ASA/PIX: عنونة IP الثابتة لعميل IPSec VPN ASDM تكوين لامثلو CLI عم

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل ال cisco 5500 sery Adaptive Security Appliance (ASA) أن يزود العنوان ساكن إستاتيكي إلى ال VPN زبون مع ال يكيف أمن أداة مدير (ASDM) أو CLI. يوفر برنامج إدارة قاعدة بيانات المحول (ASDM) إدارة ومراقبة أمان على مستوى عالمي من خلال واجهة إدارة سهلة الاستخدام قائمة على الويب. بمجرد اكتمال تكوين Cisco ASA، يمكن التحقق منه باستخدام عميل Cisco VPN.

ارجع إلى مثال تكوين المصادقة PIX/ASA 7.x و Cisco VPN Client 4.x مع Windows 2003 IAS RADIUS (مقابل Active Directory) لإعداد اتصال VPN للوصول عن بعد بين عميل 4.x) Cisco VPN ل Windows) وجهاز الأمان PIX 500 Series 7.x. يقوم مستخدم عميل شبكة VPN البعيدة بالمصادقة مقابل Active Directory باستخدام خادم RADIUS لخدمة مصادقة الإنترنت (IAS) ل Microsoft Windows 2003.

ارجع إلى PIX/ASA 7.x و Cisco VPN Client 4.x لمثال تكوين مصادقة Cisco Secure ACS من أجل إعداد اتصال VPN للوصول عن بعد بين عميل 4.x) Cisco VPN ل Windows) وجهاز الأمان PIX 500 Series 7.x مع خادم التحكم في الوصول الآمن من Cisco (ACS) الإصدار 3.2) للمصادقة الموسعة (Xauth).

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM أو CLI بإجراء تغييرات التكوين.

ملاحظة: ارجع إلى السماح بوصول HTTPS ل ASDM أو PIX/ASA 7.x: SSH على مثال تكوين الواجهة الداخلية والخارجية للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو SSH (Secure Shell).

المكونات المستخدمة

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

- برنامج جهاز الأمان القابل للتكيف الإصدار x.7 من Cisco والإصدارات الأحدث
- Adaptive Security Device Manager، الإصدار x.5 والإصدارات الأحدث
- Cisco VPN Client الإصدار x.4 والإصدارات الأحدث

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX الإصدار x.7 والإصدارات الأحدث.

الاصطلاحات

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

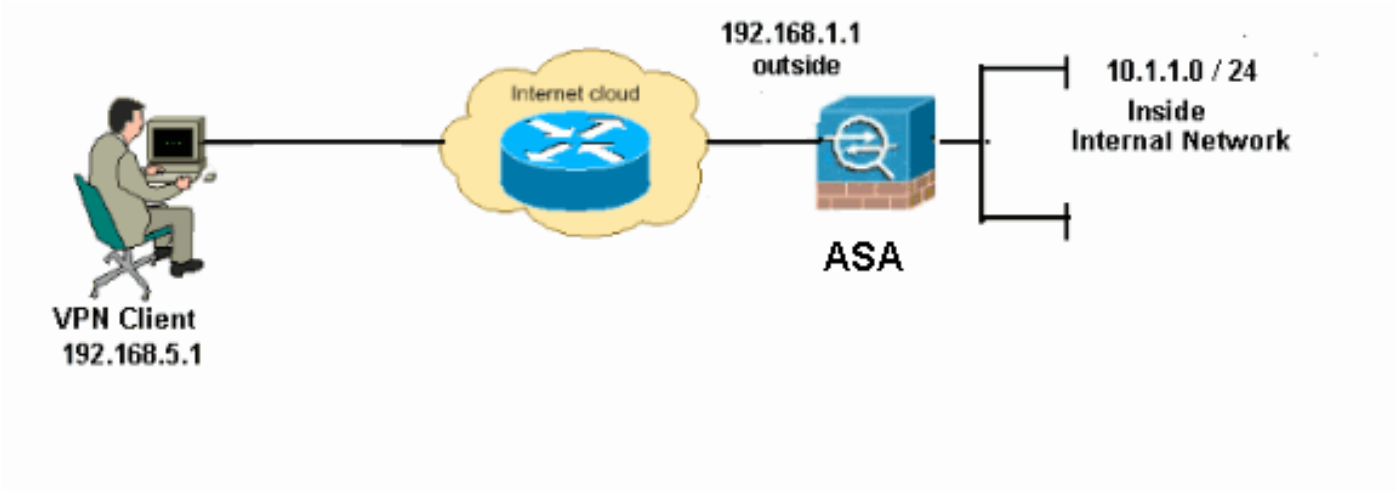
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



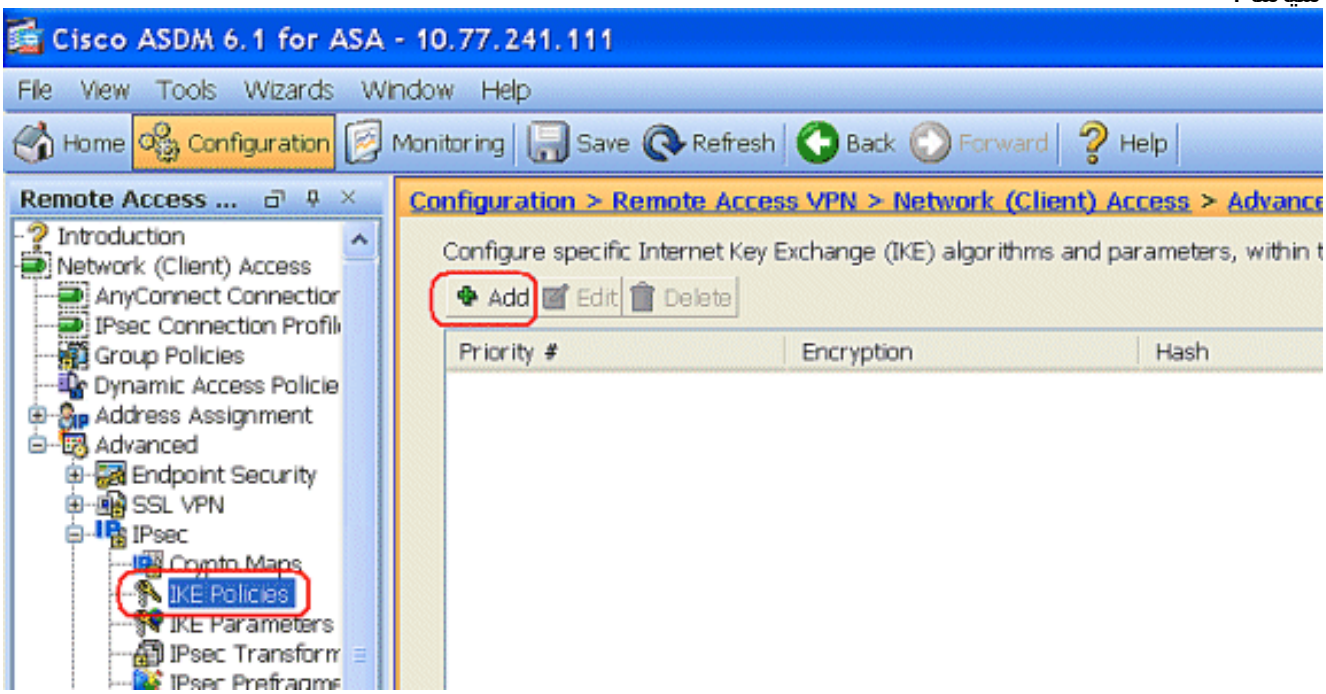
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي كان استعملت في مختبر بيئة.

تكوين شبكة VPN للوصول عن بعد (IPSec)

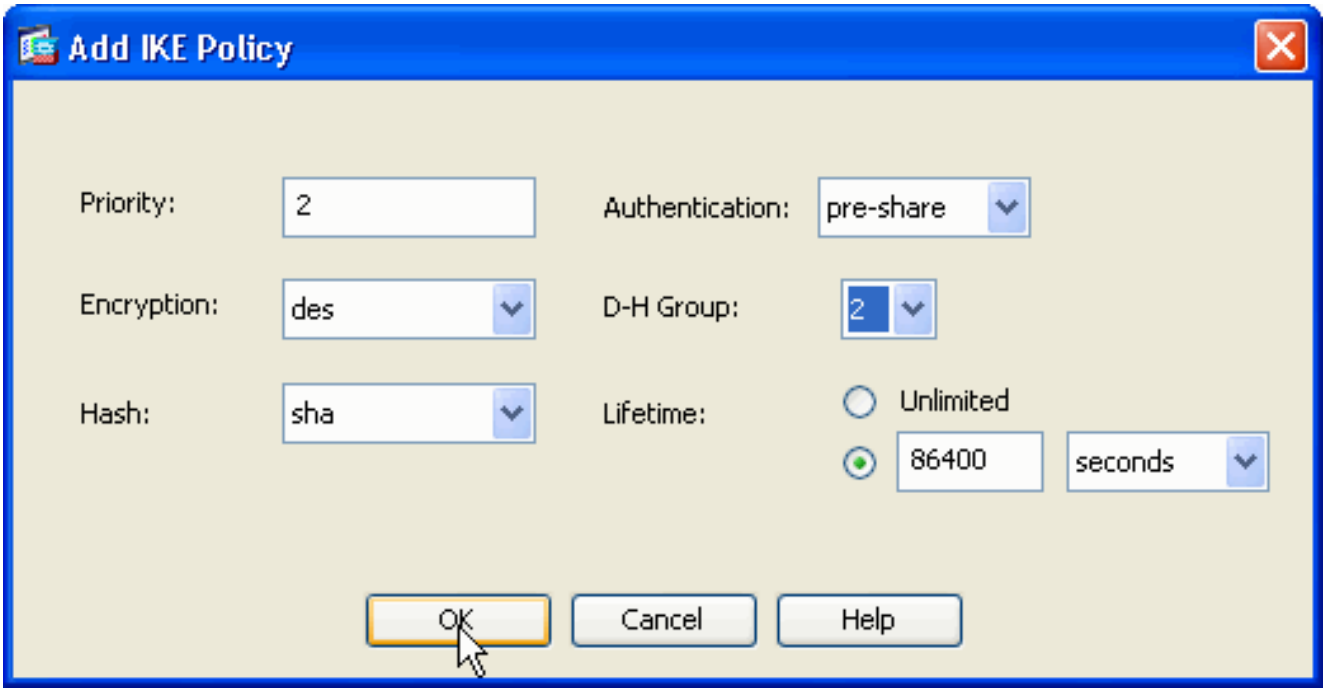
إجراء ASDM

أتمت هذا steps in order to شكلت الوصول عن بعد VPN:

1. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ > متقدم > IPSec > سياسات IKE>إضافة** in order to خلقت ISAKMP سياسة.



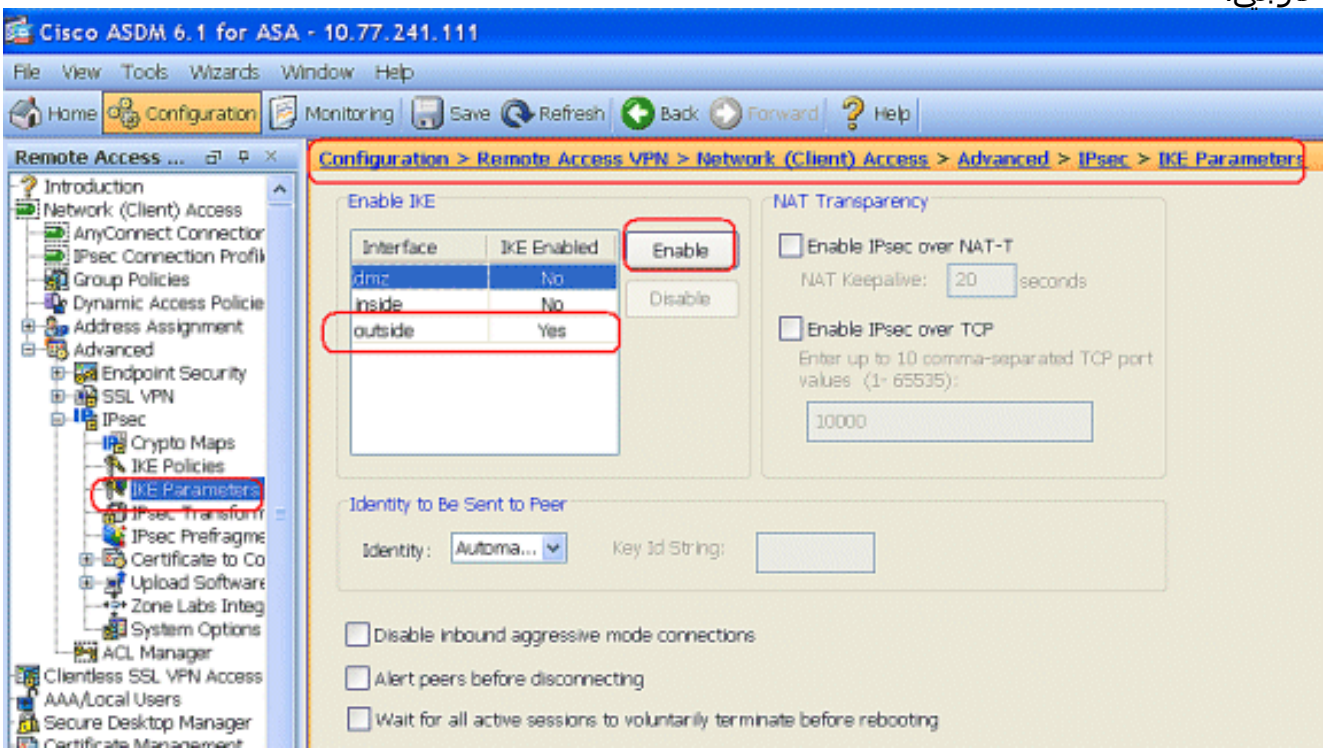
2. توفير تفاصيل سياسة ISAKMP.



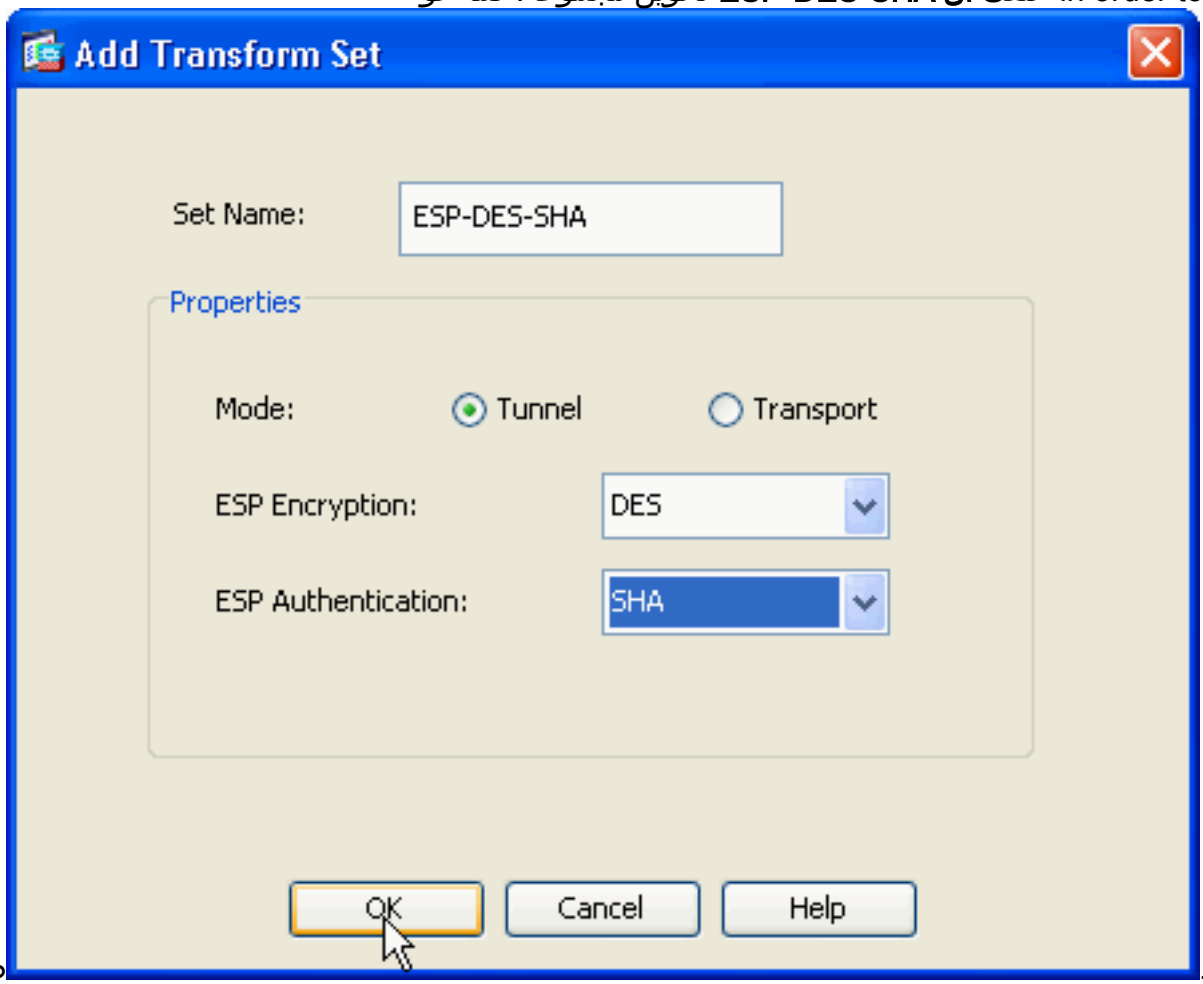
طقطقة **ok** و**يطبق**.

3. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>متقدم>IKE>IPSec معلم** أن يمكن ال IKE على

القارن
خارجي.



