Probleemoplossing voor WAN MACSEC op routers

Inhoud

Inleiding

Dit document beschrijft basis-WAN MACSEC-protocol om werking en probleemoplossing voor Cisco IOS® XE-routers te begrijpen.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

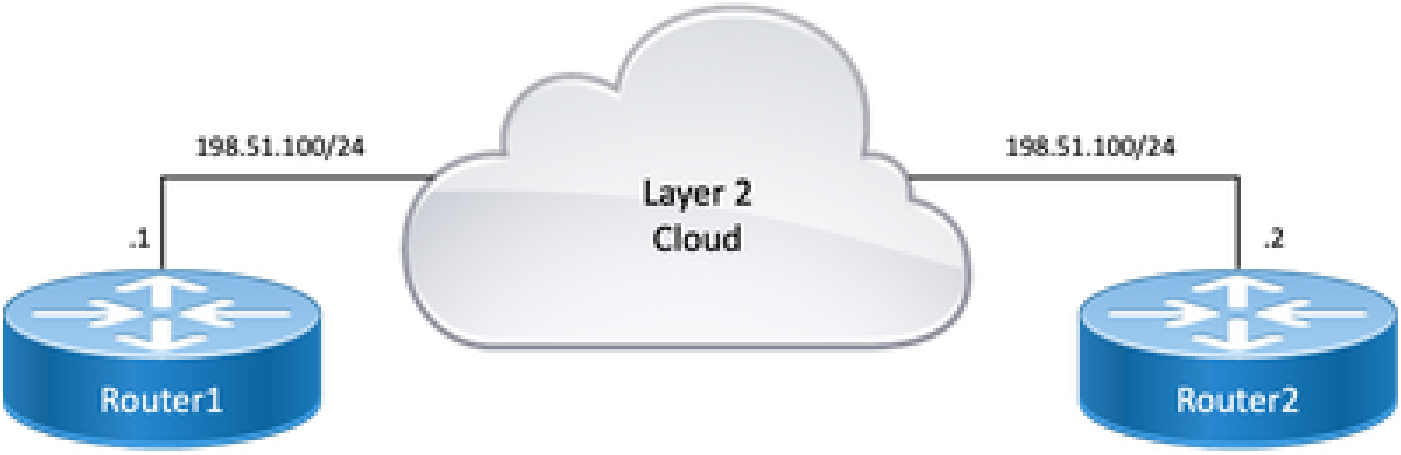
Gebruikte componenten

De informatie in dit document is specifiek voor Cisco IOS XE-routers zoals ASR 1000, ISR 4000 en Catalyst 8000-families. Zoek naar specifieke hardware en software voor MACSEC ondersteuning.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Topologiediagram

MACSEC - Overzicht voor probleemoplossing

MACsec is een IEEE 802.1AE-standaard gebaseerde Layer 2 hop-by-hop-encryptie die gegevensvertrouwelijkheid, gegevensintegriteit en authenticatie van de dataoorsprong biedt voor mediatransformatie onafhankelijke protocollen met AES-128-encryptie, alleen host-georiënteerde links (koppelingen tussen netwerktoegangsapparaten en endpointapparaten zoals een PC of IP-telefoon) kunnen worden beveiligd met MACsec.

- Pakketten worden gedecrypteerd op toegangspoorten.
- De pakketten zijn duidelijk in het apparaat.
- De pakketten zijn versleuteld op de uitgangspoort.

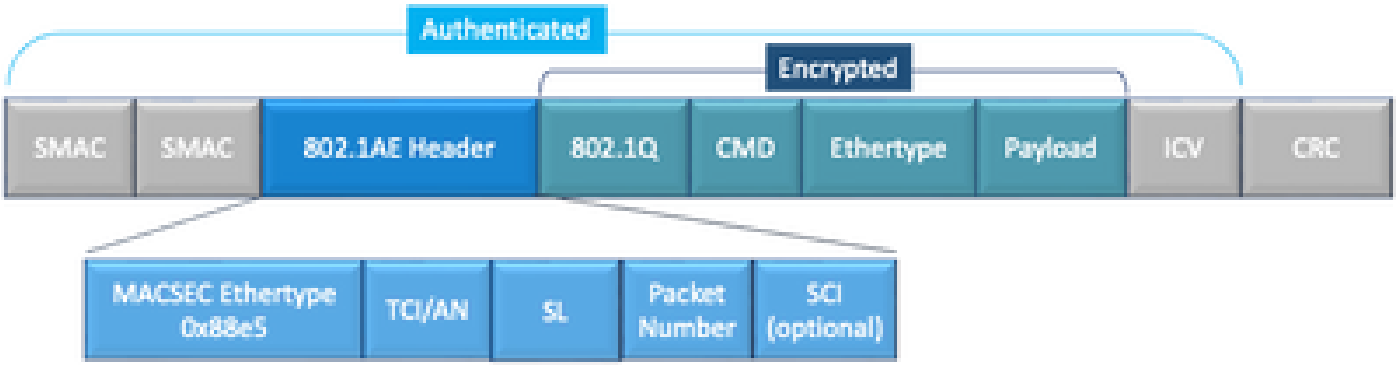
MACsec biedt beveiligde communicatie via bekabelde LAN's wanneer MACsec wordt gebruikt om de communicatie tussen eindpunten op een LAN te beveiligen, wordt elk pakket op de bedrading versleuteld met symmetrische sleutelcryptografie, zodat de communicatie niet via de bedrading kan worden bewaakt of gewijzigd. Wanneer MACsec wordt gebruikt in combinatie met security group tags (SGTs), biedt het bescherming voor de tag samen met de gegevens in de payload van het frame.

MACsec biedt MAC-Layer versleuteling via bekabelde netwerken door out-of-band methoden voor versleuteling te gebruiken.

MACsec-pakketindeling

Met 802.1AE (MACsec) worden frames versleuteld en beveiligd met een

integriteitscontrolewaarde (ICV) zonder impact op IP MTU of fragmentatie en minimale L2 MTU impact: ~40 bytes (minder dan gigantisch babyframe).



Voorbeeld van MACSEC-pakketindeling

- MACsec EtherType: 0x88e5, wijst aan dat frame een MACsec frame is.
- TCI/AN: TAG Control Information/Association Number. Is het MACsec-versienummer indien vertrouwelijkheid of integriteit alleen worden gebruikt.
- SLB: lengte van de versleutelde gegevens.
- PN: pakketnummer gebruikt voor bescherming tegen terugspelen.
- SCI: Secure Channel-id. Elke connectiviteitsassociatie (CA) is een virtuele poort (MAC-adres van de fysieke interface plus 16-bits poort-ID).
- ICV: integriteitscontrolewaarde.

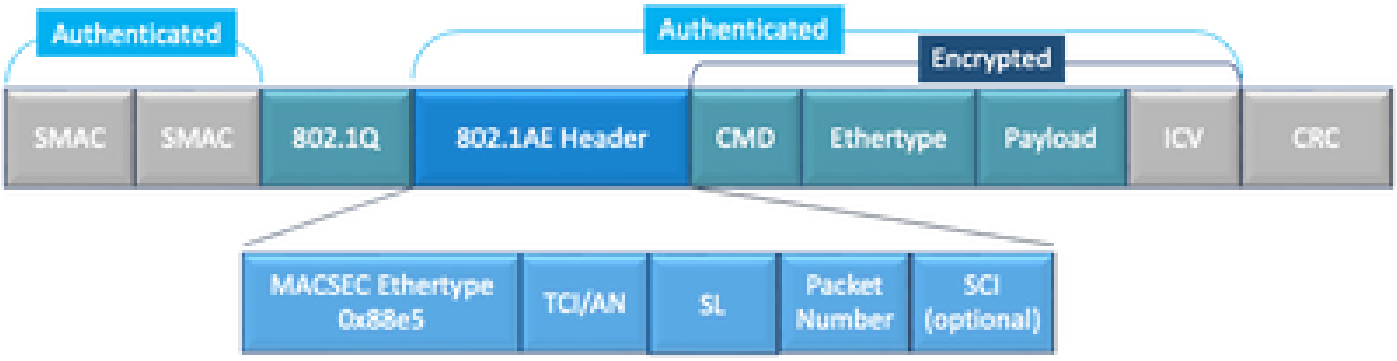
WAN-MACSEC

Ethernet is verder geëvolueerd dan een privaat LAN-transport en omvat nu een groot aantal WAN- of MAN-transportopties. WAN MACSEC biedt end-to-end codering via Layer 2 Ethernet WAN-service, point-to-point of point-to-multipoint, met behulp van AES 128 of 256-bits.

WAN MACsec is gebaseerd op (LAN) MACsec, vandaar de naam (en gescheiden van IPsec), maar biedt verschillende extra mogelijkheden die niet eerder beschikbaar zijn.

WAN MACSEC-pakketindeling

Er is een mogelijkheid dat serviceproviders MACsec ethertype niet ondersteunen en L2-service niet kunnen differentiëren als de tag is versleuteld, zodat WAN MACSEC alle frame na 802.1Q-headers versleutelt:



Een van de nieuwe verbeteringen bevat 802.1Q-tags in de Clear (ook wel ClearTag genoemd). Deze verbetering maakt het mogelijk om de 802.1Q-tag buiten de versleutelde MACsec-header te tonen. Het blootstellen van dit gebied verstrekt verscheidene ontwerpopties met MACsec, en in voor openbare vervoerders Ethernet van de Carrier, is het noodzakelijk voor het leveraging van bepaalde vervoerdiensten.

De MKA-functieondersteuning biedt tunnelinformatie zoals VLAN-tag (802.1Q-tag) in het duidelijke zodat de serviceprovider multiplexing van services kan bieden, zodat multipoint-to-point services of multipoint services naast elkaar kunnen bestaan op één fysieke interface en gedifferentieerd kunnen worden op basis van de nu zichtbare VLAN-id.

Naast servicemultiplexing maakt VLAN-tag in het Clear ook het mogelijk dat serviceproviders Quality of Service (QoS) leveren aan het versleutelde Ethernet-pakket via het SP-netwerk op basis van het veld 802.1P (CoS) dat nu zichtbaar is als deel van de 802.1Q-tag.

WAN MACSEC-terminologie

MKA	MACSec Key Agreement, gedefinieerd in IEEE 802.1XREV-2010 - Key Agreement Protocol voor het ontdekken van MACSec-peers en het onderhandelen van sleutels.
MSK	Master Session Key, gegenereerd tijdens EAP-uitwisseling. Supplicant en authenticatieserver gebruiken de MSK om CAK te genereren
CAK	De sleutel van de Vereniging van de connectiviteit wordt afgeleid van MSK. Is een lange-leven hoofdsleutel die wordt gebruikt om alle andere sleutels te produceren die voor MACSec worden gebruikt.
CKN	Key Name - identificeert de CAK.
SAK	Secure Association Key - afgeleid van de CAK en is de sleutel die door de aanvrager en de switch wordt gebruikt om verkeer voor een bepaalde sessie te versleutelen.
KS	Key Server verantwoordelijk voor: • Het selecteren van en het adverteren van een cijferreeks • Het genereren van de SAK van de CAK.
KEK	Key Encrypting Key - gebruikt ter bescherming van MACsec-toetsen (SAK)

MACSEC Key Agreement Protocol (MKA) en cryptografische overzicht

MKA is het mechanisme van het controlevliegtuig dat door WAN MACsec wordt gebruikt; gespecificeerd in IEEE Std 802.1X die wederzijds geverifieerde MACsec-peers plus de volgende acties ontdekt:

- Hiermee wordt een CA (Connectivity Association) opgericht en beheerd.
- Beheert live/potentiele peer-lijst.

- Onderhandeling over coderingssuite.
- Selecteert Key Server (KS) onder de leden van een CA.
- Secure Association Key (SAK)-afleiding en -beheer.
- Secure Key-distributie.
- Belangrijke installatie.
- Rekey.

Eén lid wordt gekozen als de Key server op basis van de ingestelde key-server prioriteit (laagste), als de KS-prioriteit gelijk is onder peers, dan wint de laagste SCI.

KS genereert een SAK pas nadat alle potentiële peers live zijn geworden en er ten minste één live peer is. Het verspreidt de SAK en het algoritme dat wordt gebruikt aan andere deelnemers met behulp van de MKA PDU of MKPDU in een versleuteld formaat.

Deelnemers controleren het door de SAK verzonden algoritme en installeren het als het wordt ondersteund, met behulp van het op elke MKPDU om de laatste sleutel aan te geven die ze hebben; anders wijzen ze SAK af

Wanneer geen MKPDU wordt ontvangen van een deelnemer na 3 hartslag (elke hartslag is van 2 seconden standaard), worden peers verwijderd uit de live peer lijst; als een klant de verbinding verbreekt, blijft de deelnemer op de switch MKA gebruiken tot er 3 hartslagen zijn verstreken nadat de laatste MKPDU van de client is ontvangen.

Voor dit proces, zijn er twee methodes om encryptiesleutels te drijven:

- Vooraf gedeelde toetsen
- 802.1x/EAP

Vooraf gedeelde toetsen

Als u vooraf gedeelde sleutels gebruikt, moeten CAK=PSK en CKN handmatig worden ingevoerd. Voor belangrijke levenstijd, zorg ervoor dat u een zeer belangrijke het omvergooien en overlapping tijdens re-key tijd aan hebt:

- Verwissel en installeer nieuwe SAK-toets en bind deze aan idle SA.
- Schoon de oude SAK-toets en wijs een nieuwe ongebruikte SA toe.

Configuratievoorbeeld:

<#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
```

Met vetgedrukte woorden wordt bedoeld:
M_Key: Sleutelnaam ketting.

Sleutel 01: Connectiviteit Association Sleutelnaam (hetzelfde als CKN).

aes-128-cmac: MKA-verificatiecode.

12345678901234567890123456789012: Connectivity Association Key (CAK).

Beleid definiëren:

<#root>

```
mka policy example
 macsec-cipher-suite

gcm-aes-256
```

Wanneer gcm-aes-256 verwijst naar coderingssuite(s) voor beveiligde associatiesleutel (SAK)-afleiding.

Opmerking: dit is basisbeleidsconfiguratie, meer opties zoals vertrouwelijkheid-offset, zaaksleutel, inclusief-icv-indicator en meer zijn beschikbaar voor gebruik afhankelijk van de implementatie.

Interface:

```
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
```

Opmerking: Als er geen mka-beleid is geconfigureerd of toegepast, is standaard beleid ingeschakeld en kan worden bekeken via mka standaard-beleid detail tonen.

802.1x/EAP

Als u de EAP-methode gebruikt, worden alle toetsen gegenereerd vanaf de Master Session Key (MSK). In het EAP-framework (IEEE 802.1X Extensible Authentication Protocol) worden EAPoL-MKA-frames tussen apparaten uitgewisseld, terwijl de Ether Type van EAPoL-frames 0x888E zijn, terwijl de pakketinhoud in een EAPOL Protocol Data Unit (PDU) wordt aangeduid als een MACsec Key Agreement PDU (MKPDU). Deze EAPoL-frames bevatten de CKN van de afzender, de belangrijkste serverprioriteit en de MACsec-functies.

Opmerking: standaard verwerken de switches EAPoL-MKA-frames, maar ze worden niet doorgestuurd.

Configuratievoorbeeld van MACsec-encryptie op basis van certificaten:

Inschrijving in het certificaat (vereist certificaatautoriteit):

```
  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
```

802.1x-verificatie en AAA-configuratie vereist:

```
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
```

EAP-TLS-profiel en 802.1X-referenties:

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

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

Interface:

```
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
```

WAN MACSEC-oplossingen voor probleemoplossing

Configuratie

Controleer de juiste configuratie en implementatie ondersteuning afhankelijk van het platform; toetsen en parameters moeten overeenkomen. Enkele gemeenschappelijke logboeken om te identificeren als er een probleem bij configuratie is zijn volgende degenen:

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

Controleer de MACsec-mogelijkheid van de hardware van de peers of verlaag de vereisten voor

de MACsec-mogelijkheid door de MACsec-configuratie voor de interface te wijzigen.

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

Er zijn sommige optionele parameters die router kan verwachten of niet gebaseerd op configuratie en verschillende standaardinstellingen van het platform, ervoor zorgen dat u omvat of verwerpt op configuratie.

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

Er is een configuratie mismatch op de policy algoritme suite, zorg ervoor dat de juiste match.

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

MKPDU heeft een of meer van de volgende validatiecontroles mislukt:

- Geldige MAC-adres en EAPOL-header: controleer de configuratie van beide interfaces, pakketopname op toegangsinterface kan huidige waarden bevestigen.
- Geldige CKN en algoritme Agility: zorg voor geldige sleutels en algoritme suites.
- ICV-verificatie: ICV-verificatie is een optionele parameter, configuratie beide uiteinden moeten overeenkomen.
- Correct ordelijk bestaan van MKA payloads: mogelijke interoperabiliteitskwestie.
- MI-verificatie indien peers bestaan: lididentificatiecontrole, uniek voor elke deelnemer.
- MN-verificatie indien peers bestaan: Berichtnummerverificatie, uniek op elke verzonden MKPDU en incrementen op elke transmissie.

Operationele aangelegenheden

Als de configuratie eenmaal is ingesteld, kunt u het bericht %MKA-5-SESSION_START zien maar u moet controleren of de sessie omhoog komt, een goed commando om mee te beginnen is tonen mka sessies [interface 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
```

Status verwijst naar de sessie van het bedieningsvliegtuig; Beveiligd betekent dat Rx en Tx SAK is geïnstalleerd, zo niet, dan verschijnt deze als Niet beveiligd.

- Als de status op Init blijft, controleer fysieke interfacestatus, connectiviteit via ping voor peers en configuratiegelijke. Op dit punt is er geen MKPDU ontvangen en live peers, sommige platforms doen padding terwijl andere niet; neem tot 32 bytes van header overhead en zorg voor een grotere MTU voor een goede werking.
- Als de status in behandeling blijft, controleert u of MKPDU in- of uitstappen in het controlevlak of fouten/dalingen van MKPDU worden gedropt.
- Als de status blijft staan op Not Secure, is de MKA-interface actief en stroomt MKPDU's door, maar SAK is niet geïnstalleerd, in dit geval wordt het volgende logbestand weergegeven:

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

Dit is te wijten aan geen MACsec-ondersteuning, ongeldige MACsec-configuratie of andere MKA-uitval aan lokale of peer kant voorafgaand aan de oprichting van een Secure Channel (SC) en installatie van Secure Associations (SA) in MACsec. U kunt de detailopdracht gebruiken voor meer informatie tonen mka sessie [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 Priority	RxSA Installed	SSCI
272DA12A009CD0A3D313FADF	**14712**	**40b5.c133.020a/0012**	**1**	**YES**	**0**

Potential Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI

Zoek naar SAK-informatie over peers en relevante gegevens gemarkeerd om een beter inzicht te krijgen in de situatie, als er een andere SAK is, onderzoek dan de gebruikte sleutel en de levenslange of SAK-rekey-opties geconfigureerd, als er vooraf gedeelde toetsen worden gebruikt, kunt u tonen mka-sleutelhangers gebruiken:

<#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>
```

CAK wordt nooit getoond maar u kunt bevestigen keychain naam en CKN.

Als de sessie is ingesteld maar u heeft flaps of intermitterende verkeersstroom, moet u controleren of MKPDU's correct stromen tussen peers, als er een time-out is, kunt u het volgende bericht zien:

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

Als er één peer is, wordt MKA Session beëindigd, als je meerdere peers hebt en MKA heeft geen MKPDU ontvangen van een van zijn peers gedurende meer dan 6 seconden, Live Peer wordt verwijderd uit de Live Peers List, kunt u beginnen met mka statistieken tonen [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
```

MKPDU's verzonden en ontvangen moeten vergelijkbare getallen hebben voor één peer, zorgen dat ze aan beide uiteinden toenemen bij Rx en Tx, om de problematische richting te bepalen of te begeleiden, als er verschillen zijn kunt u debug mka linksec-interface frames inschakelen voor beide uiteinden:

```
*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
```

In het geval dat er geen MKPDU ontvangen, zoek naar inkomende interfacefouten of dalingen, status van de peers interfaces en mka sessie; in het geval u beide routers verzenden maar niet ontvangen hebt, MKPDUs zijn verloren op de media en moeten controleren tussenapparaten voor correct doorsturen.

Als u geen MKPDU's verzendt, controleert u op fysieke interfacestatus (lijn en fouten/dalingen) en configuratie; controleer of u deze pakketten op regelvliegtuigniveau genereert, of FIA-tracering en Embedded Packet Capture (EPC) voor dit doel betrouwbare tools zijn. Raadpleeg Probleemoplossing met de functie Cisco IOS XE Datapath Packet Trace

U kunt debug mka gebeurtenissen gebruiken en zoeken naar redenen kan leiden volgende stappen.

Opmerking: Gebruik voorzichtig debug mka en debug mka diagnostiek als ze toestandsmachine en zeer gedetailleerde informatie tonen die kan leiden tot

---

controlevliegtuigproblemen op de router.

Als de sessie beveiligd en stabiel is maar het verkeer niet doorstroomt, controleert u op versleuteld verkeer door beide peers te verzenden:

<#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
```

SecY-tellers zijn huidige pakketten op een fysieke interface, terwijl de andere zijn gerelateerd aan de Tx Secure Channel-gemiddelden van pakketten die worden versleuteld en verzonden en Rx Secure Association betekent geldige pakketten die op de interface worden ontvangen.

Meer debugs zoals debug mka fouten en debug mka pakketten helpt bij het identificeren van problemen, gebruik deze laatste met voorzorgsmaatregelen zoals kan zware vastlegging veroorzaken.

Gerelateerde informatie

- Configuratiehandleiding voor MACsec en MKA
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.