Configuration de WAN MACsec sur Catalyst 8500 avec des sous-interfaces

Table des matières

Introduction

Ce document décrit le processus de configuration de la sécurité MACsec (Media Access Control Security) WAN sur les plates-formes Cisco Catalyst 8500 avec sous-interfaces.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Concepts réseau avancés, notamment le WAN, les VLAN et le cryptage
- Compréhension de MACsec (IEEE 802.1AE) et de la gestion des clés (IEEE 802.1X-2010)
- Connaissance de l'interface de ligne de commande (CLI) Cisco IOS® XE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

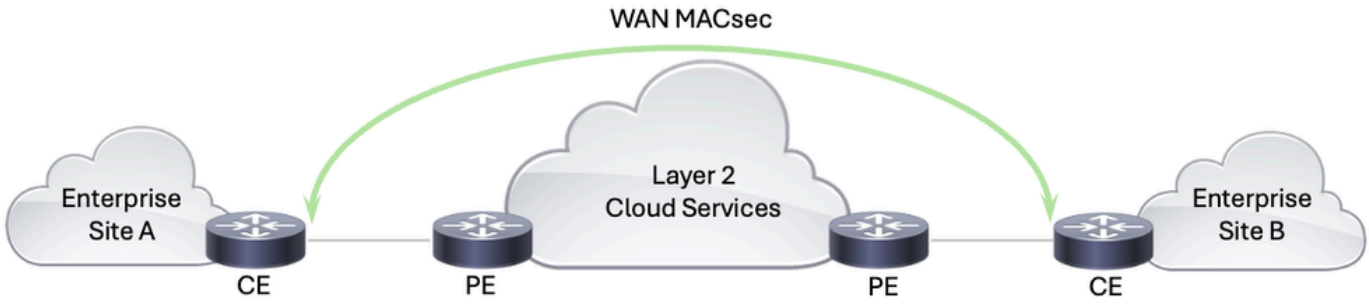
- Plates-formes de périphérie Cisco Catalyst 8500

- Cisco IOS XE version 17.14.01a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

WAN MACsec est une solution de sécurité conçue pour protéger le trafic réseau sur les réseaux WAN en utilisant les fonctionnalités de MACsec. Lorsque vous utilisez un réseau de fournisseur de services pour échanger des données, il est important de chiffrer les données en transit afin d'éviter toute falsification. Le WAN MACsec est facile à déployer et à gérer, ce qui le rend idéal pour les entreprises qui ont besoin de protéger leur trafic réseau contre la manipulation des données, comme les écoutes et les attaques de l'homme du milieu. Il fournit un cryptage transparent à débit de ligne, garantissant que les données restent sécurisées et sans compromis lorsqu'elles traversent diverses infrastructures réseau, y compris les réseaux des fournisseurs de services, les environnements cloud et les réseaux d'entreprise.



Solution WAN MACsec

Pour partager un bit d'historique, MACsec, défini par la norme IEEE 802.1AE, assure une communication sécurisée sur les réseaux Ethernet en garantissant la confidentialité, l'intégrité et l'authenticité de l'origine des données pour les trames Ethernet. Fonctionnant au niveau de la couche liaison de données (couche 2) du modèle OSI (Open Systems Interconnection), MACsec chiffre et authentifie les trames Ethernet pour sécuriser la communication entre les noeuds. Initialement conçu pour les réseaux locaux, MACsec a évolué pour prendre également en charge les déploiements WAN. Il offre un cryptage à débit de ligne, garantissant une latence et une surcharge minimales, ce qui est essentiel pour les réseaux à haut débit.

IEEE 802.1X-2010 est une modification de la norme IEEE 802.1X d'origine, qui définit le contrôle d'accès réseau basé sur les ports. La révision de 2010 introduit le protocole MACsec Key Agreement (MKA), qui est essentiel pour la gestion des clés de cryptage dans les implémentations MACsec. MKA gère la distribution et la gestion des clés cryptographiques utilisées par MACsec pour chiffrer et déchiffrer les données. MKA est une norme qui contribue à l'interopérabilité multifournisseur pour les déploiements MACsec, en prenant en charge les échanges de clés sécurisés et les mécanismes de réencodage, essentiels pour maintenir une sécurité continue dans les environnements WAN dynamiques.

Dans les déploiements WAN MACsec, la norme IEEE 802.1AE (MACsec) fournit les mécanismes

fondamentaux de chiffrement et de sécurité au niveau de la couche liaison de données, garantissant ainsi la protection de toutes les trames Ethernet lorsqu'elles traversent le réseau. IEEE 802.1X-2010 avec le protocole MKA, gère la tâche critique de distribution et de gestion des clés de cryptage nécessaires au fonctionnement de MACsec. Ensemble, ces normes garantissent que WAN MACsec peut fournir un cryptage robuste et à haut débit sur les réseaux étendus, fournissant une protection complète des données en transit tout en préservant l'interopérabilité et la facilité de gestion.

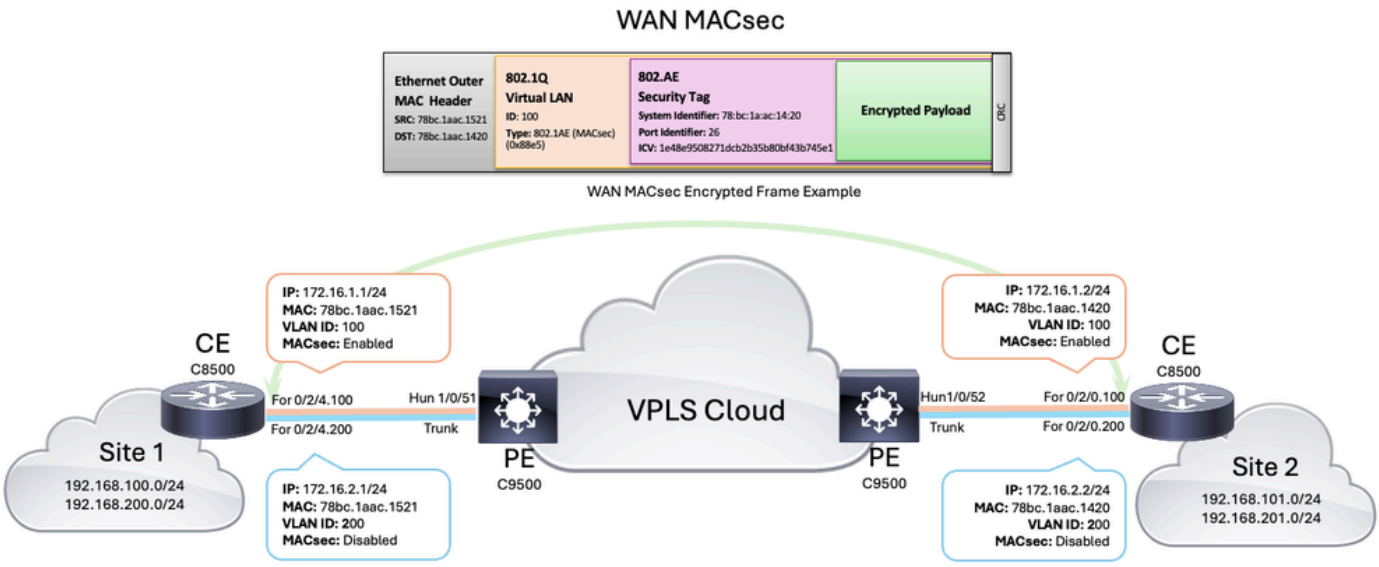
Pour relever les défis uniques des environnements WAN, certaines améliorations ont été apportées aux déploiements MACsec traditionnels :

- Balise 802.1Q en clair : cette fonctionnalité permet à la balise VLAN 802.1Q d'être exposée en dehors de l'en-tête MACsec chiffré, facilitant ainsi des conceptions de réseau plus flexibles, en particulier dans les environnements de transport Ethernet public. Cette fonctionnalité est essentielle pour l'intégration de MACsec avec les services Carrier Ethernet, car elle permet la coexistence du trafic chiffré et non chiffré sur le même réseau, simplifiant ainsi l'architecture réseau et réduisant les coûts.
- Adaptabilité sur Ethernet opérateur public : les mises en oeuvre MACsec modernes de réseau étendu peuvent s'adapter aux services Ethernet de l'opérateur public. Cette adaptabilité inclut la modification de l'adresse de destination et de l'EtherType du protocole EAPoL (Ethernet Authentication Protocol over LAN), permettant ainsi à MACsec de fonctionner de manière transparente sur les réseaux Ethernet opérateur qui peuvent autrement consommer ou bloquer ces trames.

WAN MACsec représente une avancée significative dans le chiffrement Ethernet, répondant au besoin croissant de connexions WAN sécurisées et à haut débit. Sa capacité à fournir un cryptage à débit de ligne, la prise en charge de conceptions de réseau flexibles et l'adaptabilité aux services des opérateurs publics en font un composant essentiel des architectures de sécurité réseau modernes. En tirant parti de WAN MACsec, les entreprises peuvent renforcer la sécurité de leurs liaisons WAN haut débit tout en simplifiant leurs architectures réseau et en réduisant la complexité opérationnelle.

Configurer

Diagramme du réseau



Topologie WAN MACsec

Configurations

Étape 1 : Configuration de base des périphériques

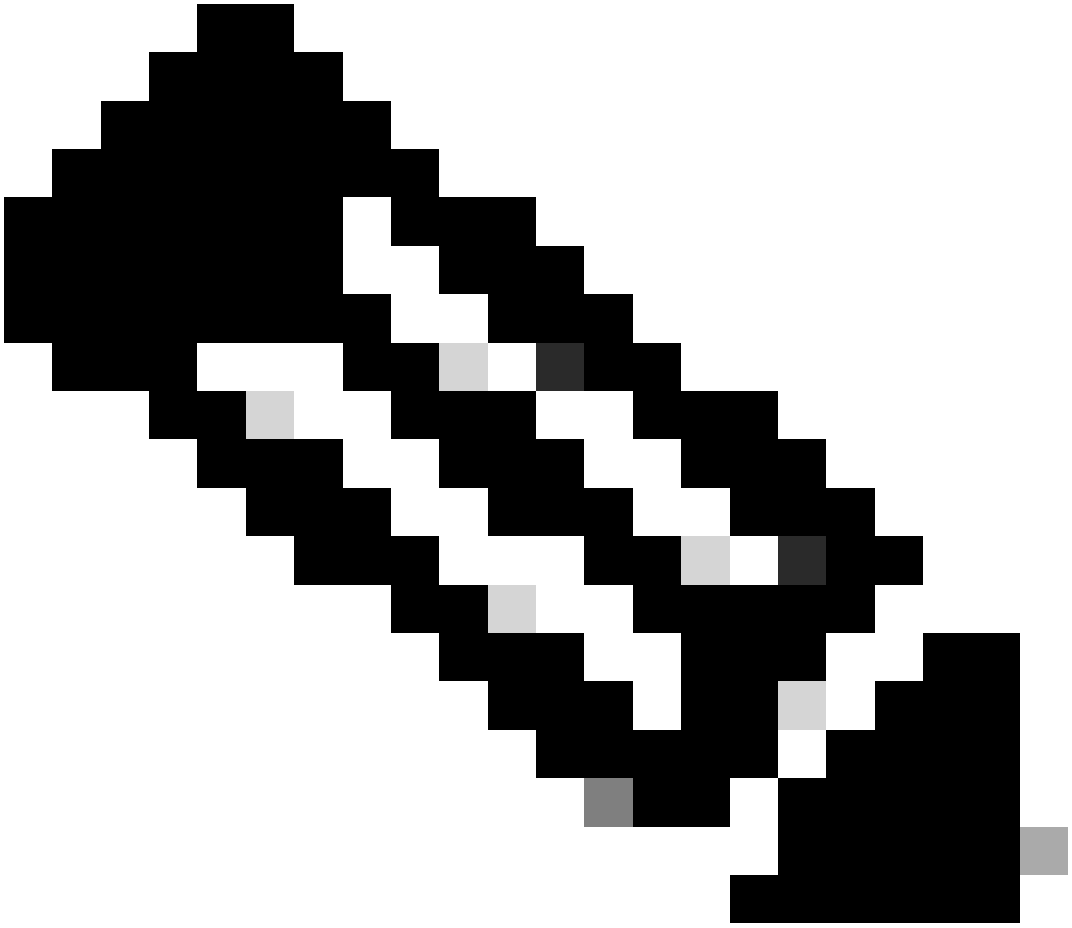
Pour démarrer la configuration, vous devez d'abord définir les sous-interfaces qui seront utilisées pour la segmentation du trafic et la connexion au fournisseur de services. Pour ce scénario, deux sous-interfaces sont définies pour le VLAN 100 associé au sous-réseau 172.16.1.0/24 et le VLAN 200 associé au sous-réseau 172.16.2.0/24 (plus tard, une seule sous-interface sera configurée avec 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.**

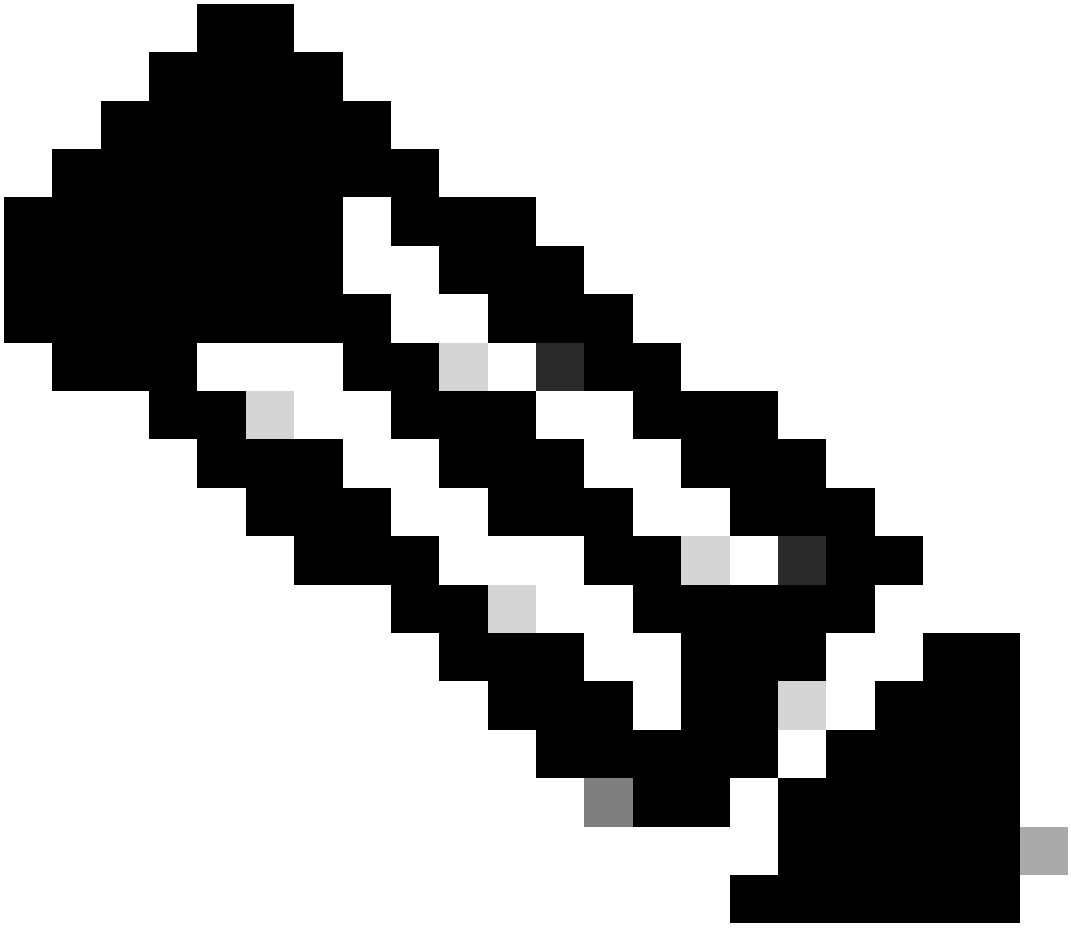
Étape 2 : configurez la chaîne de clés MACsec

N'oubliez pas que la norme IEEE 802.1X-2010 spécifie que les clés de chiffrement MACsec peuvent être dérivées d'une clé prépartagée (PSK), par le protocole EAP (Extensible Authentication Protocol) 802.1X ou choisies et distribuées par un serveur de clés MAC. Dans cet exemple, les clés prédéfinies sont utilisées et configurées manuellement via la chaîne de clés MACsec, et elles sont égales à la clé d'association de connectivité (CAK), qui est la clé primaire utilisée pour dériver toutes les autres clés de chiffrement utilisées dans MACsec.

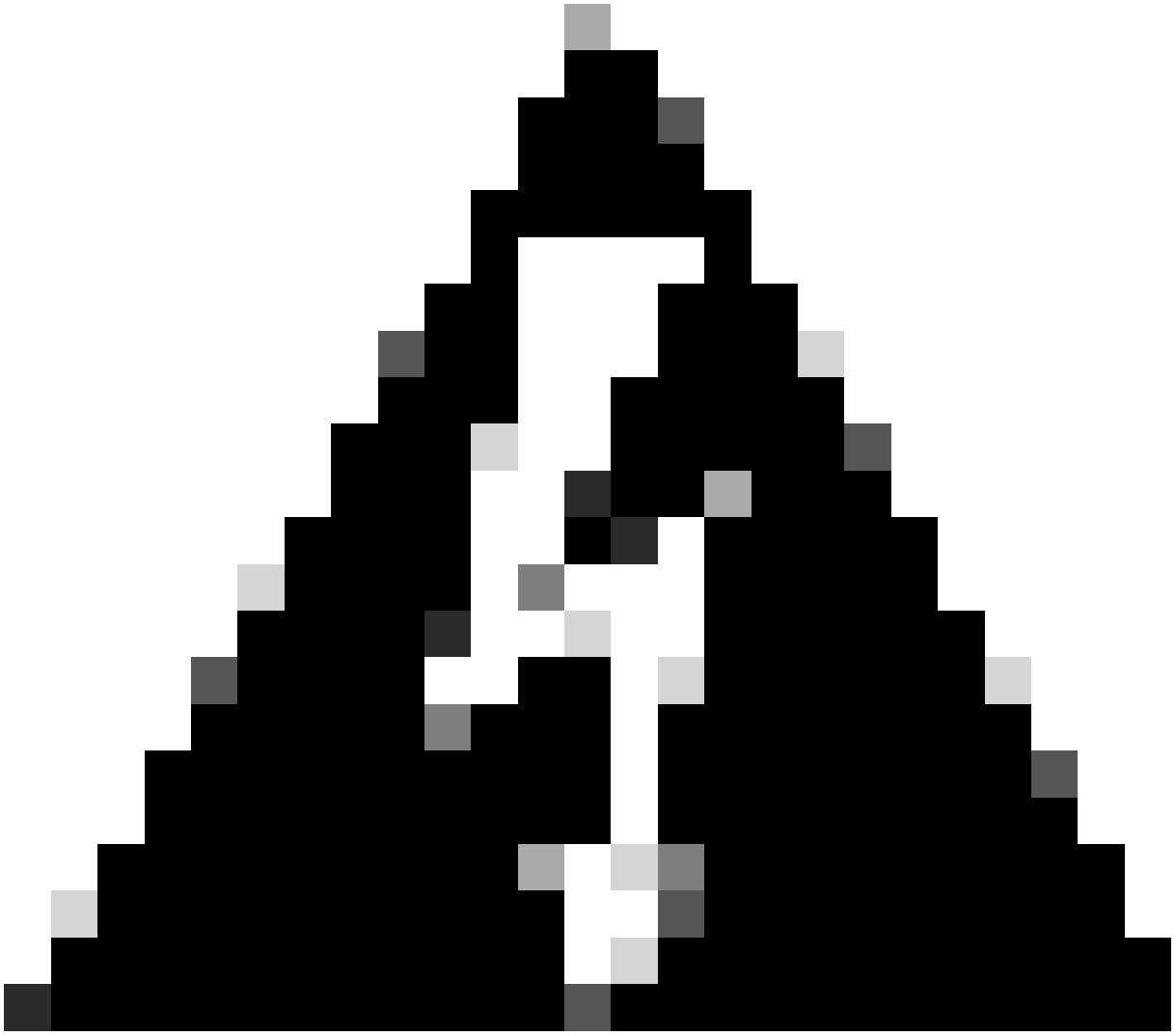
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1**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



Remarque : lors de la configuration de la chaîne de clés MACsec, n'oubliez pas que la chaîne de clés doit se composer de chiffres hexadécimaux uniquement, l'algorithme de chiffrement aes-128-cmac nécessite une clé de 32 chiffres hexadécimaux et l'algorithme de chiffrement aes-256-cmac nécessite une clé de 64 chiffres hexadécimaux.



Remarque : n'oubliez pas que lorsque vous utilisez plusieurs clés, une période de chevauchement entre elles est nécessaire pour obtenir une substitution de clé sans heurt après l'expiration de la durée de vie de la clé spécifiée.



Avertissement : il est important de s'assurer que les horloges des deux routeurs sont synchronisées ; par conséquent, l'utilisation du protocole NTP (Network Time Protocol) est fortement recommandée. Si vous ne le faites pas, vous risquez d'empêcher l'établissement de sessions MKA ou de les faire échouer à l'avenir.

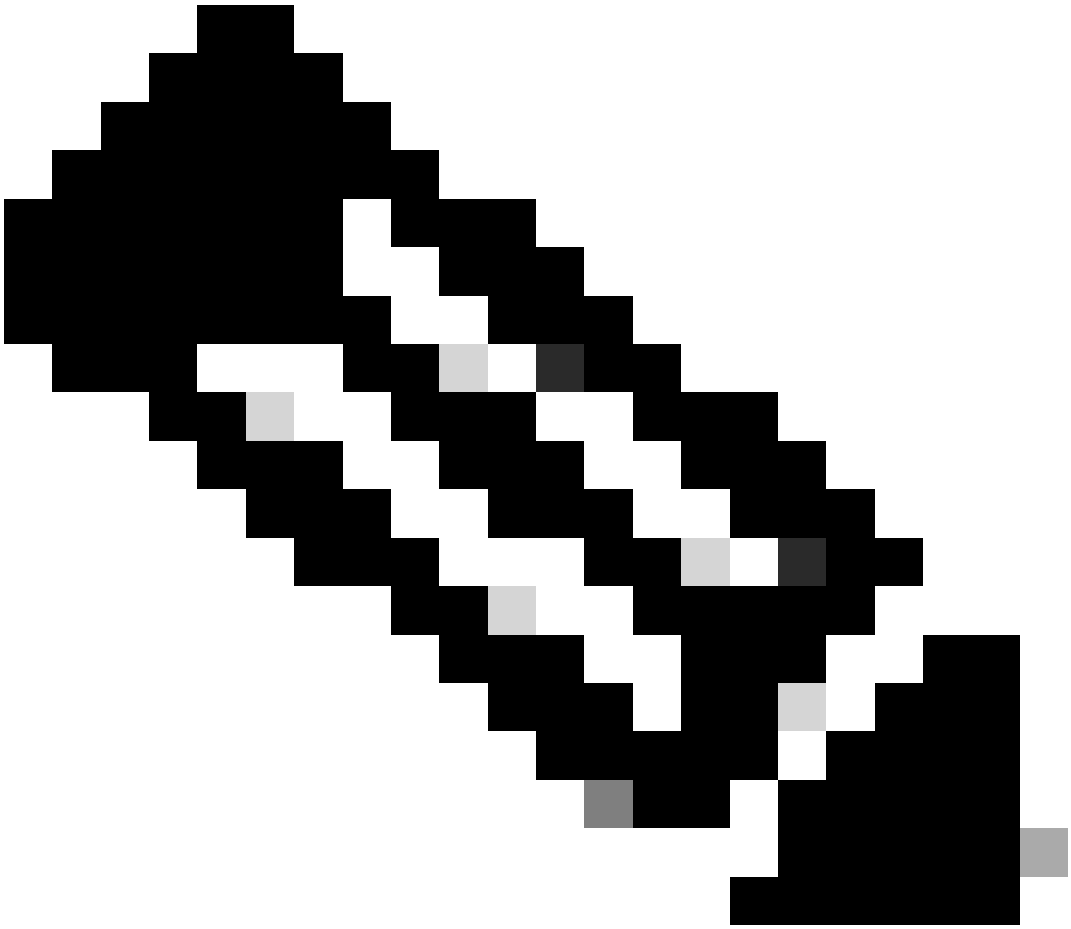
Étape 3 : configurez la stratégie MKA

Bien que la stratégie MKA par défaut puisse être utile pour la configuration initiale et les réseaux simples, la configuration d'une stratégie MKA personnalisée pour WAN MACsec est généralement recommandée pour répondre à des exigences spécifiques en matière de sécurité, de conformité et de performances. Les politiques personnalisées offrent une plus grande flexibilité et un meilleur contrôle, garantissant ainsi une sécurité réseau robuste et personnalisée en fonction de vos besoins.

Lors de la configuration de votre stratégie MKA, il y a différents éléments qui peuvent être sélectionnés, tels que, Key Server Priority, Delay Protection for the MACsec Key Agreement Packet Data Unit (MKPDU), Cipher Suite, entre autres. Dans cette plate-forme et les versions

logicielles, les chiffrements suivants peuvent être utilisés :

Chiffrement MACsec	Description
gcm-aes-128	Galois/Counter Mode (GCM) avec Advanced Encryption Standard (AES) à l'aide d'une clé de 128 bits
gcm-aes-256	Galois/Counter Mode (GCM) avec AES utilisant une clé de 256 bits (niveau de cryptage supérieur)
gcm-aes-xpn-128	Galois/Counter Mode (GCM) avec AES utilisant une clé de 128 bits, avec Extended Packet Numbering (XPN)
gcm-aes-xpn-256	Galois/Counter Mode (GCM) avec AES utilisant une clé de 256 bits, avec XPN (niveau de cryptage plus élevé)



Remarque : XPN améliore le chiffrement GCM-AES en prenant en charge une

numérotation des paquets plus longue, ce qui améliore la sécurité pour les sessions de très longue durée ou les environnements à haut débit. L'utilisation de liaisons haut débit, par exemple 40 Gbit/s ou 100 Gbit/s, peut entraîner des temps de transfert de clé très courts, car le numéro de paquet (PN) dans la trame MACsec, généralement basé sur le nombre de paquets envoyés, peut être rapidement épuisé à ces vitesses. XPN étend la séquence de numérotation des paquets et élimine le besoin fréquent d'une nouvelle clé SAK (Security Association Key) qui peut se produire dans les liaisons à haute capacité.

Dans cet exemple, le chiffre sélectionné pour la stratégie MKA est gcm-aes-xpn-256, et d'autres éléments auront la valeur par défaut :

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**

Étape 4 : Configurez MACsec au niveau de l'interface et de la sous-interface

Dans ce scénario, même si l'interface physique n'est pas configurée avec une adresse IP, certaines commandes macsec doivent être appliquées à ce niveau pour que la solution fonctionne. La stratégie MACsec et la chaîne de clés sont appliquées au niveau de la sous-interface (voir l'exemple de configuration) :

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**

Commandes appliquées au niveau de l'interface physique

a. MTU est défini sur 9216 car le fournisseur de services utilisé dans la topologie autorise les trames Jumbo, mais ce n'est pas obligatoire

b. La commande macsec dot1q-in-clear active l'option d'avoir l'étiquette VLAN (dot1q) dans la zone clear (non cryptée)

c. La commande macsec access-control should-secure permet l'envoi ou la réception de paquets non chiffrés provenant de l'interface physique ou de la sous-interface (cette commande est nécessaire si certaines sous-interfaces nécessitent un chiffrement et d'autres non, en raison du comportement MACsec par défaut où elle ne permet pas l'envoi ou la réception de paquets non

chiffrés provenant de la même interface physique où MACsec est activé)

Commandes appliquées au niveau de la sous-interface

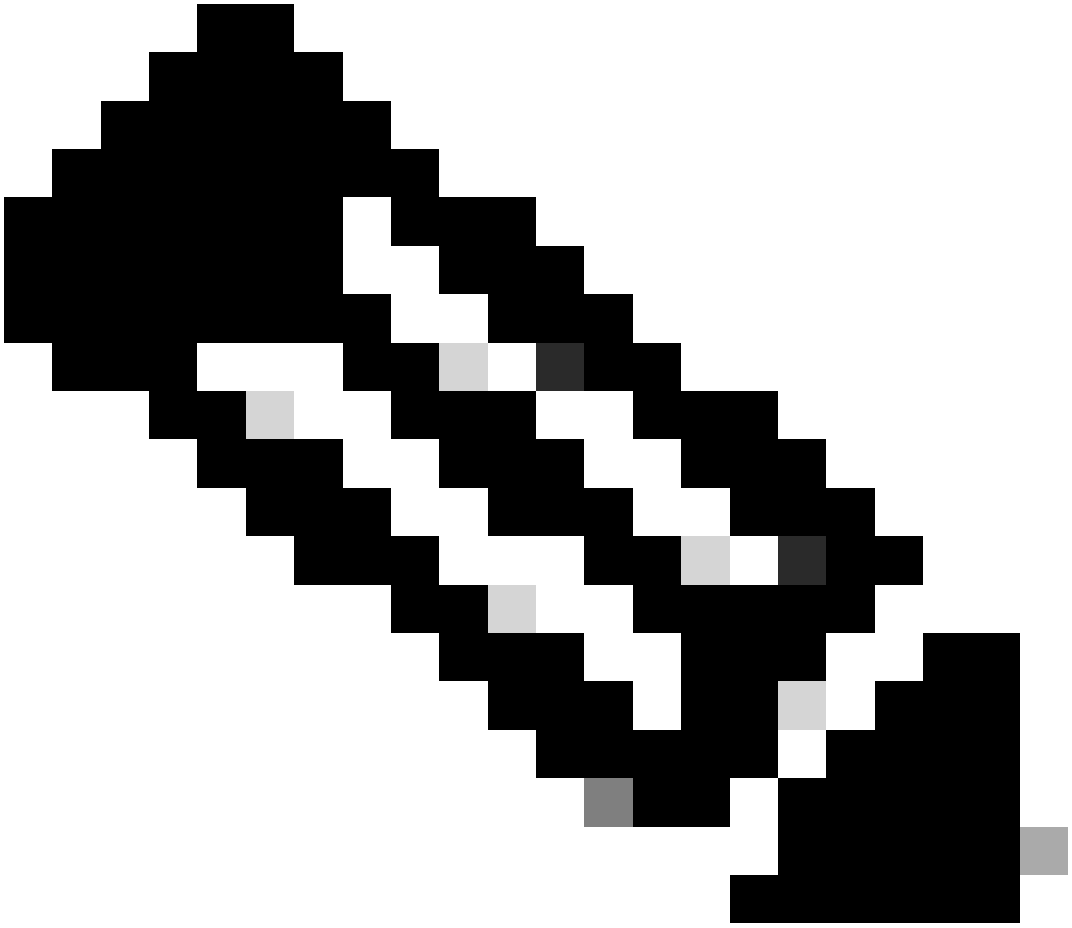
a. Maintenant, la commande eapol destination-address broadcast-address est nécessaire pour changer l'adresse MAC de destination des trames EAPoL (qui par défaut est une adresse MAC de multidiffusion 01:80:C2:00:00:03) en une adresse MAC de diffusion afin de s'assurer que le fournisseur de services les diffuse et ne les abandonne pas ou ne les consomme pas.

b. La commande eapol eth-type 876F, est également utilisée pour modifier le type Ethernet par défaut de la trame EAPoL (qui est par défaut 0x888E) et la remplacer par 0x876F. Ceci est à nouveau nécessaire pour empêcher le fournisseur de services d’abandonner ou d’utiliser ces trames.

c. Les commandes mka policy <policy name> et mka pre-shared-key-chain <key chain name> sont utilisées pour appliquer la stratégie personnalisée et la chaîne de clés à la sous-interface.

d. Enfin, la commande macsec active MACsec au niveau de la sous-interface.

Dans la configuration actuelle, sans les modifications EAPoL précédentes, les commutateurs 9500 côté fournisseur de services ne transmettaient pas les trames EAPoL.



Remarque : les commandes MACsec telles que dot1q-in-clear et should-secure sont héritées par les sous-interfaces. En outre, les commandes EAPoL peuvent être définies au niveau de l'interface physique et, dans de tels cas, ces commandes sont également héritées par les sous-interfaces. Cependant, la configuration explicite des commandes EAPoL sur la sous-interface remplace la valeur ou la stratégie héritée pour cette sous-interface.

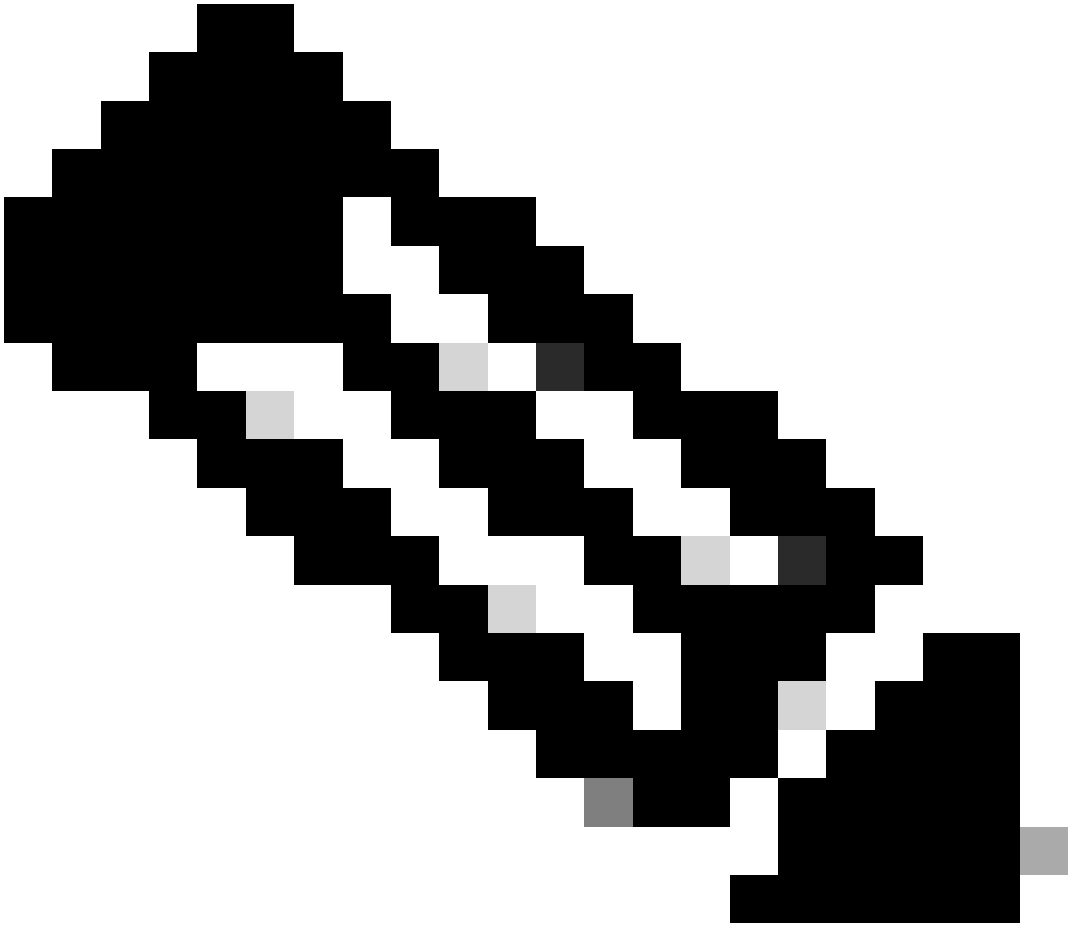
Vérifier

Une fois la configuration appliquée, le résultat suivant présente la configuration en cours de chaque routeur Customer Edge (CE) C8500 (une partie de la configuration a été omise) :

```
<#root>
8500-1#
```

```
show running-config


Building configuration...

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

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

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

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


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

interface FortyGigabitEthernet0/2/4
```

```
 mtu 9216
 no ip address
 no negotiation auto
 cdp enable

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

!

interface FortyGigabitEthernet0/2/4.100

 encapsulation dot1Q 100
 ip address 172.16.1.1 255.255.255.0


ip mtu 9184

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

!

interface FortyGigabitEthernet0/2/4.200

 encapsulation dot1Q 200
 ip address 172.16.2.1 255.255.255.0
!
!
router eigrp 100
 network 172.16.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip forward-protocol nd
!
!
!
control-plane
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
!
!
!
!
!
!
end

8500-1#
```



Remarque : après avoir activé MACsec, en appliquant la commande macsec, le MTU de cette interface est automatiquement ajusté et réduit de 32 octets pour tenir compte de la surcharge MACsec.

Ensuite, vous pouvez trouver une liste de commandes essentielles qui peuvent être utilisées pour vérifier et vérifier l'état de MACsec entre les homologues. Ces commandes vous fournissent des informations détaillées sur les sessions MACsec, les chaînes de clés, les stratégies et les statistiques actuelles :

show mka sessions - Cette commande affiche l'état actuel des sessions MKA.

show mka sessions detail - Cette commande fournit des informations détaillées sur chaque session MKA.

show mka keychains - Cette commande affiche les chaînes de clés utilisées pour MACsec et l'interface attribuée.

show mka policy - Cette commande affiche les stratégies appliquées, les interfaces et la suite de

chiffrement utilisée.

show mka summary - Cette commande fournit un résumé des sessions MKA et des statistiques.

show macsec statistics interface <nom de l'interface> - Cette commande affiche les statistiques MACsec pour une interface spécifiée et permet d'identifier si du trafic chiffré est envoyé et reçu.

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
```

L'accessibilité des différentes sous-interfaces est réussie, ainsi que l'accessibilité entre les sous-réseaux 192.168.0.0/16. Les tests ping suivants montrent que la connectivité a réussi :

```
<#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#
```

Après avoir capturé les paquets d'un test ICMP sur le périphérique Provider Edge (PE), vous pouvez comparer les trames chiffrées et non chiffrées. Notez que l'en-tête MAC externe Ethernet est identique sur les deux trames, avec l'étiquette dot1q visible. Cependant, la trame chiffrée affiche un EtherType de 0x88E5 (MACsec), tandis que la trame non chiffrée affiche un EtherType de 0x800 (IPv4) avec les informations de protocole ICMP :

Trame cryptée 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]
```

Informations connexes

- Améliorations de la prise en charge WAN MACSEC et MKA
- Innovations en matière de cryptage Ethernet (802.1AE - MACsec) pour sécuriser les déploiements WAN haut débit (1-100GE)
- Dépannage de WAN MACSEC sur les routeurs

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.