PIX 6.x：RADIUS 認証を使った PPTP の設定例

内容

概要

Point-to-Point Tunneling Protocol（PPTP）は、企業のプライベート ネットワーク内のサーバと安全に通信するためにリモート クライアントがパブリック IP ネットワークを使用することを可能にする、レイヤ 2 のトンネリング プロトコルです。PPTP は IP をトンネル伝送します。PPTP については、RFC 2637sで説明されています。 PIXファイアウォールでのPPTPサポートは、PIXソフトウェアリリース5.1で追加されました。PIXのドキュメントに、PPTPとそのPIXでの使用に関する詳細が記載されています。このドキュメントでは、PPTP をローカル、TACACS+、および RADIUS 認証とともに使用するための PIX の設定方法について説明します。また、このドキュメントでは、一般的な問題のトラブルシューティングに役立つヒントと例を示しています。

このドキュメントでは、PIXへのPPTP接続を設定する方法を説明します。セキュリティアプライアンスを介してPPTPを許可するようにPIXまたはASAを設定するには、『PIXを介したPPTP/L2TP接続の許可』を参照してください。

Windows 2000および2003で使用するPIXファイアウォールおよびVPNクライアントを設定するには、『Microsoft Windows 2000および2003 IAS RADIUS認証を使用するCisco Secure PIX Firewall 6.xおよびCisco VPN Client 3.5 for Windows』をを参照0003000303300333003030030030000000000303で0000000000000Internet Authentication Service(IAS)RADIUSサーバ。

RADIUS認証用にCisco Secure ACS for Windowsを使用するVPN 3000コンセントレータでPPTPを設定するには、『Cisco Secure ACS for Windows RADIUS認証を使用したVPN 3000コンセントレータおよびPPTPの設定』を参照してください。

ユーザがネットワークに入ることを許可する前に、ルータへのPC接続をセットアップし、Cisco Secure Access Control System(ACS)3.2 for Windowsサーバにユーザ認証を提供する方法については、『Cisco Secure ACS for WindowsルータPPTP認証の設定』を参照してください。

注：PPTPの用語では、RFCに従って、PPTPネットワークサーバ(PNS)がサーバ（この場合はPIXまたは呼び出し先）であり、PPTPアクセスコンセントレータ(PAC)がクライアント（PCまたは呼び出し側）です。

注：PPTPクライアントのPIXでは、スプリットトンネリングはサポートされていません。

注：PIX 6.xでPPTPが動作するにはMS-CHAP v1.0が必要です。Windows VistaはMS-CHAP v1.0をサポートしていないため、PIX 6.xのPPTPはWindows Vistaでは動作しません。PPTPは、PIXバージョン7.x以降ではサポートされていません。

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、Cisco Secure PIX Firewallソフトウェアリリース6.3(3)に基づくものです。

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については、『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。

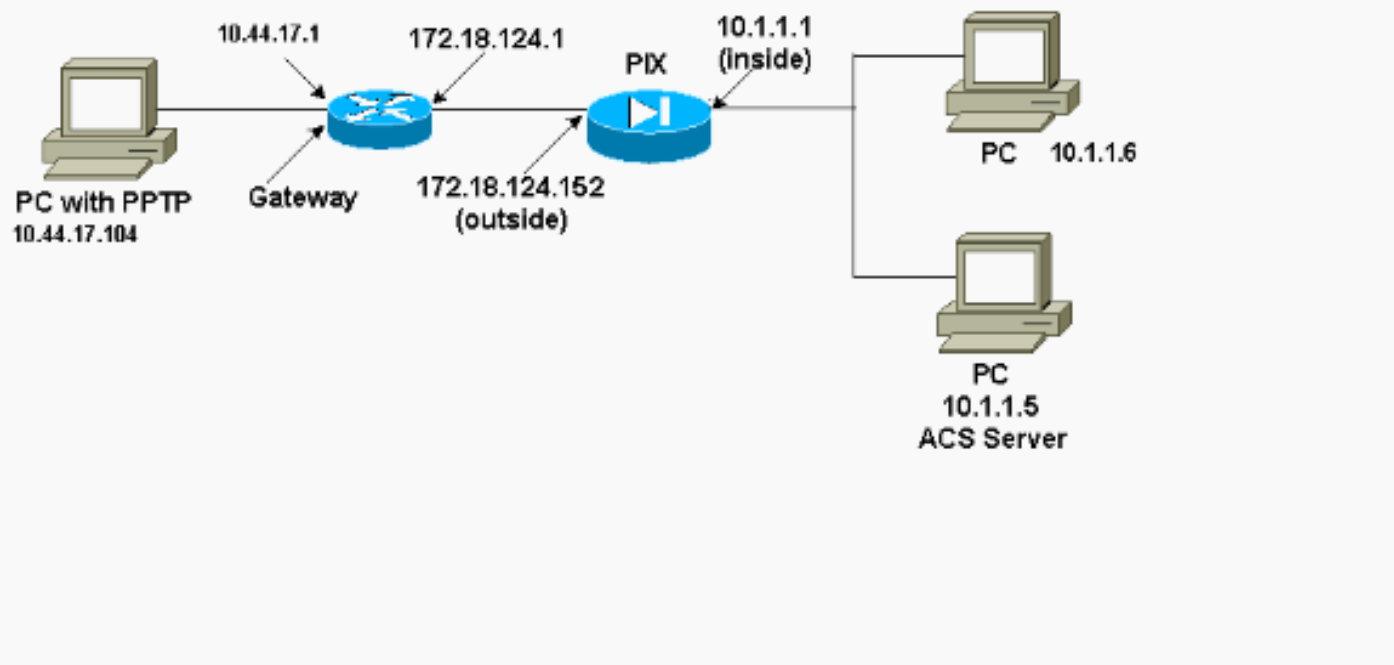
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



PIX Firewallの設定のヒント

認証 タイプ - CHAP、PAP、MS-CHAP

3つすべての認証方式(CHAP、PAP、MS-CHAP)に同時に設定されたPIXは、PCの設定方法に関係なく、接続する最適な機会を提供します。これは、トラブルシューティングの目的に適しています。

```
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp authentication pap
```

Microsoft Point-to-Point Encryption（MPPE）

PIX FirewallでMPPE暗号化を設定するには、次のコマンド構文を使用します。

```
vpdn group 1 ppp encryption mppe 40|128|auto [required]
```

このコマンドで、required はオプションのキーワードです。MS-CHAP が設定されていなければなりません。

クライアントPCでのPPTP機能の設定

注：ここでは、Microsoftソフトウェアの構成に関する情報は、Microsoftソフトウェアの保証またはサポートには含まれていません。Microsoftソフトウェアのサポートは、MicrosoftおよびMicrosoftサポートWebサイトから利用できます 。

Windows 98

Windows 98に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 の順に選択します。[next] をクリックします。
2. **Select from List** をクリックし、**Network Adapter** を選択します。[next] をクリックします。
3. 左パネルで **[Microsoft]**、右パネルで **[Microsoft VPN Adapter]** を選択します。

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 の順に選択します。
2. **[Make new connection]をクリックします。**[デバイスの選択]で、**Microsoft VPN Adapter**を使用して**接続します。**VPN サーバ IP アドレスには PIX トンネル エンドポイントの IP アドレスを指定します。
3. Windows 98のデフォルト認証では、パスワード暗号化（CHAPまたはMS-CHAP）が使用されます。 PAPを許可するようにPCを変更するには、**[Properties] > [Server types]を選択します。**[Require encrypted password] のチェックマークを外します。この領域でデータの暗号化（MPPE または MPPE なし）を設定できます。

Windows 2000

Windows 2000でPPTP機能を設定するには、次の手順を実行します。

1. [スタート] > [プ**ログラム] > [アクセサリ] > [通信] > [ネットワークとダイヤルアップ接続]を選択します。**
2. Make new connection をクリックし、Next をクリックします。
3. Connect to a private network through the Internet と Dial a connection priorを選択します（LAN がある場合は選択しないでください）。 [next] をクリックします。
4. トンネル エンドポイント（PIX/ルータ）のホスト名または IP アドレスを入力します。
5. パスワード タイプを変更する場合は、**Properties > Security for the connection > Advanced** の順に選択します。デフォルトは MS-CHAP と MS-CHAP v2 です（CHAP または PAP ではありません）。 この領域でデータの暗号化（MPPE または MPPE なし）を設定できます。

Windows NT

PPTP用のNTクライアントを設定するには、『Microsoftクライアントおよびサーバ でのPPTPのインストール 、設定、および使用』を参照してください。

PIX の設定

PIX の設定 - ローカル認証、暗号化なし

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
   192.168.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 10baset
interface ethernet2 10baset
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 172.18.124.152 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
ip local pool pptp-pool 192.168.1.1-192.168.1.50
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.201-172.18.124.202
nat (inside) 0 access-list 101
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

```
floodguard enable
sysopt connection permit-pptp
isakmp identity hostname
telnet timeout 5
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 client configuration address local pptp-
pool
vpdn group 1 client authentication local
vpdn username cisco password cisco
vpdn enable outside
terminal width 80
Cryptochecksum:a72d9f71d1a31332307fcd348e02410d
: end
```

PIX 設定 - 暗号化を用いるローカル認証

このコマンドをPIX設定 – Local Authentication, No Encryption設定、PCおよびPIXに自動ネゴシエーションで40ビット暗号化またはなし（PC設定に基づく）に追加した場合。

```
vpdn group 1 ppp encryption mppe auto
```

PIXで3DES機能が有効になっている場合は、**show versionコマンドを実行**すると、次のメッセージが表示されます。

- バージョン6.3以降：
  `VPN-3DES-AES: Enabled`
- バージョン6.2以前：
  `VPN-3DES: Enabled`

128 ビット暗号化も可能です。ただし、これらのメッセージのいずれかが表示された場合、PIXでは128ビット暗号化が有効になっていません。

- バージョン6.3以降：
  ```
  Warning: VPN-3DES-AES license is required
  for 128 bits MPPE encryption
  ```
- バージョン6.2以前：
  ```
  Warning: VPN-3DES license is required
  for 128 bits MPPE encryption
  ```

MPPEコマンドの構文を次に示します。

```
vpdn group ppp encryption mppe 40|128|auto [required]
```

PC および PIX は、MPPE とともに MS-CHAP 認証の設定を行う必要があります。

PIX の設定 - TACACS+/RADIUS 認証、暗号化なし

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
   192.168.1.0 255.255.255.0
pager lines 24
logging on
logging timestamp
no logging standby
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 10baset
interface ethernet2 10baset
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 172.18.124.152 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
ip local pool pptp-pool 192.168.1.1-192.168.1.50
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.201-172.18.124.202
nat (inside) 0 access-list 101
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
!--- Use either RADIUS or TACACS+ in this statement.
aaa-server AuthInbound protocol radius | tacacs+
aaa-server AuthInbound (outside) host 172.18.124.99
cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-pptp
isakmp identity address
telnet 10.1.1.5 255.255.255.255 inside
telnet 10.1.1.5 255.255.255.255 pix/intf2
telnet timeout 5
```

```
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 client configuration address local pptp-
pool
vpdn group 1 client authentication aaa AuthInbound
vpdn enable outside
terminal width 80
Cryptochecksum:96e9c93cb0a6ad6f53581dd7b61ac763
: end
[OK]
```

PIX 設定：暗号化を用いるRADIUS認証

RADIUS を使用する場合、および RADIUS サーバ（ベンダー固有のアトリビュート 26、Microsoft の場合）が MPPE キーイングをサポートする場合は、MPPE 暗号化を追加できます。TACACS+ サーバは特別な MPPE キーを返すことができないため、TACACS+ 認証は暗号化と併用できません。Cisco Secure ACS for Windows 2.5以降のRADIUSではMPPEがサポートされています（すべてのRADIUSサーバでMPPEがサポートされていません）。

RADIUS認証が暗号化なしで機能することを前提として、前の設定に次のコマンドを含めることで暗号化を追加します。

```
vpdn group 1 ppp encryption mppe auto
```

PCとPIXは、40ビットの暗号化を自動ネゴシエートするか、または（PCの設定に基づいて）「なし」を自動ネゴシエートします。

PIXで3DES機能が有効になっている場合は、**show versionコマンドを実行**すると、次のメッセージが表示されます。

```
VPN-3DES: Enabled
```

128 ビット暗号化も可能です。ただし、このメッセージが表示された場合、PIXでは128ビット暗号化が有効になっていません。

```
Warning: VPN-3DES license is required
for 128 bits MPPE encryption
```

MPPEコマンドの構文を次の出力に示します。

```
vpdn group ppp encryption mppe 40|128|auto [required]
```

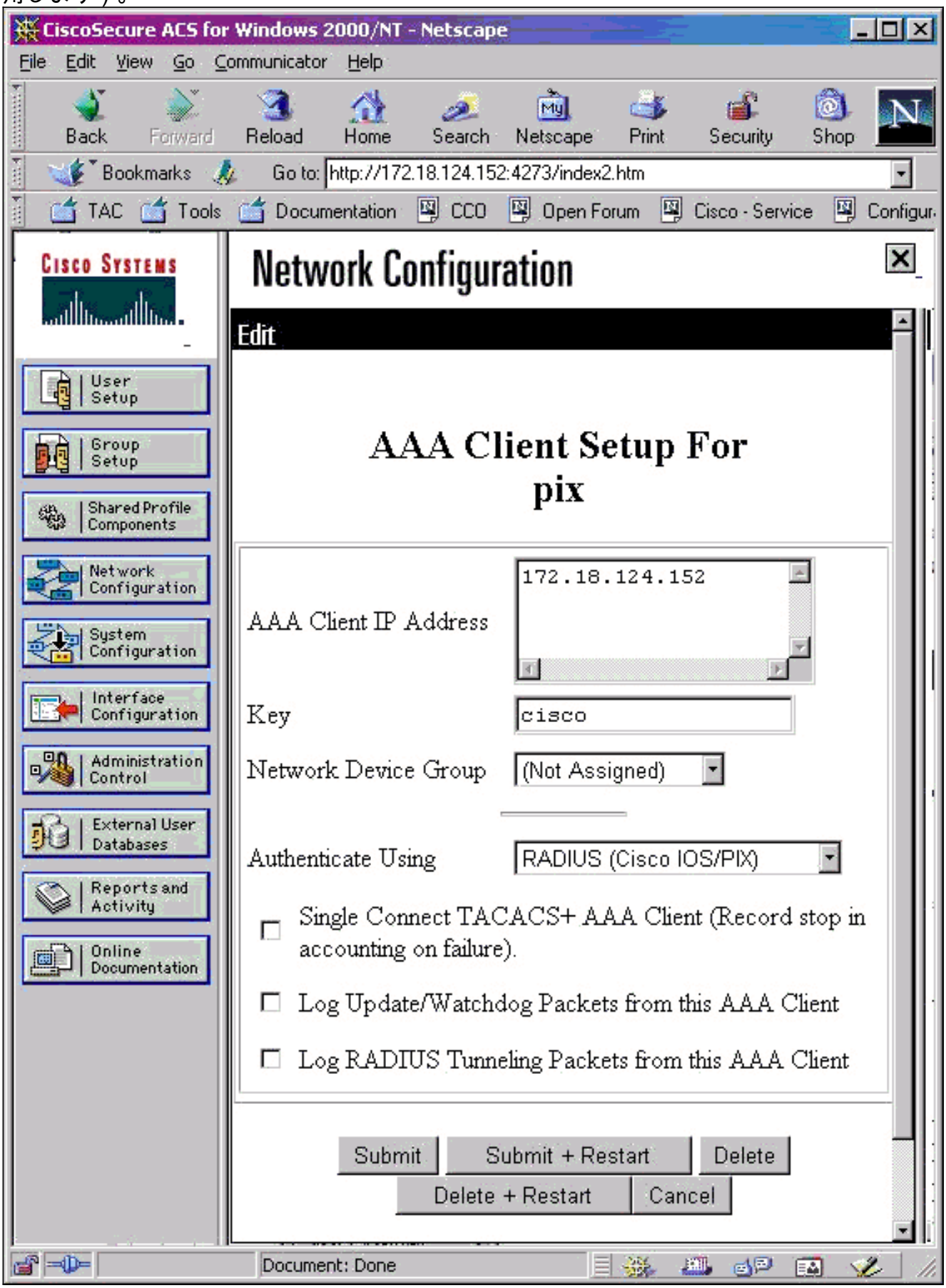
PC および PIX は、MPPE とともに MS-CHAP 認証の設定を行う必要があります。

Cisco Secure ACS for Windows 3.0の設定

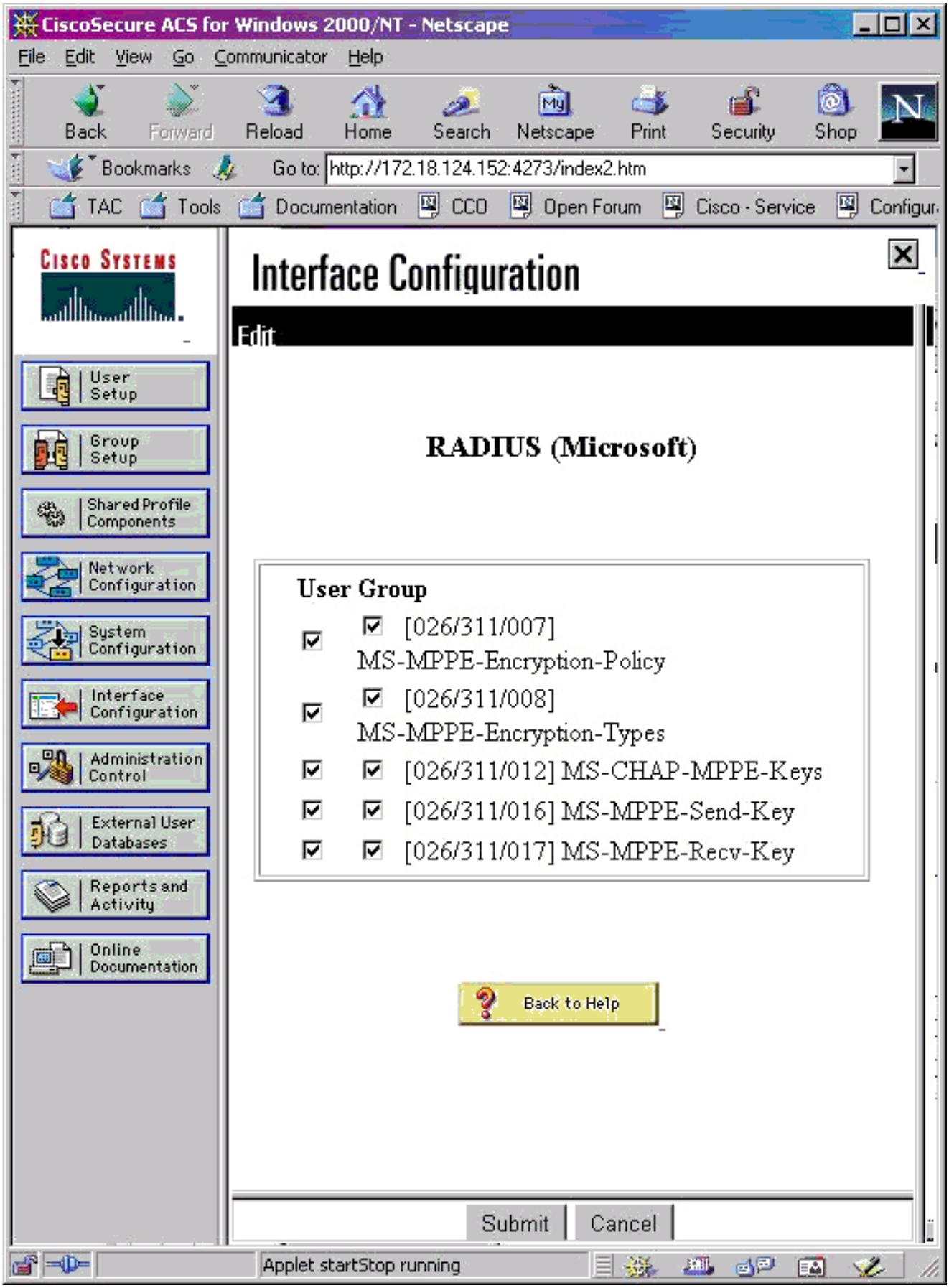
暗号化を用いるRADIUS認証

Cisco Secure ACS for Windows 3.0を設定するには、次の手順を使用します。ACSバージョン3.1および3.2にも同じ設定手順が適用されます。

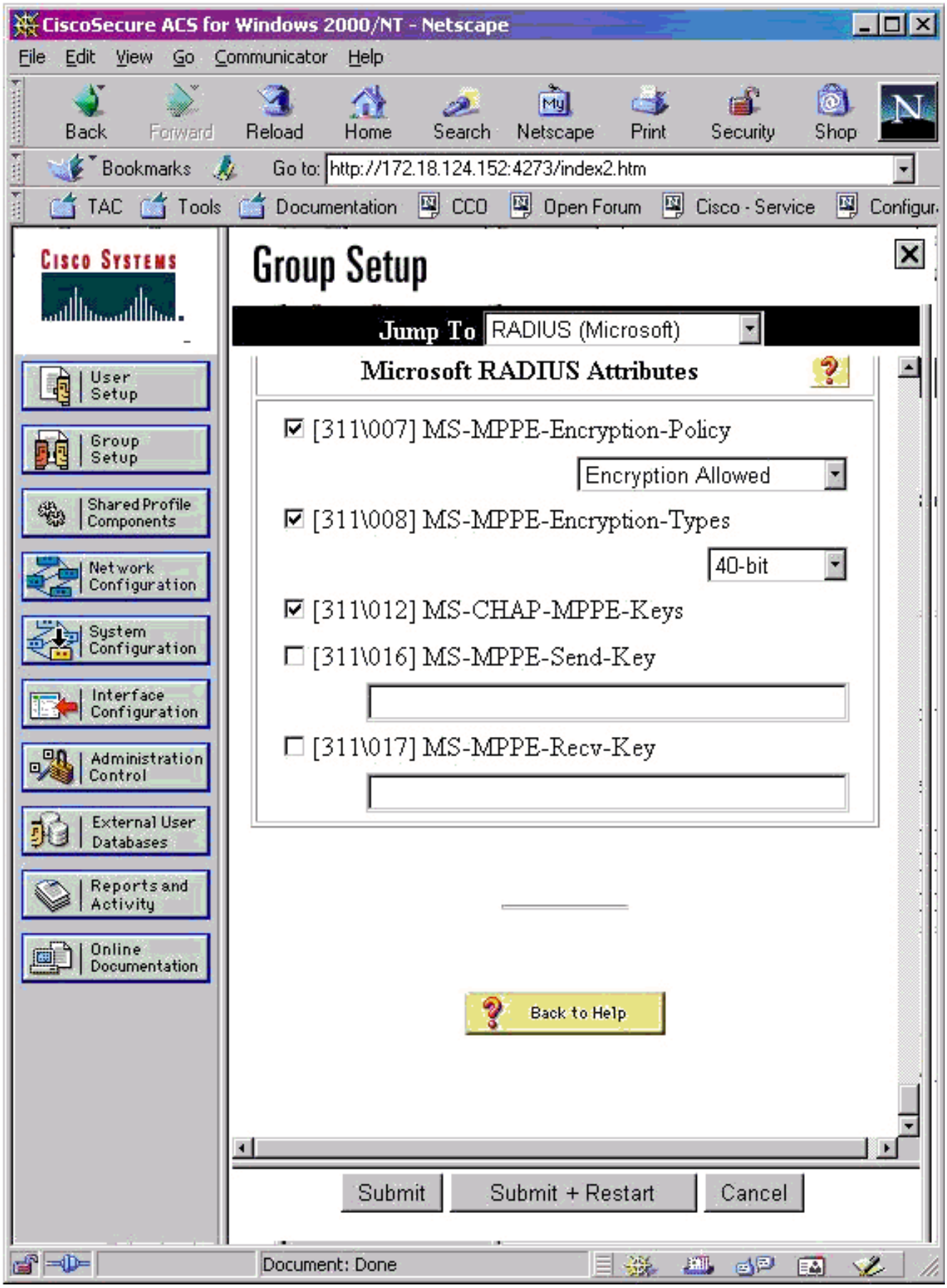
1. Cisco Secure ACS for Windows サーバの Network Configuration に PIX を追加し、ディクショナリタイプを特定します（ここでは MPPE キーを送信できるように Cisco IOS/PIX を使用します）。



2. [Interface Configuration] > [RADIUS (Microsoft)]を開き、MPPE属性をチェックして、グループインターフェイスに表示されるようにします。



3. ユーザを追加します。ユーザのグループに、MPPE [RADIUS (Microsoft)]属性を追加します。これらの属性は暗号化のために有効にする必要があり、PIXが暗号化用に設定されていない場合はオプションです。



確認

この項では、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紹介しています。

PIX (Post Authentication) show コマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

show vpdnコマンドは、**トンネル**とセッションの情報をリストします。

```
PIX#show vpdn

PPTP Tunnel and Session Information (Total tunnels=1 sessions=1)

Tunnel id 13, remote id is 13, 1 active sessions
  Tunnel state is estabd, time since event change 24 secs
  remote   Internet Address 10.44.17.104, port 1723
  Local    Internet Address 172.18.124.152, port 1723
  12 packets sent, 35 received, 394 bytes sent, 3469 received

Call id 13 is up on tunnel id 13
Remote Internet Address is 10.44.17.104
  Session username is cisco, state is estabd
    Time since event change 24 secs, interface outside
    Remote call id is 32768
    PPP interface id is 1
    12 packets sent, 35 received, 394 bytes sent, 3469 received
    Seq 13, Ack 34, Ack_Rcvd 12, peer RWS 64
    0 out of order packets
```

クライアントPCの確認

MS-DOSウィンドウまたは[ファイル名を指定して実行]ウィンドウで、ipconfig /allと入力**します**。PPPアダプタ部分は、次の出力を示しています。

```
PPP adapter pptp:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . :
```

また、[Details]をクリックして、PPTP接続の情報を表示することもできます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- PCからPIXトンネルエンドポイントへの総称ルーティングカプセル化(GRE)およびTCP 1723への接続が必要です。ファイアウォールまたはアクセスリストによってブロックされている可能性がある場合は、PCをPIXの近くに移動します。
- Windows 98およびWindows 2000 PPTPは、設定が最も簡単です。問題が生じたときは、複数の PC およびオペレーティング システムを試してください。接続が成功した後、PCの[Details]をクリックして、接続に関する情報を表示します。たとえば、PAP、CHAP、IP、暗

号化などを使用するかどうか。

- RADIUSやTACACS+を使用する場合は、まずローカル（ユーザ名とパスワード）認証を設定します。これが機能しない場合、RADIUSまたはTACACS+サーバを使用した認証は機能しません。
- 最初に、PC の Security 設定で可能な認証タイプ（PAP、CHAP、MS-CHAP）がすべて使用可能になっていることを確認し、Require data encryption のボックスのチェックをはずしておきます（データ暗号化は PIX でも PC でもオプションにしておきます）。
- 認証タイプはネゴシエートされるので、PIX には可能なすべてのタイプを設定します。たとえば、PCがMS-CHAP専用に設定され、ルータがPAP専用に設定されている場合は、何も同意しません。
- PIXが2つの異なる場所のPPTPサーバとして動作し、各ロケーションの内部に独自のRADIUSサーバがある場合、自身のRADIUSサーバでサービスを提供する両方の場所に1つのPIXを使用することはサポートされません。
- 一部の RADIUS サーバは MPPE をサポートしません。RADIUSサーバがMPPEキーイングをサポートしていない場合、RADIUS認証は機能しますが、MPPE暗号化は機能しません。
- Windows 98 以降では、PAP または CHAP を使用する場合、PIX に送信されるユーザ名は Dial-Up Networking（DUN; ダイヤルアップ ネットワーク）接続で入力されるユーザ名と同一です。ただし、MS-CHAPを使用する場合は、次のように、ドメイン名をユーザ名の前に追加できます。DUN に入力されたユーザ名 -「cisco」Windows 98 ボックスで設定されたドメイン -「DOMAIN」PIXに送信されたMS-CHAPユーザ名：「DOMAIN\cisco」PIX 上のユーザ名 -「cisco」結果 - 無効なユーザ名/パスワードこれは、動作を示すWindows 98 PCからのPPPログのセクションです。

```
02-01-2001 08:32:06.78 - Data 0038: 49 53 4c 41 42 5c 63 69 | DOMAIN\ci
02-01-2001 08:32:06.78 - Data 0040: 73 63 6f 00 00 00 00 00 | sco.....
|
|
02-01-2001 08:32:06.80 - Data 0000: c2 23 04 01 00 1a 41 75 | .#...^ZAu
02-01-2001 08:32:06.80 - Data 0008: 74 68 65 6e 74 69 63 61 | thentica
02-01-2001 08:32:06.80 - Data 0010: 74 69 6f 6e 20 66 61 69 | tion fai
02-01-2001 08:32:06.80 - Data 0018: 6c 65 64 2e 00 00 00 00 | led.....
02-01-2001 08:32:06.80 - CHAP : Login failed: username, password,
   or domain was incorrect.
```

Windows 98およびMS-CHAPをPIXに使用している場合は、非ドメインユーザ名に加えて、「DOMAIN\username」をPIXに追加できます。

```
vpdn username cisco password cisco
vpdn username DOMAIN\cisco password cisco
```

注：AAAサーバでリモート認証を実行する場合も同様です。

トラブルシューティングのためのコマンド

PPTPイベントの予想されるシーケンスの詳細については、PPTP RFC 2637を参照してください。PIXでは、適切なPPTPシーケンスの重要なイベントは次のように表示されます。

```
SCCRQ (Start-Control-Connection-Request)
SCCRP (Start-Control-Connection-Reply)
OCRQ (Outgoing-Call-Request)
OCRP (Outgoing-Call-Reply)
```

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

PIX debug コマンド

- **debug ppp io**:PPTP PPP仮想インターフェイスのパケット情報を表示します。
- **debug ppp error ：PPP 接続のネゴシエーションと操作に関するプロトコル エラーとエラー統計情報を表示します。**
- **debug vpdn errors**：PPP トンネルの確立を阻害するエラー、または確立されたトンネルをクローズする原因になるエラーを表示します。
- **debug vpdn packet**:VPDNの通常のトンネル確立またはシャットダウンの一部であるL2TPエラーとイベントを表示します。
- **debug vpdn events：通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。**
- **debug ppp uauth**:PPTP PPP仮想インターフェイスAAAユーザ認証デバッグメッセージを表示します。

PIX の clear コマンド

このコマンドは設定モードで実行する必要があります。

- **clear vpdn tunnel [all | *[id tunnel_id]*]**：設定から1つ以上のPPTPトンネルを削除します。

注意：clear vpdnコマンドを*発行*しないで**ください**。これを発行すると、すべての vpdn コマンドが削除されます。

クライアントPCでのPPPロギングの有効化

さまざまなWindowsおよびMicrosoftオペレーティングシステムのPPPデバッグをオンにするには、次の手順を実行します。

Windows 95

Windows 95マシンでPPPロギングを有効にするには、次の手順を実行します。

1. コントロール パネルの Network オプションで、インストールされたネットワーク コンポーネントのリストから Microsoft Dial-Up Adapter をダブルクリックします。
2. [Advanced] タブをクリックします。Property リストからオプション Record A Log File をクリックし、Value リストから Yes をクリックします。次に [OK] をクリックします。
3. コンピュータをシャットダウンして再起動すると、このオプションが有効になります。ppplog.txt という名前のファイルにログが保存されます。

Windows 98

Windows 98マシンでPPPロギングを有効にするには、次の手順を実行します。

1. Dial-Up Networking で接続アイコンをシングルクリックし、次に File > Properties の順に選択します。
2. Server Types タブをクリックします。
3. オプション Record a log file for this connection を選択します。ログファイルは C:\Windows\ppplog.txtにあります

Windows 2000

Windows 2000マシンでPPP口ギングを有効にするには、Microsoft Support Page に移動し、「Enable PPP Logging in Windows」を検索します。

Windows NT

NTシステムでPPP口ギングを有効にするには、次の手順を実行します。

1. キーSYSTEM\CurrentControlSet\Services\RasMan\PPP を見つけ、[Logging] を0から1に変更します。これにより、<winnt root>\SYSTEM32\RAS directoryにPPP.LOGというファイルが作成されます。
2. PPPセッションをデバッグするには、まず口ギングを有効にしてから、PPP接続を開始します。接続が失敗または終了したら、PPP.LOG を調べて何が起きたのかを確認します。

詳細については、Microsoftサポートページを参照し 、「Windows NTでのPPP口ギングの有効化」を検索してください。

追加の Microsoft 側の問題

PPTPのトラブルシューティングで考慮すべきMicrosoft関連の問題を次に示します。MS-DOS ウィンドウまたは Run ウィンドウから ipconfig /all と入力します。

- 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 Remote Access Service (RAS) connections are automatically disconnected when you log off from a RAS client.You can remain connected by enabling the KeepRasConnections registry key on the RAS client.
- 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Windowsベースのワークステーションまたはメンバサーバからドメインにログインし、ドメインコントローラが見つからない場合は、この問題を示すエラーメッセージは表示されません。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。
- 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の問題が発生した場合は、NetBIOS名を解決するためにLmhostsファイルを使用する必要があります。名前解決およびドメイン検証で使用するLmhostsファイルを作成するには、特定の手順に従う必要があります。

debug 出力例

PIX のデバッグ - ローカル認証

このデバッグ出力は、重要なイベントをイタリック体で示しています。

```
PPTP: new peer fd is 1

Tnl 42 PPTP: Tunnel created; peer initiated PPTP:
   created tunnel, id = 42

PPTP: cc rcvdata, socket fd=1, new_conn: 1
PPTP: cc rcv 156 bytes of data
```

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 42 PPTP: CC I 009c00011a2b3c4d000100000100000000000010000... Tnl 42 PPTP: CC I SCCRQ Tnl 42 PPTP: protocol version 0x100 Tnl 42 PPTP: framing caps 0x1 Tnl 42 PPTP: bearer caps 0x1 Tnl 42 PPTP: max channels 0 Tnl 42 PPTP: firmware rev 0x0 Tnl 42 PPTP: hostname "local" Tnl 42 PPTP: vendor "9x" Tnl 42 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd *SCCRP = Start-Control-Connection-Reply - message code bytes 9 & 10 = 0002* Tnl 42 PPTP: CC O SCCRP PPTP: cc snddata, socket fd=1, len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 168 bytes of data *OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007* Tnl 42 PPTP: CC I 00a800011a2b3c4d000700000000000000000dac00000... Tnl 42 PPTP: CC I OCRQ Tnl 42 PPTP: call id 0x0 Tnl 42 PPTP: serial num 0 Tnl 42 PPTP: min bps 56000:0xdac0 Tnl 42 PPTP: max bps 64000:0xfa00 Tnl 42 PPTP: bearer type 3 Tnl 42 PPTP: framing type 3 Tnl 42 PPTP: recv win size 16 Tnl 42 PPTP: ppd 0 Tnl 42 PPTP: phone num Len 0 Tnl 42 PPTP: phone num "" Tnl/Cl 42/42 PPTP: l2x store session: tunnel id 42, session id 42, hash_ix=42 PPP virtual access open, ifc = 0 Tnl/Cl 42/42 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/Cl 42/42 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d00080000002a00000100000000fa... *!--- Debug following this last event is flow of packets.* PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 27, data: ff03c021010100170206000a000005060011372107 02... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c22380050609894ab407020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 39, seq 1, ack 1, data: 3081880b00170000000000010000000 1ff03c0210101... PPP xmit, ifc = 0, Len: 17 data: ff03c0210401000d0206000a00000d0306 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 2, ack 1, data: 3081880b00110000000000002000000 01ff03c0210401... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 2, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c22380050609894ab407020802 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 34, seq 3, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data: ff03c0210102000e05060011372107020802 PPP xmit, ifc = 0, Len: 18 data: ff03c0210202000e05060011372107020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 34, seq 3, ack 3, data: 3081880b00120000000000003000000 03ff03c0210202... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08d36602863630eca8 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 31, seq 4, ack 3, data: 3081880b000f000000000040000000 3c2230101000d... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 76, seq 4, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a31d4d0a397a064668bb00d954a85... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 5, ack 4, data: 3081880b00060000000000005000000 04c22303010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 58, seq 5, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 44, data: ff038021010100280206002d0f010306000000008106... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a030663636302 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 6, ack 5, data: 3081880b000c000000000060000000 5802101010 00a... PPP xmit, ifc = 0, Len: 38 data: ff038021040100220206002d0f018106000000008206... Interface outside - PPTP xGRE: Out paket, PPP Len 36 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 52, seq 7, ack 5, data: 3081880b00240000000000007000000 05802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data: ff0380fd0101000f120601000011105000104 PPP xmit, ifc = 0, Len: 8 data: ff0380fd01010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 8, ack 6, data: 3081880b00060000000000008000000 0680fd01010004 PPP xmit, ifc = 0, Len: 19 data: ff0380fd0401000f120601000011105000104 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 9, ack 6, data: 3081880b00110000000000009000000 0680fd0401000f... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 7, ack 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a030663636302 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 8, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd02010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 9, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd01020004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd02020004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 10, ack 9, data: 3081880b00060000000000000a0000000 980fd02020004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 10, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd05030004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd06030004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22,

seq 11, ack 10, data: 3081880b000600000000000b0000000a80fd06030004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 48, seq 11 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010200220306000000008106000000008206... PPP xmit, ifc = 0, Len: 32 data: ff0380210402001c810600000000820600000000 8306... Interface outside - PPTP xGRE: Out paket, PPP Len 30 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 46, seq 12, ack 11, data: 3081880b001e00000000000c0000000b80210402001c... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 12, ack 12 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210103000a0306000000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210303000a0306ac100101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 13, ack 12, data: 3081880b000c00000000000d0000000c80210303000a... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 13, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210104000a0306ac100101 PPP xmit, ifc = 0, Len: 14 data: ff0380210204000a0306ac100101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 14, ack 13, data: 3081880b000c00000000000e0000000d80210204000a... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 41, seq 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data: ff0300214500001cc80000008001e5ccac100101e000... PPP IP Pkt: 4500001cc80000008001e5ccac100101e00000020a00... 603104: PPTP Tunnel created, tunnel_id is 42, remote_peer_ip is 99.99.99.5 ppp_virtual_interface_id is 1, client_dynamic_ip is 172.16.1.1 username is john, MPPE_key_strength is None outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 15 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060ca0000008011176bac100101ac10... PPP IP Pkt: 45000060ca0000008011176bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060cb0000008011166bac100101ac10... PPP IP Pkt: 45000060cb0000008011166bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060cc0000008011156bac100101ac10... PPP IP Pkt: 45000060cc0000008011156bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 18 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060d00000008011116bac100101ac10... PPP IP Pkt: 45000060d00000008011116bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 19 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060d200000080110f6bac100101ac10... PPP IP Pkt: 45000060d200000080110f6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 20 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060d300000080110e6bac100101ac10... PPP IP Pkt: 45000060d300000080110e6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 41, seq 21 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data: ff0300214500001cd60000008001d7ccac100101e000... PPP IP Pkt: 4500001cd60000008001d7ccac100101e00000020a00... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 22 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060d80000008011096bac100101ac10... PPP IP Pkt: 45000060d80000008011096bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 23 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060da0000008011076bac100101ac10... PPP IP Pkt: 45000060da0000008011076bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 24 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060db0000008011066bac100101ac10... PPP IP Pkt: 45000060db0000008011066bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 25 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060de0000008011036bac100101ac10... PPP IP Pkt: 45000060de0000008011036bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 26 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060e00000008011016bac100101ac10... PPP IP Pkt: 45000060e00000008011016bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 109, seq 27 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data: ff03002145000060e10000008011006bac100101ac10... PPP IP Pkt: 45000060e10000008011006bac100101ac10ffff0089... inside:172.16.255.255/137 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 41, seq 28 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data: ff0300214500001ce40000008001c9ccac100101e000... PPP IP Pkt: 4500001ce40000008001c9ccac100101e00000020a00...

PIX のデバッグ - RADIUS 認証

このデバッグ出力は、重要なイベントをイタリック体で示しています。

```
PIX#terminal monitor
PIX# 106011: Deny inbound (No xlate) icmp src
   outside:172.17.194.164 dst
   outside:172.18.124.201 (type 8, code 0)
106011: Deny inbound (No xlate) icmp src
   outside:172.17.194.164 DST
   outside:172.18.124.201 (type 8, code 0)

PIX#
PPTP: soc select returns rd mask = 0x1
PPTP: new peer FD is 1

Tnl 9 PPTP: Tunnel created; peer initiatedPPTP:
   created tunnel, id = 9

PPTP: cc rcvdata, socket FD=1, new_conn: 1
PPTP: cc rcv 156 bytes of data

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 9 PPTP: CC I
009c00011a2b3c4d000100000100000000000010000... Tnl 9 PPTP: CC I SCCRQ Tnl 9 PPTP: protocol
version 0x100 Tnl 9 PPTP: framing caps 0x1 Tnl 9 PPTP: bearer caps 0x1 Tnl 9 PPTP: max channels
0 Tnl 9 PPTP: firmware rev 0x870 Tnl 9 PPTP: hostname "" Tnl 9 PPTP: vendor "Microsoft Windows
NT" Tnl 9 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-
Reply - message code bytes 9 & 10 = 0002 Tnl 9 PPTP: CC O SCCRP PPTP: cc snddata, socket FD=1,
Len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max
soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0
PPTP: cc rcv 168 bytes of data OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007
Tnl 9 PPTP: CC I 00a800011a2b3c4d000700004000e4f50000012c05f5... Tnl 9 PPTP: CC I OCRQ Tnl 9
PPTP: call id 0x4000 Tnl 9 PPTP: serial num 58613 Tnl 9 PPTP: min bps 300:0x12c Tnl 9 PPTP: max
BPS 100000000:0x5f5e100 Tnl 9 PPTP: bearer type 3 Tnl 9 PPTP: framing type 3 Tnl 9 PPTP: recv
win size 64 Tnl 9 PPTP: ppd 0 Tnl 9 PPTP: phone num Len 0 Tnl 9 PPTP: phone num "" Tnl/Cl 9/9
PPTP: l2x store session: tunnel id 9, session id 9, hash_ix=9 PPP virtual access open, ifc = 0
Tnl/CL 9/9 PPTP: vacc-ok -> state change wt-vacc to estabd OCRP = Outgoing-Call-Reply - message
code bytes 9 & 10 = 0008 Tnl/CL 9/9 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data:
002000011a2b3c4d000800000009400001000000000fa... PPTP: cc waiting for input, max soc FD = 1
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 60, seq 0 PPP rcvd, ifc = 0, pppdev: 1, Len:
48, data: ff03c0210100002c0506447e217e070208020d030611... PPP xmit, ifc = 0, Len: 23 data:
ff03c021010100130305c2238005065a899b2307020802 Interface outside - PPTP xGRE: Out paket, PPP Len
23 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 39, seq 1, ack 0, data:
3081880b00174000000000010000000ff03c0210101... PPP xmit, ifc = 0, Len: 38 data:
ff03c021040000220d03061104064e131701beb613cb.. . Interface outside - PPTP xGRE: Out paket, PPP
Len 38 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 54, seq 2, ack 0, data:
3081880b00264000000000002000000000ff03c0210400... PPTP: soc select returns rd mask = 0x2 PPTP: cc
rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I
001800011a2b3c4d000f000000090000fffffffffffff... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for
input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 39, seq 1, ack 1 PPP
rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c2238005065a899b2307020802 outside
PPTP: Recvd xGRE pak from 10.44.17.104, Len 34, seq 2, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len:
18, data: ff03c0210101000e0506447e217e07020802 PPP xmit, ifc = 0, Len: 18 data:
ff03c0210201000e0506447e217e07020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18
outside PPTP: Sending xGRE pak to 10.44.17.104, Len 34, seq 3, ack 2, data:
3081880b00124000000000003000000002ff03c0210201... PPP xmit, ifc = 0, Len: 17 data:
ff03c2230101000d08f3686cc47e37ce67 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside
PPTP: Sending xGRE pak to 10.44.17.104, Len 31, seq 4, ack 2, data:
3081880b000f400000000004000000002c2230101000d... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 36, seq 3, ack 3 PPP rcvd, ifc = 0, pppdev: 1, Len: 22, data:
ff03c0210c020012447e217e4d5352415356352e3030 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len
45, seq 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 35, data:
ff03c0210c03001f447e217e4d535241532d312d4349... PPTP: soc select returns rd mask = 0x2 PPTP: cc
rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I
```

001800011a2b3c4d000f000000090000000000000000... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 76, seq 5, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000... uauth_mschap_send_req: pppdev=1, ulen=4, user=john 6031 uauth_mschap_proc_reply: pppdev = 1, status = 1 PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 5, ack 5, data: 3081880b000640000000000500000005c22303010004 CHAP peer authentication succeeded for john outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 72, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 6, ack 6, data: 3081880b000640000000000600000006c22303010004 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 7, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0104000a120601000001 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0101000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 7, ack 7, data: 3081880b000c4000000000070000000780fd0101000a... PPP xmit, ifc = 0, Len: 14 data: ff0380fd0304000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 8, ack 7, data: 3081880b000c4000000000080000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010500220306000000008106000000008206... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a0306ac127c98 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 9, ack 8, data: 3081880b000c4000000000090000000880210101000a... PPP xmit, ifc = 0, Len: 32 data: ff0380210405001c8106000000008206000000008306.. . Interface outside - PPTP xGRE: Out paket, PPP Len 30 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 46, seq 10, ack 8, data: 3081880b001e40000000000a000000080210405001c... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 9, ack 7 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0201000a120601000020 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 10, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0106000a120601000020 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0206000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 11, ack 10, data: 3081880b000c40000000000b0000000a80fd0206000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 11, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a0306ac127c98 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 12, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210107000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210307000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 12, ack 12, data: 3081880b000c40000000000c0000000c80210307000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 24, seq 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210108000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210308000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 13, ack 13, data: 3081880b000c40000000000d0000000d80210308000a... 0 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 14, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210109000a0306c0a80101 PPP xmit, ifc = 0, Len: 14 data: ff0380210209000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 14, ack 14, data: 3081880b000c40000000000e0000000e80210209000a... 2: PPP virtual interface 1 - user: john aaa authentication started 603103: PPP virtual interface 1 - user: john aaa authentication succeed 109011: Authen Session Start: user 'joh outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 117, seq 15, ack 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9000bccf59b71755d9af7330dae3bbc94d28... PPP Encr/Comp Pkt: 9000bccf59b71755d9af7330dae3bbc94d28e431d057... PPP IP Pkt: 4500006002bb000080117629c0a80101ffffffff0089... n', sid 3 603104: PPTP Tunnel created, tunnel_id is 9, remote_peer_ip is 10.44.17.104 ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1 username is john, MPPE_key_strength is 40 bits outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9001f8348351ef9024639ed113b43adfeb44... PPP Encr/Comp Pkt: 9001f8348351ef9024639ed113b43adfeb4489af5ab3... PPP IP Pkt: 4500006002bd000080117627c0a80101ffffffff0089... ide outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9002cc73cd65941744a1cf30318cc4b4b783... PPP Encr/Comp Pkt: 9002cc73cd65941744a1cf30318cc4b4b783e825698a... PPP IP Pkt: 4500006002bf000080117625c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 18 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:

ff0300fd9003aaa545eaeeda0f82b5999e2fa9ba3245... PPP Encr/Comp Pkt:
9003aaa545eaeeda0f82b5999e2fa9ba324585a1bc8d... PPP IP Pkt:
4500006002c1000080117623c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 19 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90045b35d080900ab4581e64706180e3540e... PPP Encr/Comp Pkt:
90045b35d080900ab4581e64706180e3540ee15d664a... PPP IP Pkt:
4500006002c3000080117621c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 20 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90052878b256edbd17b42f2cb672ba80b40a... PPP Encr/Comp Pkt:
90052878b256edbd17b42f2cb672ba80b40a79760cef... PPP IP Pkt:
4500006002c500008011761fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 21 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900632359a2c07e79106c5e282e3892e60de... PPP Encr/Comp Pkt:
900632359a2c07e79106c5e282e3892e60ded6c6d4d1... PPP IP Pkt:
4500006002c700008011761dc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 22 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90070ca6ea48b2ad26987d52a4e109ca68b6... PPP Encr/Comp Pkt:
90070ca6ea48b2ad26987d52a4e109ca68b6758569d3... PPP IP Pkt:
4500006002c900008011761bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 23 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90085aba60edf57e50eea4d523596cb9d690... PPP Encr/Comp Pkt:
90085aba60edf57e50eea4d523596cb9d69057715894... PPP IP Pkt:
4500006002cb000080117619c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 24 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90094b73b6c962272b60d32f135b5f29f2a5... PPP Encr/Comp Pkt:
90094b73b6c962272b60d32f135b5f29f2a58bacd050... PPP IP Pkt:
4500006002cc000080117618c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 345, seq 25 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd900a86307ed9537df5389ea09223d62c20fd... PPP Encr/Comp Pkt:
900a86307ed9537df5389ea09223d62c20fd9e34072f... PPP IP Pkt:
4500014802cf00008011752dc0a80101ffffffff0044... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 26 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900b45303a5fe7b2dc3f62db739b4bb1b802... PPP Encr/Comp Pkt:
900b45303a5fe7b2dc3f62db739b4bb1b80253278fad... PPP IP Pkt:
4500006002d1000080117613c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 27 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900ceb5aaaecc832df3c12bc6c519c25b4db... PPP Encr/Comp Pkt:
900ceb5aaaecc832df3c12bc6c519c25b4dba569d10... PPP IP Pkt:
4500006002d2000080117612c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 28 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900dbdaaf071c2bd1c92c1f56085813d1a77... PPP Encr/Comp Pkt:
900dbdaaf071c2bd1c92c1f56085813d1a778cc61c29... PPP IP Pkt:
4500006002d500008011760fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 29 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900e97de47036d95a0721ef6b28479b8efde... PPP Encr/Comp Pkt:
900e97de47036d95a0721ef6b28479b8efde8e16b398... PPP IP Pkt:
4500006002d600008011760ec0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 30 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900f75bf4c8cbcf11464bf52bd7f6155c7d6... PPP Encr/Comp Pkt:
900f75bf4c8cbcf11464bf52bd7f6155c7d62ea2ca5e... PPP IP Pkt:
4500006002d900008011760bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 31 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd9010f221e7ba169702765529e4ffa368dba5... PPP Encr/Comp Pkt:
9010f221e7ba169702765529e4ffa368dba5610921ae... PPP IP Pkt:
4500006002da00008011760ac0a80101ffffffff0089... from (192.168.1.1) to 255.255.255.255 on
interface outside outside PPTP: Recvd xGRE pak from 10.44.17.104, len 231, seq 32 PPP rcvd, ifc
= 0, pppdev: 1, len: 222, data: ff0300fd9011c23a03921c1e10ccc38847cb8056fa93... PPP Encr/Comp
Pkt: 9011c23a03921c1e10ccc38847cb8056fa9387018912... PPP IP Pkt:
450000d602dd000080117591c0a80101ffffffff008a... side outside PPTP: Recvd xGRE pak from
10.44.17.104, len 345, seq 33 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd90127d7213f35cd1d82d8988e28e0930ecc1... PPP Encr/Comp Pkt:
90127d7213f35cd1d82d8988e28e0930ecc104a993f... PPP IP Pkt:
4500014802df00008011751dc0a80101ffffffff0044...

不具合の原因

同時PPTPトンネル

PIX 6.xでは127を超える接続を接続できず、次のエラーメッセージが表示されます。

%PIX-3-213001:PPTP制御デーモンソケットio acceptエラー、errno = 5

ソリューション：

PIX 6.xでは、128の同時セッションのハードウェア制限があります。PPTPリスニングソケットに1つ差し引くと、最大接続数は127になります。

PIX と PC が認証をネゴシエートできない

PC認証プロトコルは、PIXが実行できないプロトコル(バージョン1ではなくShiva Password Authentication Protocol(SPAP)およびMicrosoft CHAPバージョン2(MS-CHAP v.2)に対して設定されます)。 PCとPIXが認証について合意できない。PCに次のメッセージが表示されます。

```
Disconnected - Error 732: Your computer and the remote computer
    could not agree on PPP control protocols
```

PIX と PC が暗号化をネゴシエートできない

PCは暗号化のみに設定され、**vpdn group 1 ppp encrypt mppe 40 required**コマンドはPIXから削除されます。PCとPIXが暗号化について合意できず、PCに次のメッセージが表示されます。

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

PIX と PC が暗号化をネゴシエートできない

PIXは**vpdn group 1 ppp encrypt mppe 40 required**とPC **for no encryption allowed**に設定されています。これにより、PCにメッセージは生成されませんが、セッションが切断され、PIXデバッグに次の出力が表示されます。

```
PPTP: Call id 8, no session id protocol: 21,
    reason: mppe required but not active, tunnel terminated
603104: PPTP Tunnel created, tunnel_id is 8,
    remote_peer_ip is 10.44.17.104
ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1
username is cisco, MPPE_key_strength is None
603105: PPTP Tunnel deleted, tunnel_id = 8,
    remote_peer_ip = 10.44.17.104
```

PIX MPPE RADIUS の問題

PIXは**vpdn group 1 ppp encrypt mppe 40 required**に設定されており、RADIUSサーバへの認証で許可された暗号化用のPCはMPPEキーを返しません。PCに次のメッセージが表示されます。

```
Error 691: Access was denied because the username
```

```
    and/or password was invalid on the domain.
```

PIXのデバッグには次のように表示されます。

```
2: PPP virtual interface 1 -
   user: cisco  aaa authentication started
603103: PPP virtual interface 1 -
   user: cisco  aaa authentication failed
403110: PPP virtual interface 1,
   user: cisco missing MPPE key from aaa server
603104: PPTP Tunnel created,
   tunnel_id is 15,
   remote_peer_ip is 10.44.17.104
   ppp_virtual_interface_id is 1,
   client_dynamic_ip is 0.0.0.0
   username is Unknown,
   MPPE_key_strength is None
603105: PPTP Tunnel deleted,
   tunnel_id = 15,
   remote_peer_ip = 10.44.17.104
```

PCに次のメッセージが表示されます。

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

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- PPTP に関するサポート ページ
- RFC 2637:Point-to-Point Tunneling Protocol（PPTP）
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems