

Risoluzione dei problemi relativi a MACSEC WAN sui router

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Cenni preliminari su MACSEC per la risoluzione dei problemi](#)

[Formato pacchetto MACsec](#)

[WAN-MACSEC](#)

[Formato pacchetto MACSEC WAN](#)

[Terminologia MACSEC WAN](#)

[Panoramica del protocollo MKA \(MACSEC Key Agreement Protocol\) e della crittografia](#)

[Chiavi già condivise](#)

[802.1x/EAP](#)

[Risoluzione dei problemi relativi a MACSEC WAN](#)

[Configurazione](#)

[Problemi operativi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il protocollo MACSEC WAN di base per comprendere il funzionamento e la risoluzione dei problemi dei router Cisco IOS® XE.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni di questo documento sono specifiche per i router Cisco IOS XE come le famiglie ASR 1000, ISR 4000 e Catalyst 8000. Cercare il supporto MACSEC hardware e software specifico.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia

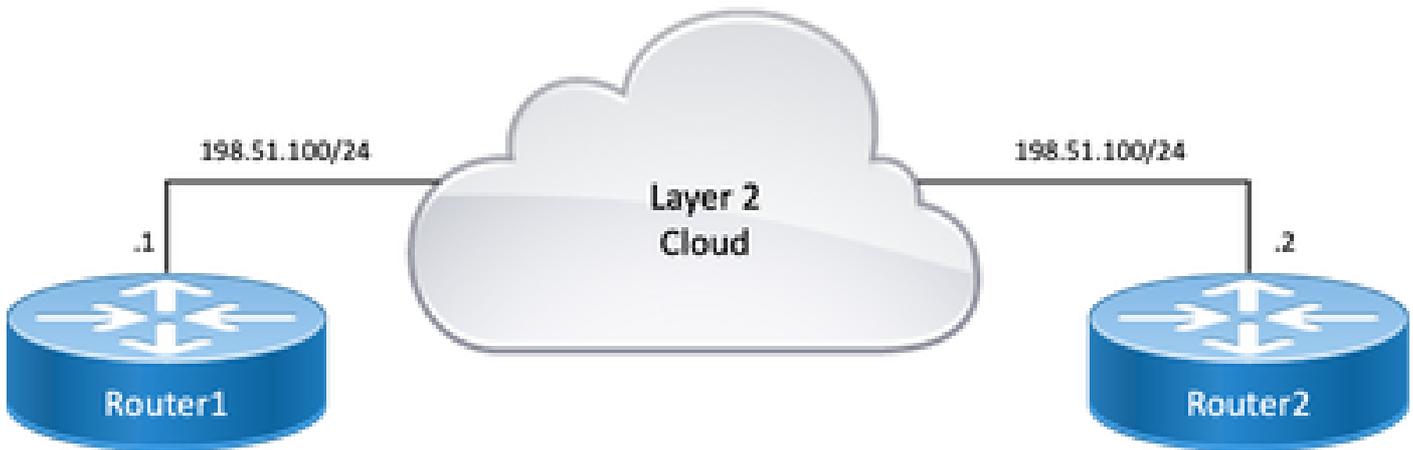


Diagramma topologico

Cenni preliminari su MACSEC per la risoluzione dei problemi

MACsec è una crittografia basata su standard IEEE 802.1AE Layer 2 hop-by-hop che fornisce riservatezza dei dati, integrità dei dati e autenticazione dell'origine dei dati per i protocolli indipendenti dall'accesso ai supporti con crittografia AES-128. Utilizzando MACsec è possibile proteggere solo i collegamenti verso host (collegamenti tra dispositivi di accesso alla rete e dispositivi endpoint come un PC o un telefono IP).

- I pacchetti vengono decrittografati sulla porta in entrata.
- I pacchetti nel dispositivo non sono crittografati.
- I pacchetti vengono crittografati sulla porta di uscita.

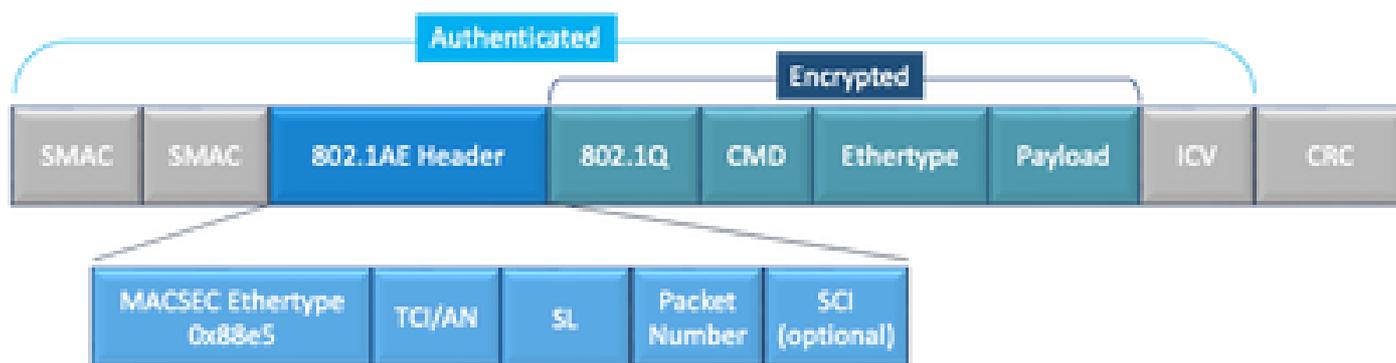
MACsec fornisce comunicazioni sicure sulle LAN cablate. Quando MACsec viene usato per proteggere la comunicazione tra gli endpoint su una LAN, ciascun pacchetto sul cavo viene criptato usando la crittografia a chiave simmetrica, in modo che la comunicazione non possa essere monitorata o modificata sul cavo. Quando MACsec viene utilizzato insieme ai tag del gruppo di sicurezza (SGT), fornisce la protezione per il tag insieme ai dati contenuti nel payload del frame.

MACsec fornisce la crittografia a livello MAC su reti cablate utilizzando metodi fuori banda per la crittografia delle chiavi.

Formato pacchetto MACsec

Con 802.1AE (MACsec), i frame vengono crittografati e protetti con un valore di controllo

dell'integrità (ICV) senza impatto sulla MTU o sulla frammentazione IP e con un impatto MTU L2 minimo: circa 40 byte (meno di un frame giant per bambini).



Esempio di formato di pacchetto MACSEC

- EtherType MACsec: 0x88e5, indica che il frame è un frame MACsec.
- TCI/AN: informazioni di controllo del tag/codice di associazione. È il numero di versione di MACsec se la riservatezza o l'integrità vengono utilizzate da sole.
- SL: lunghezza dei dati crittografati.
- PN: numero del pacchetto utilizzato per la protezione della riproduzione.
- SCI: Secure Channel Identifier. Ogni associazione di connettività (CA) è una porta virtuale (indirizzo MAC dell'interfaccia fisica più ID porta a 16 bit).
- ICV: Valore controllo integrità.

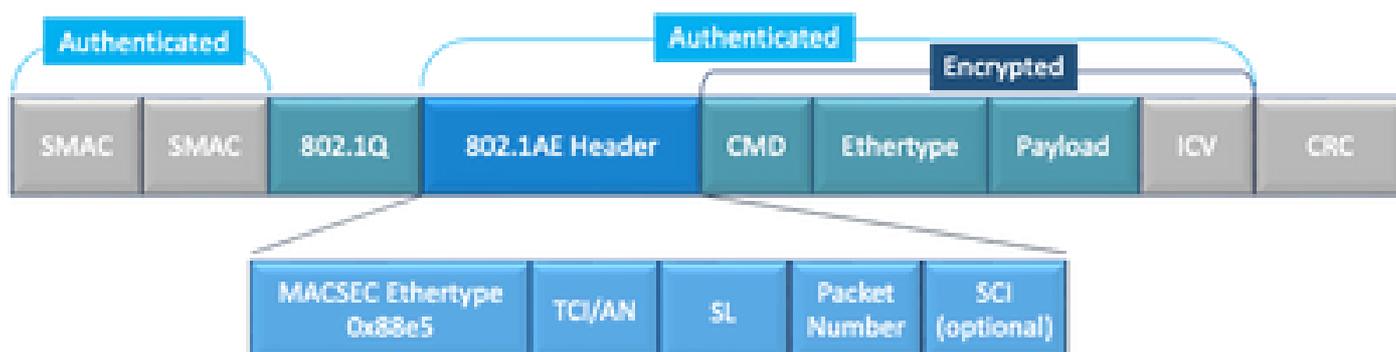
WAN-MACSEC

Ethernet si è evoluto oltre il trasporto LAN privato, per includere una varietà di opzioni di trasporto WAN o MAN. La tecnologia MACSEC per WAN fornisce la crittografia end-to-end su servizi WAN Ethernet di layer 2 point-to-point o point-to-multipoint con AES a 128 o 256 bit.

WAN MACsec è basato su (LAN) MACsec, da cui il nome (e separato da IPsec), ma offre diverse funzionalità aggiuntive non disponibili in precedenza.

Formato pacchetto MACSEC WAN

È possibile che il provider di servizi non supporti l'ethertype MACsec e non sia in grado di differenziare il servizio L2 se il tag è crittografato, in modo che il MAC WAN cripti tutto il frame dopo le intestazioni 802.1Q:



Uno dei nuovi miglioramenti include i tag 802.1Q in Clear (alias ClearTag). Questo miglioramento consente di esporre il tag 802.1Q all'esterno dell'intestazione MACsec crittografata. L'esposizione di questo campo fornisce diverse opzioni di progettazione con MACsec, e in per i provider di trasporto pubblici Carrier Ethernet, è necessario per sfruttare alcuni servizi di trasporto.

Il supporto della funzione MKA fornisce informazioni sul tunneling, ad esempio il tag VLAN (tag 802.1Q), in modo che il provider di servizi possa fornire il multiplexing dei servizi in modo che più servizi point-to-point o multipoint possano coesistere su un'unica interfaccia fisica e differenziati in base all'ID VLAN ora visibile.

Oltre al multiplexing dei servizi, il tag VLAN in chiaro consente ai provider di servizi di fornire QoS (Quality of Service) al pacchetto Ethernet crittografato nella rete SP in base al campo 802.1P (CoS), ora visibile come parte del tag 802.1Q.

Terminologia MACSEC WAN

MKA	MACSec Key Agreement, definito in IEEE 802.1XREV-2010 - Protocollo di accordo chiave per il rilevamento dei peer MACSec e delle chiavi di negoziazione.
MSK	Chiave di sessione master, generata durante lo scambio EAP. Il richiedente e il server di autenticazione utilizzano MSK per generare CAK
CAK	La chiave di associazione di connettività deriva da MSK. È una chiave master di lunga durata utilizzata per generare tutte le altre chiavi utilizzate per MACSec.
CKN	Nome chiave associazione connettività: identifica la chiave CAK.
SAK	Chiave di associazione sicura: derivata dalla chiave CAK ed è la chiave utilizzata dal supplicant e dallo switch per crittografare il traffico di una determinata sessione.
KS	Server principale responsabile di: <ul style="list-style-type: none">• Selezione e annuncio di una suite di cifratura• Generazione della chiave SAK dalla chiave CAK.
KEK	Chiave di crittografia - utilizzata per proteggere le chiavi MACsec (SAK)

Panoramica del protocollo MKA (MACSEC Key Agreement Protocol) e della crittografia

MKA è il meccanismo del control plane utilizzato da MACsec WAN; specificato in IEEE Std 802.1X che individua i peer MACsec reciprocamente autenticati e le azioni successive:

- Stabilisce e gestisce una CA (Connectivity Association).
- Gestisce l'elenco di peer attivi/potenziati.
- Negoziazione suite di cifratura.

- Seleziona il server di chiavi tra i membri di una CA.
- Derivazione e gestione della chiave di associazione sicura (SAK).
- Distribuzione di chiavi protette.
- Installazione della chiave.
- Reimposta.

Un membro viene scelto come server di chiave in base alla priorità configurata del server di chiave (priorità più bassa), se la priorità KS è la stessa tra i peer, prevale la priorità SCSI più bassa.

KS genera un SAK solo dopo che tutti i potenziali pari sono diventati vivi e c'è, almeno, un pari vivo. Distribuisce la chiave SAK e la cifratura utilizzata ad altri partecipanti utilizzando la PDU MKA o la MKPDU in formato criptato.

I partecipanti controllano la cifratura inviata dal SAK e la installano se è supportata, utilizzando su ogni MKPDU per indicare la chiave più recente di cui dispongono; in caso contrario, rifiutano SAK

Quando non si riceve alcun MKPDU da un partecipante dopo 3 heartbeat (ogni heartbeat è di 2 secondi per impostazione predefinita), i peer vengono eliminati dalla lista peer attiva; ad esempio, se un client si disconnette, il partecipante sullo switch continua a utilizzare MKA fino a quando non sono trascorsi 3 heartbeat dopo che l'ultimo MKPDU è stato ricevuto dal client.

Per questo processo, esistono due metodi per guidare le chiavi di crittografia:

- Chiavi già condivise
- 802.1x/EAP

Chiavi già condivise

Se si utilizzano chiavi già condivise, è necessario immettere manualmente CAK=PSK e CKN. Per la durata della chiave, verificare di disporre di un rollover e di una sovrapposizione della chiave durante il tempo di reimpostazione della chiave per:

- Sostituire e installare la nuova chiave SAK e associarla all'associazione di sicurezza inattiva.
- Rimuovere la vecchia chiave SAK e allocare una nuova associazione di protezione inattiva.

Esempio di configurazione:

```
<#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
```

Dove il grassetto si riferisce:

M_Key: nome della catena di chiavi.

key 01: nome della chiave di associazione di connettività (uguale a CKN).

aes-128-cmac: crittografia di autenticazione MKA.

12345678901234567890123456789012: chiave di associazione connettività (CAK).

Definire il criterio:

```
<#root>
```

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

```
gcm-aes-256
```

Dove **gcm-aes-256** fa riferimento alle suite di cifratura per la derivazione della chiave di associazione sicura (SAK).

 Nota: questa è la configurazione di base della policy. A seconda dell'implementazione, sono disponibili altre opzioni, ad esempio **confidenzialità-offset**, **sak-rekey**, **include-icv-index** e altre ancora.

Interfaccia:

```
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
```

 Nota: se non viene configurato o applicato alcun criterio MKA, il criterio predefinito è abilitato e può essere esaminato tramite `show mka default-policy detail`.

802.1x/EAP

Se si utilizza il metodo EAP, tutte le chiavi vengono generate dalla chiave della sessione master (MSK). Con il framework EAP (Extensible Authentication Protocol) IEEE 802.1X, MKA scambia frame EAPoL-MKA tra dispositivi, il tipo Ether di frame EAPoL è 0x888E, mentre il corpo del pacchetto in un'unità PDU (Protocol Data Unit) EAPoL è indicato come MKPDU (MACsec Key Agreement PDU). Questi frame EAPoL contengono il nome della connessione (CKN) del mittente, la priorità del server chiave e le funzionalità MACsec.

 Nota: per impostazione predefinita, gli switch elaborano i frame EAPoL-MKA ma non li inoltrano.

Esempio di configurazione della crittografia MACsec basata su certificati:

Registrazione del certificato (è necessaria l'Autorità di certificazione):

```
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
```

Autenticazione 802.1x e configurazione AAA necessarie:

```
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
```

Profilo EAP-TLS e credenziali 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
!
```

Interfaccia:

```
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
```

Risoluzione dei problemi relativi a MACSEC WAN

Configurazione

Verificare che la configurazione e l'implementazione supportino la piattaforma in uso. Le chiavi e i parametri devono corrispondere. Di seguito sono elencati alcuni dei log comuni che consentono di identificare eventuali problemi riscontrati durante la configurazione:

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

Controllare la funzionalità MACsec dell'hardware dei peer o ridurre i requisiti per la funzionalità MACsec modificando la configurazione MACsec per l'interfaccia.

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

Esistono alcuni parametri opzionali che il router può prevedere o meno in base alla configurazione e alle diverse impostazioni predefinite della piattaforma, accertarsi di includere o eliminare la configurazione.

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

Mancata corrispondenza di configurazione nella suite di cifratura dei criteri. Verificare la corrispondenza.

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

MKPDU non ha superato uno o più controlli di convalida successivi:

- Indirizzo MAC valido e intestazione EAPOL: controllare la configurazione di entrambe le interfacce, l'acquisizione dei pacchetti sull'interfaccia in entrata può confermare i valori correnti.
- Agilità CKN e algoritmo valida: verificare che le chiavi e le suite di algoritmi siano valide.
- Verifica ICV: la verifica ICV è un parametro facoltativo. La configurazione deve corrispondere a entrambe le estremità.
- Esistenza ordine corretto dei payload MKA: possibile problema di interoperabilità.
- Verifica MI se esistono peer: verifica dell'identificatore del membro, univoca per ciascun partecipante.
- Verifica MN se esistono peer: verifica del numero di messaggio, univoca su ogni MKPDU trasmesso e incrementale su ogni trasmissione.

Problemi operativi

Una volta impostata la configurazione, è possibile visualizzare il messaggio %MKA-5-SESSION_START ma è necessario controllare l'attivazione della sessione. Per iniziare, è consigliabile utilizzare il comando `show mka sessions [interface name]` (nome_interfaccia):

<#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
=====
```

Interface Port-ID	Local-TxSCI Peer-RxSCI	Policy-Name MACsec-Peers	Inherited Status	Key-Server CKN
Te0/1/2	40b5.c133.0e8a/0012			

Example

NO

NO

18 40b5.c133.020a/0012 1

Secured

01

Lo stato si riferisce alla sessione del control plane; Protetto significa che Rx e Tx SAK sono installati, altrimenti appare come Non protetto.

- Se lo stato rimane su Init, controllare lo stato dell'interfaccia fisica, la connettività tramite ping per i peer e la configurazione. A questo punto non viene ricevuta alcuna MKPDU e i peer attivi, alcune piattaforme eseguono il padding, a differenza di altre; considerare fino a 32 byte di sovraccarico dell'intestazione e garantire un'MTU più grande per il corretto funzionamento.
- Se lo stato rimane su In sospeso, verificare se MKPDU viene rilasciato in entrata o in uscita nel control plane o se vengono rilevati errori o rilasci nelle interfacce.
- Se lo stato resta impostato su Non protetto, l'interfaccia MKA è attiva e le MKPDU passano attraverso ma la chiave SAK non è installata, in questo caso viene visualizzato il log successivo:

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

Ciò è dovuto al mancato supporto di MACsec, a una configurazione MACsec non valida o a un altro errore MKA sul lato locale o peer prima della creazione di un canale sicuro (SC, Secure Channel) e dell'installazione di associazioni sicure (SA, Secure Associations) in MACsec. Per ulteriori informazioni, è possibile utilizzare il comando `detail show mka session [interface nome_interfaccia] 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:

Table with 6 columns: MI, MN, Rx-SCI (Peer), KS Priority, RxSA Installed, SSCI. Row 1: 272DA12A009CD0A3D313FADF, 14712, 40b5.c133.020a/0012, 1, YES, 0

Potential Peers List:

Table with 6 columns: MI, MN, Rx-SCI (Peer), KS Priority, RxSA Installed, SSCI

Cercare le informazioni SAK sui peer e i dati rilevanti evidenziati per comprendere meglio la situazione, se è presente una SAK diversa, esaminare le chiavi utilizzate e la durata o le opzioni di reimpostazione delle chiavi SAK configurate. Se vengono utilizzate chiavi già condivise, è possibile utilizzare show mka keychains:

<#root>

Router1#

show mka keychains

MKA PSK Keychain(s) Summary...

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

=====

Master_Key

01

Te0/1/2

<HIDDEN>

CAK non viene mai visualizzato, ma è possibile confermare il nome del portachiavi e il nome CKN.

Se la sessione è stata stabilita ma si dispone di flap o di un flusso del traffico intermittente, è necessario verificare se i pacchetti MKPDU passano correttamente tra i peer. In caso di timeout, viene visualizzato il messaggio seguente:

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

Se è presente un peer, la sessione MKA viene terminata, nel caso in cui si disponga di più peer e MKA non abbia ricevuto una MKPDU da uno dei peer per più di 6 secondi, Live Peer viene rimosso dall'elenco dei peer attivi, è possibile iniziare con show mka statistics [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
```

I pacchetti MKPDU trasmessi e ricevuti devono avere numeri simili per un peer, accertarsi che aumentino a Rx e Tx a entrambe le estremità, per determinare o guidare la direzione problematica, se ci sono differenze è possibile abilitare debug mka linksec interface frame a entrambe le estremità:

```
*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
```

Se non è stata ricevuta alcuna MKPDU, verificare la presenza di errori o perdite di interfacce in ingresso, lo stato delle interfacce peer e la sessione MKPDU. Se entrambi i router inviano ma non ricevono questa informazione, i MKPDU vengono persi sul supporto e occorre controllare i dispositivi intermedi per verificare la corretta inoltro.

Se non si stanno inviando pacchetti MKPDU, verificare lo stato dell'interfaccia fisica (linea ed errori/gocce) e la configurazione; verificare se si stanno generando questi pacchetti a livello di control plane; FIA trace e Embedded Packet Capture (EPC) sono strumenti affidabili a tale scopo. Per ulteriori informazioni, fare riferimento alla sezione [Risoluzione dei problemi relativi alla funzionalità Cisco IOS XE Datapath Packet Trace](#)

È possibile utilizzare gli eventi mka di debug e cercare i motivi che possono guidare i passaggi successivi.



Nota: procedere con cautela alla diagnostica debug mka e debug mka poiché queste informazioni mostrano la macchina a stati e informazioni molto dettagliate che possono causare problemi al control plane sul router.

Se la sessione è protetta e stabile ma il traffico non scorre, verificare la presenza di traffico crittografato che invia entrambi i peer:

```
<#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

I contatori SecY sono pacchetti correnti sull'interfaccia fisica, mentre gli altri sono relativi al canale Tx Secure, che significa pacchetti che vengono criptati e trasmessi, mentre Rx Secured Association indica pacchetti validi ricevuti sull'interfaccia.

Altri debug, ad esempio debug mka errors e debug mka packets, consentono di identificare i problemi. Usare quest'ultimo per precauzione, in quanto può causare un pesante log.

Informazioni correlate

- [Guida alla configurazione di MACsec e MKA](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).