

Traffico MACSec XPN tra Catalyst 9500 e Nexus 9000 con aumento di pacchetti non validi ed errori FCS

Sommario

Problema

Quando MACSec XPN viene abilitato tra un Catalyst 9500-28C8D e un Nexus N9K-C93180YC-FX, la sessione MKA viene stabilita correttamente ma il traffico dati non passa attraverso il collegamento. Catalyst 9500 segnala un aumento dei "pacchetti non validi" nelle statistiche ASA e errori di input FCS sull'interfaccia fisica. In particolare, sono stati osservati i seguenti sintomi:

- Nessuna connettività dopo l'attivazione di MACSec
- La sessione MKA è stata stabilita, ma sul lato Catalyst 9500 sono visualizzate le statistiche SA con i valori "PKTS 118 non validi" in aumento e "PKT validi: 0"
- Incremento degli errori di input FCS sull'interfaccia fisica Catalyst 9500
- La rimozione della configurazione MACSec ripristina immediatamente la connettività e arresta gli errori FCS

Le sessioni MKA sono state stabilite su entrambi i dispositivi e hanno negoziato con successo la cifratura GCM-AES-XPN-256. Sul lato Nexus la crittografia era attiva, ma Catalyst 9500 ha ricevuto pacchetti crittografati e li ha rifiutati a causa di una mancata corrispondenza di convalida, pertanto non sono stati accettati pacchetti validi.

Ambiente

- Catalyst 9500-28C8D con Cisco IOS®
- Nexus N9K-C93180YC-FX
- Configurazione di MACSec XPN utilizzando la suite di cifratura GCM-AES-XPN-256

- Interfaccia 400 Gigabit Ethernet (FourHcentoGigE1/0/15 su Catalyst, Ethernet1/52 su Nexus)
- Catalyst 9500 configurato come key server priority 1, Nexus configurato come key server priority 100
- Algoritmo di crittografia AES-256-CMAC per chiavi già condivise

Risoluzione

Il problema è stato risolto implementando una soluzione che modifica l'assegnazione del ruolo server-chiave tra i dispositivi. La risoluzione consigliata prevede le seguenti fasi:

Passaggio 1: Identificazione del problema di configurazione del server delle chiavi

Verificare la configurazione corrente della priorità del server delle chiavi su entrambi i dispositivi. La configurazione problematica mostrava:

Configurazione di Catalyst 9500:

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 1
  macsec-cipher-suite gcm-aes-xpn-256
```

Configurazione Nexus:

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 100
```

Passaggio 2: Implementazione soluzione alternativa al ruolo server chiave

Configurare il dispositivo Nexus come server di chiavi MACSec anziché Catalyst 9500. In questo

caso è necessario regolare i valori di priorità del server di chiavi in modo che Nexus assuma il ruolo di server di chiavi.

Modificare la configurazione di Nexus in modo che abbia un valore di priorità server della chiave inferiore (i valori più bassi hanno una priorità più alta):

```
macsec policy MEHEALTH-ORG-XPB
  key-server-priority 1
```

Modificare la configurazione di Catalyst 9500 in modo che abbia un livello di priorità del server delle chiavi più alto:

```
mka policy MEHEALTH-ORG-XPB
  key-server priority 100
  macsec-cipher-suite gcm-aes-xpn-256
```

Passaggio 3: Verifica del funzionamento di MACSec

Dopo aver implementato la modifica del ruolo server chiave, verificare che:

- Sessioni MKA stabilite correttamente su entrambi i dispositivi
- Il traffico di dati passa attraverso il collegamento abilitato per MACSec
- Sulle statistiche della SA Catalyst 9500, non è in corso alcun incremento di "pacchetti non validi"
- Errori di input FCS non si verificano nell'interfaccia fisica

Questa soluzione consente il corretto funzionamento della configurazione di MACSec XPN fino al completamento dell'analisi della piattaforma e della pianificazione dell'aggiornamento software.

Causa

La causa principale di questo problema è correlata all'ID bug Cisco CSCvs00410, che descrive

uno scenario in cui le sessioni MKA vengono stabilite correttamente, ma i dati non possono passare attraverso il collegamento quando si utilizza AES-256-XPB con Catalyst 9500 nel ruolo di server chiave in determinate condizioni di interoperabilità con i dispositivi Nexus. Questo comportamento si manifesta come una mancata corrispondenza di convalida in cui Catalyst 9500 rifiuta i pacchetti crittografati da Nexus, causando un aumento dei conteggi dei pacchetti non validi e degli errori FCS. È stata rilevata una discrepanza relativa al fatto che Cisco IOS sia elencato come risolto per questo problema, che richiede ulteriori indagini da parte del team della piattaforma Catalyst.

Contenuto correlato

- Cisco Bug ID CSCvs00410 - Sessione MKA attiva ma non in grado di passare i dati attraverso il collegamento quando si usa AES-256-XPB con ruolo server chiave Catalyst 9500

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).