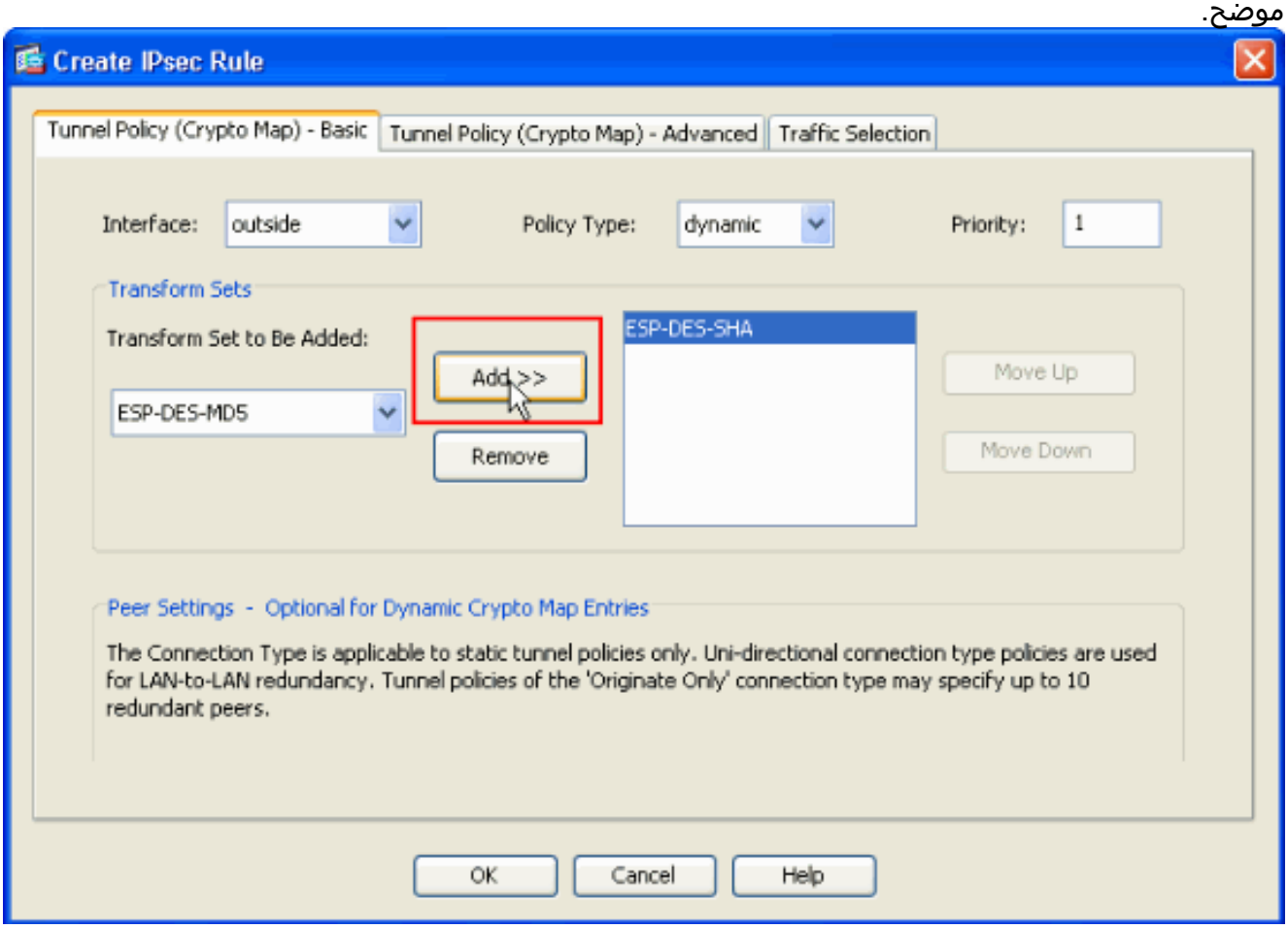
4. أخترت **تشكيل>Remote Access VPN>شبكة (زبون) منفذ > متقدم > IPSec > مجموعات تحويل IPSec > إضافة** in order to خلقت ال **ESP-DES-SHA** تحويل مجموعة، كما هو



موضح. طقة
طقة **ok** و**يطبق**.

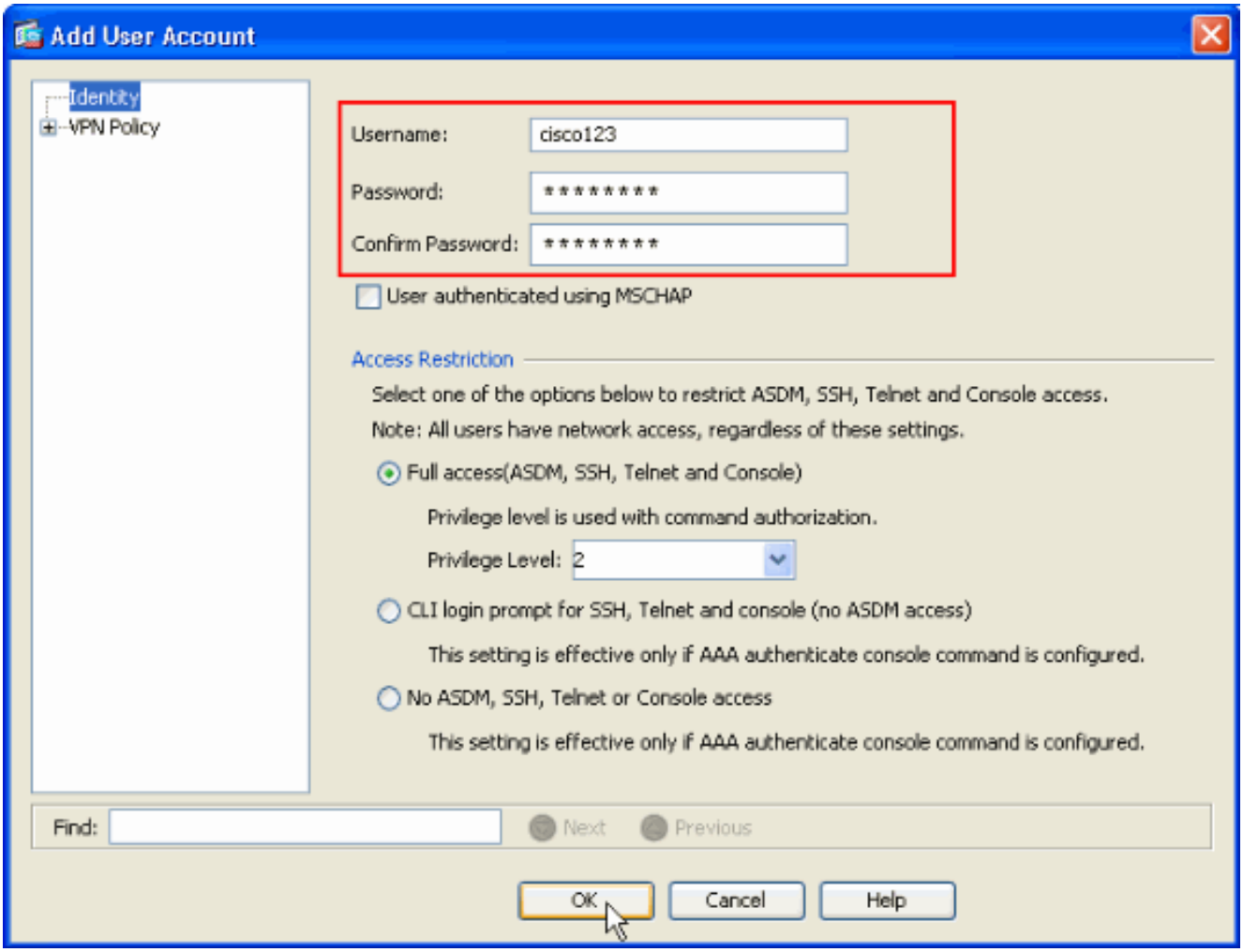
5. أختر **Configuration > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > Advanced > IPSec > Crypto Maps (خرائط التشفير) > Add** لإنشاء خريطة تشفير باستخدام السياسة

الديناميكية للأولوية 1، كما هو
موضح.

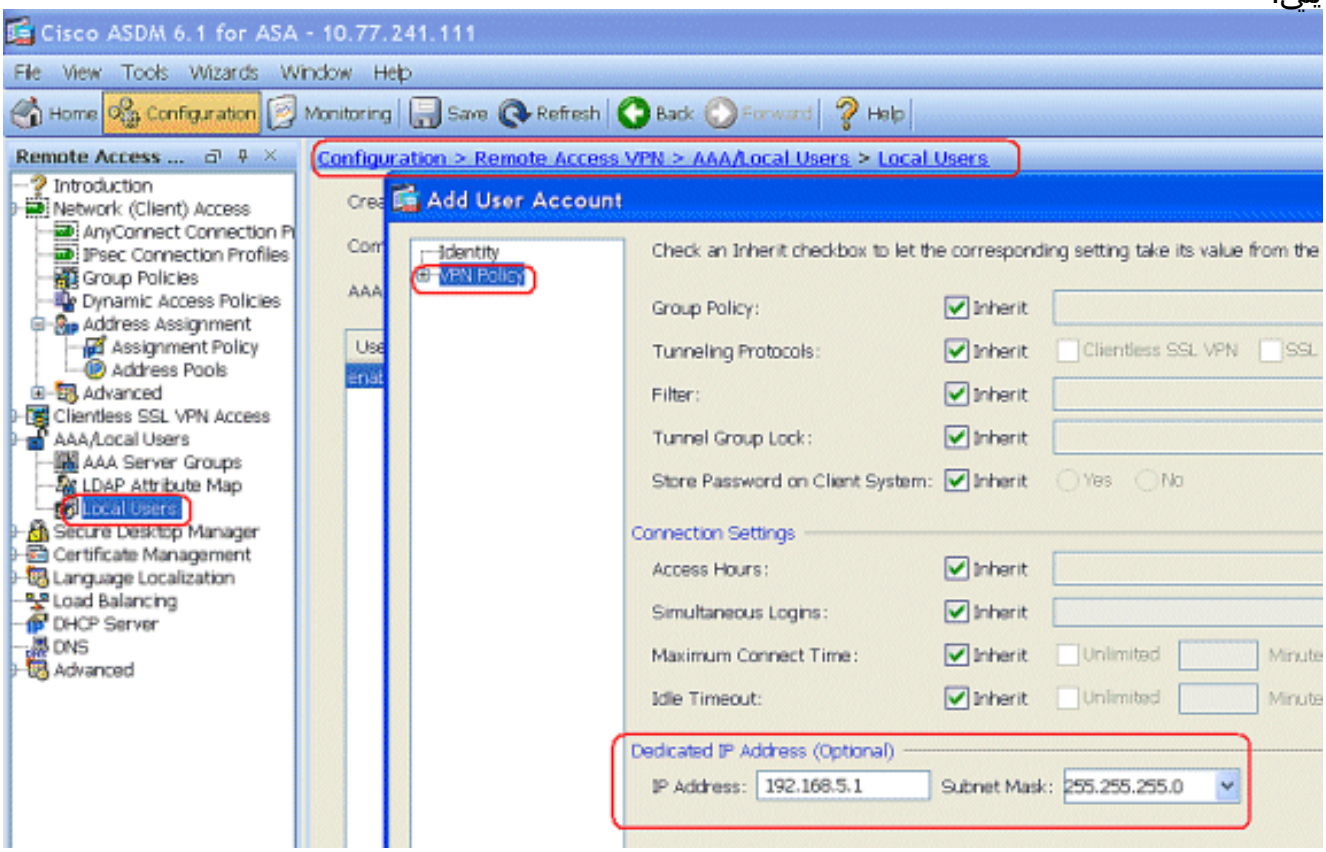


طقطقة **ok** و**يطبق**.

6. أخترت **تشكيل>Remote Access VPN (الوصول عن بعد)>AAA>AAA setup>مستعمل محلي>يضيف** in order to خلقت المستعمل حساب (مثلا، username - cisco123 وكلمة - cisco123) ل VPN زبون منفذ.

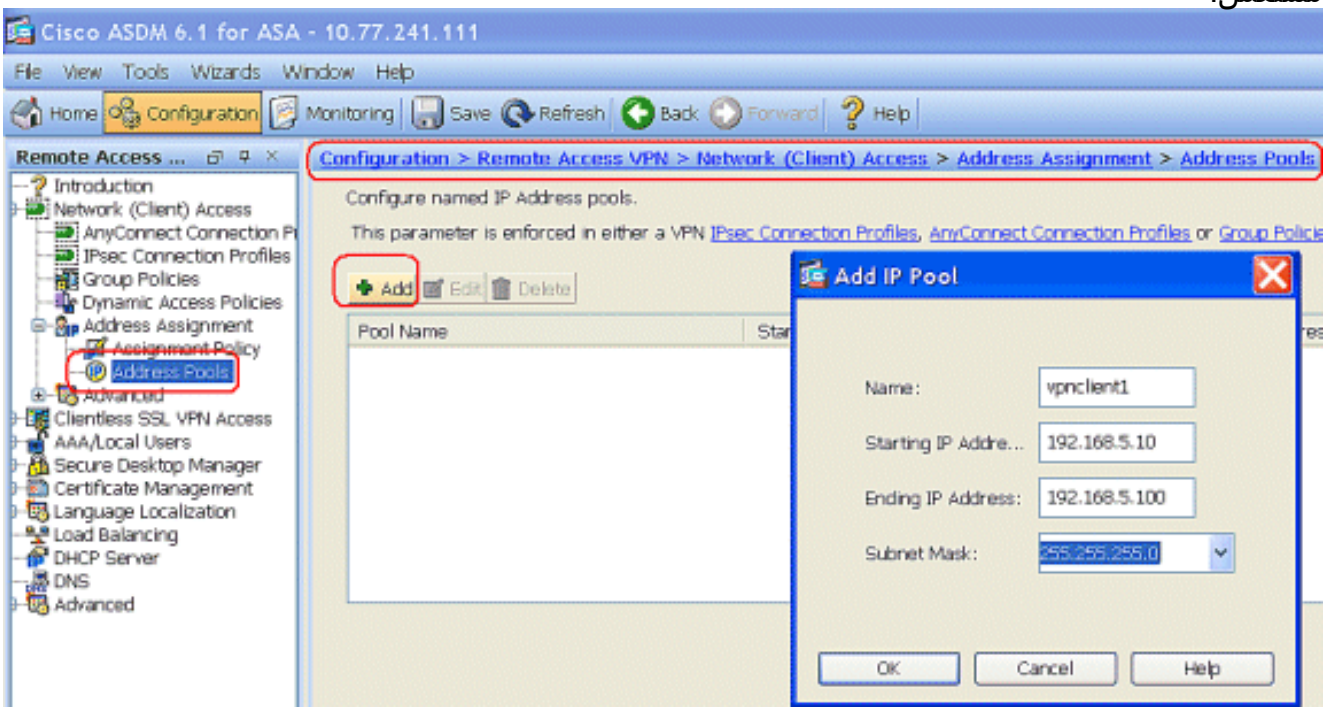


7. انتقل إلى **سياسة شبكة VPN** وأضفت **عنوان IP الثابت/المخصص** للمستخدم "Cisco123"، كما يلي.

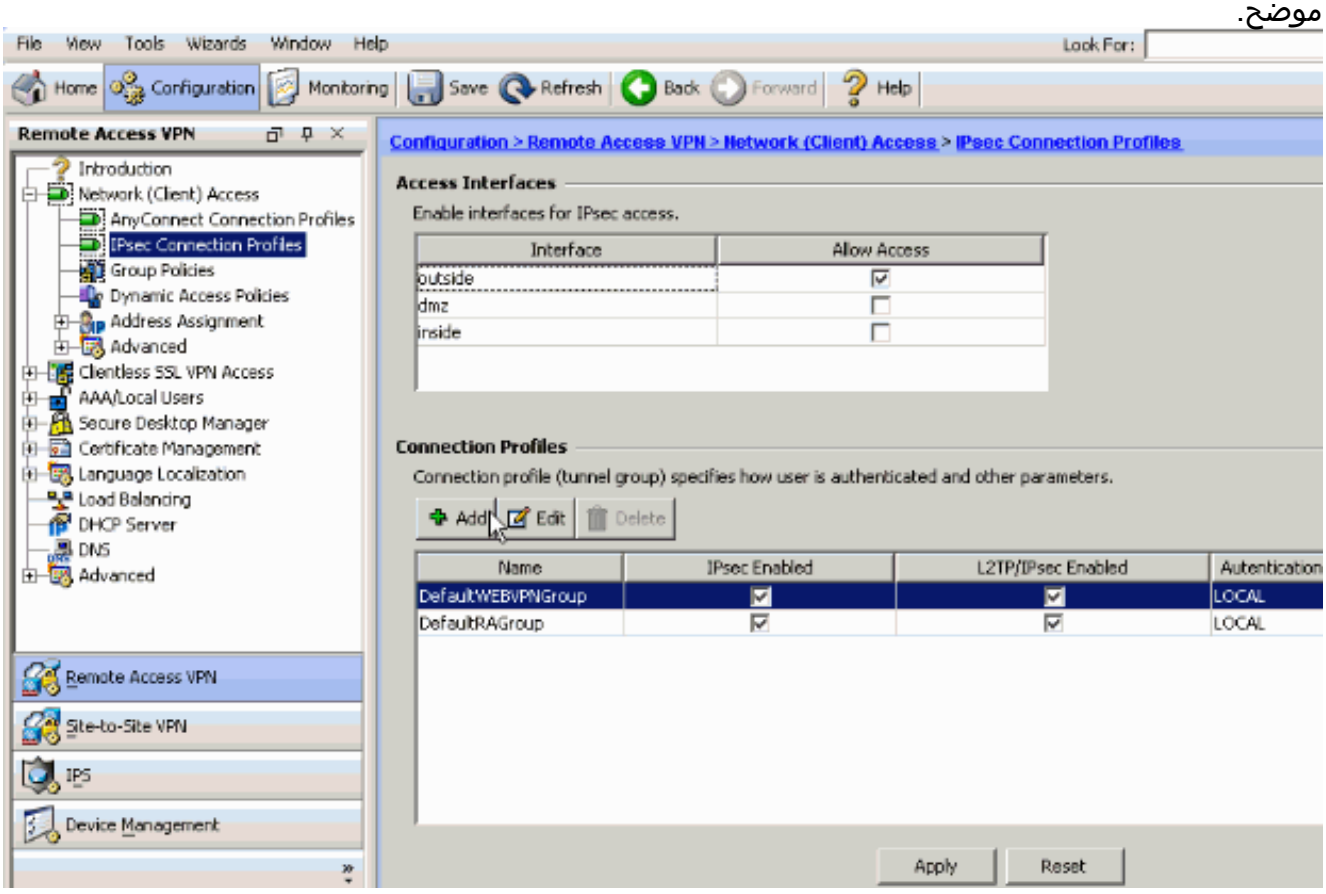


8. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>عنوان تعيين>عنوان** بركة وطقطقة **يضيف** أن يضيف ال VPN زبون ل VPN زبون

