أستكشاف أخطاء WAN MACsec وإصلاحها على الموجهات

المحتويات

المقدمة

يصف هذا المستند بروتوكول WAN MACsec الأساسي لمفهوم العملية واستكشاف أخطاء وإصلاحها. موجه Cisco IOS® XE

المتطلبات الأساسية

المتطلبات

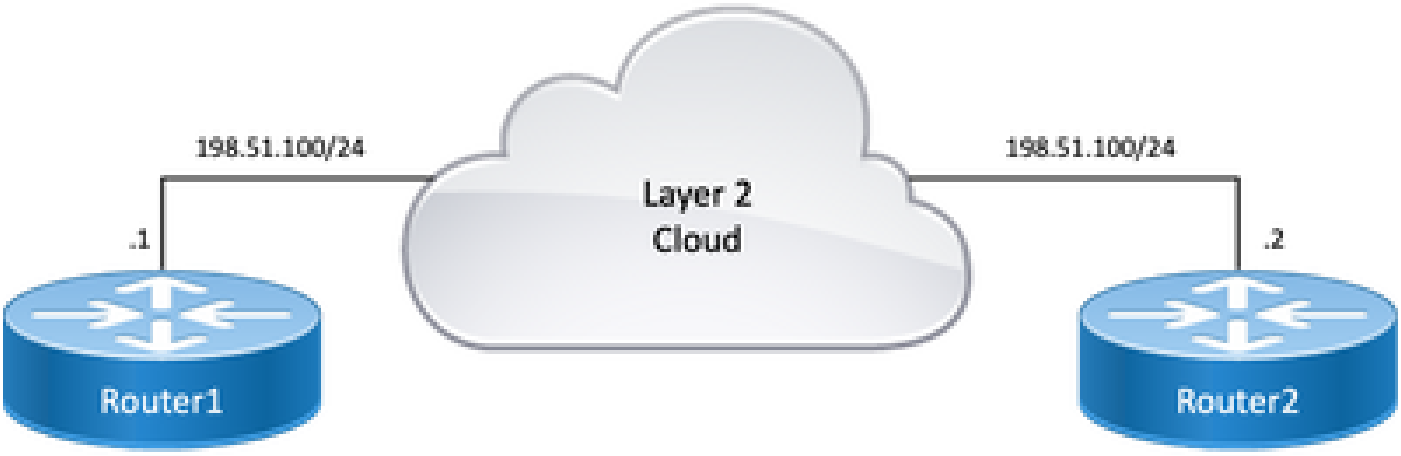
لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تكون المعلومات الواردة في هذه المستند محددة لموجهات Cisco IOS XE مثل أسر ASR 1000 و ISR 4000 و Catalyst 8000. ابحث عن دعم MACsec لأجهزة وبرامج معينة.

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

المخطط



مخطط الطوبولوجيا

نظرة عامة على MACsec لاستكشاف الأخطاء وإصلاحها

MACsec هو تشفير خطوة بخطوة من المستوى الثاني يستند إلى معيار IEEE 802.1AE يوفر سرية البيانات ونزاهة البيانات ومصادقة أصل البيانات للبروتوكولات المستقلة للوصول إلى الوسائط باستخدام تشفير AES-128، يمكن تأمين الارتباطات الأمامية فقط للمضيف (الارتباطات بين أجهزة الوصول إلى الشبكة وأجهزة النقطة الطرفية مثل جهاز الكمبيوتر الشخصي أو هاتف بروتوكول الإنترنت) باستخدام MACsec.

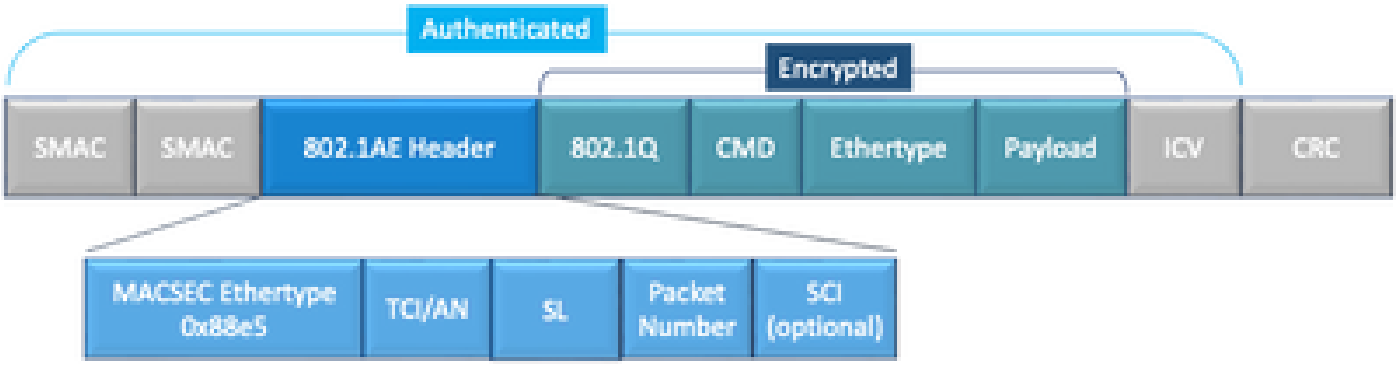
- يتم فك تشفير الحزم على منفذ الدخول.
- تكون الحزم واضحة في الجهاز.
- يتم تشفير الحزم على منفذ المخرج.

يوفر MacSec اتصال آمن على شبكات LAN السلكية، عندما يتم إستخدام MacSec لتأمين الاتصال بين نقاط النهاية على شبكة LAN، يتم تشفير كل حزمة على السلك باستخدام تشفير مفتاح متماثل، بحيث لا يمكن مراقبة الاتصال أو تغييره على السلك. عند إستخدام MACsec بالاقتران مع علامات مجموعة الأمان (SGTs)، فإنه يوفر حماية لعلامة التمييز مع البيانات الموجودة في حمولة الإطار.

يوفر MACsec تشفير طبقة MAC عبر الشبكات السلكية باستخدام طرق خارج النطاق للتردد لتشفير keing.

تنسيق حزمة MacSec

باستخدام 802.1ae (MacSec)، يتم تشفير الإطارات وحمايتها باستخدام قيمة تحقق من التكامل (ICV) دون تأثير على IP MTU أو التجزئة والحد الأدنى لتأثير MTU من المستوى الثاني: ما يقرب من 40 بايت (أقل من إطار الطفل العملاق).



مثال تنسيق حزمة Macsec

- MacSec EtherType: 0x88e5، يعيّن أن الإطار هو إطار MacSec.
- TCI/AN: معلومات التحكم في العلامات/رقم الاقتران. وهو رقم إصدار MACsec إذا تم إستخدام السرية أو التكامل منفردين.
- sl: طول البيانات المشفرة.
- PN: رقم الحزمة المستخدم لحماية إعادة التشغيل.
- SCI: معرف قناة الأمان. كل توصيل اقتران (CA) وهو منفذ ظاهري (عنوان MAC للواجهة المادية بالإضافة إلى معرف منفذ 16-بت).
- ICV: قيمة التحقق من السلامة.

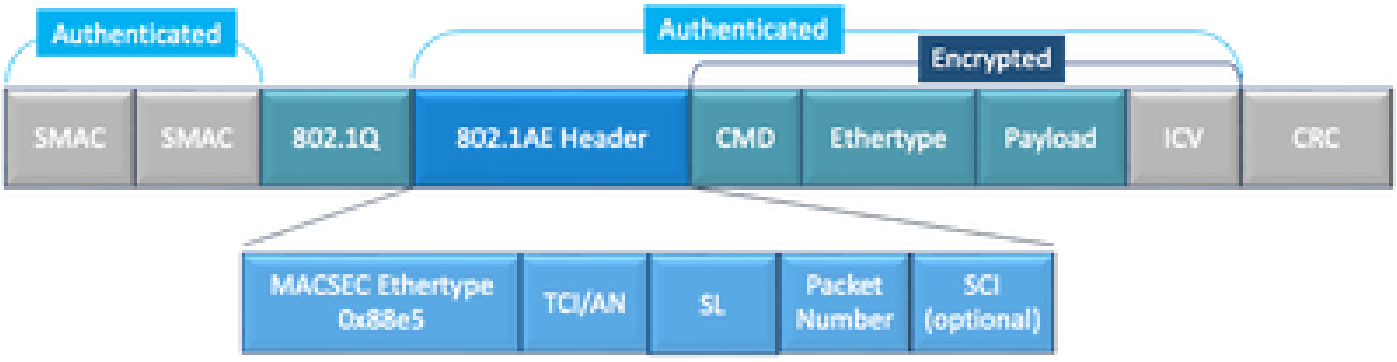
WAN-MACSEC

تطورت شبكة إيثرنت إلى ما هو أبعد من النقل عبر شبكة LAN الخاصة، لتتضمن مجموعة متنوعة من خيارات النقل عبر شبكة WAN أو MAN. يوفر بروتوكول WAN MACsec تشفيرا شاملا عبر خدمة شبكة إيثرنت WAN من الطبقة 2 إما من نقطة إلى نقطة أو من نقطة إلى عدة نقاط باستخدام AES 128 أو 256-بت.

يستند WAN MacSec إلى (LAN) MacSec، وبالتالي الاسم (ومنفصل عن IPsec)، ولكنه يوفر العديد من الإمكانيات الإضافية غير المتاحة سابقا.

تنسيق حزمة WAN MACsec

هناك أحتمالية أن موفر الخدمة ال يدعم MacSec etherType وال يمكنه التمييز بين خدمة L2 إذا تم تشفير العلامة بحيث يقوم WAN MACsec بتشفير كل الإطار بعد رؤوس 802.1Q:



علامة WAN MACSEC 802.1Q في مثال مسح تنسيق الحزمة

يتضمن أحد التحسينات الجديدة علامات 802.1Q في Clear (المعروف أيضا باسم

ClearTag). يتيح هذا التحسين إمكانية عرض علامة 802.1Q خارج رأس MACsec المشفر. يوفر الكشف عن هذا الحقل العديد من خيارات التصميم مع MACsec، وفي حالة موفري نقل Carrier Ethernet العام، يكون ذلك ضروريا للاستفادة من خدمات نقل معينة.

يوفر دعم ميزة MKA معلومات الاتصال النفقي مثل علامة VLAN (علامة 802.1Q) في الوضوح بحيث يمكن لموزعي الخدمة توفير تجميع الخدمة بحيث يمكن للمداخلات المتعددة النقاط إلى VLAN فرعي على بناء وتختلف واحدة مادية واجهة على شبكات تتعايش أن طاقات النقاط المتعددة أو نقطة المرئي الآن.

بالإضافة إلى تجميع الخدمات، تتيح علامة VLAN في clear أيضا لموزعي الخدمة توفير جودة الخدمة (QoS) لحزمة الإيثرنت المشفرة عبر شبكة SP استنادا إلى حقل 802.1P (CoS) الذي يظهر الآن كجزء من علامة 802.1Q.

مصطلحات WAN MACsec

MKA	إتفاقية مفتاح MACec، المعرفة في IEEE 802.1XREV-2010 - بروتوكول الاتفاقية الأساسية لاكتشاف نظائر MACec ومفاتيح التفاوض.
إم إس كي	مفتاح الجلسة الرئيسية، يتم إنشاؤه أثناء تبادل EAP. يستخدم ملقم الطلب والمصادقة MSK لإنشاء CAK
كاك	يتم اشتقاق مفتاح اقتران الاتصال من MSK. مفتاح رئيسي طويل العمر يستخدم لإنشاء كافة المفاتيح الأخرى المستخدمة ل MACec.
CKN	اسم مفتاح اقتران الاتصال - يحدد CAK.
كاس	مفتاح الاقتران الآمن - مشتق من CAK وهو المفتاح المستخدم من قبل المتلقي والمحول لتشفير حركة مرور البيانات لجلسة عمل معينة.
كس	الخادم الرئيسي المسؤول عن: • تحديد مجموعة شفرة والإعلان عنها • إنشاء SAK من CAK.
كيك	مفتاح تشفير المفتاح - يستخدم لحماية مفاتيح MacSec (SAK)

نظرة عامة على بروتوكول إتفاقية المفاتيح (MKA) وتشفير MACSEC

MKA هو آلية مستوى التحكم المستخدمة من قبل WAN MacSec؛ محدد في IEEE Std 802.1X الذي يكتشف نظائر MACsec المصدق عليها بشكل متبادل بالإضافة إلى الإجراءات التالية:

- إنشاء CA (اقتران الاتصال) وإدارته.
- إدارة قائمة النظراء المباشرة/المحتملة.
- تفاوض مجموعة التشفير.
- يختار الخادم الرئيسي (KS) بين أعضاء المرجع المصدق.
- اشتقاق مفتاح الاقتران الآمن (SAK) وإدارته.
- توزيع المفتاح الآمن.

- تثبيت المفتاح.
- ريكي.

يتم إختيار وضع واحد كخادم أساسي استنادا إلى أولوية خادم المفاتيح التي تم تكوينها (الأقل)، إذا كانت أولوية KS هي نفسها بين الأقران، فعندئذ تكون أقل SCI هي الفائزة.

إن بنك كيه إس ال يولد جاجز إلا بعد أن يصبح كل أقرانه المحتملين على قيد الحياة وبعد أن يصبح هناك كاهن واحد على الأقل على قيد الحياة. إنه يوزع ال SAK والشفرة المستخدمة للمشاركين الآخرين باستخدام MKA PDU أو MKPDU بتنسيق مشفر.

يتحقق المشاركون من الشفرة المرسلة من قبل SAK ويركبونها إذا كانت مدعومة، ويستخدمونها على كل MKPDU للإشارة إلى أحدث مفتاح لديهم، وإلا فإنهم يرفضون SAK

عندما لا يتم تلقي MKPDU من المشاركين بعد 3 مرات تلقائيا (كل مرات تلقائيا 2 ثانية بشكل افتراضي)، يتم حذف النظراء من قائمة النظراء المباشرة؛ على سبيل المثال، إذا تم قطع اتصال أحد العملاء، يستمر المشارك على المحول في تشغيل MKA إلى أن تنتهي 3 مرات تلقائيا بعد تلقي آخر MKPDU من العميل.

لهذه العملية، هناك طريقتان لتشغيل مفاتيح التشفير:

- المفاتيح المشتركة مسبقا
- 802.1x/EAP

المفاتيح المشتركة مسبقا

إذا كنت تستخدم مفاتيح مشتركة مسبقا، فيجب إدخال CAK=PSK و CKN يدويا. بالنسبة لتقلب المفتاح، تأكد من أن لديك مرور وقت انتهاء المفتاح القديم وإدخال المفتاح التالي لأجل:

- قم بتبادل مفتاح SAK الجديد وتثبيته وربطه ب SA الداخلي.
- قم بإزالة مفتاح SAK القديم وتخصيص SA داخلي جديد.

مثال التكوين:

<#root>

```
key chain
```

M_Key

```
 macsec
```

key 01

```
   cryptographic-algorithm
```

aes-128-cmac

```
  key-string
```

12345678901234567890123456789001

```
   lifetime 12:59:59 Oct 1 2023 duration 5000
 key 02
   cryptographic-algorithm aes-128-cmac
```

```
  key-string 12345678901234567890123456789002
   lifetime 14:00:00 Oct 1 2023 16:15:00 Oct 1 2023
 key 03
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789003
   lifetime 16:15:00 Oct 1 2023 17:15:00 Oct 1 2023
  key 04
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
   lifetime 17:00:00 Oct 1 2023 infinite
```

حيث تشير الكلمات الجريئة إلى:
M_Key: اسم سلسلة المفاتيح.

المفاتح 01: اسم مفاتح اقتران الاتصال (مثل CKN).

AES-128-CMAC: تشفير مصادقة MKA.

12345678901234567890123456789012: مفاتح اقتران الاتصال (CAK).

تحديد النهج:

<#root>

```
mka policy example
 macsec-cipher-suite
```

gcm-aes-256

أين يشير GCM-aes-256 إلى مجموعة (مجموعات) تشفير التشفير مفاتح الارتباط الآمن (SAK).

ملاحظة: هذا هو التكوين الأساسي للسياسات، وهناك المزيد من الخيارات مثل موازنة السرية، وsak-rekey، و include-icv-indicator، والمزيد متاحة للاستخدام يتوقف على التنفيذ.

الواجهة:

```
interface TenGigabitEthernet0/1/2
 mtu 2000
 ip address 198.51.100.1 255.255.255.0
 ip mtu 1468
 eapol destination-address broadcast-address
 mka policy example
 mka pre-shared-key key-chain M_Key
 macsec
end
```

ملاحظة: في حالة عدم تكوين نهج MKA أو تطبيقه، يتم تمكين النهج الافتراضي ويمكن مراجعته عبر تفاصيل النهج الافتراضية لـ MKA.

802.1x/EAP

إذا كنت تستخدم أسلوب EAP، فإنه يتم إنشاء كل المفاتيح من مفتاح الجلسة الرئيسية (MSK). باستخدام إطار عمل بروتوكول المصادقة الموسع (EAP) وفق IEEE 802.1X، يقوم MKA بتبادل إطارات EAPoL-MKA بين الأجهزة، ويكون عون Ether لإطارات EAPoL وهو 0x888E بينما يشار إلى نص الحزمة في وحدة بيانات بروتوكول EAPOL (PDU) على أنه PDU لاتفاقية مفاتيح MacSec (MKPDU). تحتوي إطارات EAPoL هذه على CKN الخاص بالمرسل، وأولوية الخادم الرئيسي، وقدرات MACsec.

ملاحظة: تقوم المحولات بشكل افتراضي بمعالجة إطارات EAPoL-MKA ولكنها لا تقوم بإعادة توجيهها.

مثال تكوين تشفير MacSec المستند إلى الشهادة:

تسجيل الشهادة (يتطلب المرجع المصدق):

```
  crypto pki trustpoint EXAMPLE-CA
   enrollment terminal
   subject-name CN=ASR1000@user.example, C=IN, ST=KA, OU=ENG,O=Example
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:

  crypto pki authenticate EXAMPLE-CA
```

يلزم توفر مصادقة وفق لمعيار 802. 1x وتهيئة المصادقة والتفويض والمحاسبة (AAA):

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4  auth-port 1645 acct-port 1646
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

تصيف EAP-TLS ومسوغات 802. 1X:

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint EXAMPLE-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@user.example
 pki-trustpoint EXAMPLE-CA
!
```

الواجهة:

```
interface TenGigabitEthernet0/1/2
 macsec network-link
 authentication periodic
 authentication timer reauthenticate
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

أستكشاف أخطاء WAN MACsec وإصلاحها

التكوين

تحقق من صحة التكوين ودعم التنفيذ على حسب النظام الأساسي، ويجب أن تتطابق المفاتيح والمعلمات. بعض من ال log أن يعين إن هناك مشكلة على تشكيل أن التالي يكون:

```
%MKA-3-INVALID_MACSEC_CAPABILITY : Terminating MKA Session because no peers had the required MACsec Cap
```

تحقق من قدرة MacSec الخاصة بالأجهزة النظيرة أو قم بتقليل متطلبات قدرة MacSec من خلال تغيير تكوين MacSec للواجهة.

```
%MKA-3-INVALID_PARAM_SET : %s, Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s
```

هناك بعض المعلمات الاختيارية التي يمكن للموجه توقعها أو التي لا يمكن توقعها
استنادا إلى التكوين والإعدادات الافتراضية المختلفة للنظام الأساسي، تأكد من
تضمينها أو تجاهلها على التكوين.

```
%MKA-4-MKA_MACSEC_CIPHER_MISMATCH: Lower/Higher strength MKA-cipher than macsec-cipher for RxSCI %s, Au
```

هناك عدم تطابق في التكوين على مجموعة تشفير النهج، تأكد من التطابق المناسب.

```
%MKA-3-MKPDU_VALIDATE_FAILURE : MKPDU validation failed for Local-TxSCI %s, Peer-RxSCI %s, Audit-Sessio
```

فشل MKPDU في واحد أو أكثر من عمليات التحقق التالية من الصحة:

- عنوان MAC وعنوان EAPOL صالح: تحقق من تكوين كل الواجهات، يمكن أن يدعم التطاق
  الحزمة على واجهة الدخول القيم الحالية.
- CKN ومرونة الخوارزمية الصحيحتين: تأكد من صحة المفاتيح ومجموعات الخوارزميات.
- التحقق من ICV: التحقق من ICV عبارة عن معلمة إختيارية، ويجب أن تتطابق كل
  نهايتي التكوين.
- وجود أمر صحيح لحمولات MKA: مشكلة قابلية التشغيل البيني المحتملة.
- التحقق من MI في حالة وجود نظائر: التحقق من معرف العضو، فريد لكل مشارك.
- التحقق من MN في حالة وجود نظائر: التحقق من رقم الرسالة، فريد على كل وحدة
  بيانات MKPDU يتم إرسالها وزيادات على كل عملية إرسال.

رابعا - المسائل التشغيلية

بمجرد تعيين التكوين، يمكنك الاطلاع على رسالة MKA-5-SESSION_START٪ ولكن يجب
التحقق من ظهور جلسة العمل، أحد الأوامر الجيدة للبدء بها هو show mka session [interface
_name]:

<#root>

```
Router1#
```

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
=============================================================================================
Te0/1/2         40b5.c133.0e8a/0012
```

Example

NO

NO

18 40b5.c133.020a/0012 1

Secured

01

تشير الحالة إلى جلسة مستوى التحكم، ويعني Secure أن Rx و Tx SAK يتم تثبيتهما، إذا لم يكن كذلك، ثم تظهر غير مؤمنة.

- إذا ظلت الحالة على Init، فحص القارن طبيعي دولة، موصولية عن طريق إختبار الاتصال لنظراء ومطابقة تشكيل. عند هذه النقطة ال توجد وحدات بيانات MKPDU موقت ال امني بين التحميل بالأساسية الأنظمة بعض موقت و، مباشرة قران وأ مستلمة بعض الأنظمة الأخرى بذلك، ويتم التعامل مع ما يصل إلى 32 بايت من مصروفات الرأس والتأكد من وجود وحدة الحد الأقصى للنقل (MTU) أكبر للتشغيل السليم.
- إذا ظلت الحالة في حالة تعليق، فتحقق مما إذا كان يتم إسقاط MKPDU إما مدخل أو مخرج في مستوى التحكم أو أخطاء/عمليات إسقاط الواجهات.
- إذا بقيت الحالة على غير مؤمن، MKA قارن فوق و MKPDUs يتدفق من خلال لكن SAK لم يتم تثبيته، في هذه الحالة يظهر السجل التالي:

```
%MKA-5-SESSION_UNSECURED : MKA Session was not secured for Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionI
```

يرجع السبب في ذلك إلى عدم دعم MACsec أو تكوين MACsec غير صالح أو فشل MKA آخر على الجانب المحلي أو النظير قبل إنشاء قناة آمنة (SC) وتثبيت الاقترانات الآمنة (SA) في MACsec. يمكنك إستخدام الأمر detail للحصول على مزيد من المعلومات show mka session [interface interface_name] detail:

<#root>

```
Router1#
```

show mka sessions detail

```
MKA Detailed Status for MKA Session
===================================
```

Status: SECURED - Secured MKA Session with MACsec

```
Local Tx-SCI............. 40b5.c133.0e8a/0012
```

```
Interface MAC Address.... 40b5.c133.0e8a
MKA Port Identifier...... 18
Interface Name........... TenGigabitEthernet0/1/2
Audit Session ID.........

CAK Name (CKN)........... 01

Member Identifier (MI)... DC5F7E3E38F4210925AAC8CA
Message Number (MN)...... 14462
EAP Role................. NA
Key Server............... NO

MKA Cipher Suite......... AES-128-CMAC


Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... 272DA12A009CD0A3D313FADF00000001 (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.......... Example
Key Server Priority...... 2
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......... 0080C20001000002 (GCM-AES-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
  ------------------------------------------------------------------------------------
  272DA12A009CD0A3D313FADF  14712       40b5.c133.020a/0012  1         YES            0


Potential Peers List:
  MI                       MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                            Priority  Installed
  ------------------------------------------------------------------------------------
```

ابحث عن معلومات SAK عن الأقران والبيانات ذات الصلة التي يتم إبرازها لفهم الوضع بشكل أفضل، إذا كان هناك SAK مختلف في موضع، وأفحص خيارات المفاتيح المستخدمة وخيارات العمر الافتراضي أو خيارات مفاتيح SAK المكونة، إذا تم إستخدام المفاتيح المشتركة مسبقا، يمكنك إستخدام سلاسل مفاتيح show mka:

<#root>

```
Router1#

show mka keychains


MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                          Interface(s)
Name             Latest CAK                                                          Applied
===============================================================================================

Master_Key


01

                                                                          Te0/1/2
                 <HIDDEN>
```

لم يتم عرض CAK فقط ولكن يمكنك تأكيد اسم سلسلة المفاتيح و CKN.

إن تصحف يغبني تنأ ،عطقتم رورم ةكرح قفدت وأ تارج كيدل نكلو لمع ةسلج ءاشنإ مت اذإ MKPDUs قفدتي لكشب صحيح بين الأقران، إن هناك مهلة، أنت يستطيع رأيت الرسالة التالية:

```
%MKA-4-KEEPALIVE_TIMEOUT : Keepalive Timeout for Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s, CKN
```

إذا كان هناك نظير واحد، MKA يتم إنهاؤه جلسة، في حالة أن كيدل العديد من الأقران وMKA لم يستلم MKPDU من أحد الأقران لأكثر من 6 ثوان، يتم إزالة Live Peer من قائمة الأقران الأحياء، يمكنك البدء بإحصائيات show mka [interface_name]:

<#root>

```
Router1#

show mka statistics interface TenGigabitEthernet0/1/2


MKA Statistics for Session
==========================
Reauthentication Attempts.. 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..... 0
   SAKs Received..... 1
   SAK Responses Received.. 0

MKPDU Statistics


MKPDUs Validated & Rx... 11647

      "Distributed SAK".. 1
      "Distributed CAK".. 0


MKPDUs Transmitted..... 11648

      "Distributed SAK".. 0
      "Distributed CAK".. 0
```

يجب أن يكون لـ MKPDUs التي يتم إرسالها واستقبالها أرقام مماثلة لنظير واحد، تأكد من زيادتها في كل النهايتين Rx و Tx، لتحديد وجهة الإتجاه المسبب، إذا كانت هناك إختلافات يمكنك تمكين تصحيح أخطاء mka linkSec من كل النهايتين:

```
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
*Sep 20 21:14:12.101: MKA-LLI-MKPDU: MKPDU transmitted: Interface [Te0/1/2: 18] with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
```

في حالة عدم إستلام وحدات بيانات بروتوكول الجسر (MKPDU)، ابحث عن أخطاء الواجهة الواردة أو عمليات الإسقاط، حالة واجهات الأقران وجلسة عمل MKA؛ في حالة وجود كل الموجهين قيد الإرسال و الى يتم الاستلام، يتم فقد وحدات بيانات بروتوكول الجسر (MKPDU) على الوسائط ويلزم فحص الأجهزة الوسيطة لإعادة التوجيه الصحيحة.

إذا لم تكن ترسل وحدات بيانات بروتوكول الجسر (MKPDUs)، فتحقق من حالة الواجهة المادية (الخط والأخطاء/عمليات الإسقاط) والتكوين، وفحص ما إذا كنت تقوم بإنشاء هذه الحزم على مستوى مستوى التحكم، فتتبع FIA والتقاط الحزم المضمن (EPC) هو أداة يمكن الاعتماد عليها لهذا الغرض. ارجع إلى [أستكشاف الأخطاء وإصلاحها باستخدام ميزة تعقب حزمة بيانات Cisco IOS XE]

يمكنك إستخدام أحداث debug mka والبحث عن أسباب يمكن أن ترشد الخطوات التالية.

ملاحظة: يرجى الاستخدام مع توخي الحذر لتشخيصات MKA وتصحيح الأخطاء MKA أثناء إظهارها لجاز الحالة ومعلومات تفصيلية للغاية يمكن أن تتسبب في حدوث مشاكل في مستوى التحكم على الموجه.

إذا كانت الجلسة آمنة ومستقرة ولكن حركة المرور لا تتدفق، فتحقق من حركة المرور المشفرة التي ترسل الى النظامين:

```
<#root>
```

```
Router1#
```

show macsec statistics interface TenGigabitEthernet 0/1/2

```
MACsec Statistics for TenGigabitEthernet0/1/2
 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: 98020

```
  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0
```

Egress Encrypted Octets: 98012

```
 Controlled Port Counters
  IF In Octets:             595380
  IF In Packets:            5245
  IF In Discard:            0
  IF In Errors:             0
  IF Out Octets:            596080
  IF Out Packets:           5254
  IF Out Errors:            0

 Transmit SC Counters (SCI: 40B5C1330E8B0013)
  Out Pkts Protected:       0
```

Out Pkts Encrypted: 970

```
 Transmit SA Counters (AN 0)
  Out Pkts Protected:       0
```

Out Pkts Encrypted: 970

```
 Receive SA Counters (SCI: 40B5C133020B0013  AN 0)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
```

In Pkts OK: 967

In Pkts Invalid: 0

```
  In Pkts Not Valid:        0
  In Pkts Not using SA:     0
  In Pkts Unused SA:        0
  In Pkts Late:             0
```

عدادات SecY هي الحزم الحالية على الواجهة المادية، بينما تتعلق الأخرى بقناة Tx الآمنة تعني الحزم التي يتم تشفيرها وإرسالها والقتران الآمن Rx يعني الحزم الصالحة التي يتم استقبالها على الواجهة.

يساعد المزيد من تصحيح الأخطاء مثل أخطاء mka debug وحزم mka debug على تحديد المشكلات، يرجى إستخدام هذه الأخيرة مع الاحتياط كما يمكن أن تحث على التسجيل المكثف.

معلومات ذات صلة

- دليل تكوين MacSec و MKA
- الدعم التقني والتنزيلات من Cisco

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).