

عالم عمل ماسقنا يقي فن ب حامس ل ا ASA/PIX: نيوكت ل ا ثم ي ل ع VPN

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [المنتجات ذات الصلة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [تكوين الاتصال النفقي المنقسم على ASA](#)
- [تكوين ASA 7.x باستخدام Adaptive Security Device Manager \(ASDM\) 5.x](#)
- [تكوين ASA 8.x مع Adaptive Security Device Manager \(ASDM\) 6.x](#)
- [تكوين ASA 7.x والإصدارات الأحدث عبر CLI](#)
- [تكوين PIX 6.x من خلال CLI \(واجهة سطر الأوامر\)](#)
- [التحقق من الصحة](#)
- [الاتصال بعمل شبكة VPN](#)
- [عرض سجل عمل شبكة VPN](#)
- [إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الاتصال](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [تحديد باستخدام عدد الإدخالات في قائمة التحكم في الوصول \(ACL\) إلى النفق المنقسم](#)
- [معلومات ذات صلة](#)

المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح لعملاء شبكات VPN بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في جهاز أمان Cisco Adaptive Security Appliance (ASA) 5500 Series. يتيح هذا التكوين لعملاء الشبكات الخاصة الظاهرية (VPN) إمكانية الوصول الآمن إلى موارد الشركة عبر IPsec أثناء منح وصول غير آمن إلى الإنترنت.

ملاحظة: يعتبر إنشاء قنوات الاتصال النفقي الكامل التكوين الأكثر أماناً لأنه لا يتيح الوصول المتزامن للجهاز إلى كل من الإنترنت وشبكة LAN الخاصة بالشركات. يسمح حل توفيق بين الاتصال النفقي الكامل والنفقي المنقسم لعملاء VPN الوصول إلى شبكة LAN المحلية فقط. راجع [PIX/ASA 7.x: السماح بالوصول إلى شبكة LAN المحلية لمثال تكوين عملاء VPN للحصول على مزيد من المعلومات.](#)

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن تكوين VPN للوصول عن بعد عاملا موجود بالفعل على ASA. ارجع إلى [PIX/ASA 7.x](#) كخادم VPN بعيد باستخدام مثال تكوين ASDM إذا لم يتم تكوين واحد بالفعل.

المكونات المستخدمة

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

• برنامج جهاز الأمان Cisco ASA 5500 Series Security Appliance Software، الإصدار x.7 والإصدارات الأحدث

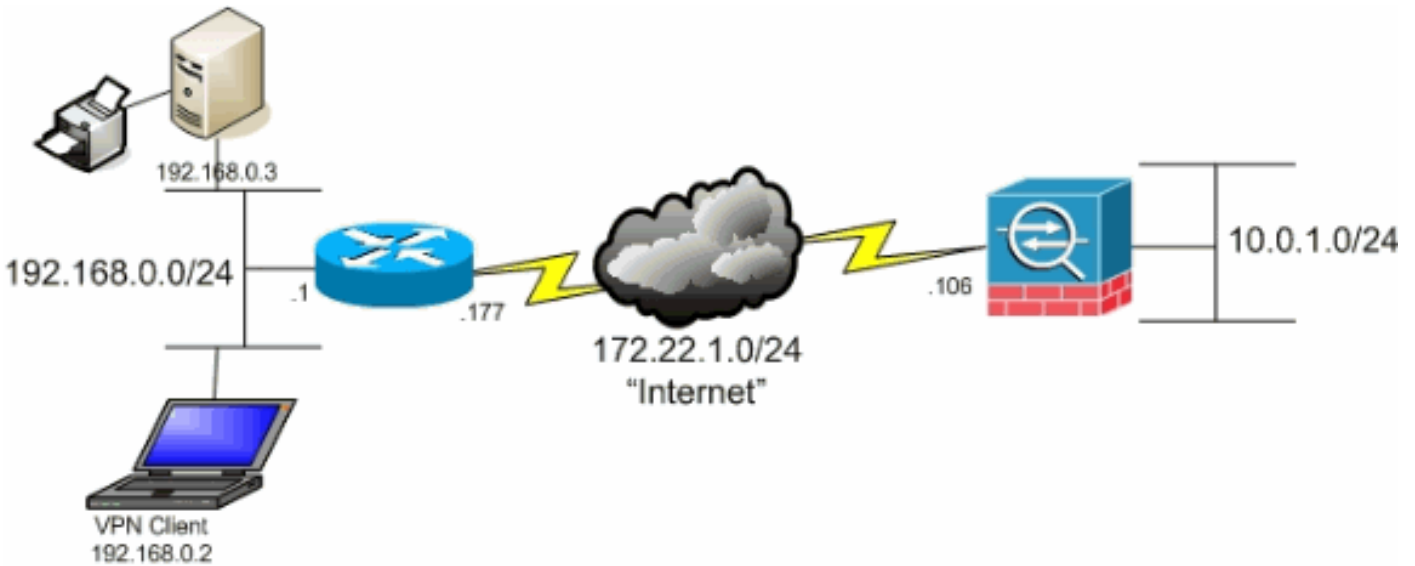
• Cisco Systems VPN Client، الإصدار 4.0.5

ملاحظة: يحتوي هذا المستند أيضا على تكوين PIX 6.x CLI المتوافق مع عميل Cisco VPN 3.x.

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.



المنتجات ذات الصلة

كما يمكن استخدام هذا التكوين مع برنامج جهاز الأمان Cisco PIX 500 Series Security Appliance Software، الإصدار x.7.

الاصطلاحات

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

معلومات أساسية

في سيناريو أساسي VPN Client إلى ASA، يتم تشفير جميع حركات مرور البيانات من عميل شبكة VPN وإرسالها إلى ASA بغض النظر عن الوجهة الخاصة بها. استنادا إلى التكوين الخاص بك وعدد المستخدمين المدعومين، يمكن أن تصبح عملية الإعداد هذه ذات نطاق ترددي كبير. يمكن أن يعمل تقسيم الاتصال النفقي على تخفيف هذه المشكلة

لأنه يسمح للمستخدمين بإرسال حركة المرور الموجهة إلى شبكة الشركة عبر النفق فقط. 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 ASA

تكوين ASA 7.x باستخدام Adaptive Security Device Manager (ASDM) 5.x

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة.

1. أختارت تشكيل <VPN> عام <مجموعة سياسة وحدد المجموعة سياسة أن أنت تريد أن يمكن محلي منفذ في. ثم انقر فوق

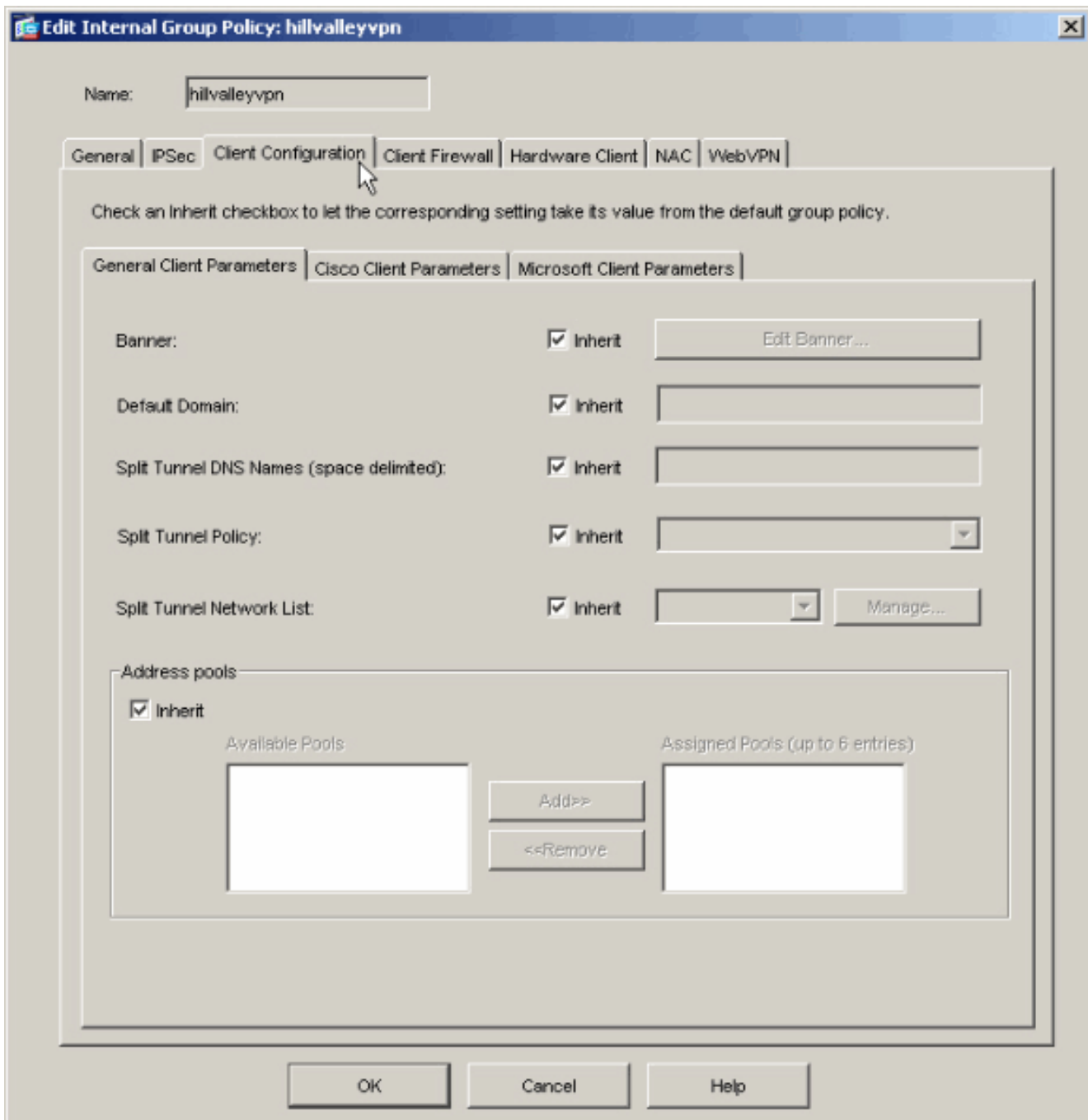
تحرير.

The screenshot shows the Cisco ASDM 5.x configuration interface. The navigation pane on the left is set to 'VPN' > 'General' > 'Group Policy'. The main configuration area displays the 'Group Policy' configuration page. A table lists the existing group policies:

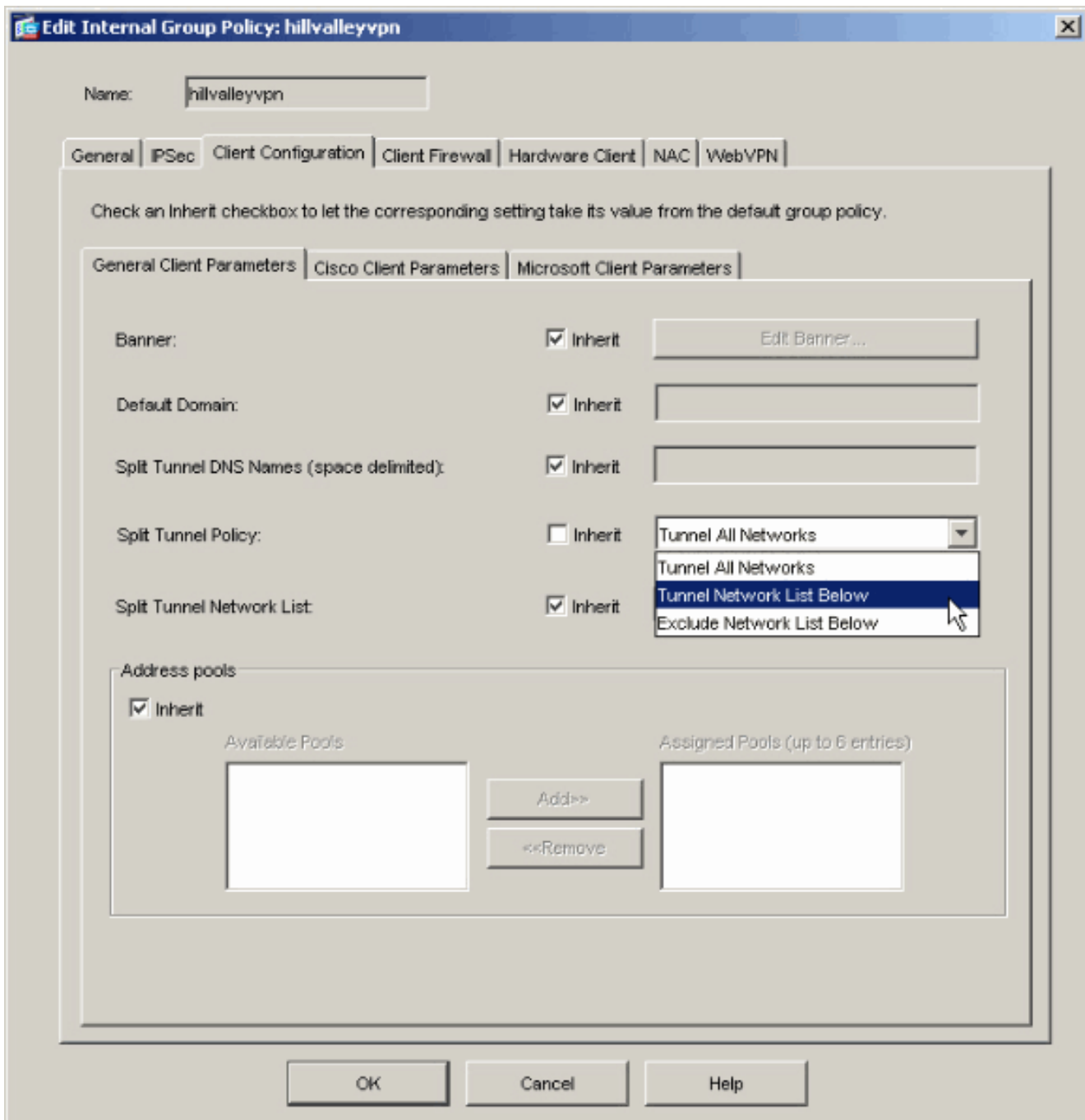
Name	Type	Tunneling Protocol	AAA Server Group
intvalleyvpn	Internal	IPSec	-- N/A --
OrbiGrpPolicy (System Defa...	Internal	L2TP/IPSec, IPSec	-- N/A --

Buttons for 'Add', 'Edit', and 'Delete' are visible to the right of the table. The 'Edit' button is highlighted. The status bar at the bottom indicates 'Configuration changes saved successfully.' and the system time is 8/1/06 7:28:38 PM UTC.

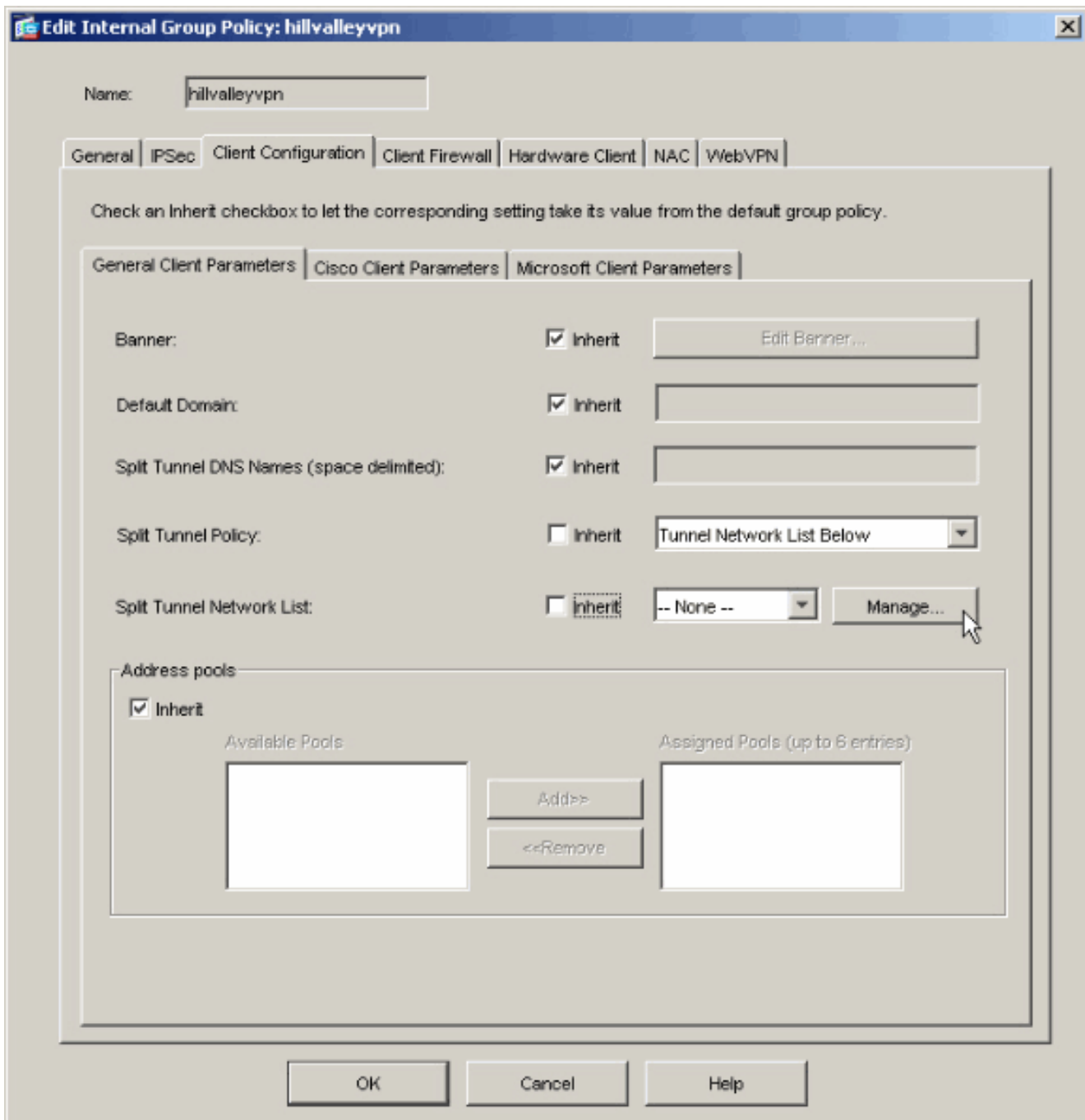
2. انتقل إلى علامة التبويب تكوين العميل.



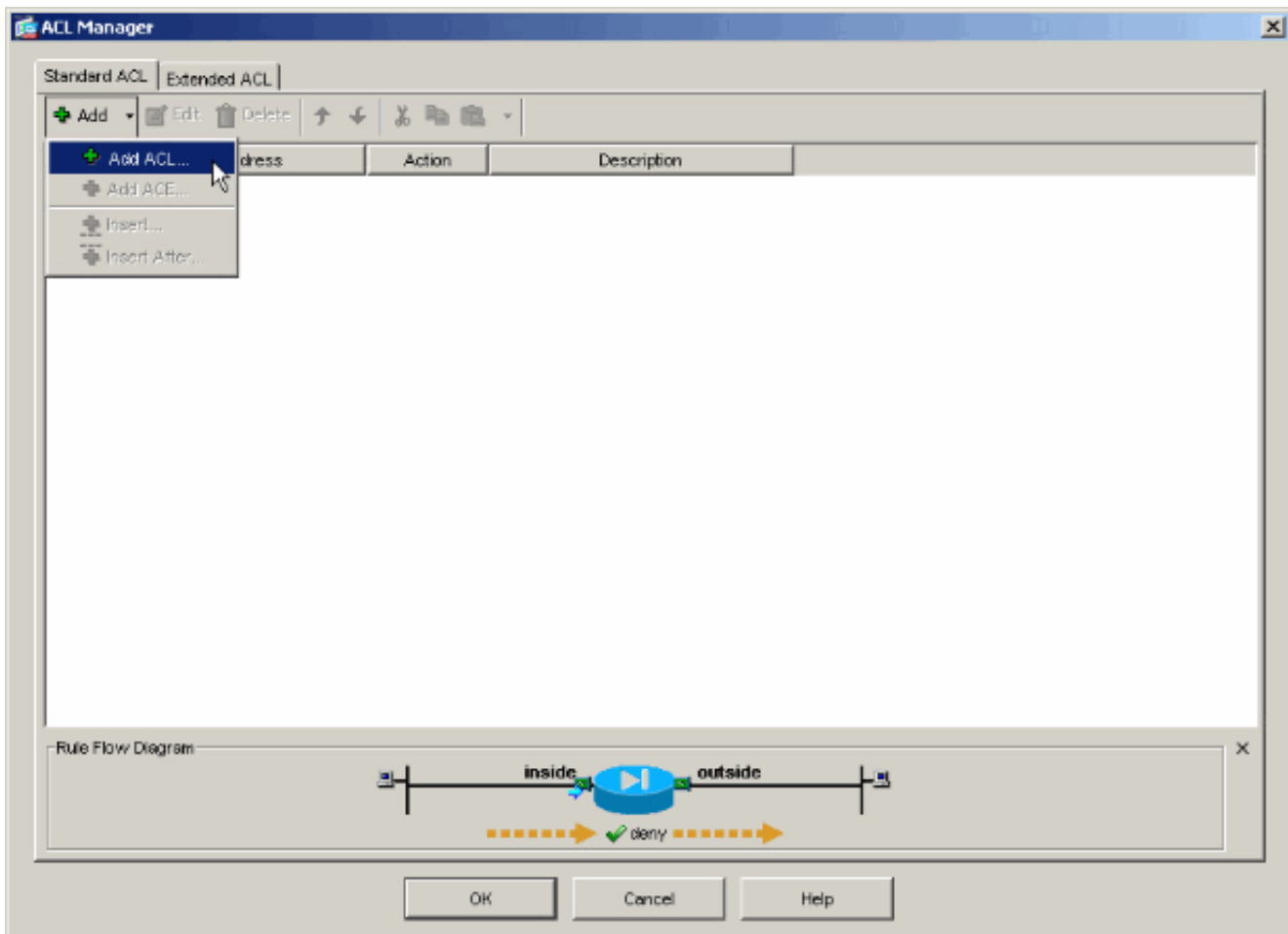
3. قم بإلغاء تحديد مربع **Inherit** لنهج النفق المقسم واختر قائمة شبكة النفق أدناه.



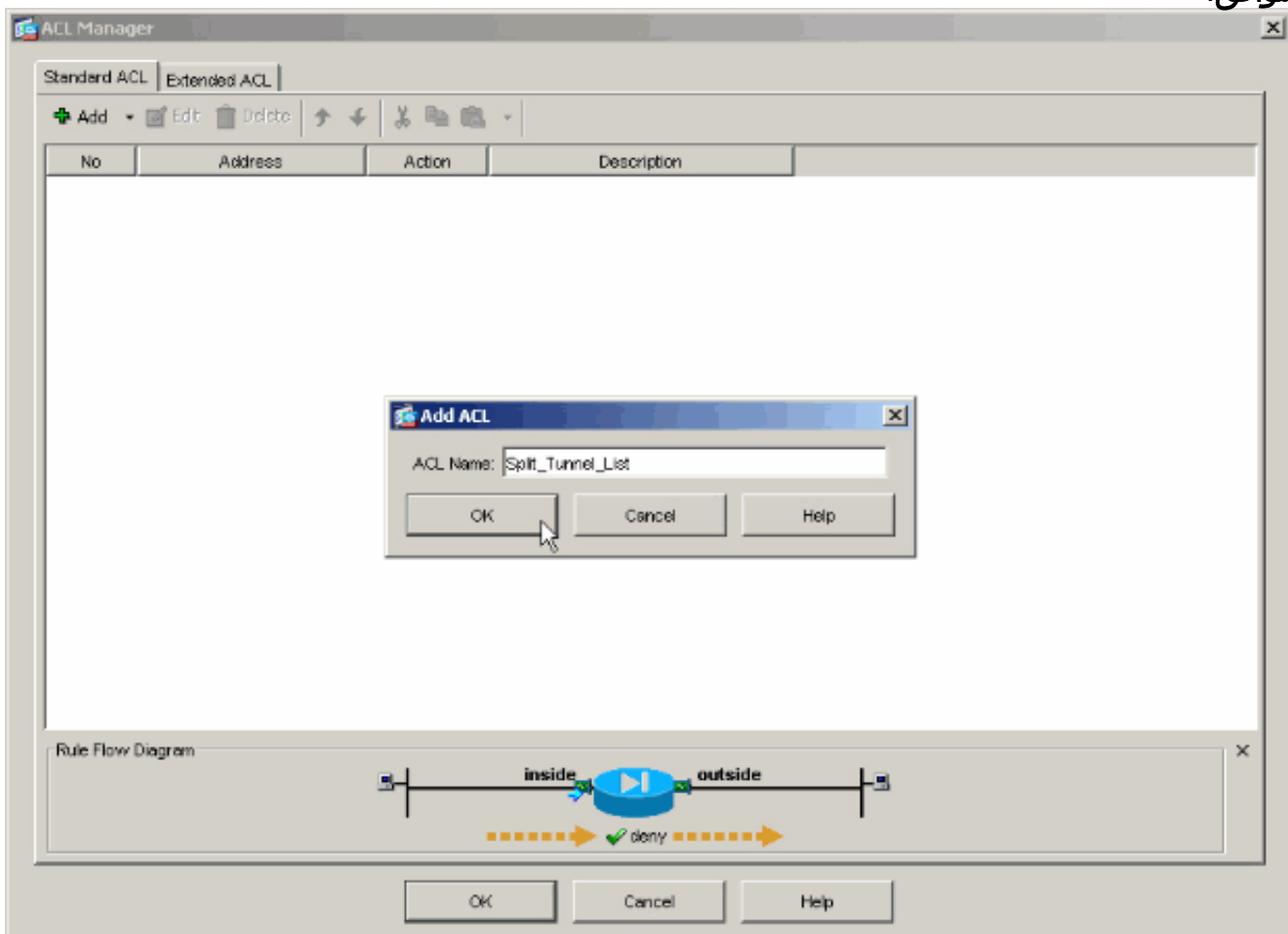
4. قم بإلغاء تحديد مربع **Inherit** لقائمة شبكات النفق المقسم ثم انقر فوق إدارة لتشغيل إدارة قائمة التحكم في الوصول (ACL).



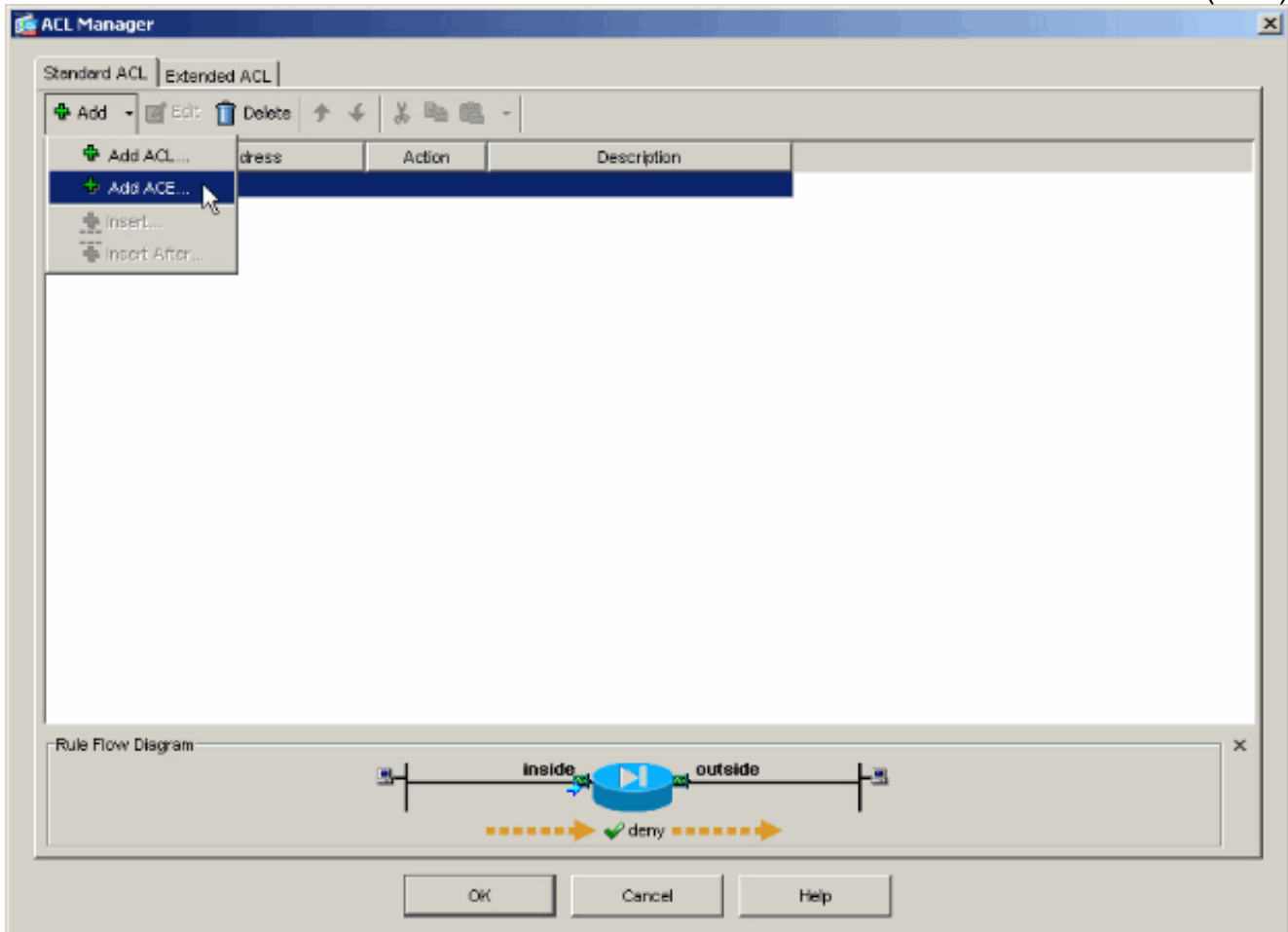
5. ضمن إدارة قائمة التحكم في الوصول (ACL)، أختار إضافة < قائمة التحكم في الوصول (ACL).. لإنشاء قائمة وصول جديدة.



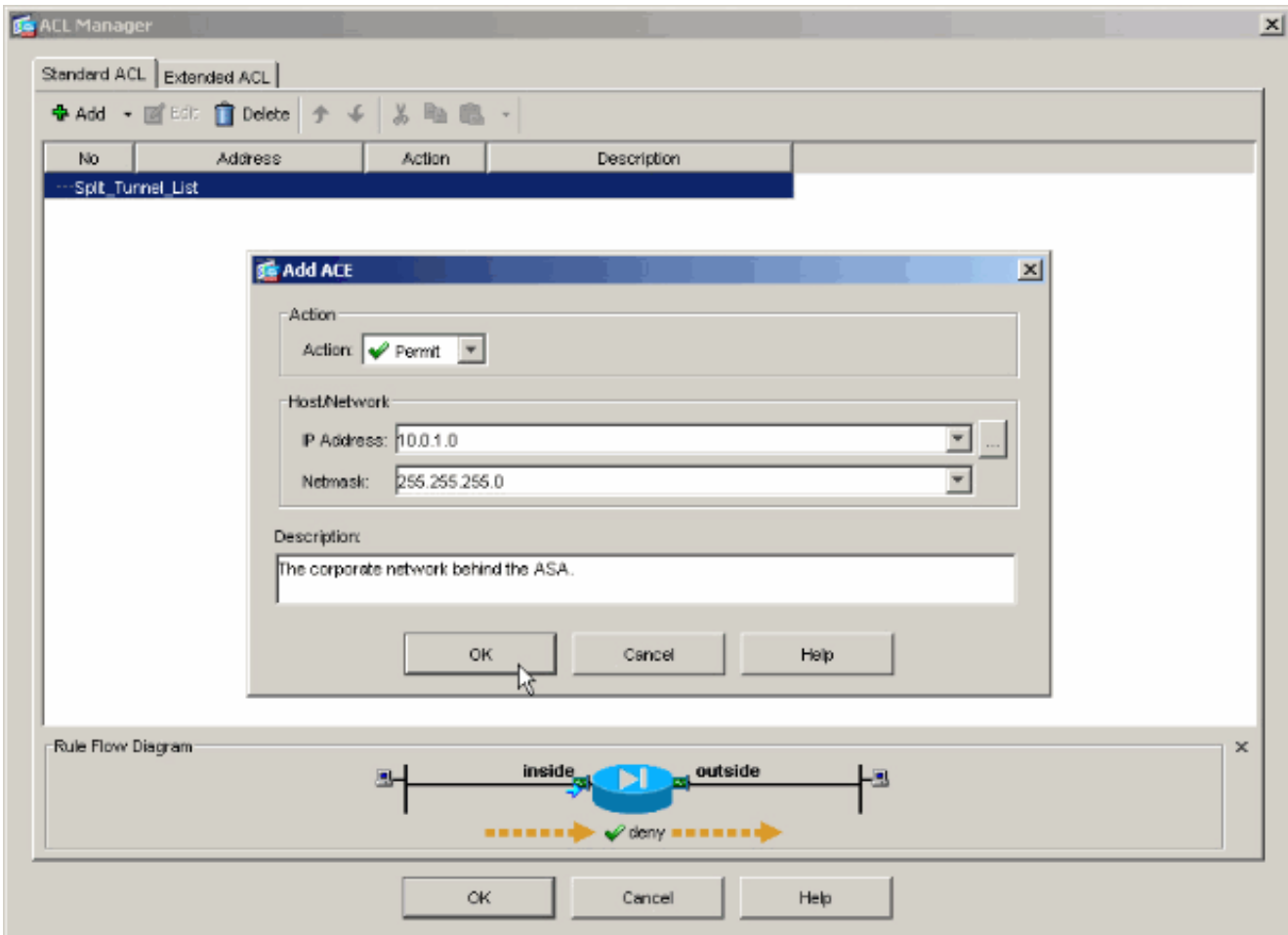
6. قم بتوفير اسم لقائمة التحكم بالوصول (ACL) وانقر فوق موافق.



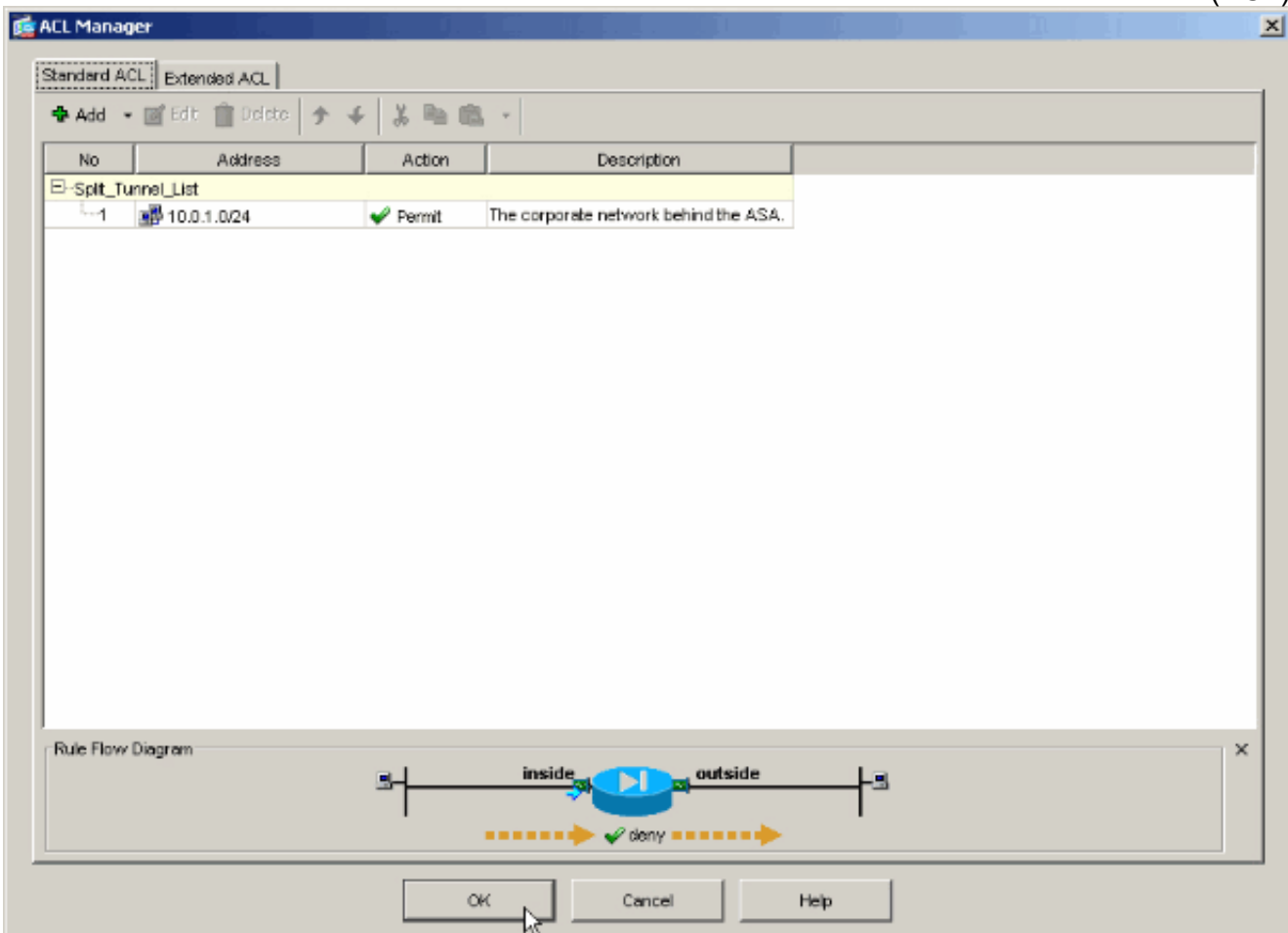
7. بمجرد إنشاء قائمة التحكم في الوصول، اختر إضافة < إضافة ACE.. لإضافة إدخال التحكم في الوصول



8. عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 24/10.0.1.0. اختر سماح. اختر عنوان IP من 10.0.1.0 اختر قناع شبكة 255.255.255.0. (إختياري) قم بتوفير وصف. وانقر فوق .OK



9. انقر فوق موافق للخروج من إدارة قائمة التحكم في الوصول (ACL).



10. تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق.

Edit Internal Group Policy: hillvalleyvpn

Name:

General | IPsec | Client Configuration | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner: Inherit

Default Domain: Inherit

Split Tunnel DNS Names (space delimited): Inherit

Split Tunnel Policy: Inherit

Split Tunnel Network List: Inherit

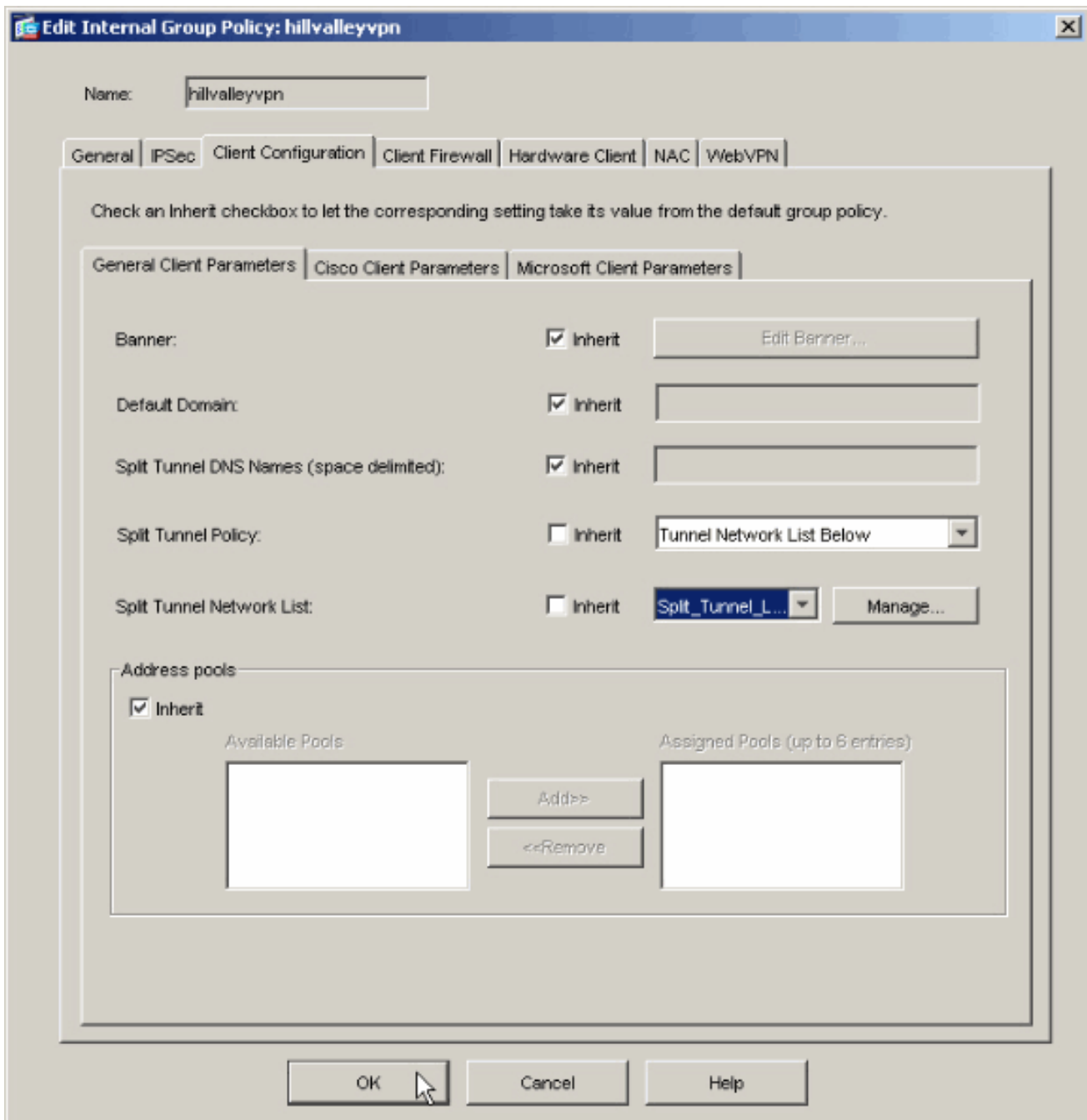
Address pools

Inherit

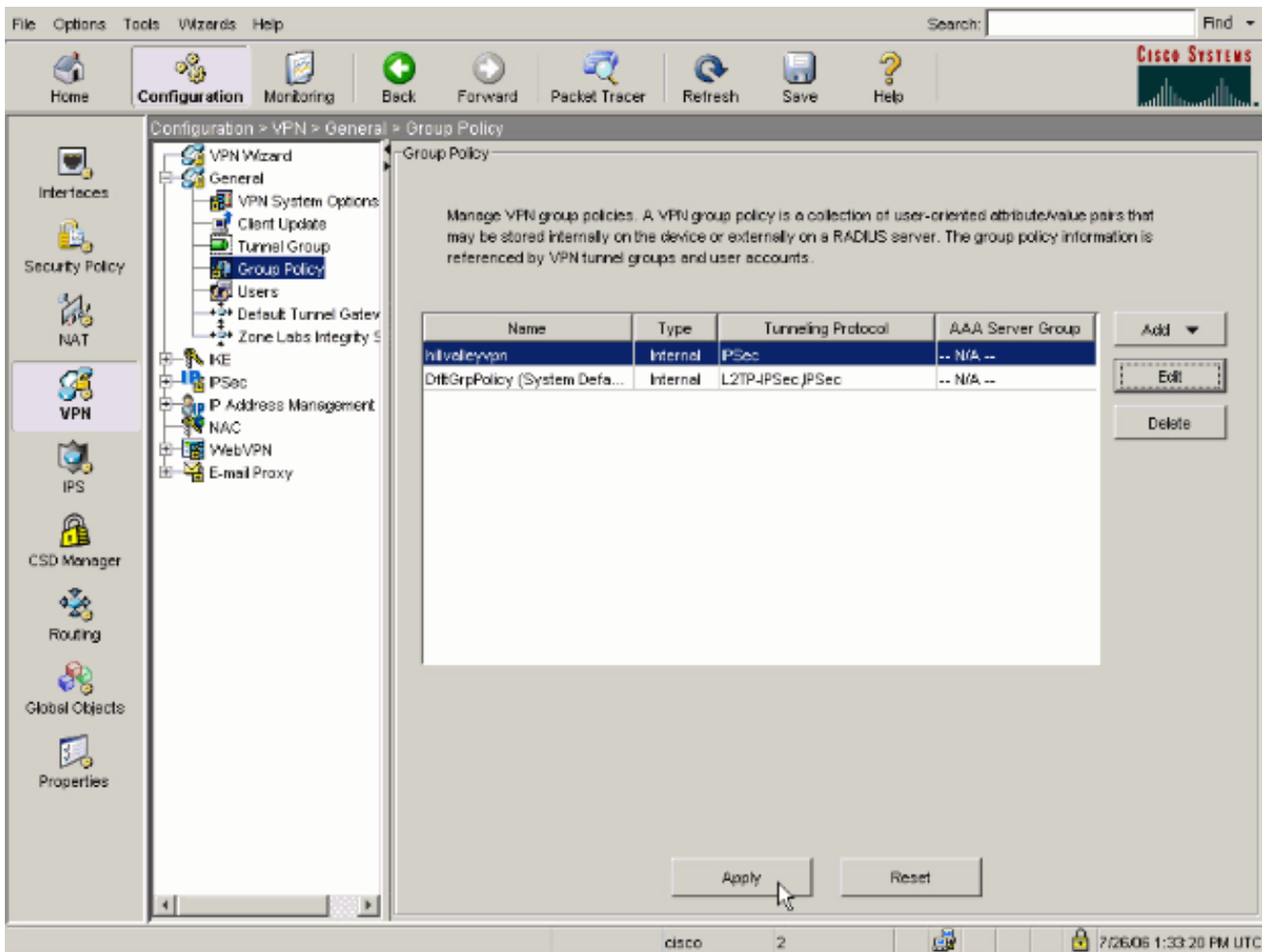
Available Pools

Assigned Pools (up to 6 entries)

11. انقر فوق موافق للعودة إلى تكوين "نهج المجموعة".



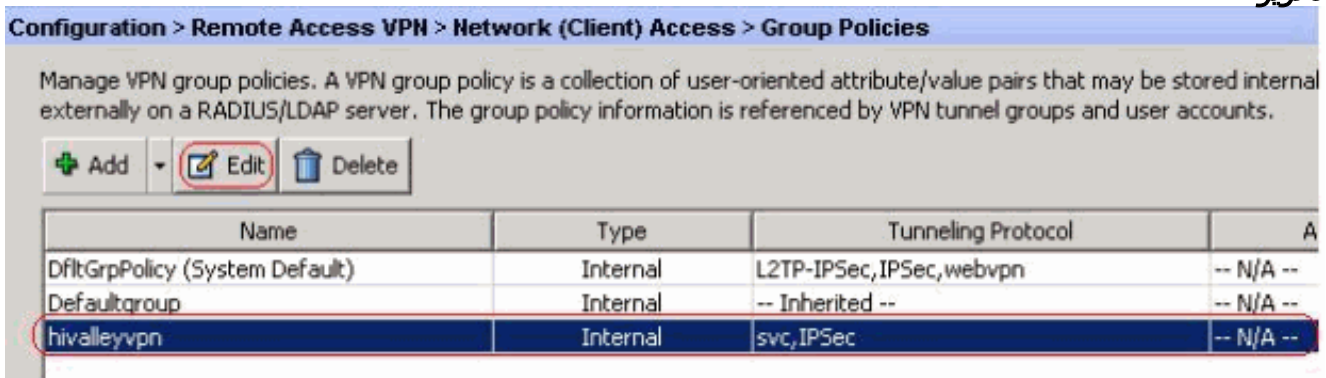
12. طقطقة يطبق وبعد ذلك يرسل (إن يتطلب) in order to أرسلت الأمر إلى ال .ASA



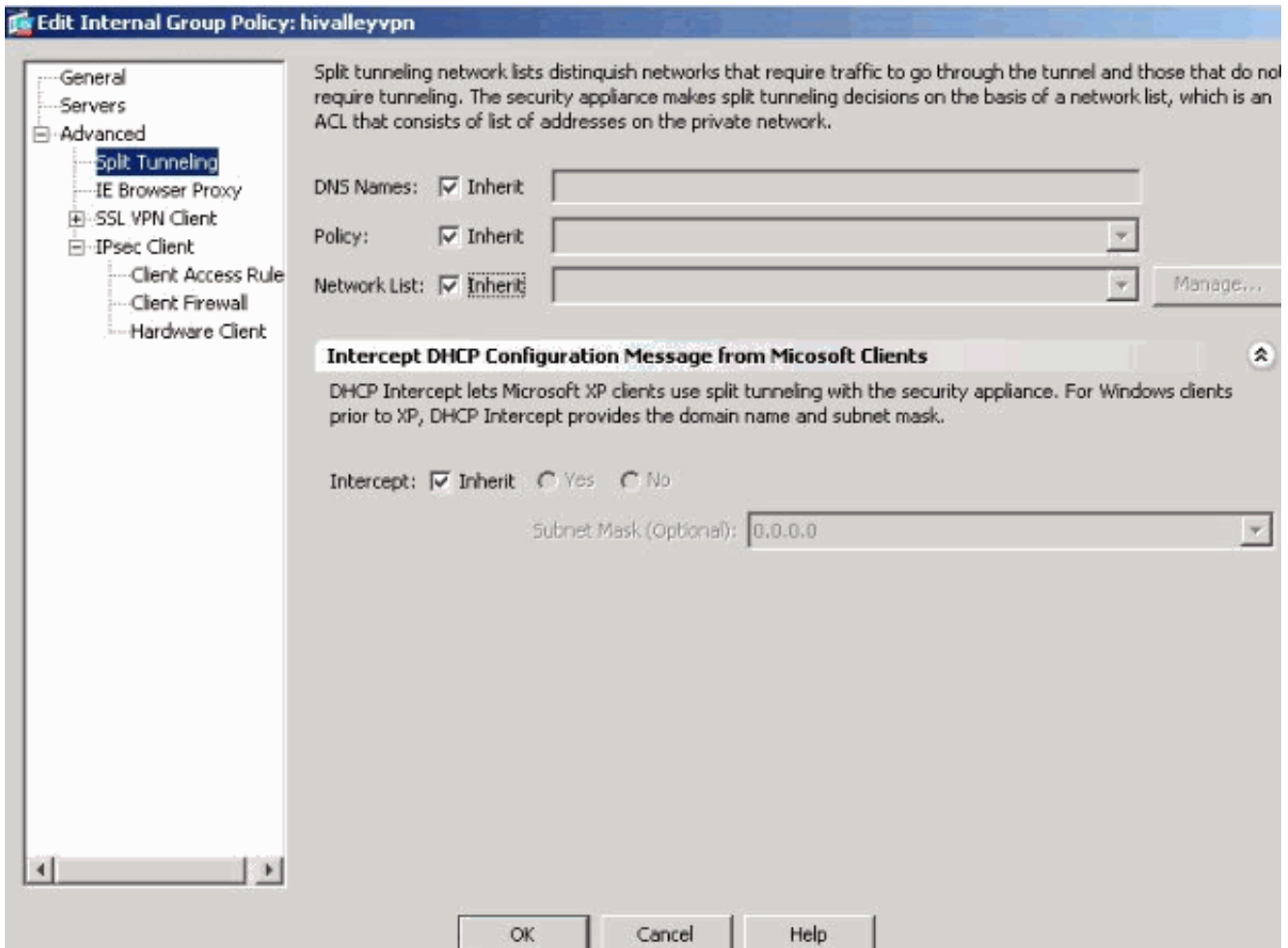
تكوين ASA 8.x مع Adaptive Security Device Manager (ASDM) 6.x

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة.

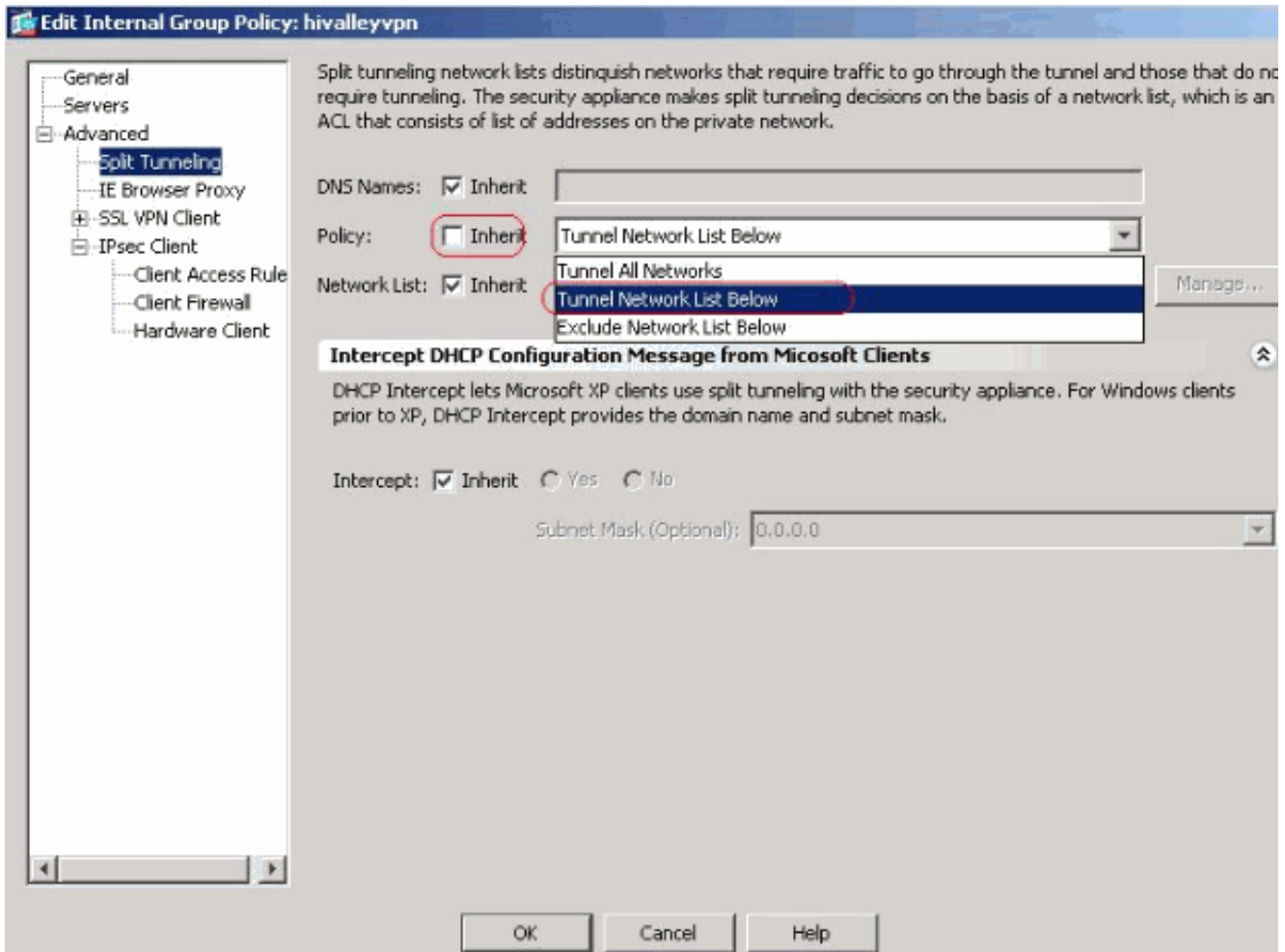
1. اختر Configuration (تكوين) < Remote Access VPN (وصول عن بعد) < Network (عميل) Access (وصول الشبكة) < Group Policy (نهج المجموعة)، واختر Group Policy (نهج المجموعة) الذي تريد تمكين الوصول إلى LAN المحلي فيه. ثم انقر فوق تحرير.



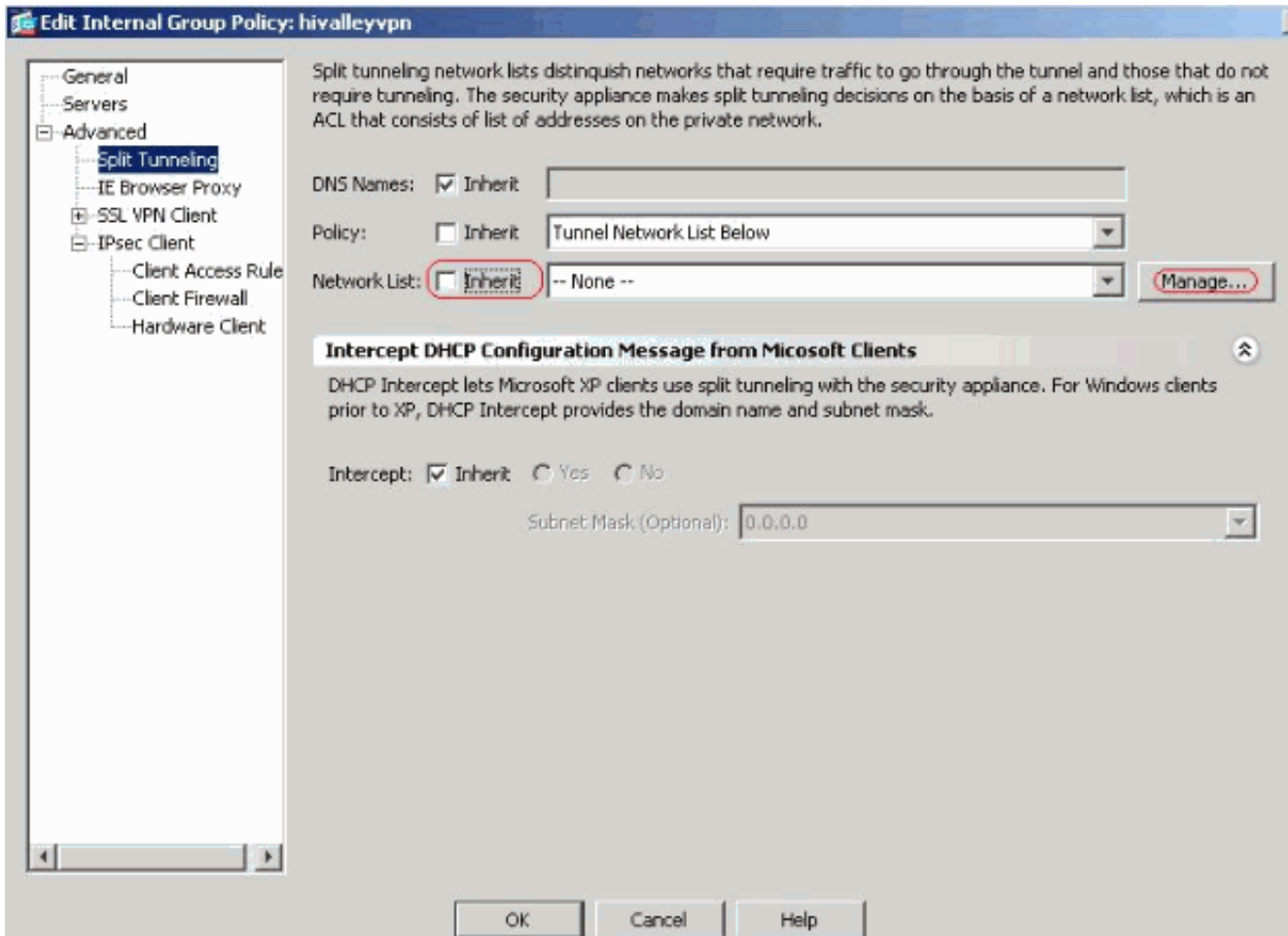
2. انقر فوق تقسيم الاتصال النفقي.



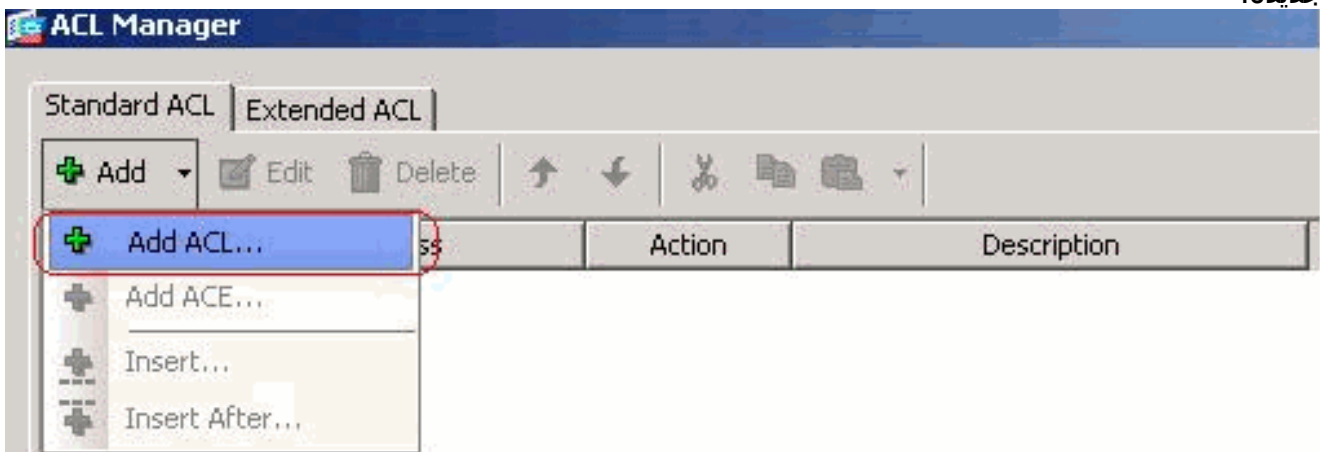
3. قم بإلغاء تحديد مربع **Inherit** لنهج النفق المقسم، واختر قائمة شبكة النفق أدناه.



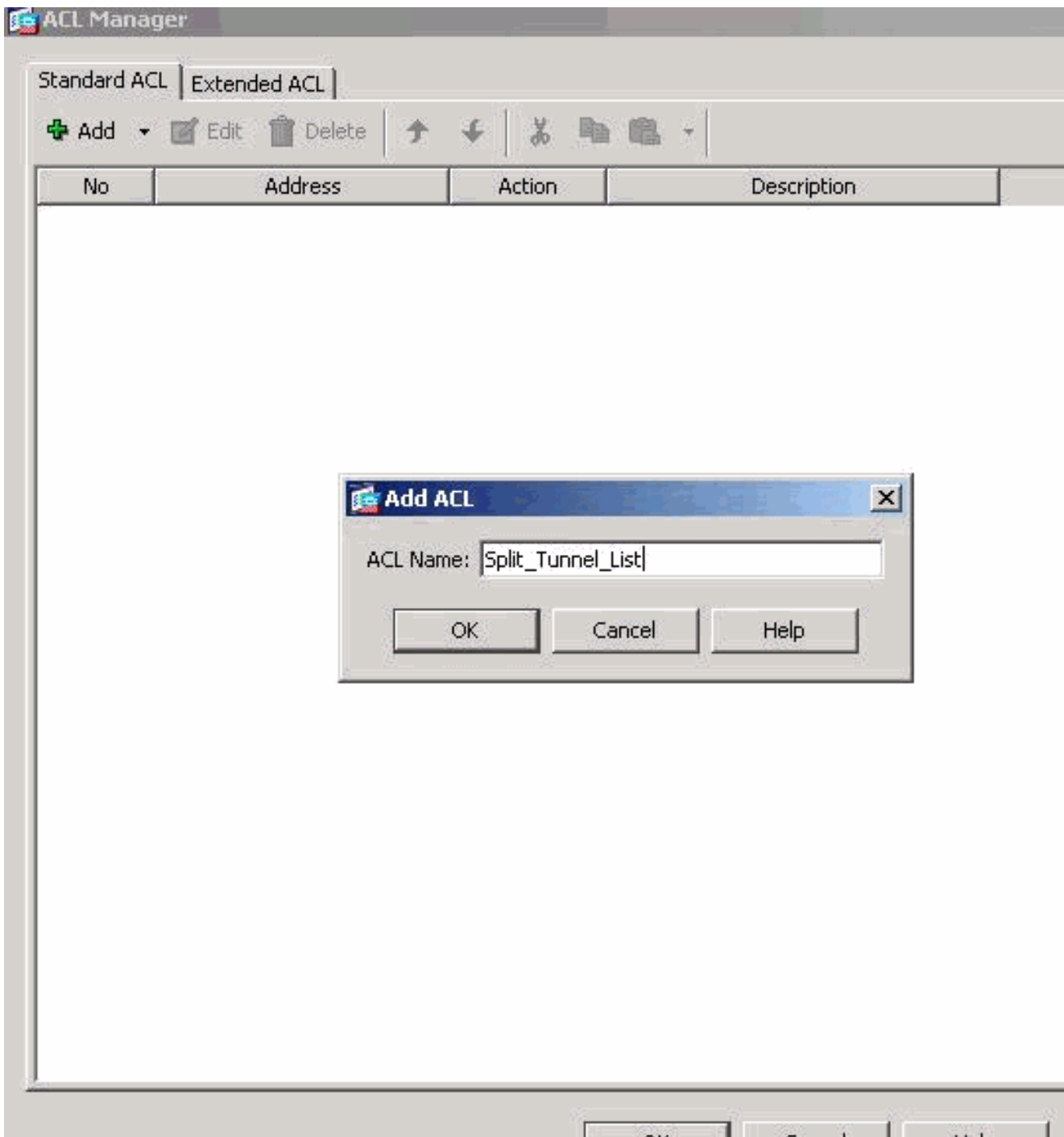
4. قم بإلغاء تحديد مربع **Inherit** لقائمة شبكات النفق المقسم، ثم انقر فوق **Manage** لتشغيل إدارة قائمة التحكم في الوصول (ACL).



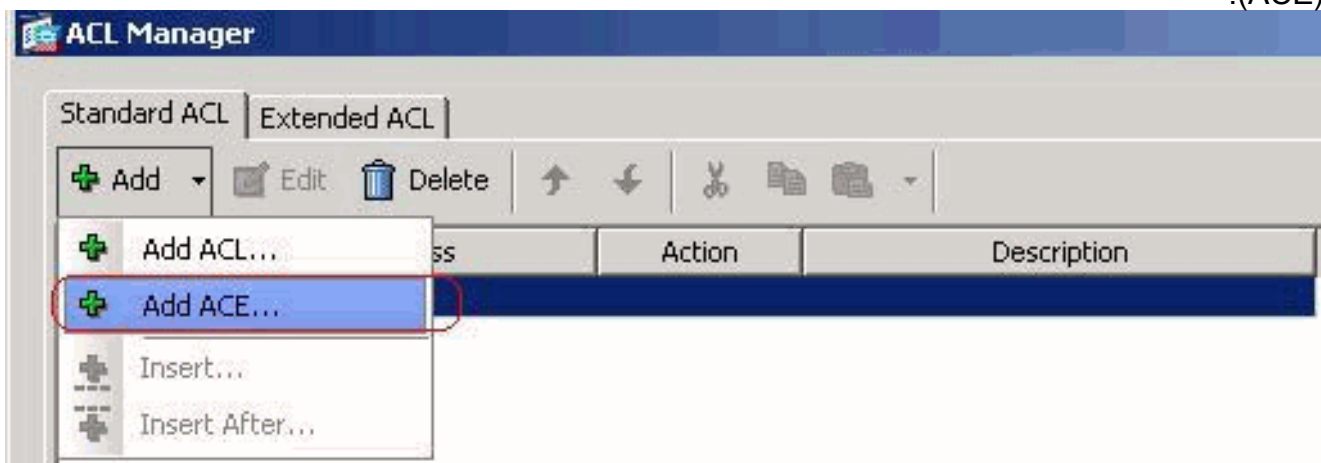
5. ضمن إدارة قائمة التحكم في الوصول (ACL)، أختار إضافة < قائمة التحكم في الوصول (ACL) .. لإنشاء قائمة وصول جديدة.



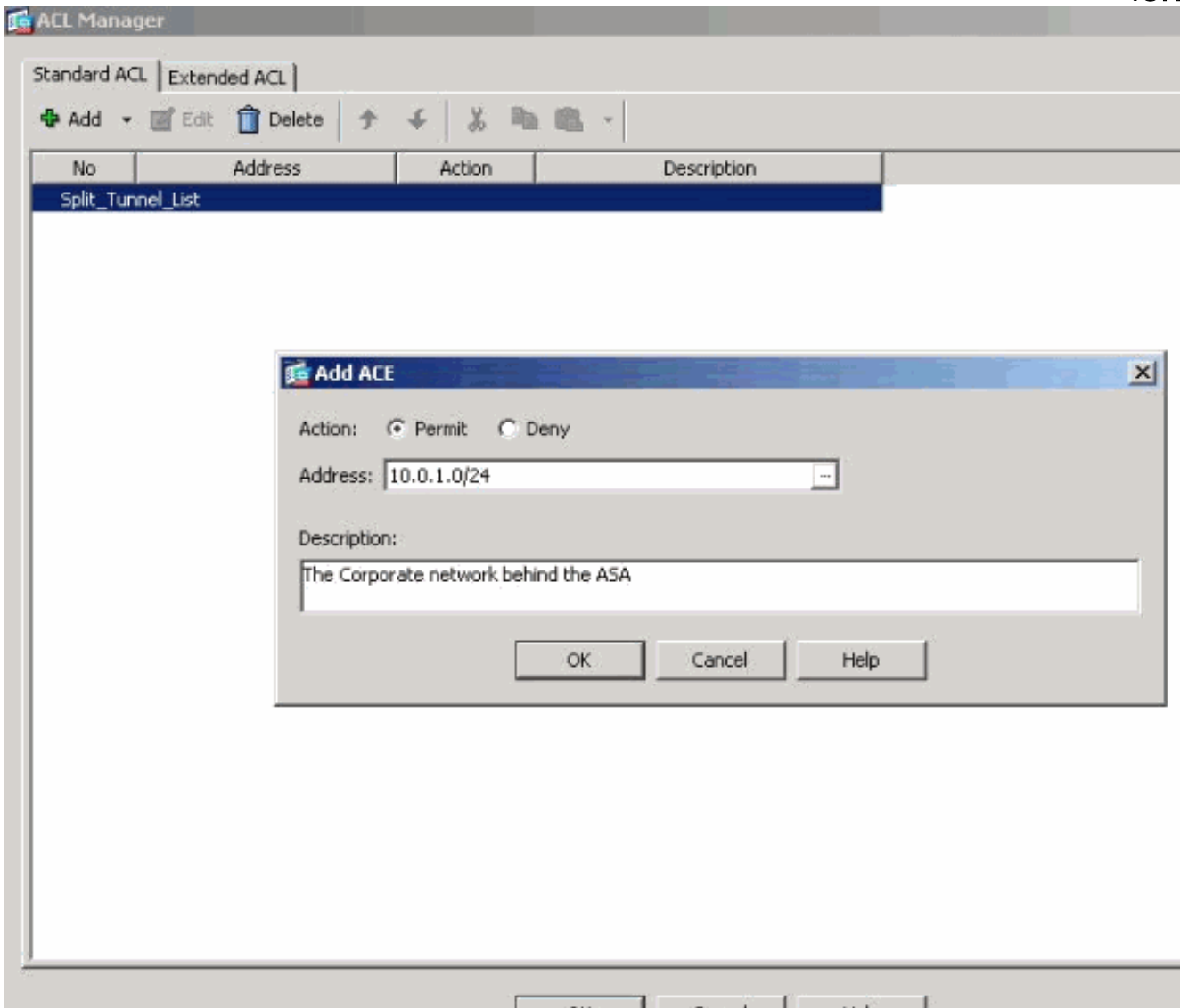
6. قم بتوفير اسم لقائمة التحكم بالوصول (ACL)، وانقر فوق موافق.



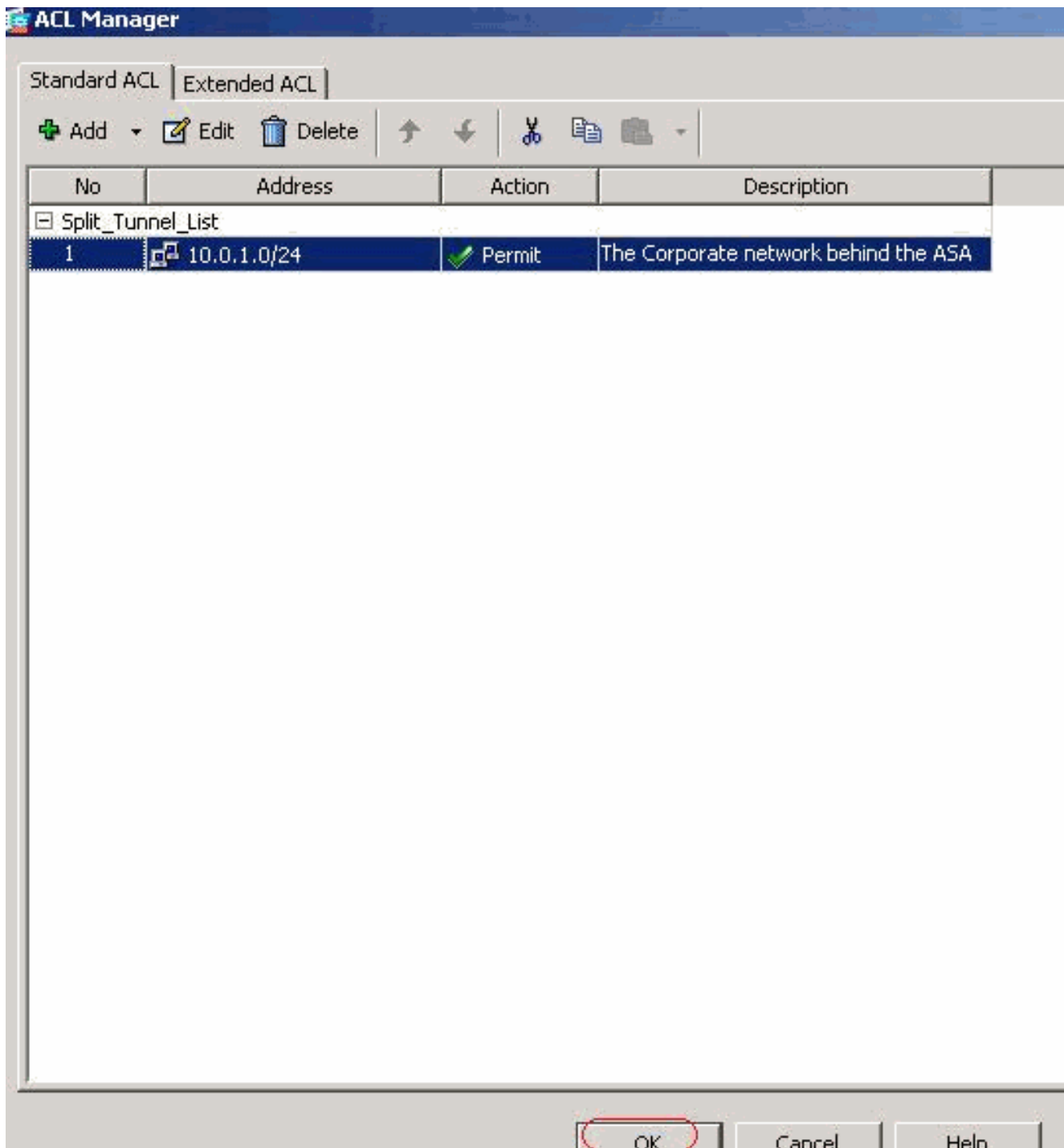
7. بمجرد إنشاء قائمة التحكم في الوصول، أختار إضافة < إضافة ACE.. لإضافة إدخال التحكم في الوصول (ACE).



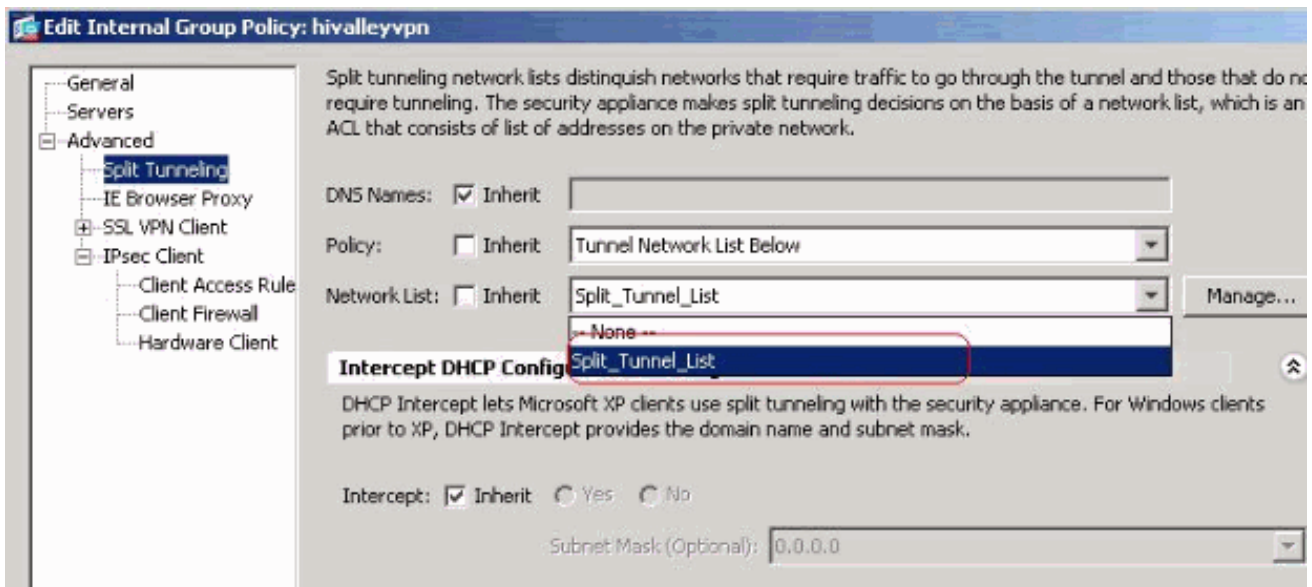
8. عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 24/10.0.1.0. طقطقت ال يسمح لاسلكي زر. أختار عنوان الشبكة باستخدام القناع 24/10.0.1.0. (إختياري) قم بتوفير وصف. وانقر فوق



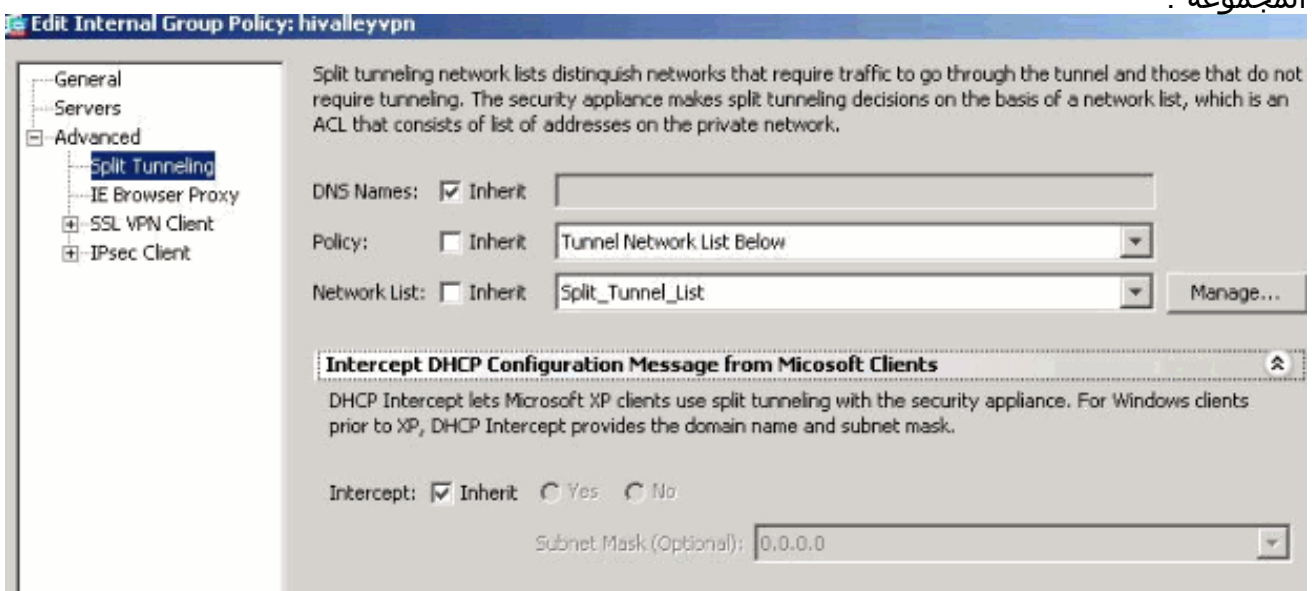
9. انقر فوق موافق للخروج من إدارة قائمة التحكم في الوصول (ACL).



10. تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق المقسم.






11. انقر فوق موافق للعودة إلى تكوين "نهج المجموعة".



12. طقطقة يطبق وبعد ذلك يرسل (إن يتطلب) in order to أرسلت الأمر إلى ال .ASA

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

 Add  Edit  Delete

Name	Type	Tunneling Protocol	
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A --
Defaultgroup	Internal	-- Inherited --	-- N/A --
hivalleyvpn	Internal	svc,IPSec	-- N/A --

Apply

Reset

تكوين ASA 7.x والإصدارات الأحدث عبر CLI

بدلاً من استخدام ASDM، أنت تستطيع أتمتة هذا steps في ال ASA CLI in order to سمحت انقسام tunneling على ال ASA:

ملاحظة: تكوين اتصال CLI النفقي المنقسم هو نفسه لكل من ASA 7.x و x.8.

1. أدخل إلى وضع التكوين.

```
ciscoasa>enable
***** :Password
ciscoasa#configure terminal
#(ciscoasa(config)
```

2. قم بإنشاء قائمة الوصول التي تعرف الشبكة خلف ASA.
ciscoasa(config)#access-list Split_Tunnel_List remark The corporate network behind the ASA
ciscoasa(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

3. أدخل وضع تكوين "نهج المجموعة" للنهج الذي ترغب في تعديله.
ciscoasa(config)#group-policy hillvalleyvpn attributes
#(ciscoasa(config-group-policy)

4. حدد نهج نفق التقسيم. في هذه الحالة، يتم تحديد النهج tunnelspecified.
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified

.5 حدد قائمة الوصول إلى النفق المقسم. في هذه الحالة، تكون القائمة **SPLIT_TUNNEL_LIST**
ciscoasa(config-group-policy)#split-tunnel-network-list value Split_Tunnel_List

.6 قم بإصدار هذا الأمر:
ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes

.7 إقران نهج المجموعة بمجموعة النفق
ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn

.8 خرجت الإثبات تشكيل أسلوب.

```
ciscoasa(config-group-policy)#exit
ciscoasa(config)#exit
#ciscoasa
```

.9 احفظ التكوين على ذاكرة الوصول العشوائي غير المتطايرة (NVRAM) واضغط على Enter عند طلبها لتحديد اسم الملف المصدر.

```
ciscoasa#copy running-config startup-config
```

```
?[Source filename [running-config
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a
```

```
(bytes copied in 3.470 secs (1282 bytes/sec 3847
#ciscoasa
```

تكوين PIX 6.x من خلال CLI (واجهة سطر الأوامر)

أكمل الخطوات التالية:

.1 قم بإنشاء قائمة الوصول التي تعرف الشبكة خلف PIX.

```
PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

.2 قم بإنشاء مجموعة VPN **VPN3000** وحدد قائمة التحكم في الوصول للنفق المنقسم إليها كما هو موضح:

```
PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
```

ملاحظة: ارجع إلى [Cisco Secure PIX Firewall 6.x](#) و [Cisco VPN Client 3.5 ل Windows](#) مع مصادقة [Microsoft Windows 2000](#) و [IAS RADIUS 2003](#) للحصول على مزيد من المعلومات حول تكوين الوصول عن بعد VPN ل PIX 6.x.

التحقق من الصحة

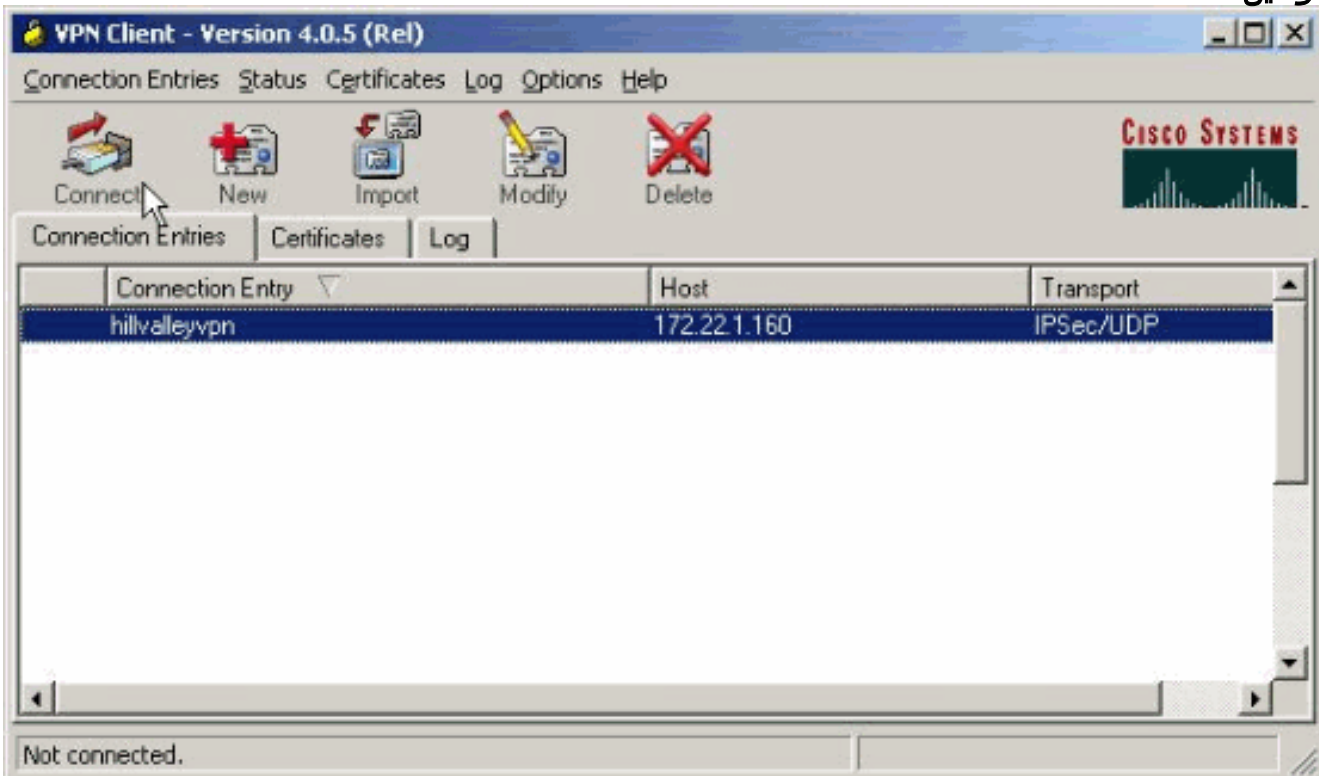
اتباع الخطوات الواردة في هذه الأقسام للتحقق من التكوين الخاص بك.

- [الاتصال بعميل شبكة VPN](#)
- [عرض سجل عميل شبكة VPN](#)
- [إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الإتصال](#)

الاتصال بعميل 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.

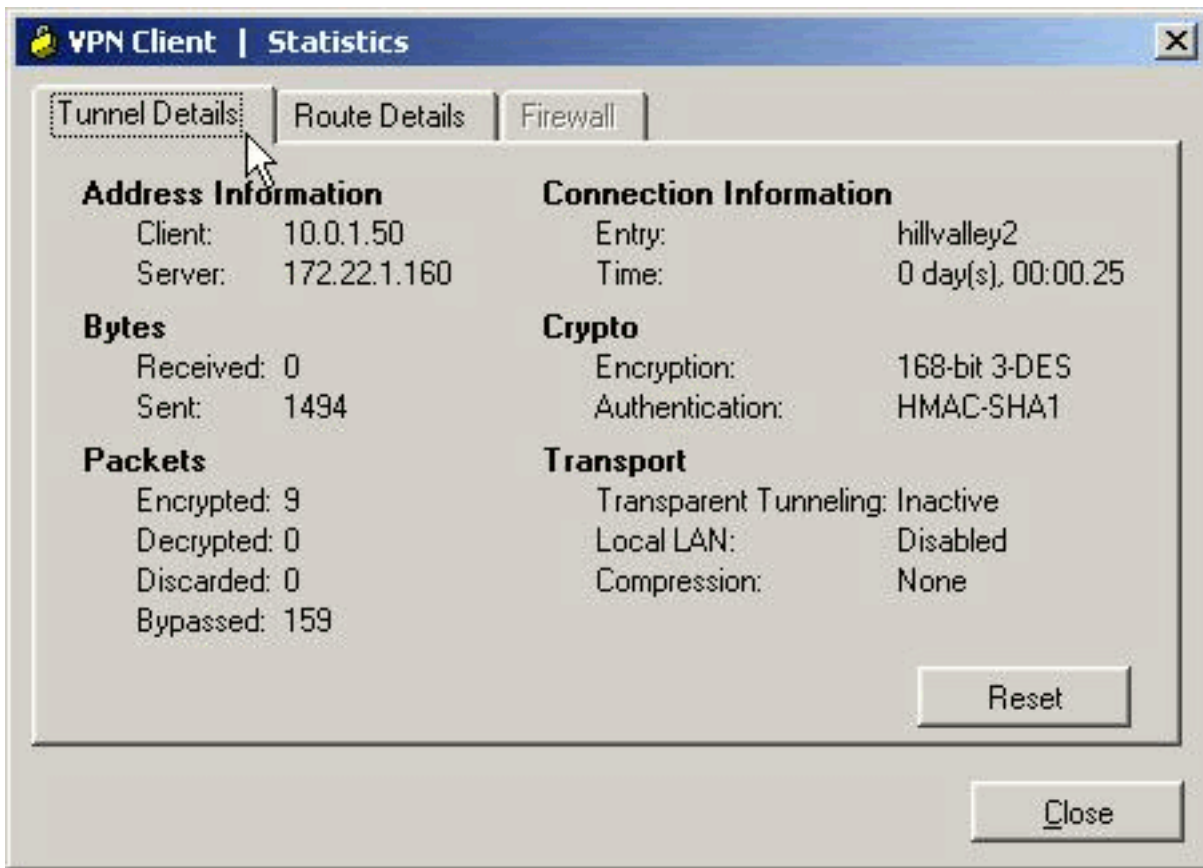


2. أدخل بيانات الاعتماد الخاصة

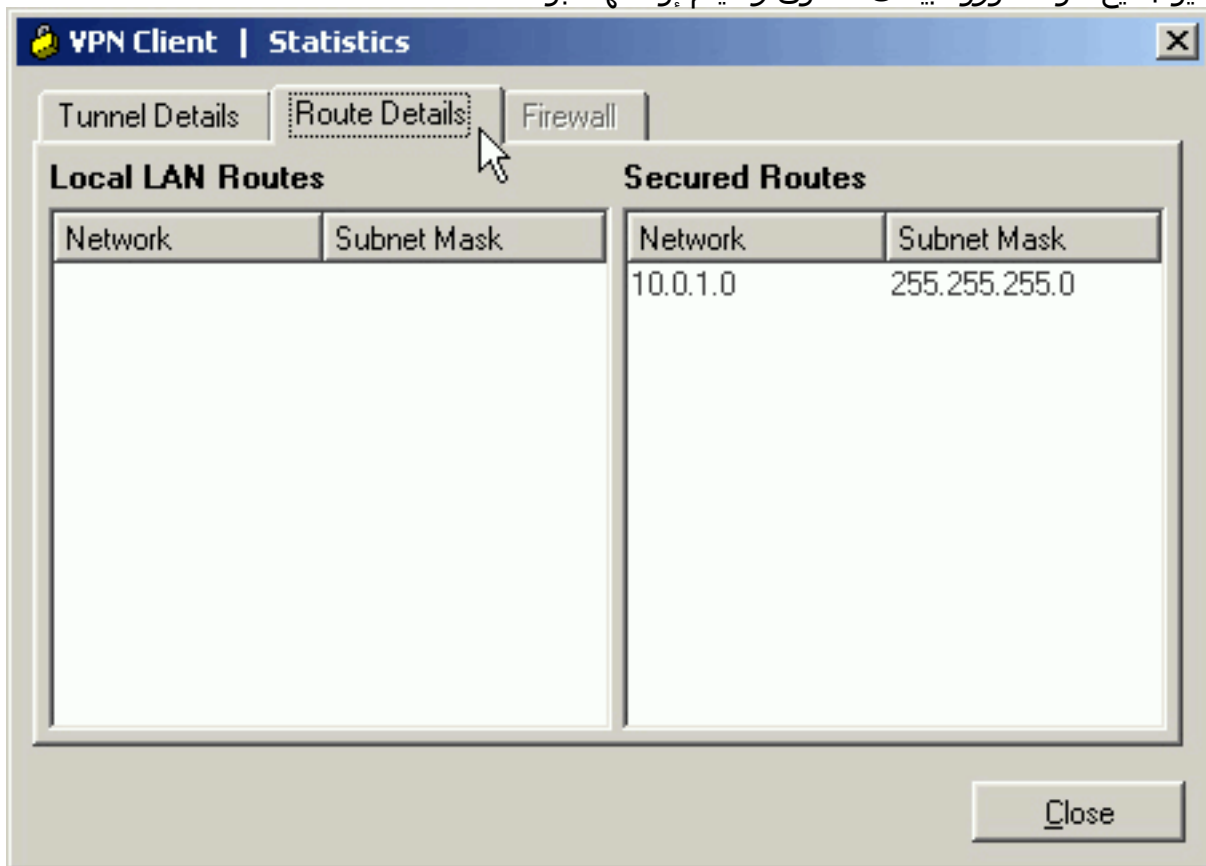


بك.

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



المرو. 4. انتقل إلى علامة التبويب تفاصيل المسار للاطلاع على الموجهات التي يقوم عميل شبكة VPN بتأمينها إلى ASA. في هذا المثال، يقوم عميل الشبكة الخاصة الظاهرية (VPN) بتأمين الوصول إلى 24/10.0.1.0 بينما لا يتم تشفير جميع حركة مرور البيانات الأخرى ولا يتم إرسالها عبر النفق.

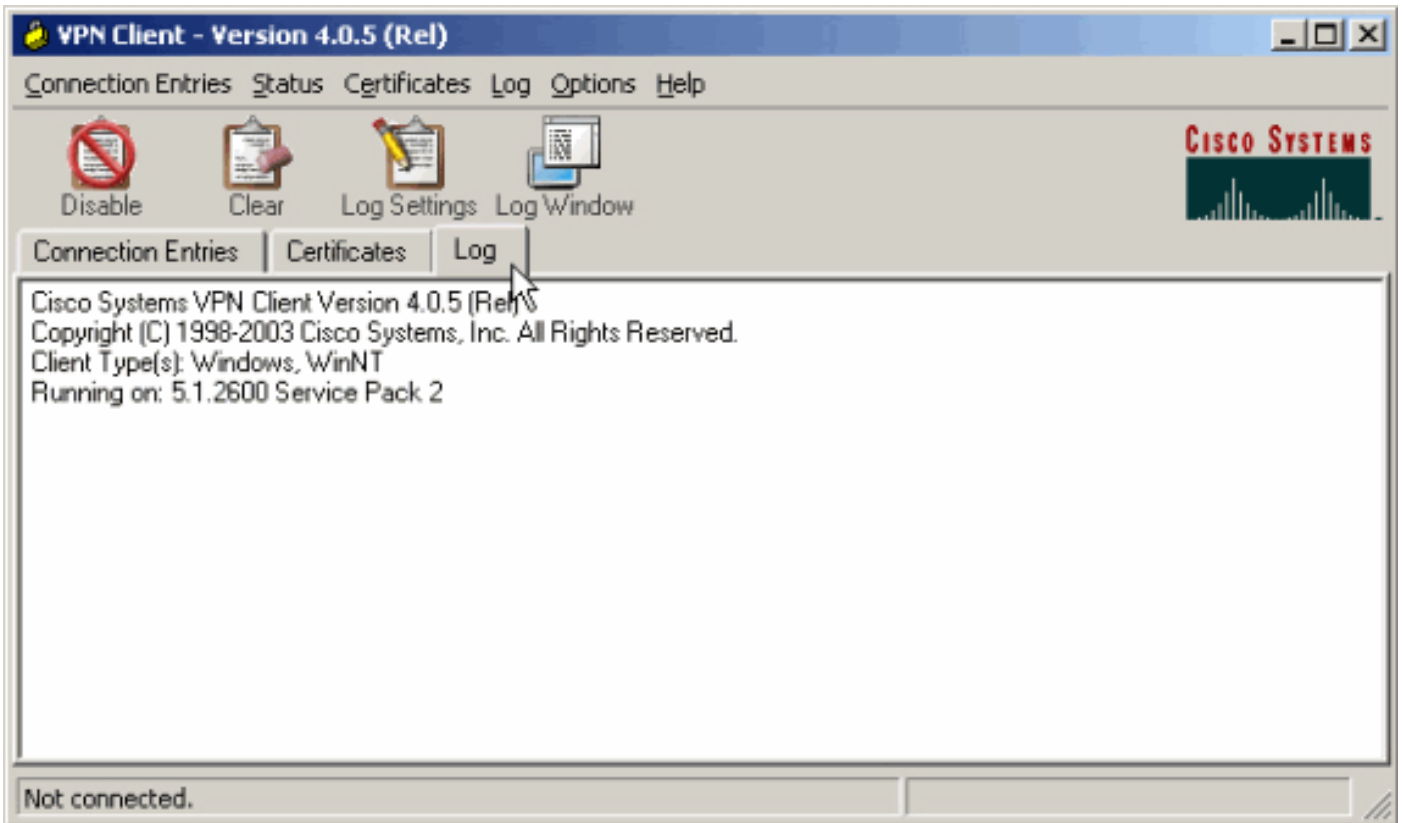


النفق.

[عرض سجل عميل شبكة VPN](#)

عندما يفحص أنت ال VPN زبون سجل، أنت يستطيع حددت ما إذا أو لا المعلمة أن يعين انقسام tunneling يكون

ثبتت. لعرض السجل، انتقل إلى علامة التبويب "السجل" في عميل شبكة VPN. ثم انقر فوق إعدادات السجل لضبط ما تم تسجيله. في هذا المثال، يتم تعيين IKE على 3 - مرتفع بينما يتم تعيين كل 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 07/27/06 14:20:09.532 1
.Attempting to establish a connection with 172.22.1.160

Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a ---!
firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20
14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160 22 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208
07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 26 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version
7.2(1) built by root on Wed 31-May-06 14:45 !--- *Split tunneling is permitted and the remote LAN
is defined.* 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 30 14:20:14.238 07/27/06
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 !--- *Output is supressed*

إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الاتصال

هناك طريقة إضافية لاختبار تكوين عميل شبكة VPN لنفقي منقسم أثناء إنشاء قنوات في ASA هي استخدام الأمر ping في سطر الأوامر في Windows. ال LAN المحلي من ال VPN زبون 24/192.168.0.0 ومضيف آخر حاضر على الشبكة مع عنوان 192.168.0.3.

```
C:\>ping 192.168.0.3
:Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

:Ping statistics for 192.168.0.3
(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
:Approximate round trip times in milli-seconds
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

استكشاف الأخطاء وإصلاحها

تحديد باستخدام عدد الإدخالات في قائمة التحكم في الوصول (ACL) إلى النفق المقسم

هناك تقييد يحتوي على عدد الإدخالات في قائمة التحكم بالوصول (ACL) المستخدمة للنفق المقسم. يوصى بعدم استخدام أكثر من 50 إلى 60 إدخال ACE للحصول على وظائف مرضية. يوصى بتنفيذ ميزة تقسيم الشبكة إلى شبكات فرعية لتغطية نطاق من عناوين IP.

معلومات ذات صلة

- [PIX/ASA 7.x كخادم VPN بعيد باستخدام مثال تكوين ASDM](#)
- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [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 ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي 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 د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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