PIX 6.x： RADIUS 認証を使った PPTP の設定例

目次

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。 exitPIX Firewall 上での PPTP のサポートは、PIX ソフトウェア リリース 5.1 で追加されました。 PIX ドキュメントには、PPTP の詳細と PIX との使用方法に関する情報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。

この資料に PIX への PPTP 接続を設定する方法を示されています。 PIX か ASA をセキュリティ アプライアンス モデルを通して割り当て PPTP に設定するために、PPTP/L2TP 接続を PIX によって許可することを参照して下さい。

Windows 2000 および 2003 年の Internet Authentication Service （ IAS ） RADIUSサーバと併用するため PIXファイアウォールおよび VPN クライアントを設定するために Cisco Secure PIX Firewall 6.x および Microsoft Windows 2000 および 2003 IAS RADIUS認証を用いる Windows のための Cisco VPN Client 3.5 を参照して下さい。

Cisco Secure ACS for Windows RADIUS認証での VPN 3000 コンセントレータおよび PPTP の RADIUS認証のための Cisco Secure ACS for Windows で VPN 3000 コンセントレータの PPTP を設定するために設定を参照して下さい。

ネットワークにユーザを許可する前に、Cisco Secure ACS for Windows ルータ PPTP 認証の Cisco Secure Access Control System （ ACS ）に Windows サーバにユーザ認証を 3.2 提供するルータに PC接続を設定するために設定を参照して下さい。

注: PPTP 用語では、RFC ごとに、PPTP Network Server （ PNS ）はサーバ（ この場合、PIX、または呼び出し側 ）であり、PPTP Access Concentrator （ PAC ）はクライアント（ PC、または発信者 ）です。

注: 分割トンネリングは PPTP クライアントのための PIX でサポートされません。

注: PPTP がはたらくことをように PIX 6.x は MS-CHAP v1.0 が必要とします。Windows Vista は MS-CHAP v1.0 をサポートしません。 つまり PIX 6.x の PPTP は Windows Vista のためにはたらきません。 PPTP は PIXバージョン 7.x およびそれ以降でサポートされません。

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基づいた on Cisco セキュア PIX ファイアウォール ソフトウェア リリース 6.3(3) 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、クリアな（ デフォルト ）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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）を使用してください。

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。

PIXファイアウォールのための設定ヒント

認証 タイプ - CHAP、PAP、MS-CHAP

すべての 3 つの認証方式（CHAP、PAP、MS-CHAP）のために設定される PIX は同時に PC が設定されてもいかに接続する最もよい可能性を提供します。 これはトラブルシューティングを行うのによい概念です。

```
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ファイアウォールの MPPE暗号化を設定するためにこのコマンド構文を使用して下さい。

```
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 の PPTP 機能を設定して下さい

注: マイクロソフト社ソフトウェア 設定に関係したの入手可能な情報はここにマイクロソフト社ソフトウェアのためのあらゆる保証かサポートが付いていません。 マイクロソフト社ソフトウェアのためのサポートは Microsoft からおよびマイクロソフトのサポート Webサイトで利用できます 。

Windows 98

Windows 98 で PPTP 機能をインストールするために次の手順に従って下さい。

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 機能を設定するために次の手順に従って下さい。

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 して下さい。 **select** に関しては**デバイスは**、接続さ

れま **Microsoft VPN アダプタを**使用します。 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 デフォルトの認証はパスワード暗号化を使用します（CHAP か MS-CHAP）。 PC をまた PAP を許可するために変更するために Properties > Server types の順に選択 して下さい。 Require encrypted password のチェックをはずします。 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 の PPTP 機能を設定するために次の手順に従って下さい。

1. Start > Programs > Accessories > Communications > Network & Dialup connections の順に選択 して下さい。
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

Microsoft クライアント および サーバと PPTP のインストールし、設定、PPTP のための NT クライアントを設定するのに使用することを参照して下さい。

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

PIX 設定にこのコマンドを追加すれば-ローカル認証、No encryption 設定、PC および PIX は 40 ビット 暗号化またはどれもオート・ネゴシエートしません（PC 設定に基づいて）。

vpdn group 1 ppp encryption mppe auto

PIX に有効に なる トリプル DES 機能がある場合 **show version コマンドは**このメッセージを表示する。

- バージョン 6.3 および それ 以降:`VPN-3DES-AES: Enabled`
- バージョン 6.2 および それ 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 1 つが表示する、そして PIX は 128-bit 暗号化のために有効に なりません。

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

MPPE コマンドのための構文はここに示されています。

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 および それ以降 RADIUS は MPPE をサポートします (すべての RADIUSサーバは MPPE をサポートしません) 。

RADIUS認証が暗号化なしではたらくという想定のもとで、以前のコンフィギュレーションにこのコマンドを含めることによって暗号化を追加して下さい:

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

PC および PIX は 40 ビット 暗号化またはどれもオート・ネゴシエートしません（PC 設定に基づいて）。

PIX に有効に なる トリプル DES 機能がある場合 **show version コマンドは**このメッセージを表示する。

```
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する、PIX は 128-bit 暗号化のために有効に なりません。

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

MPPE コマンドのための構文はこの出力で示されています。

```
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。

Windows 3.0 のための設定 Cisco Secure ACS

暗号化を用いるRADIUS認証

Windows 3.0 のための Cisco Secure ACS を設定するためにこれらのステップを使用して下さい。 同じ 設定ステップは ACS にバージョン 3.1 および 3.2 を加えます。

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. オープンインターフェイス **設定 > RADIUS（Microsoft）は**およびそれらをグループインターフェイスに現われさせます MPPE属性をチェックします。
3. ユーザを追加して下さい。 ユーザ・グループでは、追加して下さい MPPE [RADIUS（Microsoft）] アトリビュート 暗号化のためのこれらの属性を有効に して下さい、PIX が暗号化のために設定されないときオプションです。

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示しています。

PIX (Post Authentication) show コマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

show vpdn コマンド リストはセッション情報トンネル伝送し。

```
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

から MS DOS ウィンドウでは、または Run ウィンドウ、**ipconfig /all** をタイプして下さい。 PPP アダプタ部分はこの出力を示します。

```
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 PPTP 接続の情報を表示するために『Details』 をクリック することができます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- PC からの 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 のための接続がある必要があります。 これはファイアウォールかアクセス リストによってブロックされるという可能性があったら、PIX に近い方の PC を移動して下さい。
- Windows 98 および Windows 2000 PPTP は最も設定し易いです。 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。 接続の成功の後で、接続についての情報を表示するために PC で『Details』 をクリック して下さい。 たとえば、PAP を使用するかどうか、CHAP、IP、暗号化、等。
- RADIUS や TACACS+ を使用するように意図する場合最初にローカル（PIX のユーザ名 および パスワード）認証を設定することを試みて下さい。 これがはたらかない場合、RADIUS または TACACS+ サーバとの認証ははたらきません。
- 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 PAP だけの MS-CHAP およびルータだけのために設定されれば、決して協定がありません。
- PIX が 2 つの異なる場所のための PPTP サーバとして機能し、各位置に内部の自身の RADIUSサーバがあれば、自身の RADIUSサーバによって保守される両方の場所のための単一 PIX を使用して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ない場合、RADIUS認証ははたらきますが、MPPE暗号化ははたらきません。
- 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。 しかし MS-CHAP を使用するとき、ドメイン名はユーザ名の先頭に追加 することができますたとえば: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 される MS-CHAP ユーザ名-「ドメイン\ 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.
```

非ドメインユーザ名を持っていることに加えて PIX に Windows 98 および MS-CHAP を、使用すれば、PIX に「ドメイン\ユーザ名」を追加できます:

vpdn username cisco password cisco vpdn username DOMAIN\cisco password cisco **注:** AAAサーバのリモート 認証を行う場合、同じは適用します。

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シーケンスの情報は PPTP RFC 2637 にあります 。
PIX で、よい PPTP シーケンスの重大なイベントは示します:

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および動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 error**：PPP トンネルの確立を阻止するエラー、または確立されたトンネルをクローズするエラーを表示します。
- debug vpdn packets - VPDN で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 エラーおよび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の 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 [すべて |** [id tunnel_id]] - 1 つ以上の PPTP トンネルを設定から削除します。

注意： clear vpdn コマンドを発行しないで下さい。 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 をログオンするイネーブル PPP

さまざまな Windows およびマイクロソフトオペレーティングシステムのための Pppデバッグをつけるためにこれらの手順を完了して下さい。

Windows 95

Windows 95 マシンをログオンする PPP を有効に するために次の手順に従って下さい。

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 マシンをログオンする PPP を有効に するために次の手順に従って下さい。

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 マシンをログオンする PPP を有効に するため「イネーブル PPP ログオン Windows のためのマイクロソフトのサポート ページおよび検索に行くため」。

Windows NT

NT システムをログオンする PPP を有効に するために次の手順に従って下さい。

1. 鍵システム\ CurrentControlSet \サービス\ RasMan \ PPP を見つけ、0 から 1.にロギングを変更して下さい。 これは PPP.Login を <winnt root>\SYSTEM32\RAS ディレクトリと呼ばれるファイルを作成します。
2. 記録 する PPP セッション、最初イネーブルをデバッグし、次に PPP 接続を開始するため。 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、参照して下さい「PPP ログオン Windows NT を有効に するためのマイクロソフトのサポート ページおよび検索を」。

追加の Microsoft 側の問題

PPTP をトラブルシューティングするとき考慮するべき複数の Microsoft関連の問題はここにリストされています。 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からのドメインにログオンするか、またはメンバー サーバおよびドメインコントローラが見つけることができなければこの問題を示す工ラーメッセージを受け取りません。 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 ネットワークの名前解決問題に直面する場合、NetBIOS 名を変換するために Lmhost 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 バリデーションで使用するために Lmhost ファイルを作成するために特定のプロシージャに従って下さい。

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*イタリック体*で重大なイベントを示します。

```
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
009c00011a2b3c4d0001000001000000000000010000... 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: 009c00011a2b3c4d0002000001000100000000030000... 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:
ff03c021010100170206000a00000506001137210702... 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:
3081880b00110000000000002000000001ff03c0210401... 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:
3081880b00120000000000003000000003ff03c0210202... 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: 3081880b000f000000000400000003c2230101000d... 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: 3081880b000600000000000500000004c22303010004 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: 3081880b000c000000000060000000580210101000a... 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: 3081880b00240000000000070000000580210401002 2... 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: 3081880b000600000000000080000000680fd01010004 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: 3081880b001100000000000090000000680fd0401000f... 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: 3081880b000600000000000a0000000980fd02020004 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: ff0380210103000a030600000000 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*イタリック体*で重大なイベントを示します。

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: 3081880b00264000000000020000000ff03c0210400... 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 001800011a2b3c4d000f000000090000ffffffffffff... 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: 3081880b0012400000000000300000002ff03c0210201... 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: 3081880b000f4000000000400000002c2230101000d... 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: ff03c2230201003a31000000000000000000000000000... 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: ff03c2230201003a31000000000000000000000000000... 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: 3081880b000c400000000007000000780fd0101000a... 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: 3081880b000c400000000008000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010500220306000000081060000000082 06... 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: 3081880b000c400000000009000000080210101000a... PPP xmit, ifc = 0, Len: 32 data: ff0380210405001c810600000000820600000000 8306.. . 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 の 127 以上の接続を接続することができこのエラーメッセージが現れます:

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

解決策：

PIX 6.x の 128 人の並行 セッションのハードウェアの制約があります。 PPTP 受信ソケットのための 1 つを引く場合、最大数 is127 接続。

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 によってがすることができない物のために設定 されます（Shivaパスワード認証プロトコル（SPAP）および 1）バージョンの代りの Microsoft CHAP バージョン 2（MS-CHAP v.2）。 PC および PIX は認証に一致することができません。 PC はこのメッセージを表示する:

```
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**暗号化されるただ**のために設定 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 および PIX は暗号化に一致することができ、PC はこのメッセージを表示する:

```
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 は許可される no encryption の **vpdn group 1 ppp encrypt mppe 40 required** および PC のために設定 されます。 これは PC のメッセージを表示しませんが、セッション切断および PIX デバッグはこの出力を示します:

```
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** のために設定 され、RADIUSサーバに認証と許可される暗号化のための PC は MPPE キーを戻しません。 PC はこのメッセージを表示します:

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

PIX デバッグは示します:

```
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 はこのメッセージを表示します:

```
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; ポイントツーポイント トンネリング プロトコル)
- Requests for Comments (RFC)
- テクニカルサポート - Cisco Systems