ASA/PIX: عنونة عميل VPN ل IPsec باستخدام ASDM تكوين مثال مع DHCP خادم

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 لجعل خادم DHCP يوفر عنوان IP العميل لجميع عملاء VPN باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) أو CLI (واجهة سطر الأوامر). 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 Cisco VPN 4.x) ل Windows) وجهاز الأمان PIX 500 Series 7.x. يقوم مستخدم عميل شبكة VPN البعيدة بالمصادقة مقابل خدمة 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 Cisco VPN 4.x) ل Windows) وجهاز الأمان PIX 500 Series 7.x باستخدام 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.

معلومات أساسية

تلبي شبكات VPN الخاصة بالوصول عن بعد متطلبات الموظفين كثيري التنقل للاتصال بأمان بشبكة المؤسسة. يستطيع مستخدمو الأجهزة المحمولة إعداد اتصال آمن باستخدام برنامج عميل شبكة VPN المثبت على أجهزة الكمبيوتر الخاصة بهم. يقوم عميل شبكة VPN ببدء اتصال بجهاز موقع مركزي تم تكوينه لقبول هذه الطلبات. في هذا المثال، جهاز الموقع المركزي هو جهاز الأمان القابل للتكيف ASA 5500 Series الذي يستخدم خرائط التشفير الديناميكية.

في إدارة عنوان جهاز الأمان، يجب تكوين عناوين IP التي توصل عميلا بمورد على الشبكة الخاصة، عبر النفق، والسماح للعميل بالعمل كما لو كان متصلا مباشرة بالشبكة الخاصة. علاوة على ذلك، نحن نتعامل فقط مع عناوين IP الخاصة التي يتم تعيينها للعملاء. تعد عناوين IP التي تم تعيينها لموارد أخرى على الشبكة الخاصة الخاصة بك جزءا من مسؤوليات إدارة الشبكة الخاصة بك، وليس جزءا من إدارة VPN. لذلك، عندما تتم مناقشة عناوين IP هنا، فإننا نعني عناوين IP هذه المتاحة في مخطط عنونة الشبكة الخاصة لديك التي تتيح للعميل العمل كنقطة نهاية نفق.

التكوين

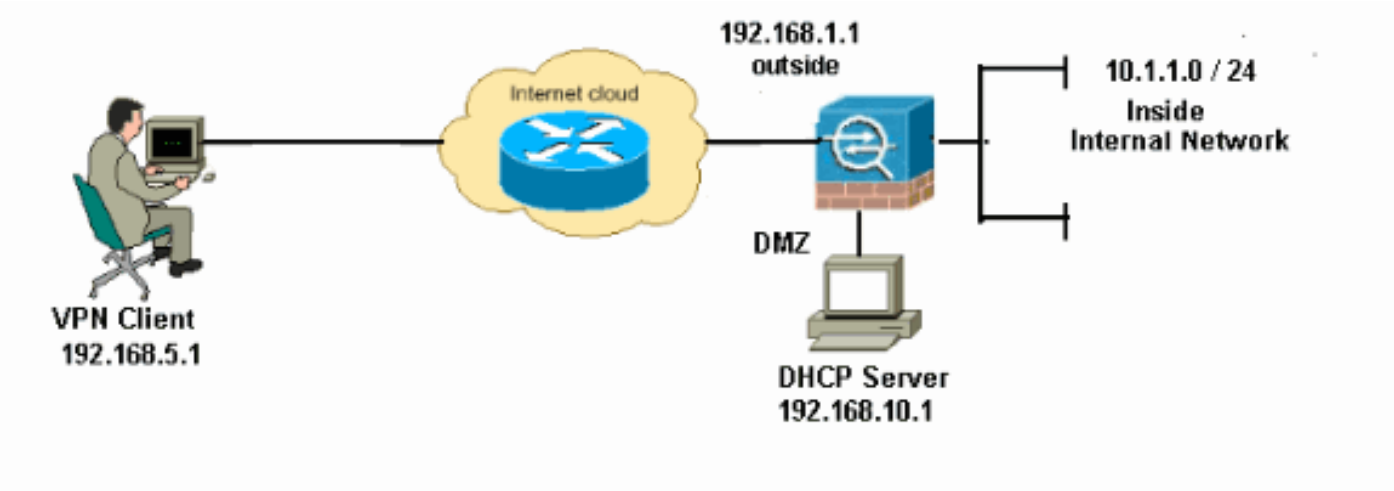
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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:



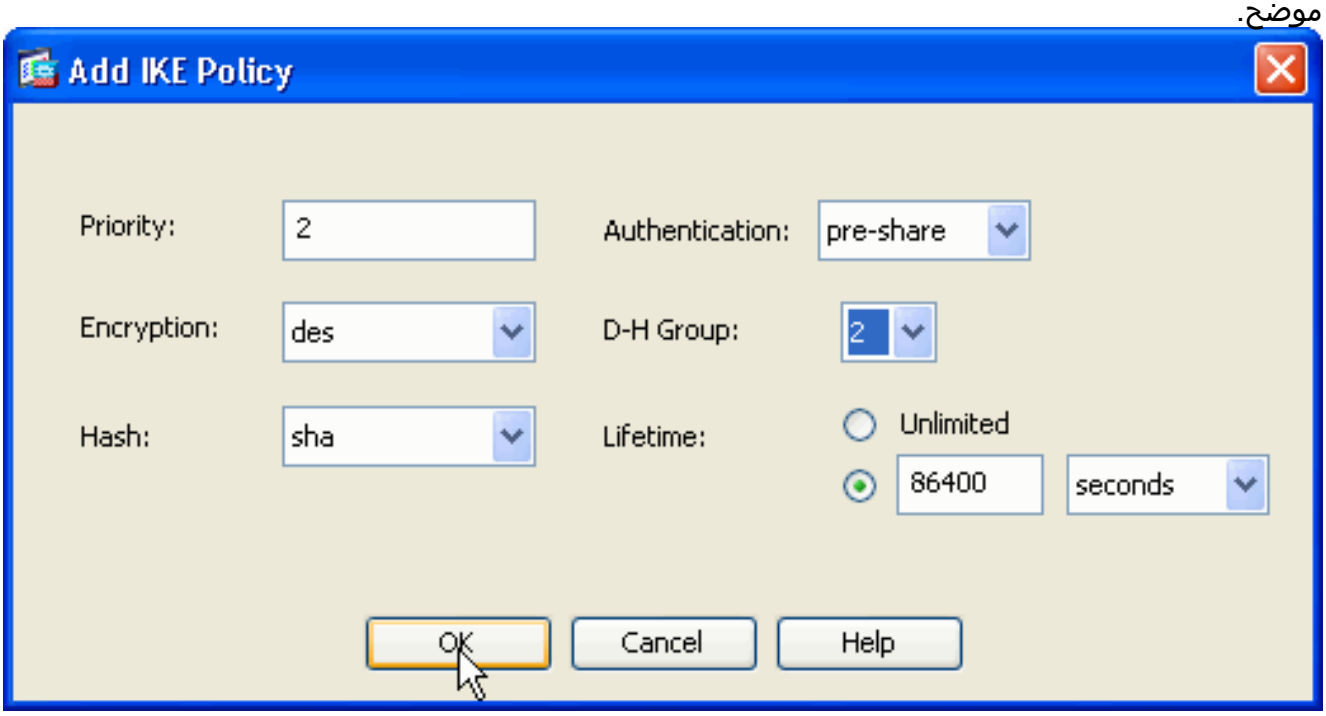
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

تكوين شبكة VPN للوصول عن بعد (IPSec)

إجراء ASDM

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

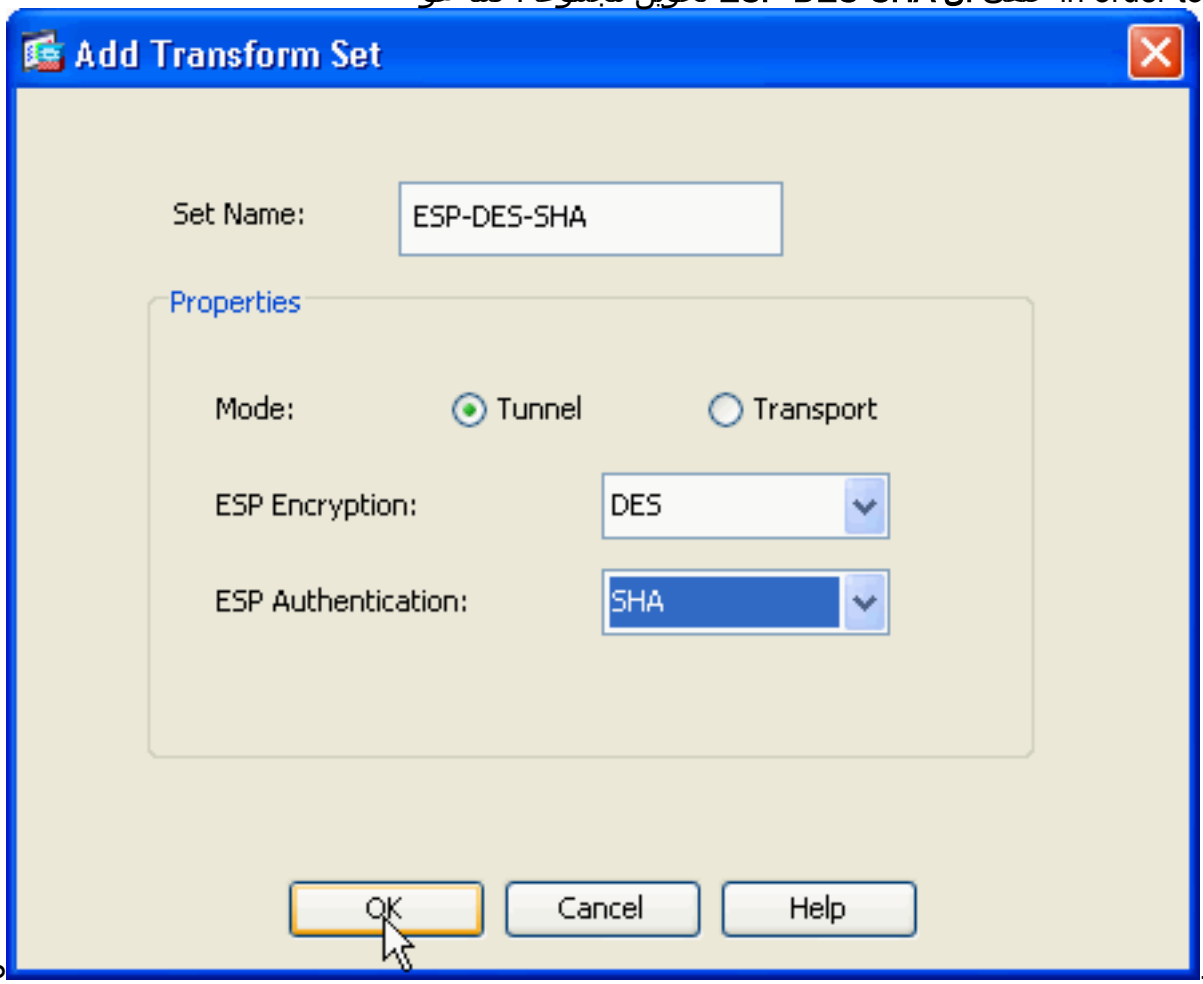
1. أختر **تكوين > Remote Access VPN (الوصول عن بعد) > Network (العميل) > Access > Advanced > IPSec > سياسات** in order to **IKE > Add** خلقت ISAKMP Policy 2، كما هو موضح.



طقطقة **ok** و**يطبق**.

2. أخترت **تشكيل>Remote Access VPN>شبكة (زبون) منفذ > متقدم > IPSec > مجموعات تحويل IPSec >**

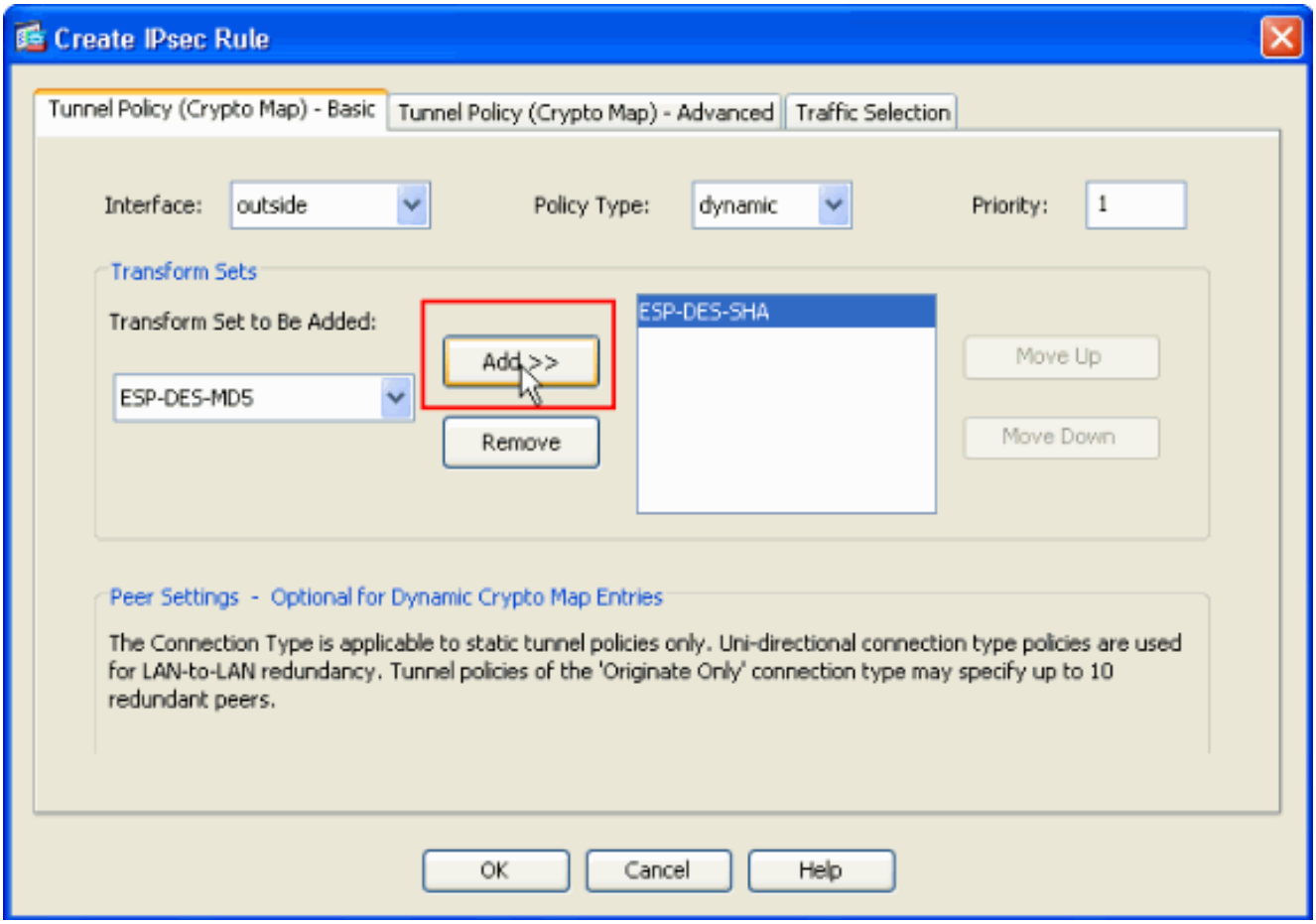
إضافة in order to خلقت **ESP-DES-SHA ال** تحويل مجموعة، كما هو



موضح. طقة

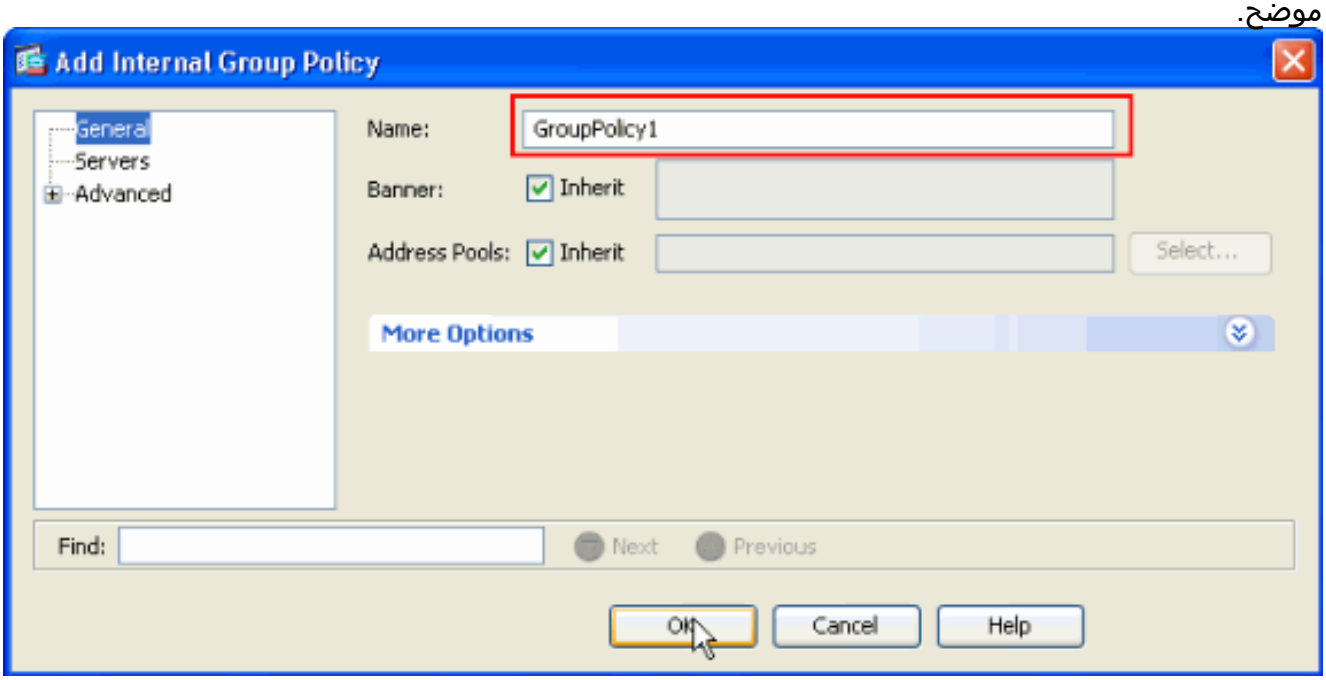
طقة **ok** و**يطبق**.

3. أختر **Configuration > Remote Access VPN (الوصول عن بعد) > Network (العميل) > Access** **Crypto Maps > IPSec > Advanced (خرائط التشفير) > Add** لإنشاء خريطة تشفير باستخدام السياسة الديناميكية للأولوية 1، كما هو موضح.



