ASA 7.2(2): SSL VPN Client (SVC) لعامة الإنترنت VPN على مثال تكوين العصا

المحتويات

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

المقدمة

يوضح هذا المستند كيفية إعداد جهاز أمان قابل للتكيف (ASA) 7.2.2 لإجراء SSL VPN على جهاز تثبيت. ينطبق هذا الإعداد على حالة محددة لا يسمح فيها ASA بنفق التقسيم ويتصل المستخدمون مباشرة ب ASA قبل السماح لهم بالانتقال إلى الإنترنت.

ملاحظة: في الإصدار 7.2.2 من ASA، تسمح الكلمة الأساسية *intra-interface* لأمر وضع التكوين **نفسه--security traffic** بأن تدخل جميع حركة المرور الواجهة نفسها وتخرج منها (ليس فقط حركة مرور IPsec).

المتطلبات الأساسية

المتطلبات

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

- يحتاج جهاز أمان Hub ASA إلى تشغيل الإصدار 7.2.2
- Cisco SSL VPN Client (SVC) 1.x **ملاحظة:** قم بتنزيل حزمة عميل SSL VPN (sslclient-win*.pkg) من تنزيل برامج Cisco (للعملاء المسجلين فقط). انسخ SVC إلى ذاكرة Flash (الذاكرة المؤقتة) على ASA. يجب تنزيل SVC إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع تثبيت قسم برنامج SVC من *دليل تكوين سطر أوامر Cisco Security Appliance، الإصدار 7.2* للحصول على مزيد من المعلومات.

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
- كمبيوتر يعمل بنظام التشغيل Windows 2000 Professional أو Windows XP
- 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 المُستخدمة 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 البعيدين فوائد IPSec VPN Client دون الحاجة إلى مسؤولي الشبكة لتثبيت 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.

لإنشاء 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 استوفى المستخدم تسجيل الدخول والمصادقة، وقام جهاز الأمان بتعريف المستخدم على أنه يتطلب SVC، يقوم جهاز الأمان بتنزيل SVC إلى الكمبيوتر البعيد. إذا كان جهاز الأمان يحدد أن المستخدم لديه خيار إستخدام SVC، فإن جهاز الأمان يقوم بتنزيل SVC إلى الكمبيوتر البعيد أثناء عرض إرتباط على شاشة المستخدم لتخطي تثبيت SVC.

بعد التنزيل، يقوم SVC بتثبيت نفسه وتكوينه، ومن ثم يبقى SVC أو يقوم بإلغاء تثبيت نفسه (حسب التكوين) من الكمبيوتر البعيد عند إنهاء الاتصال.

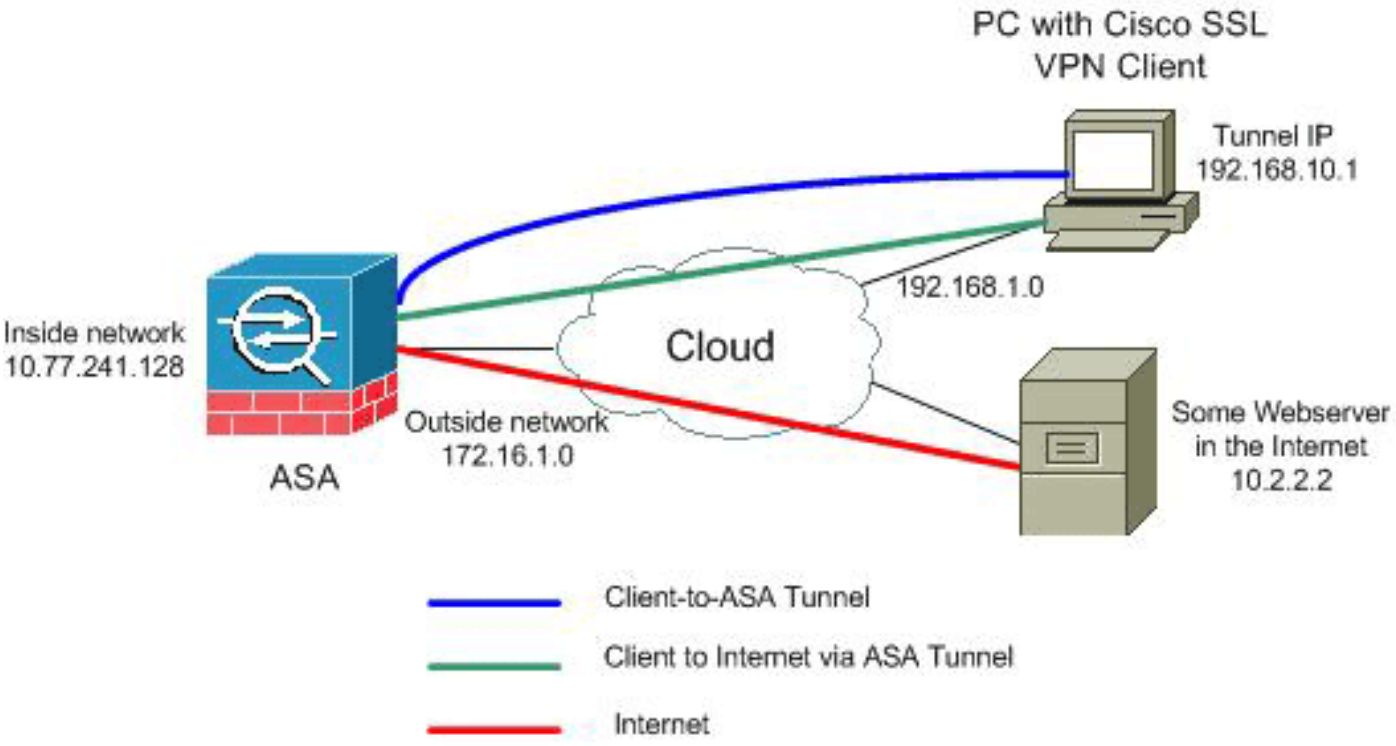
التكوين

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. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

تكوينات ASA 7.2(2) باستخدام ASDM 5.2(2)

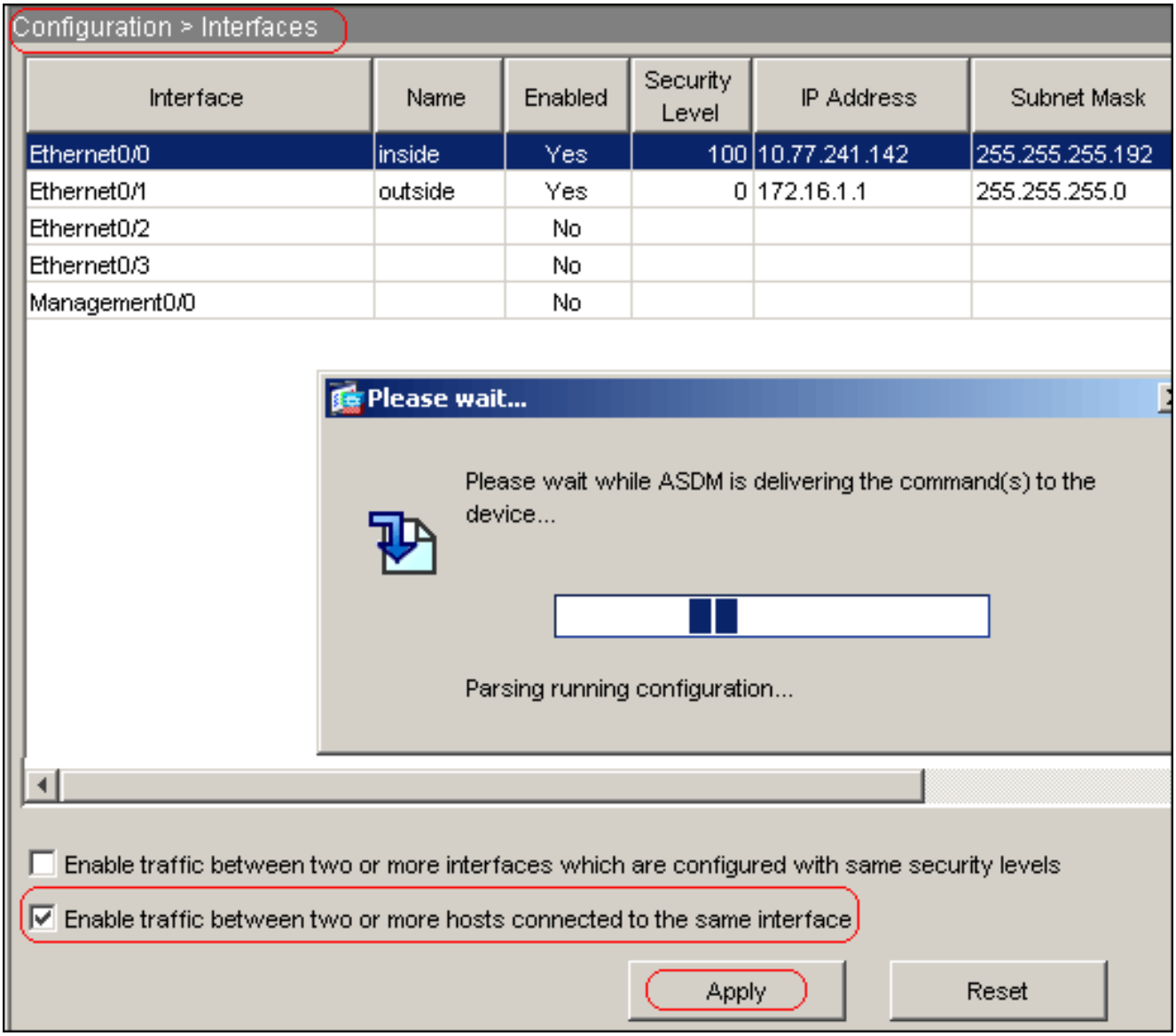
يفترض هذا المستند أن التكوينات الأساسية، مثل تكوين الواجهة، قد تم إنشاؤها بالفعل وتعمل بشكل صحيح.

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.

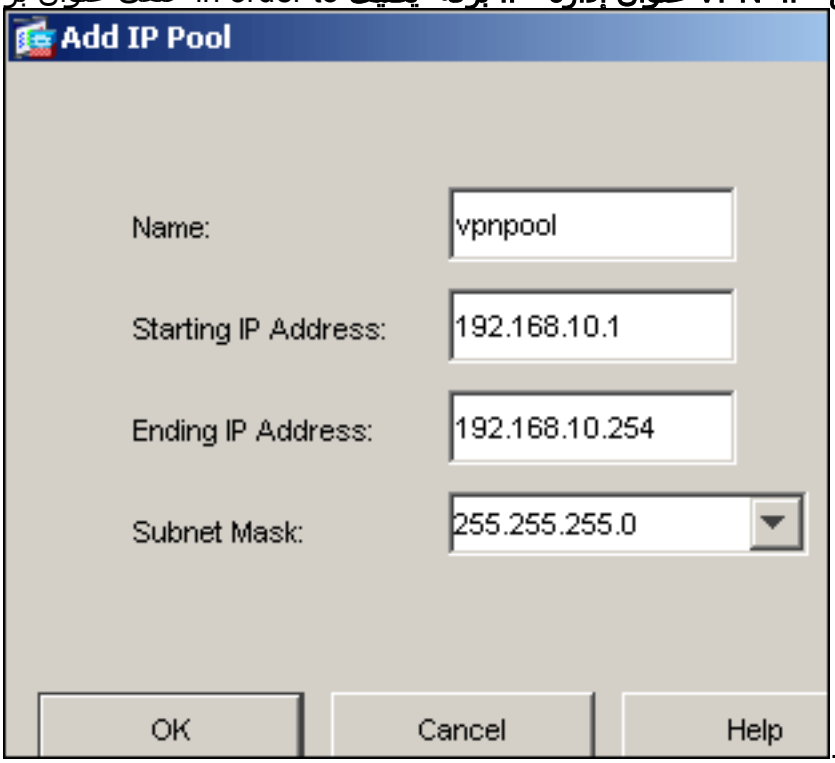
أتمت هذا steps in order to شكلت ال SSL VPN على a stick في ASA:

1. أخترت **تشكيل>قارن**، وفحصت ال **يمكن حركة مرور بين إثنان أو أكثر مضيف يربط إلى ال نفسه قارن** تدقيق in order to سمحت SSL VPN حركة مرور أن يدخل ويخرج ال نفسه قارن.
2. طقطقة **يطبق**.



ملاحظة: فيما يلي أمر تكوين CLI المكافئ:

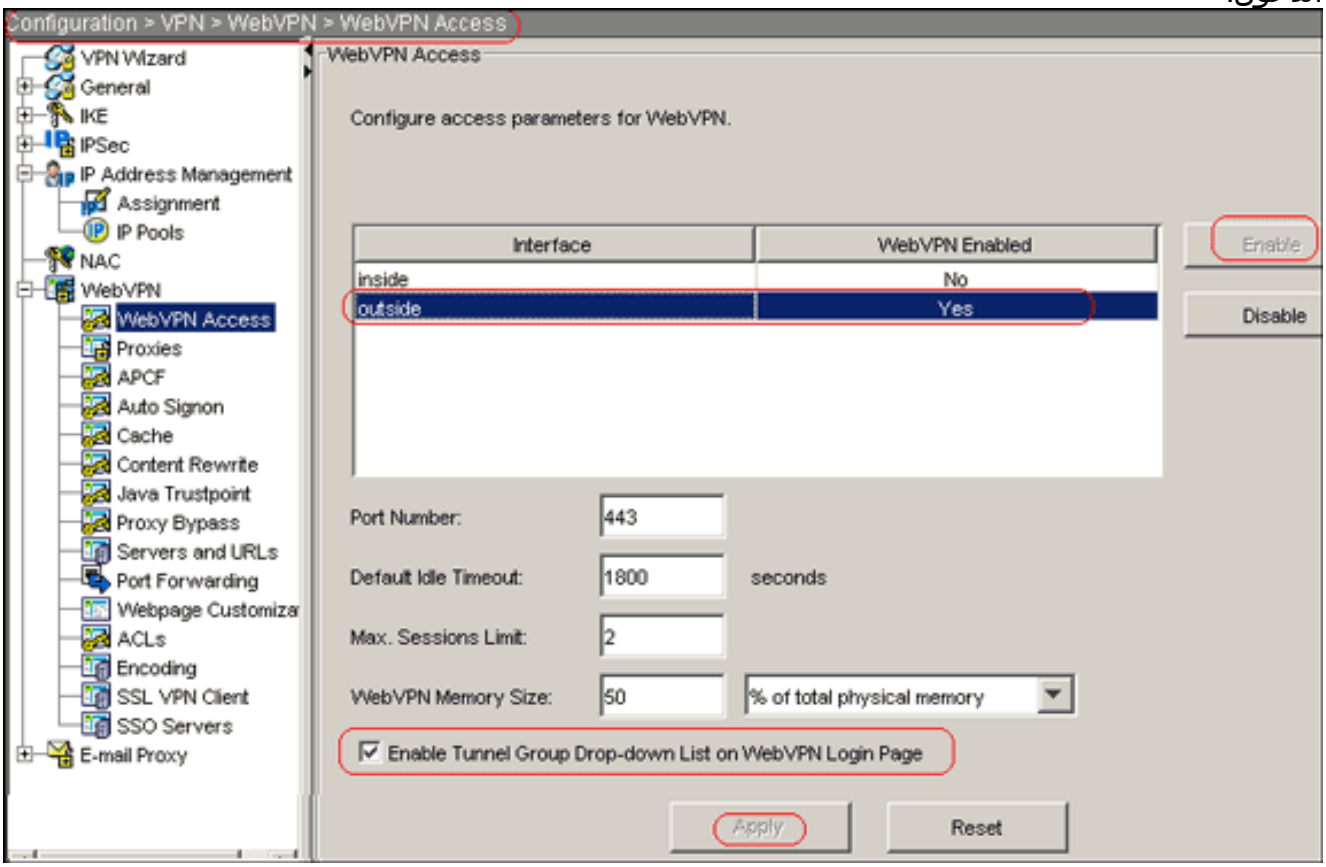
3. أخترت **تشكيل>IP>VPN عنوان إدارة>IP بركة>يضيف** in order to خلقت عنوان بركة يعين



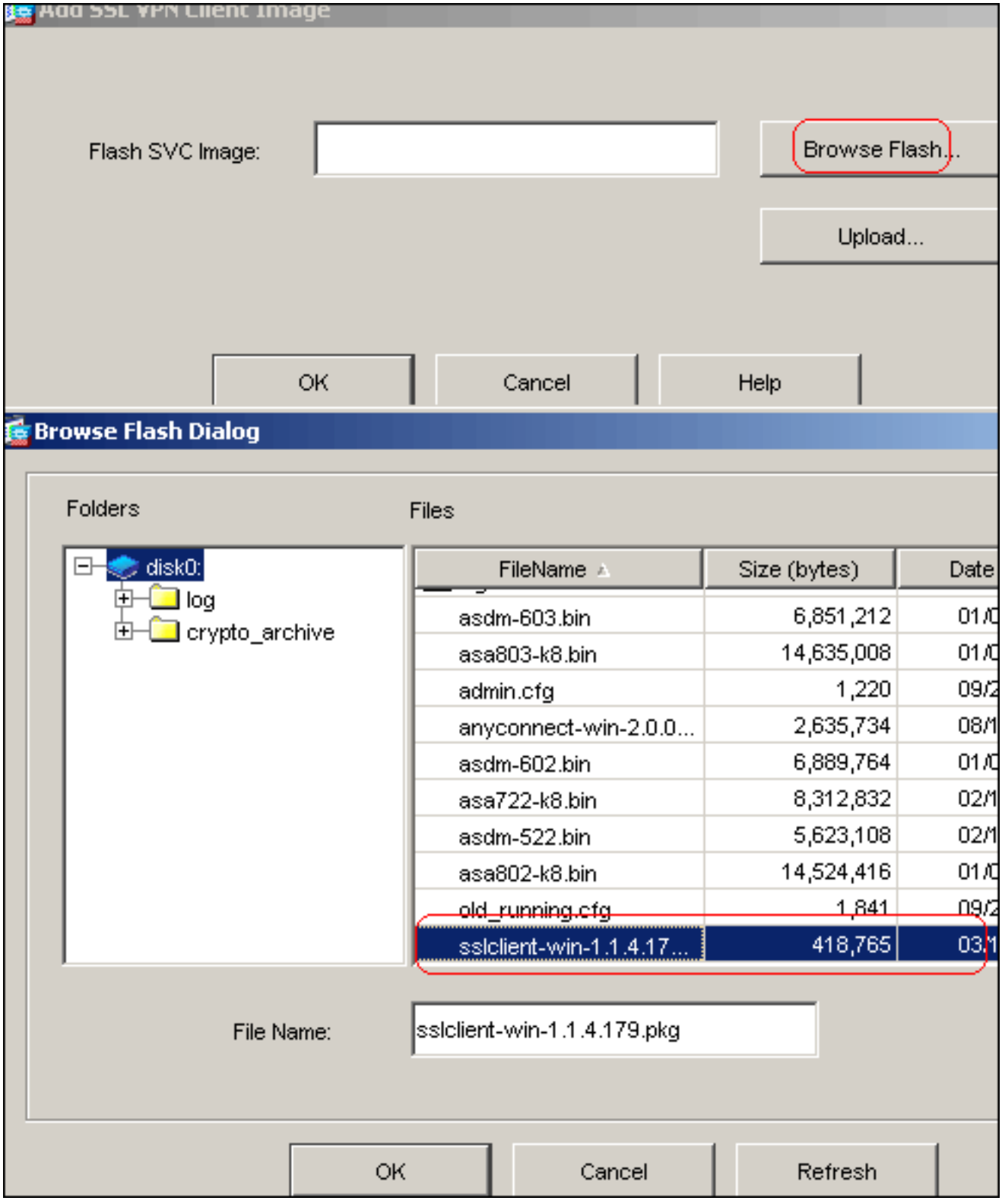
VPNPOOL.

4. طقطقة **يطبق.ملاحظة:** فيما يلي أمر تكوين CLI المكافئ:

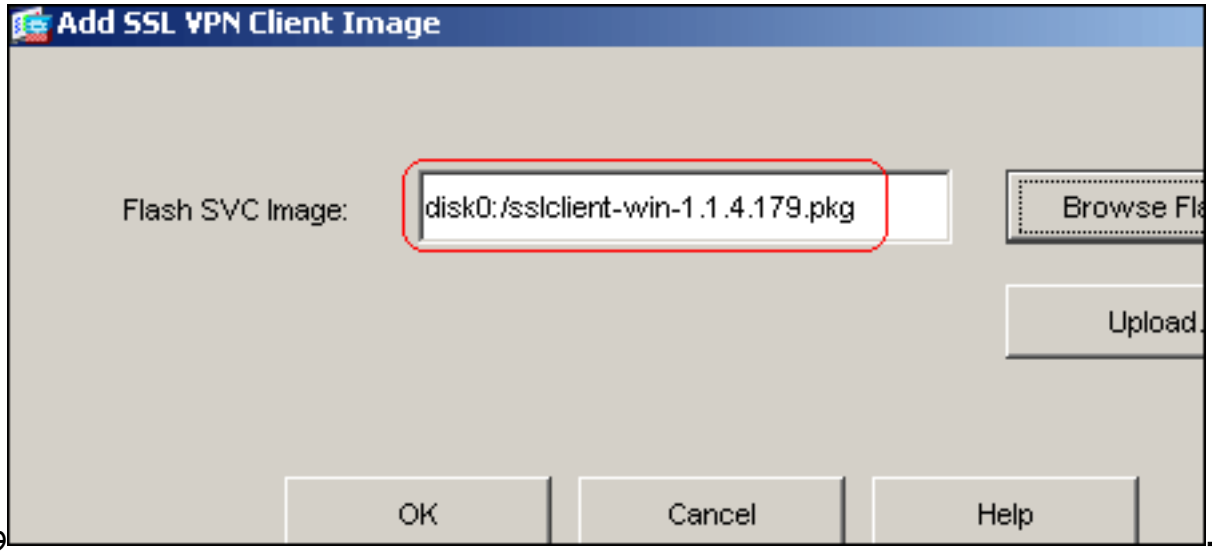
5. تمكين WebVPN:أخترت **تشكيل>WebVPN>WebVPN>VPN منفذ**، وعينت القارن خارجي.طقطقة **يمكن**.حدد خانة الاختيار **تمكين القائمة المنسدلة لمجموعة النفق على صفحة تسجيل الدخول إلى WebVPN** للسماح للمستخدمين باختيار مجموعاتهم الخاصة من صفحة تسجيل الدخول.



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

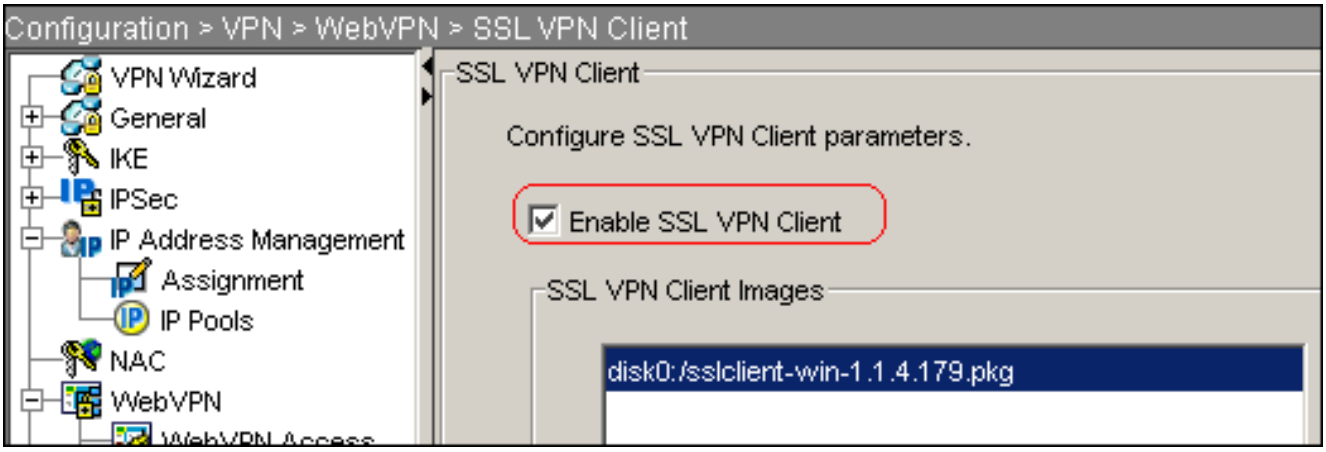

Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin 6,851,212
asa803-k8.bin 14,635,008
admin.cfg 1,220
anyconnect-win-2.0.0... 2,635,734
asdm-602.bin 6,889,764
asa722-k8.bin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

وانقر فوق



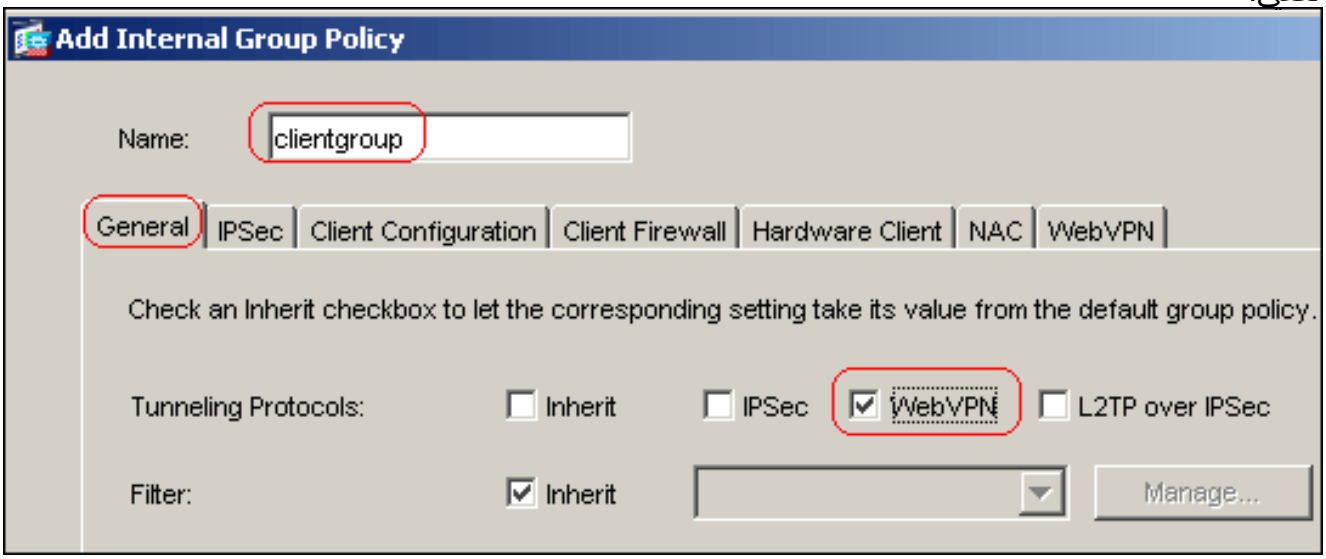
وانقر **OK**.

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

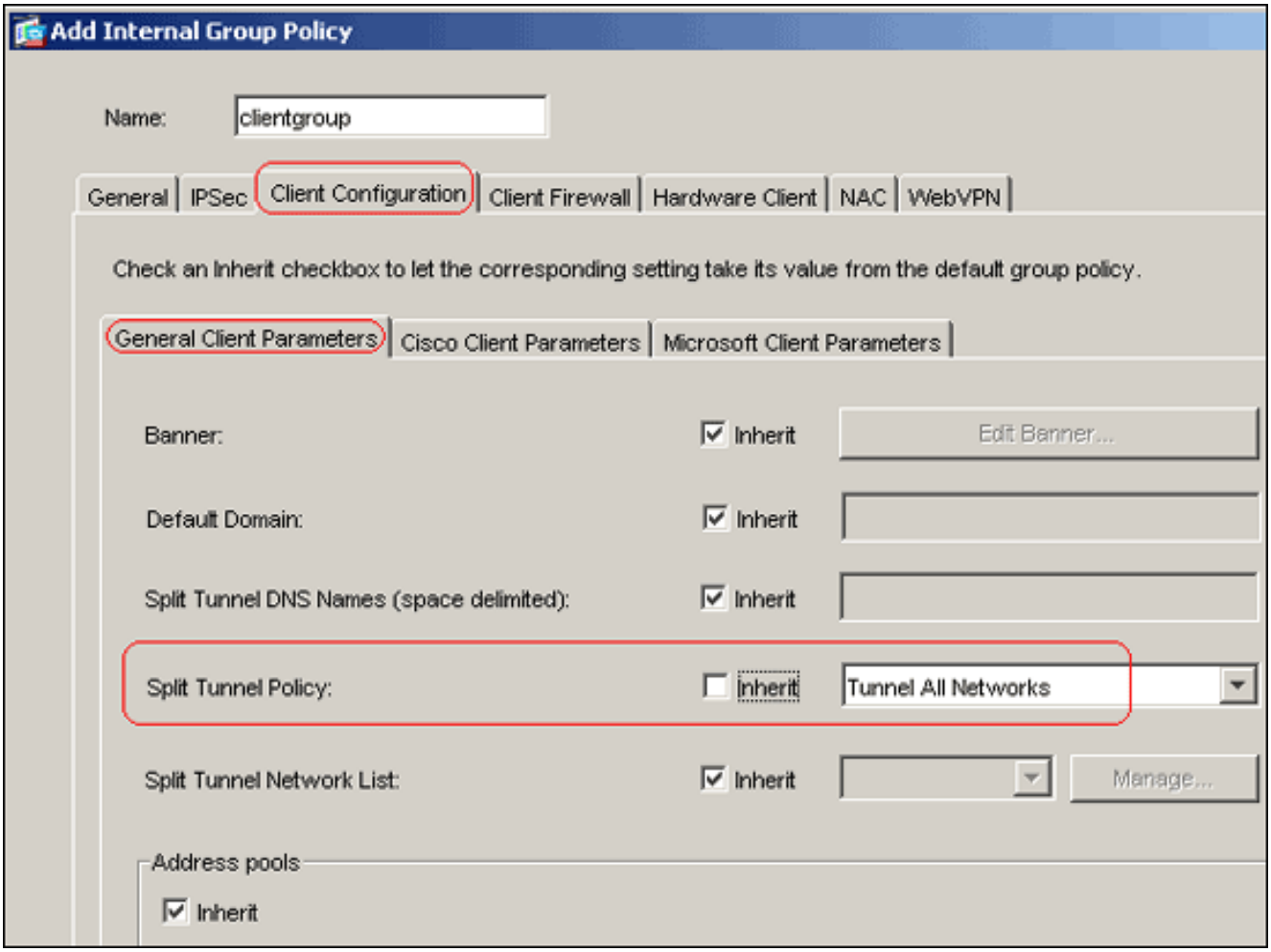


ملاحظة: فيما يلي أوامر تكوين CLI المكافئة:

