

MACSec XPN Traffic Fails Between Catalyst 9500 and Nexus 9000 with Increasing Invalid Packets and FCS Errors

Contents

Issue

When MACSec XPN is enabled between a Catalyst 9500-28C8D and a Nexus N9K-C93180YC-FX, the MKA session establishes successfully but no data traffic passes through the link. The Catalyst 9500 reports increasing "Notvalid pkts" under SA statistics and FCS input errors on the physical interface. Specifically, these symptoms were observed:

- No connectivity after MACSec is enabled
- MKA session shows as established, but the Catalyst 9500 side shows SA Statistics with "Notvalid pkts 118" increasing and "Valid pkts: 0"
- FCS input errors increment on the Catalyst 9500 physical interface
- Removing the MACSec configuration immediately restores connectivity and stops FCS errors

The MKA sessions were established on both devices and successfully negotiated GCM-AES-XPN-256 cipher. The Nexus side showed encryption as active, but the Catalyst 9500 received encrypted packets and rejected them due to validation mismatch, resulting in zero valid packets being accepted.

Environment

- Catalyst 9500-28C8D running Cisco IOS®
- Nexus N9K-C93180YC-FX
- MACSec XPN configuration using GCM-AES-XPN-256 cipher suite
- 400 Gigabit Ethernet interface (FourHundredGigE1/0/15 on Catalyst, Ethernet1/52 on Nexus)
- Catalyst 9500 configured as key-server priority 1, Nexus configured as key-server priority 100
- AES-256-CMAC cryptographic algorithm for pre-shared keys

Resolution

The issue was resolved by implementing a workaround that changes the key-server role assignment between the devices. The recommended resolution involves these steps:

Step 1: Identify the Key-Server Configuration Issue

Verify the current key-server priority configuration on both devices. The problematic configuration showed:

Catalyst 9500 configuration:

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

Nexus configuration:

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

Step 2: Implement Key-Server Role Workaround

Configure the Nexus device as the MACSec key server instead of the Catalyst 9500. This involves adjusting the key-server priority values so that the Nexus assumes the key-server role.

Modify the Nexus configuration to have a lower key-server priority value (lower values have higher priority):

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

Modify the Catalyst 9500 configuration to have a higher key-server priority value:

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

Step 3: Verify MACSec Operation

After implementing the key-server role change, verify that:

- MKA sessions establish successfully on both devices
- Data traffic passes through the MACSec-enabled link
- No "Notvalid pkts" are incrementing on the Catalyst 9500 SA statistics
- FCS input errors are not occurring on the physical interface

This workaround allows the MACSec XPN configuration to function properly until platform investigation and software upgrade planning can be completed.

Cause

The root cause of this issue is related to Cisco Bug ID CSCvs00410, which describes a scenario where MKA sessions establish successfully but data cannot pass across the link when using AES-256-XPN with a Catalyst 9500 in the key-server role under certain interoperability conditions with Nexus devices. The behavior manifests as a validation mismatch where the Catalyst 9500 rejects encrypted packets from the Nexus, resulting in increasing invalid packet counts and FCS errors. There was a noted discrepancy regarding Cisco IOS being listed as fixed for this defect, requiring further investigation by the Catalyst platform team.

Related Content

- Cisco Bug ID CSCvs00410 - MKA session up but unable to pass data across link when using AES-256-XPN with Catalyst 9500 key-server role