تكوين الاتصال النفقي المنقسم لعملاء VPN على ASA

المحتويات

المقدمة

يصف هذا وثيقة العملية أن يسمح VPN زبون أن ينفذ إلى الإنترنت أثناء tunneling في cisco ASA 5500 sery أمن جهاز.

المتطلبات الأساسية

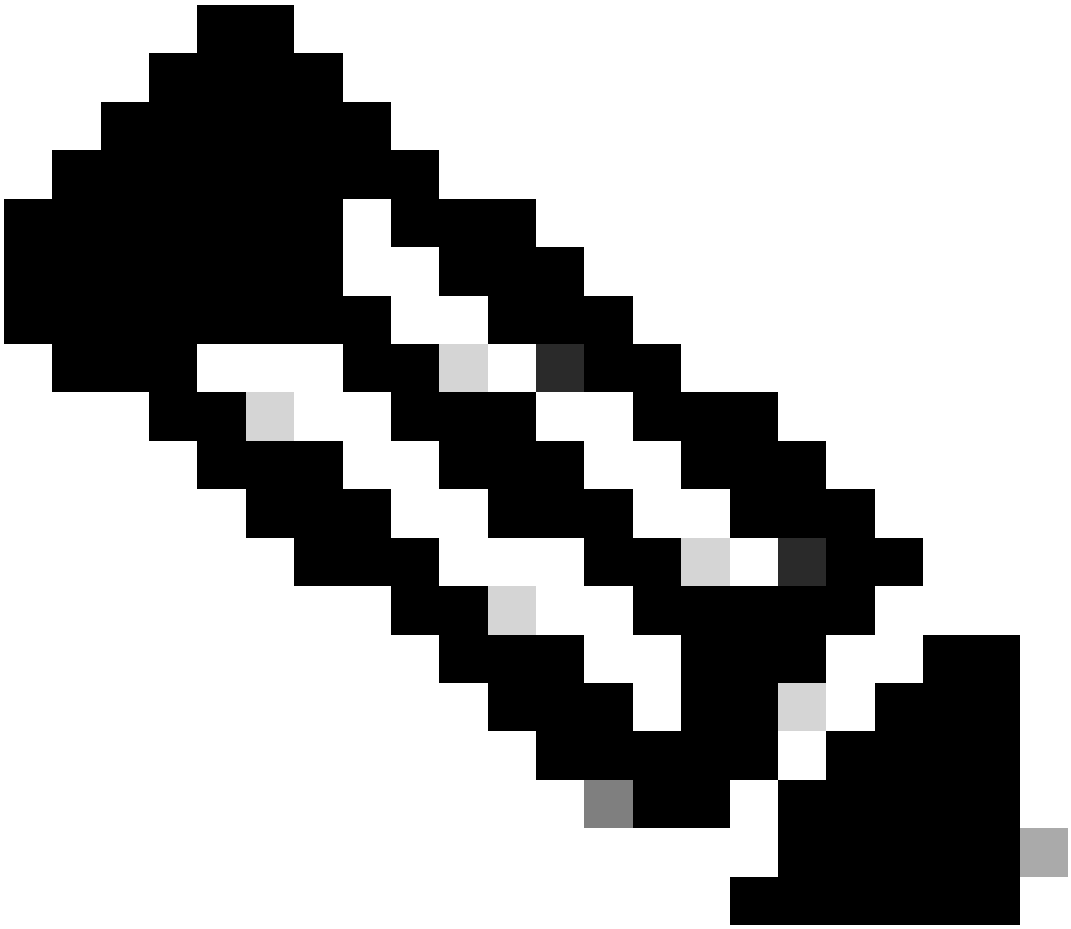
المتطلبات

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

المكونات المستخدمة

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

- برنامج جهاز الأمان Cisco ASA 5500 Series Security Appliance Software، الإصدار 7.x والإصدارات الأحدث
- Cisco Systems VPN Client، الإصدار 4.0.5
- مدير أجهزة حلول الأمان المعدلة (ASDM)

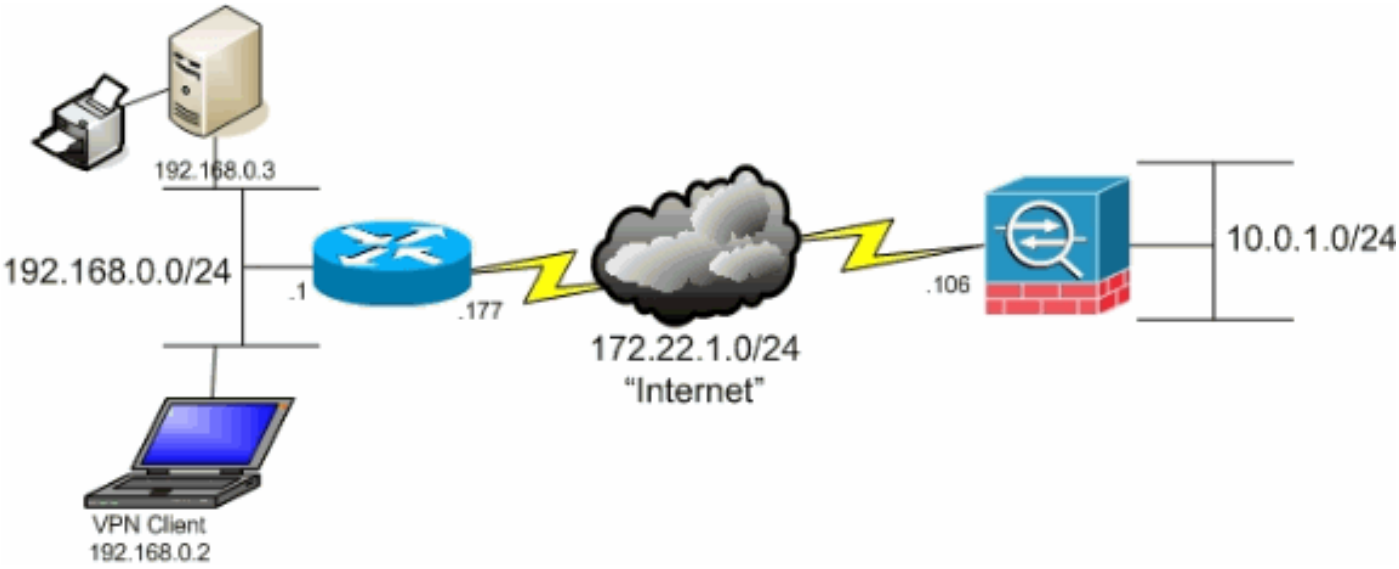


ملاحظة: يحتوي هذه المستند أيضا على تكوين PIX 6.x CLI المتوافق مع عميل Cisco VPN 3.x.

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

الرسم التخطيطي للشبكة

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



الرسم التخطيطي للشبكة

المنتجات ذات الصلة

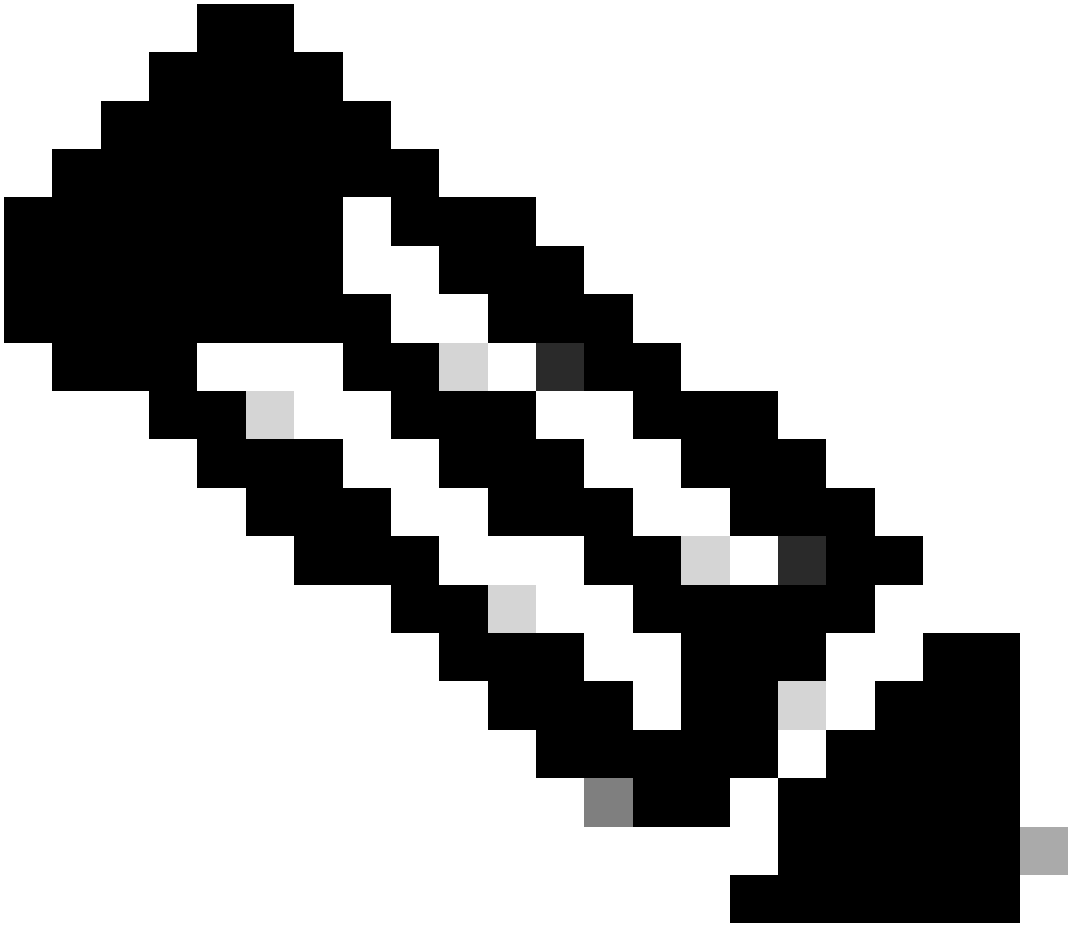
كما يمكن إستخدام هذا التكوين مع برنامج جهاز الأمان Cisco PIX 500 Series Security Appliance Software، الإصدار 7.x.

الاصطلاحات

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

معلومات أساسية

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 الاتصال النفقي الكامل التكوين الأكثر أمانا لأنه لا يمكن الوصول المتزامن للجهاز إلى كل من الإنترنت وشبكة LAN الخاصة بالشركات. يسمح حل توفيقي 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.

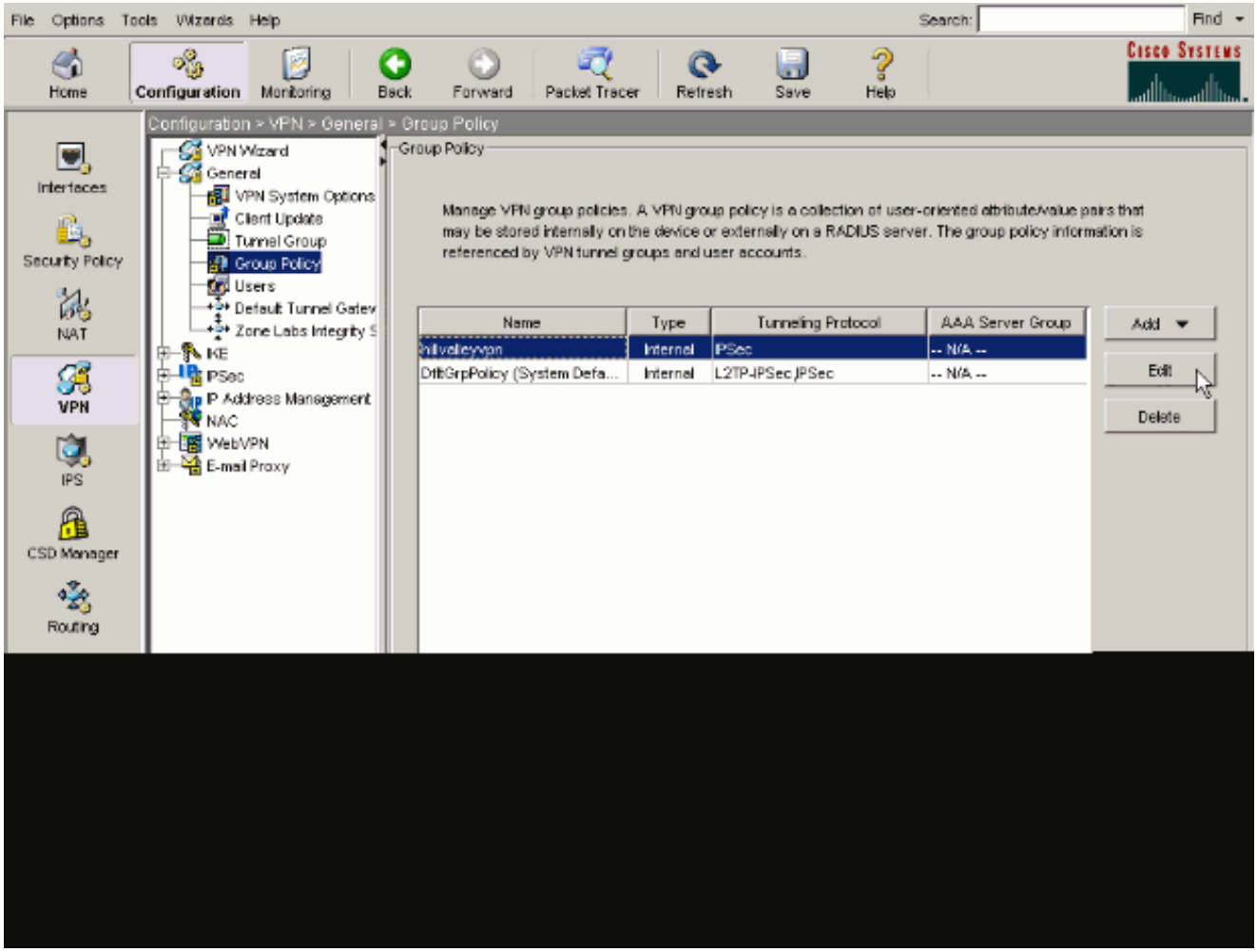
في سيناريو أساسي VPN Client إلى ASA، يتم تشفير جميع حركات مرور البيانات من عميل شبكة VPN وإرسالها إلى ASA بغض النظر عن الوجهة الخاصة بها. استنادا إلى التكوين الخاص بك وعدد المستخدمين المدعومين، يمكن أن تصبح عملية الإعداد هذه ذات نطاق ترددي كبير. يمكن أن يعمل تقسيم الاتصال النفقي على تخفيف هذه المشكلة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

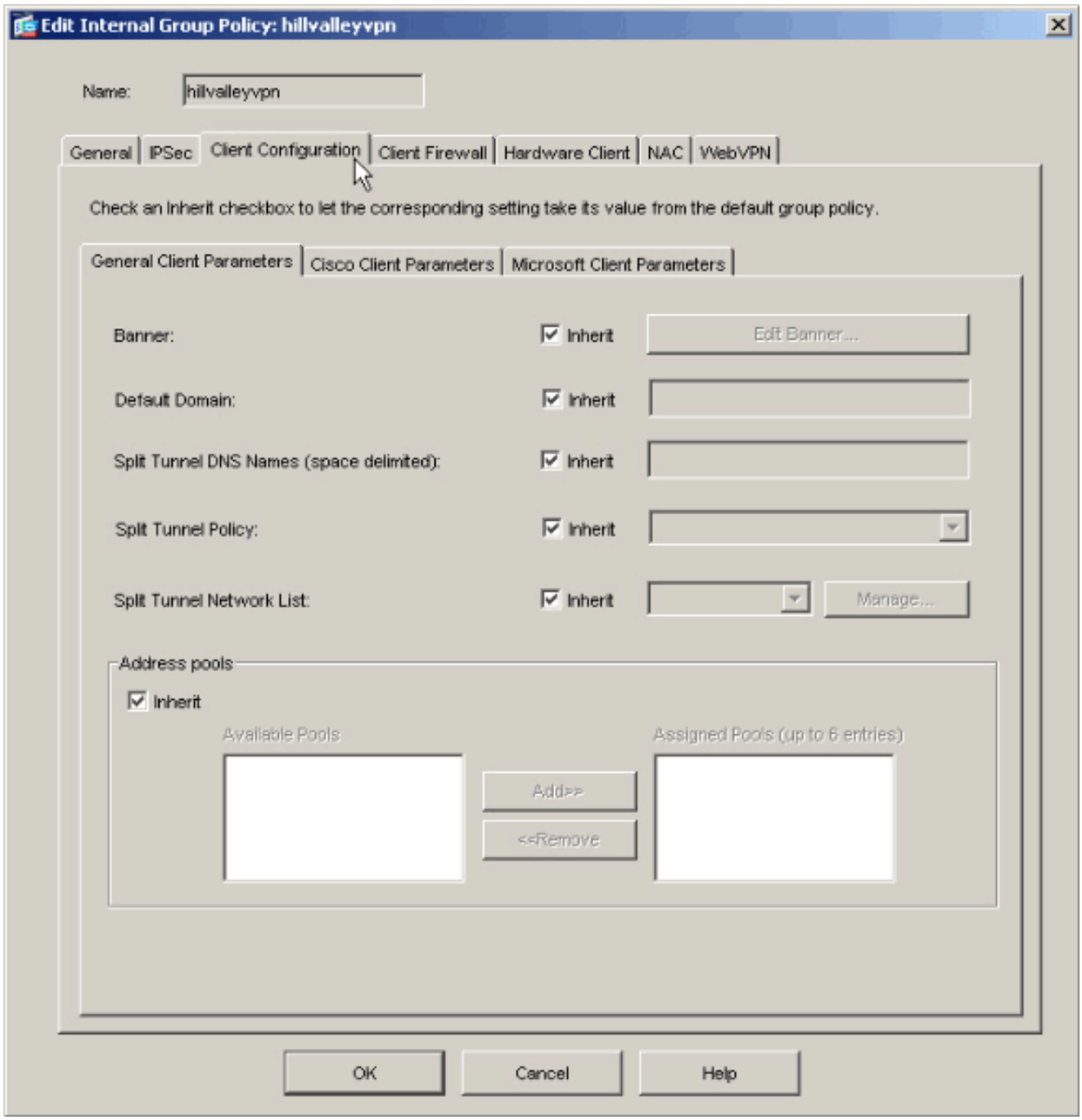
تكوين ASA 7.x باستخدام Adaptive Security Device Manager (ASDM) 5.x

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

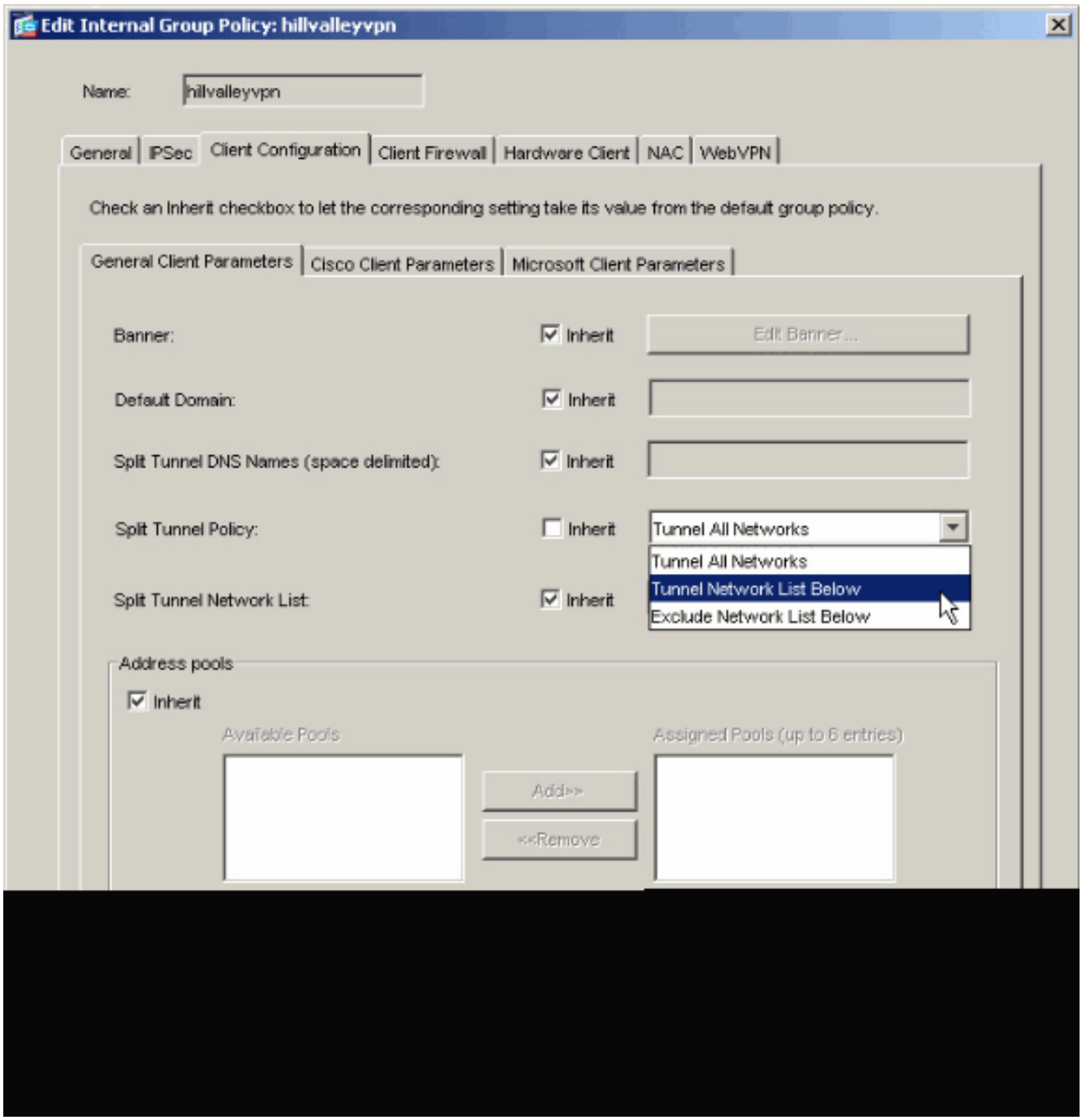
1. أخترت تشكيل>VPN>عام>مجموعة سياسة وحدد المجموعة سياسة أن أنت تريد أن يمكن محلي منفذ في. ثم انقر فوق تحرير .



2. انتقل إلى علامة التبويب تكوين العميل.

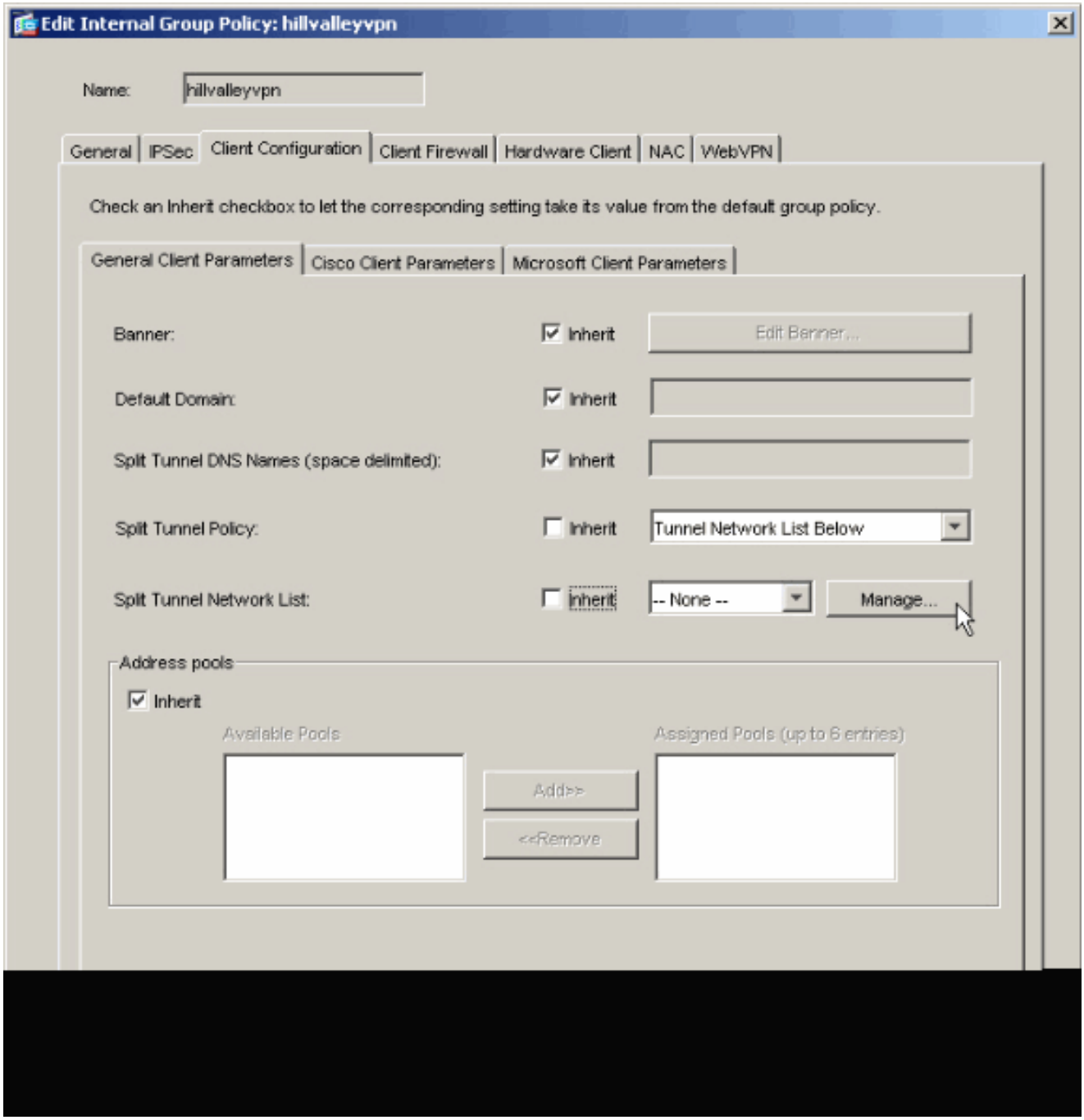


3. قم بإلغاء تحديد مربع Inherit لنهج النفق المقسم واختر Tunnel Network List Below ..



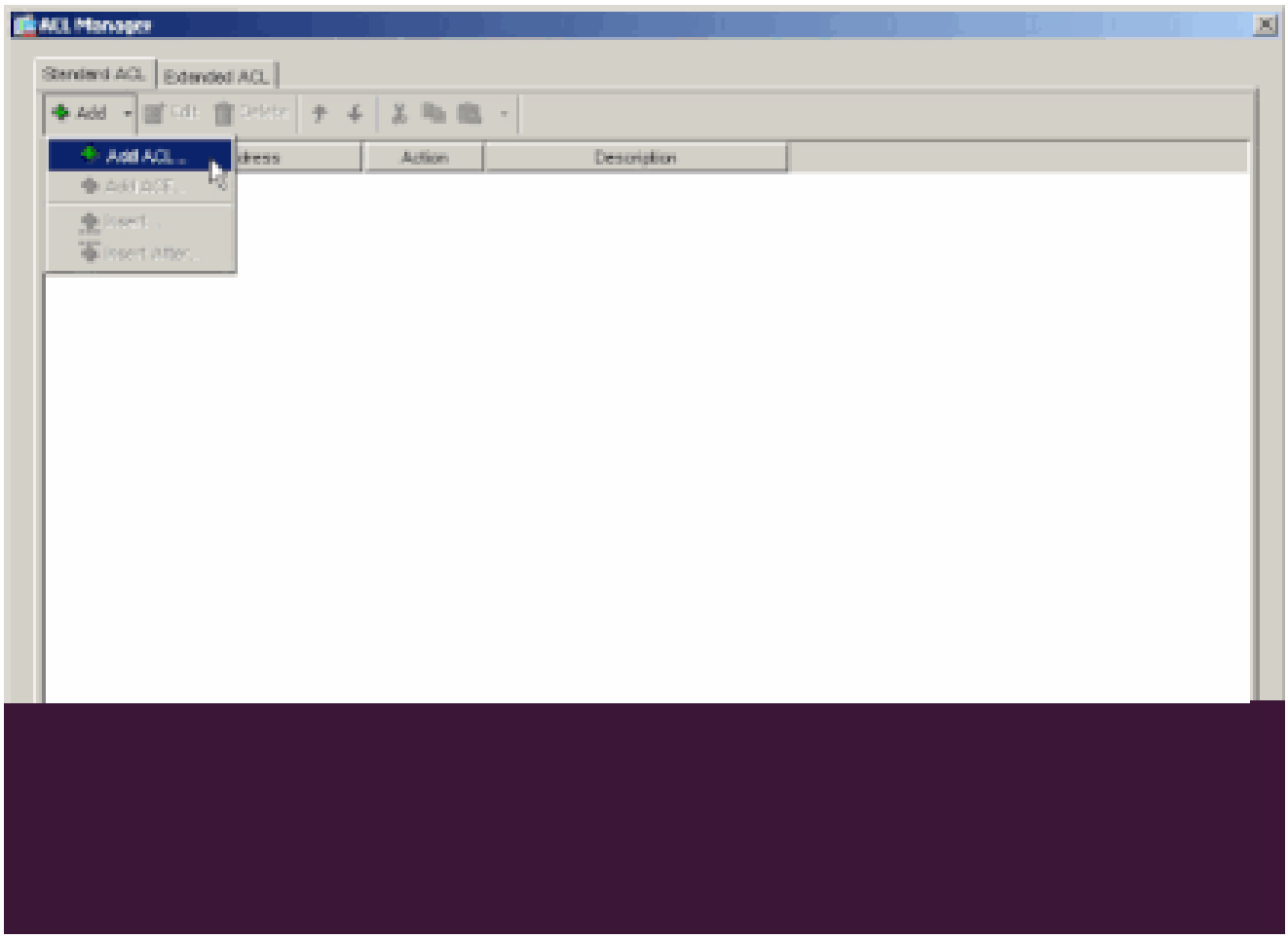
•

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



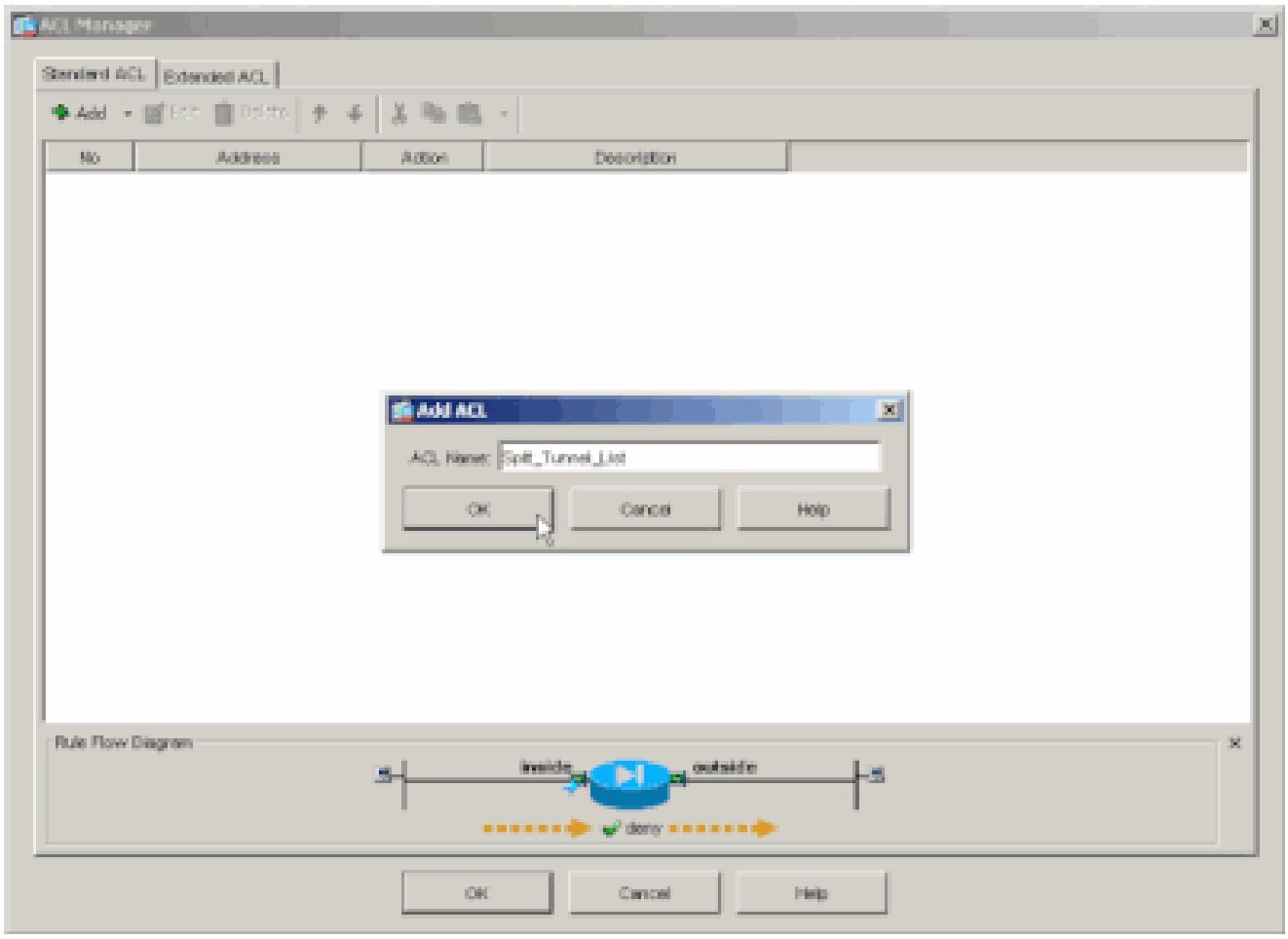
•

ضمن إدارة قائمة التحكم بالوصول (ACL)، أختر إضافة > إضافة قائمة التحكم بالوصول (ACL)... لإنشاء قائمة وصول جديدة.



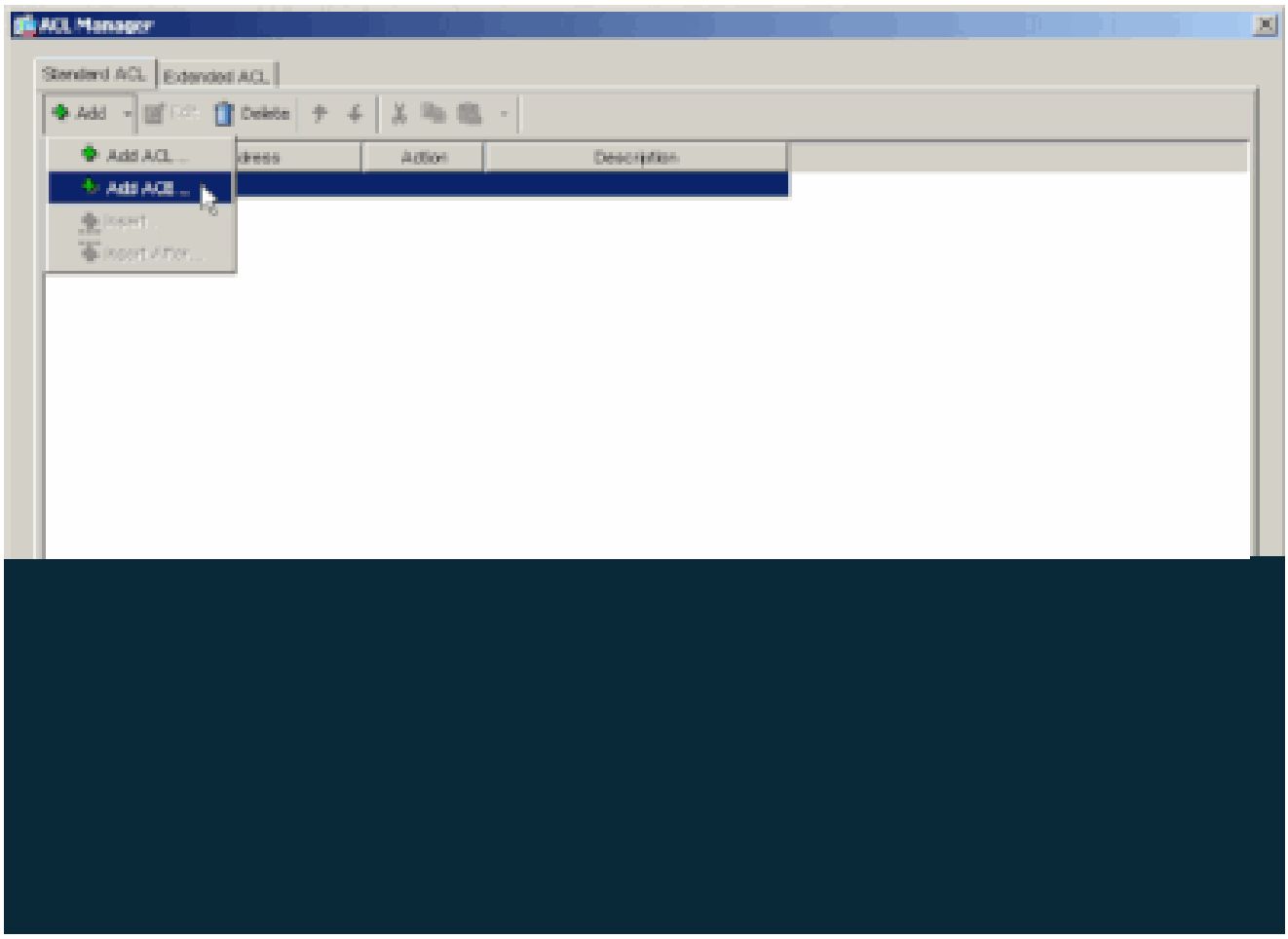
•

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



•

بمجرد إنشاء قائمة التحكم بالوصول (ACL)، أختر **إضافة > إضافة ACE...** لإضافة إدخال التحكم في الوصول (ACE).



•

عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 10.0.1.0/24.

a.

أختر **تصريح** .

b.

أختر عنوان IP **10.0.1.0**

c.

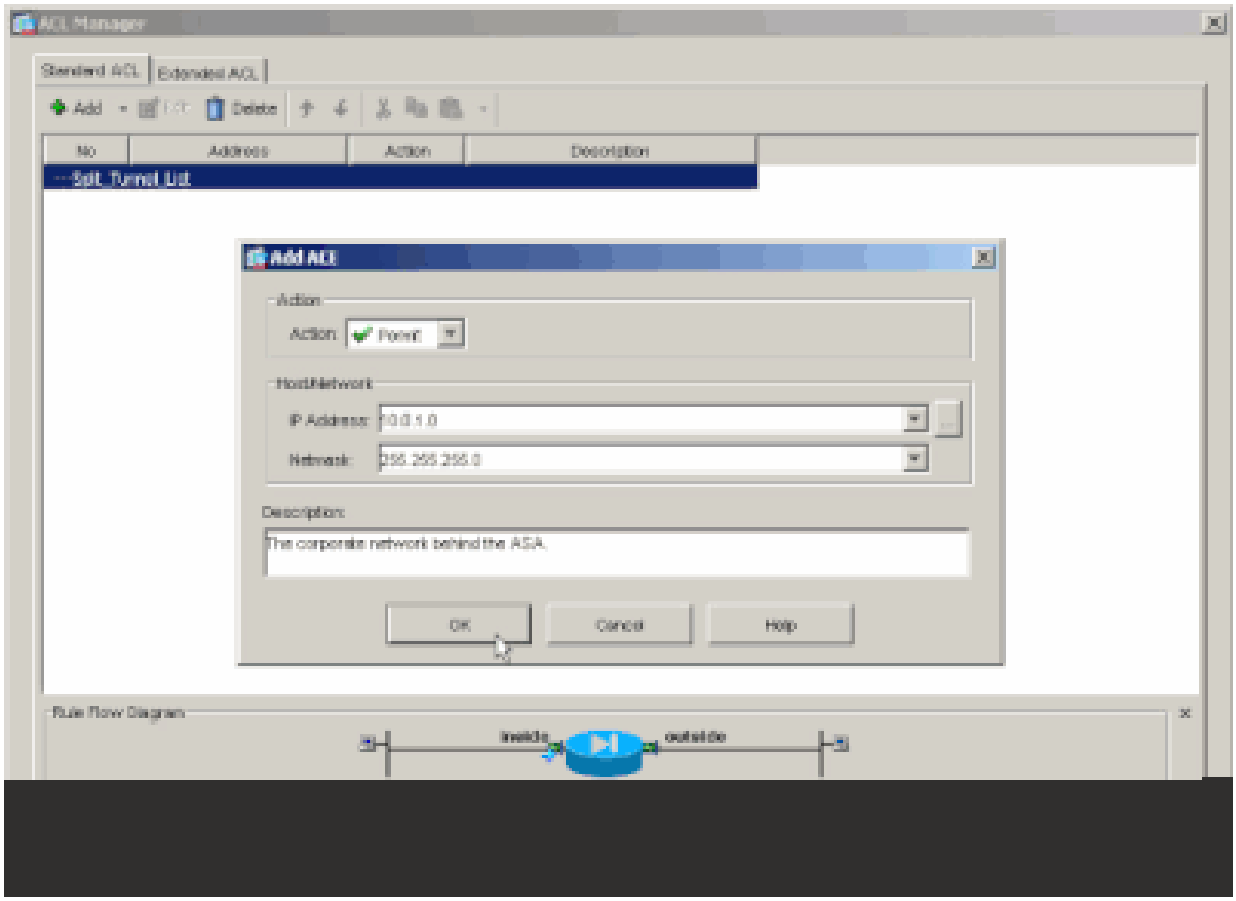
أختر قناع شبكة من **255.255.255.0**.

d.

(اختياري) قم بتوفير وصف.

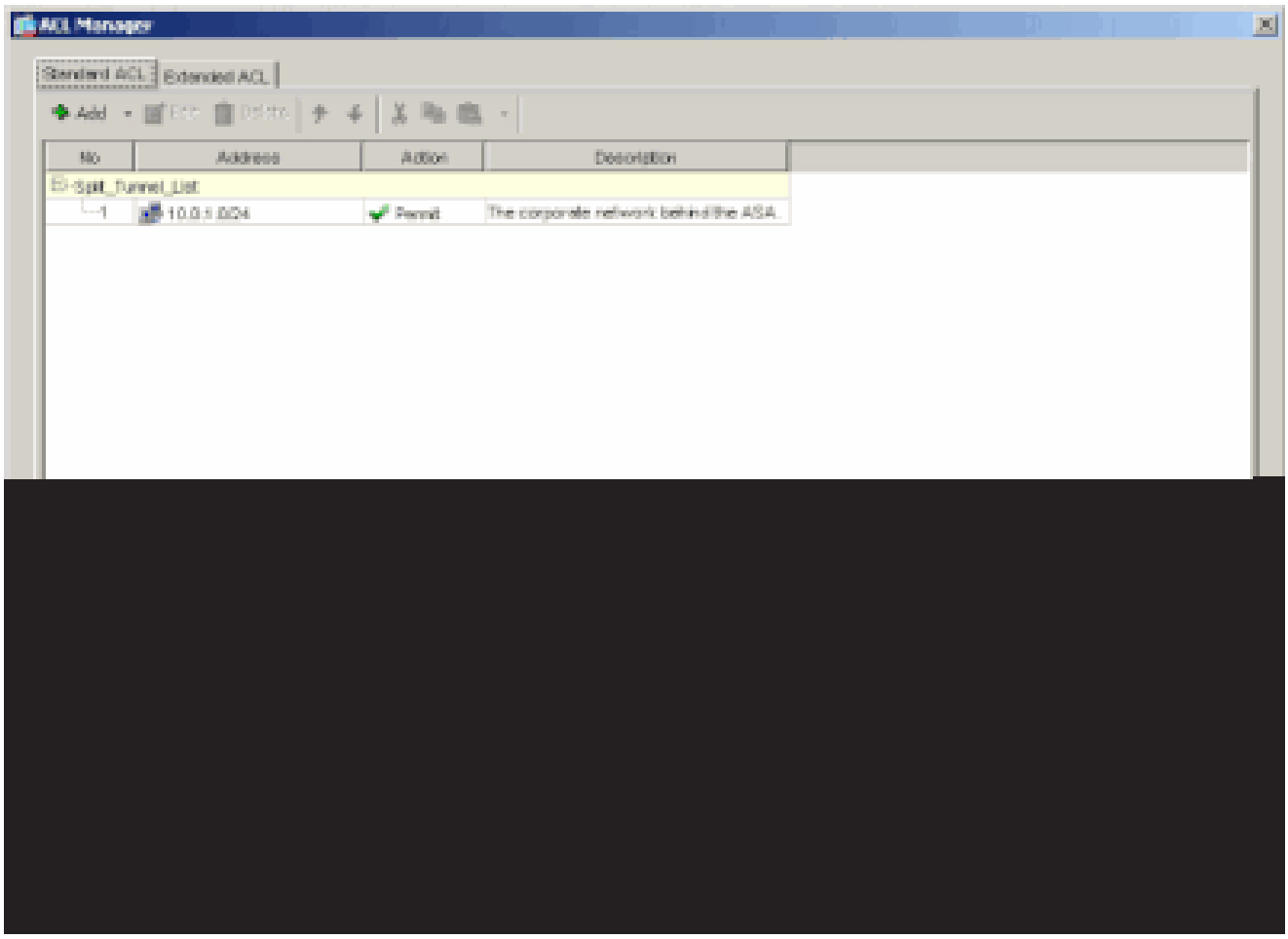
e.

طقطقة **ok**.



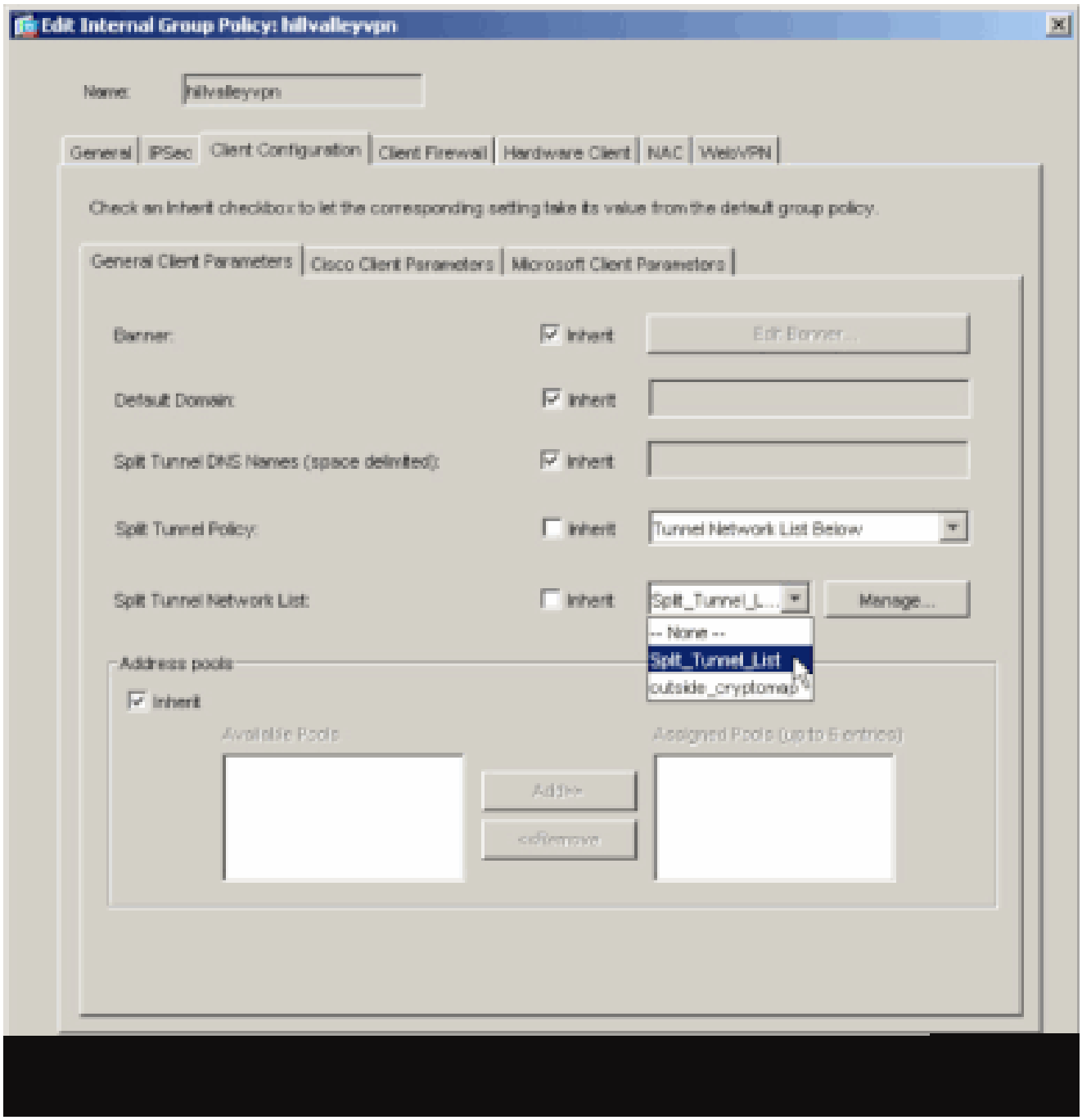
•

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



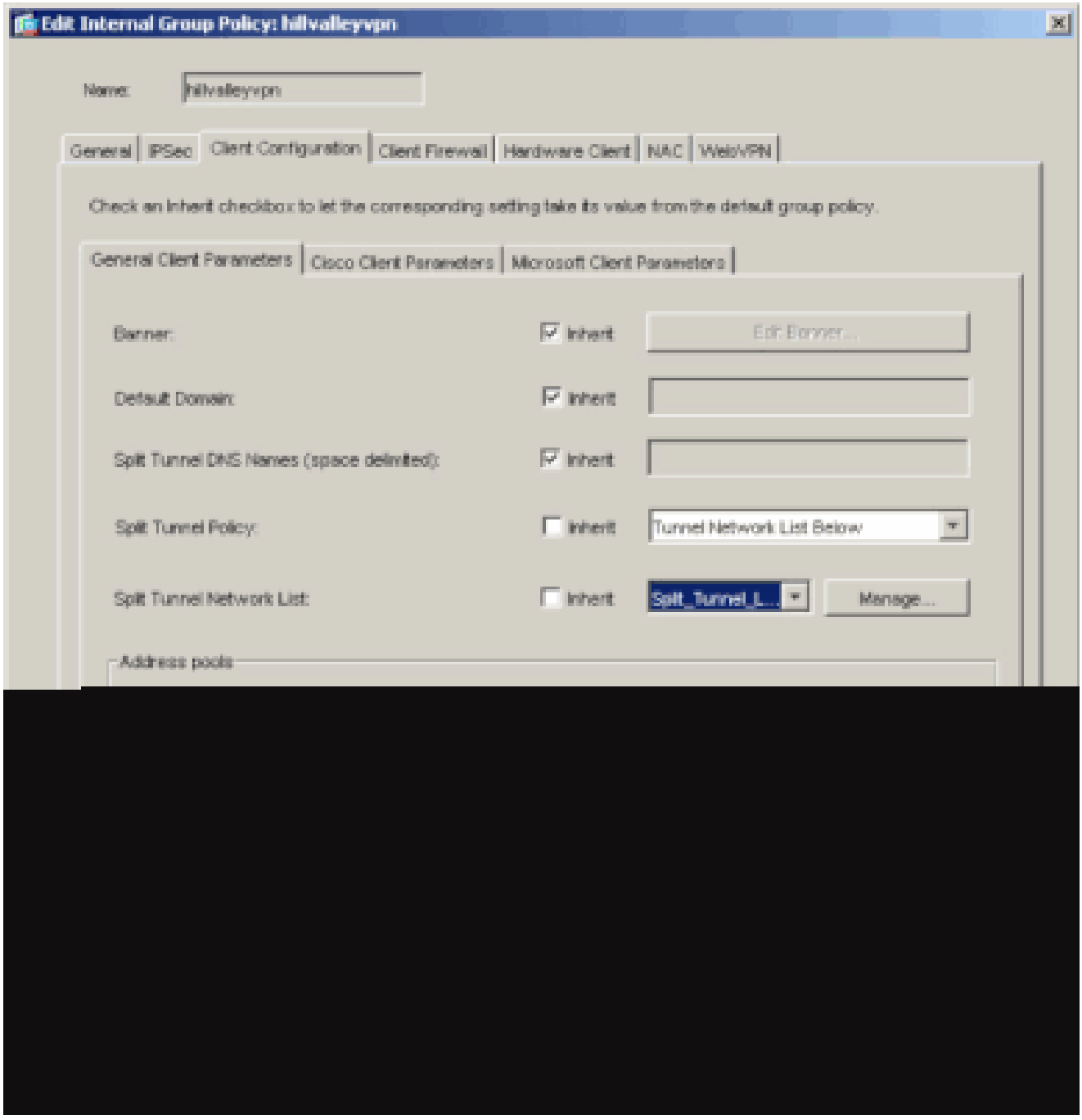
•

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



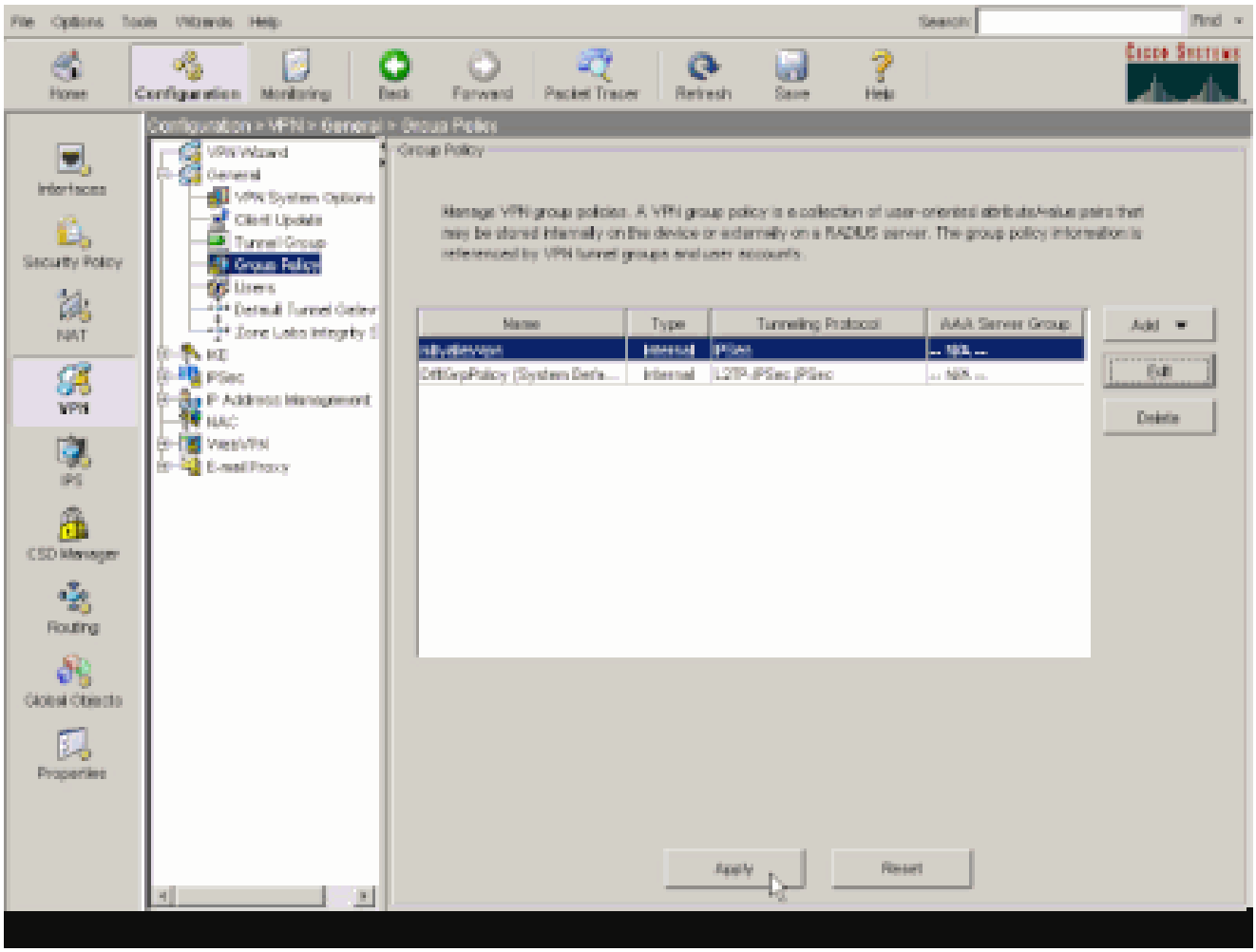
•

انقر فوق موافق للعودة إلى تكوين "نهج المجموعة".



•

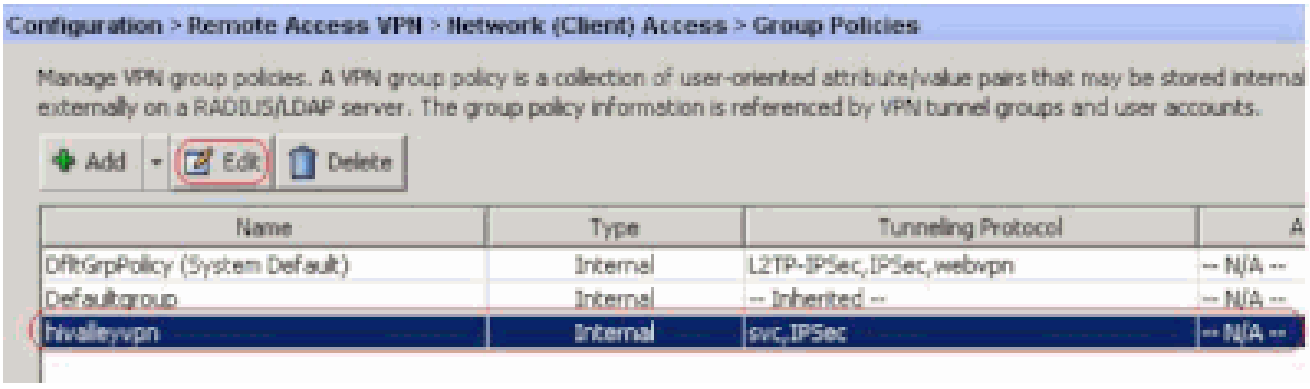
طقطقة يطبق وبعد ذلك يرسل (إن يتطلب) in order to أرسلت الأمر إلى ال ASA.



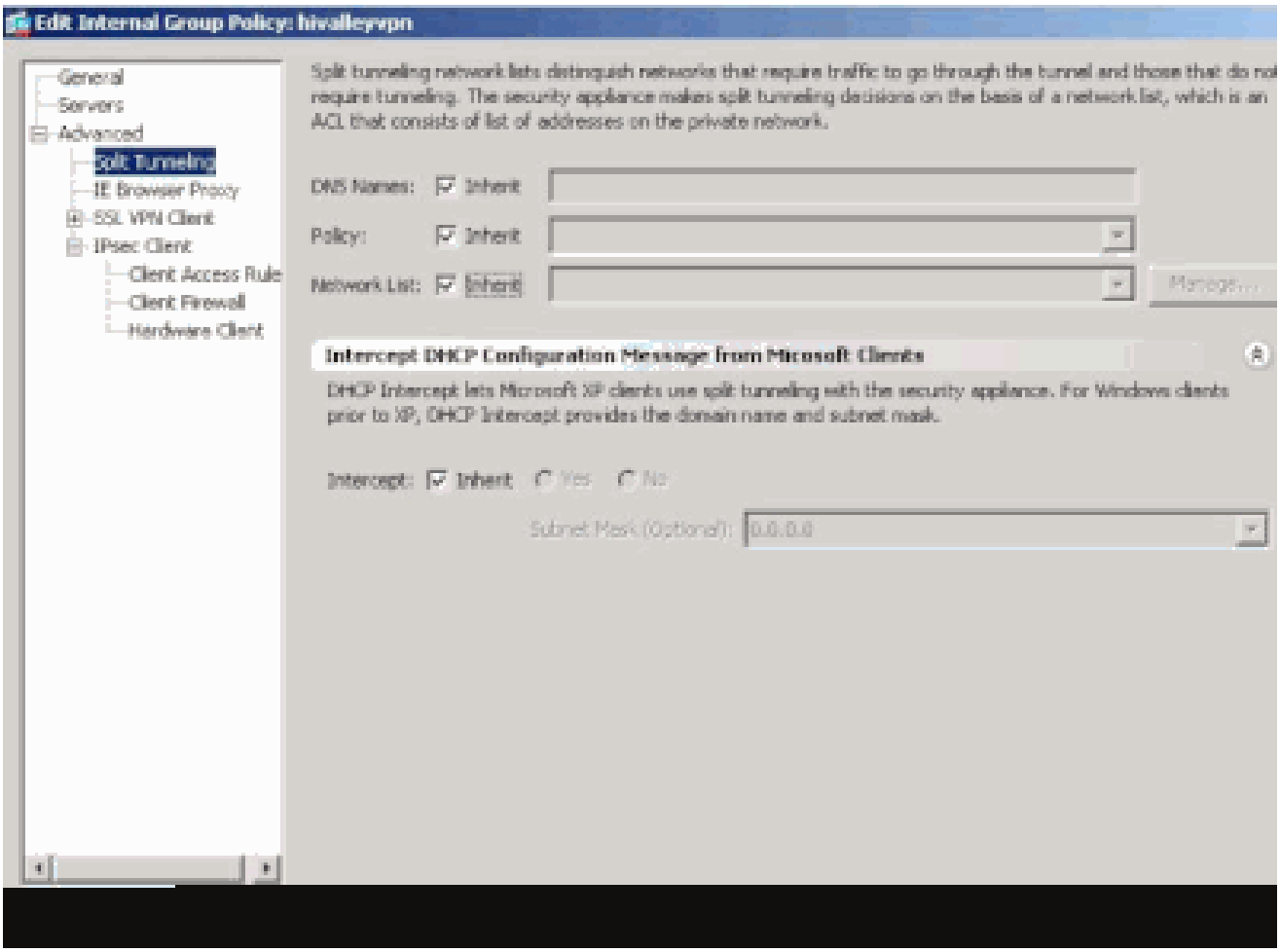
تكوين ASA 8.x مع ASDM 6.x

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

- أخترت تشكيلوصول عن بعد VPN>شبكة (زبون) منفذمجموعة نهج، واخترت المجموعة سياسة حيث أنت تريد أن يمكن محلي وصول. ثم انقر فوق تحرير.

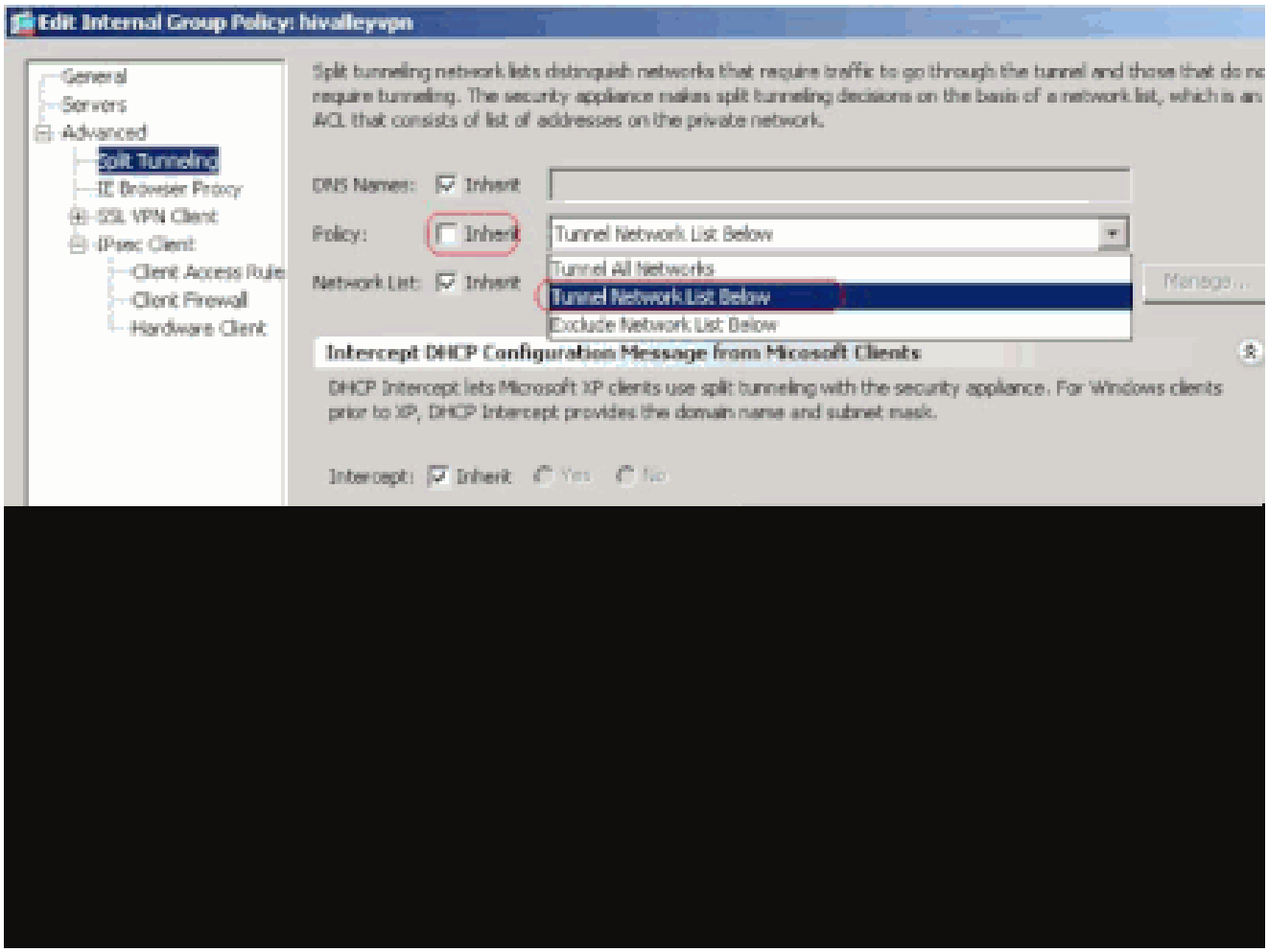


- طقطقة تقسيم **tunneling**.



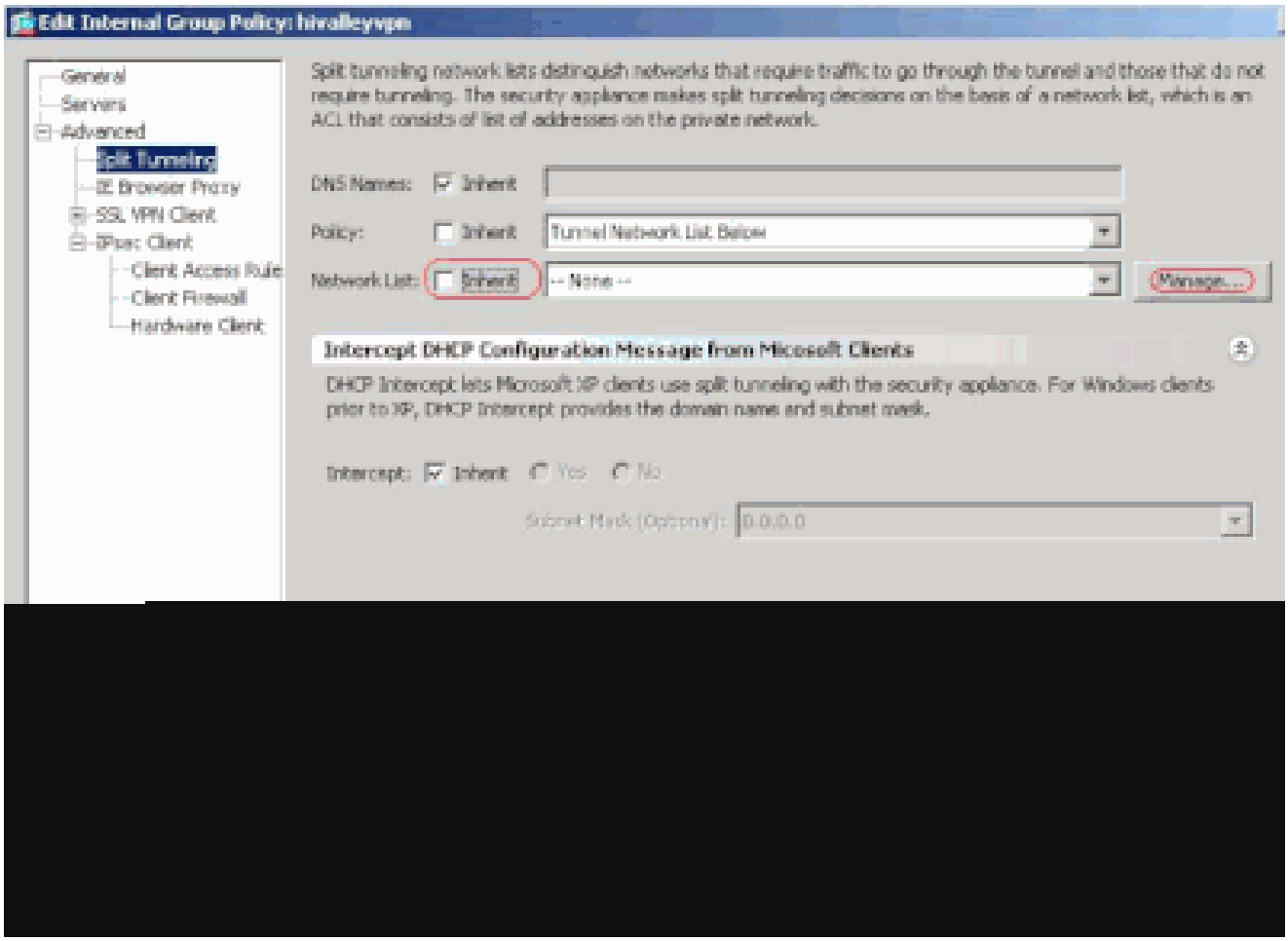
•

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



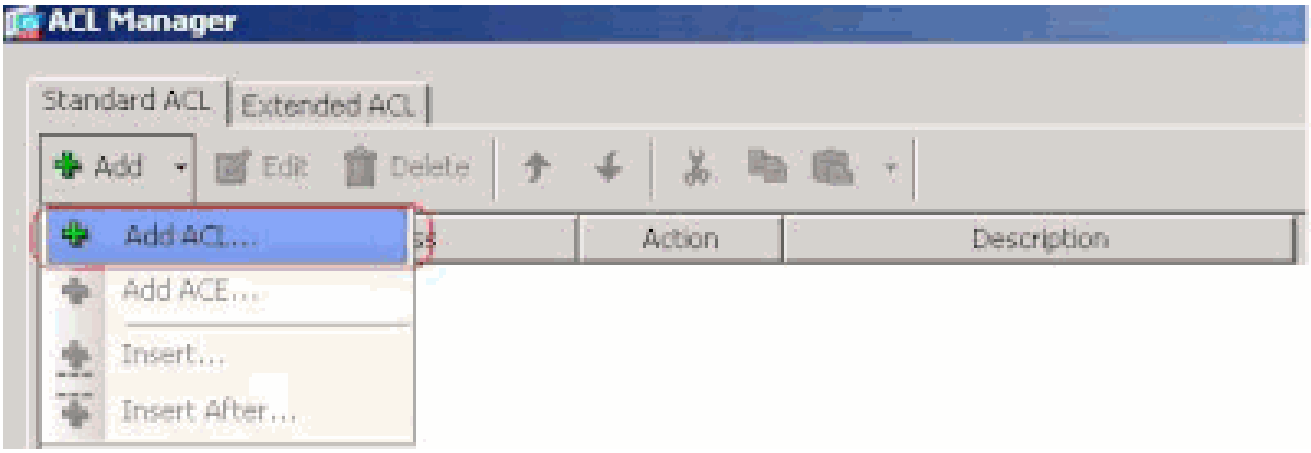
•

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



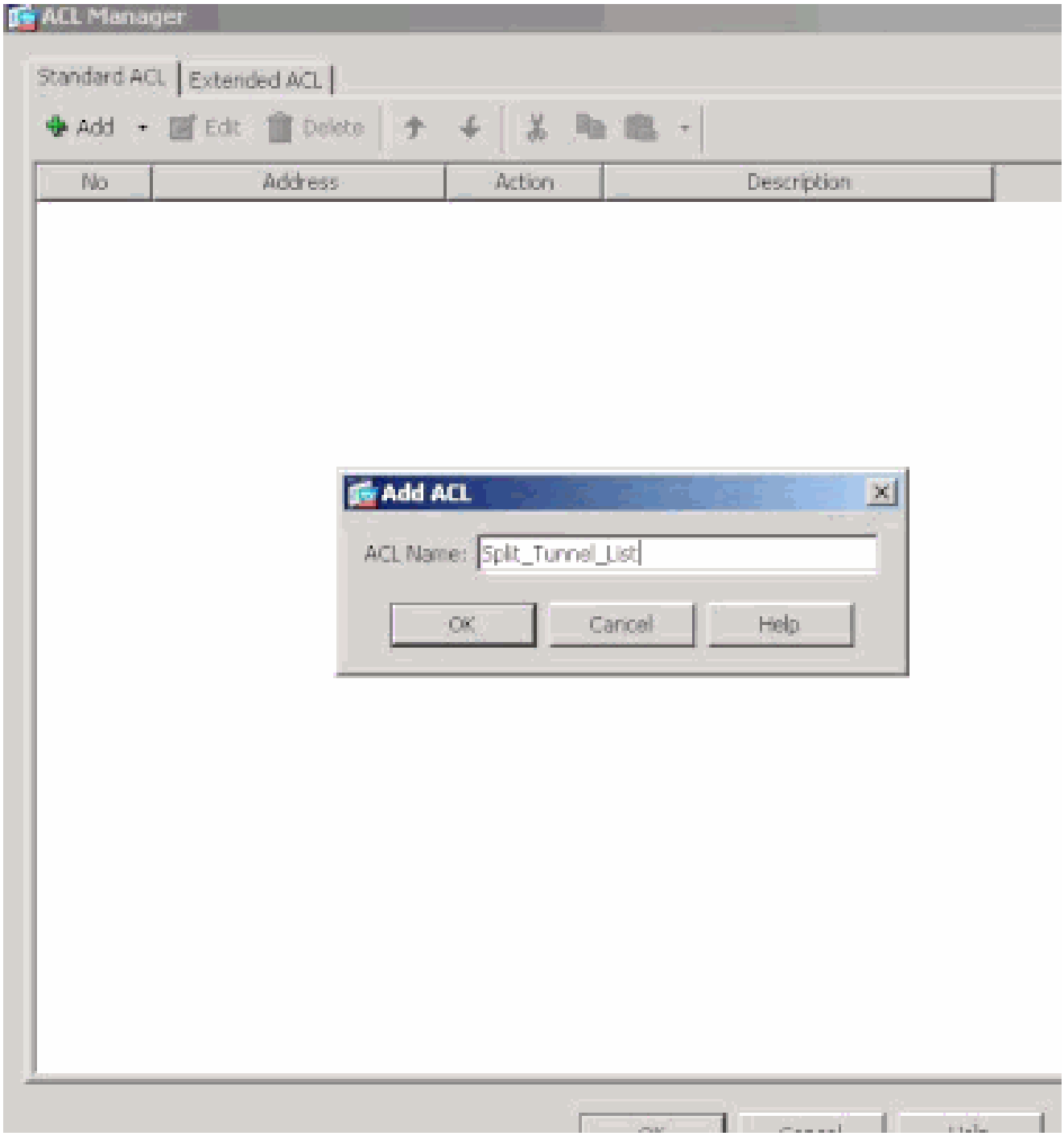
•

ضمن إدارة قائمة التحكم بالوصول (ACL)، أختر إضافة > إضافة قائمة التحكم بالوصول (ACL)... لإنشاء قائمة وصول جديدة.

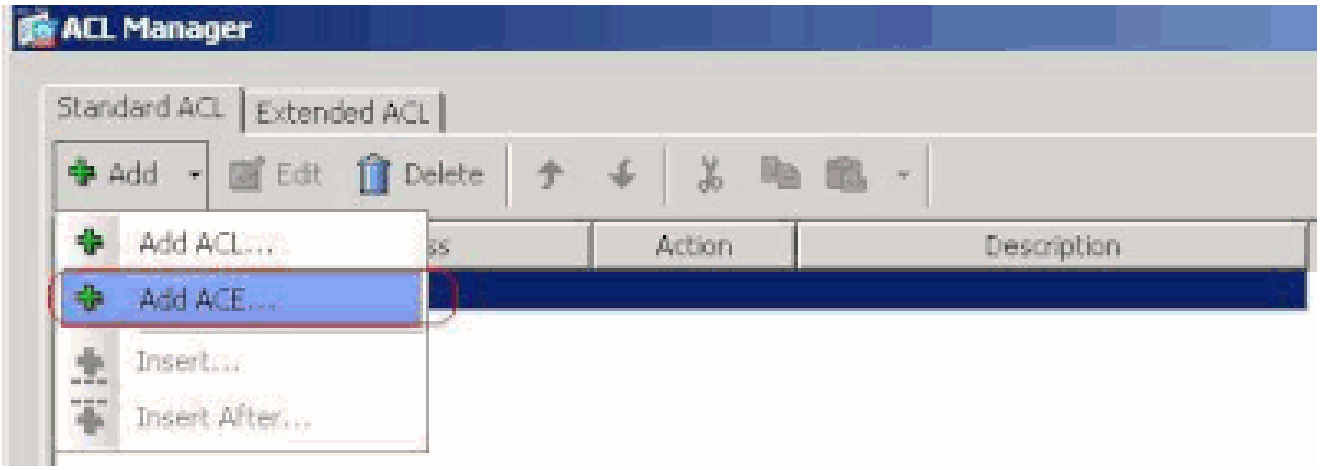


•

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



- بمجرد إنشاء قائمة التحكم في الوصول، أختر **إضافة > إضافة ACE...** لإضافة إدخال التحكم في الوصول (ACE).



•

عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 10.0.1.0/24.

a.

طقطقت ال يسمح لاسلكي زر.

b.

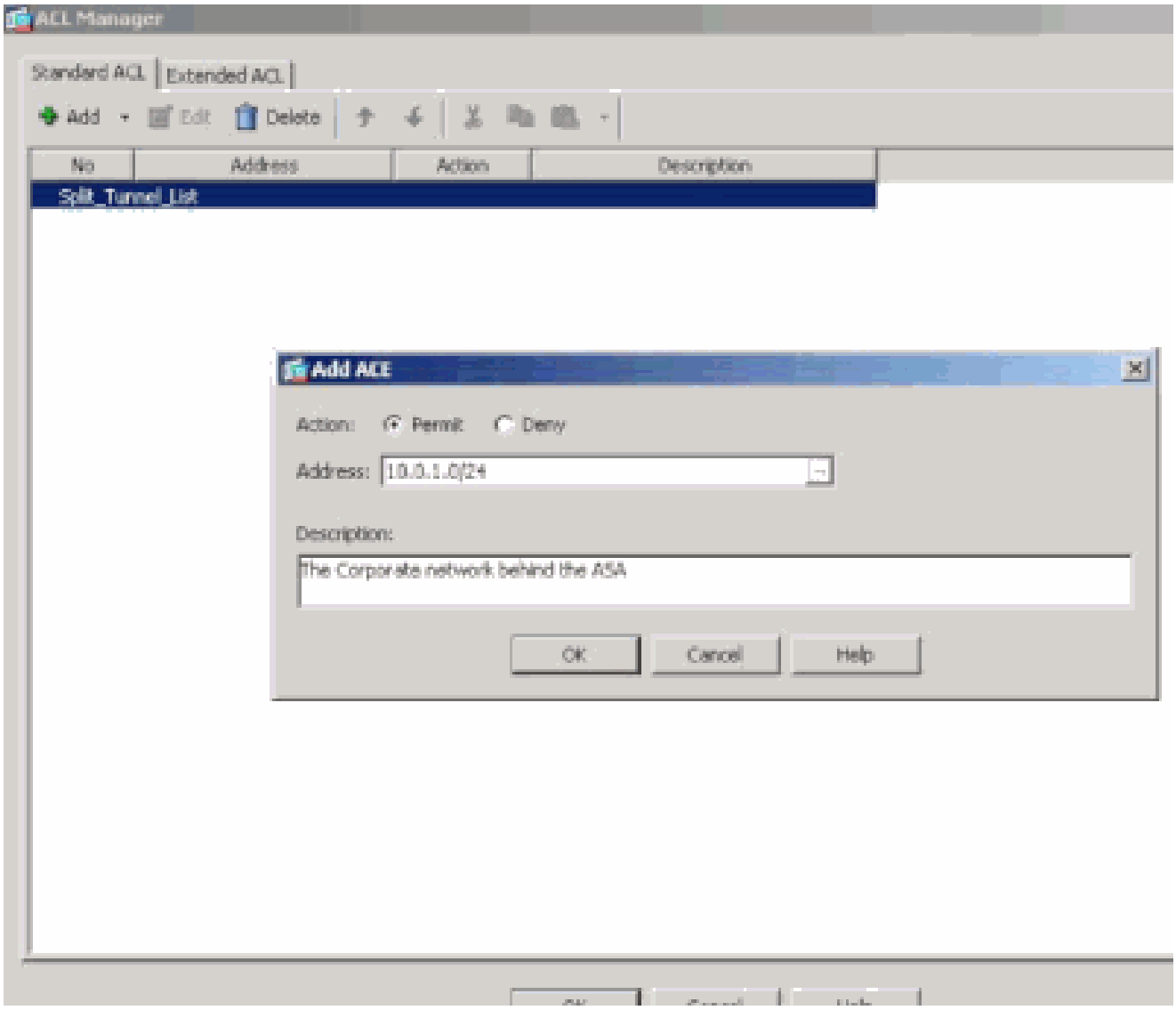
أختر عنوان الشبكة باستخدام القناع **10.0.1.0/24**.

c.

(إختياري) قم بتوفير وصف.

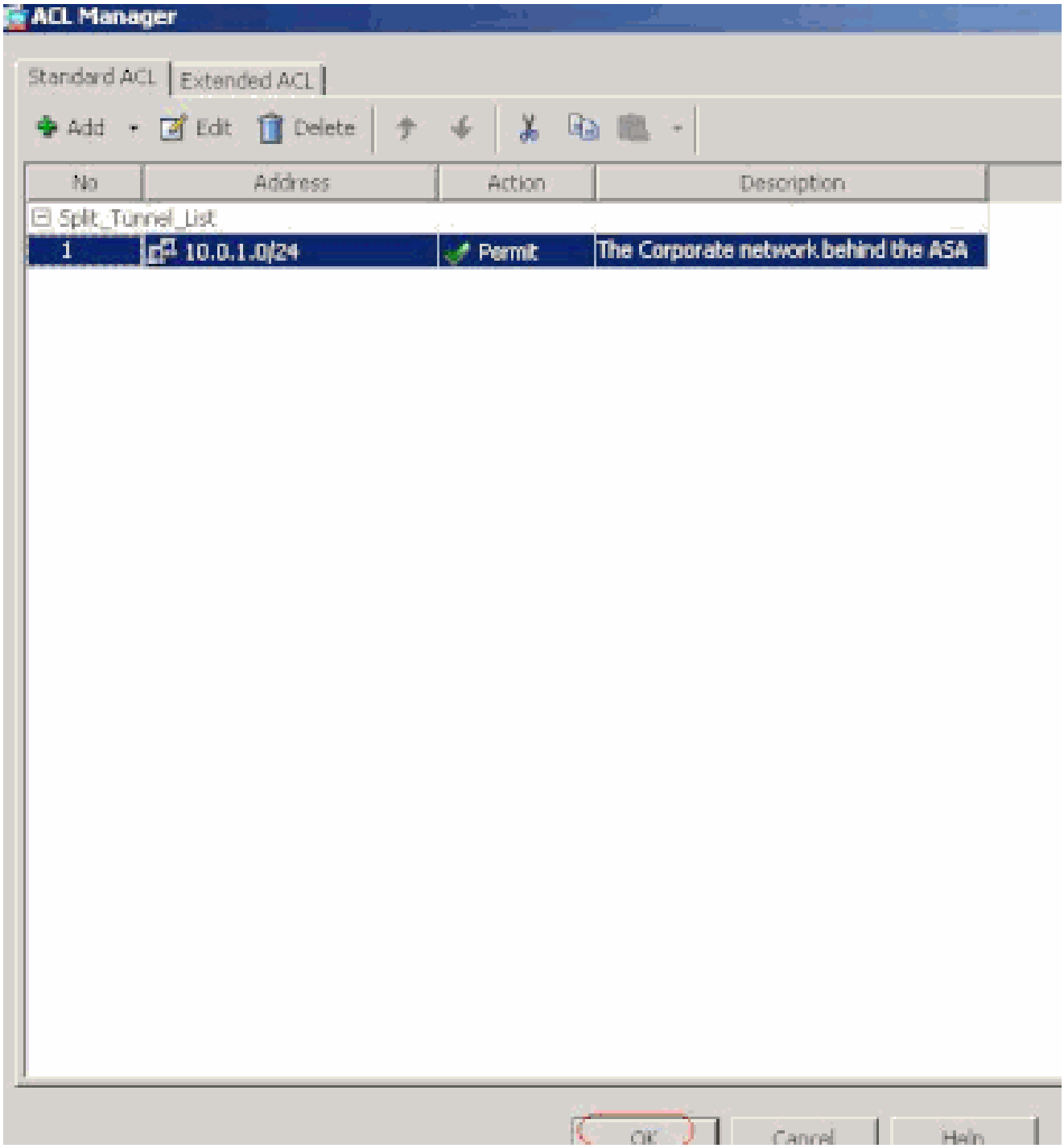
d.

وانقر فوق OK.



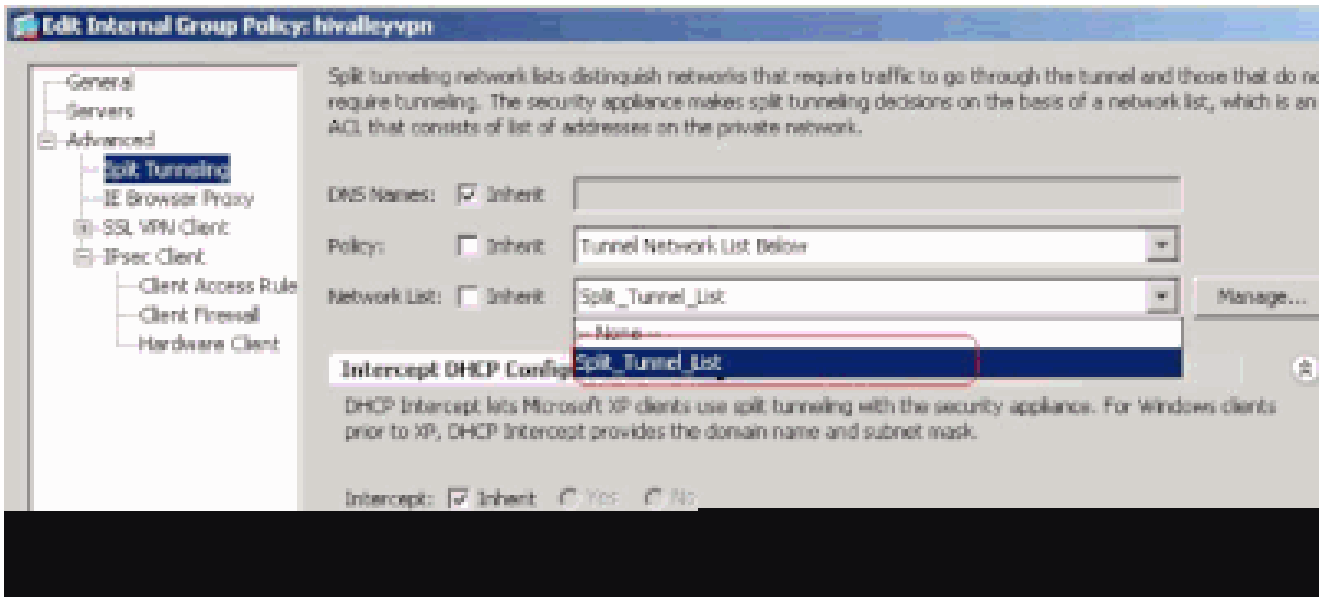
•

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



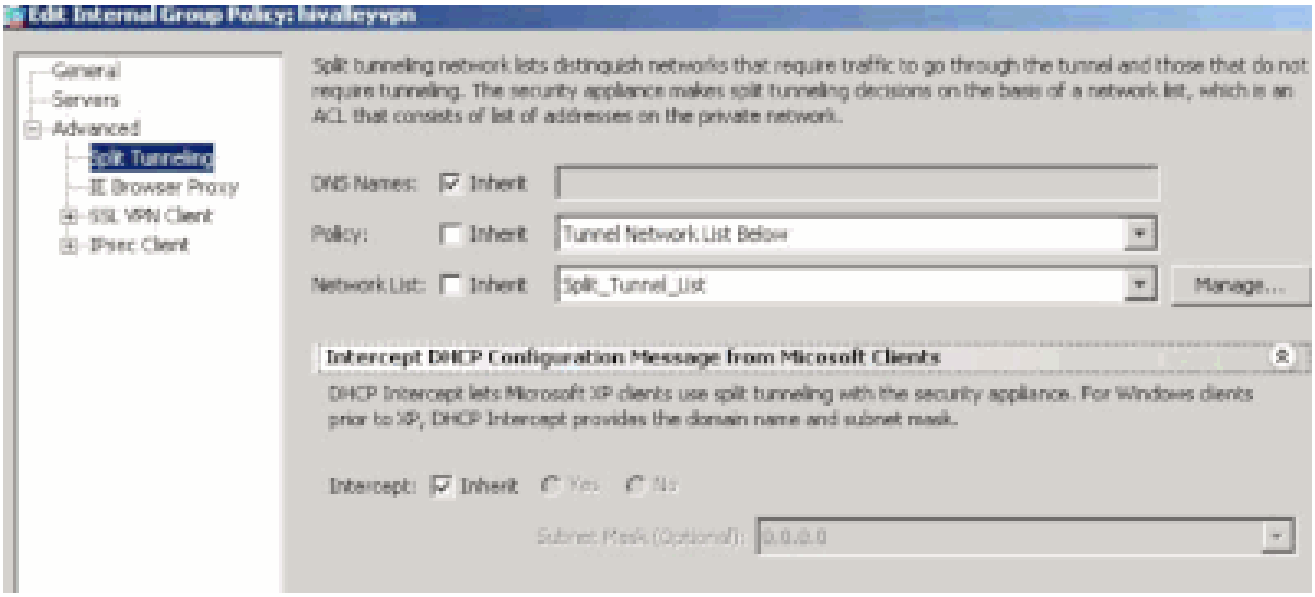
•

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



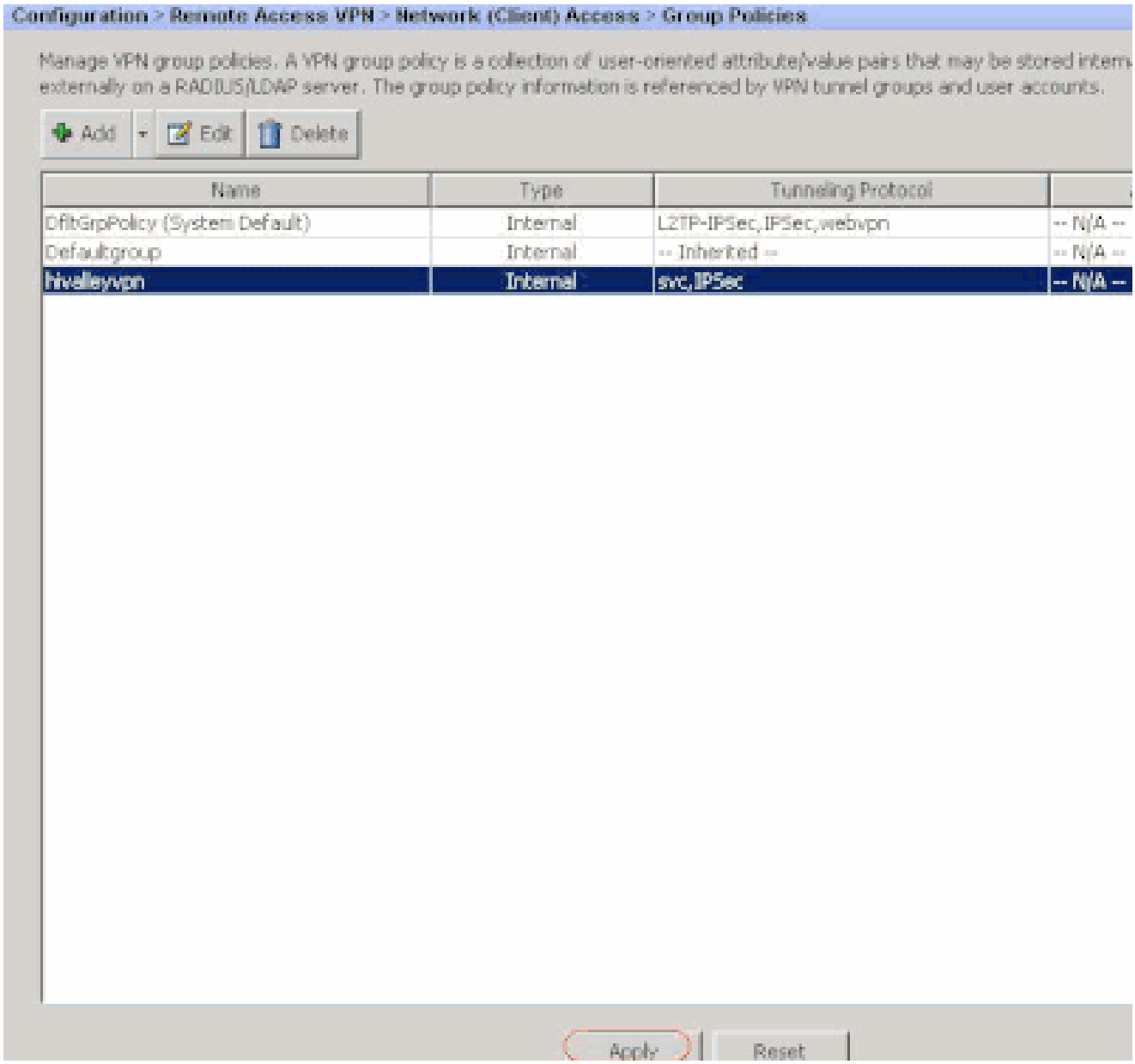
•

انقر فوق موافق للعودة إلى تكوين "نهج المجموعة".



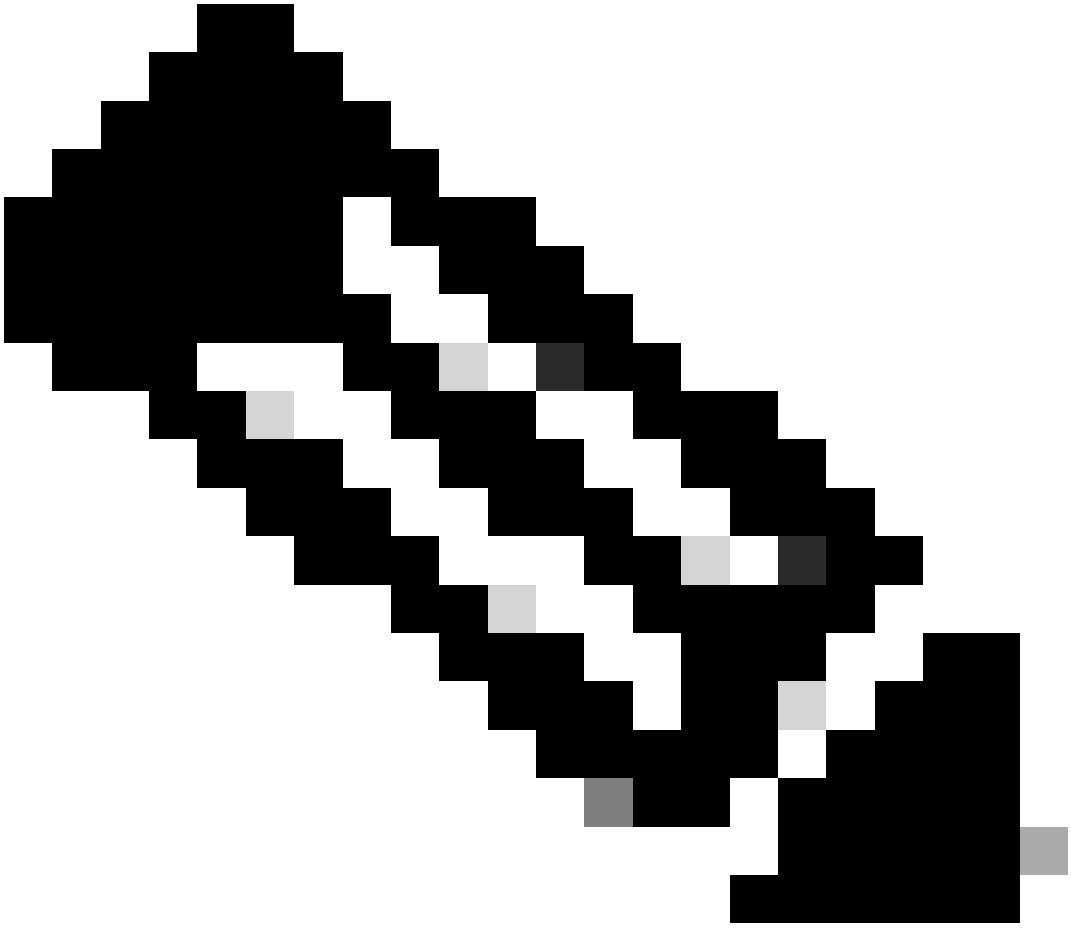
•

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



تكوين ASA 7.x والإصدارات الأحدث عبر CLI

بدلا من إستخدام ASDM، أنت يستطيع أتمت هذه steps في ال ASA CLI in order to سمحت انقسام tunneling على ال ASA:



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

-

ادخل إلى وضع التكوين.

```
<#root>

ciscoasa>
```

```
enable
```

```
Password: ********
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

- قم بإنشاء قائمة الوصول التي تعرف الشبكة خلف ASA.

```
<#root>

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
```

- أدخل وضع تكوين "نهج المجموعة" للنهج الذي ترغب في تعديله.

```
<#root>
```

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

- حدد نهج نفق التقسيم. في هذه الحالة، يتم تحديد النهج.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

- حدد قائمة الوصول إلى النفق المقسم. في هذه الحالة، تكون القائمة هي **SPLIT_TUNNEL_LIST**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

- قم بإصدار هذا الأمر:

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

- إقران نهج المجموعة بمجموعة النفق

<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

- خرجت الإثنان تشكيل أسلوب.

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

```
exit
```

```
ciscoasa#
```

- احفظ التكوين إلى ذاكرة الوصول العشوائي غير المتطايرة (NVRAM) واضغط **Enter** عند طلبها لتحديد اسم الملف المصدر.

```
<#root>

ciscoasa#

copy running-config startup-config


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

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

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

أكمل الخطوات التالية:

- قم بإنشاء قائمة الوصول التي تعرف الشبكة خلف PIX.

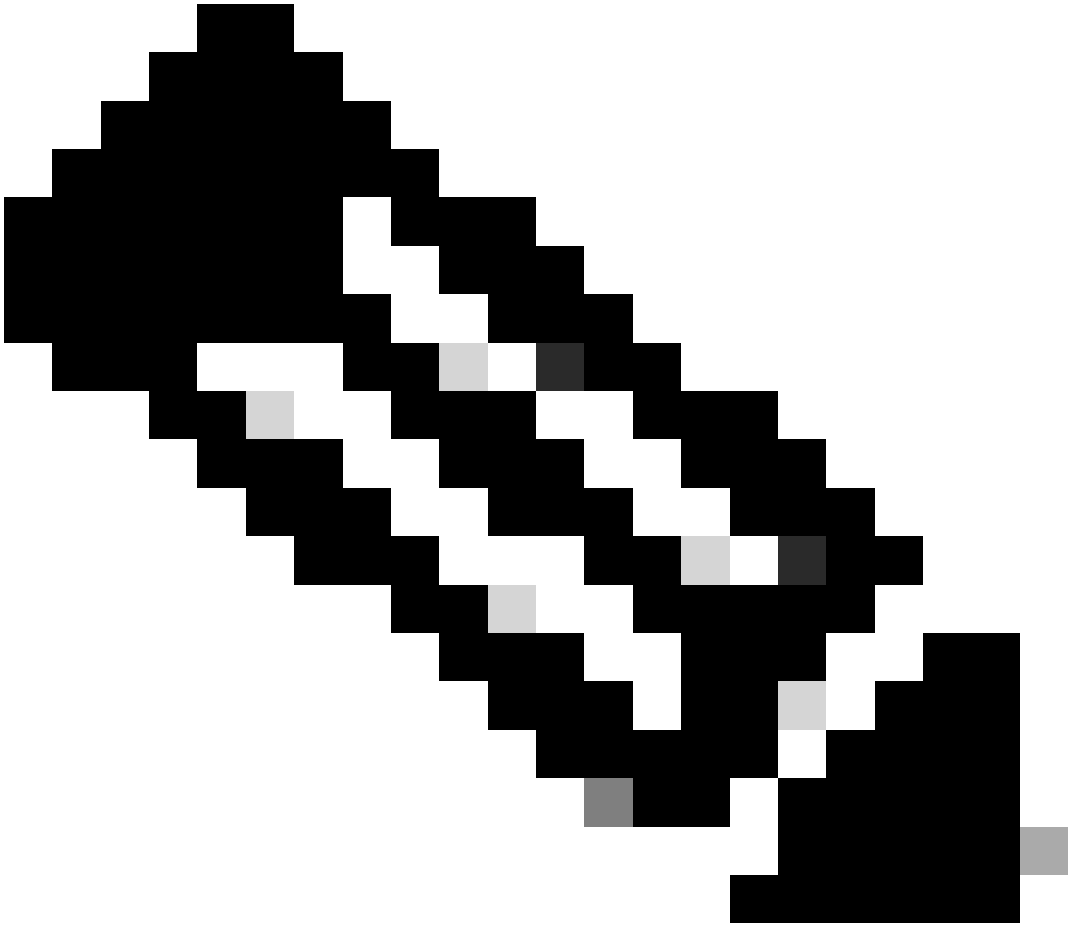
```
<#root>

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

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

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



ةظحالم: ارجع إلى Cisco Secure PIX Firewall 6.x و Cisco VPN Client 3.5 ل Windows مع ةقداصم Microsoft Windows 2000 و 2003 IAS RADIUS للحصول على مزيد من المعلومات حول تكوين الوصول عن بعد VPN ل PIX 6.x.

التحقق من الصحة

أتمت ال steps في اذه قسم in order to دقق تشكيلك.

- ةكبش VPN ليمعلا لاتصا

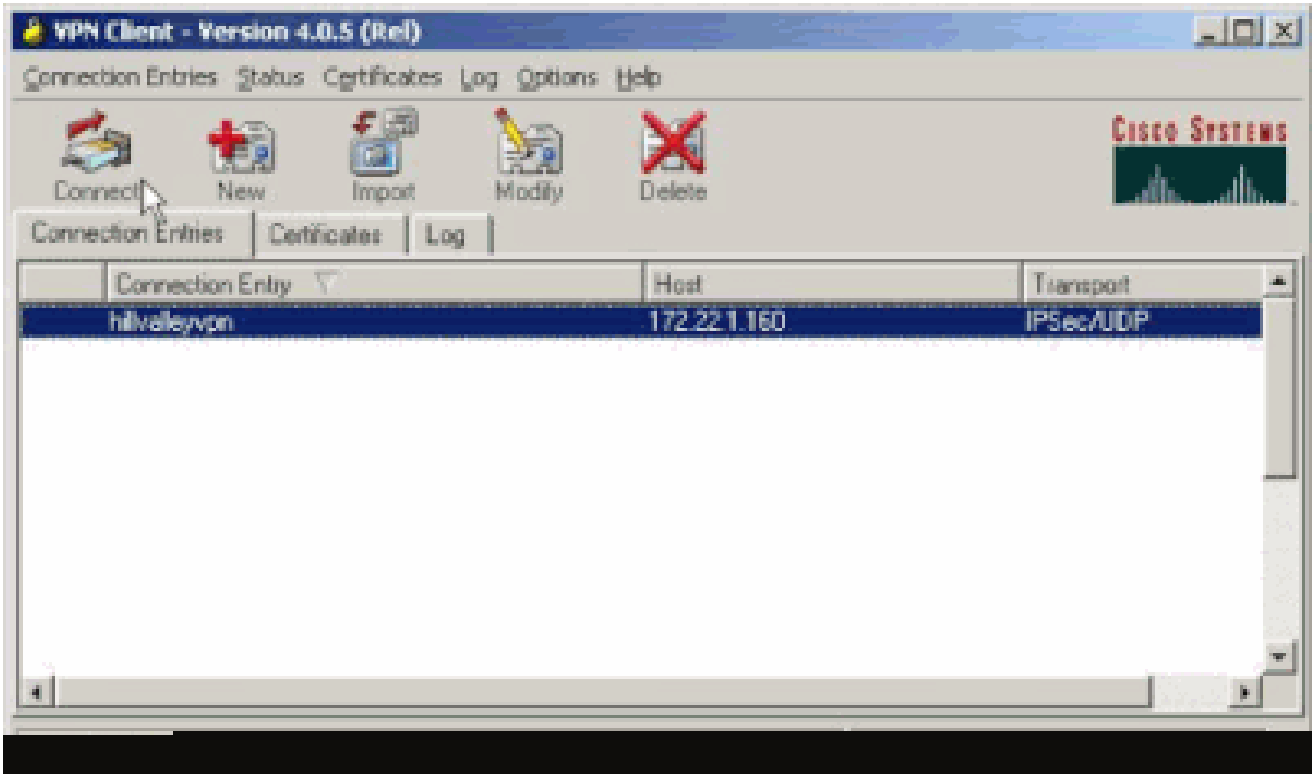
- عرض سجل عميل شبكة VPN

- اختبار الوصول الى شبكة LAN المحلية باستخدام اختبار الاتصال

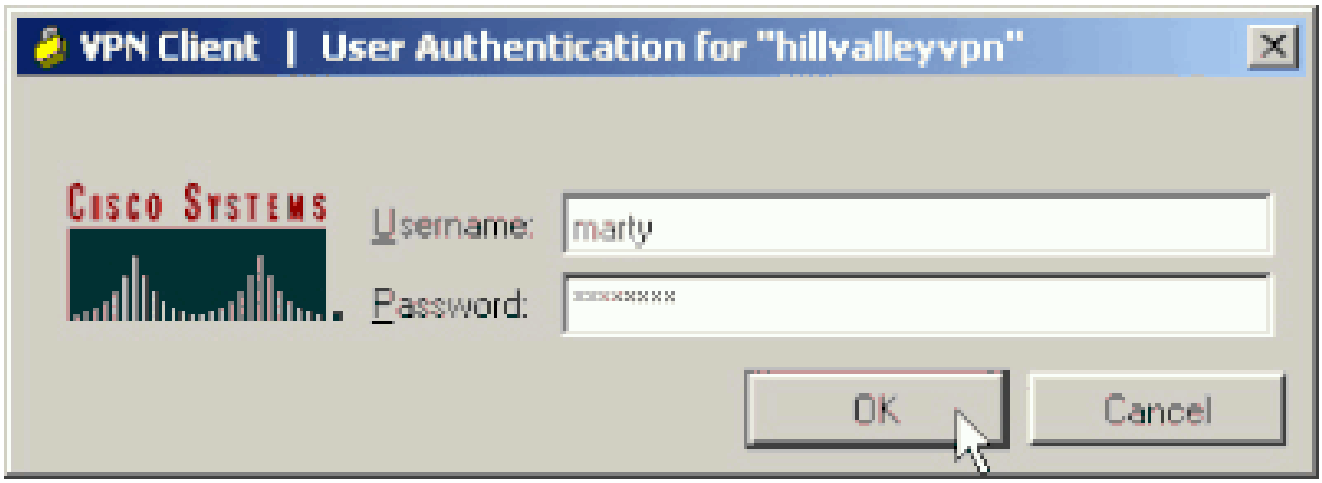
الاتصال بعميل شبكة VPN

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

- أختر إدخال الاتصال الخاص بك من القائمة ثم انقر على توصيل.

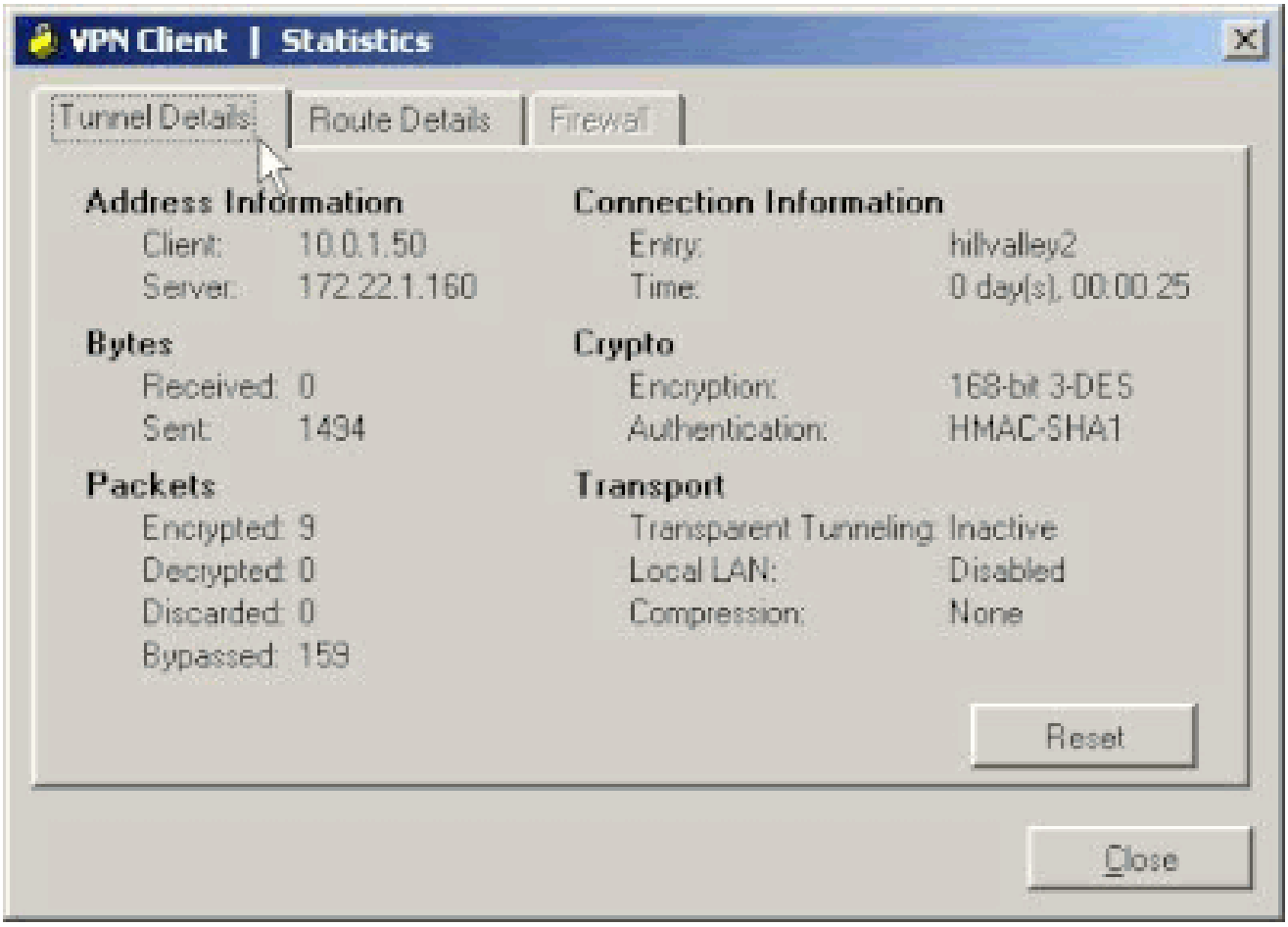


- أدخل بيانات الاعتماد الخاصة بك.



•

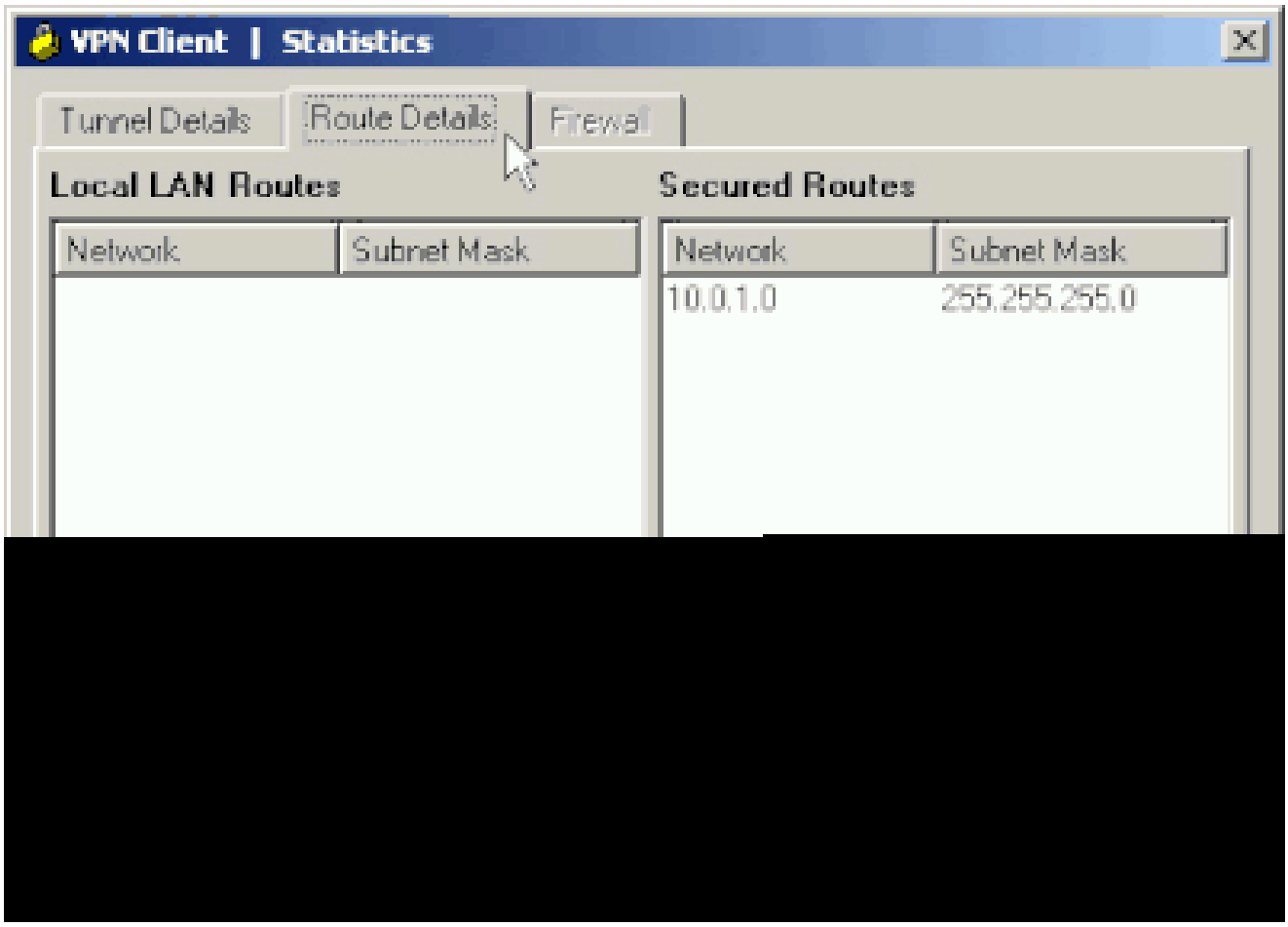
أختر الحالة > الإحصائيات... لعرض نافذة تفاصيل النفق حيث يمكنك فحص تفاصيل النفق ورؤية تدفق حركة المرور.



•

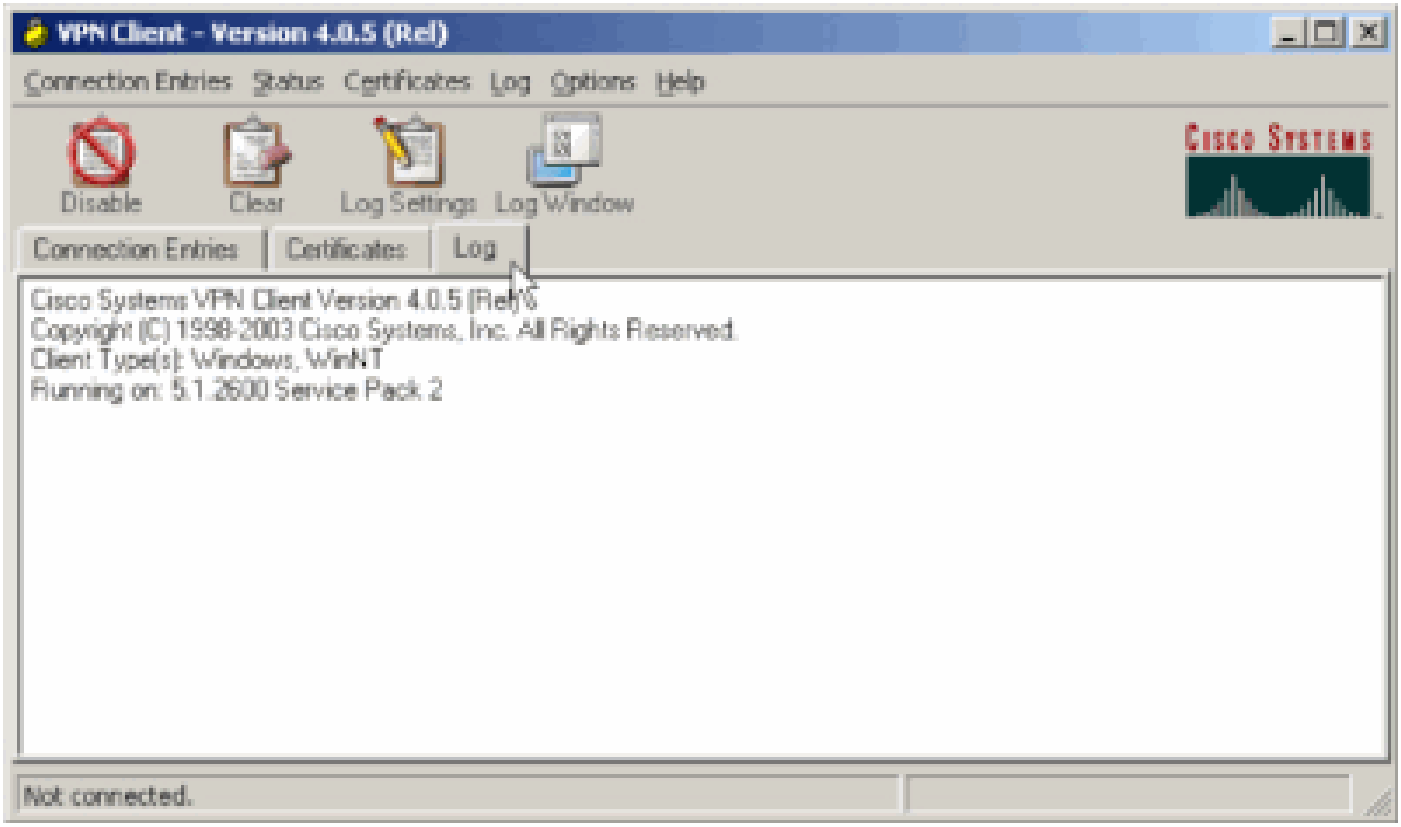
انتقل إلى علامة التبويب تفاصيل المسار للاطلاع على الموجهات التي يقوم عميل شبكة VPN بتأمينها إلى ASA.

في هذا المثال، يقوم عميل الشبكة الخاصة الظاهرية (VPN) بتأمين الوصول إلى 10.0.1.0/24 بينما تم تشفير جميع حركة مرور البيانات الأخرى والتي تم إرسالها عبر النفق.



عرض سجل عميل شبكة VPN

عندما يفحص أنت ال VPN بدون سجل، أنت يستطيع حددت ما إذا وأ ال المعلمة أن يعين النقسام 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

1      14:20:09.532  07/27/06  Sev=Info/6    IKE/0x6300003B
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 الشبكة الخاصة الظاهرية (VPN) إلنشاء قنوات اتصال نفق مقسمة أثناء إنشاء قنوات في ASA هي إستخدام الأمر **ping** في سطر الأوامر في Windows. الـ LAN المحلي من الـ VPN بزبون 192.168.0.0/24 وموضع آخر حاضر على الشبكة مع عنوان 192.168.0.3.

```
<#root>

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 Cisco ASA 5500 Series Adaptive Security Appliances**
- **الدعم الفني والتنزيلات من Cisco**

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).