Cisco VPN 5000 シリーズ Concentrator での証明書の生成およびインストレーション

内容

概要

このドキュメントでは、Cisco VPN 5000シリーズコンセントレータで証明書を生成する方法、およびVPN 5000 Clientに証明書をインストールする方法について手順を追って説明します。

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、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN 5000コンセントレータソフトウェアバージョン5.2.16US
- Cisco VPN Client 5.0.12

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。

VPN クライアントのためのVPN 5000 Concentrator 証明

次に示す手順を実行します。

1. タイムサーバがない場合は、sys clockコマンドを使用して日付と時刻を設定する必要**があり**

ます。

```
RTP-5008# sys clock 12/14/00 12:15
```

日付と時刻が正しく設定されていることを確認するには、sys dateコマンドを実行します。

2. VPNコンセントレータの証明書ジェネレータ機能を有効にします。

```
RTP-5008# configure certificates

[ Certificates ]# certificategenerator=on

*[ Certificates ]# validityperiod=365
```

3. ルート証明書を作成します。

```
*RTP-5008# certificate generate root 512 locality rtp state nc
country us organization "cisco" commonname "cisco" days 365
```

4. サーバ証明書を作成します。

```
*RTP-5008# certificate generate server 512 locality rtp state nc
country us organization "cisco" commonname "cisco" days 365
```

5. 証明書を確認します。

```
*RTP-5008# certificate verify
```

6. Privacy Enhanced Mail(PEM)形式で証明書を表示し、その証明書をテキストエディタにコピーしてクライアントにエクスポートします。必ず、最初の行、最後の行、および最後の行の後のキャリッジリターンを含めてください。

```
*RTP-5008# show certificate pem root

-----BEGIN PKCS7-----

MIAGCSqGSIb3DQEHAqCAMIIBmAIBATEAMIAGAQAAAKCCAYYwggGCMIIBLKADAgEC

AgRAP0AJMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBAcTA3J0cDELMAkGA1UECBMC

bmMxCzAJBgNVBAYTAnVzMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY2lzY28o

HhcNMDAwNzE0MDYzOTIzWhcNMDEwNzE0MDYzOTIzWjBIMQwwCgYDVQQHEwNydHAx

CzAJBgNVBAgTAm5jMQswCQYDVQQGEwJ1czEOMAwGA1UEChMFY2lzY28xDjAMBgNV

BAMTBWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAML/buEqz3PnWQ5M6Seq

gE9uf7sZNUbHKZCp+GP9EpRkFuaYCD9vYZ3+MRTphiY55tDRmxTEglvK6l8sYIKd

XDcCAwEAATANBgkqhkiG9w0BAQQFAANBABuRHckNTXEAXSwyj7c5bEnAMCvI4Whd

ZRzVST5/QVRPjcaLXb0QJP47CzNecONfmM0bZ3n2nxBnbNDimJQbCgwxAAAAAAA=

-----END PKCS7-----
```

7. VPN Clientを開き、証明書認証用に設定します。
8. VPN ClientのConfigurationタブで、Addを選択します。
9. [Login Method] で[Certificate]を選択し、ログイン名とプライマリVPNサーバアドレス（または完全修飾ドメイン名）を入力します。 必要に応じて、セカンダリVPNサーバエントリを追加します。
10. 「OK」を選択し、「ログイン・プロパティ」ウィンドウを閉じます。
11. [Certificates] > [Import]に移動し、証明書がある場所を参照して証明書ファイルを選択します。
12. [ルート証明書(Root Certificates)]フィールドに証明書がリストされている状態で、VPN

Clientの[設定(Configuration)]タブをクリックします。

13. [Connect]ボタンを選択して、VPN接続を開始します。

関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- Cisco VPN 5000クライアント
- IPSec (IPセキュリティプロトコル)
- テクニカルサポート - Cisco Systems