تكوين WAN MACsec على Catalyst 8500 باستخدام الواجهات الفرعية

المحتويات

المقدمة

يصف هذا المستند عملية تكوين أمان التحكم في الوصول إلى وسائط شبكات WAN (MACsec) على الأنظمة الأساسية Cisco Catalyst 8500 باستخدام الواجهات الفرعية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مفاهيم الشبكة المتقدمة، بما في ذلك شبكة الاتصال واسعة النطاق (WAN) والشبكات المحلية الظاهرية (VLANs) والتشفير
- فهم بروتوكول MacSec (IEEE 802. 1ae) وإدارة المفاتيح (IEEE 802. 1x-2010)
- التشابه مع cisco ios® XE أمر خط قارن (CLI)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

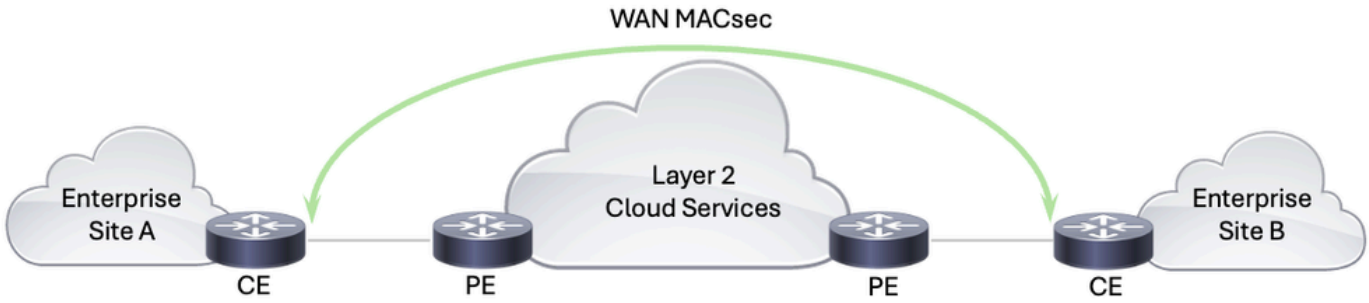
- الأنظمة الأساسية للطرف سلسلة Cisco Catalyst 8500

- Cisco IOS XE، الإصدار 17.14.01a

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

WAN MacSec هو حل أمان مصمم لحماية حركة مرور الشبكة عبر شبكات WAN باستخدام تقنيات MacSec. عند إستخدام شبكة موزد الخدمة لتبادل البيانات، من المهم تشفير البيانات أثناء النقل لمنع التلاعب. يتميز برنامج WAN MacSec بسهولة النشر والإدارة، مما يجعله مثاليا للمؤسسات التي تحتاج إلى حماية حركة مرور بيانات الشبكة لديها من التلاعب بالبيانات، مثل التنصت وهجمات الدخيل. وهو يوفر تشفيرا سلسا وبسرعة خطية، مما يضمن بقاء البيانات آمنة ودون أي خطر لأنها تجتاز بنى تحتية مختلفة للشبكة، بما في ذلك شبكات موزدي الخدمة وبيئات الشبكات وشبكات المؤسسات.



حل WAN MacSec

لمشاركة القليل من المحفوظات، يوفر MACsec، والذي تم تعريفه بواسطة معيار IEEE 802.1AE، إتصالات آمنة على شبكات إيثرنت من خلال ضمان سرية البيانات، والسلامة، والأصل لإطارات إيثرنت. نظرا لأنه يعمل في طبقة إرتباط البيانات (الطبقة 2) من نموذج الاتصال الأنظمة المفتوحة (OSI)، يقوم MacSec بتشفير إطارات الإيثرنت ومصادقتها لتأمين الاتصال بين العقد. نظرا لتصميمه في الأصل للشبكات المحلية (LANs)، فقد تم تطوير ميزة MacSec لدعم عمليات نشر شبكات WAN أيضا. وهو يوفر تشفيرا بسرعة الخط، مما يضمن الحد الأدنى من زمن الوصول والنفقات الإضافية، وهو أمر بالغ الأهمية للشبكات عالية السرعة.

IEEE 802.1X-2010 هو تعديل على معيار IEEE 802.1X الأصلي، الذي يحدد التحكم في الوصول إلى الشبكة القائمة على المنافذ. تقدم مراجعة 2010 بروتوكول إتفاقية مفتاح MACsec (MKA)، والذي يعد ضروريا لإدارة مفاتيح التشفير في عمليات تنفيذ MACsec. تقوم MKA بمعالجة توزيع مفاتيح التشفير التي يستخدمها MacSec لتشفير البيانات وفك تشفيرها وإدارتها. يعد MKA معيارا يسامح في قابلية التشغيل البيني لعدة موردين لعمليات نشر MACsec، ويدعم عمليات تبادل المفاتيح آليا وآليات إعادة صياغة المفاتيح، وهو أمر حيوي للحفاظ على الأمان المستمر في بيئات WAN الديناميكية.

في عمليات نشر WAN MACsec، يوفر IEEE 802.1AE (MacSec) التشفير الأساسي وآليات الأمان في طبقة إرتباط البيانات، مما يضمن أن جميع إطارات الإيثرنت محمية أثناء عبورها الشبكة. يقوم IEEE 802.1X-2010 باستخدام بروتوكول MKA بالمهمة الحيوية لتوزيع مفاتيح التشفير الضرورية لتشغيل MacSec وإدارتها. تضمن هذه المعايير معا إمكانية

توفير ميزة تشفير WAN MACsec تشفيرا قويا فائق السرعة عبر شبكات واسعة، مما يوفر حماية شاملة للبيانات أثناء النقل مع الحفاظ على إمكانية التشغيل البيني وسهولة الإدارة في نفس الوقت.

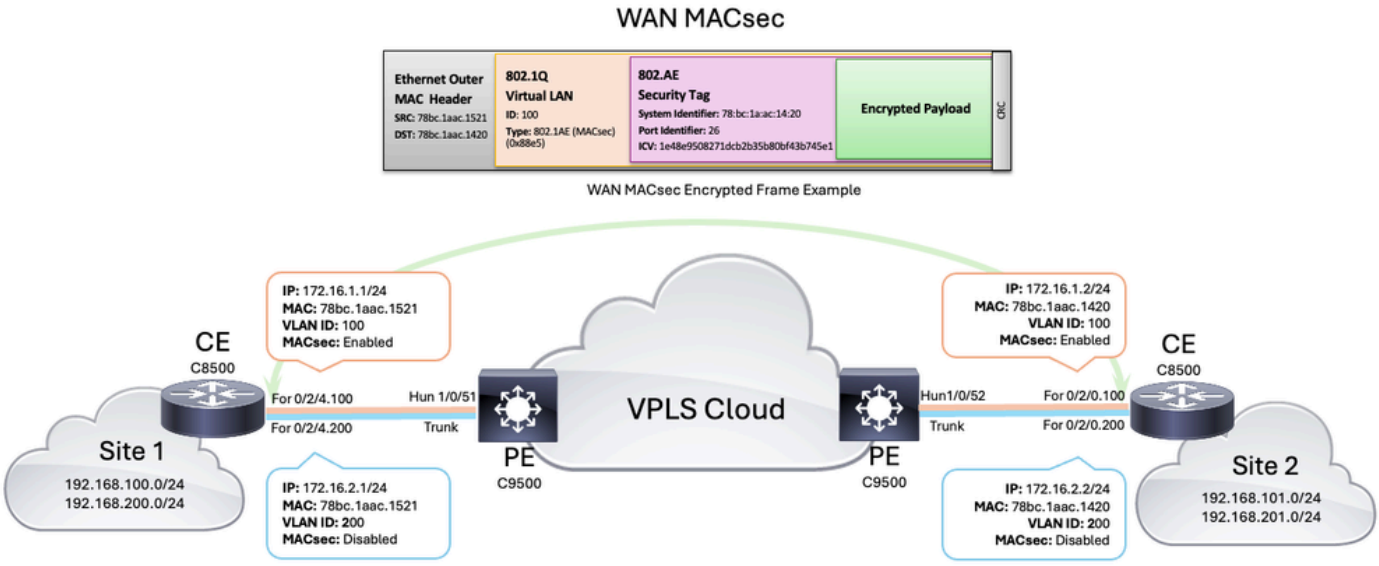
ولمواجهة التحديات الفريدة لبيئات شبكات WAN، تم إجراء بعض التحسينات على عمليات نشر MACsec التقليدية:

- علامة 802.1Q في clear: تتيح هذه الميزة عرض علامة الشبكة المحلية الظاهرية (VLAN) وفقا لمعيار 802.1Q خارج الرأس المشفر لبروتوكول MacSec، مما يسهل تصميمات شبكة أكثر مرونة، وخاصة في بيئات النقل عبر شبكة إيثرنت العامة. وتعد هذه الإمكانية ضرورية لدمج وحدة التحكم في الوصول للوسائط (MACsec) مع خدمات شبكة الإيثرنت Carrier Ethernet، حيث إنها تسمح بوجود حركة مرور مشفرة وغير مشفرة على نفس الشبكة، مما يعمل على تبسيط بنية الشبكة وتقليل التكاليف
- إمكانية التكيف عبر إيثرنت النواقل العام: يمكن أن تتكيف عمليات تنفيذ WAN MACsec الحديثة مع خدمات إيثرنت النواقل العام. تتضمن هذه القابلية للتكيف تعديل بروتوكول مصادقة الإيثرنت عبر عنوان وجهة LAN (EAPoL) و EtherType، مما يسمح لـ MACsec بالعمل بسلاسة عبر شبكات الإيثرنت التي يمكنها خلاف ذلك إستهلاك هذه الإطارات أو حظرها

يمثل WAN MacSec تقدما مهما في تشفير الإيثرنت، مما يلبي الحاجة المتزايدة لاتصالات WAN الآمنة عالية السرعة. قدرتها على توفير تشفير بمعدل الخط ودعم التصميمات المرنة للشبكة وإمكانية التكيف مع خدمات النواقل العامة تجعلها مكونا هاما في بنى أمان الشبكات الحديثة. من خلال الاستفادة من ميزة WAN MacSec، يمكن للمؤسسات تحقيق أمان قوي لارتباطات WAN عالية السرعة الخاصة بها مع تبسيط بنى الشبكات الخاصة بها وتقليل تعقيدات التشغيل في نفس الوقت.

التكوين

الرسم التخطيطي للشبكة



مخطط WAN MacSec

التكوينات

الخطوة 1: تكوين الجهاز الأساسي

قبل التكوين، يلزمك أولا تحديد الواجهات الفرعية التي سيتم إستخدامها لتجزئة حركة المرور والاتصال بمزود الخدمة. لهذا السيناريو، يتم تحديد واجهتين فرعيتين لشبكة VLAN 100 المقترنة بالشبكة الفرعية 172.16.1.0/24 وشبكة VLAN 200 المرتبطة بالشبكة الفرعية 172.16.2.0/24 (سيتم تكوين واجهة فرعية واحدة فقط طوال الحل مع MACsec).

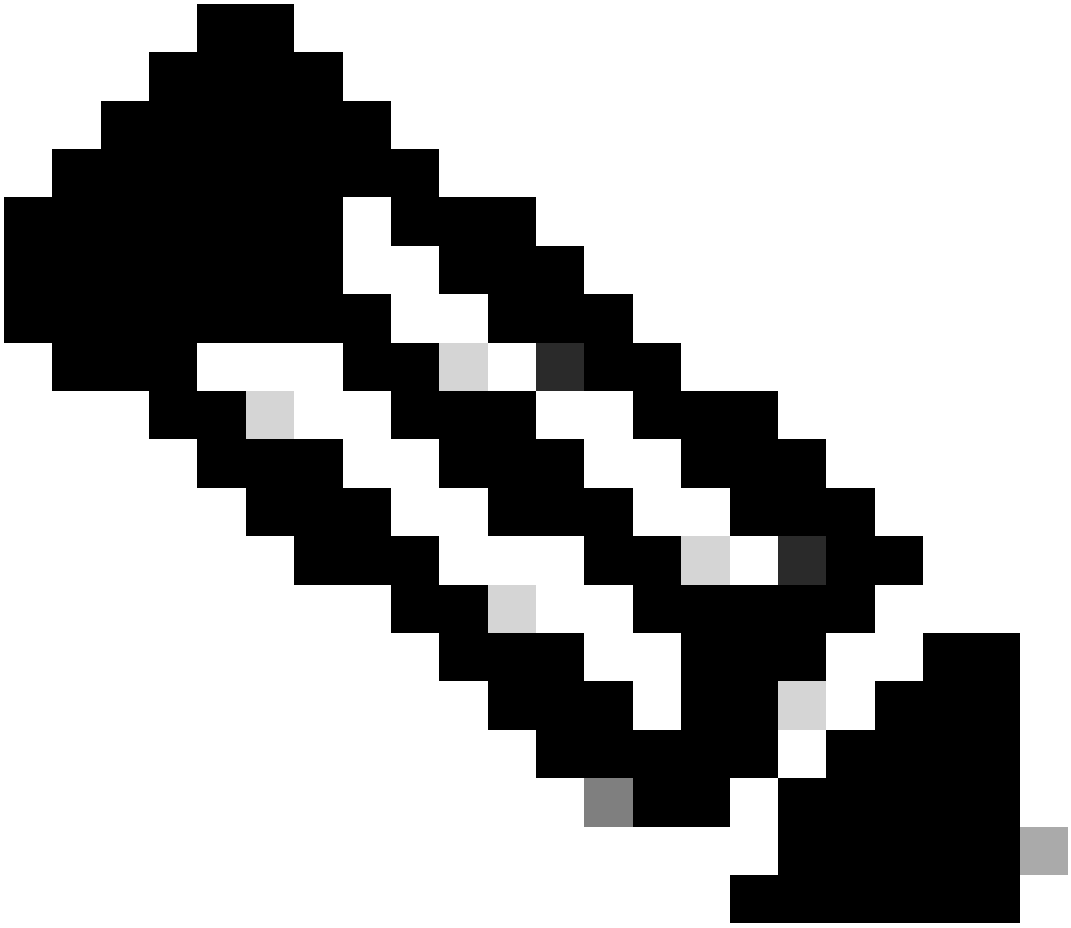
CE 8500-1	CE 8500-2
<#root> interface FortyGigabitEthernet0/2/4.100 **encapsulation dot1Q 100 ip address 172.16.1.1 255.255.255.0** ! interface FortyGigabitEthernet0/2/4.200 **encapsulation dot1Q 200 ip address 172.16.2.1 255.255.255.0**	<#root> interface FortyGigabitEthernet0/2/0.100 **encapsulation dot1Q 100 ip address 172.16.** ! interface FortyGigabitEthernet0/2/0.200 **encapsulation dot1Q 200 ip address 172.16.**

الخطوة 2: تكوين سلسلة مفاتيح MacSec

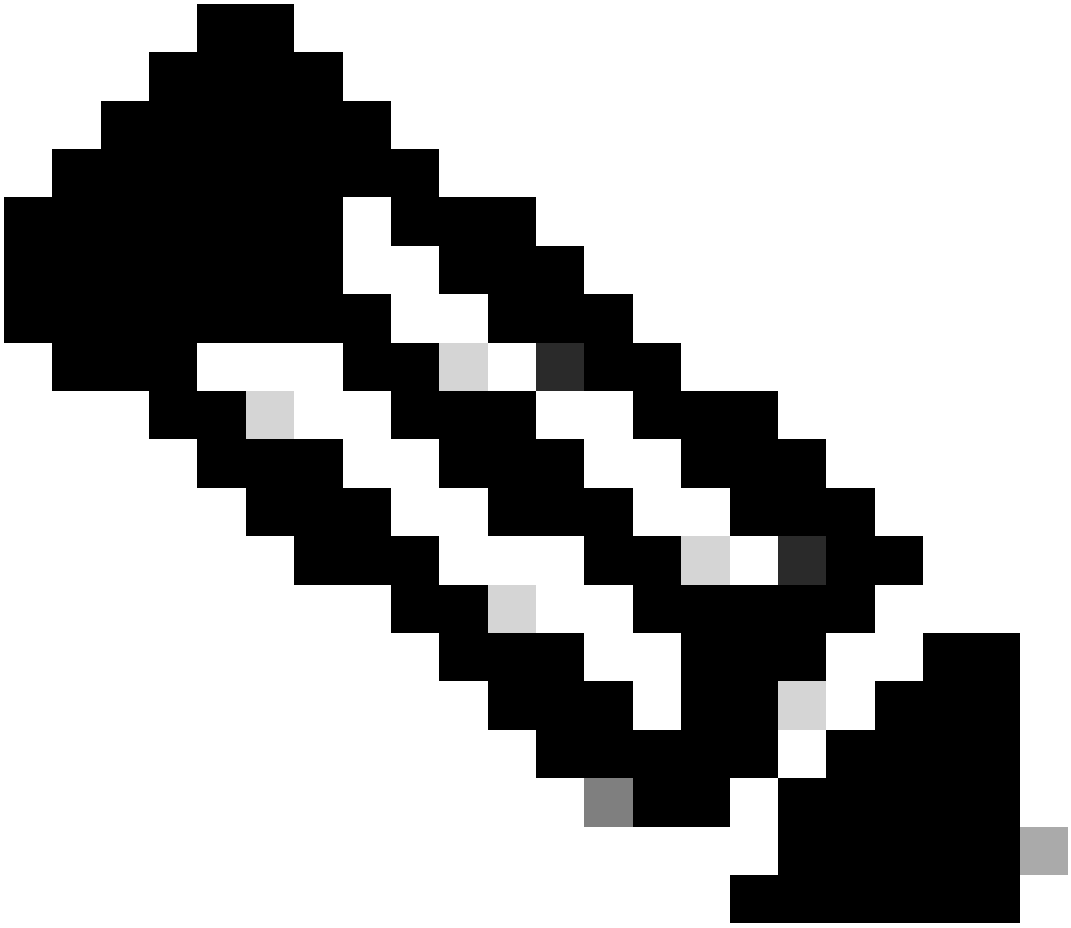
تذكر أن مقياس IEEE 802.1X-2010 يحدد أن مفاتيح تشفير MacSec يمكن أن تكون مشتقة من مفتاح مشترك مسبقا (PSK)، ببروتوكول المصادقة الموسع (EAP) 802.1X أو أن يتم إختيارها وتوزيعها بواسطة خادم مفاتيح MKA. في هذا المثال، يتم إستخدام PSKs وتكوينها يدويا من خلال سلسلة مفاتيح MacSec، وهذه تساوي مفتاح اقتران الاتصال (CAK)، وهو المفتاح الرئيسي المستخدم لاستخلاص جميع مفاتيح التشفير الأخرى المستخدمة في 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**	<#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**

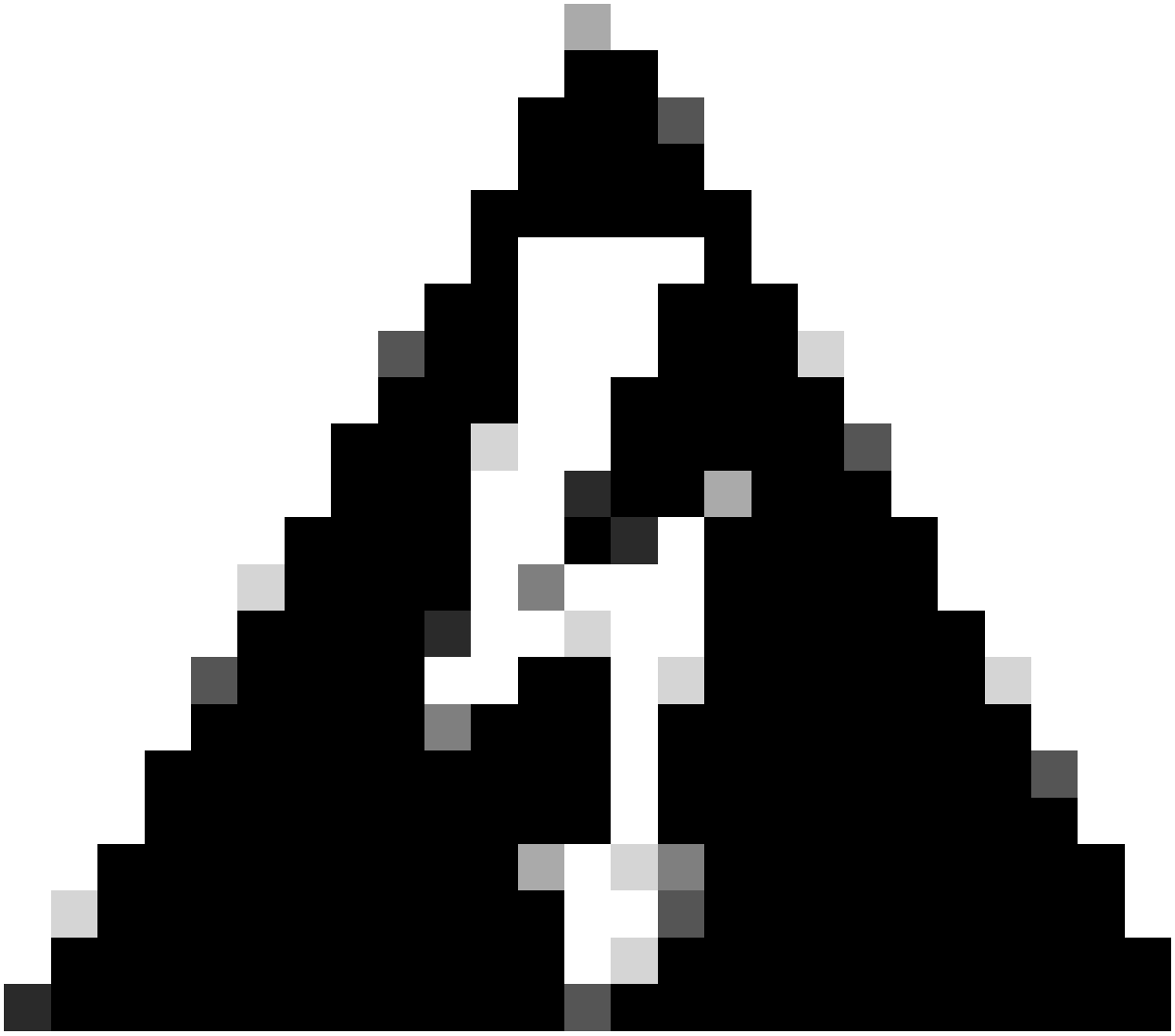
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
lifetime 00:00:00 Jun 1 2024 duration 864000	lifetime 00:00:00 Jun 1 202
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
key 02	key 02
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
cryptographic-algorithm aes-256-cmac	cryptographic-algorithm aes
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
key-string b5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e2	key-string b5b2df4657bd8c02
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
lifetime 23:00:00 Jun 1 2024 infinite	lifetime 23:00:00 Jun 1 202
8500-1(config-keychain-macsec-key)#	8500-2(config-keychain-macs
exit	exit
8500-1(config-keychain-macsec)#	8500-2(config-keychain-macs
exit	exit



ملاحظة: أثناء تكوين سلسلة مفاتيح MACsec، تذكر أن سلسلة المفاتيح يجب أن تتكون من أرقام سداسية عشرية فقط، تتطلب خوارزمية التشفير AES-128-cmac وجود مفتاح مكون من 32 رقم hex وخوارزمية AES-256-cmac المشفرة تتطلب مفتاح مكون من 64 رقم سداسية عشرية.



ملاحظة: تذكر أنه عند إستخدام مفاتيح متعددة، تكون هناك حاجة إلى فترة زمنية متداخلة فيما بينها لتحقيق إعادة توجيه للمفتاح بدون انقطاع بعد انتهاء مدة صلاحية المفتاح المحدد.



تحذير: من المهم التأكد من مزامنة ساعات كل الموجهين، وبالتالي، يوصى بشدة باستخدام بروتوكول وقت الشبكة (NTP). ويمكن أن يؤدي عدم القيام بذلك إلى منع إنشاء جلسات الهيئة أو التسبب في فشلها في المستقبل.

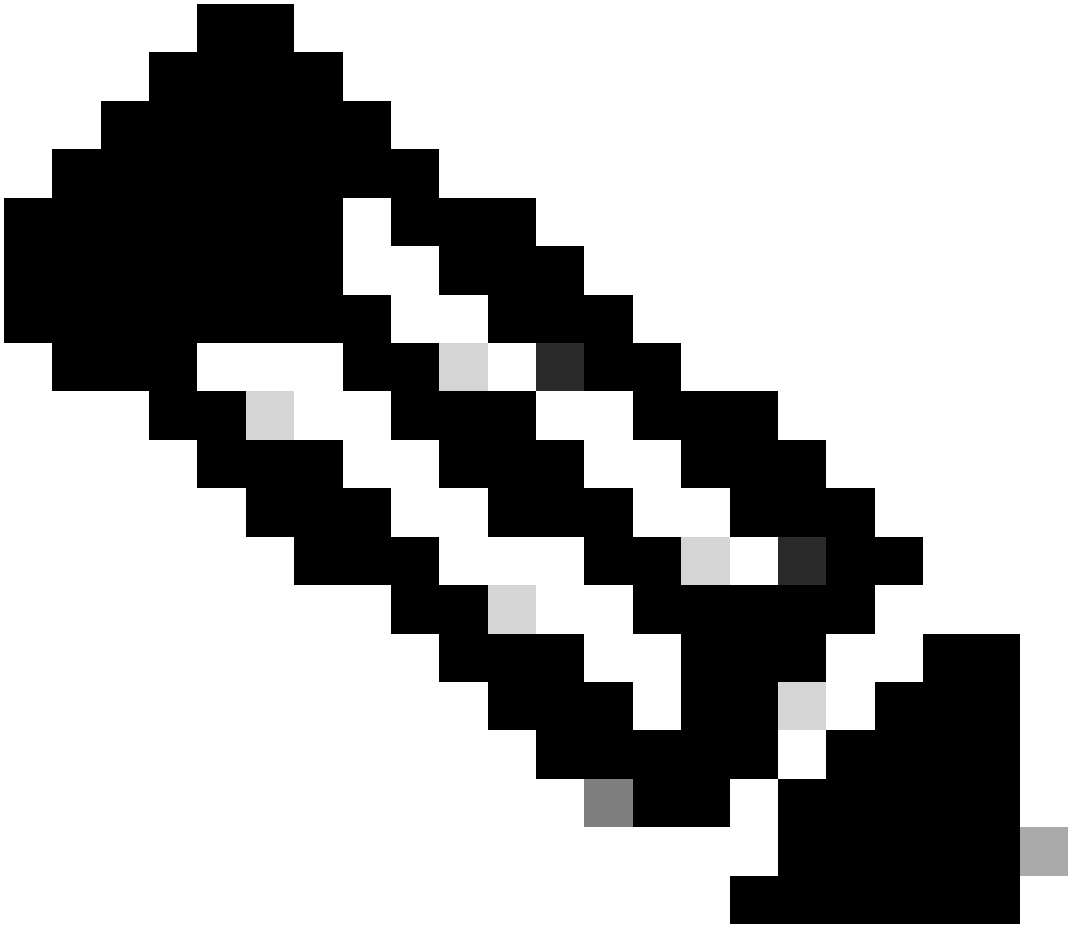
الخطوة 3: تكوين سياسة MKA

بينما يمكن أن تكون سياسة MKA الافتراضية مفيدة للإعداد الأولي والشبكات البسيطة، يوصى بشكل عام بتكوين سياسة MKA مخصصة لـ WAN MACsec لتلبية متطلبات الأمان والتوافق والأداء المحددة. توفر السياسات المخصصة قدرا أكبر من المرونة والتحكم، مما يضمن أن أمان الشبكة لديك يتسم بالقوة ويتم تخصيصه لتلبية إحتياجاتك.

عند تكوين سياسة MKA الخاصة بك، هناك عناصر مختلفة يمكن تحديدها، مثل أولوية خادم المفاتيح وحماية التأخير لوحدة بيانات حزمة إتفاقية مفتاح MACsec (MKPDU) ومجموعة التشفير، من بين عناصر أخرى. في هذا النظام الأساسي وإصدارات البرنامج يمكن إستخدام الشفرات التالية:

الوصف	تشفير MacSec

gcm-aes-128	وضع Galois/العداد (GCM) مع معيار التشفير المتقدم (AES) باستخدام مفتاح 128-بت
gcm-aes-256	وضع Galois/العداد (GCM) مع AES باستخدام مفتاح 256 بت (قوة تشفير أعلى)
gcm-aes-xpn-128	وضع Galois/العداد (GCM) مع AES باستخدام (XPN) مفتاح 128-بت، مع ترقيم حزم موسع
gcm-aes-xpn-256	وضع Galois/العداد (GCM) مع AES باستخدام مفتاح 256 بت، مع XPN (قوة تشفير أعلى)



ملاحظة: تعمل شبكة XPN على تحسين تشفير GCM-AES من خلال دعم ترقيم الحزم الأطول، والذي يحسن من الأمان للجلسات التي تستغرق وقتًا طويلاً جدًا أو البيئات التي تتطلب سعة معالجة عالية. يمكن أن يتسبب إستخدام الارتباطات عالية السرعة، على سبيل المثال، بسرعة 40 جيجابت في الثانية أو 100 جيجابت في الثانية، في مرور وقت قصير جدًا على مفتاح الشبكة لأن رقم الحزمة (PN) داخل إطار MACsec، والذي عادة ما يعتمد على عدد الحزم المرسلة، يمكن استنفاده بسرعة بهذه السرعات. تعمل شبكة XPN على توسيع تسلسل ترقيم الحزم وتقليل الحاجة إلى مفتاح اقتران الأمان المتكرر (SAK) الذي يمكن أن يحدث في الارتباطات عالية السعة.

في هذا المثال، التشفير المحدد لنهج MKA هو GCM-aes-xpn-256، والعناصر الأخرى ستكون لها القيمة الافتراضية:

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**

الخطوة 4: تكوين MACsec على مستوى الواجهة والواجهة الفرعية

في هذا السيناريو، على الرغم من أنه لم يتم تكوين الواجهة المادية باستخدام عنوان IP، إلا أنه يلزم تطبيق بعض أوامر macSEC على هذا المستوى لكي يعمل الحل. يتم تطبيق سياسة MACsec وسلسلة المفاتيح على مستوى الواجهة الفرعية (راجع مثال التكوين):

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** 8500-1(config)# **interface FortyGigabitEthernet0/2/4** 8500-1(config-if)# **mtu 9216** 8500-1(config-if)# **cdp enable** 8500-1(config-if)# **macsec dot1q-in-clear 1** 8500-1(config-if)# **macsec access-control should-secure** 8500-1(config-if)#	<#root> 8500-2# **configure terminal** 8500-2(config)# **interface FortyGigabitEthernet0/2/0** 8500-2(config-if)# **mtu 9216** 8500-2(config-if)# **cdp enable** 8500-2(config-if)# **macsec dot1q-in-clear 1** 8500-2(config-if)# **macsec access-control should-secure** 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**

الأوامر المطبقة على مستوى الواجهة المادية

أ. MTU إلى 9216 لأن مزود الخدمة المستخدم في المخطط يسمح بإطارات ضخمة، لكن هذا ليس متطلبا

b. يمكن الأمر macsec dot1q-in-clear الخيار أن يكون له علامة VLAN (dot1q) في clear (غير مشفر)

c. يسمح الأمر macSec control الوصول-secure بإرسال الحزم غير المشفرة من الواجهة المادية أو الواجهة الفرعية أو استقبالها (يلزم هذا الأمر إذا كانت بعض الواجهات الفرعية تتطلب التشفير والبعض الآخر لا تتطلب التشفير، وهذا يرجع إلى السلوك الافتراضي ل MACsec حيث لا يسمح بإرسال أي حزم غير مشفرة أو استقبالها من نفس الواجهة المادية حيث يتم تمكين MACsec)

الأوامر المطبقة على مستوى الواجهة الفرعية

a. الآن، يلزم الأمر eapol destination-address broadcast-address لتغيير عنوان MAC للوجهة من إطارات EAPoL (والذي يكون بشكل افتراضي عنوان MAC متعدد البث 01:80:C2:00:00:03) إلى عنوان MAC للبث للتأكد من أن مزود الخدمة يفيض عليهم ولا يسقطهم أو يستهلكهم.

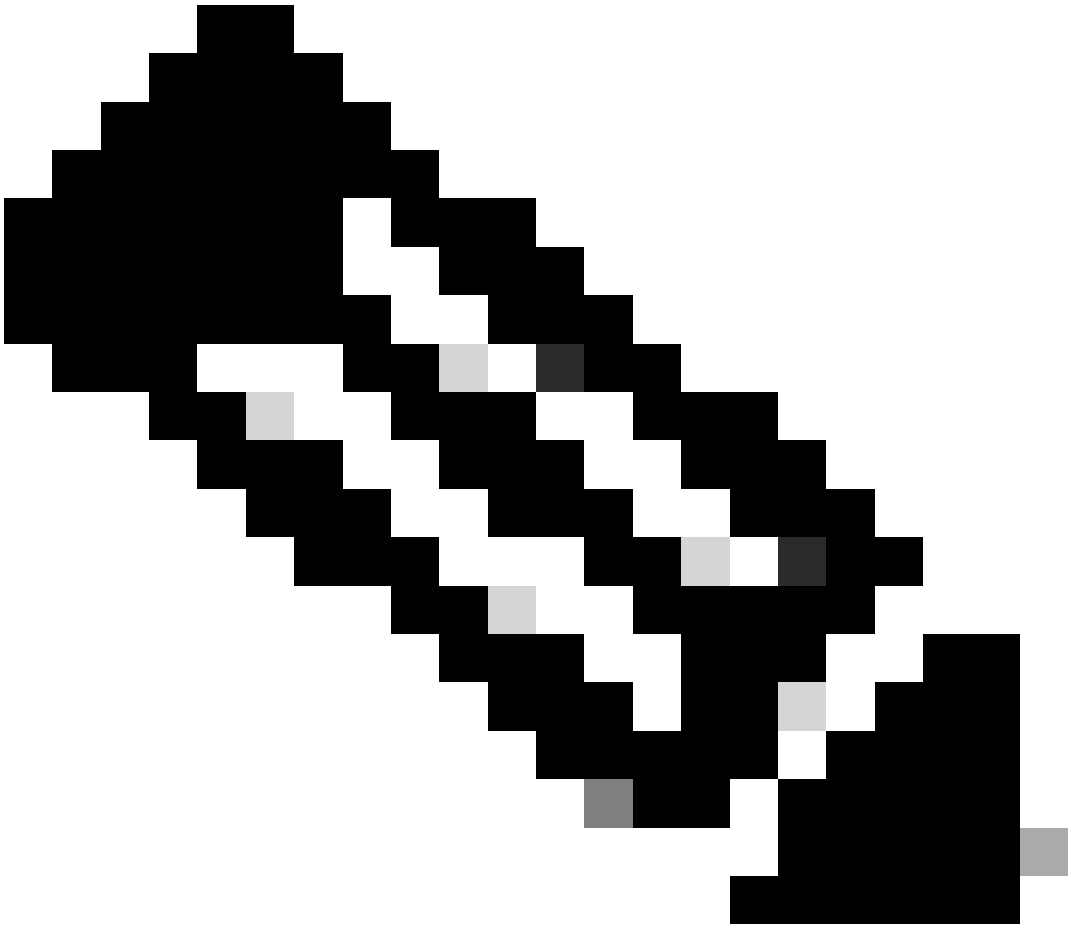
ب. يتم إستخدام الأمر eapol th-type 876F، كذلك لتغيير نوع إيثرنت الافتراضي لإطار EAPoL (والذي يكون بشكل افتراضي 0x888E) وتغييره إلى 0x876F. يلزم مرة أخرى هذا لمنع

مزود الخدمة من إسقاط هذه الإطارات أو إستهلاكها.

c. يتم إستخدام الأوامر mka policy <name> وmka pre-shared-key-series <key series name> لتطبيق السياسة المخصصة وسلسلة المفاتيح على الواجهة الفرعية.

د. وأخيرا وليس آخرا، فإن الأمر macSec يمكن MacSec على مستوى الواجهة الفرعية.

في الإعداد الحالي، ودون تغييرات EAPoL السابقة، لم تكن محولات 9500 في جانب مزود الخدمة تقوم بإعادة توجيه إطارات EAPoL.



ملاحظة: يتم توريث أوامر MACsec مثل dot1q-in-clear وshould-secure بواسطة الواجهات الفرعية. وبالإضافة إلى ذلك، يمكن تعيين أوامر EAPoL على مستوى الواجهة المادية، وفي هذه الحالات، يتم توريث هذه الأوامر أيضا بواسطة الواجهات الفرعية. ومع ذلك، فإن التكوين الصريح لأوامر EAPoL على الواجهة الفرعية يحل محل القيمة الموروثة أو النهج الخاص بتلك الواجهة الفرعية.

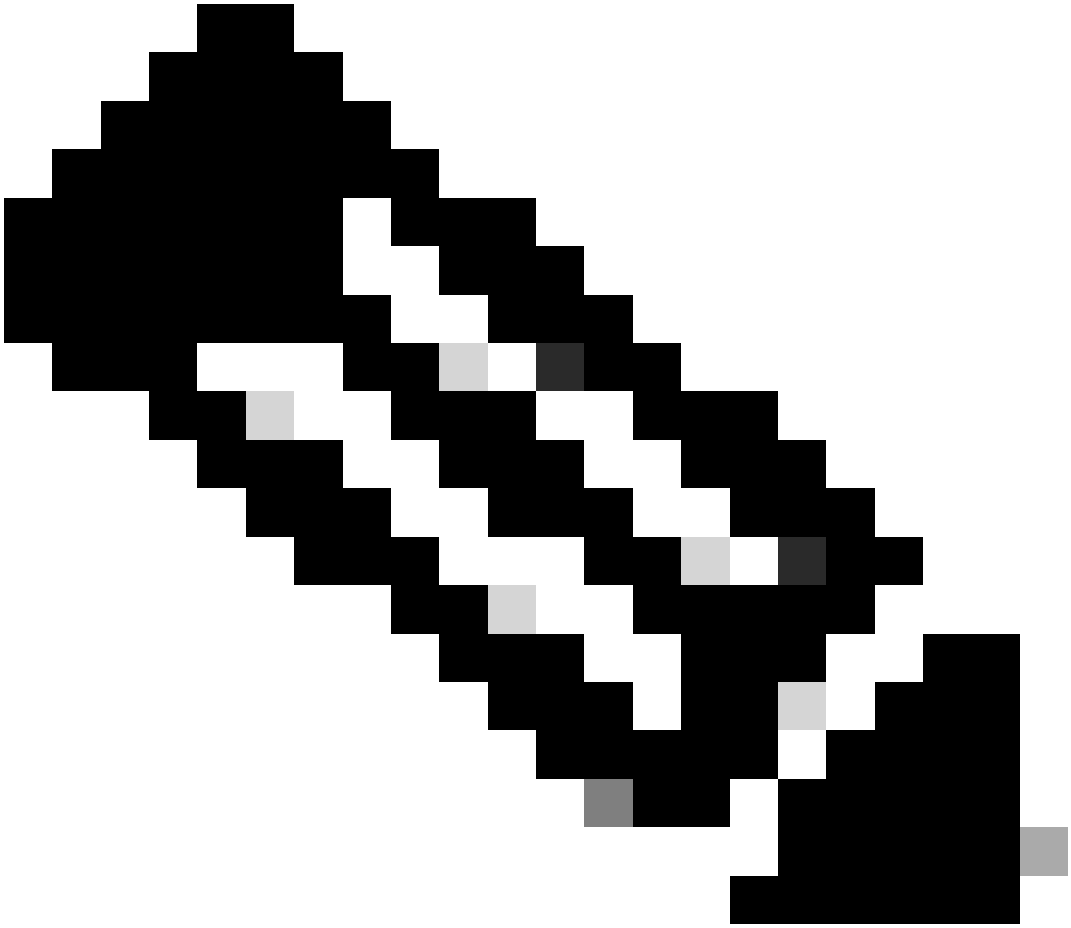
التحقق من الصحة

لكل من الصلة ذي تشغيله الجاري التكوين التالي الإخراج، يعرض تطبيق التكوين بمجرد (تم حذف بعض التكوين) Customer Edge (CE) C8500 من موجه من موجه:

```
<#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#
```



ملاحظة: لاحظ أنه بعد تمكين MACsec، من خلال تطبيق الأمر macSec، يتم ضبط 32 بايت لحساب مصروفات MacSec الإضافية.

بعد ذلك، يمكنك العثور على قائمة من الأوامر الأساسية التي يمكن إستخدامها للتحقق من حالة MACsec بين الأقران والتحقق منها. توفر كل هذه الأوامر معلومات تفصيلية حول جلسات عمل MACsec الحالية وسلاسل المفاتيح والسياسات والإحصائيات:

عرض mka جلسة - يعرض هذه أمر الحالي MKA جلسة وضع.

show mka جلسة تفصيلي - يوفر هذا الأمر معلومات تفصيلية حول كل جلسة MKA.

show mka keySeries - يعرض هذا الأمر سلاسل المفاتيح المستخدمة لـ MACsec والواجهة المعينة.

show mka policy - يعرض هذا الأمر السياسات المطبقة، والواجهات ومجموعة التشفير المستخدمة.

show mka summary - يوفر هذا الأمر ملخصا لجلسات عمل MKA والإحصائيات.

show macsec statistics interface <interface name> - يعرض هذا الأمر إحصائيات MACsec لواجهة محددة، ويساعد على تحديد ما إذا كانت حركة المرور المشفرة يتم إرسالها واستقبالها.

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
```

يعي إمكانية الوصول من الواجهات الفرعية المختلفة أمر ان اجح، بالإضافة إلى إمكانية الوصول بين الشبكات الفرعية 192.168.0.0/16. تظهر إختبارات الاتصال التالية الاتصال الناجح:

<#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#
```

بعد التقاط الحزم من إختبار ICMP على جهاز حافة الموفر (PE)، يمكنك مقارنة الإطارات المشفرة وغير المشفرة. لاحظ أن رأس MAC الخارجي لشبكة الإيثرنت هو نفسه على الك الإطارين، مع علامة تمييز dot1q مرئية. ومع ذلك، يعرض الإطار المشفر نوع EtherType من 0x88E5 (MACsec)، بينما يعرض الإطار غير المشفر نوع EtherType من 0x0800 (IPv4) مع معلومات بروتوكول ICMP:

Encrypted Frame 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]
```

معلومات ذات صلة

- تحسينات دعم WAN MACsec و MKA
- الابتكارات في تشفير الإنترنت (802.1ae - MacSec) لتأمين عمليات نشر WAN عالية السرعة (1-100GE)
- أستكشاف أخطاء WAN MACsec وإصلاحها على الموجهات

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).