Nexus 9000スイッチのMACSec MKA PDU整合性チェック障害の解決

内容

お問い合わせ内容

Nexus 9000スイッチ間で設定されたMedia Access Control Security(MACSec)では、MACsec Key Agreement(MKA)セッションが「セキュア」と表示されますが、約2秒ごとに繰り返されるエラーメッセージが生成されます。 次のパターンは、システムログをフラッディングします。

```
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
```

これらの成功メッセージと失敗メッセージが交互に発生することで、過剰なログエントリが作成され、MACSecの機能を維持しながらエントリを修復する必要があります。

環境

- 製品：Cisco Nexusスイッチ
- テクノロジー：MACSec（リンク暗号化）

解決策

この問題を解決するには、フォールバックキーチェーン設定を変更して、プライマリキーチェーンで設定されているものとは異なるキーIDを使用します。

1. 次のコマンドを使用して、既存のMACSecキーチェーン設定を確認し、プライマリとフォール

バックのキーチェーン間で一致するキーIDを特定します。

```
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. 次のコマンドを使用して、フォールバックキーチェーンを変更し、別のキーIDを使用します。 たとえば、プライマリキーチェーンでキーID 01を使用する場合、フォールバックキーチェーンでキーID 10を使用するように設定します。

```
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. システムログをモニタして、交互に発生するCTS_MKPDU_ICV_SUCCESSメッセージとCTS_MKPDU_ICV_FAILUREメッセージが表示されなくなったことを確認します。

原因

根本原因は、フォールバックキーチェーンがプライマリキーチェーンと同じキーIDを使用する設定の競合です。これにより、MKAプロトコルのあいまいさが生じ、システムがプライマリキーとフォールバックキーの評価を切り替える際に整合性チェックが交互に成功または失敗します。この競合を防ぐには、『Nexus MACSec Configuration Guide』に「The fallback key ID should not match any key ID from a primary keychain」と記載されています。

関連コンテンツ

- Nexus MACSec構成ガイド

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。