デジタル証明書を使用した Windows 2000 と VPN 3000 コンセントレータ間の L2TP over IPSec の設定例

目次

概要

このドキュメントでは、L2TP/IPSec 組み込みクライアントを使用している Windows 2000 クライアントから VPN 3000 コンセントレータに接続する手順について順を追って説明します。 デジタル証明書（Certificate Enrollment Protocol（CEP）のないスタンドアロンのルート認証局（CA））を使用して VPN コンセントレータへの接続を認証していることを想定しています。 このドキュメントでは、説明のために Microsoft 証明書サービスを使用します。 それを設定する方法 のドキュメントのためのマイクロソフト社Webサイトを参照して下さい。

注: これは Windows 2000 画面の外観が変更できるのでだけ例です。

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 Cisco VPN 3000 コンセントレータ シリーズのためです。

目的

このプロシージャでは、これらのステップを完了します:

1. ルート証明を得て下さい。
2. クライアントのための ID証明を得て下さい。
3. Network Connection ウィザードの助けによって VPN 3000 への接続を作成して下さい。
4. VPN 3000 コンセントレータを設定して下さい。

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。

ルート証明を得て下さい

ルート証明を得るためにこれらの手順を完了して下さい:

1. ブラウザウィンドウを開き、Microsoft Certificate Authority （通常 http://servername か CA/certsrv の IP アドレス）のための URL を打ち込んで下さい。証明書検索および要求 ディスプレイのための Welcome ウィンドウ。
2. Welcome ウィンドウでタスクを選択し、『Retrieve the CA certificate or certificate revocation list』 を選択 し、『Next』 をクリック して下さい。
3. Retrieve the CA certificate or certificate revocation list ウィンドウから、左隅で『Install this CA certification path』 をクリック して下さい。これは信頼されたルート 認証機関ストアに CA 認証を追加します。 これはどの認証でもこのクライアントへのこの CA 問題信頼されることを意味します。

クライアントのための ID証明を得て下さい

クライアントのための ID証明を得るためにこれらのステップを完了して下さい:

1. ブラウザウィンドウを開き、Microsoft Certificate Authority のための URL を入力して下さい（通常 CA/certsrv の http://servername か IP アドレス）。証明書検索および要求 ディスプレイのための Welcome ウィンドウ。
2. Welcome ウィンドウから、タスクを選択し、『Request a certificate』 を選択 し、『Next』 をクリック して下さい。
3. Choose Request Type ウィンドウから、『Advanced request』 を選択 し、『Next』 をクリック して下さい。
4. 高度証明書要求 ウィンドウから、『Submit a certificate request to this CA using a form』 を選択 して下さい。
5. フィールド次をこの例記入して下さい。部門（組織ユニット）の値は VPN コンセントレー

タで設定されるグループを一致する必要があります。 大きいキーサイズをより 1024 規定しない で下さい。 **使用 ローカルマシンの記憶装置**にチェックボックスを選択することを忘れないでいて下さい。 終了したら、[Next] をクリックします。基づいて CA サーバがどのようにに設定されるか、このウィンドウは時々現われます。 それが場合、CA 管理者に連絡するため。

6. メインスクリーンに到達するために『Home』 をクリック し 『Check on pending certificate』 を選択 し、『Next』 をクリック して下さい。
7. [Certificate Issued] ウィンドウで、[Install this certificate] をクリックします。
8. クライアント 認証を表示するために、Start > Run の順に選択 し、Microsoft Management Console （ MMC ）を行います。
9. 『Console』 をクリック し、『Add/Remove Snap-in』 を選択 して下さい。
10. リストから『Add』 をクリック し、『Certificate』 を選択 して下さい。
11. 認証のスコープを頼むウィンドウが現われるとき、『Computer Account』 を選択 して下さい。
12. CA サーバの認証が信頼されたルート認証局の下にあることを確認して下さい。 また **> 個人的 > 認証ことをルート > 認証 (ローカル コンピュータ) を**『Console』 を選択 することによって認証があるこのイメージに示すようにことを、確認して下さい。

Network Connection ウィザードを使用して VPN 3000 への接続を作成して下さい

Network Connection ウィザードの助けによって VPN 3000 への接続を作成するためにこのプロシージャを完了して下さい:

1. **My Network Places を**右クリックし、『Properties』 を選択 し、『Make new connection』 をクリック して下さい。
2. Network Connection Type ウィンドウから、『Connect to a private network through the Internet』 を選択 し、次に『Next』 をクリック して下さい。
3. VPN コンセントレータのパブリックインターフェイスのホスト名か IP アドレスを入力し、『Next』 をクリック して下さい。
4. 接続有効時間帯で、『Only for myself』 を選択 し、『Next』 をクリック して下さい。
5. パブリックネットワーク ウィンドウで、最初 の 接続 (ISP アカウント) に自動的にダイヤルするためにかどうか選択して下さい。
6. Destination Address 画面で、VPN 3000 コンセントレータのホスト名か IP アドレスを入力し、『Next』 をクリック して下さい。
7. Network Connection Wizard ウィンドウで、接続の名前を入力し、『Finish』 をクリック して下さい。この例では、接続は指名されます「Cisco 団体 VPN」。と
8. Virtual Private Connection ウィンドウで、『Properties』 をクリック して下さい。
9. Properties ウィンドウで、Networking タブを選択して下さい。
10. Type of VPN server I am calling の下で、プルダウン メニューから『L2TP』 を選択 し、**インターネット プロトコル TCP/IP を**強調表示し、『Properties』 をクリック して下さい。
11. Advanced > Options > Properties の順に選択 して下さい。
12. IPセキュリティ ウィンドウで、『Use this IP security policy』 を選択 して下さい。
13. **クライアント (応答して下さい)** ポリシーをプルダウン メニューから選択し、Connect 画面に戻るまでだけ数回を『OK』 をクリック して下さい。
14. 接続を開始するために、ユーザ名 および パスワードを入力し、『Connect』 をクリック して下さい。

VPN 3000 コンセントレータの設定

ルート証明を得て下さい

VPN 3000 コンセントレータのためのルート証明を得るためにこれらのステップを完了して下さい:

1. CA にブラウザをポイントして下さい (通常 http://ip_add_of_ca/certsrv/) のような何かは、**CA 認証か証明書無効リストを取得し**、『Next』 をクリック します。
2. ローカルディスクでファイルをどこかに『Download CA certificate』 をクリック し、保存して下さい。
3. VPN 3000 コンセントレータで、Administration > Certificate Management の順に選択 し、**CA 認証を**『Click here to install a certificate』 をクリック し、**インストールして下さい。**
4. 『Upload File from Workstation』 をクリック して下さい。
5. ちょうどダウンロードした CA 認証 ファイルを『Browse』 をクリック し、選択して下さい。
6. ファイル名を強調表示し、『Install』 をクリック して下さい。

VPN 3000 コンセントレータのための ID証明を得て下さい

VPN 3000 コンセントレータのための ID証明を得るためにこれらのステップを完了して下さい:

1. ConfAdministration > Certificate Management > Enroll > Identity Certificate の順に選択 し、そして『Enroll via PKCS10 Request （ Manual ）』 をクリック して下さい。 ここに示されているように書式に記入し、『Enroll』 をクリック して下さい。ブラウザウィンドウは証明書要求とポップアップします。 それはこの出力と同じようなテキストが含まれている必要があります:
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```
2. ブラウザを CA サーバにポイントし、**要求を認証**チェックし、『Next』 をクリック して下さい。
3. **拡張要求を**チェックし、『Next』 をクリック し、『Submit a certificate request using a base64 encoded PKCS -10 file or a renewal request using a base64 encoded PKCS -7 file』 を選択 して下さい。
4. [Next] をクリックします。 テキスト領域で以前に示されている証明書要求のテキストをカット アンド ペーストして下さい。 [Submit] をクリックします。
5. 基づいて CA サーバがどのようにに設定されるか、『Download CA certificate』 をクリックすることができます。 またはすぐに認証が CA によって発行されたので、CA サーバに戻り、**保留中の認証のチェックを**チェックして下さい。
6. 『Next』 をクリック し、要求を選択し、再度『Next』 をクリック して下さい。
7. 『Download CA certificate』 をクリック し、ローカルディスクでファイルを保存して下さい。
8. VPN 3000 コンセントレータで、Administration > Certificate Management > Install，の順に

選択 し、『Install certificate obtained via enrollment』 をクリック して下さい。それから「進行中のステータスの Pending 要求を」、次このイメージ見ます。

9. 、**ワークステーションからのアップロード ファイル**によって続かれて『Install』 をクリック して下さい。
10. ファイルを『Browse』 をクリック し、選択して下さい CA によって発行される認証が含まれている。
11. ファイル名を強調表示し、『Install』 をクリック して下さい。
12. Administration > Certificate Management の順に選択 して下さい。 このイメージと同じような画面は現われます。

クライアントのためのプールを設定して下さい

クライアントのためのプールを設定するためにこのプロシージャを完了して下さい:

1. IP アドレスの利用可能 な 範囲を割り当てるために、ブラウザを VPN 3000 コンセントレータの内部インターフェイスにポイントし、Configuration > System > Address Management > Pools > Add の順に選択 して下さい。
2. 内部ネットワークのあらゆるその他のデバイスによって競合しない規定 し、『Add』 をクリック して下さい IP アドレスの範囲を。
3. VPN 3000 コンセントレータをプールを使用するように言うために Configuration > System > Address Management > Assignment の順に選択 し、**使用 アドレス プール** ボックスをチェックし、次このイメージ 『Apply』 をクリック して下さい。

IKEプロポーザルを設定して下さい

IKEプロポーザルを設定するためにこれらのステップを完了して下さい:

1. このイメージに示すようにパラメータを、Configuration > System > Tunneling Protocols > IPSec > IKE Proposals の順に選択 し、『Add』 をクリック し、選択して下さい。
2. 『Add』 をクリック し、右の列の新しい提案を強調表示し、『Activate』 をクリック して下さい。

SA を設定して下さい

Security Association （ SA ）を設定するためにこのプロシージャを完了して下さい:

1. Configuration > Policy Management > Traffic Management > SA の順に選択 し、『ESP-L2TP-TRANSPORT』 をクリック して下さい。この SA が利用できないか、または他の目的でそれを使用したら、この 1 と同じような新しい SA を作成して下さい。 SA の異なる設定は受諾可能です。 セキュリティポリシーに基づいてこのパラメータを変更して下さい。
2. **デジタル認証** プルダウン メニューの下で前もって設定したデジタル認証を選択して下さい。 **IKE-for-win2k** インターネット キー エクスチェンジ（ IKE ）提案を選択して下さい。**注**: これは必須ではないです。 L2TP/IPSec クライアントが VPN コンセントレータに接続するとき、ページ **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** のアクティブなカラムの下で設定されるすべての IKEプロポーザルは順序で試みられます。このイメージは SA のために必要とされる設定を示します:

グループおよびユーザを設定して下さい

グループおよびユーザを設定するためにこのプロシージャを完了して下さい:

1. [Configuration] > [User Management] > [Base Group] を選択します。
2. General タブの下で、**L2TP Over IPSec** がチェックされることを確かめて下さい。
3. IPSec タブの下で、**ESP-L2TP-TRANSPORT** SA 選択して下さい。
4. PPTP/L2TP タブの下で、すべての **L2TP 暗号化** オプションのチェックを外して下さい。
5. Configuration > User Management > Users の順に選択 し、『Add』 をクリック して下さい。
6. Windows 2000 クライアントから接続するのに使用するパスワードおよび名前を入力して下さい。 集団 選択の下で『Base Group』 を選択 することを確かめて下さい。
7. General タブの下で、**L2TP Over IPSec** トンネリング プロトコルをチェックして下さい。
8. IPSec タブの下で、**ESP-L2TP-TRANSPORT** SA 選択して下さい。
9. PPTP/L2TP タブの下で、すべての **L2TP 暗号化** オプションのチェックを外し、『Add』 をクリック して下さい。L2TP/IPSec Windows 2000 クライアントの助けによって接続現在できます。**注:** 基礎群を遠隔 L2TP/IPSec 結合を許可するために設定することを選択しました。 着信接続を許可するために SA の Organization Unit （ OU ） フィールドと一致するグループを設定することもまた可能性のあるです。 設定は同一です。

デバッグ情報

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1
```

```
288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
```

```
353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES
```

```
416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
```

```
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)
```

```
464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID
```

```
484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
```

```
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

トラブルシューティング情報

このセクションはそれぞれにおけるいくつかのよくある問題およびトラブルシューティングの方法を説明します。

- サーバは開始することができません。たぶん、IPSec サービスは開始しません。 Start > Programs > Administrative tools > Service の順に選択 し、**IPSec サービスが**有効に なることを確かめて下さい。

- Error 786: 有効なマシン認証無し。このエラーはローカルマシンの認証における問題を示唆します。 容易に認証を検知 するために、Start > Run の順に選択 し、MMC を実行して下さい。 『Console』 をクリック し、『Add/Remove Snap-in』 を選択 して下さい。 リストから『Add』 をクリック し、『Certificate』 を選択 して下さい。 認証のスコープを頼むウィンドウが現われるとき、『Computer Account』 を選択 して下さい。この場合 CA サーバの認証が**信頼されたルート認証局**の下にあることを確認できます。 **> 個人的 > 認証ことを**またこのイメージに示すように、**ルート > 認証 (ローカル コンピュータ) を**『Console』 を選択 することによって認証があることを確認できます。**認証を**クリックして下さい。 すべてが正しいことを確認して下さい。 この例では、認証と関連付けられるプライベートキーがあります。 ただし、この認証は切れました。 これは問題の原因です。
- Error 792: セキュリティ ネゴシエーション タイムアウト。長時間以降にこのメッセージが現れます。Cisco VPN 3000 コンセントレータ FAQ で説明されているように関連したデバッグをつけて下さい。 それらに目を通して下さい。 この出力と同じような何かを見る必要があります:
```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```
これは IKEプロポーザルが正しく設定されなかったことを示します。この資料の IKEプロポーザル セクションの設定からの情報を確認して下さい。
- Error 789: セキュリティレイヤはプロセスエラーに出会います。Cisco VPN 3000 コンセントレータ FAQ で説明されているように関連したデバッグをつけて下さい。 それらに目を通して下さい。 この出力と同じような何かを見る必要があります:
```
11315 02/15/2002 15:36:32.030
SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported
```

```
11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- 使用されるバージョンこの出力を表示するために Monitoring > System Status の順に選択 して下さい:

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB
```

関連情報

- IPSec ネゴシエーション/IKE プロトコル 製品サポート
- テクニカルサポート - Cisco Systems