Configurar WAN MACsec no Catalyst 8500 com subinterfaces

Contents

Introdução

Este documento descreve o processo para configurar o Media Access Control Security (MACsec) de WAN em plataformas Cisco Catalyst 8500 com subinterfaces.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos de rede avançados, incluindo WAN, VLANs e criptografia
- Compreensão de MACsec (IEEE 802.1AE) e gerenciamento de chaves (IEEE 802.1X-2010)
- Familiaridade com a Interface de Linha de Comando (CLI - Command Line Interface) do Cisco IOS® XE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

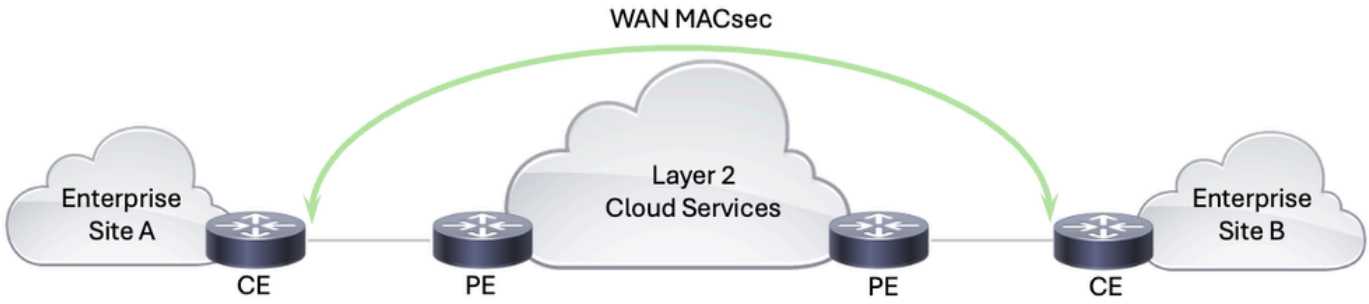
- Plataformas de borda Cisco Catalyst 8500 Series

- Cisco IOS XE versão 17.14.01a

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O WAN MACsec é uma solução de segurança projetada para proteger o tráfego de rede em redes WAN utilizando os recursos do MACsec. Ao usar uma rede de provedores de serviços para trocar dados, é importante criptografar os dados em trânsito para evitar adulteração. O WAN MACsec é fácil de implantar e gerenciar, tornando-o ideal para empresas que precisam proteger seu tráfego de rede contra a manipulação de dados, como espionagem e ataques man-in-the-middle. Ele fornece criptografia de taxa de linha contínua, garantindo que os dados permaneçam seguros e sem comprometimento enquanto atravessam várias infraestruturas de rede, incluindo redes de provedores de serviços, ambientes de nuvem e redes corporativas.



Solução WAN MACsec

Para compartilhar um pouco do histórico, o MACsec, definido pelo padrão IEEE 802.1AE, fornece comunicação segura em redes Ethernet, garantindo confidencialidade de dados, integridade e autenticidade de origem para quadros Ethernet. Operando na camada de enlace (camada 2) do modelo Open Systems Interconnection (OSI), o MACsec criptografa e autentica quadros Ethernet para proteger a comunicação entre nós. Projetado originalmente para LANs, o MACsec evoluiu para suportar também implantações de WAN. Ele oferece criptografia de taxa de linha, garantindo latência e sobrecarga mínimas, que são cruciais para redes de alta velocidade.

O IEEE 802.1X-2010 é uma emenda ao padrão original do IEEE 802.1X, que define o Controle de Acesso à Rede Baseado em Porta. A revisão de 2010 introduz o protocolo MACsec Key Agreement (MKA), que é essencial para o gerenciamento de chaves de criptografia em implementações MACsec. O MKA lida com a distribuição e o gerenciamento de chaves criptográficas usadas pelo MACsec para criptografar e descriptografar dados. O MKA é um padrão que contribui para a interoperabilidade de vários fornecedores para implantações MACsec, suportando trocas de chave seguras e mecanismos de rechaveamento, essenciais para manter a segurança contínua em ambientes de WAN dinâmicos.

Em implantações WAN MACsec, o IEEE 802.1AE (MACsec) fornece os mecanismos fundamentais de criptografia e segurança na camada de enlace, garantindo que todos os quadros

Ethernet sejam protegidos enquanto atravessam a rede. O IEEE 802.1X-2010 com o protocolo MKA lida com a tarefa crítica de distribuir e gerenciar as chaves de criptografia necessárias para que o MACsec funcione. Juntos, esses padrões garantem que o WAN MACsec possa fornecer criptografia robusta de alta velocidade em redes de longa distância, fornecendo proteção abrangente para dados em trânsito, mantendo a interoperabilidade e a facilidade de gerenciamento.

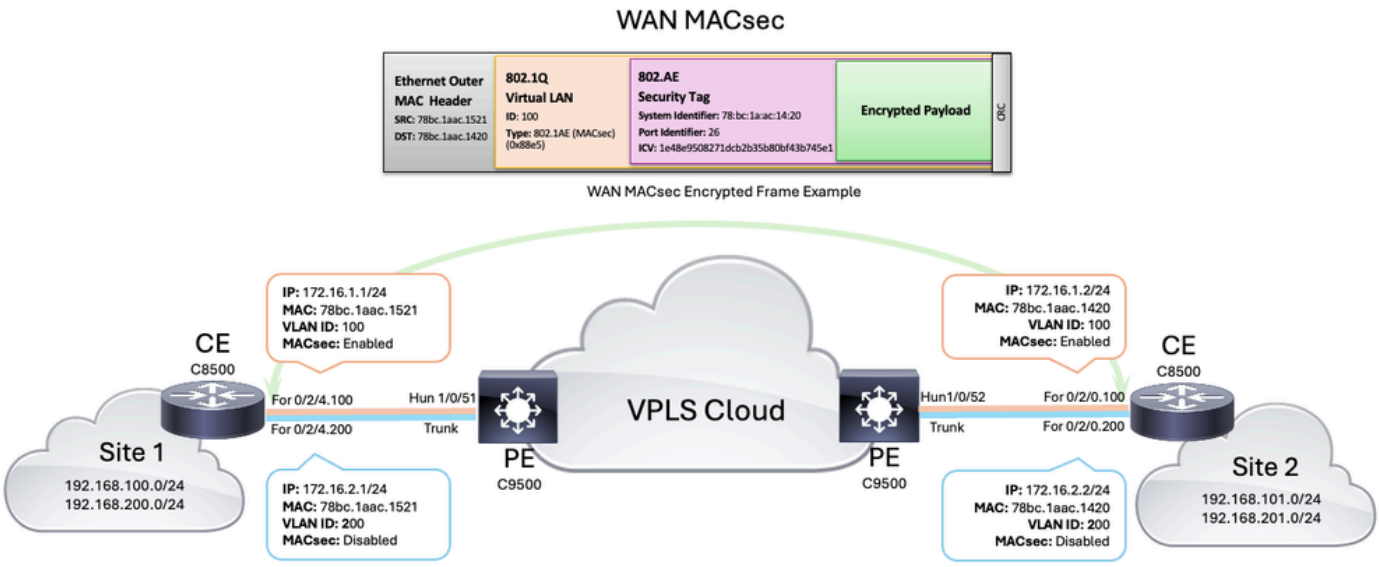
Para lidar com os desafios exclusivos dos ambientes de WAN, foram feitos alguns aprimoramentos nas implantações tradicionais de MACsec:

- Tag 802.1Q no Clear: Este recurso permite que a tag VLAN 802.1Q seja exposta fora do cabeçalho MACsec criptografado, facilitando projetos de rede mais flexíveis, especialmente em ambientes de transporte Ethernet públicos. Esse recurso é essencial para a integração do MACsec com os serviços Carrier Ethernet, pois permite a coexistência de tráfego criptografado e não criptografado na mesma rede, simplificando a arquitetura de rede e reduzindo custos.
- Adaptabilidade sobre Public Carrier Ethernet: as implementações modernas de WAN MACsec podem se adaptar aos serviços de Ethernet de operadora pública. Essa adaptabilidade inclui a modificação do endereço de destino do EAPoL (Ethernet Authentication Protocol over LAN) e do EtherType, permitindo que o MACsec funcione perfeitamente em redes Carrier Ethernet que, de outra forma, poderiam consumir ou bloquear esses quadros.

O WAN MACsec representa um avanço significativo na criptografia Ethernet, atendendo à necessidade crescente de conexões WAN seguras e de alta velocidade. Sua capacidade de fornecer criptografia de taxa de linha, suporte para projetos de rede flexíveis e adaptabilidade a serviços de operadora pública fazem dele um componente crítico das arquiteturas de segurança de rede modernas. Aproveitando o WAN MACsec, as organizações podem obter uma segurança robusta para seus links de WAN de alta velocidade, ao mesmo tempo em que simplificam suas arquiteturas de rede e reduzem a complexidade operacional.

Configurar

Diagrama de Rede



Topologia WAN MACsec

Configurações

Etapa 1: Configuração básica do dispositivo

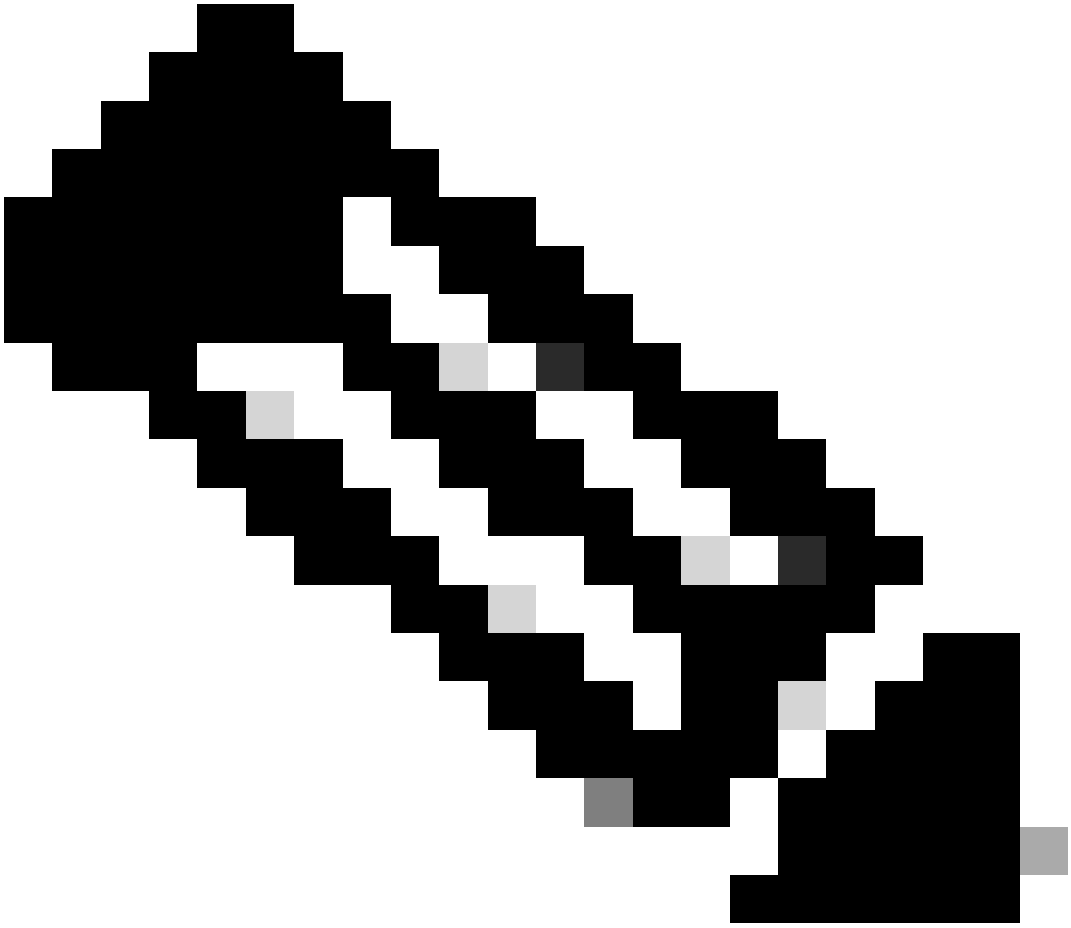
Para iniciar a configuração, você primeiro precisa definir as subinterfaces que serão usadas para a segmentação de tráfego e a conexão com o provedor de serviços. Para esse cenário, duas subinterfaces são definidas para a VLAN 100 associada à sub-rede 172.16.1.0/24 e a VLAN 200 associada à sub-rede 172.16.2.0/24 (posteriormente, apenas uma subinterface será configurada com 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.**

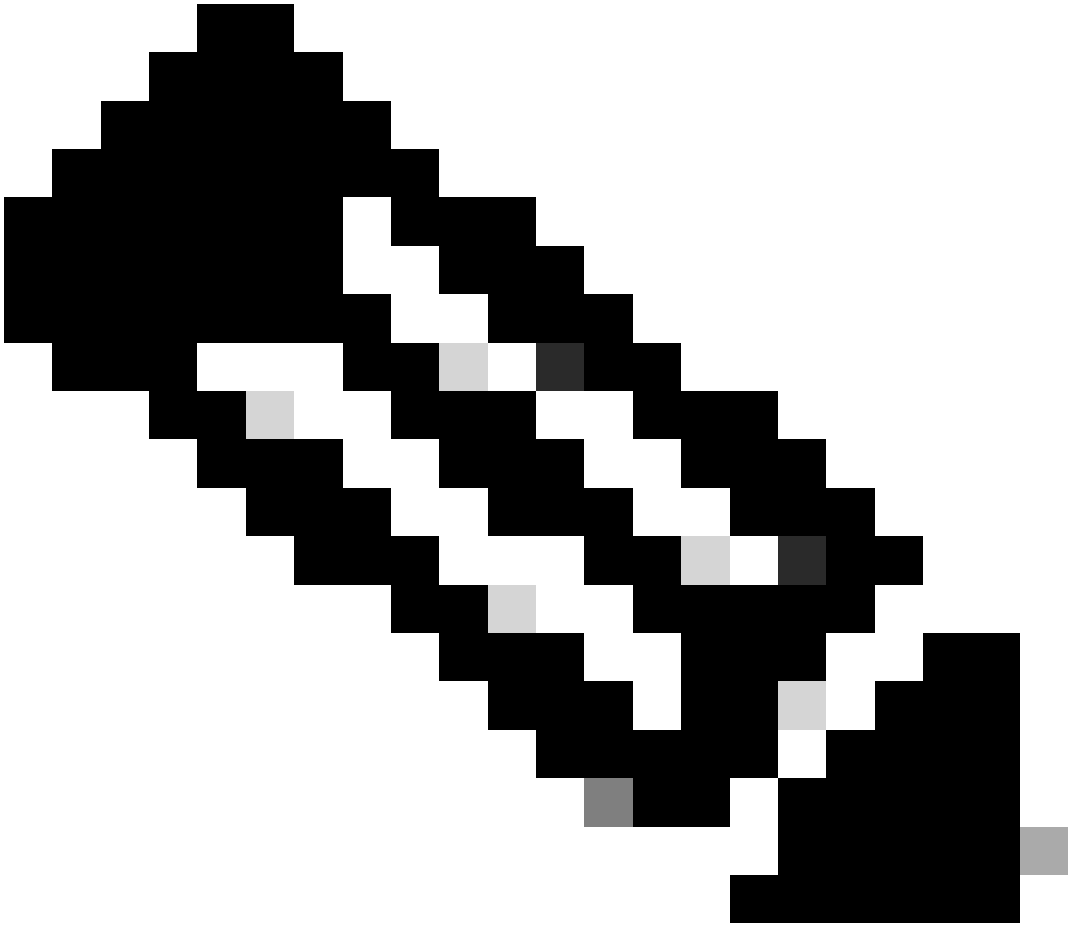
Etapa 2: Configurar a cadeia de chaves MACsec

Lembre-se de que o padrão IEEE 802.1X-2010 especifica que as chaves de criptografia MACsec podem ser derivadas de uma chave pré-compartilhada (PSK), pelo protocolo de autenticação extensível (EAP) 802.1X ou escolhidas e distribuídas por um servidor de chave MKA. Neste exemplo, as PSKs são usadas e configuradas manualmente por meio da cadeia de chaves MACsec e são iguais à Chave de Associação de Conectividade (CAK), que é a chave primária usada para derivar todas as outras chaves de criptografia usadas no MACsec.

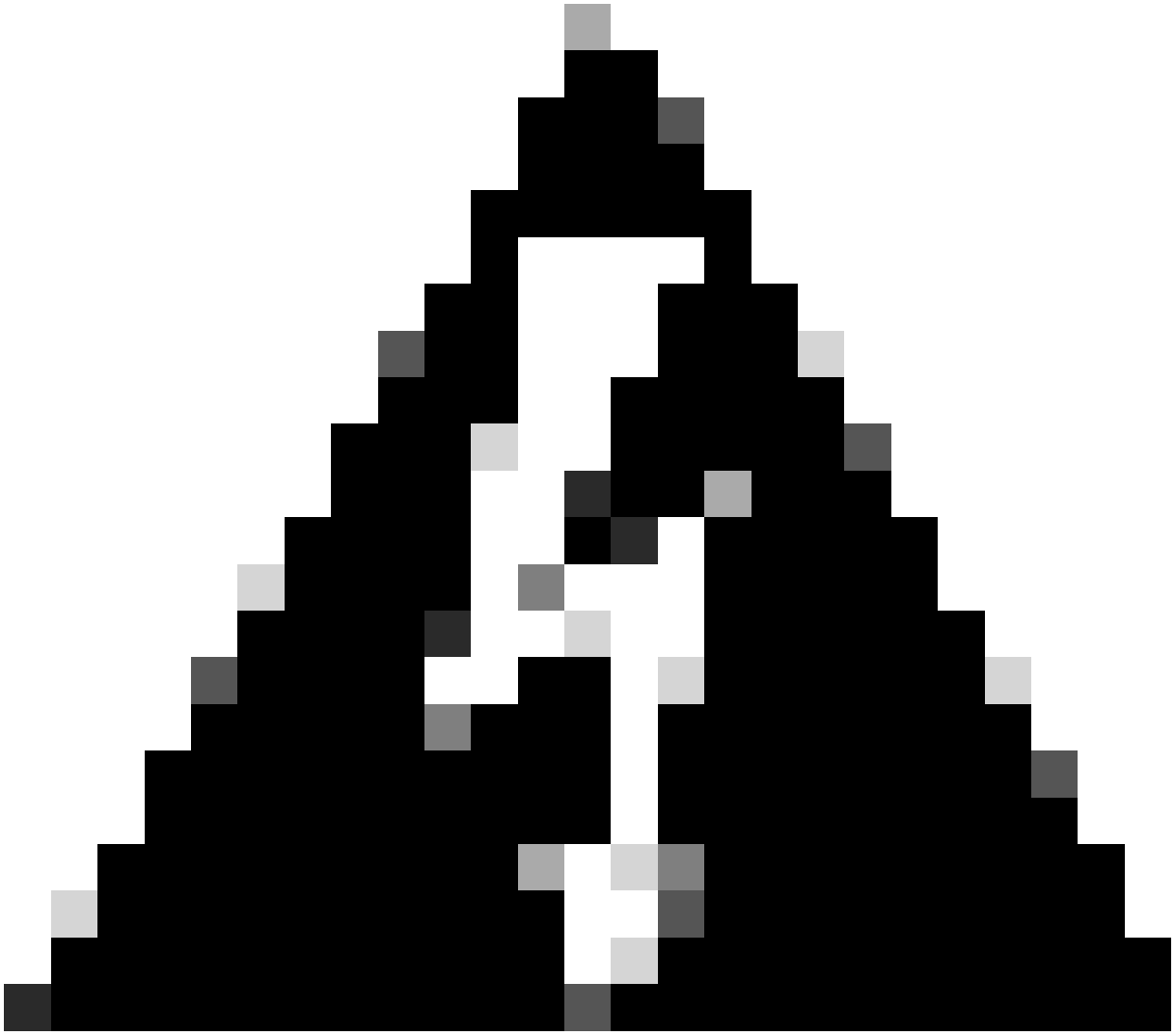
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1**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



Observação: ao configurar a cadeia de chaves MACsec, lembre-se de que a sequência de chaves deve consistir apenas em dígitos hexadecimais, o algoritmo de criptografia aes-128-cmac requer uma chave de 32 dígitos hexadecimais e o algoritmo de criptografia aes-256-cmac requer uma chave de 64 dígitos hexadecimais.



Observação: lembre-se de que, ao usar várias chaves, é necessário um período de tempo de sobreposição entre elas para obter uma sobreposição de chave sem êxito após a expiração do tempo de vida da chave especificado.



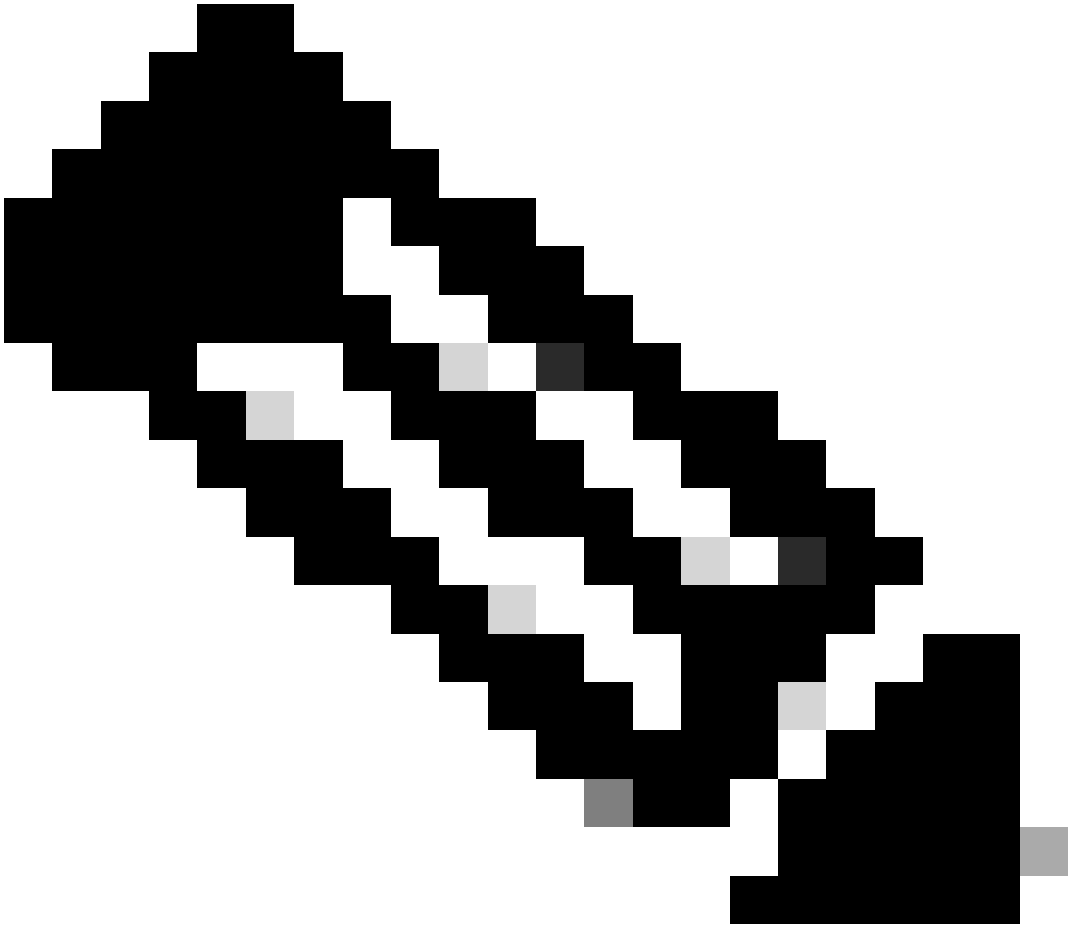
Aviso: é importante garantir que os relógios de ambos os roteadores estejam sincronizados; portanto, o uso do Network Time Protocol (NTP) é altamente recomendado. Deixar de fazer isso pode impedir o estabelecimento de sessões MKA ou fazer com que elas falhem no futuro.

Etapa 3: Configure a política MKA

Embora a política MKA padrão possa ser útil para a configuração inicial e para redes simples, a configuração de uma política MKA personalizada para WAN MACsec é geralmente recomendada para atender a requisitos específicos de segurança, conformidade e desempenho. As políticas personalizadas oferecem maior flexibilidade e controle, garantindo que a segurança da sua rede seja robusta e personalizada de acordo com as suas necessidades.

Ao configurar sua política MKA, existem diferentes elementos que podem ser selecionados, como a Prioridade do servidor chave, Proteção de atraso para a Unidade de dados de pacote de acordo de chave MACsec (MKPDU), Conjunto de cifras, entre outros. Nesta plataforma e versões de software, as próximas cifras podem ser usadas:

Cifra MACsec	Descrição
gcm-aes-128	GCM (Galois/Counter Mode) com AES (Advanced Encryption Standard) usando uma chave de 128 bits
gcm-aes-256	GCM (Galois/Counter Mode) com AES usando uma chave de 256 bits (maior força de criptografia)
gcm-aes-xpn-128	GCM (Galois/Counter Mode) com AES usando uma chave de 128 bits, com numeração de pacotes estendida (XPN - Extended Packet Numbering)
gcm-aes-xpn-256	GCM (Galois/Counter Mode) com AES usando uma chave de 256 bits, com XPN (criptografia mais forte)



Observação: o XPN aprimora a cifra GCM-AES ao suportar uma numeração de pacotes mais longa, o que melhora a segurança para sessões de longa duração ou ambientes de

alto throughput. O uso de links de alta velocidade, por exemplo, 40 Gb/s ou 100 Gb/s, pode causar tempos de transferência de chave muito curtos porque o número do pacote (PN) dentro do quadro MACsec, normalmente baseado no número de pacotes enviados, poderia ser esgotado rapidamente nessas velocidades. O XPN estende a sequência de numeração de pacotes e elimina a necessidade de rechaveamento frequente da chave de associação de segurança (SAK) que pode ocorrer em links de alta capacidade.

Neste exemplo, a cifra selecionada para a política MKA é gcm-aes-xpn-256, e outros elementos terão o valor padrão:

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**

Etapa 4: Configure o MACsec no nível da interface e da subinterface

Nesse cenário, mesmo que a interface física não esteja sendo configurada com um endereço IP, alguns comandos macsec precisam ser aplicados nesse nível para que a solução funcione. A política MACsec e a cadeia de chaves são aplicadas no nível da subinterface (consulte o exemplo de configuração):

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 no Nível da Interface Física

a. A MTU é definida como 9216, pois o provedor de serviços usado na topologia permite quadros jumbo, mas isso não é um requisito

b. O comando macsec dot1q-in-clear permite que a opção tenha a marcação VLAN (dot1q) em clear (não criptografada)

c. O comando macsec access-control should-secure permite que pacotes não criptografados da interface ou subinterface física sejam enviados ou recebidos (esse comando é necessário se algumas subinterfaces exigirem criptografia e outras não, isso se deve ao comportamento padrão do MACsec, que não permite que pacotes não criptografados sejam transmitidos ou recebidos da

mesma interface física em que o MACsec está habilitado)

Comandos aplicados no nível da subinterface

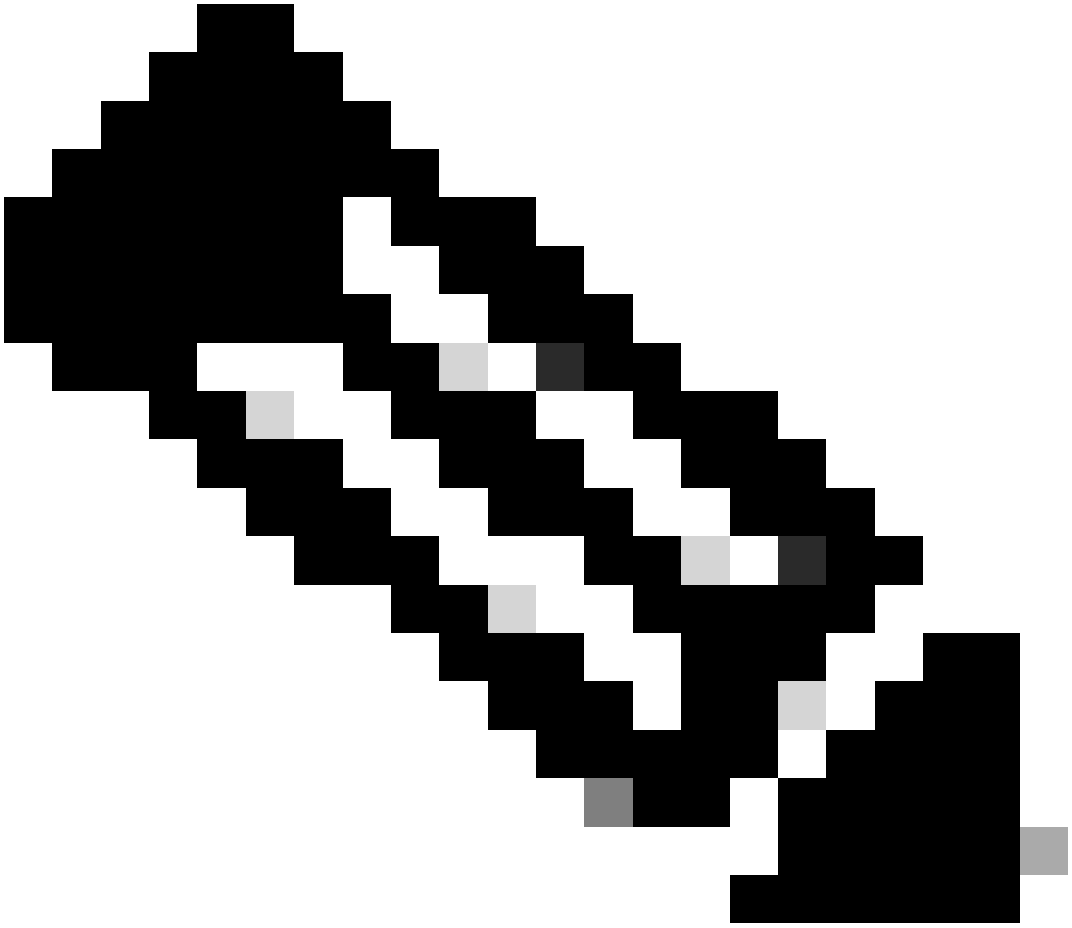
a. Agora, o comando eapol destination-address broadcast-address é necessário para alterar o endereço MAC de destino dos quadros EAPoL (que por padrão é um endereço MAC multicast 01:80:C2:00:00:03) para um endereço MAC de broadcast para garantir que o provedor de serviços os inunde e não os descarte ou consuma.

b. O comando eapol eth-type 876F é usado também para alterar o tipo de ethernet padrão do quadro EAPoL (que por padrão é 0x888E) e alterá-lo para 0x876F. Isso é necessário novamente para evitar que o provedor de serviços descarte ou consuma esses quadros.

c. Os comandos mka policy <policy name> e mka pre-shared-key-chain <key chain name> são usados para aplicar a política personalizada e a cadeia de chaves à subinterface.

d. E por último, mas não menos importante, o comando macsec habilita o MACsec no nível da subinterface.

Na configuração atual, sem as alterações EAPoL anteriores, os switches 9500 no lado do provedor de serviços não estavam encaminhando os quadros EAPoL.



Observação: os comandos MACsec como dot1q-in-clear e should-secure são herdados pelas subinterfaces. Além disso, os comandos EAPoL podem ser definidos no nível da interface física e, nesses casos, esses comandos também são herdados pelas subinterfaces. No entanto, a configuração explícita de comandos EAPoL na subinterface substitui o valor ou a política herdados para essa subinterface.

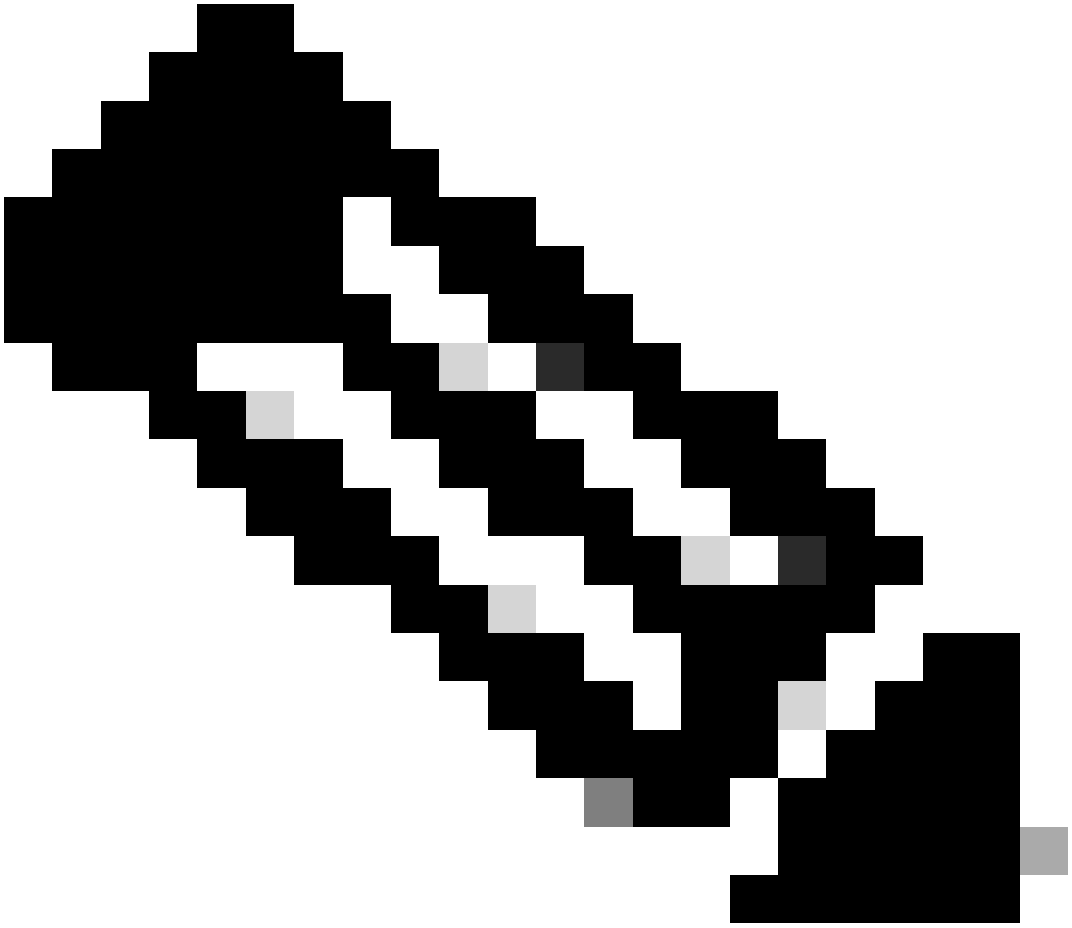
Verificar

Uma vez aplicada a configuração, a próxima saída mostra a configuração atual relevante de cada roteador Customer Edge (CE) C8500 (parte da configuração foi omitida):

```
<#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#
```



Observação: Observe que após ativar o MACsec, aplicando o comando macsec, o MTU nessa interface é automaticamente ajustado e reduzido em 32 bytes para considerar a sobrecarga do MACsec.

Em seguida, você encontrará uma lista de comandos essenciais que podem ser utilizados para verificar e verificar o status do MACsec entre os correspondentes. Esses comandos fornecem informações detalhadas sobre as sessões, os conjuntos de chaves, as políticas e as estatísticas atuais do MACsec:

show mka sessions - Este comando exibe o status das sessões MKA atuais.

show mka sessions detail - Este comando fornece informações detalhadas sobre cada sessão MKA.

show mka keychain -Este comando mostra os keychain usados para o MACsec e a interface atribuída.

show mka policy - esse comando exibe as políticas aplicadas, as interfaces e o conjunto de cifras

usados.

show mka summary - Este comando fornece um resumo das sessões e estatísticas do MKA.

show macsec statistics interface <nome da interface> - Este comando mostra as estatísticas do MACsec para uma interface especificada e ajuda a identificar se o tráfego criptografado está sendo enviado e recebido.

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
```

A acessibilidade das diferentes subinterfaces é bem-sucedida, assim como a acessibilidade entre as sub-redes 192.168.0.0/16. Os próximos testes de ping demonstram a conectividade bem-sucedida:

```
<#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#
```

Depois de capturar pacotes de um teste ICMP no dispositivo PE (Provider Edge), você pode comparar os quadros criptografados e não criptografados. Observe que o cabeçalho MAC do roteador Ethernet é o mesmo em ambos os quadros, com a tag dot1q visível. No entanto, o quadro criptografado mostra um EtherType de 0x88E5 (MACsec), enquanto o quadro não criptografado exibe um EtherType de 0x0800 (IPv4) junto com as informações de protocolo ICMP:

Quadro criptografado VLAN 100

<#root>

F241.03.03-9500-1#

show monitor capture cap buffer detail | begin Frame 80

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

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

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

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

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

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

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

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

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

Data (102 bytes)

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

Informações Relacionadas

- Melhorias de suporte de MACSEC e MKA de WAN
- Inovações em criptografia Ethernet (802.1AE - MACsec) para proteger implantações de WAN de alta velocidade (1-100GE)
- Solucionar problemas do MACSEC da WAN em roteadores

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.