Konfigurieren von WAN MACsec auf Catalyst 8500 mit Subschnittstellen

Inhalt

Einleitung

Dieses Dokument beschreibt den Prozess zur Konfiguration der WAN Media Access Control Security (MACsec) auf Cisco Catalyst 8500-Plattformen mit Subschnittstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Erweiterte Netzwerkkonzepte wie WAN, VLANs und Verschlüsselung
- Grundlegendes zu MACsec (IEEE 802.1AE) und Schlüsselverwaltung (IEEE 802.1X-2010)
- Vertrautheit mit Cisco IOS® XE Command Line Interface (CLI)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

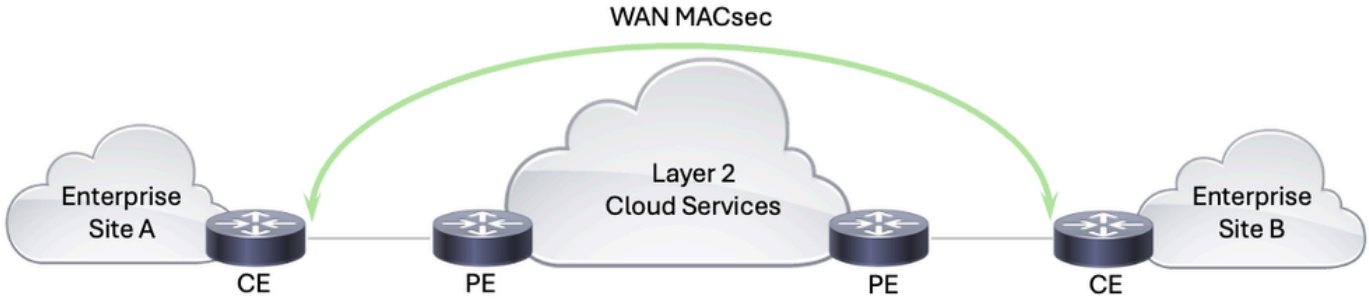
- Cisco Catalyst Edge-Plattformen der Serie 8500

- Cisco IOS XE Version 17.14.01a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

WAN MACsec ist eine Sicherheitslösung, die entwickelt wurde, um den Netzwerkverkehr in WAN-Netzwerken durch die Nutzung der Funktionen von MACsec zu schützen. Wenn ein Service-Provider-Netzwerk für den Datenaustausch verwendet wird, ist es wichtig, übertragene Daten zu verschlüsseln, um Manipulationen zu verhindern. WAN MACsec ist einfach bereitzustellen und zu verwalten und eignet sich ideal für Unternehmen, die ihren Netzwerkverkehr vor Datenmanipulation wie Lauschangriffen und Man-in-the-Middle-Angriffen schützen müssen. Die nahtlose Line-Rate-Verschlüsselung stellt sicher, dass die Daten sicher und ohne Einschränkungen durch verschiedene Netzwerkinfrastrukturen wie Service Provider-Netzwerke, Cloud-Umgebungen und Unternehmensnetzwerke übertragen werden.



WAN MACsec-Lösung

MACsec ist nach dem IEEE 802.1AE-Standard definiert und bietet sichere Kommunikation in Ethernet-Netzwerken, um die Datenvertraulichkeit, Integrität und Ursprungsauthentizität für Ethernet-Frames sicherzustellen. MACsec arbeitet auf der Sicherungsschicht (Layer 2) des OSI-Modells (Open Systems Interconnection) und verschlüsselt und authentifiziert Ethernet-Frames, um die Kommunikation zwischen Knoten zu sichern. Ursprünglich für LANs entwickelt, wurde MACsec weiterentwickelt, um auch WAN-Bereitstellungen zu unterstützen. Dank Line-Rate-Verschlüsselung werden Latenz und Overhead minimiert, was für Hochgeschwindigkeitsnetzwerke von entscheidender Bedeutung ist.

IEEE 802.1X-2010 ist eine Ergänzung zum ursprünglichen IEEE 802.1X-Standard, der eine Port-basierte Netzwerkzugriffskontrolle definiert. Mit der Version 2010 wurde das MACsec Key Agreement (MKA)-Protokoll eingeführt, das für die Verwaltung von Verschlüsselungsschlüsseln in MACsec-Implementierungen unerlässlich ist. MKA übernimmt die Verteilung und Verwaltung von kryptografischen Schlüsseln, die von MACsec zum Verschlüsseln und Entschlüsseln von Daten verwendet werden. MKA ist ein Standard, der zur Interoperabilität mit Systemen verschiedener Hersteller für MACsec-Bereitstellungen beiträgt und sichere Schlüsselaustausch- und Schlüsselwiederholungsmechanismen unterstützt, die für die Aufrechterhaltung kontinuierlicher

Sicherheit in dynamischen WAN-Umgebungen von entscheidender Bedeutung sind.

In WAN-MACsec-Bereitstellungen stellt IEEE 802.1AE (MACsec) die grundlegenden Verschlüsselungs- und Sicherheitsmechanismen auf der Datenverbindungsebene bereit und stellt sicher, dass alle Ethernet-Frames geschützt sind, während sie das Netzwerk durchlaufen. IEEE 802.1X-2010 mit dem MKA-Protokoll übernimmt die kritische Aufgabe der Verteilung und Verwaltung der für die Funktion von MACsec erforderlichen Verschlüsselungsschlüssel. Zusammen stellen diese Standards sicher, dass WAN MACsec eine robuste Hochgeschwindigkeits-Verschlüsselung für WAN-Netzwerke bereitstellen kann, die einen umfassenden Schutz für die Übertragung von Daten bietet und gleichzeitig Interoperabilität und einfaches Management gewährleistet.

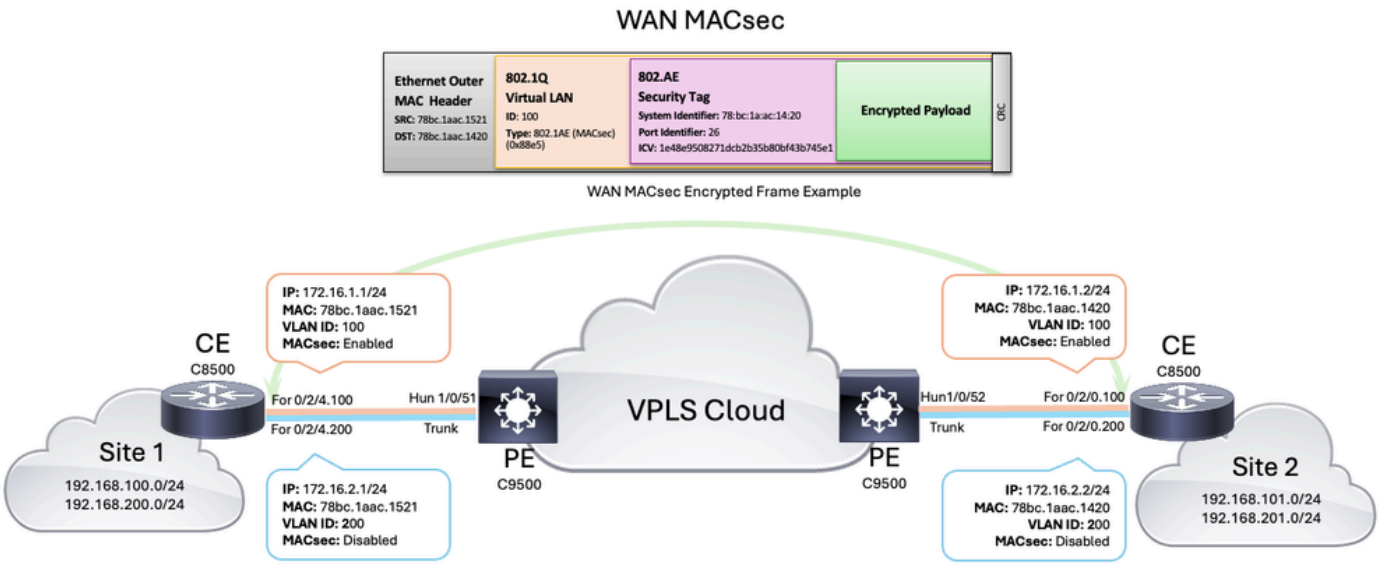
Um den besonderen Herausforderungen von WAN-Umgebungen gerecht zu werden, wurden einige Verbesserungen an den traditionellen MACsec-Bereitstellungen vorgenommen:

- 802.1Q-Tag im Clear-Modus: Mit dieser Funktion kann das 802.1Q-VLAN-Tag außerhalb des verschlüsselten MACsec-Headers freigegeben werden, wodurch flexiblere Netzwerkdesigns insbesondere in Umgebungen mit öffentlichem Ethernet-Transport möglich sind. Diese Funktion ist für die Integration von MACsec mit Carrier Ethernet-Services unerlässlich, da sie die Koexistenz von verschlüsseltem und unverschlüsseltem Datenverkehr im gleichen Netzwerk ermöglicht, die Netzwerkarchitektur vereinfacht und die Kosten senkt
- Anpassbarkeit über Public Carrier Ethernet: Moderne WAN MACsec-Implementierungen können an Public Carrier Ethernet-Services angepasst werden. Diese Anpassbarkeit umfasst die Änderung der EAPoL-Zieladresse (Ethernet Authentication Protocol over LAN) und des EtherType, sodass MACsec nahtlos über Carrier Ethernet-Netzwerke funktioniert, die diese Frames andernfalls nutzen oder blockieren können.

WAN MACsec stellt einen bedeutenden Fortschritt bei der Ethernet-Verschlüsselung dar und erfüllt so den wachsenden Bedarf an sicheren Hochgeschwindigkeits-WAN-Verbindungen. Die Möglichkeit zur Line-Rate-Verschlüsselung, Unterstützung flexibler Netzwerkdesigns und die Anpassungsfähigkeit an Services von öffentlichen Betreibern machen das System zu einer wichtigen Komponente moderner Netzwerksicherheitsarchitekturen. Durch den Einsatz von WAN MACsec erhalten Unternehmen zuverlässige Sicherheit für ihre Hochgeschwindigkeits-WAN-Verbindungen bei gleichzeitiger Vereinfachung der Netzwerkarchitektur und Verringerung der betrieblichen Komplexität.