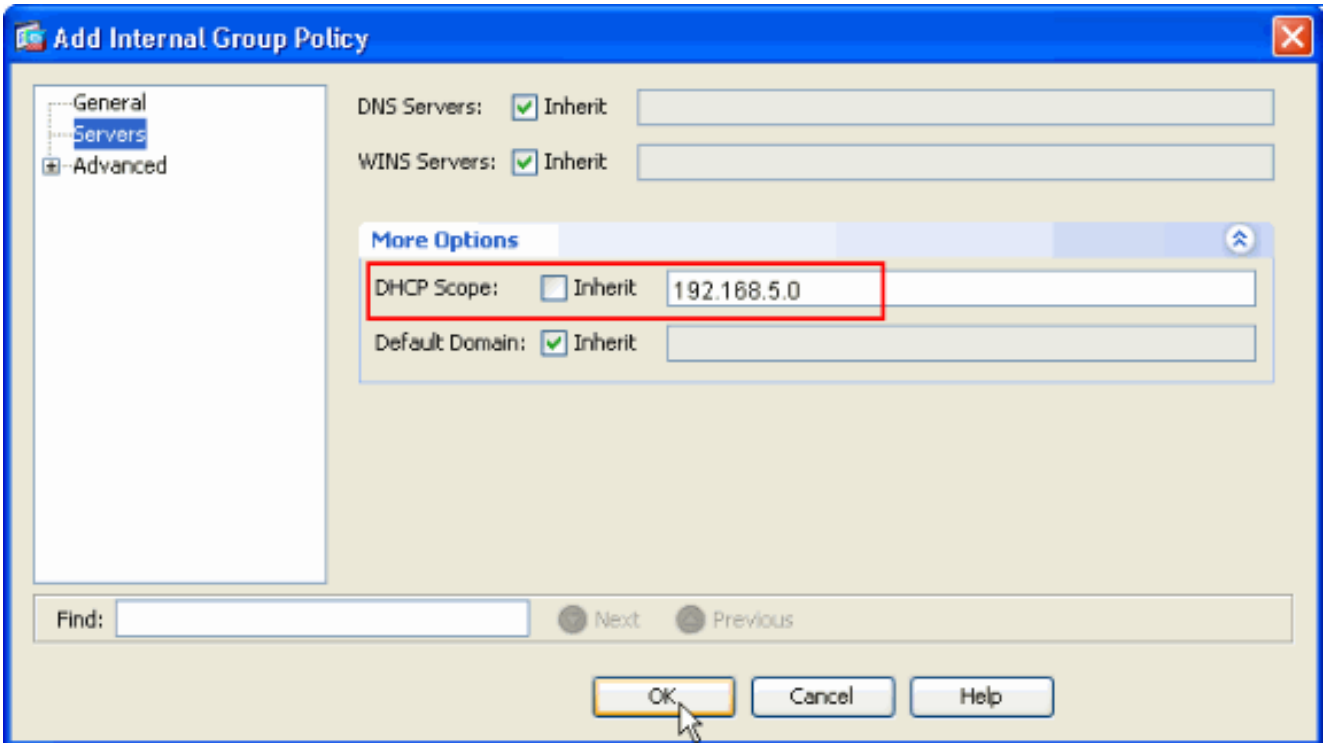
طقطقة **ok** و**يطبق**.

4. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>متقدم>مجموعة نهج>إضافة>داخلي مجموعة** سياسة in order to خلقت مجموعة سياسة (مثلا **GroupPolicy1**)، كما هو موضح.



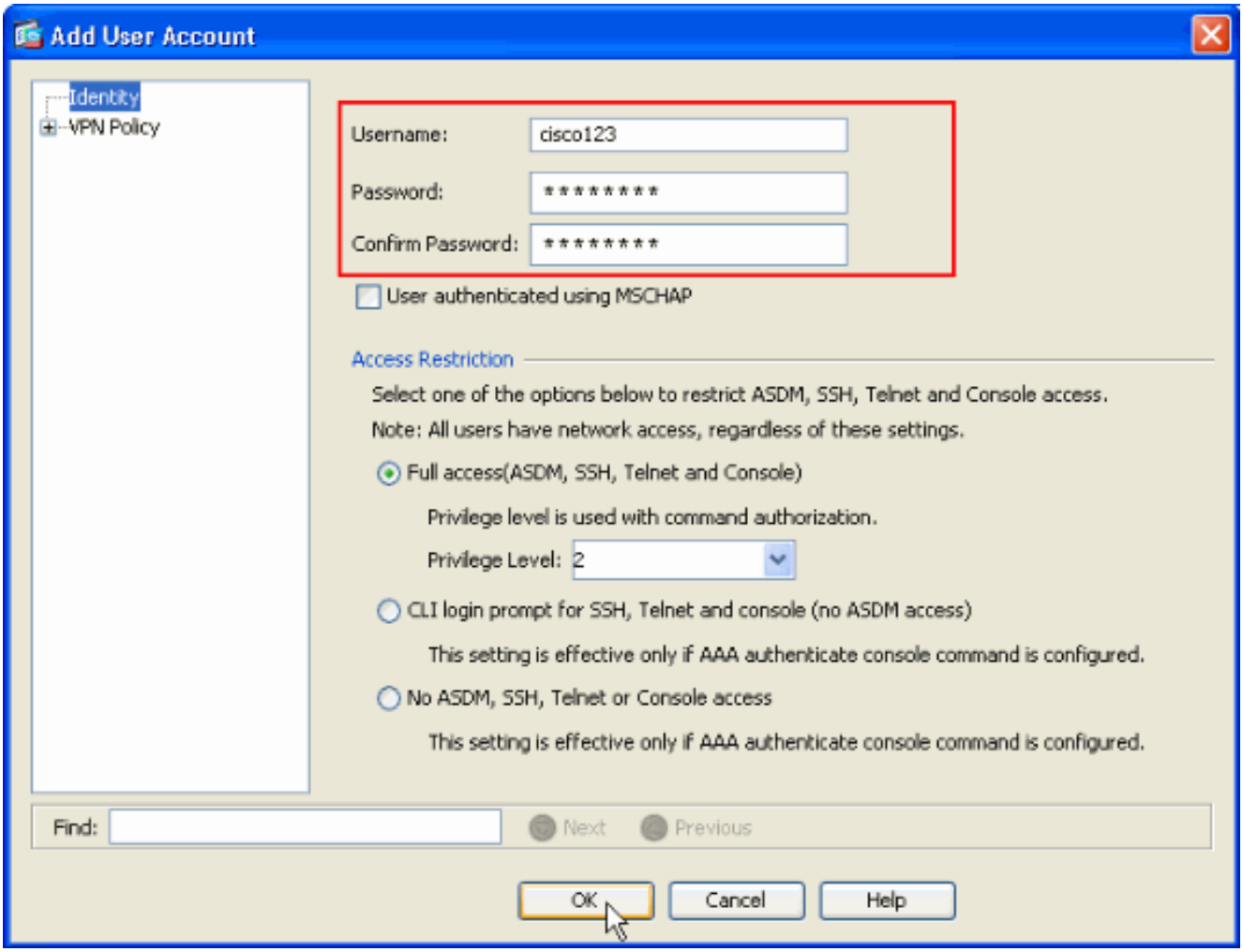
طقطقة **ok** و**يطبق**.

5. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>متقدم>مجموعة نهج>إضافة>داخلي مجموعة نهج>نادل>** in order to شكلت **ال DHCP مجال** ل ال VPN زبون مستعمل أن يكون عينت ديناميكيا.



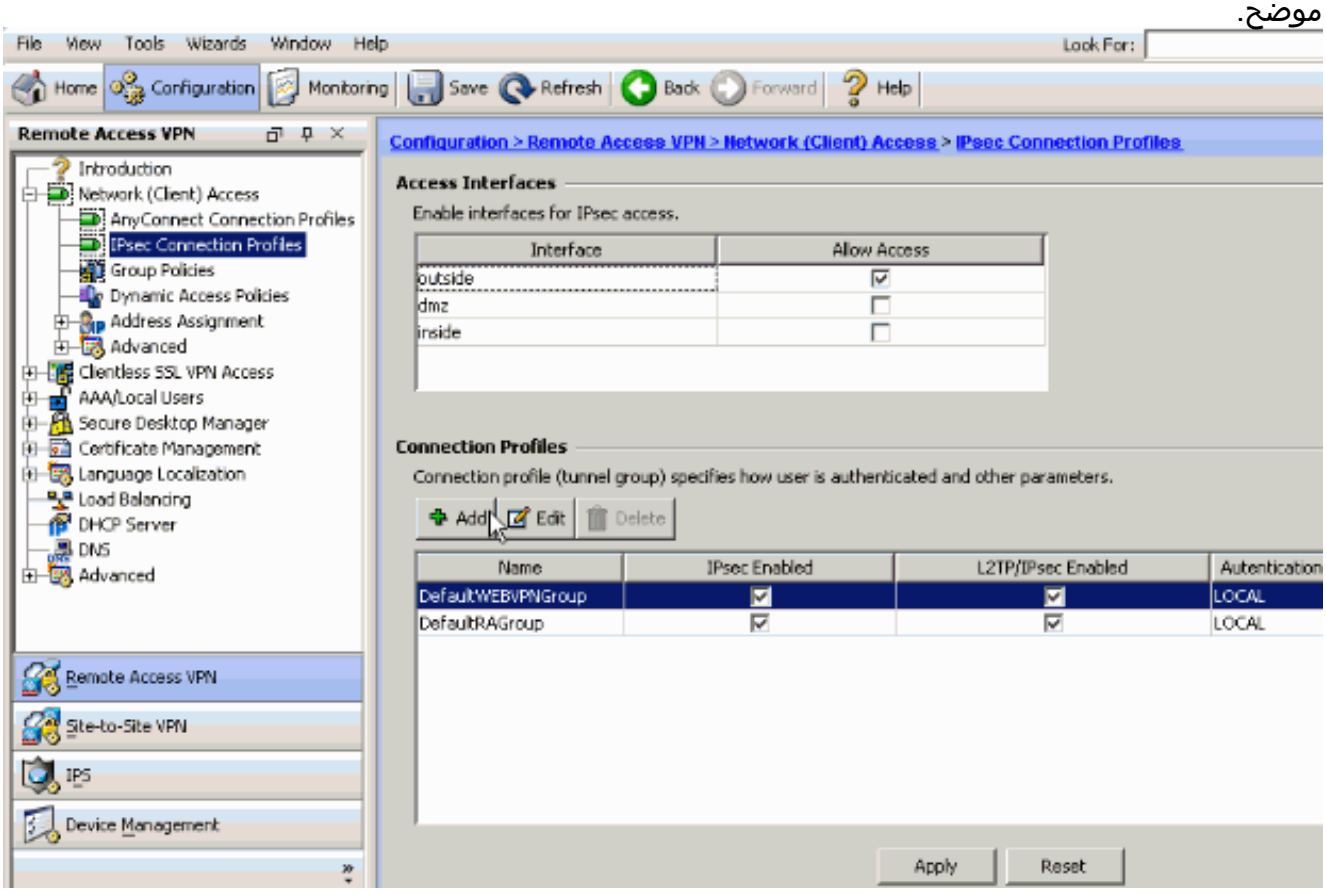
طقطقة **ok** و**يطبق**.**ملاحظة:** تكوين نطاق DHCP إختياري. راجع تكوين عنونة DHCP للحصول على مزيد من المعلومات.

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

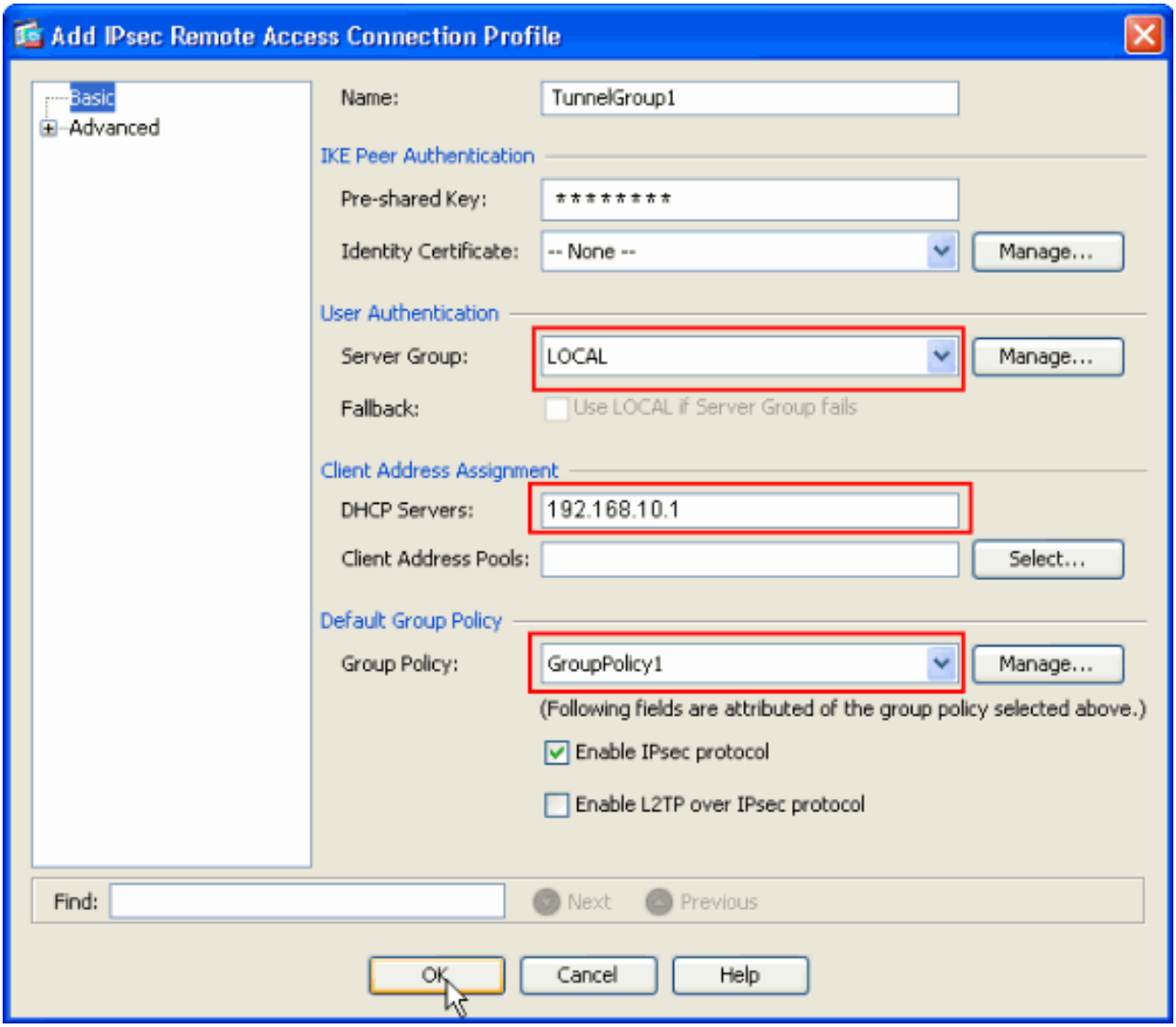


7. أخترت **تشكيل**>Remote Access VPN>**شبكة (زبون) منفذ**>IPSec **توصيل توصيفات**>**إضافة**>in order to أضفت مجموعة نفق (مثلا، **TunnelGroup1** والمفتاح سابق النشر ك Cisco123)، كما هو

موضح.

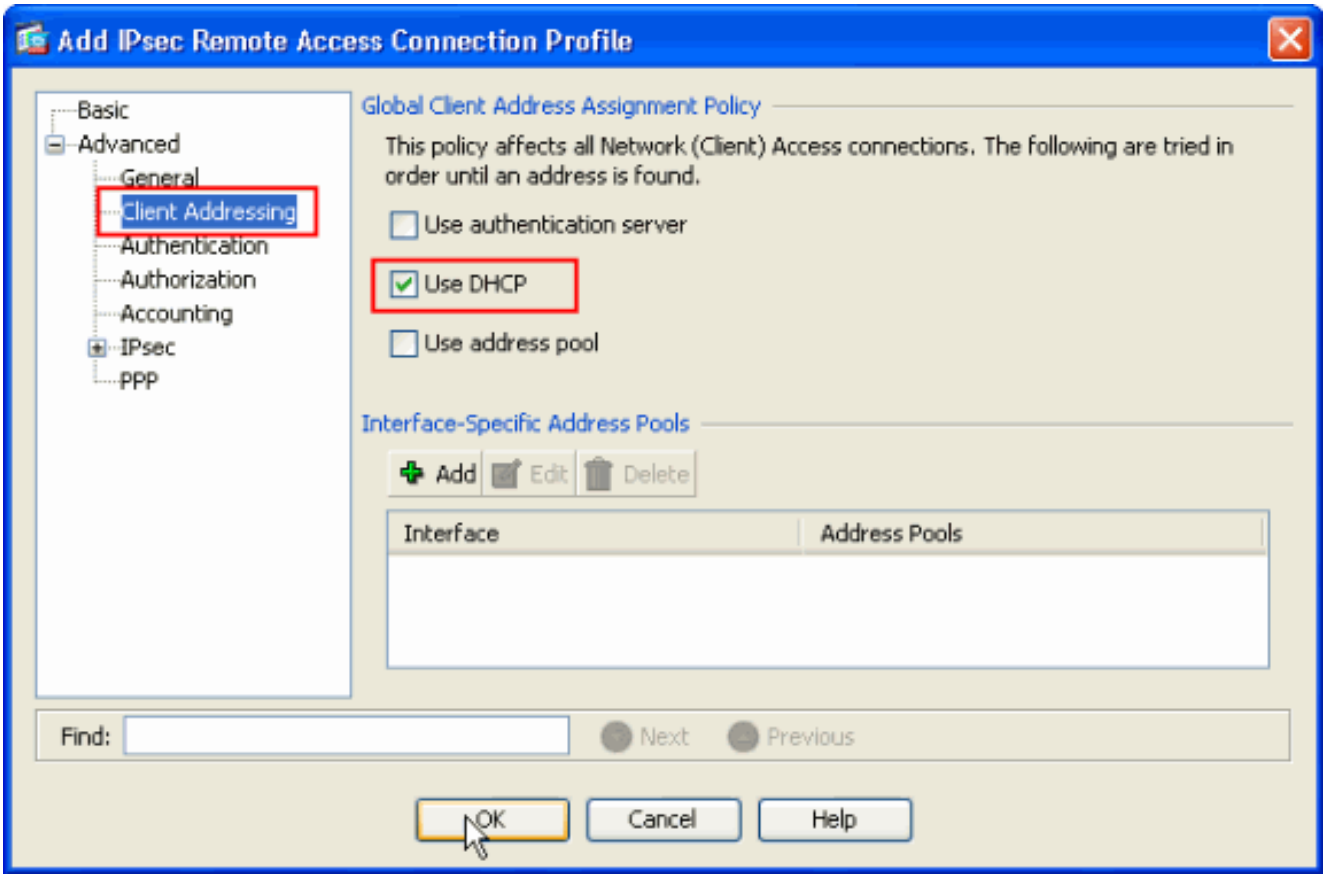


تحت علامة التبويب **أساسي** أختر مجموعة الخادم كمحلية **لحقل مصادقة المستخدم**.أختر GroupPolicy1 كنهج المجموعة لحقل نهج المجموعة الافتراضي.قم بتوفير عنوان IP لخادم DHCP في المساحة المتوفرة **لخوادم** DHCP.



وانقر فوق **OK**.

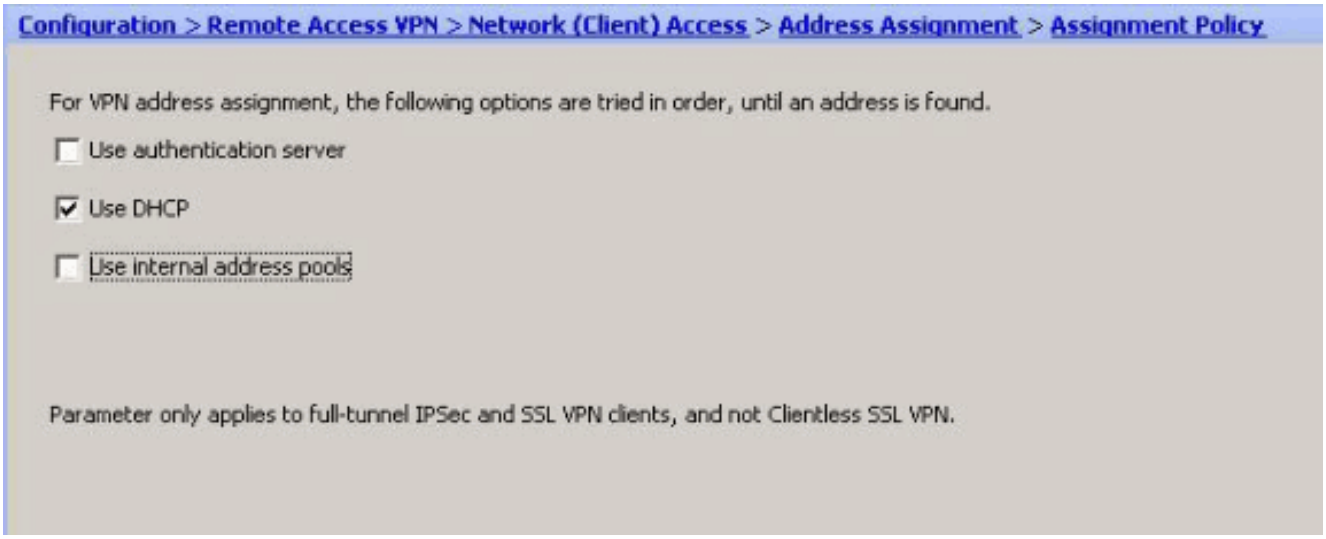
8. أخترت **متقدم>زبون عنونة >** وفحصت ال **يستعمل DHCP** تدقيق صندوق ل ال DHCP نادل أن يعين عنوان إلى ال VPN زبون.**ملاحظة:** تأكد من إلغاء تحديد خانات الاختيار **لاستخدام خادم المصادقة وإستخدام تجمع العناوين**.



تكوين ASDM 6.x

يعمل تكوين ASDM نفسه بشكل جيد مع الإصدار x.6 من ASDM، باستثناء بعض التعديلات الطفيفة فيما يتعلق بمسارات ASDM. تحتوي مسارات ASDM إلى حقول معينة على تباين من الإصدار 6.2 من ASDM والإصدارات الأحدث. وفيما يلي قائمة بالتعديلات التي أدخلت على المسارات الموجودة. هنا لا يتم إرفاق الصور الرسومية في الحالات التي تظل فيها كما هي لجميع إصدارات ASDM الرئيسية.

1. التكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > متقدم > IPSec > سياسات IKE > إضافة
2. التكوين > IPSec > Advanced > Network (Client) Access > Remote Access VPN > مجموعات تحويل IPSec > إضافة
3. التكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > متقدم > IPSec > خرائط التشفير > إضافة
4. أختر تكوين > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > Group Policy (نهج المجموعة) > Internal Group Policy > Add
5. أختر تكوين > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access (الوصول إلى الشبكة) > Group Policy (نهج المجموعة الداخلية) > Internal Group Policies> Add (نهج المجموعة الداخلية) > Servers
6. أختر تكوين > Remote Access VPN (الوصول عن بعد) > إعداد AAA/المستخدمين المحليين > المستخدمين المحليين > إضافة
7. التكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > توصيفات توصيل IPSec > إضافة
8. أختر تكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > تعيين العنوان > سياسة التعيين



كل هذه الخيارات الثلاثة مكنت بشكل افتراضي. يتبع Cisco ASA نفس الأمر لتعيين عناوين إلى عملاء VPN. عندما تقوم بإلغاء تحديد الخيارين الآخرين، لا يتحقق Cisco ASA من خيارات خادم AAA والتجمع المحلي. يمكن التحقق من الخيارات الافتراضية الممكنة بواسطة **show run all | في** أمر **vpn-add**. هذا نموذج للمخرجات لمرجع الخاص بك:

```
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0
```

أحلت ل كثير معلومة حول هذا أمر، vpn-addr-assign .

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.

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 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

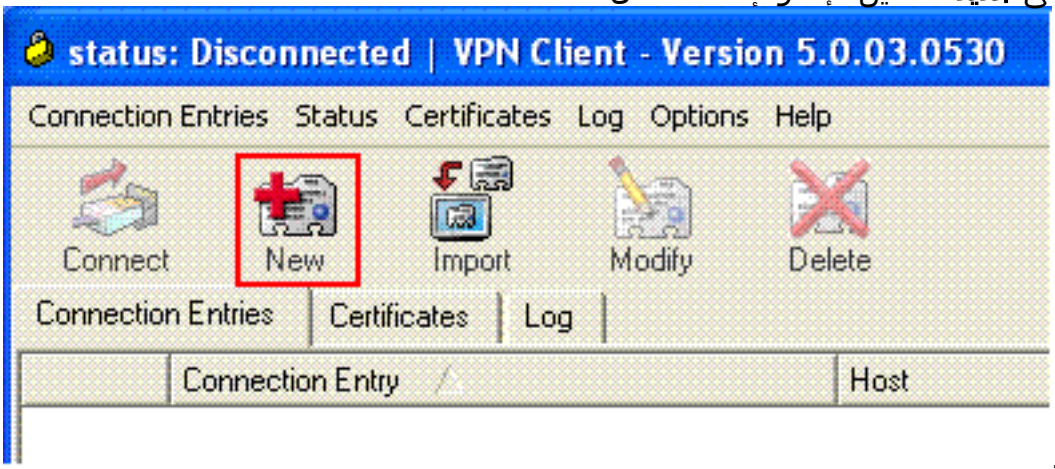
```
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
  h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
       0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
       disconnect 0:02:00 timeout uauth 0:05:00 absolute
      dynamic-access-policy-record DfltAccessPolicy http
server enable 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 DHCP Server and now by AAA or the Local
       pool.The CLI vpn-addr-assign dhcp for VPN address
     assignment through DHCP Server is hidden in the CLI
                              .provided by show run command

                                      no vpn-addr-assign aaa
                                    no vpn-addr-assign local

                                             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 GroupPolicy1 internal
                             group-policy GroupPolicy1 attributes
```

```
        define the DHCP network scope in the group ---!
policy.This configuration is Optional dhcp-network-scope
                                                192.168.5.0

    In order to identify remote access users to the ---!
        Security Appliance, !--- you can also configure
usernames and passwords on the device. username cisco123
                        password ffIRPGpDSOJh9YLq encrypted

Create a new tunnel group and set the connection !- ---!
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access !--- Define the DHCP server address to the
        tunnel group. tunnel-group TunnelGroup1 general-
attributes default-group-policy GroupPolicy1 dhcp-server
                                                192.168.10.1

         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

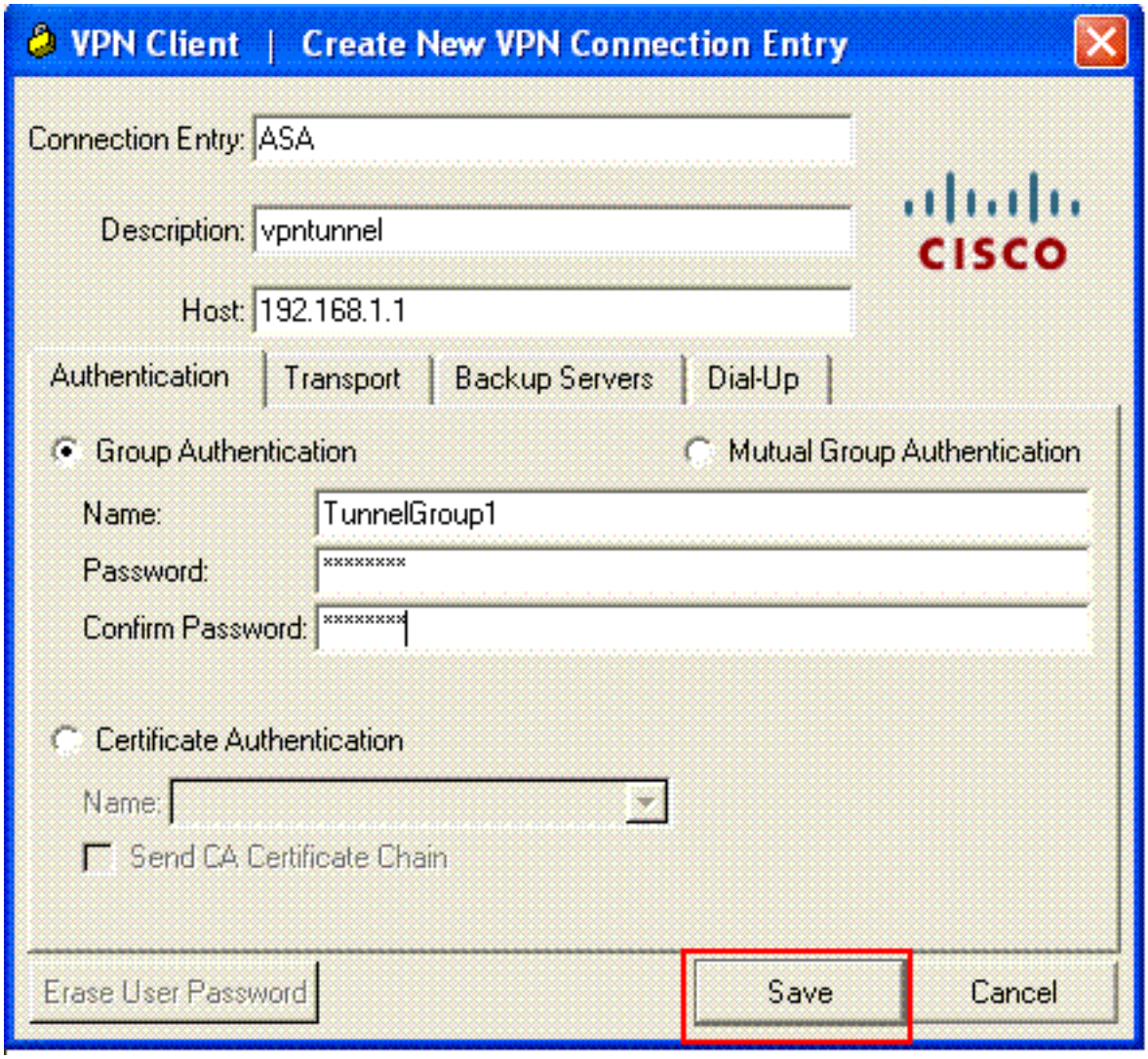
حاول الاتصال ب Cisco ASA باستخدام عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

1. حدد **Start (البدء) > Programs (البرامج) > Cisco Systems VPN Client (عميل الشبكة الخاصة الظاهرية) من Cisco (VPN)**.
2. انقر على **جديد** لتشغيل الإطار "إنشاء اتصال VPN



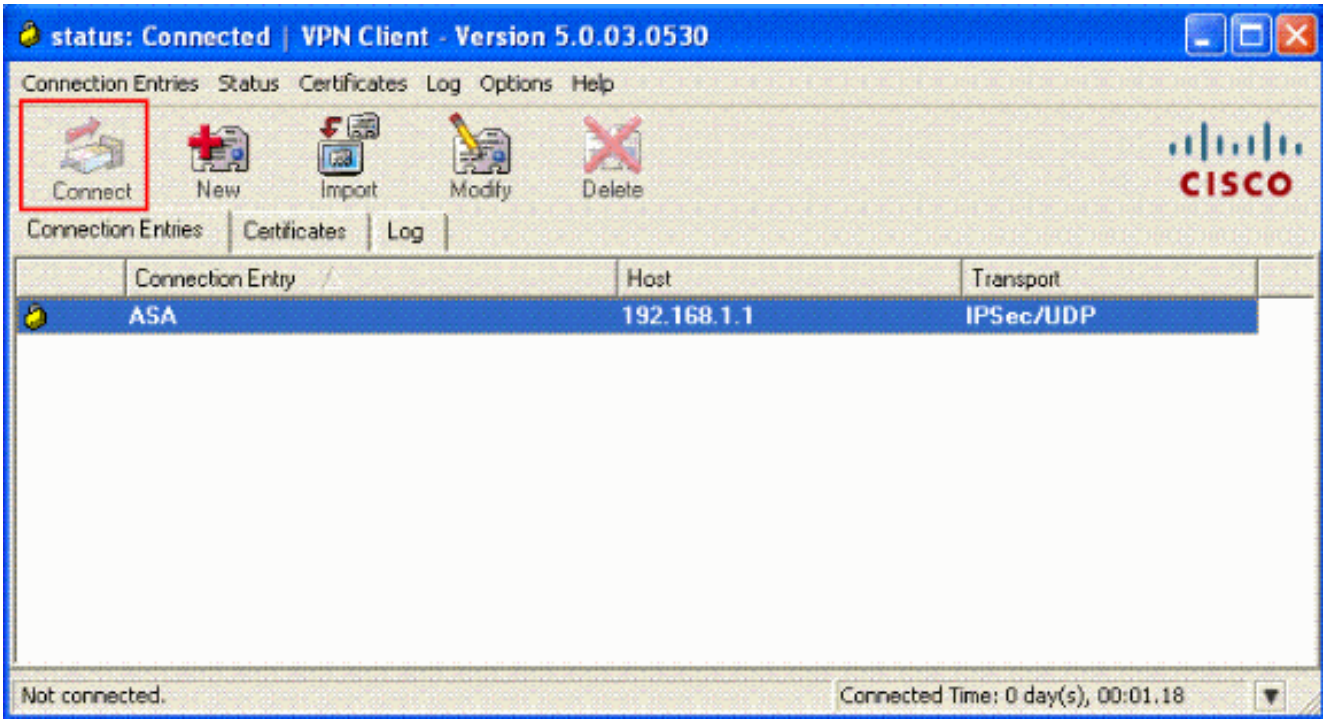
جديد".

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

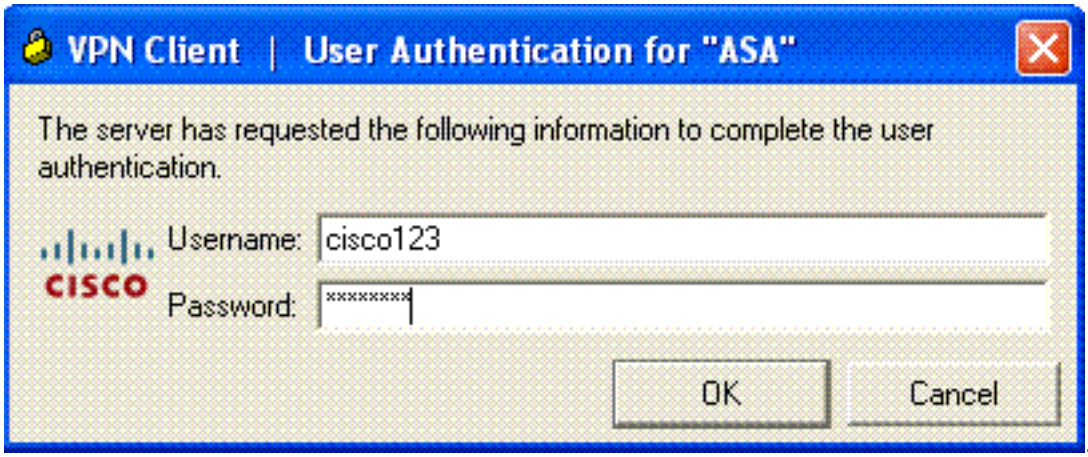


حفظ.

4. انقر على الاتصال الذي تريد إستخدامه وانقر فوق **الاتصال** من الإطار الرئيسي لعميل شبكة VPN.

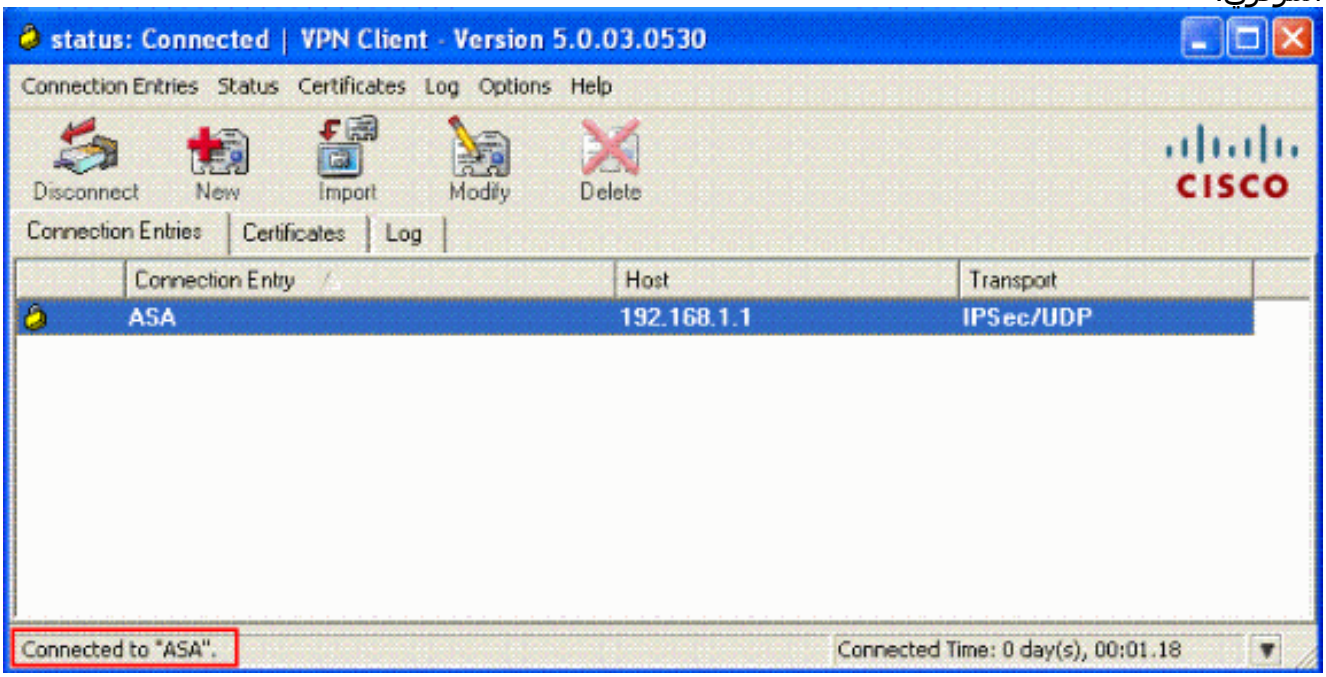


5. عندما يطلب منك، أدخل **اسم المستخدم : cisco123** و**كلمة المرور : cisco123** كما تم تكوينها في ASA أعلاه ل Xauth، وانقر فوق **موافق** للاتصال بالشبكة

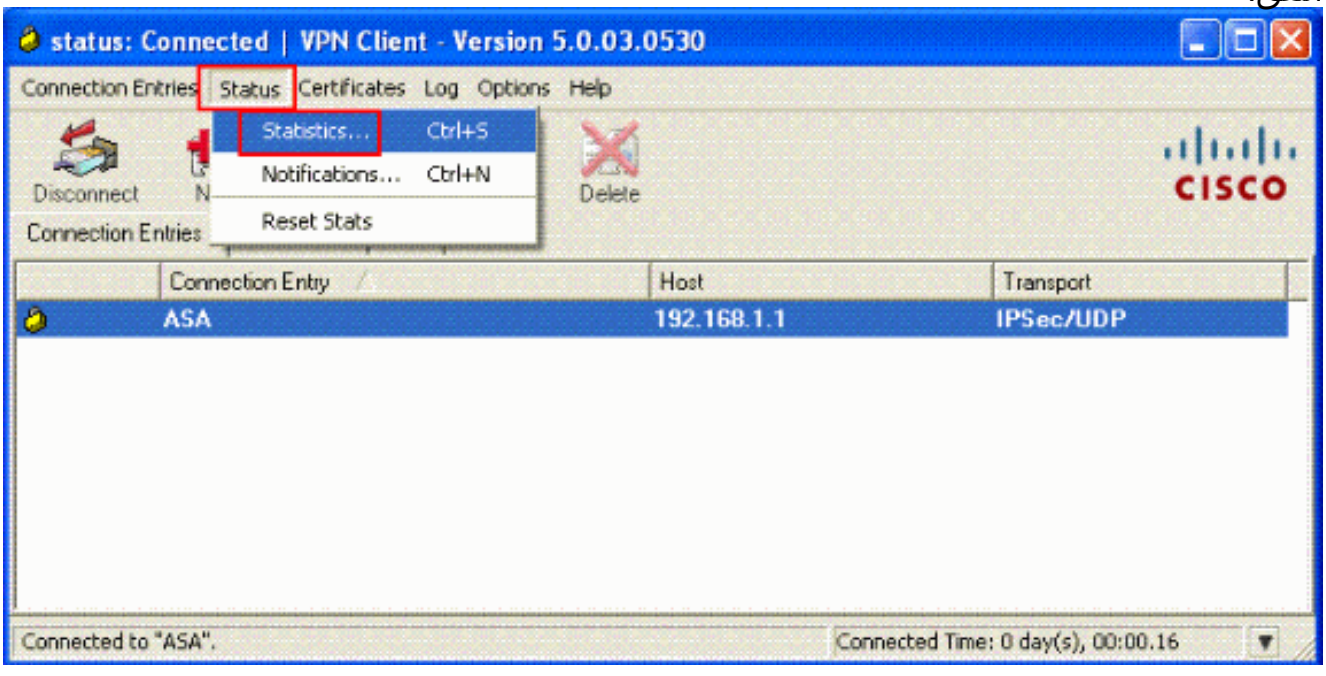


البعيدة.

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



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



التحقق من الصحة

إظهار الأوامر

أستخدم 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.

```
ASA #show crypto ipsec sa
                                    interface: outside
                Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.1

                  (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
                (remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0
                                current_peer: 192.168.1.2, username: cisco123
                                dynamic allocated peer ip: 192.168.5.1

                      pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55#
                      pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55#
                                  pkts compressed: 0, #pkts decompressed: 0#
          pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0#
           pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
       PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                          send errors: 0, #recv errors: 0#

        local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2

                           path mtu 1500, ipsec overhead 58, media mtu 1500
                                  current outbound spi: C2C25E2B

                                                       :inbound esp sas
                                        (spi: 0x69F8C639 (1777911353
                                transform: esp-des esp-md5-hmac none
                                     { ,in use settings ={RA, Tunnel
                           slot: 0, conn_id: 40960, crypto-map: dynmap
                        sa timing: remaining key lifetime (sec): 28337
                                                  IV size: 8 bytes
                                       replay detection support: Y
                                                      :outbound esp sas
                                        (spi: 0xC2C25E2B (3267517995
                                transform: esp-des esp-md5-hmac none
                                     { ,in use settings ={RA, Tunnel
                           slot: 0, conn_id: 40960, crypto-map: dynmap
                        sa timing: remaining key lifetime (sec): 28337
                                                  IV size: 8 bytes
                                       replay detection support: Y

ASA #show crypto isakmp sa

                                                       Active SA: 1
        (Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                                       Total IKE SA: 1

                                                  IKE Peer: 192.168.1.2   1
                          Type    : user              Role    : responder
                          Rekey   : no                State   : AM_ACTIVE
```

استكشاف الأخطاء وإصلاحها

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

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

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 شبكات 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 ips 7**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp 7**—يعرض مفاوضات ISAKMP للمرحلة 1.

إخراج تصحيح الأخطاء للعينة

- ASA، الإصدار 8.0
- Windows ل VPN Client 5.0

ASA، الإصدار 8.0

```
ASA#debug crypto isakmp 7
          Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR)
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le + (13)
                                                                      ngth : 856
          Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
          Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
      Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
       Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
          Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
         Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
          Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
         Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
               Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
         Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
     Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
         tion capability flags:  Main Mode:        True  Aggressive Mode:  False
         Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
                                                                           ID
          Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
```

```
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
                                                                    nelGroup1
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
                                                                  g IKE SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
            oposal # 1, Transform # 13 acceptable  Matches global IKE entry # 2
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                ing ISAKMP SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                  ing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                               ing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin
                                                             ...g keys for Responder
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                  ing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                ing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
                                                                hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                            ing Cisco Unity VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                               ing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                ing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                            ing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                 ing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti
                                                        ga/Cisco VPN3000/Cisco ASA GW VID
 (Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0
 with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le + (13)
                                                                    ngth : 368
(Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0
with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE
                                                              total length : 116 (0)
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
                                                                  g hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
                                                                hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
                                                                  g notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
                                                                   g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
            (g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
                                                                   g VID payload
 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received
                                                                 Cisco Unity client VID
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                ing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
                                                                  ing qm hash payload
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a
  1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8
 a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a
                                                                    !ttr(): Enter
```

```
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
                                                          .g MODE_CFG Reply attributes
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                          IKEGetUserAttributes: primary DNS = cleared ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                        IKEGetUserAttributes: secondary DNS = cleared ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                         IKEGetUserAttributes: primary WINS = cleared ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                       IKEGetUserAttributes: secondary WINS = cleared ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                     IKEGetUserAttributes: IP Compression = disabled ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
             IKEGetUserAttributes: Split Tunneling Policy = Disabled ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
             IKEGetUserAttributes: Browser Proxy Setting = no-modify ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
          IKEGetUserAttributes: Browser Proxy Bypass Local = disable ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                                                    .User (cisco123) authenticated ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       constructing blank hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                         constructing qm hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143
  60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14
 360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                              !process_attr(): Enter ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                        Processing cfg ACK attributes ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26
63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                              !process_attr(): Enter ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                     Processing cfg Request attributes ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                          !MODE_CFG: Received request for IPV4 address ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                        !MODE_CFG: Received request for IPV4 net mask ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                   !MODE_CFG: Received request for DNS server address ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                  !MODE_CFG: Received request for WINS server address ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                          Received unsupported transaction mode attribute: 5 ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                !MODE_CFG: Received request for Banner ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                       !MODE_CFG: Received request for Save PW setting ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                  !MODE_CFG: Received request for Default Domain Name ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                    !MODE_CFG: Received request for Split Tunnel List ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                             !MODE_CFG: Received request for Split DNS ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                           !MODE_CFG: Received request for PFS setting ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
         !MODE_CFG: Received request for Client Browser Proxy Setting ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
               !MODE_CFG: Received request for backup ip-sec peer list ,92.168.1.2
```

```
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                        Received unknown transaction mode attribute: 28684 ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                 !MODE_CFG: Received request for Application Version ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
              Client Type: WinNT  Client Application Version: 5.0.03.0530 ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                              !MODE_CFG: Received request for FWTYPE ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12 ,92.168.1.2
                                                                              !3
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                             !MODE_CFG: Received request for UDP Port ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e ,92.168.1.2
                                                                  (nabled
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                    Assigned private IP address 192.168.5.1 to remote user ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                    constructing blank hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                !Send Client Browser Proxy Attributes ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu ,92.168.1.2
                                                      ded in the mode-cfg reply
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                      constructing qm hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266
 3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
    Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
     Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                                                  PHASE 1 COMPLETED ,1.2.
 :Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection
                                                                        DPD
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                 .Starting P1 rekey timer: 950 seconds ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                          sending notify message ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                    constructing blank hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                      constructing qm hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44
with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84 (35669
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
+ (1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5
                                                  NONE (0) total length : 1022
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                           processing hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                            processing SA payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                         processing nonce payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                            processing ID payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
Received remote Proxy Host data in ID Payload:  Address 192.168.5.1, Proto ,1.2.
                                                                  col 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                            processing ID payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
```

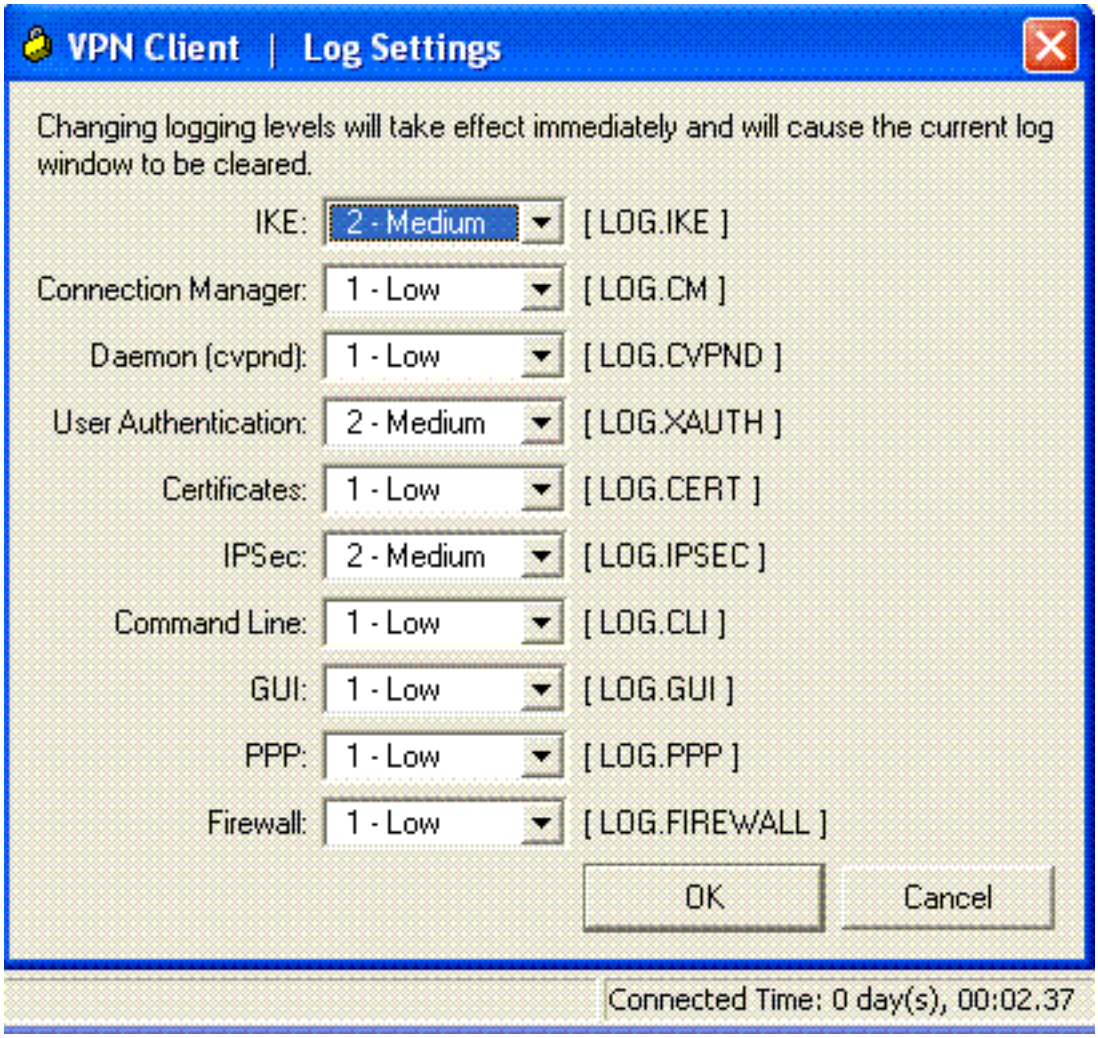
```
Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask ,1.2.
                                                  Protocol 0, Port 0 ,0.0.0.0
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                                       QM IsRekeyed old sa not found by addr ,1.2.
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                            IKE Remote Peer configured for crypto map: dynmap ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                         processing IPSec SA payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
IPSec SA Proposal # 14, Transform # 1 acceptable  Matches global IPS ,92.168.1.2
                                                                 ec SA entry # 10
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                                                  !IKE: requesting SPI ,1.2.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                          IKE got SPI from key engine: SPI = 0x31de01d8 ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       oakley constucting quick mode ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       constructing blank hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       constructing IPSec SA payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon ,1.2.
                                                                          ds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                    constructing IPSec nonce payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                            constructing proxy ID ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                          :Transmitting Proxy Id ,92.168.1.2
                                  Remote host: 192.168.5.1  Protocol 0  Port 0
                          Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                       Sending RESPONDER LIFETIME notification to Initiator ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       constructing qm hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541
 + (f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5
                                       NOTIFY (11) + NONE (0) total length : 176
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
            1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                          processing hash payload ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                           loading all IPSEC SAs ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       !Generating Quick Mode Key ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                                       !Generating Quick Mode Key ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
 Security negotiation complete for User (cisco123)  Responder, Inbound SPI ,1.2.
                                       0x31de01d8, Outbound SPI = 0x8b7597a9 =
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                     IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9 ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                        Pitcher: received KEY_UPDATE, spi 0x31de01d8 ,92.168.1.2
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
                               .Starting P2 rekey timer: 27360 seconds ,92.168.1.2
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                       Adding static route for client address: 192.168.5.1 ,1.2.
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
                                       (PHASE 2 COMPLETED (msgid=541f8e43 ,1.2.
Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78
f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
```

ASA#**debug crypto ipsec 7**

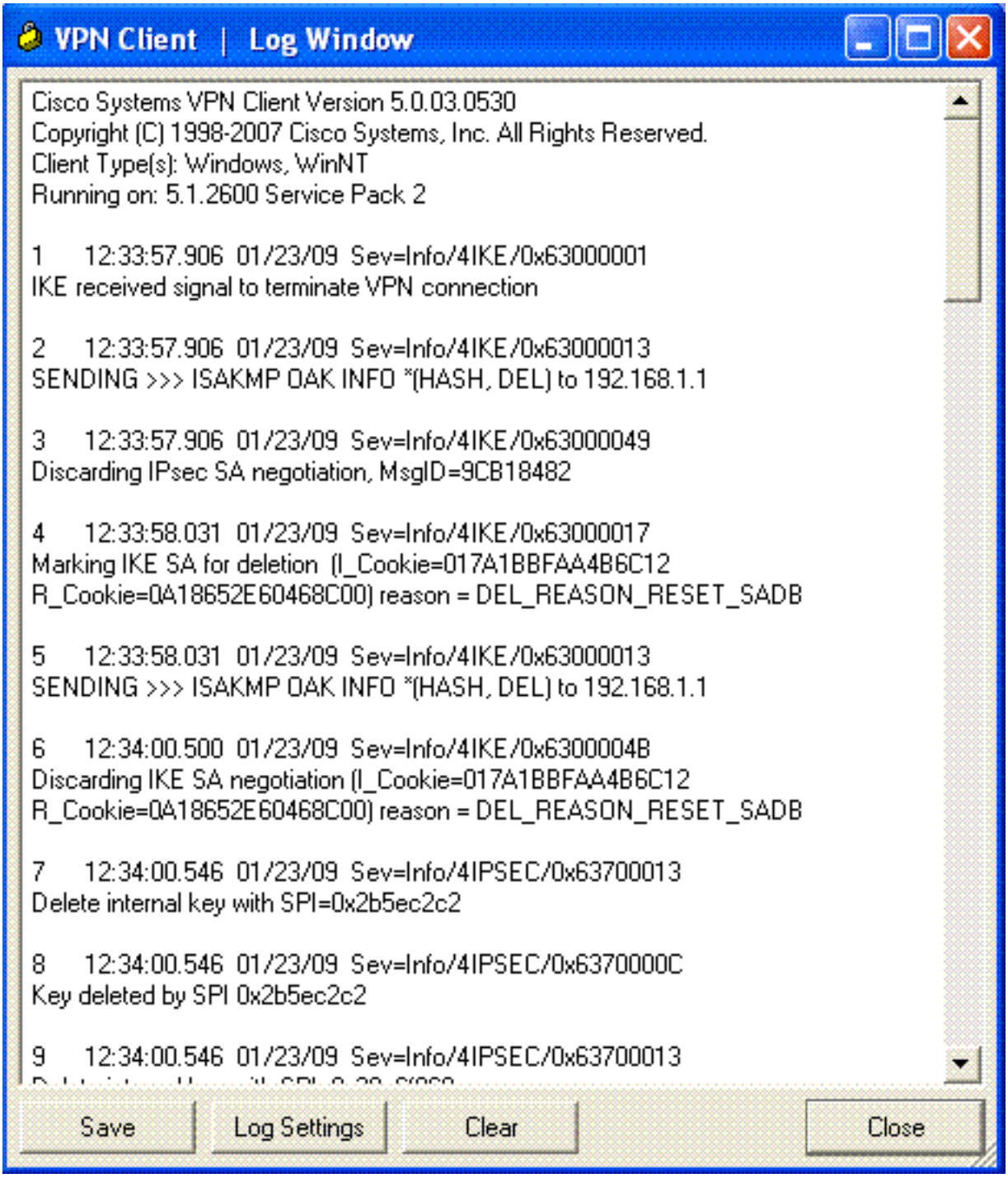
Deletes the old SAs. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: *---!* 0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 *!--- Creates new SAs.* ASA# IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI : 0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0 bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context 0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr: 192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0

Windows J VPN Client 5.0

حدد **سجل > إعدادات سجل** لتمكين مستويات السجل في عميل VPN.



حدد **سجل > سجل نافذة** لعرض إدخالات السجل في عميل VPN.



معلومات ذات صلة

- صفحة دعم أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- 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

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).