証明書満了期限と自動登録による Cisco IOS CA への自動再登録

内容

概要

すべてのデジタル証明書には、登録時に発行側の認証局(CA)サーバによって割り当てられた証明書に有効期限が組み込まれています。ISAKMPのVPN IPSec認証にデジタル証明書が使用されている場合、通信デバイスの証明書の有効期限とデバイス（VPNエンドポイント）のシステム時間が自動的にチェックされます。 これにより、使用されている証明書が有効であり、有効期限が切れていないことが確認されます。また、各VPNエンドポイント(ルータ)で内部クロックを設定する必要があるのも理由です。 VPN暗号化ルータでNetwork Time Protocol(NTP)(またはSimple Network Time Protocol(SNTP))が使用できない場合は、手動で**set clockコマンドを使用**します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、該当するプラットフォーム（Cisco IOSソフトウェアリリース12.1.2.1）のcXXXX-advsecurityk9-mz.123-5.9.Tイメージを実行するすべてのルータに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

デジタル証明書が期限切れまたは期限切れでないと見なされるのはいつですか。

- システム時刻が証明書の有効期限より後であるか、証明書の発行時刻より前である場合、証明書は期限切れ（無効）になります。
- システム時刻が証明書の発行時刻と証明書の期限切れ時刻の間である場合、証明書は期限切れではありません（有効）。

自動登録機能の目的は、現在登録されているルータがルータ証明書のライフタイムの設定済みパーセンテージでCAサーバに自動的に再登録できるようにするメカニズムをCA管理者に提供することです。これは、制御メカニズムとしての証明書の管理性とサポート性にとって重要な機能です。特定のCAを使用して、1年間のライフタイム（自動登録なし）を持つ数千のブランチVPNルータに証明書を発行した場合、発行された時間のちょうど1年で、すべての証明書が期限切れになり、すべてのブランチがIPSec経由で接続できなくなります。また、この例のように自動登録機能が「auto-enroll 70」に設定されている場合、発行された証明書の有効期間（1年）の70 %で、各ルータはトラストポイントにリストされているCisco IOS® CAサーバに新しい登録要求を自動的に発行します。

注：自動登録機能の例外の1つは、10以下に設定されている場合*は、数分*で完了することです。10より大きい*場合*は、証明書の有効期間のパーセンテージです。

Cisco IOS CA管理者が自動登録で認識する必要がある注意事項がいくつかあります。再登録を成功させるには、次のアクションを実行する必要があります。

1. Cisco IOS CAサーバで各再登録要求を手動で許可または拒否します（Cisco IOS CAサーバで「grant auto」が使用されていない場合）。Cisco IOS CAサーバは、これらの要求を許可または拒否する必要があります（Cisco IOS CAで「grant auto」が有効になっていないことを前提としています）。 ただし、再登録プロセスを開始するために、登録ルータに対する管理アクションは必要ありません。
2. 必要に応じて、新しい再登録証明書を再登録VPNルータに保存します。ルータで保留中の未保存の設定変更がない場合、新しい証明書は自動的に不揮発性RAM(NVRAM)に保存されます。 新しい証明書がNVRAMに書き込まれ、以前の証明書が削除されます。保留中の未保存の設定変更がある場合は、登録ルータで**copy run start**コマンドを発行して、設定変更と新しい再登録証明書をNVRAMに保存する必要があります。**copy run startコマンドが完了**すると、新しい証明書がNVRAMに書き込まれ、以前の証明書が削除されます。**注：新し**い再登録が成功した場合、はCAサーバ上の登録済みデバイスの以前の証明書を取り消しません。VPNデバイスが通信する際に、相互に証明書シリアル番号（一意の番号）を送信します。**注：例え**ば、証明書のライフタイムの70 %で、VPNブランチがCAに再登録する場合、そのCAには、そのホスト名に対する2つの証明書があります。ただし、登録ルータには1台（新しいルータ）しかありません。 選択した場合は、古い証明書を管理上の目的で取り消すか、または証明書の有効期限を通常どおりに切れるようにします。**注：自動登録**機能の新しいコードバージョンには、登録に使用するキーペアを「再生成」するオプションがあります。このオプションは、キーペアを再生成するために「デフォルトではありません」です。このオプションを選択した場合は、Cisco Bug ID CSCea90136（登録ユーザ専用）に注意してください。このバグ修正により、既存のIPSecトンネル（古いキーペアを使用する証明書）を介して新しいキーペアをを一時ファイルににに登録できます。自動登録には、認定の更新時に新しいキーを生成するオプションがあります。現在、これにより、新しい証明書の取得に要する時間にサービスが失われます。これは、新しいキーが存在するが、それに一致する証明書がないためです。この機能は、新しい証明書が使用可能になるまで、古いキーと証明書

を保持します。手動による登録のために、キーの自動生成も実装されています。キーは、自動登録または手動登録のために必要に応じて生成されます。見つかったバージョン – 12.3PIH03修正対象バージョン – 12.3T適用対象バージョン – 12.3PI03統合 – なし詳細については、シスコテクニカルサポートにお問い合わせください。

関連情報

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems