Configuración de WAN MACsec en Catalyst 8500 con subinterfaces

Contenido

Introducción

Este documento describe el proceso para configurar la seguridad de control de acceso a medios WAN (MACsec) en plataformas Cisco Catalyst 8500 con subinterfaces.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos de red avanzados, como WAN, VLAN y cifrado
- Información sobre MACsec (IEEE 802.1AE) y administración de claves (IEEE 802.1X-2010)
- Familiaridad con la interfaz de línea de comandos (CLI) Cisco IOS® XE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

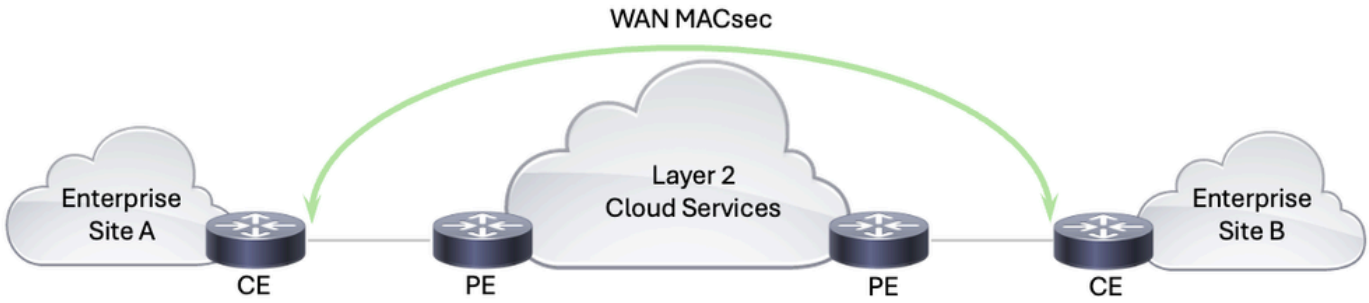
- Plataformas periféricas Cisco Catalyst serie 8500

- Cisco IOS XE versión 17.14.01a

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

WAN MACsec es una solución de seguridad diseñada para proteger el tráfico de red a través de las redes WAN mediante el uso de las funciones de MACsec. Al utilizar una red de proveedor de servicios para intercambiar datos, es importante cifrar los datos en tránsito para evitar la manipulación. WAN MACsec es fácil de implementar y gestionar, por lo que es ideal para organizaciones que necesitan proteger el tráfico de red de la manipulación de datos, como intercepciones y ataques de intrusos. Proporciona cifrado de velocidad de línea sin problemas, lo que garantiza que los datos permanezcan seguros y sin riesgos a medida que atraviesan diversas infraestructuras de red, incluidas redes de proveedores de servicios, entornos de nube y redes empresariales.



Solución WAN MACsec

Para compartir un poco de historial, MACsec, definido por el estándar IEEE 802.1AE, proporciona una comunicación segura en redes Ethernet al garantizar la confidencialidad de los datos, la integridad y la autenticidad del origen de las tramas Ethernet. MACsec, que funciona en la capa de enlace de datos (capa 2) del modelo de interconexión de sistemas abiertos (OSI), cifra y autentica las tramas Ethernet para proteger la comunicación entre nodos. Diseñado originalmente para LAN, MACsec ha evolucionado para admitir también implementaciones WAN. Ofrece cifrado de velocidad de línea, lo que garantiza una latencia y una sobrecarga mínimas, fundamentales para las redes de alta velocidad.

IEEE 802.1X-2010 es una enmienda al estándar IEEE 802.1X original, que define el control de acceso a la red basado en puertos. La revisión de 2010 introduce el protocolo MACsec Key Agreement (MKA), que es esencial para gestionar las claves de cifrado en las implementaciones de MACsec. MKA se encarga de la distribución y gestión de las claves criptográficas utilizadas por MACsec para cifrar y descifrar datos. MKA es un estándar que contribuye a la interoperabilidad entre varios proveedores para las implementaciones de MACsec, ya que admite intercambios de claves seguros y mecanismos de reintroducción de claves, lo que resulta esencial para mantener una seguridad continua en entornos WAN dinámicos.

En las implementaciones de WAN MACsec, IEEE 802.1AE (MACsec) proporciona los mecanismos de seguridad y cifrado fundamentales en la capa de enlace de datos, lo que garantiza que todas las tramas Ethernet estén protegidas a medida que atraviesan la red. IEEE 802.1X-2010 con el protocolo MKA, maneja la tarea crítica de distribuir y administrar las claves de cifrado necesarias para que MACsec funcione. Juntos, estos estándares garantizan que WAN MACsec pueda ofrecer un cifrado sólido y de alta velocidad en redes de área extensa, lo que proporciona una protección completa de los datos en tránsito a la vez que se mantiene la interoperabilidad y la facilidad de gestión.

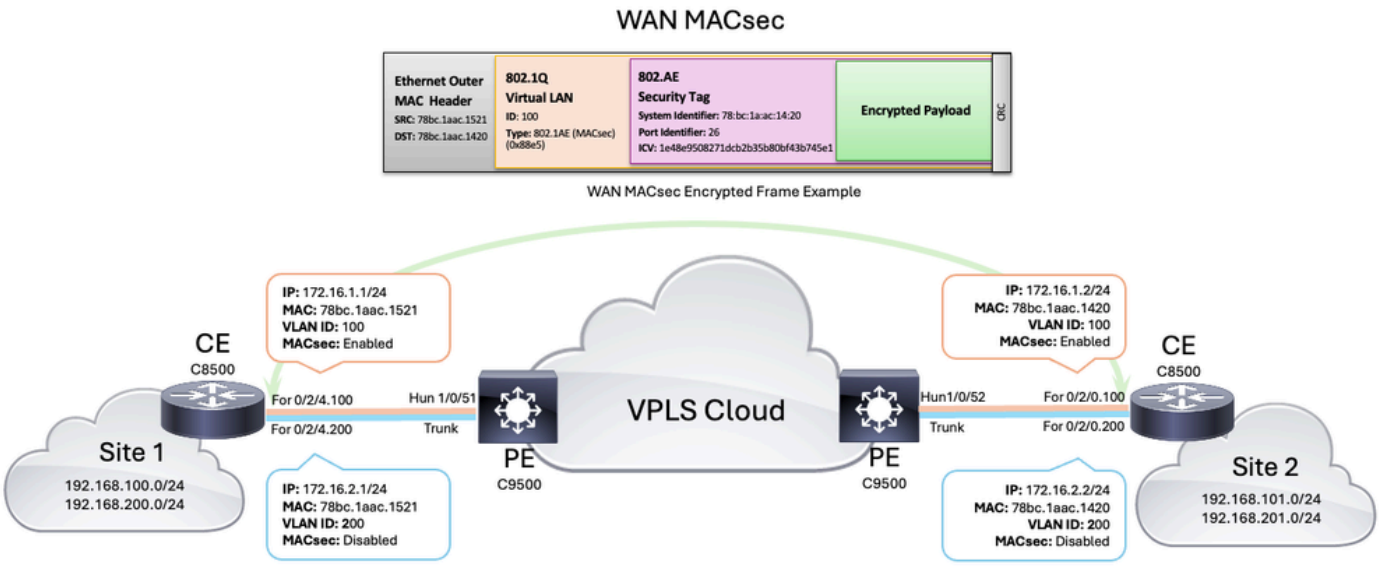
Para hacer frente a los retos específicos de los entornos WAN, se realizaron algunas mejoras en las implementaciones MACsec tradicionales:

- Etiqueta 802.1Q en el enlace Clear (Borrar): esta función permite que la etiqueta 802.1Q VLAN se exponga fuera del encabezado MACsec cifrado, lo que facilita diseños de red más flexibles, especialmente en entornos de transporte Ethernet público. Esta capacidad es esencial para integrar MACsec con los servicios Carrier Ethernet, ya que permite la coexistencia de tráfico cifrado y no cifrado en la misma red, lo que simplifica la arquitectura de red y reduce los costes.
- Adaptabilidad a través de Ethernet de operador público: las implementaciones MACsec de WAN modernas pueden adaptarse a los servicios Ethernet de operador público. Esta capacidad de adaptación incluye la modificación de la dirección de destino y el EtherType del protocolo de autenticación Ethernet sobre LAN (EAPoL), lo que permite que MACsec funcione sin problemas en redes Carrier Ethernet que, de lo contrario, pueden consumir o bloquear estas tramas.

WAN MACsec representa un avance significativo en el cifrado Ethernet, ya que satisface la creciente necesidad de conexiones WAN seguras de alta velocidad. Su capacidad para proporcionar cifrado de velocidad de línea, compatibilidad con diseños de red flexibles y adaptabilidad a servicios de operadores públicos lo convierten en un componente fundamental de las arquitecturas de seguridad de red modernas. Gracias a WAN MACsec, las organizaciones pueden lograr una seguridad sólida para sus enlaces WAN de alta velocidad a la vez que simplifican sus arquitecturas de red y reducen la complejidad operativa.

Configurar

Diagrama de la red



Topología MACsec de WAN

Configuraciones

Paso 1: Configuración básica del dispositivo

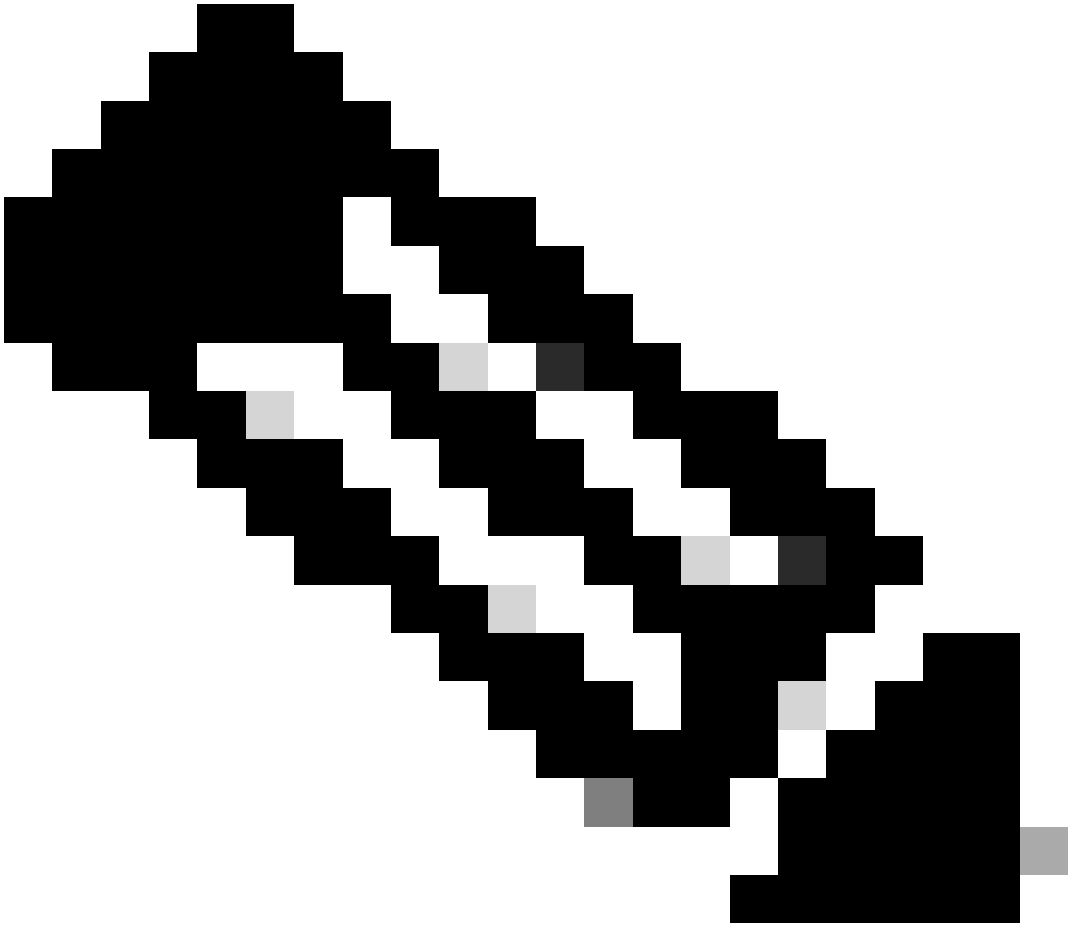
Para iniciar la configuración, primero debe definir las subinterfaces que se utilizarán para la segmentación del tráfico y la conexión con el proveedor de servicios. Para este escenario, se definen dos subinterfaces para la VLAN 100 asociada a la subred 172.16.1.0/24 y la VLAN 200 asociada a la subred 172.16.2.0/24 (más adelante, sólo se configurará una subinterfaz con MACsec).

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.**

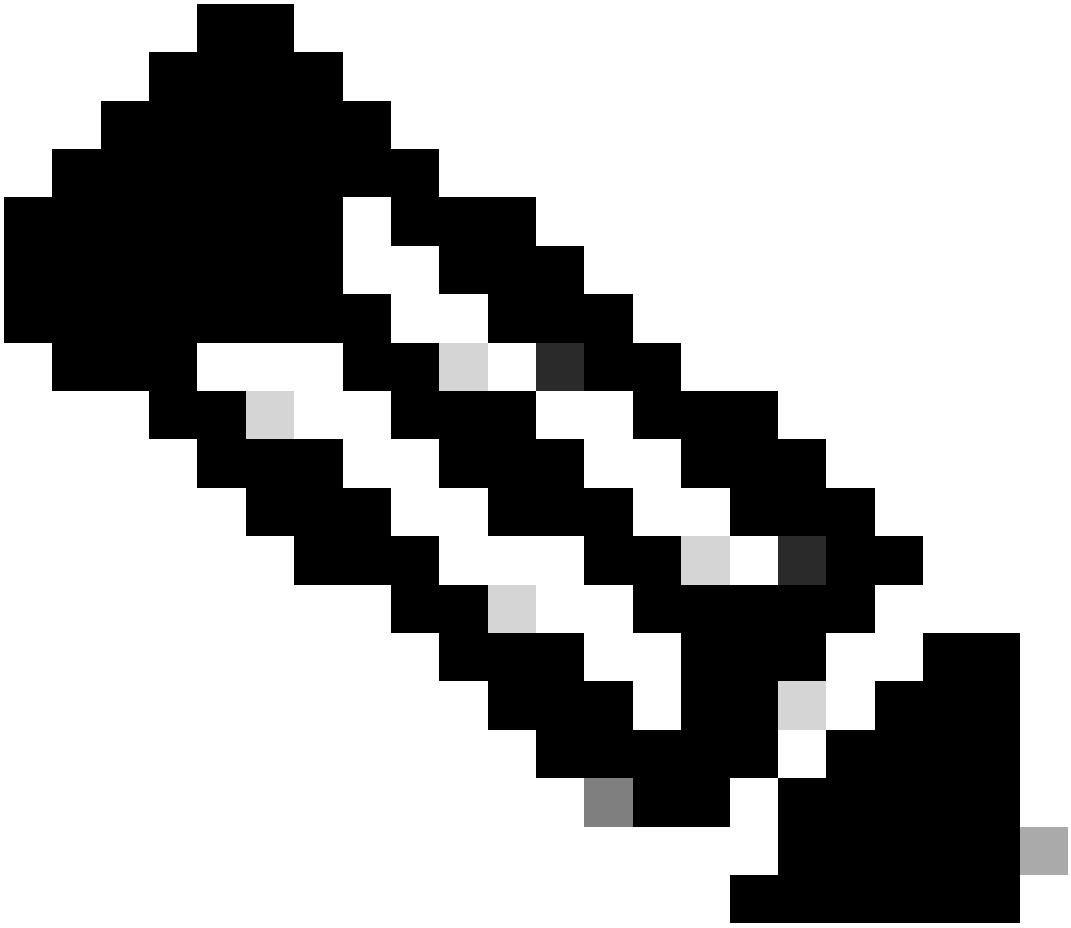
Paso 2: Configuración de MACsec Key Chain

Recuerde que el estándar IEEE 802.1X-2010 especifica que las claves de cifrado MACsec se pueden derivar de una clave precompartida (PSK), mediante el protocolo de autenticación ampliable (EAP) 802.1X o se pueden elegir y distribuir mediante un servidor de claves MKA. En este ejemplo, las PSK se utilizan y se configuran manualmente a través de la cadena de claves MACsec, que es igual a la clave de asociación de conectividad (CAK), que es la clave principal utilizada para derivar todas las demás claves de cifrado utilizadas en MACsec.

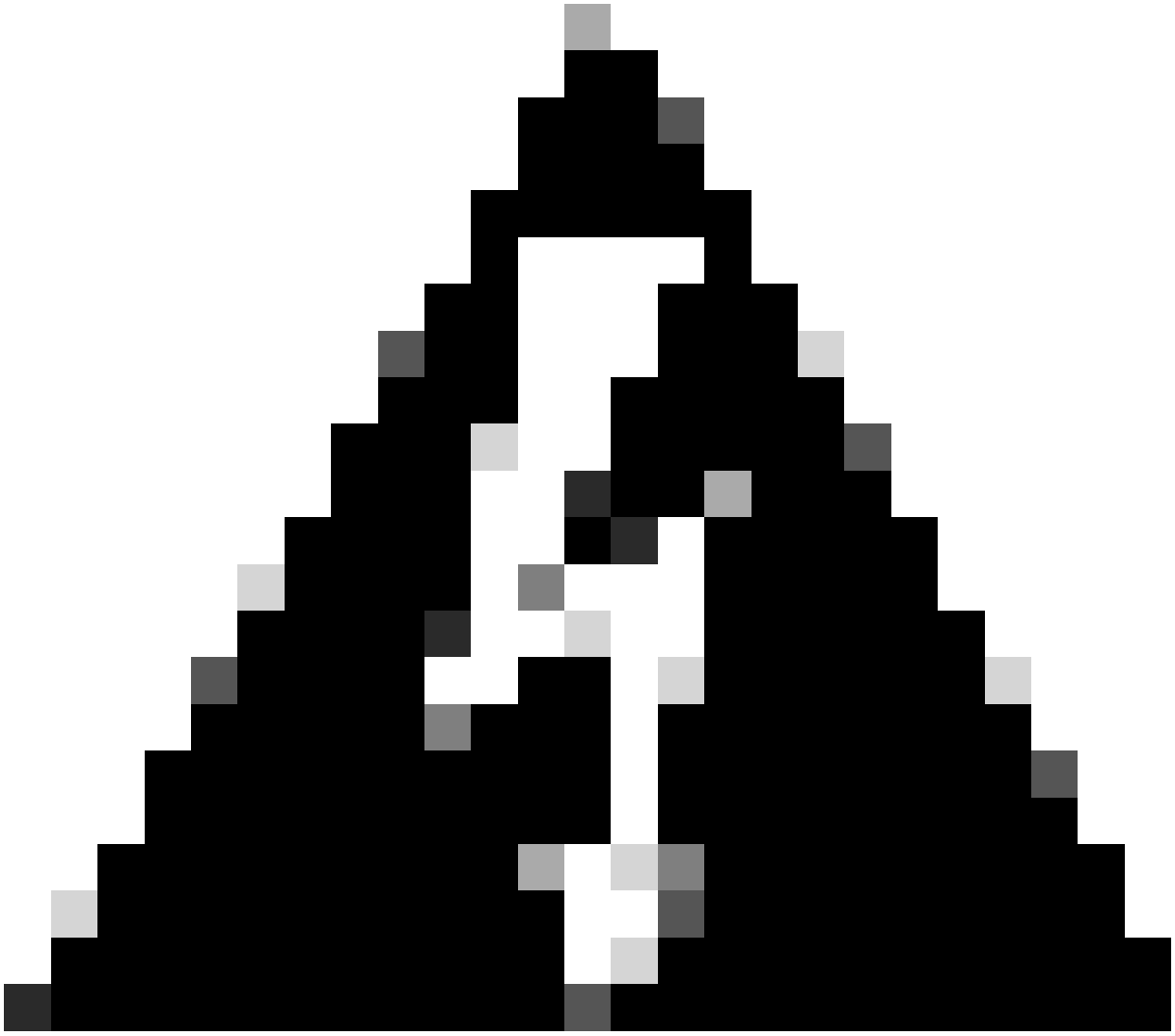
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1**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



Nota: Al configurar la cadena de claves MACsec, recuerde que la cadena de claves debe constar únicamente de dígitos hexadecimales, el algoritmo criptográfico aes-128-cmac requiere una clave de 32 dígitos hexadecimales y el algoritmo criptográfico aes-256-cmac requiere una clave de 64 dígitos hexadecimales.



Nota: recuerde que, al utilizar varias claves, se necesita un período de tiempo solapado entre ellas para lograr una sustitución de claves sin impacto una vez que ha caducado la duración de clave especificada.



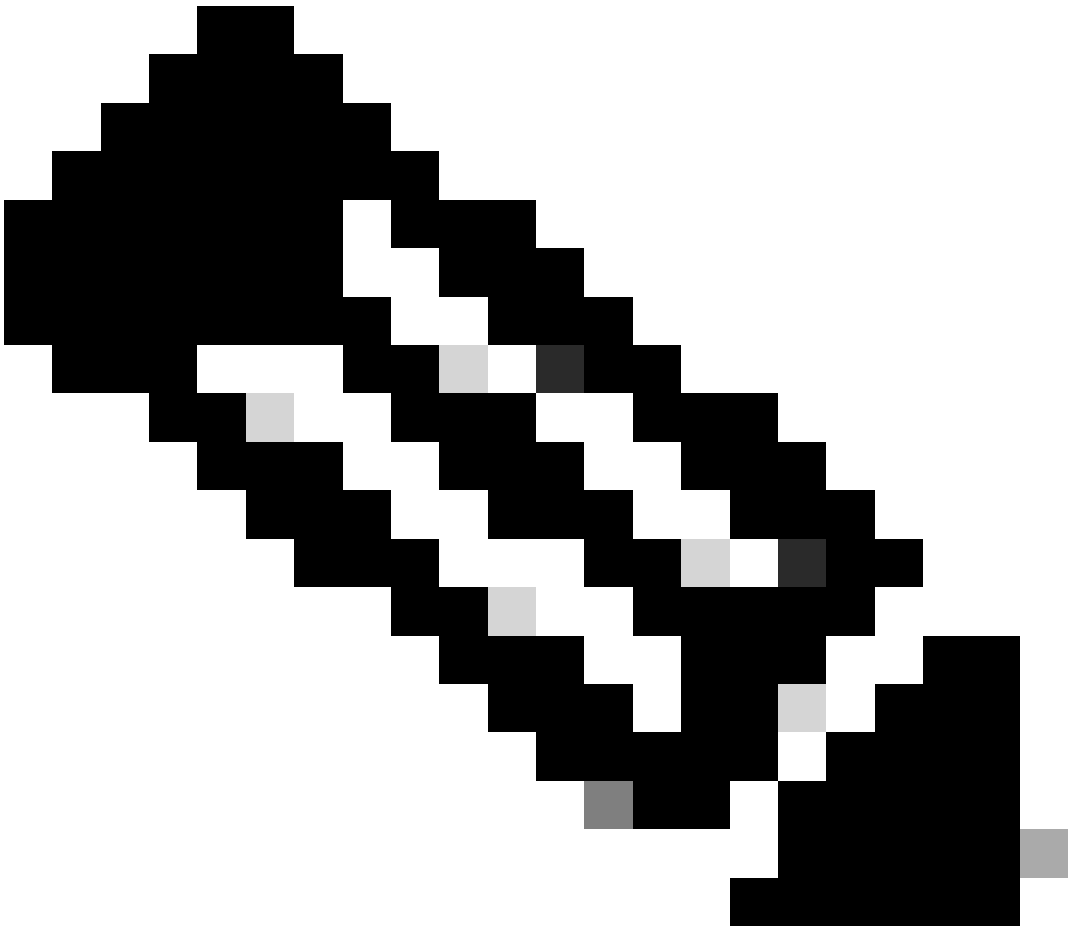
Advertencia: es importante asegurarse de que los relojes de ambos routers estén sincronizados; por lo tanto, se recomienda encarecidamente el uso del protocolo de tiempo de la red (NTP). Si no lo hace, puede impedir el establecimiento de sesiones MKA o hacer que fallen en el futuro.

Paso 3: Configurar la política MKA

Aunque la política MKA predeterminada puede ser útil para la configuración inicial y las redes sencillas, generalmente se recomienda configurar una política MKA personalizada para WAN MACsec para cumplir con los requisitos específicos de seguridad, cumplimiento y rendimiento. Las políticas personalizadas ofrecen mayor flexibilidad y control, lo que garantiza que la seguridad de la red sea sólida y esté personalizada según sus necesidades.

Al configurar su política MKA, se pueden seleccionar diferentes elementos, como la prioridad del servidor de claves, la protección contra retrasos para la unidad de datos de paquetes de acuerdo de claves MACsec (MKPDU), el conjunto Cipher, entre otros. En esta plataforma y versiones de software se pueden utilizar los siguientes cifrados:

Cifrado MACsec	Descripción
gcm-aes-128	Modo Galois/Counter (GCM) con estándar de cifrado avanzado (AES) que utiliza una clave de 128 bits
gcm-aes-256	Modo Galois/Counter (GCM) con AES mediante una clave de 256 bits (mayor seguridad de encriptación)
gcm-aes-xpn-128	Modo galois/contador (GCM) con AES mediante una clave de 128 bits, con numeración ampliada de paquetes (XPN)
gcm-aes-xpn-256	Modo galois/contador (GCM) con AES que utiliza una clave de 256 bits, con XPN (mayor potencia de encriptación)



Nota: XPN mejora el cifrado GCM-AES al admitir una numeración de paquetes más larga, lo que mejora la seguridad para sesiones de larga duración o entornos de alto rendimiento. El uso de links de alta velocidad, por ejemplo 40 Gb/s o 100 Gb/s, puede

causar tiempos de transferencia de claves muy cortos porque el número de paquete (PN) dentro de la trama MACsec, que normalmente se basa en el número de paquetes enviados, podría agotarse rápidamente a estas velocidades. XPN amplía la secuencia de numeración de paquetes y elimina la necesidad de volver a generar claves de clave de asociación de seguridad (SAK) frecuentes que pueden producirse en los enlaces de alta capacidad.

En este ejemplo, el cifrado seleccionado para la política MKA es gcm-aes-xpn-256, y otros elementos tendrán el valor predeterminado:

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**

Paso 4: Configuración de MACsec en el nivel de interfaz y subinterfaz

En este escenario, aunque la interfaz física no se esté configurando con una dirección IP, algunos comandos macsec deben aplicarse en este nivel para que la solución funcione. La política MACsec y la cadena de claves se aplican en el nivel de subinterfaz (consulte el ejemplo de configuración):

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

mtu 9216	**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**

Comandos Aplicados a Nivel de Interfaz Física

a. MTU se establece en 9216, ya que el proveedor de servicios utilizado en la topología permite tramas jumbo, pero esto no es un requisito

b. El comando macsec dot1q-in-clear habilita la opción de tener la etiqueta VLAN (dot1q) en clear (no encriptada)

c. El comando macsec access-control should-secure permite que se envíen o reciban paquetes sin cifrar de la interfaz física o subinterfaz (este comando es necesario si algunas subinterfaces requieren cifrado y otras no, esto se debe al comportamiento MACsec predeterminado, donde no permite que ningún paquete sin cifrar se transmita o reciba de la misma interfaz física donde

MACsec está habilitado)

Comandos Aplicados a Nivel de Subinterfaz

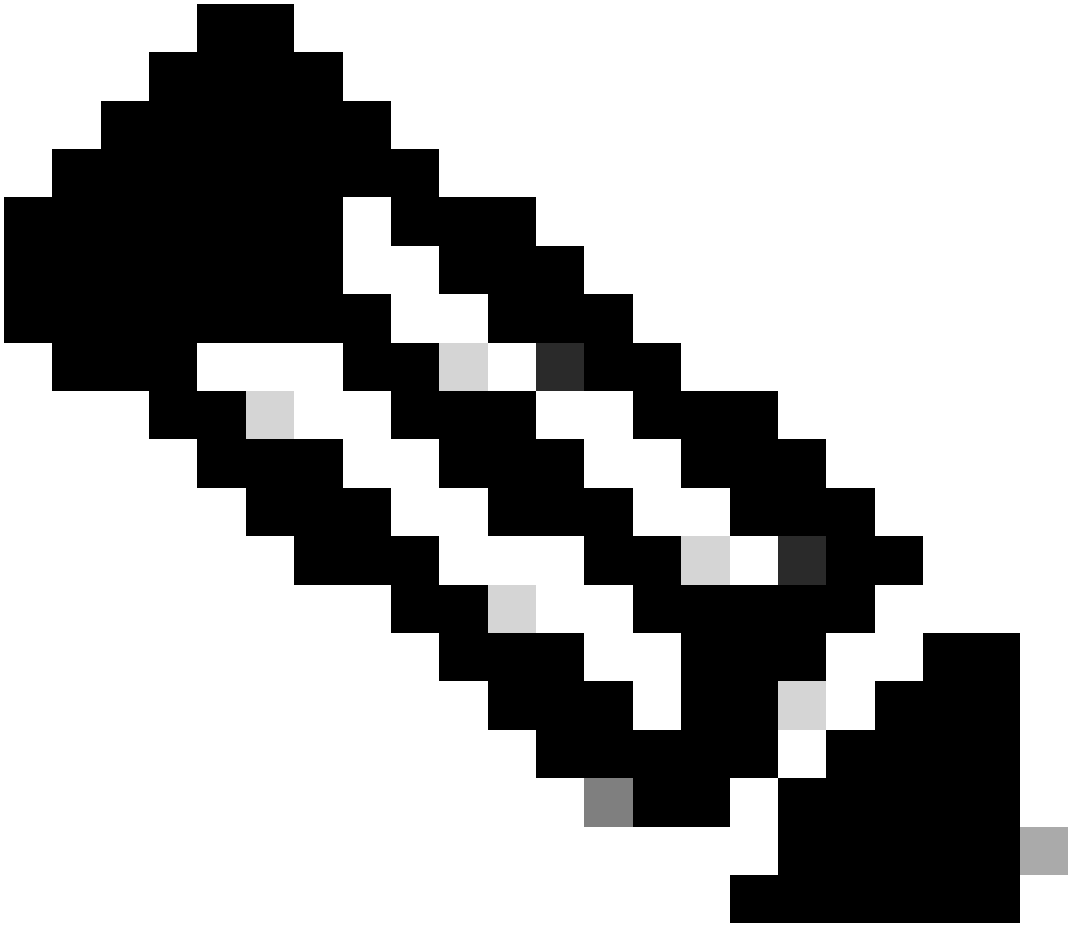
a. Ahora, el comando eapol destination-address broadcast-address es necesario para cambiar la dirección MAC de destino de las tramas EAPoL (que de forma predeterminada es una dirección MAC multicast 01:80:C2:00:00:03) a una dirección MAC de broadcast para asegurarse de que el proveedor de servicios las inunda y no las descarte o consuma.

b. El comando eapol eth-type 876F, también se utiliza para cambiar el tipo de Ethernet predeterminado de la trama EAPoL (que de forma predeterminada es 0x888E) y cambiarlo a 0x876F. De nuevo, esto es necesario para evitar que el proveedor de servicios descarte o consuma estas tramas.

c. Los comandos mka policy <policy name> y mka pre-shared-key-chain <key chain name> se utilizan para aplicar la política personalizada y la cadena de claves a la subinterfaz.

d. Y por último, pero no menos importante, el comando macsec habilita MACsec en el nivel de subinterfaz.

En la configuración actual, sin los cambios de EAPoL anteriores, los switches 9500 del lado del proveedor de servicios no remitían las tramas de EAPoL.



Nota: Los comandos MACsec como dot1q-in-clear y should-secure son heredados por las subinterfaces. Además, los comandos EAPoL se pueden establecer en el nivel de la interfaz física y, en tales casos, estas subinterfaces también heredan estos comandos. Sin embargo, la configuración explícita de los comandos EAPoL en la subinterfaz invalida el valor o la política heredados para esa subinterfaz.

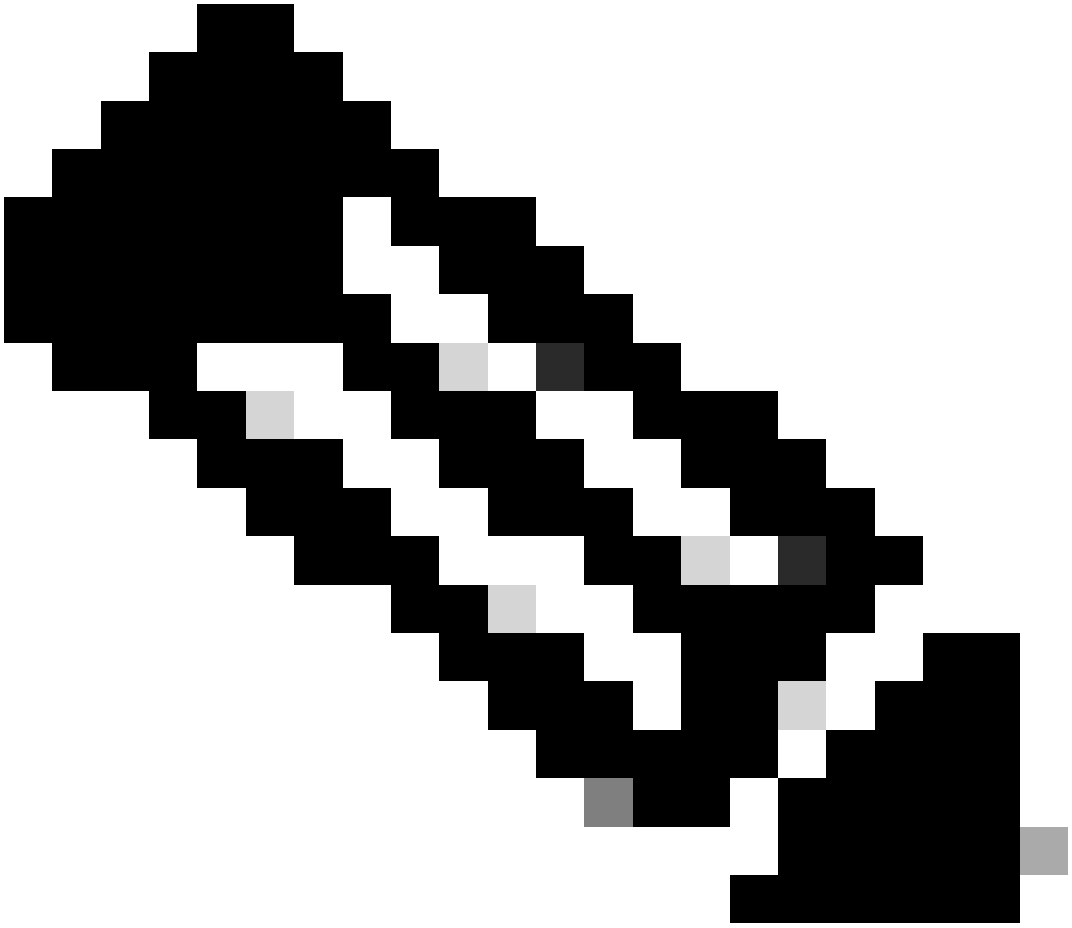
Verificación

Una vez aplicada la configuración, el siguiente resultado muestra la configuración en ejecución relevante de cada router C8500 de Customer Edge (CE) (se omitió parte de la configuración):

```
<#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#
```



Nota: Observe que después de habilitar MACsec, al aplicar el comando macsec, la MTU en esa interfaz se ajusta automáticamente y se reduce en 32 bytes para dar cuenta de la sobrecarga de MACsec.

A continuación, puede encontrar una lista de comandos esenciales que se pueden utilizar para verificar y verificar el estado de MACsec entre peers. Estos comandos le proporcionan información detallada sobre las sesiones MACsec actuales, keychains, políticas y estadísticas:

show mka sessions - Este comando muestra el estado actual de las sesiones MKA.

show mka sessions detail - Este comando proporciona información detallada sobre cada sesión MKA.

show mka keychains -Este comando muestra los keychains utilizados para MACsec y la interfaz asignada.

show mka policy - Este comando muestra las políticas aplicadas, las interfaces y el conjunto de cifrado utilizado.

show mka summary - Este comando proporciona un resumen de las sesiones MKA y las estadísticas.

show macsec statistics interface <nombre de interfaz> - Este comando muestra las estadísticas MACsec para una interfaz especificada y ayuda a identificar si se está enviando y recibiendo tráfico cifrado.

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
```

La disponibilidad desde las diferentes subinterfaces es exitosa, así como la disponibilidad entre las subredes 192.168.0.0/16. Las siguientes pruebas de ping demuestran la conectividad exitosa:

<#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#
```

Después de capturar paquetes de una prueba de ICMP en el dispositivo Provider Edge (PE), puede comparar las tramas cifradas y no cifradas. Observe que el encabezado MAC del router Ethernet es el mismo en ambas tramas, con la etiqueta dot1q visible. Sin embargo, la trama cifrada muestra un EtherType de 0x88E5 (MACsec), mientras que la trama no cifrada muestra un EtherType de 0x0800 (IPv4) junto con la información del protocolo ICMP:

Frame VLAN 100 cifrado
<#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]
```

Información Relacionada

- Mejoras en la compatibilidad de WAN MACSEC y MKA
- Innovaciones en el cifrado Ethernet (802.1AE - MACsec) para garantizar la seguridad de las implementaciones de WAN de alta velocidad (1-100 GE)
- Solucionar problemas de WAN MACSEC en routers

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).