

VPN 4.x نوبزو VPN 3000 زكرم ني ب IPsec نيوكت لاثمل RADIUS مادختساب Windows مدختساب لة قداصم و تاباسح

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [إستخدام المجموعات على مركز VPN 3000](#)
- [كيف يستخدم مركز VPN 3000 سمات المجموعة والمستخدم](#)
- [تكوين مركز VPN 3000 Series](#)
- [تكوين خادم RADIUS](#)
- [عنت عنوان ساكن إستاتيكي إلى ال VPN زبون مستعمل](#)
- [تكوين عميل شبكة VPN](#)
- [إضافة محاسبة](#)
- [التحقق من الصحة](#)
- [التحقق من مركز VPN](#)
- [التحقق من عميل شبكة VPN](#)
- [إستكشاف الأخطاء وإصلاحها](#)
- [أستكشاف أخطاء VPN Client 4.8 وإصلاحها ل Windows](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية إنشاء نفق IPsec بين مركز Cisco VPN 3000 و عميل Cisco VPN 4.x ل Microsoft Windows الذي يستخدم RADIUS لمصادقة المستخدم ومحاسبته. يوصي هذا المستند بخادم التحكم في الوصول الآمن (ACS) من Cisco لأنظمة التشغيل Windows للحصول على تكوين RADIUS أسهل لمصادقة المستخدمين الذين يقومون بالاتصال بموجه VPN 3000. مجموعة على مركز VPN 3000 هي مجموعة من المستخدمين تتم معاملتهم ككيان واحد. ويمكن لتهيئة المجموعات، مقارنة بالمستخدمين الأفراد، تبسيط إدارة النظام وتنظيم مهام التهيئة.

ارجع إلى [PIX/ASA 7.x و Cisco VPN Client 4.x ل Windows مع مثال تكوين مصادقة Microsoft Windows](#)
[2003 IAS RADIUS](#) لإعداد اتصال VPN للوصول عن بعد بين عميل (4.x ل Windows) وجهاز الأمان
PIX 500 Series 7.x الذي يستخدم خادم RADIUS لخدمة مصادقة الإنترنت (IAS) في Microsoft Windows
2003.

ارجع إلى [تكوين IPsec بين موجه Cisco IOS و عميل Cisco VPN 4.x ل Windows الذي يستخدم RADIUS](#)

[لمصادقة المستخدم](#) لتكوين اتصال بين موجه وعميل Cisco VPN 4.x الذي يستخدم RADIUS لمصادقة المستخدم.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- يتم تثبيت مصدر المحتوى الإضافي الآمن من Cisco لـ Windows RADIUS ويعمل بشكل صحيح مع الأجهزة الأخرى.
- تم تكوين مركز Cisco VPN 3000 ويمكن إدارته باستخدام واجهة HTML.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Windows لـ Cisco Secure ACS مع الإصدار 4.0
- مركز Cisco VPN 3000 Series مع ملف الصورة B.4.7.2
- عميل شبكة VPN 4.x من Cisco

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

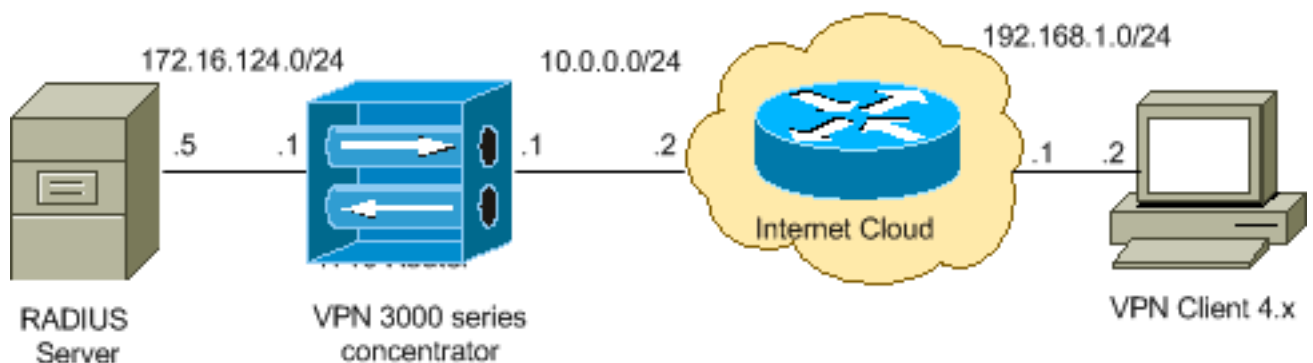
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

إستخدام المجموعات على مركز VPN 3000

يمكن تحديد مجموعات لكل من مصدر المحتوى الإضافي الآمن من Cisco ل Windows و مركز VPN 3000، ولكنهم يستخدمون المجموعات بشكل مختلف بعض الشيء. قم بتنفيذ هذه المهام من أجل تبسيط الأمور:

- قم بتكوين مجموعة واحدة على مركز VPN 3000 عندما تقوم بإنشاء النفق الأولي. وهذا غالبا ما يسمى مجموعة النفق وهو يستخدم لإنشاء جلسة عمل مشفرة لتبادل مفتاح الإنترنت (IKE) إلى مركز VPN 3000 باستخدام مفتاح مشترك مسبقا (كلمة مرور المجموعة). هذا هو نفس اسم المجموعة وكلمة المرور التي يجب تكوينها على جميع عملاء Cisco VPN الذين يرغبون في الاتصال بمركز VPN.
- قم بتكوين المجموعات على Cisco Secure ACS ل خادم Windows الذي يستخدم سمات RADIUS القياسية وسمات المورد المحددة (VSAs) لإدارة النهج. ال VSAs أن ينبغي استعملت مع ال VPN 3000 مركز يكون ال (RADIUS VPN 3000) سمة.
- قم بتكوين المستخدمين على مصدر المحتوى الإضافي الآمن من Cisco ل خادم RADIUS Windows وقم بتعيينهم إلى إحدى المجموعات التي تم تكوينها على الخادم نفسه. يرث المستخدمون السمات المحددة لمجموعتهم ويرسل Cisco Secure ACS ل Windows هذه السمات إلى مركز VPN عندما يكون المستخدم مصدقا.

كيف يستخدم مركز VPN 3000 سمات المجموعة والمستخدم

بعد أن يقوم مركز VPN 3000 بمصادقة مجموعة النفق مع مركز VPN والمستخدم مع RADIUS، يجب أن يقوم بتنظيم السمات التي تلقيتها. يستخدم مركز VPN الخصائص في هذا الترتيب من التفضيلات، سواء تمت المصادقة في مركز VPN أو مع RADIUS:

1. سمات المستخدم- تكون هذه السمات دائما ذات أسبقية على غيرها.
2. سمات مجموعة النفق- أي سمات لم يتم إرجاعها عند مصادقة المستخدم يتم تعبئتها بسمات مجموعة النفق.
3. خصائص المجموعة الأساسية- أي خصائص مفقودة من المستخدم أو مجموعة النفق تعبأ بخصائص مجموعة قاعدة مركز VPN.

تكوين مركز VPN 3000 Series

أكمل الإجراء في هذا القسم لتكوين مركز Cisco VPN 3000 للمعلومات المطلوبة لاتصال IPsec بالإضافة إلى عميل AAA لمستخدم VPN للمصادقة مع خادم RADIUS.

في إعداد المختبر هذا، يتم الوصول إلى مركز VPN أولا من خلال منفذ وحدة التحكم ويتم إضافة تكوين أدنى كما يوضح هذا الإخراج:

```
Login: admin
The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator ---!
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
```

```

Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
- #2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces
<

```

يظهر مركز VPN في التكوين السريع، ويتم تكوين هذه العناصر.

• الوقت/التاريخ

• الواجهات/الأقنعة في التكوين < الواجهات (عام=24/10.0.0.1، خاص=24/172.16.124.1)

• البوابة الافتراضية في التكوين < النظام < توجيه (10.0.0.2 > Default_Gateway IP)

عند هذه النقطة، يمكن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) من خلال HTML من الشبكة الداخلية.

ملاحظة: إذا تمت إدارة مركز الشبكة الخاصة الظاهرية (VPN) من الخارج، فعليك أيضا تنفيذ الخطوات التالية:

1. أختَر تكوين < 1-واجهات < 2-عام < 4-تحديد مرشح > 1 IP. خاص (افتراضي).

2. أختَر إدارة < حقوق الوصول > 7 < قائمة التحكم في الوصول < محطة عمل مدير إضافة 1 لإضافة عنوان IP الخاص بالمدير الخارجي.

لا تكون هذه الخطوات مطلوبة إلا إذا قمت بإدارة مركز VPN من الخارج.

بمجرد اكتمال هاتين الخطوتين، يمكن تنفيذ بقية التكوين من خلال واجهة المستخدم الرسومية (GUI) باستخدام مستعرض ويب والاتصال ب IP الخاص بالواجهة التي قمت بتكوينها للتو. في هذا المثال وعند هذه النقطة، يمكن الوصول إلى مركز VPN من خلال HTML من الشبكة الداخلية:

1. أختَر **تشكيل** < قارن in order to recheck القارن بعد أن يشكل أنت ال .gui

Configuration | Interfaces Friday, 27 October 2006
Save Needed [X] Re

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. أتمت هذا steps in order to أضفت ال cisco يؤمن ل acs ل Windows RADIUS نادل إلى ال VPN 3000 مركز تشكيل. اخترت تشكيل < نظام < خادم < مصادقة، ويضيف قطعة من القائمة يسار.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type: Selecting *Internal Server* will let you add users to database. If you are using RADIUS authentication additional authorization check, do not configure at

Authentication Server: Enter IP address or hostname.

Used For: Select the operation(s) for which this RADIUS se

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.

أختر **RADIUS** لنوع الخادم وأضف هذه المعلمات ل Cisco ACS الآمن لخادم Windows RADIUS. أترك كافة المعلمات الأخرى في حالتها الافتراضية. خادم المصادقة—أدخل عنوان IP الخاص بمصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS. سر الخادم—أدخل سر خادم RADIUS. هذا ينبغي كنت ال نفسه سر يستعمل أنت عندما يشكل أنت ال VPN 3000 مركز في ال cisco يأمن ل ACS ل Windows تشكيل. دقت—أعدت الكلمة للتحقق. وهذا يضيف خادم المصادقة في التكوين العام ل VPN 3000 Concentrator. يتم إستخدام هذا الخادم من قبل جميع المجموعات باستثناء الحالات التي يتم فيها تعريف خادم مصادقة بشكل محدد. في حالة عدم تكوين خادم مصادقة لمجموعة، فإنه يرجع إلى خادم المصادقة العام.

3. أتمت هذا steps in order to شكلت مجموعة النفق على ال VPN 3000 مركز. اختر تشكيل < إدارة المستخدم < مجموعات من القائمة اليسرى وانقر إضافة. قم بتغيير هذه المعلمات أو إضافتها في علامات تويب التكوين. لا تنقر فوق تطبيق حتى تقوم بتغيير كافة المعلمات التالية: ملاحظة: هذه المعلمات هي الحد الأدنى المطلوب لاتصالات VPN للوصول عن بعد. تفترض هذه المعلمات أيضا أنه لم يتم تغيير الإعدادات الافتراضية في المجموعة الأساسية على مركز VPN

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	ipsecgroup	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

اسم المجموعة- اكتب اسم المجموعة. على سبيل المثال، IPsecUsers. أدخل كلمة مرور- كلمة مرور للمجموعة. هذا هو المفتاح المشترك مسبقاً لجلسة عمل IKE. دقت—أعدت الكلمة للتحقق. الكتابة- أترك هذا كافتراضي:
داخلي. IPsec.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to check to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Updates needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for members. This method only applies to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization, select an authorization method. If you configure this method, you must also configure an Authorization Server.

نوع النفق — اختر الوصول عن بعد. المصادقة—RADIUS. وهذا يوضح مركز الشبكة الخاصة الظاهرية (VPN) الطريقة التي يتم استخدامها لمصادقة المستخدمين. mode config—check mode config. طقطقة يطبق.
4. أتمت هذا steps in order to شملت يتعدد صحة هوية نادل على ال VPN 3000 مركز. بمجرد تعريف المجموعة، قم بتمييز هذه المجموعة، ثم انقر فوق خوادم المصادقة أسفل عمود التعديل. يمكن تعريف خوادم المصادقة الفردية لكل مجموعة حتى إذا لم تكن هذه الخوادم موجودة في الخوادم العمومية.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	ipsecgroup (Internally Configured)	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

أخترت الخادم نوع RADIUS، وأضفت هذا معلم ل Cisco يأمن ACS ل Windows RADIUS نادل. أترك كافة المعلومات الأخرى في حالتها الافتراضية. خادم المصادقة—أدخل عنوان IP الخاص بمصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS. سر الخادم—أدخل سر خادم RADIUS. هذا ينبغي كنت ال نفسه سر يستعمل أنت عندما يشكل أنت ال VPN 3000 مركز في ال Cisco يأمن ACS ل Windows تشكيل. دقت—أعدت الكلمة للتحقق.

5. أخترت تشكيل <نظام> إدارة عنوان <تعيين وفحصت إستعمال عنوان من صحة هوية نادل in order to عينت العنوان إلى ال VPN زبون من ال ip بركة يخلق في ال RADIUS نادل ما إن الزبون يحصل صحة هوية.

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

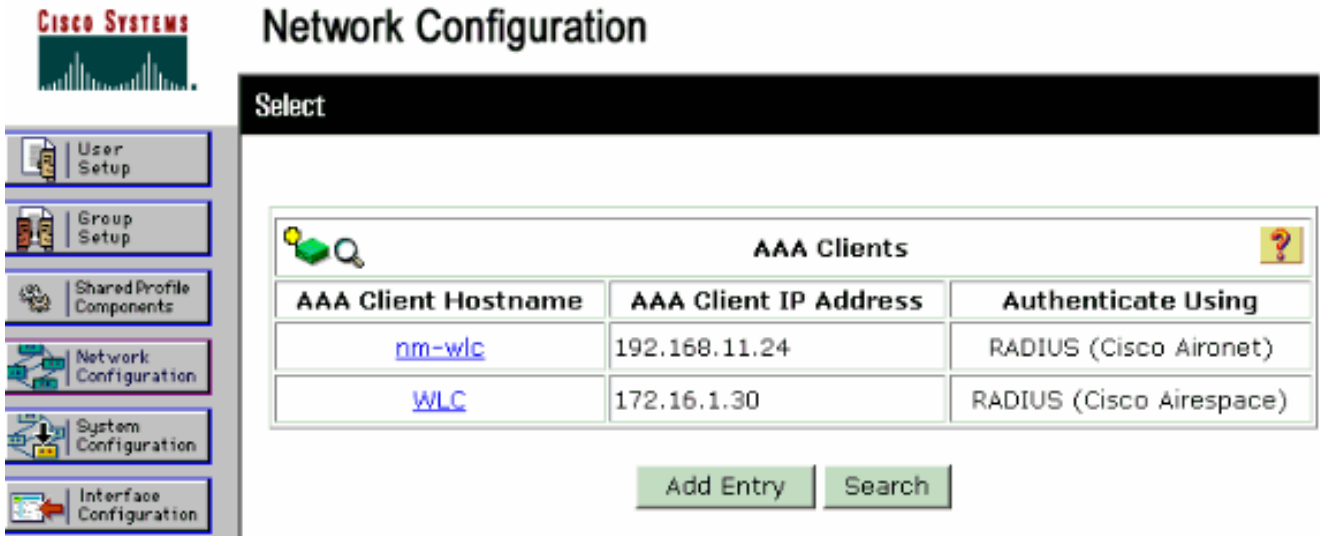
تكوين خادم RADIUS

يصف هذا القسم من المستند الإجراء المطلوب لتكوين ACS الآمن من Cisco كخادم RADIUS لمصادقة مستخدم عميل VPN التي تتم إعادة توجيهها بواسطة مركز سلسلة Cisco VPN 3000 - عميل AAA.

انقر نقرا مزدوجا على رمز **مسؤول ACS** لبدء جلسة عمل الإدارة على الكمبيوتر الشخصي الذي يشغل "مصدر المحتوى الإضافي الآمن من Cisco" لخادم Windows RADIUS. قم بتسجيل الدخول باستخدام اسم المستخدم

وكلمة المرور الملائمين، إذا لزم الأمر.

1. أتمت هذا steps in order أضفت ال VPN 3000 مركز إلى ال cisco بأمن ACS ل Windows نادل تشكيل.أختر تكوين الشبكة وانقر فوق إضافة إدخال لإضافة عميل AAA إلى خادم .RADIUS



The screenshot shows the Cisco Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main content area is titled "Select" and displays a table of AAA Clients.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

Below the table are two buttons: "Add Entry" and "Search".

قم بإضافة هذه المعلمات لمركز VPN 3000 لديك:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Submit Submit + Apply Cancel

اسم مضيف عميل AAA— أدخل اسم المضيف الخاص بمركز VPN 3000 (لدقة DNS). عنوان IP لعميل

AAA—أدخل عنوان IP الخاص بمركز VPN 3000 لديك. المفتاح—أدخل سر خادم RADIUS. يجب أن يكون هذا هو السر نفسه الذي قمت بتكوينه عند إضافة خادم المصادقة على مركز VPN. المصادقة باستخدام—أختر RADIUS (Cisco VPN 3000/ASA/PIX 7.x+). وهذا يسمح ال VSAs VPN 3000 أن يعرض في المجموعة تشكيل نافذة. انقر على إرسال. أخترت قارن تشكيل، طقطقت RADIUS (cisco VPN 3000/ASA/PIX 7.x+), وفحصت مجموعة [26] بائع خاص.

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- | | | |
|--------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/001] Access-Hours |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/002] Simultaneous-Logins |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/005] Primary-DNS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/006] Secondary-DNS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/007] Primary-WINS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/008] Secondary-WINS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/009] SEP-Card-Assignment |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/011] Tunneling-Protocols |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/012] IPSec-Sec-Association |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/013] IPSec-Authentication |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/015] IPSec-Banner1 |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/016] IPSec-Allow-Passwd-Store |

Submit

Cancel

ملاحظة: تشير 'سمة 26 RADIUS' إلى جميع السمات الخاصة بالمورد. على سبيل المثال، أختر تكوين الواجهة < RADIUS (Cisco VPN 3000) وانظر أن كل السمات المتاحة تبدأ مع 026. وهذا يوضح أن جميع هذه السمات الخاصة بالمورد تقع ضمن معيار IETF RADIUS 26. لا تظهر هذه السمات في إعداد المستخدم أو المجموعة بشكل افتراضي. خلقت in order to ظهرت في المجموعة AAA، setup زبون (في هذه الحالة VPN 3000 مركز) أن يصدق مع RADIUS في الشبكة تشكيل. ثم تحقق من السمات التي تحتاج إلى الظهور في إعداد المستخدم أو إعداد المجموعة أو كليهما من تكوين الواجهة. ارجع إلى [سمات RADIUS](#) للحصول على مزيد من المعلومات حول السمات المتاحة واستخدامها. انقر على إرسال.

2. أتمت هذا steps in order to أضفت مجموعة إلى ال cisco يأمن ل Windows تشكيل. أختر إعداد المجموعة، ثم حدد واحدة من مجموعات القوالب، على سبيل المثال، المجموعة 1، وانقر إعادة تسمية

Group Setup

Select

Group : 1: Group 1

Users in Group Edit Settings

Rename Group

المجموعة.


قم بتغيير الاسم إلى شيء مناسب لمؤسستك. على سبيل المثال، IPSECGROUP. بما أن المستخدمين تتم إضافتهم إلى هذه المجموعات، أ جعل اسم المجموعة يعكس الغرض الفعلي لهذه المجموعة. إذا تم وضع جميع المستخدمين في نفس المجموعة، فيمكنك تسميتها مجموعة مستخدمي VPN. انقر فوق تحرير الإعدادات لتحرير المعلومات في مجموعتك التي تمت إعادة تسميتها

Group Setup


Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed
 Dialup client specifies callback number
 Use Windows Database callback settings (where possible)

طقطقة

حديثاً.

ت Cisco VPN 3000 RADIUS وشكلت هذا شعار يوصي. وهذا يسمح للمستخدمين المعينين لهذه المجموعة بإرث سمات RADIUS ل Cisco VPN 3000، والتي تتيح لك تمرکز السياسات لجميع المستخدمين في Cisco Secure ACS

Group Setup

Jump To

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

ملأ .Windows

حظة: من الناحية الفنية، لا يلزم تكوين سمات VPN 3000 RADIUS طالما تم إعداد مجموعة النفق في الخطوة 3 من تكوين مركز [VPN 3000 Series](#) ولا تتغير المجموعة الأساسية في مركز VPN من الإعدادات الافتراضية الأصلية. سمات VPN 3000 **الموصى بها: Primary-DNS**— أدخل عنوان IP الخاص بخادم DNS الأساسي. **DNS الثانوي**— أدخل عنوان IP الخاص بخادم DNS الثانوي الخاص بك. **Primary-WINS**— أدخل عنوان IP الخاص بخادم WINS الأساسي. **WINS الثانوي**— أدخل عنوان IP الخاص بخادم WINS الثانوي. **بروتوكولات الاتصال النفقي**— اختر **IPsec**. وهذا يسمح باتصالات عميل IPsec فقط. غير مسموح بـ PPTP أو L2TP. **اقتران IPsec-sec**— أدخل **ESP-3DES-MD5**. وهذا يضمن اتصال جميع عملاء IPsec بأعلى تشفير متاح. **IPsec-allow-password-store**— اختر **عدم السماح** بحيث لا يسمح للمستخدمين بحفظ كلمة المرور الخاصة بهم في عميل VPN. **شعار IPsec**— أدخل شعار رسالة ترحيب ليتم تقديمه إلى المستخدم عند الاتصال. على سبيل المثال، "مرحبا بك في الوصول إلى الشبكة الخاصة الظاهرية (VPN) الخاصة بموظف شركتي!" **المجال الافتراضي ل IPsec**— أدخل اسم مجال شركتك. على سبيل المثال، "mycompany.com". هذه المجموعة من السمات غير ضرورية. غير أن إن يكون أنت غير متأكد إن القاعدة مجموعة يتغير شعار من ال VPN 3000 مركز، بعد ذلك cisco يوصي أن أنت تشكل هذا شعار: **عمليات تسجيل الدخول المتزامنة**— أدخل عدد المرات التي تسمح فيها للمستخدم بتسجيل الدخول في الوقت نفسه باسم المستخدم نفسه. التوصية هي 1 أو 2. **SEP-Card-Assign**— اختر **Any-SEP**— اختر

ON.IPsec عبر UDP— أختار إيقاف التشغيل، إلا إذا كنت تريد اتصال المستخدمين في هذه المجموعة باستخدام IPsec عبر بروتوكول UDP. إذا قمت بتحديد "تشغيل"، سيظل لعميل شبكة VPN القدرة على تعطيل IPsec محليا عبر بروتوكول UDP والاتصال بشكل طبيعي. IPsec عبر منفذ UDP—حدد رقم منفذ UDP في النطاق من 4001 إلى 49151. يتم استخدام هذا فقط إذا كان IPsec عبر UDP قيد التشغيل. تتطلب المجموعة التالية من الخصائص أن تقوم بضبط شيء ما على مركز VPN أولا قبل أن تتمكن من استخدامها. يوصى بذلك للمستخدمين المتقدمين فقط. ساعات الوصول— يتطلب ذلك إعداد نطاق من ساعات الوصول على مركز VPN 3000 ضمن التكوين < إدارة السياسة. بدلا من ذلك، استخدم "ساعات الوصول" المتوفرة في "مصدر المحتوى الإضافي الآمن من Cisco" ل Windows لإدارة هذه السمة. IPsec-split-tunnel-list— يتطلب هذا إعداد قائمة شبكة على مركز VPN تحت التكوين < إدارة السياسة < إدارة حركة مرور البيانات. هذه قائمة بالشبكات التي تم إرسالها إلى العميل والتي تخبر العميل بتشفير البيانات إلى تلك الشبكات الموجودة في القائمة فقط. أختار تعيين IP في إعداد المجموعة وفحص التعيين من تجمع خوادم AAA لتعيين عناوين IP لمستخدمي عميل VPN بمجرد أن تتم

Group Setup

Jump To IP Address Assignment

IP Assignment

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

Assigned from AAA server pool

Available Pools

Selected Pools

pool1

->

<-

Up Down


أختار

مصادقتهم.

نظام تشكيل < IP بركة in order to خلقت IP بركة ل VPN زبون مستعمل وطققة يرسل

System Configuration

Edit

New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

Submit

Cancel

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

< اختر إرسال

إعادة التشغيل لحفظ التكوين وتنشيط المجموعة الجديدة. كرر هذه الخطوات لإضافة المزيد من المجموعات.
3. تكوين المستخدمين على مصدر المحتوى الإضافي الآمن من Cisco ل Windows. اختر إعداد المستخدم،
وأدخل اسم مستخدم، وانقر فوق

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

List all users

Remove Dynamic Users

أقم بتكوين

إضافة/تحرير.
هذه المعلومات ضمن قسم إعداد
المستخدم:

User Setup

User: ipsecuser1 (New User)

 Account Disabled

Supplementary User Info

Real Name	<input type="text" value="user1"/>
Description	<input type="text" value="user1"/>

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

مصادقة كلمة المرور— اختر قاعدة بيانات ACS الداخلية. يدخل PAP الآمن من Cisco كلمة مرور للمستخدم. Cisco Secure PAP - تأكيد كلمة المرور- أعد إدخال كلمة المرور للمستخدم الجديد. المجموعة التي يتم تعيين المستخدم لها- حدد اسم المجموعة التي قمت بإنشائها في الخطوة السابقة. انقر فوق إرسال لحفظ إعدادات المستخدم وتنشيطها. كرر هذه الخطوات لإضافة مستخدمين إضافيين.

[عينت عنوان ساكن إستاتيكي إلى ال VPN زبون مستعمل](#)

أكمل الخطوات التالية:

1. إنشاء IPsecgrp جديد لمجموعة VPN.
2. قم بإنشاء مستخدم يرصد تلقي IP الثابت واختر IPSECGRP. اخترت يعين عنوان ساكن إستاتيكي مع العنوان ساكن إستاتيكي أن يكون عينت تحت الزبون عنوان

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm

Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Submit

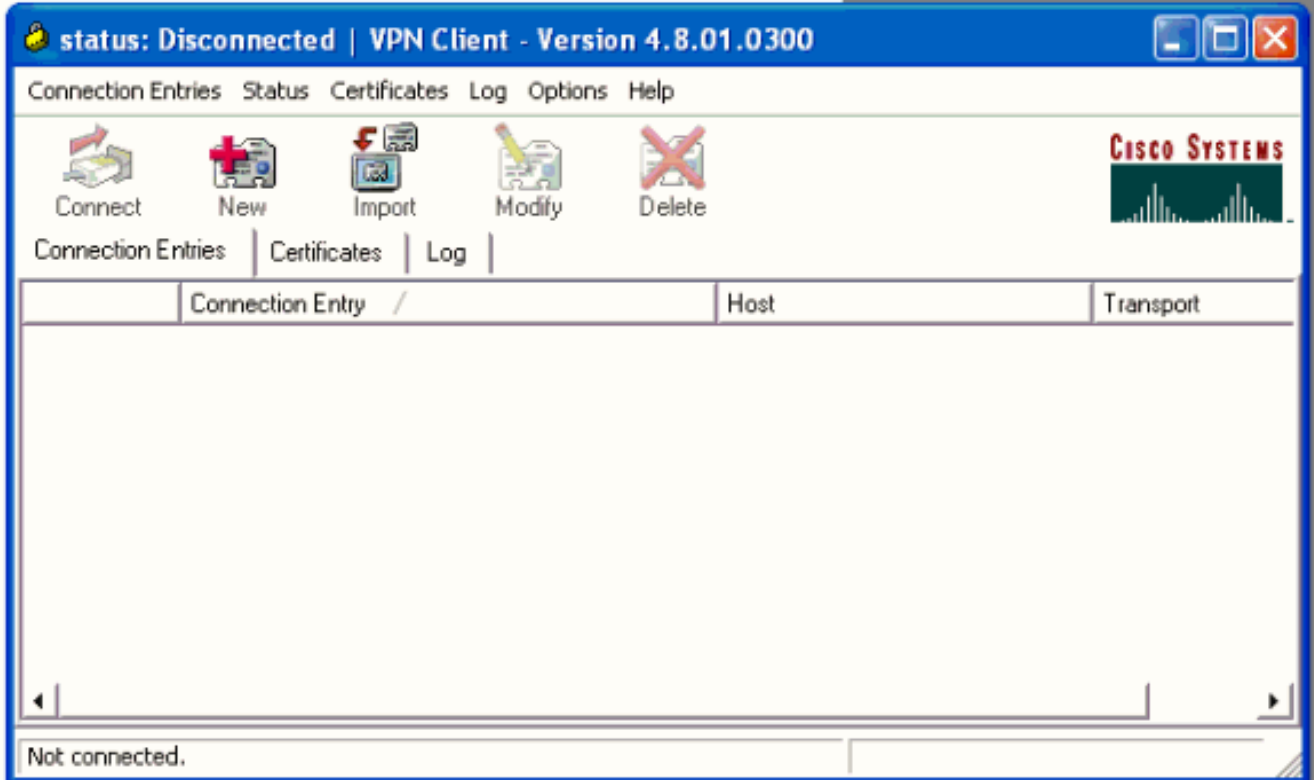
Delete

Cancel

تازل.

يصف هذا القسم تكوين جانب عميل شبكة VPN.

1. اخترت بداية برنامج Cisco Systems VPN زبون VPN زبون.
2. طقطقت جديد in order to أطلقت ال create جديد VPN توصيل مدخل نافذة.



3. عند مطالبتك، قم بتعيين اسم لإدخالك. يمكنك أيضا إدخال وصف إذا كنت تريد. عينت ال VPN 3000 مركز قارن عام عنوان في المضيف عمود واخترت مجموعة صحة هوية . ثم قم بتوفير اسم المجموعة وكلمة المرور. طقطقت حفظ in order to أتمت الجديد VPN توصيل

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [Dropdown]

Send CA Certificate Chain

Erase User Password | Save | Cancel

ملاحظ

مدخل.

ة: تأكد من تكوين عميل VPN لاستخدام نفس اسم المجموعة وكلمة المرور التي تم تكوينها في مركز VPN Cisco 3000 Series.

إضافة محاسبة

بعد عمل المصادقة، يمكنك إضافة عملية محاسبة.

1. على الـ VPN 3000، اخترت تشكيل <نظام> <خادم> <حساب نادل، وأضفت الـ cisco يأمن ACS لـ Windows نادل.
2. يمكنك إضافة خوادم محاسبة فردية إلى كل مجموعة عندما تختار تكوين <إدارة المستخدم > مجموعات، يبرز مجموعة وانقر فوق تعديل الوصول. الخوادم. ثم أدخل عنوان IP الخاص بخادم المحاسبة مع سر الخادم.

Configure and add a RADIUS user accounting server.

Accounting Server Enter IP address or hostname.

Server Port Enter the server UDP port number.

Timeout Enter the timeout for this server (se

Retries Enter the number of retries for this

Server Secret Enter the RADIUS server secret.

Verify Re-enter the server secret.

في مصدر المحتوى الإضافي الآمن من Cisco لـ Windows، تظهر سجلات المحاسبة كما يوضح هذا الإخراج:

Select

RADIUS Accounting active.csv

Regular Expression

Start Date & Time End Date & Time Rows per Page

Filtering is not applied.

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
10/27/2006	18:38:20	ipseccuser1	ipseccgroup	192.168.1.2	Start	E8700001	..	Framed	PPP
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off

[التحقق من الصحة](#)

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر `show`. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر `show`.

[التحقق من مركز VPN](#)

على جانب مركز الشبكة الخاصة الظاهرية (VPN) 3000، اختر إدارة < إدارة جلسات العمل للتحقق من إنشاء نفق VPN البعيد.

Remote Access Sessions

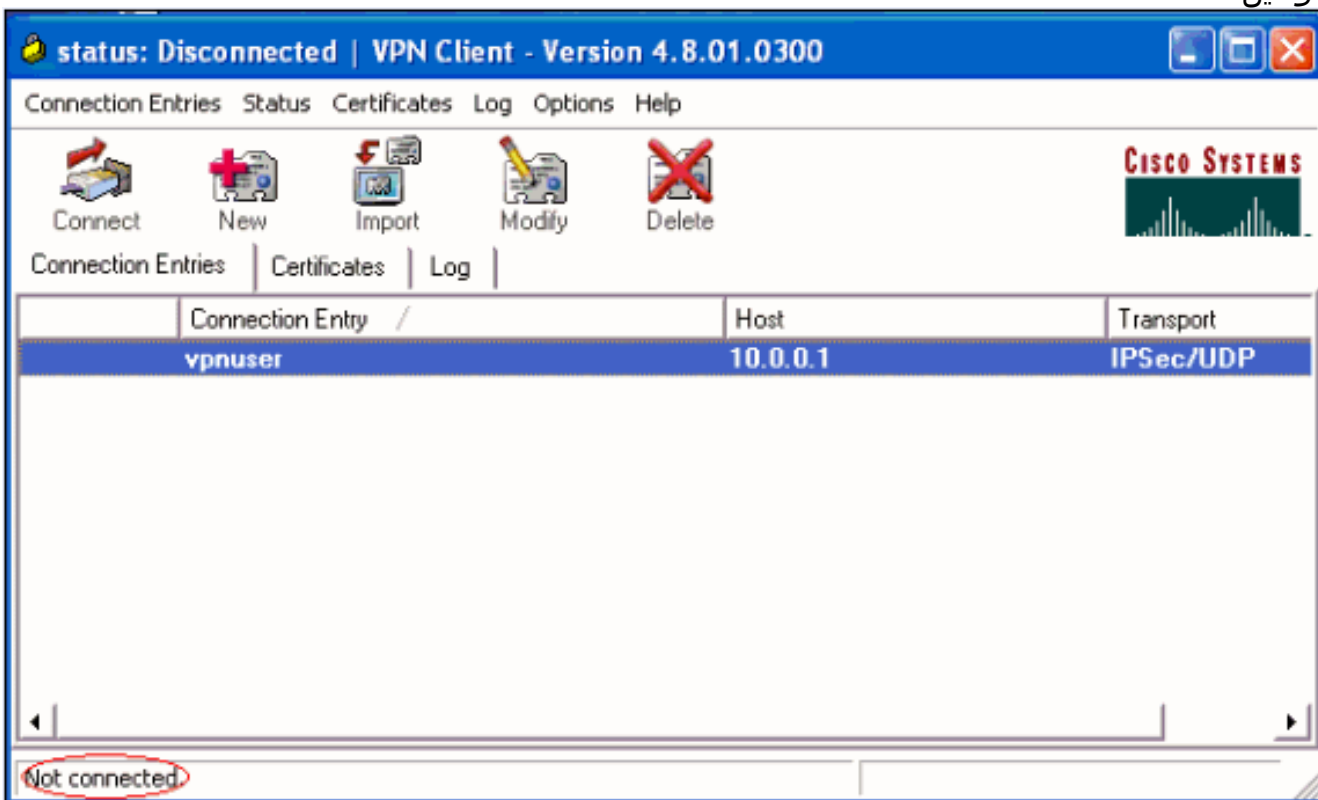
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

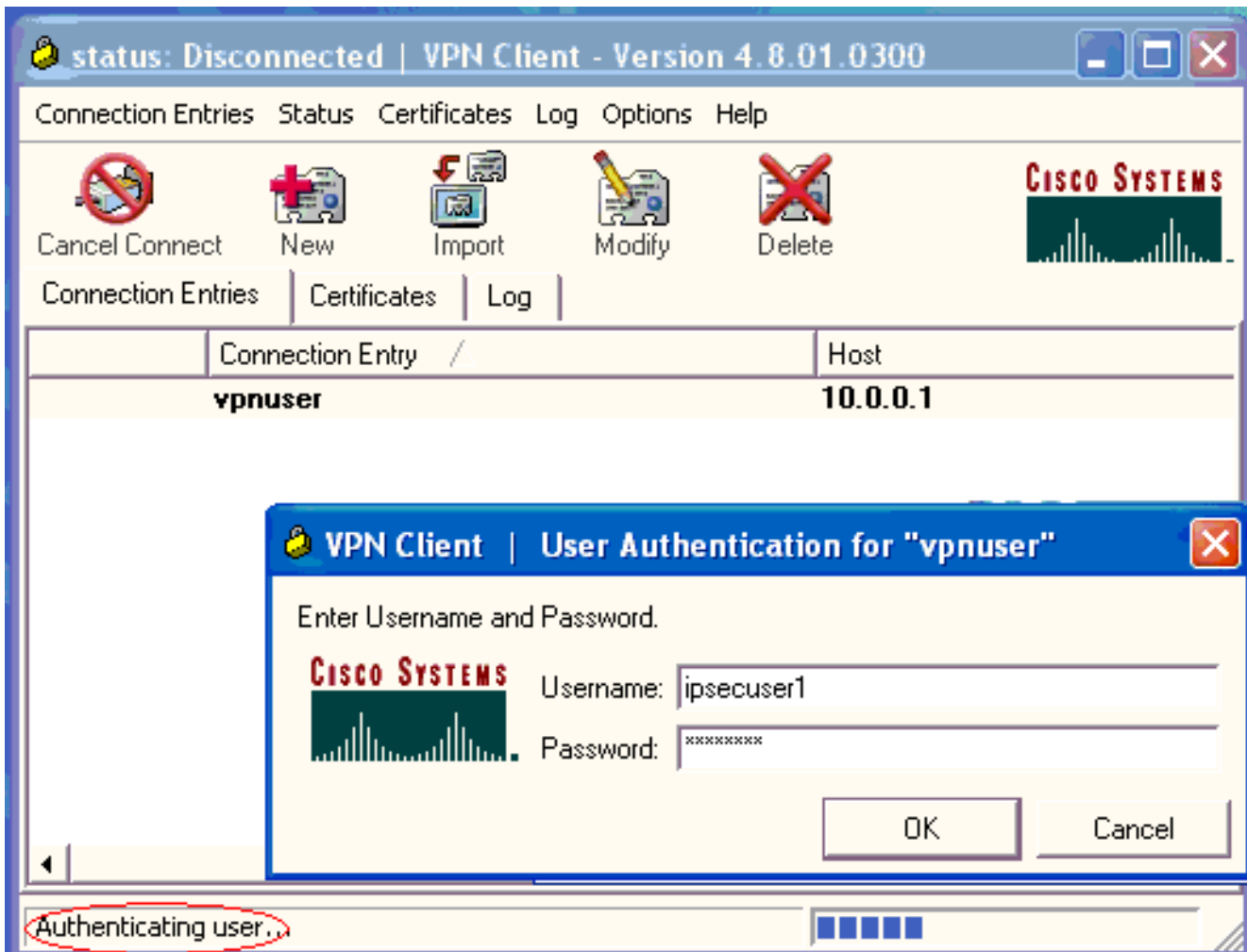
[التحقق من عميل شبكة VPN](#)

أتمت هذا steps in order to دقت ال VPN عميل.

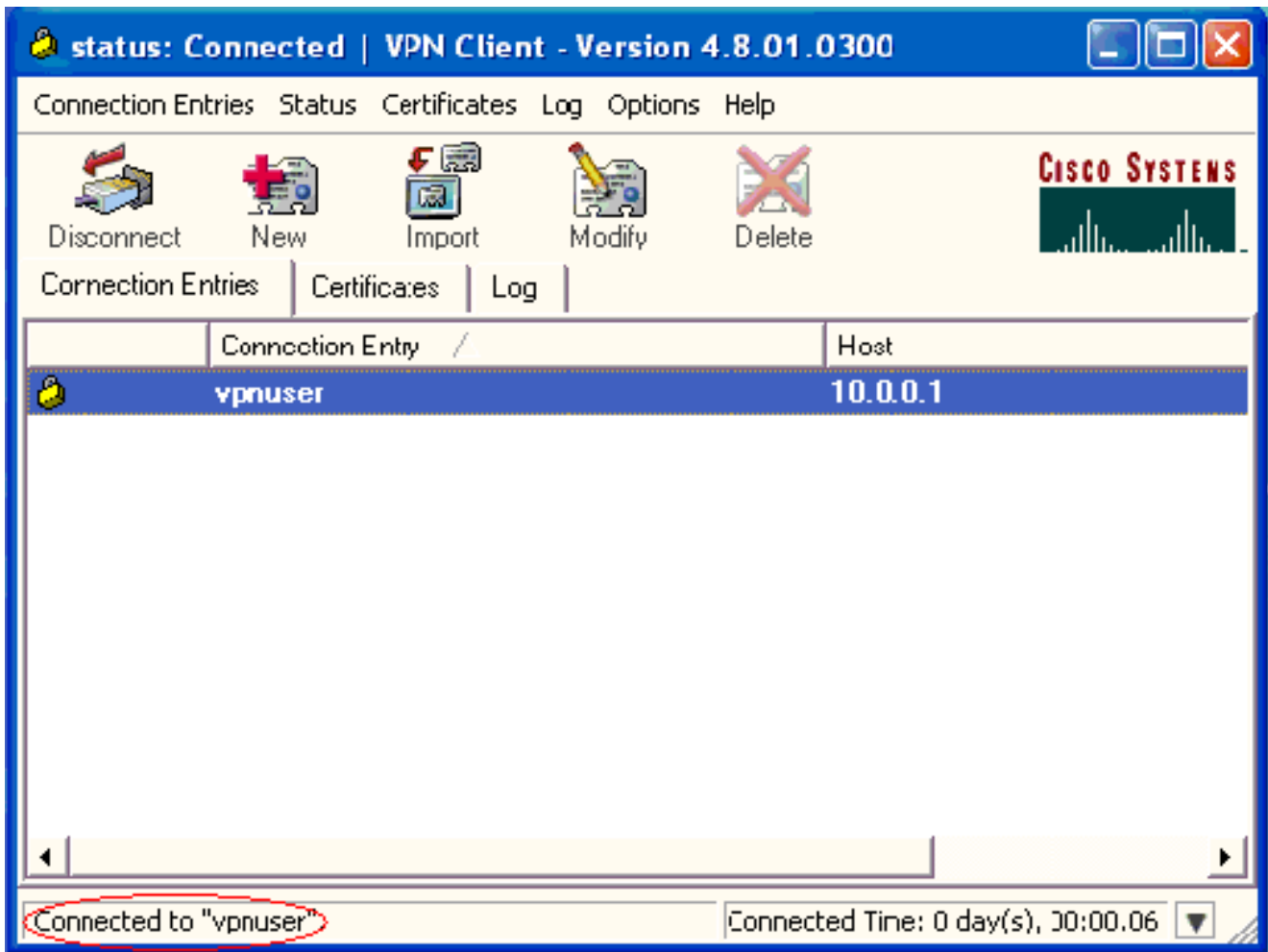
1. طقطقة [يربط](#) in order to بدأت VPN توصيل.



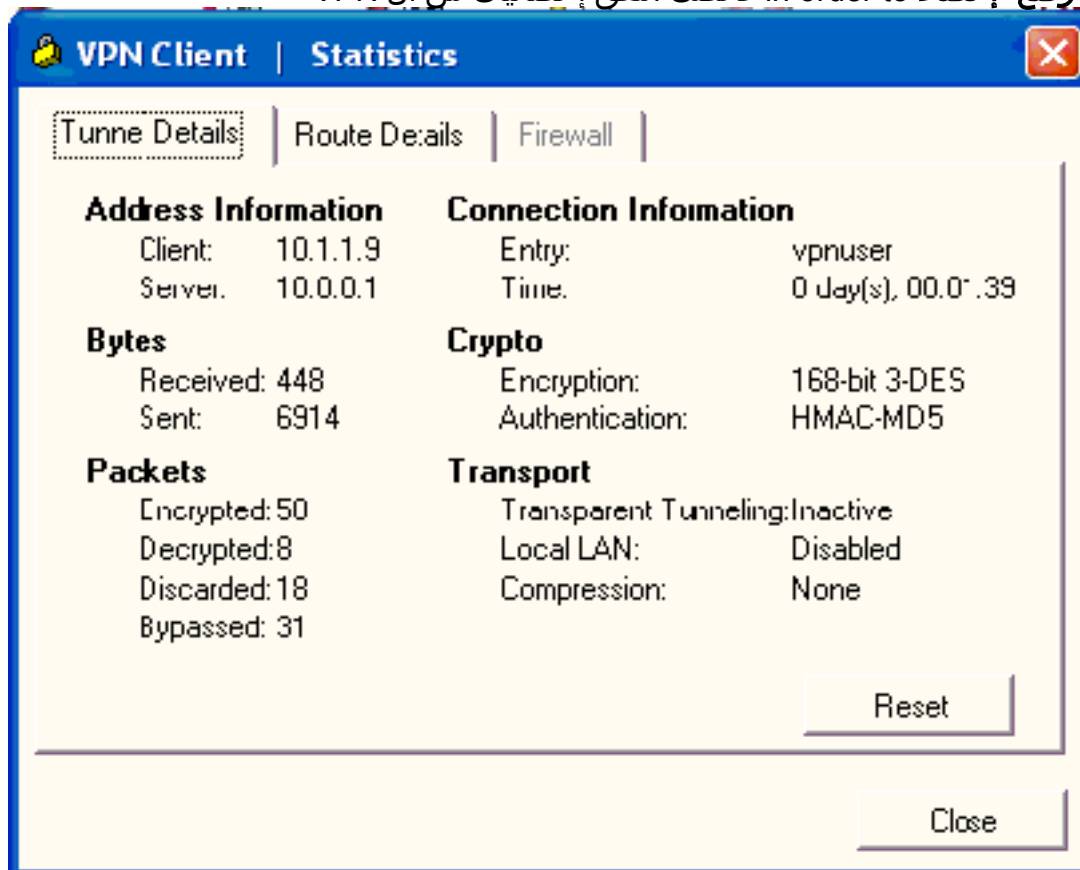
2. يظهر هذا نافذة لمصادقة المستخدم. أدخل اسم مستخدم وكلمة مرور صحيحين لإنشاء اتصال VPN.



3. يتم توصيل عميل الشبكة الخاصة الظاهرية (VPN) بمركز الشبكة الخاصة الظاهرية (VPN) 3000 في الموقع المركزي.



4. آخرت وضع إحصاء in order to فحصت النفق إحصائيات من ال VPN



زيون.

استكشاف الأخطاء وإصلاحها

أتمت هذا steps in order to تحرير تشكيلك.

1. أخترت تشكيل <نظام> نادل <صحة هوية> وأتمت هذا steps in order to اختبرت الموصولية بين ال RADIUS نادل و VPN 3000 مركز. حدد الخادم، ثم انقر فوق إختبار.

Configuration | System | Servers | Authentication

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

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct 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

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) 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"/>


أدخل اسم مستخدم وكلمة مرور RADIUS وانقر على موافق.

Configuration | System | Servers | Authentication | Test

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

Username
Password

Success

 Authentication Successful

تظهر مصادقة ناجحة.

2. إن يفشل هو، هناك إما مشكلة تشكيل أو ip موصولية إصدار. تحقق من "سجل المحاولات الفاشلة" الموجود

على خادم ACS بحثًا عن الرسائل المتعلقة بهذا الفشل. إذا لم تظهر أي رسائل في هذا السجل، فمن المحتمل أن تكون هناك مشكلة في اتصال IP. لا يصل طلب RADIUS إلى خادم RADIUS. تحقق من المرشحات المطبقة على واجهة مركز VPN 3000 المناسبة التي تسمح لحزم (1645) RADIUS بالدخول والخروج. إذا كانت مصادقة الاختبار ناجحة، وتستمر عمليات التسجيل في الدخول إلى مركز VPN 3000 في الفشل، فتتحقق من سجل الأحداث القابل للتصفية عبر منفذ وحدة التحكم. إذا لم تعمل الاتصالات، فيمكنك إضافة فئات أحداث AUTH و IKE و IPsec إلى مركز VPN عند تحديد التكوين < النظام < الأحداث < الفئات < التعديل (الخطورة إلى السجل=1-9، الخطورة إلى وحدة التحكم=1-3). كما تتوفر AUTHDBG و AUTHDBG و AUTHDECODE و iKEDBG و iKedecode و IPSECDBG و IPSECDECODE، ولكنها يمكن أن توفر معلومات كثيرة جدًا. إذا كانت هناك حاجة إلى معلومات تفصيلية حول السمات التي يتم تمريرها من خادم RADIUS، فإن AUTHDECODE و iKedecode و IPSECDECODE توفر هذا عند مستوى مستوى مستوى مستوى مستوى الخطورة إلى سجل=1-13.

3. قم باسترداد سجل الأحداث من المراقبة < سجل الأحداث.

Monitoring | Live Event Log

```

1513 10/27/2006 18:37:25.330 SEV=8 IKEDBG/81 RPT=47 192.168.1.2
SENDING Message (msgid=6679165e) with payloads :
HDR + HASH (8) + NOTIFY (11)
total length : 80

1515 10/27/2006 18:37:35.830 SEV=8 IKEDBG/81 RPT=48 192.168.1.2
RECEIVED Message (msgid=8575be96) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0)
total length : 80

1517 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=120 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
processing hash

1518 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=121 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Processing Notify payload

1519 10/27/2006 18:37:35.830 SEV=9 IKEDBG/36 RPT=10 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x653e486d)

1521 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=122 192.168.1.2

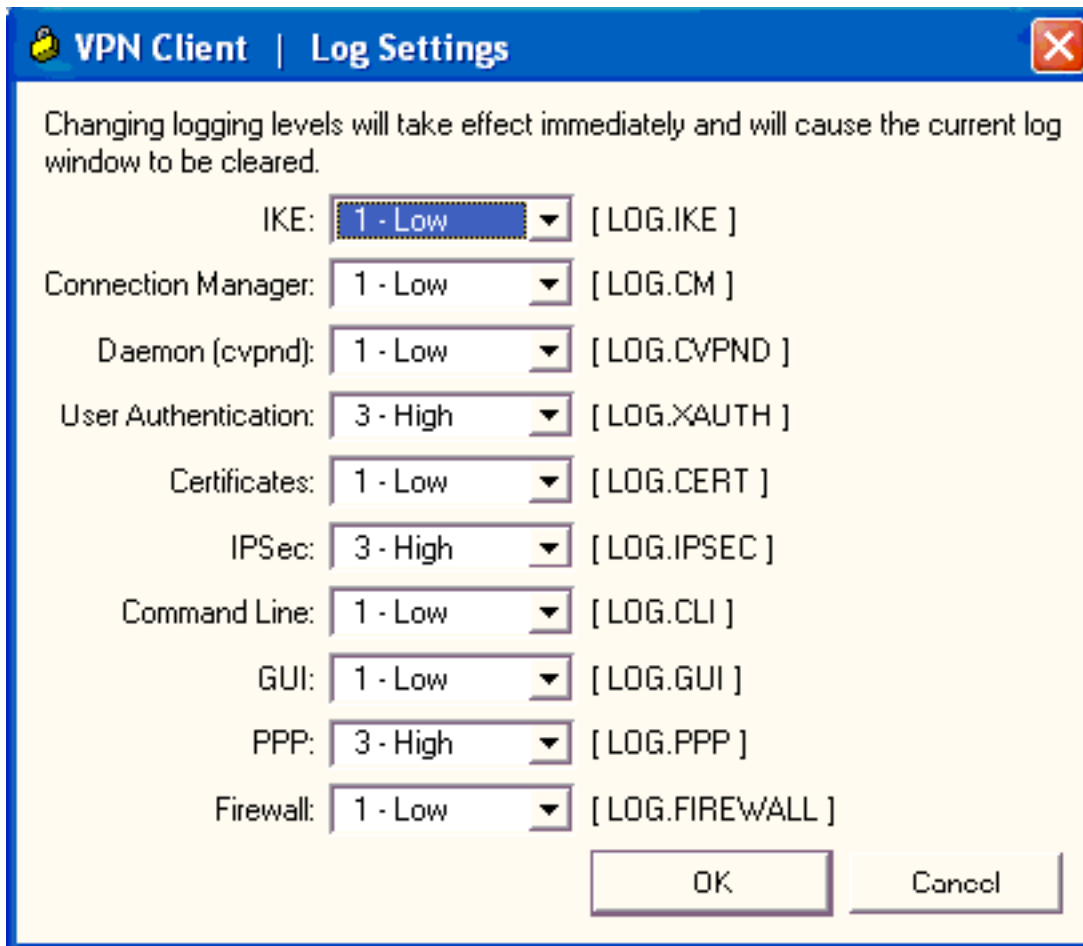
```

Pause Display Clear Display Restart Receiving.....

[أستكشاف أخطاء VPN Client 4.8 وإصلاحها ل Windows](#)

أتمت هذا steps in order to تحريت VPN زبون 4.8 ل Windows.

1. اخترت سجل < سجل عملية إعداد in order to مكنت السجل مستوى في ال VPN



زبون.
2. آخرت سجل < سجل نافذة in order to شاهدت ال log مدخل في ال VPN
زبون.

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

[معلومات ذات صلة](#)

- [صفحة دعم مركز Cisco VPN 3000 Series](#)
- [صفحة دعم عميل شبكة VPN من Cisco](#)
- [مفاوضة IPsec/بروتوكولات IKE](#)
- [مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows](#)
- [تكوين المرشحات الديناميكية على خادم RADIUS](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل