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

目次

はじめに

この文書は方法 Cisco VPN 5000 シリーズ コンセントレータで証明書を生成すると方法に関するステップバイステップの説明が VPN 5000 クライアントで証明書をインストールする含まれています。

前提条件

要件

このドキュメントに関しては個別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くものです。

- 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

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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

次の手順を実行します。

1. タイム サーバーがない場合、**sys clock コマンド**を使用して日時を設定して下さい。
   ```
   RTP-5008# sys clock 12/14/00 12:15
   ```
   日時がきちんと設定されたことを確認するために、**sys date コマンドを**実行して下さい。
2. VPN コンセントレータの証明発行システム機能をイネーブルにして下さい。
   ```
   RTP-5008# configure certificates

   [ Certificates ]# certificategenerator=on

   *[ Certificates ]# validityperiod=365
   ```
3. ルート証明を作成して下さい。
   ```
   *RTP-5008# certificate generate root 512 locality rtp state nc
   country us organization "cisco" commonname "cisco" days 365
   ```
4. サーバ証明を作成して下さい。
   ```
   *RTP-5008# certificate generate server 512 locality rtp state nc
   country us organization "cisco" commonname "cisco" days 365
   ```
5. 証明書を確認して下さい。
   ```
   *RTP-5008# certificate verify
   ```
6. Privacy Enhanced Mail（PEM）フォーマットの証明書を表示し、次に輸出のためのテキスト工ディタにクライアントに証明書をコピーして下さい。 最終行の後で開始行、最終行およびキャリッジリターンを含むことを確かめて下さい。
   ```
   *RTP-5008# show certificate pem root

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

   MIAGCSqGSIb3DQEHAqCAMIIBmAIBATEAMIAGAQAAAKCCAYYwggGCMIIBLKADAgEC

   AgRAP0AJMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBAcTA3J0cDELMAkGA1UECBMC

   bmMxCzAJBgNVBAYTAnVzMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY2lzY28o

   HhcNMDAwNzE0MDYzOTIzWhcNMDEwNzE0MDYzOTIzWjBIMQwwCgYDVQQHEwNydHAx

   CzAJBgNVBAgTAm5jMQswCQYDVQQGEwJ1czEOMAwGA1UEChMFY2lzY28xDjAMBgNV

   BAMTBWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAML/buEqz3PnWQ5M6Seq

   gE9uf7sZNUbHKZCp+GP9EpRkFuaYCD9vYZ3+MRTphiY55tDRmxTEglvK6l8sYIKd

   XDcCAwEAATANBgkqhkiG9w0BAQQFAANBABuRHckNTXEAXSwyj7c5bEnAMCvI4Whd

   ZRzVST5/QVRPjcaLXb0QJP47CzNecONfmM0bZ3n2nxBnbNDimJQbCgwxAAAAAAA=

   -----END PKCS7-----
   ```
7. 証明書認証のためにそれを設定するために VPN クライアントを開いて下さい。
8. VPN クライアントの Configuration タブで、『Add』 を選択 して下さい。
9. ログイン方式のために『Certificate』 を選択 し、次にログインネームおよびプライマリ VPN サーバアドレス入力して下さい（またはドメイン ネームの絶対表記）。 セカンダリ VPN サーバエントリを必要ならば追加して下さい。
10. Login Properties ウィンドウを閉じるために『OK』 を選択 して下さい。
11. **Certificates > Import** に行き、証明書が見つけられる参照し、証明書ファイルを選択して下

さい位置に。

12. Root Certificates フィールドにリストされて証明書が VPN クライアントの Configuration タブをクリックして下さい。
13. VPN 接続を開始するために **Connect ボタンを**選択して下さい。

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発表
- Cisco VPN 5000 Client
- IPSec（IPセキュリティプロトコル）
- テクニカルサポート - Cisco Systems