

Catalyst 9500とNexus 9000の間のMACSec XPNトラフィックが無効なパケットとFCSエラーの増加により失敗する

内容

問題

Catalyst 9500-28C8DとNexus N9K-C93180YC-FXの間でMACSec XPNを有効にすると、MKAセッションは正常に確立されますが、データトラフィックはリンクを通過しません。Catalyst 9500では、物理インターフェイスのSA統計情報とFCS入力エラーで「Notvalid pkts」の増加が報告されます。具体的には、次の症状が確認されました。

- MACSecを有効にした後に接続が確立されない
- MKAセッションは確立されたと表示されますが、Catalyst 9500側では、「Notvalid pkts 118」が増加し、「Valid pkts: 0」が表示されるSA統計情報が
- Catalyst 9500の物理インターフェイスではFCS入力エラーが増加します
- MACSec設定を削除すると、接続が直ちに復元され、FCSエラーが停止します

両方のデバイスでMKAセッションが確立され、GCM-AES-XPN-256暗号のネゴシエーションに成功しました。Nexus側では、暗号化がアクティブであると示されていますが、Catalyst 9500は暗号化されたパケットを受信し、検証の不一致のためにこれらを拒否したため、有効なパケットがゼロで受け入れられました。

環境

- Cisco IOS®が稼働するCatalyst 9500-28C8D
- Nexus N9K-C93180YC-FX
- GCM-AES-XPN-256暗号スイートを使用したMACSec XPN設定

- 400ギガビットイーサネットインターフェイス (Catalystでは400GigE1/0/15、NexusではEthernet1/52)
- Catalyst 9500はキーサーバプライオリティ1として設定され、Nexusはキーサーバプライオリティ100として設定されます。
- 事前共有キー用のAES-256-CMAC暗号化アルゴリズム

解決方法

この問題は、デバイス間のキーサーバの役割の割り当てを変更する回避策を実装することで解決されました。推奨される解決策は、次の手順で行います。

ステップ1：キーサーバの設定の問題を特定する

両方のデバイスで、現在のキーサーバのプライオリティ設定を確認します。問題のある設定は次のとおりです。

Catalyst 9500 の設定:

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

Nexusの設定：

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

ステップ2：キーサーバロールの回避策の実装

Catalyst 9500ではなく、NexusデバイスをMACSecキーサーバとして設定します。これには、

Nexusがキーサーバの役割を引き継ぐようにキーサーバのプライオリティ値を調整することが含まれます。

Nexusの設定を変更して、キーサーバのプライオリティ値を小さくします（値が小さいほど、プライオリティは高くなります）。

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

Catalyst 9500の設定を変更して、キーサーバのプライオリティ値を高くします。

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

ステップ3:MACSecの動作の確認

キーサーバの役割の変更を実装した後、次の点を確認します。

- 両方のデバイスでMKAセッションが正常に確立される
- データトラフィックはMACSec対応リンクを通過します
- Catalyst 9500のSA統計情報で「Notvalid pkts」が増加していない
- FCS入力エラーが物理インターフェイスで発生していない

この回避策により、プラットフォームの調査とソフトウェアアップグレードの計画が完了するまで、MACSec XPNの設定が正しく機能するようになります。

原因

この問題の根本原因は、Cisco Bug ID CSCvs00410に関連しています。これは、Nexusデバイスとの特定の相互運用性条件下で、キーサーバロールでCatalyst 9500とAES-256-XPNを使用する場合に、MKAセッションは正常に確立されるが、データがリンクを通過できないというシナリオを

説明しています。この動作は、Catalyst 9500がNexusからの暗号化されたパケットを拒否し、その結果、無効なパケット数とFCSエラーが増加するという、検証の不一致として現れます。この不具合で修正済みとしてリストされているCisco IOSについては明らかに食い違いがあり、Catalystプラットフォームチームによる調査が必要です。

関連コンテンツ

- Cisco Bug ID CSCvs00410:Catalyst 9500キーサーバロールでAES-256-XPNを使用すると、MKAセッションは確立されるが、リンクでデータを渡すことができない

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。