

為VPN 3000集中器PPTP配置用於Windows RADIUS身份驗證的Cisco Secure ACS

目錄

[簡介](#)

[開始之前](#)

[慣例](#)

[必要條件](#)

[採用元件](#)

[網路圖表](#)

[配置VPN 3000集中器](#)

[新增和配置Cisco Secure ACS for Windows](#)

[新增MPPE \(加密 \)](#)

[新增記帳](#)

[驗證](#)

[疑難排解](#)

[啟用調試](#)

[調試 — 良好身份驗證](#)

[可能的錯誤](#)

[相關資訊](#)

簡介

Cisco VPN 3000集中器支援本地Windows客戶端的點對點隧道協定(PPTP)隧道方法。集中器支援40位和128位加密，以實現安全的可靠連線。本文檔介紹如何在具有用於RADIUS身份驗證的Cisco Secure ACS for Windows的VPN 3000集中器上配置PPTP。

請參閱[配置Cisco Secure PIX防火牆以使用PPTP](#)來配置與PIX的PPTP連線。

請參閱[配置Cisco Secure ACS for Windows Router PPTP Authentication](#)，以設定PC與路由器的連線；這會在您允許使用者進入網路之前，為適用於Windows伺服器的思科安全存取控制系統(ACS)3.2提供使用者驗證。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

必要條件

本檔案假設在新增適用於Windows RADIUS驗證的Cisco Secure ACS之前，本地PPTP驗證正在運作。有關本地PPTP身份驗證的詳細資訊，請參閱[如何使用本地身份驗證配置VPN 3000集中器PPTP](#)。有關要求和限制的完整清單，請參閱[何時在Cisco VPN 3000集中器上支援PPTP加密？](#)

採用元件

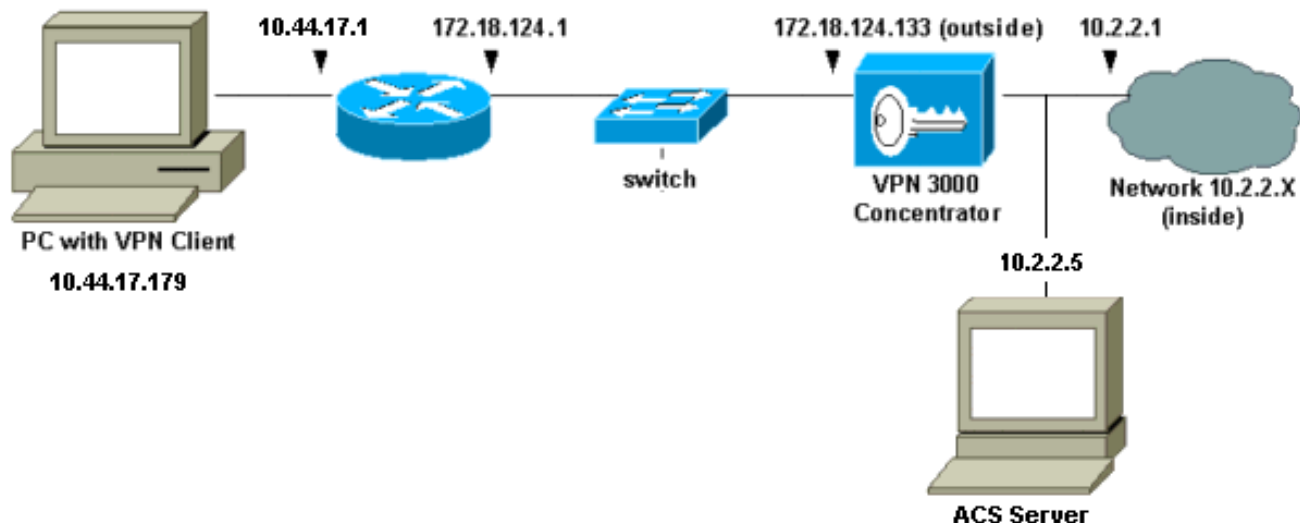
本檔案中的資訊是根據以下軟體和硬體版本。

- Cisco Secure ACS for Windows 2.5及更高版本
- VPN 3000 Concentrator 2.5.2.C版及更高版本（此配置已在版本4.0.x中驗證。）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

網路圖表

本文檔使用下圖所示的網路設定。



配置VPN 3000集中器

新增和配置Cisco Secure ACS for Windows

按照以下步驟配置VPN集中器以使用Cisco Secure ACS for Windows。

1. 在VPN 3000 Concentrator上，轉到**Configuration > System > Servers > Authentication Servers**，然後新增Cisco Secure ACS for Windows伺服器和金鑰（本示例中為「cisco123」）。

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Enter IP address or hostname.

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

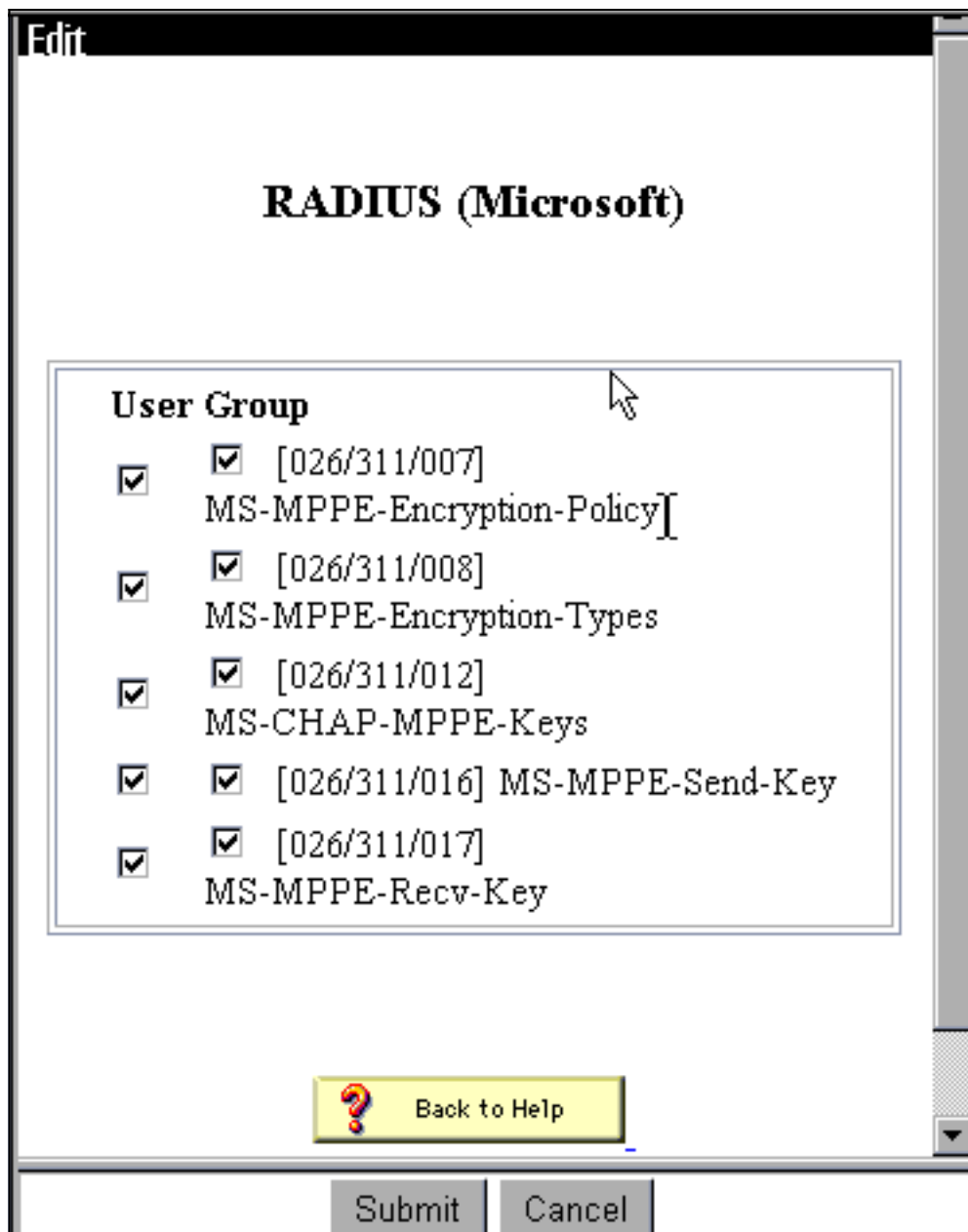
2. 在Cisco Secure ACS for Windows中，將VPN集中器新增到ACS伺服器網路配置中，並識別字

Access Server Setup For VPN3000

Network Access Server IP Address	<input type="text" value="10.2.2.1"/>
Key	<input type="text" value="cisco123"/>
Network Device Group	<input type="text" value="(Not Assigned)"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>
<input type="checkbox"/>	Single Connect TACACS+ NAS (Record stop in accounting on failure).
<input type="checkbox"/>	Log Update/Watchdog Packets from this Access Server
<input type="checkbox"/>	Log Radius Tunneling Packets from this Access Server

典型別。

3. 在Cisco Secure ACS for Windows中，轉至**Interface Configuration > RADIUS(Microsoft)**，然後檢查Microsoft點對點加密(MPPE)屬性，以使屬性顯示在組介面中。



4. 在Cisco Secure ACS for Windows中，新增使用者。在使用者組中，新增MPPE(Microsoft RADIUS)屬性，以防以後需要加密。

Access Restrictions	Token Cards	Password Aging
IP Address Assignment	IETF Radius	Cisco VPN3000 Radius
MS MPPE Radius		

Microsoft RADIUS Attributes ?

[311\007] MS-MPPE-Encryption-Policy
Encryption Allowed

[311\008] MS-MPPE-Encryption-Types
40-bit

[311\012] MS-CHAP-MPPE-Keys

[311\016] MS-MPPE-Send-Key

[311\017] MS-MPPE-Recv-Key

5. 在VPN 3000 Concentrator上，轉到**Configuration > System > Servers > Authentication Servers**。從清單中選擇身份驗證伺服器，然後選擇**測試**。通過輸入使用者名稱和密碼，測試從VPN集中器到Cisco Secure ACS for Windows伺服器的身份驗證。如果身份驗證正常，VPN集中器應顯示「身份驗證成功」消息。Cisco Secure ACS for Windows中的故障記錄在**Reports and Activity > Failed Attempts**中。在預設安裝中，這些報告儲存在C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts中的磁碟上。

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

User Name

Password


OK Cancel

6. 由於您現在已驗證從PC到VPN集中器以及從VPN集中器到Cisco Secure ACS for Windows伺服器的身份驗證有效，因此您可以將Cisco Secure ACS for Windows伺服器移到伺服器清單頂部，重新配置VPN集中器以將PPTP使用者傳送到Cisco Secure ACS for Windows RADIUS。要在VPN集中器上執行此操作，請轉至**Configuration > System > Servers > Authentication Servers**。

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
10.2.2.5 (Radius) 	Add
Internal (Internal)	Modify
	Delete
	Move Up
	Move Down
	Test

7. 轉至 Configuration > User Management > Base Group，然後選擇PPTP/L2TP頁籤。在VPN集中器基本組中，確保PAP和MSCHAPv1的選項已啟用。

General

IPSec

PPTP/L2TP

PPTP/L2TP Parameters

Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

8. 選擇General頁籤，並確保在Tunneling Protocols部分允許PPTP。

Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.

9. 在Cisco Secure ACS for Windows RADIUS伺服器中測試使用者的PPTP身份驗證。如果這不起作用，請參閱[調試](#)部分。

[新增MPPE \(加密 \)](#)

如果適用於Windows RADIUS PPTP身份驗證的Cisco Secure ACS工作不加密，則可以將MPPE新增到VPN 3000集中器。

1. 在VPN集中器上，轉至**Configuration > User Management > Base Group**。
2. 在「PPTP加密」一節下，選中**Required**、**40-bit**和**128-bit**的選項。由於並非所有PC都支援40位和128位加密，因此請選中這兩個選項以允許協商。
3. 在「PPTP身份驗證協定」一節下，選中**MSCHAPv1**的選項。（在之前的步驟中，您已配置用於Windows 2.5的Cisco Secure ACS使用者屬性進行加密。）

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
PPTP Encryption	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

註：應識別PPTP客戶端，以獲得最佳或所需的資料加密和MSCHAPv1（如果存在選項）。

新增記帳

建立身份驗證後，可以將記帳新增到VPN集中器。轉到**Configuration > System > Servers > Accounting Servers**，然後新增Cisco Secure ACS for Windows伺服器。

在Cisco Secure ACS for Windows中，記帳記錄如下所示。

```
Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id,
Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets,
Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
03/18/2000,08:16:20,CSNTUSER,Default Group,,Start,8BD00003,,Framed,
PPP,,,,,1.2.3.4,1163,10.2.2.1
03/18/2000,08:16:50,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,
PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

啟用調試

如果連線不起作用，您可以通過轉至**Configuration > System > Events > Classes > Modify**將PPTP和AUTH事件類新增到VPN集中器。您還可以新增PPTPDBG、PPTPDECODE、AUTHDBG和AUTHDECODE事件類，但這些選項可能提供過多資訊。

Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Class Name <input type="text" value="PPTP"/>	
Enable <input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log <input type="text" value="1-9"/>	Select the range of severity values to enter in the log.
Severity to Console <input type="text" value="1-3"/>	Select the range of severity values to display on the console.
Severity to Syslog <input type="text" value="None"/>	Select the range of severity values to send to a Syslog server.
Severity to Email <input type="text" value="None"/>	Select the range of severity values to send via email to the recipient list.
Severity to Trap <input type="text" value="None"/>	Select the range of severity values to send to an SNMP system.

您可以轉至**Monitoring > Event Log**來檢索事件日誌。

Monitoring | Event Log

Select Filter Options

Event Class: All Classes (dropdown menu showing AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu showing 1, 2, 3)

Client IP Address: 0.0.0.0 (text input)

Events/Page: 100 (dropdown menu)

Direction: Oldest to Newest (dropdown menu)

Navigation buttons: <<<, <<, >>, >>>, Get Log, Save Log, Clear Log

```

1 12/04/2000 14:51:32.600 SEV=4 AUTH/22 RPT=21
User pptpuser disconnected

2 12/04/2000 14:51:32.600 SEV=4 PPTP/35 RPT=14 10.44.17.179
Session closed on tunnel 10.44.17.179 (peer 0, local 45636, serial 0), re
Administrative shutdown (No additional info)

4 12/04/2000 14:51:32.640 SEV=4 PPTP/34 RPT=14 10.44.17.179
Tunnel to peer 10.44.17.179 closed, reason: Stop-Local-Shutdown (No addit
info)

6 12/04/2000 14:51:49.150 SEV=4 PPTP/47 RPT=15 10.44.17.179
Tunnel to peer 10.44.17.179 established

```

調試 — 良好身份驗證

VPN集中器上的良好調試將類似於以下內容。

```

1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected

```

可能的錯誤

您可能會遇到如下所示的可能錯誤。

[用於Windows RADIUS伺服器的Cisco Secure ACS上的使用者名稱或密碼錯誤](#)

- VPN 3000集中器調試輸出

```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established
```

```
7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179
```

```
8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23
```

```
9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser
```

```
11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )
```

```
12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```

- Cisco Secure ACS for Windows日誌輸出

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

- 使用者看到的消息 (來自Windows 98)

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

在集中器上選擇了「需要MPPE加密」，但是未為MS-CHAP-MPPE-Keys和MS-CHAP-MPPE-Types配置適用於Windows伺服器的Cisco Secure ACS

- VPN 3000集中器調試輸出如果已開啟AUTHDECODE (1-13嚴重性) 和PPTP調試 (1-9嚴重性)，則日誌顯示面向Windows伺服器的Cisco Secure ACS不會從伺服器的access-accept (部分日誌) 中傳送供應商特定的屬性26(0x1A)。

```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE .N...u.l6Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF ..//.....
```

```
2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```

- Cisco Secure ACS for Windows日誌輸出未顯示任何故障。

- 使用者看到的消息

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

[相關資訊](#)

- [Cisco VPN 3000系列集中器支援頁面](#)
- [Cisco VPN 3000系列使用者端支援頁面](#)
- [IPSec支援頁面](#)
- [Cisco Secure ACS for Windows支援頁](#)
- [RADIUS 支援頁面](#)
- [PPTP支援頁面](#)

- [RFC 2637:點對點通道通訊協定\(PPTP\)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)