Konfigurieren

Netzwerkdiagramm



WAN-MACsec-Topologie

Konfigurationen

Schritt 1: Grundlegende Gerätekonfiguration

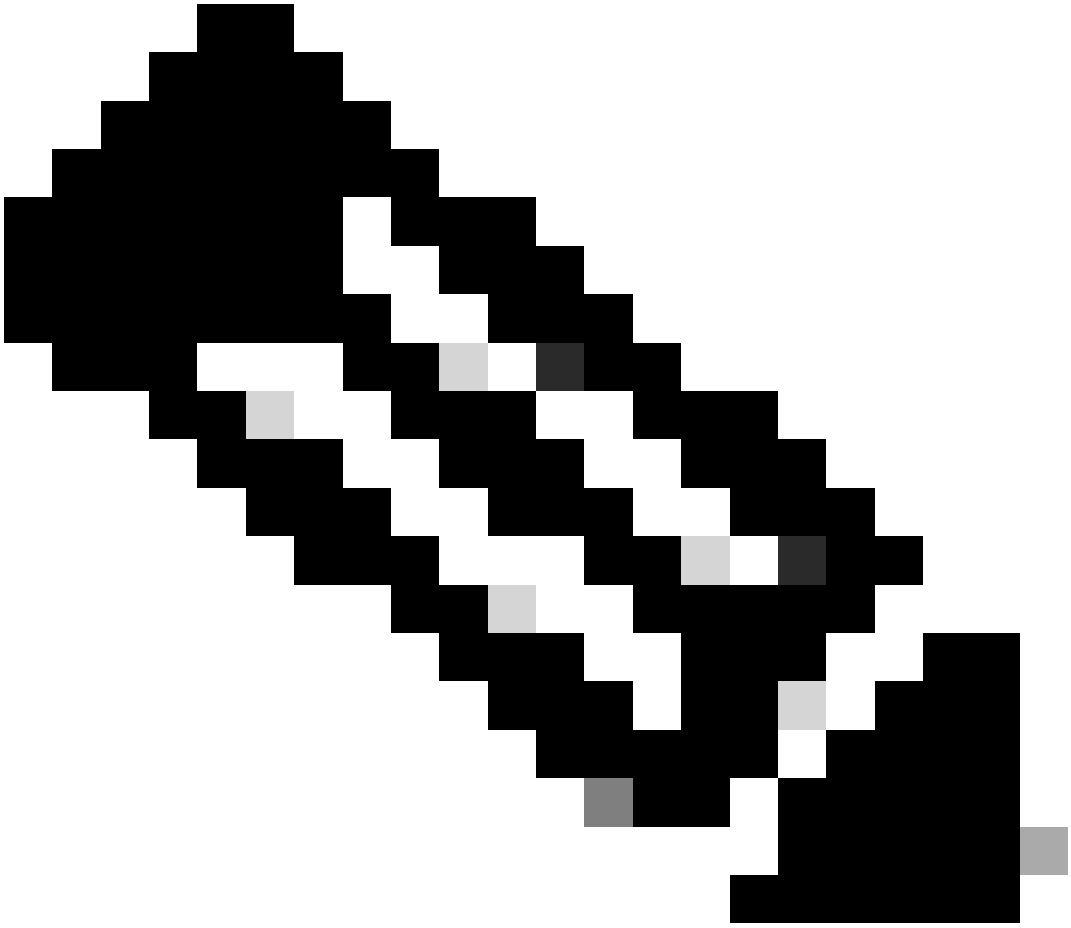
Zum Starten der Konfiguration müssen Sie zunächst die Subschnittstellen definieren, die für die Segmentierung des Datenverkehrs und die Verbindung zum Service Provider verwendet werden. In diesem Szenario werden zwei Subschnittstellen für VLAN 100 definiert, das dem Subnetz 172.16.1.0/24 zugeordnet ist, und für VLAN 200, das dem Subnetz 172.16.2.0/24 zugeordnet ist (später wird nur eine Subschnittstelle mit MACsec konfiguriert).

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.**

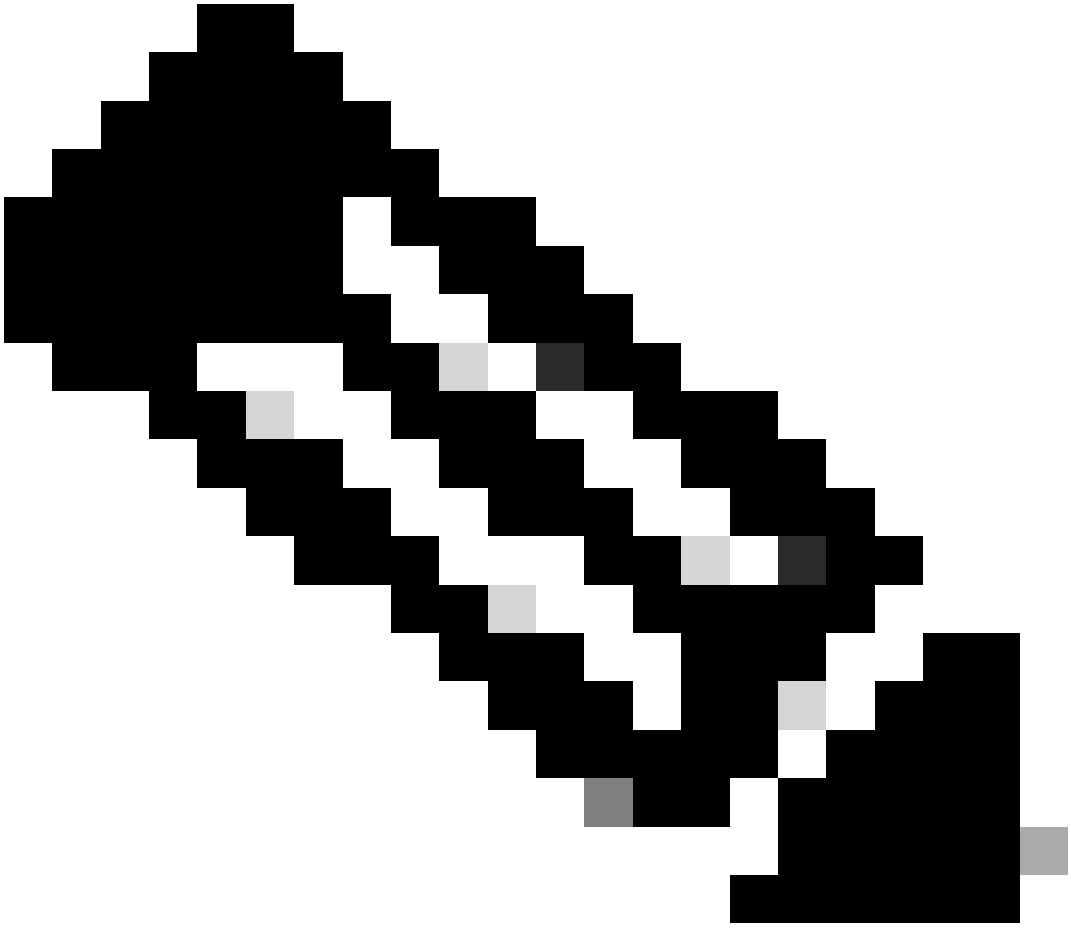
Schritt 2: Konfigurieren der MACsec-Schlüsselkette

Denken Sie daran, dass der IEEE 802.1X-2010-Standard angibt, dass die MACsec-Verschlüsselungsschlüssel von einem Pre-Shared Key (PSK) durch das 802.1X Extensible Authentication Protocol (EAP) abgeleitet oder von einem MKA-Schlüsselserver ausgewählt und verteilt werden können. In diesem Beispiel werden PSKs verwendet und manuell über die MACsec-Schlüsselkette konfiguriert. Diese entsprechen dem Connectivity Association Key (CAK), dem Primärschlüssel für die Ableitung aller anderen in MACsec verwendeten Verschlüsselungsschlüssel.

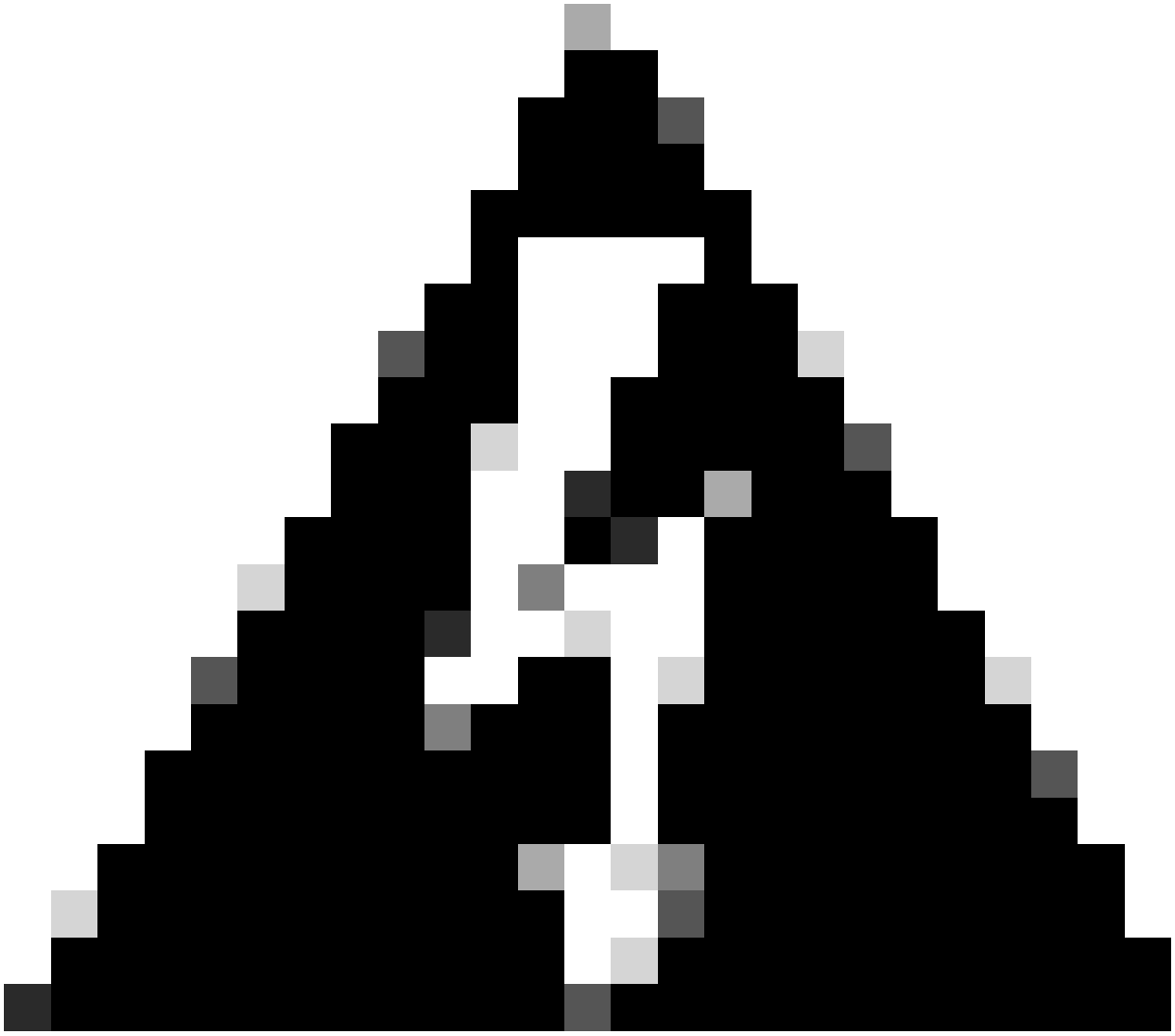
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1** **8500-1(config-keychain-macsec-key)#** **lifetime 00:00:00 Jun 1 2024 duration 864000** **8500-1(config-keychain-macsec-key)#** **key 02** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string b5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e2** **8500-1(config-keychain-macsec-key)#** **lifetime 23:00:00 Jun 1 2024 infinite** **8500-1(config-keychain-macsec-key)#** **exit** **8500-1(config-keychain-macsec)#** **exit**	<#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** **8500-2(config-keychain-macs** **key 02** **8500-2(config-keychain-macs** **cryptographic-algorithm aes** **8500-2(config-keychain-macs** **key-string b5b2df4657bd8c02** **8500-2(config-keychain-macs** **lifetime 23:00:00 Jun 1 202** **8500-2(config-keychain-macs** **exit** **8500-2(config-keychain-macs** **exit**



Hinweis: Denken Sie bei der Konfiguration der MACsec-Schlüsselkette daran, dass die Schlüsselzeichenfolge nur aus Hexadezimalziffern bestehen muss. Der Verschlüsselungsalgorithmus aes-128-cmac erfordert einen Schlüssel mit 32 Hexadezimalziffern, und der Verschlüsselungsalgorithmus aes-256-cmac erfordert einen Schlüssel mit 64 Hexadezimalziffern. 1.



Hinweis: Denken Sie daran, dass sich die Zeitintervalle bei Verwendung mehrerer Schlüssel überschneiden muss, um nach Ablauf der angegebenen Schlüssellebensdauer ein Rollover bei einem unterbrechungsfreien Schlüssel zu erreichen.



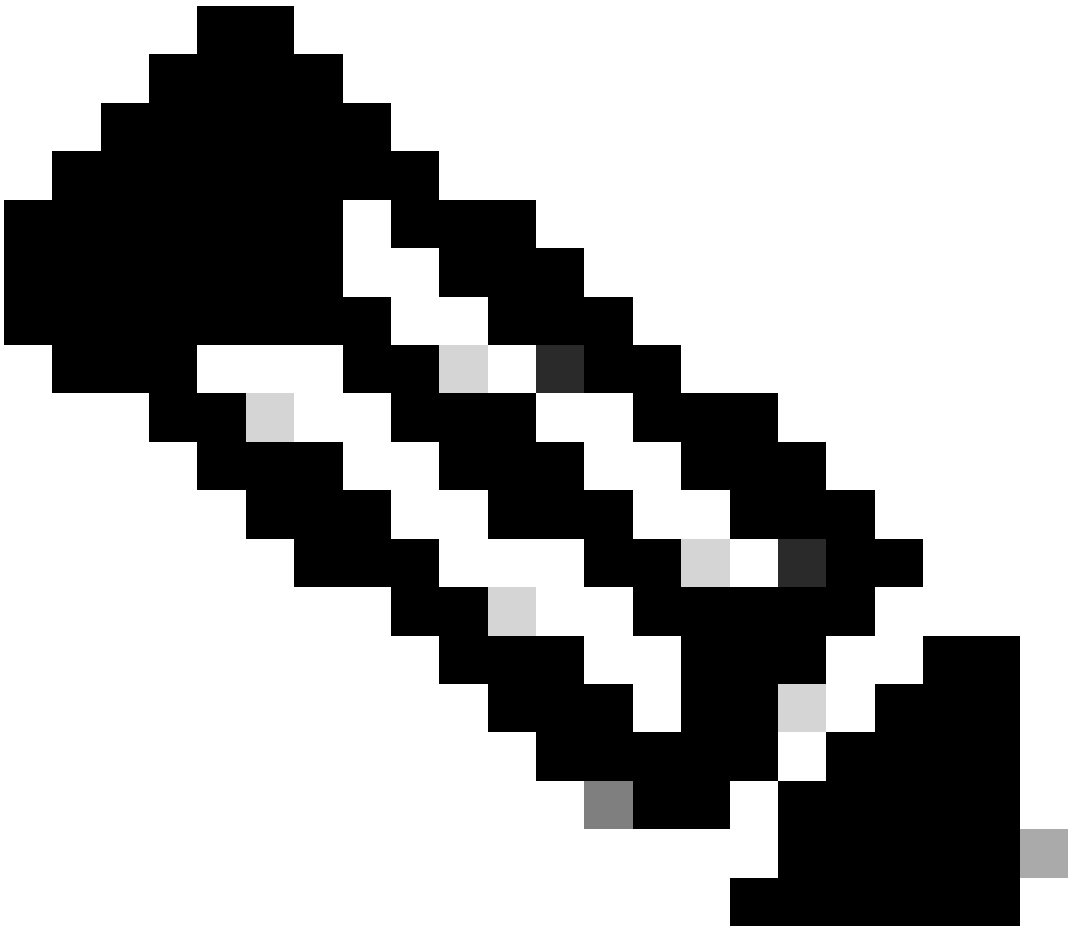
Warnung: Es ist wichtig, die Uhren beider Router zu synchronisieren. Daher wird die Verwendung des Network Time Protocol (NTP) dringend empfohlen. Andernfalls kann die Einrichtung von MKA-Sitzungen verhindert oder in Zukunft zum Scheitern verurteilt werden.

Schritt 3: Konfigurieren der MKA-Richtlinie

Während die Standard-MKA-Richtlinie für die Ersteinrichtung und einfache Netzwerke nützlich sein kann, wird die Konfiguration einer benutzerdefinierten MKA-Richtlinie für WAN MACsec im Allgemeinen empfohlen, um bestimmte Sicherheits-, Compliance- und Leistungsanforderungen zu erfüllen. Kundenspezifische Richtlinien bieten mehr Flexibilität und Kontrolle und stellen sicher, dass Ihre Netzwerksicherheit robust und an Ihre Anforderungen angepasst ist.

Beim Konfigurieren der MKA-Richtlinie können verschiedene Elemente ausgewählt werden, z. B. Key Server Priority, Delay Protection for the MACsec Key Agreement Packet Data Unit (MKPDU), Cipher Suite usw. In diesen Plattform- und Softwareversionen können die folgenden Chiffren verwendet werden:

MACsec-Verschlüsselung	Beschreibung
GCM-AES-128	Galois-/Zählermodus (GCM) mit Advanced Encryption Standard (AES) mit 128-Bit-Schlüssel
GCM-AES-256	Galois/Counter Mode (GCM) mit AES mit 256-Bit-Schlüssel (höhere Verschlüsselungsstärke)
gcm-aes-xpn-128	Galois-/Zählermodus (GCM) mit AES über einen 128-Bit-Schlüssel mit Extended Packet Numbering (XPN)
gcm-aes-xpn-256	Galois/Counter Mode (GCM) mit AES mit 256-Bit-Schlüssel, mit XPN (höhere Verschlüsselungsstärke)



Hinweis: XPN verbessert die GCM-AES-Verschlüsselung durch Unterstützung einer längeren Paketnummerierung, wodurch die Sicherheit für langlebige Sitzungen oder Umgebungen mit hohem Durchsatz verbessert wird. Die Verwendung von Hochgeschwindigkeitsverbindungen, z. B. 40 Gbit/s oder 100 Gbit/s, kann zu sehr kurzen

Schlüsselbereitstellungszeiten führen, da die Paketnummer (PN) innerhalb des MACsec-Frames, die in der Regel auf der Anzahl der gesendeten Pakete basiert, bei diesen Geschwindigkeiten schnell erschöpft sein könnte. Mit XPN wird die Paketnummerierungssequenz erweitert, und es ist kein häufiger SAK-Schlüssel (Security Association Key) erforderlich, der bei Verbindungen mit hoher Kapazität auftreten kann.

In diesem Beispiel ist die ausgewählte Verschlüsselung für die MKA-Richtlinie gcm-aes-xpn-256, und andere Elemente haben den Standardwert:

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**

Schritt 4: Konfigurieren von MACsec auf Schnittstellen- und Subschnittstellenebene

Obwohl in diesem Szenario die physische Schnittstelle nicht mit einer IP-Adresse konfiguriert wird, müssen einige Macsec-Befehle auf dieser Ebene angewendet werden, damit die Lösung funktioniert. Die MACsec-Richtlinie und die Schlüsselkette werden auf Ebene der Subschnittstelle angewendet (siehe Konfigurationsbeispiel):

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

8500-1(config-if)#	8500-2(config-if)#
cdp enable	**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**

Auf Ebene der physischen Schnittstelle angewendete Befehle

a. Die MTU ist auf 9216 festgelegt, da der in der Topologie verwendete Service Provider Jumbo Frames zulässt. Dies ist jedoch keine Anforderung.

b. Mit dem Befehl macsec dot1q-in-clear wird die Option aktiviert, bei der das VLAN-Tag (dot1q) unverschlüsselt ist.

c. Mit dem Befehl macsec access-control should-secure können unverschlüsselte Pakete von der physischen Schnittstelle oder Subschnittstelle gesendet oder empfangen werden (dieser Befehl ist erforderlich, wenn einige Subschnittstellen eine Verschlüsselung erfordern und andere nicht, da dies auf das standardmäßige MACsec-Verhalten zurückzuführen ist, bei dem keine unverschlüsselten Pakete von derselben physischen Schnittstelle gesendet oder empfangen

werden können, auf der MACsec aktiviert ist)

Auf Subschnittstellenebene angewendete Befehle

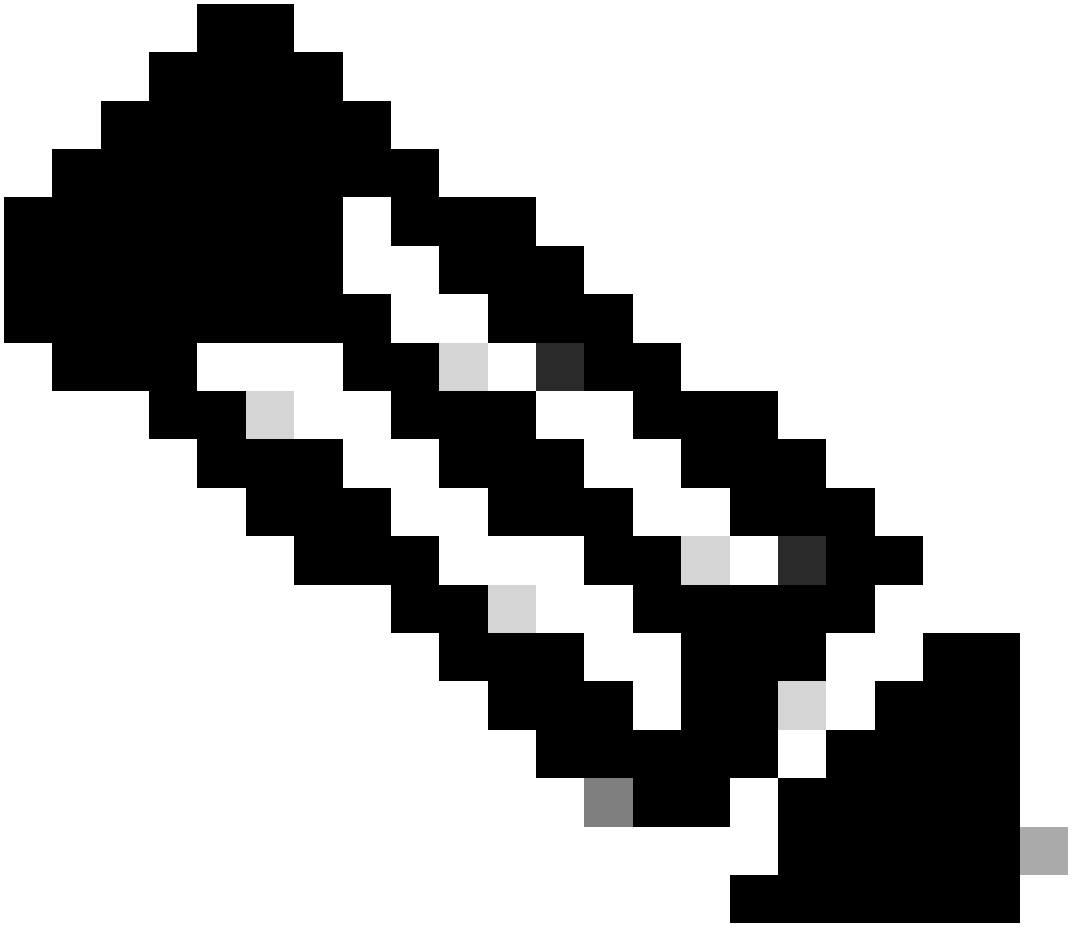
a. Nun wird der Befehl eapol destination-address broadcast-address benötigt, um die Ziel-MAC-Adresse der EAPoL-Frames (standardmäßig eine Multicast-MAC-Adresse 01:80:C2:00:00:03) in eine Broadcast-MAC-Adresse zu ändern, um sicherzustellen, dass der Service Provider sie nicht verwirft oder konsumieren.

b. Mit dem Befehl eapol eth-type 876F wird auch der Standard-Ethernet-Typ des EAPoL-Frames (standardmäßig 0x888E) und 0x876F geändert. Dies ist wiederum erforderlich, damit der Service Provider diese Frames nicht verwirft oder verbraucht.

c. Die Befehle mka policy <Policy-Name> und mka pre-shared-key-chain <Key-Chain-Name> werden verwendet, um die benutzerdefinierte Richtlinie und Key-Chain auf die Subschnittstelle anzuwenden.

d. Und nicht zuletzt aktiviert der Befehl macsec MACsec auf Subschnittstellenebene.

In der aktuellen Konfiguration wurden die EAPoL-Frames von den 9500-Switches auf Seiten des Service Providers ohne die vorherigen EAPoL-Änderungen nicht weitergeleitet.



Hinweis: MACsec-Befehle wie dot1q-in-clear und should-secure werden von den Subschnittstellen übernommen. Zusätzlich können EAPoL-Befehle auf der Ebene der physischen Schnittstelle festgelegt werden. In solchen Fällen werden diese Befehle auch von den Subschnittstellen übernommen. Die explizite Konfiguration von EAPoL-Befehlen auf der Subschnittstelle überschreibt jedoch den geerbten Wert oder die Richtlinie für diese Subschnittstelle.

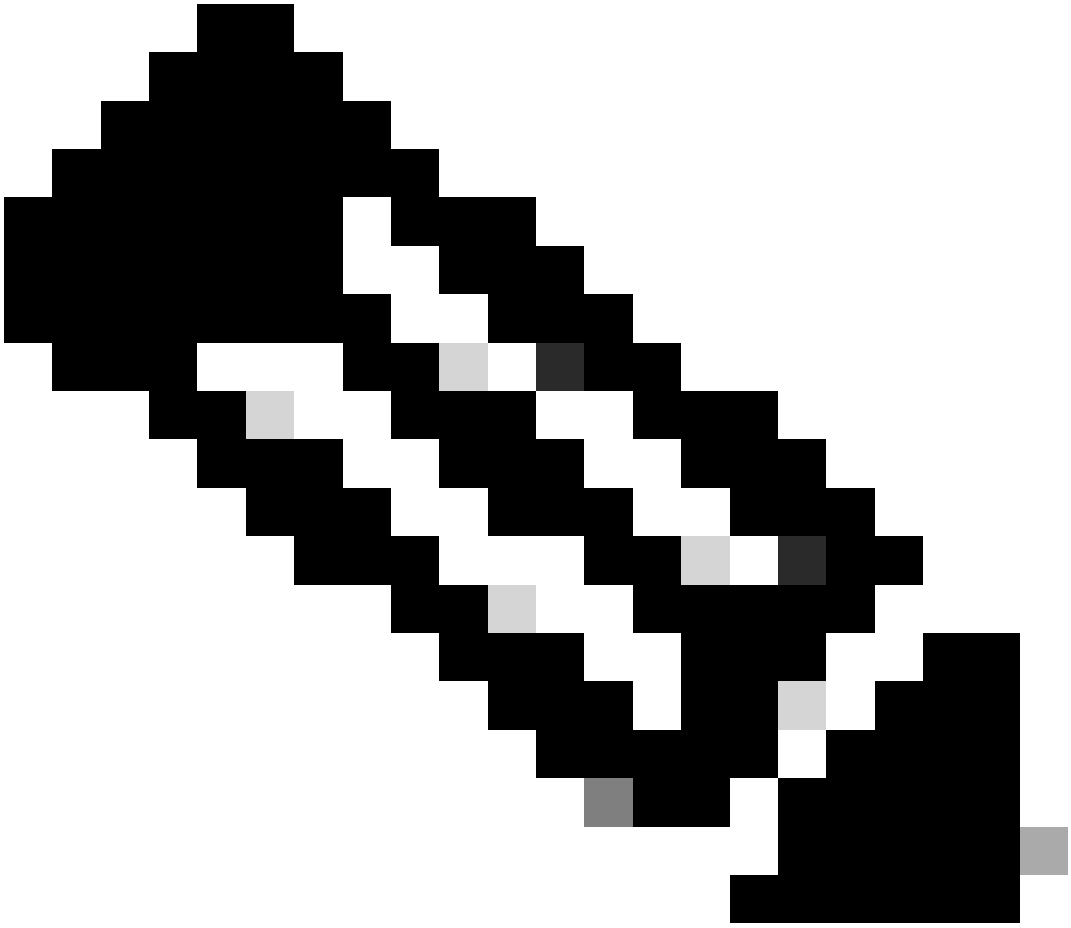
Überprüfung

Nach Anwendung der Konfiguration zeigt die nächste Ausgabe die relevante aktuelle Konfiguration von jedem C8500-Router am Customer Edge (CE) an (einige Konfigurationen wurden ausgelassen):

```
<#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#
```



Hinweis: Beachten Sie, dass nach der Aktivierung von MACsec durch Anwendung des Macsec-Befehls die MTU an dieser Schnittstelle automatisch angepasst und um 32 Byte reduziert wird, um den MACsec-Overhead zu berücksichtigen.

Als Nächstes finden Sie eine Liste der wichtigsten Befehle, mit denen der Status von MACsec zwischen Peers überprüft und überprüft werden kann. Diese Befehle liefern Ihnen detaillierte Informationen zu aktuellen MACsec-Sitzungen, Schlüsselbändern, Richtlinien und Statistiken:

show mka sessions - Mit diesem Befehl wird der aktuelle MKA-Sitzungsstatus angezeigt.

show mka sessions detail - Dieser Befehl liefert detaillierte Informationen zu jeder MKA-Sitzung.

show mka keychains - Dieser Befehl zeigt die für MACsec verwendeten Schlüsselketten und die zugeordnete Schnittstelle an.

show mka policy - Mit diesem Befehl werden die angewendeten Richtlinien, die verwendeten Schnittstellen und die verwendete Verschlüsselungssuite angezeigt.

show mka summary - Dieser Befehl bietet eine Zusammenfassung der MKA-Sitzungen und -Statistiken.

show macsec statistics interface <Schnittstellenname> - Dieser Befehl zeigt die MACsec-Statistiken für eine angegebene Schnittstelle an und hilft zu identifizieren, ob verschlüsselter Datenverkehr gesendet und empfangen wird.

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
```

Die Erreichbarkeit über die verschiedenen Subschnittstellen und die Erreichbarkeit zwischen den Subnetzen 192.168.0.0/16 war erfolgreich. Die folgenden Ping-Tests zeigen die erfolgreiche Verbindung:

```
<#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#
```

Nach der Erfassung von Paketen aus einem ICMP-Test auf dem PE-Gerät (Provider Edge) können Sie die verschlüsselten und unverschlüsselten Frames vergleichen. Beachten Sie, dass der äußere Ethernet-MAC-Header auf beiden Frames identisch ist und das dot1q-Tag sichtbar ist. Der verschlüsselte Frame zeigt jedoch den EtherType 0x88E5 (MACsec) an, während der unverschlüsselte Frame den EtherType 0x0800 (IPv4) zusammen mit den ICMP-Protokollinformationen anzeigt:

VLAN 100 für verschlüsselten Frame
<#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]
```

Zugehörige Informationen

- WAN MACSEC- und MKA-Unterstützung - Erweiterungen
- Innovationen bei der Ethernet-Verschlüsselung (802.1AE - MACsec) für die Sicherung von Hochgeschwindigkeits-WAN-Bereitstellungen (1-100GE)
- Fehlerbehebung bei WAN MACSEC auf Routern

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.