

ي ق فن ل ل اص ت ال ا م ي س ق ت ب ح ام س ل ا : ASA 8.x ن ي و ك ت ل ا ث م ي ل ع AnyConnect VPN ل ي م ع ل ASA

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [تكوين ASA باستخدام ASDM 6.0\(2\)](#)
- [تكوين ASA CLI](#)
- [إنشاء اتصال SSL VPN باستخدام SVC](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح بوصول عميل Cisco AnyConnect VPN إلى الإنترنت أثناء إنشاء قنوات لها في جهاز الأمان القابل للتكيف (ASA) من Cisco 8.0.2. يتيح هذا التكوين للعميل إمكانية الوصول الآمن إلى موارد الشركة عبر SSL أثناء منح وصول غير آمن إلى الإنترنت باستخدام الاتصال النفقي المنقسم.

المتطلبات الأساسية

المتطلبات

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

- يحتاج جهاز الأمان ASA إلى تشغيل الإصدار x.8
- العميل AnyConnect VPN 2.x من Cisco (ملاحظة: تنزيل حزمة عميل AnyConnect-VPN (AnyConnect VPN) (win*.pkg) من [تنزيل برامج Cisco](#) (للعلماء المسجلين فقط). انسخ عميل AnyConnect VPN إلى ذاكرة ASA flash، والتي يجب تنزيلها إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع قسم [تثبيت عميل AnyConnect](#) من دليل تكوين ASA للحصول على مزيد من المعلومات.

المكونات المستخدمة

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

- Cisco 5500 Series ASA أن يركض برمجية صيغة 8.0(2)
- إصدار عميل AnyConnect SSL VPN من Cisco لـ Windows 2.0.0343
- جهاز الكمبيوتر الذي يقوم بتشغيل Microsoft Vista أو Windows XP SP2 أو Windows 2000 Professional مع SP4 مع Microsoft Installer الإصدار 3.1
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 6.0(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

يوفر عميل AnyConnect VPN من Cisco اتصالات SSL الآمنة بجهاز الأمان للمستخدمين عن بعد. دون وجود عميل تم تثبيته مسبقاً، يقوم المستخدمون عن بعد بإدخال عنوان IP في المستعرض الخاص بهم من واجهة تم تكوينها لقبول اتصالات SSL VPN. ما لم يتم تكوين جهاز الأمان لإعادة توجيه طلبات http:// إلى https://، يجب على المستخدمين إدخال عنوان URL في النموذج <address>:https://.

بعد إدخال عنوان URL، يتصل المستعرض بتلك الواجهة ويعرض شاشة تسجيل الدخول. إذا استوفى المستخدم تسجيل الدخول والمصادقة، وقام جهاز الأمان بتعريف المستخدم على أنه يتطلب من العميل، فإنه يقوم بتنزيل العميل الذي يتطابق مع نظام تشغيل الكمبيوتر البعيد. بعد التنزيل، يقوم العميل بتثبيت نفسه وتكوينه وإنشاء اتصال SSL آمن ويبقى أو يقوم بإلغاء تثبيت نفسه (حسب تكوين جهاز الأمان) عند إنهاء الاتصال.

في حالة عميل تم تثبيته مسبقاً، عندما يقوم المستخدم بالتصديق، يقوم جهاز الأمان بفحص مراجعة العميل وترقية العميل حسب الضرورة.

عندما يقوم العميل بالتفاوض على اتصال SSL VPN باستخدام جهاز الأمان، فإنه يتصل باستخدام أمان طبقة النقل (TLS)، وبشكل اختياري، أمان طبقة نقل البيانات (DTLS). تتجنب DTLS مشاكل زمن الوصول والنطاق الترددي المقترنة ببعض اتصالات SSL، وتحسن أداء تطبيقات الوقت الفعلي الحساسة لتأخيرات الحزم.

يمكن تنزيل عميل AnyConnect من جهاز الأمان أو يمكن تثبيته يدوياً على الكمبيوتر البعيد بواسطة مسؤول النظام. ارجع إلى [دليل مسؤول عميل AnyConnect VPN من Cisco](#) للحصول على مزيد من المعلومات حول كيفية تثبيت العميل يدوياً.

يقوم جهاز الأمان بتنزيل العميل استناداً إلى نهج المجموعة أو سمات اسم المستخدم الخاصة بالمستخدم الذي يقوم بإنشاء الاتصال. يمكنك تكوين جهاز الأمان لتنزيل العميل تلقائياً، أو يمكنك تكوينه لمطالبة المستخدم البعيد حول ما إذا كان سيتم تنزيل العميل أم لا. وفي الحالة الأخيرة، إذا لم يستجب المستخدم، فيمكنك تكوين جهاز الأمان إما لتنزيل العميل بعد فترة المهلة أو لتقديم صفحة تسجيل الدخول.

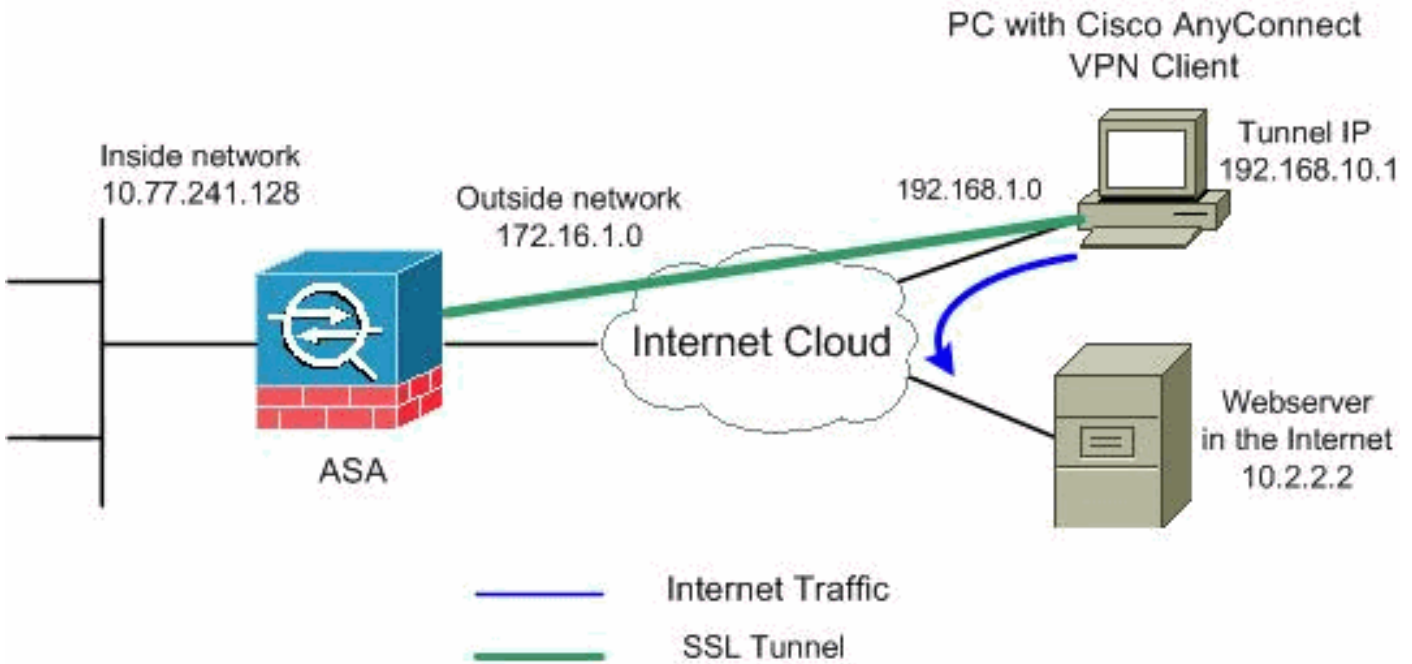
التكوين

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

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [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.

تكوين ASA باستخدام (ASDM 6.0(2)

يفترض هذا المستند أن التكوين الأساسي، مثل تكوين الواجهة، 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.

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

1. أخترت تشكيل وصول عن بعد VPN شبكة (زبون) منفذ عنوان إدارة عنوان بركة إضافة in order to خلقت

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

عنوان بركة IP VPNpool.

2. طقطقة يطبق. CLI تشكيل مكافئ:

3. تمكين WebVPN. أخترت تشكيل <وصول عن بعد VPN> شبكة <زبون> منفذ SSL VPN توصيل وتحت منفذ قارن، طقطقت ال يسمح منفذ ويمكن DTLS للقارن خارجي. تحقق أيضا من تمكين وصول عميل VPN AnyConnect من Cisco أو وصول عميل SSL VPN القديم على الواجهة المحددة في خانة الاختيار الجدول أدناه لتمكين SSL VPN على الواجهة الخارجية.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

Access Interfaces

Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

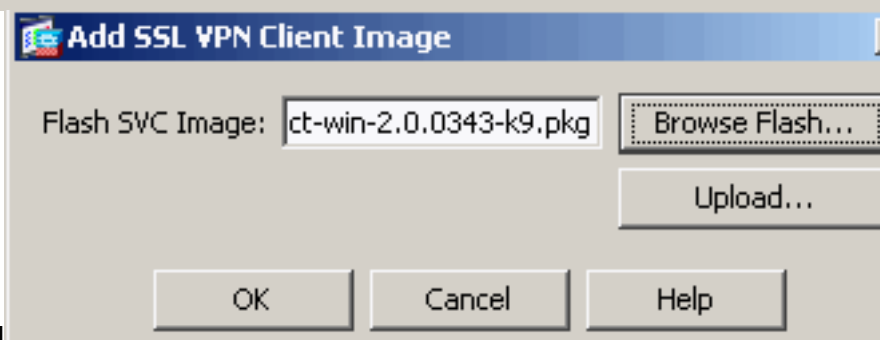
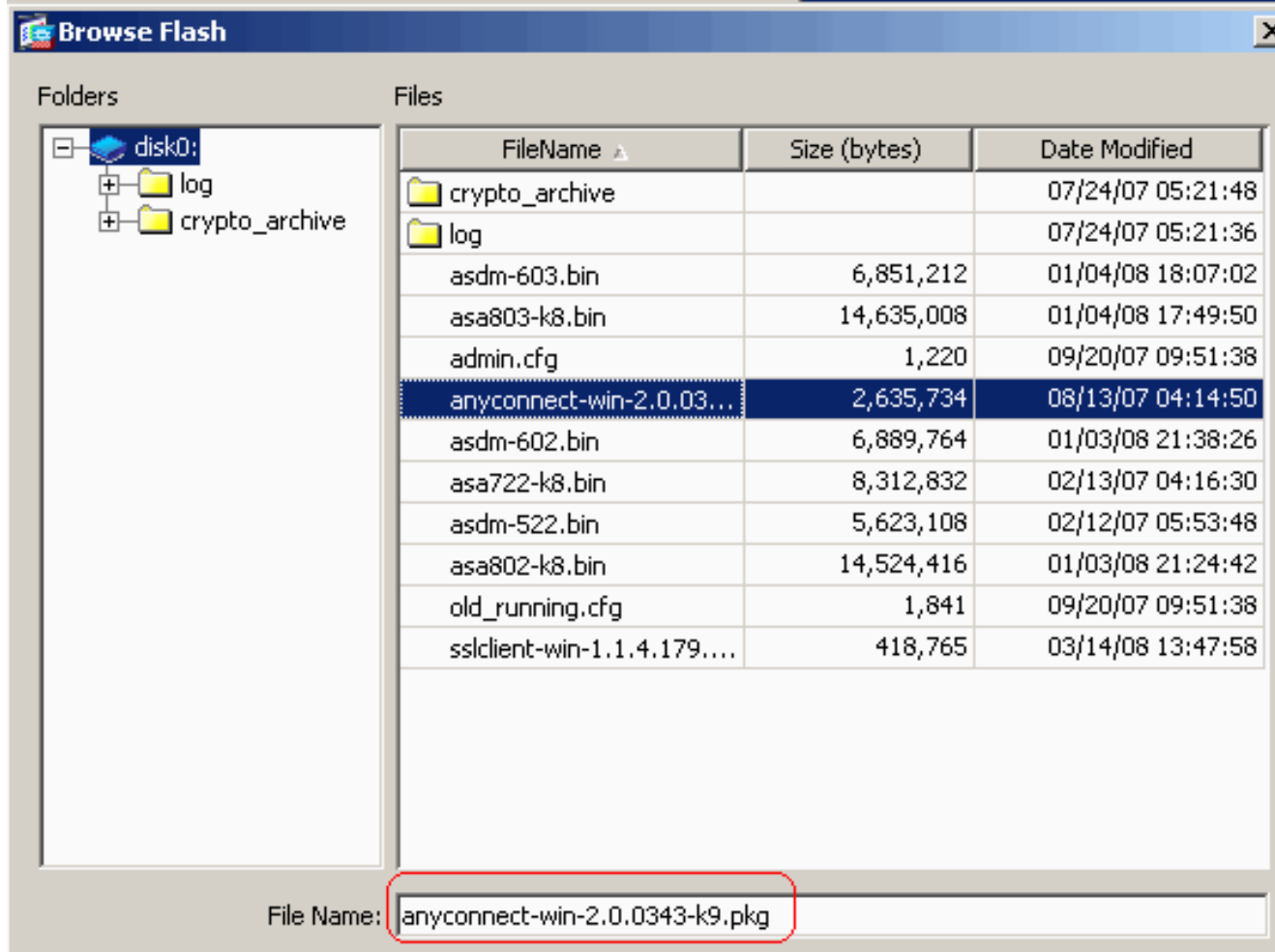
Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

DTLS Port:

Click here to [Assign Certificate to Interface](#).

طقطقة يطبق. أخترت Configuration > Remote Access VPN < (التكوين) Network < (العميل) Access (الوصول إلى الشبكة) < SSL VPN < إعدادات العميل > Advanced > Add in order to أضفت ال Cisco AnyConnect VPN Client Image من ذاكرة Flash (الذاكرة المؤقتة) ل ASA كما هو



انقر فوق إضافة

وانقر فوق OK (Add).

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

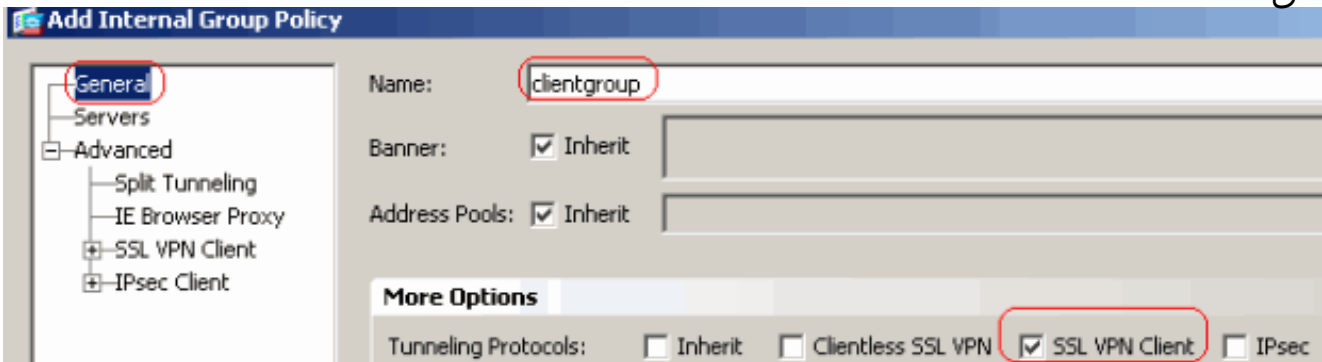
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t

+ Add ✎ Replace 🗑 Delete ⬆ Move UP ⬇ Move Down

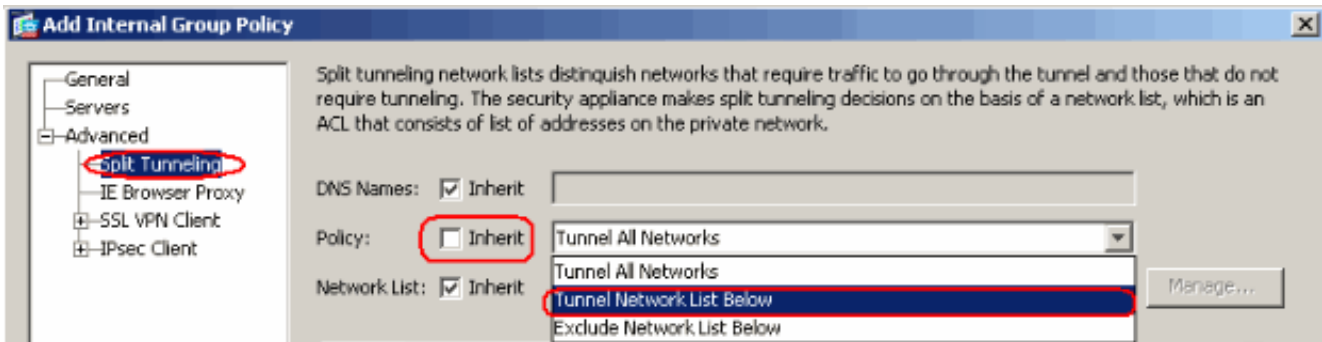
disk0:/anyconnect-win-2.0.0343-k9.pkg

CLI تشكيل مكافئ:

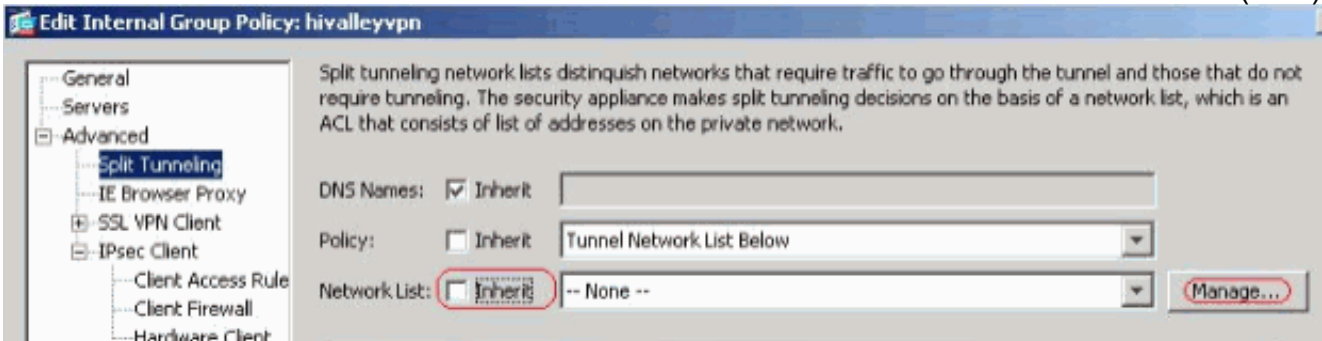
4. تكوين نهج المجموعة. اخترت تشكيل <وصول عن بعد VPN> شبكة (زبون) منفذ <مجموعة نهج in order to خلقت داخلي مجموعة زبون سياسة مجموعة. تحت علامة التبويب عام، حدد خانة الاختيار SSL VPN Client لتمكين WebVPN كبروتوكول نفق.



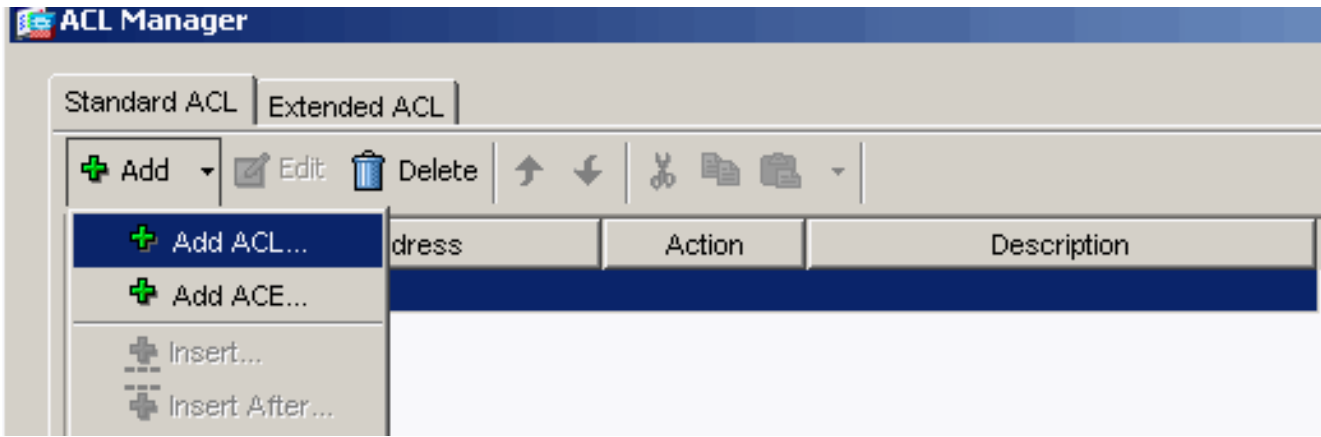
في علامة التبويب خيارات متقدمة < تقسيم الاتصال النفقي، قم بإلغاء تحديد خانة الاختيار Inherit لنهج النفق المقسم واختر قائمة شبكة النفق أدناه من القائمة المنسدلة.



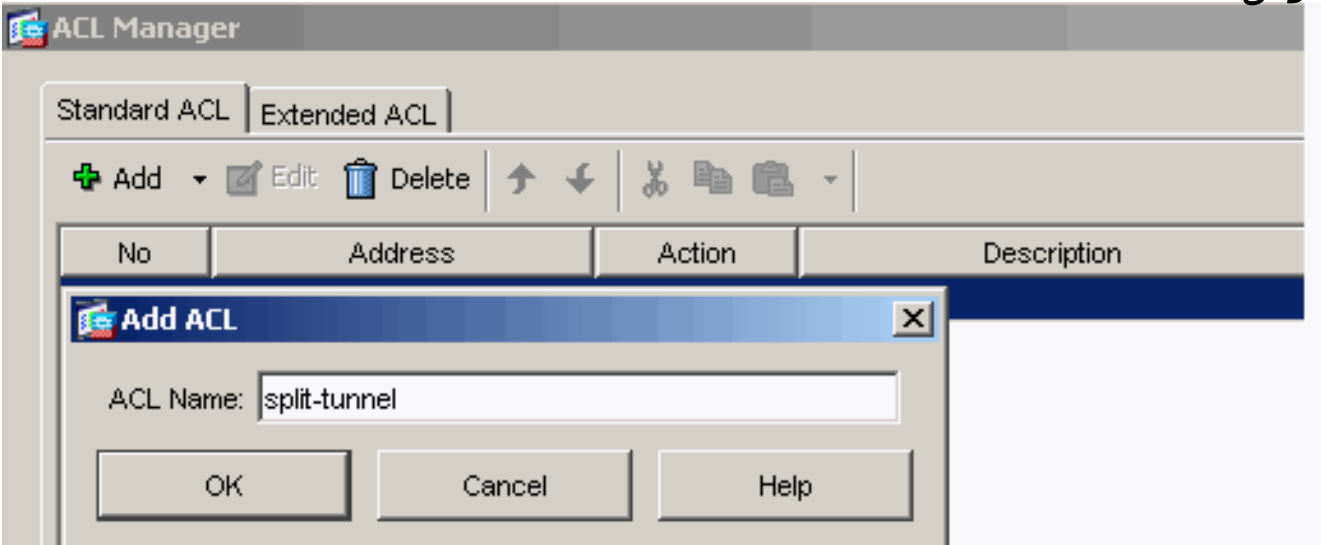
قم بإلغاء تحديد خانة الاختيار Inherit لقائمة شبكات النفق المقسم ثم انقر فوق Manage لتشغيل إدارة قائمة التحكم في الوصول (ACL).



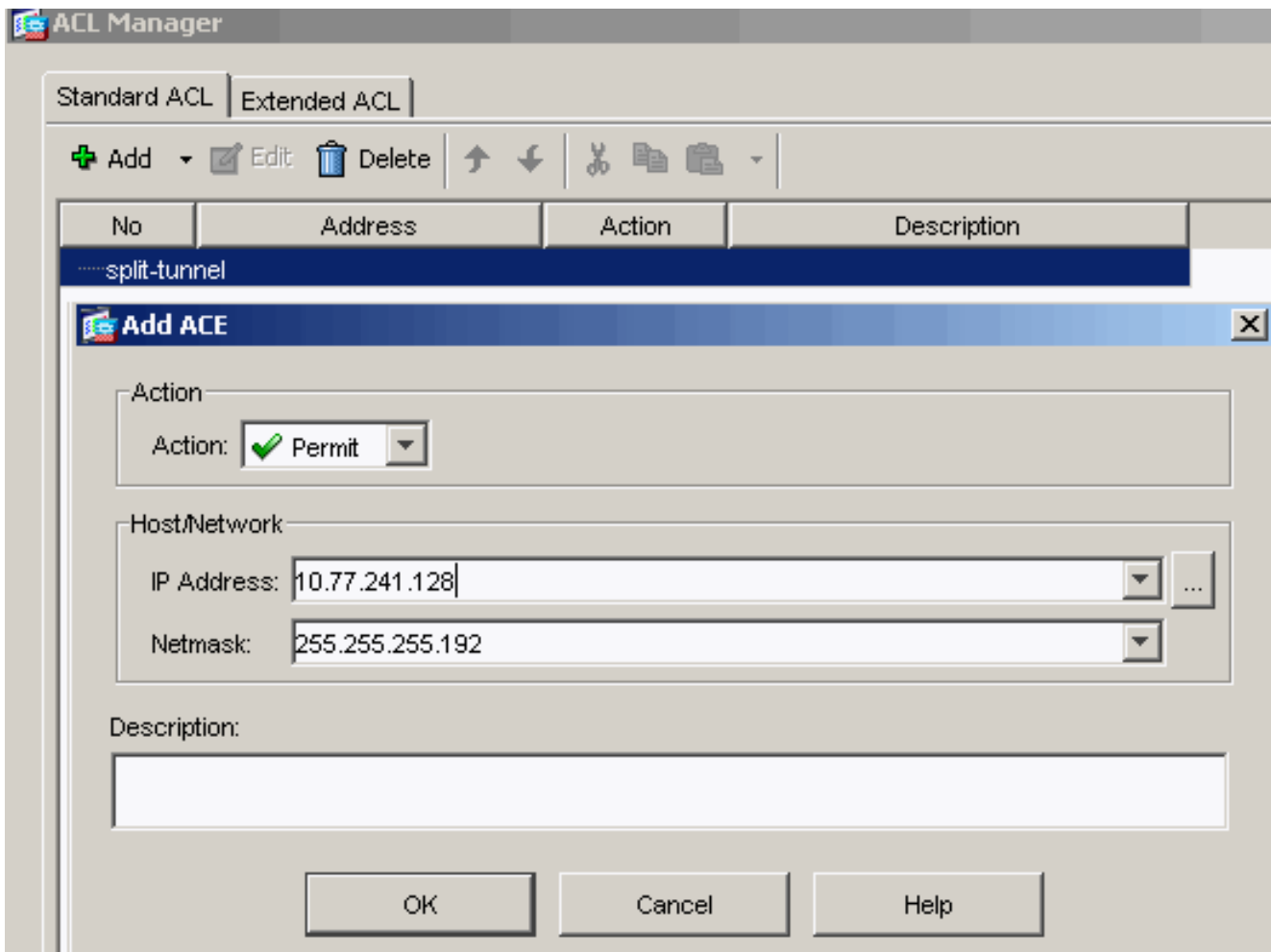
ضمن إدارة قائمة التحكم في الوصول (ACL)، اختر إضافة < قائمة التحكم في الوصول (ACL) .. لإنشاء قائمة وصول جديدة.



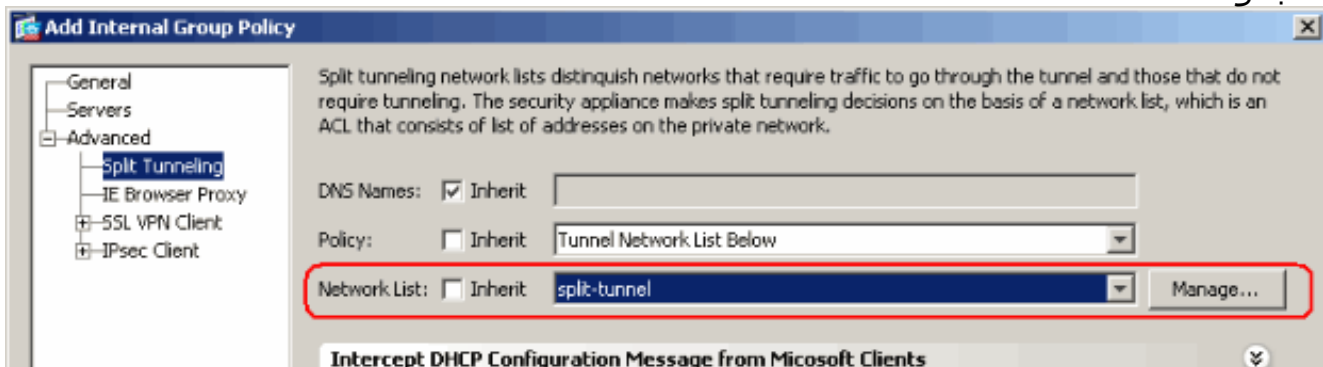
قم بتوفير اسم لقائمة التحكم بالوصول (ACL) وانقر فوق موافق.



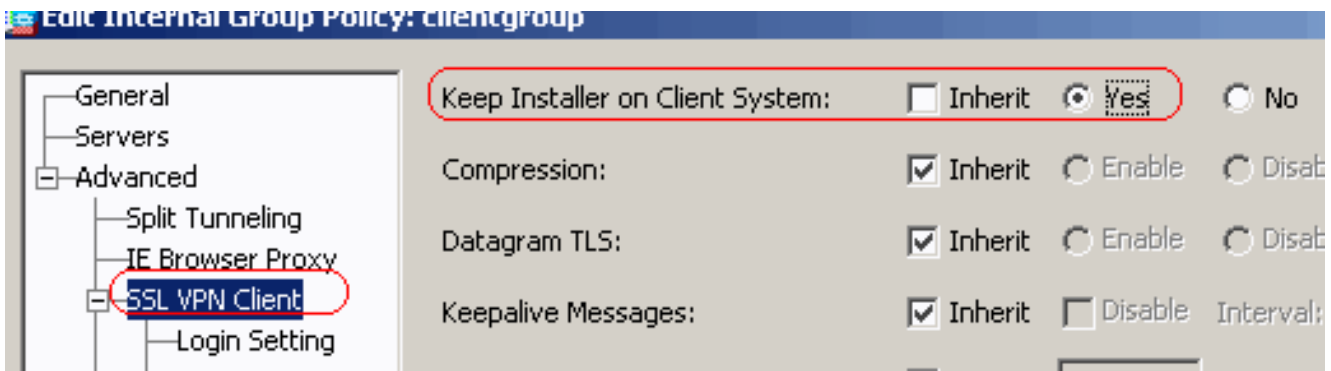
بمجرد إنشاء اسم قائمة التحكم في الوصول، اختر إضافة < إضافة ACE لإضافة إدخال التحكم في الوصول (ACE). عيّن ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 26/10.77.241.128 وحدد السماح كإجراء. انقر فوق موافق للخروج من إدارة قائمة التحكم في الوصول (ACL).



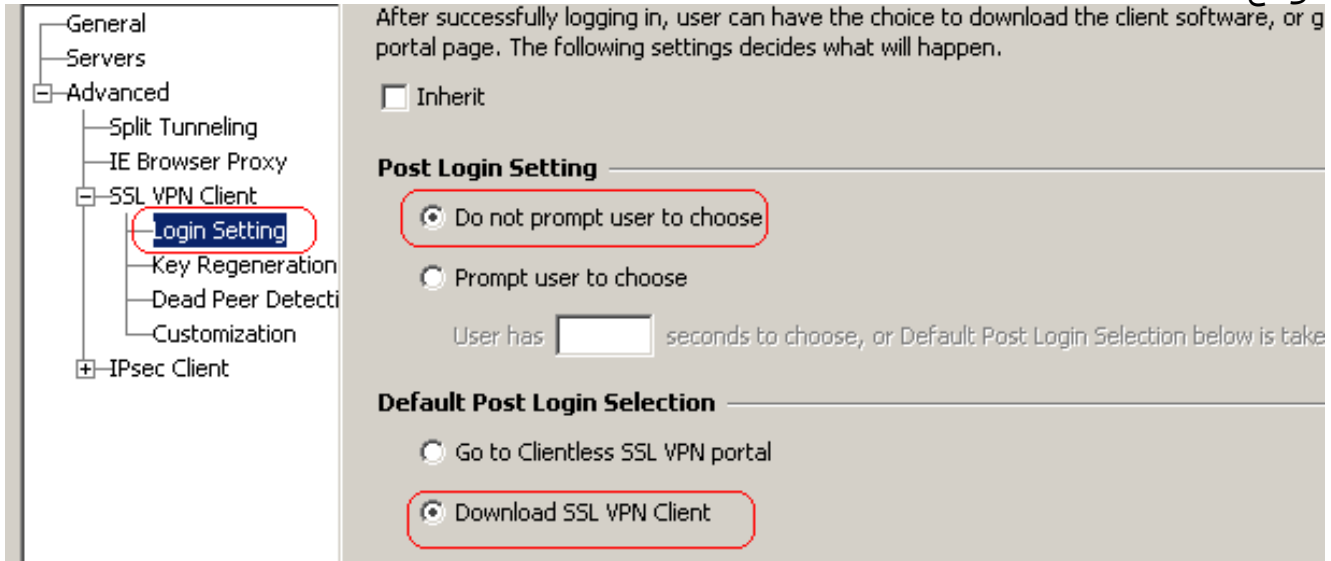
تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق المنقسم. انقر فوق موافق للعودة إلى تكوين "نهج المجموعة".



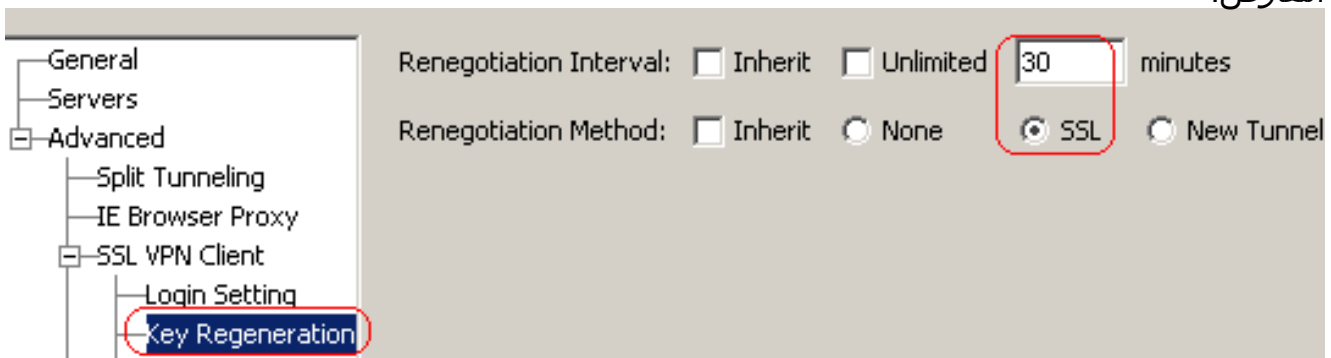
على الصفحة الرئيسية، انقر فوق تطبيق ثم إرسال (إذا كان ذلك مطلوباً) لإرسال الأوامر إلى ASA. قم بتكوين إعدادات SSL VPN ضمن وضع نهج المجموعة للحصول على خيار إبقاء المثبت على نظام العميل، قم بإلغاء تحديد خانة الاختيار توريث، وانقر فوق الزر نعم للانتقاء. يسمح هذا الإجراء لبرنامج SVC بالبقاء على جهاز العميل. لذلك، لا يتطلب ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خياراً جيداً للمستخدمين البعيدين الذين غالباً ما يصلون إلى شبكة الشركة.



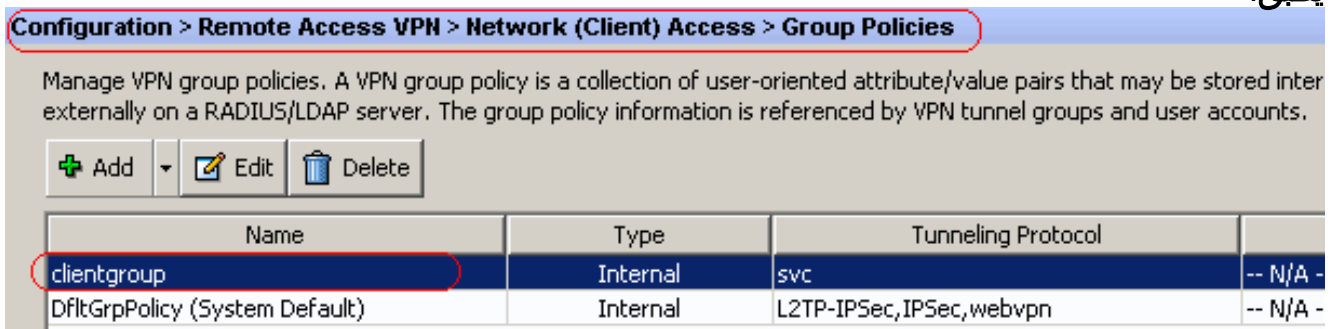
انقر فوق إعداد تسجيل الدخول لتعيين إعداد تسجيل الدخول إلى مادة النشر وتحديد تسجيل الدخول إلى مادة النشر الافتراضي كما هو موضح.



الخيار الفاصل الزمني لإعادة التفاوض، قم بإلغاء تحديد خانة الاختيار **Inherit**، وإلغاء تحديد خانة الاختيار **Unlimited**، وأدخل عدد الدقائق حتى المفتاح. يتم تحسين الأمان عن طريق تعيين حدود على طول الوقت الذي يكون فيه المفتاح صالحاً. 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.



طقطقت ok وبعد ذلك يطبق.



CLI تشكيل مكافئ:

5. أخترت تشكيل <Remote Access VPN عن بعد> AAA <محلي مستعمل> يضيف in order to خلقت جديد مستعمل حساب ssluser1. طقطقت ok وبعد ذلك يطبق.

Add User Account

Identity

Username: ssluser1

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Member-of

Member-of: Add >> Delete

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 2

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

CLI تشكيل مكافئ:

6. أخترت تشكيل <Remote Access VPN (الوصول عن بعد)> AAA إعداد <AAA نادل مجموعة> تحرير in order to عدلت التقصير نادل مجموعة محلي ب يفحص ال enable محلي تأمين المستخدم مع أقصى قيمة محاولات ك .16

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts: 16

OK

Cancel

Help

7. طقطقت ok وبعد ذلك يطبق CLI تشكيل مكافئ:

8. تكوين مجموعة النفق. اخترت تشكيل <Remote Access VPN> شبكة (زبون) منفذ <SSL VPN> توصيل توصيفات <إضافة> in order to خلقت جديد نفق مجموعة sslgroup. في علامة التبويب أساسي، يمكنك تنفيذ قائمة التكوينات كما هو موضح: قم بتسمية مجموعة النفق باسم SSLGROUP. اخترت تحت عنوان تعيين، العنوان بركة vpnPool من القائمة المنسدلة. ضمن "نهج المجموعة الافتراضي"، اختر مجموعة عملاء نهج المجموعة من القائمة المنسدلة.

Add SSL VPN Connection Profile

Basic
Advanced

Name: sslgroup

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: vpnpool

Default Group Policy

Group Policy: clientgroup

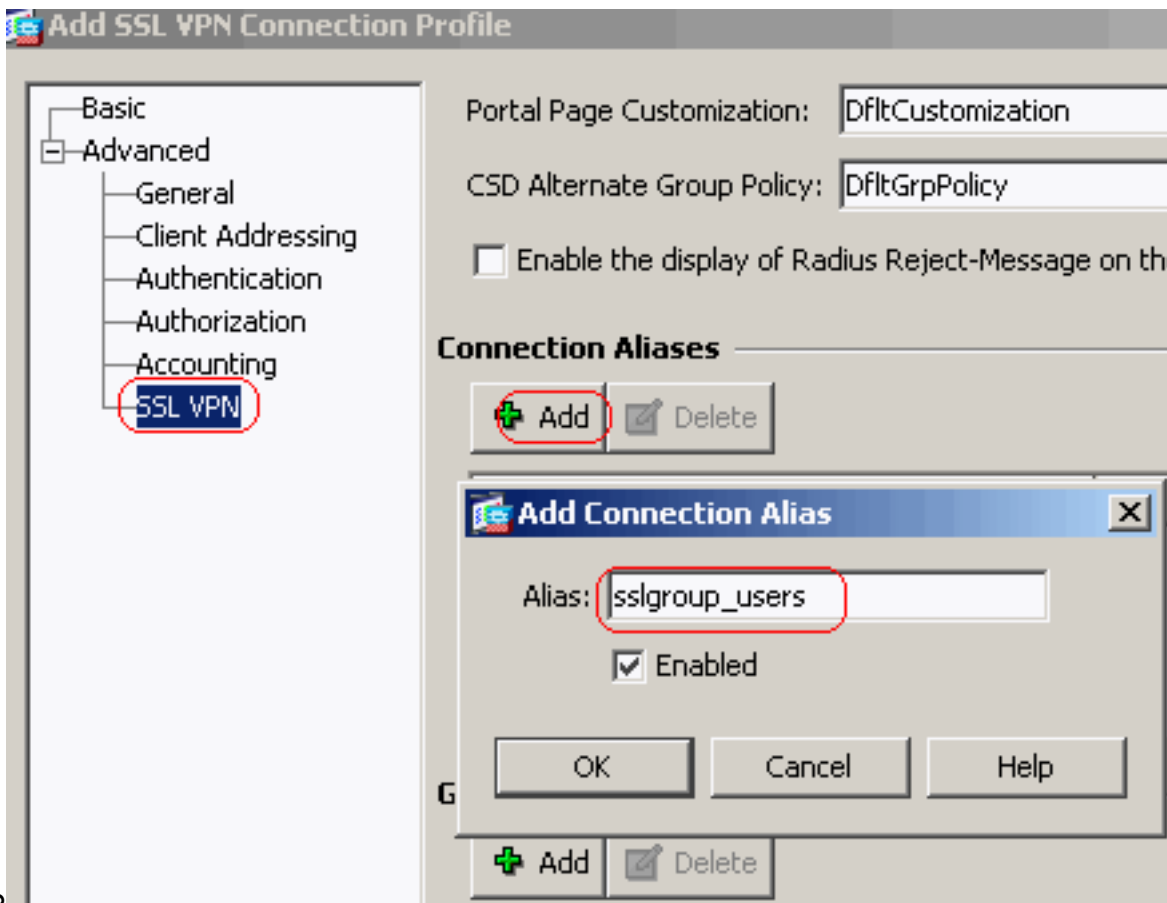
SSL VPN Client Protocol: Enabled

OK

Cancel

Help

تحت علامة التبويب SSL VPN < أسماء مستعارة الاتصال، حدد اسم اسم المجموعة المستعار على هيئة sslgroup_users وانقر على

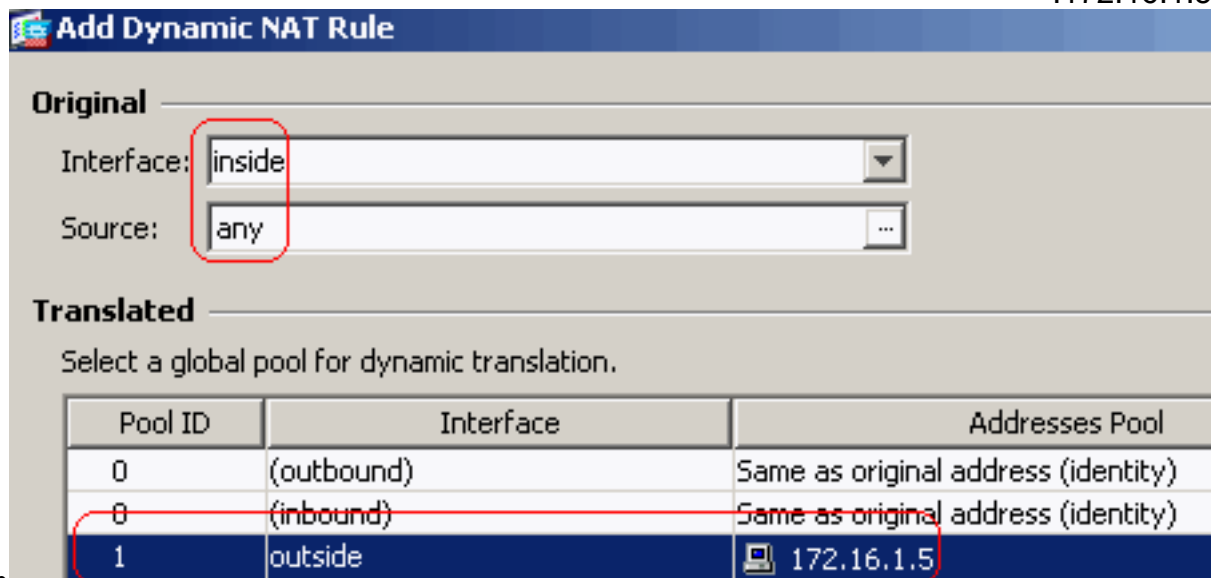


طقط

موافق.

وقت ok وبعد ذلك يطبق CLI تشكيل مكافئ:

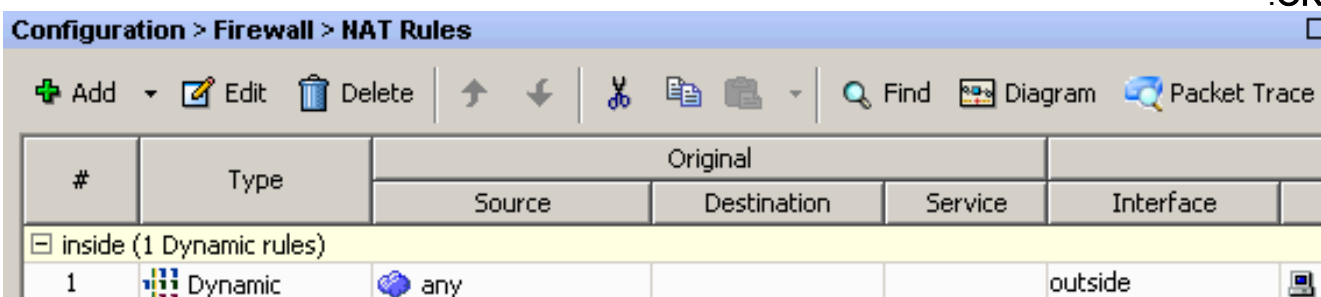
9. تكوين NAT. اخترت تشكيل <جدار حماية> قاعدة nat إضافة حركي nat قاعدة لذلك الحركة مرور أن يأتي من الشبكة الداخلية يستطيع كنت ترجمت مع خارج عنوان 172.16.1.5.



وانقر

فوق OK. وانقر فوق

OK.



طقطقة يطبق. CLI تشكيل مكافئ:

.10

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
```

تكوين ASA CLI

(Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
Saved :
:
(ASA Version 8.0(2
!
hostname ciscoasa
domain-name default.domain.invalid
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
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
domain-name default.domain.invalid
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 logging enable logging asdm informational
mtu inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0
```

```
The address pool for the Cisco AnyConnect SSL VPN ---!
Clients no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.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
```

```
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 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
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
    webvpn
    enable outside

Enable WebVPN on the outside interface svc image ---!
    disk0:/anyconnect-win-2.0.0343-k9.pkg 1

Assign an order to the AnyConnect SSL VPN Client ---!
    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 group-policy clientgroup internal

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

Specify SSL as a permitted VPN 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 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. svc ask none default svc

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

    Create a user account "ssluser1" tunnel-group ---!
    sslgroup type remote-access

    Create a tunnel group "sslgroup" with type as ---!
remote access 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 prompt ---!
    hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
#(ciscoasa(config)

```

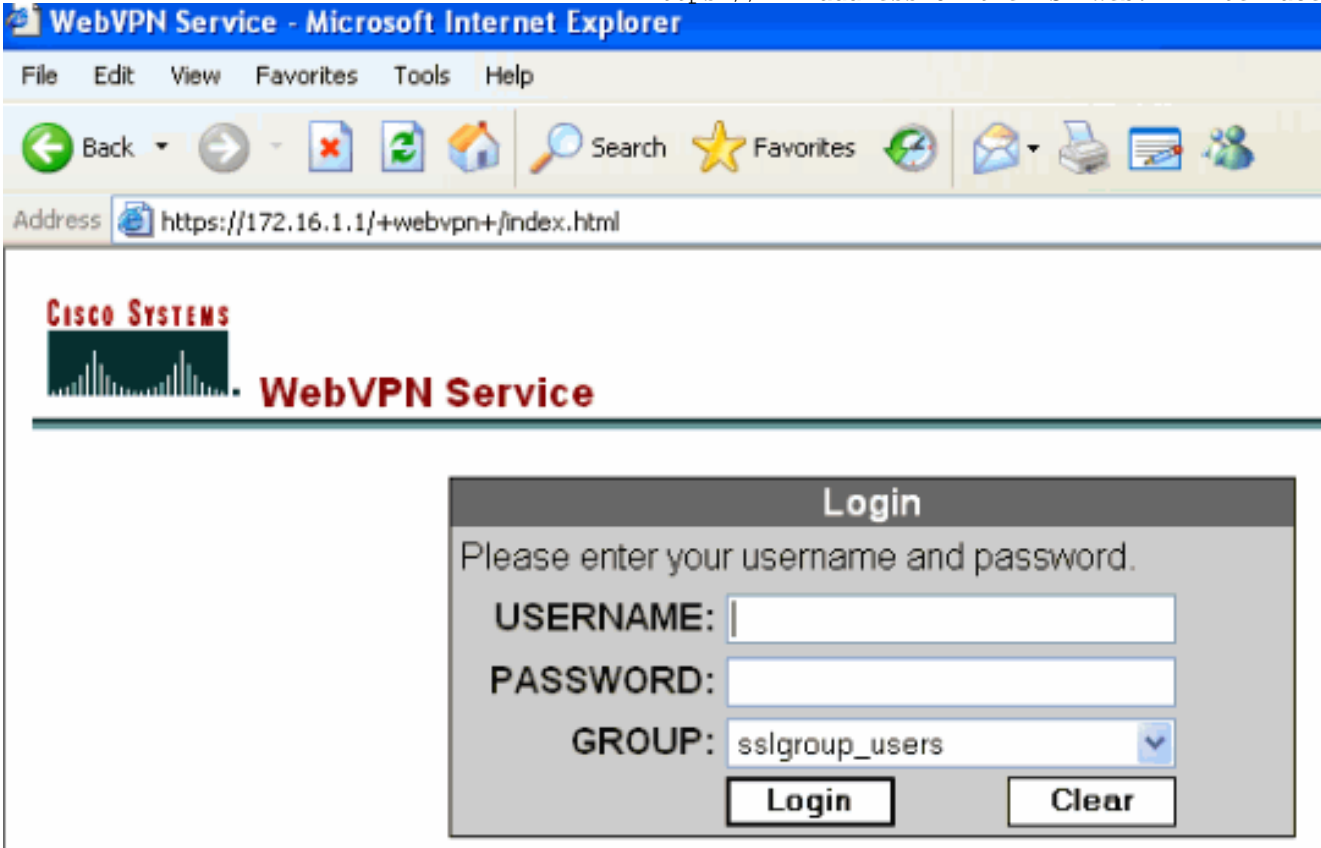
أتمت هذا steps in order to خلت SSL VPN توصيل مع ASA:

1. أدخل عنوان URL أو عنوان IP الخاص بواجهة WebVPN الخاصة بـ ASA في مستعرض الويب لديك بالتنسيق كما هو موضح.

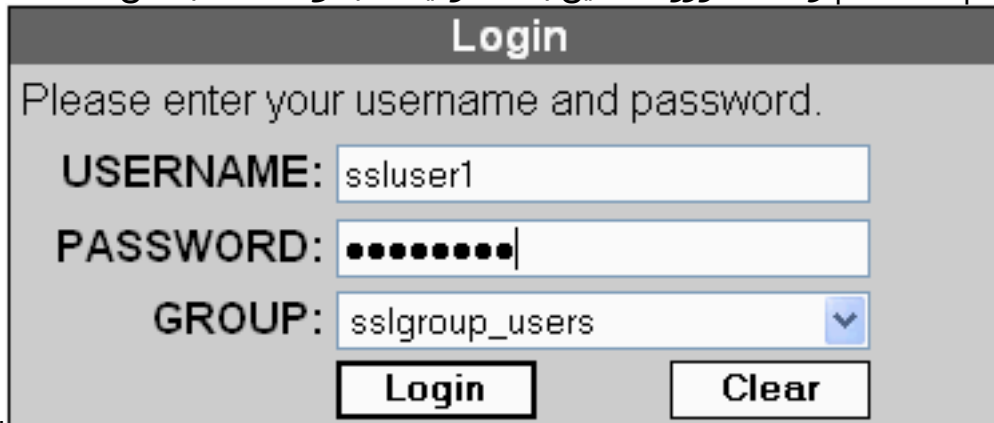
https://url

أو

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



2. أدخل اسم المستخدم وكلمة المرور الخاصين بك. أختار أيضا مجموعتك المقابلة من القائمة المنسدلة كما هو



يظهر هذا نافذة

موضح.

قبل أن ال SSL VPN أنشئت توصيل.



Cisco AnyConnect VPN Client



VPN Client Downloader



Please wait while the VPN connection is established.

Cancel



- Microsoft Java

- Sun Java

- Download

- Connected

Help

Cancel

ملاحظة: يجب تثبيت برنامج ActiveX في الكمبيوتر قبل تنزيل SVC. تتلقى هذا الإطار بمجرد تأسيس الاتصال.



Cisco AnyConnect VPN Client



WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Microsoft Java
- Sun Java
- Download
- Connected

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:

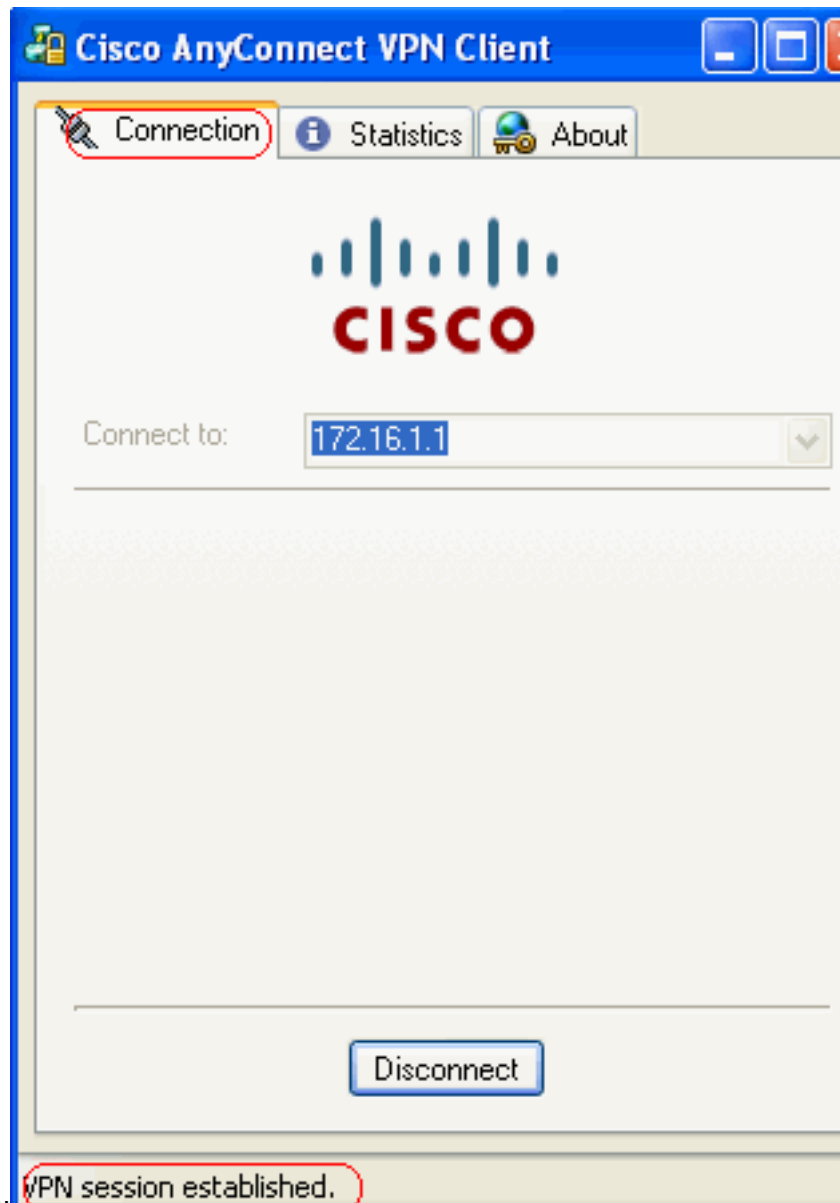


Help

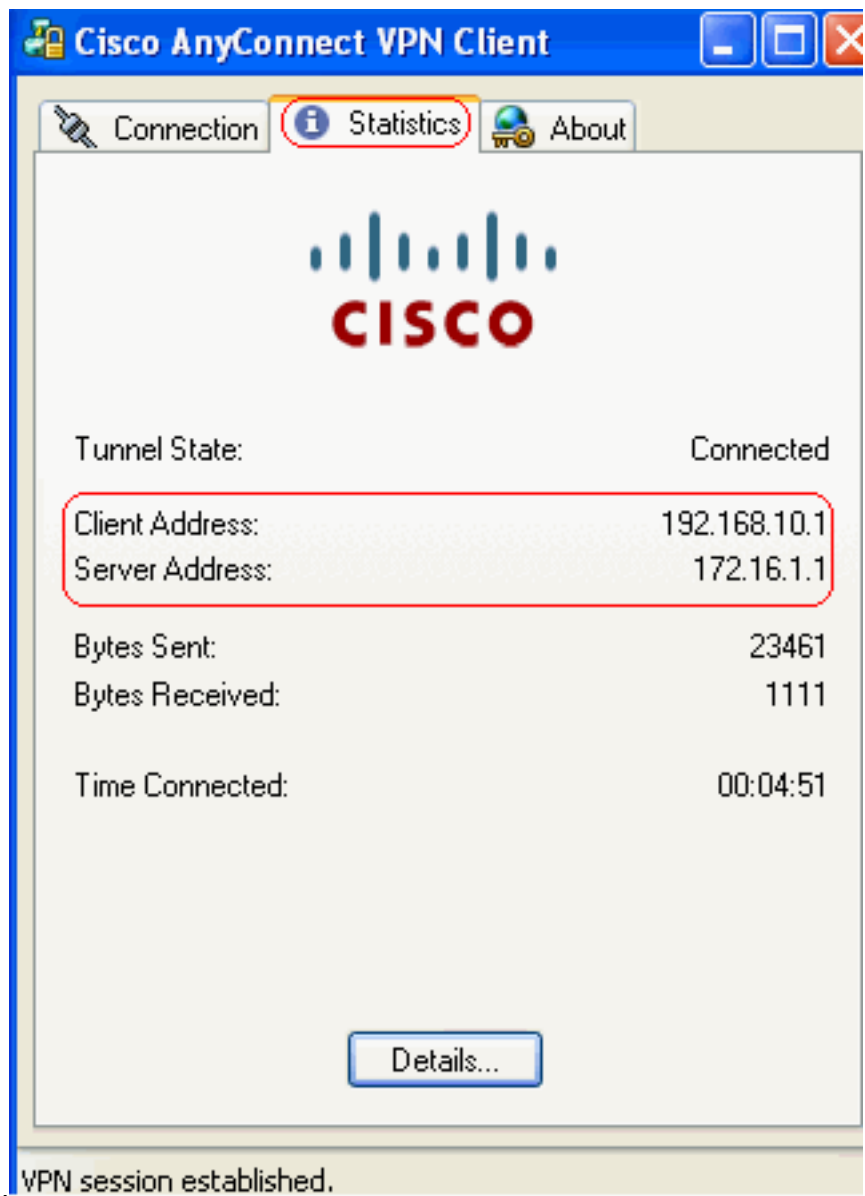
Cancel

Cisco AnyConnect
Connected

3. انقر فوق القفل الذي يظهر في شريط المهام



بالكمبيوتر. يظهر هذا الإطار ويوفر
معلومات حول اتصال SSL. على سبيل المثال، 192.168.10.1 هو عنوان IP المعين بواسطة ASA، وما إلى



بيدي هذا نافذة ال cisco

VPN session established.

ذلك.

AnyConnect VPN زبون صيغة



معلومة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرَج الأمر **show**.

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

```
ciscoasa#show webvpn svc
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 .1
+CISCO STC win2k
2,0,0343
Mon 04/23/2007 4:16:34.63
```

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 : 12

Assigned IP : 192.168.10.1 Public IP : 192.168.1.1
 Protocol : Clientless SSL-Tunnel DTLS-Tunnel
 Encryption : RC4 AES128 Hashing : SHA1
 Bytes Tx : 194118 Bytes Rx : 197448
 Group Policy : clientgroup Tunnel Group : sslgroup
 Login Time : 17:12:23 IST Mon Mar 24 2008
 Duration : 0h:12m:00s
 NAC Result : Unknown
 VLAN Mapping : N/A VLAN : none

- **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، أختبرت VPN>VPN>monitore>إحصاء>جلسة in order to عرفت الحالي WebVPN جلسة في ال .ASA

Monitoring > VPN > VPN Statistics > Sessions

Sessions

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
		Clientless	With Client	Total		
0	0	0	0	0	0	0

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

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
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1
```

```
!ciscoasa#Called vpn_remove_uauth: success
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
(np_svc_destroy_session(0xB000
```

2. **ملاحظة:** إذا انتقل الكمبيوتر إلى وضع الاستعداد أو الإسبات، يمكن إنهاء اتصال SSL VPN. بالمثل، يمكنك استخدام الأمر **vpn-sessiondb logoff svc** لإنهاء جميع جلسات عمل SVC.

```
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, e
(tc
!Called vpn_remove_uauth: success
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
(np_svc_destroy_session(0xA000
```

```

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

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 AnyConnect VPN Client 2, 0, 0343...
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
'
'Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343
()webvpn_cstp_parse_request_field
input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B...
'7D75F4EDEF26
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
'625B92C1338D631B08B7D75F4EDEF26
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
'08B7D75F4EDEF26
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
'5F4EDEF26
()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: 'X-CSTP-MTU: 1206...
'Processing CSTP header line: 'X-CSTP-MTU: 1206
()webvpn_cstp_parse_request_field
'input: 'X-CSTP-Address-Type: IPv4...
'Processing CSTP header line: 'X-CSTP-Address-Type: IPv4
()webvpn_cstp_parse_request_field
input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40...
'642E22C6AF9B9501758FF3B7B5545973C06F6393C92E59693
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
'BAC12031550B1812D40642E22C6AF9B9501758FF3B7B5545973C06F6393C92E59693
()webvpn_cstp_parse_request_field
'input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA...
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
'SHA:DES-CBC-SHA-
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
(np_svc_create_session(0x3000, 0xD41611E8, TRUE
webvpn_svc_np_setup
SVC ACL Name: NULL

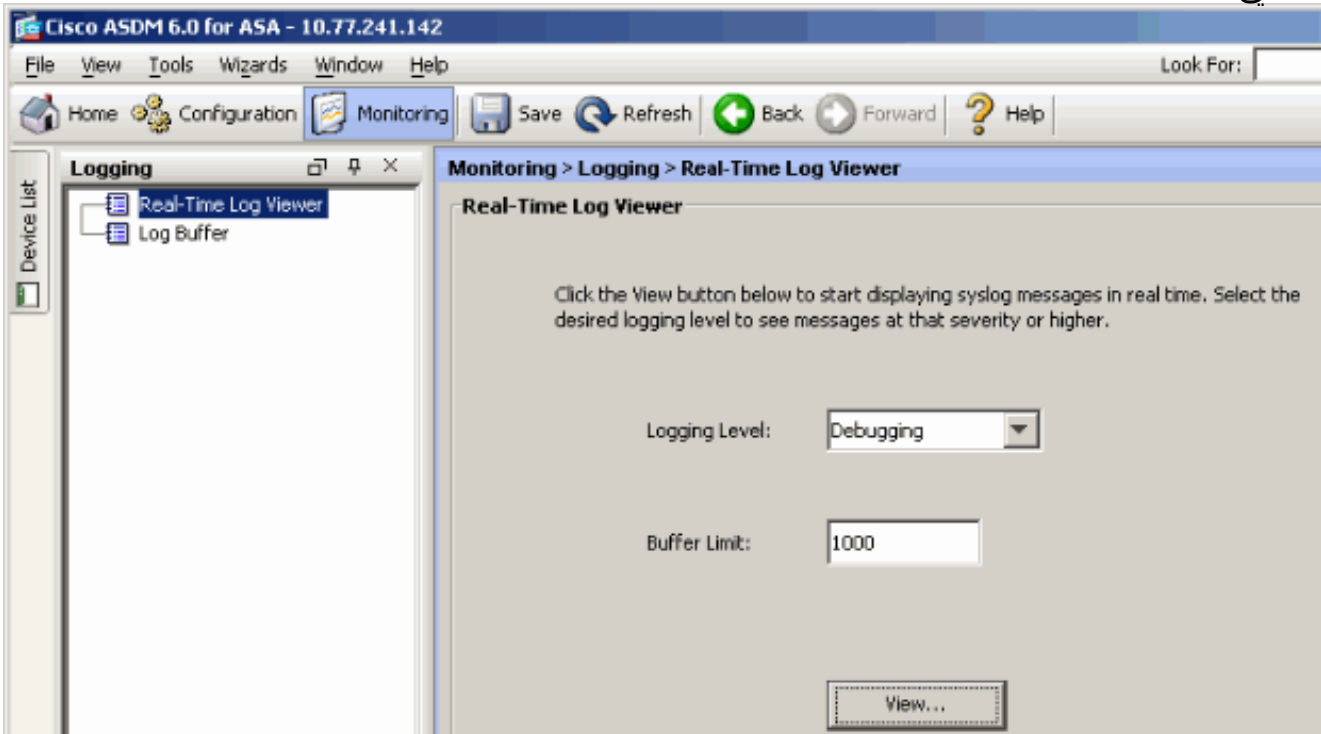
```

```

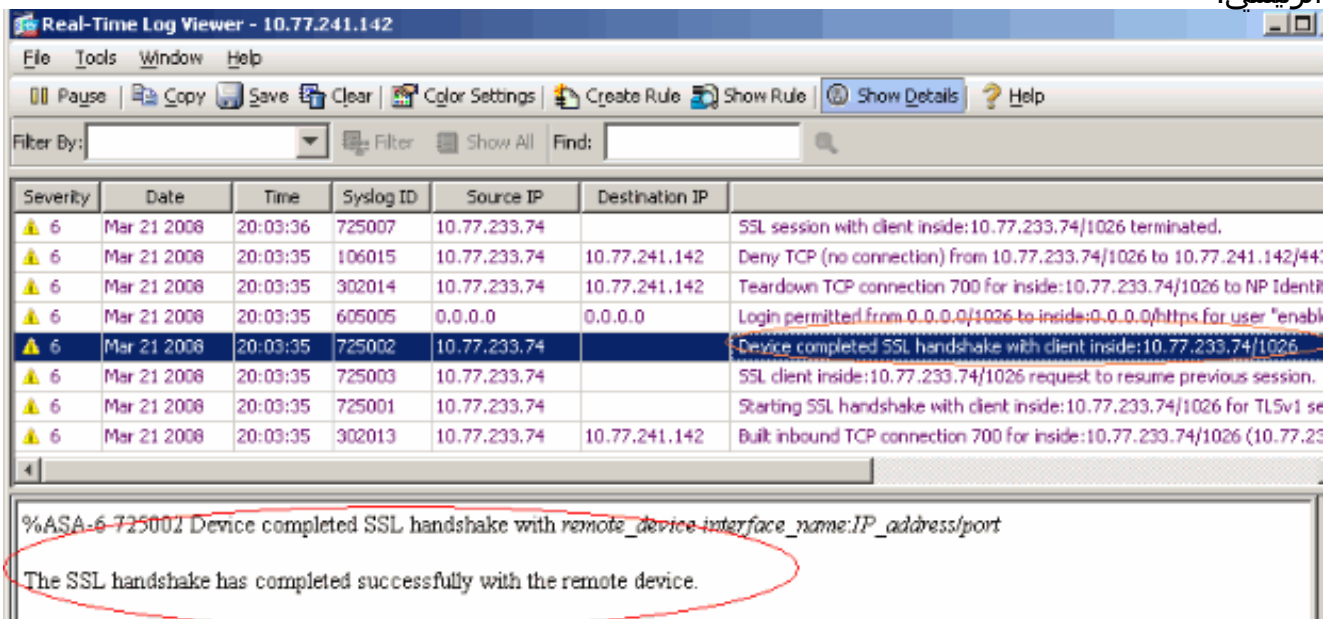
SVC ACL ID: -1
SVC ACL ID: -1
!vpn_put_uauth success
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy

```

4. في ASDM، أختبر مراقبة < تسجيل < عارض السجل في الوقت الفعلي < عرض لعرض الأحداث في الوقت الفعلي.



يوضح هذا المثال أنه تم إنشاء جلسة عمل SSL باستخدام جهاز الطرف الرئيسي.



[معلومات ذات صلة](#)

- [صفحة دعم جهاز الأمان القابل للتكيف طراز Series 5500 من Cisco](#)
- [ملاحظات الإصدار الخاصة بعميل AnyConnect VPN، الإصدار 2.0](#)
- [ASA/PIX: السماح بنفقي انقسام لعملاء VPN على مثال تكوين ASA](#)
- [يسمح الموجه لعملاء VPN بتوصيل IPsec والإترنت باستخدام مثال تكوين انقسام الاتصال النفقي](#)
- [عمل PIX/ASA 7.x و VPN لشبكة VPN العامة عبر الإترنت على مثال تكوين العصا](#)
- [SSL VPN Client \(SVC\) على ASA مع مثال تكوين ASDM](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل