

Microsoft IAS を使用した L2TP のための Cisco IOS および Windows 2000 クライアントの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[Microsoft IAS 用の Windows 2000 Advanced Server の設定](#)

[RADIUS クライアントの設定](#)

[IAS 上のユーザの設定](#)

[Windows ユーザへのリモート アクセス ポリシーの適用](#)

[L2TPのためのWindows 2000クライアントの設定](#)

[Windows 2000 クライアントのためのIPSecの無効化](#)

[L2TP用Cisco IOSの設定](#)

[暗号化の有効化](#)

[debug コマンドと show コマンド](#)

[スプリット トンネリング](#)

[トラブルシューティング](#)

[問題 1：無効にされないIPSec](#)

[問題 2：エラー 789](#)

[問題 3：トンネル認証においての問題](#)

[関連情報](#)

概要

このドキュメントでは、MicrosoftのInternet Authentication Server(IAS)を使用して、レイヤ2トンネルプロトコル(L2TP)用のCisco IOS®ソフトウェアおよびWindows 2000クライアントを設定する方法について説明します。

リモートの[Microsoft Windows 2000からL2TP over IP Security\(IPSec\)を設定する方法の詳細については、『事前共有キーを使用したWindows 2000/XP PCとPIX/ASA 7.2間の2のTP over IPSSecurity』](#)の設定例ユーザ認証用のMicrosoft Windows 2003 IAS RADIUSサーバとの事前共有キーを使用して、PIXセキュリティアプライアンスの企業オフィスに0/2003およびXPクライアントを接続します。

リモートの[Microsoft Windows 2000およびMicrosoft Windows 2000からL2TP over IPSecを設定する方法の詳細は、『事前共有キーを使用したWindows 2000またはXPクライアントからCisco](#)

[VPN 30000000シリーズコンセントレータ000000000000への000への00000000000への00000000000000000000への000への00の000000000000 XPクライアントから企業サイトにアクセスします。](#)

[前提条件](#)

[要件](#)

このドキュメントに関しては個別の前提条件はありません。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Active Directoryを使用するMicrosoft 2000 advancedサーバにインストールされたMicrosoft IASオプションコンポーネント
- Cisco 3600ルータ
- Cisco IOSソフトウェアリリースc3640-io3s56i-mz.121-5.T

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。

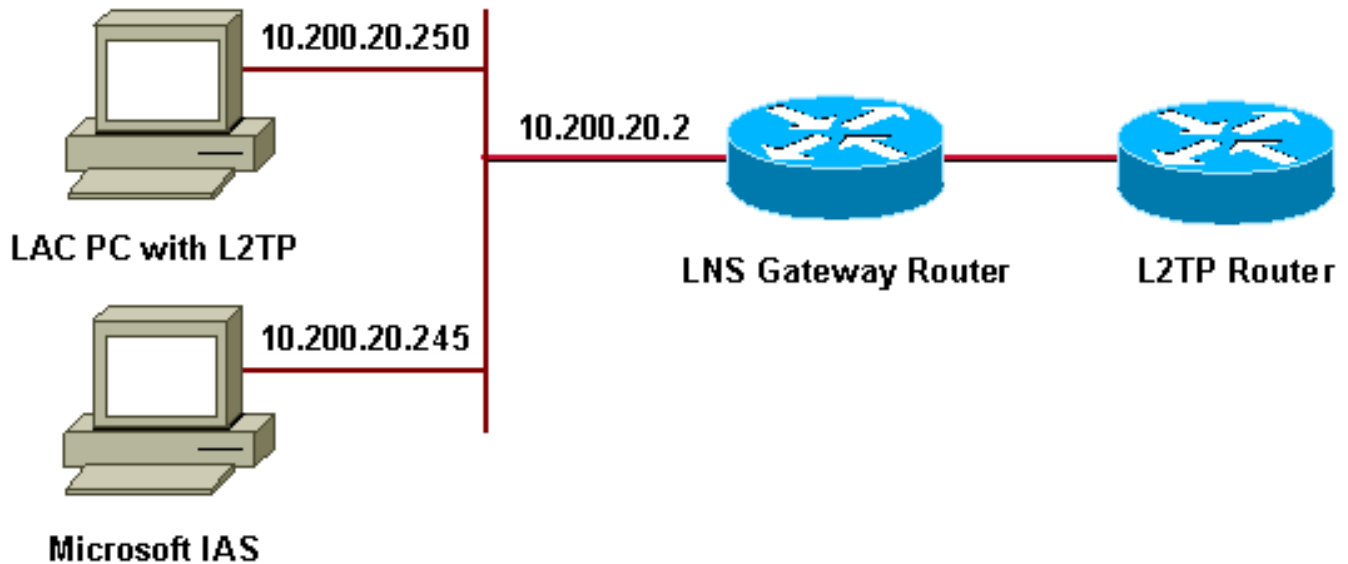
[設定](#)

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：このドキュメント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 セットアップを使用します。



このドキュメントでは、ダイヤルアップクライアントに次のIPプールを使用します。

- ゲートウェイルータ : 192.168.1.2 ~ 192.168.1.254
- LNS : 172.16.10.1 ~ 172.16.10.1

Microsoft IAS 用の Windows 2000 Advanced Server の設定

Microsoft IAS がインストールされていることを確認します。Microsoft IASをインストールするには、管理者としてログインし、次の手順を実行します。

1. [Network Services] で、すべてのチェックボックスがオフになっていることを確認します。
2. [Internet Authentication Server (IAS)]チェックボックスをオンにし、[OK]をクリックします。
3. [Windows Components] ウィザードで、[Next] をクリックします。プロンプトが表示されたら、Windows 2000 CD を挿入します。
4. 必要なファイルがコピーされたら、[完了]をクリックして、すべてのウィンドウを閉じます。リポートする必要はありません。

RADIUS クライアントの設定

次のステップを実行します。

1. [Administrative Tools] から [Internet Authentication Server] コンソールを開き、[Clients] をクリックします。
2. [Friendly Name]ボックスに、ネットワークアクセスサーバ(NAS)のIPアドレスを入力します。
3. [Use this IP]をクリックします。
4. [Client-Vendor]ドロップダウンリストで、[RADIUS Standard]が選択されていることを確認します。
5. [Shared Secret]ボックスと[Confirm Shared Secret]ボックスにパスワードを入力し、[Finish]をクリックします。
6. コンソールツリーで、[インターネット認証サービス]を右クリックし、[開始]をクリックしま

す。

7. コンソールを閉じます。

IAS 上のユーザの設定

CiscoSecureとは異なり、Windows 2000 Remote Authentication Dial-In User Server(RADIUS)ユーザデータベースは、Windowsユーザデータベースに密接にバインドされています。

- Active DirectoryがWindows 2000 Serverにインストールされている場合は、**Active Directory Users and Computers**から新しいダイヤルアップユーザを作成します。
- Active Directoryがインストールされていない場合は、[管理ツール(Administrative Tools)]の[ローカルユーザとグループ(Local Users and Groups)]を使用して新しいユーザを作成できます。

Active Directoryのユーザの設定

Active Directoryを使用してユーザを設定するには、次の手順を実行します。

1. [Active Directory Users and Computers] コンソールで、**ドメインを展開**します。
2. [ユーザ]を右クリックしてスクロールし、[新しいユーザ]を選択します。
3. 「tac」という名前の新しいユーザを作成します。
4. [パスワード]および[パスワードの確認]ダイアログボックスにパスワードを入力します。
5. [User Must Change Password at Next Logon] オプションをオフにして、[Next] をクリックします。
6. ユーザーtacの「プロパティ」ボックスを開きます。[Dial-in] タブに切り替えます。
7. [Remote Access Permission (Dial-in or VPN)] で、[Allow Access] をクリックして [OK] をクリックします。

Active Directoryがインストールされていない場合のユーザの設定

Active Directoryがインストールされていない場合にユーザを設定するには、次の手順を実行します。

1. [管理ツール]で、[コンピュータの管理]をクリックします。
2. [Computer Management] コンソールを展開し、[Local Users and Groups] をクリックします。
3. [ユーザ]を右クリックしてスクロールし、[新しいユーザ]を選択します。
4. [パスワード]および[パスワードの確認]ダイアログボックスにパスワードを入力します。
5. [User Must Change Password at Next Logon] オプションをオフにして、[Next] をクリックします。
6. 新しいユーザーtacのプロパティボックスを開きます。[Dial-in] タブに切り替えます。
7. [Remote Access Permission (Dial-in or VPN)] で、[Allow Access] をクリックして [OK] をクリックします。

Windows ユーザへのリモート アクセス ポリシーの適用

リモートアクセスポリシーを適用するには、次の手順を実行します。

1. [管理ツール]からインターネット認証サーバコンソールを開き、[リモートアクセスポリシー]をクリックします。
2. [Specify the Conditions to Match]の[Add]ボタンをクリックし、[Service-type]を追加します。使用可能なタイプとして[フレーム]を選択します。選択したタイプに追加し、[OK]を押します。
3. [Specify the Conditions to Match] の [Add] ボタンをクリックし、[Framed Protocol] を追加します。使用可能なタイプとして[PPP]を選択します。選択したタイプに追加し、[OK]を押します。
4. [Specify the Conditions to Match] の [Add] ボタンをクリックし、ユーザが所属する Windows グループを追加するために [Windows-Groups] を追加します。グループを選択し、選択したタイプに追加します。[OK] をクリックします。
5. [Allow Access if Dial-in Permission is Enabled Properties]で、[Grant Remote Access Permission]を選択します。
6. コンソールを閉じます。

L2TPのためのWindows 2000クライアントの設定

L2TP用のWindows 2000クライアントを設定するには、次の手順を実行します。

1. [スタートメニュー]から[設定]を選択し、次のいずれかのパスに従います。[Control Panel] > [Network and Dial-up Connections]または[Network and Dial-up Connections] > [Make New Connection]
2. ウィザードを使用して、L2TPという名前の接続を作成します。この接続は、インターネット経由でプライベート ネットワークに接続します。L2TPトンネルゲートウェイのIPアドレスまたは名前も指定する必要があります。
3. [Control Panel] の [Network and Dial-up Connections] ウィンドウに新しい接続が表示されます。ここから、マウスの右ボタンをクリックして、プロパティを編集します。
4. [Networking]タブで、[Type Of Server I Am Calling]が[L2TP]に設定されていることを確認します。
5. ローカルプールまたはDHCPを使用して、ゲートウェイからこのクライアントに動的な内部アドレスを割り当てる場合は、TCP/IPプロトコルを選択します。クライアントがIPアドレスを自動的に取得するように設定されていることを確認します。DNS情報を自動的に発行することもできます。[Advanced]ボタンを使用すると、静的なWINSおよびDNS情報を定義できます。[Options]タブを使用すると、IPSecをオフにしたり、接続に別のポリシーを割り当てたりできます。Securityタブで、PAP、CHAP、MS-CHAP、Windowsドメインログオンなどのユーザ認証パラメータを定義できます。
6. 接続が設定されたら、それをダブルクリックしてログイン画面を起動し、[Connect]をクリックします。

Windows 2000 クライアントのためのIPSec の無効化

1. 作成したダイヤルアップ接続L2TPのプロパティを編集します。新しい接続L2TPを右クリックし、[L2TPのプロパティ]ウィンドウを表示します。
2. [ネットワーク]タブの[インターネットプロトコル(TCP/IP)のプロパティ]をクリックします。[詳細設定]タブをダブルクリックします。[オプション]タブに移動し、[IP security properties]をクリックします。[Do not use IPSEC]が選択されている場合は、このチェックボックスをオンにします。

注：Microsoft Windows 2000クライアントにはデフォルトのリモートアクセスおよびポリシーエージェントサービスがあり、デフォルトではL2TPトラフィックのポリシーが作成されます。このデフォルトポリシーでは、IPSecと暗号化のないL2TPトラフィックは許可されません。Microsoftクライアントのレジストリエディタを編集すると、Microsoftのデフォルト動作を無効にできます。このセクションでは、Windowsレジストリを編集し、L2TPトラフィックのIPSecのデフォルトポリシーを無効にする手順について説明します。Windowsレジストリの編集については、Microsoftのドキュメントを参照してください。

レジストリエディタ(Regedt32.exe)を使用して、新しいレジストリエントリを追加し、IPSecを無効にします。詳細については、MicrosoftのマニュアルまたはRegedt32.exeのMicrosoftのヘルプトピックを参照してください。

L2TPまたはIPSec接続の各Windows 2000ベースのエンドポイントコンピュータにProhibitIpSecレジストリ値を追加して、L2TPおよびIPSecトラフィックの自動フィルタが作成されないようにする必要があります。ProhibitIpSecレジストリ値が1に設定されている場合、Windows 2000ベースのコンピュータはCA認証を使用する自動フィルタを作成しません。代わりに、ローカルまたはActive Directory IPSecポリシーをチェックします。Windows 2000ベースのコンピュータにProhibitIpSecレジストリ値を追加するには、Regedt32.exeを使用してレジストリでこのキーを見つけます。

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

このキーに次のレジストリ値を追加します。

Value Name: ProhibitIpSec

Data Type: REG_DWORD

Value: 1

注：変更を有効にするには、Windows 2000ベースのコンピュータを再起動する必要があります。詳細については、次のMicrosoftの記事を参照してください。

- Q258261:L2TPで使用されるIPSECポリシーの無効化
- Q240262：事前共有キーを使用したL2TP/IPSec接続の設定方法

L2TP用Cisco IOSの設定

次の設定では、IPSecを使用しないL2TPに必要なコマンドの概要を示します。この基本設定が機能したら、IPSecを設定することもできます。

```
angela

Building configuration...
Current configuration : 1595 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname angela
!
logging rate-limit console 10 except errors
!--- Enable AAA services here. aaa new-model aaa
authentication login default group radius local aaa
```

```
authentication login console none aaa authentication ppp
default group radius local aaa authorization network
default group radius local enable password ww ! memory-
size iomem 30 ip subnet-zero ! ! no ip finger no ip
domain-lookup ip host rund 172.17.247.195 ! ip audit
notify log ip audit po max-events 100 ip address-pool
local ! ! !--- Enable VPN/VPDN services and define
groups and !--- specific variables required for the
group. vpdn enable no vpdn logging ! vpdn-group
L2TP_Windows 2000Client !--- Default L2TP VPDN group. !-
-- Allow the Router to accept incoming requests. accept-
dialin protocol L2TP virtual-template 1 no L2TP tunnel
authentication !--- Users are authenticated at the NAS
or LNS !--- before the tunnel is established. This is
not !--- required for client-initiated tunnels. ! ! call
rsvp-sync ! ! ! ! ! ! controller E1 2/0 ! ! interface
Loopback0 ip address 172.16.10.100 255.255.255.0 !
interface Ethernet0/0 ip address 10.200.20.2
255.255.255.0 half-duplex ! interface Virtual-Template1
ip unnumbered Loopback0 peer default ip address pool
default ppp authentication ms-chap ! ip local pool
default 172.16.10.1 172.16.10.10 ip classless ip route
0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ww ! end angela# *Mar 12 23:10:54.176: L2TP:
I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.176: Tnl 8663 L2TP: New tunnel created for
remote RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:10:54.176: Tnl 8663 L2TP: O SCCRQ to
RSHANMUG-W2K1.cisco.com tnlid 5 *Mar 12 23:10:54.180:
Tnl 8663 L2TP: Tunnel state change from idle to wait-
ctl-reply *Mar 12 23:10:54.352: Tnl 8663 L2TP: I SCCCN
from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12 23:10:54.352:
Tnl 8663 L2TP: Tunnel state change from wait-ctl-reply
to established *Mar 12 23:10:54.352: Tnl 8663 L2TP: SM
State established *Mar 12 23:10:54.356: Tnl 8663 L2TP: I
ICRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/C1 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/C1 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/C1 8663/44
L2TP: I ICCN from RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/C1 8663/44 L2TP: Session state
change from wait-connect to established *Mar 12
23:10:54.544: Vi1 VPDN: Virtual interface created for
*Mar 12 23:10:54.544: Vi1 PPP: Phase is DOWN, Setup [0
sess, 0 load] *Mar 12 23:10:54.544: Vi1 VPDN: Clone from
Vtemplate 1 filterPPP=0 blocking *Mar 12 23:10:54.620:
Tnl/C1 8663/44 L2TP: Session with no hwidb *Mar 12
23:10:54.624: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up *Mar 12 23:10:54.624: Vi1 PPP: Using
set call direction *Mar 12 23:10:54.624: Vi1 PPP:
Treating connection as a callin *Mar 12 23:10:54.624:
Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0
load] *Mar 12 23:10:54.624: Vi1 LCP: State is Listen
*Mar 12 23:10:54.624: Vi1 VPDN: Bind interface
direction=2 *Mar 12 23:10:56.556: Vi1 LCP: I CONFREQ
```

```
[Listen] id 1 len 44 *Mar 12 23:10:56.556: Vi1 LCP:
MagicNumber 0x595E7636 (0x0506595E7636) *Mar 12
23:10:56.556: Vi1 LCP: PFC (0x0702) *Mar 12
23:10:56.556: Vi1 LCP: ACFC (0x0802) *Mar 12
23:10:56.556: Vi1 LCP: Callback 6 (0x0D0306) *Mar 12
23:10:56.556: Vi1 LCP: MRRU 1614 (0x1104064E) *Mar 12
23:10:56.556: Vi1 LCP: EndpointDisc 1 Local *Mar 12
23:10:56.556: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.556: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.556: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
trivially *Mar 12 23:10:56.556: Vi1 LCP: O CONFREQ
[Listen] id 1 len 15 *Mar 12 23:10:56.556: Vi1 LCP:
AuthProto MS-CHAP (0x0305C22380) *Mar 12 23:10:56.556:
Vi1 LCP: MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.560: Vi1 LCP: O CONFREQ [Listen] id 1 len 34
*Mar 12 23:10:56.560: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:10:56.560: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.560: Vi1 LCP: EndpointDisc 1 Local *Mar
12 23:10:56.560: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.560: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.700: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:10:56.700: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 12 23:10:56.704: Vi1 LCP:
MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.704: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.704: Vi1 LCP: MagicNumber 0x595E7636
(0x0506595E7636) *Mar 12 23:10:56.704: Vi1 LCP: PFC
(0x0702) *Mar 12 23:10:56.704: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:10:56.704: Vi1 LCP: O CONFACK [ACKrcvd] id 2
len 14 *Mar 12 23:10:56.708: Vi1 LCP: MagicNumber
0x595E7636 (0x0506595E7636) *Mar 12 23:10:56.708: Vi1
LCP: PFC (0x0702) *Mar 12 23:10:56.708: Vi1 LCP: ACFC
(0x0802) *Mar 12 23:10:56.708: Vi1 LCP: State is Open
*Mar 12 23:10:56.708: Vi1 PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load] *Mar 12 23:10:56.708: Vi1
MS-CHAP: O CHALLENGE id 28 len 21 from angela *Mar 12
23:10:56.852: Vi1 LCP: I IDENTIFY [Open] id 3 len 18
magic 0x595E7636 MSRASV5.00 *Mar 12 23:10:56.872: Vi1
LCP: I IDENTIFY [Open] id 4 len 27 magic 0x595E7636
MSRAS-1- RSHANMUG-W2K1 *Mar 12 23:10:56.880: Vi1 MS-
CHAP: I RESPONSE id 28 len 57 from tac *Mar 12
23:10:56.880: AAA: parse name=Virtual-Access1 idb
type=21 tty=-1 *Mar 12 23:10:56.880: AAA: name=Virtual-
Access1 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=1 channel=0 *Mar 12 23:10:56.884: AAA/MEMORY:
create_user (0x6273D024) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1 *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): port='Virtual-Access1'
list='' action=LOGIN service=PPP *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): using default list *Mar
12 23:10:56.884: AAA/AUTHEN/START (3634835145):
Method=radius (radius) *Mar 12 23:10:56.884: RADIUS:
ustruct sharecount=0 *Mar 12 23:10:56.884: RADIUS:
Initial Transmit Virtual-Access1 id 173
10.200.20.245:1645, Access-Request, len 129 *Mar 12
23:10:56.884: Attribute 4 6 0AC81402 *Mar 12
23:10:56.884: Attribute 5 6 00000001 *Mar 12
23:10:56.884: Attribute 61 6 00000001 *Mar 12
23:10:56.884: Attribute 1 5 7461631A *Mar 12
23:10:56.884: Attribute 26 16 000001370B0A0053 *Mar 12
23:10:56.884: Attribute 26 58 0000013701341C01 *Mar 12
```



```
23:10:56.884: Attribute 6 6 00000002 *Mar 12
23:10:56.884: Attribute 7 6 00000001 *Mar 12
23:10:56.900: RADIUS: Received from id 173
10.200.20.245:1645, Access-Accept, len 116 *Mar 12
23:10:56.900: Attribute 7 6 00000001 *Mar 12
23:10:56.900: Attribute 6 6 00000002 *Mar 12
23:10:56.900: Attribute 25 32 502605A6 *Mar 12
23:10:56.900: Attribute 26 40 000001370C22F6D5 *Mar 12
23:10:56.900: Attribute 26 12 000001370A061C4E *Mar 12
23:10:56.900: AAA/AUTHEN (3634835145): status = PASS
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
Port='Virtual-Access1' list='' service=NET *Mar 12
23:10:56.900: AAA/AUTHOR/LCP: Vi1 (1995716469)
user='tac' *Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP
(1995716469): send AV service=ppp *Mar 12 23:10:56.900:
Vi1 AAA/AUTHOR/LCP (1995716469): send AV protocol=lcp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
found list default *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/LCP (1995716469): Method=radius (radius) *Mar
12 23:10:56.904: RADIUS: unrecognized Microsoft VSA type
10 *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR (1995716469):
Post authorization status = PASS_REPL *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP:
Processing AV
mschap_mppe_keys*1p1T11=lv101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:56.904: Vi1 MS-CHAP: O SUCCESS id 28
len 4 *Mar 12 23:10:56.904: Vi1 PPP: Phase is UP [0
sess, 0 load] *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM:
(0): Can we start IPCP? *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/FSM (2094713042): Port='Virtual-Access1'
list='' service=NET *Mar 12 23:10:56.904:
AAA/AUTHOR/FSM: Vi1 (2094713042) user='tac' *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM
(2094713042): send AV protocol=ip *Mar 12 23:10:56.904:
Vi1 AAA/AUTHOR/FSM (2094713042): found list default *Mar
12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042):
Method=radius (radius) *Mar 12 23:10:56.908: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:56.908:
Vi1 AAA/AUTHOR (2094713042): Post authorization status =
PASS_REPL *Mar 12 23:10:56.908: Vi1 AAA/AUTHOR/FSM: We
can start IPCP *Mar 12 23:10:56.908: Vi1 IPCP: O CONFREQ
[Closed] id 1 len 10 *Mar 12 23:10:56.908: Vi1 IPCP:
Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.040: Vi1 CCP: I CONFREQ [Not negotiated] id 5
len 10 *Mar 12 23:10:57.040: Vi1 CCP: MS-PPC supported
bits 0x01000001 (0x120601000001) *Mar 12 23:10:57.040:
Vi1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP
(0x80FD0105000A120601000001) *Mar 12 23:10:57.052: Vi1
IPCP: I CONFREQ [REQsent] id 6 len 34 *Mar 12
23:10:57.052: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.052: Vi1 IPCP: PrimaryDNS 0.0.0.0
(0x810600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 12
23:10:57.052: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 12
23:10:57.052: Vi1 AAA/AUTHOR/IPCP: Start. Her address
0.0.0.0, we want 0.0.0.0 *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 12
23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=lv101~11a1W11151\1V1M1#11Z1`1k1}
```

```
111 *Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
0.0.0.0 *Mar 12 23:10:57.056: Vi1 IPCP: Pool returned
172.16.10.1 *Mar 12 23:10:57.056: Vi1 IPCP: O CONFREJ
[REQsent] id 6 len 28 *Mar 12 23:10:57.056: Vi1 IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Mar 12
23:10:57.056: Vi1 IPCP: PrimaryWINS 0.0.0.0
(0x820600000000) *Mar 12 23:10:57.056: Vi1 IPCP:
SecondaryDNS 0.0.0.0 (0x830600000000) *Mar 12
23:10:57.056: Vi1 IPCP: SecondaryWINS 0.0.0.0
(0x840600000000) *Mar 12 23:10:57.060: Vi1 IPCP: I
CONFACK [REQsent] id 1 len 10 *Mar 12 23:10:57.060: Vi1
IPCP: Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.192: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP: Address 0.0.0.0
(0x030600000000) *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Processing AV service=ppp *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 IPCP: O CONFNAK
[ACKrcvd] id 7 len 10 *Mar 12 23:10:57.192: Vi1 IPCP:
Address 172.16.10.1 (0x0306AC100A01) *Mar 12
23:10:57.324: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.324: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1, we want
172.16.10.1 *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:57.324: AAA/AUTHOR/IPCP: Vi1 (413757991)
user='tac' *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): send AV service=ppp *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR/IPCP (413757991): send AV protocol=ip
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
send AV addr*172.16.10.1 *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP (413757991): found list default *Mar 12
23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
Method=radius (radius) *Mar 12 23:10:57.324: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR (413757991): Post authorization status =
PASS_REPL *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP:
Reject 172.16.10.1, using 172.16.10.1 *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV
service=ppp *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV addr*172.16.10.1 *Mar 12 23:10:57.328: Vi1
AAA/AUTHOR/IPCP: Authorization succeeded *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Done. Her address
172.16.10.1, we want 172.16.10.1 *Mar 12 23:10:57.328:
Vi1 IPCP: O CONFACK [ACKrcvd] id 8 len 10 *Mar 12
23:10:57.328: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.328: Vi1 IPCP: State
is Open *Mar 12 23:10:57.332: Vi1 IPCP: Install route to
172.16.10.1 *Mar 12 23:10:57.904: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Virtual-Access1, changed
state to up *Mar 12 23:11:06.324: Vi1 LCP: I ECHOREP
[Open] id 1 len 12 magic 0x595E7636 *Mar 12
```

```
23:11:06.324: Vi1 LCP: Received id 1, sent id 1, line up
```

```
angela#show vpdn
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions
8663 5 RSHANMUG-W2K1.c est 192.168.1.56 1701 1
LocID RemID TunID Intf Username State Last Chg Fastswitch
44 1 8663 Vi1 tac est 00:00:18 enabled
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
*Mar 12 23:11:16.332: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x595E7636
*Mar 12 23:11:16.332: Vi1 LCP: Received id 2, sent id 2, line upsh caller
ip
Line UserIP AddressLocal NumberRemote Number<->
Vi1 tac172.16.10.1--in
```

```
angela#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 10.200.20.1 to network 0.0.0.0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C172.16.10.0/24 is directly connected, Loopback0
C172.16.10.1/32 is directly connected, Virtual-Access1
10.0.0.0/24 is subnetted, 1 subnets
C10.200.20.0 is directly connected, Ethernet0/0
S 192.168.1.0/24 [1/0] via 10.200.20.250
S* 0.0.0.0/0 [1/0] via 10.200.20.1
```

```
*Mar 12 23:11:26.328: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic
0x595E7636
*Mar 12 23:11:26.328: Vi1 LCP: Received id 3, sent id 3, line up172.16.10.1
```

```
angela#ping 172.16.10.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 156/160/168 ms
```

暗号化の有効化

interface virtual-template 1の下に**ppp encrypt mppe 40**コマンドを追加します。Microsoftクライアントでも暗号化が選択されていることを確認してください。

```
*Mar 12 23:27:36.608: L2TP: I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 13
*Mar 12 23:27:36.608: Tnl 31311 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:27:36.608: Tnl 31311 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com
tnlid 13
*Mar 12 23:27:36.612: Tnl 31311 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:27:36.772: Tnl 31311 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.772: Tnl 31311 L2TP: Tunnel state change from
```

wait-ctl-reply to established
*Mar 12 23:27:36.776: Tnl 31311 L2TP: SM State established
*Mar 12 23:27:36.780: Tnl 31311 L2TP: I ICRQ from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session FS enabled
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: New session created
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 13/1
*Mar 12 23:27:36.924: Tnl/Cl 31311/52 L2TP: I ICCN from
RSHANMUG-W2K1.cisco.com tnl 13, cl 1
*Mar 12 23:27:36.928: Tnl/Cl 31311/52 L2TP: Session state change from
wait-connect to established
*Mar 12 23:27:36.928: Vi1 VPDN: Virtual interface created for
*Mar 12 23:27:36.928: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:27:36.928: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:27:36.972: Tnl/Cl 31311/52 L2TP: Session with no hwidb
*Mar 12 23:27:36.976: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:27:36.976: Vi1 PPP: Using set call direction
*Mar 12 23:27:36.976: Vi1 PPP: Treating connection as a callin
*Mar 12 23:27:36.976: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:27:36.976: Vi1 LCP: State is Listen
*Mar 12 23:27:36.976: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:27:38.976: Vi1 LCP: TIMEout: State Listen
*Mar 12 23:27:38.976: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:27:38.976: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:27:38.976: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:38.976: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:38.984: Vi1 LCP: I CONFREQ [REQsent] id 1 len 44
*Mar 12 23:27:38.984: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:38.984: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:38.984: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.984: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.984: Vi1 LCP: (0x10D0AC0000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREQ [REQsent] id 1 len 34
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.988: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.988: Vi1 LCP: (0x10D0AC0000000A)
*Mar 12 23:27:39.096: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:27:39.096: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:39.096: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:39.128: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: State is Open
*Mar 12 23:27:39.128: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:27:39.128: Vi1 MS-CHAP: O CHALLENGE id 32 len 21 from angela
*Mar 12 23:27:39.260: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x4B4817ED MSRASV5.00
*Mar 12 23:27:39.288: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic

0x4B4817ED MSRAS-1- RSHANMUG-W2K1

```
*Mar 12 23:27:39.296: Vi1 MS-CHAP: I RESPONSE id 32 len 57 from tac
*Mar 12 23:27:39.296: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:27:39.296: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:27:39.296: AAA/MEMORY: create_user (0x6273D528) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): using default list
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): Method=radius (radius)
*Mar 12 23:27:39.296: RADIUS: ustruct sharecount=0
*Mar 12 23:27:39.300: RADIUS: Initial Transmit Virtual-Access1 id 181
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:27:39.300: Attribute 4 6 0AC81402
*Mar 12 23:27:39.300: Attribute 5 6 00000001
*Mar 12 23:27:39.300: Attribute 61 6 00000001
*Mar 12 23:27:39.300: Attribute 1 5 7461631A
*Mar 12 23:27:39.300: Attribute 26 16 000001370B0AFC72
*Mar 12 23:27:39.300: Attribute 26 58 0000013701342001
*Mar 12 23:27:39.300: Attribute 6 6 00000002
*Mar 12 23:27:39.300: Attribute 7 6 00000001
*Mar 12 23:27:39.312: RADIUS: Received from id 181 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:27:39.312: Attribute 7 6 00000001
*Mar 12 23:27:39.312: Attribute 6 6 00000002
*Mar 12 23:27:39.312: Attribute 25 32 502E05AE
*Mar 12 23:27:39.312: Attribute 26 40 000001370C225042
*Mar 12 23:27:39.312: Attribute 26 12 000001370A06204E
*Mar 12 23:27:39.312: AAA/AUTHEN (2410248116): status = PASS
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.316: AAA/AUTHOR/LCP: Vi1 (2365724222) user='tac'
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV protocol=lcp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): found list default
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): Method=radius
(radius)
*Mar 12 23:27:39.316: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR (2365724222): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: O SUCCESS id 32 len 4
*Mar 12 23:27:39.316: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.320: AAA/AUTHOR/FSM: Vi1 (1499311111) user='tac'
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV service=ppp
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV protocol=ip
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): found list default
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): Method=radius
(radius)
*Mar 12 23:27:39.320: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR (1499311111): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 12 23:27:39.320: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.320: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
```

```
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (327346364):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.324: AAA/AUTHOR/FSM: Vi1 (327346364) user='tac'
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV service=ppp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV protocol=ccp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): found list default
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): Method=radius
(radius)
*Mar 12 23:27:39.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR (327346364): Post authorization status
= PASS_REPL
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar 12 23:27:39.324: Vi1 CCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.324: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.460: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar 12 23:27:39.460: Vi1 CCP: MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.464: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar 12 23:27:39.464: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.472: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:27:39.472: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:27:39.476: Vi1 IPCP: O CONFREQ [REQsent] id 6 len 28
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.480: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.484: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.488: Vi1 CCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.488: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.596: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
```

```

*Mar 12 23:27:39.596: Vi1 CCP: State is Open
*Mar 12 23:27:39.600: Vi1 MPPE: Generate keys using RADIUS data
*Mar 12 23:27:39.600: Vi1 MPPE: Initialize keys
*Mar 12 23:27:39.600: Vi1 MPPE: [40 bit encryption] [stateless mode]
*Mar 12 23:27:39.620: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.620: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.624: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.624: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.756: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.756: AAA/AUTHOR/IPCP: Vi1 (2840659706) user='tac'
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV service=ppp
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV protocol=ip
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV
addr*172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): found list
default
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): Method=radius
(radius)
*Mar 12 23:27:39.756: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR (2840659706): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Done. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.760: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.760: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.760: Vi1 IPCP: State is Open
*Mar 12 23:27:39.764: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:27:40.316: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:27:46.628: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x4B4817ED
*Mar 12 23:27:46.628: Vi1 LCP: Received id 1, sent id 1, line up
*Mar 12 23:27:56.636: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x4B4817ED
*Mar 12 23:27:56.636: Vi1 LCP: Received id 2, sent id 2, line upcaller ip
Line UserIP AddressLocal NumberRemote Number<->
Vi1 tac172.16.10.1--in

```

```

angela#show ppp mppe virtual-Access 1
Interface Virtual-Access1 (current connection)
Software encryption, 40 bit encryption, Stateless mode
packets encrypted = 0 packets decrypted= 16
sent CCP resets = 0 receive CCP resets = 0
next tx coherency = 0 next rx coherency= 16

```

```
tx key changes = 0      rx key changes= 16
rx pkt dropped = 0      rx out of order pkt= 0
rx missed packets = 0
*Mar 12 23:28:06.604: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic
0x4B4817ED
*Mar 12 23:28:06.604: Vi1 LCP: Received id 3, sent id 3, line up
```

```
angela#ping 172.16.10.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/196/204 ms
```

```
angela#show ppp mppe virtual-Access 1
```

```
Interface Virtual-Access1 (current connection)
```

```
Software encryption, 40 bit encryption, Stateless mode
```

```
packets encrypted = 5      packets decrypted= 22
```

```
sent CCP resets = 0      receive CCP resets = 0
```

```
next tx coherency = 5      next rx coherency= 22
```

```
tx key changes = 5      rx key changes= 22
```

```
rx pkt dropped = 0      rx out of order pkt= 0
```

```
rx missed packets = 0
```

```
angela#ping 172.16.10.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 184/200/232 ms
```

```
angela#ping 172.16.10.1sh ppp mppe virtual-Access 1
```

```
Interface Virtual-Access1 (current connection)
```

```
Software encryption, 40 bit encryption, Stateless mode
```

```
packets encrypted = 10      packets decrypted= 28
```

```
sent CCP resets = 0      receive CCP resets = 0
```

```
next tx coherency = 10      next rx coherency= 28
```

```
tx key changes = 10      rx key changes= 28
```

```
rx pkt dropped = 0      rx out of order pkt= 0
```

```
rx missed packets = 0
```

```
angela#
```

[debug コマンドと show コマンド](#)

debug コマンドを使用する前に、[「デバッグコマンドの重要な情報」](#)を参照してください。

[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。

正常に動作しない場合は、最小限のデバッグに次のコマンドが含まれます。

- **debug aaa authentication** : AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization** : AAA/TACACS+ 許可に関する情報を表示します。
- **debug ppp negotiation** : PPP の開始時に送信される PPP パケットを表示します。PPP の開始時には PPP オプションがネゴシエートされます。
- **debug ppp authentication**: Challenge Authentication Protocol(CHAP)パケット交換やPassword Authentication Protocol(PAP)交換などの認証プロトコルメッセージを表示します。
- **debug radius** - RADIUS に関連するデバッグの詳細情報を表示します。

認証は機能するが、Microsoft Point-to-Point Encryption(MPPE)暗号化に問題がある場合は、次のいずれかのコマンドを使用します。

- `debug ppp mppe packet` : 着信した発信MPPEトラフィックをすべて表示します。
- `debug ppp mppe event` : 重要な MPPE の発生を表示します。
- `debug ppp mppe detailed` : 詳細な MPPE 情報を表示します。
- `debug vpdn l2x-packets`:Level 2 Forwarding(L2F)プロトコルヘッダーとステータスに関するメッセージを表示します。
- `debug vpdn events` : 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イベントに関するメッセージを表示します。
- `debug vpdn errors` : 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エラーを表示します。
- `debug vpdn packets` : 交換される各プロトコル パケットを表示します。このオプションを使用すると、大量のデバッグ メッセージが出力されるため、通常は単一のアクティブ セッションを持つデバッグ シャーシだけで使用してください。
- `show vpdn` : アクティブなL2Fプロトコルトンネル(VPDN)およびバーチャルプライベートダイヤルアップネットワーク(VPDN)のメッセージ識別子に関する情報を表示します。

`show vpdn ?`他のvpdn固有のshowコマンドを表示

スプリット トンネリング

ゲートウェイルータがインターネットサービスプロバイダー(ISP)ルータであると仮定します。Point-to-Point Tunneling Protocol(PPTP)トンネルがPCでアップすると、PPTPルートは以前のデフォルトよりも高いメトリックでインストールされるため、インターネット接続が失われます。これを解決するには、Microsoftのルーティングを変更してデフォルトを削除し、デフォルトルートを再インストールします(これは、PPTPクライアントに割り当てられたIPアドレスを知っている必要があります。現在の例では、172.16.10.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

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使用できる情報を示します。

問題 1 : 無効にされないIPSec

症状

PCユーザに次のメッセージが表示されます。

```
Error connecting to L2TP:
Error 781: The encryption attempt failed because
no valid certificate was found.
```

解決方法

[仮想プライベート接続]ウィンドウの[プロパティ]セクションに移動し、[セキュリティ]タブをクリックします。[データ暗号化を要求する]オプションを無効にします。

問題 2 : エラー 789

症状

リモートコンピュータとの初期ネゴシエーション中にセキュリティ層で処理エラーが発生したため、L2TP接続の試行が失敗しました。

Microsoft Remote AccessおよびPolicy Agentサービスは、L2TPが暗号化を提供しないため、L2TPトラフィックに使用されるポリシーを作成します。これは、Microsoft Windows 2000 Advanced Server、Microsoft Windows 2000 Server、およびMicrosoft Windows 2000 Professionalに適用されます。

解決方法

レジストリエディタ(Regedt32.exe)を使用して、新しいレジストリエントリを追加し、IPSecを無効にします。Regedt32.exeについては、MicrosoftのドキュメントまたはMicrosoftのヘルプトピックを参照してください。

L2TPまたはIPSec接続の各Windows 2000ベースのエンドポイントコンピュータにProhibitIpSecレジストリ値を追加して、L2TPおよびIPSecトラフィックの自動フィルタが作成されないようにする必要があります。ProhibitIpSecレジストリ値が1に設定されている場合、Windows 2000ベースのコンピュータはCA認証を使用する自動フィルタを作成しません。代わりに、ローカルまたはActive Directory IPSecポリシーをチェックします。Windows 2000ベースのコンピュータにProhibitIpSecレジストリ値を追加するには、Regedt32.exeを使用してレジストリでこのキーを見つけます。

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

このキーに次のレジストリ値を追加します。

Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1

注：変更を有効にするには、Windows 2000ベースのコンピュータを再起動する必要があります。

問題 3：トンネル認証においての問題

ユーザは、トンネルが確立される前にNASまたはLNSで認証されます。これは、MicrosoftクライアントからのL2TPのようなクライアント起動トンネルでは必要ありません。

PCユーザに次のメッセージが表示されます。

```
Connecting to 10.200.20.2..  
Error 651: The modem(or other connecting device) has reported an error.  
Router debugs:
```

```
*Mar 12 23:03:47.124: L2TP: I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 1  
*Mar 12 23:03:47.124: Tnl 30107 L2TP: New tunnel created for remote  
RSHANMUG-W2K1.cisco.com, address 192.168.1.56  
*Mar 12 23:03:47.124: Tnl 30107 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com  
tnlid 1  
*Mar 12 23:03:47.124: Tnl 30107 L2TP: Tunnel state change from idle to  
wait-ctl-reply  
*Mar 12 23:03:47.308: Tnl 30107 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
```

```
tntl 1
*Mar 12 23:03:47.308: Tnl 30107 L2TP: Got a Challenge Response in SCCCN
from RSHANMUG-W2K1.cisco.com
*Mar 12 23:03:47.308: AAA: parse name= idb type=-1 tty=-1
*Mar 12 23:03:47.308: AAA/MEMORY: create_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): port='' list='default'
action=SENDAUTH service=PPP
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): found list default
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=radius (radius)
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): no authenstruct
hwidb
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): Failed sendauthen
for angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = FAIL
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=LOCAL
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): SENDAUTH no password for
angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): no methods left to try
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): failed to authenticate
*Mar 12 23:03:47.308: VPDN: authentication failed, couldn't find user
information for angela
*Mar 12 23:03:47.308: AAA/MEMORY: free_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: O StopCCN to
RSHANMUG-W2K1.cisco.com tnlid 1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: Tunnel state change from
wait-ctl-reply to shutting-down
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Shutdown tunnel
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Tunnel state change from
shutting-down to idle
*Mar 12 23:03:47.324: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 1
*Mar 12 23:03:47.448: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 2
```

関連情報

- [レイヤ2トンネリングプロトコル\(L2TP\)](#)
- [デジタル証明書を使用した Windows 2000 と VPN 3000 コンセントレータ間の L2TP over IPsec の設定例](#)
- [認証を使用するPIX Firewall および Windows 2000 マシン間の L2TP Over IPsec 設定](#)
- [レイヤ2トンネルプロトコル](#)
- [バーチャルプライベートネットワークの設定](#)
- [RADIUS でのレイヤ2トンネルプロトコル認証の設定](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)