# Configuration des clients Cisco IOS et Windows 2000 pour L2TP à l'aide de Microsoft IAS

## Contenu



## Introduction

Ce document fournit des instructions sur la façon de configurer le logiciel Cisco IOS® et les clients Windows 2000 pour le protocole L2TP (Layer 2 Tunnel Protocol) à l'aide du serveur d'authentification Internet (IAS) de Microsoft.

Référez-vous à Exemple de configuration de L2TP sur IPsec entre un PC Windows 2000/XP et PIX/ASA 7.2 à l'aide de clés prépartagées pour plus d'informations sur la façon de configurer L2TP sur IP Security (IPSec) à partir de clients Microsoft Windows 2000/2003 et XP distants vers un bureau de sécurité PIX à l'entreprise à l'aide de clés pré-partagées avec Microsoft Windows 2 Serveur RADIUS IAS003 pour l'authentification des utilisateurs.

Référez-vous à Configuration de L2TP sur IPSec depuis un client Windows 2000 ou XP vers un concentrateur Cisco VPN 3000 à l'aide de clés prépartagées pour plus d'informations sur la façon

de configurer L2TP sur IPSec à partir de clients Microsoft Windows 2000 et XP distants vers un site d'entreprise à l'aide d'une méthode cryptée.

# Conditions préalables

## Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Composant facultatif Microsoft IAS installé sur un serveur avancé Microsoft 2000 avec Active Directory
- Un routeur Cisco 3600
- Logiciel Cisco IOS Version c3640-io3s56i-mz.121-5.T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

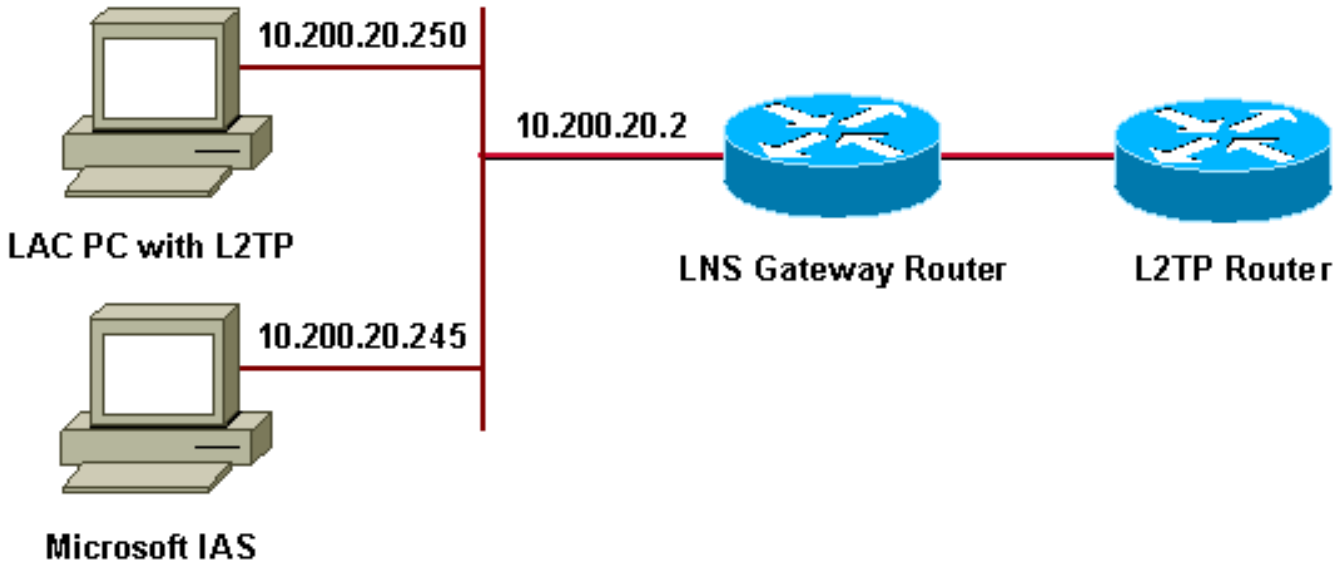
# Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque :** Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :




Ce document utilise ces pools d'adresses IP pour les clients commutés :

- Routeur de passerelle : 192.168.1.2 ~ 192.168.1.254
- LNS : 172.16.10.1 ~ 172.16.10.1

## Configuration de Windows 2000 Advanced Server pour Microsoft IAS

Vérifiez que Microsoft IAS est installé. Pour installer Microsoft IAS, connectez-vous en tant qu'administrateur et procédez comme suit :

1. Sous **Services réseau**, vérifiez que toutes les cases à cocher sont désactivées.
2. Cochez la case **Internet Authentication Server (IAS)**, puis cliquez sur **OK**.
3. Dans l'assistant Composants Windows, cliquez sur **Suivant**. Si vous y êtes invité, insérez le CD Windows 2000.
4. Une fois les fichiers requis copiés, cliquez sur **Terminer**, puis fermez toutes les fenêtres. Vous n'avez pas besoin de redémarrer.

## Configuration des clients RADIUS

Procédez comme suit :

1. Dans **Outils d'administration**, ouvrez la **console Internet Authentication Server** et cliquez sur **Clients**.
2. Dans la **zone Friendly Name**, saisissez l'adresse IP du serveur d'accès au réseau (NAS).
3. Cliquez sur **Utiliser cette adresse IP**.
4. Dans la liste déroulante **Client-Fournisseur**, assurez-vous que **RADIUS Standard** est sélectionné.
5. Dans les zones **Secret partagé** et **Confirmer le secret partagé**, saisissez le mot de passe, puis cliquez sur **Terminer**.
6. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Internet Authentication Service**, puis cliquez sur **Start**.
7. Fermez la console.

## Configuration des utilisateurs sur IAS

Contrairement à CiscoSecure, la base de données utilisateur RADIUS (Remote Authentication Dial-In User Server) de Windows 2000 est étroitement liée à la base de données utilisateur Windows.

- Si Active Directory est installé sur votre serveur Windows 2000, créez vos nouveaux utilisateurs à distance à partir d'**Utilisateurs et ordinateurs Active Directory**.
- Si Active Directory n'est pas installé, vous pouvez utiliser **Utilisateurs et groupes locaux** à partir des **Outils d'administration** afin de créer de nouveaux utilisateurs.

### Configuration des utilisateurs dans Active Directory

Complétez ces étapes afin de configurer les utilisateurs avec Active Directory :

1. Dans la console **Utilisateurs et ordinateurs Active Directory**, développez votre domaine.
2. Cliquez avec le bouton droit de la souris sur la **liste déroulante Utilisateurs** pour sélectionner **Nouvel utilisateur**.
3. Créez un nouvel utilisateur appelé tac.
4. Entrez votre mot de passe dans les boîtes de dialogue **Mot de passe** et **Confirmer le mot de passe**.
5. Effacez l'option **L'utilisateur doit changer de mot de passe lors de la prochaine connexion** et cliquez sur **Suivant**.
6. Ouvrez la zone **Propriétés** de l'utilisateur tac. Passez à l'onglet **Composer**.
7. Sous **Autorisation d'accès à distance (accès commuté ou VPN)**, cliquez sur **Autoriser l'accès**, puis sur **OK**.

### Configuration des utilisateurs si aucun Active Directory n'est installé

Complétez ces étapes afin de configurer les utilisateurs si Active Directory n'est pas installé :

1. Dans les **Outils d'administration**, cliquez sur **Gestion de l'ordinateur**.
2. Développez la console **Gestion de l'ordinateur** et cliquez sur **Utilisateurs et groupes locaux**.
3. Cliquez avec le bouton droit sur **Utilisateurs** pour sélectionner **Nouvel utilisateur**.
4. Entrez un mot de passe dans les boîtes de dialogue **Mot de passe** et **Confirmer le mot de passe**.
5. Effacez l'option **L'utilisateur doit changer de mot de passe lors de la prochaine connexion** et cliquez sur **Suivant**.
6. Ouvrez la zone **Propriétés** du nouvel utilisateur tac. Passez à l'onglet **Composer**.
7. Sous **Autorisation d'accès à distance (accès commuté ou VPN)**, cliquez sur **Autoriser l'accès**, puis sur **OK**.

## Application d'une stratégie d'accès à distance à l'utilisateur Windows

Complétez ces étapes afin d'appliquer une stratégie d'accès à distance :

1. Dans **Outils d'administration**, ouvrez la console **Internet Authentication Server** et cliquez sur **Remote Access Policies**.

2. Cliquez sur le bouton **Ajouter** dans **Spécifier les conditions à respecter** et ajouter **le type de service**. Choisissez le type disponible **Framed**. Ajoutez-le aux types sélectionnés et appuyez sur **OK**.
3. Cliquez sur le bouton **Ajouter** sur **Spécifier les conditions à respecter** et ajouter **le protocole encadré**. Choisissez le type disponible en tant que **PPP**. Ajoutez-le aux types sélectionnés et appuyez sur **OK**.
4. Cliquez sur le bouton **Ajouter** dans **Spécifier les conditions à respecter** et ajouter **Windows-Groups** pour ajouter le groupe Windows auquel appartient l'utilisateur. Choisissez le groupe et ajoutez-le aux types sélectionnés. Appuyez sur **OK**.
5. Sur **Allow Access if Dial-in Permission is Enabled Properties**, sélectionnez **Grant Remote Access Permission**.
6. Fermez la console.

## Configuration du client Windows 2000 pour L2TP

Complétez ces étapes afin de configurer le client Windows 2000 pour L2TP :

1. Dans le **menu Démarrer**, sélectionnez **Paramètres**, puis suivez l'un des chemins suivants :**Panneau de configuration > Connexions réseau et accès à distance***OU***Connexions réseau et accès à distance > Créer une nouvelle connexion**
2. Utilisez l'Assistant pour créer une connexion appelée **L2TP**. Cette connexion se connecte à un réseau privé via Internet. Vous devez également spécifier l'adresse IP ou le nom de la passerelle de tunnel L2TP.
3. La nouvelle connexion apparaît dans la fenêtre **Connexions réseau et accès à distance** sous **Panneau de configuration**. À partir de là, cliquez sur le bouton droit de la souris pour modifier les propriétés.
4. Sous l'onglet **Mise en réseau**, assurez-vous que le **type de serveur que j'appelle** est défini sur L2TP.
5. Si vous prévoyez d'allouer une adresse interne dynamique à ce client à partir de la passerelle, via un pool local ou DHCP, sélectionnez **Protocole TCP/IP**. Assurez-vous que le client est configuré pour obtenir automatiquement une adresse IP. Vous pouvez également émettre des informations DNS automatiquement.Le bouton **Avancé** vous permet de définir des informations WINS et DNS statiques.L'onglet **Options** vous permet de désactiver IPSec ou d'affecter une autre stratégie à la connexion.Sous l'onglet **Sécurité**, vous pouvez définir les paramètres d'authentification utilisateur, tels que PAP, CHAP ou MS-CHAP, ou l'ouverture de session de domaine Windows.
6. Lorsque la connexion est configurée, vous pouvez double-cliquer dessus pour lancer l'écran de connexion, puis **Se connecter**.

## Désactivation d'IPSec pour le client Windows 2000

1. Modifiez les propriétés de la connexion à distance L2TP que vous venez de créer. Cliquez avec le bouton droit sur la nouvelle connexion **L2TP** pour obtenir la fenêtre **Propriétés L2TP**.
2. Sous l'onglet **Réseau**, cliquez sur **Propriétés du protocole Internet (TCP/IP)**. Double-cliquez sur l'onglet **Avancé**. Accédez à l'onglet **Options**, cliquez sur **Propriétés de sécurité IP** et, si **Ne pas utiliser IPSEC** est sélectionné, vérifiez-le deux fois.

**Remarque :** les clients Microsoft Windows 2000 disposent d'un accès distant et de services Policy Agent par défaut qui, par défaut, créent une stratégie pour le trafic L2TP. Cette stratégie par

défaut n'autorise pas le trafic L2TP sans IPSec et chiffrement. Vous pouvez désactiver le comportement par défaut de Microsoft en modifiant l'Éditeur du Registre client Microsoft. La procédure permettant de modifier le Registre Windows et de désactiver la stratégie par défaut d'IPSec pour le trafic L2TP est indiquée dans cette section. Reportez-vous à la documentation Microsoft pour modifier le Registre Windows.

Utilisez l'Éditeur de Registre (Regedt32.exe) pour ajouter la nouvelle entrée de Registre pour désactiver IPSec. Pour plus d'informations, reportez-vous à la documentation de Microsoft ou à la rubrique d'aide de Microsoft pour Regedt32.exe.

Vous devez ajouter la valeur de Registre ProhibitIpSec à chaque ordinateur de point de terminaison Windows 2000 d'une connexion L2TP ou IPSec pour empêcher la création du filtre automatique pour le trafic L2TP et IPSec. Lorsque la valeur de Registre ProhibitIpSec est définie sur une, votre ordinateur Windows 2000 ne crée pas le filtre automatique qui utilise l'authentification CA. Il recherche plutôt une stratégie IPSec locale ou Active Directory. Afin d'ajouter la valeur de Registre ProhibitIpSec à votre ordinateur Windows 2000, utilisez Regedt32.exe pour localiser cette clé dans le Registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Ajoutez cette valeur de Registre à cette clé :

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

**Remarque :** Vous devez redémarrer votre ordinateur Windows 2000 pour que les modifications prennent effet. Pour plus d'informations, reportez-vous aux articles suivants de Microsoft :

- Q258261 - Désactivation de la stratégie IPSEC utilisée avec L2TP
- Q240262 - Configuration d'une connexion L2TP/IPSec à l'aide d'une clé pré-partagée

## Configuration de Cisco IOS pour L2TP

Ces configurations décrivent les commandes requises pour L2TP sans IPSec. Une fois que cette configuration de base fonctionne, vous pouvez également configurer IPSec.

**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     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
```

## Pour activer le chiffrement

Ajoutez la commande **ppp encrypt mppe 40** sous **interface virtual-template 1**. Assurez-vous que le chiffrement est également sélectionné dans le client Microsoft.

```
*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#
```

# Commandes debug et show

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Si les choses ne fonctionnent pas, le **débogage** minimal inclut les commandes suivantes :

- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.
- **debug ppp negotiation** - Affiche les paquets PPP transmis lors du démarrage PPP, où les options PPP sont négociées.
- **debug ppp authentication** - Affiche les messages de protocole d'authentification, qui incluent les échanges de paquets CHAP (Challenge Authentication Protocol) et les échanges PAP (Password Authentication Protocol).
- **debug radius** : affiche les informations de débogage détaillées associées au RADIUS.

Si l'authentification fonctionne, mais qu'il existe des problèmes avec le chiffrement MPPE (Microsoft Point-to-Point Encryption), utilisez l'une des commandes suivantes :

- **debug ppp mppe packet** : affiche tout le trafic MPPE sortant entrant.
- **debug ppp mppe event** : affiche les occurrences MPPE clés.
- **debug ppp mppe detail** : affiche des informations MPPE détaillées.
- **debug vpdn l2x-packets** —Affiche les messages relatifs aux en-têtes et à l'état du protocole L2F (Level 2 Forwarding).
- **debug vpdn events** : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel.
- **debug vpdn errors** : affiche les erreurs qui empêchent l'établissement d'un tunnel ou les erreurs qui provoquent la fermeture d'un tunnel établi.
- **debug vpdn packets** —Affiche chaque paquet de protocole échangé. Cette option peut entraîner un grand nombre de messages de débogage et ne doit généralement être utilisée que sur un châssis de débogage avec une seule session active.
- **show vpdn** - Affiche des informations sur le tunnel de protocole L2F actif et les identificateurs de message dans un réseau commuté privé virtuel (VPDN).

Vous pouvez également utiliser la commande **show vpdn ?** pour afficher d'autres commandes **show** spécifiques à vpdn.

### transmission tunnel partagée

Supposez que le routeur de passerelle est un routeur de fournisseur d'accès à Internet (FAI). Lorsque le tunnel PPTP (Point-to-Point Tunneling Protocol) apparaît sur le PC, la route PPTP est installée avec une métrique supérieure à la métrique par défaut précédente, de sorte que nous perdons la connectivité Internet. Pour y remédier, modifiez le routage Microsoft afin de supprimer le routage par défaut et réinstallez le routage par défaut (ceci nécessite de connaître l'adresse IP attribuée au client PPTP ; pour l'exemple actuel, il s'agit de 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
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Problème 1 : IPSec non désactivé

#### Symptôme

L'utilisateur du PC voit ce message :

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

#### Solution

Accédez à la section **Propriétés** de la fenêtre **Connexion privée virtuelle** et cliquez sur l'onglet **Sécurité**. Désactivez l'option **Exiger le chiffrement des données**.

## Problème 2 : Erreur 789

### Symptôme

La tentative de connexion L2TP échoue car la couche de sécurité a rencontré une erreur de traitement lors des négociations initiales avec l'ordinateur distant.

Les services Microsoft Remote Access et Policy Agent créent une stratégie qui est utilisée pour le trafic L2TP car L2TP ne fournit pas de chiffrement. Ceci s'applique à Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server et Microsoft Windows 2000 Professional.

### Solution

Utilisez l'Éditeur de Registre (Regedt32.exe) pour ajouter la nouvelle entrée de Registre pour désactiver IPSec. Reportez-vous à la documentation de Microsoft ou à la rubrique d'aide de Microsoft pour Regedt32.exe.

Vous devez ajouter la valeur de Registre ProhibitIpSec à chaque ordinateur de point de terminaison Windows 2000 d'une connexion L2TP ou IPSec pour empêcher la création du filtre automatique pour le trafic L2TP et IPSec. Lorsque la valeur de Registre ProhibitIpSec est définie sur une, votre ordinateur Windows 2000 ne crée pas le filtre automatique qui utilise l'authentification CA. Il recherche plutôt une stratégie IPSec locale ou Active Directory. Afin d'ajouter la valeur de Registre ProhibitIpSec à votre ordinateur Windows 2000, utilisez Regedt32.exe pour localiser cette clé dans le Registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Ajoutez cette valeur de Registre à cette clé :

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

**Remarque :** Vous devez redémarrer votre ordinateur Windows 2000 pour que les modifications prennent effet.

## Problème 3 : Problème d'authentification du tunnel

Les utilisateurs sont authentifiés au niveau du NAS ou du LNS avant l'établissement du tunnel. Ceci n'est pas nécessaire pour les tunnels initiés par le client, comme L2TP, à partir d'un client Microsoft.

L'utilisateur du PC voit ce message :

```
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
```

# Informations connexes

- Protocole L2TP (Layer Two Tunneling Protocol)
- Exemple de configuration de L2TP sur IPsec entre Windows 2000 et le concentrateur VPN 3000 à l'aide de certificats numériques
- Configuration de L2TP sur IPSec entre un pare-feu PIX Firewall et un PC Windows 2000 à l'aide de certificats
- Protocole de tunnel de couche 2
- Configuration de réseaux privés virtuels
- Configuration de l'authentification du protocole L2TP (Layer 2 Tunnel Protocol) avec RADIUS
- Support et documentation techniques - Cisco Systems