サブインターフェイスを使用したCatalyst 8500でのWAN MACsecの設定

内容

はじめに

このドキュメントでは、サブインターフェイスを備えたCisco Catalyst 8500プラットフォームでWAN Media Access Control Security(MACsec)を設定するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WAN、VLAN、暗号化などの高度なネットワーキングの概念
- MACsec(IEEE 802.1AE)およびキー管理(IEEE 802.1X-2010)の理解
- Cisco IOS® XEコマンドラインインターフェイス(CLI)に精通していること

使用するコンポーネント

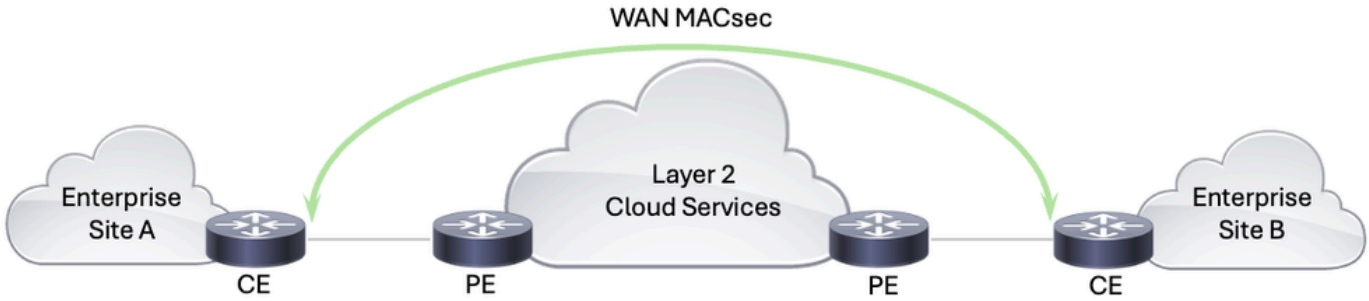
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst 8500 シリーズ エッジ プラットフォーム
- Cisco IOS XEバージョン17.14.01a

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

WAN MACsecは、MACsecの機能を利用してWANネットワーク全体のネットワークトラフィックを保護するように設計されたセキュリティソリューションです。サービスプロバイダーネットワークを使用してデータを交換する際は、転送中のデータを暗号化して改ざんを防ぐことが重要です。WAN MACsecは導入と管理が簡単で、盗聴や中間者攻撃などのデータ操作からネットワークトラフィックを保護する必要がある組織に最適です。シームレスなラインレートの暗号化を実現し、サービスプロバイダーのネットワーク、クラウド環境、企業ネットワークなど、さまざまなネットワークインフラストラクチャを通過する際にもデータの安全性を確保し、妥協を許さないようにします。



WAN MACsecソリューション

IEEE 802.1AE規格で定義されているMACsecは、イーサネットフレームのデータの機密性、整合性、および発信元の信頼性を確保することにより、イーサネットネットワーク上で安全な通信を提供します。オープンシステムインターコネクション(OSI)モデルのデータリンク層（レイヤ2）で動作するMACsecは、イーサネットフレームを暗号化および認証して、ノード間の通信を保護します。元々はLAN用に設計されたMACsecは、WANの導入もサポートするように進化しました。ラインレートの暗号化を提供し、遅延とオーバーヘッドを最小限に抑えます。これは高速ネットワークに不可欠です。

IEEE 802.1X-2010は、ポートベースのネットワークアクセスコントロールを定義する元のIEEE 802.1X標準に対する修正です。2010年の改訂では、MACsec実装の暗号キーの管理に不可欠なMACsec Key Agreement(MKA)プロトコルが導入されました。MKAは、MACsecがデータの暗号化と復号化に使用する暗号キーの配布と管理を行います。MKAは、ダイナミックWAN環境で継続的なセキュリティを維持するために不可欠な、MACsec導入のマルチベンダー相互運用性に貢献し、安全なキー交換とキー再生成メカニズムをサポートする標準です。

WAN MACsec環境では、IEEE 802.1AE(MACsec)によってデータリンク層に基本的な暗号化およびセキュリティメカニズムが提供され、ネットワークを通過するすべてのイーサネットフレームが保護されます。MKAプロトコルを使用するIEEE 802.1X-2010は、MACsecの機能に必要な暗号キーの配布と管理という重要なタスクを処理します。これらの標準により、WAN MACsecはワイドエリアネットワーク全体で堅牢な高速暗号化を実現でき、相互運用性と管理の容易さを維持し

ながら、転送中のデータを包括的に保護できます。

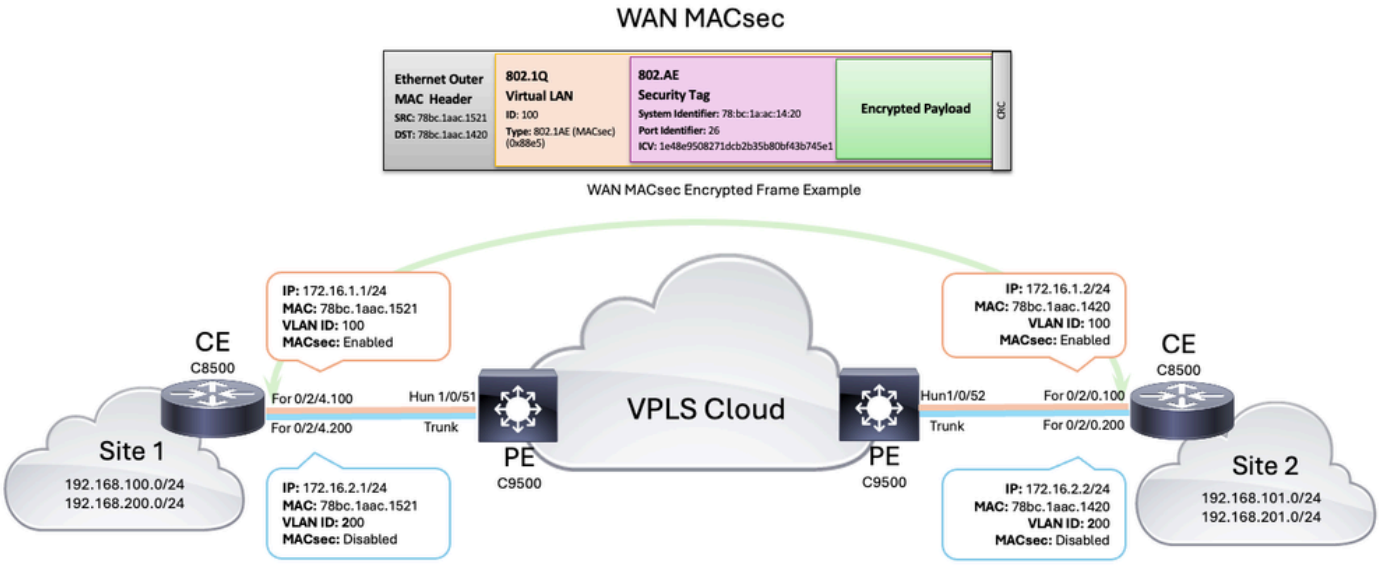
WAN環境に固有の課題に対処するために、従来のMACsec導入に対していくつかの機能拡張が行われました。

- クリアな802.1Qタグ：この機能により、802.1Q VLANタグを暗号化されたMACsecヘッダーの外部に公開でき、特にパブリックなイーサネット転送環境において、より柔軟なネットワーク設計を促進します。この機能は、同じネットワーク上に暗号化トラフィックと非暗号化トラフィックを共存させ、ネットワークアーキテクチャを簡素化してコストを削減できるため、MACsecをキャリアイーサネットサービスと統合する際に不可欠です。
- パブリックキャリアイーサネット上での適応性：最新のWAN MACsec実装は、パブリックキャリアイーサネットサービスに適応できます。この適応性には、Ethernet Authentication Protocol over LAN(EAPoL)の宛先アドレスとEtherTypeの変更が含まれ、これにより、通常であればフレームを消費またはブロックすることのあるキャリアイーサネットネットワーク上で、MACsecがシームレスに機能します。

WAN MACsecは、イーサネット暗号化の大きな進歩を表し、高速で安全なWAN接続に対する二ーズの高まりに対応します。ラインレートの暗号化、柔軟なネットワーク設計のサポート、およびパブリックキャリアサービスへの適合性を提供する機能を備えているため、最新のネットワークセキュリティアーキテクチャの重要なコンポーネントとなっています。WAN MACsecを活用することで、高速WANリンクの堅牢なセキュリティを実現すると同時に、ネットワークアーキテクチャを簡素化し、運用の複雑さを軽減できます。

設定

ネットワーク図



WAN MACsecトポロジ

コンフィギュレーション

ステップ1：基本的なデバイス設定

設定を開始するには、最初に、トラフィックのセグメント化とサービスプロバイダーへの接続に使用するサブインターフェイスを定義する必要があります。このシナリオでは、サブネット172.16.1.0/24に関連付けられたVLAN 100と、サブネット172.16.2.0/24に関連付けられたVLAN 200に対して2つのサブインターフェイスが定義されています（後で、1つのサブインターフェイスにのみMACsecを設定します）。

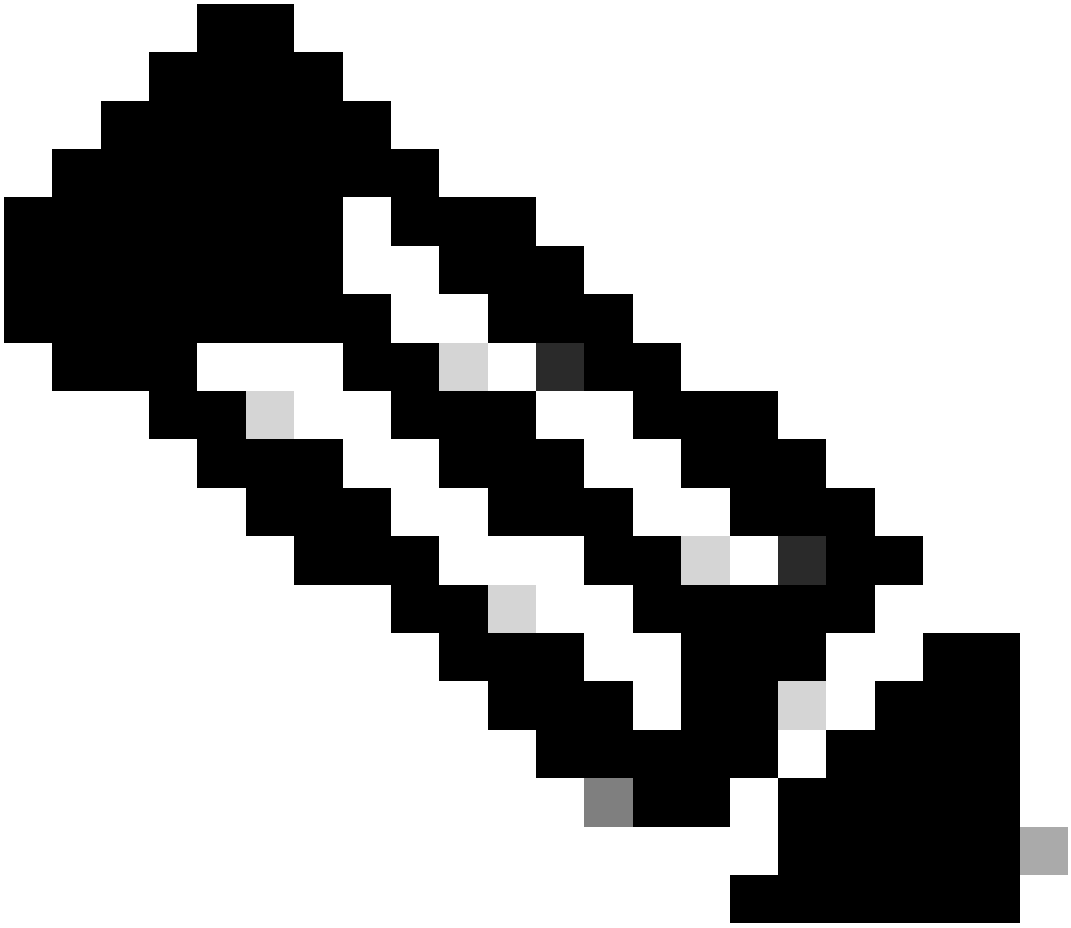
CE 8500-1	CE 8500-2
<#root> interface FortyGigabitEthernet0/2/4.100 **encapsulation dot1Q 100 ip address 172.16.1.1 255.255.255.0** ! interface FortyGigabitEthernet0/2/4.200 **encapsulation dot1Q 200 ip address 172.16.2.1 255.255.255.0**	<#root> interface FortyGigabitEthernet0/2/0.100 **encapsulation dot1Q 100 ip address 172.16.** ! interface FortyGigabitEthernet0/2/0.200 **encapsulation dot1Q 200 ip address 172.16.**

ステップ2:MACsecキーチェーンの設定

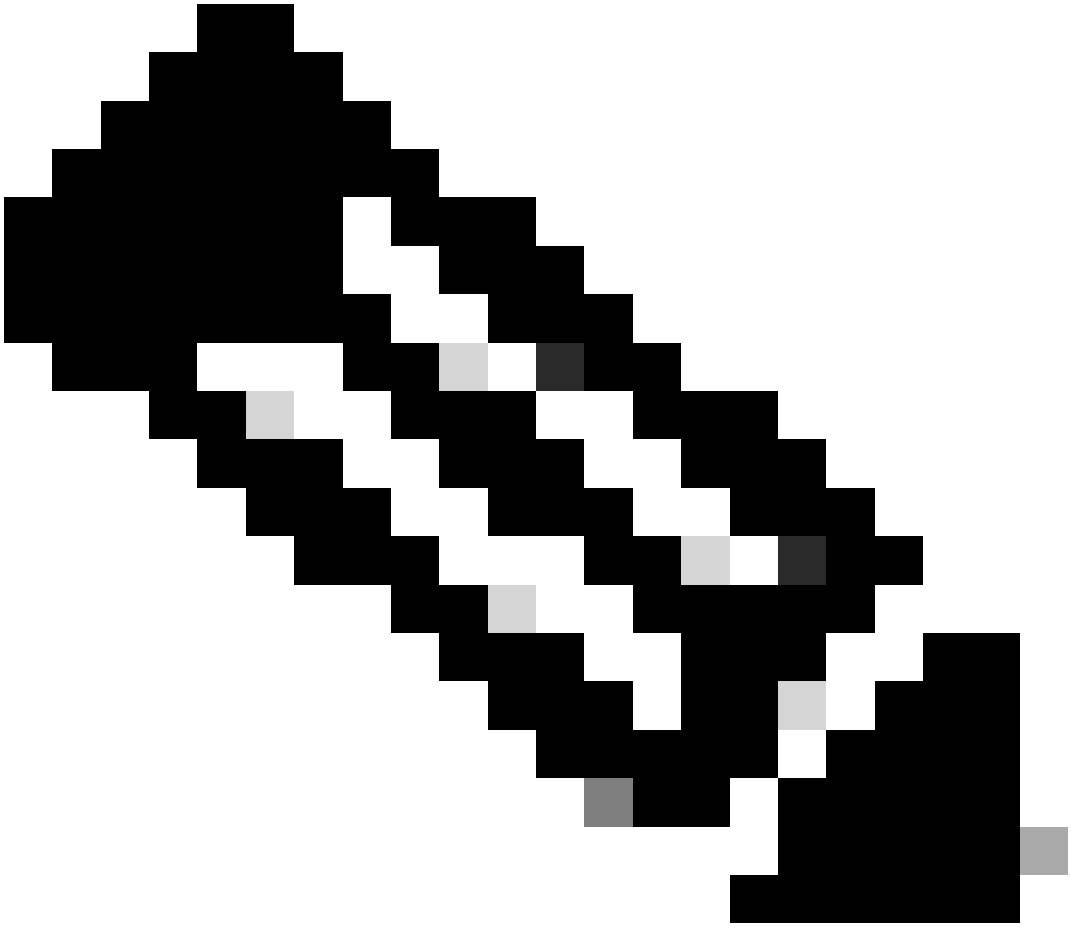
IEEE 802.1X-2010標準では、MACsec暗号キーを事前共有キー(PSK)から取得するか、802.1X拡張認証プロトコル(EAP)によって取得するか、またはMKAキーサーバによって選択および配布するように指定されていることに注意してください。この例では、PSKが使用され、MACsecキーチェーンを通じて手動で設定されます。これらは、MACsecで使用される他のすべての暗号キーを導出するために使用されるプライマリキーである接続関連キー(CAK)と同じです。

CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1** **8500-1(config-keychain-macsec-key)#** **lifetime 00:00:00 Jun 1 2024 duration 864000**	<#root> 8500-2# **configure terminal** **8500-2(config)#** **key chain keychain_vlan100** **8500-2(config-keychain-macs** **key 01** **8500-2(config-keychain-macs** **cryptographic-algorithm aes** **8500-2(config-keychain-macs** **key-string a5b2df4657bd8c02** **8500-2(config-keychain-macs** **lifetime 00:00:00 Jun 1 202**

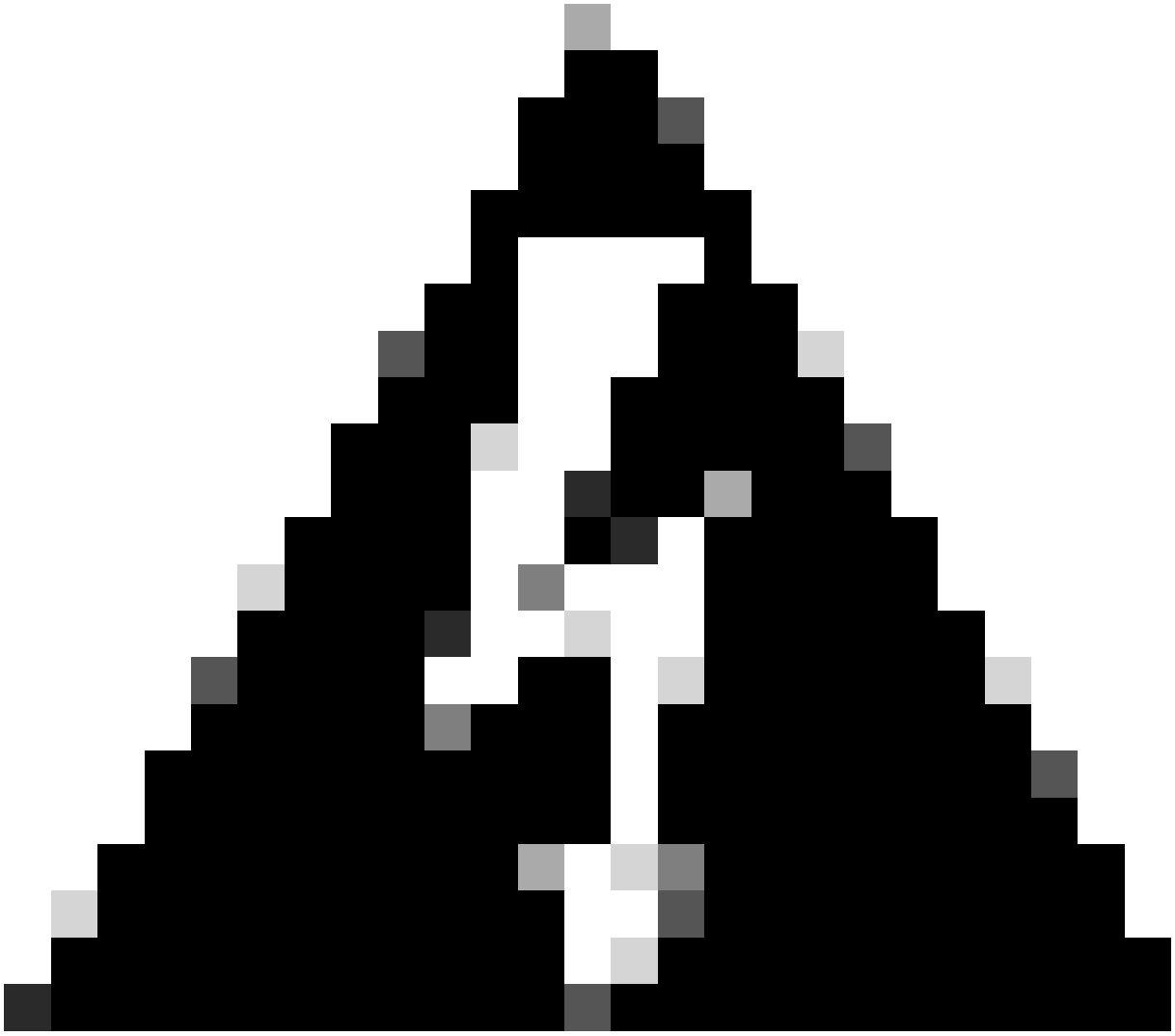
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
key 02	key 02
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
cryptographic-algorithm aes-256-cmac	cryptographic-algorithm aes
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
key-string b5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e2	key-string b5b2df4657bd8c02
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
lifetime 23:00:00 Jun 1 2024 infinite	lifetime 23:00:00 Jun 1 202
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
exit	exit
8500-1(config-keychain-macsec)#	8500-2(config-keychain-macs
exit	exit



注：MACsecキーチェーンの設定では、key-stringは16進数だけで構成される必要があり、aes-128-cmac暗号化アルゴリズムでは32桁のキーが必要であり、aes-256-cmac暗号化アルゴリズムでは64桁のキーが必要であることに注意してください。



注：複数のキーを使用する場合、指定したキーのライフタイムが経過した後にヒットレスキーロールオーバーを実行するには、それらのキー間で重複する期間が必要であることに注意してください。



警告：両方のルータのクロックが同期していることを確認することが重要です。そのため、ネットワークタイムプロトコル(NTP)の使用を強くお勧めします。そうしないと、MKAセッションの確立が妨げられたり、将来的にMKAセッションが失敗したりする可能性があります。

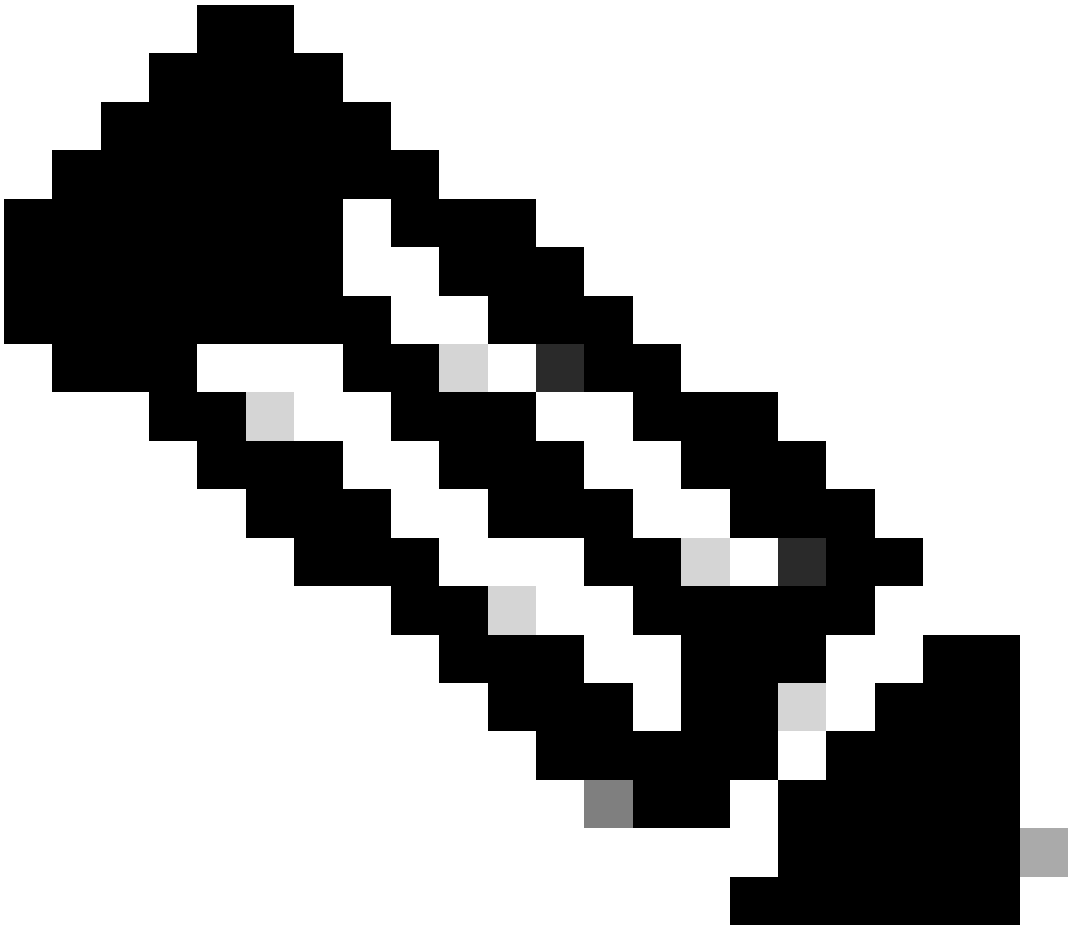
ステップ3:MKAポリシーの設定

デフォルトのMKAポリシーは初期設定や単純なネットワークに役立ちますが、特定のセキュリティ、コンプライアンス、およびパフォーマンスの要件を満たすために、一般にWAN MACsec用にカスタムMKAポリシーを設定することを推奨します。カスタムポリシーにより、柔軟性と制御性が向上し、ネットワークセキュリティが堅牢で、ニーズに合わせてカスタマイズされます。

MKAポリシーを設定する際には、キーサーバプライオリティ、MACsec Key Agreement Packet Data Unit(MKPDU)の遅延保護、暗号スイートなど、さまざまな要素を選択できます。このプラットフォームおよびソフトウェアバージョンでは、次の暗号を使用できます。

MACsec暗号	説明

gcm-aes-128	128ビットキーを使用した高度暗号化規格(AES)によるGalois/Counter Mode(GCM)
gcm-aes-256	256ビットキーを使用したAESによるGalois/Counter Mode(GCM)（暗号化の強度が高い）
gcm-aes-xpn-128	拡張パケット番号付け(XPN)による128ビットキーを使用したAESによるGalois/Counter Mode(GCM)
gcm-aes-xpn-256	256ビットキーを使用したAESによるGalois/Counter Mode(GCM)、XPN（より強力な暗号化強度）



注:XPNは、長いパケット番号付けをサポートすることでGCM-AES暗号化を強化し、非常に長い期間のセッションや高スループット環境のセキュリティを向上させます。40 Gb/sや100 Gb/sなどの高速リンクを使用すると、MACsecフレーム内のパケット番号(PN)が通常は送信されるパケット数に基づいて急速に枯渇するため、キーロールオーバー時間が非常に短くなる可能性があります。XPNはパケットの番号付けシーケンスを拡張し、大容量リンクで発生する可能性のあるセキュリティアソシエーションキー(SAK)の

頻繁なキー再生成の必要性を排除します。

この例では、MKAポリシーに対して選択された暗号はgcm-aes-xpn-256であり、他の要素はデフォルト値を持つことになります。

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. 8500-1(config)# **mka policy subint100** 8500-1(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-1(config-mka-policy)# **end**	<#root> 8500-2# **configure terminal** Enter configuration commands, one per line 8500-2(config)# **mka policy subint100** 8500-2(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-2(config-mka-policy)# **end**

ステップ4：インターフェイスレベルおよびサブインターフェイスレベルでMACsecを設定します。

このシナリオでは、物理インターフェイスにIPアドレスが設定されていない場合でも、ソリューションが機能するためにいくつかのmacsecコマンドをこのレベルで適用する必要があります。MACsecポリシーとキーチェーンは、サブインターフェイスレベルで適用されます（設定例を参照）。

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** 8500-1(config)# **interface FortyGigabitEthernet0/2/4** 8500-1(config-if)# **mtu 9216** 8500-1(config-if)# **cdp enable**	<#root> 8500-2# **configure terminal** 8500-2(config)# **interface FortyGigabitEthernet0/2/0** 8500-2(config-if)# **mtu 9216** 8500-2(config-if)# **cdp enable**

8500-1(config-if)#	8500-2(config-if)#
macsec dot1q-in-clear 1	**macsec dot1q-in-clear 1**
8500-1(config-if)#	8500-2(config-if)#
macsec access-control should-secure	**macsec access-control should-secure**
8500-1(config-if)#	8500-2(config-if)#
exit	**exit**
8500-1(config)#	8500-1(config)#
interface FortyGigabitEthernet0/2/4.100	**interface FortyGigabitEthernet0/2/0.100**
8500-1(config-if)#	8500-2(config-if)#
eapol destination-address broadcast-address	**eapol destination-address broadcast-address**
8500-1(config-if)#	8500-2(config-if)#
eapol eth-type 876F	**eapol eth-type 876F**
8500-1(config-if)#	8500-2(config-if)#
mka policy subint100	**mka policy subint100**
8500-1(config-if)#	8500-2(config-if)#
mka pre-shared-key key-chain keychain_vlan100	**mka pre-shared-key key-chain keychain_vlan100**
8500-1(config-if)#	8500-2(config-if)#
macsec	**macsec**
8500-2(config-if)#	8500-2(config-if)#
end	**end**

物理インターフェイスレベルで適用されるコマンド

a.トポロジで使用されているサービスプロバイダーがジャンボフレームを許可しているため、MTUは9216に設定されていますが、これは要件ではありません

b.コマンドmacsec dot1q-in-clearにより、オプションでVLAN(dot1q)タグをクリア（暗号化なし）にできます。

macsec access-control should-secureコマンドは、物理インターフェイスまたはサブインターフェイスからの暗号化されていないパケットの送受信を許可します（このコマンドは、一部のサブインターフェイスで暗号化が必要な場合と、不要な場合があります。これは、MACsecが有効になっている同じ物理インターフェイスからの暗号化されていないパケットの送受信を許可しないデフォルトのMACsec動作が原因です）。

