Beheben von MACSec MKA PDU Integrity Check-Fehlern auf Nexus 9000-Switches

Inhalt

Problem

Die zwischen den Nexus 9000-Switches konfigurierte Media Access Control Security (MACSec) zeigt die MACsec Key Agreement (MKA)-Sitzung als "sicher" an, generiert jedoch etwa alle zwei Sekunden wiederholte Fehlermeldungen. Das folgende Muster überflutet die Systemprotokolle:

```
device# %CTS-5-CTS_MKPDU_ICV_SUCCESS: MACSec: MKPDU verified. Primary keys match for Interface
device# %CTS-4-CTS_MKPDU_ICV_FAILURE: MACSec: MKA PDU integrity check failed for Interface
```

Diese abwechselnden Erfolgs- und Fehlermeldungen führen zu übermäßig langen Protokolleinträgen, die unter Wahrung der MACSec-Funktionalität korrigiert werden müssen.

Umwelt

- Produkt: Cisco Nexus Switches
- Technologie: MACSec (Link Encryption)

Auflösung

Um dieses Problem zu beheben, ändern Sie die Fallback-Schlüsselbund-Konfiguration so, dass andere Schlüssel-IDs als die in der primären Schlüsselbund-Konfiguration verwendet werden:

1. Überprüfen Sie Ihre vorhandenen MACSec-Schlüsselkettenkonfigurationen, um

übereinstimmende Schlüssel-IDs zwischen primären und Fallback-Schlüsselketten mit diesem Befehl zu identifizieren.

```
device# show running-configuration
...
key chain primary macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
key chain fallback macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
...
```

2. Ändern Sie den Fallback-Schlüsselbund, sodass er mit diesen Befehlen eine andere Schlüssel-ID verwendet. Wenn der primäre Schlüsselbund beispielsweise die Schlüssel-ID 01 verwendet, konfigurieren Sie den Fallback-Schlüsselbund so, dass er stattdessen die Schlüssel-ID 10 verwendet.

```
device# configure terminal
device(config)# key chain fallback macsec
device(config)# no key 01
device(config)# key 10
device(config)# key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
```

3. Überwachen Sie die Systemprotokolle, um sicherzustellen, dass die abwechselnden Meldungen CTS_MKPDU_ICV_SUCCESS und CTS_MKPDU_ICV_FAILURE nicht mehr angezeigt werden.

Ursache

Die Ursache hierfür ist ein Konfigurationskonflikt, bei dem der Fallback-Schlüsselbund dieselbe Schlüssel-ID verwendet wie der primäre Schlüsselbund. Dies führt zu Mehrdeutigkeiten im MKA-Protokoll, sodass die Integritätsprüfung abwechselnd erfolgreich verläuft und fehlschlägt, wenn das System zwischen der Auswertung des primären und des Fallback-Schlüssels umschaltet. Im Nexus MACSec-Konfigurationsleitfaden heißt es, dass die Fallback-Schlüssel-ID mit keiner Schlüssel-ID einer primären Schlüsselkette übereinstimmen sollte, um diesen Konflikt zu vermeiden.

Verwandte Inhalte

- Nexus MACSec - Konfigurationsanleitung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.