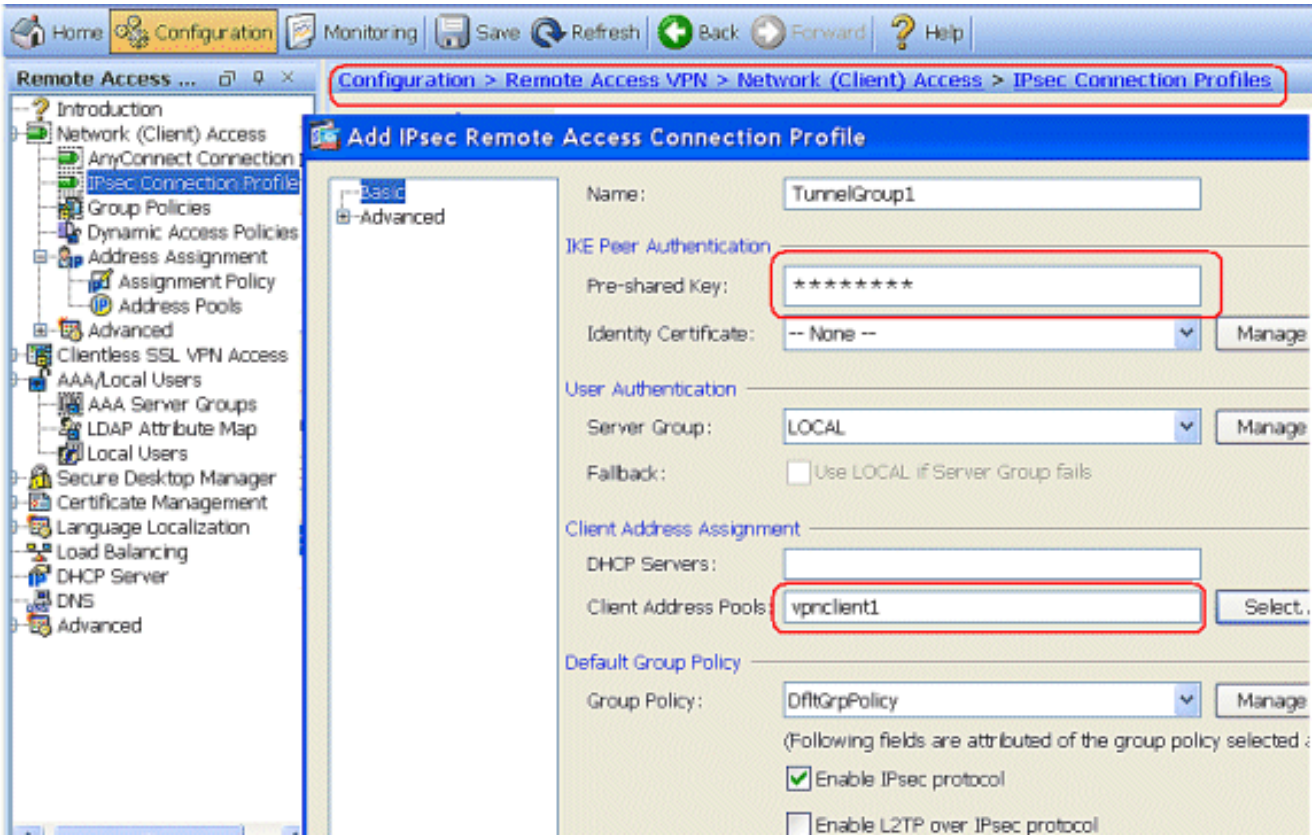
مستعمل.



9. أخترت **تشكيل>Remote Access VPN>شبكة (زبون) منفذ>IPSec توصيل ملفات تعريف > إضافة** in order to أضفت a نفق مجموعة (مثلا، TunnelGroup1 والمفتاح متصل مسبقا ك cisco123)، كما هو موضح.

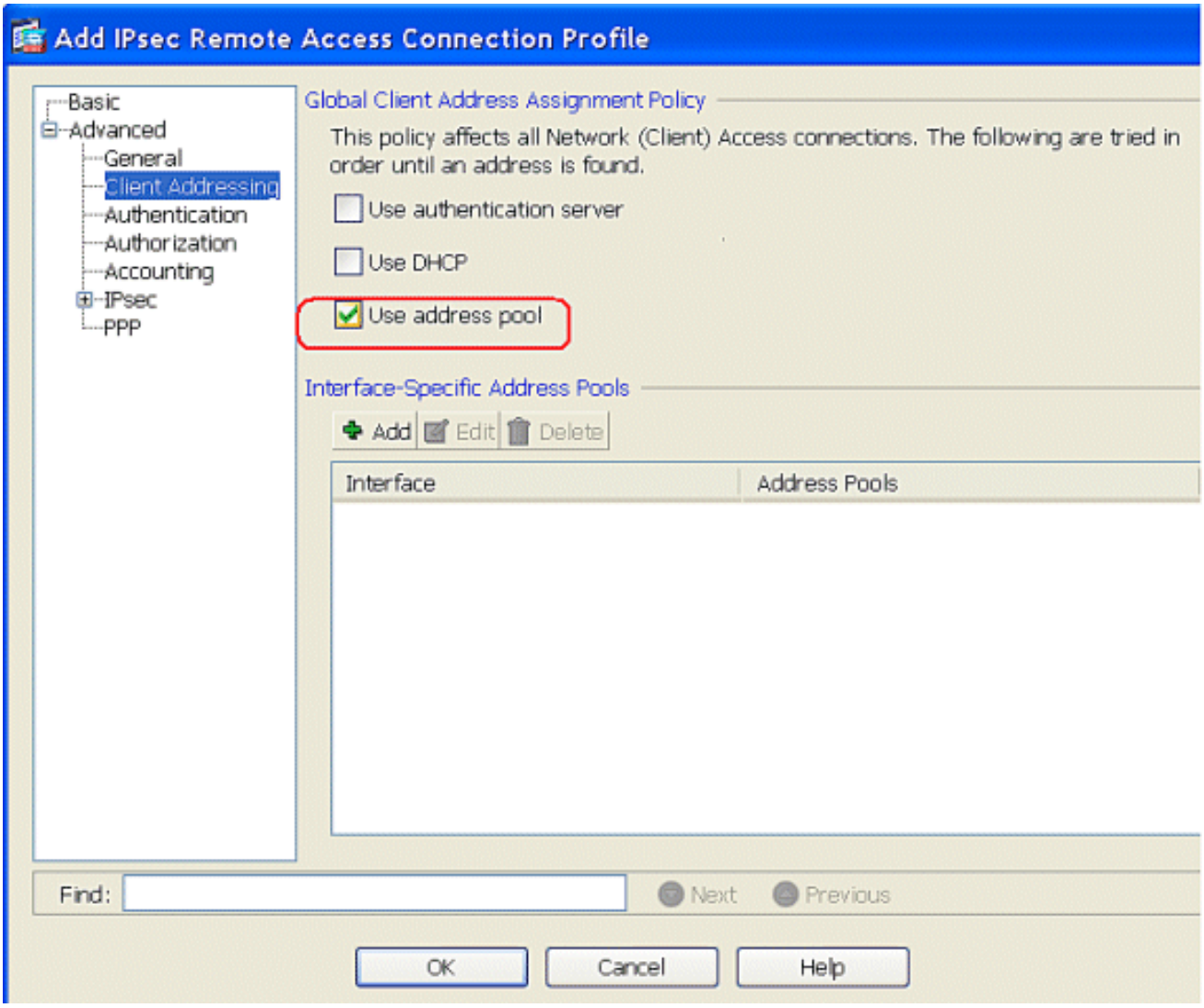


تحت علامة التبويب **أساسي**، أختر مجموعة الخادم كمجموعة **محلية** لحقل مصادقة المستخدم.أخترت **vpnClient1** كالزبون عنوان بركة ل ال VPN زبون
مستعمل.



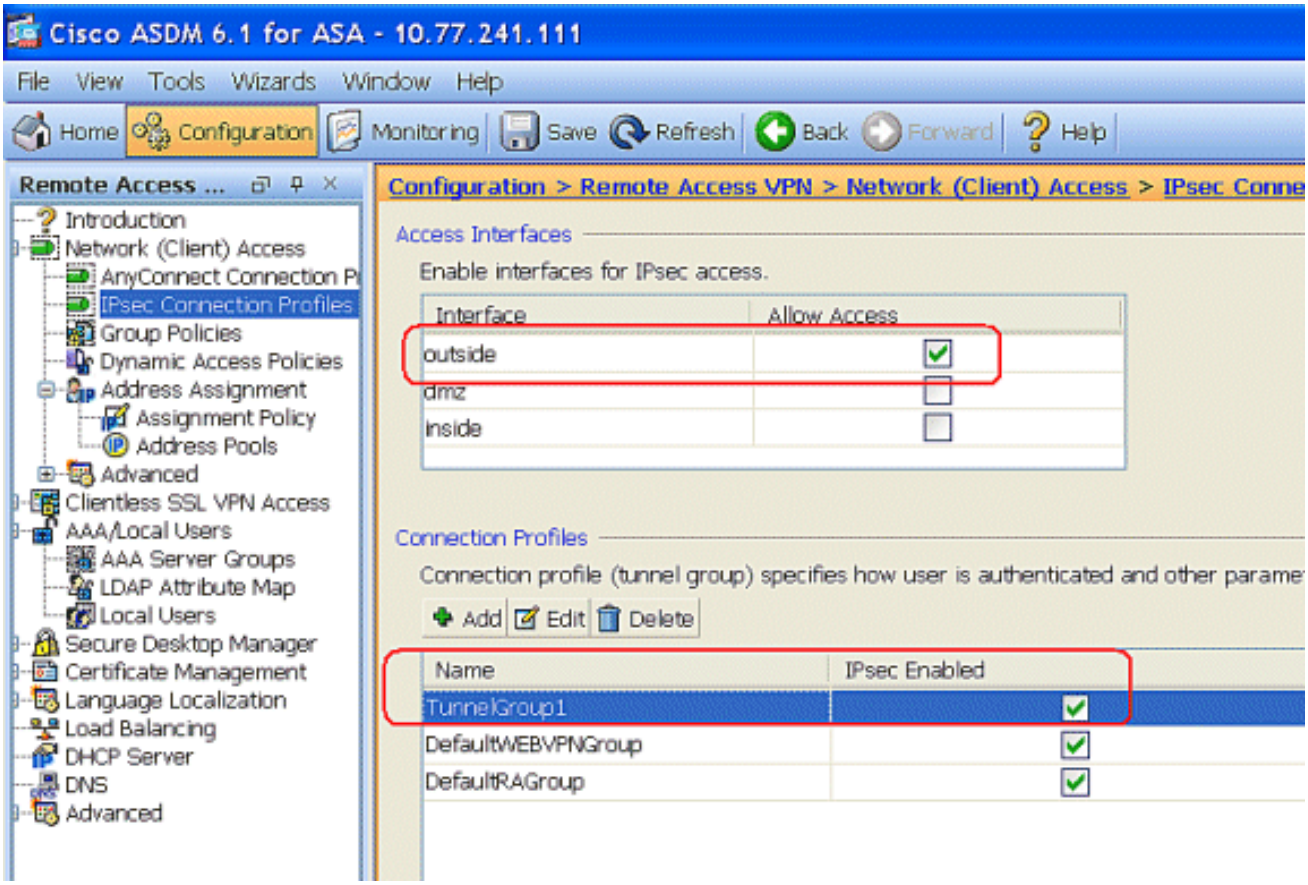
وانقر فوق **OK**.

10. أخترت **متقدم>زبون عنونة** وفحصت **ال use عنوان بركة** تدقيق صندوق أن يعين العنوان إلى ال VPN زبون.**ملاحظة:** تأكد من إلغاء تحديد خانات الاختيار **لاستخدام خادم المصادقة** واستخدام DHCP.



وانقر فوق **OK**.

11. قم بتمكين الواجهة **الخارجية** للوصول إلى IPSec. انقر فوق **تطبيق** للمتابعة.



تكوين ASA/PIX باستخدام CLI

أتمت هذا steps in order to شكلت ال DHCP نادل أن يزود عنوان إلى ال VPN زبون من الأمر خط. ارجع إلى تكوين شبكات VPN للوصول عن بعد أو مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances للحصول على مزيد من المعلومات حول كل أمر يتم إستخدامه.

يتم تشغيل التكوين على جهاز ASA
ASA# sh run (ASA Version 8.0(2 ! *Specify the hostname for the Security Appliance. ---!* hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted names ! *!--- Configure the outside and inside* *interfaces.* interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! interface Ethernet0/1 nameif outside security-level 0 ip address 192.168.1.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 50 ip address 192.168.10.2 255.255.255.0 *!--- Output is suppressed.* passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive access-list 101 extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 mtu dmz 1500 **ip local pool vpnclient1 192.168.5.10-192.168.5.100** **mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 *Specify the location of the ASDM image for ASA to ---!*

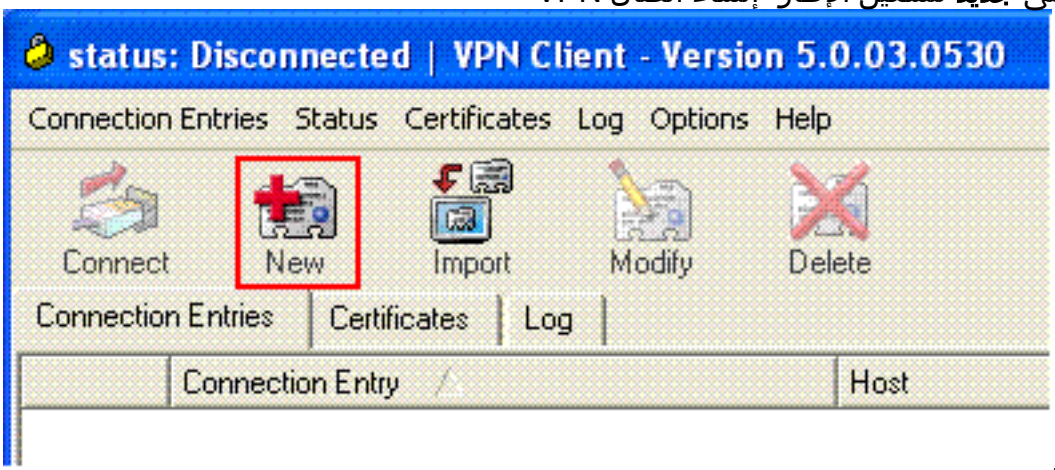
```
fetch the image for ASDM access. asdm image disk0:/asdm-
 613.bin no asdm history enable arp timeout 14400 global
  (outside) 1 192.168.1.5 nat (inside) 0 access-list 101
    nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 192.168.1.2 1 timeout xlate 3:00:00 timeout conn
    1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
  0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
       0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
   timeout uauth 0:05:00 absolute dynamic-access-policy-
 record DfltAccessPolicy http server enable http 0.0.0.0
  0.0.0.0 inside no snmp-server location no snmp-server
    contact snmp-server enable traps snmp authentication
    linkup linkdown coldstart crypto ipsec transform-set
     ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map
  outside_dyn_map 1 set transform-set ESP-DES-SHA crypto
  map outside_map 1 ipsec-isakmp dynamic outside_dyn_map
   !--- Specifies the interface to be used with !--- the
      settings defined in this configuration. crypto map
outside_map interface outside !--- PHASE 1 CONFIGURATION
 ---! !--- This configuration uses ISAKMP policy 2. !---
 The configuration commands here define the Phase !--- 1
   policy parameters that are used. crypto isakmp enable
 outside crypto isakmp policy 2 authentication pre-share
encryption des hash sha group 2 lifetime 86400 no crypto
 isakmp nat-traversal !--- Specifies that the IP address
 to the vpn clients are assigned by the local and not by
      AAA or dhcp. The CLI vpn-addr-assign local for VPN
     address assignment through ASA is hidden in the CLI
                              .provided by show run command

                                        no vpn-addr-assign aaa
                                       no vpn-addr-assign dhcp

                                              telnet timeout 5
                                                 ssh timeout 5
                                            console timeout 0
                                  threat-detection basic-threat
                        threat-detection statistics access-list
                                                              !
                                   class-map inspection_default
                              match default-inspection-traffic
                                                              !
                                                              !
                      policy-map type inspect dns preset_dns_map
                                                   parameters
                                 message-length maximum 512
                                     policy-map global_policy
                                    class inspection_default
                                 inspect dns preset_dns_map
                                                 inspect ftp
                                          inspect h323 h225
                                           inspect h323 ras
                                            inspect netbios
                                                 inspect rsh
                                               inspect rtsp
                                             inspect skinny
                                              inspect esmtp
                                             inspect sqlnet
                                             inspect sunrpc
                                               inspect tftp
                                                inspect sip
                                              inspect xdmcp
                                                              !
```

```
                                service-policy global_policy global
                                                                   !
                              group-policy DfltGrpPolicy attributes
                                  vpn-tunnel-protocol IPSec webvpn
                                group-policy GroupPolicy1 internal

    In order to identify remote access users to the ---!
         Security Appliance, !--- you can also configure
  usernames and passwords on the device. !--- specify the
  IP address to assign to a particular user, use the vpn-
            framed-ip-address command !--- in username mode

    username cisco123 password ffIRPGpDSOJh9YLq encrypted
                                  username cisco123 attributes
        vpn-framed-ip-address 192.168.5.1 255.255.255.0
Create a new tunnel group and set the connection !- ---!
-- type to remote-access. tunnel-group TunnelGroup1 type
          remote-access tunnel-group TunnelGroup1 general-
    attributes address-pool vpnclient1 !--- Enter the pre-
        shared-key to configure the authentication method.
    tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
                                  key * prompt hostname context
     Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
                                                        #ASA
```

تكوين عميل شبكة VPN من Cisco

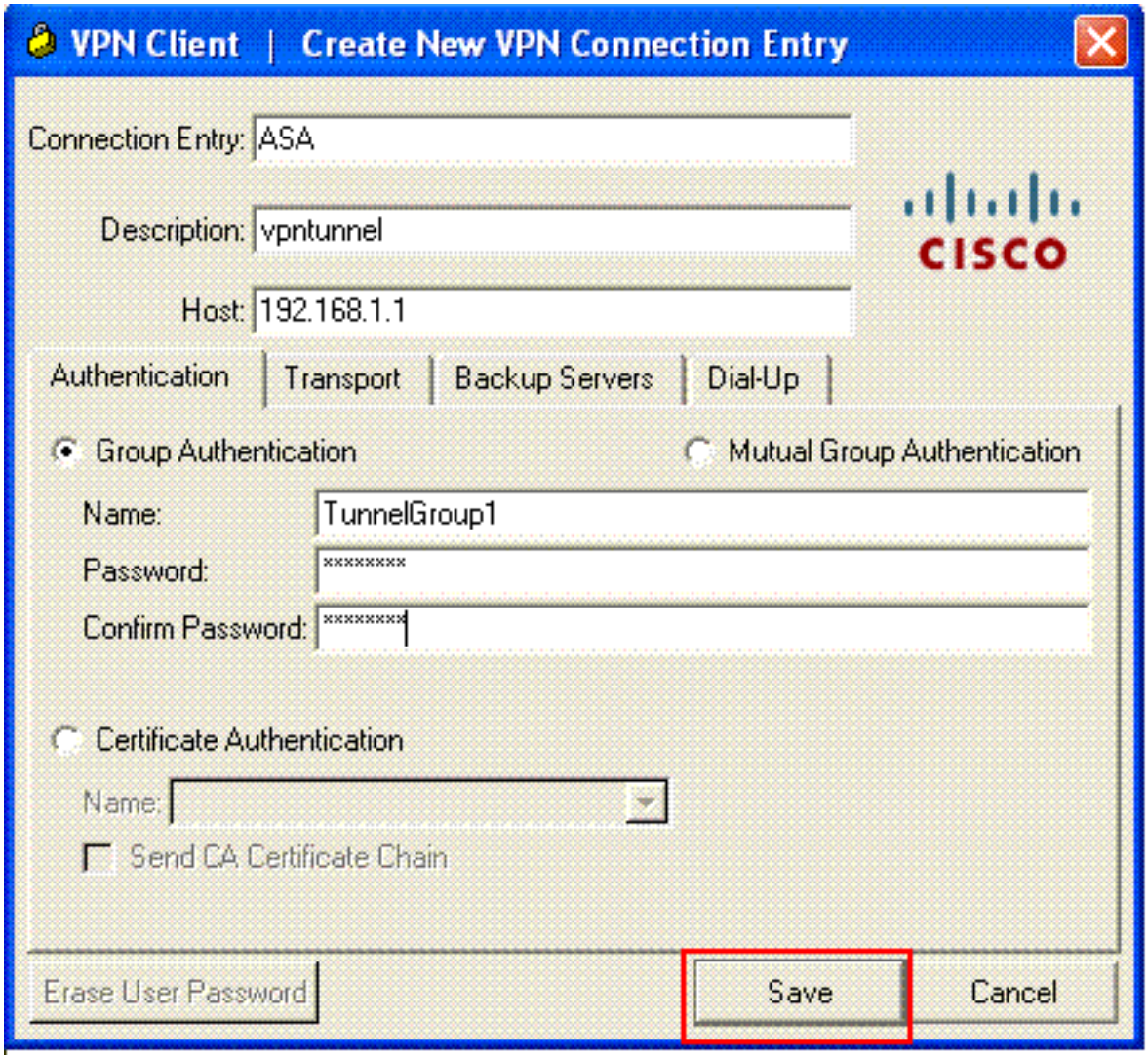
حاول الاتصال ب Cisco ASA مع عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

1. أخترت **بداية>برنامج>Cisco Systems VPN زبون>VPN زبون**.
2. انقر على **جديد** لتشغيل الإطار "إنشاء اتصال VPN



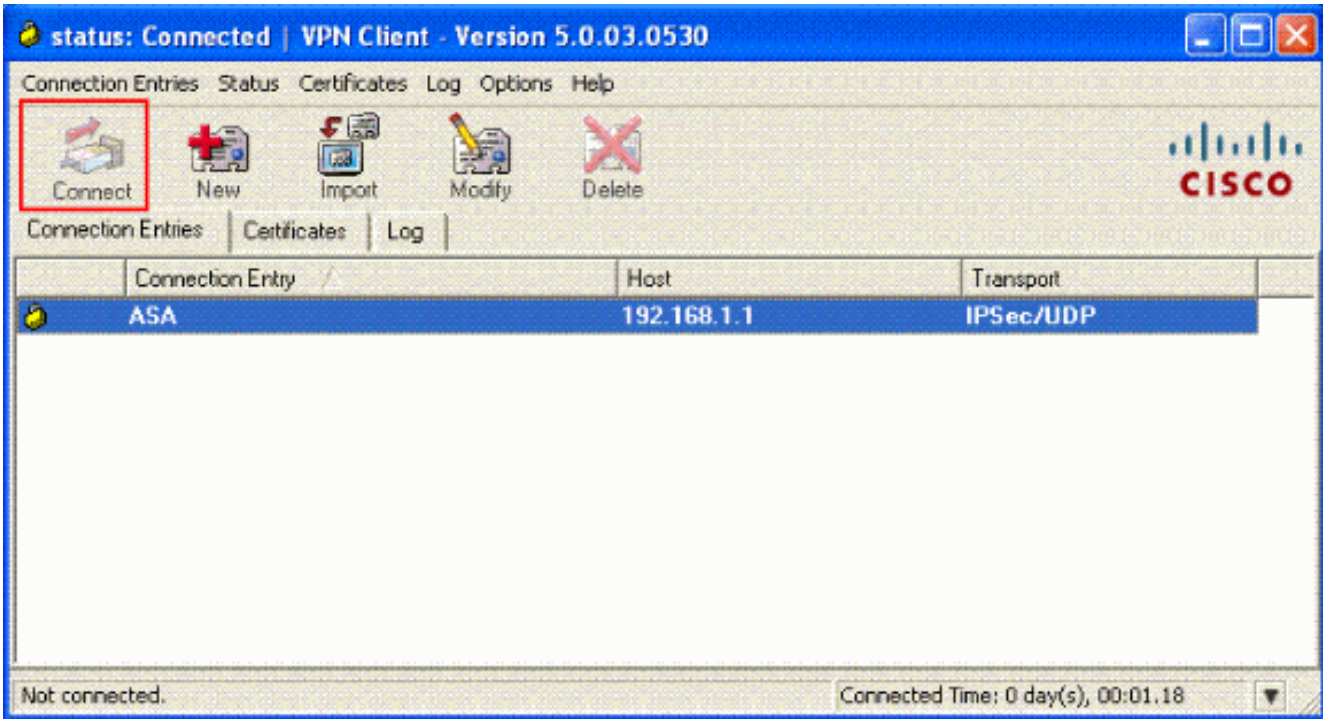
جديد".

3. املأ تفاصيل إتصالك الجديد.أدخل اسم "إدخال الاتصال" مع وصف. دخلت **العنوان خارجي من ال ASA** في المضيف صندوق. ثم أدخل اسم مجموعة نفق VPN (TunnelGroup1) وكلمة المرور (مفتاح مشترك مسبقا - Cisco123) كما تم تكوينها في ASA. طقطقة

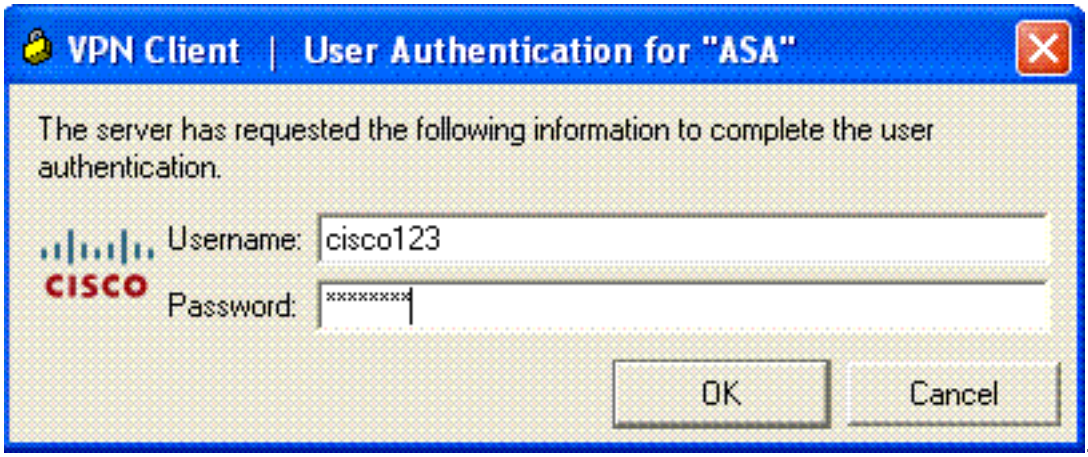


حفظ.

4. انقر فوق الاتصال الذي تريد إستخدامه، ثم انقر فوق **الاتصال** من الإطار الرئيسي لعميل شبكة VPN.

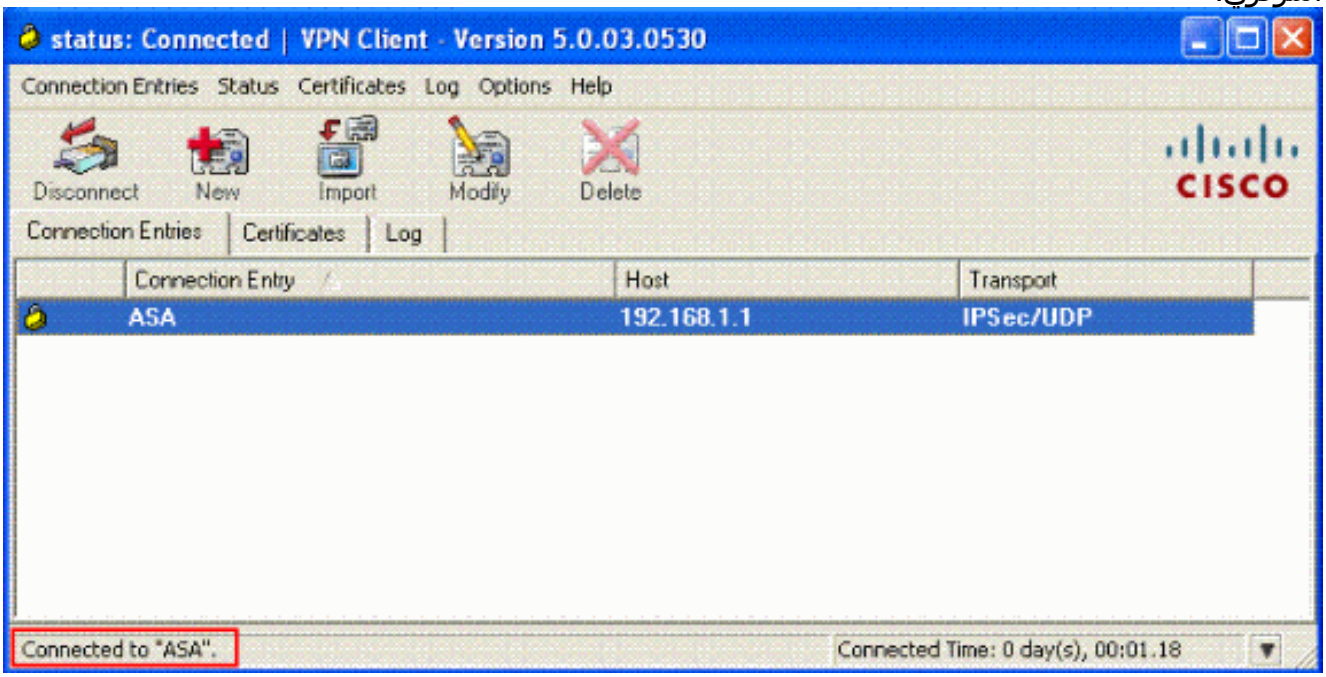


5. عندما يطلب منك، أدخل **اسم المستخدم : cisco123** و**كلمة المرور : cisco123** كما تم تكوينها في ASA ل Xauth، وانقر فوق **موافق** للاتصال بالشبكة

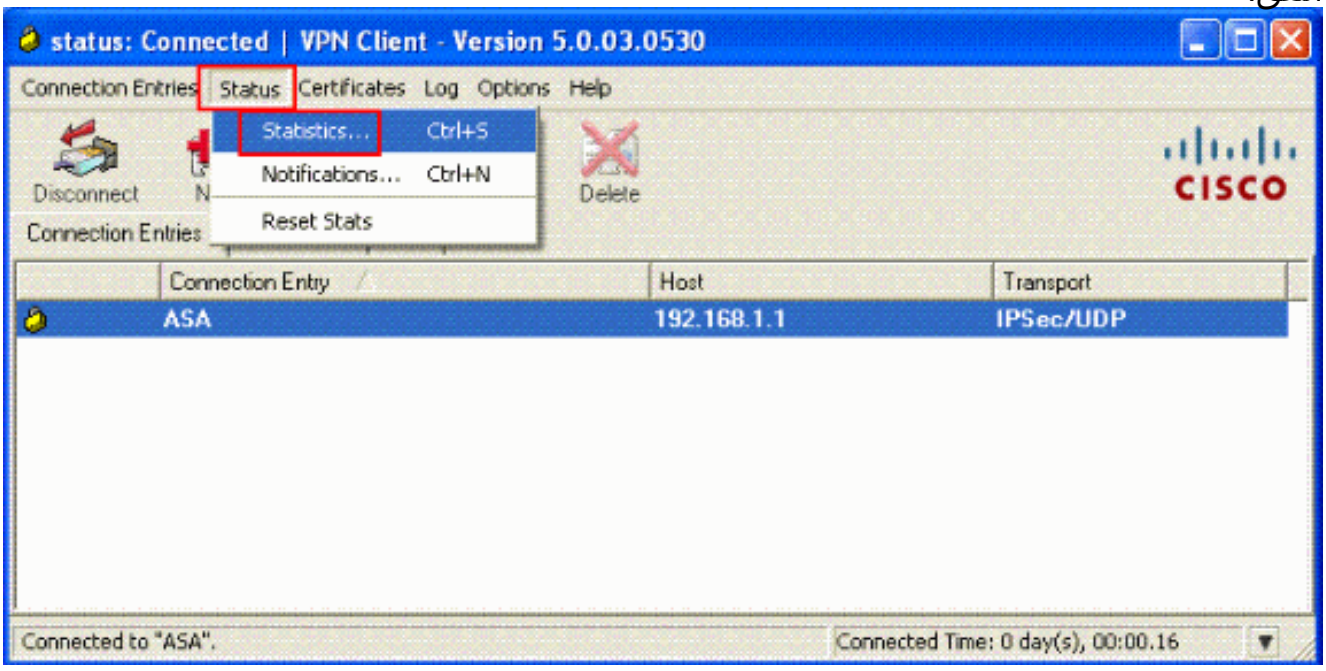


البعيدة.

6. يتم توصيل عميل شبكة VPN مع ASA في الموقع المركزي.



7. بمجرد تأسيس الاتصال بنجاح، أختر **إحصائيات** من قائمة الحالة للتحقق من تفاصيل النفق.



التحقق من الصحة

إظهار الأوامر

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show crypto isakmp sa**— يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل SAs الحالية.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. يتم عرض إخراج تصحيح الأخطاء للعينة أيضا.

ملاحظة: للحصول علي مزيد من المعلومات حول أستكشاف أخطاء الوصول عن بعد IPSec VPN وإصلاحها، ارجع إلى حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) الخاصة ب L2L والوصول عن بعد IPSec وإصلاحها.

مسح الاقترانات الأمنية

عند أستكشاف الأخطاء وإصلاحها، تأكد من مسح اقترانات الأمان الموجودة بعد إجراء تغيير. في الوضع ذي الامتيازات ل PIX، أستخدم الأوامر التالية:

- **مسح [crypto] ipSec sa**— يحذف رسائل IPSec النشطة. تشفير الكلمة الأساسية إختياري.
- **مسح [crypto] isakmp sa**— يحذف شبكات IKE النشطة. تشفير الكلمة الأساسية إختياري.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug crypto ipSec 7**—يعرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp 7**—يعرض مفاوضات ISAKMP للمرحلة 1.

معلومات ذات صلة

- صفحة دعم أجهزة الأمان القابلة للتكيف Cisco من ASA 5500 Series
- مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances Command References
- صفحة دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- مرجع أوامر أجهزة الأمان Cisco PIX 500 Series Security Appliances
- مدير أجهزة حلول الأمان المعدلة من Cisco
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- صفحة دعم عميل شبكة VPN من Cisco
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco

- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

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).