目次

概要

有効期限に構築されるすべてのデジタル証明書に登録の間に発行認証局（CA）サーバによって割り当てられる認証であります。 デジタル認証が ISAKMP の VPN IPSec 認証のために使用されたりとき、デバイス（VPN エンドポイント）に通信 デバイスの認証満了時間およびシステムの時刻の自動検査があります。 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。 それはまた各 VPN エンドポイント（ルータ）の内部クロックをなぜ設定 する*必要があるか*です。 Network Time Protocol（NTP）（か簡易ネットワーク タイム プロトコル[SNTP]）VPN 暗号 ルータで可能性のあるではないです場合、手動**一定 clock コマンドを**使用して下さい。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報はそのそれぞれプラットフォームのための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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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。

デジタル認証はいつ考えられる切れたとまたは切れませんか。

- 認証はシステムの時刻が認証満了時間以降にまたは認証の発行された時の前にある場合期限

切れです（無効）。
- 認証はシステムの時刻が発行される認証時間および認証の切らされた時間にまたはの間にある場合期限切れではないです（有効な）。

自動登録機能の目的は現在登録されたルータが自動的にルータ認証のライフタイムの設定されたパーセントの CA サーバと再登録するようにメカニズムを CA 管理者に与えることです。 これは制御機構として認証の管理性/サポート可能性のための重要な機能です。 可能性としては発行すればのに特定の CA を 1 年ライフタイムのブランチ VPN ルータの桁に認証を（なしで自動登録して下さい）使用したら、丁度 1 年間の発行された時間で、認証すべては切れ、ブランチすべてはIPSec によって接続を失います。 また自動登録機能が「設定 されたら、発された認証（1 年）のライフタイムの 70% で 70"、次をこの例、そして、各ルータ自動的に発行します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登録して下さい。

注自動登録機能への 1 例外は *10 との等しいかまたはそれ以下*に設定 される場合ことです、分にあります。 *10 より大きい*場合、それはパーセントとしての認証のライフタイムです。

Cisco IOS CA 管理者が自動登録するわかっているとを必要がある警告があります。 管理者は成功する再登録のためのこれらの操作を実行する必要があります:

1. （「アクセス許可自動」が Cisco IOS CA サーバで使用されなかったら）手動で Cisco IOS CA サーバの各再登録要求を許可するか、または拒否して下さい。Cisco IOS CA サーバは依然として（Cisco IOS CA が有効に なる「アクセス許可自動」を備えていないという想定のもとで）これらの要求のそれぞれを与えるか、または拒否する必要があります。 ただし再登録プロセスを開始するために、登録ルータの管理行為が必要となりません。
2. 適切であれば再登録 VPN Router の新しい再登録された認証を保存して下さい。ルータで保留中の保存されていないコンフィギュレーション変更がない場合新しい認証は Non-volatile RAM （NVRAM）に自動的に保存されます。 新しい認証は NVRAM に書かれ、前の認証は削除されます。保留中の保存されていないコンフィギュレーション変更がある場合 NVRAM にコンフィギュレーション変更および新しい再登録された認証を保存するために登録ルータの **copy run start コマンドを**発行して下さい。 **copy run start コマンドが**完了すれば、そして新しい認証は NVRAM に書かれ、前の認証は削除されます。**注**新しい再登録が正常なとき、それはそれのための前の認証を CA サーバの登録されたデバイス取り消しません。 VPN デバイスが交信を行うとき、互いを認証通し番号（固有の番号）送信 します。**注**たとえば、認証のライフタイムの 70% にあり、VPN ブランチが CA と再登録することその CA にそのホスト名のための 2 つの認証があります。 ただし、登録ルータに 1 つがありますただ（より新しい 1）。 に選択する場合、管理上古い認証を取り消すことができますまたはそれが普通切れるようにして下さい。**注**自動登録機能のコードバージョンにオプションが登録に使用するキー ペアを「再生する」あります。このオプションはキー ペアを再生する「ないデフォルト」です。このオプションが選択された場合、Cisco バグ ID CSCea90136 を理解しておいて下さい。 このバグ修正は新しい証明書登録が（古いキー ペアを使用している）に既存の IPSecトンネル起こる間、新しいキー ペアがテンポラリファイルに置かれることができるように可能にします。auto-enroll 認証 更新時間に新しいキーを生成するオプションがあります。 現在新しい認証を得るために奪取 する時これによりサービスの損失を引き起こします。 これは New 鍵それと一致する認証がないが、という理由によります。この機能は新しい認証が利用できるまで古いキーおよび認証を保ちます。Automatic 鍵 生成はまた手動登録のために設定されます。 （ ）必要に応じてキーは自動か手動登録のために生成されます。見つけられるバージョン- 12.3PIH03固定内部 12.3T であるバージョンに適用されるバージョン- 12.3PI03統合された内部どれもその他の情報に関しては、連絡先 Cisco テクニカルサポート。

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