CDP URLが複数のCRLダウンロードURLと一致しないために発生するIOS XE証明書検証エラーの解決

内容

問題

追加のCRLダウンロードURLの場所がDynamic Multipoint VPN(DMVPN)ハブデバイスに追加されると、IKEネゴシエーションの失敗が原因で一部のスポークトンネルが確立に失敗し、ハブに次のエラーが記録されます。

```
%PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed
```

証明書チェーンの検証は成功し、CRLは正常にダウンロードされますが、失効チェックは次のエラーで失敗することがあります。

```
No CRL found with matching CDP
revocation status = 2
```

この問題は、DMVPNハブルータが、同じCRLファイルを指す複数の証明書失効リスト(CRL)ダウンロードURLの場所を使用する場合に発生します。CRLのダウンロード場所にはIPベースとFQDNベースの両方のURLが含まれますが、スポークルータに発行された証明書のCRL分散ポイント(CDP)にはFQDNベースのURLしかありません。

環境

- 証明書ベースのIKE認証を使用してIPSecが設定されたIOS® XEソフトウェアを実行するシスコデバイス。

- 同じCRLファイルをホストするIPベースおよびFQDNベースの両方のURLを持つ複数のCRLダウンロード場所。
- ピアデバイスに対して発行された証明書には、CDP内に1つのURLしかありません。
- 証明書失効チェックの強制実行中に証明書ベースの認証を使用するIPsecトンネル構成。

解決方法

この問題を解決するには、PKI環境全体で単一の正規のCDP URLを標準化し、CRL検証中にURLが正確に一致するようにします。

推奨される実装手順

1. ハブ構成からIPベースのCRLダウンロードURLを削除する（それらのIPベースのCRL URLが証明書CDPに含まれていない場合）

```
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA1.crl
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA2.crl
```

2. スポーク証明書のCDPと一致するFQDNベースのCRLダウンロードURLのみを設定する

```
crypto pki crl download url http://crl.examplecompnay.com/prod/Example%20Company%20Issuing%20CA1.crl
crypto pki crl download url http://crl.examplecompany.com/prod/Example%20Company%20Issuing%20CA2.crl
```

3. 発行側のCAテンプレートを更新して、一貫したCDP URLを使用する

発行側のCAテンプレートが、FQDNベースのCDP URLだけを新しく発行された証明書にスタンプしていることを確認します。

4. ハブおよびスポーク証明書の再登録（新しいCDP URLに変更する場合）

新しいCDP URLを実装する場合は、発行側CAを変更して新しいCDP URLを発行し、ハブ証明書とスポーク証明書の両方を再登録して新しいURLを伝達します。

冗長性の実装

CRLプロバイダーの冗長性について、たとえば、同じCRLを異なるURLの場所で発行して、ホスティングデバイスの障害から保護するには、次のコマンドを使用して、単一のFQDNの背後にバックエンドの冗長性を実装します。

- DNSフェールオーバー
- ロードバランサ
- 冗長CRLインフラストラクチャ

IOS XEは、同じCRLファイルを参照している場合でも、異なるホスト名/IPを異なるCDPとして扱うため、異なるホスト名/IPを持つ複数のCDPを使用しないでください。

確認

変更を実装した後、CRLのキャッシングとトンネルの確立を確認します。

```
show crypto pki crl
```

IKEv2セッションが正常に確立されたことを確認します。

```
show crypto session details
```

原因

この問題は、CRL検証中のIOS XEの正確なCDP URL照合動作によって引き起こされます。revocation-check crlを有効にしてピア証明書を検証する場合、IOS XEは検証対象の証明書に埋め込まれたCDP URLと、ハブの解析されたCRLキャッシュに保存されているCRLに関連付けられたCDP URLの間で、正確な文字列照合を実行します。

次の障害シーケンスが発生します。

1. ハブは、IPベースのCDP URLを使用してCRLを正常にダウンロードし、そのURLの下に内部的にキャッシュします。
2. スポーク証明書は、CDPでFQDNベースのURLを参照します。
3. 失効検証中、IOS XEはFQDN URLに一致するキャッシュされたCRLを検索します。
4. IOS XEはIPベースとFQDNベースのURLを異なるCDPとして扱うため、完全に一致するURLは見つかりませんでした。
5. ルータは、「No CRL found with matching CDP」を失効ステータス= 2で返します。
6. 証明書の検証が%PKI-3-CERTIFICATE_INVALIDで失敗します。

IOS XEは、同じ発行者に対して同じCRLコンテンツを返す場合でも、異なるURL形式（IPとFQDN）を同等として正規化しません。

関連コンテンツ

- 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。