ASA/PIX 8.x: تفويض RADIUS (ACS 4.x) للوصول إلى VPN باستخدام قائمة التحكم في الوصول (ACL) القابلة للتنزيل مع CLI ومثال تكوين ASDM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان لمصادقة المستخدمين للوصول إلى الشبكة. ونظرا لأنه يمكنك تمكين تراخيص RADIUS ضمنيا، فلا يحتوي هذا القسم على أي معلومات حول تكوين تفويض RADIUS على جهاز الأمان. وهو يوفر معلومات حول كيفية معالجة جهاز الأمان لمعلومات قائمة الوصول التي يتم تلقيها من خوادم RADIUS.

يمكنك تكوين خادم RADIUS لتنزيل قائمة الوصول إلى جهاز الأمان أو اسم قائمة الوصول في وقت المصادقة. يسمح للمستخدم فقط بما هو مسموح به في قائمة الوصول الخاصة بالمستخدم.

قوائم الوصول القابلة للتنزيل هي أكثر الوسائل قابلية للتطوير عند إستخدام مصدر المحتوى الإضافي الآمن من Cisco لتوفير قوائم الوصول المناسبة لكل مستخدم. لمزيد من المعلومات حول ميزات قائمة الوصول القابلة للتنزيل و Cisco Secure ACS، ارجع إلى تكوين خادم RADIUS لإرسال قوائم التحكم في الوصول القابلة للتنزيل وقوائم التحكم في الوصول إلى IP القابلة للتنزيل.

ارجع إلى ASA 8.3 والإصدارات الأحدث: تفويض RADIUS (ACS 5.x) للوصول إلى VPN باستخدام قائمة التحكم في الوصول (ACL) القابلة للتنزيل مع CLI ومثال تكوين ASDM للتكوين المتطابق على Cisco ASA مع الإصدارات 8.3 والإصدارات الأحدث.

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
- Cisco Adaptive Security Device Manager، الإصدار x.5 والإصدارات الأحدث
- Cisco VPN Client الإصدار x.4 والإصدارات الأحدث
- Cisco Secure Access Control Server 4.x

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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

يمكنك إستخدام قوائم التحكم في الوصول إلى IP القابلة للتنزيل لإنشاء مجموعات من تعريفات قائمة التحكم في الوصول (ACL) التي يمكنك تطبيقها على العديد من المستخدمين أو مجموعات المستخدمين. تسمى هذه المجموعات من تعريفات قائمة التحكم بالوصول (ACL) محتويات قائمة التحكم بالوصول (ACL). أيضا، عندما تقوم بدمج NAFs، فإنك تتحكم في محتويات قائمة التحكم في الوصول (ACL) التي يتم إرسالها إلى عميل AAA والذي يسعى المستخدم إلى الوصول منه. وهذا يعني أن قائمة التحكم في الوصول إلى IP القابلة للتنزيل تتضمن تعريفا واحدا أو أكثر من تعريفات محتوى قائمة التحكم في الوصول (ACL)، ويقترن كل واحد منها مع NAF أو (بشكل افتراضي) مرتبط بجميع عملاء AAA. تتحكم ميزة التحكم في الشبكة (NAF) في إمكانية تطبيق محتويات قائمة التحكم في

الوصول (ACL) المحددة وفقا لعنوان IP الخاص بعميل AAA. لمزيد من المعلومات حول NAFs وكيف تنظم قوائم التحكم في الوصول إلى IP القابلة للتنزيل، راجع حول عوامل تصفية الوصول إلى الشبكة.

تعمل قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل بهذه الطريقة:

1. عندما يمنح ACS للمستخدم حق الوصول إلى الشبكة، يحدد ACS ما إذا كانت قائمة التحكم في الوصول إلى IP قابلة للتنزيل يتم تعيينها لذلك المستخدم أو لمجموعة المستخدم.
2. إذا قام ACS بتحديد موقع قائمة تحكم في الوصول إلى IP قابلة للتنزيل تم تعيينها للمستخدم أو مجموعة المستخدم، فإنه يحدد ما إذا كان إدخال محتوى ACL مقترنا بعميل AAA الذي أرسل طلب مصادقة RADIUS.
3. يرسل ACS، كجزء من جلسة عمل المستخدم، حزمة RADIUS لقبول الوصول، سمة تحدد قائمة التحكم في الوصول (ACL) المسماة، وإصدار قائمة التحكم في الوصول (ACL) المسماة.
4. إذا رد عميل AAA بأنه لا يحتوي على الإصدار الحالي من قائمة التحكم في الوصول (ACL) في ذاكرة التخزين المؤقت الخاصة به، أي أن قائمة التحكم في الوصول (ACL) جديدة أو تم تغييرها، فإن ACS يرسل قائمة التحكم في الوصول (ACL) (جديدة أو محدثة) إلى الجهاز.

قوائم التحكم في الوصول إلى IP القابلة للتنزيل هي بديل لتكوين قوائم التحكم في الوصول (ACL) في سمة [26/9/1 RADIUS Cisco-AV-pair] لكل مستخدم أو مجموعة مستخدم. يمكنك إنشاء قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل مرة واحدة، ثم منحها اسما، ثم تعيين قائمة التحكم في الوصول إلى IP القابلة للتنزيل لكل مستخدم أو مجموعة مستخدمين قابلين للتطبيق إذا قمت بإرجاع اسمها. تكون هذه الطريقة أكثر فعالية من إذا قمت بتكوين سمة زوج RADIUS من Cisco-av لكل مستخدم أو مجموعة مستخدمين.

علاوة على ذلك، عند إستخدام قوائم التحكم في الوصول (NAF)، يمكنك تطبيق محتويات مختلفة لقائمة التحكم في الوصول (ACL) على نفس المستخدم أو مجموعة المستخدمين فيما يتعلق بعميل AAA الذي يستخدمونه. لا يلزم تكوين إضافي لعميل AAA بعد تكوين عميل AAA لاستخدام قوائم التحكم في الوصول إلى IP القابلة للتنزيل من ACS. تتم حماية قوائم التحكم في الوصول (ACL) القابلة للتنزيل بواسطة نظام النسخ الاحتياطي أو النسخ المتماثل الذي قمت بإنشائه.

عندما تدخل تعريفات قائمة التحكم في الوصول (ACL) في واجهة ويب ACS، لا تستخدم إدخالات الكلمة الأساسية أو الاسم؛ في جميع الجوانب الأخرى، أستخدم صياغة أمر قائمة التحكم في الوصول (ACL) القياسية والأسماء لعميل AAA الذي تنوي تطبيق قائمة التحكم في الوصول إلى IP القابلة للتنزيل عليه. تتضمن تعريفات قائمة التحكم في الوصول (ACL) التي تدخلها في ACS أمر واحد أو أكثر من أوامر قائمة التحكم في الوصول (ACL). يجب أن يكون كل أمر قائمة تحكم في الوصول (ACL) على سطر منفصل.

يمكنك إضافة واحد أو أكثر من محتويات قائمة التحكم في الوصول (ACL) المسماة إلى قائمة التحكم في الوصول (ACL) إلى IP القابلة للتنزيل. بشكل افتراضي، ينطبق كل محتوى قائمة تحكم في الوصول (ACL) على جميع عملاء AAA، ولكن، إذا قمت بتعريف قوائم التحكم في الوصول (NAF)، فيمكنك تقييد إمكانية تطبيق كل محتوى قائمة التحكم في الوصول (ACL) على عملاء AAA المدرجة في NAF التي تقوم بربطها. وهذا يعني، عند إستخدام قوائم التحكم في الوصول (NAF)، يمكنك تطبيق كل محتوى من قوائم التحكم في الوصول (ACL) إلى IP، داخل قائمة تحكم في الوصول (ACL) واحدة قابلة للتنزيل، على العديد من أجهزة الشبكة المختلفة أو مجموعات أجهزة الشبكة وفقا لاستراتيجية أمان الشبكة لديك.

يمكنك أيضا تغيير ترتيب محتويات قائمة التحكم في الوصول (ACL) في قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل. يقوم ACS بفحص محتويات قائمة التحكم في الوصول (ACL)، بدءا من أعلى الجدول، وتنزيلات محتوى قائمة التحكم في الوصول (ACL) الأول الذي يعثر عليه مع NAF الذي يتضمن عميل AAA الذي يتم إستخدامه. عند تعيين الترتيب، يمكنك التأكد من كفاءة النظام إذا قمت بوضع محتويات قائمة التحكم في الوصول (ACL) الأكثر قابلية للتطبيق على نحو أعلى في القائمة. يجب عليك أن تدرك أنه إذا كانت إجراءات العمل الموحدة الخاصة بك تتضمن مجموعات من عملاء AAA الذين يتداخلون، فيجب عليك الانتقال من الإجراءات الخاصة إلى الأكثر عمومية. على سبيل المثال، يقوم ACS بتنزيل أي محتويات قائمة التحكم في الوصول (ACL) باستخدام إعداد NAF لجميع عملاء AAA ولا يأخذ في الاعتبار أي محتويات أقل في القائمة.

من أجل إستخدام قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل على عميل AAA معين، يجب أن يتبع عميل AAA هذه الاتجاهات:

- إستخدام RADIUS للمصادقة
- دعم قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل

هذه أمثلة على أجهزة Cisco التي تدعم قوائم التحكم في الوصول إلى IP القابلة للتنزيل:

- أجهزة ASA و PIX
- مركزات VPN 3000-Series
- أجهزة Cisco التي تشغل IOS الإصدار 12.3(8)T أو الأحدث

هذا مثال على التنسيق الذي يجب عليك إستخدامه لإدخال قوائم التحكم في الوصول (ACL) إلى VPN 3000/ASA/PIX 7.x+ في مربع تعريفات قائمة التحكم في الوصول (ACL):

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

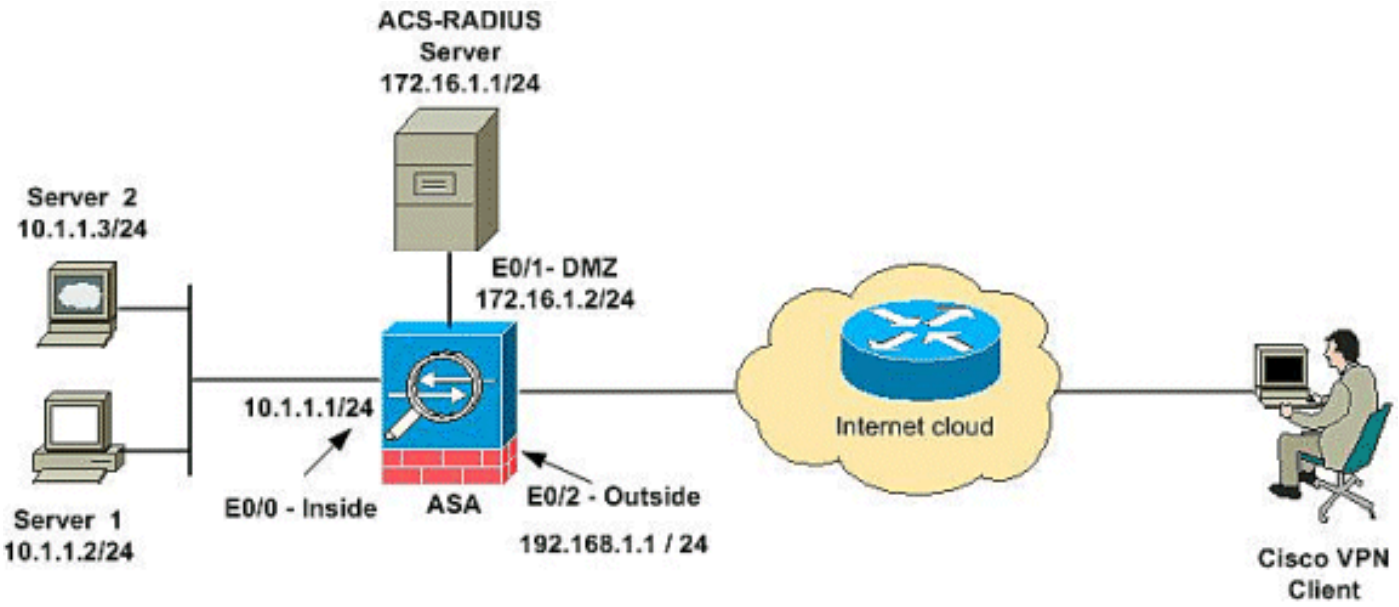
التكوين

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:



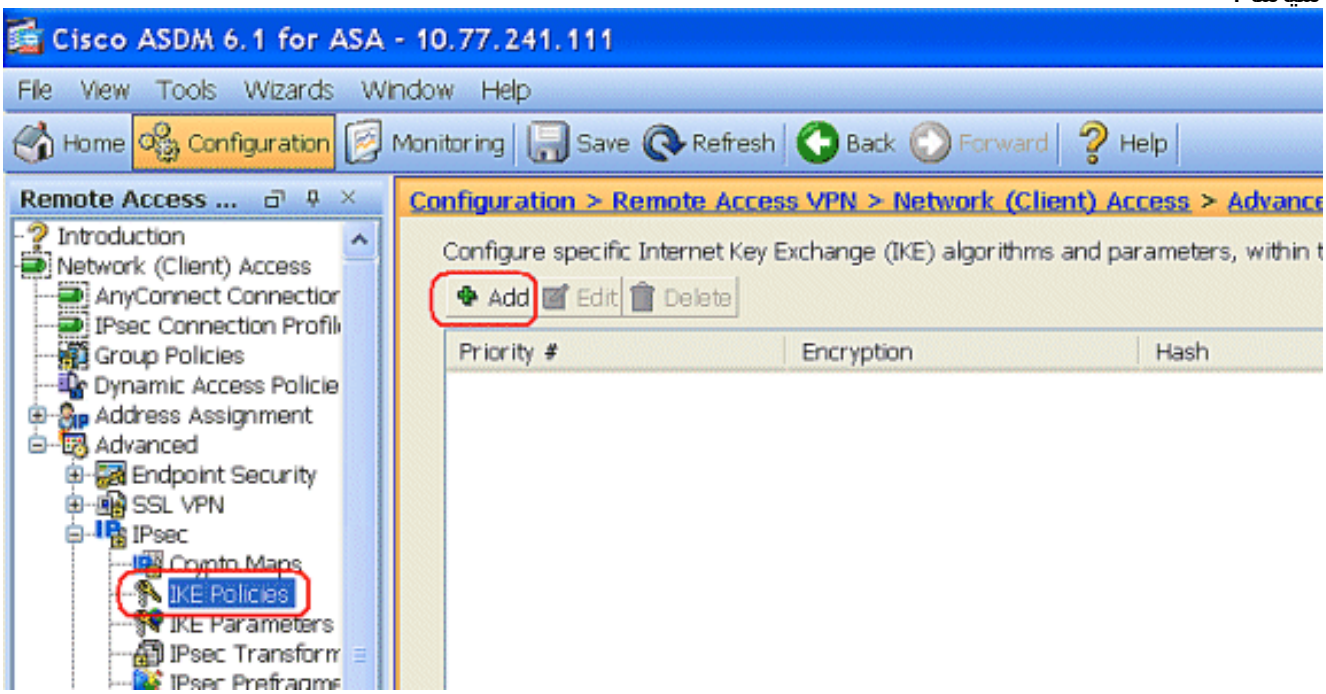
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

تكوين شبكة VPN للوصول عن بعد (IPSec)

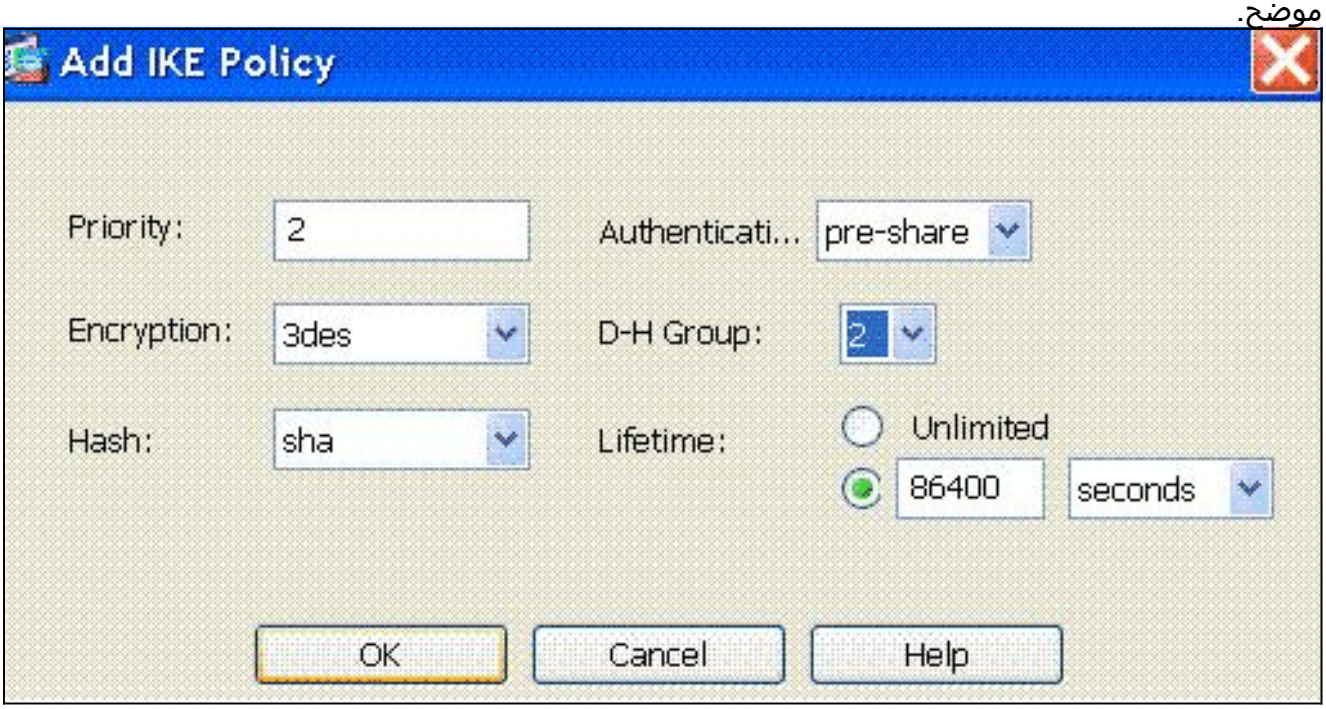
إجراء ASDM

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.



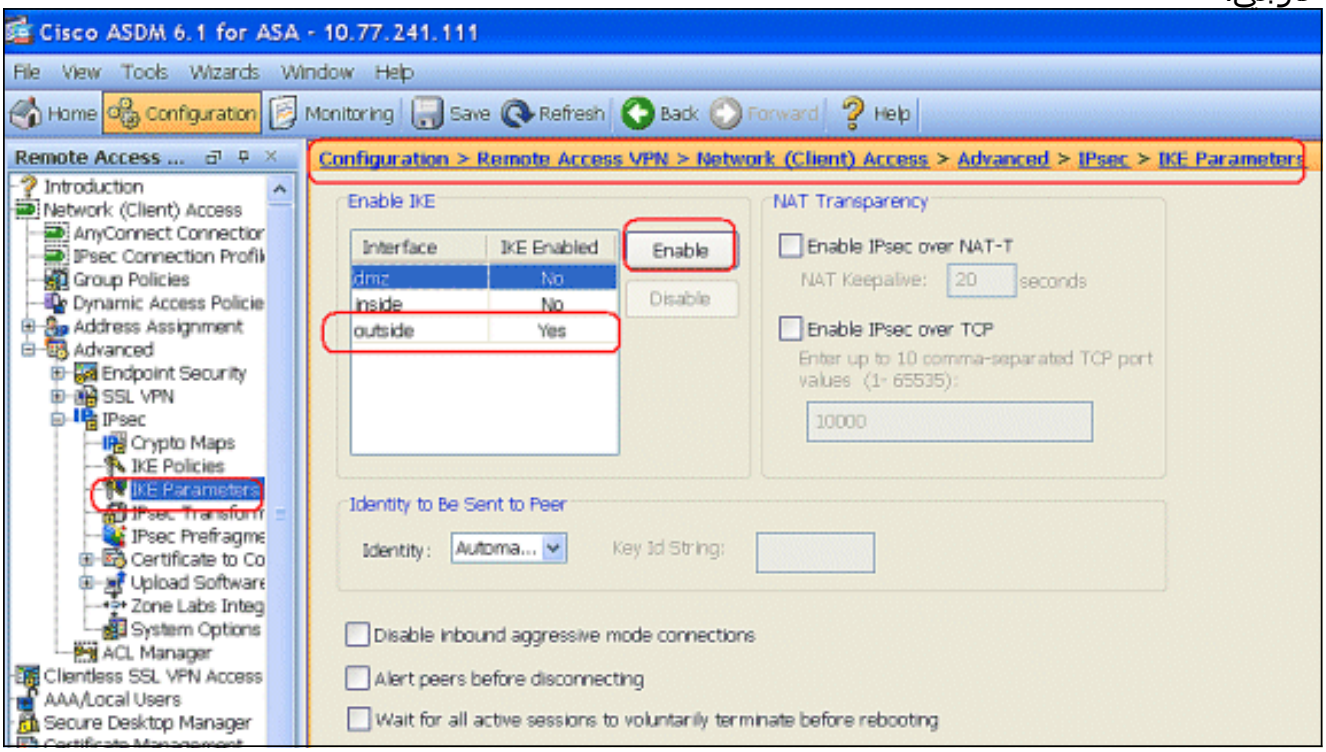
2. قم بتوفير تفاصيل سياسة ISAKMP كما هو موضح.



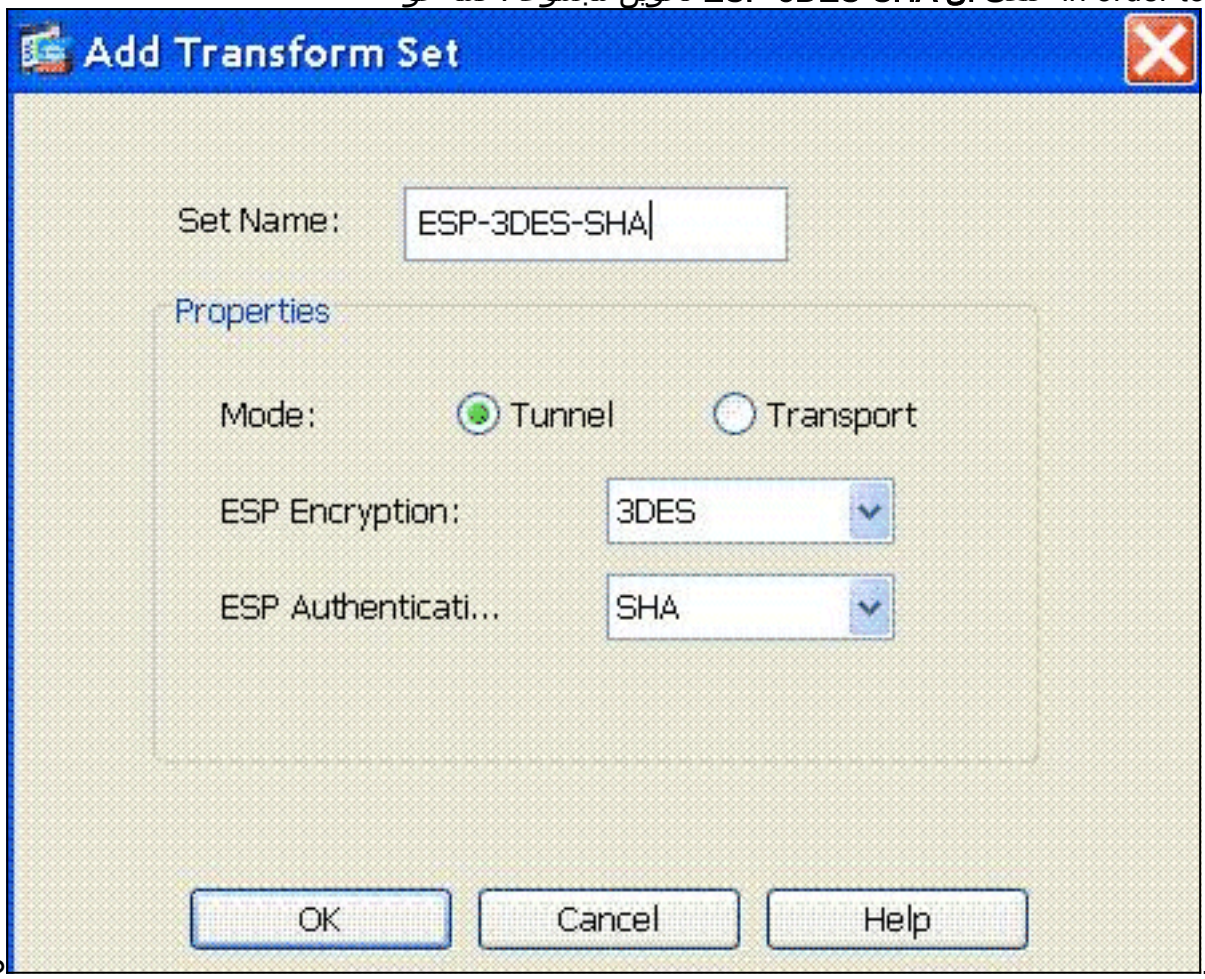
طقطقة **ok** و**يطبق**.

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

قارن
خارجي.



4. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ > متقدم > IPSec > مجموعات تحويل IPSec > إضافة** in order to خلقت ال **ESP-3DES-SHA** تحويل مجموعة، كما هو

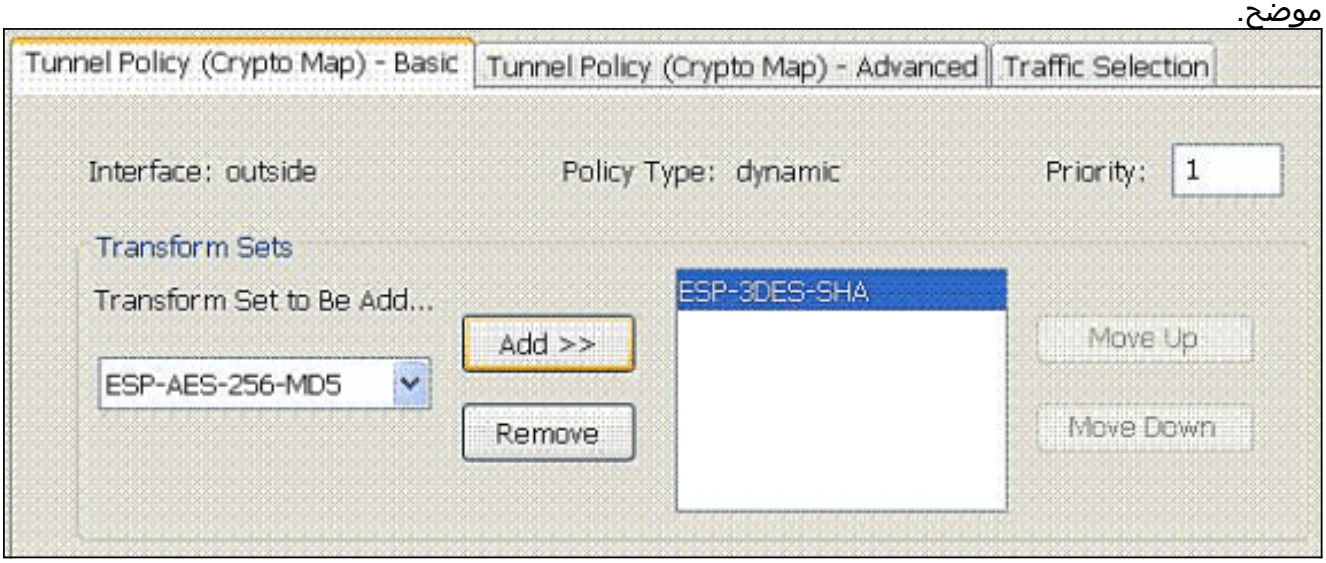


موضح.ط

قطقطة **ok** و**يطبق**.

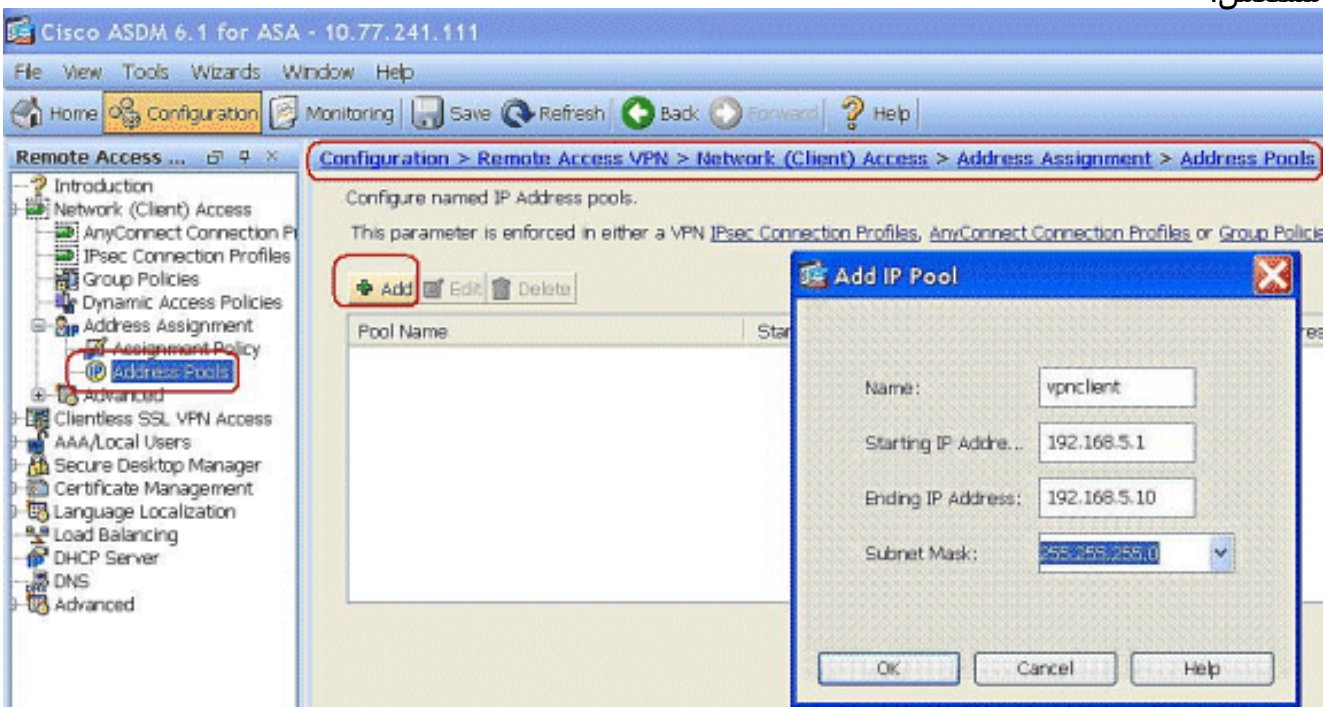
5. أختر **Configuration > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > Advanced > IPSec > Crypto Maps (خرائط التشفير) > Add** لإنشاء خريطة تشفير باستخدام السياسة

الديناميكية للأولوية 1، كما هو
موضح.

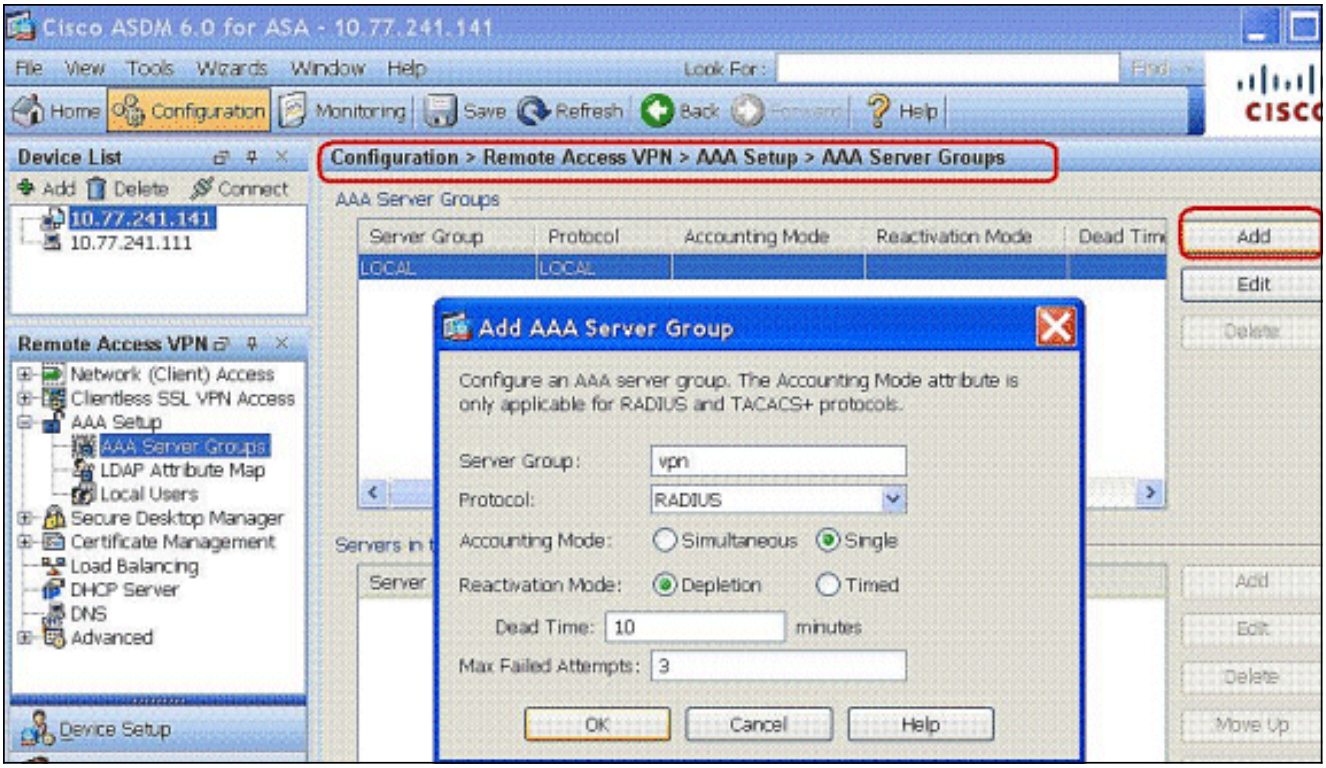


طقطقة **ok** و**يطبق**.

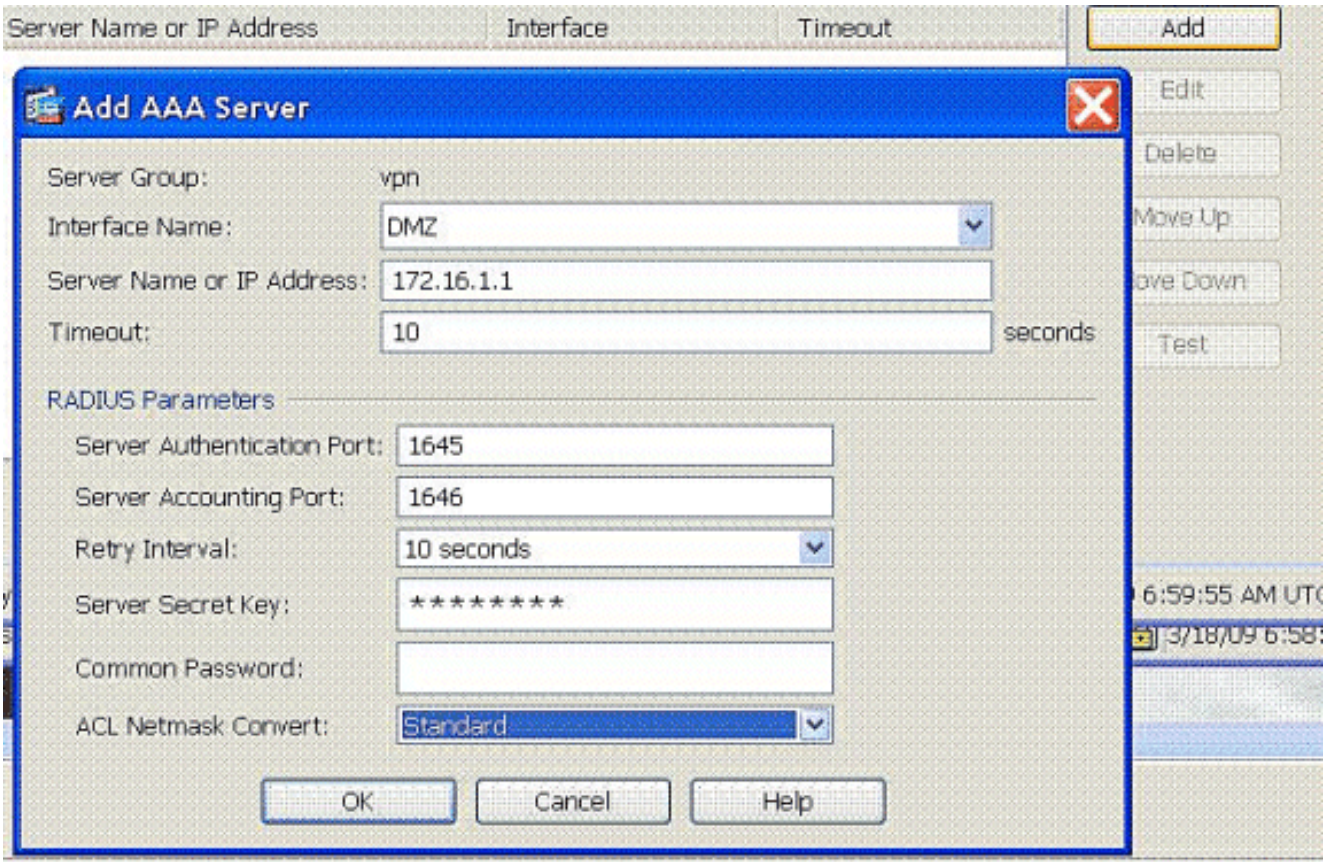
6. أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>عنوان تعيين>عنوان** بركة وطقطقة **يضيف** أن يضيف ال VPN زبون ل ال VPN زبون
مستعمل.



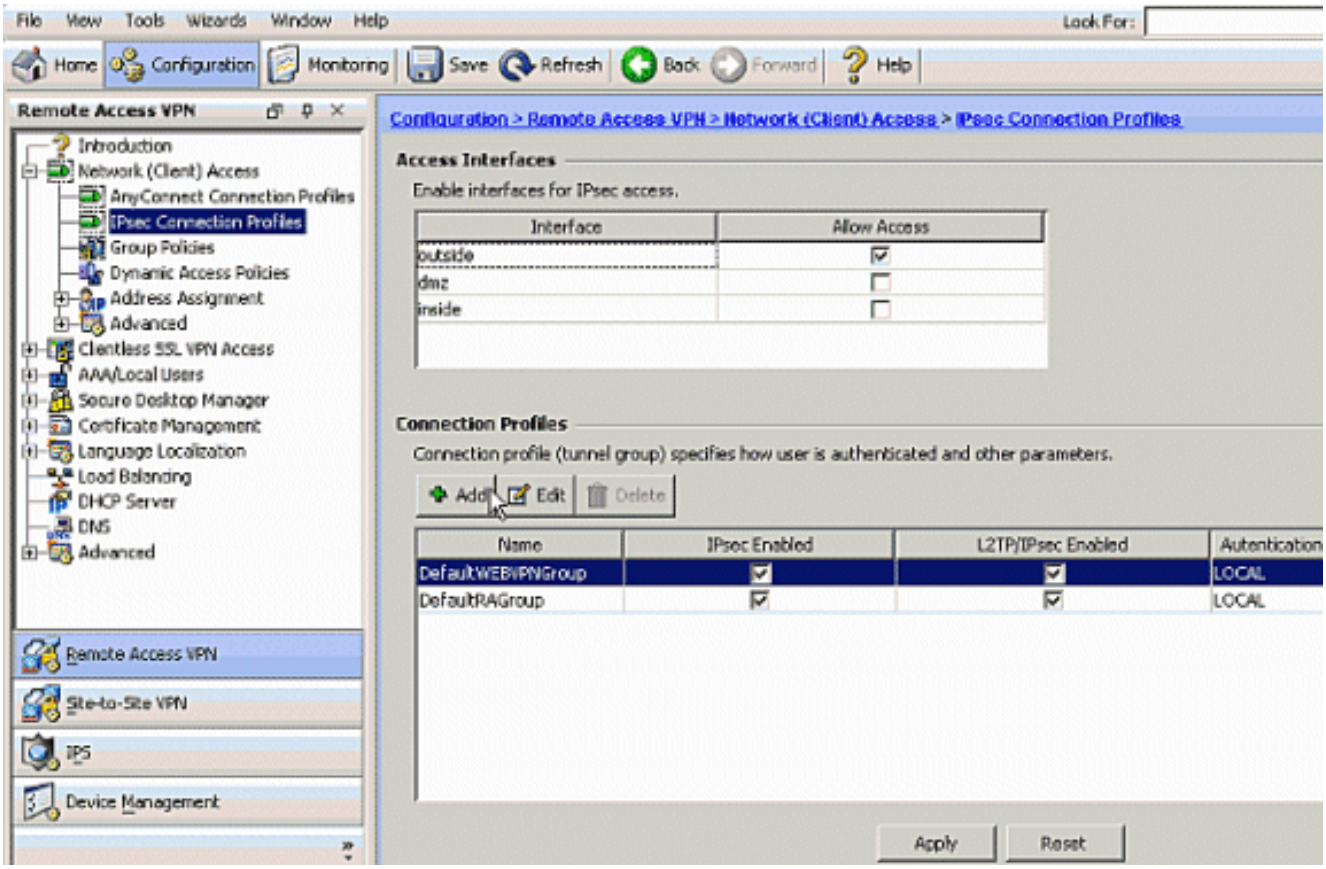
7. أخترت **تشكيل>وصول عن بعد AAA setup>AAA VPN نادل مجموعة ويضيف** طقطقة أن يضيف ال AAA نادل مجموعة إسم وبروتوكول
.



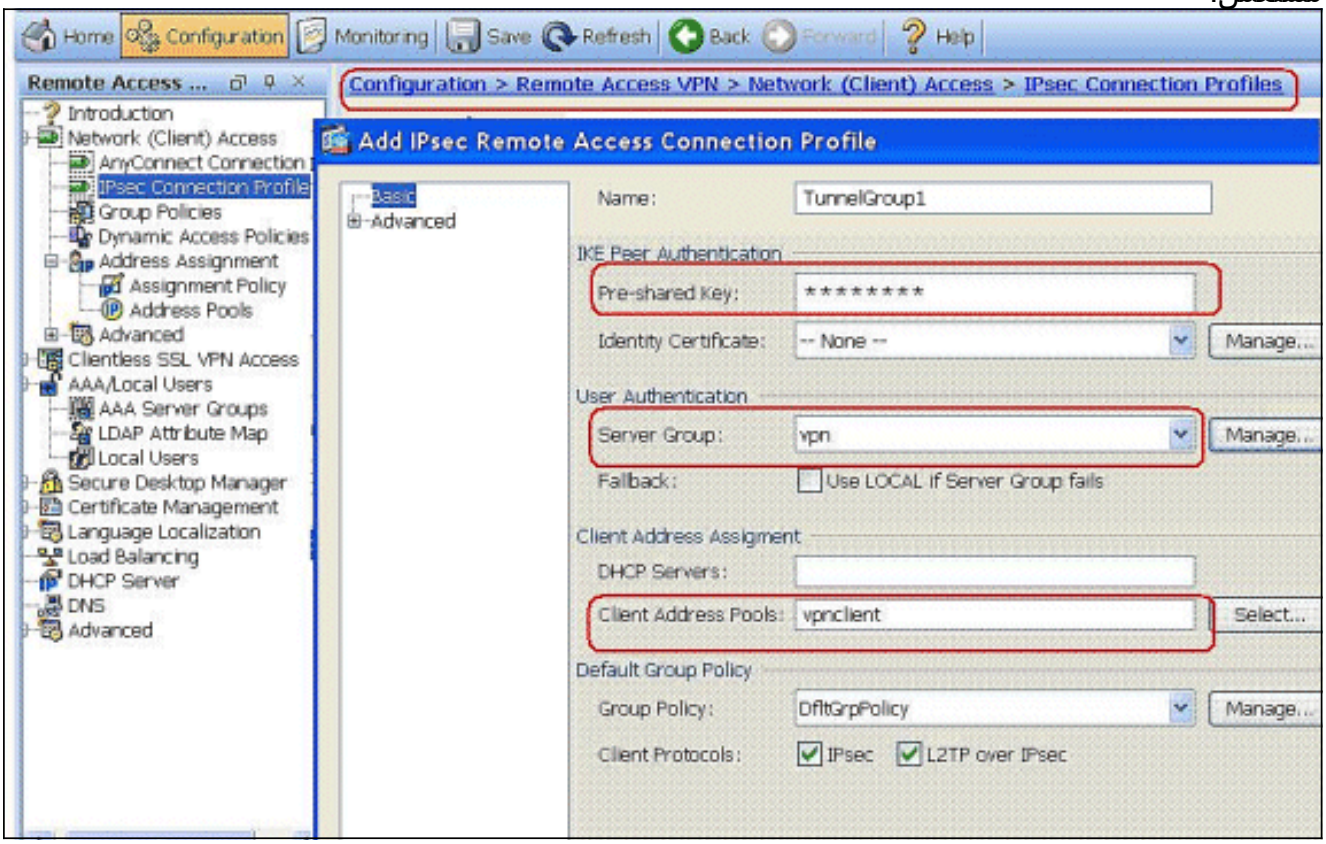
إضافة عنوان IP لخادم ACS) AAA) والواجهة التي يتصل بها. قم أيضا بإضافة المفتاح "سر الخادم" في منطقة معلمات RADIUS. وانقر فوق
.**OK**



8. أختر **Configuration > Remote Access VPN (الوصول عن بعد) > Network (Client) Access > ملفات تعريف اتصال** in order to **IPSec > Add** أضفت مجموعة نفق، على سبيل المثال، **TunnelGroup1** والمفتاح المشترك مسبقا على هيئة Cisco123، كما هو موضح.

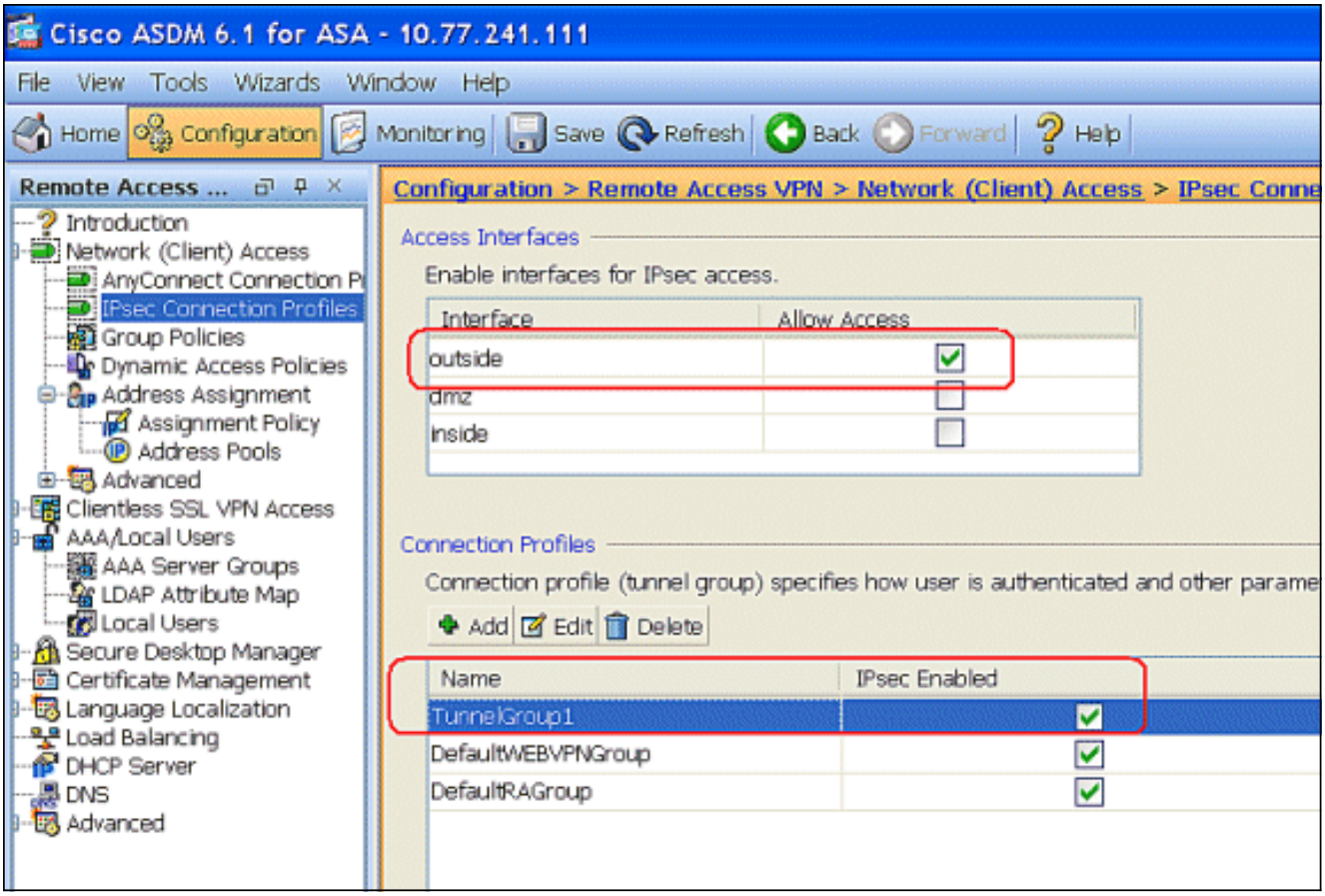


تحت علامة التبويب أساسي، أختر مجموعة الخادم كشبكة **VPN** لحقل مصادقة المستخدم.أخترت **vpnClient** كالزبون عنوان بركة ل ال VPN زبون مستعمل.



وانقر فوق **OK**.

9. 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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2
access-list new extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
```

```
                                                    mtu dmz 1500

  ip local pool vpnclient1 192.168.5.1-192.168.5.10 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 !--- Create the AAA server group
   "vpn" and specify the protocol as RADIUS. !--- Specify
     the CSACS server as a member of the "vpn" group and
       provide the !--- location and key. aaa-server vpn
                                             protocol radius
                                      max-failed-attempts 5
                    aaa-server vpn (DMZ) host 172.16.1.1
                                          retry-interval 1
                                                timeout 30
                                             key cisco123
                                          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

     PHASE 2 CONFIGURATION ---! !--- The encryption ---!
   types for Phase 2 are defined here. !--- A Triple DES
     encryption with !--- the sha hash algorithm is used.
   crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
                                                sha-hmac

         Defines a dynamic crypto map with !--- the ---!
       specified encryption settings. crypto dynamic-map
        outside_dyn_map 1 set transform-set ESP-3DES-SHA

 Binds the dynamic map to the IPsec/ISAKMP process. ---!
            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 3des
                                                  hash sha
                                                  group 2
```

```
                                                    lifetime 86400

                                    no crypto isakmp nat-traversal

                                                  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
        Associate the vpnclient pool to the tunnel group ---!
        using the address pool. !--- Associate the AAA server
              group (VPN) with the tunnel group. tunnel-group
                 TunnelGroup1 type remote-access tunnel-group
                                TunnelGroup1 general-attributes
                                        address-pool vpnclient
                                  authentication-server-group vpn

                 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
```

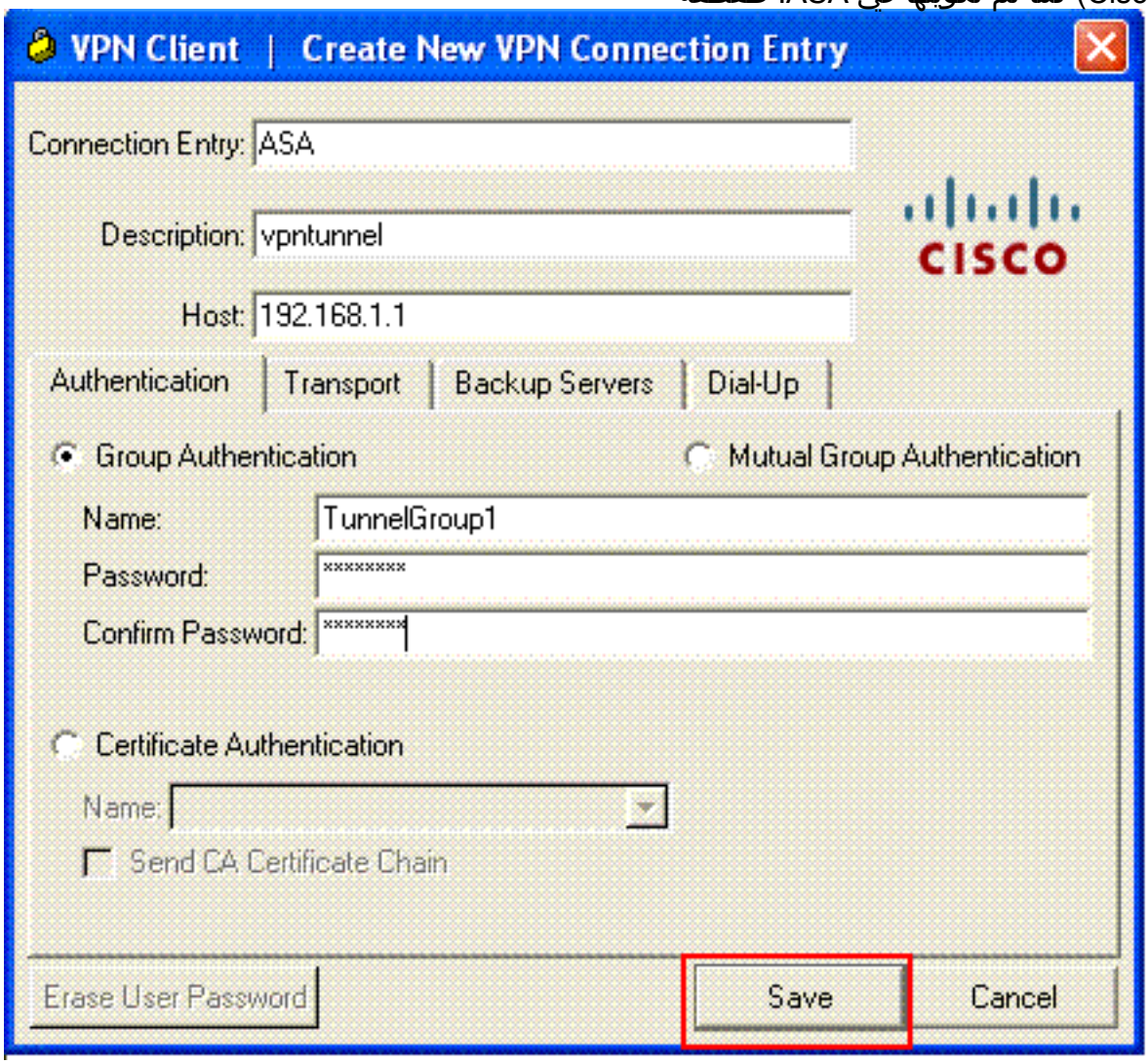
تكوين عميل شبكة VPN من Cisco

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

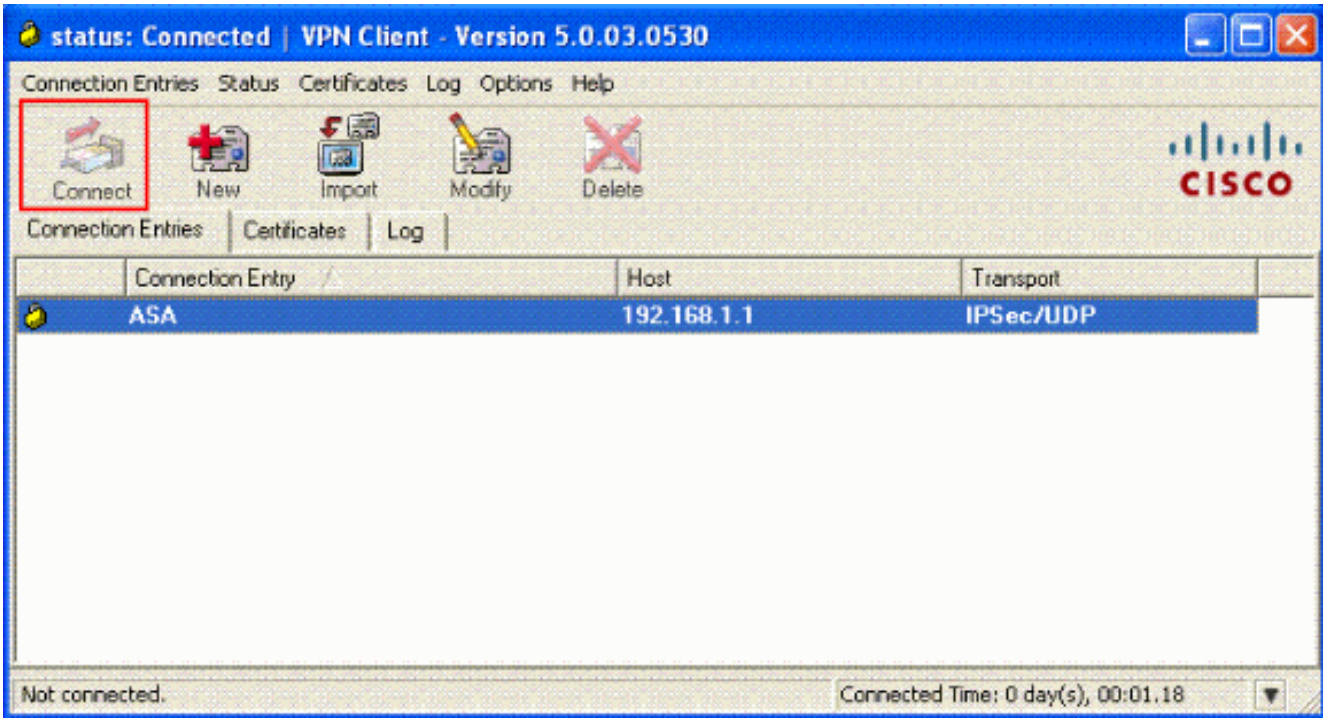
جديد".

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

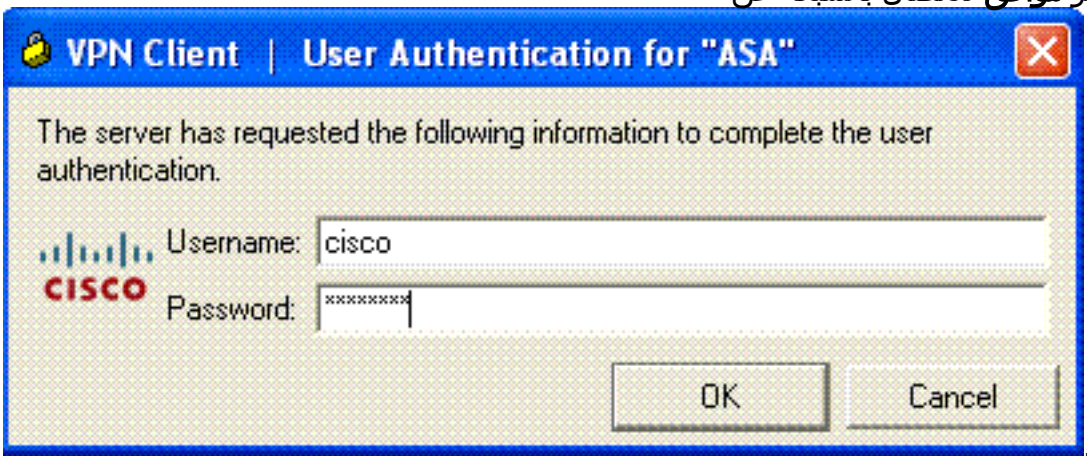


حفظ.

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

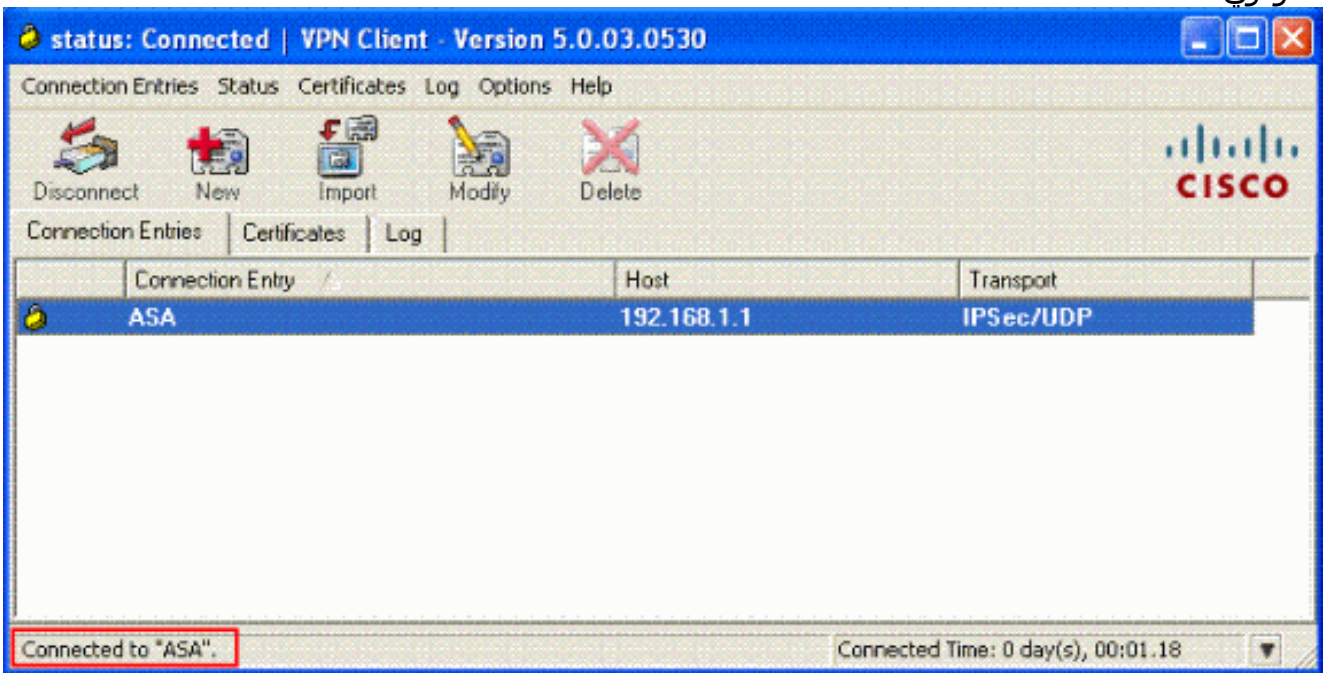


5. عندما يطلب منك، أدخل **اسم المستخدم:cisco** و**كلمة المرور : password1** كما تم تكوينه في ASA ل xauth، وانقر **موافق** للاتصال بالشبكة عن

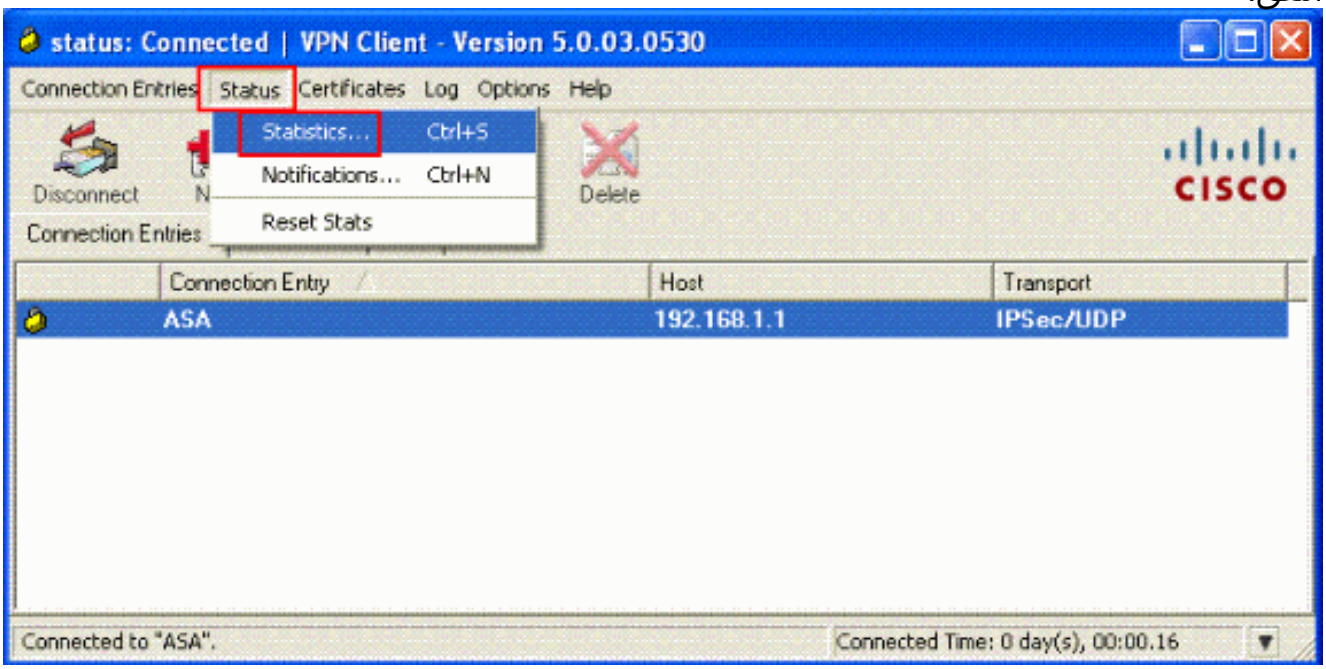


بعد.

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.



تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي

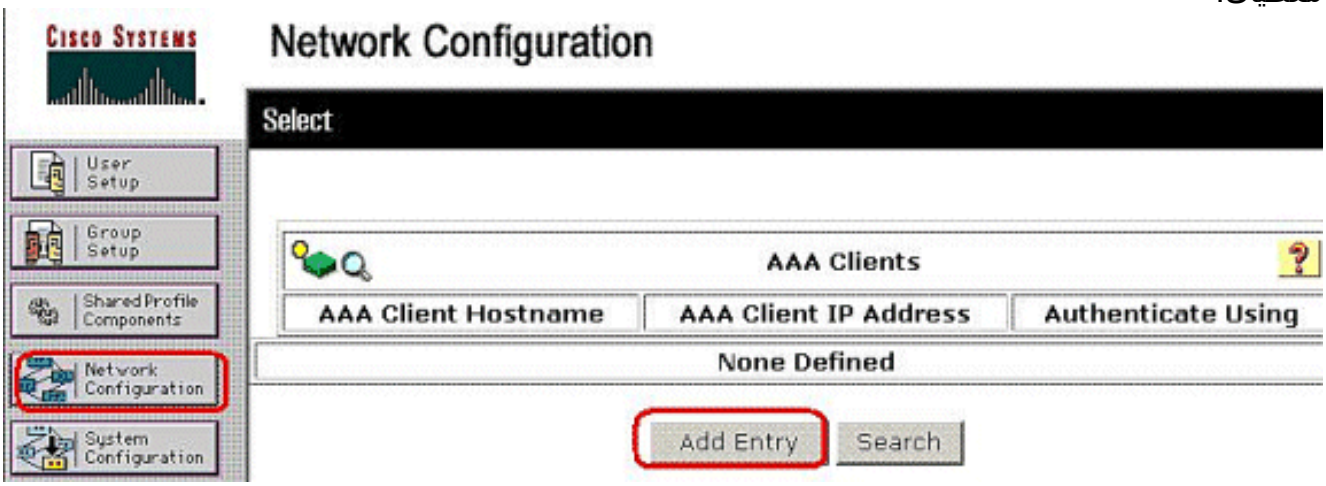
يمكنك تكوين قوائم الوصول القابلة للتنزيل على Cisco Secure ACS كمكون ملف تعريف مشترك ثم تعيين قائمة الوصول إلى مجموعة أو مستخدم فردي.

لتنفيذ قوائم الوصول الديناميكية، يجب تكوين خادم RADIUS لدعمه. عندما يقوم المستخدم بالمصادقة، يرسل خادم RADIUS قائمة وصول أو اسم قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يتم السماح بالوصول إلى خدمة معينة أو رفضه بواسطة قائمة الوصول. يحذف جهاز الأمان قائمة الوصول عند انتهاء صلاحية جلسة عمل المصادقة.

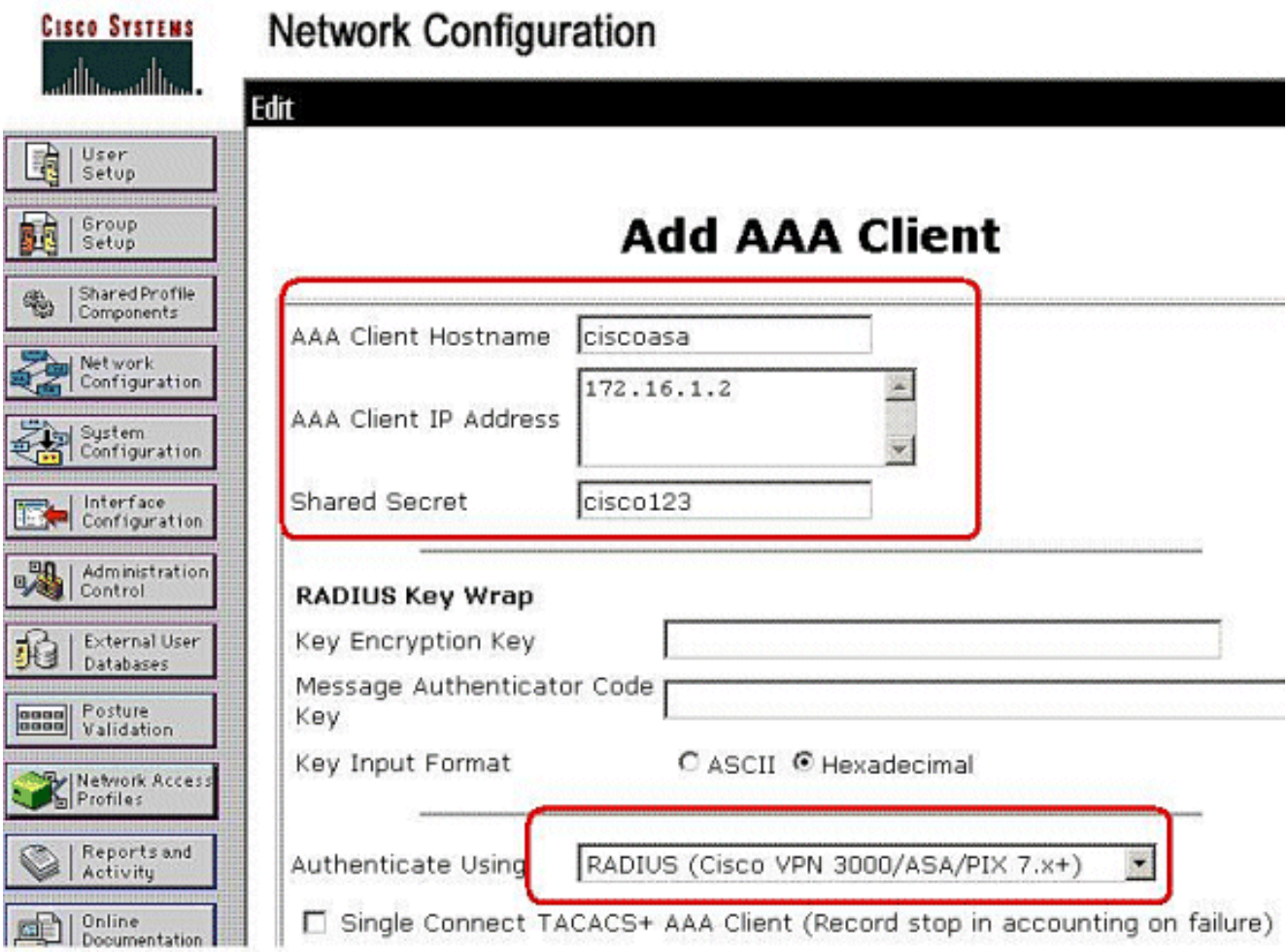
في هذا المثال، تتم مصادقة مستخدم **"cisco"** ل IPSec VPN بنجاح، ويرسل خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول (ACL)، راجع قسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة.

أتمت هذا steps in order to شكلت RADIUS في cisco يأمن acs.

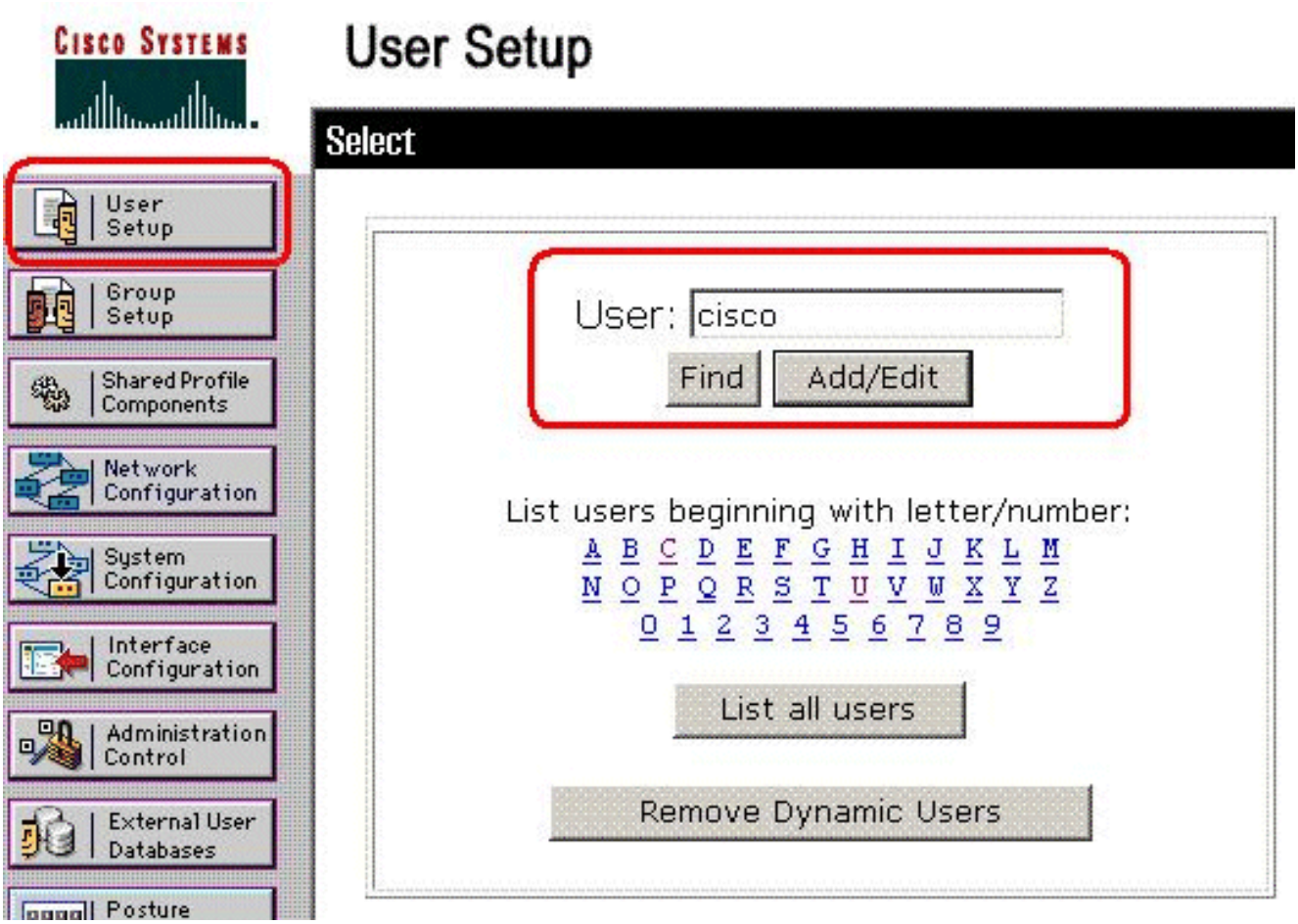
1. أخترت **شبكة تشكيل** على اليسار، وطقطقة **يضيف مدخل** أن يضيف مدخل ل ال ASA في ال RADIUS نادل قاعدة
معطيات.



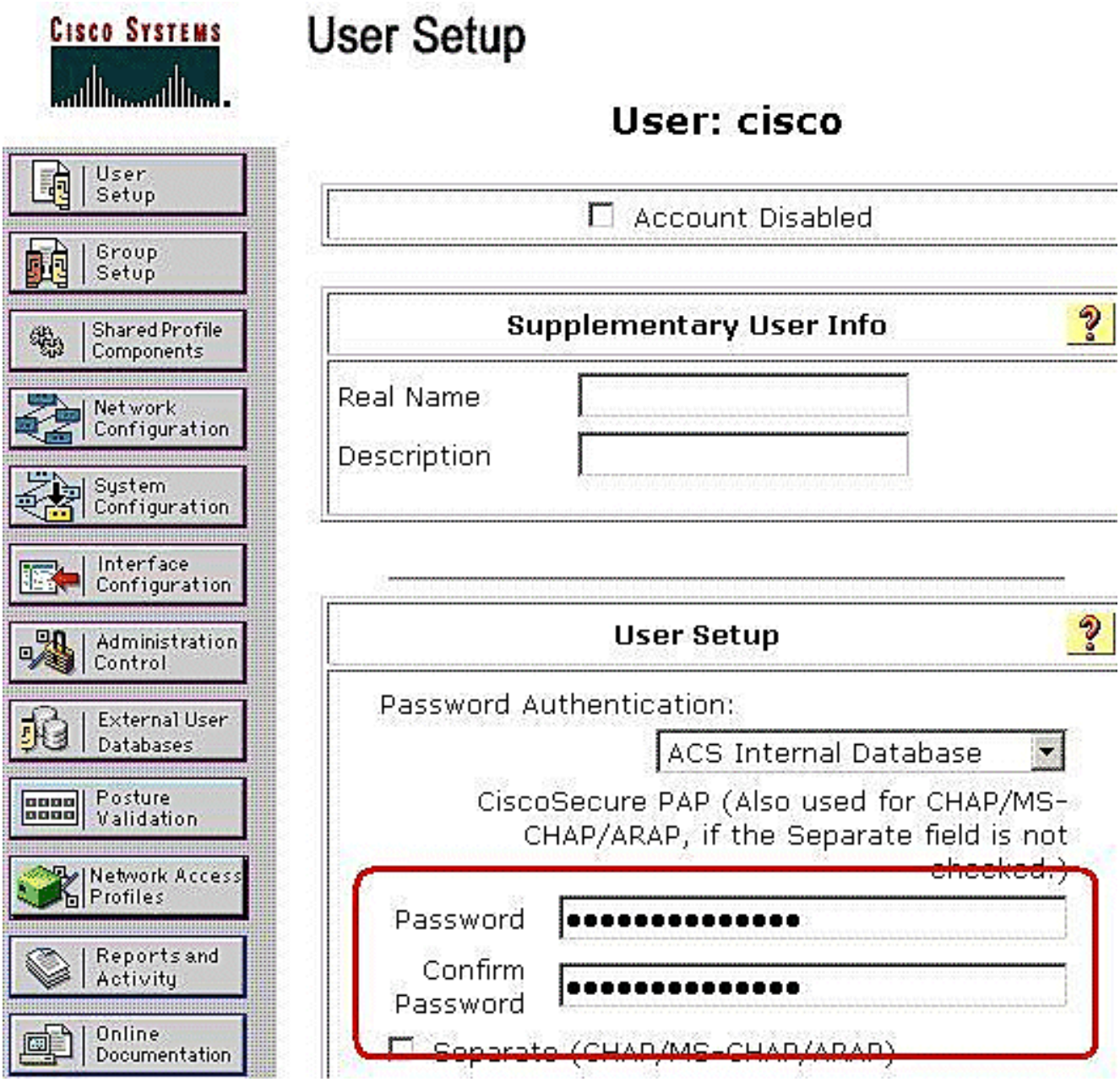
2. أدخل **172.16.1.2** في حقل عنوان IP للعميل، وأدخل **"Cisco123"** لحقل المفتاح السري المشترك. أختر **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** في *المصادقة باستخدام* المربع المنسدل. انقر على **إرسال**.



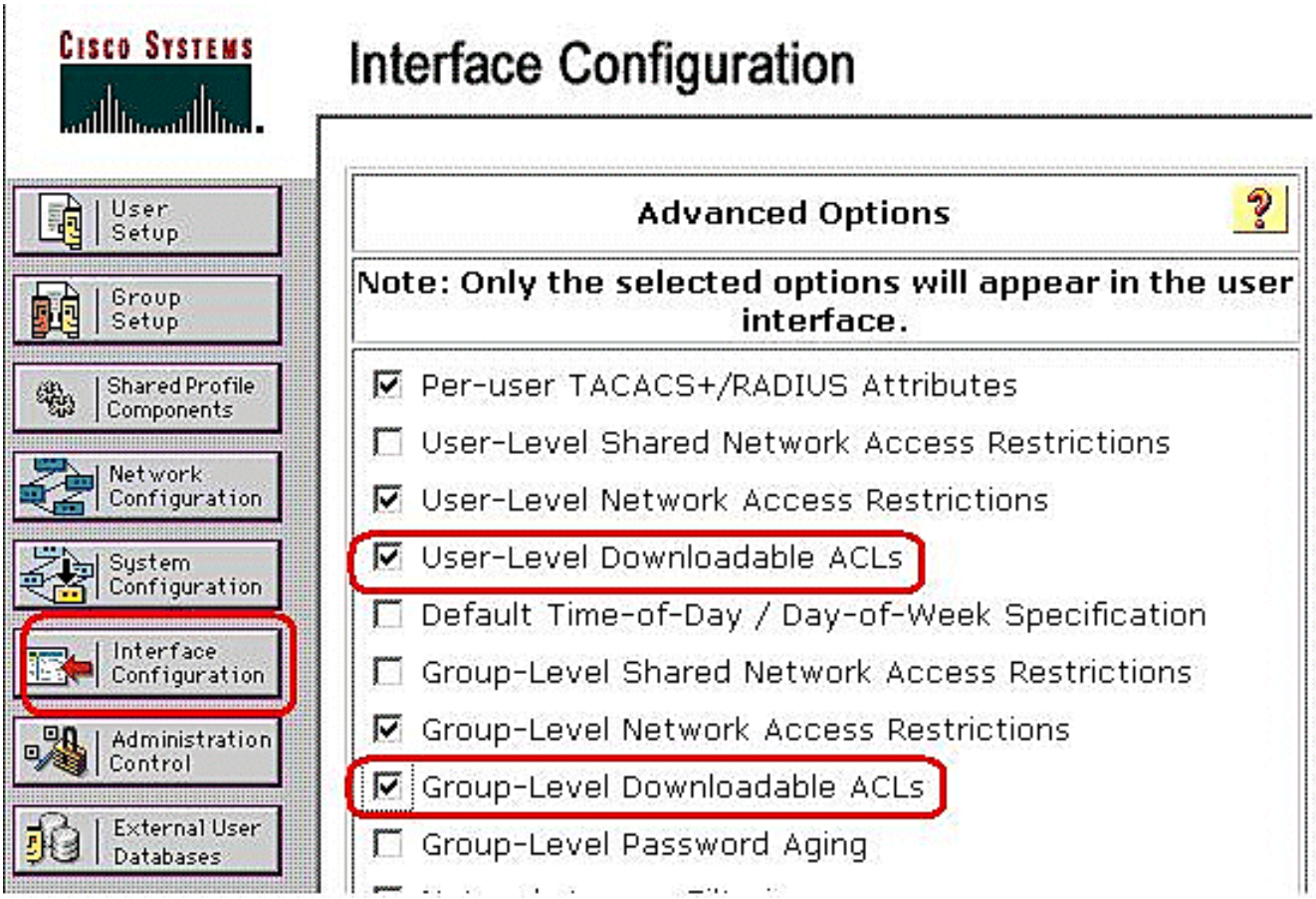
3. دخلت ال username في المستعمل مجال في ال cisco يأمن قاعدة معطيات، وطقطقة **يضيف/يحرر**.في هذا مثال، ال username
cisco.



4. في الإطار التالي، أدخل كلمة المرور ل **"cisco"**. في هذا مثال، الكلمة أيضا **كلمة1**. عند الانتهاء، انقر فوق **إرسال**.

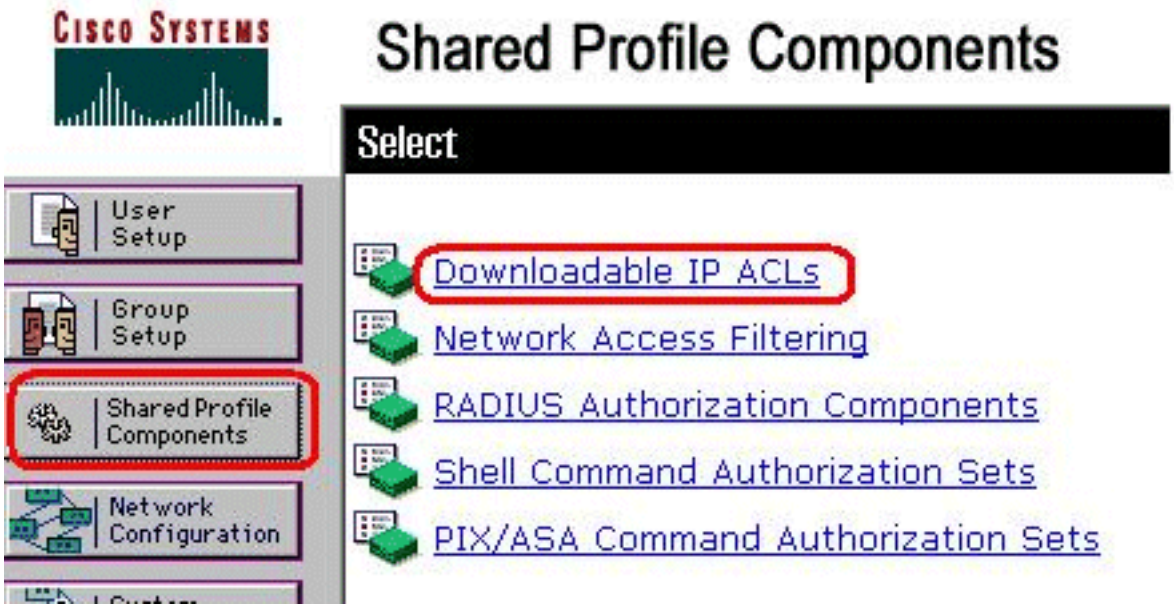


5. إنك تستخدم صفحة الخيارات المتقدمة لتحدد أي الخيارات المتقدمة التي يعرضها ACS. يمكنك تبسيط الصفحات التي تظهر في مناطق أخرى من واجهة ويب ACS إذا قمت بإخفاء الخيارات المتقدمة التي لا تستخدمها. انقر فوق **تكوين الواجهة**، ثم انقر فوق **الخيارات المتقدمة** لفتح صفحة الخيارات المتقدمة.



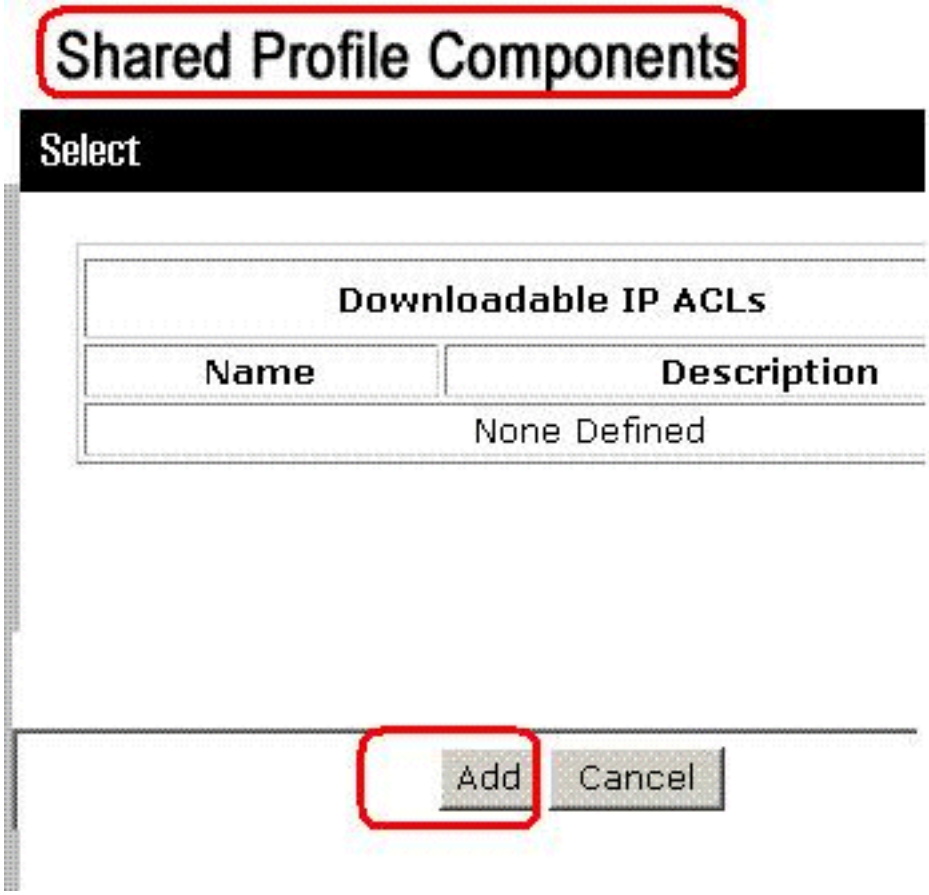
حدد المربع الخاص بقوائم ACL **القابلة للتنزيل على مستوى المستخدم** وقوائم التحكم في الوصول (ACL) **القابلة للتنزيل على مستوى المجموعة**.**قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المستخدم** - عند الاختيار، يتيح هذا الخيار قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل (قوائم التحكم في الوصول) في صفحة إعداد المستخدم.**قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المجموعة** - عند الاختيار، يتيح هذا الخيار قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل في صفحة إعداد المجموعة.

6. في شريط التنقل، انقر على **مكونات ملف التعريف المشترك**، وانقر على **قوائم التحكم في الوصول إلى IP القابلة للتنزيل**.**ملاحظة:** إذا لم تظهر *قوائم التحكم في الوصول إلى IP القابلة للتنزيل* في صفحة مكونات ملف التعريف المشترك، فيجب تمكين قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المستخدم أو خيار قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المجموعة أو كلاهما في صفحة الخيارات المتقدمة من قسم تكوين



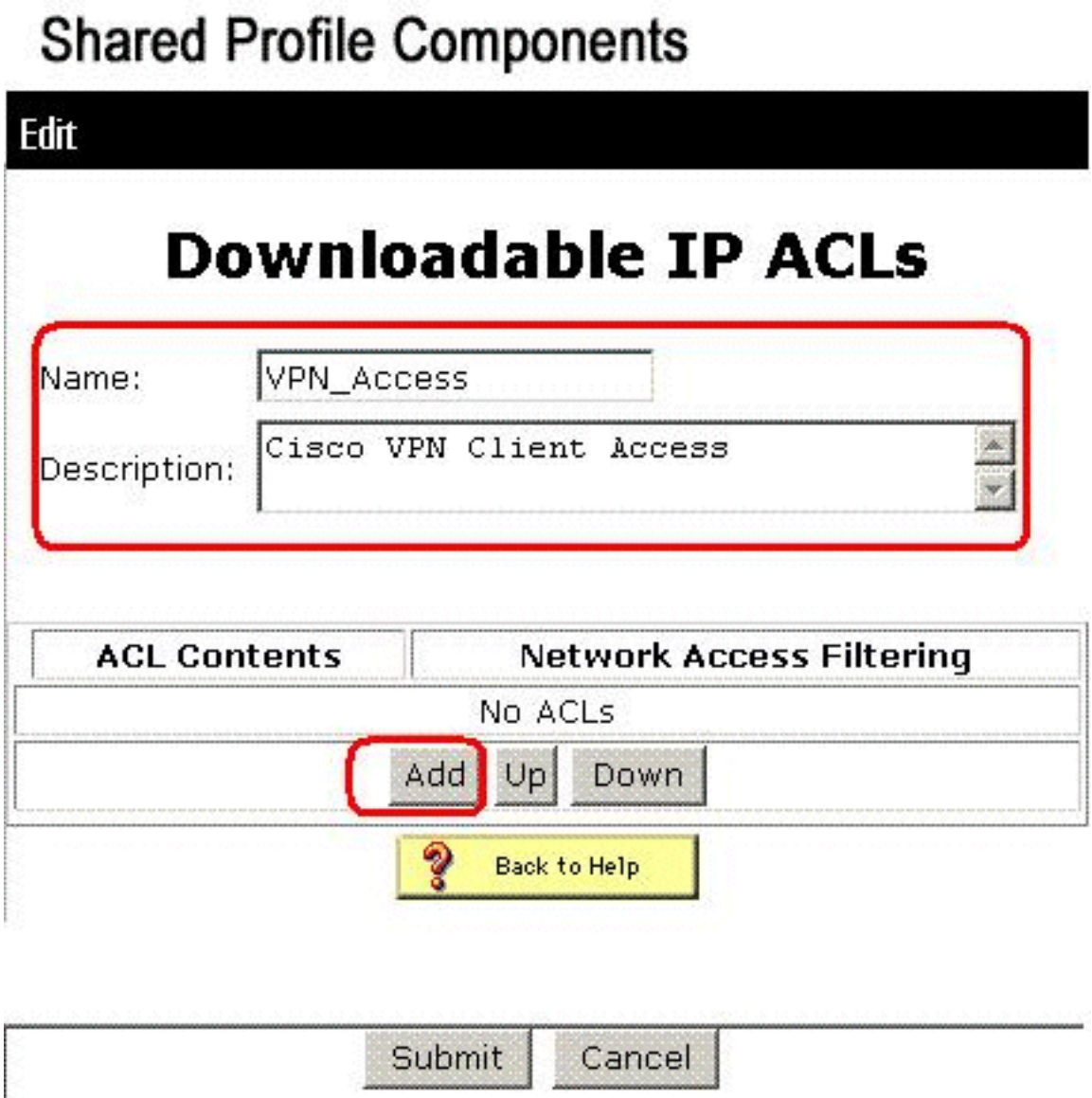
الواجهة.

7. انقر فوق **إضافة (Add)**. تظهر صفحة قوائم التحكم في الوصول إلى IP القابلة



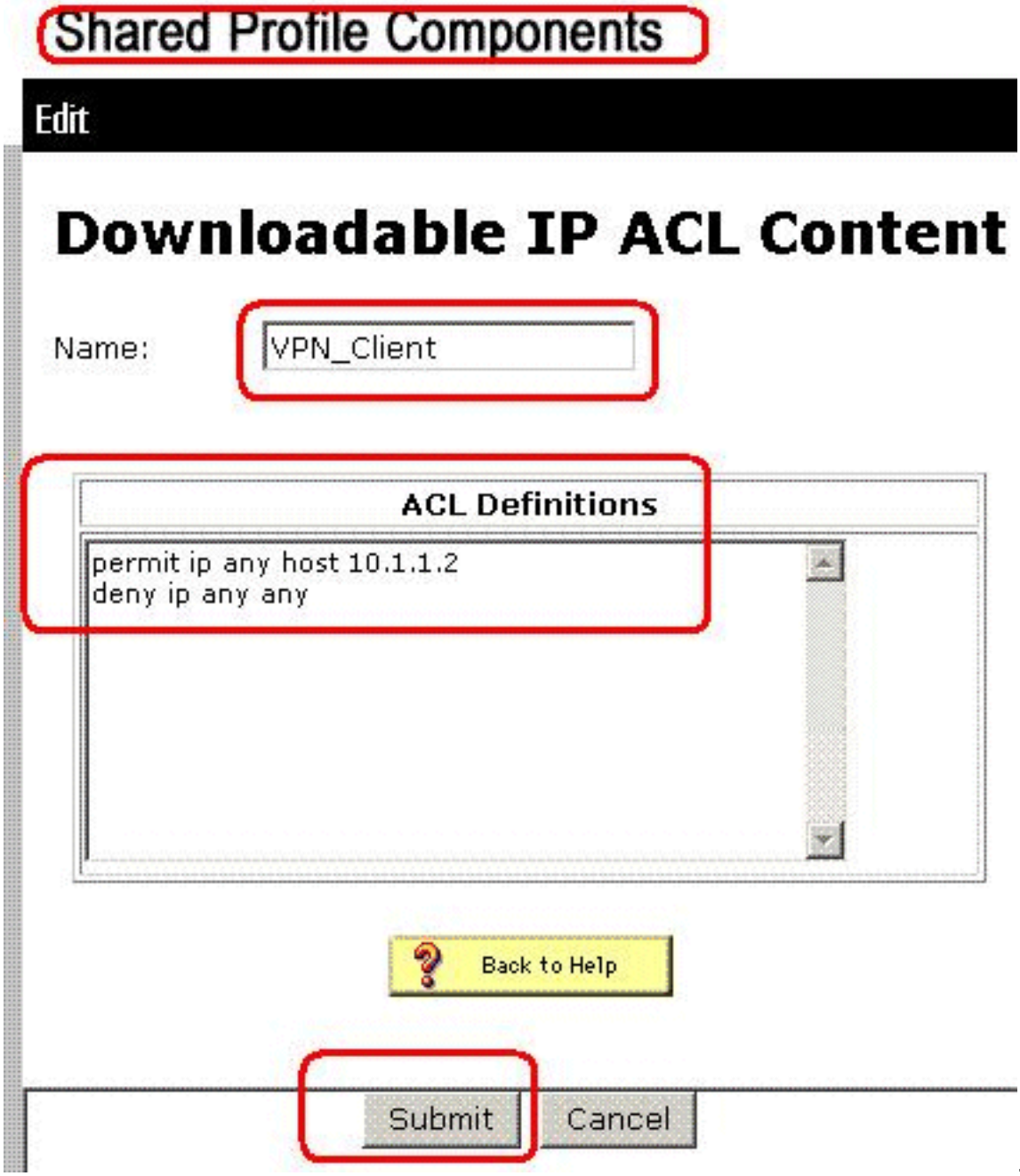
للتنزيل.

8. في مربع الاسم، اكتب اسم قائمة التحكم في الوصول (ACL) إلى IP الجديدة.**ملاحظة:** يمكن أن يحتوي اسم قائمة التحكم في الوصول إلى IP على ما يصل إلى 27 حرفا. يجب ألا يحتوي الاسم على مسافات أو أي من هذه الأحرف: واصلة (-) أو قوس أيسر ([) أو قوس أيسر (]) أو شرطة مائلة (/) أو شرطة مائلة خلفية (\) أو علامات تنصيص (") أو قوس أيسر (<) أو قوس زاوية يمنى (>) أو شرطة (-).في مربع الوصف، اكتب وصفا لقائمة التحكم في الوصول (ACL) إلى IP الجديدة. يمكن أن يصل الوصف إلى 1000



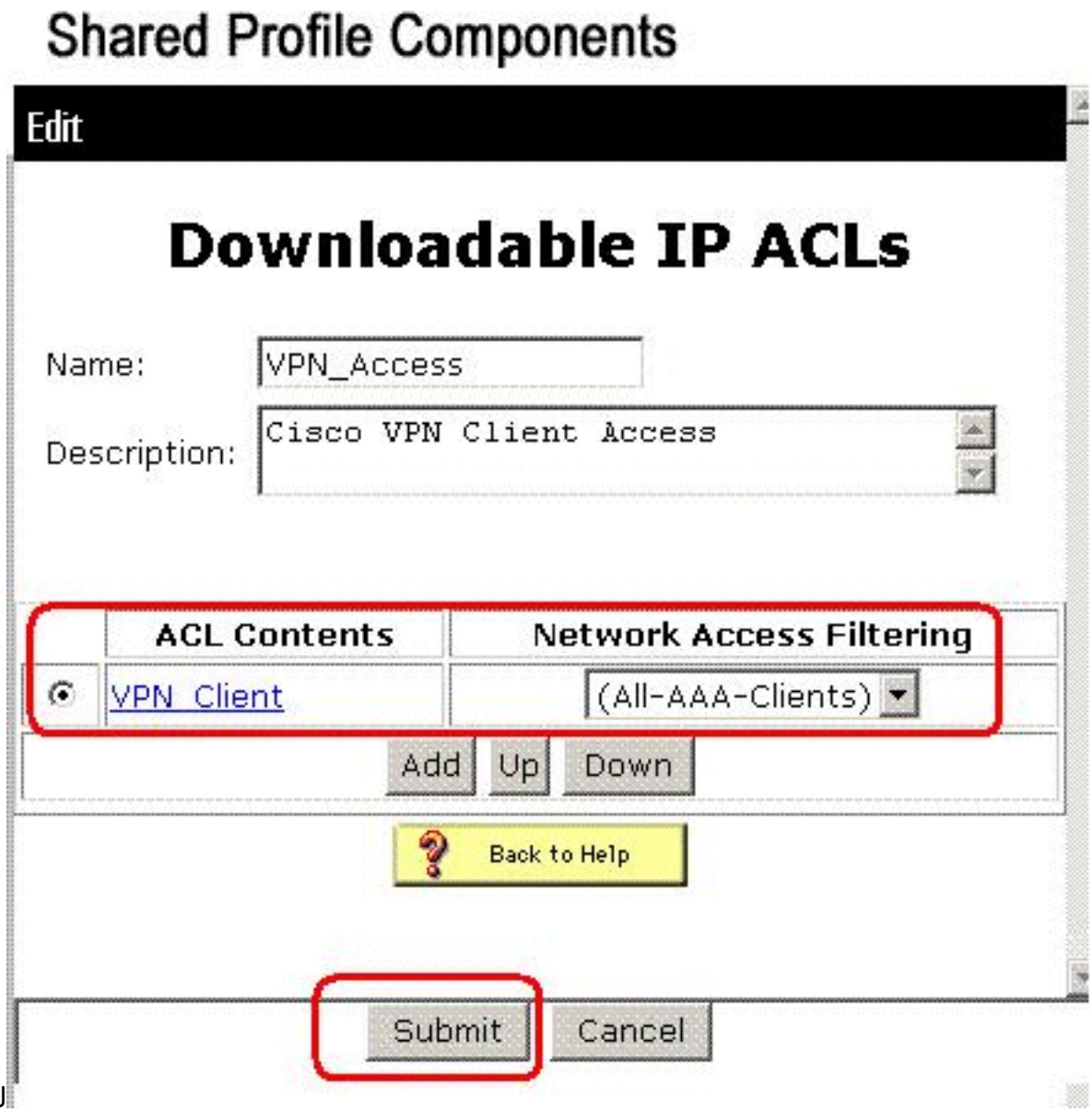
لإضافة حرف.
محتوى قائمة التحكم في الوصول (ACL) إلى قائمة التحكم في الوصول (ACL) إلى IP الجديدة، انقر فوق **إضافة**.

9. في مربع الاسم، اكتب اسم محتوى قائمة التحكم بالوصول (ACL) الجديد.**ملاحظة:** يمكن أن يحتوي اسم محتوى قائمة التحكم في الوصول (ACL) على ما يصل إلى 27 حرفا. يجب ألا يحتوي الاسم على مسافات أو أي من هذه الأحرف: واصلة (-) أو قوس أيسر ([) أو قوس أيسر ([) أو شرطة مائلة (/) أو شرطة مائلة خلفية (\) أو علامات تنصيص (") أو قوس أيسر (<) أو قوس زاوية يمنى (>) أو شرطة (-).في مربع تعريفات قائمة التحكم في الوصول (ACL)، اكتب تعريف قائمة التحكم في الوصول (ACL) الجديد.**ملاحظة:** عند إدخال تعريفات قائمة التحكم في الوصول (ACL) في واجهة ويب ACS، لا تستخدم إدخالات الكلمة الأساسية أو الاسم؛ وبدلا من ذلك، ابدأ بالكلمة الأساسية السماح أو الرفض.لحفظ محتوى قائمة التحكم في الوصول (ACL)، انقر فوق



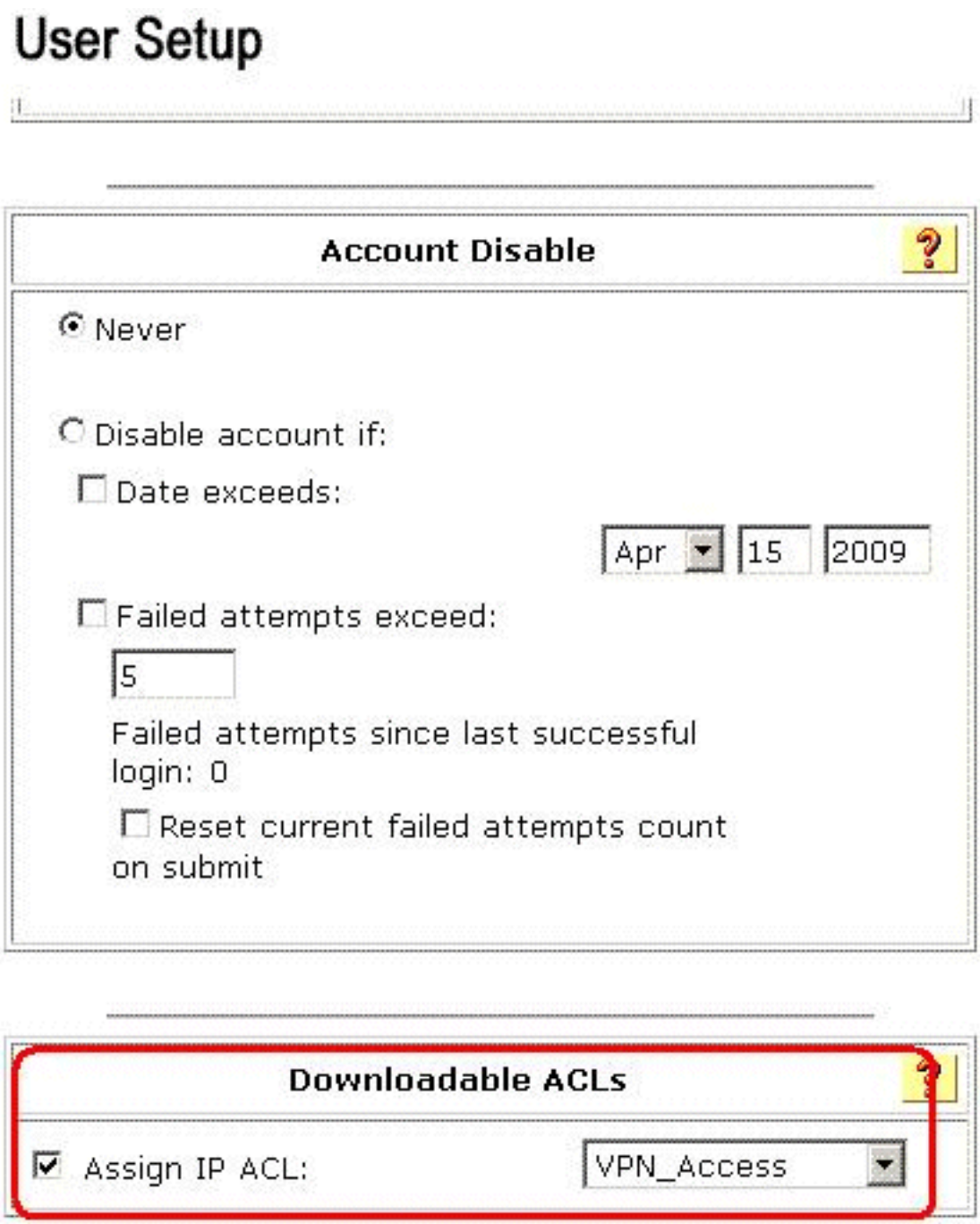
إرسال.

10. تظهر صفحة قوائم التحكم في الوصول إلى IP القابلة للتنزيل مع محتوى قائمة التحكم في الوصول (ACL) الجديد المدرج بالاسم في عمود محتويات قائمة التحكم في الوصول (ACL). لربط NAF بمحتوى قائمة التحكم في الوصول، أختر NAF من مربع تصفية الوصول إلى الشبكة إلى يمين المحتوى الجديد لقائمة التحكم في الوصول. وبشكل افتراضي، يكون NAF (جميع عملاء AAA). إذا لم تقم بتعيين NAF، فإن ACS يربط محتوى قائمة التحكم في الوصول (ACL) بجميع أجهزة الشبكة، وهو الإعداد الافتراضي.



لتعيين ترتيب محتويات قائمة التحكم في الوصول (ACL)، انقر فوق زر الاختيار الخاص بتعريف قائمة التحكم في الوصول (ACL)، ثم انقر فوق **أعلى** أو **أسفل** لإعادة وضعه في القائمة.لحفظ قائمة التحكم في الوصول (ACL) إلى IP، انقر فوق **إرسال**.**ملاحظة:** ترتيب محتويات قائمة التحكم في الوصول (ACL) هام. ومن الأعلى إلى الأسفل، يقوم ACS بتنزيل تعريف قائمة التحكم في الوصول (ACL) الأول فقط الذي يحتوي على إعداد NAF قابل للتطبيق، والذي يتضمن الإعداد الافتراضي لجميع عملاء AAA، إذا تم إستخدامه. بشكل نموذجي، تنتقل قائمة محتويات قائمة التحكم في الوصول (ACL) من القائمة التي تحتوي على أكثر (أضيق) NAF تحديدا إلى القائمة التي تحتوي على أكثر NAF عامة (جميع عملاء AAA).**ملاحظة:** يدخل ACS قائمة التحكم في الوصول (ACL) إلى IP الجديدة، والتي تدخل حيز التنفيذ على الفور. على سبيل المثال، إذا كانت قائمة التحكم في الوصول (ACL) إلى IP مخصصة للاستخدام مع جدران حماية PIX، فإنها تتوفر ليتم إرسالها إلى أي جدار حماية PIX يحاول مصادقة المستخدم الذي لديه قائمة التحكم في الوصول (ACL) إلى IP القابلة للتنزيل التي تم تعيينها إلى ملف تعريف المستخدم أو المجموعة الخاص به.

11. انتقل إلى صفحة إعداد المستخدم وقم بتحرير صفحة المستخدم. تحت قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل، انقر فوق خانة الاختيار **تعيين قائمة التحكم في الوصول (ACL) إلى IP**. أختر قائمة تحكم في الوصول (ACL) إلى IP من القائمة. في حالة الانتهاء من تكوين خيارات حساب المستخدم، انقر فوق **إرسال** لتسجيل



الخيارات.

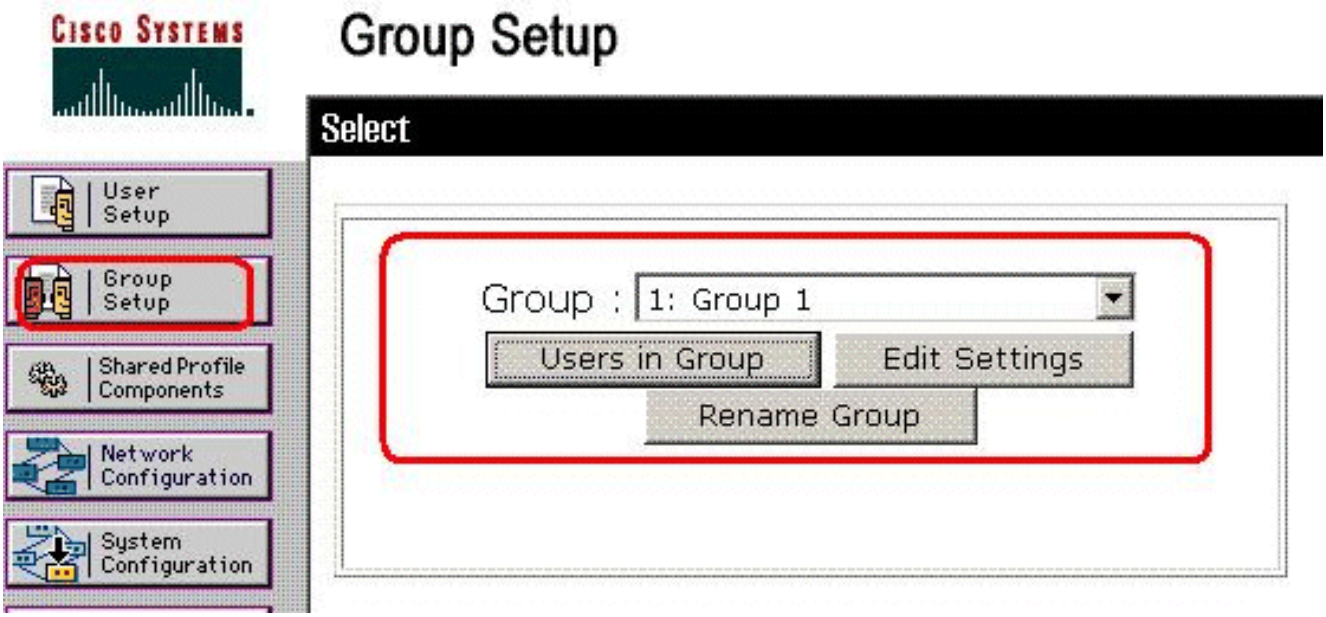
تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة

أكمل الخطوات من 1 إلى 9 من تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي واتبع هذه الخطوات لتكوين قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة في Cisco ACS الآمن.

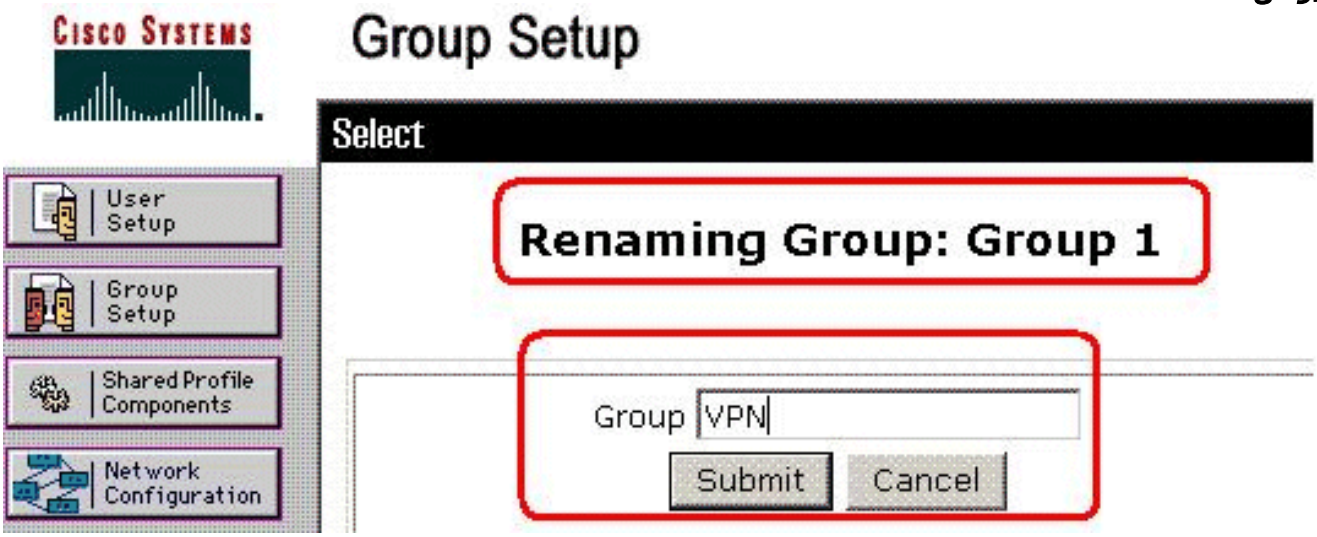
في هذا المثال، ينتمي مستخدم شبكة VPN ل "cisco IPSec" إلى مجموعات VPN. يتم تطبيق سياسات مجموعة VPN على جميع المستخدمين في المجموعة.

تتم مصادقة مستخدم مجموعة **cisco**"VPN"بنجاح، ويرسل خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول (ACL)، ارجع إلى قسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة.

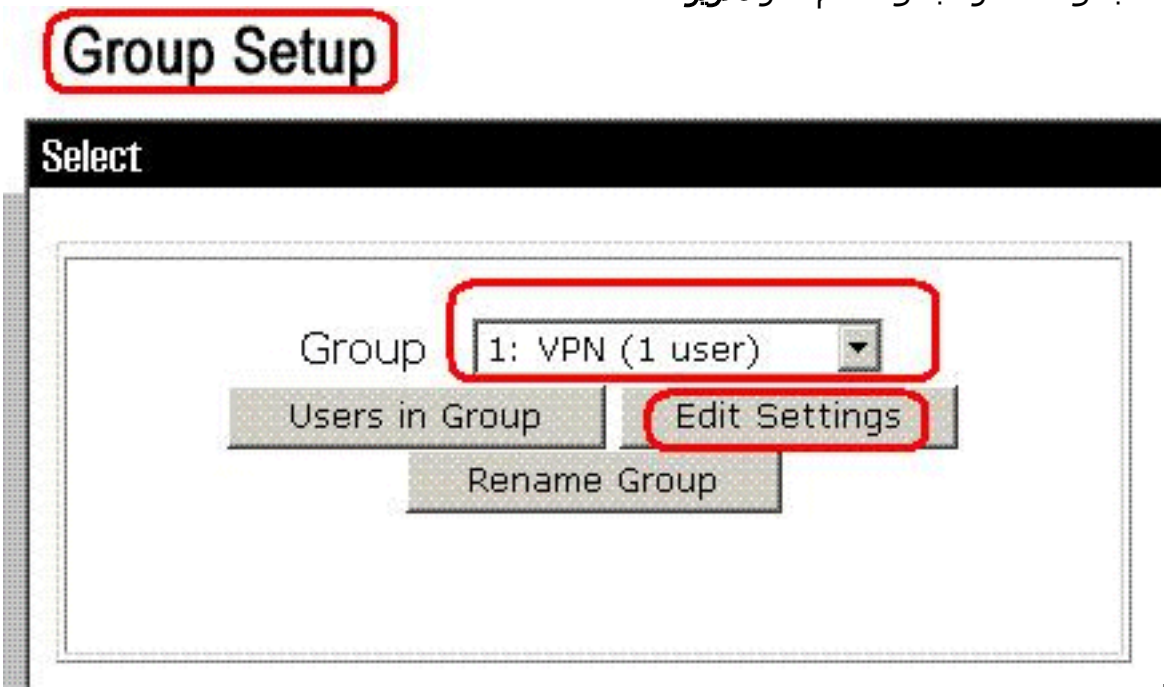
1. في شريط التنقل، انقر فوق **إعداد المجموعة**. يتم فتح صفحة تحديد إعداد المجموعة.



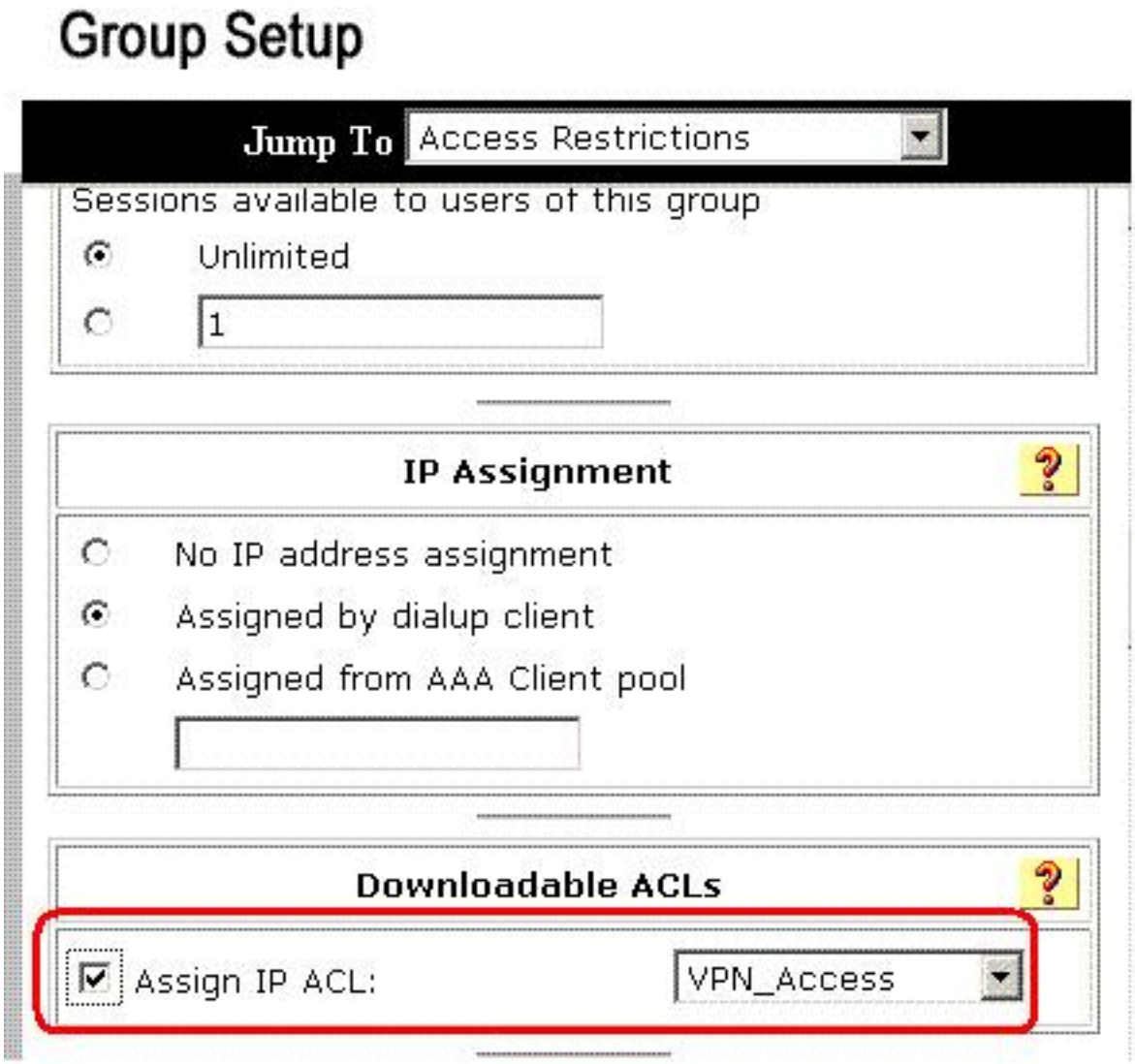
2. عينت مجموعة 1 إلى **VPN**، وطقطقة **يرسل**.



3. من قائمة المجموعة، أختر مجموعة، ثم انقر **تحرير الإعدادات**.

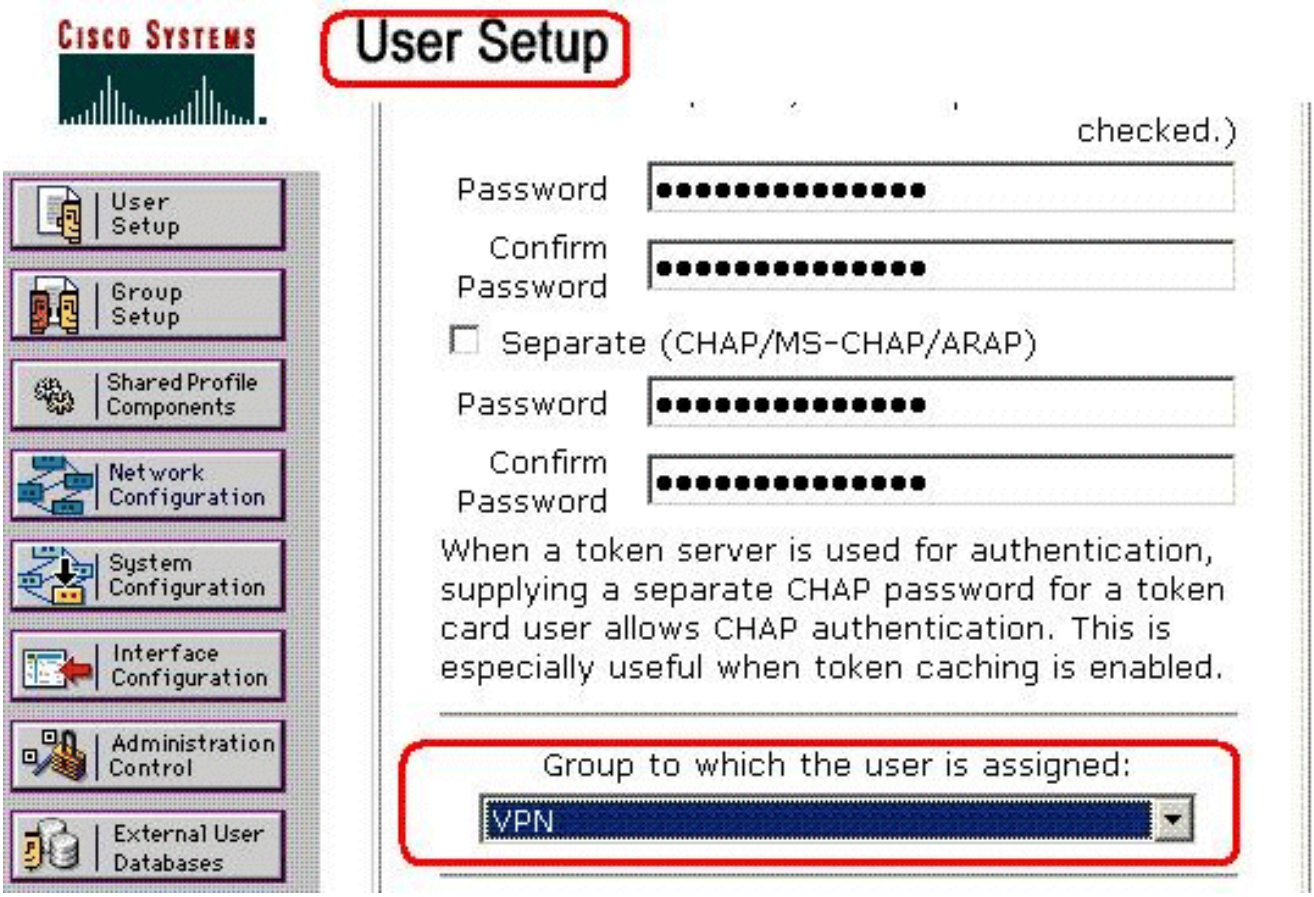


4. تحت قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل، انقر فوق خانة الاختيار **تعيين قائمة التحكم في الوصول (ACL) إلى IP**. أختر قائمة تحكم في الوصول (ACL) إلى IP من



القائمة.

5. لحفظ إعدادات المجموعة التي قمت بإجرائها للتو، انقر فوق **إرسال**.
6. انتقل إلى "إعداد المستخدم" وقم بتحرير المستخدم الذي تريد إضافته إلى المجموعة: **VPN**. عند الانتهاء، انقر فوق
إرسال.



يتم الآن تطبيق قائمة التحكم في الوصول (ACL) القابلة للتنزيل التي تم تكوينها لمجموعة VPN على هذا المستخدم.

7. لمتابعة تحديد إعدادات المجموعة الأخرى، قم بتنفيذ إجراءات أخرى في هذا الفصل، حسب ما يكون منطبقا

تكوين إعدادات IETF RADIUS لمجموعة مستخدمين

لتنزيل اسم لقائمة وصول قمت بإنشائها بالفعل على جهاز الأمان من خادم RADIUS عند مصادقة المستخدم، قم بتكوين السمة IETF RADIUS filter-id (السمة رقم 11) كما يلي:

```
filter-id=acl_name
```

تتم مصادقة مستخدم مجموعة **cisco**"VPN" بنجاح، ويقوم خادم RADIUS بتنزيل اسم قائمة التحكم في الوصول (جديد) لقائمة وصول قمت بإنشائها بالفعل على جهاز الأمان . يمكن للمستخدم "cisco" الوصول إلى جميع الأجهزة الموجودة داخل شبكة ASA **باستثناء** خادم 10.1.1.2. للتحقق من قائمة التحكم في الوصول (ACL)، راجع قسم قائمة التحكم في الوصول إلى معرف التصفية.

وفقا للمثال، تم تكوين قائمة التحكم في الوصول (ACL) المسماة **جديدة** للتصفية في ASA.

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

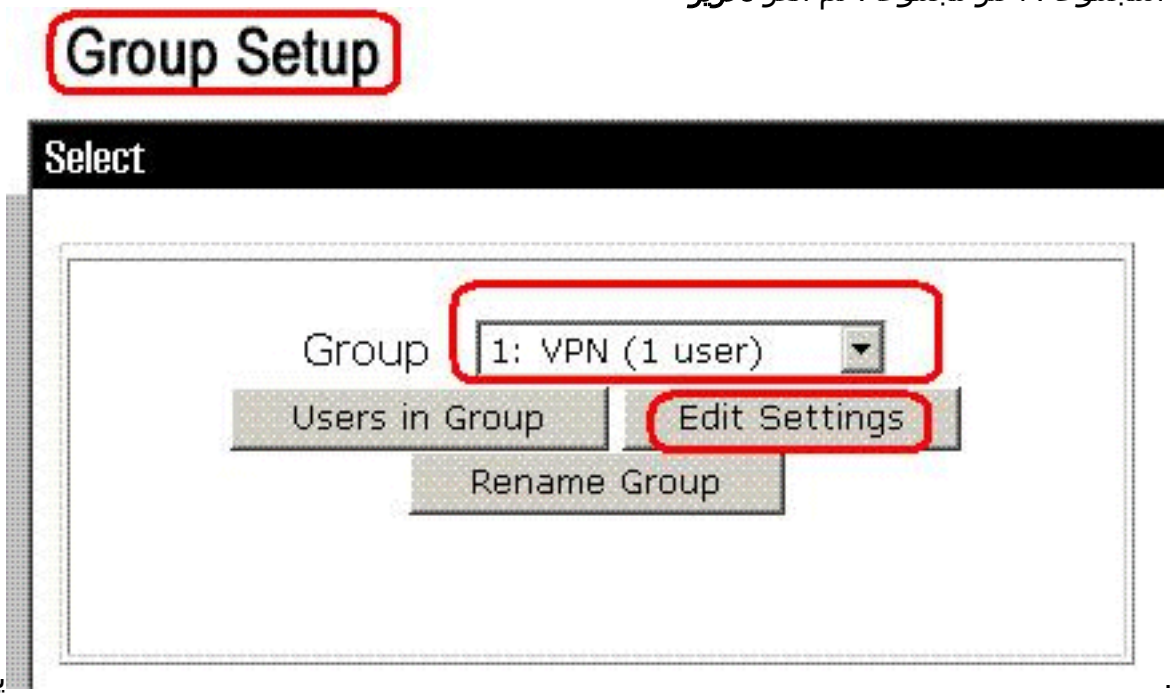
تظهر هذه المعلمات فقط عندما تكون صحيحة. لقد قمت بتهيئة

- عميل AAA لاستخدام أحد بروتوكولات RADIUS في تكوين الشبكة
- سمات RADIUS على مستوى المجموعة في صفحة RADIUS (IETF) في قسم تكوين الواجهة بواجهة الويب

يتم إرسال سمات RADIUS كملف تعريف لكل مستخدم من ACS إلى عميل AAA الطالب.

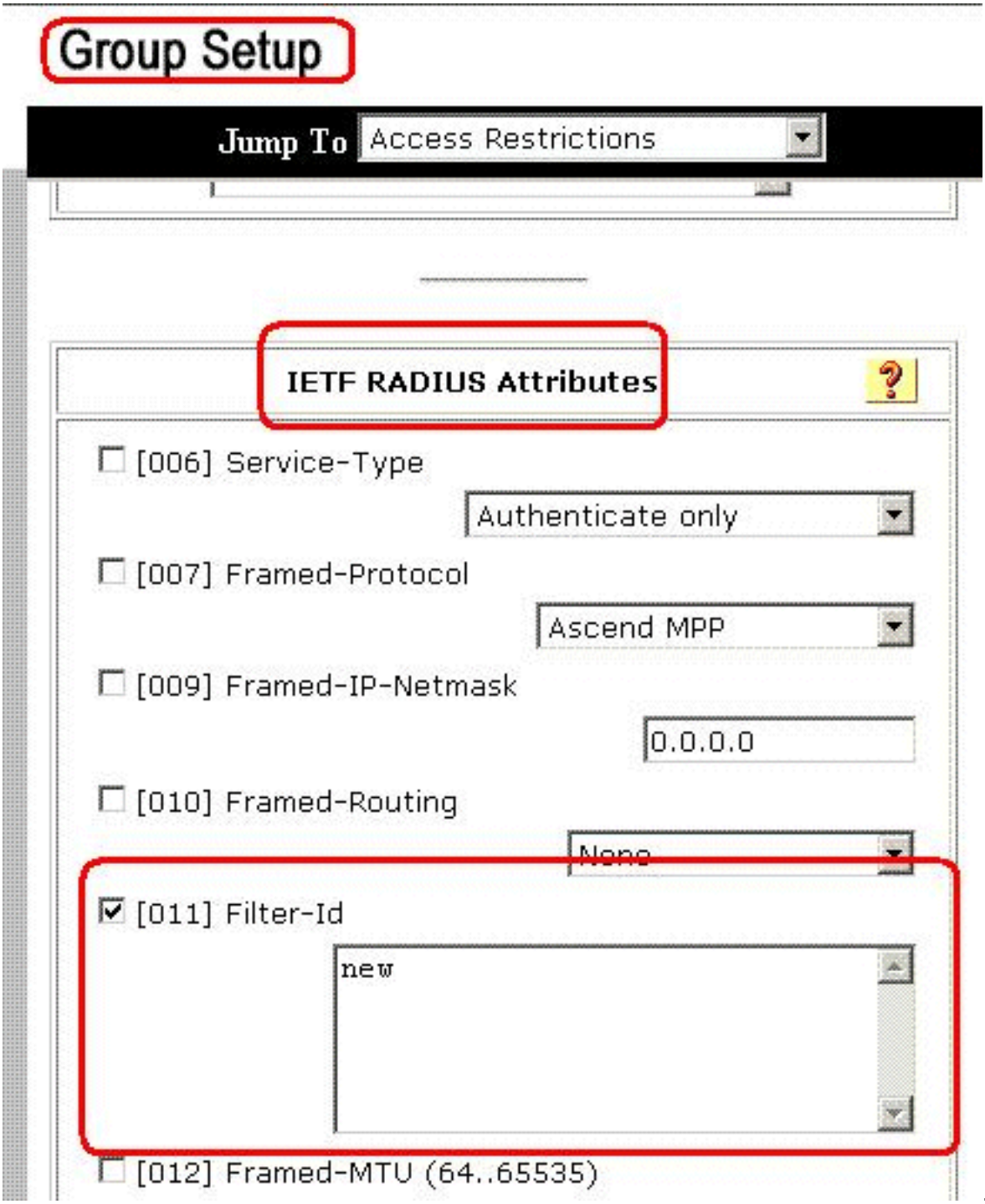
لتكوين إعدادات سمة IETF RADIUS لتطبيقها كتخويل لكل مستخدم في المجموعة الحالية، قم بتنفيذ هذه الإجراءات:

1. في شريط التنقل، انقر فوق **إعداد المجموعة**.يتم فتح صفحة تحديد إعداد المجموعة.
2. من قائمة المجموعة، أختر مجموعة، ثم انقر **تحرير**



يظ **الإعدادات**.
هر اسم المجموعة في أعلى صفحة إعدادات المجموعة.

3. قم بالتمرير إلى سمات RADIUS الخاصة ب IEFT. لكل سمة IETF RADIUS، يجب عليك تخويل المجموعة الحالية. حدد خانة الاختيار الخاصة بسمة **Filter-Id [011]**، ثم قم بإضافة اسم قائمة التحكم في الوصول (ACL) المحدد من قبل ASA (**جديد**) في التخويل الخاص بالسمة في الحقل. ارجع إلى *عرض* ASA *الذي يشغل* إخراج



التكوين.

4. لحفظ إعدادات المجموعة التي قمت بإجرائها وتطبيقها مباشرة، انقر فوق **إرسال وتطبيق**.**ملاحظة:** لحفظ إعدادات مجموعتك وتطبيقها لاحقا، انقر فوق **إرسال**. عندما تكون مستعدا لتنفيذ التغييرات، أختر **تكوين النظام > التحكم في الخدمة**. ثم أختر **إعادة التشغيل**.

التحقق من الصحة

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** .

إظهار أوامر التشفير

- **show crypto isakmp sa**— يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.

```
ciscoasa# sh 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: 192.168.10.2   1
Type    : user            Role    : responder
Rekey   : no              State   : AM_ACTIVE
                                                #ciscoasa
```

- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل SAs الحالية.

```
                                    ciscoasa# sh crypto ipsec sa
                                              interface: outside
                    ,Crypto map tag: outside_dyn_map, seq num: 1
                                       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: 192.168.10.2, username: cisco
                         dynamic allocated peer ip: 192.168.5.1

                                :pkts encaps: 65, #pkts encrypt#
                                              pkts digest: 65# ,65
                                :pkts decaps: 65, #pkts decrypt#
                                              pkts verify: 65# ,65
                     pkts compressed: 0, #pkts decompressed: 0#
                    :pkts not compressed: 4, #pkts comp failed#
                                           pkts decomp failed: 0# ,0
                    :pre-frag successes: 0, #pre-frag failures#
                                            fragments created: 0# ,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.: 192.168.10.2

                               ,path mtu 1500, ipsec overhead 58
                                                media mtu 1500
                                  current outbound spi: EEF0EC32

                                                :inbound esp sas
                                          (spi: 0xA6F92298 (2801345176
                             transform: esp-3des esp-sha-hmac none
                                  { ,in use settings ={RA, Tunnel
                              :slot: 0, conn_id: 86016, crypto-map
                                                outside_dyn_map
                    :(sa timing: remaining key lifetime (sec
                                                           28647
                                             IV size: 8 bytes
                                        replay detection support: Y
                                                       :outbound esp sas
                                          (spi: 0xEEF0EC32 (4008766514
                             transform: esp-3des esp-sha-hmac none
                                  { ,in use settings ={RA, Tunnel
                              :slot: 0, conn_id: 86016, crypto-map
                                                outside_dyn_map
                    sa timing: remaining key lifetime (sec): 28647
                                             IV size: 8 bytes
                                        replay detection support: Y
```

قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة

تحقق من قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم Cisco. يتم تنزيل قوائم التحكم في الوصول (ACL) من CSACS.

```
ciscoasa(config)# sh access-list
,access-list cached ACL log flows: total 0
          (denied 0 (deny-flow-max 4096
            alert-interval 300
               access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
                hitcnt=0) 0x8719a411) 255.255.255.0 192.168.5.0

(access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
                    ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
 access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
                          ip any any (hitcnt=40) 0x7c718bd1
```

قائمة التحكم في الوصول (ACL) لمعرف عامل التصفية

تم تطبيق Filter-ID [011] على المجموعة - VPN، ويتم تصفية مستخدمي المجموعة وفقا لقائمة التحكم في الوصول (ACL) (الجديدة) المعرفة في ASA.

```
ciscoasa# sh access-list
,access-list cached ACL log flows: total 0
          (denied 0 (deny-flow-max 4096
            alert-interval 300
               access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
       255.255.255.0 192.168.5.0 255.255.255.0
                hitcnt=0) 0x8719a411)
               access-list new; 2 elements
   access-list new line 1 extended deny ip
       any host 10.1.1.2 (hitcnt=4) 0xb247fec8
 access-list new line 2 extended permit ip any any
                hitcnt=39) 0x40e5d57c)
```

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) ل L2L و Remote Access.

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
- مدير أجهزة حلول الأمان المعدلة من Cisco
- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- صفحة دعم عميل شبكة VPN من Cisco
- خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows
- 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).