Resolve MACSec MKA PDU Integrity Check Failures on Nexus 9000 Switches

Contents

Issue

Media Access Control Security (MACSec) configured between Nexus 9000 switches shows the MACsec Key Agreement (MKA)
session as "secure" but generates repeated error messages approximately every two seconds. The following pattern fl

```
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
```

These alternating success and failure messages create excessive log entries that need to be remediated while maintain

Environment

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

Resolution

To resolve this issue, modify the fallback keychain configuration to use different key IDs than those configured in th

1.
Review your existing MACSec keychain configurations to identify matching key IDs between primary and fallback with this command.

```
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. Change the fallback keychain to use a different key ID with these commands. For example, if the primary keychain uses key ID 01, configure the fallback keychain to use key ID 10 i

```
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.
Monitor the system logs to confirm that the alternating CTS_MKPDU_ICV_SUCCESS and CTS_MKPDU_ICV_FA

Cause

The root cause is a configuration conflict where the fallback keychain uses the same key ID as the primary keychain. This creates ambiguity in the MKA protocol, causing the integrity check to alternately succeed and fail as the system switches between evaluating the primary and fallback keys. The Nexus MACSec Configuration Guide states, "The fallback key ID should not match any key ID from a primary keychain" to prevent this conflict.

Related Content

- Nexus MACSec Configuration Guide
- Cisco Technical Support & Downloads