WAN MACsec op Catalyst 8500 met subinterfaces configureren

Inhoud

Inleiding

Dit document beschrijft het proces voor het configureren van WAN Media Access Control Security (MACsec) op Cisco Catalyst 8500-platforms met subinterfaces.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Geavanceerde netwerkconcepten, inclusief WAN, VLAN's en codering
- Inzicht in MACsec (IEEE 802.1AE) en sleutelbeheer (IEEE 802.1X-2010)
- Bekendheid met Cisco IOS® XE Command Line Interface (CLI)

Gebruikte componenten

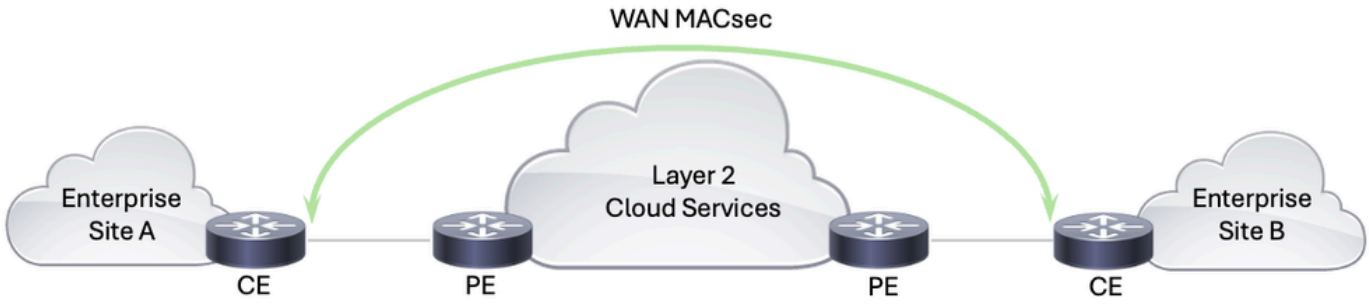
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 8500 Series Edge-platforms
- Cisco IOS XE versie 17.14.01a

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

WAN MACsec is een beveiligingsoplossing die is ontworpen om netwerkverkeer via WAN-netwerken te beveiligen door gebruik te maken van de functies van MACsec. Wanneer u een netwerk van serviceproviders gebruikt om gegevens uit te wisselen, is het belangrijk om gegevens tijdens het transport te versleutelen om manipulatie te voorkomen. WAN MACsec is eenvoudig te implementeren en te beheren, waardoor het ideaal is voor organisaties die hun netwerkverkeer moeten beveiligen tegen gegevensmanipulatie, zoals afluisteren en man-in-the-middle aanvallen. Het biedt naadloze, lijnsnelheidsencryptie, die ervoor zorgt dat gegevens veilig en compromisloos blijven aangezien het diverse netwerkinfrastructuur, met inbegrip van de netwerken van de dienstverlener, wolkenmilieu's, en ondernemingsnetwerken oversteekt.



WAN MACsec-oplossing

Om een beetje geschiedenis te delen, verstrekt MACsec, die door de norm IEEE 802.1AE wordt bepaald, veilige communicatie op Ethernet netwerken door gegevensvertrouwelijkheid, integriteit, en oorsprongsethechtheid voor Ethernet kaders te verzekeren. MACsec werkt op de datalink-laag (Layer 2) van het model Open Systems Interconnection (OSI) en versleutelt en verifieert Ethernet-frames om de communicatie tussen knooppunten te beveiligen. Oorspronkelijk ontworpen voor LAN's, is MACsec geëvolueerd om ook WAN-implementaties te ondersteunen. Het biedt lijn-tarief encryptie, die minimale latentie en overheadkosten verzekeren, die voor hoge-snelheidsnetwerken essentieel zijn.

IEEE 802.1X-2010 is een wijziging van de oorspronkelijke IEEE 802.1X-standaard, waarin poortgebaseerde netwerktoegangscontrole wordt gedefinieerd. De herziening van 2010 introduceert het protocol MACsec Key Agreement (MKA), dat essentieel is voor het beheer van coderingssleutels in MACsec-implementaties. MKA behandelt de distributie en het beheer van cryptografische sleutels die door MACsec worden gebruikt om gegevens te versleutelen en te ontsleutelen. MKA is een standaard die bijdraagt aan de interoperabiliteit van meerdere leveranciers voor MACsec-implementaties, die veilige sleuteluitwisselingen en rekeying-mechanismen ondersteunt, cruciaal voor het handhaven van continue beveiliging in dynamische WAN-omgevingen.

In WAN MACsec-implementaties biedt IEEE 802.1AE (MACsec) de fundamentele encryptie- en beveiligingsmechanismen op de datalink-laag, zodat alle Ethernet-frames worden beveiligd wanneer ze over het netwerk worden verzonden. IEEE 802.1X-2010 met het MKA protocol, behandelt de kritieke taak van het distribueren en beheren van de encryptie sleutels noodzakelijk voor MACsec om te functioneren. Samen zorgen deze standaarden ervoor dat WAN MACsec robuuste, snelle codering kan leveren via breedbandnetwerken, waardoor uitgebreide bescherming van gegevens tijdens het transport mogelijk wordt, terwijl de interoperabiliteit en het beheergemak worden behouden.

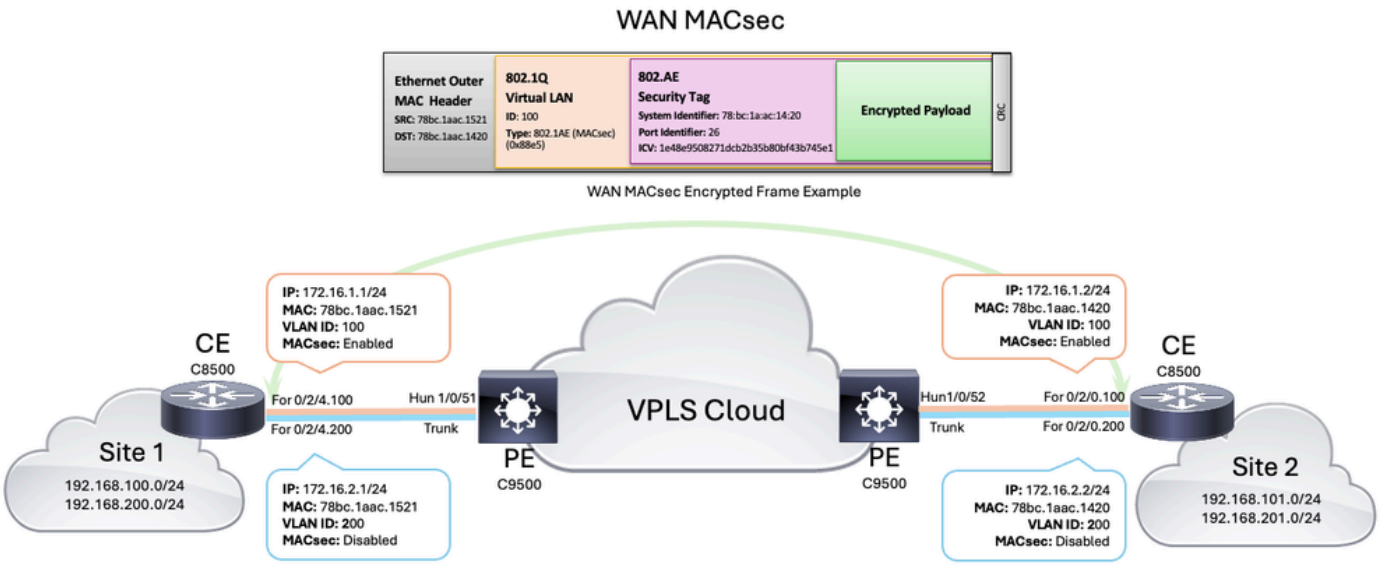
Om de unieke uitdagingen van WAN-omgevingen aan te pakken, zijn enkele verbeteringen aangebracht in de traditionele MACsec-implementaties:

- 802.1Q Tag in het Clear: Deze functie maakt het mogelijk om de 802.1Q VLAN-tag buiten de versleutelde MACsec-header te belichten, waardoor flexibelere netwerkontwerpen mogelijk worden, vooral in openbare Ethernet-transportomgevingen. Dit vermogen is essentieel voor het integreren van MACsec met Carrier Ethernet-services, omdat het de coëxistentie van versleuteld en niet-versleuteld verkeer op hetzelfde netwerk mogelijk maakt, waardoor de netwerkarchitectuur wordt vereenvoudigd en de kosten worden verminderd. De
- Aanpasbaarheid via Public Carrier Ethernet: moderne WAN MACsec-implementaties kunnen worden aangepast aan openbare Ethernet-services van carriers. Dit aanpassingsvermogen omvat het wijzigen van het EAPoL-doeladres (Ethernet Verification Protocol over LAN) en EtherType, waardoor MACsec naadloos kan functioneren via Carrier Ethernet-netwerken die deze frames anders kunnen gebruiken of blokkeren.

WAN MACsec vertegenwoordigt een aanzienlijke vooruitgang in Ethernet-codering, waardoor tegemoet wordt gekomen aan de groeiende behoefte aan snelle, beveiligde WAN-verbindingen. Zijn vermogen om lijn-rate encryptie, steun voor flexibele netwerkontwerpen, en aanpassingsvermogen aan openbare dragerdiensten te verstrekken maken het een kritieke component van moderne netwerkveiligheidsarchitecturen. Door gebruik te maken van WAN MACsec, kunnen organisaties robuuste beveiliging voor hun snelle WAN-links realiseren terwijl ze hun netwerkarchitecturen vereenvoudigen en de operationele complexiteit verminderen.

