White paper

Cisco public

Securing High-Speed Interconnection Over Equinix Fabric Using Cisco WAN MACsec For Public And Private Sector

Contents

Abstract

The transition for applications moving to the cloud continues to grow at a rapid pace. This shift continues to require agencies/enterprises to rethink WAN architectures and security designs in order to provide the optimal user experience, security, and visibility of those applications.

The purpose of this document is to add a key element of this rethinking process for “inter-regional” connectivity, specifically describing how customers can provide secure high-speed interconnection between Equinix data centers up to line rate using Cisco WAN MACsec over Equinix Fabric.

Introduction

The larger government/enterprise network designers and operators already lived the early stages of applications moving to the clouds. Recall that prior to this shift, private data centers were the “center of the universe” for these global agency/enterprise networks. These private data centers hosted customer applications on-premises (which also was the established “hub” site for the enterprise WAN) as well as the security stack for externally and internally bound traffic (internet, partner, etc.).

As applications and data began moving to hybrid multicloud architectures, the private data center model had to evolve as new traffic patterns became sub-optimal and increasingly asymmetric. This was due to traffic being home run to the on-premises data center first, instead of a direct path to the hybrid and/or multicloud-hosted applications. This sub-optimal traffic pattern not only induced unnecessary latency, because a large percentage of the traffic was externally destined, on-premises firewalls and security stacks were unable to keep pace – often misaligned with these dynamically evolving traffic flows.

A major step to aligning WAN and security design with this transition to hybrid multicloud was in establishing a presence in colocation “meet me” points, providing traffic destined to applications hosted in cloud-native and/or cloud-adjacent private enclaves a more optimal and low-latency path. Additionally, this new “meet me” point also required a level of security to and from on-premises infrastructure as well as remote colocation-to-colocation deployments.

This paper provides a secure solution that targets these on-premises-to-colocation and colocation-to-colocation requirements. Equinix provides the functions and colocation services for these “meet me” points and, with Equinix Fabric, the WAN transport between these locations. Cisco is providing the capability to secure this transport at speeds up to line rate using WAN MACsec.

Equinix Fabric

Equinix Fabric is an on-demand Network-as a-Service (NaaS) platform providing point-to-point EVPL and EPL services across more than 55 global metros. As a purpose-built carrier-class network, Equinix Fabric provides private, resilient, high-speed, low-latency connectivity, allowing customers to be assured their data is delivered to the intended destinations.

Today, Equinix Fabric offers two different point-to-point connectivity services to our customers, Ethernet Virtual Private Line (EVPL), a VLAN-based service, and Ethernet Private Line (EPL), a port-based service. These circuits, called Virtual Connections (VCs), can be deployed locally within a metro or globally between metros (see **Figure 1**).

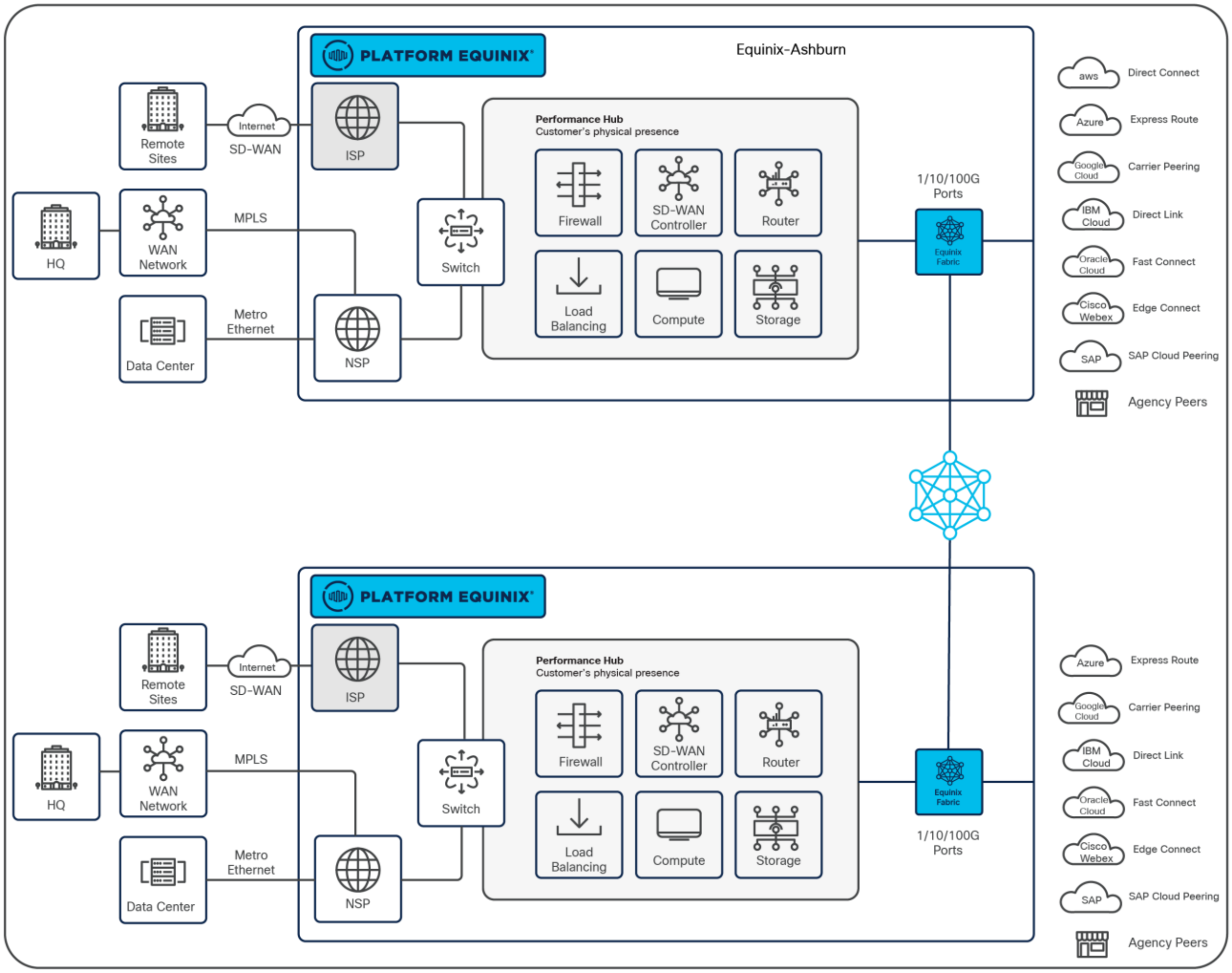


Figure 1.
Metro-to-metro Equinix fabric

EVPL allows customers to connect to multiple destinations using the same physical port. This is facilitated by the customer using 802.1Q VLAN tagging at their edge Fabric port with each destination using a different VLAN. EVPL drops certain Layer 2 Control Protocol (L2CP) traffic such as STP and LACP and frames needed for MACsec, such as EAPoL.

EPL allows for connectivity only between two locations. Since EPL is a port-based service, all traffic is passed between the two EPL ports. EPL supports tagged and untagged Ethernet traffic and is a “highly transparent” service, meaning it passes all Ethernet traffic except for Ethernet Pause frames (used for flow control). As such, all L2CP frames, other than the Pause frame, are passed transparently. This allows protocols such as STP, LACP, MACsec, and others to work across an EPL connection “natively.”

The complete, end-to-end virtual connections are created by the customers themselves from within the Equinix Fabric portal or via API. This enables the on-demand nature of Equinix Fabric allowing for VCs to be turned up or down within minutes. Equinix Fabric also offers industry-standard performance SLAs covering such areas as latency, packet loss, jitter, and interface availability.

The customer portal provisioned Equinix Fabric service provides on-demand EVPL and EPL “Virtual Connections” from 50 Mbit to 10 Gbit. EVPL supports VCs as large as the physical port speed down to the smallest, 50-Mb VC. Any number of VCs are supported per the EVPL port. Equinix leaves it up to the customer to decide upon an oversubscription ratio, or if they want to oversubscribe at all.

This interconnection framework provides unprecedented granularity and utility, enabling customers to provision persistent and/or non-persistent intra- and/or inter-metro connections as mission requirements dictate. This on-demand and variable interconnection methodology also introduces new efficiencies from a cost and mission agility perspective, enabling customers to dynamically right-size and utilize transport as needs dictate, delivered in a monthly billable consumption model that can be prorated for partial month use accordingly.

As both public- and private-sector customers look to establish regionally distributed and geostrategic digital edge locations, the ability to deploy globally extensible high-speed encryption is becoming key. Customers desire to multiplex multiple services over their Equinix Fabric port(s) and, in many cases, have a need to encrypt some or all of this traffic. Cisco WAN MACsec in combination with Equinix Fabric provides exactly what’s needed to accomplish these goals.

WAN MACsec Primer

In 2012, Cisco introduced a suite of enhancements in selected router platforms referred to as WAN MACsec that specifically targeted MACsec to be run over the WAN. The goal of WAN MACsec was to provide MACsec encryption at rates that aligned with Ethernet standards while also providing enhancements that allowed operators to leverage carrier Ethernet offerings (802.1Q) and allow the router supporting WAN MACsec to adjust to the multitude and inconsistent forwarding of certain protocols, MAC addresses, and Ethertypes. WAN MACsec gave operators the flexibility to virtually run over any public carrier Ethernet service, simplifying installations, while offering design capabilities with MACsec never seen before over public Ethernet transport.

Below is a summary of these extended capabilities with Cisco WAN MACsec offering:

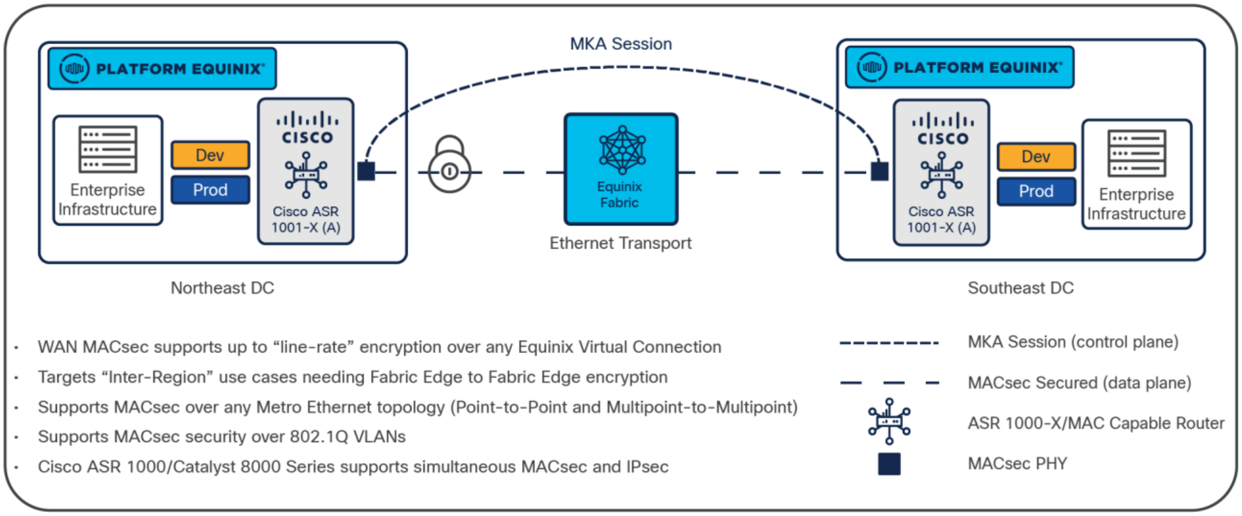
- **Standards-based MACsec Key Exchange (MKA)** – Leverages standard IEEE 802.1X-rev capabilities.
- **AES-256 (AES/GCM) Support** – Supports stronger ciphers with AES-256, with the option for AES-128, if desired.
- **802.1Q Tag in Clear** – WAN MACsec Encapsulation exposes the IEEE 802.1Q tag, “Tag in the Clear” (2 tags are optional), opening up a variation of Metro Ethernet topologies and design options.

- **Enhanced Network Features over Public Carrier Ethernet Providers** – Offers operators ability to tune MACsec/MKA functions to adapt to the Ethernet carrier being used, such as MKA MAC addresses and Ethertypes within the EAPoL encapsulation.
- **Automation Options for MACsec** – The MACsec configuration and operation capabilities are exposed in extensive YANG models (both native and open) as well as support in Cisco Network Service Orchestrator (NSO).

This combination of Cisco WAN MACsec capabilities over Equinix Fabric offers customers a secure, high-speed, inter-region transport without the overhead and performance limitations of other encryption technologies. Readers interested in a deeper dive on MACsec and how it operates, as well as Cisco WAN MACsec and its common deployment use cases, can refer to the Cisco WAN MACsec White Paper.

WAN MACsec over Equinix Fabric – Testing overview

Cisco and Equinix joined forces to demonstrate Equinix Data Center Interconnect, running Cisco WAN MACsec over the Equinix Fabric EVPL offering. For this, as shown in **Figure 2**, the testing was done between Equinix colocation facilities in Miami, Florida, and Ashburn, Virginia. Devices under test were two Cisco ASR 1001-X platforms testing over a 10GE EVPL connection. All traffic was secured with Cisco WAN MACsec enabled on the interfaces and an 802.1Q-provisioned EVC with an MTU of 9100. It should be noted that, for this validation testing, Pre-Shared Keys (PSK) were used for MKA key exchange; however, Cisco MACsec also supports certificate-based MACsec encryption using EAP-TLS. To demonstrate segmentation with this solution, which is a common customer requirement, two Layer 3 VPNs were leveraged, “Dev” and “Prod,” which are using IP BGP VPNs and Segment Routing MPLS using WAN MACsec over the Equinix Fabric transport.



- 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

Figure 2.
Cisco WAN MACsec over Equinix Fabric – test topology

While functionality over performance was the focus of this testing, **Table 1** shows the MACsec performance numbers for the ASR 1001-X (IOS XE 16.6 and later) used for WAN MACsec validation testing.

Table 1. Performance numbers on the Cisco ASR 1001-X router

Frame Size	Aggregate Rate Bits (bps)	Line Rate per port (%)	ESP CPU (%)
64	10064767891.17	65.59	93.33
iMIX	17763891467.40	93.14	26
1418	19311044388.60	97.89	9

For the test setup shown in Figure 2 above, several key areas were tested and validated to prove successful operation of Cisco WAN MACsec over Equinix Fabric, including:

- Establishing a secure MKA session (control plane) over the Equinix Fabric using AES-256 ciphers (AES-256-CMAC)
- Protecting the traffic (data plane) using 802.1AE with AES-256 cipher (GCM-AES-256) protection
- Leveraging the WAN MACsec enhancement to modify the MAC address for successful MKA session exchange
- Leveraging the WAN MACsec enhancement to modify the Ethertype for successful MKA session exchange
- Supporting the ability to run MACsec session granularity at the 802.1Q level of segmentation over the Equinix Fabric using the Cisco 802.1Q tag in the clear enhancement
- Validating WAN MACsec was able to properly adjust the interface MTU size, accounting for additional overhead the MACsec header appends to each packet
- Successfully run advanced services securely over MACsec, such as (MPLS with Segment Routing), BGP/MPLS IP VPN, and Bidirectional Forward Detection (BFD).

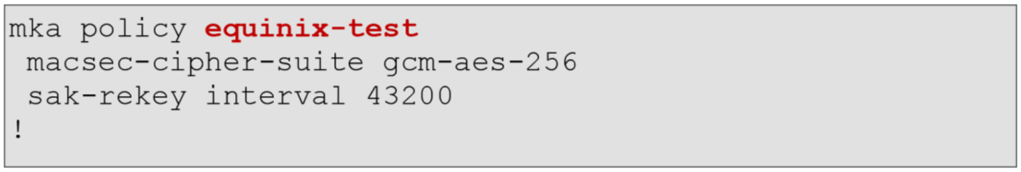
It should be noted that the ASR 1001-X used in this test is transitioning to end of sale by Cisco, with the transition to the Cisco Catalyst 8500 platform moving forward. However, the configuration examples used below for configuring MACsec are identical in both the ASR 1001-X and Catalyst 8500 using IOS XE.

Example: WAN MACsec configuration overview and examples

Below are example configurations used for the Cisco WAN MACsec over Equinix Fabric validation testing. Basic test setup components and protocols included:

- Platform Used: Cisco ASR 1001-X
- Interface Speed: 10GE
- MTU: 9100 (MACsec 9068)
- Equinix Fabric Service: 802.1Q EVPL Service
- MACsec Details: IEEE 802.1AE running AES-256-CMAC (MKA) and GCM-AES-256 (MACsec).

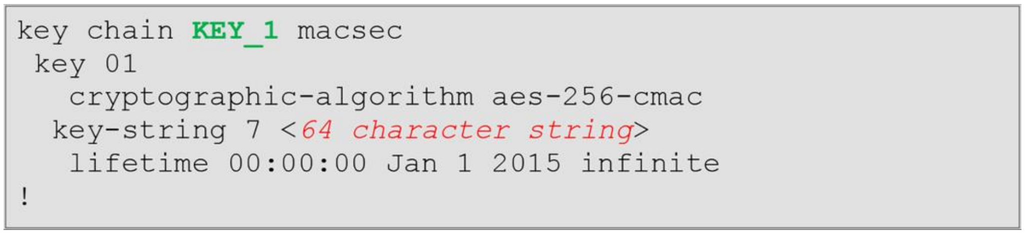
The first step, shown in **Figure 3**, is configuring the encryption algorithms to be used [gcm-aes-128 | gcm-aes-256], and in this example, we are leveraging the stronger cipher of gcm-aes-256 and configuring the desired interval (optional) for which initiates a SAK rekey process.



```
mka policy equinix-test
 macsec-cipher-suite gcm-aes-256
 sak-rekey interval 43200
!
```

Figure 3.
Example for encryption algorithms and re-key internal options

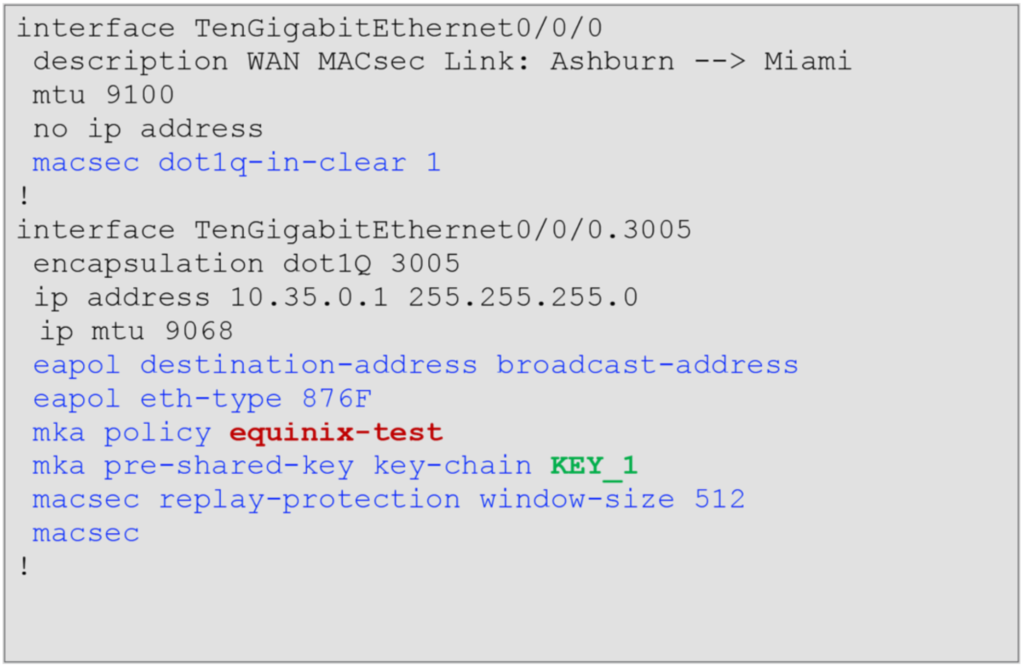
The second step, shown in **Figure 4**, is to configure the encryption algorithm functions for the MKA control packets for MACsec. This process creates a keychain (KEY_1), a key, and then sets the authentication algorithm to be used. Finally, the lifetime for the key string is set, and in this case defined as “infinite.” The operator does have the ability to tailor the lifetime of that key configuring multiple keys in the key chain triggering MKA to rollover to the next key in a hitless fashion.



```
key chain KEY_1 macsec
 key 01
   cryptographic-algorithm aes-256-cmac
  key-string 7 <64 character string>
   lifetime 00:00:00 Jan 1 2015 infinite
!
```