サブインターフェイスレベルで適用されるコマンド

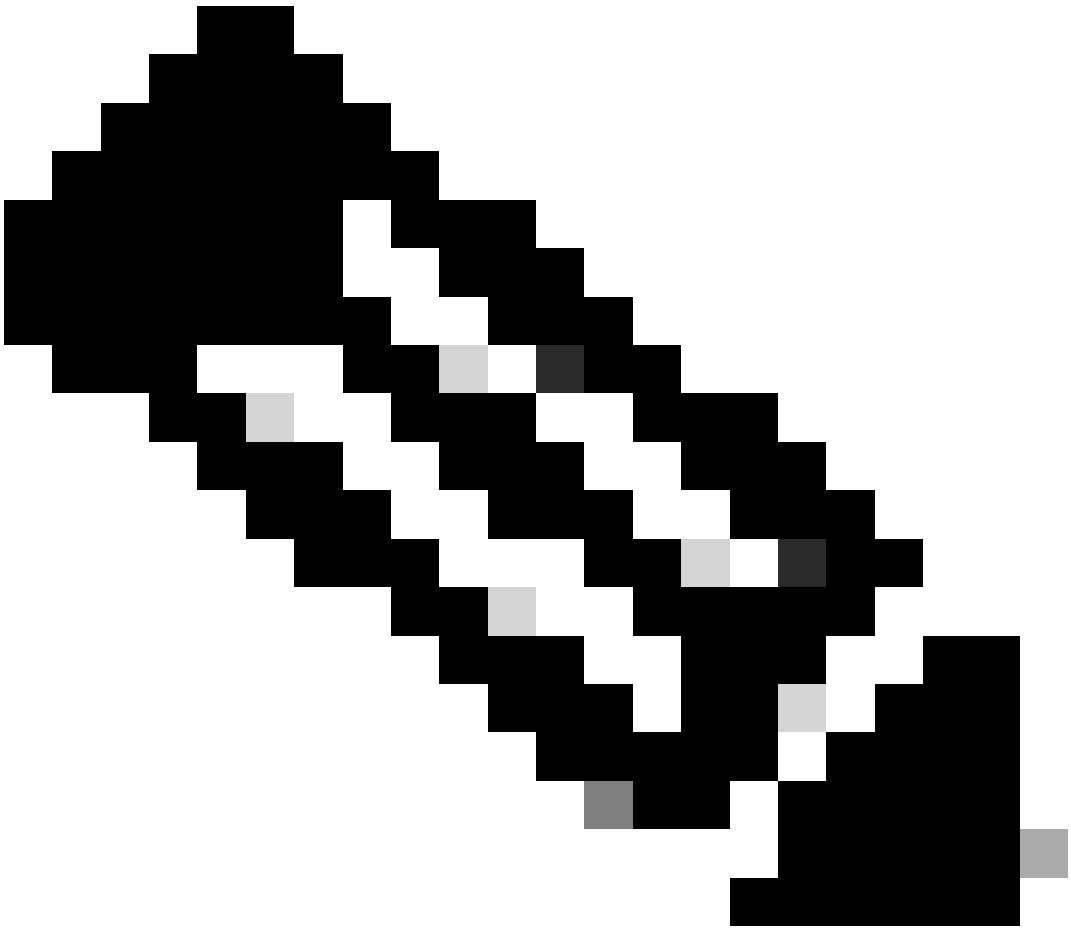
a.ここで、コマンドeapol destination-address broadcast-addressは、EAPoLフレームの宛先MACアドレス(デフォルトでは、マルチキャストMACアドレス01:80:C2:00:00:03)をブロードキャストMACアドレスに変更して、サービスプロバイダーが確実にパケットをフラッディングし、ドロップや使用を行わないようにするために必要です。

b. eapol eth-type 876Fコマンドを使用して、EAPoLフレームのデフォルトのイーサネットタイプ（デフォルトは0x888E）を変更し、これを0x876Fに変更することもできます。サービスプロバイダーがこれらのフレームを廃棄または消費しないようにするため、この手順も必要になります。

c.コマンドmka policy <policy name>およびmka pre-shared-key key-chain <key chain name>は、カスタムポリシーとキーチェーンをサブインターフェイスに適用するために使用されます。

d.最後に、macsecコマンドはサブインターフェイスレベルでMACsecを有効にします。

現在のセットアップでは、以前にEAPoLを変更していない場合、サービスプロバイダー側の9500スイッチはEAPoLフレームを転送していませんでした。



注:dot1q-in-clearやshould-secureなどのMACsecコマンドは、サブインターフェイスに継承されます。 また、EAPoLコマンドは物理インターフェイスレベルで設定できます。その場合、これらのコマンドはサブインターフェイスにも継承されます。 ただし、サブインターフェイスでEAPoLコマンドを明示的に設定すると、そのサブインターフェイスの継承された値またはポリシーが上書きされます。

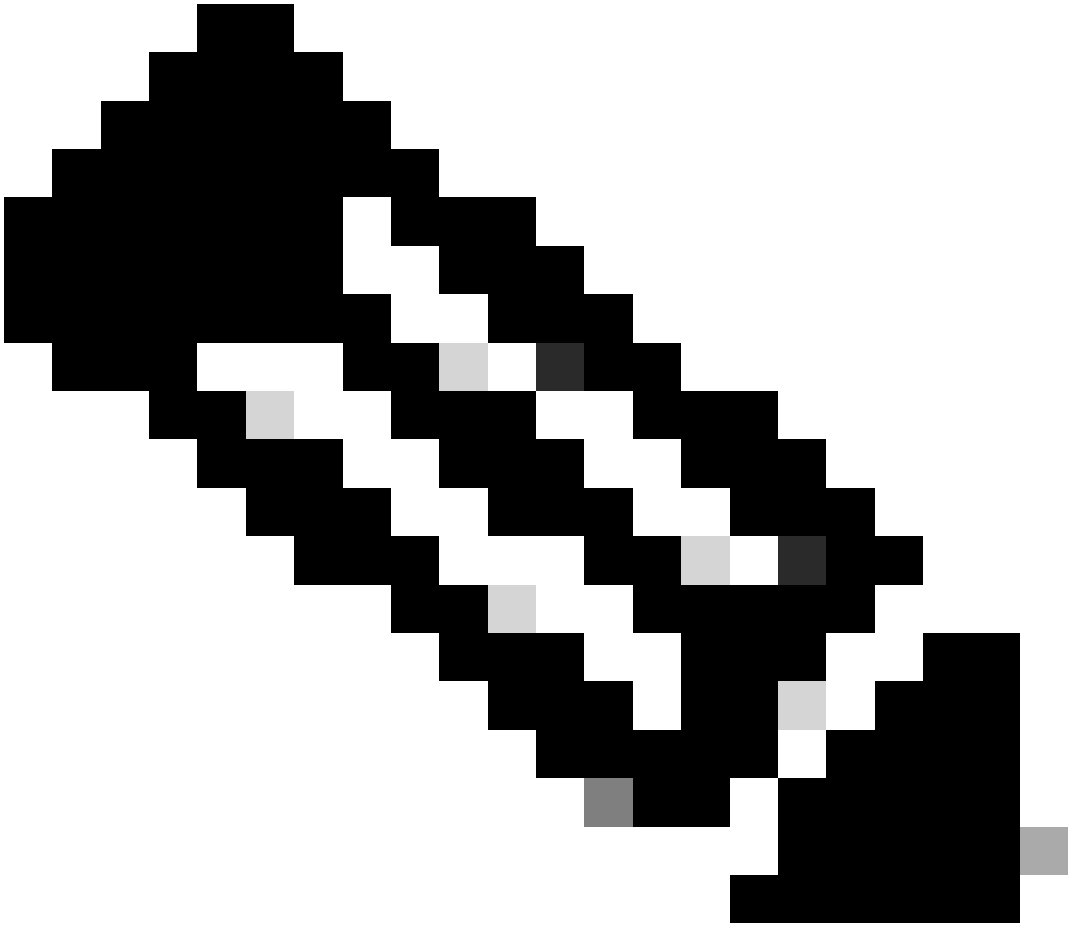
確認

設定が適用されると、次の出力は、各カスタマーエッジ(CE)C8500ルータの関連する実行コンフィギュレーションを示します（一部の設定は省略されました）。

```
<#root>
8500-1#
show running-config

Building configuration...

Current configuration : 8792 bytes
!
!
version 17.14
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
!
hostname 8500-1
!
boot-start-marker
boot system flash bootflash:c8000aep-universalk9.17.14.01a.SPA.bin
boot-end-marker
!
!
no logging console
no aaa new-model
!
!

key chain keychain_vlan100 macsec key 01 cryptographic-algorithm aes-256-cmac key-string a5b2df4657bd8c

!
!
!
!
!
!
license boot level network-premier addon dna-premier
!
!
spanning-tree extend system-id
!
```

```
mka policy subint100 macsec-cipher-suite gcm-aes-xpn-256


!
!
!
!
!
!
cdp run
!
!
!
!
interface Loopback100
 ip address 192.168.100.10 255.255.255.0
!
interface Loopback200
 ip address 192.168.200.10 255.255.255.0
!
!

interface FortyGigabitEthernet0/2/4

 mtu 9216
 no ip address
 no negotiation auto
 cdp enable

 macsec dot1q-in-clear 1 macsec access-control should-secure

!

interface FortyGigabitEthernet0/2/4.100

 encapsulation dot1Q 100
 ip address 172.16.1.1 255.255.255.0


ip mtu 9184

 eapol destination-address broadcast-address eapol eth-type 876F mka policy subint100 mka pre-shared-key

!

interface FortyGigabitEthernet0/2/4.200

 encapsulation dot1Q 200
 ip address 172.16.2.1 255.255.255.0
!
!
router eigrp 100
 network 172.16.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip forward-protocol nd
!
!
!
control-plane
!
!
!
!
!
```

```
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
!
!
!
!
!
!
end

8500-1#
```



注：MACsecを有効にした後でmacsecコマンドを適用すると、そのインターフェイスのMTUが自動的に調整され、MACsecオーバーヘッドを考慮して32バイト縮小されることに注意してください。

次に、ピア間のMACsecのステータスを確認するために使用できる重要なコマンドのリストを示します。次のコマンドは、現在のMACsecセッション、キーチェーン、ポリシー、および統計情報に関する詳細情報を提供します。

show mka sessions ：このコマンドは、現在のMKAセッションのステータスを表示します。

show mka sessions detail：このコマンドは、各MKAセッションに関する詳細情報を提供します。

show mka keychains:このコマンドは、MACsecに使用されるキーチェーンおよび割り当てられたインターフェイスを表示します。

show mka policy：このコマンドは、適用されたポリシー、使用されたインターフェイスと暗号スイートを表示します。

show mka summary：このコマンドは、MKAセッションと統計情報の概要を提供します。

show macsec statistics interface <interface name>：このコマンドは、指定されたインターフェイスのMACsec統計情報を表示し、暗号化されたトラフィックが送受信されているかどうかを識別するのに役立ちます。

CE 8500-1

```
<#root>

8500-1#

show 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
=========================================================================================================

Fo0/2/4.100

     78bc.1aac.1521/001a

subint100

         NO                  NO

26

              78bc.1aac.1420/001a  1

Secured
```

```
           02


8500-1#
show mka sessions detail


MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

TX-SSCI.................. 2
Local Tx-SCI............. 78bc.1aac.1521/001a

Interface MAC Address.... 78bc.1aac.1521

MKA Port Identifier...... 26
Interface Name........... FortyGigabitEthernet0/2/4.100
Audit Session ID.........
CAK Name (CKN)........... 02
Member Identifier (MI)... 8387013B6C4D6106D4443285
Message Number (MN)...... 439243
EAP Role................. NA
Key Server............... NO

MKA Cipher Suite......... AES-256-CMAC


Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... F5720CC2E83183F1E673DACD00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)


MKA Policy Name.......... subint100

Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO

SAK Cipher Suite......... 0080C20001000004 (GCM-AES-XPN-256)

MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------
```

```
  F5720CC2E83183F1E673DACD  439222      78bc.1aac.1420/001a  0         YES            1

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA           SSCI
                                                             Priority

Installed

  ------------------------------------------------------------------------------

8500-1#

show mka keychains


MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                    Interface(s)
Name             Latest CAK                                                    Applied
=============================================================================================

keychain_vlan100 02 Fo0/2/4.100


                 <HIDDEN>

8500-1#

show mka policy


MKA Policy defaults :
         Send-Secure-Announcements: DISABLED

MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
=============================================================================
*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128
                                             GCM-AES-256


subint100 0 FALSE 0 FALSE TRUE GCM-AES-XPN-256 Fo0/2/4.100




8500-1#

show mka summary


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
=============================================================================================
```

```
Fo0/2/4.100     78bc.1aac.1521/001a  subint100         NO                NO
26              78bc.1aac.1420/001a  1                 Secured           02



MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 14
   Fallback Secured........... 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 13
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 2
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics


MKPDUs Validated & Rx...... 737255

      "Distributed SAK"..... 18
      "Distributed CAK"..... 0


MKPDUs Transmitted......... 738485

      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures.............. 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
```

```
   KEK Derivation.................. 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation.................. 0
   Tx SC Creation.................. 0
   Rx SA Installation.............. 0
   Tx SA Installation.............. 0

MKPDU Failures
   MKPDU Tx........................... 0
   MKPDU Rx ICV Verification.............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation.................... 0
   MKPDU Rx Bad Peer MN................... 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0

8500-1#
```

show macsec statistics interface Fo0/2/4.100

```
MACsec Statistics for FortyGigabitEthernet0/2/4.100
 SecY Counters
  Ingress Untag Pkts:       0
  Ingress No Tag Pkts:      0
  Ingress Bad Tag Pkts:     0
  Ingress Unknown SCI Pkts: 0
  Ingress No SCI Pkts:      0
  Ingress Overrun Pkts:     0
  Ingress Validated Octets: 0
```

Ingress Decrypted Octets: 11853398

```
  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0
```

Egress Encrypted Octets: 11782598

```
 Controlled Port Counters
  IF In Octets:             14146226
  IF In Packets:            191065
  IF In Discard:            0
  IF In Errors:             0
  IF Out Octets:            14063174
  IF Out Packets:           190042
  IF Out Errors:            0

 Transmit SC Counters (SCI: 78BC1AAC1521001A)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048
 Transmit SA Counters (AN 0)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048

 Receive SA Counters (SCI: 78BC1AAC1420001A  AN 0)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
```

```
 In Pkts OK:               191069
 In Pkts Invalid:          0
 In Pkts Not Valid:        0
 In Pkts Not using SA:     0
 In Pkts Unused SA:        0
 In Pkts Late:             0
```

異なるサブインターフェイスからの到達可能性と、192.168.0.0/16サブネット間の到達可能性が成功します。次のpingテストでは、接続が正常に行われたことが示されます。

<#root>

8500-1#

ping 172.16.1.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

ping 172.16.2.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

ping 192.168.101.10 source 192.168.100.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

プロバイダーエッジ(PE)デバイスでICMPテストからパケットをキャプチャした後、暗号化フレームと非暗号化フレームを比較できます。イーサネットの外側のMACヘッダーが両方のフレームで同じで、dot1qタグが表示されていることに注意してください。ただし、暗号化されたフレームではEtherTypeが0x88E5(MACsec)と表示され、暗号化されていないフレームではICMPプロトコル情報とともにEtherTypeが0x0800(IPv4)と表示されます。

暗号化されたフレームVLAN 100

<#root>

F241.03.03-9500-1#

show monitor capture cap buffer detail | begin Frame 80

```
Frame 80: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface /tmp/epc_ws/wif_to
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 29, 2024 23:50:16.528191000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1722297016.528191000 seconds
    [Time delta from previous captured frame: 0.224363000 seconds]
    [Time delta from previous displayed frame: 0.224363000 seconds]
    [Time since reference or first frame: 21.989269000 seconds]
    Frame Number: 80
    Frame Length: 150 bytes (1200 bits)
    Capture Length: 150 bytes (1200 bits)
    [Frame is marked: False]
    [Frame is ignored: False]


[Protocols in frame: eth:ethertype:vlan:ethertype:macsec:data]

Ethernet II, Src: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21), Dst: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)

    Destination: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)
        Address: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
        Address: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

 Type: 802.1Q Virtual LAN (0x8100) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100

    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100

 Type: 802.1AE (MACsec) (0x88e5) 802.1AE Security tag

    0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
        0... .... = VER: 0x0
        .0.. .... = ES: Not set
        ..1. .... = SC: Set
        ...0 .... = SCB: Not set
        .... 1... = E: Set
        .... .1.. = C: Set
    .... ..00 = AN: 0x0
    Short length: 0

 Packet number: 147 System Identifier: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21) Port Identifier: 26 ICV: 2

Data (102 bytes)

0000  99 53 71 3e f6 c7 9b bb 00 21 68 48 d6 ca 26 af   .Sq>.....!hH..&.
0010  80 a5 76 40 19 c9 45 97 b3 5a 48 d3 2d 30 72 a6   ..v@..E..ZH.-0r.
0020  96 47 6e a7 4c 30 90 e5 70 10 80 e8 68 00 5f ad   .Gn.L0..p...h._.
0030  7f dd 4a 70 a8 46 00 ef 7d 56 fe e2 66 ba 6c 1b   ..Jp.F..}V..f.l.
0040  3a 07 44 4e 5e e7 04 cb cb f4 03 71 8d 40 da 55   :.DN^......q.@.U
0050  9f 1b ef a6 3a 1e 42 c7 05 e6 9e d0 39 6e b7 3f   ....:.B.....9n.?
0060  f2 82 cf 66 f2 5b                                 ...f.[
    Data: 9953713ef6c79bbb00216848d6ca26af80a5764019c94597b^@&
    [Length: 102]
```

関連情報

- WAN MACSECおよびMKAサポートの機能拡張
- 高速(1 ～ 100GE)WANの導入を保護するイーサネット暗号化(802.1AE - MACsec)の革新技術
- ルータ上のWAN MACSECのトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。