

# دليل VPN عالم عمل يقي فنلندا لاصت الالميسقت VPN 3000 زكرم نيوكت لالم

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [تكوين الاتصال النفقي المنقسم على مركز VPN](#)
- [التحقق من الصحة](#)
- [الاتصال بعميل شبكة VPN](#)
- [عرض سجل عميل شبكة VPN](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح لعملاء الشبكة الخاصة الظاهرية (VPN) بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في مركز تجميع الشبكة الخاصة الظاهرية (VPN) من السلسلة 3000. يتيح هذا التكوين لعملاء الشبكات الخاصة الظاهرية (VPN) إمكانية الوصول الآمن إلى موارد الشركة عبر IPsec أثناء منح وصول غير آمن إلى الإنترنت.

**ملاحظة:** قد يشكل تقسيم الاتصال النفقي خطرا على الأمان عند تكوينه. نظرا لأن عملاء الشبكة الخاصة الظاهرية (VPN) لديهم وصول غير آمن إلى الإنترنت، يمكن اختراق هذه الشبكات بواسطة المهاجم. وقد يتمكن هذا المهاجم بعد ذلك من الوصول إلى شبكة LAN الخاصة بالشركة عبر نفق IPsec. يمكن أن يكون هناك حل وسط بين الاتصال النفقي الكامل والنفقي المنقسم للسماح بوصول عملاء VPN للشبكة المحلية الظاهرية (LAN) فقط. راجع [السماح بالوصول إلى شبكة LAN المحلية لعملاء VPN على مثال تكوين مركز VPN 3000](#) للحصول على مزيد من المعلومات.

## المتطلبات الأساسية

### المتطلبات

يفترض هذا المستند أن تكوين شبكة VPN للوصول عن بعد يعمل موجود بالفعل على مركز الشبكة الخاصة الظاهرية (VPN). ارجع إلى [IPsec مع عميل VPN على مثال تكوين مركز VPN 3000](#) إذا لم يتم تكوين واحد بالفعل.

### المكونات المستخدمة

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

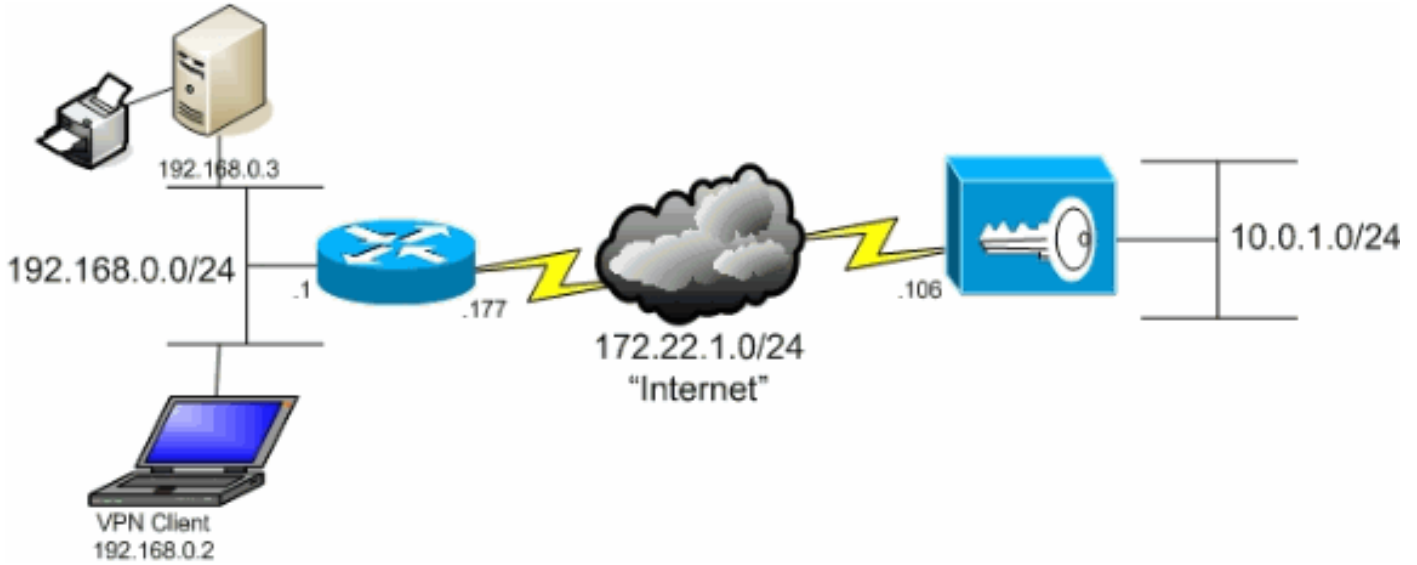
• برنامج Cisco VPN 3000 Concentrator Series، الإصدار H.4.7.2

• Cisco VPN Client، الإصدار 4.0.5

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.

## الرسم التخطيطي للشبكة

يتواجد عميل شبكة VPN على شبكة SOHO نموذجية ويتصل عبر الإنترنت بالمكتب الرئيسي.



## الاصطلاحات

راجع اصطلاحات تلمحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

## معلومات أساسية

في سيناريو عميل شبكة VPN الأساسية إلى مركز شبكة VPN، يتم تشفير جميع حركات مرور البيانات من عميل شبكة VPN وإرسالها إلى مركز الشبكة الخاصة الظاهرية (VPN) بغض النظر عن الوجهة. استناداً إلى التكوين الخاص بك وعدد المستخدمين المدعومين، يمكن أن تصبح عملية إعداد كهذه ذات نطاق ترددي كبير. يمكن أن تعمل ميزة تقسيم الاتصال النفقي على تخفيف هذه المشكلة من خلال السماح للمستخدمين بإرسال حركة المرور الموجهة فقط إلى شبكة الشركة عبر النفق. يتم إرسال جميع حركات المرور الأخرى مثل المراسلة الفورية أو البريد الإلكتروني أو الاستعراض العرضي إلى الإنترنت عبر الشبكة المحلية (LAN) لعميل الشبكة الخاصة الظاهرية (VPN).

## تكوين الاتصال النفقي المنقسم على مركز VPN

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة. قم أولاً بإنشاء قائمة شبكات. تقوم هذه القائمة بتعريف الشبكات الوجهة التي يرسل إليها عميل VPN حركة مرور مشفرة. بمجرد إنشاء القائمة، أضف القائمة إلى نهج تقسيم الاتصال النفقي الخاص بمجموعة النفق العميل.

1. أخترت تشكيل <إدارة سياسة> حركة مرور إدارة <شبكة قائمة وطققة يضيف.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists

Save Needed

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

CISCO SYSTEMS

2. تقوم هذه القائمة بتعريف الشبكات الوجهة التي يرسل إليها عميل VPN حركة مرور مشفرة. قم بإدخال هذه الشبكات يدويا، أو انقر فوق **إنشاء قائمة محلية** لإنشاء قائمة تستند إلى إدخلات التوجيه على الواجهة الخاصة لمركز VPN. في هذا المثال، تم إنشاء القائمة تلقائيا.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Network List

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/w.w.w.w** (e.g. 10.10.0.0/0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.mmm addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

CISCO SYSTEMS

3. بمجرد أن يتم إنشائها أو تعيبتها، قم بتوفير اسم للقائمة وانقر إضافة.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name:

Network List:

Buttons: Add, Cancel, Generate Local List

Notes:

- Name of the Network List you are adding. The name must be unique.
- Enter the Networks and Wildcard masks using the following format **n.n.n.n/w.n.n.n** (e.g. 10.10.0.0/0.255.255).
- Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

4. بمجرد إنشاء قائمة الشبكة، قم بتعيينها على مجموعة نفق. أختَر تكوين < إدارة المستخدم > مجموعات، وحدد المجموعة التي تريد تغييرها، وانقر فوق تعديل المجموعة.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups

Save Needed

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 modify other group parameters, select a group and click the appropriate button.

Actions: Add Group, Modify Group, Delete Group

Current Groups: ipsecgroup (Internally Configured)

Modify: Authentication Servers, Authorization Servers, Accounting Servers, Address Pools, Client Update, Bandwidth Assignment, WebVPN Servers and URLs, WebVPN Port Forwarding

5. انتقل إلى علامة التبويب تكوين العميل الخاصة بالمجموعة التي أختَر تعديلها.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

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 | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

### Client Configuration Parameters

Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> <li>Select a method to use or disable backup servers.</li> <li>Enter up to 10 IPsec backup server addresses/names starting from high priority to low.</li> <li>Enter each IPsec backup server address/name on a single line.</li> </ul>

6. قم بالتمرير لأسفل إلى مقاطع "سياسة تقسيم الاتصال النفقي" و"قائمة تقسيم الاتصال النفقي للشبكة" وانقر فوق شبكات النفق فقط في القائمة.

7. أختار القائمة التي تم إنشاؤها مسبقا من القائمة المنسدلة. في هذه الحالة يكون المكتب الرئيسي. خانة الاختيار Inherit؟ يتم إفراغ خانة الاختيار تلقائيا في كلتا الحالتين.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Split Tunneling Policy

Tunnel everything  
 Allow the networks in list to bypass the tunnel  
 Only tunnel networks in the list

Split Tunneling Network List

Main Office

Default Domain Name

Split DNS Names

Apply Cancel

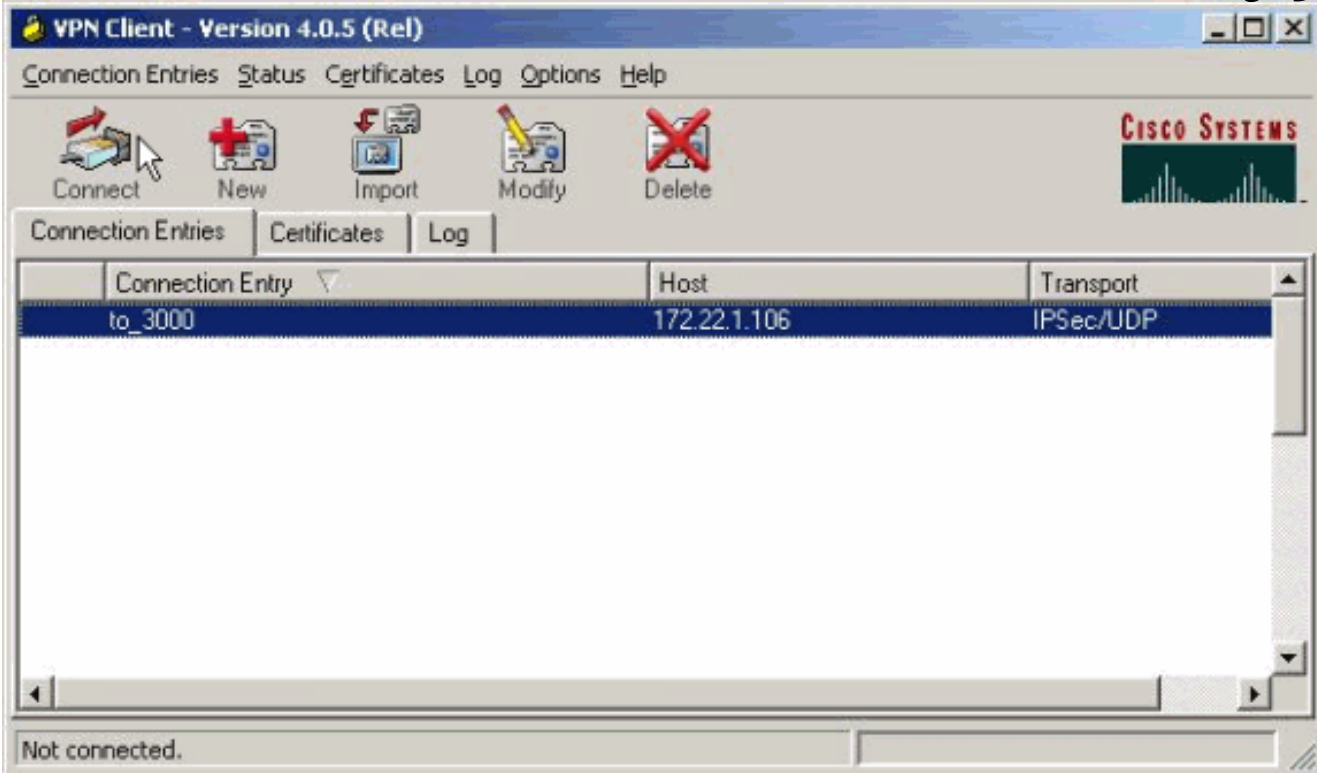
8. انقر فوق تطبيق عند الانتهاء.

[التحقق من الصحة](#)

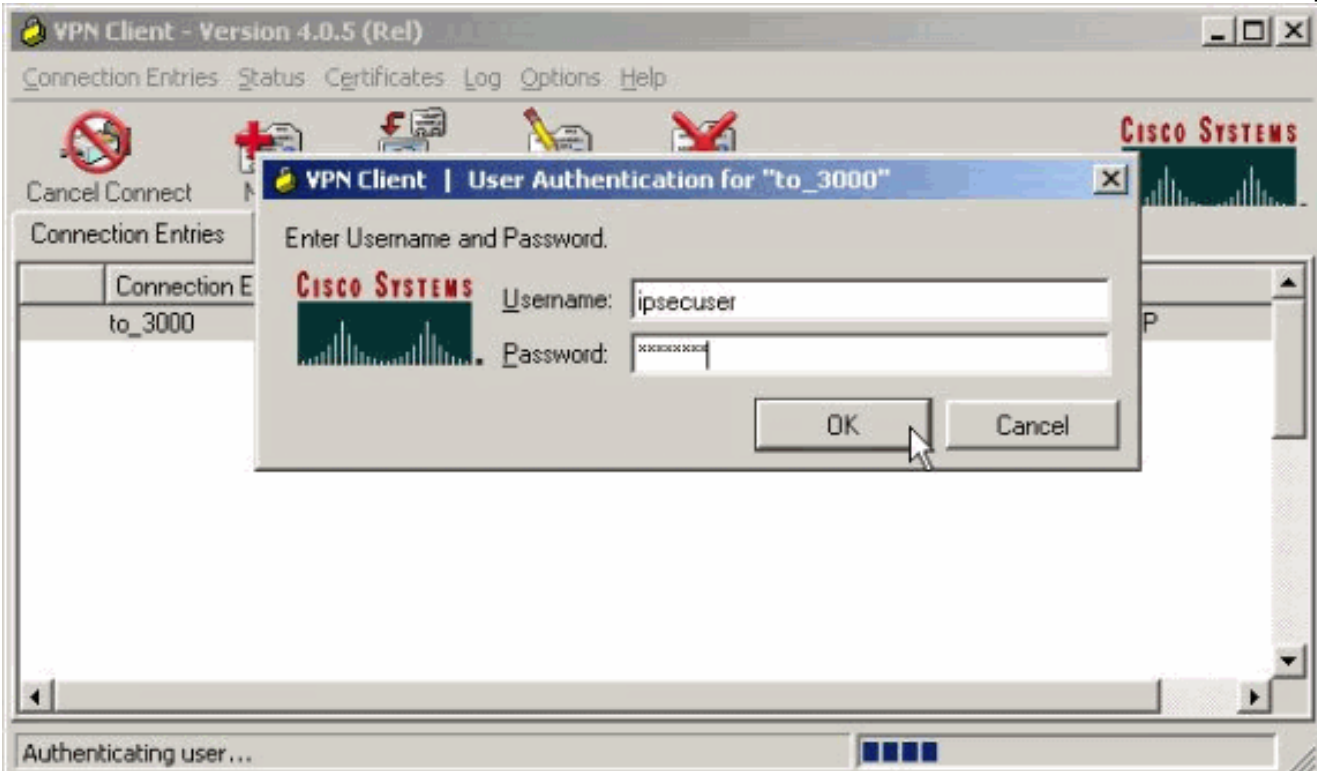
## الاتصال بعمل شبكة VPN

قم بتوصيل عميل الشبكة الخاصة الظاهرية (VPN) بمركز الشبكة الخاصة الظاهرية (VPN) للتحقق من التكوين الخاص بك.