Configureren

Netwerkdiagram



WAN MACsec-topologie

Configuraties

Stap 1: Basis apparaatconfiguratie

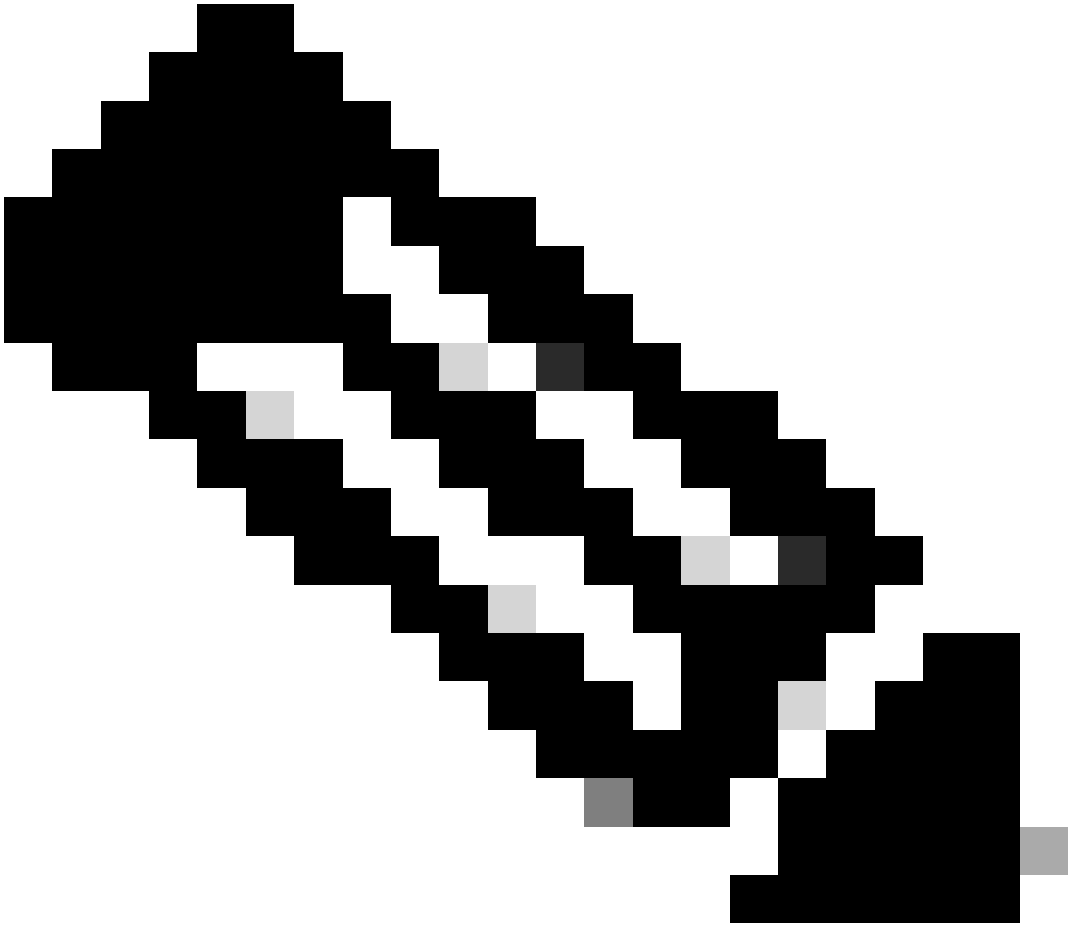
Om de configuratie te starten, moet u eerst de subinterfaces definiëren die gebruikt gaan worden voor de verkeerssegmentatie en de verbinding met de serviceprovider. Voor dit scenario worden twee subinterfaces gedefinieerd voor VLAN 100 gekoppeld aan subnetverbinding 172.16.1.0/24 en VLAN 200 gekoppeld aan subnetverbinding 172.16.2.0/24 (later wordt slechts één subinterface geconfigureerd met MACsec).

CE 8500-1 switch	CE 8500-2 router
<#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.**

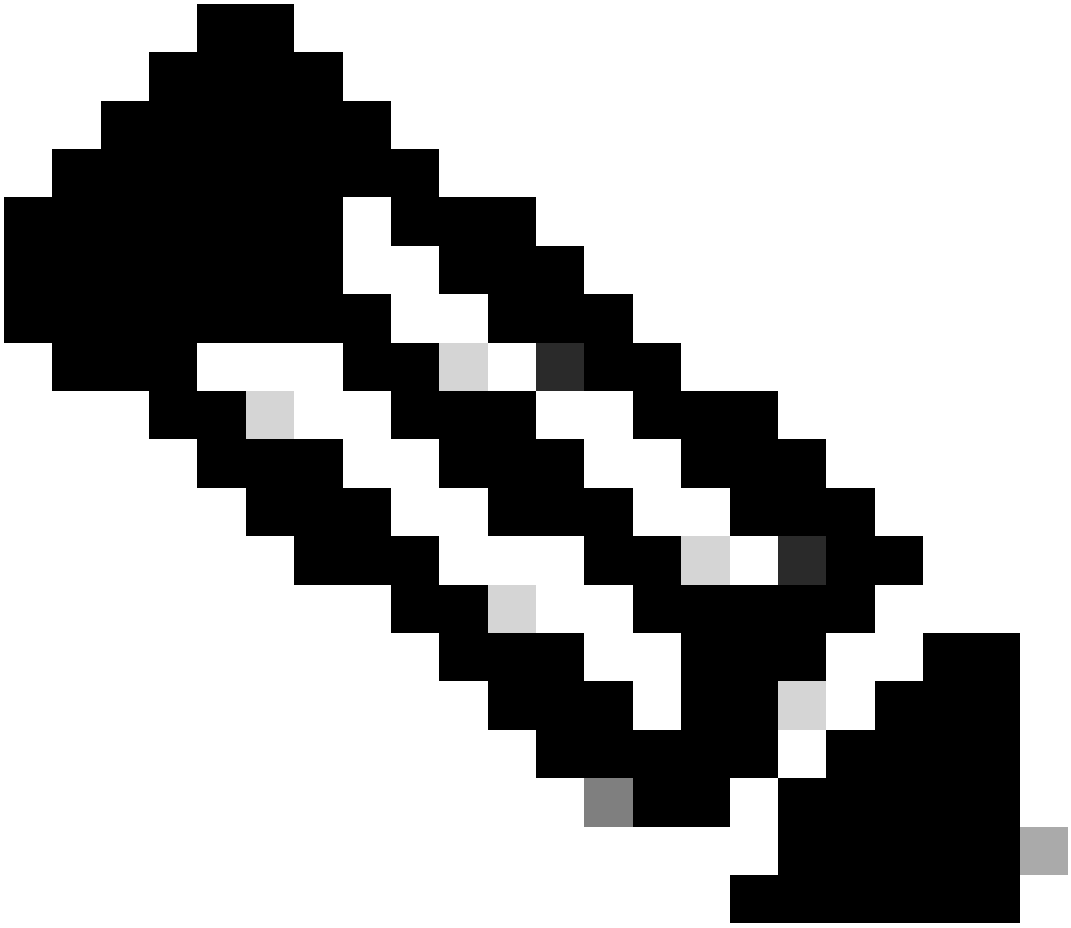
Stap 2: De sleutelketen van MACsec configureren

Vergeet niet dat de IEEE 802.1X-2010-standaard aangeeft dat de MACsec-coderingssleutels kunnen worden afgeleid van een Pre-Shared Key (PSK), door 802.1X Extensible Authentication Protocol (EAP) of gekozen en gedistribueerd door een MKA-sleutelserver. In dit voorbeeld worden PSK's handmatig ingesteld via de MACsec-sleutelketen, en deze zijn gelijk aan de Connectivity Association Key (CAK), die de primaire sleutel is die wordt gebruikt om alle andere coderingssleutels af te leiden die in MACsec worden gebruikt.

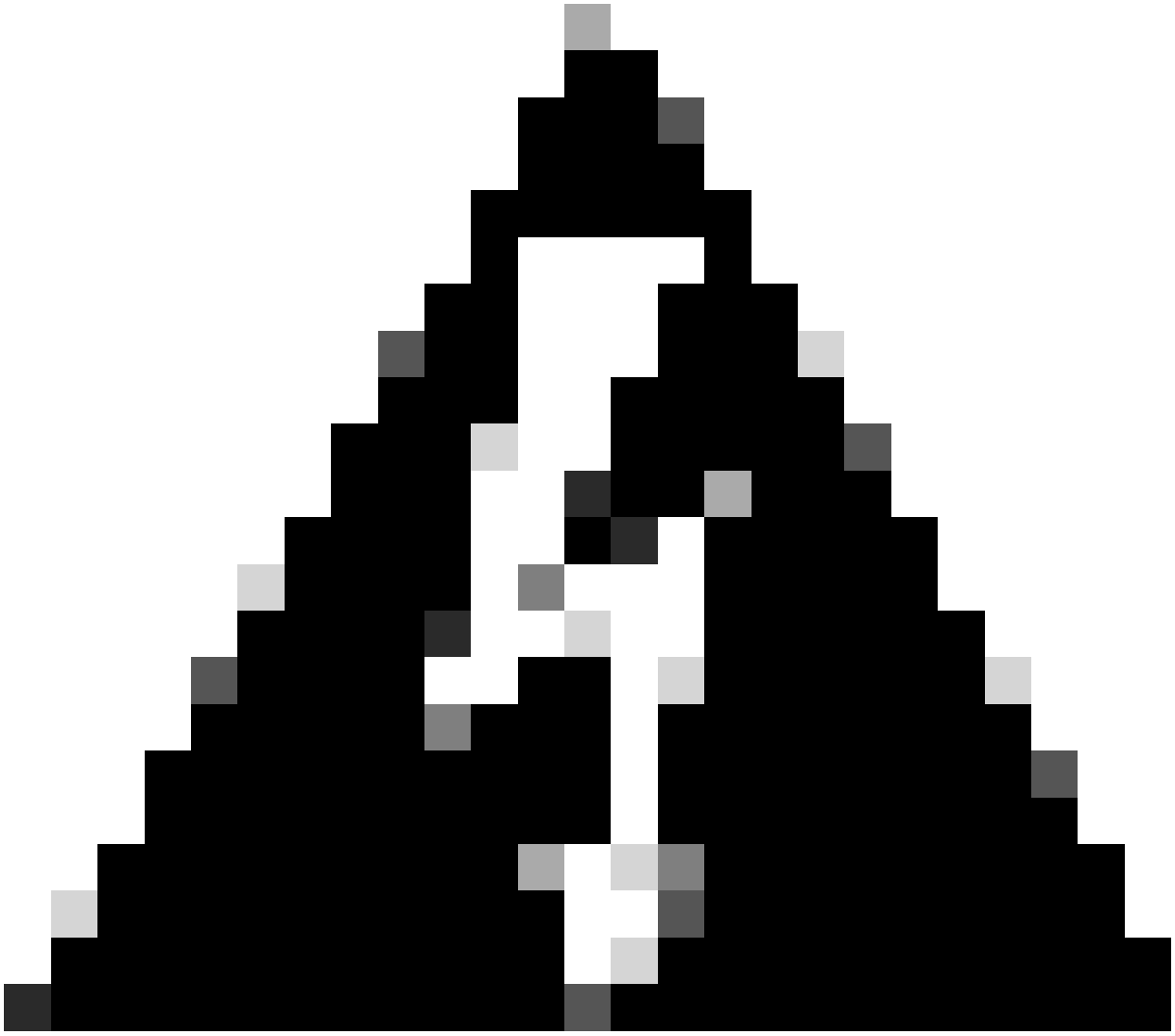
CE 8500-1 switch	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1** **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**



Opmerking: tijdens het configureren van de MACsec-sleutelketen, vergeet niet dat de sleutelstring alleen uit hexadecimale cijfers moet bestaan, de aes-128-cmac cryptografische algoritme vereist een sleutel van 32 hexadecimale cijfers en de aes-256-cmac cryptografische algoritme vereist een sleutel van 64 hexadecimale cijfers.



Opmerking: Onthoud dat bij het gebruik van meerdere sleutels een overlappende tijdsperiode tussen deze sleutels nodig is om een hitless key rollover te bereiken nadat de opgegeven key life is verlopen.



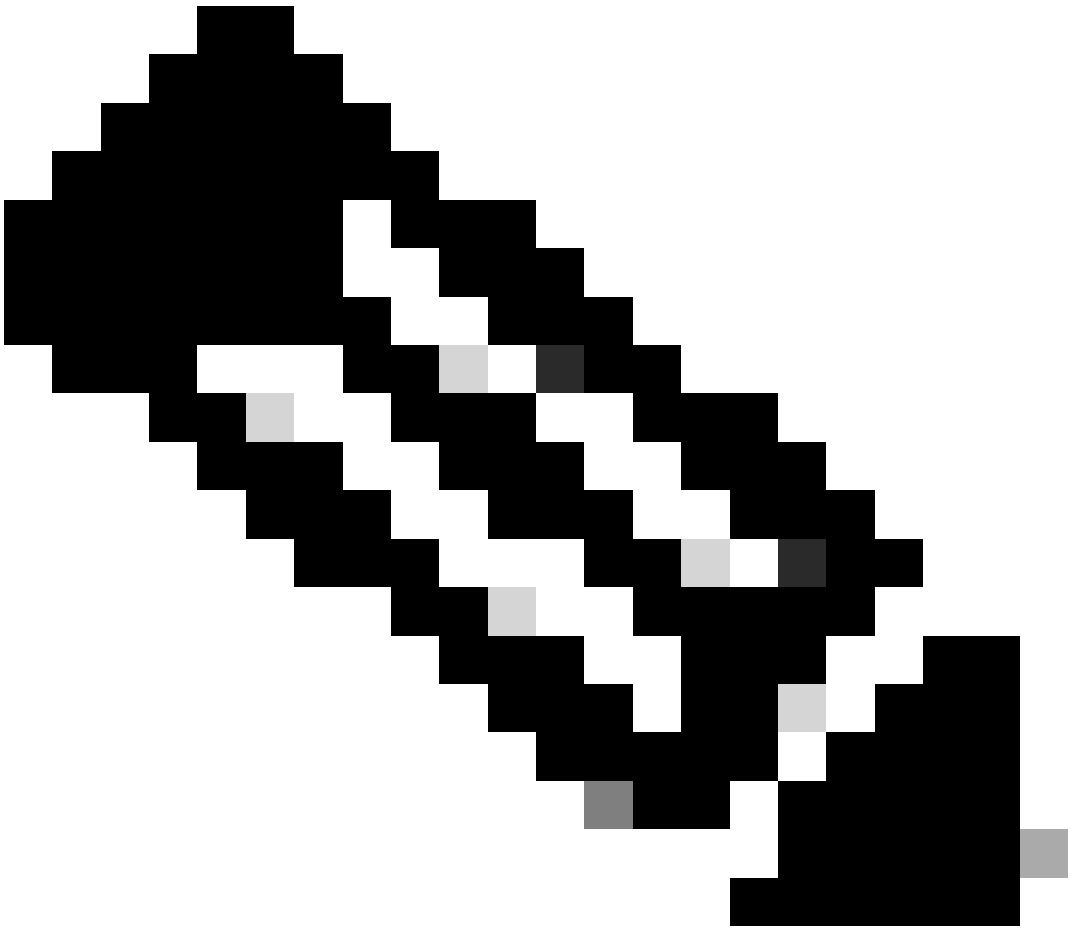
Waarschuwing: het is belangrijk om ervoor te zorgen dat de klokken van beide routers gesynchroniseerd zijn; daarom wordt het gebruik van Network Time Protocol (NTP) ten zeerste aanbevolen. Als dit niet het geval is, kan dit de oprichting van MKA-sessies verhinderen of ertoe leiden dat ze in de toekomst mislukken.

Stap 3: MKA-beleid configureren

Terwijl het standaard MKA-beleid nuttig kan zijn voor initiële installatie en eenvoudige netwerken, wordt het configureren van een aangepast MKA-beleid voor WAN MACsec over het algemeen aanbevolen om te voldoen aan specifieke eisen op het gebied van beveiliging, naleving en prestaties. Aangepaste beleidslijnen bieden meer flexibiliteit en controle, waardoor uw netwerkbeveiliging robuust is en op uw behoeften is afgestemd.

Bij het configureren van uw MKA-beleid zijn er verschillende elementen die kunnen worden geselecteerd, zoals: Key Server Priority, Delay Protection voor de MACsec Key Agreement Packet Data Unit (MKPDU), Cypher Suite, onder andere. In dit platform en softwareversies kunnen de volgende algoritmen worden gebruikt:

MACsec-algoritme	Beschrijving
GCM-aes-128 switch	Galois/Counter Mode (GCM) met Advanced Encryption Standard (AES) met behulp van een 128-bits sleutel
GCM-aes-256	Galois/Counter Mode (GCM) met AES met behulp van een 256-bits sleutel (hogere coderingssterkte)
GCM-aes-xpn-128 sensor	Galois/Counter Mode (GCM) met AES met behulp van een 128-bits sleutel en Extended Packet Numbering (XPN)
gcm-aes-xpn-256 inch	Galois/Counter Mode (GCM) met AES met behulp van een 256-bits sleutel, met XPN (hogere coderingssterkte)



Opmerking: XPN verbetert het GCM-AES-algoritme door een langere pakketnummering te ondersteunen, wat de beveiliging verbetert voor zeer langdurige sessies of omgevingen met hoge doorvoersnelheid. Het gebruik van snelle verbindingen, bijvoorbeeld 40 Gb/s of

100 Gb/s, kan zeer korte zeer belangrijke het omvergooitijden veroorzaken omdat het Aantal van het Pakket (PN) binnen het kader van MACsec, dat typisch op het aantal verzonden pakketten wordt gebaseerd, bij deze snelheden snel kon worden uitgeput. XPN breidt de pakketnummerreeks uit en elimineert de noodzaak voor een frequente Security Association Key (SAK) sleutel die kan voorkomen in koppelingen met hoge capaciteit.

In dit voorbeeld is het geselecteerde algoritme voor het MKA-beleid gcm-aes-xpn-256, en andere elementen gaan de standaardwaarde hebben:

CE 8500-1 switch	CE 8500-2 router
<#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**

Stap 4: Configureer MACsec op interface- en subinterfaceniveau

In dit scenario, alhoewel de fysieke interface niet met een IP adres wordt gevormd, moeten sommige macsec bevelen op dit niveau voor de oplossing worden toegepast om te werken. Het MACsec-beleid en de sleutelketen worden op subinterfaceniveau toegepast (zie het configuratievoorbeeld):

CE 8500-1 switch	CE 8500-2 router
<#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**

Opdrachten toegepast op fysiek interfaceniveau

a. MTU is ingesteld op 9216 omdat de serviceprovider die in de topologie wordt gebruikt jumboframes toestaat, maar dit is geen vereiste

b. Met de opdracht macsec dot1q-in-clear kan de optie de VLAN (dot1q)-tag in de clear (niet versleuteld) hebben

c. De opdracht macsec access-control should-secure maakt het mogelijk om niet-versleutelde pakketten van de fysieke interface of subinterface te verzenden of ontvangen (deze opdracht is nodig als sommige subinterfaces versleuteling vereisen en sommige andere niet, dit komt door het standaard MACsec gedrag waar het niet toestaat dat niet-versleutelde pakketten worden verzonden of ontvangen van dezelfde fysieke interface waar MACsec is ingeschakeld)

Opdrachten toegepast op subinterfaceniveau

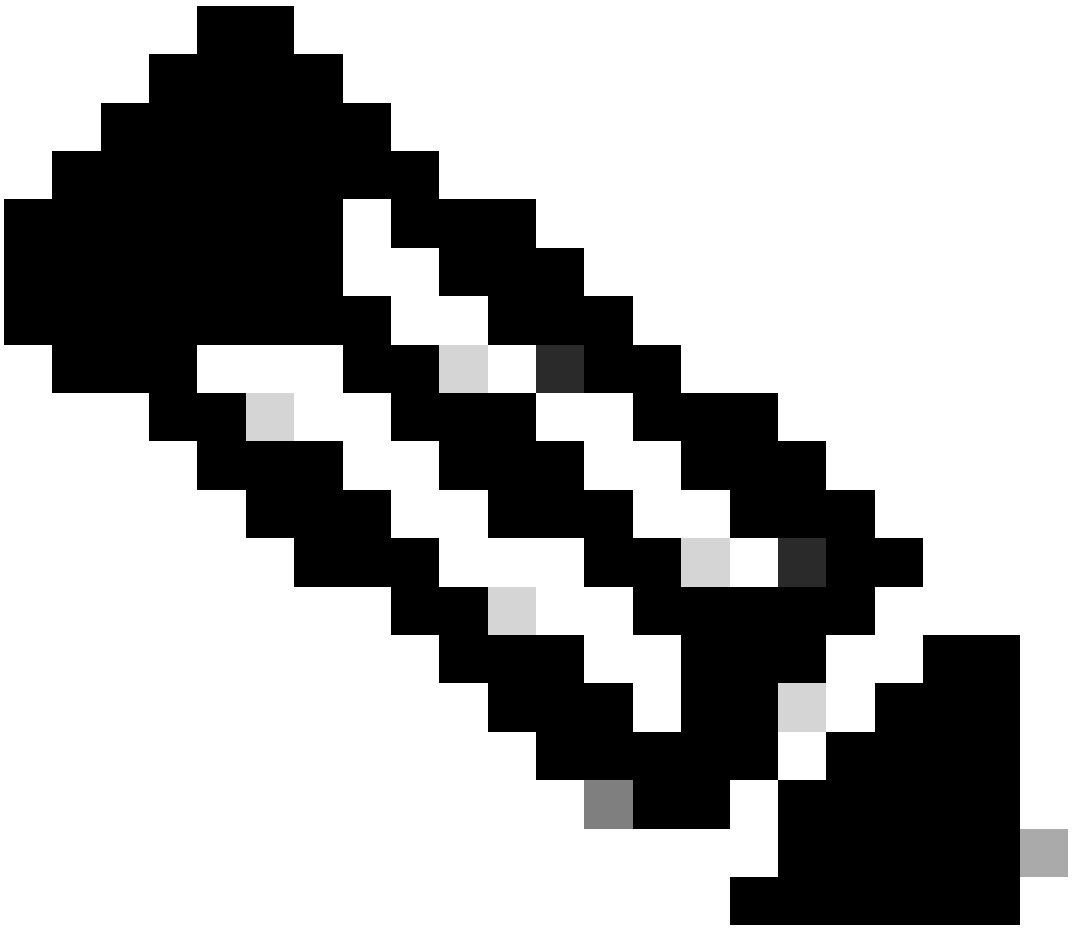
a. Nu, is het bevel eapol bestemming-adres uitzending-adres nodig om het bestemmingsMAC adres van de kaders EAPoL (dat door gebrek een multicast adres van MAC 01:80:C2:00:00:03 is) in een uitzendingMAC adres te veranderen om ervoor te zorgen dat de dienstverlener hen overstroomt en hen niet laat vallen of verbruikt.

b. De opdracht eapol eth-type 876F, wordt ook gebruikt om het standaard ethernettype van het EAPoL frame (dat standaard 0x888E is) te veranderen en het te veranderen in 0x876F. Dit is opnieuw nodig om te voorkomen dat de serviceprovider deze frames laat vallen of gebruikt.

c. De opdrachten mka policy **<**policy name**>** en mka pre-shared-key-key-chain **<**key chain name**>** worden gebruikt om het aangepaste beleid en de key chain op de subinterface toe te passen.

d. En last but not least, de macsec-opdracht maakt MACsec mogelijk op subinterfaceniveau.

In de huidige installatie, zonder de eerdere EAPoL-wijzigingen, werden de 9500 switches aan de kant van de serviceprovider de EAPoL-frames niet doorgestuurd.



Opmerking: MACsec-opdrachten zoals dot1q-in-clear en should-secure worden geërfd door de subinterfaces. Bovendien kunnen EAPoL-opdrachten worden ingesteld op het fysieke interfaceniveau, en in dergelijke gevallen worden deze opdrachten ook geërfd door de subinterfaces. De expliciete configuratie van EAPoL-opdrachten op de subinterface heeft echter voorrang op de geërfde waarde of het geërfde beleid voor die subinterface.

Verifiëren

Zodra de configuratie is toegepast, toont de volgende uitvoer de relevante actieve configuratie van elke Customer Edge (CE) C8500-router (bepaalde configuratie is weggelaten):

```
<#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
```

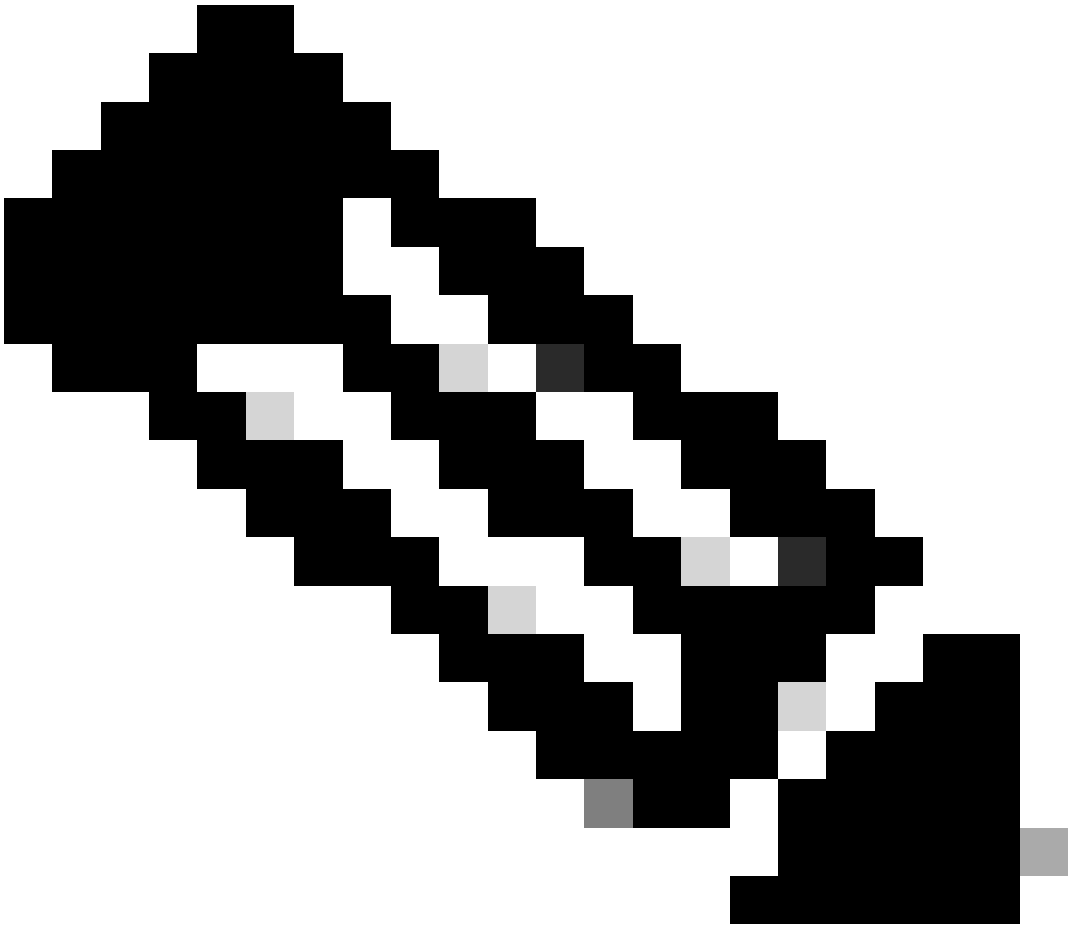
```
!
mka policy subint100 macsec-cipher-suite gcm-aes-xpn-256


!
!
!
!
!
!
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-ke
!
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#
```



Opmerking: Na het inschakelen van MACsec, door het toepassen van de macsec opdracht, wordt de MTU op die interface automatisch aangepast en verminderd met 32 bytes om rekening te houden met de MACsec overhead.

Vervolgens vindt u een lijst met essentiële opdrachten die kunnen worden gebruikt om de status van MACsec tussen peers te controleren en te verifiëren. Deze opdrachten bieden u gedetailleerde informatie over de huidige MACsec-sessies, sleutelhangers, beleidsregels en statistieken:

mka sessies tonen - Deze opdracht geeft de huidige MKA sessiestatus weer.

toon mka sessies detail - Deze opdracht geeft gedetailleerde informatie over elke MKA sessie.

show mka keychains -Dit commando toont de keychains die gebruikt worden voor MACsec en de toegewezen interface.

mkb-beleid tonen - Deze opdracht geeft het toegepaste beleid, de gebruikte interfaces en de coderingssuite weer.

toon mka samenvatting - Dit bevel verstrekt een samenvatting van de zittingen MKA en de statistieken.

toon macsec statistieken interface <interface name> - Deze opdracht toont de MACsec statistieken voor een gespecificeerde interface, en het helpt te identificeren als gecodeerd verkeer wordt verzonden en ontvangen.

CE 8500-1 switch

```
<#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
```

Bereikbaarheid van de verschillende subinterfaces is succesvol, evenals bereikbaarheid tussen de 192.168.0.0/16 subnetten. De volgende pingtests tonen de succesvolle connectiviteit aan:

```
<#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#
```

Na het opnemen van pakketten van een ICMP-test op het Provider Edge (PE)-apparaat, kunt u de versleutelde en niet-versleutelde frames vergelijken. Merk op dat de Ethernet-router MAC-header hetzelfde is op beide frames, waarbij de dot1q-tag zichtbaar is. Het versleutelde frame toont echter een EtherType van 0x88E5 (MACsec), terwijl het niet-versleutelde frame een EtherType van 0x0800 (IPv4) samen met de ICMP-protocolinformatie weergeeft:

Versleuteld frame VLAN 1000

```
<#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]
```

Gerelateerde informatie

- Verbeteringen in WAN MACSEC- en MKA-ondersteuning
- Innovaties in Ethernet-encryptie (802.1AE - MACsec) voor snelle WAN-implementaties (1-100 GE)
- Probleemoplossing voor WAN MACSEC op routers

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.