ローカル認証でのVPN 3000 Concentrator PPTP の設定方法

目次

はじめに

Cisco VPN 3000 コンセントレータは、ネイティブの Windows クライアントに対して Point-to-Point Tunnel Protocol（PPTP）トンネリングをサポートしています。 保護された信頼性のある接続のために、これらの VPN のコンセントレータで使用できる 40 ビットおよび 128 ビットの暗号化をサポートしています。

Cisco Secure Access Control Server（ACS）を使用して拡張認証がある PPTP のユーザの VPN コンセントレータを設定するには、『Cisco Secure ACS for Windows の RADIUS 認証を使用した VPN 3000 コンセントレータの PPTP の設定』を参照してください。

前提条件

要件

この設定を試行する前に、『Cisco VPN 3000 コンセントレータで PPTP 暗号化がサポートされる条件』 に記載されている前提条件を満たしていることを確認します。

使用するコンポーネント

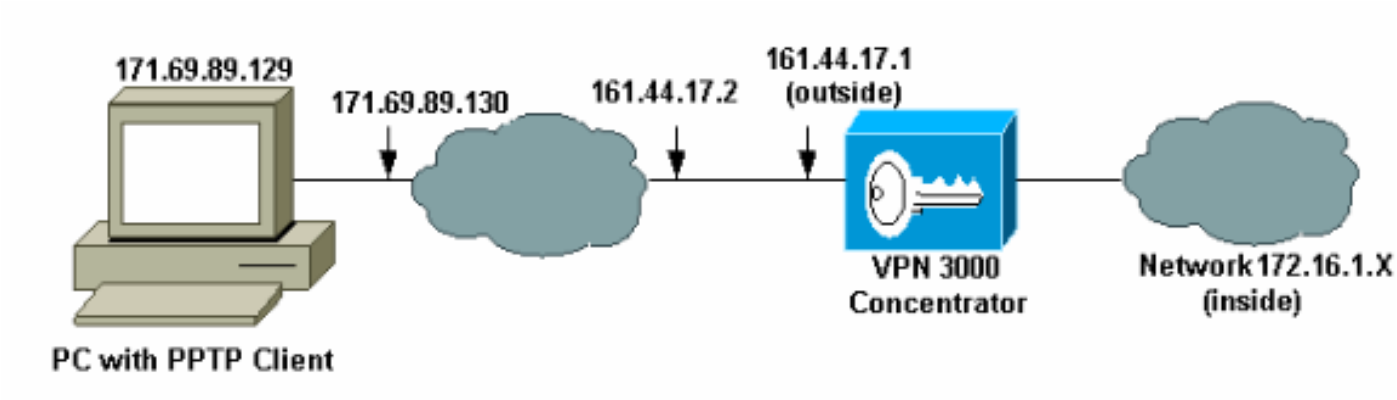
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 4.0.4.A の Cisco VPN 3015 コンセントレータ
- PPTP クライアントを使用する Windows PC

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。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



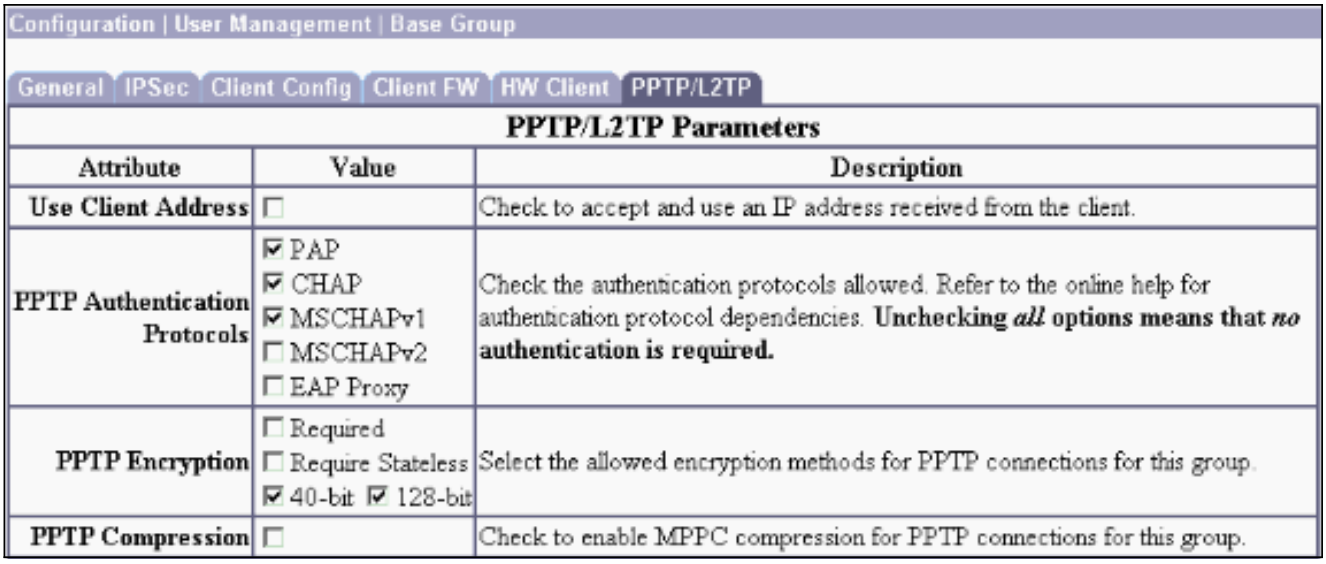
表記法

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。

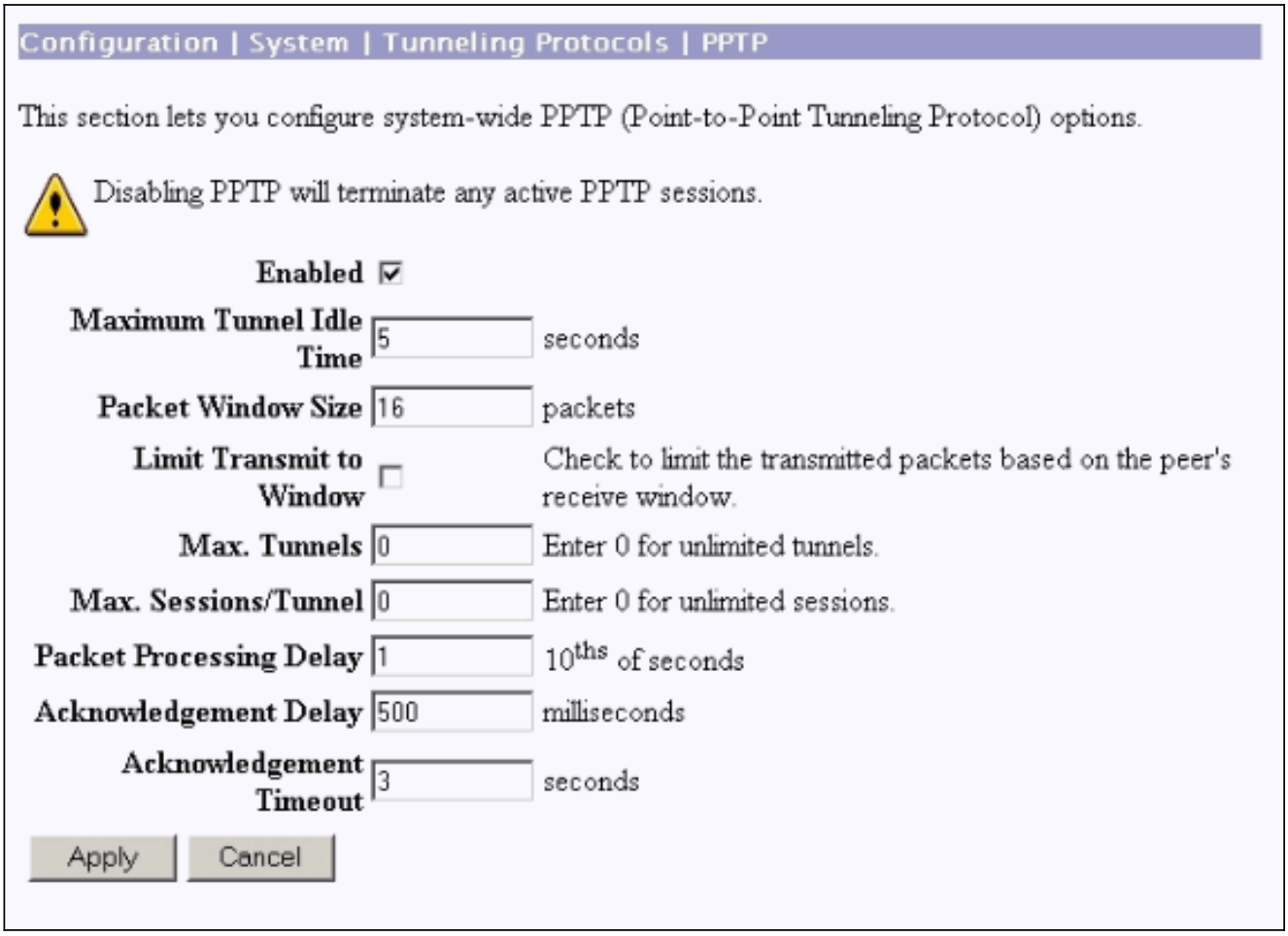
ローカル認証で VPN 3000 コンセントレータを設定する

VPN 3000 コンセントレータをローカル認証で設定するには、次の手順を実行します。

1. VPN コンセントレータで該当する IP アドレスを設定し、接続できることを確認します。
2. [Configuration] > [User Management] > [Base Group] の [PPTP/L2TP] タブで [PAP] 認証が選択されていることを確認します。



3. [Configuration] > [System] > [Tunneling Protocols] > [PPTP] の順に選択し、[Enabled] にチェックマークが付いていることを確認します。



4. [Configuration] > [User Management] > [Groups] > [Add] の順に選択し、PPTP グループを設定します。 この例では、グループ名は「pptpgroup」、パスワード（および確認用パスワード）は「cisco123」です。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Mode Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	pptpgroup	Enter a unique name for the group.
Password	**********	Enter the password for the group.
Verify	**********	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

Add | Cancel

5. グループの [General] タブで、[PPTP] オプションが認証プロトコルで有効になっていることを確認します。

Configuration | User Management | Base Group

General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		Enter the IP address of the secondary WINS server.

SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	☐	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

6. [PPTP/L2TP] タブで、[PAP] 認証を有効にし、[encryption] を無効にします（暗号化は、後からいつでも有効にすることができます）。

Configuration | User Management | Groups | Modify pptpgroup

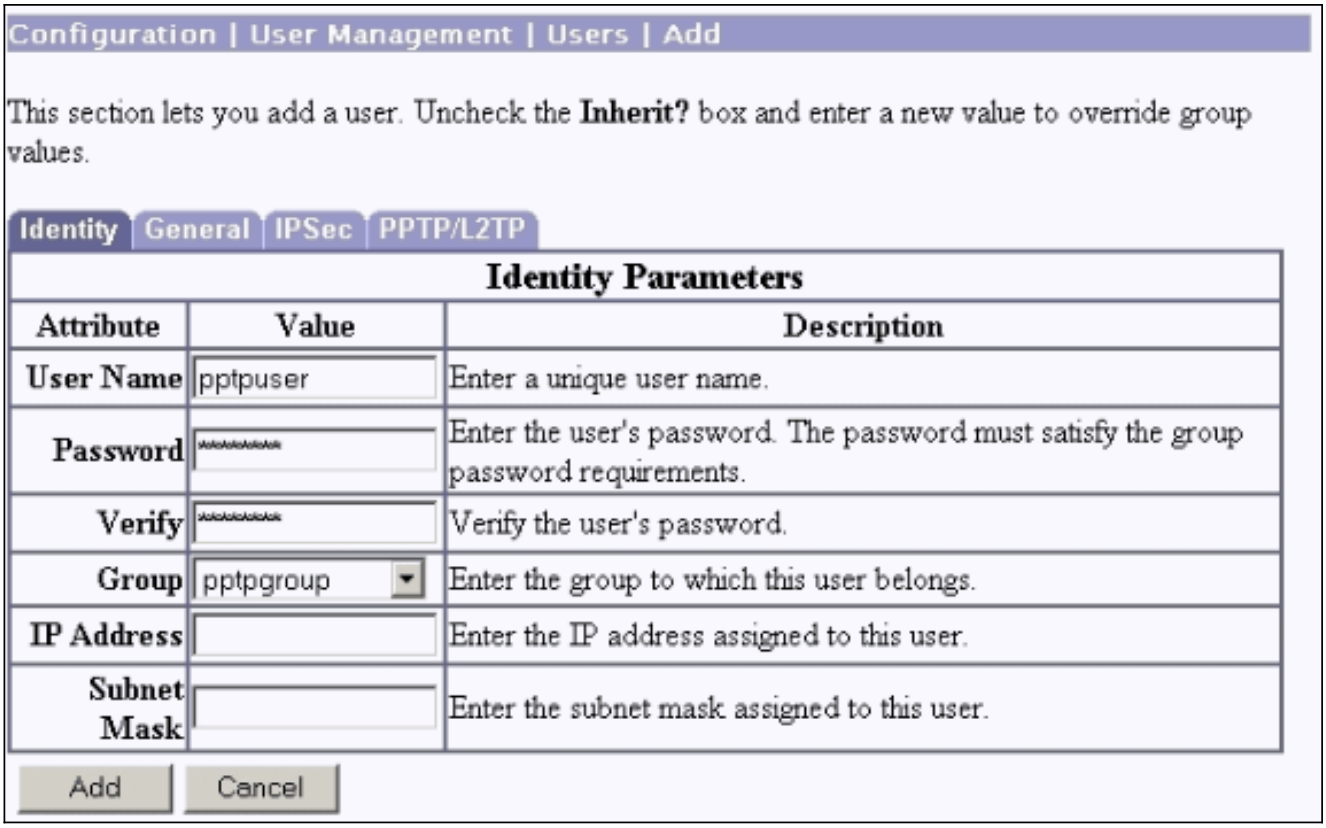
Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

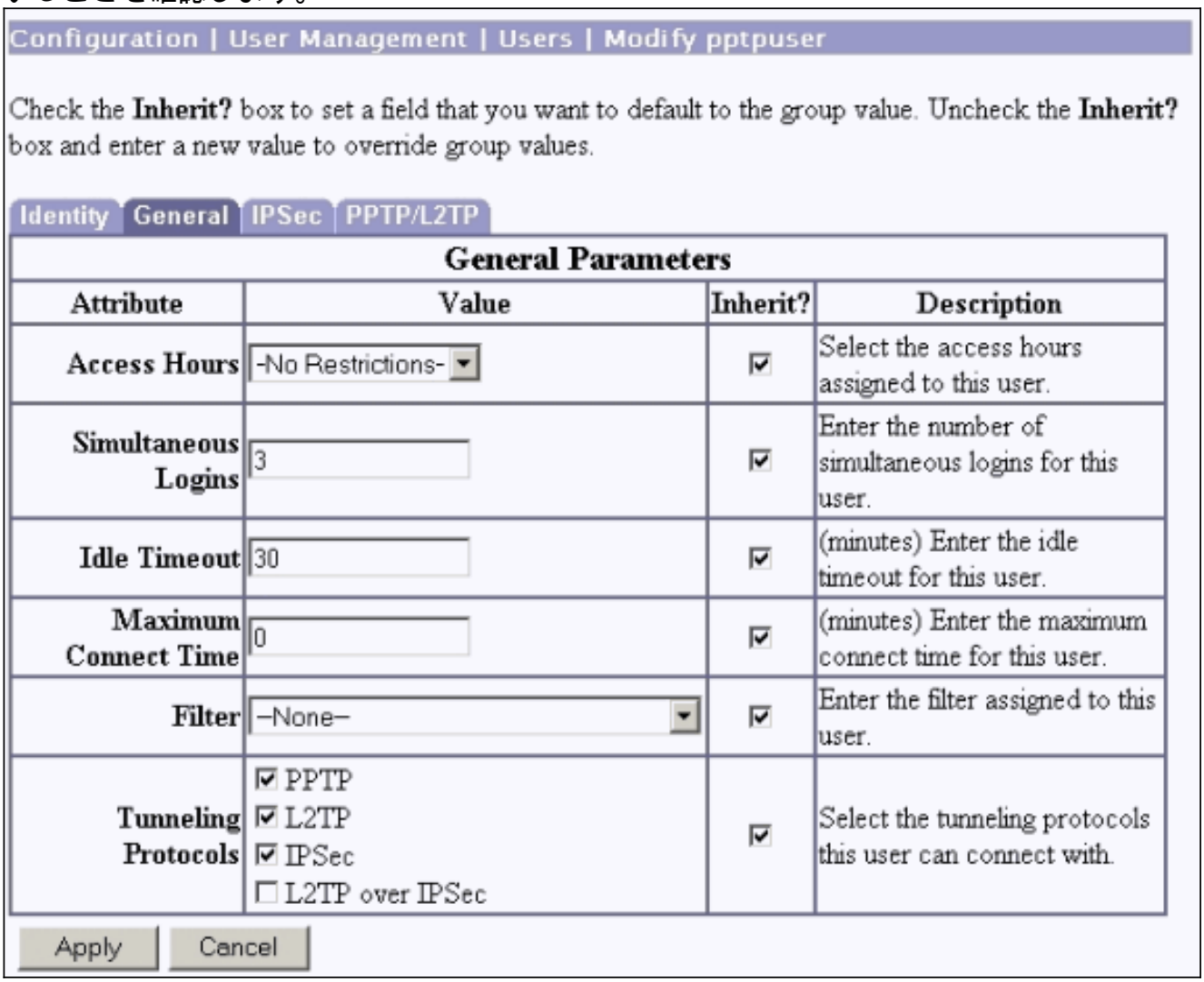
PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☑	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☐ Required ☐ Require Stateless ☐ 40-bit ☐ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

7. [Configuration] > [User Management] > [Users] > [Add] の順に選択し、PPTP 認証のためにローカル ユーザ（ユーザ名は「pptpuser」）をパスワード **cisco123** で設定します。 以前に定義した「pptpgroup」にユーザを入れます。

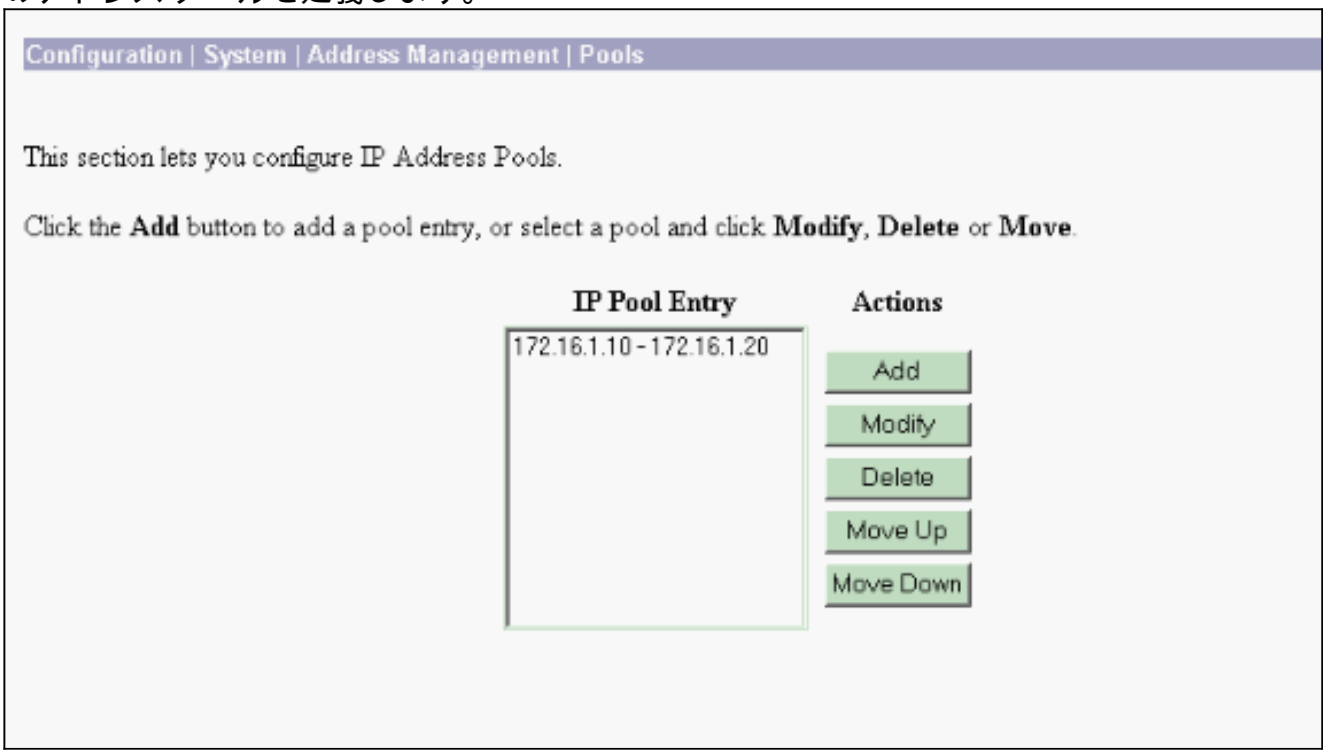


8. ユーザの [General] タブで、[PPTP] オプションがトンネリング プロトコルで有効になっていることを確認します。

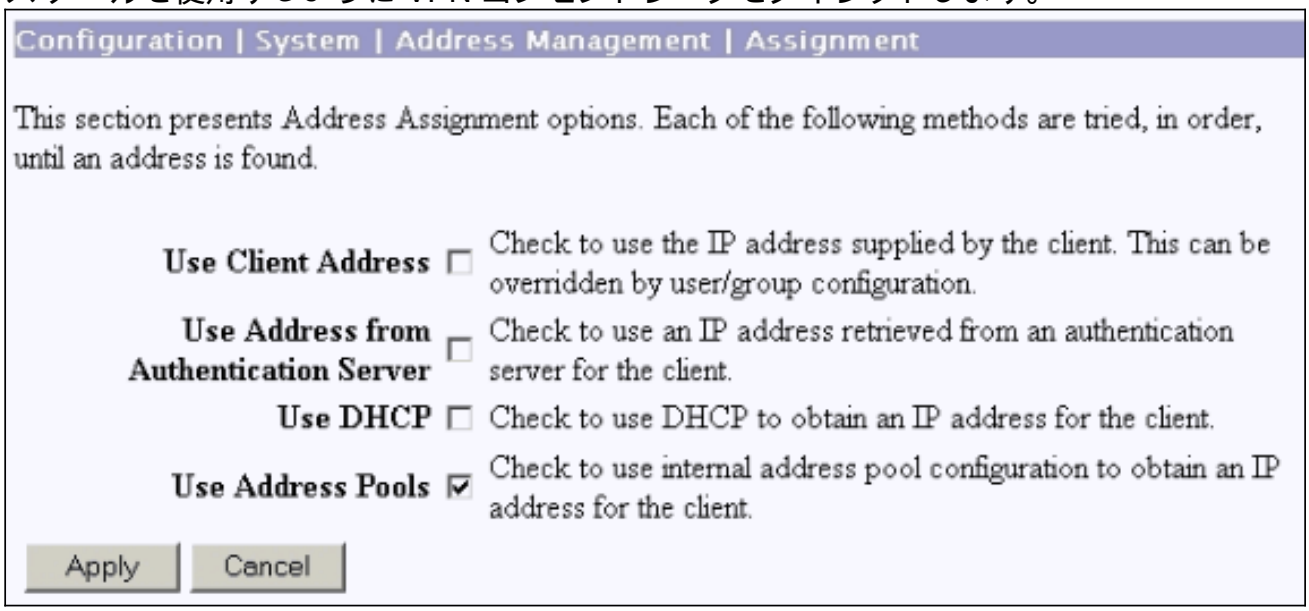


9. [Configuration] > [System] > [Address Management] > [Pools] の順に選択し、アドレス管理

のアドレス プールを定義します。



10. [Configuration] > [System] > [Address Management] > [Assignment] の順に選択し、アドレス プールを使用するように VPN コンセントレータをダイレクトします。



Microsoft PPTP クライアント設定

注: ここで説明している Microsoft ソフトウェアの設定に関するすべて情報は、Microsoft ソフトウェアに関する保証やサポートを伴うものではありません。 Microsoft ソフトウェアに関するサポートは、Microsoft から入手できます。

Windows 98 - PPTP 機能のインストールおよび設定

インストール

PPTP 機能をインストールするには、次の手順を実行します。

1. [Start] > [Settings] > [Control Panel] > [Add New Hardware (Next)] > [Select from List] > [Network Adapter (Next)] の順に選択します。
2. 左パネルで [Microsoft]、右パネルで [Microsoft VPN Adapter] を選択します。

設定

PPTP 機能を設定するには、次の手順を実行します。

1. [Start] > [Programs] > [Accessories] > [Communications] > [Dial Up Networking] > [Make new connection] の順に選択します。
2. [Select a device] プロンプトで [Microsoft VPN Adapter] を使用して接続します。 3000 トンネル エンドポイントは、VPN サーバ IP です。

Windows 98 のデフォルト認証では、パスワード暗号化 (たとえば、CHAP または MSCHAP) が使用されます。 最初にこの暗号化を無効にするには、[Properties] > [Server types] の順に選択し、[Encrypted Password] と [Require Data Encryption] ボックスのチェックマークを外します。

Windows 2000 - PPTP 機能の設定

PPTP 機能を設定するには、次の手順を実行します。

1. [Start] > [Programs] > [Accessories] > [Communications] > [Network and Dialup connections] > [Make new connection] の順に選択します。
2. [Next] をクリックし、[Connect to a private network through the Internet] > [Dial a connection prior] の順に選択します (LAN を使用する場合はこれを選択しないでください)。
3. 再び [Next] をクリックし、VPN 3000 コンセントレータの外部インターフェイスであるトンネル エンドポイントのホスト名または IP アドレスを入力します。 この例では、IP アドレスは 161.44.17.1 です。

パスワード タイプを PAP として追加するには、[Properties] > [Security for the connection] > [Advanced] の順に選択します。 デフォルトは、CHAP または PAP ではなく、MSCHAP と MSCHAPv2 です。

データの暗号化は、このエリアで設定できます。 最初は、ここで無効にします。

Windows NT

PPTP のために Windows NT クライアントを設定する方法の詳細については、Microsoft's website にアクセスしてください。

Windows Vista

PPTP 機能を設定するには、次の手順を実行します。

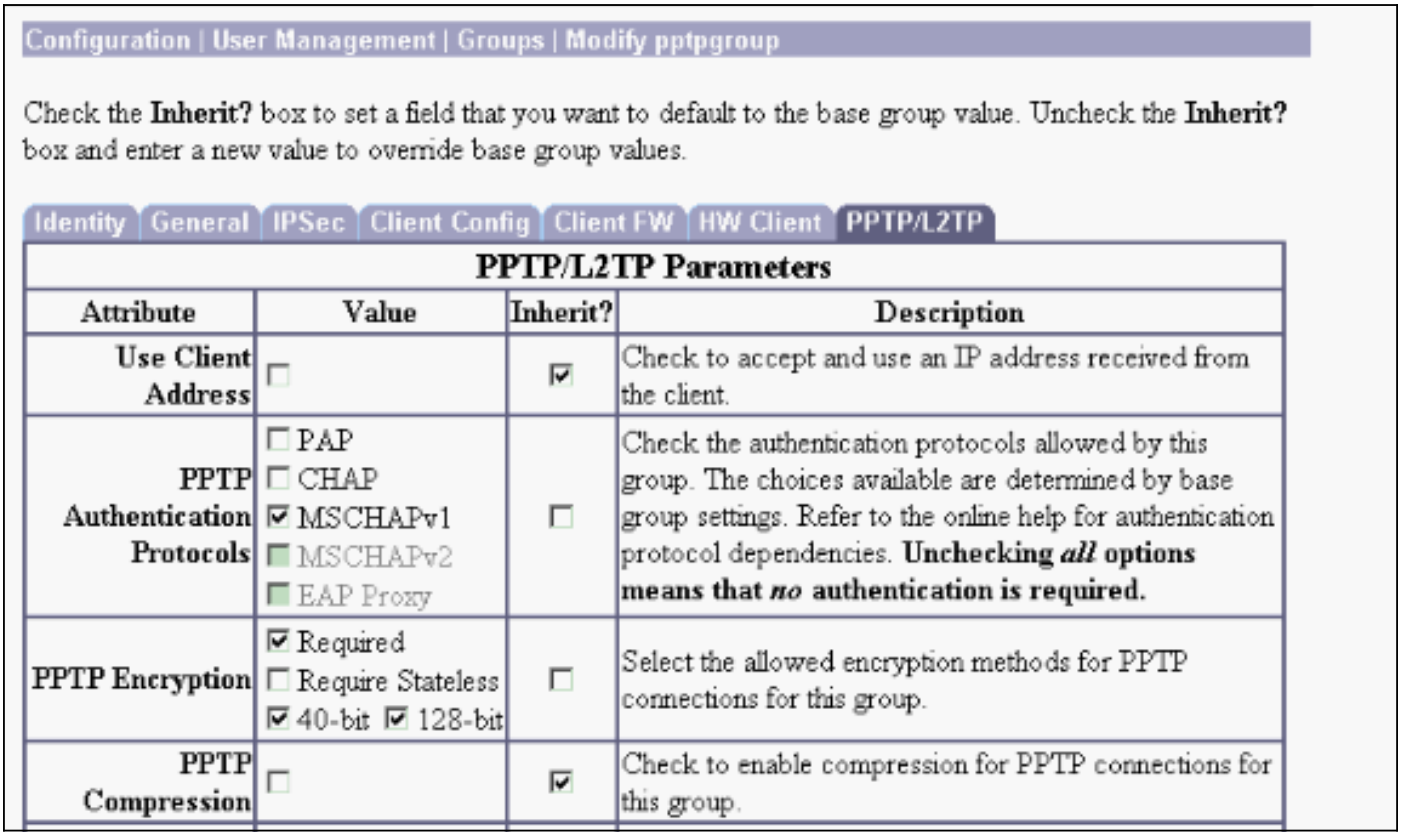
1. [Start] ボタンで [Connect To] を選択します。
2. [Set up a connection or network] を選択します。
3. [Connect to a workplace] を選択し、[Next] をクリックします。
4. [Use my Internet Connection (VPN)] を選択します。**注:** 「Do you want to use a connection that you already have」というプロンプトが表示されたら、[No, create a new connection] を

選択し、[Next]をクリックします。

5. [Internet Address] フィールドに、たとえば **pptp.vpn.univ.edu** などを入力します。
6. [Destination Name] フィールドに、たとえば **UNIVVPN** などを入力します。
7. [User Name] フィールドに、自分の UNIV Logon ID を入力します。 UNIV Logon ID は、**@univ.edu** の前にある電子メール アドレスの部分です。
8. [Password] フィールドに、自分の UNIV Logon ID のパスワードを入力します。
9. [Create] ボタン、[Close] ボタンの順にクリックします。
10. VPN 接続を作成した後、VPN サーバに接続するには、[Start] をクリックし、[Connect to] をクリックします。
11. ウィンドウで VPN 接続を選択し、[Connect] をクリックします。

MPPE（暗号化）の追加

暗号化を追加する前に、PPTP 接続が暗号化なしで動作することを確認します。 たとえば、接続が完了することを確認するために PPTP クライアントで [Connect] ボタンをクリックします。 暗号化が必要な場合は、MSCHAP 認証を使用する必要があります。 VPN 3000 で [Configuration] > [User Management] > [Groups] の順に選択します。 次に、グループの [PPTP/L2TP] タブで、[PAP] のチェックマークを外し、[MSCHAPv1] にチェックマークを付け、[Required for PPTP Encryption] にチェックマークを付けます。



PPTP クライアントは、オプションまたは必須のデータ暗号化と MSCHAPv1（オプションの場合）用として再設定する必要があります。

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

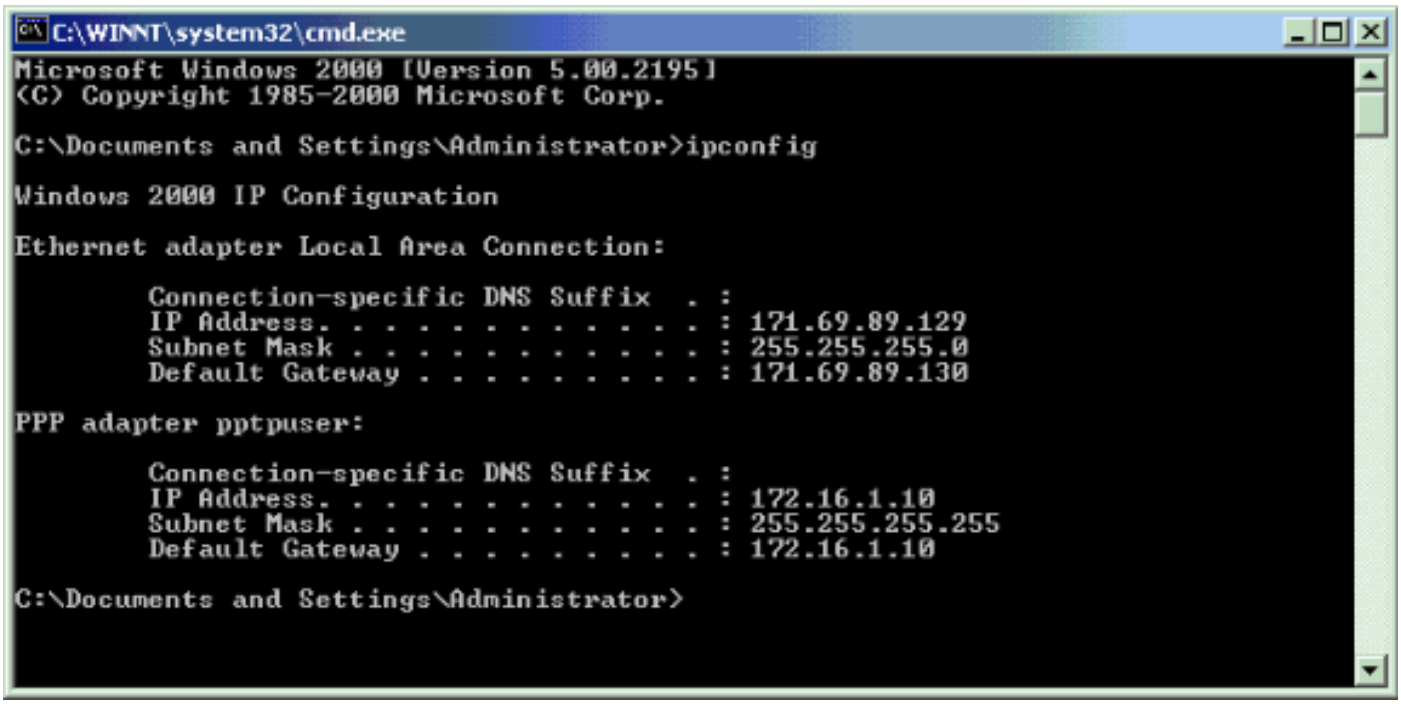
VPN コンセントレータの確認

前述の「Microsoft PPTP クライアント設定」セクションで作成した PPTP クライアントからダイヤルすることよって PPTP セッションを開始できます。

すべてのアクティブな PPTP セッションのパラメータと統計情報を表示するには、VPN コンセントレータの [Administration] > [Administer Sessions] ウィンドウを使用します。

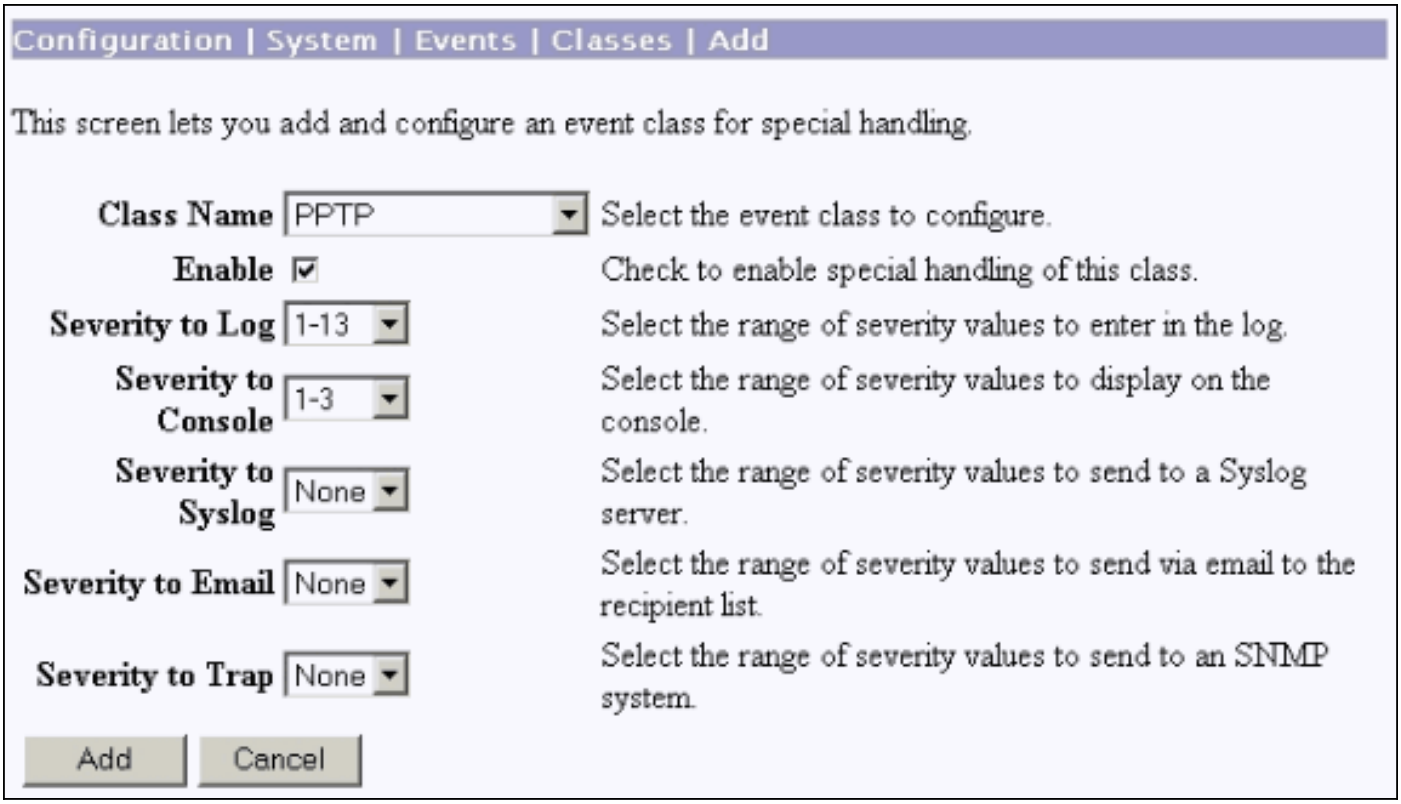
PC の確認

PC に 2 つの IP アドレスが設定されていることを確認するには、PC のコマンド モードで **ipconfig** コマンドを発行します。 1 つは PC 自体の IP アドレス、もう 1 つは IP アドレス プールから VPN コンセントレータによって割り当てられた IP アドレスです。 次の例では、IP アドレス 172.16.1.10 が VPN コンセントレータによって割り当てられた IP アドレスです。

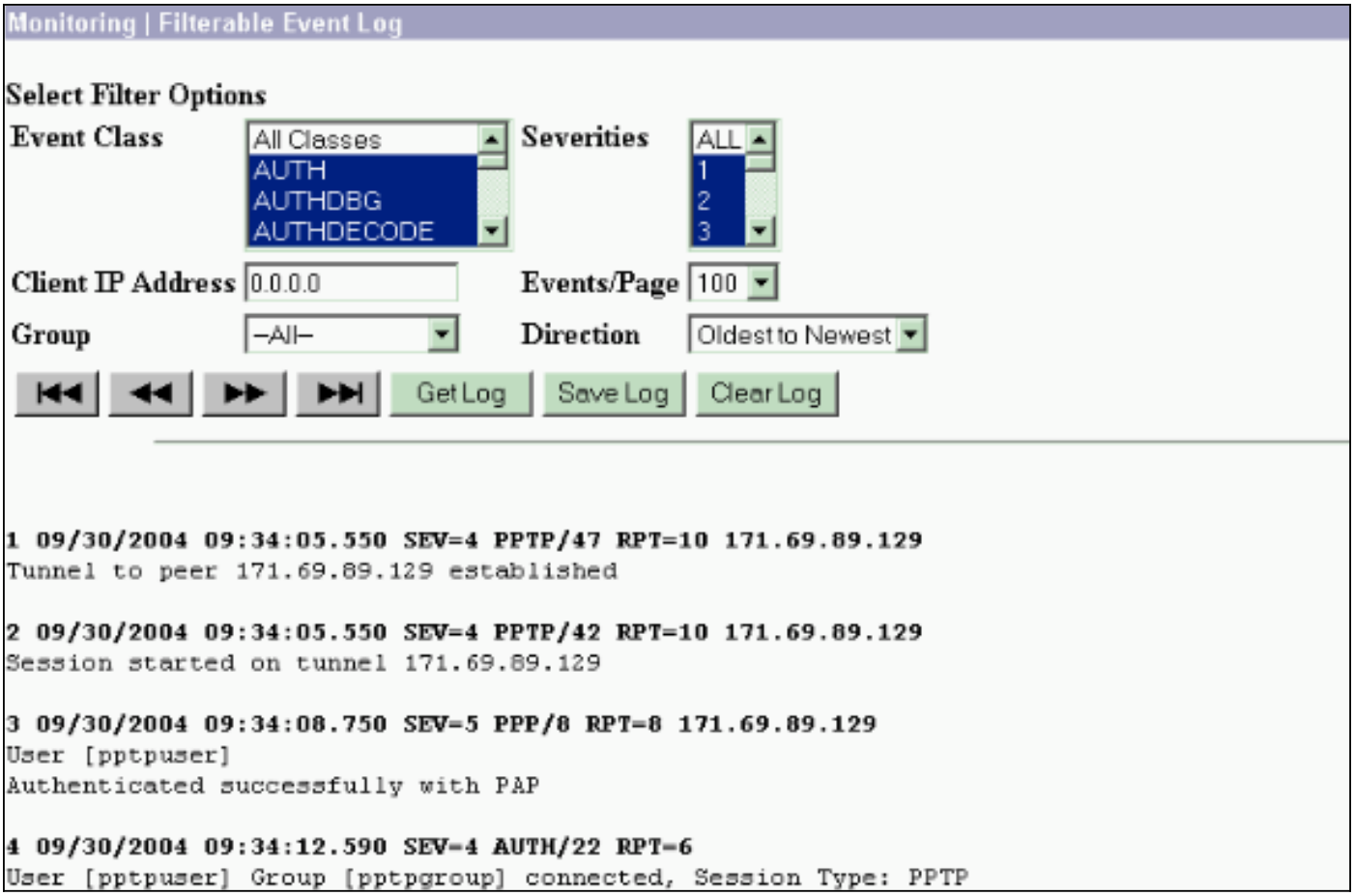


デバッグ

接続が正しく機能しない場合は、PPTP イベント クラスのデバッグ出力を VPN コンセントレータに追加できます。 [Configuration] > [System] > [Events] > [Class] > [Modify] または [Add] (図に表示) の順に選択します。 PPTPDBG と PPTPDECODE イベント クラスも使用できますが、これらは情報が多すぎる場合があります。



イベント ログは、[Monitoring] > [Event Log] で取得できます。



VPN 3000 デバッグ - 認証の成功

```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
```

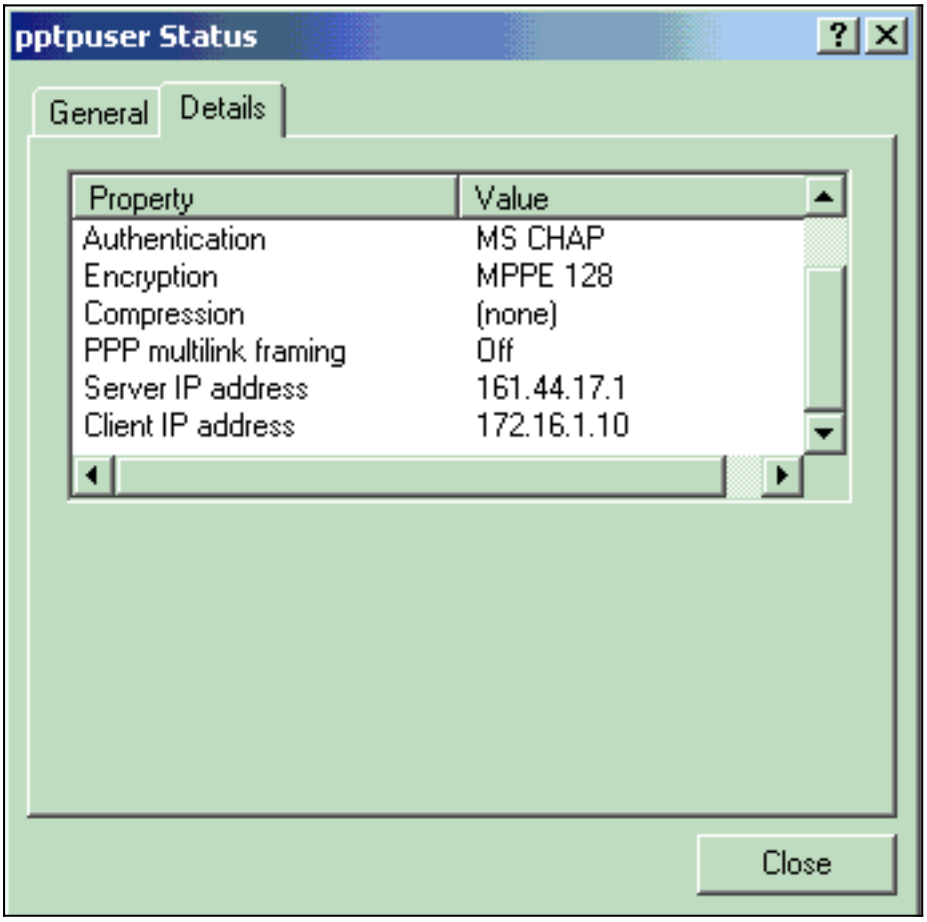
```
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
   User [pptpuser]
   Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
   User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

Windows PC のパラメータを確認するには、PPTP のユーザ ステータスの [Details] ウィンドウをクリックします。



トラブルシューティング

発生する可能性のあるエラーを次に示します。

- **ユーザ名またはパスワードが正しくない**VPN 3000 コンセントレータ デバッグ出力：

```
1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
   Authentication rejected: Reason = User was not found
   handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
   User [pptpusers]
```

```
   disconnected.. failed authentication ( MSCHAP-V1 )

6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
   Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
   reason: Error (No additional info)

8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)
```

ユーザに表示されるメッセージ（Windows 98 から）：

```
Error 691: The computer you have dialed in to has denied access
because the username and/or password is invalid on the domain.
```

ユーザに表示されるメッセージ（Windows 2000 から）：

```
Error 691: Access was denied because the username and/or
password was invalid on the domain.
```

- **"[Encryption Required] が PC では選択されているが、VPN コンセントレータでは選択されていない**ユーザに表示されるメッセージ（Windows 98 から）：

```
Error 742: The computer you're dialing in to does not support the data
encryption requirements specified.
Please check your encryption settings in the properties of the connection.
If the problem persists, contact your network administrator.
```

ユーザに表示されるメッセージ（Windows 2000 から）：

```
Error 742: The remote computer does not support
the required data encryption type
```

- **"40 ビットの暗号化のみをサポートする PC を使用する VPN コンセントレータで [Encryption Required]（128 ビット）が選択されている**VPN 3000 コンセントレータ デバッグ出力：

```
4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [ pptpuser ] disconnected.
PPTP Encryption configured as REQUIRED.. remote client not supporting it.
```

ユーザに表示されるメッセージ（Windows 98 から）：

```
Error 742:  The remote computer does not support
the required data encryption type.
```

ユーザに表示されるメッセージ（Windows 2000 から）：

```
Error 645 Dial-Up Networking could not complete the connection to the server.
Check your configuration and try the connection again.
```

- **VPN 3000 コンセントレータが MSCHAPv1 用に設定されていて PC が PAP 用に設定されているが、認証方式について合意できない**VPN 3000 コンセントレータ デバッグ出力：

```
8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129

User [pptpuser] disconnected. Authentication protocol not allowed.
```

ユーザに表示されるメッセージ（Windows 2000 から）：

```
Error 691:  Access was denied because the username and/or password
was invalid on the domain.
```

解決すべきありうるMicrosoft側の問題

- **ログオフ後に RAS 接続をアクティブなまま維持する方法**Windows のリモート アクセス サービス（RAS）クライアントからログオフすると、RAS 接続が自動的に切断されます。 ログオフ後も RAS クライアントが接続されたままにするため、レジストリで **KeepRasConnections** キーを有効にします。 詳細については、Microsoft Knowledge Base Article - 158909 を参照してください。
- **キャッシュされたクレデンシャルを使用してログインするときにユーザに警告が通知されない**この問題の症状では、Windows ベースのワークステーションやメンバー サーバからドメインにログインを試みたときにドメイン コントローラが見つからず、エラー メッセージが表示されません。 その代わり、キャッシュされたクレデンシャルを使用してローカル コンピュータにログインされます。 詳細については、Microsoft Knowledge Base Article - 242536 を参照してください。

- **ドメインの検証および他の名前解決に関する問題のために LMHOSTS ファイルを作成する方法**TCP/IP ネットワークで名前解決に関する問題が発生し、NetBIOS 名の解決のために LMHOSTS ファイルを使用することが必要な場合があります。 この記事では、名前解決とドメインの検証に役立てるために、LMHOSTS ファイルを正しく作成する方法について説明します。 詳細については、Microsoft Knowledge Base Article - 180094 を参照してください。

関連情報

- RFC 2637： Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）
- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco VPN 3000 コンセントレータで PPTP 暗号化がサポートされる条件
- Cisco Secure ACS for Windows の RADIUS 認証を使用した VPN 3000 コンセントレータと PPTP の設定
- Cisco VPN 3000 コンセントレータに関するサポートページ
- Cisco VPN 3000 Client に関するサポートページ
- IP セキュリティ（IPSec）製品に関するサポートページ
- PPTP 製品に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems