ASA 7.1/7.2: السماح بنفق انقسام SVC على مثال تكوين ASA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
تكوينات ASA باستخدام ASDM 5.2(2)
التكوين (ASA 7.2(2 باستخدام CLI
إنشاء اتصال SSL VPN باستخدام SVC
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يوفر هذا المستند إرشادات خطوة بخطوة حول كيفية السماح لعملاء طبقة مأخذ التوصيل الآمنة (SVC) VPN (SSL) بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في جهاز الأمان القابل للتكيف (ASA) من Cisco. يتيح هذا التكوين ل SVC الوصول الآمن إلى موارد الشركة من خلال SSL ويمنح وصولا غير آمن إلى الإنترنت باستخدام الاتصال النفقي المنقسم.

تعرف القدرة على إرسال حركة المرور الآمنة وغير الآمنة على نفس الواجهة باسم تقسيم الاتصال النفقي. يتطلب تقسيم الاتصال النفقي تحديد حركة المرور المؤمنة بالضبط وما هي وجهة حركة المرور هذه، بحيث تدخل حركة المرور المحددة فقط النفق، بينما يتم إرسال الباقي غير مشفر عبر الشبكة العامة (الإنترنت).

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- امتيازات إدارية محلية على جميع محطات العمل البعيدة
- عناصر تحكم Java و ActiveX على محطة العمل البعيدة
- لم يتم حظر المنفذ 443(SSL) في أي مكان على مسار الاتصال

المكونات المستخدمة

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

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 7.2(2) من البرنامج
- إصدار عميل Cisco SSL VPN ل Windows 1.1.4.179 **ملاحظة:** قم بتنزيل حزمة عميل SSL VPN (sslclient-win*.pkg) من تنزيل برامج Cisco (للعملاء المسجلين فقط). انسخ SVC إلى ذاكرة Flash (الذاكرة المؤقتة) ل ASA، والتي يجب تنزيلها إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع تثبت قسم برنامج SVC في دليل تكوين ASA للحصول على مزيد من المعلومات.
- كمبيوتر يعمل بنظام التشغيل Windows 2000 Professional SP4 أو Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 5.2(2)

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.

الاصطلاحات

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

معلومات أساسية

ال SSL VPN Client (SVC) هو تقنية VPN tunneling التي تمنح المستخدمين عن بعد فوائد IPsec VPN Client دون الحاجة إلى أن يقوم مسؤولو الشبكة بتثبيت وتكوين عملاء IPsec VPN على أجهزة الكمبيوتر البعيدة. يستخدم SVC تشفير SSL الموجود بالفعل على الكمبيوتر البعيد بالإضافة إلى تسجيل دخول WebVPN ومصادقة جهاز الأمان.

من أجل إنشاء جلسة SVC، يدخل المستخدم البعيد عنوان IP الخاص بواجهة WebVPN الخاصة بجهاز الأمان في المستعرض، ويتصل المستعرض بتلك الواجهة ويعرض شاشة تسجيل الدخول إلى WebVPN. إذا كنت تريد التحقق من تسجيل الدخول والمصادقة، ويقوم جهاز الأمان بتعريفك على أنك تحتاج إلى SVC، فإن جهاز الأمان يقوم بتنزيل SVC إلى الكمبيوتر البعيد. إذا قام جهاز الأمان بتعريفك بخيار إستخدام SVC، فإن جهاز الأمان يقوم بتنزيل SVC إلى الكمبيوتر البعيد أثناء تقديمه إرتباط على الإطار لتخطي تثبيت SVC.

بعد التنزيل، يقوم SVC بتثبيت نفسه وتكوينه، ومن ثم يبقى SVC أو يقوم بإلغاء تثبيت نفسه، والذي يعتمد على التكوين، من الكمبيوتر البعيد عند إنهاء الاتصال.

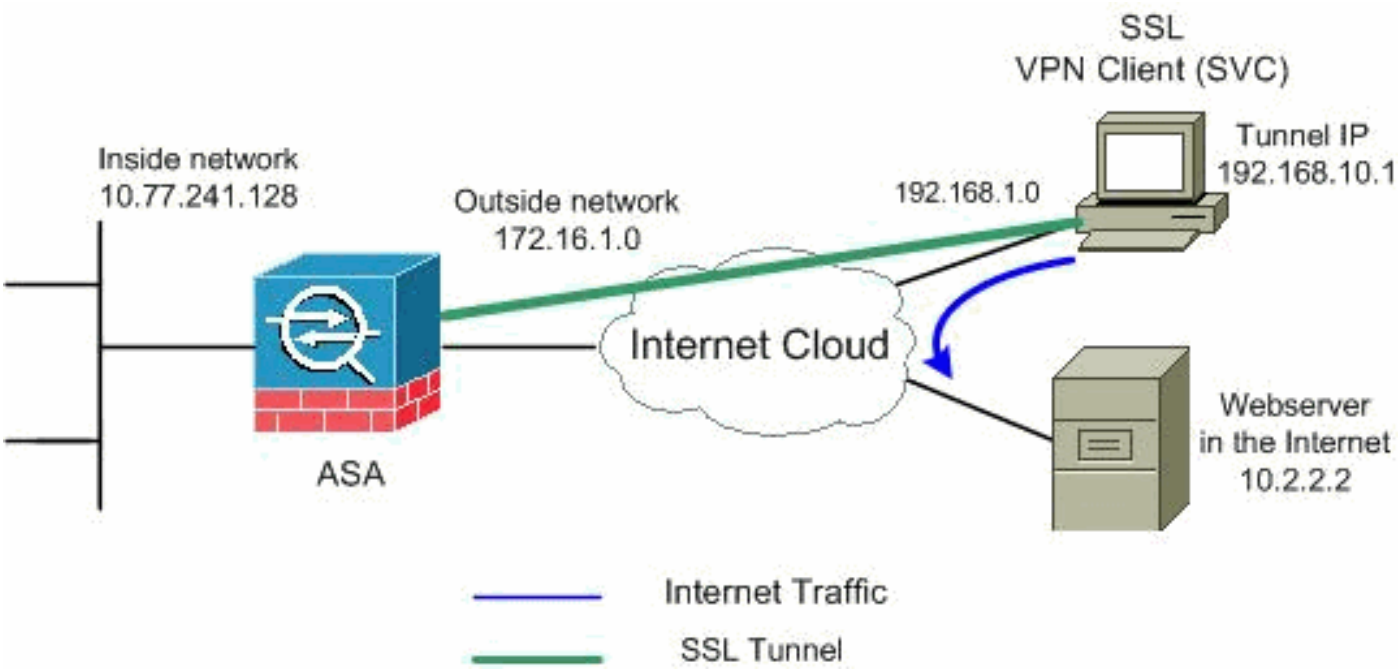
التكوين

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:

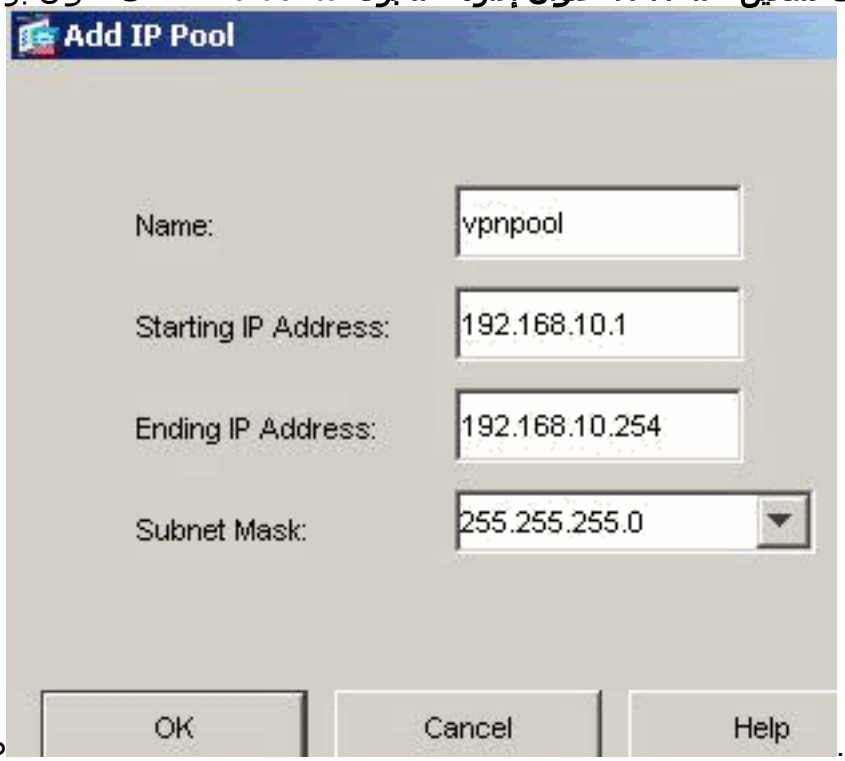


ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

تكوينات ASA باستخدام ASDM 5.2(2)

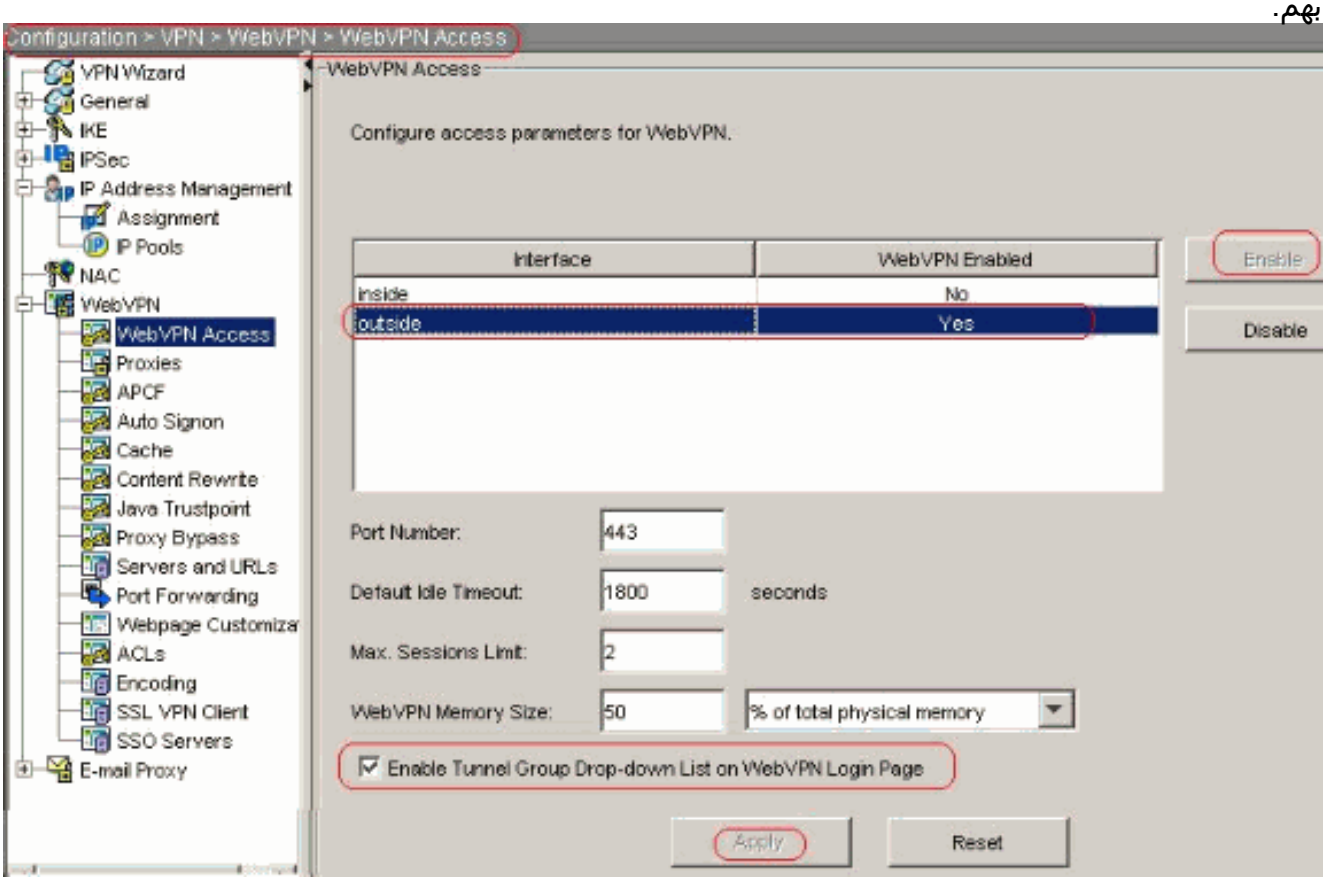
أتمت هذا steps in order to شكلت ال SSL VPN على ASA مع انقسام tunneling كما هو موضح:

1. يفترض المستند أن التكوين الأساسي مثل تكوين الواجهة وما إلى ذلك قد تم إنشاؤه بالفعل ويعمل بشكل صحيح.**ملاحظة:** ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.**ملاحظة:** لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. راجع ASDM و WebVPN الذي تم تمكينه على نفس واجهة ASA للحصول على مزيد من المعلومات.
2. أخترت **تشكيل>IP>VPN عنوان إدارة>IP بركة** in order to خلقت عنوان بركة: **VPNpool** ل VPN

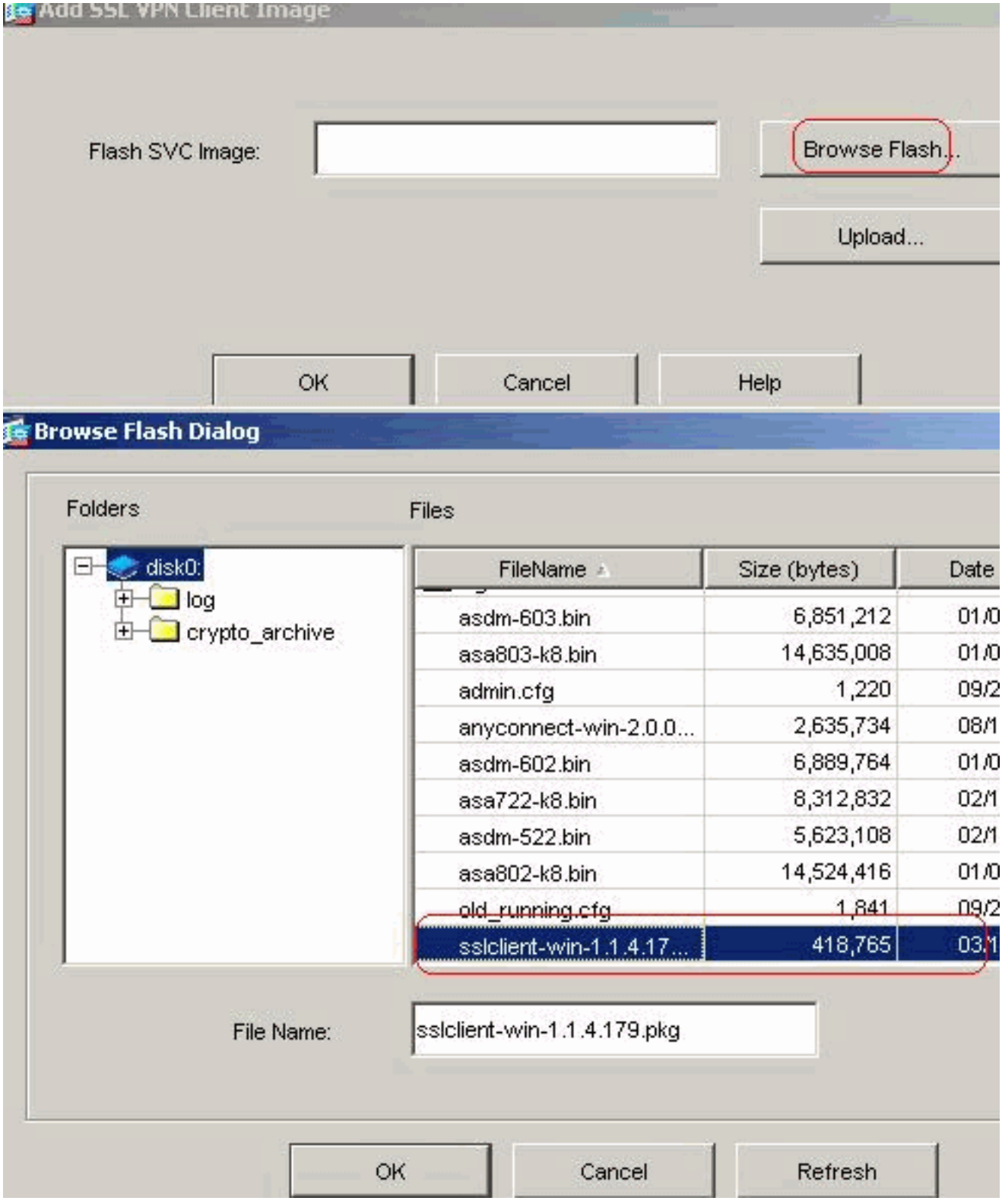


زبون. طقطقة **يطبق**.
3. **تمكين WebVPN**أخترت **تشكيل>WebVPN>WebVPN>VPN منفذ** وأبرزت القارن خارجي مع ماوس وطقطقة **يمكن**. حدد خانة الاختيار **تمكين القائمة المنسدلة لمجموعة النفق على صفحة تسجيل الدخول إلى**

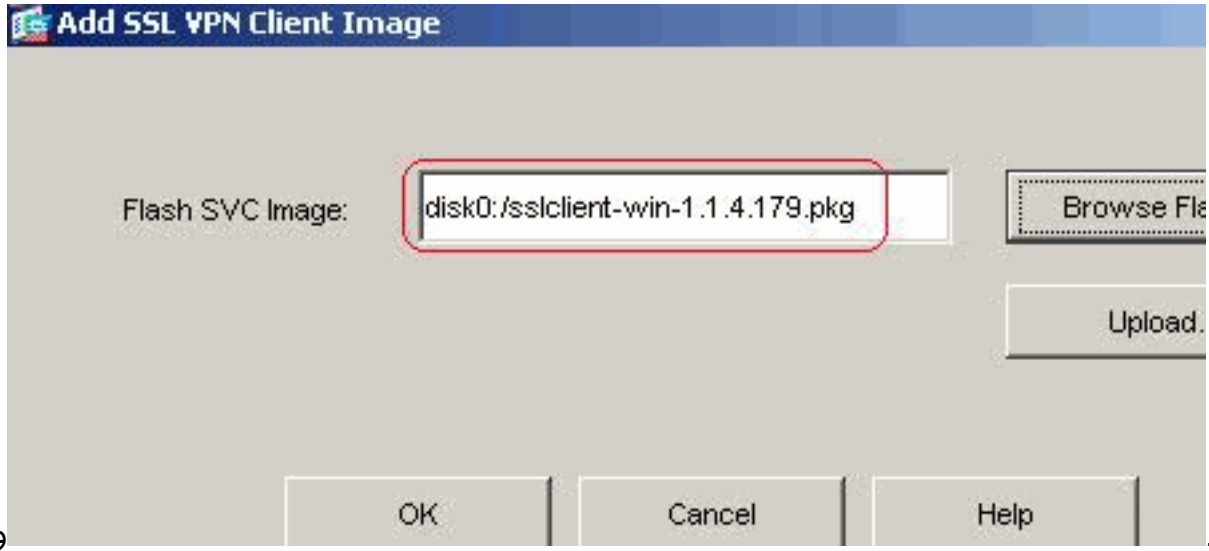
WebVPN لتمكين ظهور القائمة المنسدلة في صفحة تسجيل الدخول للمستخدمين، لاختيار المجموعات الخاصة بهم.



طقطقة **يطبق**.أخترت **تشكيل>SSL VPN>WebVPN>VPN زبون>إضافة** in order to أضفت ال SSL VPN زبون صورة من البرق ذاكرة من ASA كما هو موضح.

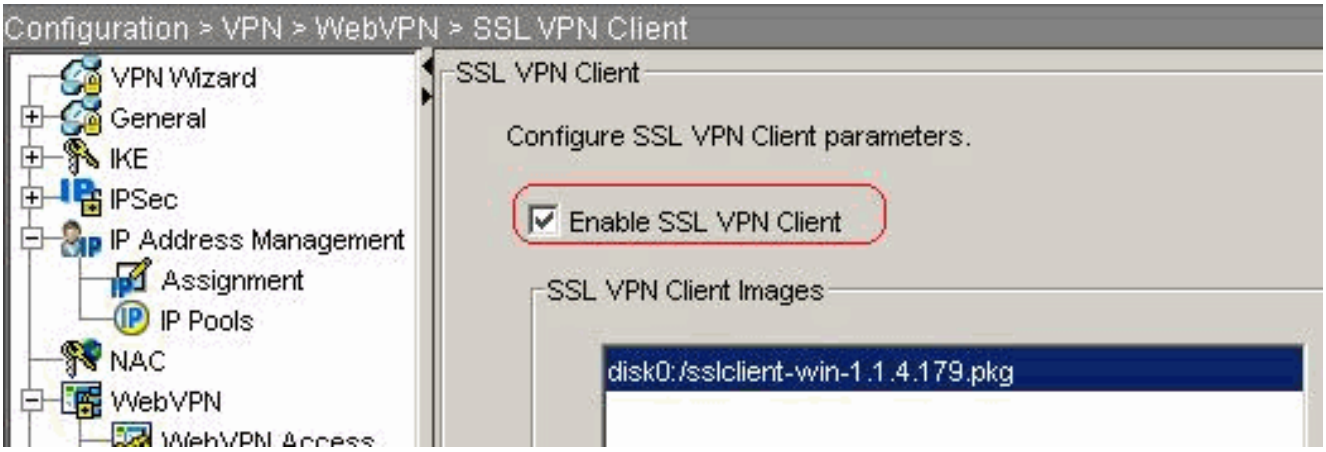

Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin 6,851,212 01/0
asa803-k8.bin 14,635,008 01/0
admin.cfg 1,220 09/2
anyconnect-win-2.0.0... 2,635,734 08/1
asdm-602.bin 6,889,764 01/0
asa722-k8.bin 8,312,832 02/1
asdm-522.bin 5,623,108 02/1
asa802-k8.bin 14,524,416 01/0
old_running.cfg 1,841 09/2
sslclient-win-1.1.4.17... 418,765 03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

وانقر فوق



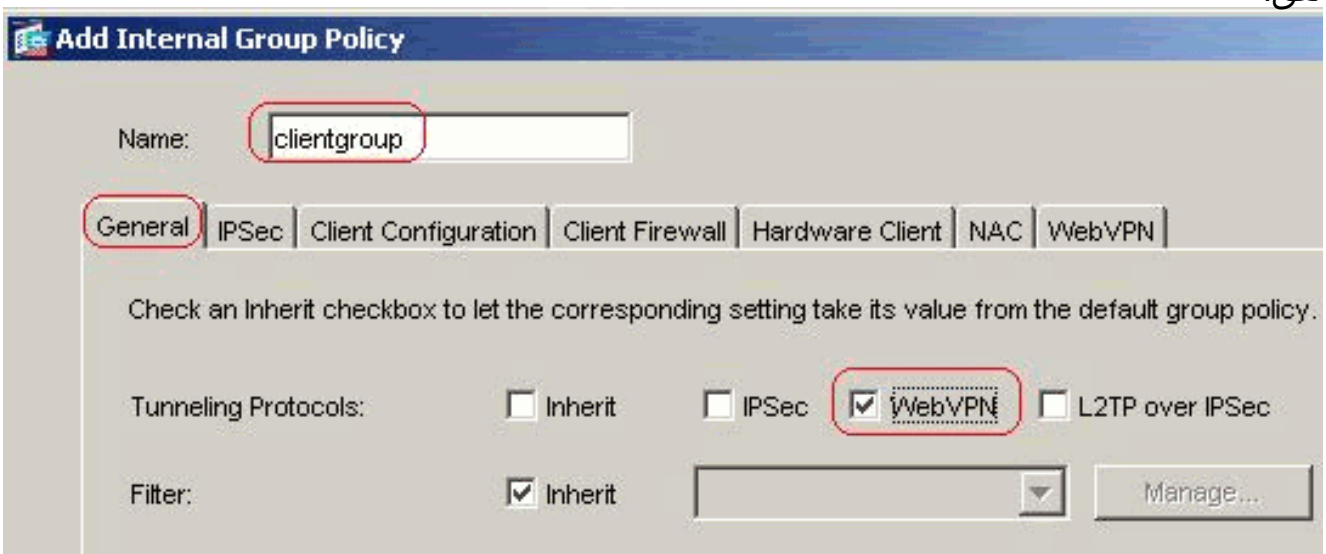
وانقر **OK**.

فوق **OK**.انقر فوق خانة الاختيار **SSL VPN Client**.

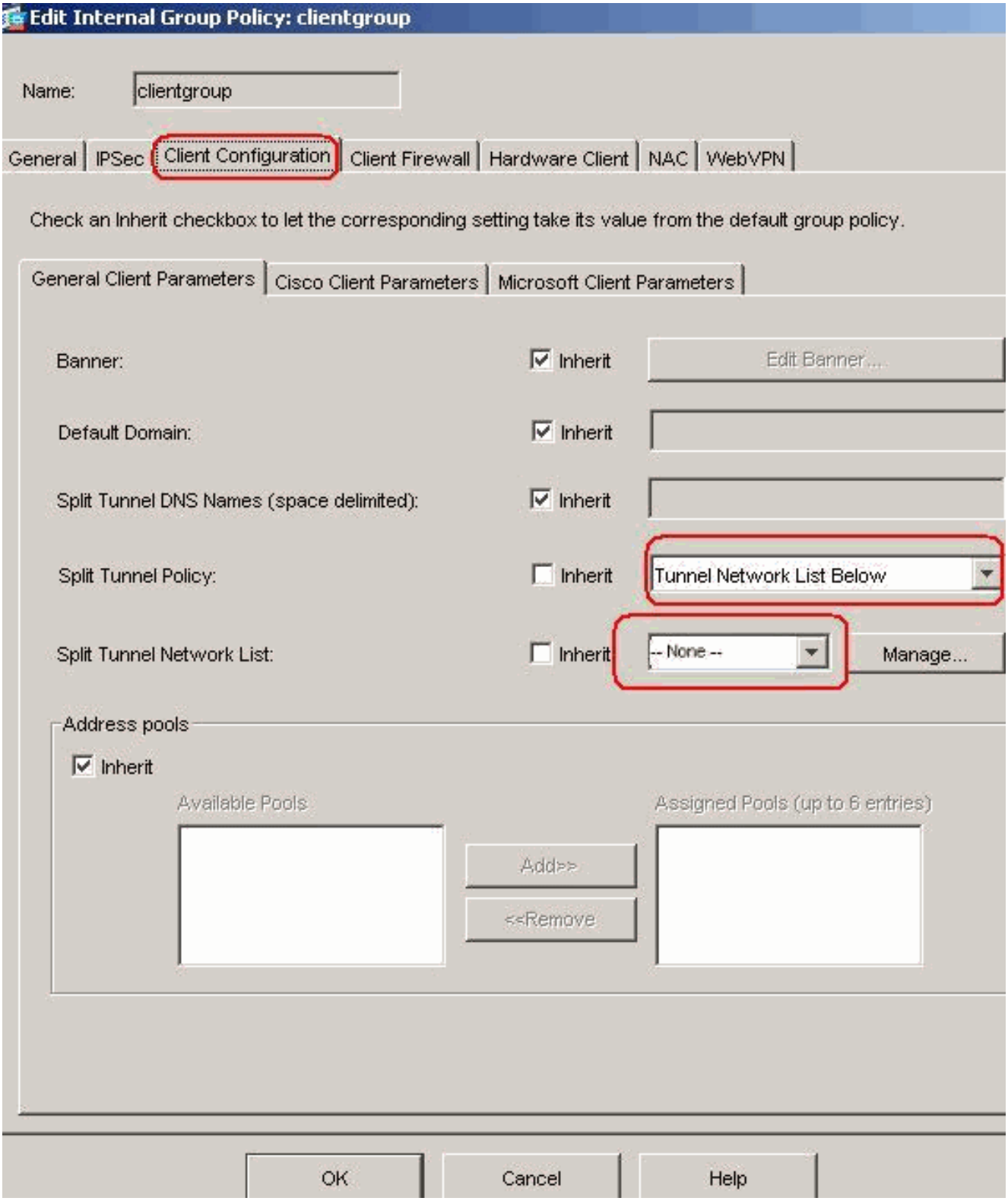


طقطقة **يطبق**.**CLI تشكيل مكافئ:**

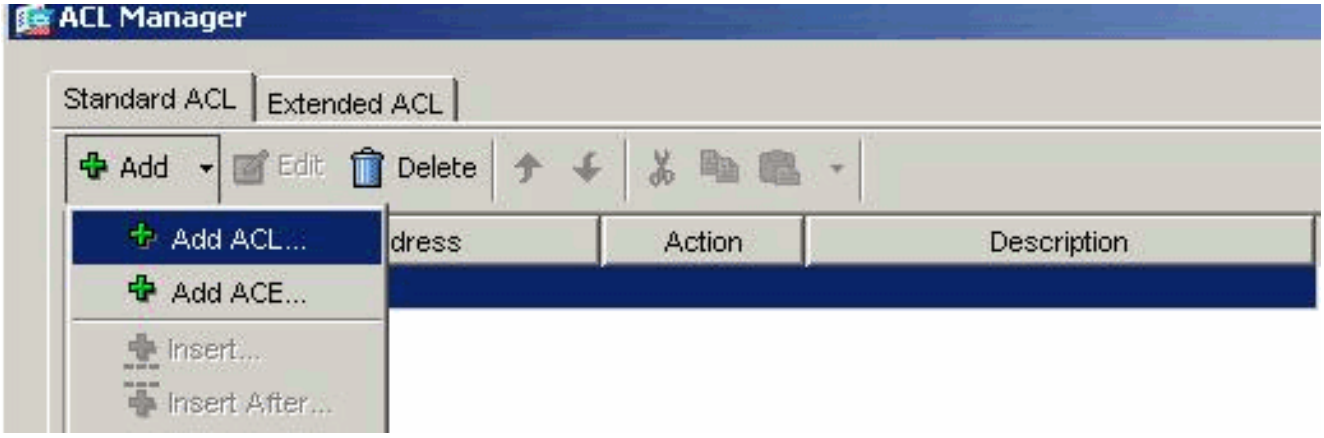
4. **تكوين نهج المجموعة**أخترت **تشكيل>VPN>عام>مجموعة سياسة>إضافة (داخلي مجموعة سياسة)** in order to خلقت داخلي مجموعة **زبون** سياسة مجموعة. تحت **عام**، أختر خانة الاختيار **WebVPN** لتمكين WebVPN كبروتوكول نفق.



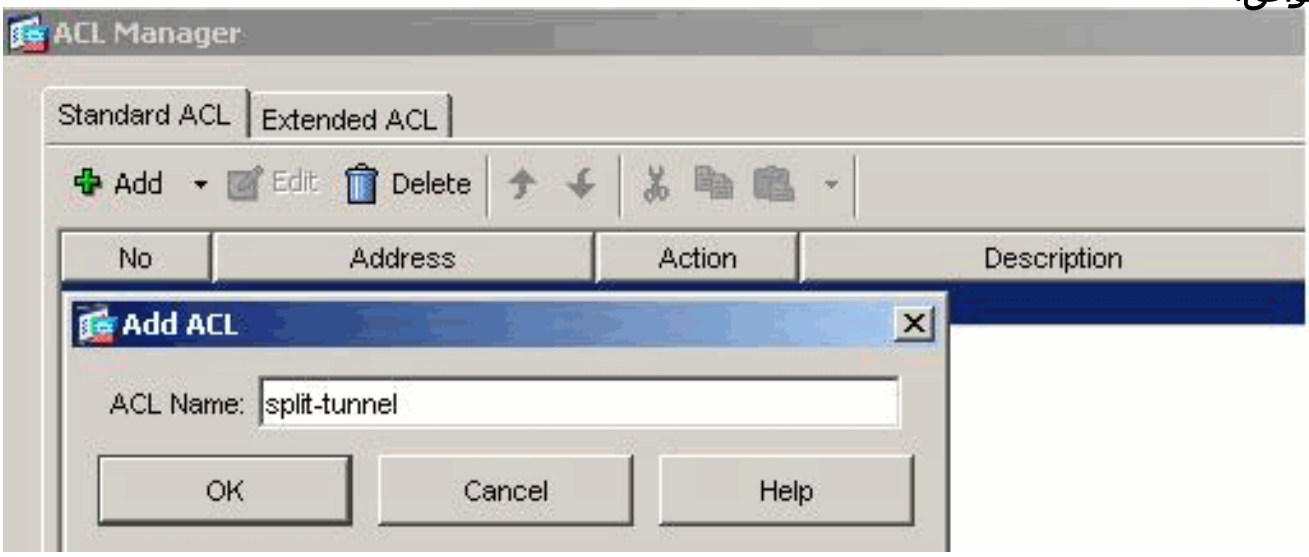
في علامة التبويب **تكوين العميل > معلمات العميل العامة**، قم بإلغاء تحديد مربع **Inherit** لنهج النفق المقسم واختر **قائمة شبكة النفق أدناه** من القائمة المنسدلة.قم بإلغاء تحديد مربع **Inherit** لقائمة **شبكات النفق المقسم** ثم انقر فوق **Manage** لتشغيل إدارة قائمة التحكم في الوصول (ACL).



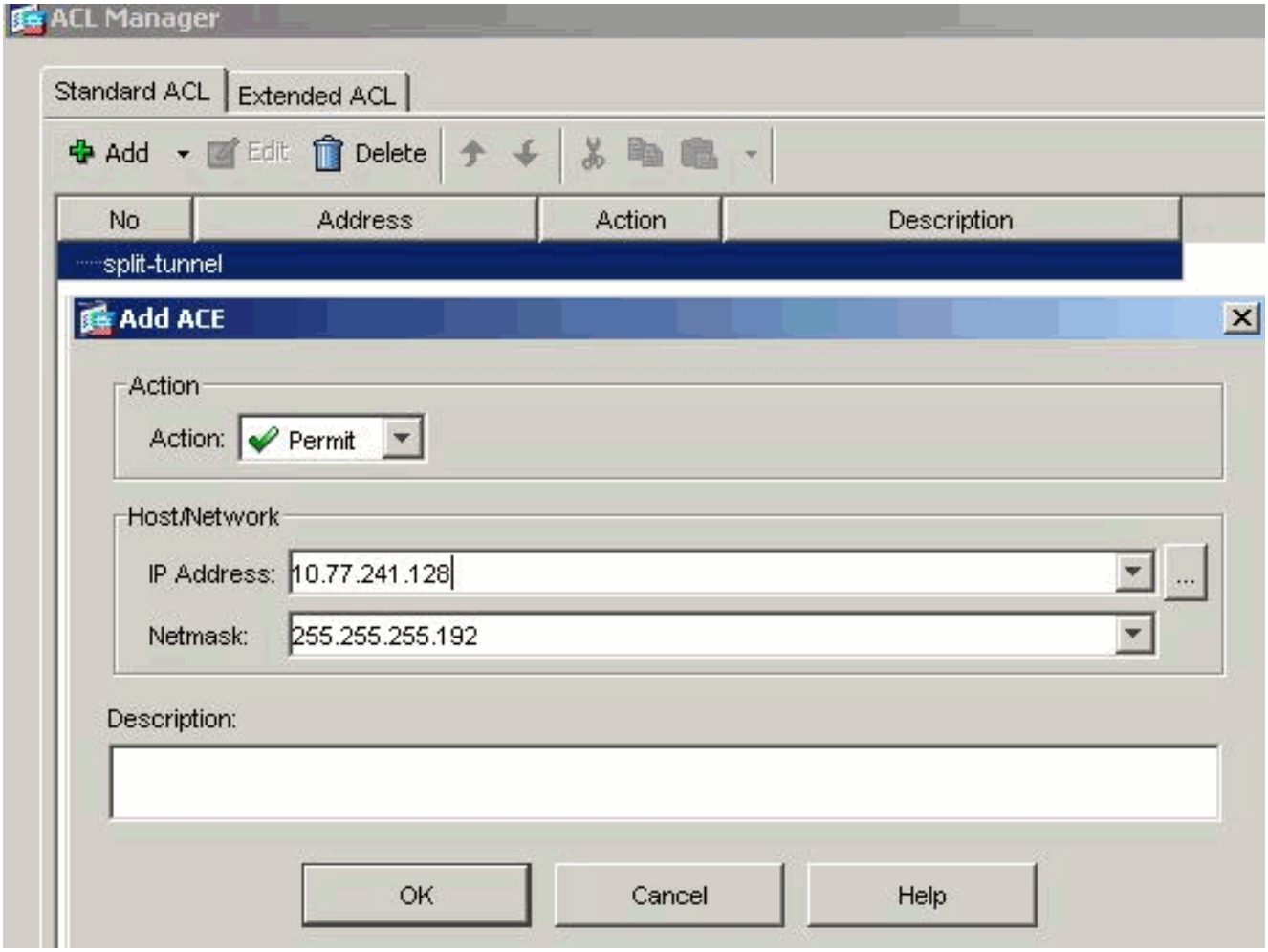
ضمن إدارة قائمة التحكم في الوصول (ACL)، أختر **إضافة > قائمة التحكم في الوصول (ACL)**.. لإنشاء قائمة وصول
جديدة.



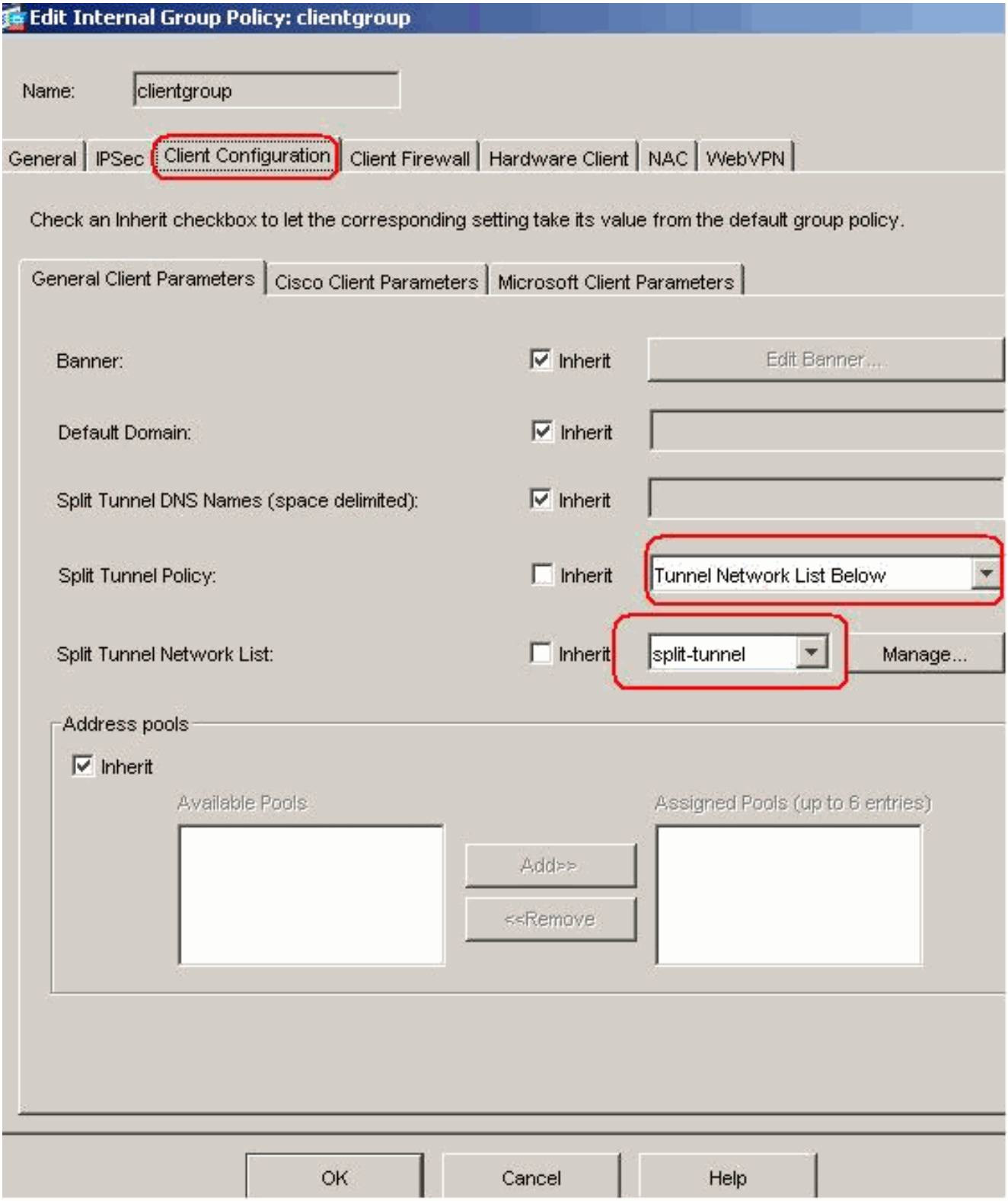
قم بتوفير اسم لقائمة التحكم بالوصول (ACL) وانقر فوق **موافق**.



بمجرد إنشاء اسم قائمة التحكم في الوصول، أختر **إضافة > إضافة ACE** لإضافة إدخال التحكم في الوصول (ACE).عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 26/10.77.241.128 واختر **السماح**.انقر فوق **موافق** للخروج من إدارة قائمة التحكم في الوصول (ACL).

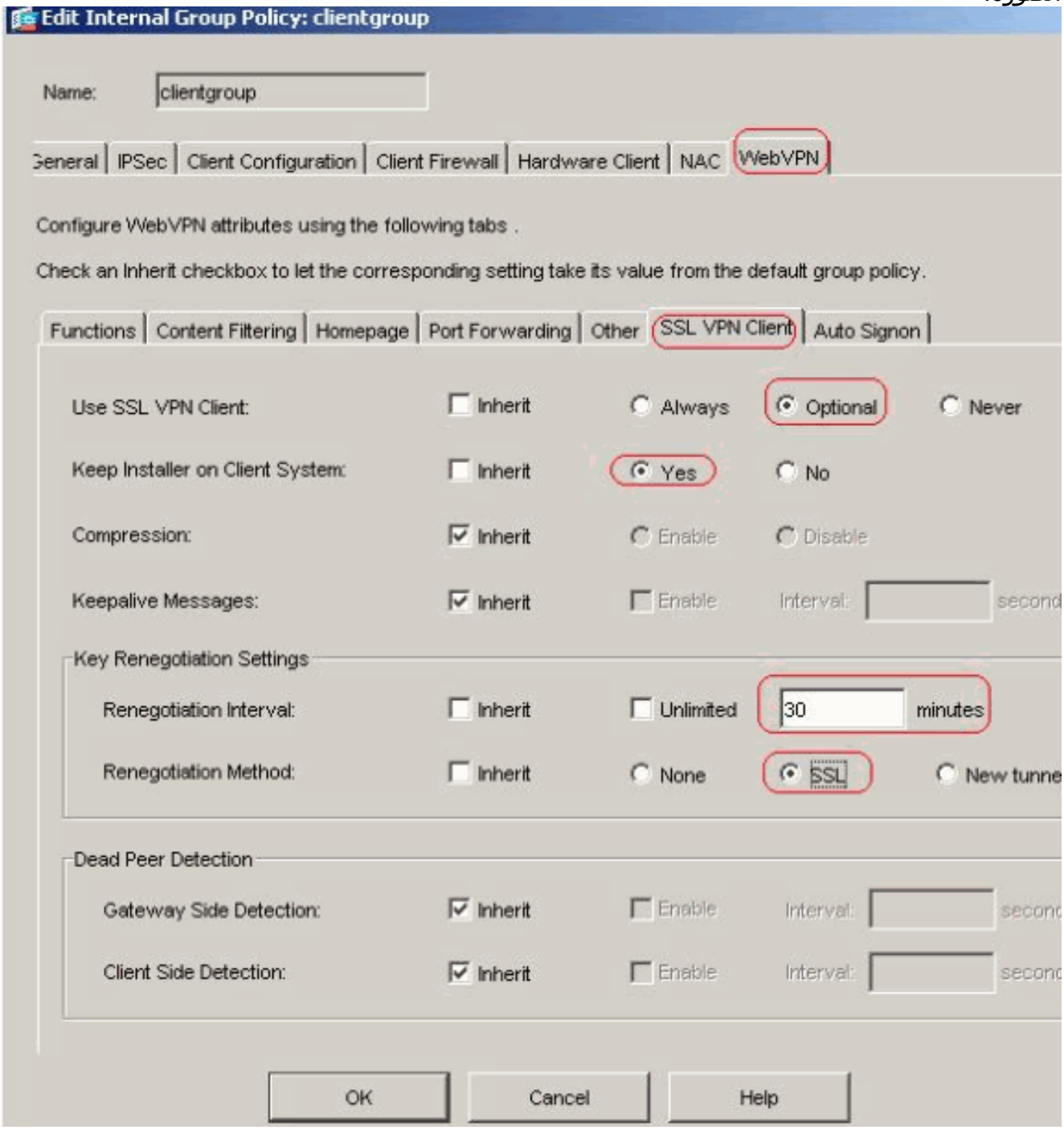


تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق المقسم.انقر فوق **موافق** للعودة إلى تكوين "نهج المجموعة".



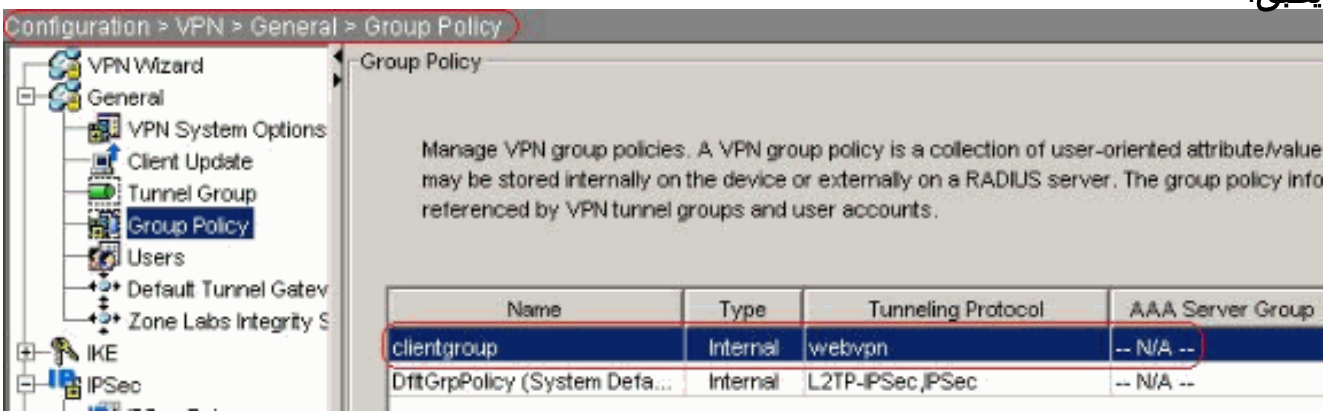
في الصفحة الرئيسية، انقر فوق **تطبيق** ثم **إرسال** (إذا كان ذلك مطلوبا) لإرسال الأوامر إلى ASA.لخيار إستخدام SSL VPN Client، قم بإلغاء تحديد خانة الاختيار **Inherit** وانقر فوق زر الاختيار **الاختياري**.يتيح هذا الخيار للعميل البعيد إختيار ما إذا كان سيتم النقر فوق **WebVPN > عميل SSLVPN** علامة التبويب، واختر الخيارات التالية:لا تقم بتنزيل SVC. يضمن الاختيار الدائم تنزيل SVC إلى محطة العمل البعيدة أثناء كل اتصال SSL VPN.للحصول على خيار إبقاء المثبت على نظام العميل، قم بإلغاء تحديد خانة الاختيار **توريث**، وانقر فوق الزر **نعم** للانتقاء.يسمح هذا الإجراء لبرنامج SVC بالبقاء على جهاز العميل، وبالتالي، لا يتطلب الأمر من ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا للمستخدمين البعيدين الذين غالبا ما يصلون إلى شبكة الشركة.لخيار الفاصل الزمني لإعادة التفاوض، قم بإلغاء تحديد خانة الاختيار **Inherit**، وإلغاء تحديد خانة الاختيار **Unlimited**، وأدخل عدد الدقائق حتى المفتاح.يتم تحسين الأمان عند تعيين الحدود على طول الوقت الذي يكون فيه المفتاح صالحا.لخيار طريقة إعادة التفاوض، قم بإلغاء تحديد خانة الاختيار **Inherit**، وانقر فوق زر انتقاء **SSL**. يمكن أن تستخدم إعادة التفاوض نفق SSL الحالي أو نفق جديد تم

إنشاؤه صراحة لإعادة التفاوض.يجب تكوين سمات عميل SSL VPN الخاصة بك كما هو موضح في هذه الصورة:



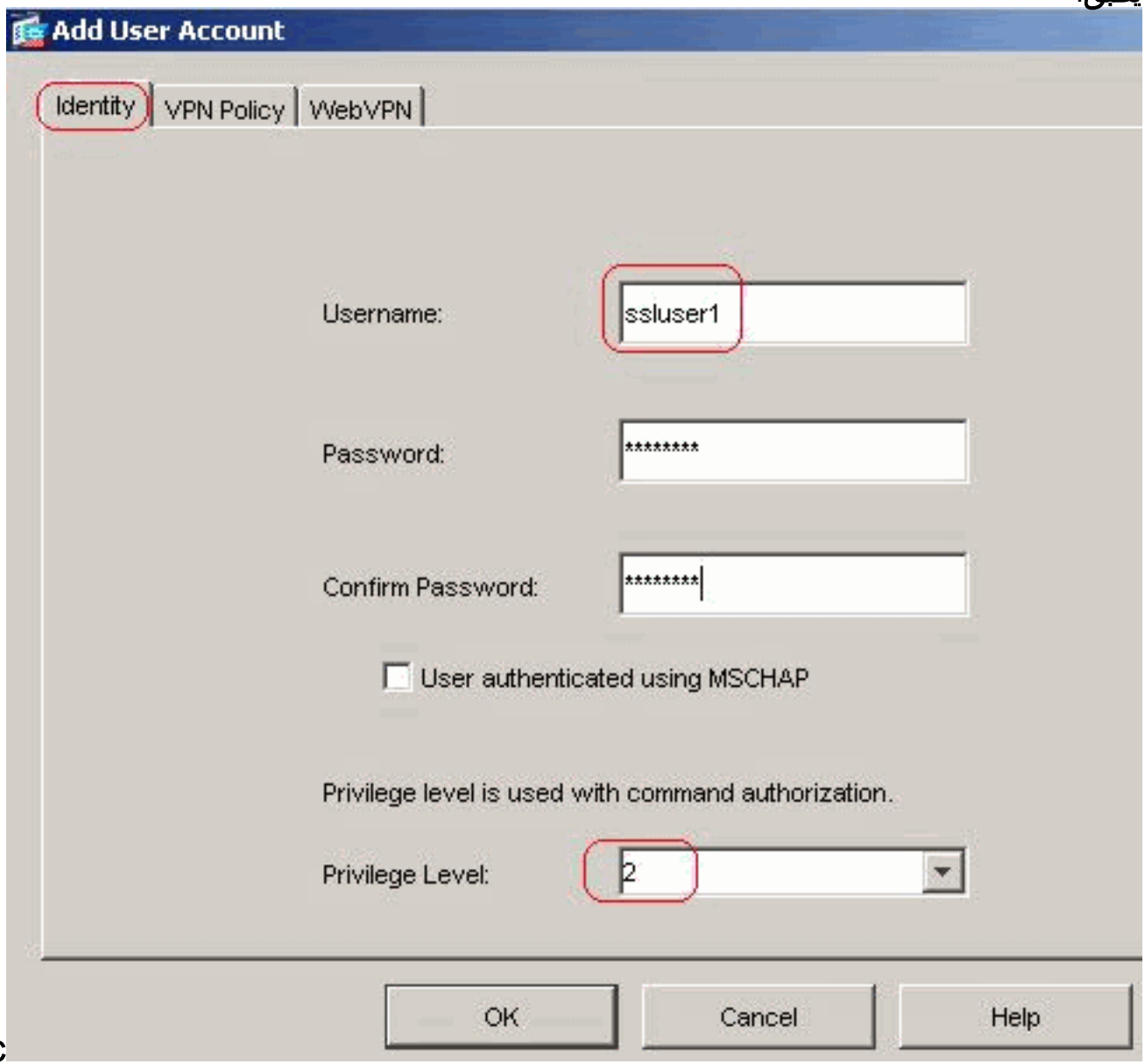
طقطقت **ok** وبعد ذلك

يطبق.



CLI تشكيل مكافئ:

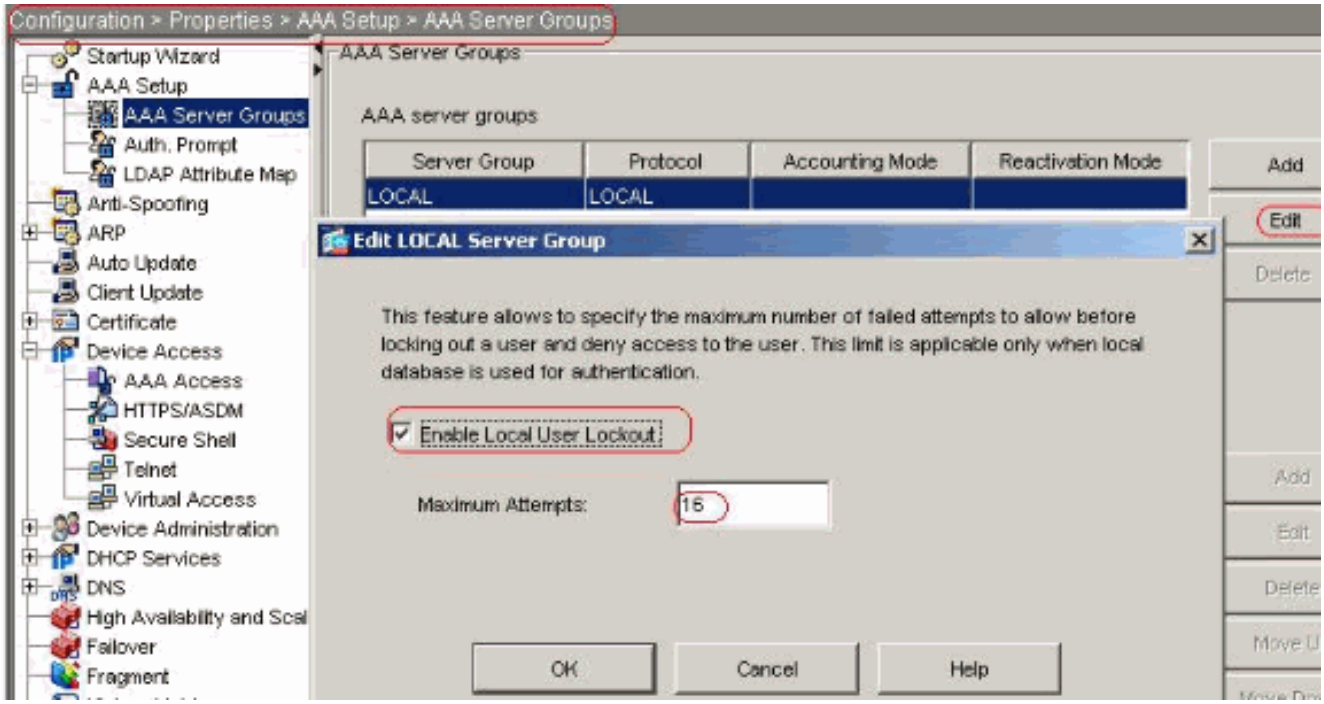
5. أخترت **تشكيل>VPN>عام>مستعمل>يضيف** in order to خلقت جديد مستعمل حساب **ssluser1**. طقطقت **ok** وبعد ذلك
يطبق.



C

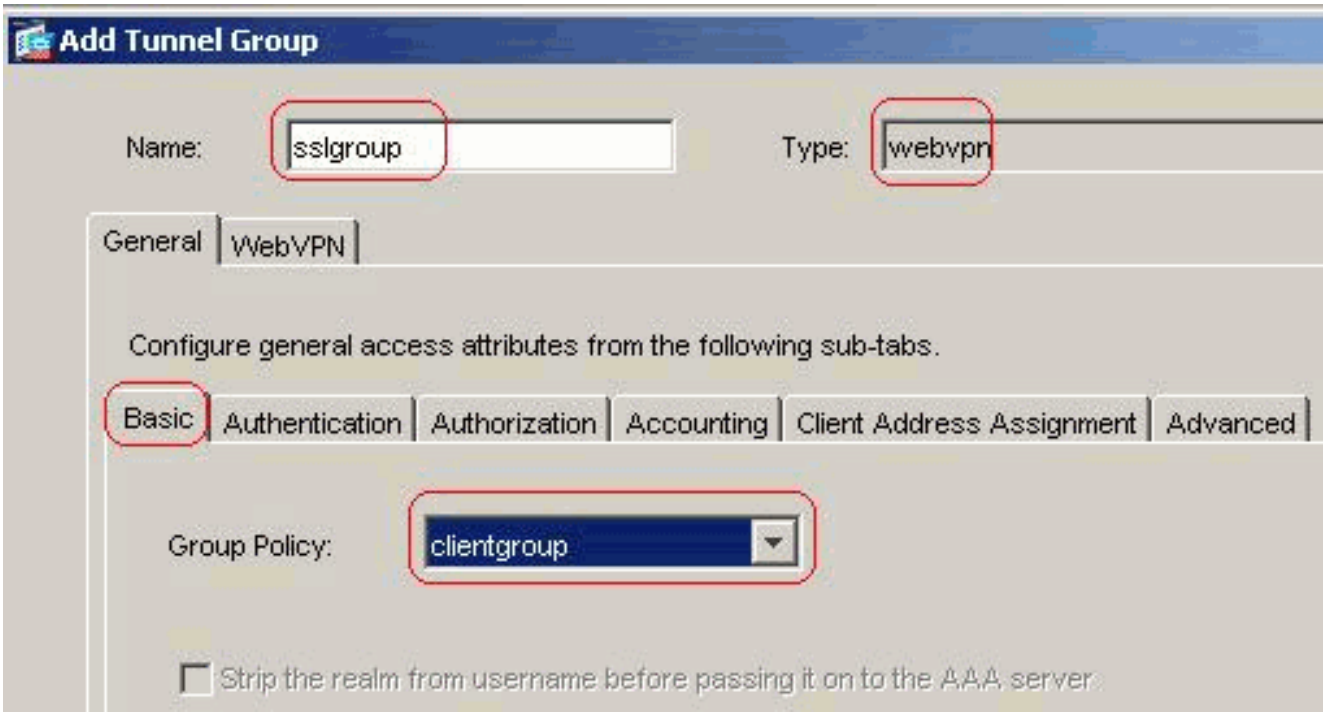
LI تشكيل مكافئ:

6. أخترت **تشكيل>خصائص>AAA setup>AAA نادل مجموعة>**يحرر in order to عدلت التقصير نادل مجموعة **محلي** واخترت **ال enable مستعمل قفل**تدقيق صندوق مع الحد الأقصى يحاول قيمة ك
16.

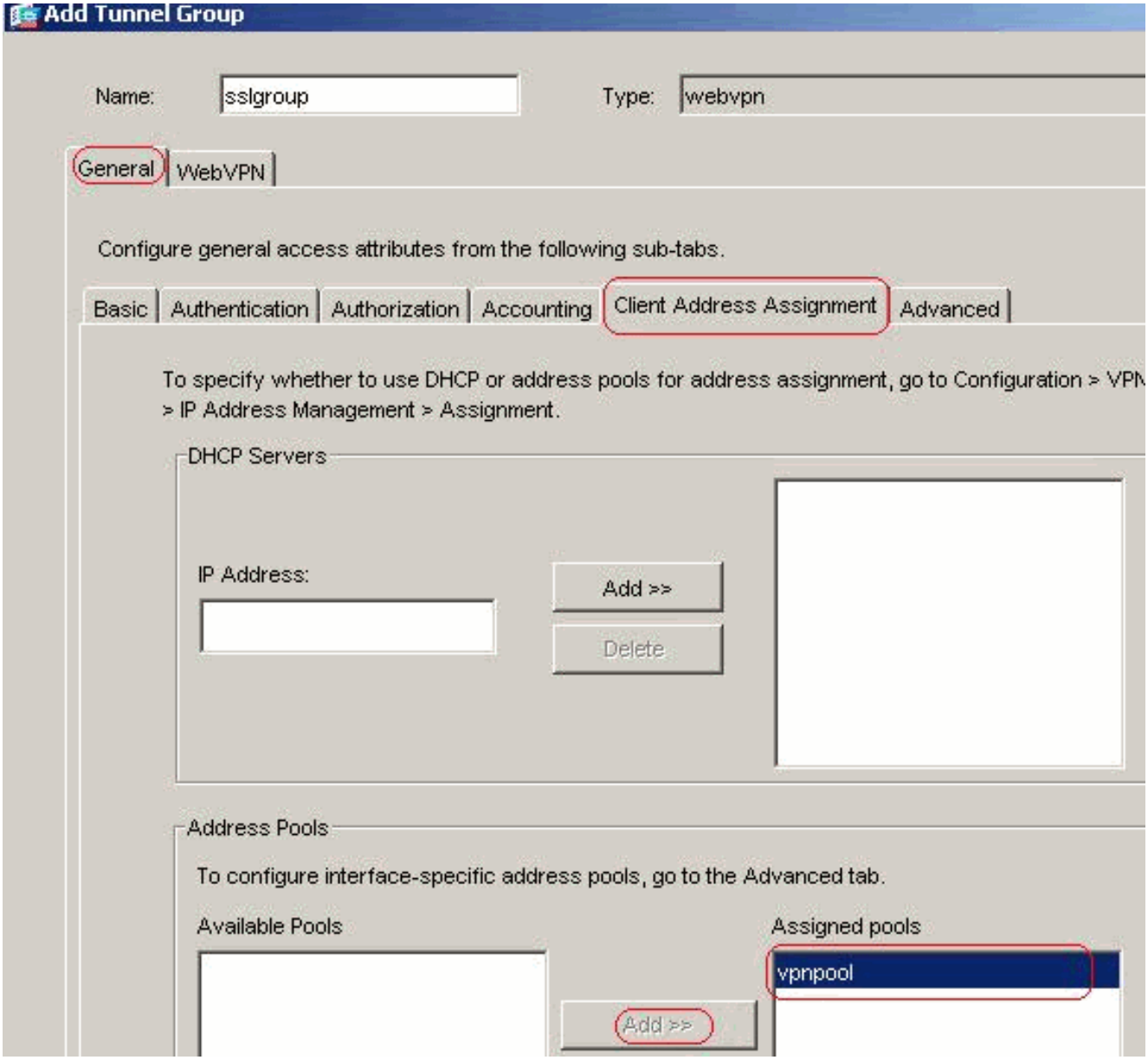


CLI تشكيل مكافئ:

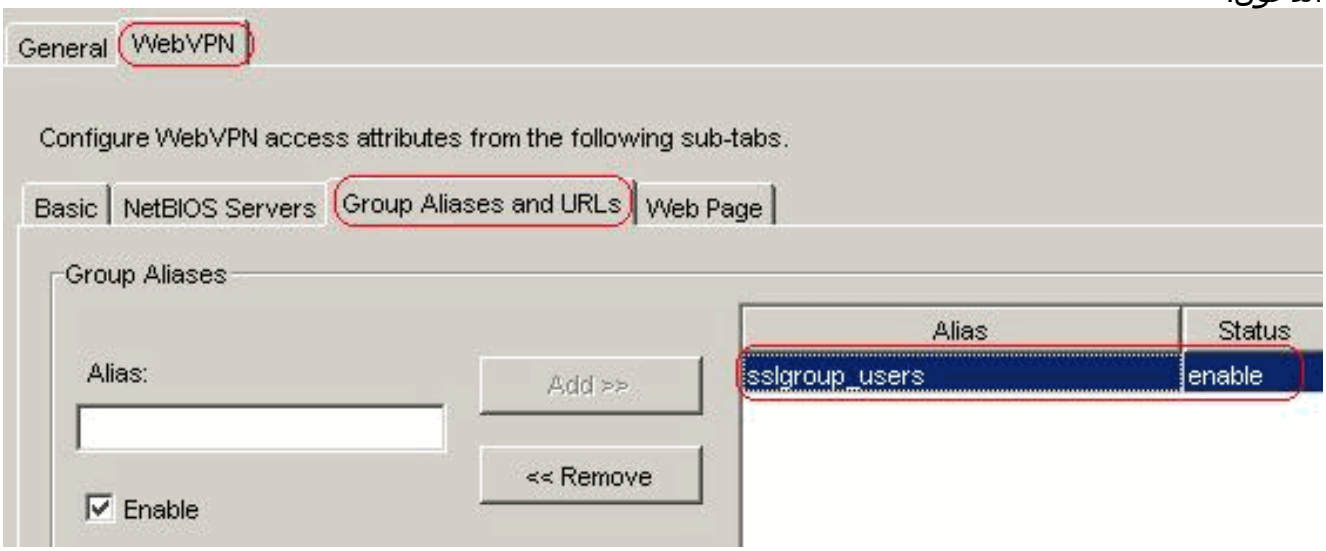
7. **تكوين مجموعة النفق**أخترت **تشكيل>VPN>عام>نفق مجموعة>يضيف (WebVPN منفذ)** in order to خلقت جديد نفق مجموعة **sslgroup**.في علامة التبويب **عام > أساسي**، أختر "نهج المجموعة" **كمجموعة عملاء** من القائمة المنسدلة.



في **عام > علامة التبويب تعيين عنوان العميل**، ضمن تجمعات العناوين، انقر فوق **إضافة >>** لتعيين تجمع العناوين المتوفر **vpnPool**.

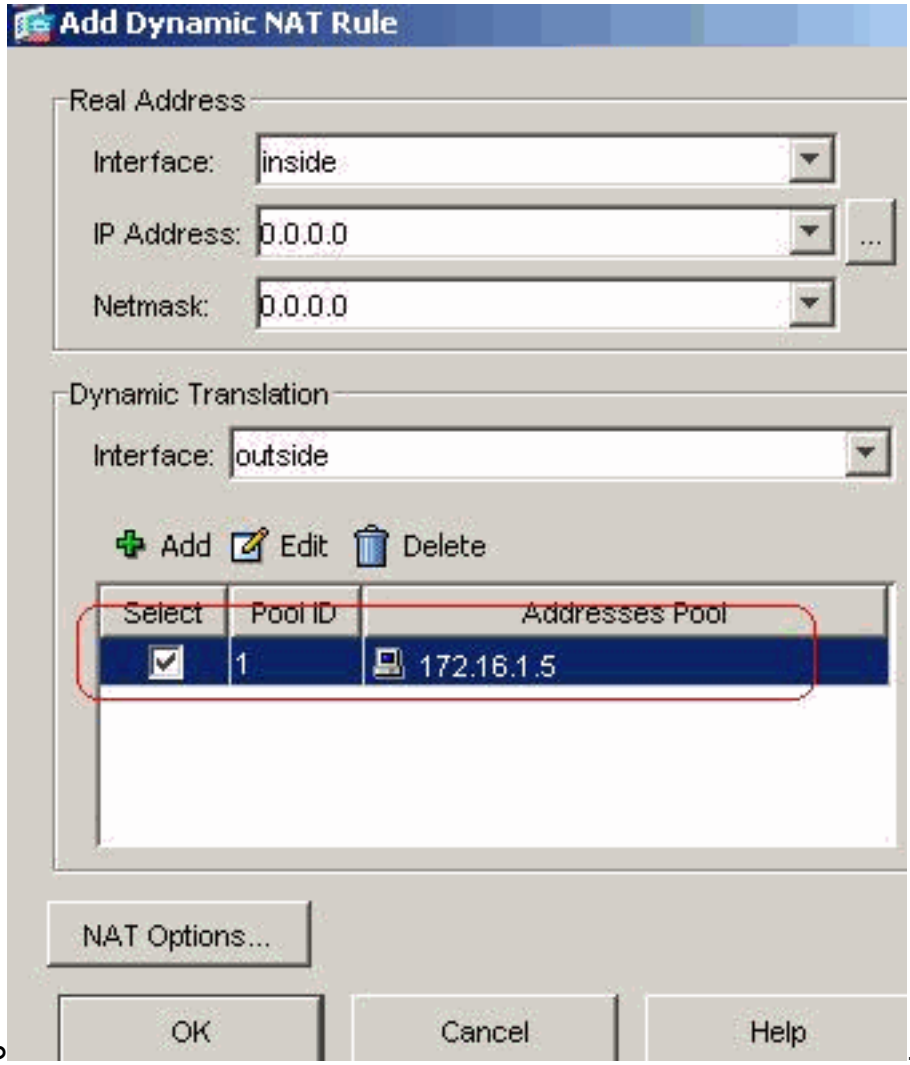


في علامة التبويب **WebVPN > أسماء المجموعات المستعارة وعناوين URL**، اكتب اسم الاسم المستعار في مربع المعلمة وانقر **إضافة >>**لجعله يظهر في قائمة أسماء المجموعات في صفحة تسجيل الدخول.



طقطقت **ok** وبعد ذلك **يطبق**.**CLI تشكيل مكافئ:**

8. **تكوين NAT**أخترت **تشكيل>nat>إضافة>إضافة>قاعدة nat حركي** لحركة المرور أن يأتي من الشبكة الداخلية أن يستطيع كنت ترجمت مع خارج عنوان



طقطقة **ok** وطقطقة 172.16.1.5.

يطبق في الصفحة الرئيسية.**CLI تشكيل مكافئ:**

9. قم بتكوين إعفاء nat لحركة مرور البيانات العائدة من الشبكة الداخلية إلى عميل VPN.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

التكوين (ASA 7.2(2 باستخدام CLI

(Cisco ASA 7.2(2
ciscoasa#**show running-config** Saved : : (ASA Version 7.2(2 ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/1 nameif outside security-level 0

```
                    ip address 172.16.1.1 255.255.255.0
                                                       !
                                        interface Ethernet0/2
                                                  shutdown
                                                 no nameif
                                          no security-level
                                              no ip address
                                                       !
                                        interface Ethernet0/3
                                                  shutdown
                                                 no nameif
                                          no security-level
                                              no ip address
                                                       !
                                     interface Management0/0
                                                  shutdown
                                                 no nameif
                                          no security-level
                                              no ip address
                                                       !
                               passwd 2KFQnbNIdI.2KYOU encrypted
                                                ftp mode passive

  access-list split-tunnel standard permit 10.77.241.128
                                                255.255.255.192
   ACL for Split Tunnel network list for encryption. ---!
     access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
     - ACL to define the traffic to be exempted from NAT.
pager lines 24 mtu inside 1500 mtu outside 1500 ip local
                      pool vpnpool 192.168.10.1-192.168.10.254

         The address pool for the SSL VPN Clients no ---!
failover icmp unreachable rate-limit 1 burst-size 1 asdm
     image disk0:/asdm-522.bin no asdm history enable arp
                timeout 14400 global (outside) 1 172.16.1.5

 The global address for Internet access used by VPN ---!
       Clients. !--- Note: Uses an RFC 1918 range for lab
     setup. !--- Apply an address from your public range
  provided by your ISP. nat (inside) 0 access-list nonat
    The traffic permitted in "nonat" ACL is exempted ---!
                 from NAT. nat (inside) 1 0.0.0.0 0.0.0.0


                    access-group 100 in interface outside
                route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                       :sip-disconnect 0:02
                                timeout uauth 0:05:00 absolute
                      group-policy clientgroup internal

     Create an internal group policy "clientgroup". ---!
                      group-policy clientgroup attributes
                              vpn-tunnel-protocol webvpn

 Enable webvpn as tunneling protocol. split-tunnel- ---!
                                    policy tunnelspecified
             split-tunnel-network-list value split-tunnel
```

```
Encrypt the traffic specified in the split tunnel ---!
                                        ACL only. webvpn
                                          svc required

    Activate the SVC under webvpn mode. svc keep- ---!
                                      installer installed

When the security appliance and the SVC perform a ---!
      rekey, !--- they renegotiate the crypto keys and
initialization vectors, !--- and increase the security
                        of the connection. svc rekey time 30

Command that specifies the number of minutes !--- ---!
   from the start of the session until the rekey takes
place, !--- from 1 to 10080 (1 week).  svc rekey method
                                                    ssl

Command that specifies that SSL renegotiation !--- ---!
takes place during SVC rekey. username ssluser1 password
                                    ZRhW85jZqEaVd5P. encrypted

    Create an user account "ssluser1". aaa local ---!
                          authentication attempts max-fail 16

  Enable the AAA local authentication. 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 tunnel-
                                  group sslgroup type webvpn

    Create a tunnel group "sslgroup" with type as ---!
      WebVPN. tunnel-group sslgroup general-attributes
                                        address-pool vpnpool

      Associate the address pool vpnpool created. ---!
                                default-group-policy clientgroup

  Associate the group policy "clientgroup" created. ---!
                          tunnel-group sslgroup webvpn-attributes

                                 group-alias sslgroup_users enable

Configure the group alias as sslgroup-users. telnet ---!
   timeout 5 ssh timeout 5 console timeout 0 ! 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
                                                    webvpn
                                          enable outside

  Enable WebVPN on the outside interface. svc image ---!
                          disk0:/sslclient-win-1.1.4.179.pkg 1

    Assign an order to the SVC image. svc enable ---!

 Enable the security appliance to download !--- SVC ---!
   images to remote computers. tunnel-group-list enable
```

```
Enable the display of the tunnel-group list !--- on ---!
                the WebVPN Login page. prompt hostname context
   Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
                                                  #ciscoasa
```

إنشاء اتصال SSL VPN باستخدام SVC

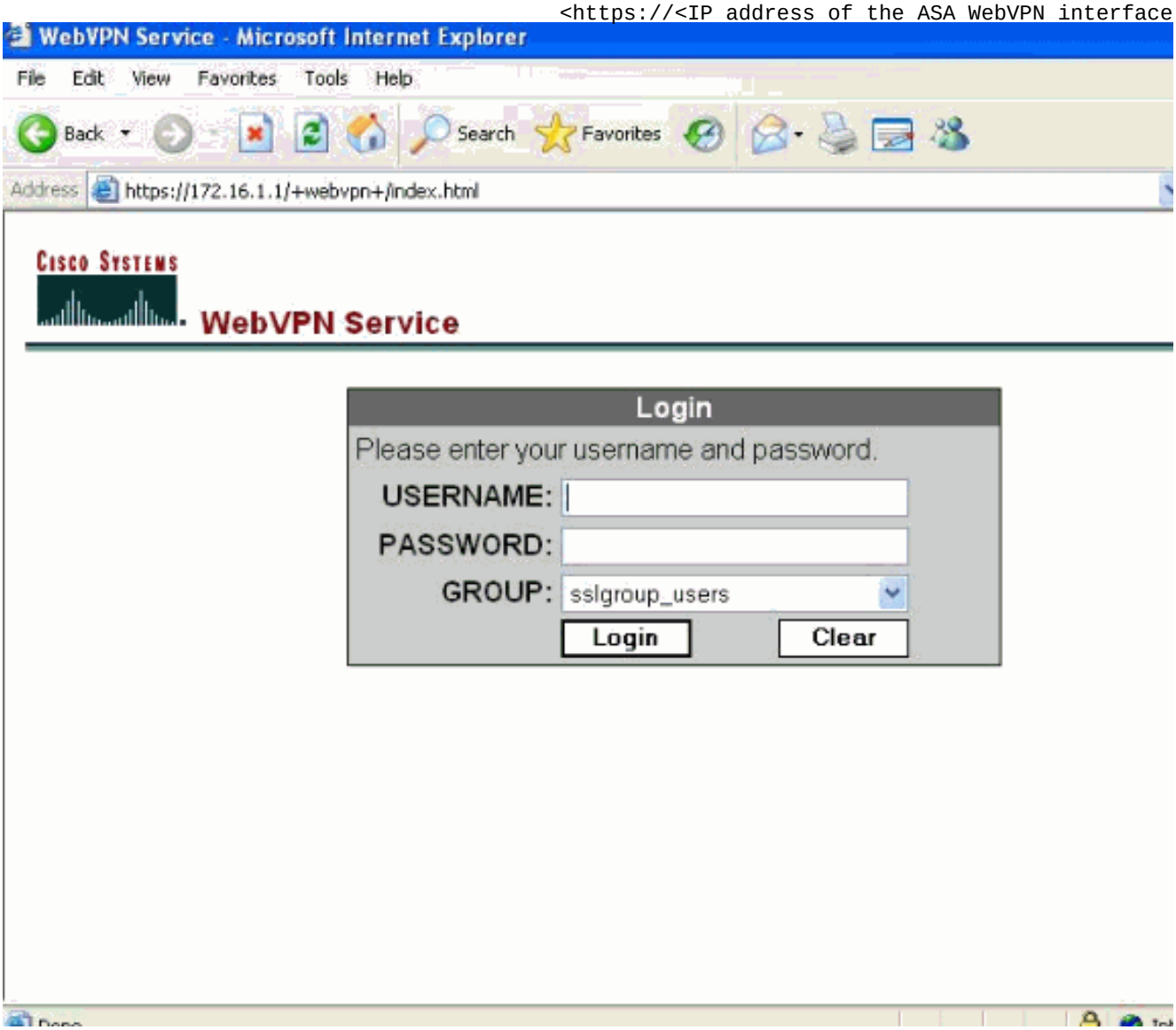
أكمل هذه الخطوات لإنشاء اتصال SSL VPN مع ASA.

1. اكتب عنوان URL أو عنوان IP الخاص بواجهة WebVPN ل ASA في مستعرض الويب بالتنسيق كما هو موضح.

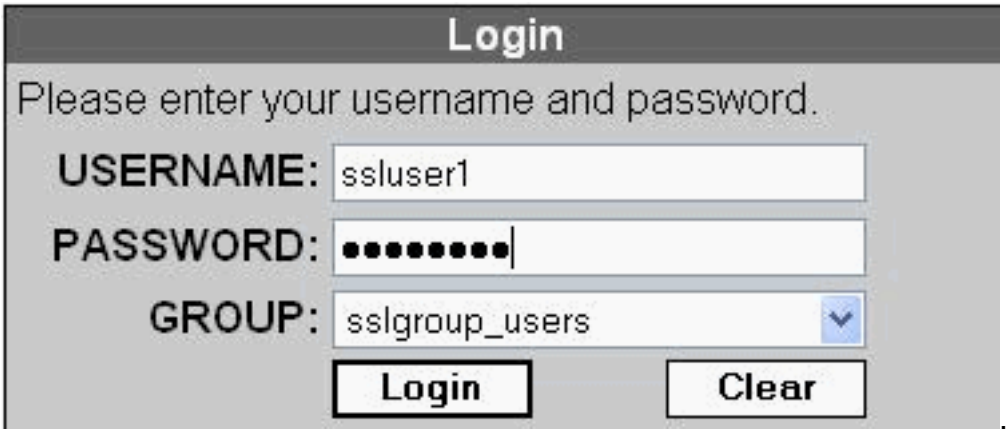
```
https://url
```

أو

```
<https://<IP address of the ASA WebVPN interface
```



2. أدخل اسم المستخدم وكلمة المرور ثم أختر المجموعة المقابلة لك من القائمة المنسدلة كما هو



موضح.

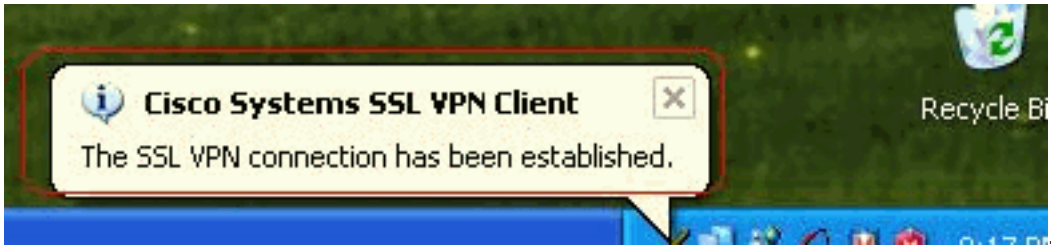
3. يجب تثبيت برنامج ActiveX في الكمبيوتر قبل تنزيل

.SVC

4. تظهر هذه الإطارات قبل إنشاء اتصال SSL

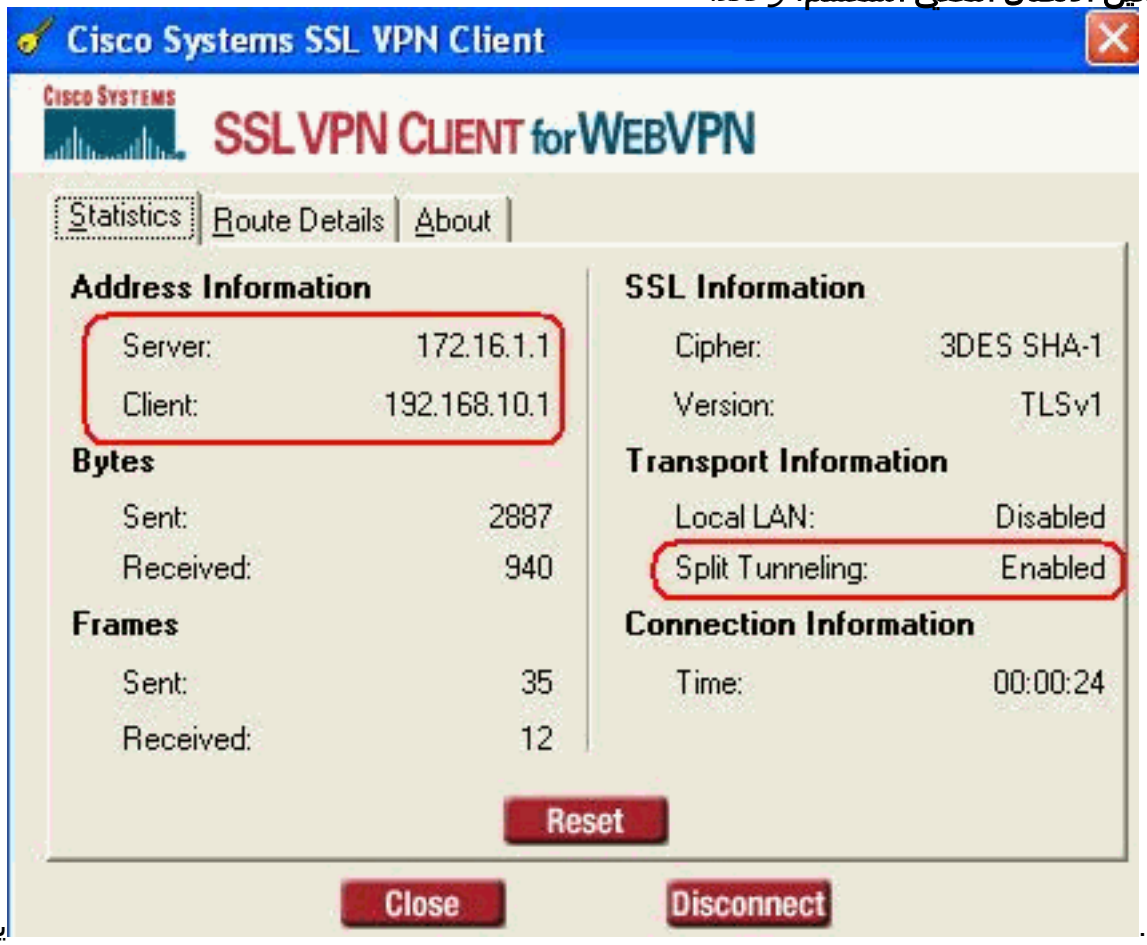
.VPN

5. يمكنك الحصول على هذه النوافذ بمجرد تأسيس

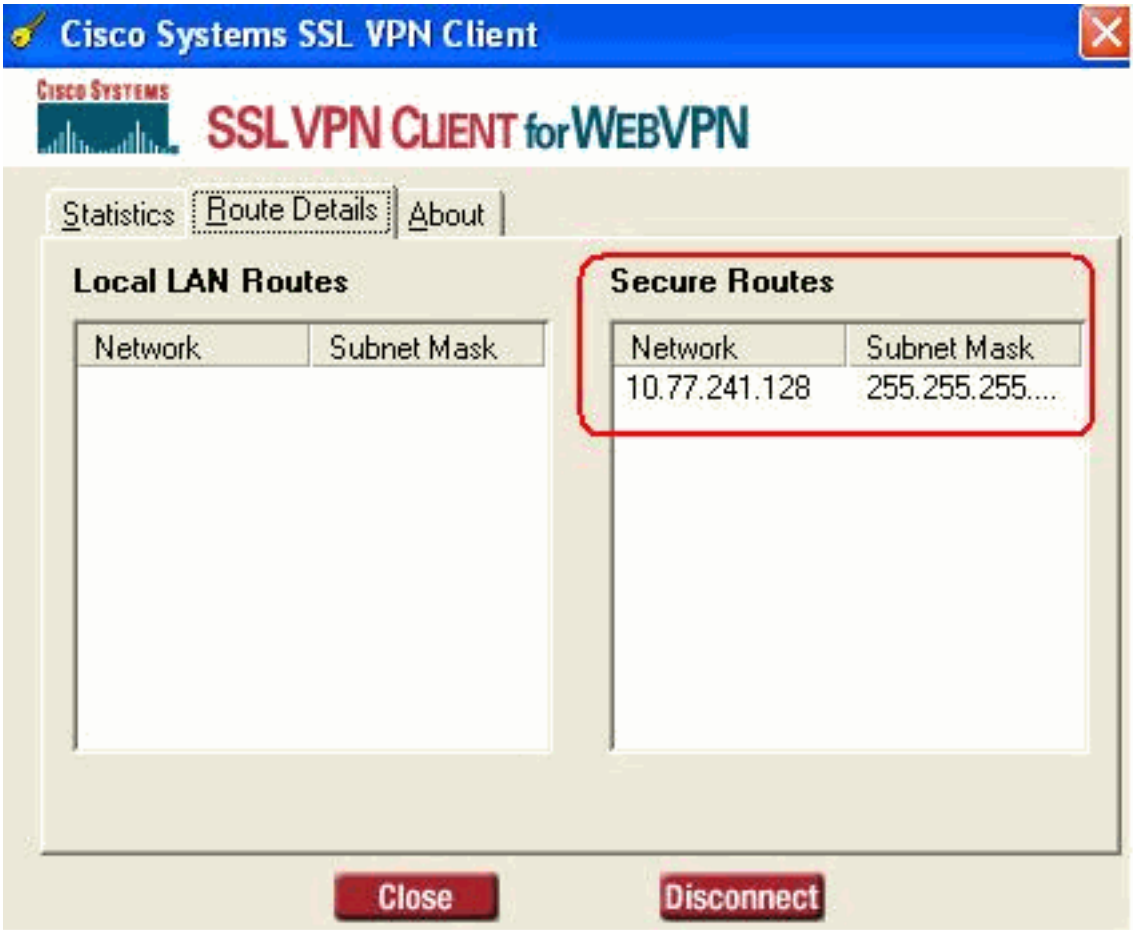


الاتصال.

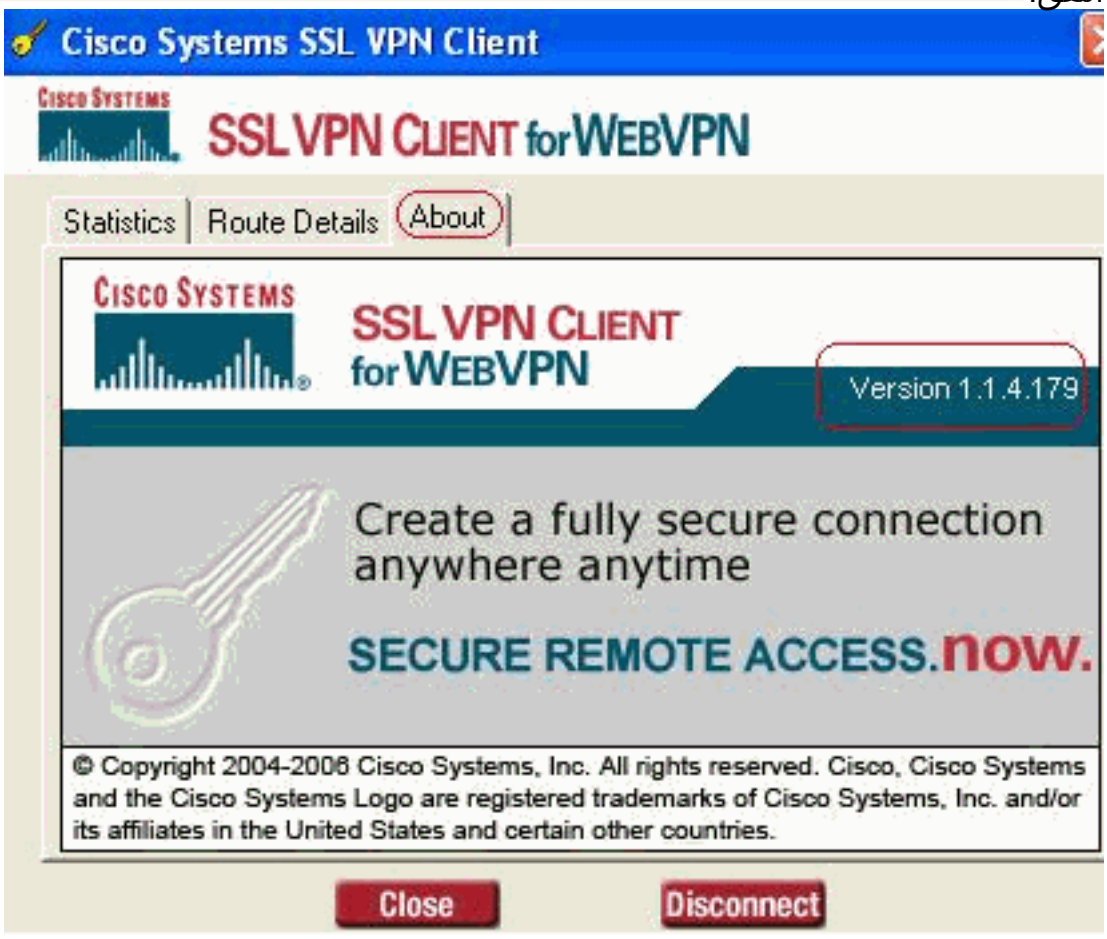
6. انقر فوق المفتاح الأصفر الذي يظهر في شريط مهام الكمبيوتر. تظهر هذه الإطارات التي تعطي معلومات حول اتصال SSL. على سبيل المثال، **192.168.10.1** هو عنوان IP المعين للعميل والخادم IP لعنوان 172.16.1.1، **يتم تمكين الاتصال النفقي المنقسم**، وهكذا



دواليك. يمكنك أيضا التحقق من الشبكة الآمنة التي سيتم تشفيرها بواسطة SSL، ويتم تنزيل قائمة الشبكة من قائمة الوصول عبر النفق المنقسم التي تم تكوينها في ASA.في هذا المثال، يؤمن عميل SSL VPN الوصول إلى 24/10.77.241.128 بينما لا يتم تشفير جميع حركة مرور البيانات الأخرى ولا يتم إرسالها عبر



النفق.



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** .

- **show webVPN svc**— يعرض صور SVC المخزنة في ذاكرة ASA المؤقتة.

```
ciscoasa#show webvpn svc
disk0:/sslclient-win-1.1.4.179.pkg 1 .1
CISCO STC win2k+ 1.0.0
1,1,4,179
Fri 01/18/2008 15:19:49.43

SSL VPN Client(s) installed 1
```

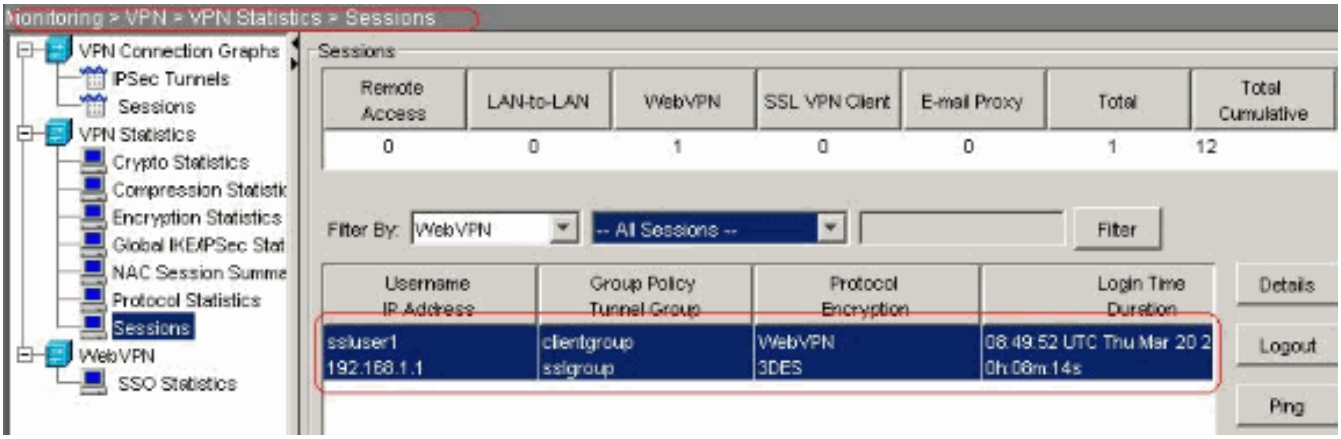
- **show vpn-sessiondb svc**— يعرض المعلومات حول إتصالات SSL الحالية.

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1          Public IP    : 192.168.1.1
Protocol     : SVC                   Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                Bytes Rx     : 5082
(Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
:  Filter Name
```

- **show webVPN group-alias**—يعرض الاسم المستعار الذي تم تكوينه لمجموعات مختلفة.

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- في ASDM، أخترت **monitore>VPN>VPN إحصائيات>VPN>جلسة** in order to علمت حول الحالي WebVPN جلسة في ال ASA.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. **<VPN-sessionDB logoff name <username>**— أمر أن يدون ال SSL VPN جلسة ل ال username خاص.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
!Called vpn_remove_uauIth: success
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

بالمثل، يمكنك إستخدام الأمر **vpn-sessiondb logoff svc** لإنهاء جميع جلسات عمل SVC.

2. **ملاحظة:** إذا انتقل الكمبيوتر إلى وضع الاستعداد أو الإسبات، يمكن إنهاء اتصال SSL VPN.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
(SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc
!Called vpn_remove_uauth: success
webvpn_svc_np_tear_down: no ACL
```

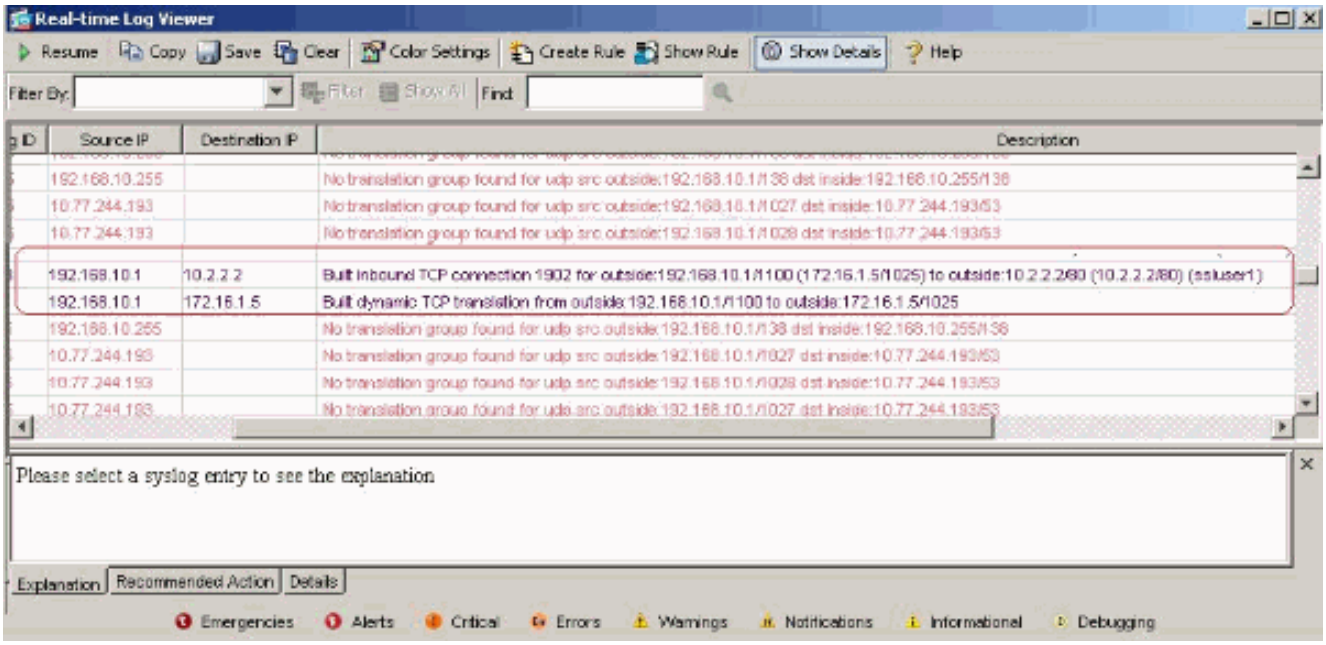
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

3. **debug webVPN svc <1-255>**يوفر أحداث WebVPN في الوقت الفعلي لإنشاء الجلسة.

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
()http_parse_cstp_method
'input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1...
()webvpn_cstp_parse_request_field
'input: 'Host: 172.16.1.1...
'Processing CSTP header line: 'Host: 172.16.1.1
()webvpn_cstp_parse_request_field
'input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179...
,Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4
'179
'Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179
()webvpn_cstp_parse_request_field
'input: 'X-CSTP-Version: 1...
'Processing CSTP header line: 'X-CSTP-Version: 1
'Setting version to '1
()webvpn_cstp_parse_request_field
'input: 'X-CSTP-Hostname: tacweb...
'Processing CSTP header line: 'X-CSTP-Hostname: tacweb
'Setting hostname to: 'tacweb
()webvpn_cstp_parse_request_field
'input: 'X-CSTP-Accept-Encoding: deflate;q=1.0...
'Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0
()webvpn_cstp_parse_request_field
input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486...
'D5BC554D2
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
'CF236DB5E8BE70B1486D5BC554D2
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
'486D5BC554D2
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
'C554D2
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
```

```
SVC ACL ID: -1
!vpn_put_uauth success
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

4. في ASDM، أختر **مراقبة > تسجيل > عارض السجل في الوقت الفعلي > عرض** لعرض الأحداث في الوقت الفعلي. يوضح هذا المثال معلومات جلسة العمل بين SVC 192.168.10.1 و WebServer 10.2.2.2 في الإنترنت من خلال ASA 172.16.1.5.



معلومات ذات صلة

- دعم منتجات أجهزة الأمان القابلة للتكيف طراز Cisco من Series 5500
- ASA/PIX: السماح بنفقي انقسام لعملاء VPN على مثال تكوين ASA
- يسمح الموجه لعملاء VPN بتوصيل IPsec والإنترنت باستخدام مثال تكوين انقسام الاتصال النفقي
- عميل PIX/ASA 7.x و VPN لشبكة VPN العامة عبر الإنترنت على مثال تكوين العصا
- (SSL VPN Client (SVC على ASA مع مثال تكوين ASDM
- 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).