Figure 4.
Example for encryption algorithms for MKA control packets

The third and final step, shown in **Figure 5**, is to apply MACsec and MKA to the interface. The relevant MACsec commands are shown in BLUE, and this validation test leveraged 802.1Q tag in the clear, allowing MACsec to expose the 802.1Q tags to the Equinix Fabric service.



```
interface TenGigabitEthernet0/0/0
 description WAN MACsec Link: Ashburn --> Miami
 mtu 9100
 no ip address
 macsec dot1q-in-clear 1
!
interface TenGigabitEthernet0/0/0.3005
 encapsulation dot1Q 3005
 ip address 10.35.0.1 255.255.255.0
  ip mtu 9068
 eapol destination-address broadcast-address
 eapol eth-type 876F
 mka policy equinix-test
 mka pre-shared-key key-chain KEY_1
 macsec replay-protection window-size 512
 macsec
!
```

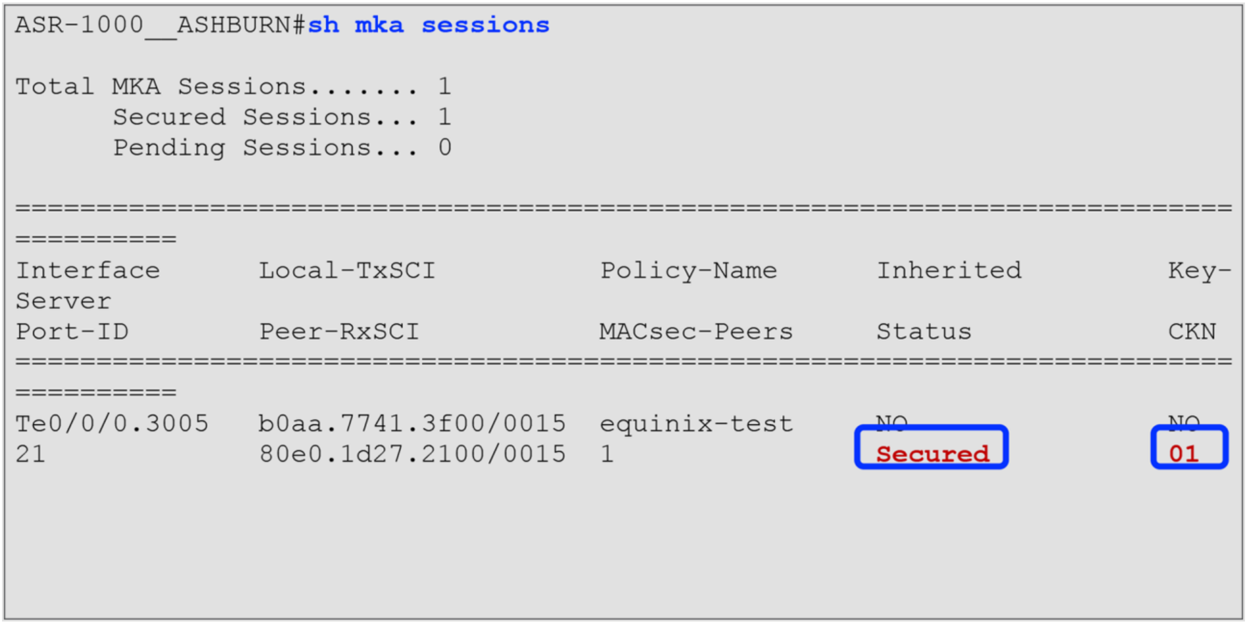
Figure 5.
Example for applying WAN MACsec to the interface and command options

Another key area that was required for this MACsec validation testing over Equinix Fabric was the use of Cisco MACsec enhancements for MKA session establishment, specifically the use of EAPoL configuration modifications. EAPoL for MACsec leverages a well-known MAC address (01:80:c2:00:00:03) and Ethertype (0x888e) for establishing a MACsec session.

A quick background for the reader, public Ethernet transport solutions vary in how they handle certain MAC addresses and Ethertypes, and in many cases, well-known EAPoL attributes used for MKA are either consumed or dropped by the carrier. For this reason, Cisco WAN MACsec offers the operator the ability to modify these attributes through the use of **eapol destination-address and eapol eth-type** commands as shown in Figure 5 above. These commands allow the operator to configure alternative parameters (shown in Figure 5 above, MAC = “broadcast-address” and Ethertype = “”876F”) for those public Ethernet providers that do not forward the default MKA EAPoL MAC and Ethertype values. It was determined in our validation testing that these Cisco WAN MACsec EAPoL commands are required to successfully run MACsec over the Equinix Fabric service.

Example: Output and status for the configured MKA session

To start the confirmation process of validating the MACsec session being up and active, **Figure 6** describes a valuable output command to confirm this. This is an important command for the operator to understand for verifying the MKA session is up and secured, as well as which CKN key is being leveraged for the MKA session. Important information shown here from the "**show mka sessions**" output is the "Status" verifying that the session shows "**Secured**," as well as the CKN being used, which is "**01**" in this example from the testing and configuration from Figure 4 above.



```
ASR-1000__ASHBURN#sh mka sessions

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

===========================================================================
==========
Interface      Local-TxSCI         Policy-Name      Inherited         Key-
Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
===========================================================================
==========
Te0/0/0.3005   b0aa.7741.3f00/0015 equinix-test     NO                NO
21             80e0.1d27.2100/0015 1                Secured           01
```

Figure 6.
Output and status for the MKA session and CKN in operation

For use cases where multiple sessions will exist, an aggregated count is also available and shown above for **Total MKA Sessions.** The other output shown above aligns with the keychain configuration (refer to Figure 4 above) such as the interface, local peer, and policy name, all of which is useful for troubleshooting and observing each secure session(s). More details for the MACsec configuration and output can be found here.

To better align the test deployment with actual customers, the Cisco solution testing also demonstrated the use of segmentation, Dev and Prod in Figure 2 above, with BGP/MPLS IP VPNs and the use of Segment Routing (SR) over MACsec for those customers requiring multi-tenant separation between Equinix data centers and advanced routing services using SR.

SR was chosen for its growth in adoption and is the path forward method of forwarding packets within the construct of source routing, where the source router encodes a segment ID (SID) path list in the packet header to the destination, in an ordered fashion. SIDs can be MPLS labels as well as IPv6 headers where SRv6 is used, and SR can integrate easily with Layer 3 VPN, Layer 2 VPN, and Ethernet VPN as well as offer very granular traffic engineering. Details around SR are outside the scope of this document, but more info can be found at this link.

Summary

This document provides a validated design overview for those customers requiring secure “inter-regional” connectivity between two or more Equinix data centers, leveraging the flexibility and agility of Cisco WAN MACsec over Equinix Fabric Ethernet transport. Cisco and Equinix have enjoyed a longstanding partnership with a focus on sustained innovation. Thousands of Equinix customers deploy their Cisco infrastructure at geo-strategic locations to establish proximal adjacency to hundreds of integrated service providers and mission partners. Intuitive, rapidly orchestrated, and highly secure interconnection with a growing field of interoperable service providers will remain our focus as we collectively work to continuously refine the customer experience and enable their varied digital transformation pursuits at the digital edge.

References

Hill, C., and Orr, S. (2016). Innovations in Ethernet Encryption (802.1AE - MACsec) for Securing High Speed (1-100GE) WAN Deployments White Paper www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

Hill, C., and Kowal, M. (2019). The Multiplanar Backbone (MPBB) White Paperwww.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Federal/The_Multiplanar_Backbone_MPBB.pdf

Hill, C., and Mosher, S. (2020). Cisco Software-Defined WAN for Secure Networks - Redefining WAN Delivery in the Cloud Era White Paperwww.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741640.html

Equinix Fabricwww.equinix.com/interconnection-services/equinix-fabric

Equinix Solution Validation Centerwww.equinix.com/services/advisory/solution-validation-centers

(2021). Site-to-Any-Cloud and Site-to-Site Use Cases with Cisco SD-WAN and Equinix White Paper www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-2373512.html

Wiggins, Don (2022). 3 Ways to Extend Cybersecurity Infrastructure to the Edge Blog https://blog.equinix.com/blog/2022/03/17/3-ways-to-extend-cybersecurity-infrastructure-to-the-edge/

Cisco IOS-XE MACsec Configuration Guide (Cisco IOS XE 17) www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book/m_wan_macsec_MKA_support_enhancements.html

Cisco IOS-XE Segment Routing Configuration Guide (Cisco IOS XE 17) www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-17/segrt-xe-17-book-cat8000.html

Cisco Catalyst 8500 Configuration Guide www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/software-configuration-guide/c8500-software-config-guide.html

Authors

Craig Hill
Distinguished Architect
Cisco Systems, Inc.

Chris Hocker
Solutions Architect
Cisco Systems, Inc.

Don Wiggins
Senior Global Solutions Architect
Equinix

Richard Carrara
Senior Principal Solutions Architect
Equinix

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-153087-00 09/22