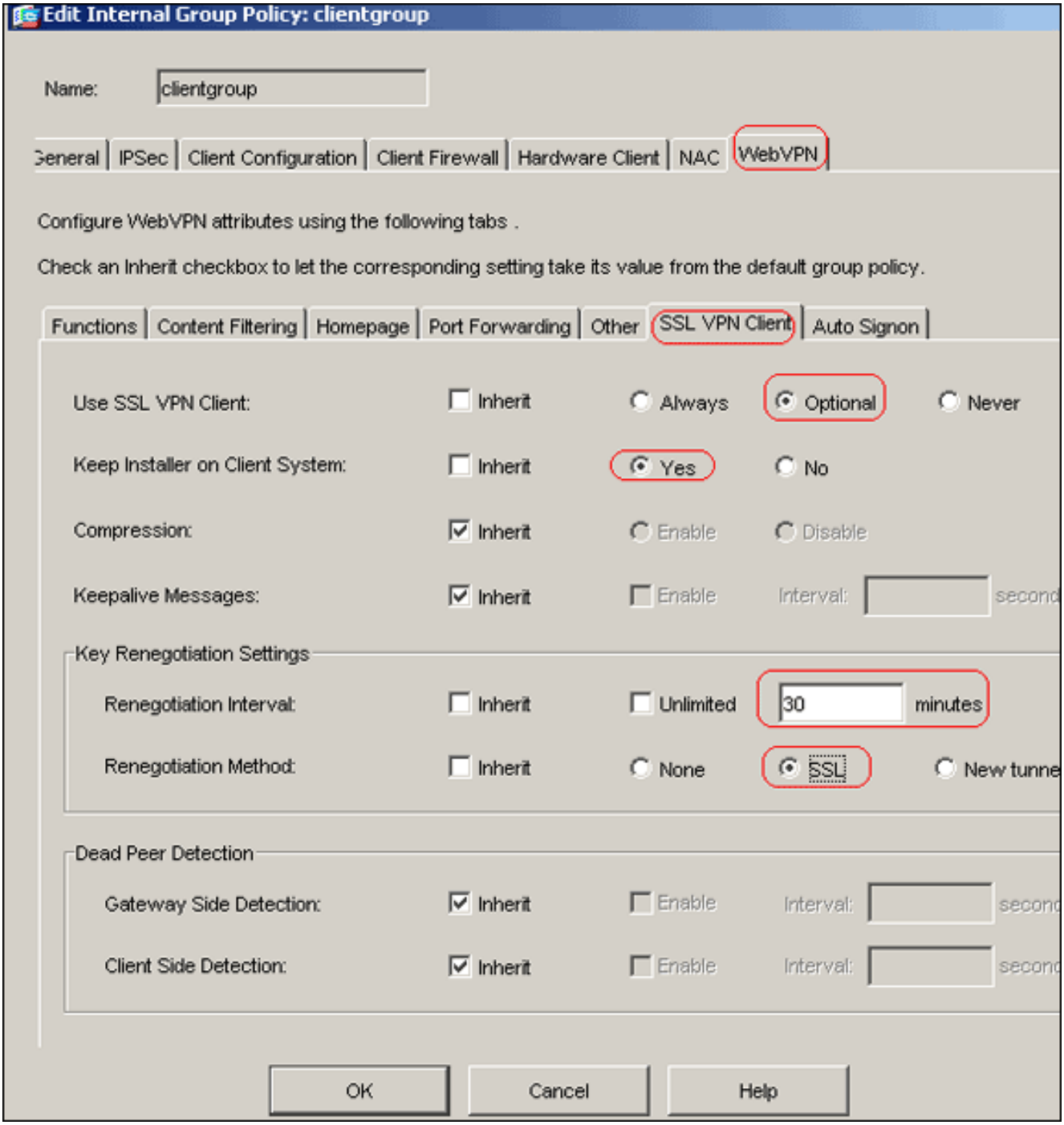
6. تكوين نهج المجموعة:أخترت **تشكيل>VPN>عام>مجموعة سياسة>إضافة (داخلي مجموعة سياسة)** in order to خلقت داخلي مجموعة سياسة يعين *زبونGroup*.انقر فوق علامة التبويب **عام**، وحدد خانة الاختيار **WebVPN** لتمكين WebVPN كبروتوكول اتصال نفقي.



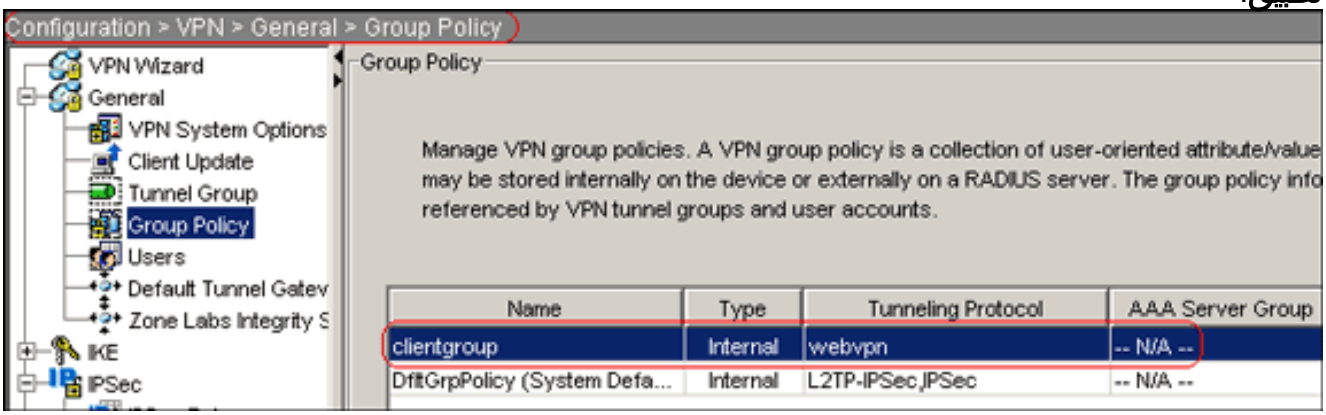
انقر فوق علامة التبويب **تكوين العميل**، ثم انقر فوق علامة التبويب **معلمات العميل العامة**.أختر **Tunnel all Networks** من القائمة المنسدلة لسياسة النفق المقسم لجعل جميع الحزم تنتقل من الكمبيوتر الشخصي البعيد من خلال نفق آمن.



انقر فوق علامة التبويب **WebVPN > SSLVPN Client**، واختر الخيارات التالية:لخيار إستخدام SSL VPN Client، قم بإلغاء تحديد خانة الاختيار **Inherit (توريث)**، وانقر فوق زر الاختيار **الاختياري**.يسمح هذا الخيار للعميل البعيد باختيار ما إذا كان سيتم تنزيل SVC أم لا. 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** للانتقاءيتيح هذا الخيار لبرنامج SVC البقاء على جهاز العميل. لذلك، لا يتطلب 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.**ملاحظة:** يتم تحسين الأمان من خلال تعيين حدود لطول المدة التي يكون فيها المفتاح صالحا.لخيار طريقة إعادة التفاوض، قم بإلغاء تحديد خانة الاختيار **Inherit**، وانقر فوق زر انتقاء **SSL**.**ملاحظة:** يمكن لإعادة التفاوض إستخدام نفق SSL الحالي أو نفق جديد تم إنشاؤه تحديدا لإعادة التفاوض.يجب تكوين سمات عميل SSL VPN الخاصة بك كما هو موضح في هذه الصورة:



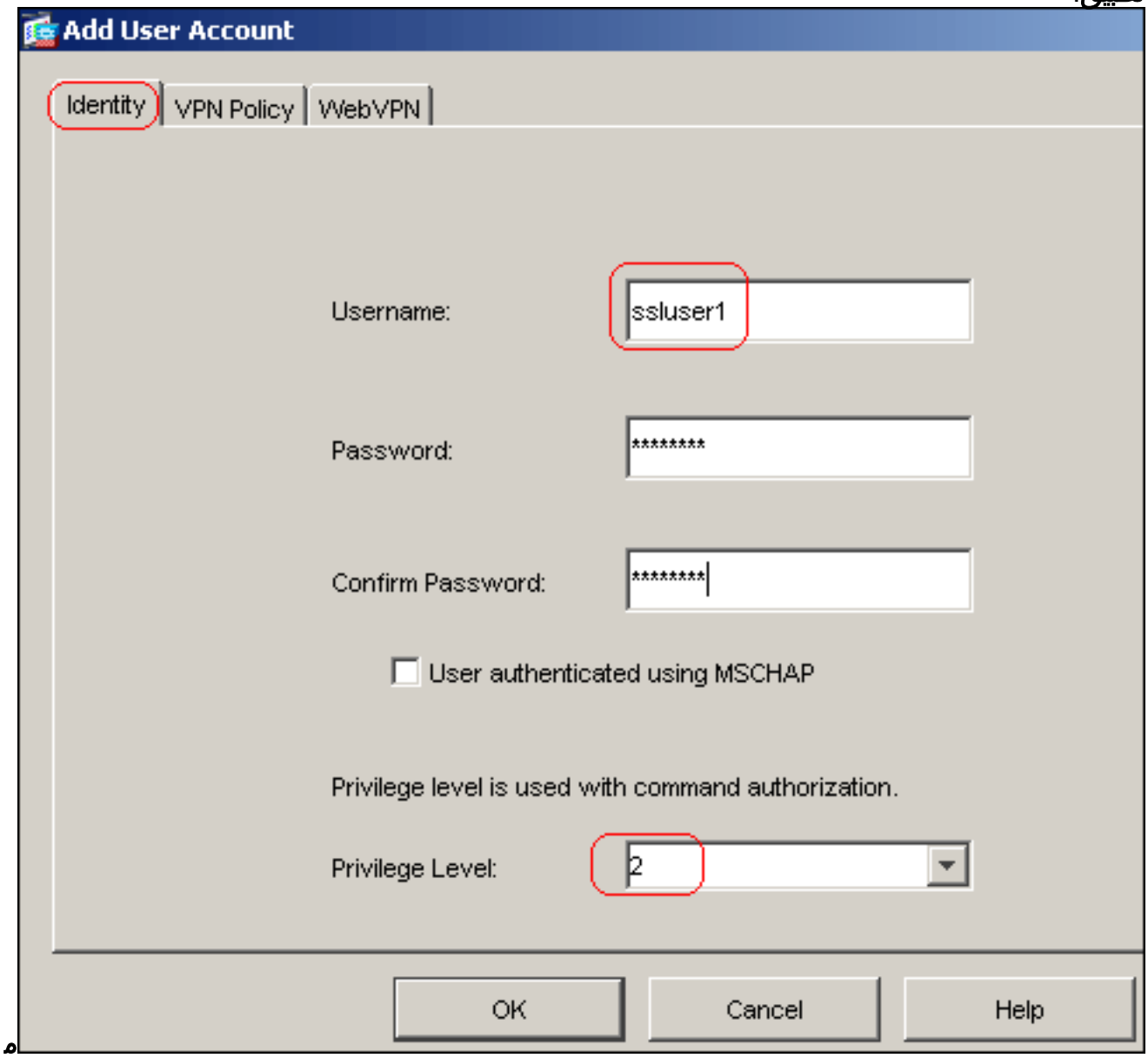
انقر فوق **موافق**، ثم انقر فوق **تطبيق**.



ملاحظة: فيما يلي أوامر تكوين CLI المكافئة:

7. أخترت **تشكيل>VPN>عام>مستعمل>يضيف** in order to خلقت جديد مستعمل حساب *ssluser1*.
8. انقر فوق **موافق**، ثم انقر فوق

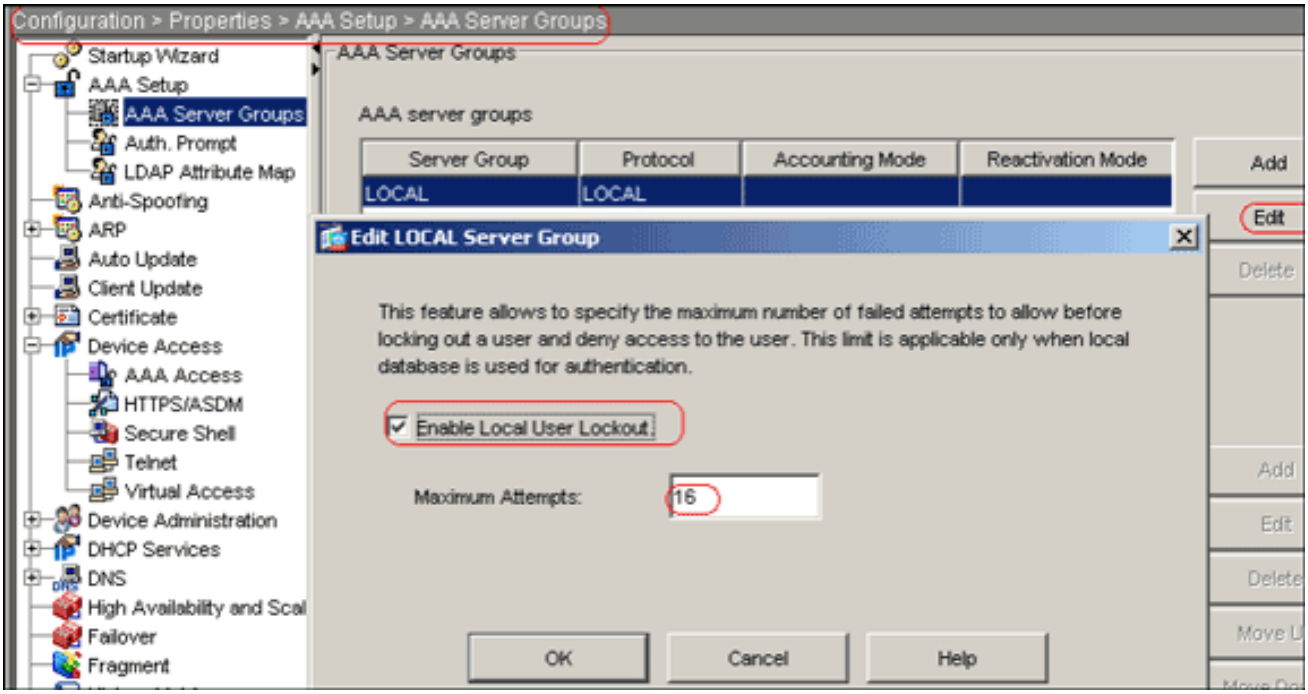
تطبيق.



م

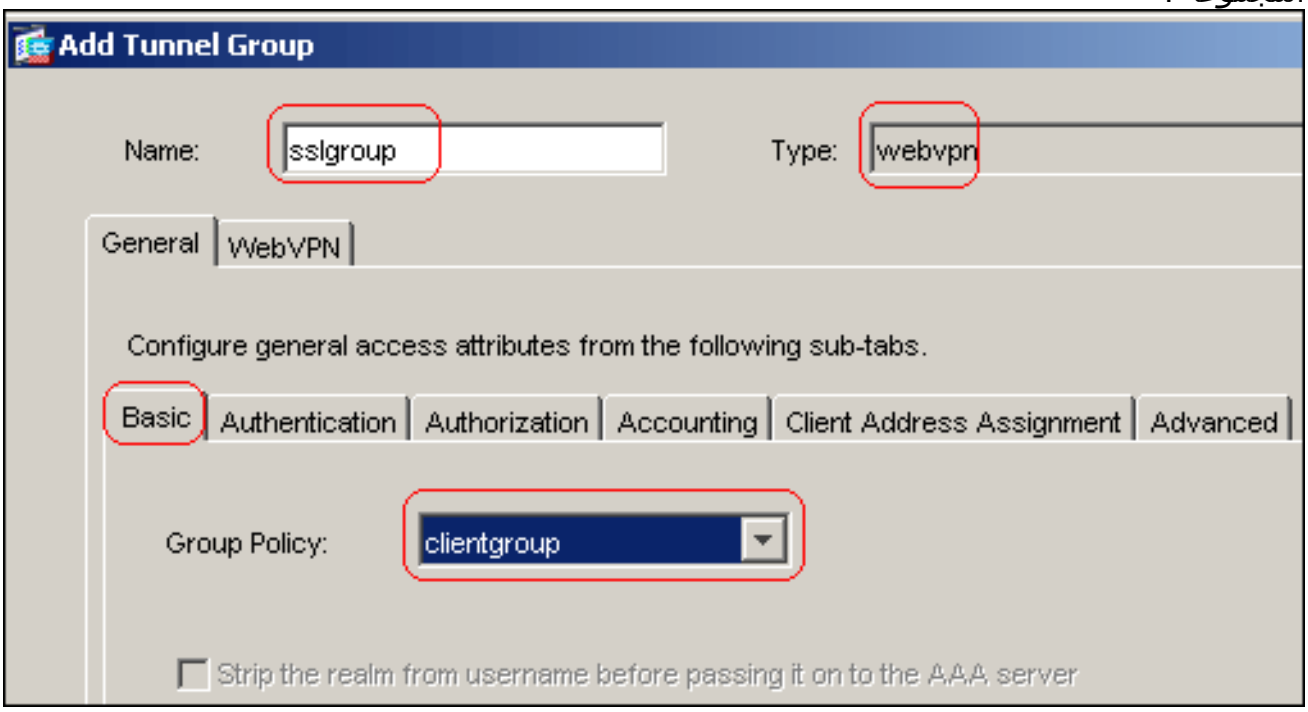
لاحظة: فيما يلي أمر CLI المكافئ:

9. أختر **التكوين > الخصائص > إعداد AAA > مجموعات خوادم AAA > تحرير**.
10. حدد مجموعة الخوادم الافتراضية *المحلية*، وانقر فوق **تحرير**.
11. في شاشة تحرير مجموعة الخوادم المحلية، انقر خانة الاختيار **تمكين تأمين المستخدم المحلي**، وأدخل 16 في مربع النص الحد الأقصى للمحاولات.
12. وانقر فوق **OK**.

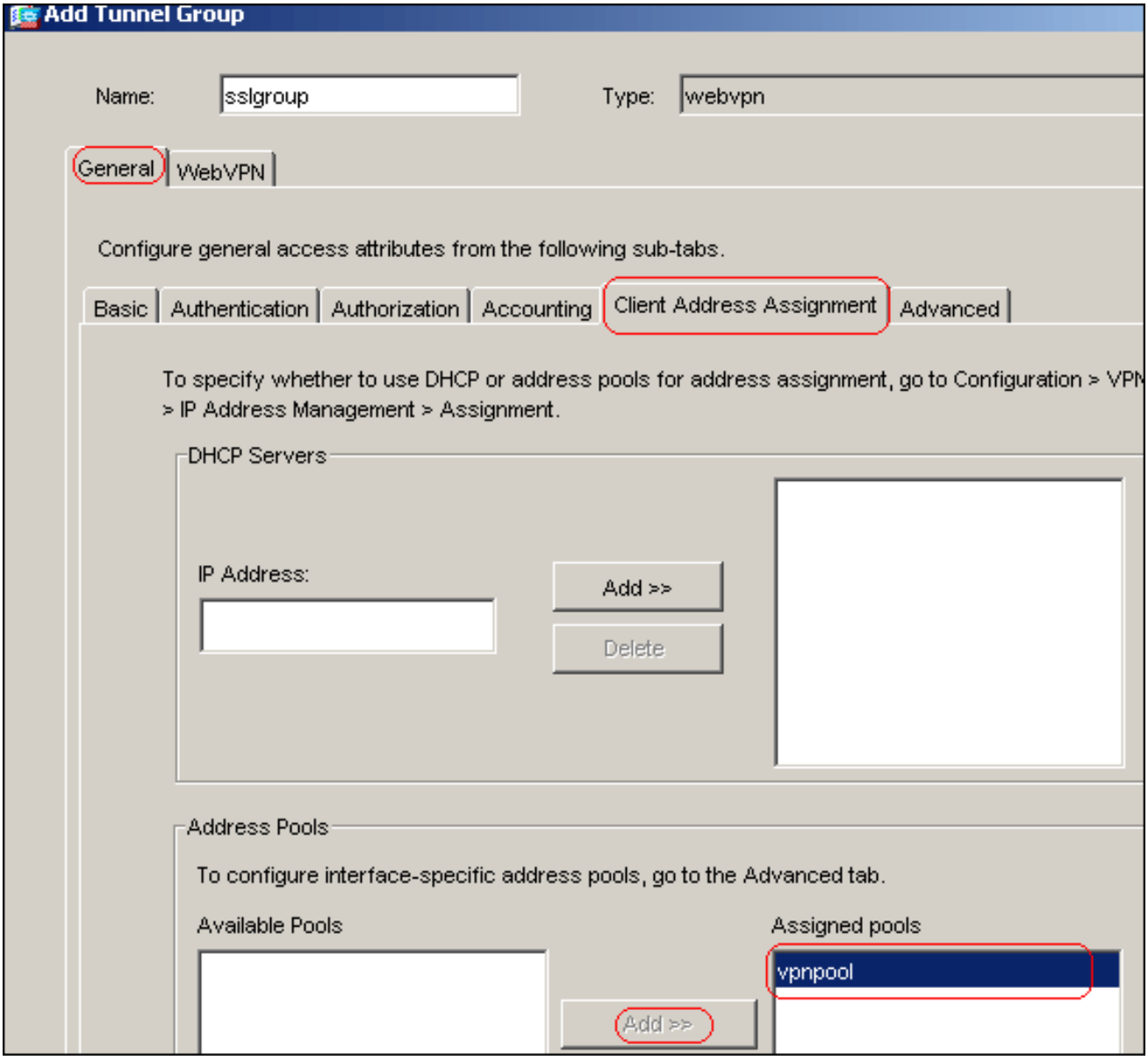


ملاحظة: فيما يلي أمر CLI المكافئ:

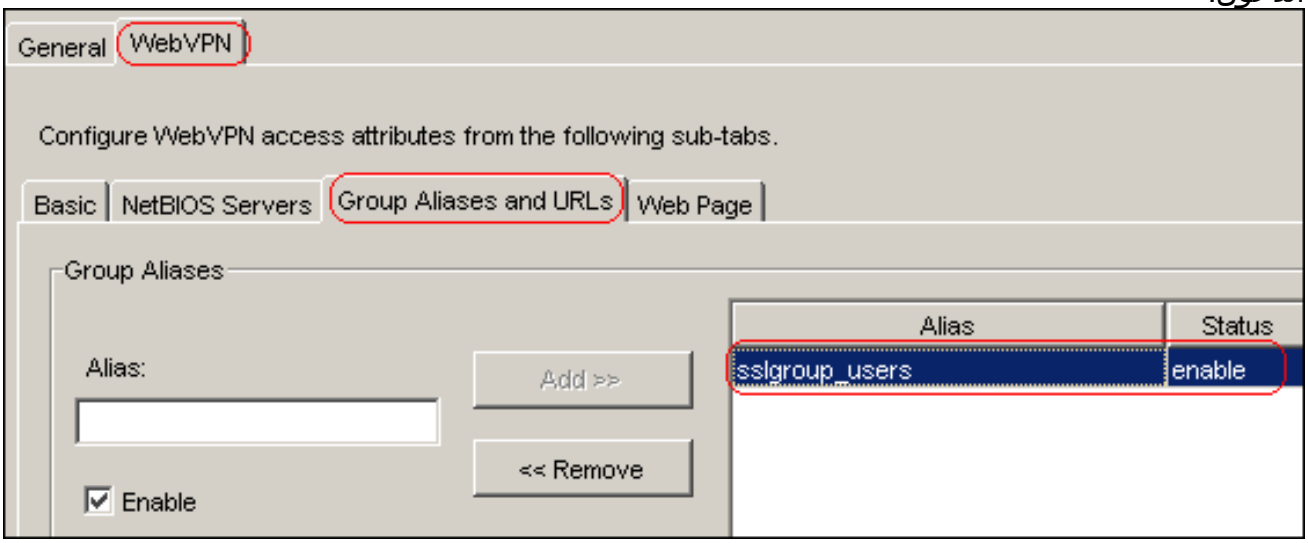
13. تكوين مجموعة النفق:أخترت **تشكيل>VPN>عام>نفق مجموعة>إضافة(WebVPN منفذ)** in order to خلقت جديد نفق مجموعة يعين *sslgroup*.انقر *صفحة* **عام**، ثم انقر صفحة **أساسي**.أختر **ClientGroup** من القائمة المنسدلة "نهج المجموعة".



انقر فوق علامة التبويب **تعيين عنوان العميل**، ثم انقر فوق **إضافة** لتعيين تجمع العناوين المتوفر *vpnPool*.

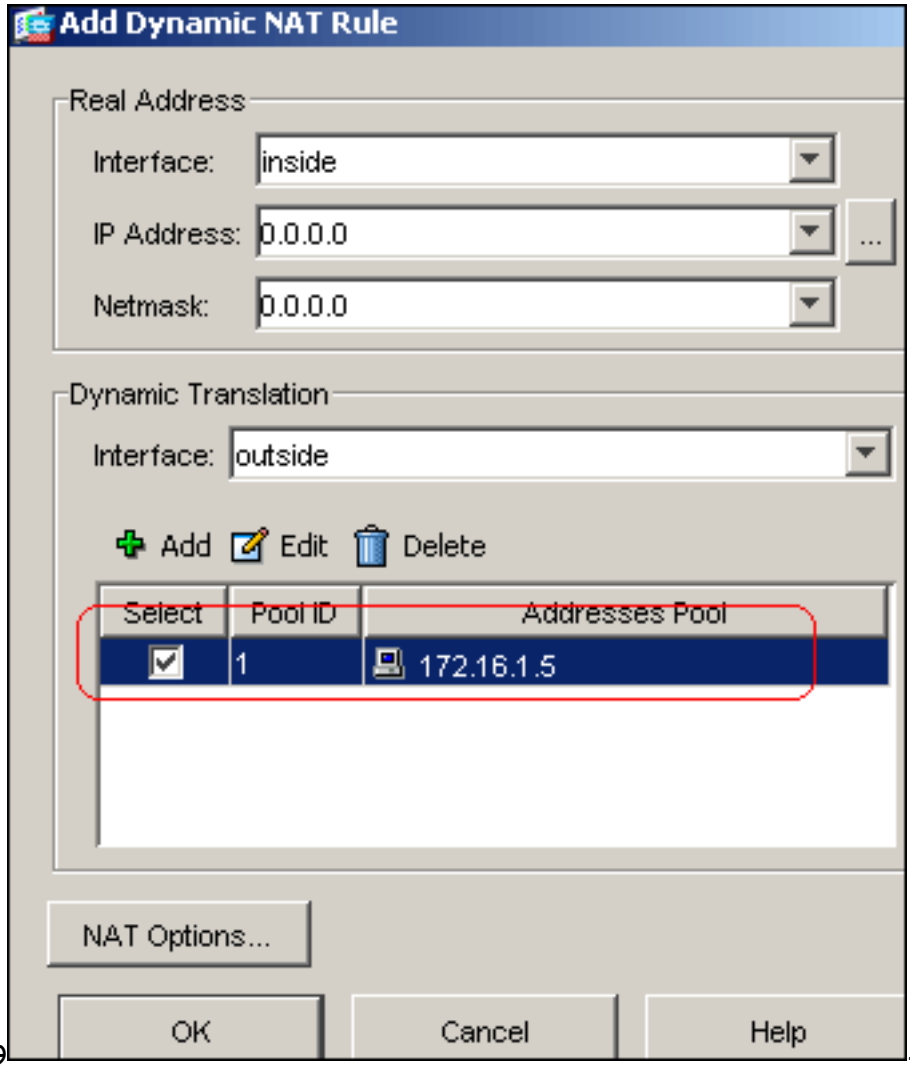


انقر فوق علامة التبويب **WebVPN**، ثم انقر فوق علامة التبويب **أسماء مستعارة للمجموعة وعناوين URL**.اكتب اسم الاسم المستعار في مربع المعلمة، وانقر فوق **إضافة** لإضافته إلى قائمة أسماء المجموعات في صفحة تسجيل
الدخول.



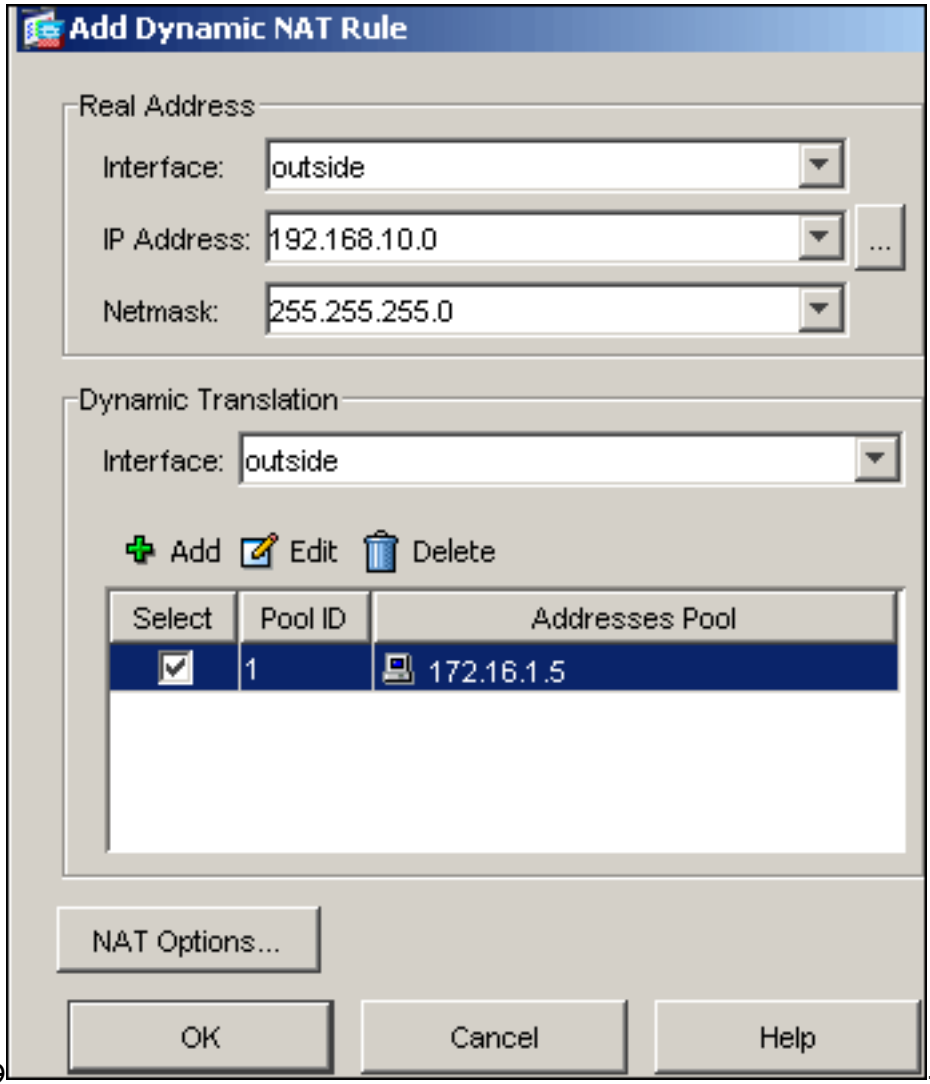
انقر فوق **موافق**، ثم انقر فوق **تطبيق.ملاحظة:** فيما يلي أوامر تكوين CLI المكافئة:

14. تكوين NAT:أخترت **تشكيل>nat>إضافة>إضافة>قاعدة nat حركي** أن يسمح الحركة مرور أن يأتي من الشبكة الداخلية أن يكون ترجمت مع الإستعمالمن الخارجي عنوان



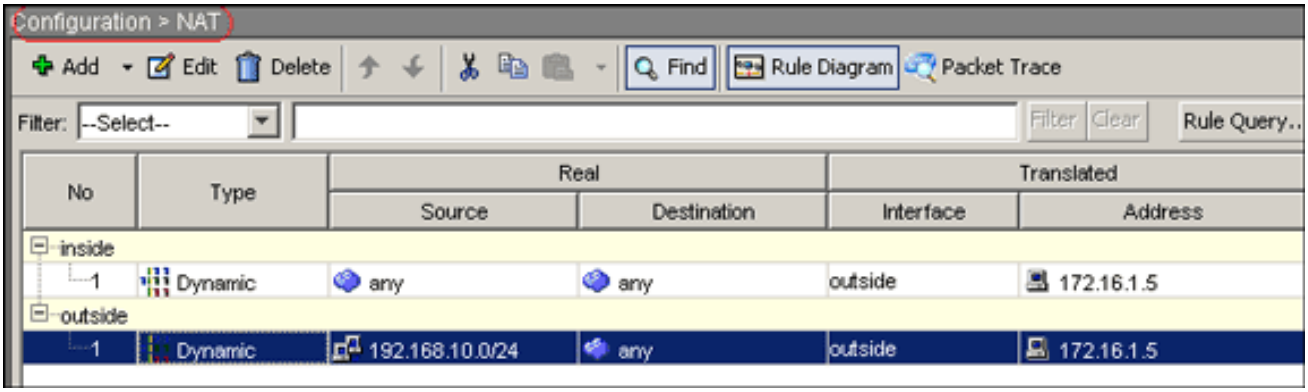
وانقر فوق 172.16.1.5.

OK.أخترت **تشكيل>nat>يضيف>إضافة قاعدة nat حركي** أن يسمح الحركة مرور أن يأتي من الشبكة الخارجية 192.168.10.0 أن يكون ترجمت مع الإستعمالمن العنوان الخارجي



وانقر فوق 172.16.1.5.

OK.



طقطقة **يطبق**.**ملاحظة:** فيما يلي أوامر تكوين CLI المكافئة:

تكوين ASA 7.2(2) 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
same-security-traffic permit intra-interface

Command that permits the SSL VPN traffic to enter ---!
!--- and exit the same interface. access-list 100
extended permit icmp any any 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) 1 0.0.0.0 0.0.0.0

The NAT statement to define what to encrypt !--- ---!
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

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 tunnelall

Encrypt all the traffic coming from the SSL VPN ---!
Clients. 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, increasing 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
```

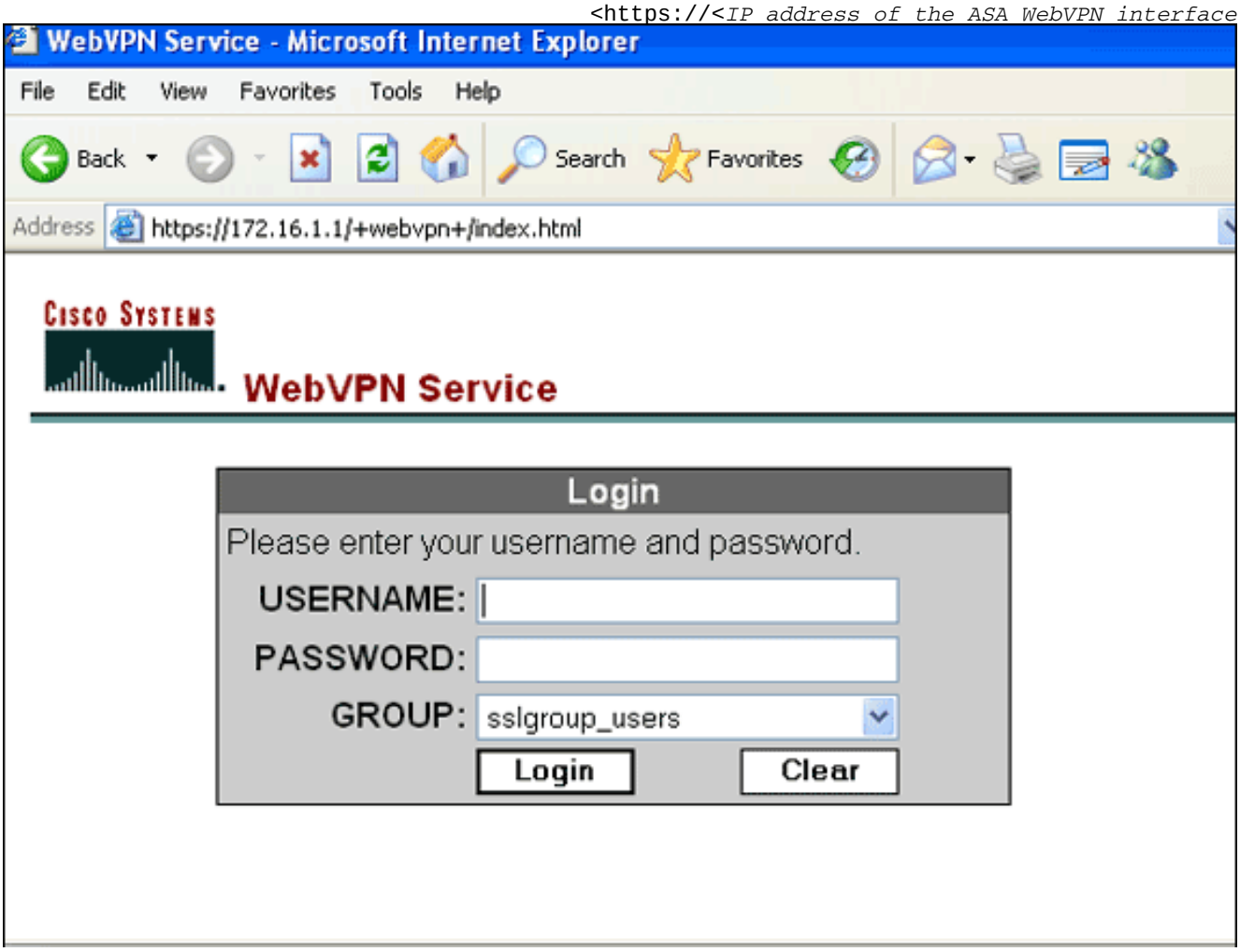
```
    Assign an order to the SVC image. svc enable ---!

    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

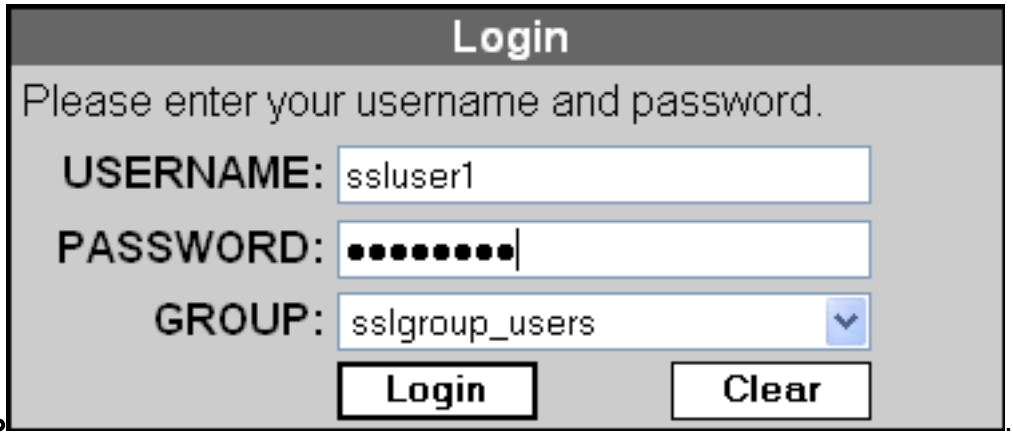
أكمل هذه الخطوات لإنشاء اتصال SSL VPN مع ASA.

1. اكتب في حقل العنوان لمستعرض الويب الخاص بك عنوان URL أو عنوان IP لواجهة WebVPN الخاصة ب ASA.على سبيل المثال:

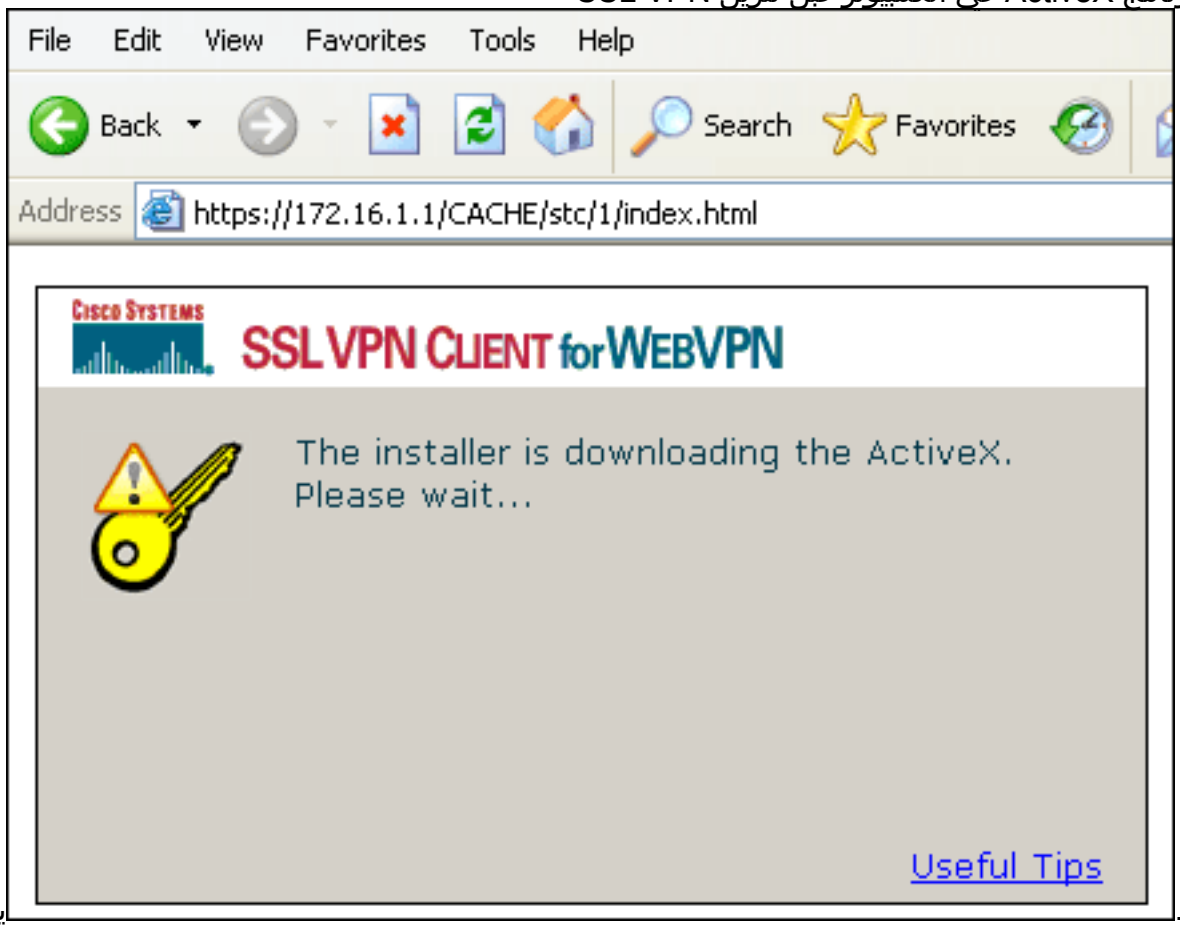
```
<https://<IP address of the ASA WebVPN interface
```



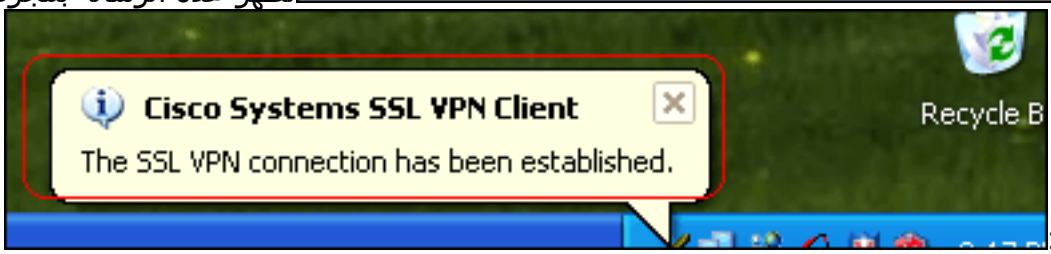
2. أدخل اسم المستخدم وكلمة المرور، ثم أختر المجموعة الخاصة بك من القائمة المنسدلة الخاصة



ملاحظة: يجب تثبيت برنامج ActiveX في الكمبيوتر قبل تنزيل SSL VPN Client. يظهر مربع الحوار هذا عند تأسيس الاتصال:

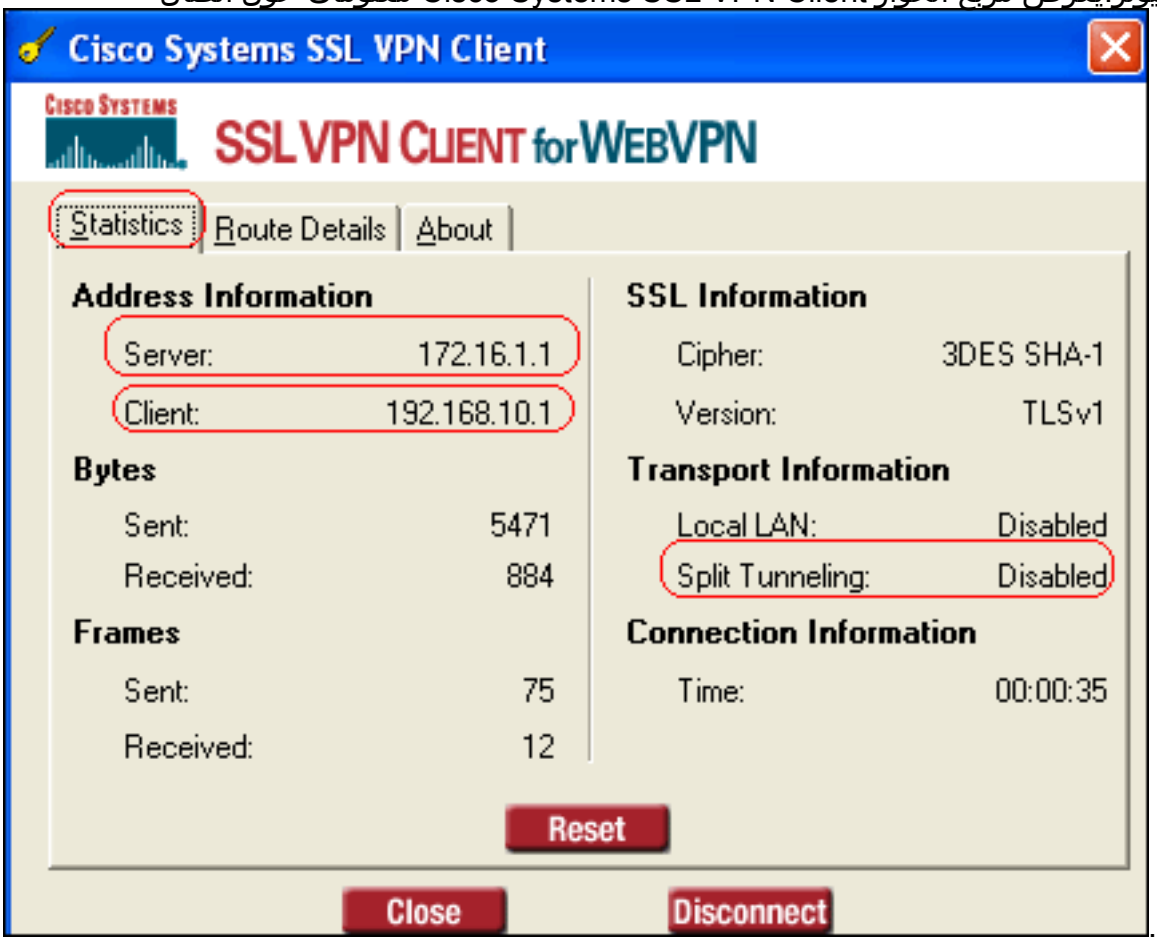


تظهر هذه الرسالة بمجرد تأسيس الاتصال:

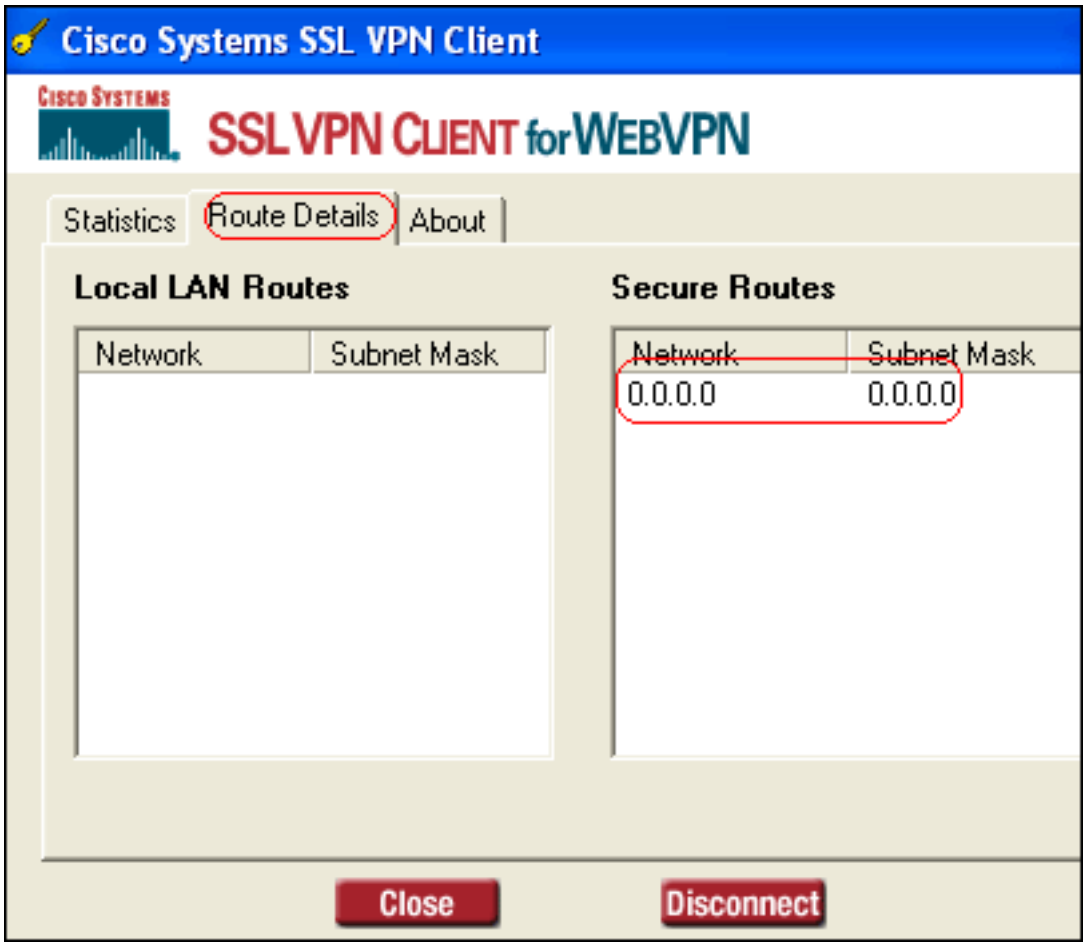


3. بمجرد تأسيس الاتصال، انقر نقرا مزدوجا على رمز المفتاح الأصفر الذي يظهر في شريط المهام على

الكمبيوتر.يعرض مربع الحوار Cisco Systems SSL VPN Client معلومات حول اتصال



.SSL



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.

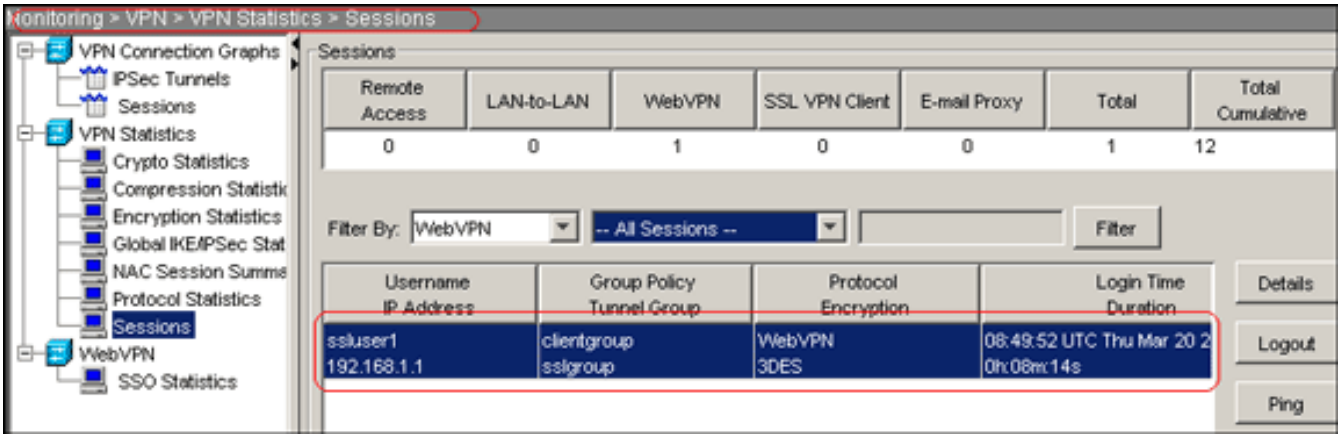
```
ciscoasa#show vpn-sessiondb svc

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 شاهدت معلومة حول الحالي WebVPN جلسة في ال ASA.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- **<VPN-sessionDB logoff name <*username*>**—يسمح أنت أن يدون خارج ال SSL VPN جلسة ل ال يعين مستعمل إسم.

```
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، أنت يستطيع استعملت الأمر **vpn-sessiondb logoff svc** in order to أنهيت all the SVC جلسة.**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
```

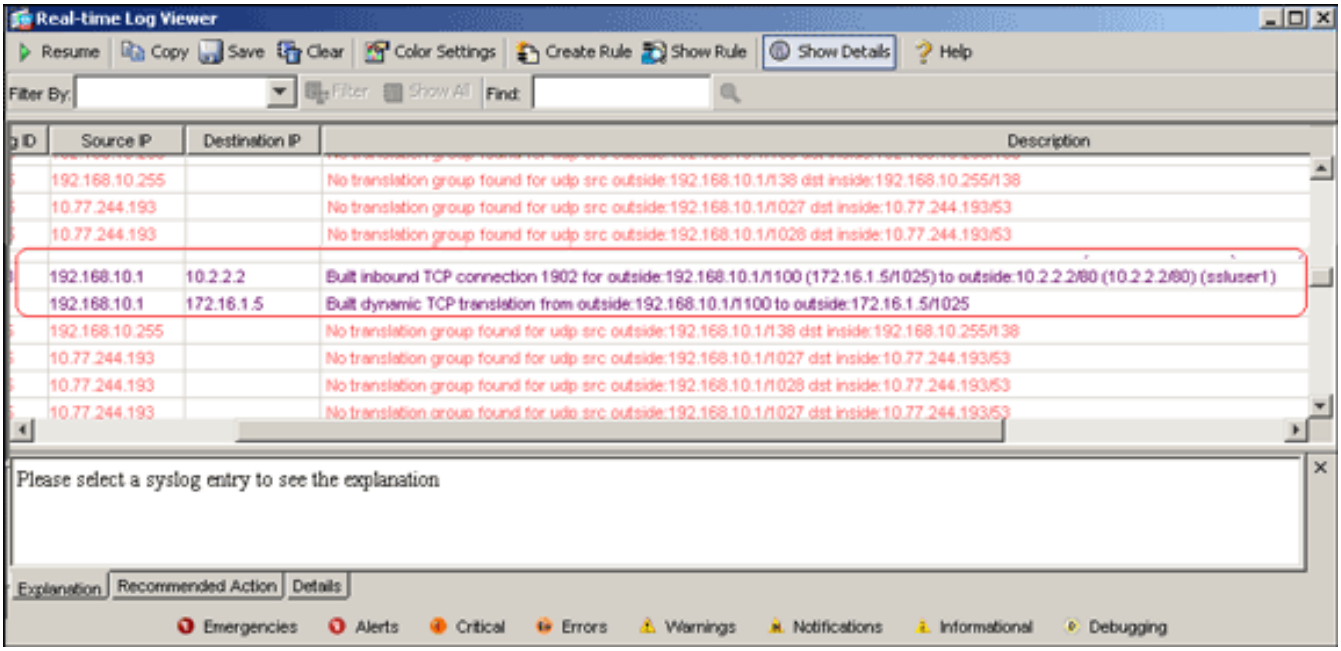
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **<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
```

- في ASDM، أختر **مراقبة > تسجيل > عارض السجل في الوقت الفعلي > عرض** لعرض الأحداث في الوقت الفعلي. تظهر هذه الأمثلة معلومات الجلسة بين 192.168.10.1 SVC و 10.2.2.2 WebServer في الإنترنت عبر ASA 172.16.1.5.



معلومات ذات صلة

- صفحة دعم جهاز الأمان القابل للتكيف طراز 5500 Series من Cisco
- 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).