

MACSec XPN-Datenverkehr fällt zwischen Catalyst 9500 und Nexus 9000 mit zunehmender Anzahl von ungültigen Paketen und FCS-Fehlern aus

Inhalt

Problem

Wenn MACSec XPN zwischen einem Catalyst 9500-28C8D und einem Nexus N9K-C93180YC-FX aktiviert ist, wird die MKA-Sitzung erfolgreich eingerichtet, aber es wird kein Datenverkehr über die Verbindung weitergeleitet. Der Catalyst 9500 meldet eine Erhöhung der Anzahl der ungültigen Pakete unter den SA-Statistiken und FCS-Eingabefehlern an der physischen Schnittstelle. Im Einzelnen wurden diese Symptome beobachtet:

- Keine Verbindung nach Aktivierung von MACSec
- Die MKA-Sitzung wird wie gewohnt angezeigt, aber auf der Seite des Catalyst 9500 werden die SA-Statistiken mit "Ungültige Pkte 118" und "Gültige Pkte: 0"
- FCS-Eingabefehler werden auf der physischen Schnittstelle von Catalyst 9500 erhöht
- Das Entfernen der MACSec-Konfiguration stellt sofort die Verbindung wieder her und stoppt FCS-Fehler

Die MKA-Sitzungen wurden auf beiden Geräten eingerichtet und erfolgreich mit der GCM-AES-XPN-256-Verschlüsselung ausgehandelt. Auf der Nexus-Seite war die Verschlüsselung aktiv, aber der Catalyst 9500 empfing verschlüsselte Pakete und lehnte sie aufgrund von Validierungsfehlern ab. Es wurden keine gültigen Pakete akzeptiert.

Umwelt

- Catalyst 9500-28C8D mit Cisco IOS®

- Nexus N9K-C93180YC-FX
- MACSec-XPB-Konfiguration mit der GCM-AES-XPB-256-Verschlüsselungs-Suite
- 400-Gigabit-Ethernet-Schnittstelle (FourHundredGigE1/0/15 auf Catalyst, Ethernet1/52 auf Nexus)
- Catalyst 9500 als Schlüsselserverpriorität 1 konfiguriert, Nexus als Schlüsselserverpriorität 100 konfiguriert
- AES-256-CMAC Verschlüsselungsalgorithmus für Pre-Shared Keys

Auflösung

Das Problem wurde durch die Implementierung einer Problemumgehung behoben, die die Zuweisung der Schlüsselserverrollen zwischen den Geräten ändert. Die empfohlene Lösung umfasst folgende Schritte:

Schritt 1: Identifizieren des Schlüsselserver-Konfigurationsproblems

Überprüfen Sie die aktuelle Schlüsselserver-Prioritätskonfiguration auf beiden Geräten. Die problematische Konfiguration ergab Folgendes:

Catalyst 9500-Konfiguration:

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

Nexus-Konfiguration:

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

Phase 2: Umgehung der SchlüsselsERVERrolle implementieren

Konfigurieren Sie das Nexus-Gerät anstelle des Catalyst 9500 als MACSec-SchlüsselsERVER. Dazu müssen die Prioritätswerte für den SchlüsselsERVER so angepasst werden, dass der Nexus die SchlüsselsERVERrolle übernimmt.

Ändern Sie die Nexus-Konfiguration so, dass die Priorität des SchlüsselsERVERs niedriger ist (niedrigere Werte haben höhere Priorität):

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

Ändern Sie die Catalyst 9500-Konfiguration so, dass die Priorität des SchlüsselsERVERs höher ist:

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

Schritt 3: MACSec-Betrieb überprüfen

Überprüfen Sie nach dem Implementieren der SchlüsselsERVER-Rollenänderung Folgendes:

- MKA-Sitzungen auf beiden Geräten erfolgreich eingerichtet
- Datenverkehr durchläuft die MACSec-fähige Verbindung
- Keine "ungültigen Pakete" in den Catalyst 9500 SA-Statistiken inkrementiert
- FCS-Eingabefehler treten nicht an der physischen Schnittstelle auf.

Diese Problemumgehung ermöglicht die ordnungsgemäße Funktion der MACSec XPX-Konfiguration, bis die Plattformuntersuchung und die Planung des Software-Upgrades abgeschlossen werden können.

Ursache

Die Ursache dieses Problems liegt in der Cisco Bug-ID CSCvs00410, die ein Szenario beschreibt, in dem MKA-Sitzungen erfolgreich eingerichtet wurden, Daten jedoch nicht über den Link übertragen werden können, wenn AES-256-XPN mit einem Catalyst 9500 in der Schlüsselserversrolle unter bestimmten Interoperabilitätsbedingungen mit Nexus-Geräten verwendet wird. Das Verhalten zeigt sich in einer nicht übereinstimmenden Validierung, bei der der Catalyst 9500 verschlüsselte Pakete vom Nexus zurückweist, was zu einer höheren Anzahl ungültiger Pakete und FCS-Fehlern führt. Es bestand eine bekannte Diskrepanz bezüglich der Auflistung von Cisco IOS als behoben für diesen Fehler, die einer weiteren Untersuchung durch das Catalyst Plattform-Team bedarf.

Verwandte Inhalte

- Cisco Bug-ID CSCvs00410 - MKA-Sitzung gestartet, jedoch keine Daten über Verbindung weiterleiten können, wenn AES-256-XPN mit Catalyst 9500-Schlüsselserversrolle verwendet wird

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.