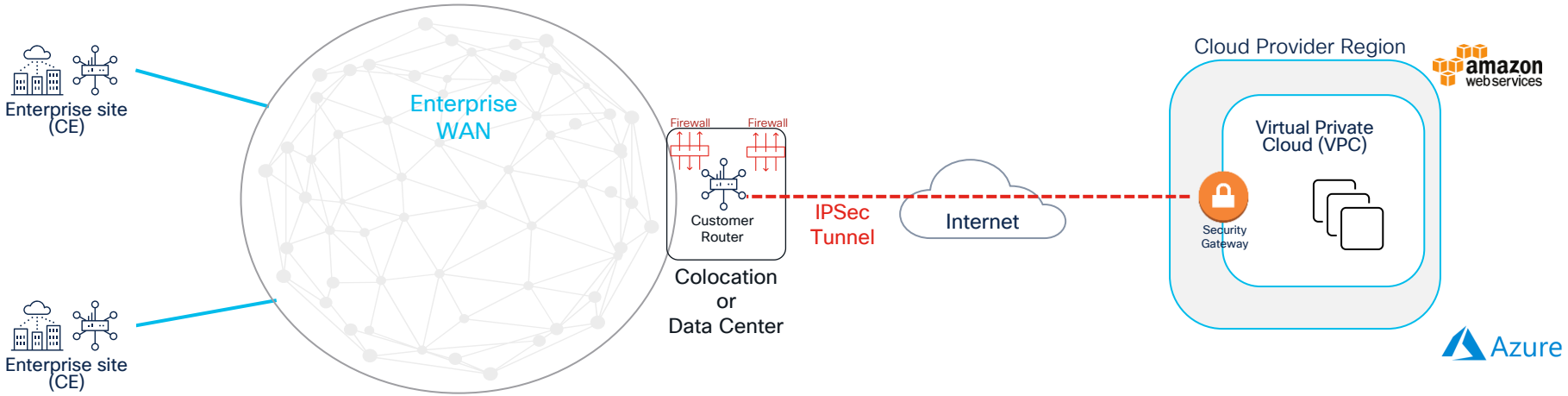
- Offers flexible "Cloud On Ramp" access to any XaaS, carrier, cross-connect, ISP peer
- Multicloud Prep: Sets the table for multi-cloud support (current or future)

Public Internet Access Options

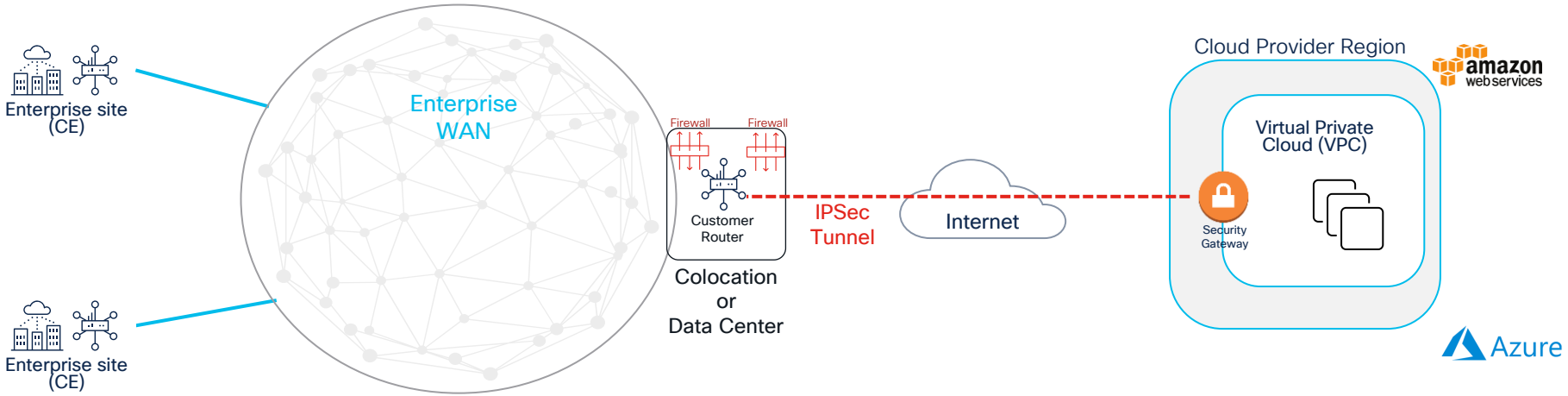


cisco Live!

IPSec VPN tunnels into the cloud provider



IPSec VPN tunnels into the cloud provider



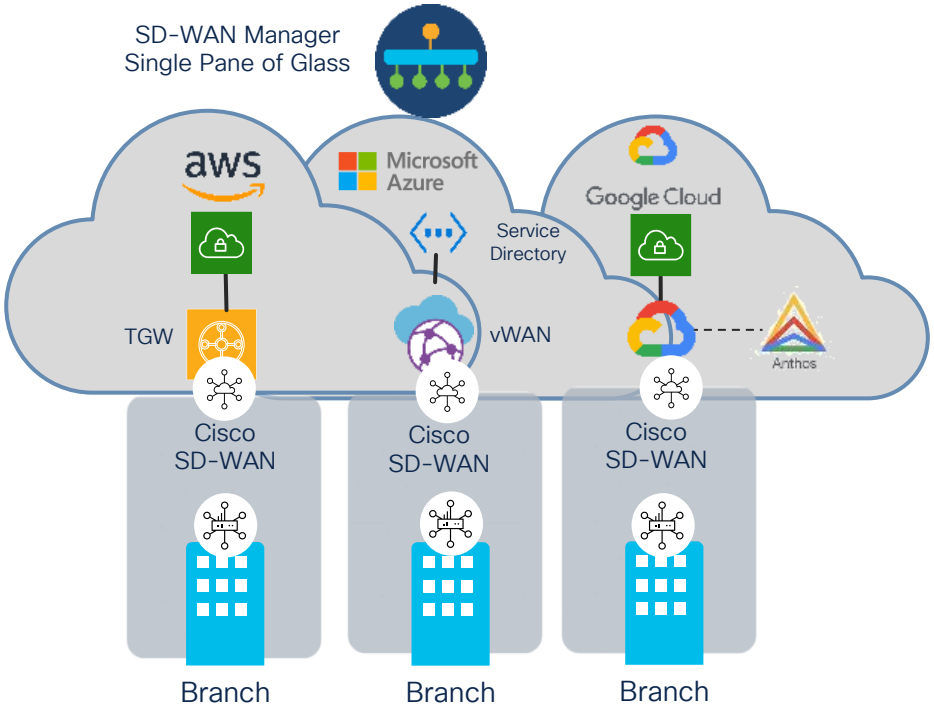
Key Benefits

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

Deployment Targets

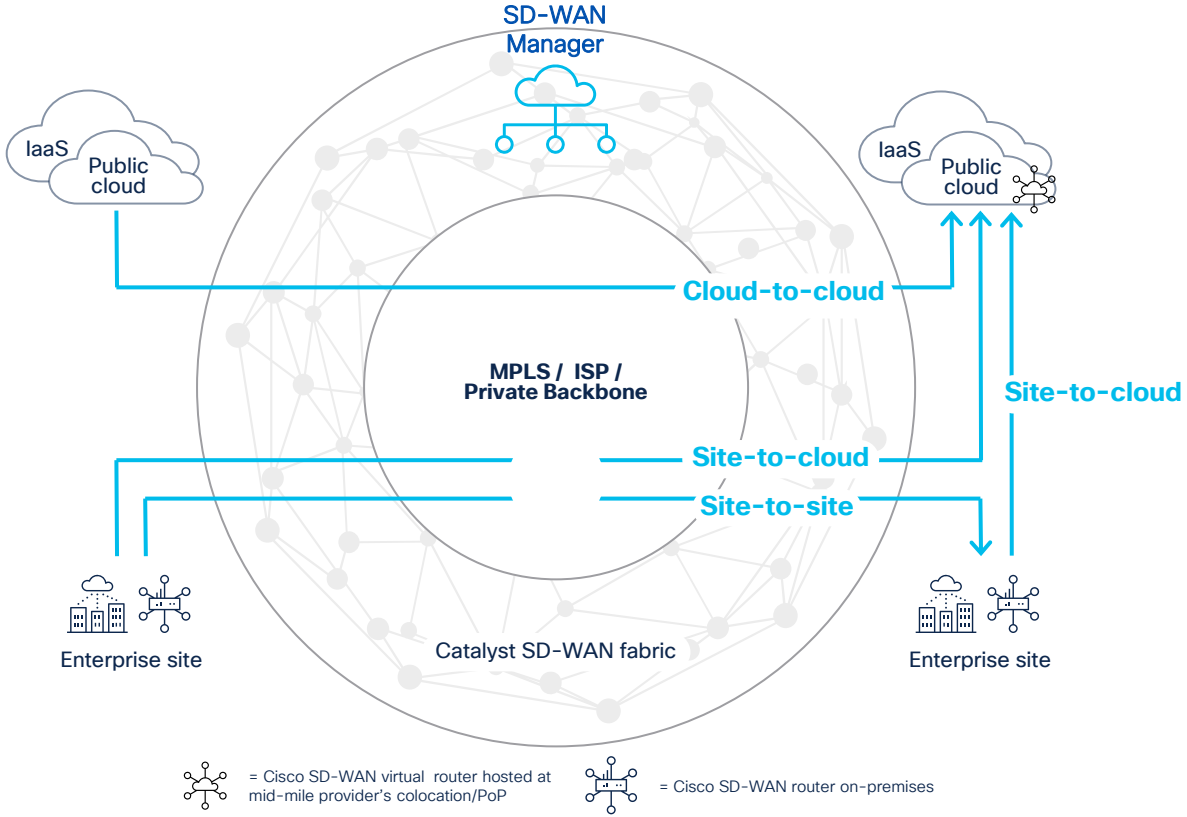
- Targets low-scale connections into the cloud
- High BW and deterministic QoS not needed
- Ideal for lab environments and smaller workloads
- Must always cautious of egress charges

Cloud OnRamp Multicloud Using Cisco SD-WAN



cisco Live!

Cisco SD-WAN Cloud OnRamp (IaaS)



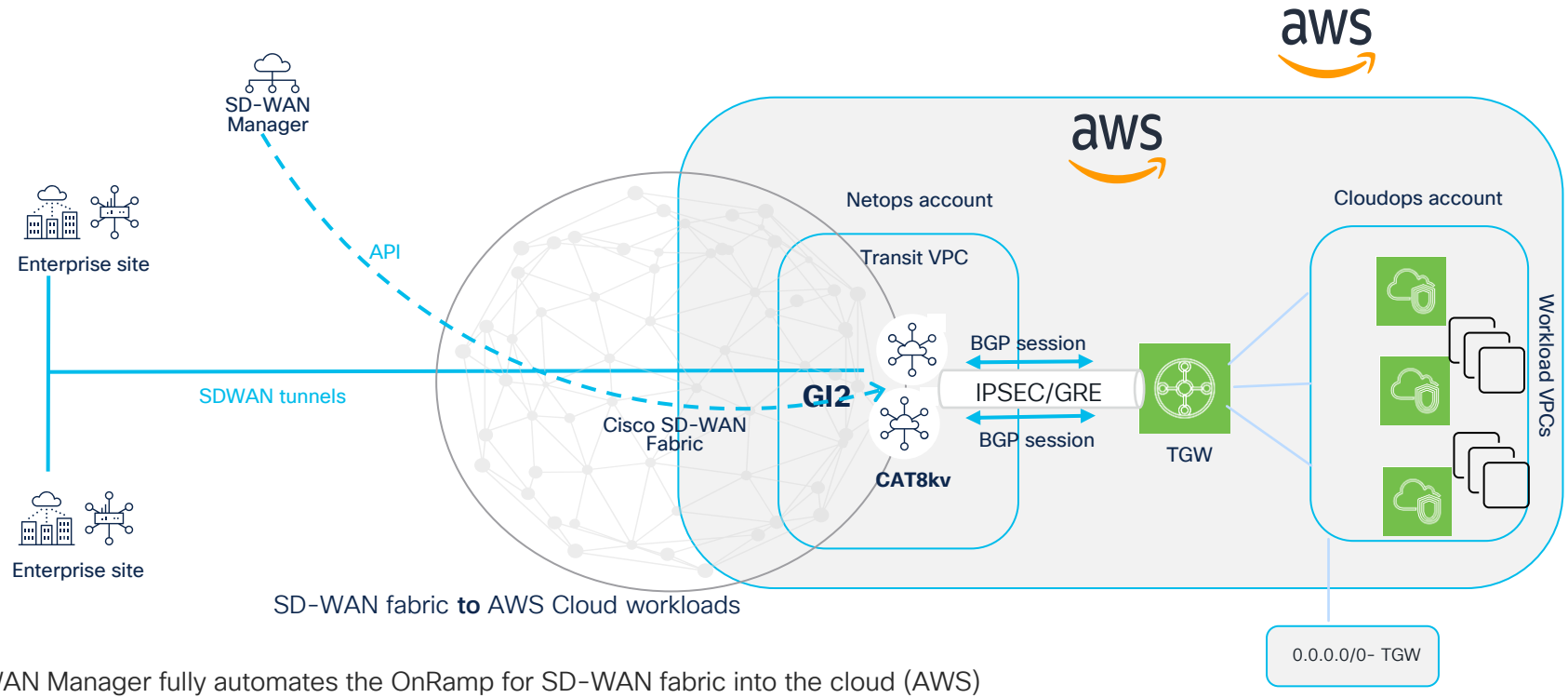
Key Advantages

- 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

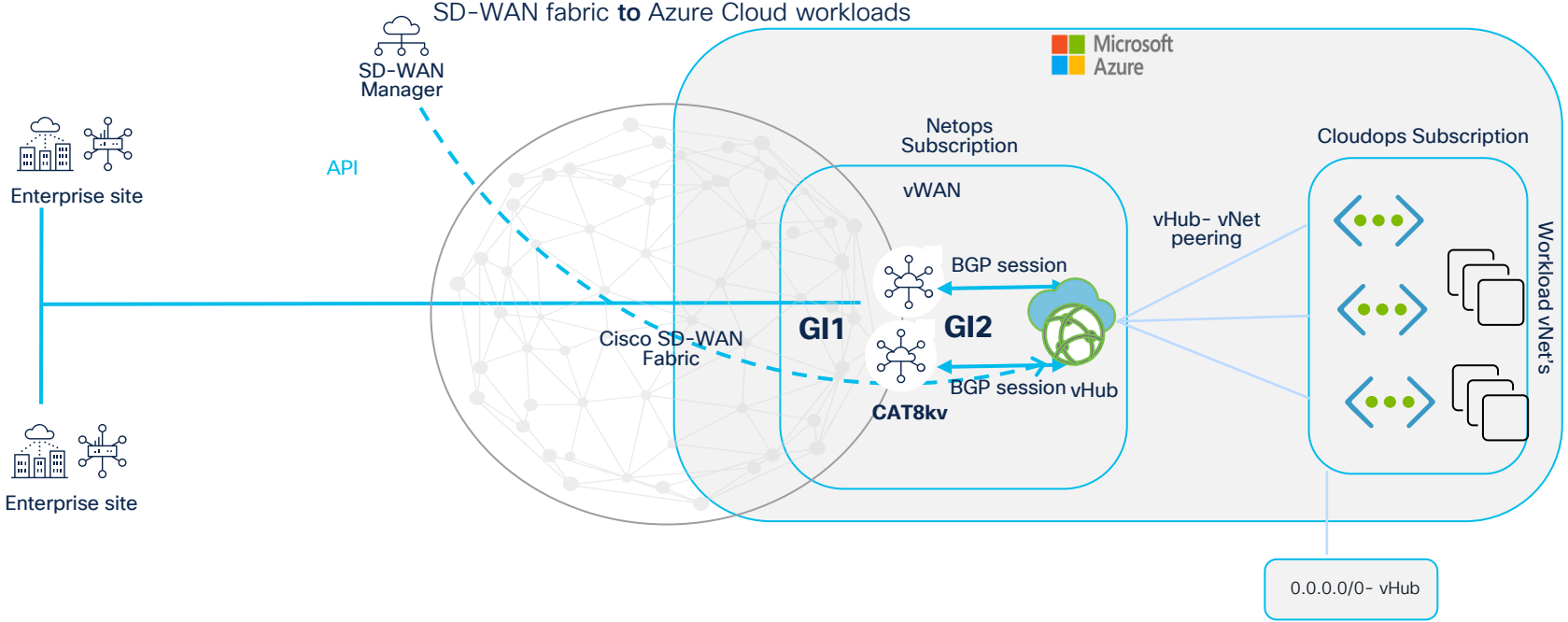
- Already operating and own SD-WAN
- Extends visibility vantage point into the public cloud for network operations
- Automation and (Infra as Code) direction for operations
- Sets table for Multicloud transition

Example: AWS - site-to-cloud



- SD-WAN Manager fully automates the OnRamp for SD-WAN fabric into the cloud (AWS)
- GRE adds 4x the BW improvement using Connect to TGW from Catalyst 8000v
- If needed, Cat8000v can drive to 30 Gbps throughput (c5n.18xlarge) @ 1400B packets

Example: Azure - site-to-cloud



- SD-WAN Manager fully automates the OnRamp for SD-WAN fabric into the cloud (Azure)
- CAT8k Network virtual appliances are hosted in vhub, running BGP to vHub control plane to learn vNet mappings

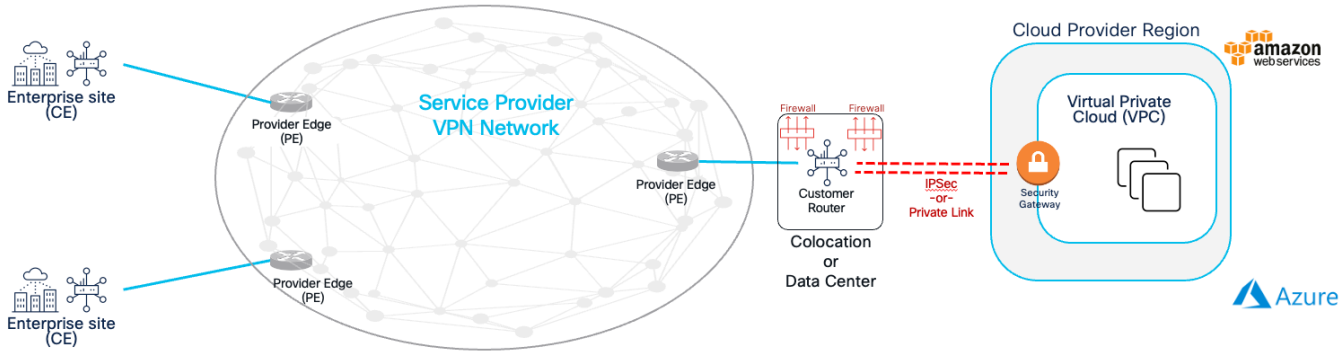
Private Link Connection to the Public Cloud

Private Access via Carrier Private IP VPN Service

cisco Live!

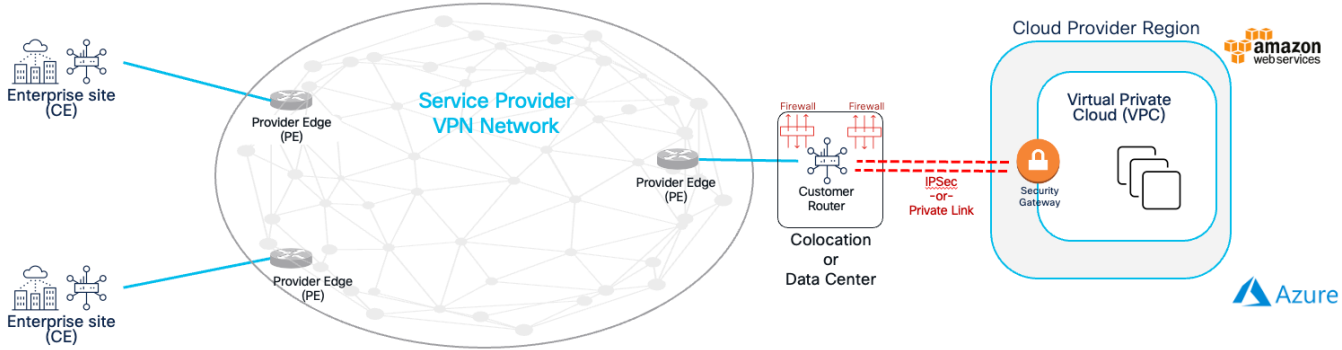
IP VPN service connectivity to the public cloud

Manual extension

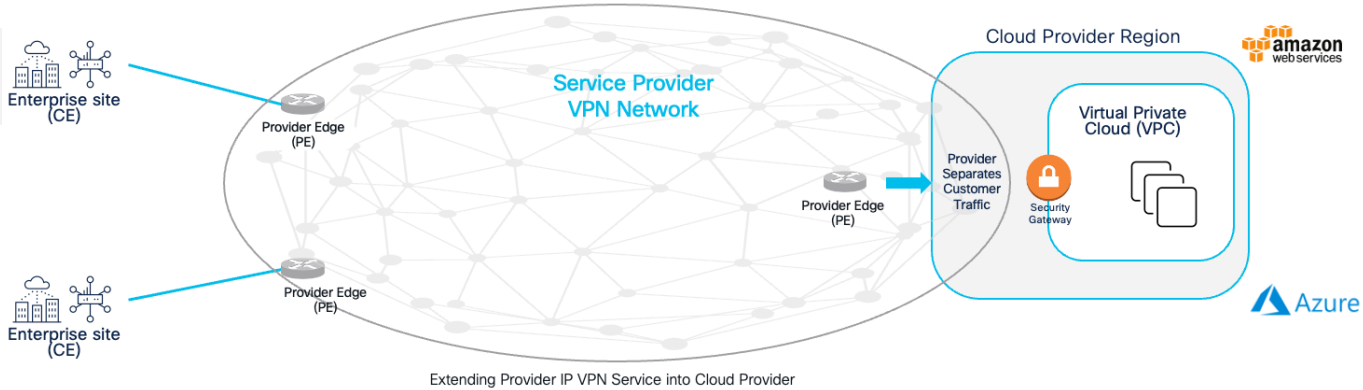


IP VPN service connectivity to the public cloud

Manual extension



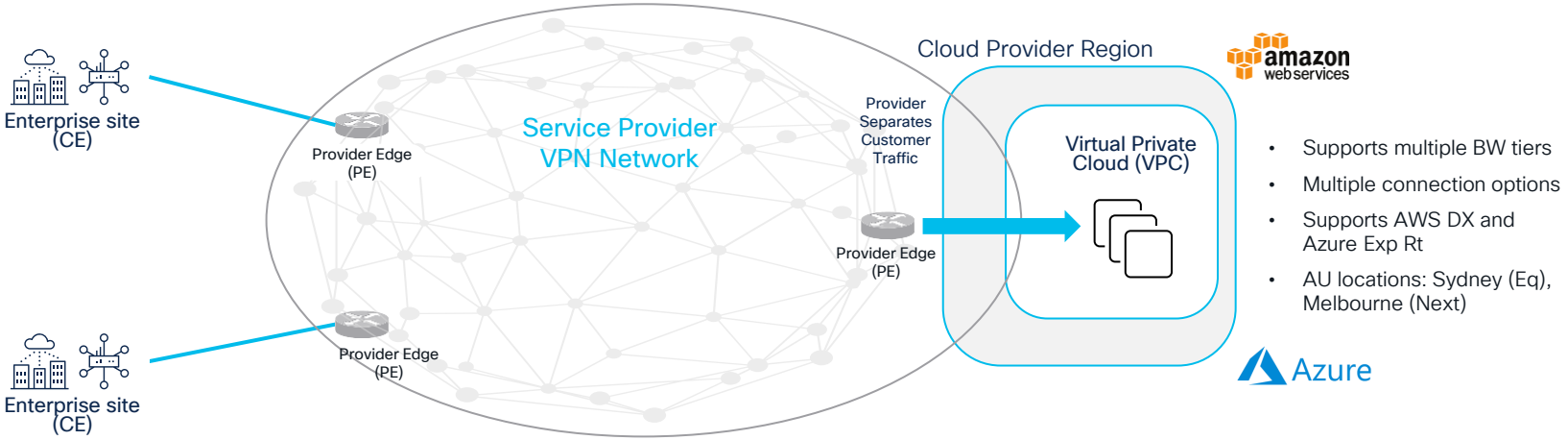
IP VPN extension



Extending Provider IP VPN Service into Cloud Provider

Example: Telstra Cloud Connector™

IP VPN service connectivity to the public cloud



Extending Provider IP VPN Service into Cloud Provider

Key Benefits

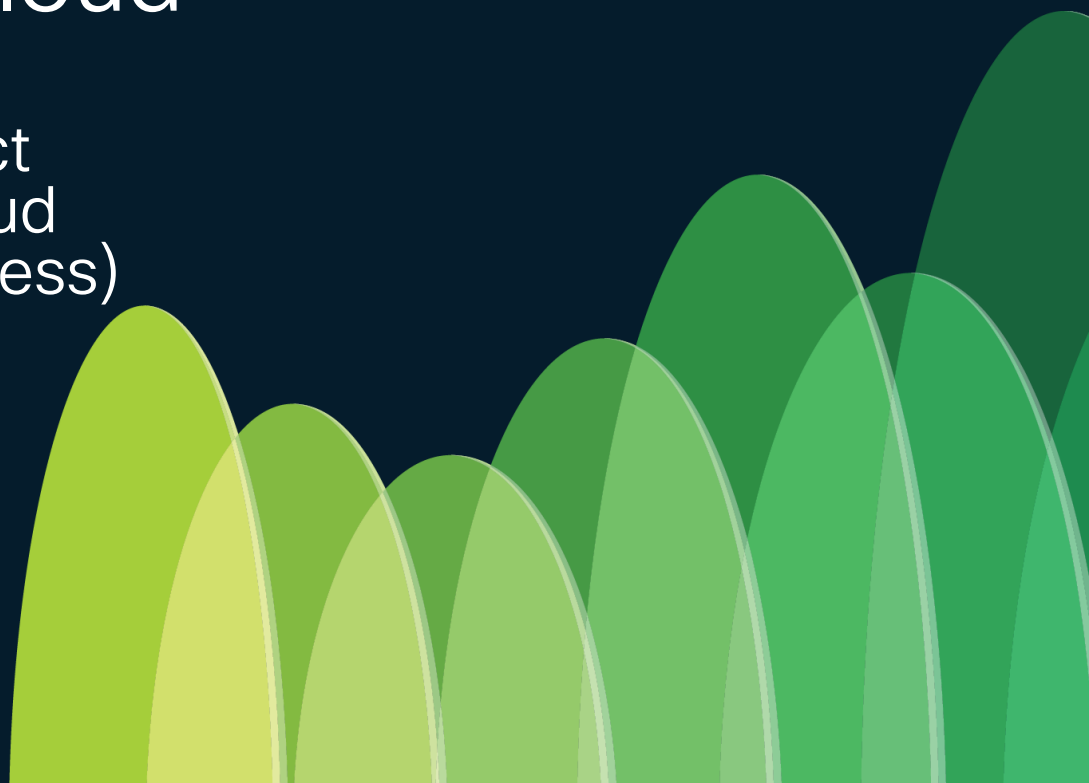
- Ideal integration with “SD-WAN Multicloud” overlay
- Leverage existing secure IP VPN transport (if utilised today)
- Leverage existing transport SLA’s in place, to public cloud
- Reduced complexity for connections into public cloud
- AU Provider offerings: Optus, Telstra Cloud Connector™

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 Options to the Cloud

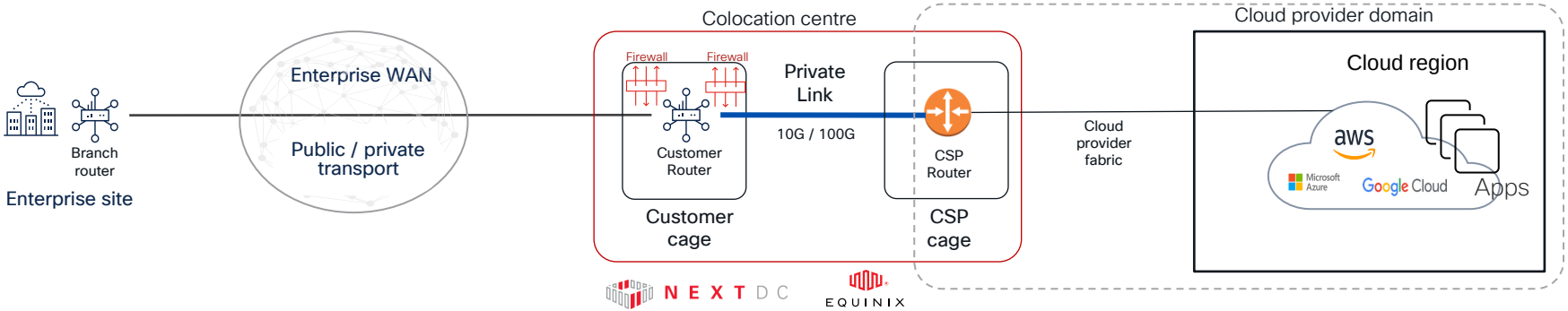
Private High Speed Direct Connections To The Cloud Provider (Back Door Access)



Private link service to public cloud provider

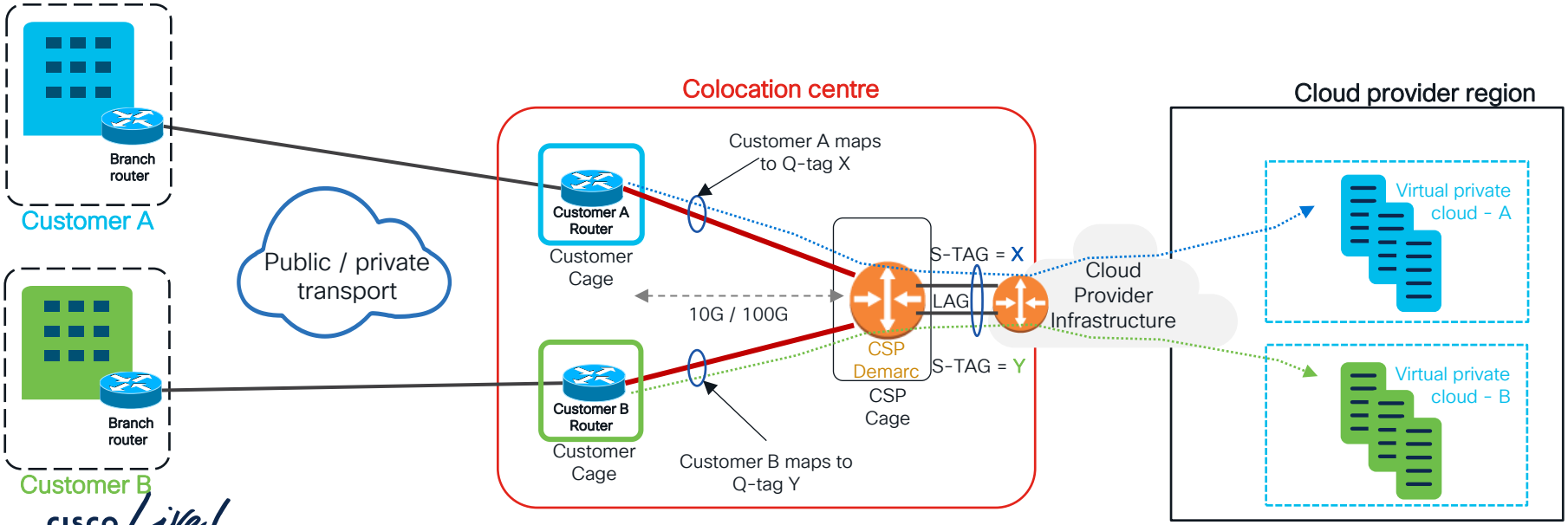
Key Offerings and Advantages

- 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



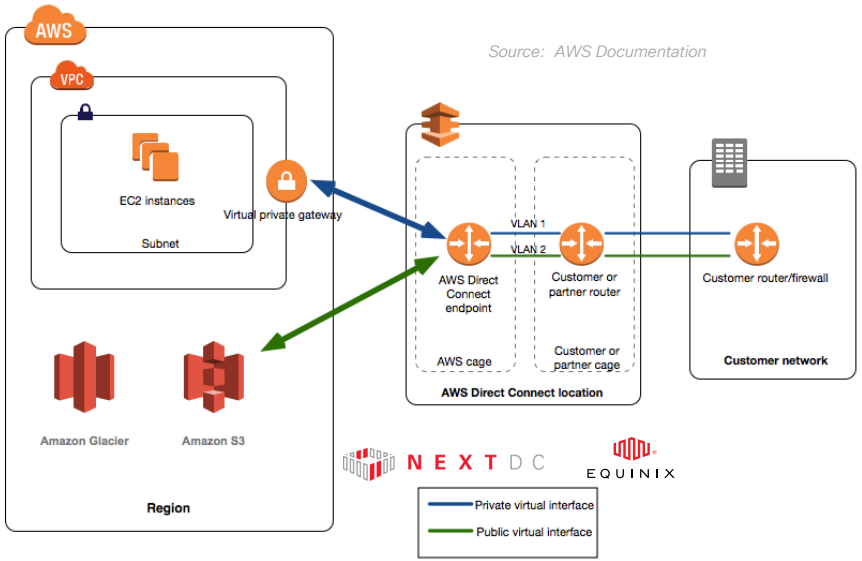
Private link service to public cloud provider
Anatomy of the service

- 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)

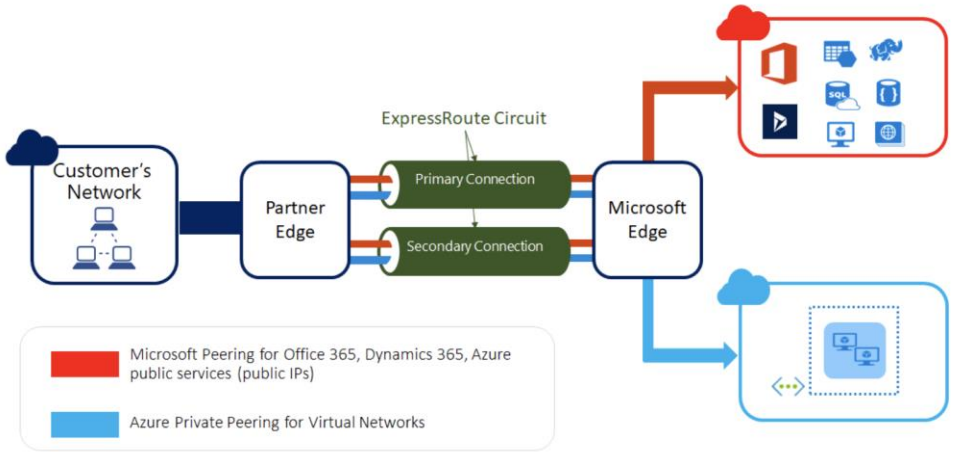


Source: https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

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

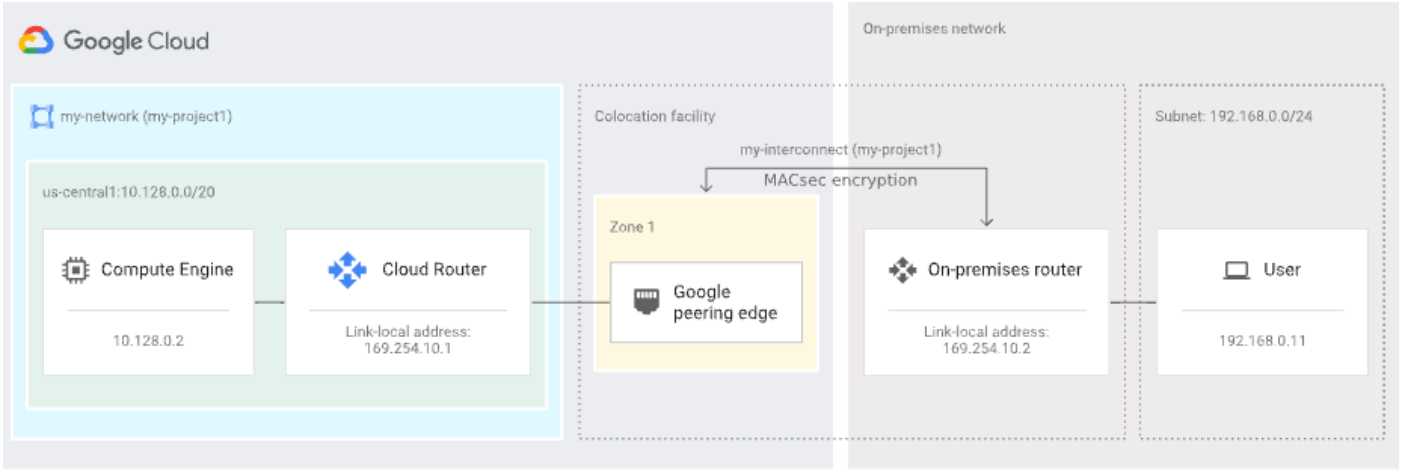
Source: Azure Documentation



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

Example: Google Cloud Interconnect

- Dedicated connection between the enterprise and customer VPC
- Traffic never traverses the public internet, and no NAT or VPN tunnels required
- 10G and 100G dedicated connections (Max: 8 x 10Gbps, and 2 x 100Gbps)
- Details at link below:



Source: Google Cloud Documentation

Google Docs Link: https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview

Securing High-Speed Private Links into the Public Cloud Providers

cisco Live!

MACsec for Cloud Interconnect overview

Google Cloud

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.

Encrypting ExpressRoute for improved security

MACsec

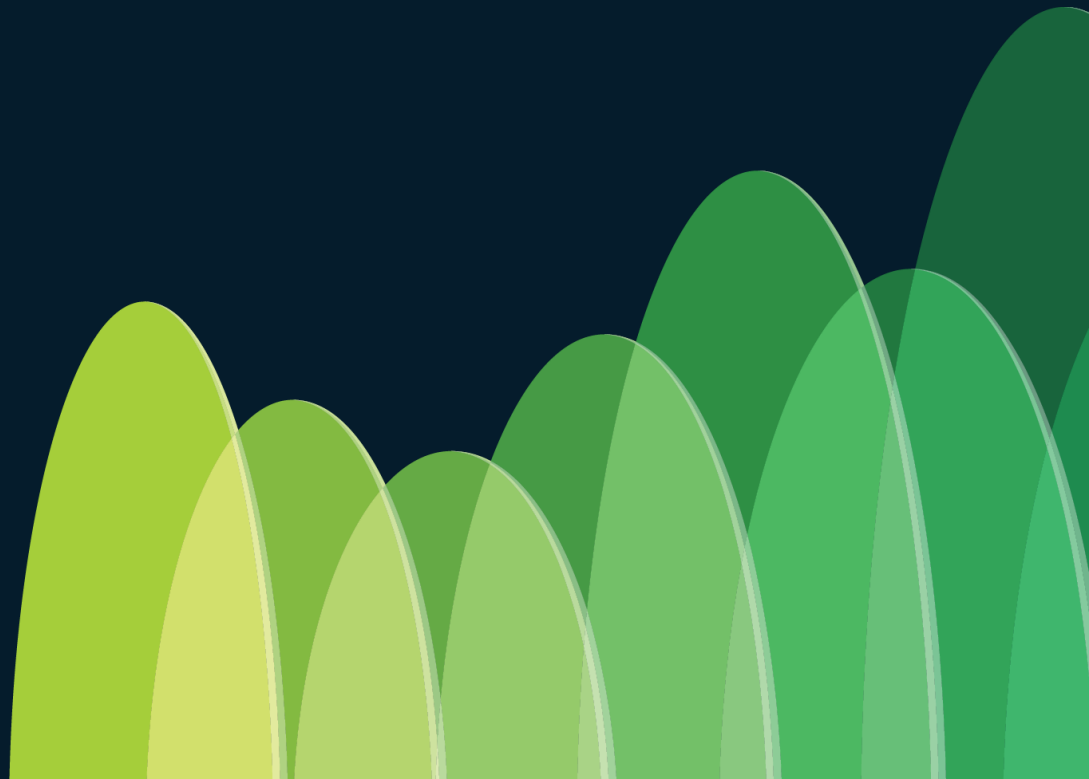
Let's start with MACsec as this solution can only apply to ExpressRoute Direct. With ExpressRoute Direct, customers establish a layer 2 private connection from their edge to Microsoft Enterprise Edge in Azure. Once you have connectivity at layer 1, your layer2 is setup which allows you to then create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

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.

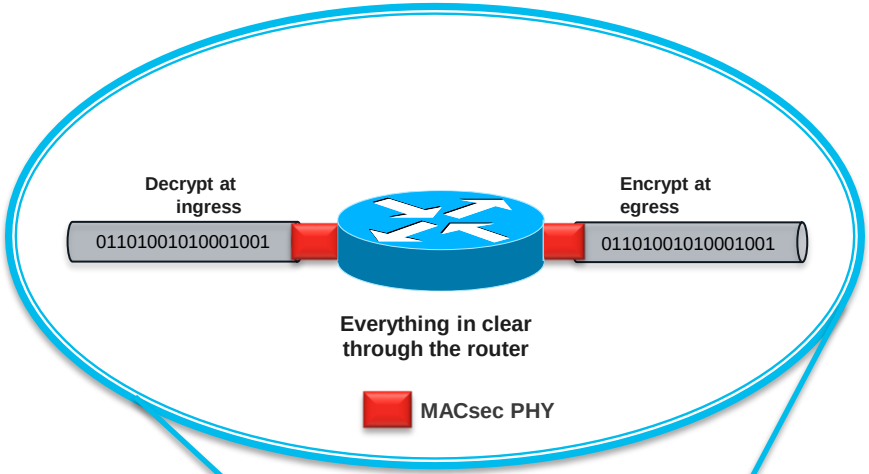
“MACsec 101”

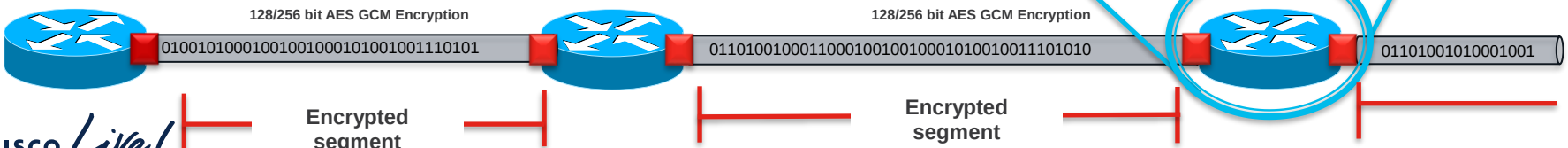


cisco Live!

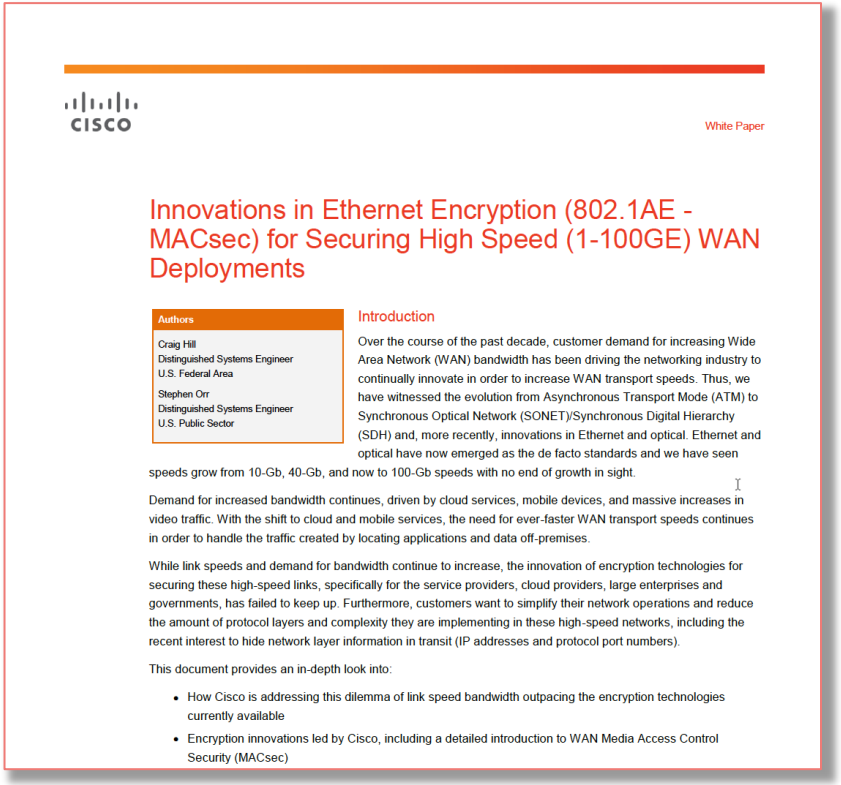
What is MAC Security (MACsec)?
Hop-by-hop encryption via IEEE 802.1AE

- 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)





White Paper – MACsec in the WAN



cisco

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)

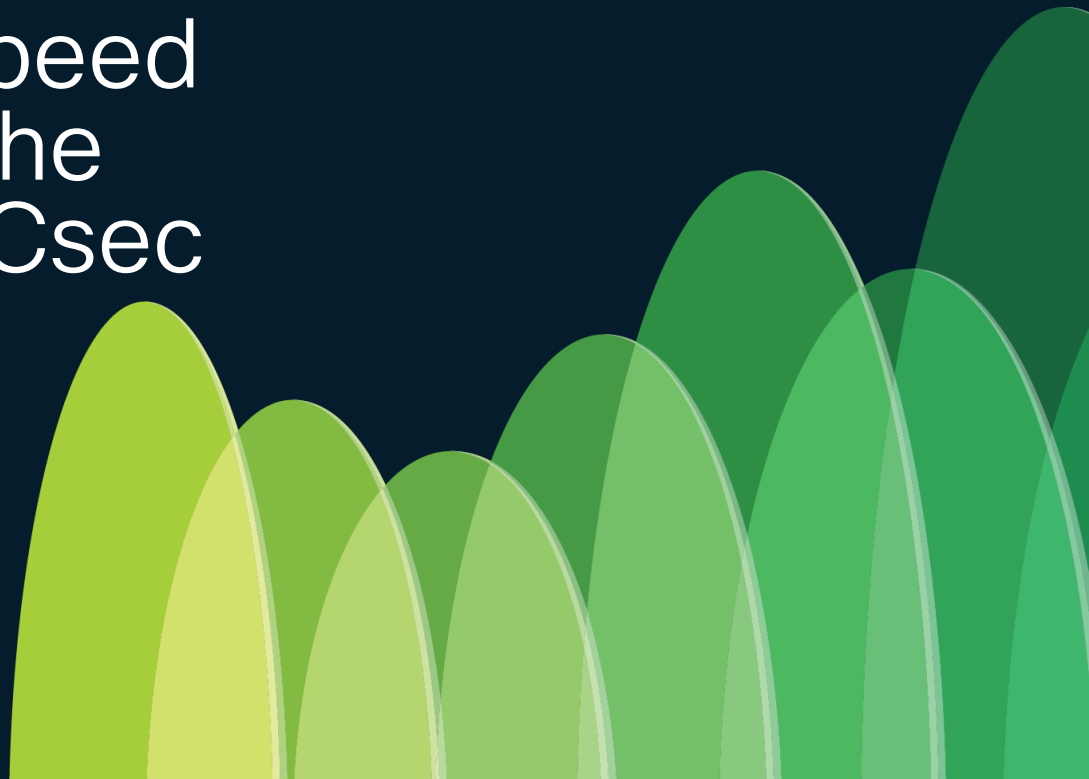
BRKRST-2309 – Introduction to WAN MACsec

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

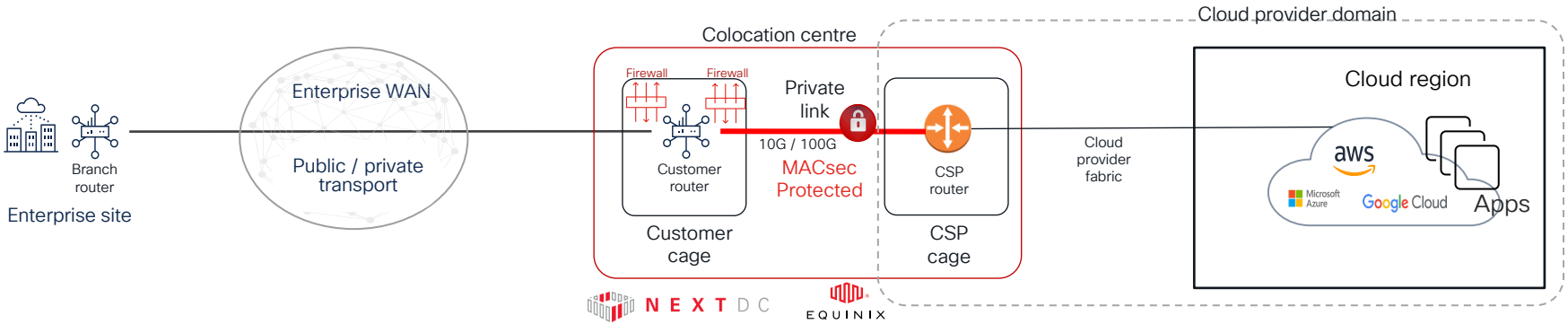
Securing High Speed Private Links to the Cloud Using MACsec



cisco Live!

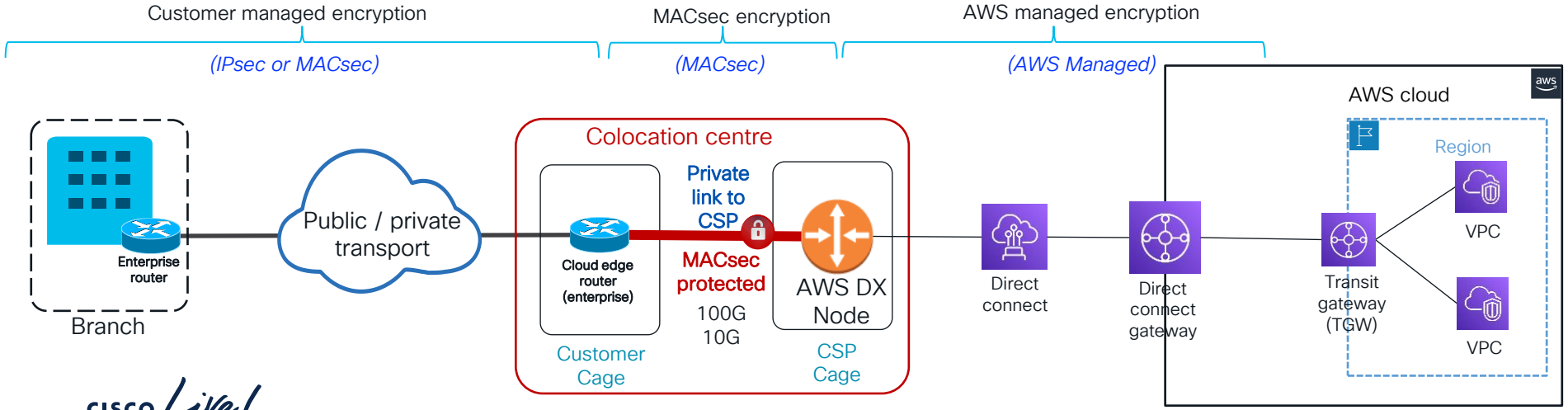
Cloud provider secure private link access
Using MACsec Encryption (10/100G)

- Major cloud providers now offer MACsec to their private link service
- Typical speeds are 10Gbps/100Gbps options (sub-rate for “hosted”)
- Targets customers wanting dedicated BW with encryption to the service
- Assumes customer has presence (or access into) in Co-Location space
- Partner options available on the cloud providers docs site

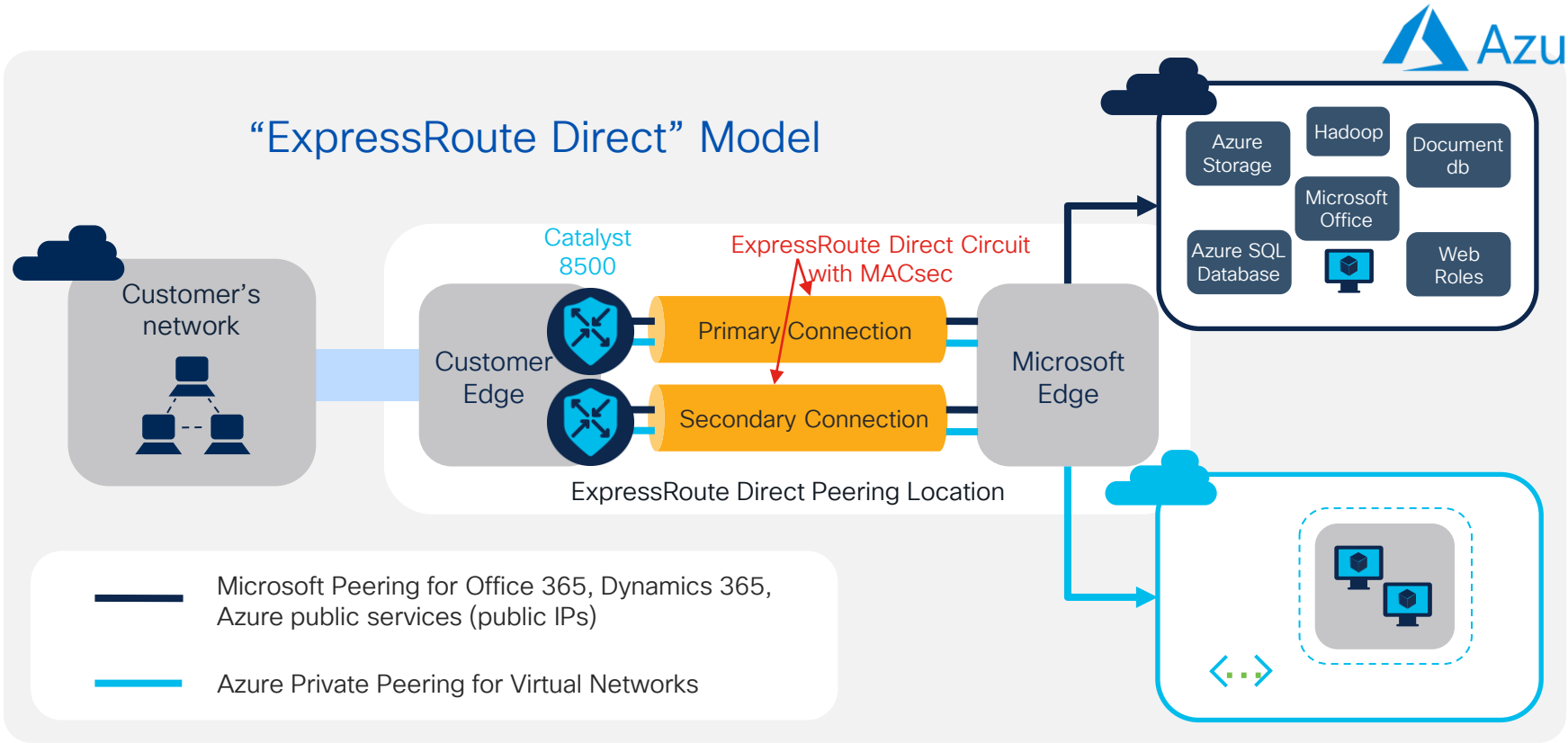


Example: AWS Direct Connect using MACsec Security

- MACsec encryption is used between customer-owned edge into AWS DX node
- Speed options are 10G / 100G dedicated link access
- Enterprise manages their own encryption into the partner colocation centre



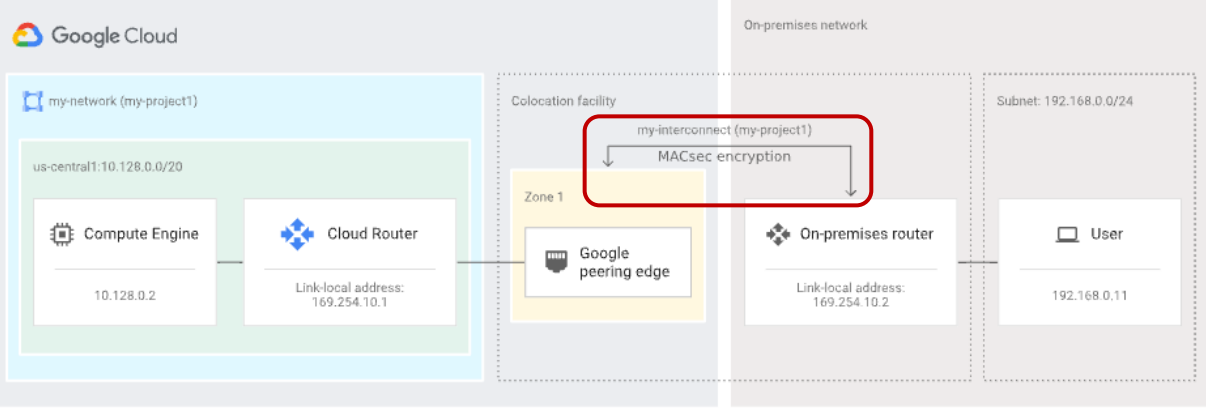
Example: Azure ExpressRoute Direct using MACsec



Example: Google Cloud Interconnect with MACsec
Private link using MACsec to Google Cloud

Google Cloud

- 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



Source: Google Cloud Docs

Google Docs Link: https://cloud.google.com/network-connectivity/docs/interconnect/concepts/macsec-overview

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.,		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		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

Google Dedicated Interconnect Sites (MACsec)
Location: Oceania

Africa | Asia | Oceania | EMEA | India | North America | South America

The Oceania geographic area supports the following regions:

- australia-southeast1 (Sydney) ✓
- australia-southeast2 (Melbourne) ✓

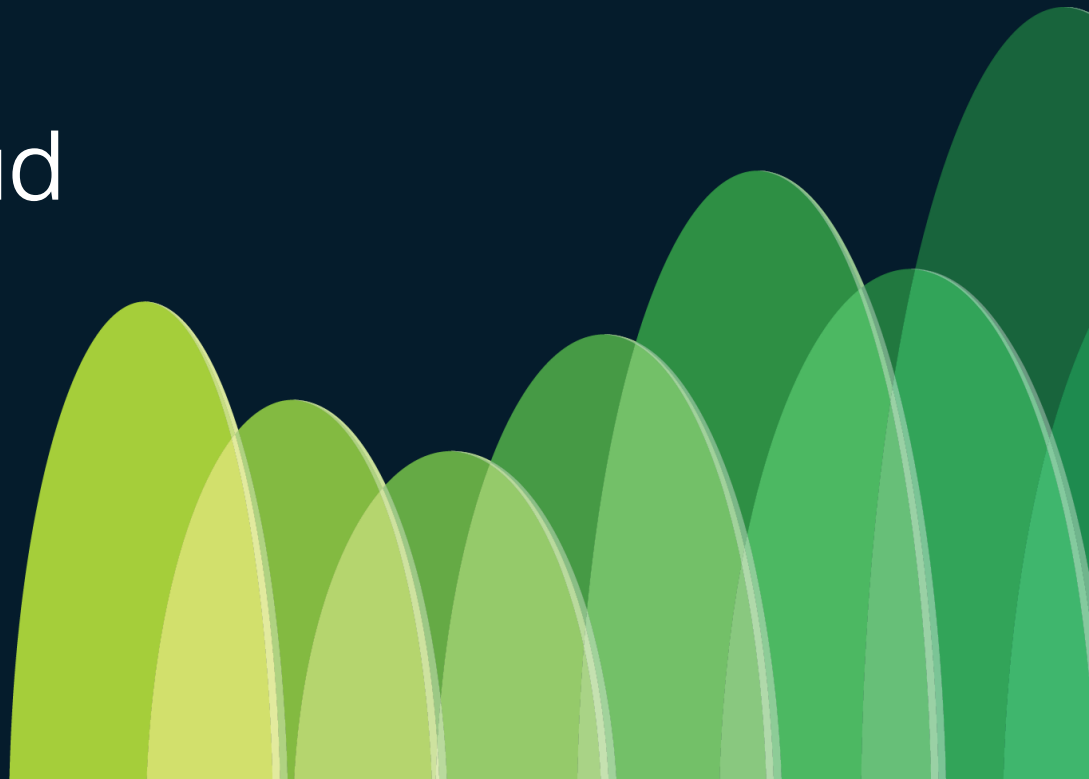
Metropolitan area	Colocation facility name	Facility	Low-latency region	Link type & MACsec support [M]
Auckland	akl-zone1-1353	Vocus Auckland - Albany		10 Gbps [M] 100 Gbps [M]
Auckland	akl-zone2-1353	Vocus Auckland - Albany		10 Gbps [M] 100 Gbps [M]
Brisbane	bne-zone1-4688	NEXTDC B2		10 Gbps [M] 100 Gbps [M]
Brisbane	bne-zone2-4688	NEXTDC B2		10 Gbps [M] 100 Gbps [M]
Canberra	cbr-zone1-9378	Equinix CA1 - Canberra		10 Gbps [M] 100 Gbps [M]
Canberra	cbr-zone2-9378	Equinix CA1 - Canberra		10 Gbps [M] 100 Gbps [M]
Melbourne	mel-zone1-1988	Equinix ME1/ME2 - Melbourne	australia-southeast2	10 Gbps [M] 100 Gbps [M]
Melbourne	mel-zone2-1988	Equinix ME1/ME2 - Melbourne	australia-southeast2	10 Gbps [M] 100 Gbps [M]
Melbourne	mel-zone1-4843	NEXTDC M2	australia-southeast2	10 Gbps [M] 100 Gbps [M]
Melbourne	mel-zone2-4843	NEXTDC M2	australia-southeast2	10 Gbps [M] 100 Gbps [M]
Perth	per-zone1-5749	Equinix PE2 - Perth (formerly Metronode Perth 2)		10 Gbps [M] 100 Gbps [M]
Perth	per-zone2-5749	Equinix PE2 - Perth (formerly Metronode Perth 2)		10 Gbps [M] 100 Gbps [M]
Sydney	syd-zone1-1605	Equinix Sydney (SY3)	australia-southeast1	10 Gbps [M] 100 Gbps [M]
Sydney	syd-zone2-1605	Equinix Sydney (SY3)	australia-southeast1	10 Gbps [M] 100 Gbps [M]
Sydney	syd-zone1-1660	NEXTDC S1	australia-southeast1	10 Gbps [M] 100 Gbps [M]
Sydney	syd-zone2-1660	NEXTDC S1	australia-southeast1	10 Gbps [M] 100 Gbps [M]

Link: https://cloud.google.com/network-connectivity/docs/interconnect/concepts/choosing-colocation-facilities#oceania

M = MACsec

Securing Private Links to the Cloud Using MACsec

Configuration Examples (IOS-XE)



cisco Live!

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 maximise cross-platform compatibility.
CAK length	This is a 64-hexadecimal character (0-9, A-E) string. Use the full length to maximise 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>

Quick XPN Overview

802.1AEbw-2013: MAC security (MACsec) - extended packet numbering

Problem statement

- The early set of ciphers for IEEE 802.1AE MACsec were **GCM-AES-128** and **GCM-AES-256**
- These ciphers use a 32-bit packet number that is unique for every packet sent within a given secure association key (SAK)
- A 32-bit packet number was fine in early, low-speed implementations
- As speeds increased, the 32-bit packet number exhausts rapidly, which causes the SAK to be refreshed at a very high frequency, causing disruption to the data flow
- It was quickly recognised that a larger packet number was needed to meet high-speed (100+ Gbps) demands when using MACsec

https://1.ieee802.org/security/802-1aebw/

Quick XPN Overview

802.1AEbw-2013: MAC security (MACsec)- extended packet numbering

Resolution

- An amendment was added to IEEE Std 802.1AE-2006 that offered enhancements using “**extended packet numbering**” or XPN
- XPN ciphers: **GCM-AES-XPN-128 / GCM-AES-XPN-256**
- These XPN ciphers increased the packet number from 32-bits to 64-bits
- This increase extends the time a SAK will refresh, specifically over high-speed links
- For 100/400 GE links, XPN ciphers for MACsec are not optional

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
!
```

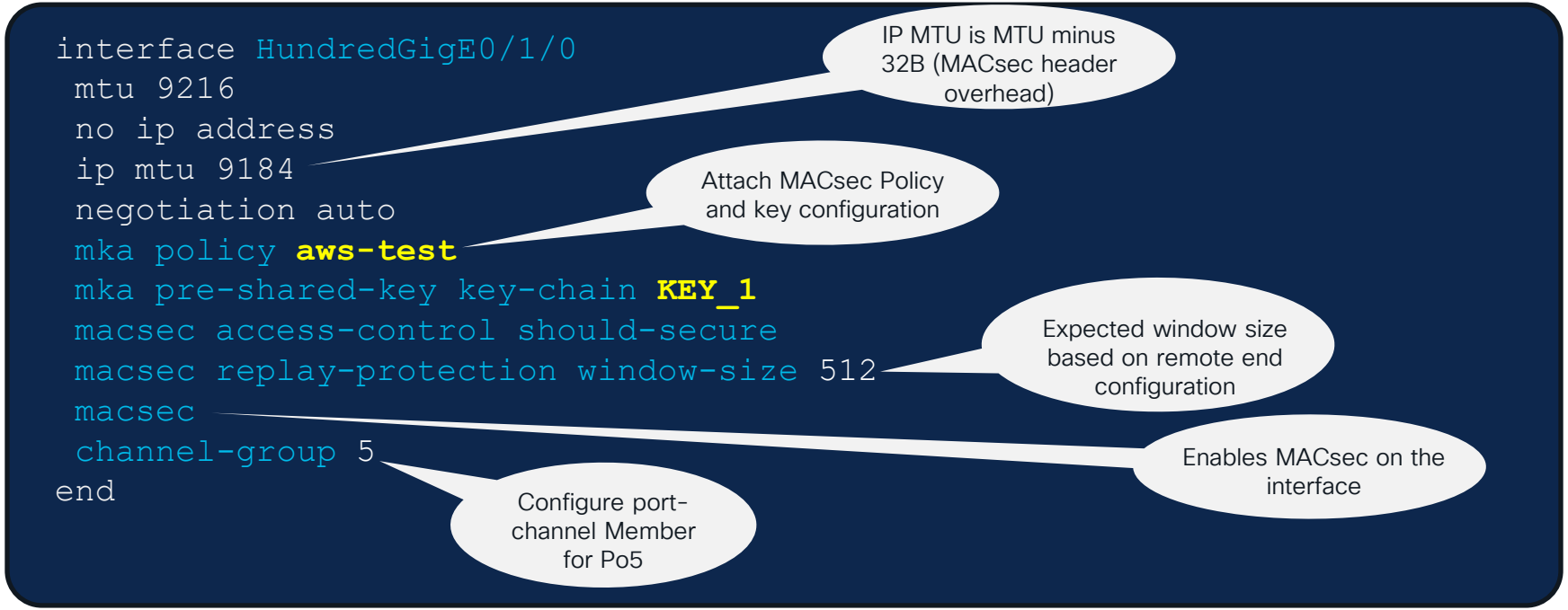
MACsec 64 hexadecimal key configuration

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

cisco Live!

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/1655479484932001lRuX

Extending Encryption into the Cloud Provider

Design Options and Awareness

cisco Live!

Extending enterprise network encryption into the cloud provider infrastructure

Public Access

- Public Internet
- Public Internet Peering Option

Private Link

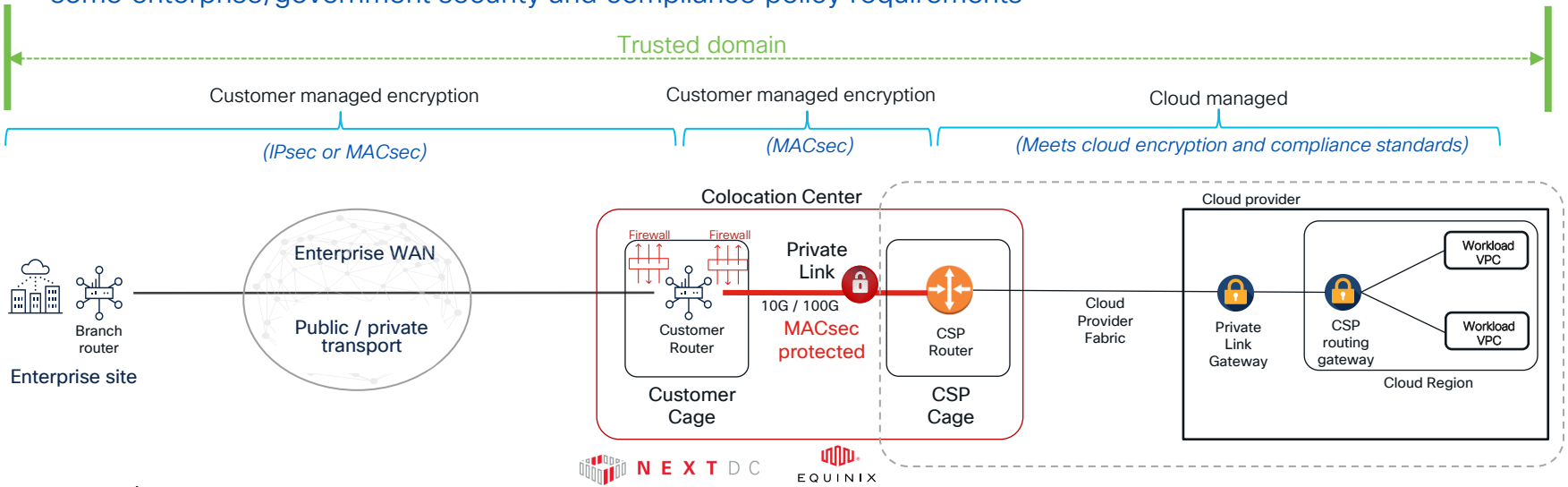
- Trusted: Encryption option for private link service (DX, ExpressRoute) into CSP ***meets the security compliance requirements*** for the enterprise standards
- Un-Trusted: Encryption option for private link service (DX, ExpressRoute) into the CSP ***does NOT meet the security compliance requirements***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

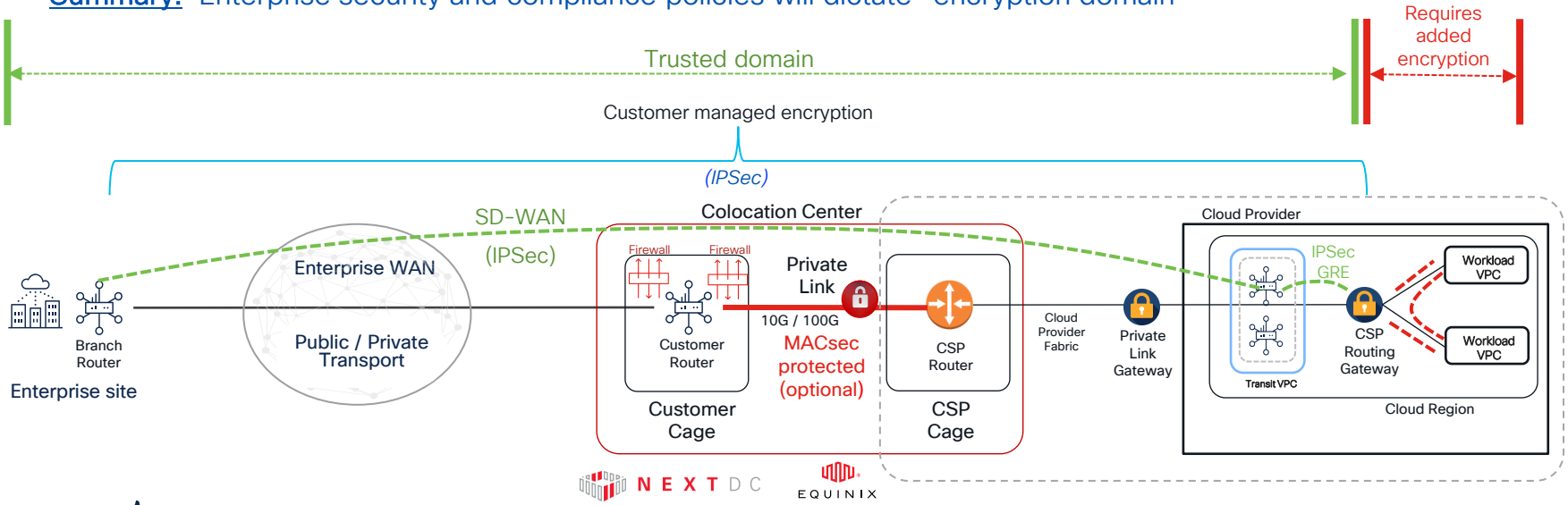
Summary: Cloud provider infrastructure, with MACsec private link encryption, assumed secure that would meet some enterprise/government security and compliance policy requirements



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

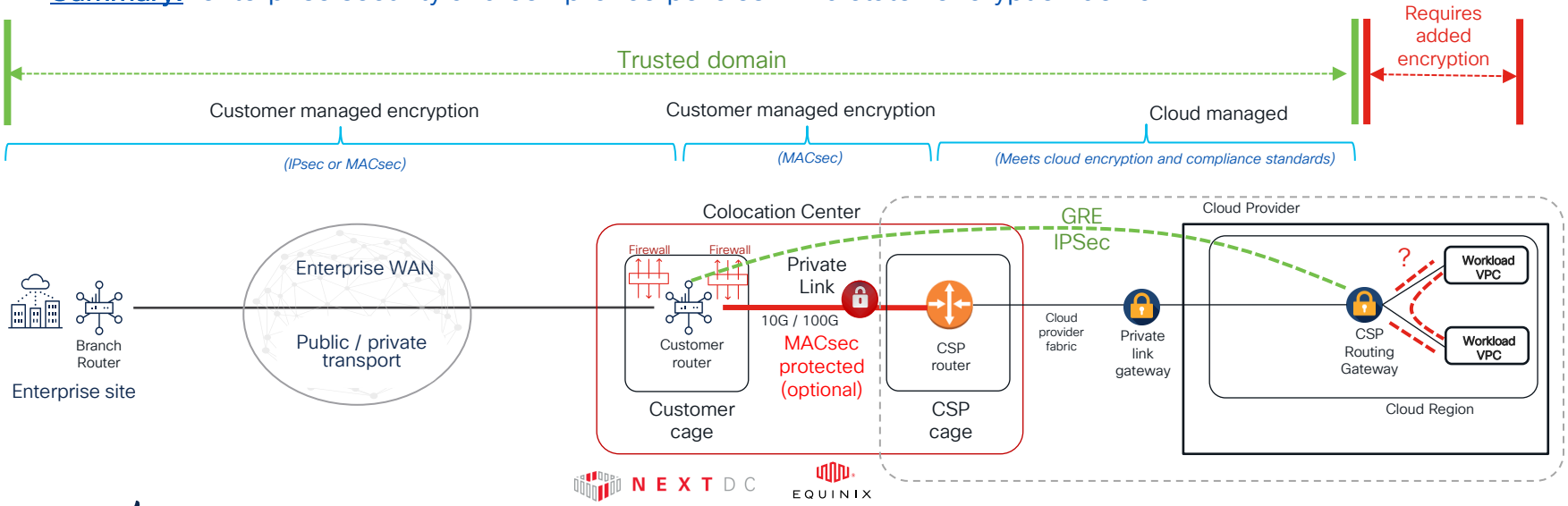
Summary: Enterprise security and compliance policies will dictate "encryption domain"



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

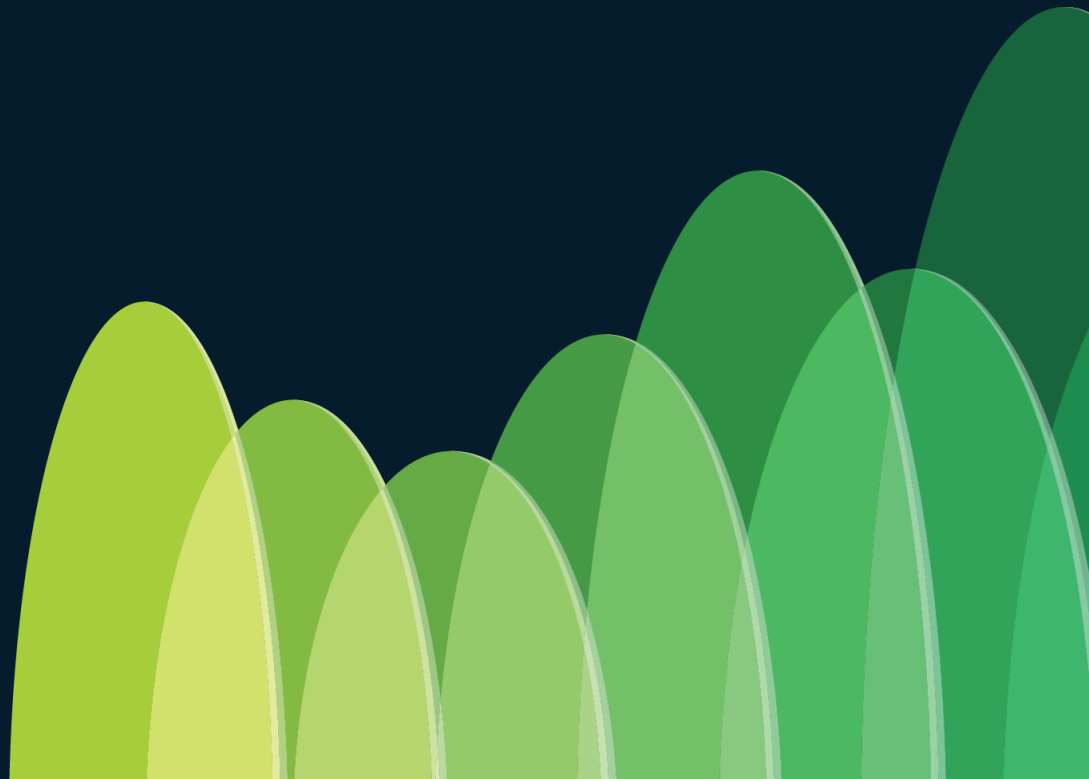
Summary: enterprise security and compliance policies will dictate "encryption domain"



Summary and caveats

- Important to align enterprise and compliance policies with encryption capabilities into the cloud
- Each cloud provider will vary how they encrypt internal network and resources
- 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/from/between the workload VPCs continue to evolve

Visibility Options into the Cloud Providers



cisco Live!

ThousandEyes visibility end to end

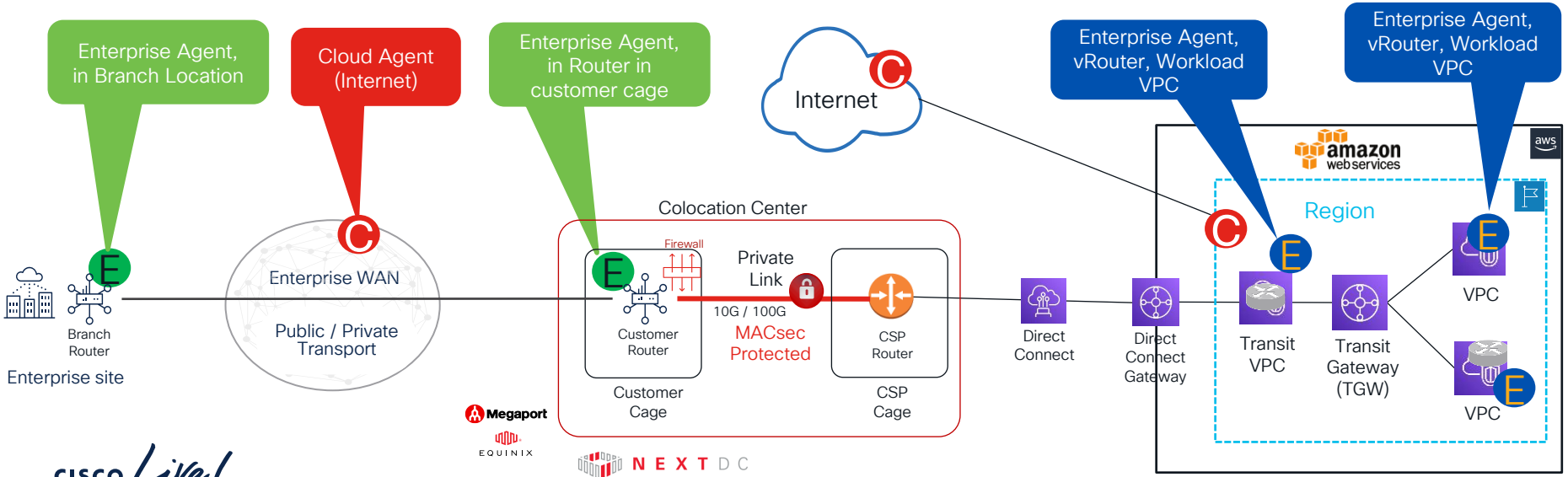
Private/public link and cloud visibility

- Extending the enterprise network into the cloud, does introduce “dark” visibility spots
- ThousandEyes offers several advantages for visibility in the WAN and cloud
- Vantage points can be deployed in various locations and footprints, 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 agents (automated via AWS CloudFormation)

Thousand Eyes – cloud agent

Thousand Eyes – ENT agent

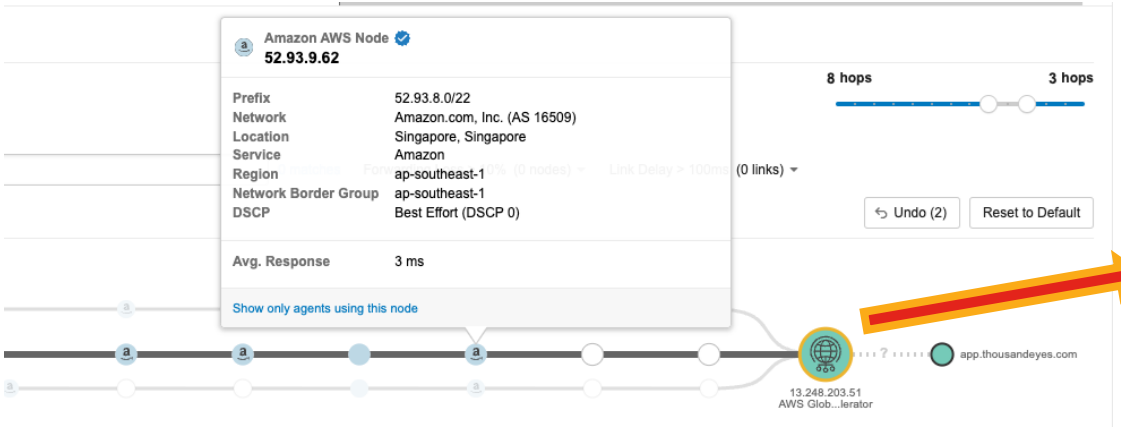
Thousand Eyes – native AWS – ENT agent



AWS network path enrichment

Extended visibility into AWS networks and services

- Leverage new data sources from our AWS partnership to enrich Path visualisation
- 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



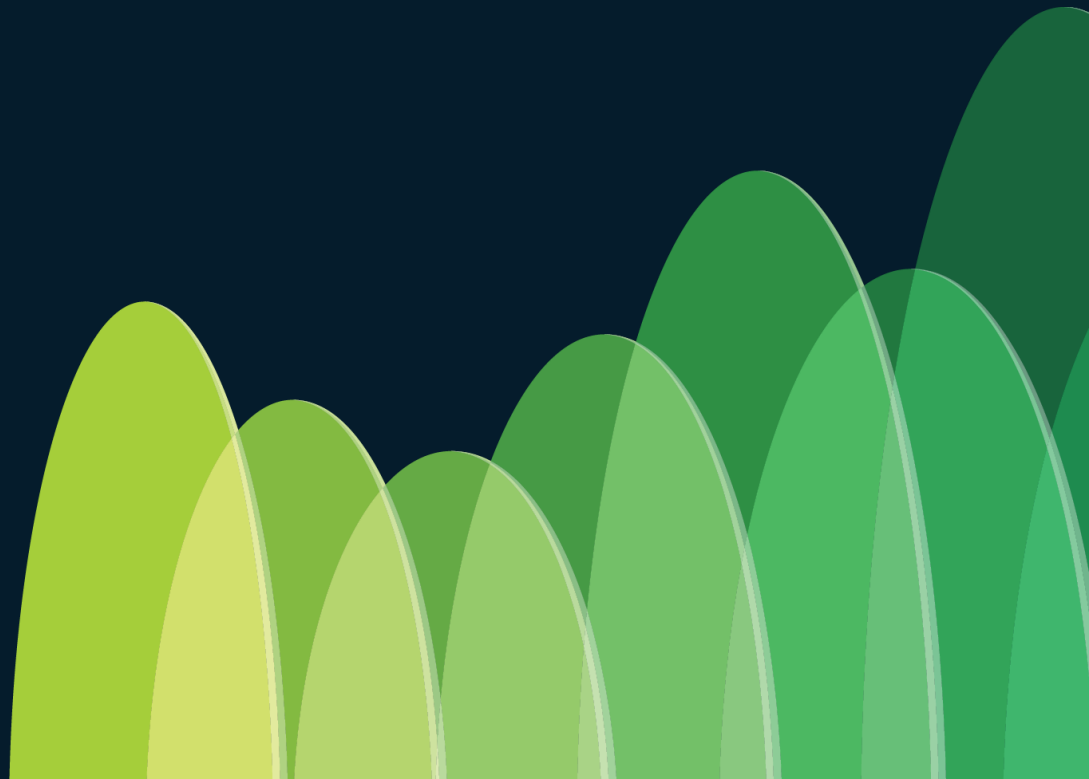
Thousand Eyes

Cloud Performance Report 2022

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

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

A Look ahead into Post Quantum Network Encryption



cisco Live!

Why and What is the Threat? Breaking Current Encryption Methods...

"Harvest now, decrypt later"

Examples of the types of problems a quantum computer is able to solve, in which a conventional computer is not, include Grover's algorithm and Shor's algorithm.

Each of these algorithms was developed by the mathematician from which they derived their names, Lov Grover and Peter Shor. Grover's algorithm leverages the processing power of quantum computing to speed up the attack on those symmetric encryption schemes using smaller key sizes. The solution to this is to simply increase the key length (e.g., AES 128 to AES 256), whereas the solution to Shor's algorithm requires an entirely new quantum-proof algorithm. The algorithm has the ability to take a key pair's public key, and relying heavily on the ability of a quantum computer to be in many states simultaneously, to derive the private key through a process of prime factorization. Through this method, Shor's algorithm effectively breaks the most commonly used asymmetric cryptosystems, including RSA, DSA, ECDSA, DH and EC-DH.

A conventional computer needs

300 trillion years

to crack RSA 2048 prime number factor encryption.

A 4,099-qubit quantum computer would need just

10 seconds

to crack the same RSA key.

Source: Baumhof, Andreas, "Breaking RSA Encryption – an Update on the State-of-the-Art," QuintessenceLabs website

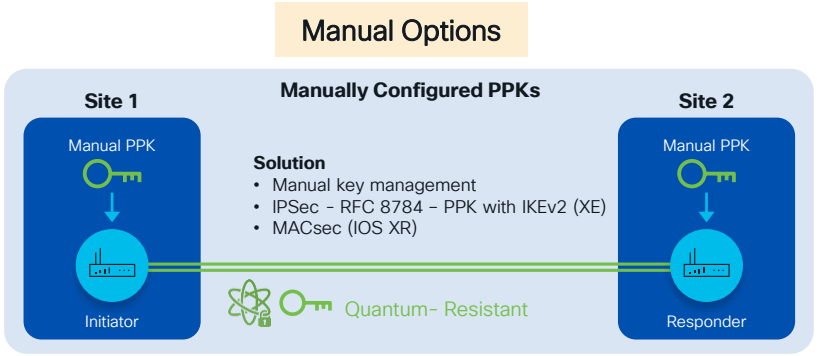
Implication

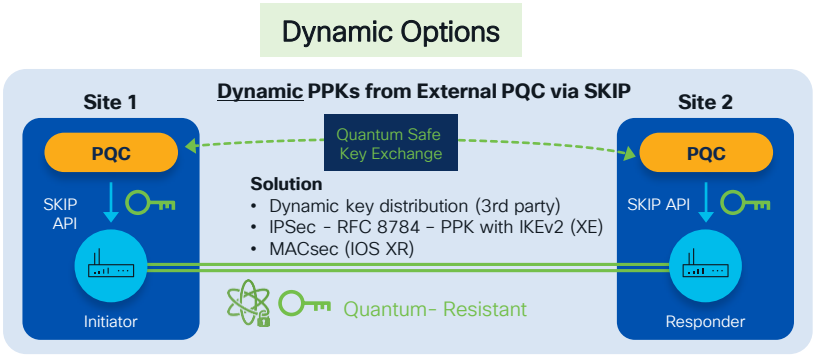
When quantum computing has sufficient size and reach, asymmetric encryption key algorithms will be susceptible to their private keys being compromised, resulting in insecure data and communications

Source: ey.com

Current Technology and Deployment Options

Quantum-Safe Encryption Options – Available Today





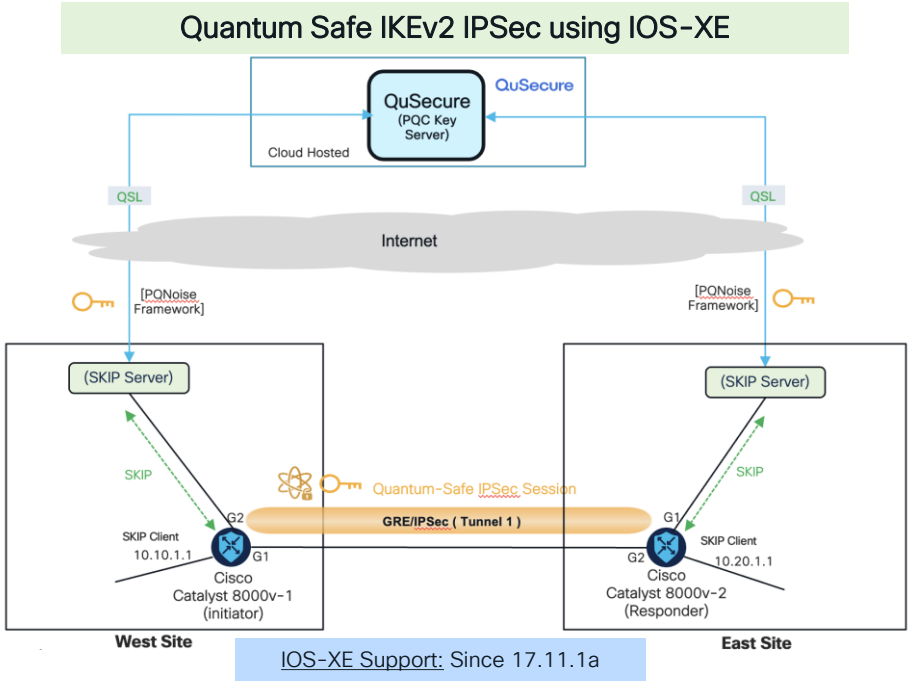
Network Encryption Options:

IPSec: RFC 8784 - PPK based IPsec encryption keys

MACsec: IEEE 802.1AE MACsec – PPK based MACsec encryption keys

PPK = Postquantum Preshared Keys

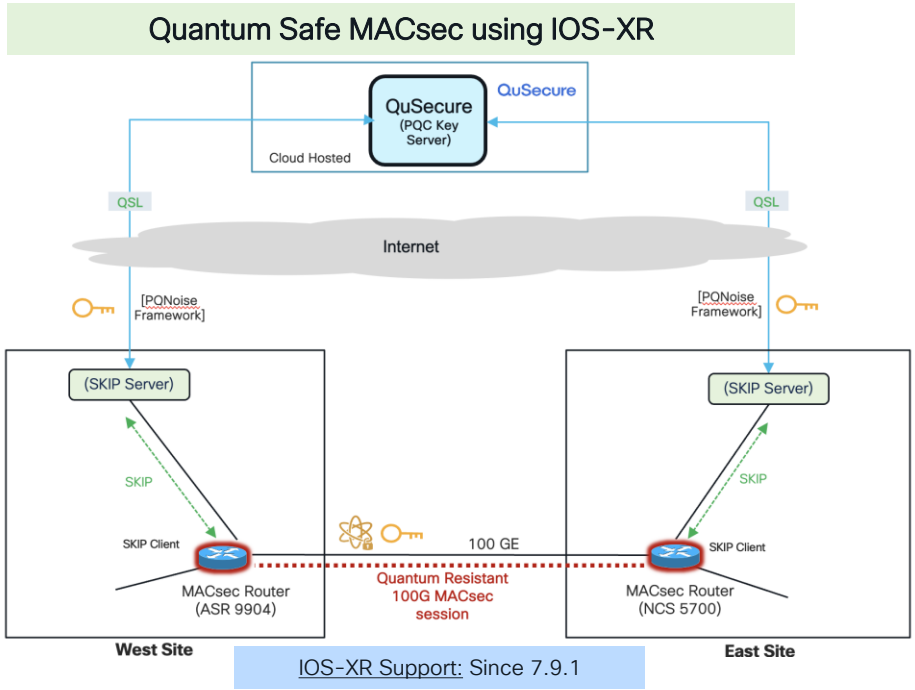
Post Quantum Solution Testing for IPSec / MACsec



- RFC 8784 offers an extension to IKEv2 to create PPL's that can be resistant to a post quantum computer threat
- Establishes post-quantum resistant IPSec session
- External key server with SKIP allows 3rd party key server

SKIP = Secure Key Integration Protocol
PPK = Postquantum Preshared Keys

Post Quantum Solution Testing for IPSec / MACsec

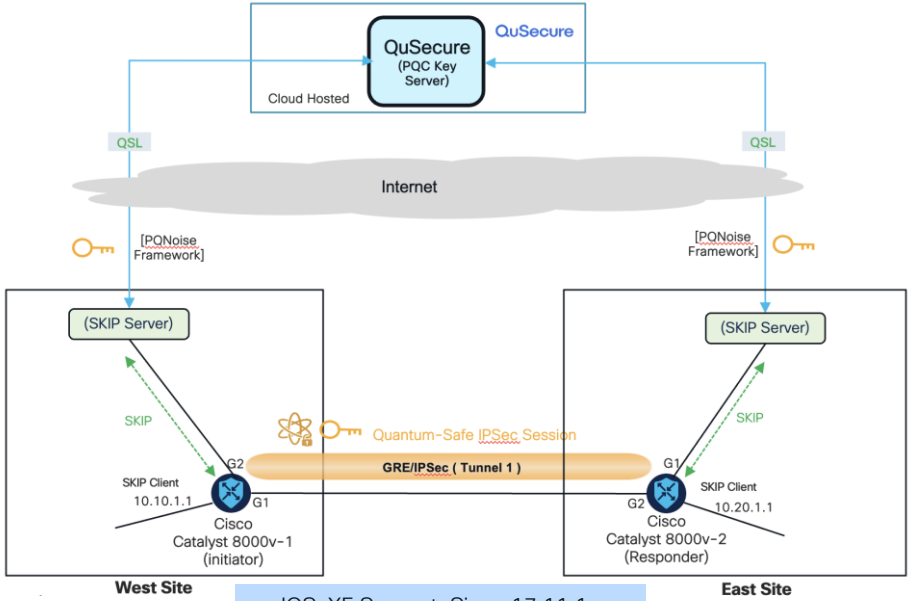


- MKA (IEEE 802.1x) extensions added to exchange quantum resistant keys (pre-shared or through 3rd party)
- Outcome is a 100 Gbps quantum resistant MACsec session
- External key server with SKIP allows 3rd party key server

SKIP = Secure Key Integration Protocol
PPK = Postquantum Preshared Keys

Post Quantum Solution Testing for IPSec / MACsec

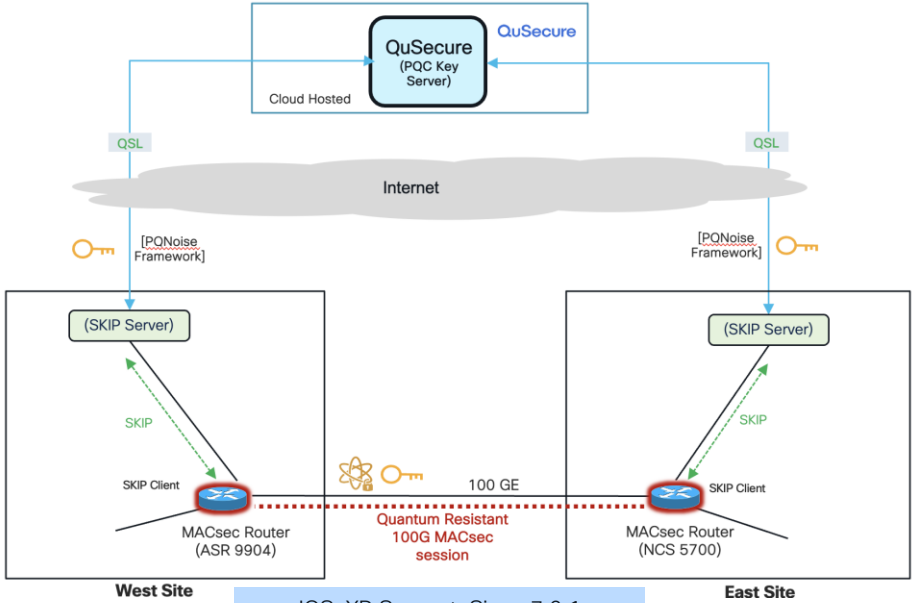
Quantum Safe IKEv2 IPSec using IOS-XE



IOS-XE Support: Since 17.11.1a

- RFC 8784 offers an extension to IKEv2 to create PPL's that can be resistant to a post quantum computer threat
- Establishes post-quantum resistant IPSec session
- External key server with SKIP allows 3rd party key server

Quantum Safe MACsec using IOS-XR

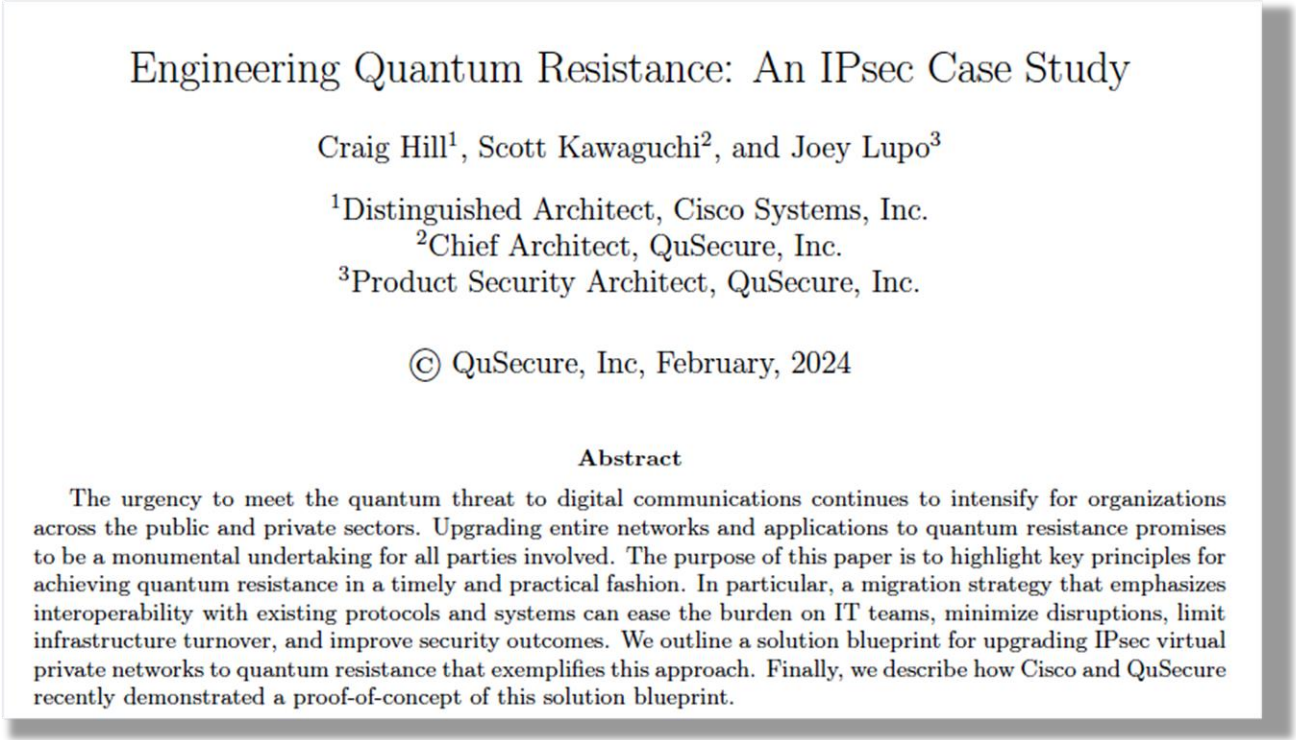


IOS-XR Support: Since 7.9.1

- MKA (IEEE 802.1x) extensions added to exchange quantum resistant keys (pre-shared or through 3rd party)
- Outcome is a 100 Gbps quantum resistant MACsec session
- External key server with SKIP allows 3rd party key server

SKIP = Secure Key Integration Protocol
PPK = Postquantum Preshared Keys

White Paper
Cisco Post-Quantum Demonstration w/ QuSecure



Engineering Quantum Resistance: An IPsec Case Study

Craig Hill[1], Scott Kawaguchi[2], and Joey Lupo[3]

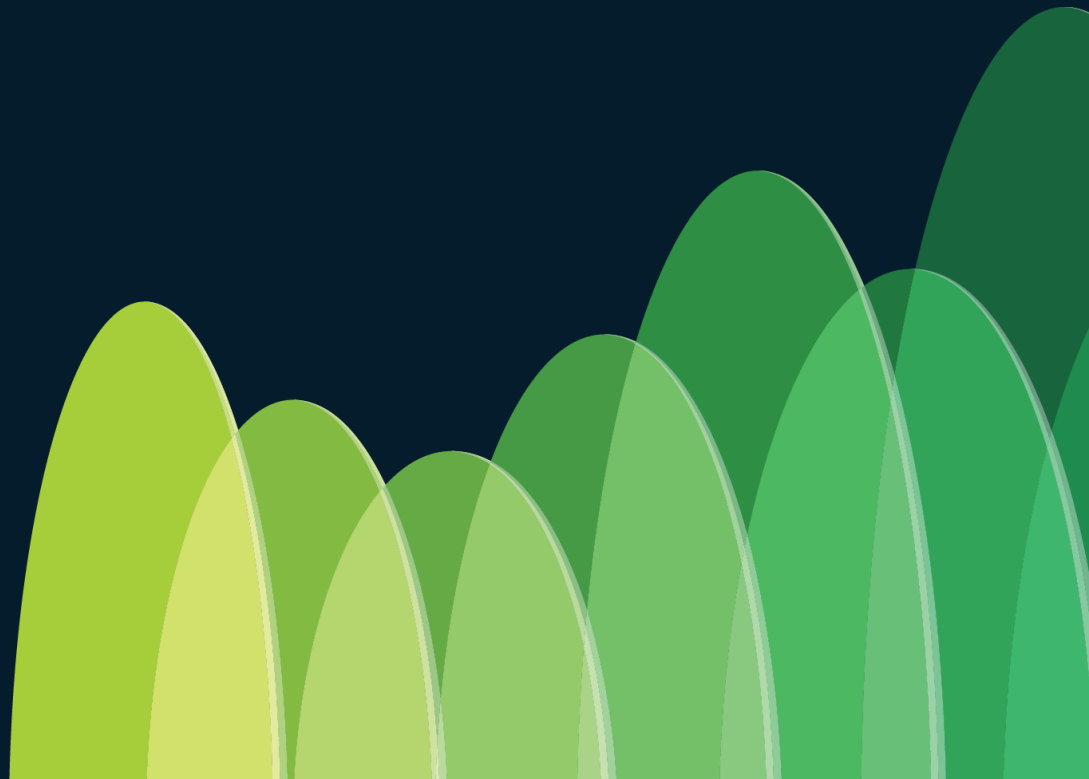
[1]Distinguished Architect, Cisco Systems, Inc.
[2]Chief Architect, QuSecure, Inc.
[3]Product Security Architect, QuSecure, Inc.

Abstract

The urgency to meet the quantum threat to digital communications continues to intensify for organizations across the public and private sectors. Upgrading entire networks and applications to quantum resistance promises to be a monumental undertaking for all parties involved. The purpose of this paper is to highlight key principles for achieving quantum resistance in a timely and practical fashion. In particular, a migration strategy that emphasizes interoperability with existing protocols and systems can ease the burden on IT teams, minimize disruptions, limit infrastructure turnover, and improve security outcomes. We outline a solution blueprint for upgrading IPsec virtual private networks to quantum resistance that exemplifies this approach. Finally, we describe how Cisco and QuSecure recently demonstrated a proof-of-concept of this solution blueprint.

Link to Paper: https://www.qusecure.com/resources/ipsec-case-study-with-cisco-core-networking/

Summary



Key takeaways from the discussion...

- Evaluate incorporating colocation centres into WAN designs to optimise 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

- Post Quantum Resistance – Case Study & Proof of Concept – Cisco / QuSecure (Hill, C., Lupo, J.)
  - https://www.qusecure.com/resources/ipsec-case-study-with-cisco-core-networking/
- 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

Complete Your Session Evaluations

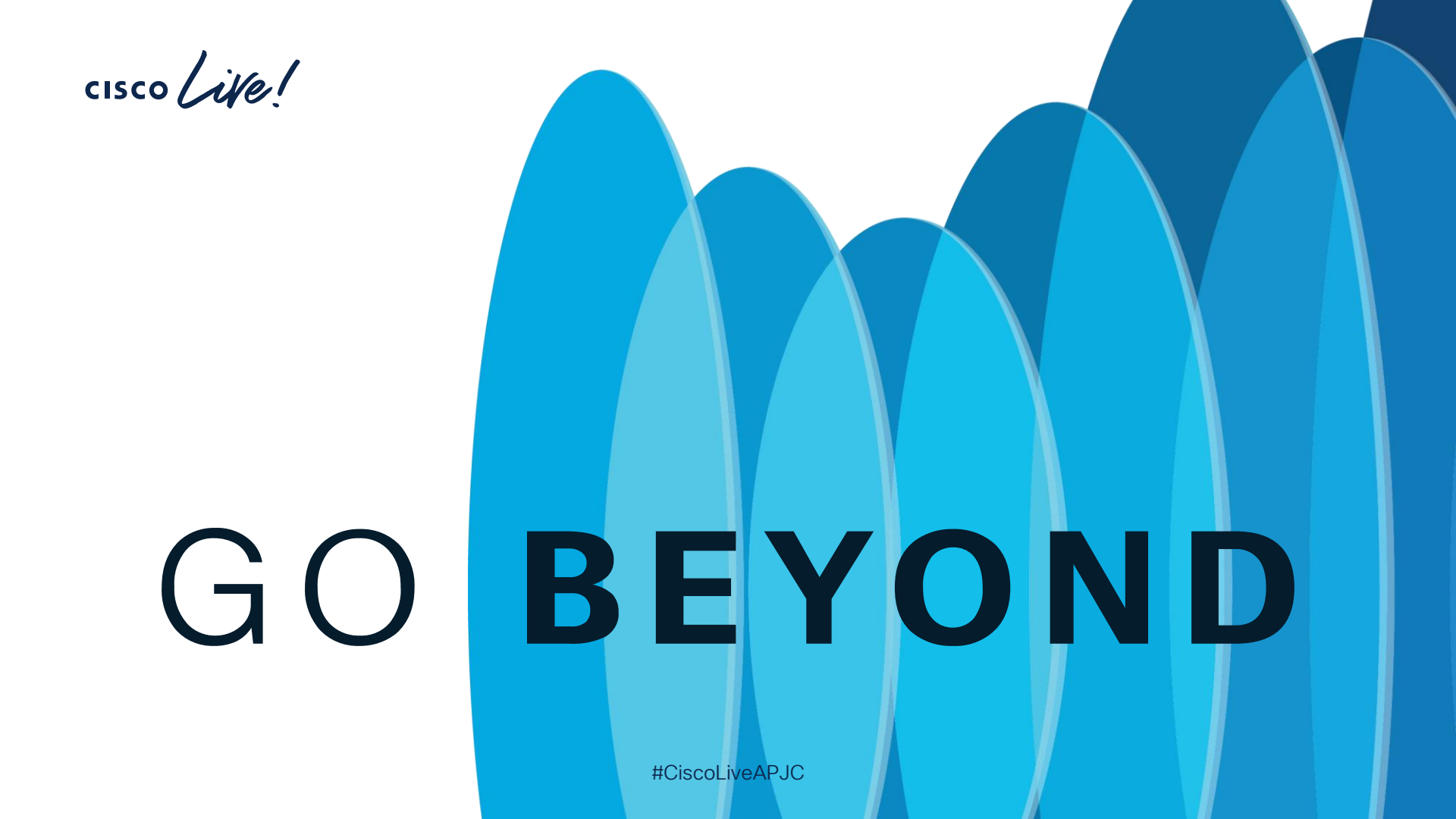
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand


cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC