

Verkeer van MACSec XPN mislukt tussen Catalyst 9500 en Nexus 9000 met toenemende ongeldige pakketten en FCS-fouten

Inhoud

uitgifte

Wanneer MACSec XPN is ingeschakeld tussen een Catalyst 9500-28C8D en een Nexus N9K-C93180YC-FX, wordt de MKA-sessie met succes tot stand gebracht, maar wordt er geen dataverkeer door de koppeling geleid. De Catalyst 9500 rapporteert toenemende "ongeldige punten" onder SA-statistieken en FCS-invoerfouten op de fysieke interface. In het bijzonder werden deze symptomen waargenomen:

- Geen connectiviteit nadat MACSec is ingeschakeld
- MKA-sessie wordt weergegeven zoals ingesteld, maar de Catalyst 9500-zijde toont SA-statistieken met "Niet geldige punten 118" en "Geldige punten: 0"
- FCS-invoerfouten nemen toe op de Catalyst 9500 fysieke interface
- Als u de MACSec-configuratie verwijdert, wordt de connectiviteit onmiddellijk hersteld en worden FCS-fouten gestopt

De MKA-sessies werden op beide apparaten ingesteld en met succes onderhandeld over GCM-AES-XPN-256-codering. De Nexus-kant toonde encryptie als actief, maar de Catalyst 9500 ontving versleutelde pakketten en wees ze af vanwege een validatie-mismatch, waardoor nul geldige pakketten werden geaccepteerd.

milieu

- Catalyst 9500-28C8D met Cisco IOS®
- Nexus N9K-C93180YC-FX

- MACSec XPN-configuratie met GCM-AES-XPN-256-coderingssuite
- 400 Gigabit Ethernet-interface (FourHundredGigE1/0/15 op Catalyst, Ethernet1/52 op Nexus)
- Catalyst 9500 geconfigureerd als key-server prioriteit 1, Nexus geconfigureerd als key-server prioriteit 100
- AES-256-CMAC cryptografisch algoritme voor vooraf gedeelde sleutels

resolutie

Het probleem is opgelost door een tijdelijke oplossing te implementeren die de toewijzing van de sleutelserversrol tussen de apparaten wijzigt. De aanbevolen resolutie omvat de volgende stappen:

Stap 1: Identificeer het probleem met de sleutelserverconfiguratie

Controleer de huidige prioriteitsconfiguratie van de key-server op beide apparaten. De problematische configuratie toonde aan:

Configuratie Catalyst 9500:

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

Nexus-configuratie:

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

Stap 2: Implementeer Key-Server Role Workaround

Het Nexus-apparaat configureren als de MACSec-sleutelserver in plaats van de Catalyst 9500. Dit houdt in dat de prioriteitswaarden van de key-server worden aangepast, zodat de Nexus de key-server rol op zich neemt.

Wijzig de Nexus-configuratie om een lagere prioriteitswaarde voor de sleutel-server te hebben (lagere waarden hebben een hogere prioriteit):

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

Wijzig de Catalyst 9500-configuratie om een hogere prioriteitswaarde voor de sleutel-server te krijgen:

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

Stap 3: Controleer de werking van MACSec

Controleer na het implementeren van de rolwijziging voor de sleutel-server of:

- MKA-sessies worden op beide apparaten met succes ingesteld
- Het dataverkeer gaat via de MACSec-link
- Geen "ongeldige pkts" stijgen op de Catalyst 9500 SA statistieken
- FCS-invoerfouten treden niet op in de fysieke interface

Met deze tijdelijke oplossing kan de configuratie van MACSec XPN naar behoren functioneren totdat het platformonderzoek en de planning van de software-upgrade zijn voltooid.

Oorzaak

De hoofdoorzaak van dit probleem is gerelateerd aan Cisco Bug ID CSCvs00410, dat een

scenario beschrijft waarin MKA-sessies succesvol worden ingesteld, maar gegevens niet over de link kunnen gaan bij gebruik van AES-256-XPB met een Catalyst 9500 in de sleutelserversrol onder bepaalde interoperabiliteitsomstandigheden met Nexus-apparaten. Het gedrag manifesteert zich als een validatie-mismatch waarbij de Catalyst 9500 versleutelde pakketten van de Nexus afwijst, wat resulteert in toenemende ongeldige pakket aantallen en FCS-fouten. Er was een opmerkelijke discrepantie met betrekking tot Cisco IOS wordt vermeld als vast voor dit defect, waarvoor nader onderzoek door het Catalyst platform team.

Gerelateerde inhoud

- Cisco Bug ID CSCvs00410 - MKA-sessie omhoog, maar kan gegevens niet doorgeven via koppeling bij gebruik van AES-256-XPB met Catalyst 9500-sleutelserversrol

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.