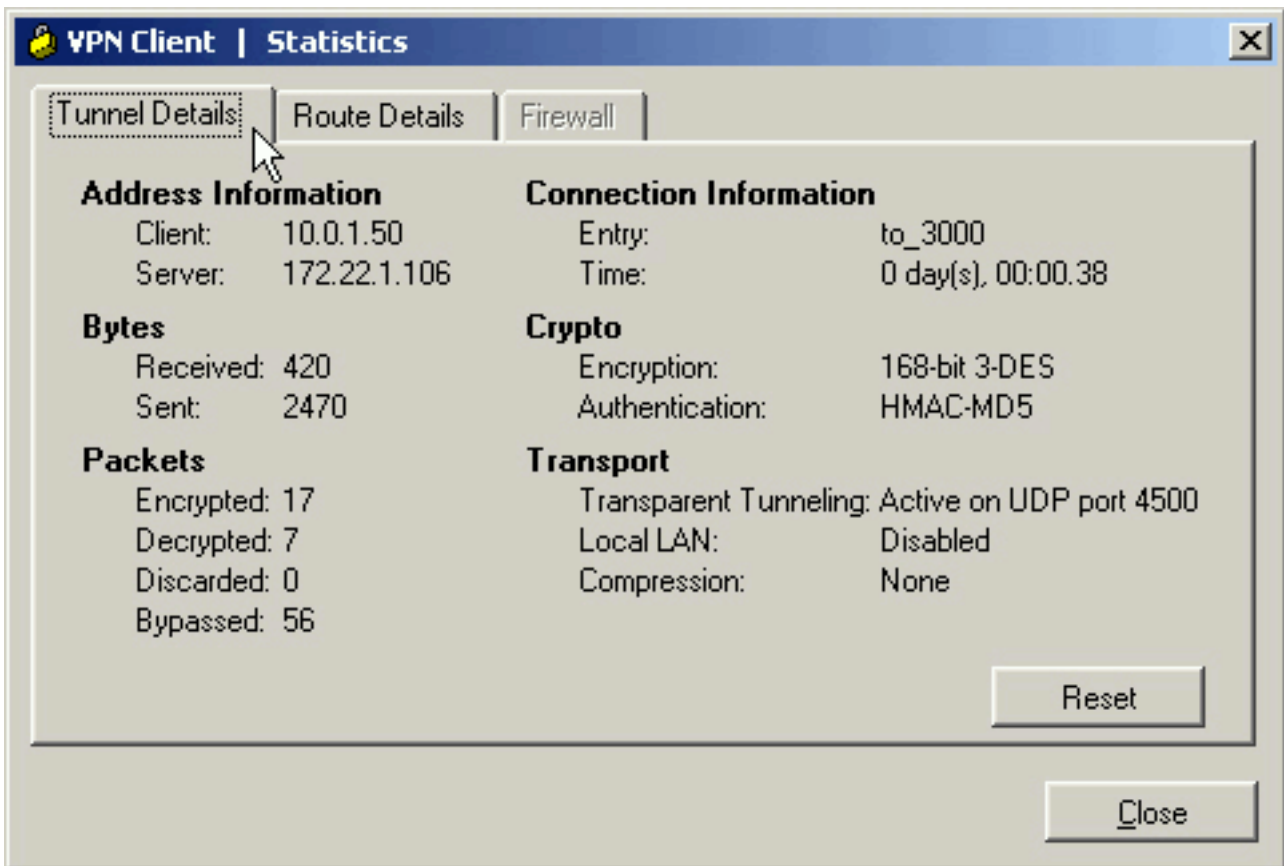
1. أختار إدخال الاتصال الخاص بك من القائمة ثم انقر على **توصيل**.



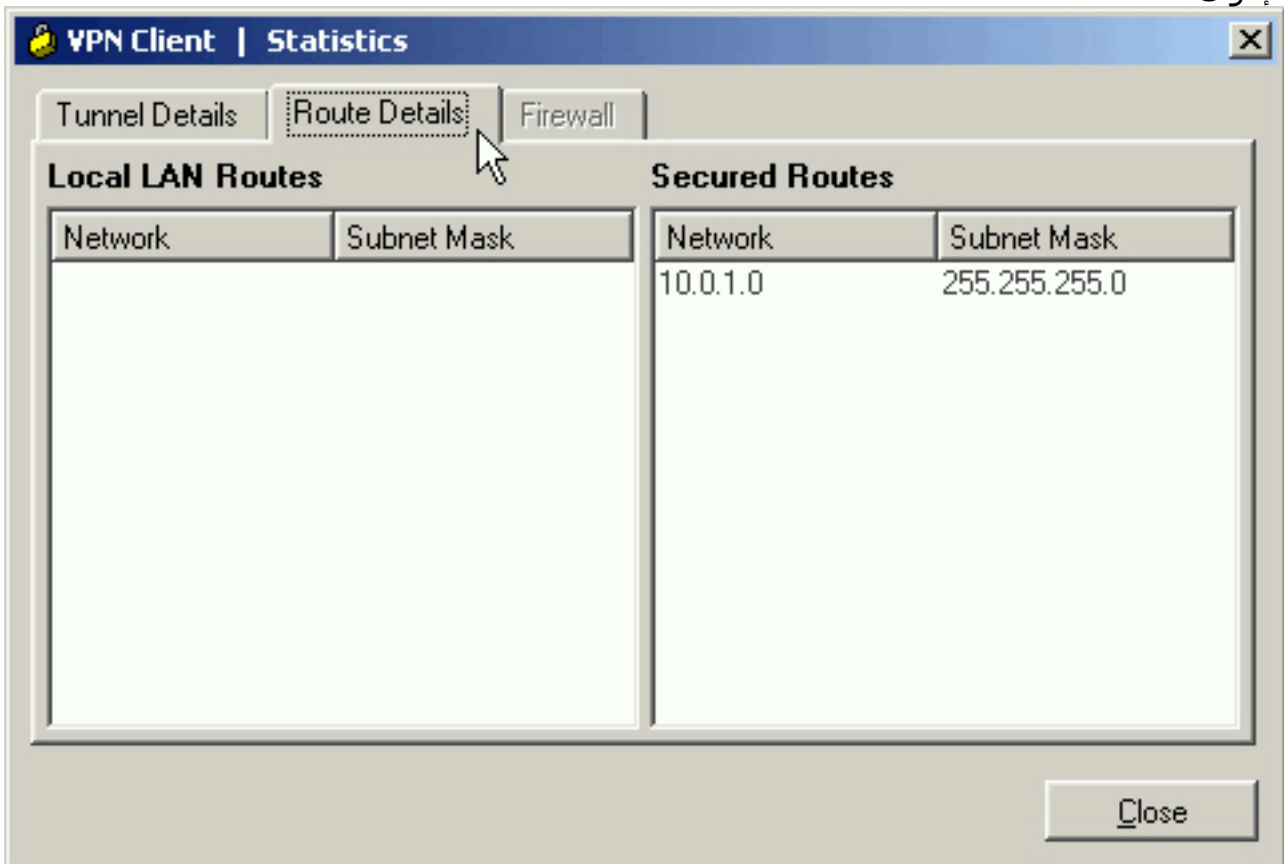
2. أدخل بيانات الاعتماد الخاصة بك.



3. أختار الحالة < الإحصائيات.. لعرض نافذة تفاصيل النفق حيث يمكنك فحص تفاصيل النفق ورؤية تدفق حركة المرور.

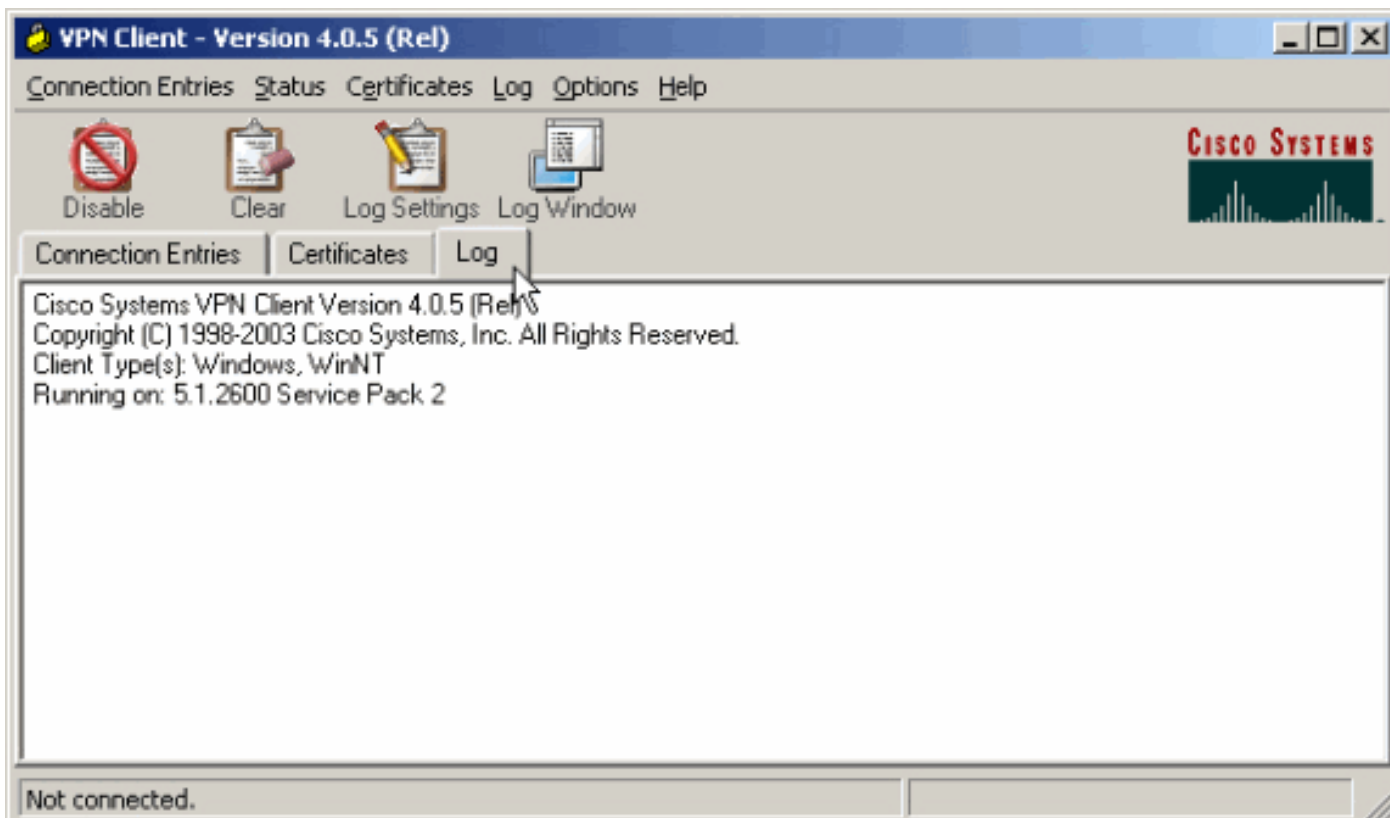


4. انتقل إلى علامة التبويب تفاصيل المسار لمعرفة الشبكات التي يرسل عميل VPN حركة مرور مشفرة إليها. في هذا المثال، يتصل عميل شبكة VPN بشكل آمن مع 24/10.0.1.0 بينما يتم إرسال جميع حركات مرور البيانات الأخرى غير مشفرة إلى الإنترنت.



[عرض سجل عميل شبكة VPN](#)

عندما يفحص أنت ال VPN زبون سجل، أنت يستطيع حددت ما إذا أو لا المعلمة أن يسمح انقسام tunneling ثبتت. انتقل إلى علامة التبويب "سجل" في "عميل VPN" لعرض السجل. انقر فوق إعدادات السجل لضبط ما تم تسجيله. في هذا المثال، يتم تعيين IKE و IPsec على 3- مرتفع بينما يتم تعيين جميع عناصر السجل الأخرى على 1 - منخفض.



(Cisco Systems VPN Client Version 4.0.5 (Rel  
 .Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved  
 Client Type(s): Windows, WinNT  
 Running on: 5.1.2600 Service Pack 2

Sev=Info/6IKE/0x6300003B 07/21/06 14:21:43.106 1  
 .Attempting to establish a connection with 172.22.1.106

*Output is supressed.* 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a ---!  
 firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall  
 Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30  
 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion  
 Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4  
 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.22.1.106 32 14:21:56.114  
 07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114  
 07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
 172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE\_CFG\_REPLY: Attribute =  
 INTERNAL\_IPV4\_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010  
 MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_NETMASK: , value = 255.255.255.0 36 14:21:56.114  
 07/21/06 Sev=Info/5 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: , value =  
 0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5  
 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SPLIT\_INCLUDE (# of split\_nets), value  
 = 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT\_NET #1 subnet = 10.0.1.0  
 mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5  
 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_PFS: , value = 0x00000000 40  
 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE\_CFG\_REPLY: Attribute = APPLICATION\_VERSION,  
 value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29  
 2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute =  
 .Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed



## استكشاف الأخطاء وإصلاحها

ارجع إلى [IPsec مع عميل VPN إلى مثال تكوين مركز VPN 3000 - استكشاف الأخطاء وإصلاحها](#) للحصول على معلومات عامة حول استكشاف أخطاء هذا التكوين وإصلاحها.

### معلومات ذات صلة

- [IPsec مع عميل VPN إلى مثال تكوين مركز VPN 3000](#)
- [مركزات Cisco VPN 3000 Series](#)
- [عميل شبكة VPN من Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا