

VPN 3000 Concentrator PPTP نيوكت ةق داصم ل Cisco Secure ACS مادختساب Windows RADIUS

المحتويات

[المقدمة](#)

[قبل البدء](#)

[الاصطلاحات](#)

[المتطلبات الأساسية](#)

[المكونات المستخدمة](#)

[الرسم التخطيطي للشبكة](#)

[تكوين مركز VPN 3000](#)

[إضافة مصدر المحتوى الإضافي الآمن من Cisco وتكوينه ل Windows](#)

[إضافة MPPE \(تشفير\)](#)

[إضافة محاسبة](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[تمكين تصحيح الأخطاء](#)

[تصحيح الأخطاء - مصادقة جيدة](#)

[الأخطاء المحتملة](#)

[معلومات ذات صلة](#)

المقدمة

يدعم مركز Cisco VPN 3000 أسلوب الاتصال النفقي لبروتوكول نفق من نقطة إلى نقطة (PPTP) لعملاء Windows الأصليين. يدعم مركز التكرير تشفير 40-بت و 128-بت من أجل توصيل آمن يمكن الاعتماد عليه. يصف هذا المستند كيفية تكوين PPTP على مركز VPN 3000 مع Cisco ACS الآمن ل Windows لمصادقة RADIUS.

ارجع إلى [تكوين جدار حماية Cisco Secure PIX لاستخدام PPTP](#) لتكوين إتصالات PPTP إلى PIX.

ارجع إلى [تكوين ACS الآمن من Cisco لمصادقة PPTP لموجه Windows](#) لإعداد اتصال جهاز كمبيوتر بالموجه؛ وهذا يوفر مصادقة المستخدم لنظام التحكم في الوصول الآمن (ACS) 3.2 من Cisco لخادم Windows قبل السماح للمستخدم بالدخول إلى الشبكة.

قبل البدء

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع [اصطلاحات تلميحات Cisco التقنية](#).

المتطلبات الأساسية

يفترض هذا المستند أن مصادقة PPTP المحلية تعمل قبل إضافة Cisco ACS الآمن لمصادقة Windows RADIUS. يرجى الاطلاع على كيفية تكوين VPN 3000 Concentrator PPTP باستخدام المصادقة المحلية للحصول على مزيد من المعلومات حول مصادقة PPTP المحلية. للحصول على قائمة كاملة من المتطلبات والقيود، يرجى الرجوع إلى متى يتم دعم تشفير PPTP على مركز Cisco VPN 3000؟

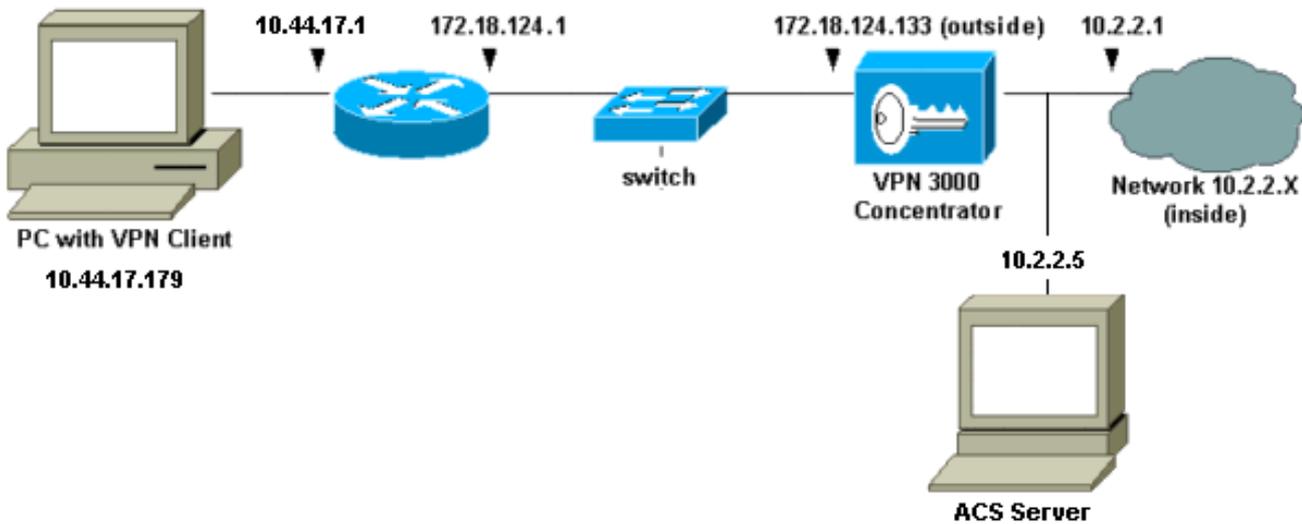
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows الإصدار 2.5 والإصدارات الأحدث
 - VPN 3000 Concentrator صيغة c.2.5.2 وفيما بعد (تم التحقق من هذا التكوين باستخدام الإصدار .x.4.0).
- تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



تكوين مركز VPN 3000

إضافة مصدر المحتوى الإضافي الآمن من Cisco وتكوينه ل Windows

اتبع هذه الخطوات لتكوين مركز VPN لاستخدام ACS الآمن من Cisco ل Windows.

1. على مركز VPN 3000، انتقل إلى التكوين < النظام < الخوادم < خوادم المصادقة وأضف مصدر المحتوى الإضافي الآمن من Cisco ل خادم ومفتاح Cisco123 ("Windows" في هذا المثال).

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. في Cisco Secure ACS ل Windows، أضيف مركز VPN إلى تكوين شبكة خادم ACS، وحدد نوع

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

Submit

Submit + Restart

Delete

Cancel

القاموس

3. في ACS الآمن من Cisco لنظام التشغيل Windows، انتقل إلى تكوين الواجهة < RADIUS (Microsoft) وحدد سمات تشفير Microsoft من نقطة إلى نقطة (MPPE) حتى تظهر السمات في واجهة

Edit

RADIUS (Microsoft)

User Group

- [026/311/007]
MS-MPPE-Encryption-Policy[
- [026/311/008]
MS-MPPE-Encryption-Types
- [026/311/012]
MS-CHAP-MPPE-Keys
- [026/311/016] MS-MPPE-Send-Key
- [026/311/017]
MS-MPPE-Recv-Key

 Back to Help

المجموعة. 4. في Cisco Secure ACS ل Windows، أضف مستخدماً. في مجموعة المستخدمين، قم بإضافة سمات (MPPE (Microsoft RADIUS، في حالة إحتياجك للتشفير في وقت

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

لاحق.

5. على مركز VPN 3000، انتقل إلى التكوين < النظام < الخوادم < خوادم المصادقة. حدد خادم مصادقة من القائمة، ثم حدد إختبار. اختبر المصادقة من مركز الشبكة الخاصة الظاهرية (VPN) إلى مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows من خلال إدخال اسم مستخدم وكلمة مرور. في مصادقة جيدة، يجب أن يعرض مركز الشبكة الخاصة الظاهرية (VPN) رسالة "نجاح المصادقة". يتم تسجيل حالات الفشل في Cisco Windows J Secure ACS في التقارير والنشاط < محاولات فاشلة. في عملية تثبيت افتراضية، يتم تخزين هذه التقارير على القرص في C:\Program Files\CiscoSecure ACS v2.5\LOG\Failed Attempts.

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. بما أنك قد قمت الآن بالتحقق من المصادقة من الكمبيوتر الشخصي إلى مركز VPN ومن المركز إلى ACS الآمن من Cisco لخدم Windows، فيمكنك إعادة تكوين مركز VPN لإرسال مستخدمي PPTP إلى Cisco ACS الآمن لـ Windows RADIUS عن طريق نقل مصدر المحتوى الإضافي الآمن من Cisco لخدم Windows إلى أعلى قائمة الخوادم. للقيام بذلك على مركز الشبكة الخاصة الظاهرية (VPN)، انتقل إلى التكوين < النظام < الخوادم < خوادم المصادقة.

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)  Internal (Internal)	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Test"/>

7. انتقل إلى التكوين < إدارة المستخدم > المجموعة الأساسية وحدد علامة التويب PPTP/L2TP. في مجموعة قاعدة مركز الشبكة الخاصة الظاهرية (VPN)، تأكد من تمكين خيارات PAP و MSCHAPv1.

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 all options means that no 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 checked="" 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 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.

8. حدد علامة التبويب عام وتأكد من السماح ب PPTP في قسم بروتوكولات الاتصال النفقي.

Idle Timeout	30	(minutes) Enter the idle time out for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		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.

Apply Cancel

9. اختبر مصادقة PPTP مع المستخدم في ال Cisco يؤمن ACS لخدم Windows RADIUS. إذا لم ينجح ذلك، فالرجاء مراجعة قسم [تصحيح الأخطاء](#).

إضافة MPPE (تشفير)

إذا كان مصدر المحتوى الإضافي الآمن من Cisco لمصادقة PPTP Windows RADIUS يعمل دون تشفير، فيمكنك إضافة MPPE إلى مركز VPN 3000.

1. على مركز الشبكة الخاصة الظاهرية (VPN)، انتقل إلى التكوين < إدارة المستخدم > المجموعة الأساسية.
2. تحت قسم لتشفير PPTP، تحقق من الخيارات ل **مطلوب**، 40-بت، و128-بت. بما أن ليس كل أجهزة الكمبيوتر تدعم كلا من تشفير 40 بت و 128 بت، تحقق من كلا الخيارين للسماح بالتفاوض.
3. تحت القسم لبروتوكولات مصادقة PPTP، تحقق من الخيار ل **MSCHAPv1**. (لقد قمت بالفعل بتكوين مصدر المحتوى الإضافي الآمن من Cisco لسماح مستخدم Windows 2.5 للتشفير في خطوة سابقة.)

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 checked="" 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.

ملاحظة: يجب التعرف على عميل PPTP لتشفير البيانات الأمل أو المطلوب و MSCHAPv1 (إذا كان هناك خيار).

إضافة محاسبة

بعد إنشاء المصادقة، يمكنك إضافة محاسبة إلى مركز الشبكة الخاصة الظاهرية (VPN). انتقل إلى التكوين < النظام < الخوادم < خوادم المحاسبة وأضف مصدر المحتوى الإضافي الآمن من Cisco لخدم Windows.

في مصدر المحتوى الإضافي الآمن من Cisco ل Windows، تظهر سجلات المحاسبة كما يلي.

```
,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
,CSNTUSER,Default Group,,Start,8BD00003,,Framed,03/18/2000,08:16:20
PPP,,,,,1.2.3.4,1163,10.2.2.1
,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,03/18/2000,08:16:50
PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تمكين تصحيح الأخطاء

إذا لم تعمل الاتصالات، يمكنك إضافة فئات أحداث PPTP و AUTH إلى مركز VPN بالانتقال إلى التكوين < النظام < الأحداث < الفئات < التعديل. يمكنك أيضا إضافة فئات أحداث PPTPDBG، و PPTPDECODE، و AUTHDBG، و AUTHDECODE، ولكن هذه الخيارات قد توفر معلومات كثيرة جدا.

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.

يمكنك إسترداد سجل الأحداث بالانتقال إلى المراقبة < سجل الأحداث.

Monitoring | Event Log

Select Filter Options

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

Severities: ALL (dropdown menu with 1, 2, 3 selected)

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

```

[تصحيح الأخطاء - مصادقة جيدة](#)

ستبدو عمليات تصحيح الأخطاء الجيدة على مركز الشبكة الخاصة الظاهرية (VPN) مماثلة لما يلي.

```

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

```

[الأخطاء المحتملة](#)

قد تواجه أخطاء محتملة كما هو موضح أدناه.

[اسم مستخدم أو كلمة مرور غير صحيحة على Cisco Secure ACS لخادم Windows RADIUS](#)

• إخراج تصحيح أخطاء مركز VPN 3000

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

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

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

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

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

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

• مصدر المحتوى الإضافي الآمن من Cisco لإخراج سجل Windows

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

• الرسالة التي يراها المستخدم (من 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
```

يتم تحديد "تشفير MPPE مطلوب" على مركز الترتيز، ولكن لم يتم تكوين مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows لأنواع MS-CHAP-MPPE و MS-CHAP-MPPE-Keys

• إخراج تصحيح أخطاء مركز VPN 3000 إذا كان AUTHDECODE (مستوى خطورة 1-13) وتصحيح أخطاء PPTP (مستوى خطورة 1-9) قيد التشغيل، يظهر السجل أن مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows لا يرسل السمة 26 (0x1a) الخاصة بالمورد في قبول الوصول من الخادم (سجل جزئي).

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

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

• لا يظهر مصدر المحتوى الإضافي الآمن من Cisco لمخرجات سجل Windows أي حالات فشل.
• الرسالة التي يراها المستخدم

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

[معلومات ذات صلة](#)

- [صفحة دعم مركز Cisco VPN 3000 Series](#)
- [صفحة دعم عمل Cisco VPN 3000 Series](#)
- [صفحة دعم IPSec](#)
- [مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows](#)
- [صفحة دعم RADIUS](#)
- [صفحة دعم PPTP](#)

- [المعيار RFC 2637: بروتوكول الاتصال النفقي من نقطة إلى نقطة \(PPTP\)](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه
ىل إأمئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل