MACSec MKA PDU Integrity Check-fouten oplossen op Nexus 9000-Switches

Inhoud

uitgeven

Media Access Control Security (MACSec) geconfigureerd tussen Nexus 9000-switches toont de MACsec Key Agreement (MKA)-sessie als "veilig", maar genereert ongeveer elke twee seconden herhaalde foutmeldingen. Het volgende patroon overspoelt de systeemlogboeken:

```
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
```

Deze afwisselende succes- en faalberichten creëren buitensporige logboekvermeldingen die moeten worden verholpen met behoud van de MACSec-functionaliteit.

milieu

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

resolutie

Om dit probleem op te lossen, wijzigt u de fallback-sleutelketenconfiguratie om andere sleutel-ID's te gebruiken dan die in de primaire sleutelketting zijn geconfigureerd:

1. Controleer uw bestaande MACSec-sleutelketenconfiguraties om overeenkomende sleutel-ID's

tussen primaire en terugvalsleutelhangers te identificeren met deze opdracht.

```
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. Wijzig de terugvalsleutelhanger om een andere sleutel-ID te gebruiken met deze opdrachten. Als de primaire sleutelhanger bijvoorbeeld sleutel-ID 01 gebruikt, configureert u de terugvalsleutelhanger om in plaats daarvan sleutel-ID 10 te gebruiken.

```
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. Controleer de systeemlogboeken om te bevestigen dat de afwisselende CTS_MKPDU_ICV_SUCCESS- en CTS_MKPDU_ICV_FAILURE-berichten niet meer worden weergegeven.

Oorzaak

De hoofdoorzaak is een configuratieconflict waarbij de fallback-sleutelhanger dezelfde sleutel-ID gebruikt als de primaire sleutelhanger. Dit creëert dubbelzinnigheid in het MKA-protocol, waardoor de integriteitscontrole afwisselend slaagt en faalt als het systeem switches tussen het evalueren van de primaire en de terugvalsleutels. De configuratiehandleiding van de Nexus MACSec vermeldt: "De ID van de terugvalsleutel mag niet overeenkomen met een ID van een primaire sleutelhanger" om dit conflict te voorkomen.

Verwante inhoud

- Configuratiehandleiding voor Nexus MACSec
- Cisco Technical Support en downloads

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.