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

目次

概要

この資料は方法で手順を 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 ）のための Cisco IOS® ソフトウェアおよび Windows 2000 クライアントを設定する提供したものです。

ユーザ認証のための Microsoft Windows 2003 IAS RADIUSサーバで事前共有キーを使用してリモート Microsoft Windows 2000 /2003 および XP クライアントからの PIX セキュリティ アプライアンス モデル オフィスに IP Security （ IPSec ）上の L2TP を設定する方法に関する詳細については事前共有キー 設定例を使用して Windows 2000 /XP PC と PIX/ASA 7.2 間の L2TP Over IPSec を参照して下さい。

Windows 2000 または XP クライアント暗号化された方式を使用してリモート Microsoft Windows 2000 および XP クライアントから企業のサイトに L2TP Over IPSec を設定する方法に関する詳

細については事前共有キーを使用した設定をからの Cisco VPN 3000 シリーズ コンセントレータに L2TP Over IPSec の参照して下さい。

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

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

- Microsoft IAS オプション コンポーネントはアクティブ ディレクトリが付いている Microsoft 2000 新型サーバでインストールしました
- 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、次のネットワーク構成を使用しています。

この資料はダイヤル式クライアントのためにこれらの 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、ログインを管理者としてインストールし、これらのステップを完了するため:

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チェックし、次に『OK』 をクリック して下さい。
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、すべてのウィンドウを『Finish』 をクリック し、次に閉じて下さい。 リブートする必要はありません。

RADIUS クライアントの設定

次の手順を実行します。

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. **表示名ボックス**では、ネットワーク アクセス サーバ（NAS）の IP アドレスを入力して下さい。
3. 『Use This IP』 をクリック して下さい。
4. **Client-Vendor** ドロップダウン リストでは、**RADIUS標準が**選択されるようにして下さい。
5. **共有秘密**では**共有秘密** ボックスを**確認し**、パスワードを入力し、それから『Finish』 をクリック すれば。
6. コンソールツリーでは、右クリック **Internet Authentication Service は**、それから『Start』 をクリック し。
7. コンソールを閉じます。

IAS 上のユーザの設定

CiscoSecure とは違って、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しっかりと結合しています。

- アクティブ ディレクトリが Windows 2000 サーバでインストールされている場合、**Active Directory Users and Computers** からの新しいダイヤル式ユーザを作成して下さい。
- アクティブ ディレクトリがインストールされていない場合、新規 ユーザを作成するために**管理ツール**からの**ローカルユーザおよびグループを**使用できます。

Active Directoryのユーザの設定

アクティブ ディレクトリでユーザを設定するためにこれらのステップを完了して下さい:

1. [Active Directory Users and Computers] コンソールで、ドメインを展開します。
2. 『New User』 を選択 するために**ユーザ スクロールを**右クリックして下さい。
3. 「**tac**」という名前の新しいユーザを作成します。
4. **Password および Confirm Password ダイアログボックス**でパスワードを入力して下さい。
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 TAC **Properties** ボックスを開いて下さい。 [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

アクティブ ディレクトリがインストールされていない場合ユーザを設定するためにこれらのステップを完了して下さい:

1. **管理ツール**から、『Computer Management』 をクリック して下さい。
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. 『New User』 を選択 するために**ユーザ スクロールを**右クリックして下さい。
4. **Password および Confirm Password ダイアログボックス**でパスワードを入力して下さい。
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. 新規 ユーザ TAC **Properties** ボックスを開いて下さい。 [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ためにこれらのステップを完了して下さい:

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、『Remote Access Policies』 をクリック して下さい。
2. **Specify the Conditions to Match の Add ボタンを**クリックし、**サービス タイプを**追加して下さい。 **フレーム化される**ように利用可能 な型を選択して下さい。 それを選択されたタイプに追加し、『OK』 を押して下さい。
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。 **PPP** として利用可能 な型を選択して下さい。 それを選択されたタイプに追加し、『OK』 を押して下さい。
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、選択されたタイプにそれを追加して下さい。 [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 して下さい。
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 のための Windows 2000 クライアントを設定するためにこれらのステップを完了して下さい:

1. **Start メニュー**から、『Settings』 を選択 し、次にこれらのパスの 1 つを従って下さい :**Control Panel > Network およびダイヤル式接続***または***ネットワークおよびダイヤル式接続 > Make New Connection**
2. **L2TP と**呼ばれる接続を作成するのにウィザードを使用して下さい。 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。 また L2TP トンネル ゲートウェイの IP アドレスか名前を規定 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、プロパティを編集するためにマウス の 右ボタンをクリックして下さい。
4. **Networking タブ**の下で、**Type Of Server I Am Calling が** L2TP に設定 されることを確かめて下さい。

5. ローカルプールか DHCP によってゲートウェイからこのクライアントへの動的内部アドレスを、割り当てることを計画したら『TCP/IP Protocol』 を選択 して下さい。 クライアントが IP アドレスを自動的に得るために設定されることを確かめて下さい。 また DNS 情報を自動的に発行できます。**Advanced ボタンは**静的WINS および DNS 情報を定義することを可能にします。**Options タブは** IPSec を消すことを可能にするかまたは接続に別のポリシーを割り当てます。**Security タブ**の下で、ユーザ認証パラメータを、PAP のような、CHAP または MS-CHAP、またはウィンドウズドメインログオン定義できます。
6. 接続が設定されるとき Login 画面を起動させるために、それをダブルクリックできましたり**接続します**。

Windows 2000 クライアントのためのIPSec の無効化

1. ちょうど作成したダイヤル式接続 L2TP のプロパティを編集して下さい。 **L2TP Properties ウィンドウを**得るために新しい接続 **L2TP を**右クリックして下さい。
2. **Networking タブ**の下で、『Internet Protocol （ TCP/IP ） properties』 をクリック して下さい。 **Advanced タブを**ダブルクリックして下さい。 **Options タブ**に行き、それを『Ip security properties』 をクリック し、**Do not use IPSEC が**選択されたら、ダブルチェックして下さい。

注: 、デフォルトで、L2TP トラフィックのためのポリシーを作成する Microsoft Windows 2000 クライアントはデフォルト 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ます。このデフォルトポリシーは IPSec および暗号化なしでは L2TP トラフィックを可能にしません。Microsoft クライアント レジストリ エディタの編集によって Microsoft デフォルトの動作をディセーブルにすることができます。 Edit ウィンドウ レジストリへのプロシージャはこのセクションで L2TP トラフィックのための IPSec のデフォルトポリシーをディセーブルにするために与えられ。 編集ウィンドウ レジストリのためのマイクロソフトのドキュメンテーションを参照して下さい。

レジストリ エディタ（Regedt32.exe）を新しいレジストリエントリを IPSec をディセーブルにするために追加するのに使用して下さい。 詳細については Regedt32.exe のための Microsoft のドキュメントか Microsoft ヘルプ トピックを参照して下さい。

L2TP または IPSec接続の各 Windows 2000 ベースのエンドポイント の コンピュータに L2TP のための自動フィルタおよび IPSecトラフィックが作成されることを防ぐために ProhibitIpSecレジストリー値を追加して下さい。 ProhibitIpSecレジストリー値が 1 つに設定 されるとき、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。 その代り、それはローカルかアクティブ ディレクトリIPSecポリシーがあるように確認します。ProhibitIpSecレジストリー値を Windows 2000 ベースのコンピュータに追加するために、レジストリでこのキーを見つけるのに Regedt32.exe を使用して下さい:

```
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: Windows 2000 ベースのコンピュータを変更を有効にするために再起動して下さい。 更に詳しい情報についてはこれらのマイクロソフトの記事を参照して下さい:

- Q258261 - L2TP と使用される IPSEC ポリシーのディセーブル化
- Q240262- 事前共有キーを使用した L2TP/IPSec 接続の設定方法

L2TP のための Cisco IOS の設定

これらのコマンドが IPSec なしで L2TP のために必要としたコンフィギュレーション輪郭。 この基本設定が機能すれば、また IPSec を設定できます。

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 SCCRP 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/Cl 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/Cl 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/Cl 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/Cl 8663/44
L2TP: I ICCN from RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/Cl 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/Cl 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 CONFREJ [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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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 User IP Address Local Number Remote Number <-> Vi1 tac 172.16.10.1 - - 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 C 172.16.10.0/24 is directly connected, Loopback0 C 172.16.10.1/32 is directly connected, Virtual-Access1 10.0.0.0/24 is subnetted, 1 subnets C 10.200.20.0 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

暗号化が Microsoft クライアントでまた選択されることを **interface virtual-template 1.**の下で **ppp encrypt mppe 40 コマンドを確かめます**追加して下さい。

```
*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 CONFREJ [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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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 CONFREJ [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=1v1O1~11a1W11151\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、『**debug コマンドの重要な情報**』を参照してください。

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。

事柄がはたらかない場合、最小**デバッグは**これらのコマンドが含まれています:

- **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** — 認証プロトコルメッセージを表示する、Challenge Authentication Protocol（CHAP）パケット交換および Password Authentication Protocol（PAP）交換が含まれている。
- **debug radius**：RADIUS に関連するデバッグの詳細情報を表示します。

認証がはたらくが、Microsoft Point-to-Point Encryption（MPPE）暗号化に問題がある場合、これらのコマンドの 1 つを使用して下さい:

- **debug ppp mppe packet**：着信および発信の MPPE トラフィックを表示します。
- **debug ppp mppe event**：キーとなる 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 ヘッダおよびステータスについてのメッセージを表示する。
- **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 トンネルについての情報およびバーチャル 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を表示する。

また **show vpdn を**使用できますか。 他の VPDN 固有の **show コマンドを**見るために命じて下さい。

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）のルータであると仮定して下さい。 ポイントツーポイント トンネリング プロトコル（PPTP）トンネルが PC で起動するとき、PPTP ルートは前のデフォルトより高いメトリックとインストールされています、従って

インターネット接続を失います。 これを直し、デフォルトを削除するために Microsoft のルーティングを修正し、デフォルト ルートを再インストールするため (必要なこれが IP アドレスを知っていて PPTP クライアント割り当てられました; 現在の例のために、これは 172.16.10.1) あります:

```
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役立つ情報について説明します。

問題 1： 無効にされないIPSec

症状

PCユーザはこのメッセージを見ます:

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

解決策

Virtual Private Connection ウィンドウの Properties セクションに行き、**Security タブを**クリックして下さい。 **Require Data Encryption オプションを**ディセーブルにして下さい。

問題 2： Error 789

症状

L2TP 接続の試みはセキュリティレイヤがリモートコンピュータとの最初のネゴシエーションの間にプロセスエラーに出会ったので失敗します。

Microsoft Remote Access and Policy Agent サービスは L2TP が暗号化を提供しないのでポリシーを作成します L2TP トラフィックのために使用される。 これは Microsoft Windows 2000 Advanced サーバ、Microsoft Windows 2000サーバおよび Microsoft Windows 2000 専門家に適当です。

解決策

レジストリ エディタ (Regedt32.exe) を新しいレジストリエントリを IPSec をディセーブルにするために追加するのに使用して下さい。 Regedt32.exe のための Microsoft のドキュメントか Microsoft ヘルプ トピックを参照して下さい。

L2TP または IPSec接続の各 Windows 2000 ベースのエンドポイント の コンピュータに L2TP のための自動フィルタおよび IPSecトラフィックが作成されることを防ぐために ProhibitIpSecレジストリー値を追加して下さい。 ProhibitIpSecレジストリー値が 1 つに設定 されるとき、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。 その代り、それはローカルかアクティブ ディレクトリIPSecポリシーがあるように確認します。 ProhibitIpSecレジストリー値を Windows 2000 ベースのコンピュータに追加するために、レジス

トリでこのキーを見つけるのに Regedt32.exe を使用して下さい:

```
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: Windows 2000 ベースのコンピュータを変更を有効にするために再起動して下さい。

問題 3： トンネル認証においての問題

ユーザは NAS か LNS でトンネルが確立される前に認証されます。 Microsoft クライアントからの L2TP のような顧客によって開始されたトンネルにこれが必要となりません。

PCユーザはこのメッセージを見ます:

```
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
tnl 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

- Layer Two Tunneling Protocol （ 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