تكوين حركة مرور بيانات AnyConnect VPN Client U-turn على ASA 9.x

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد إصدار 9.x من جهاز الأمان القابل للتكيف (ASA) من Cisco للسماح له بتوجيه حركة مرور الشبكة الخاصة الظاهرية (VPN). وهو يغطي سيناريو التكوين التالي: إعادة توجيه حركة المرور من عملاء الوصول عن بعد.

> **ملاحظة**: لتجنب تداخل عناوين IP في الشبكة، قم بتعيين مجموعة مختلفة تمامًا من عناوين IP إلى عميل VPN (على سبيل المثال، 10.x.x.x و 172.16.x.x و 192.168.x.x). يعد نظام عنونة IP هذا مفيدًا لاستكشاف أخطاء الشبكة وإصلاحها.

مسمار شعر أو دوران U

هذه سمة مفيدة لحركة مرور VPN أن يدخل قران، غير أن بعد ذلك وجهت خارج أن القران نفسه. حيث تدعم تقنية التوصيل المحوري شبكة شبكة VPN، إذا كانت لديك شبكة على سبيل المثال، فلكي تتصل أحد العملاء بحركة مرور بيانات أخرى يتم التحدث بها، يجب أن ينتقل إلى جهاز الأمان ثم يخرج من جديد إلى الشبكة الأخرى التي يتم التحدث بها.

أدخل **same-security-traffic** أمر in order to سمحت حركة مرور أن يدخل ويخرج ال نفسه قارن.

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

المتطلبات الأساسية

المتطلبات

cisco يوصي أن أنت تستوفي هذا متطلب قبل أن أنت تحاول هذا تشكيل:

- يحتاج جهاز أمان Hub ASA إلى تشغيل الإصدار 9.x.
- عميل AnyConnect VPN 3.x من Cisco**ملاحظة**: قم بتنزيل حزمة عميل AnyConnect VPN (anyconnect-win*.pkg) من [برنامج تنزيل](#) Cisco (للعملاء المسجلين فقط). انسخ عميل AnyConnect VPN إلى ذاكرة Cisco ASA Flash، والتي يجب تنزيلها إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع قسم [اتصالات عميل AnyConnect VPN](#) 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 9.1(2)
- إصدار عميل AnyConnect SSL VPN من Cisco لنظام التشغيل Windows 3.1.05152
- جهاز كمبيوتر يقوم بتشغيل نظام تشغيل مدعوم لكل [أنظمة VPN الأساسية المدعومة، سلسلة Cisco ASA](#).
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 7.1(6)

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

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

.بعد إدخال عنوان URL، يتصل المستعرض بتلك الواجهة ويعرض شاشة تسجيل الدخول. إذا استوفى المستخدم لجس الدخول والمصادقة، وحدد جهاز الأمان المستخدم على أنه في حاجة إلى 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 (يعتمد ذلك على تكوين جهاز الأمان) عند إنهاء الاتصال.في حالة عميل تم تثبيته مسبقا، 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 بأمان طبقة النقل (TLS)، ويستخدم أيضا أمان طبقة النقل (DTLS) لمخطط البيانات. تتجنب DTLS مشاكل زمن الوصول والنطاق الترددي المقترنة ببعض إتصالات SSL وتحسن أداء تطبيقات الوقت الفعلي الحساسة لتأخيرات الحزم.يمكن تنزيل عميل AnyConnect من جهاز الأمان أو يمكن

تتبيثه ويدوي ايودي على الكمبيوتر البعيد بواسطة مسؤول النظام. لمزيد من المعلومات حول كيفية تثبيت العميل يدويا، ارجع إلى [دليل مسؤول Cisco AnyConnect Secure Mobility Client](#).يقوم جهاز الأمان بتنزيل العميل استنادا إلى نهج المجموعة أو سمات اسم المستخدم الخاصة بالمستخدم الذي يقوم بإنشاء الاتصال. يمكنك تكوين جهاز الأمان لتنزيل العميل تلقائيا، 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.**ملاحظة:** تستخدم الأمثلة المستخدمة في هذا المستند IPv4. بالنسبة لحركة مرور IPv6 التي يتم تحويلها إلى وحدة، تكون الخطوات هي نفسها ولكن أستخدم عناوين IPv6 بدل من IPv4.

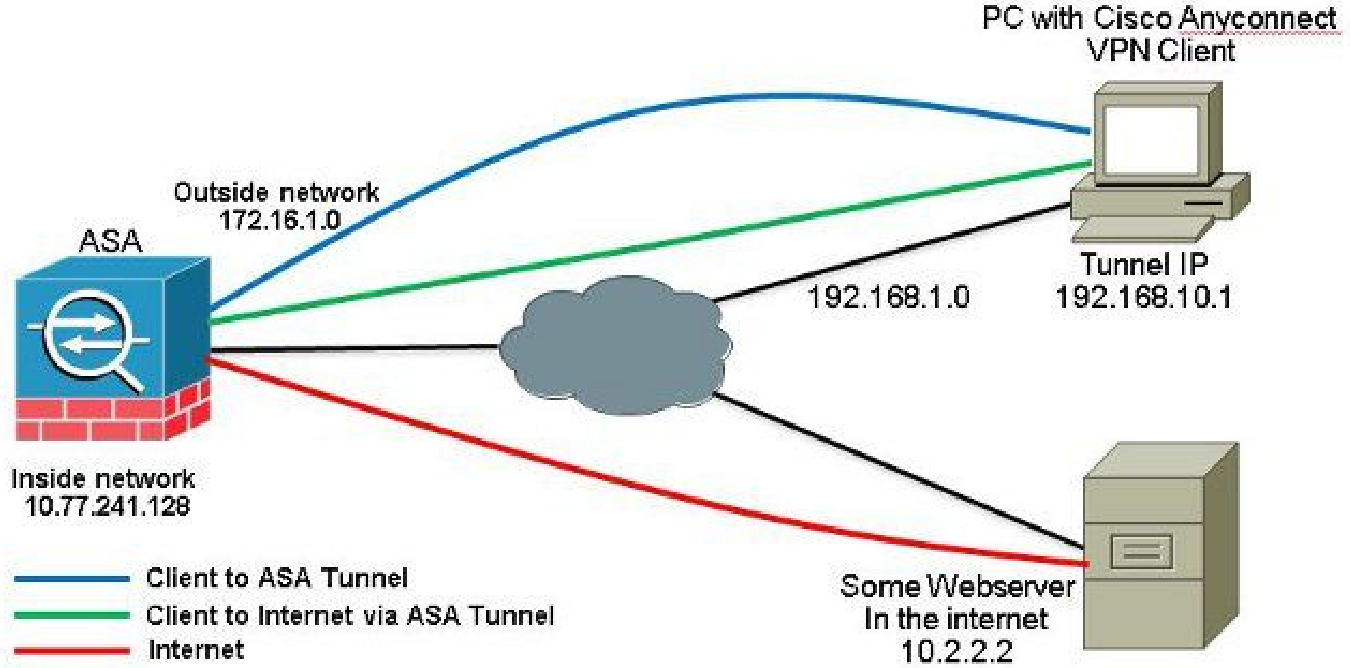
تكوين حركة مرور الوصول عن بعد للتحويل إلى وحدة

في هذا المسم، تٌقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.ملاحظة: استخدم أداة [البحث عن الأوامر](#) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تكوين ASA على AnyConnect VPN Client for Public Internet VPN

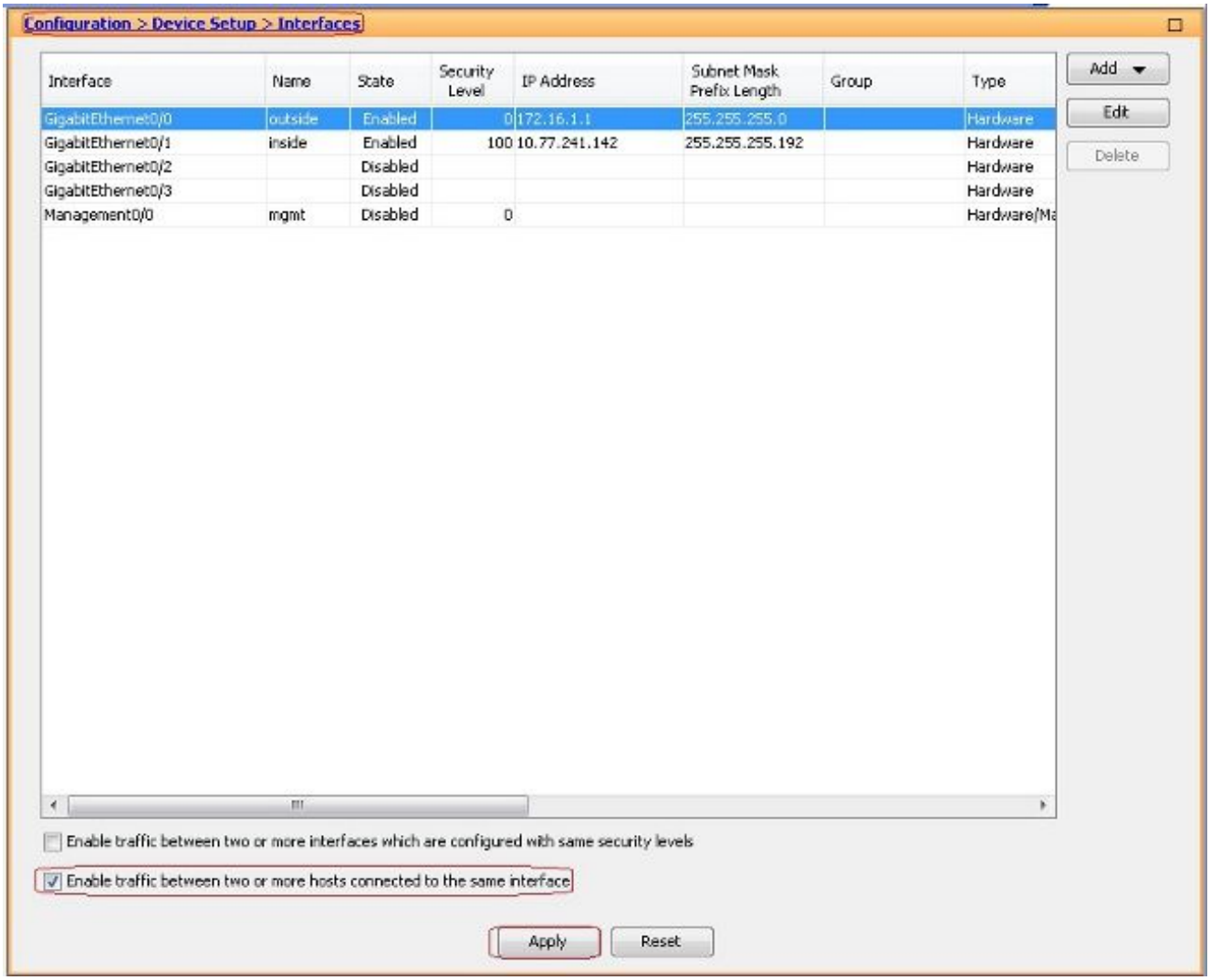
الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوينات ASA الإصدار 9.1(2) مع ASDM الإصدار 7.1(6)يفترض هذا المستند أن التكوين الأساسي، مثل تكوين الواجهة، قد تم إكماله بالفعل ويعمل بشكل صحيح.ملاحظة: ارجع إلى [إدارة الوصول إلى تكوين](#) للسماح بتكوين ASA بواسطة ASDM.ملاحظة: في الإصدار 8.0(2) والإصدارات الأحدث، يدعم ASA كل من جلسات SSL VPN (WebVPN) الخالية من العملاء وجلسات الإدارية ل ASDM في آن واحد على المنفذ 443 من الواجهة الخارجية. في الإصدارات الأقدم من الإصدار 8.0(2)، لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. ارجع [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:

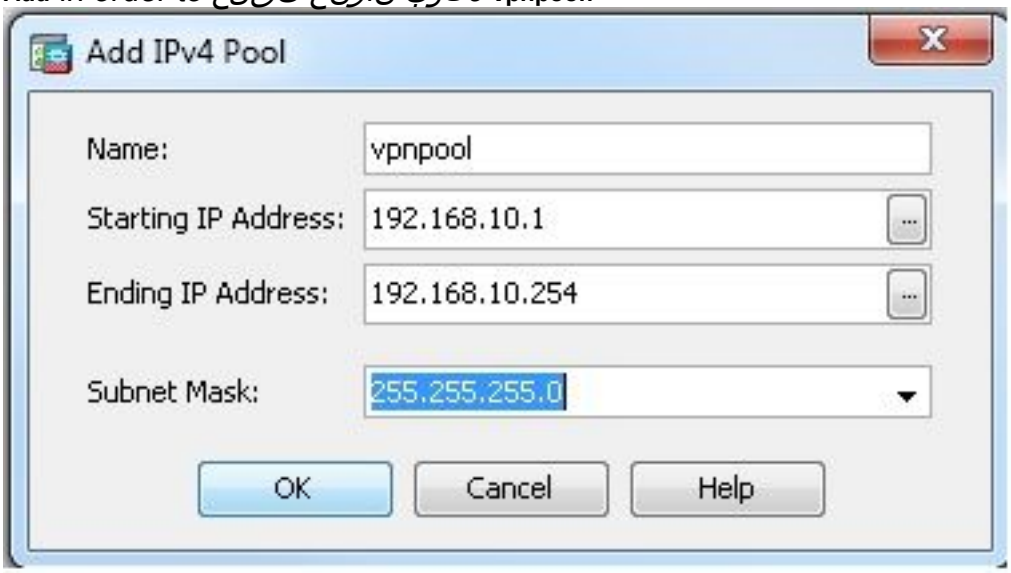
1. اختار **Configuration > Device Setup > Interfaces** وتحقق من **Enable traffic between two or more hosts connected to the same interface** خانة الاختيار للسماح لحركة مرور SSL VPN بالدخول نفس الواجهة والخروج منها. انقر **Apply**.



CLI تشكيل مكافئ:

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

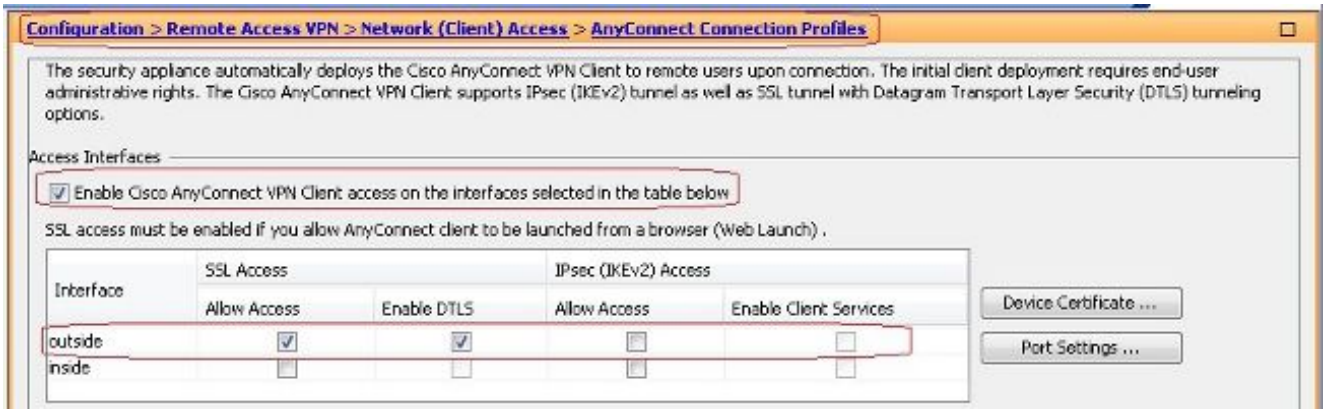
2. *راتخن* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *in order to قلخ عونان برك* **vpnpool**.



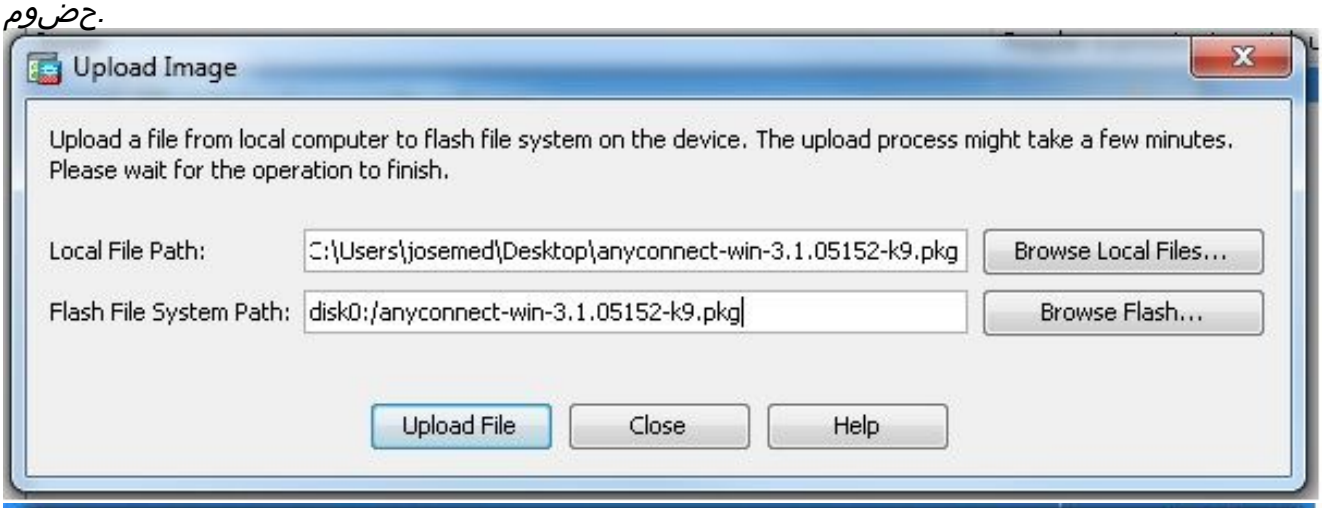
3. *انقر* **Apply**. *CLI تشكيل مكافئ:*

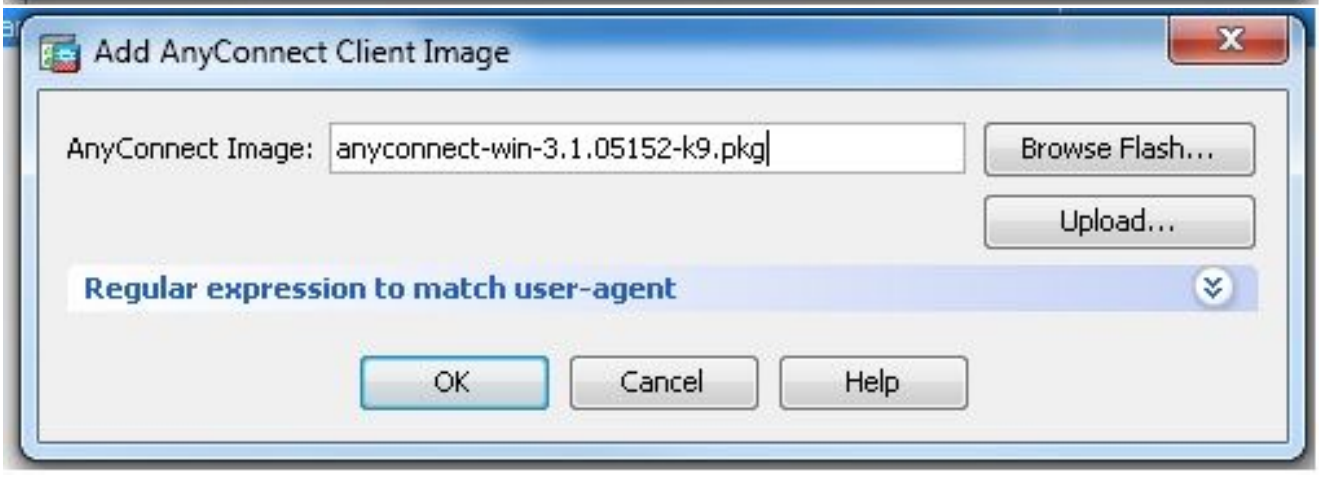
```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

4. *تمكين WebVPN.* *راتخن* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *وتحت* **Access Interfaces**، *انقر مربعات التأشير* **Allow Access** *و* **Enable DTLS** *للواجهة الخارجية. تحقق أيضا من* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *خانة الاختيار لتمكين SSL VPN على الواجهة الخارجية.*



انقر **Apply**.*اختر* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software** > **Add** *إلى إضافة حزم عميل Cisco AnyConnect VPN من ذاكرة Flash الخاصة بـ ASA كما هو موضح.*

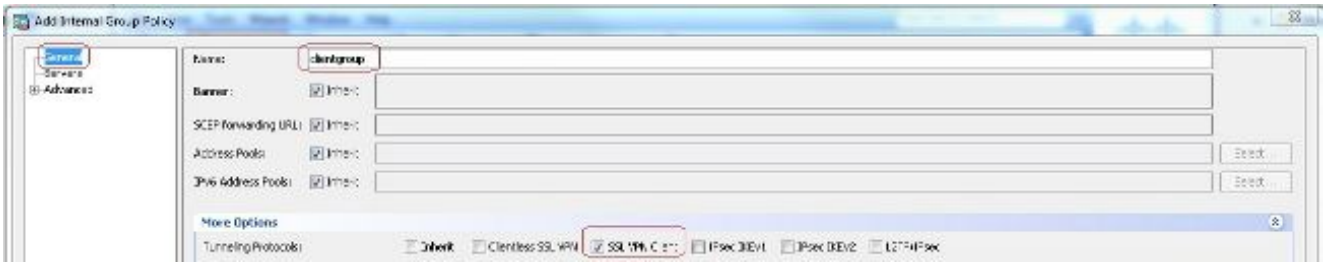




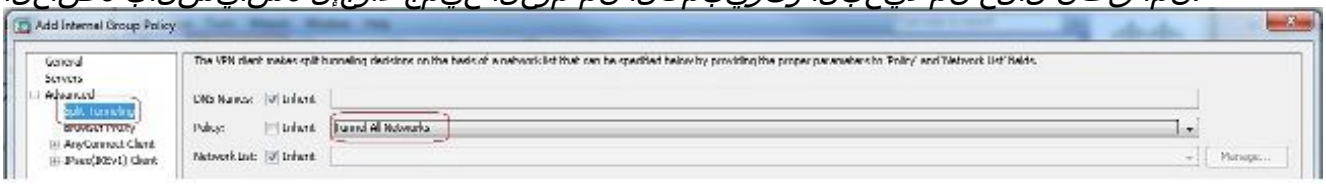
تشكيل CLI مكافئ:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

5. *تكوين مجموعة النفق.* *اختر* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *إلى إنشاء سياسة مجموعة داخلية* **clientgroup**. *تحت* **General** *علامة التبويب، حدد* **SSL VPN Client** *لتمكين WebVPN كبروتوكول نفق.*



في **Advanced > Split Tunneling** جدول، إختر **Tunnel All Networks** من القائمة المنسدلة "النهج" الخاصة بالسياسة لإجراء جميع الحزم من الكمبيوتر البعيد من خلال نفق آمن.



CLI تشكيل مكافئ:

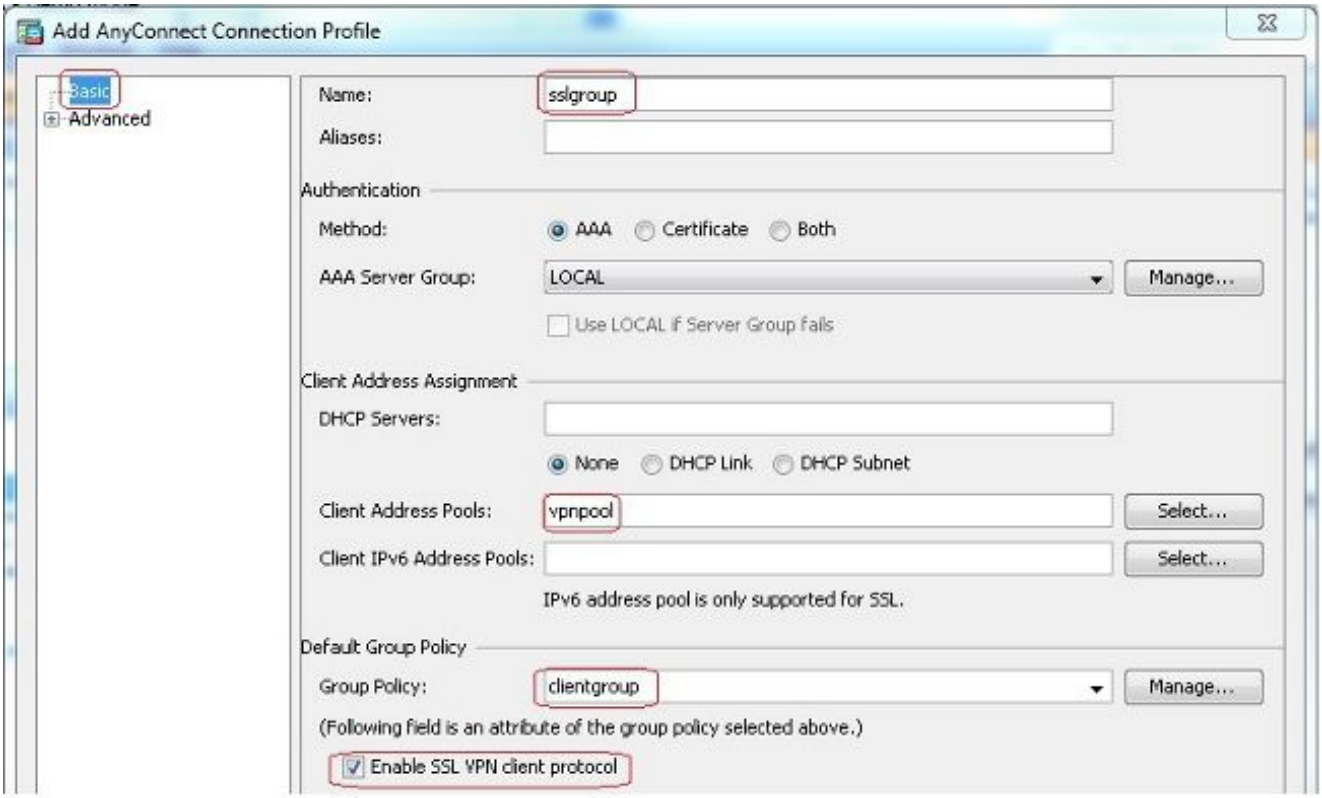
```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policyclientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelall
```

6. اختر **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** لإنشاء حساب مستخدم جديد **ssluser1**. انقر **OK** ومن ثم **Apply**.

CLI تشكيل مكافئ:

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

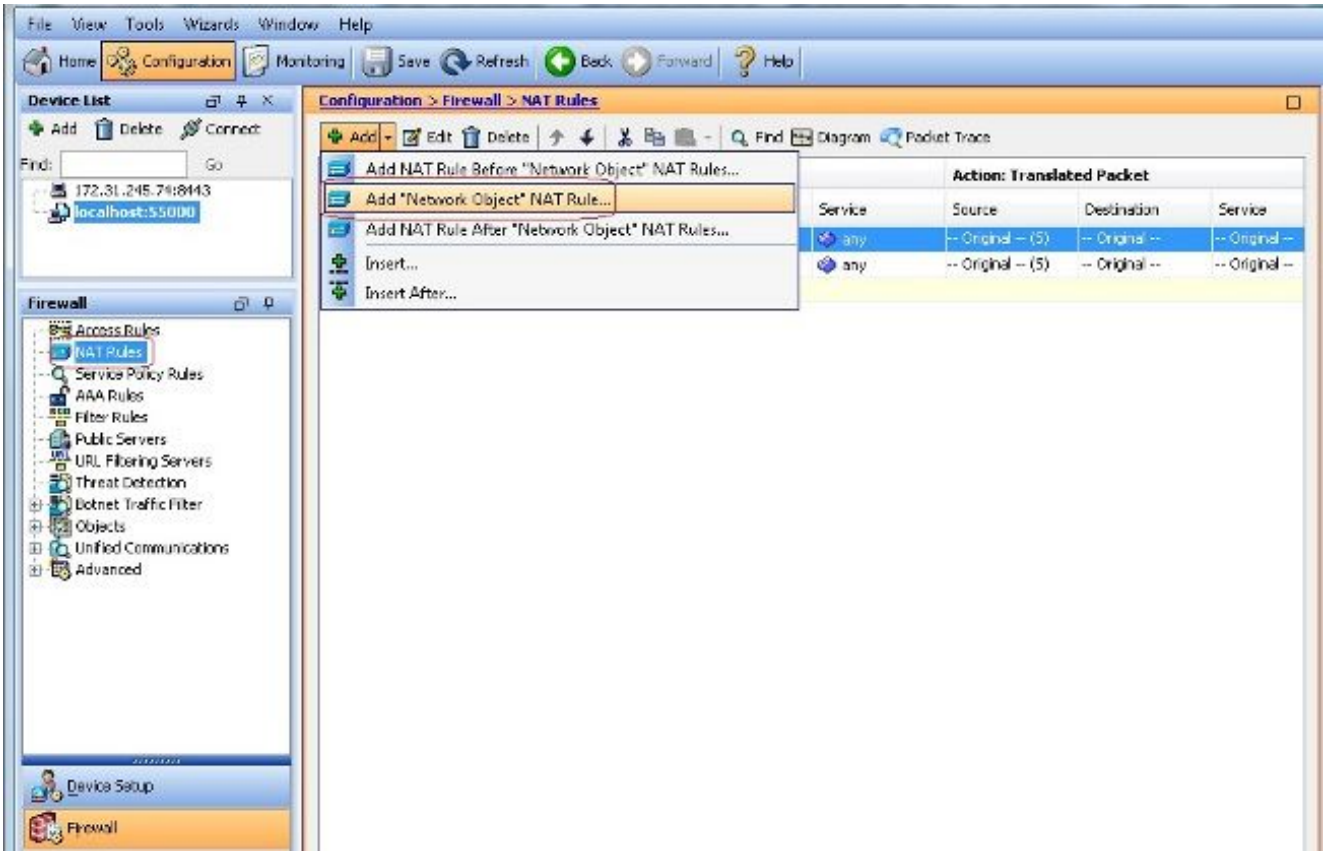
7. اختر **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** لإنشاء مجموعة نفق جديدة **sslgroup**.في **Basic** عالمة التبويب، يمكنك تنفيذ المهام التالية: تسمية مجموعة النفق **sslgroup**.تحت **Client Address Assignment**، أختر تجمع العناوين **vpnpool** من **Client Address Pools** المسمى **clientgroup** من **Group Policy**، أختر نهج المجموعة **Default Group Policy**.تحت قائمة المنسدلة.

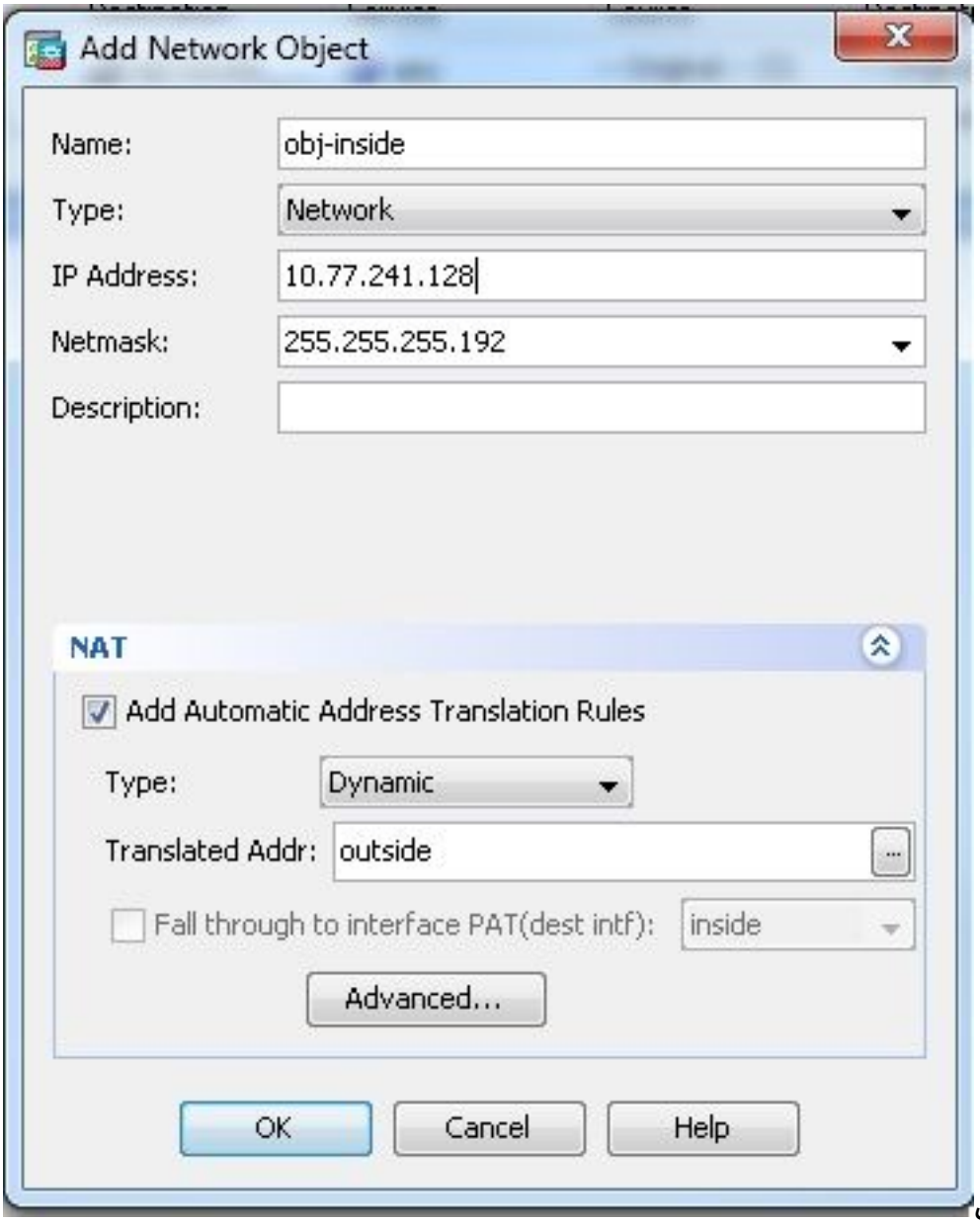


تحت **Advanced > Group Alias/Group URL** عالمة التبويب، قم بتعيين اسم المجموعة المستعار **sslgroup_users** وانقر فوق **OK**. ***CLI تشكيل مكافئ:***

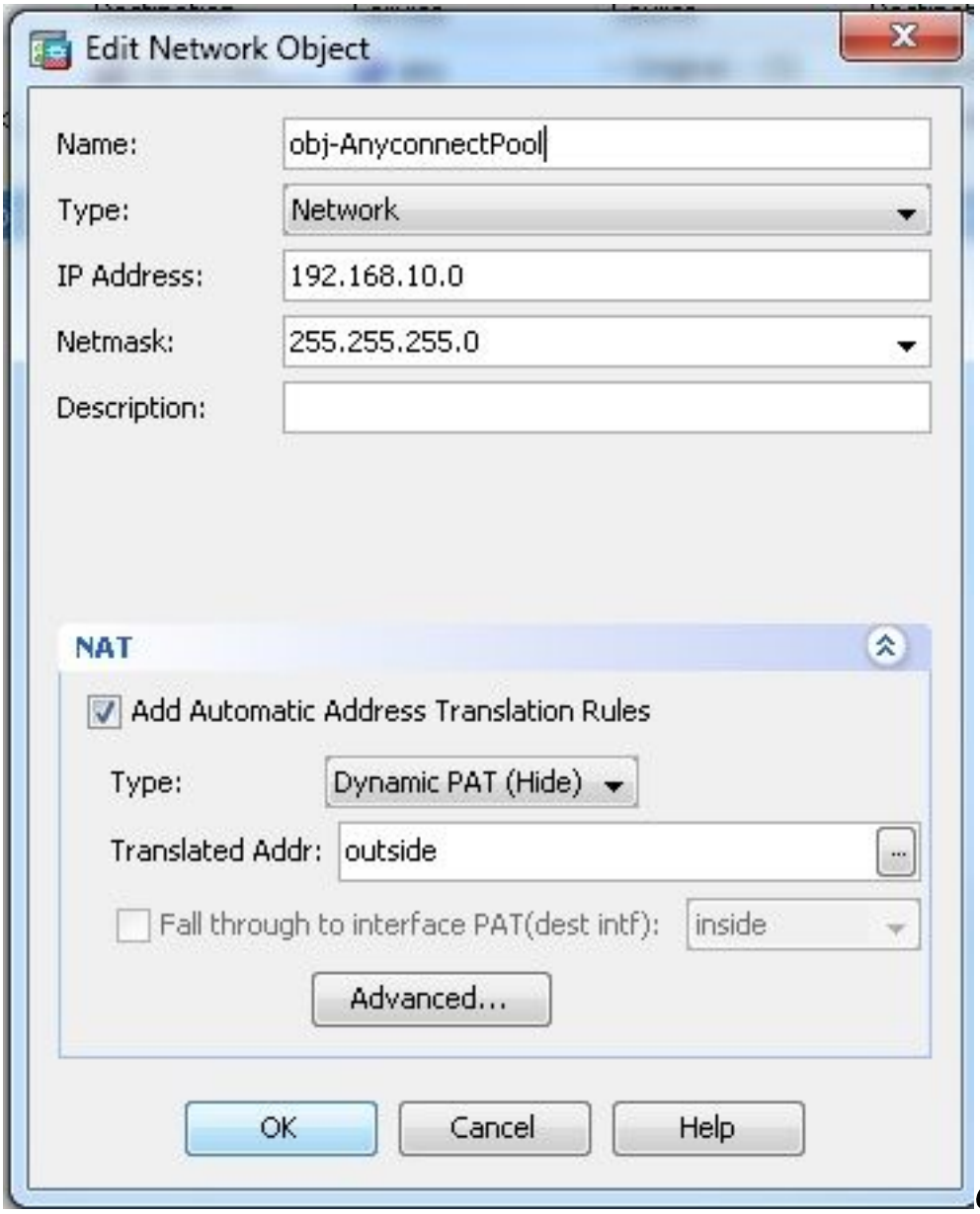
```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

8. تكوين NAT نافذ الحركة **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** لذلك يمكن ترجمة حركة المرور التي تأتي من الشبكة الداخلية باستخدام عنوان IP الخارجي 172.16.1.1.


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
Find: Go
172.31.245.71:8443
localhost:55000
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Add NAT Rule Before "Network Object" NAT Rules...
Add "Network Object" NAT Rule...
Add NAT Rule After "Network Object" NAT Rules...
Insert...
Insert After...
Action: Translated Packet
Service
Source
Destination
Service
any
-- Original -- (5)
-- Original --
-- Original --
any
-- Original -- (5)
-- Original --
-- Original --



راتخن **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *ذلك يمكن ترجمة حركة مرور بيانات VPN التي تأتي من الشبكة الخارجية باستخدام عنوان IP الخارجي 172.16.1.1.*



CLI تشكيل مكافئ:

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

CLI في تشكيل (2)9.1 رادصإلا ASA

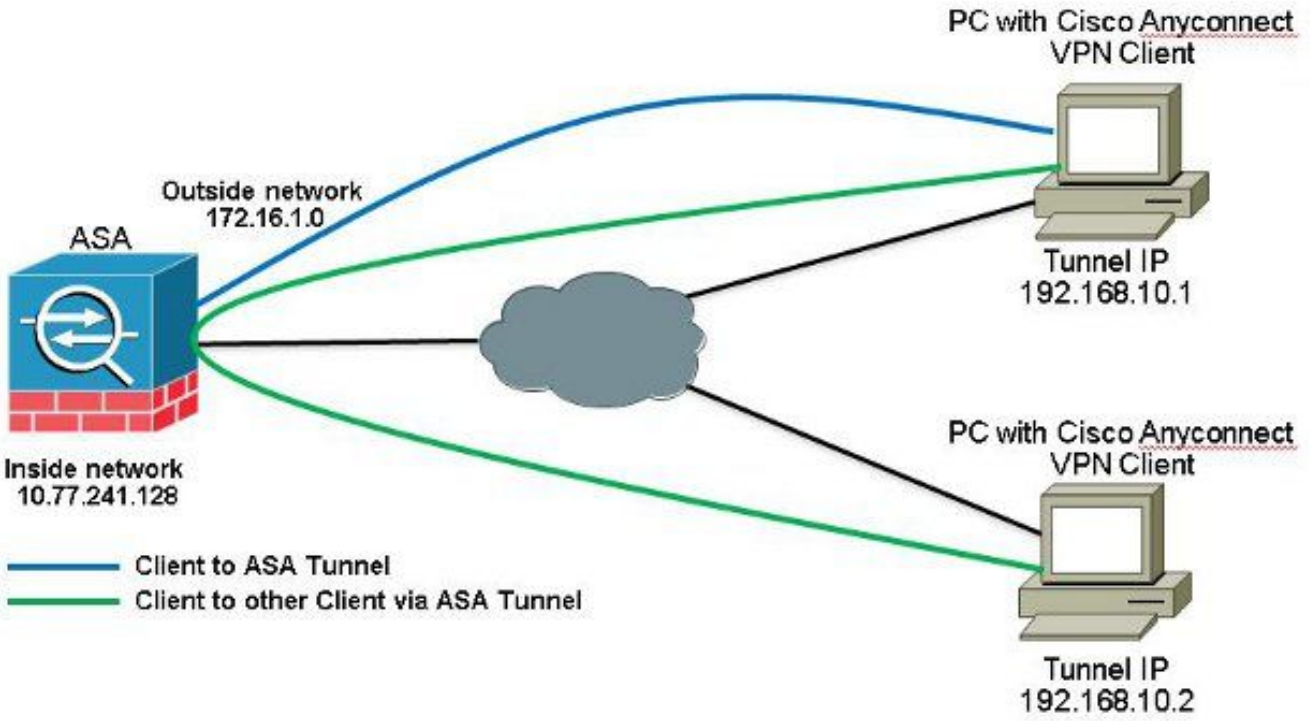
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
```

```
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated
when going to the Anyconnect Pool.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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
```

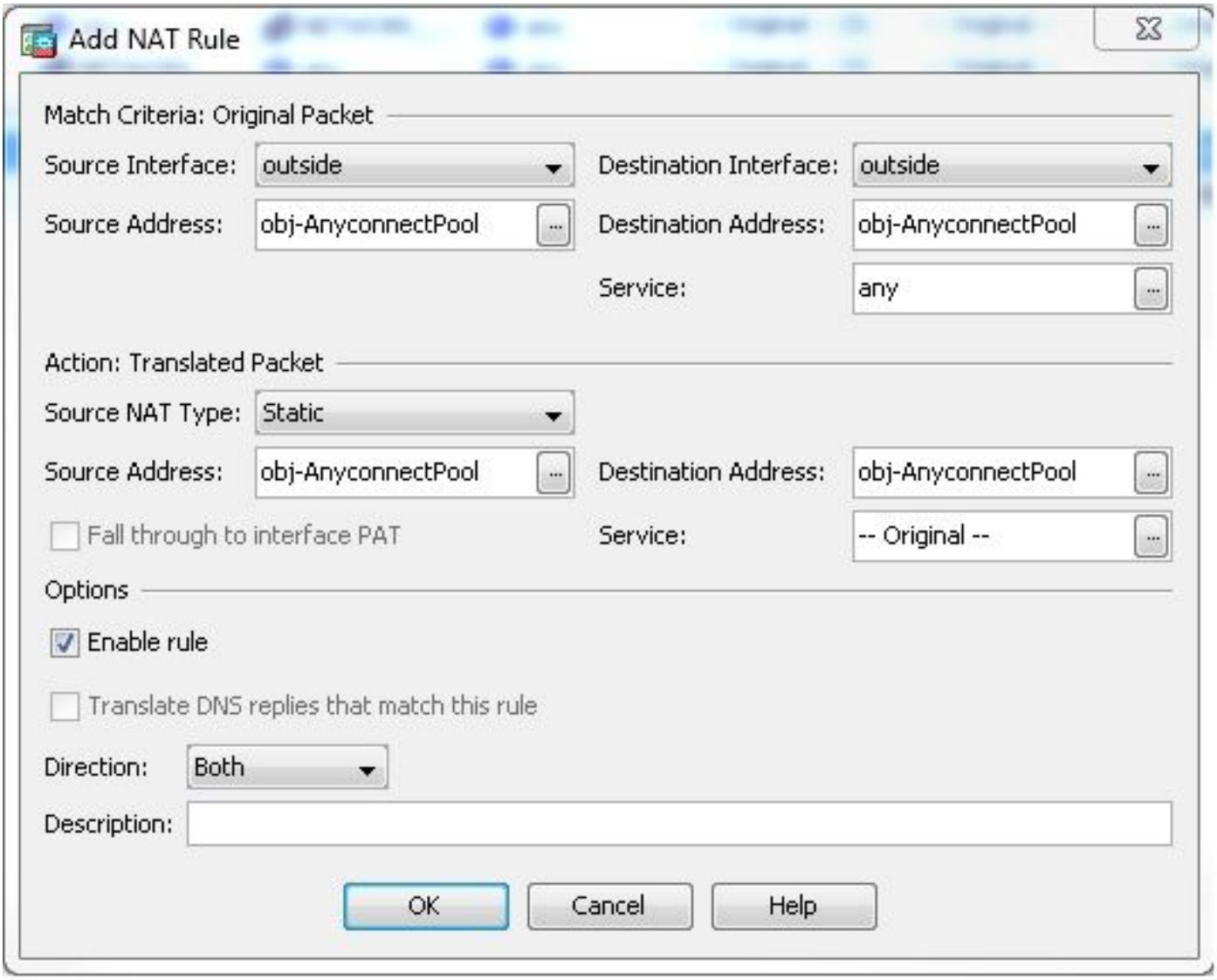
```
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection 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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

السماح بالاتصال بين عملاء AnyConnect VPN مع تكوين TunnelAll في موضع الرسم التخطيطي للشبكة



إذا كان الاتصال بين عملاء AnyConnect مطلوبا وكان NAT الخاص بشبكة الإنترنت العامة على عصا متوفرا، يلزم أيضا وجود NAT يدوي للسماح بالاتصال ثنائي الاتجاه.هذا سيناريو شائع عندما يستخدم عملاء AnyConnect خدمات الهاتف ويجب أن يكونوا قادرين على الاتصال ببعضهم البعض.تكوينات ASA الإصدار 9.1(2) مع ASDM الإصدار 7.1(6) واختر Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules لذلك لا تتم ترجمة حركة المرور التي تأتي من الشبكة الخارجية (AnyConnect Pool) وتم توجيهها إلى عميل AnyConnect آخر من نفس التجمع مع عنوان IP الخارجي 172.16.1.1.



CLI تشكيل مكافئ:

```
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
```

ASA الإصدار 9.1(2) تشكيل في CLI

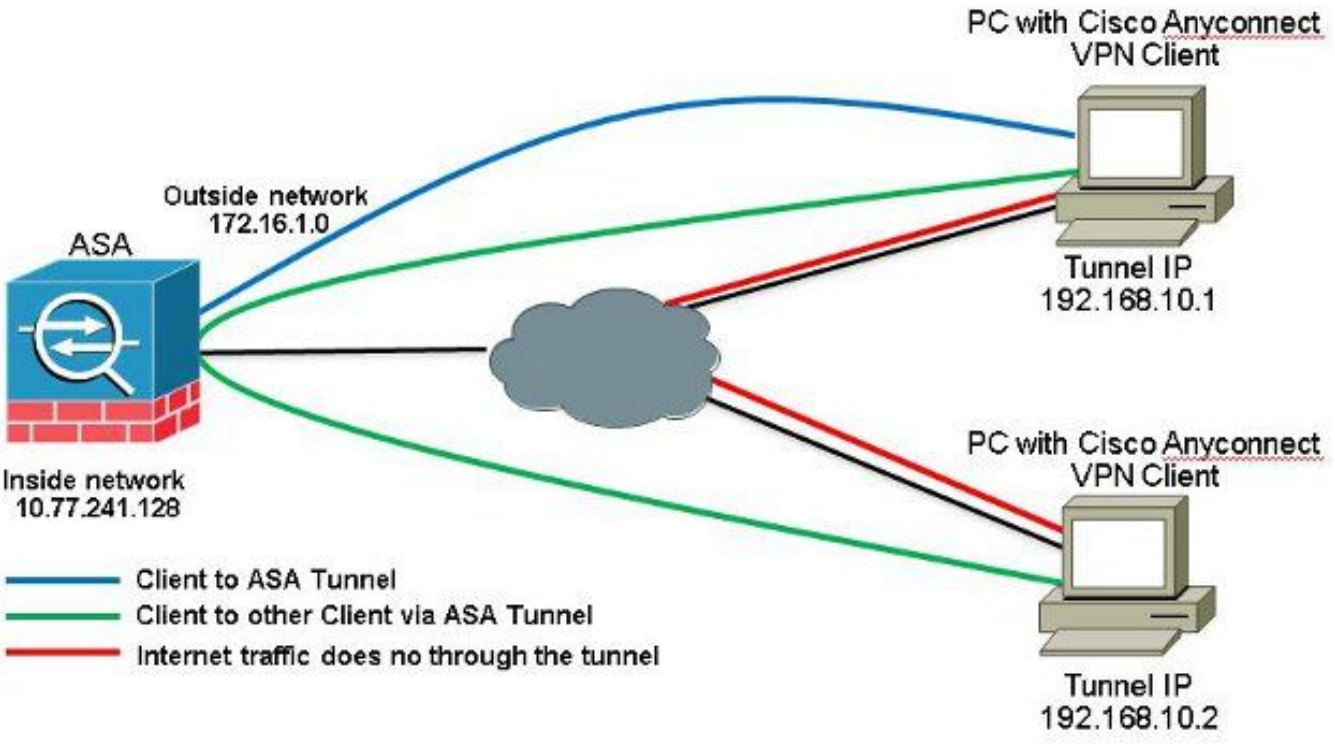
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool
destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network
destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined
to another Client within the same pool does not get translated.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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"
```

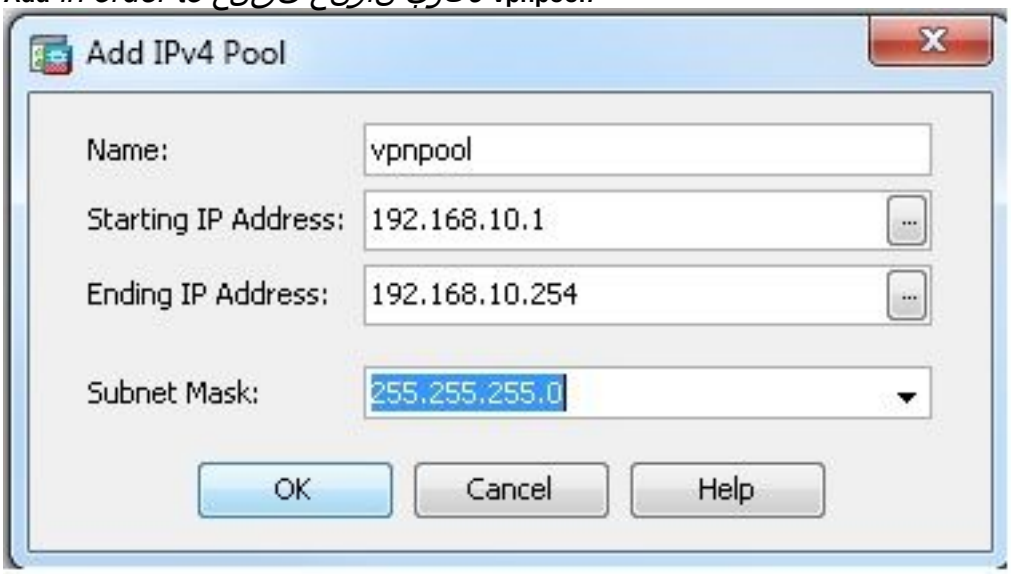
```
group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

السماح بالاتصال بين عملاء AnyConnect VPN باستخدام نفق انقسامالرسم التخطيطي للشبكة



إذا كان الاتصال بين عملاء AnyConnect مطلوبا وتم إستخدام تقنية Split-Tunnel، فلا يتطلب الأمر وجود NAT يدويا للسماح بالاتصال ثنائي الإتجاه إذا كانت هناك قاعدة NAT التي تؤثر على حركة المرور هذه التي تم تكوينها. ومع ذلك، يجب تضمين تجمع AnyConnect VPN على قائمة التحكم في الوصول (ACL) لذا النفق المقسم.هذا سيناريو شائع عندما يستخدم عملاء AnyConnect خدمات الهاتف ويجب أن يكونوا قادرين على الاتصال ببعضهم البعض.تكوينات ASA الإصدار 9.1(2) مع ASDM الإصدار 7.1(6)

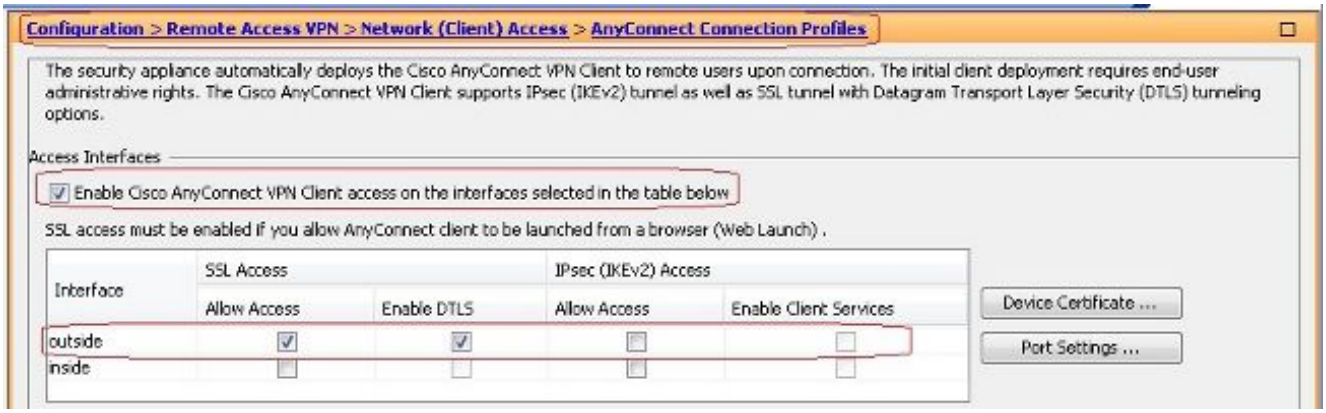
1. *تختار* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *in order to خلق عنوان بركة* **vpnpool**.



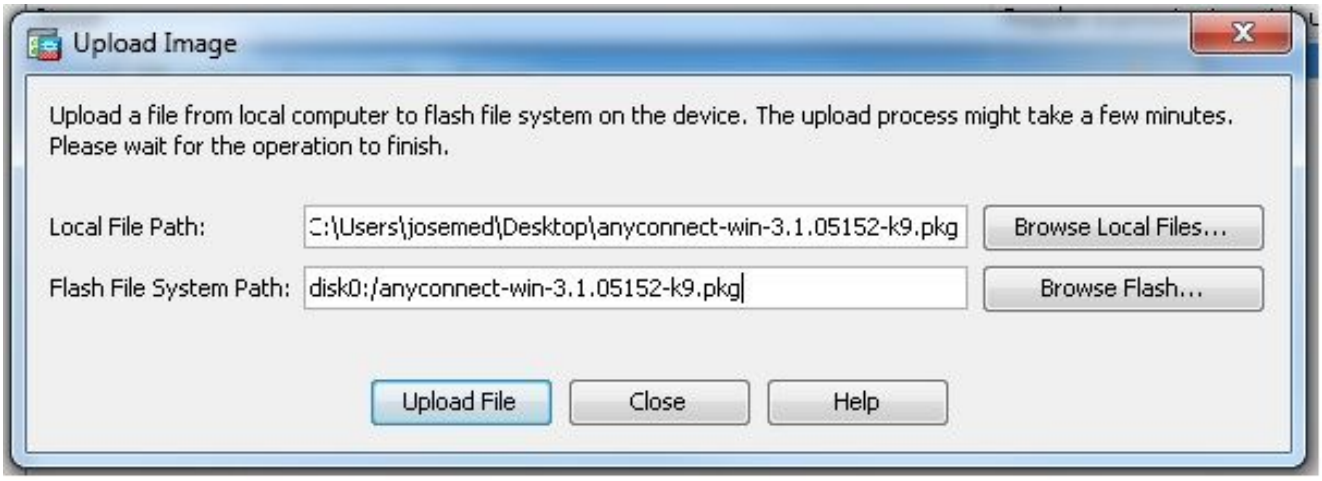
2. *انقر* **Apply**. ***CLI تشكيل مكافئ:***

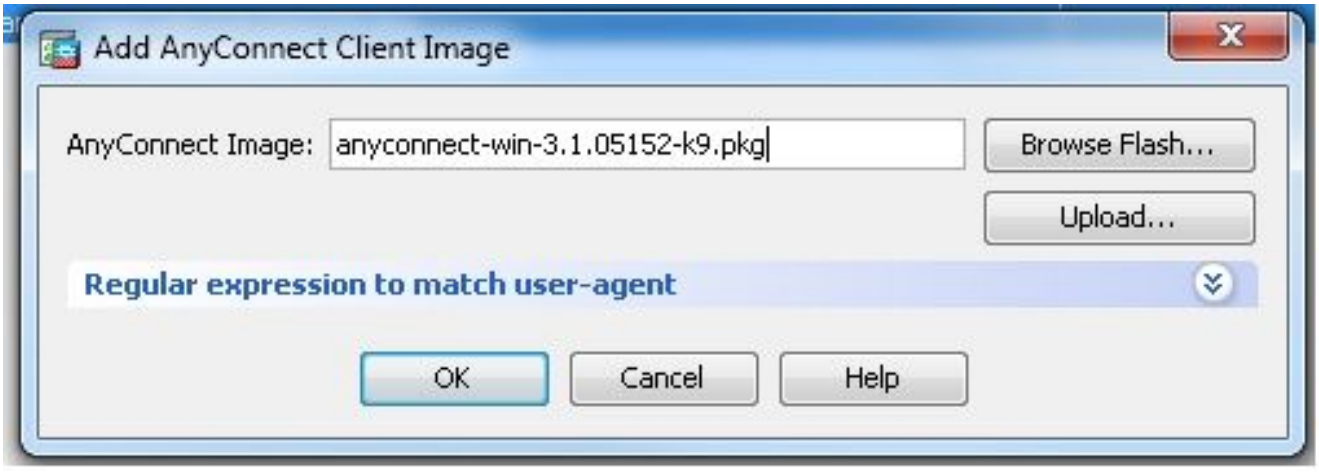
```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

3. *تمكين WebVPN. تختار* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *تحت* **Access Interfaces**، *انقر مربعات التأشير* **Allow Access** *و* **Enable DTLS** *للواجهة الخارجية. تحقق أيضا من* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *خانة الاختيار لتمكين SSL VPN على الواجهة الخارجية.*



انقر **Apply**.*اتخن* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software** *وه امك ب ASA ةصاخلا Flash ةركاذ نم Cisco AnyConnect VPN ليمع ةروص ةفاضإل* **Add** *حضوم.*

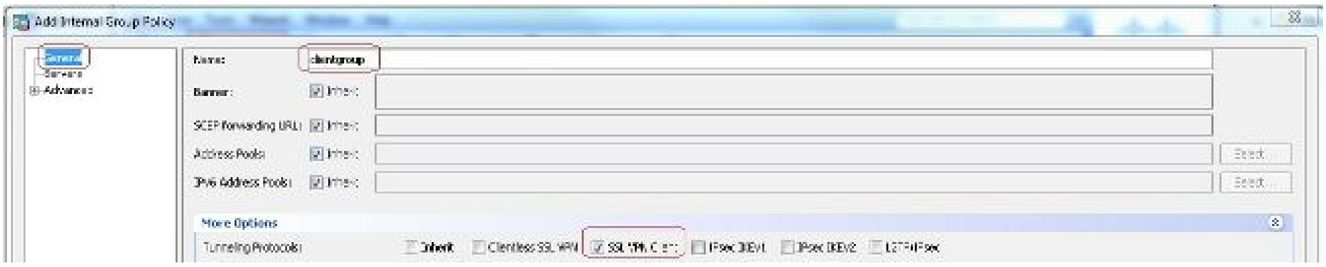




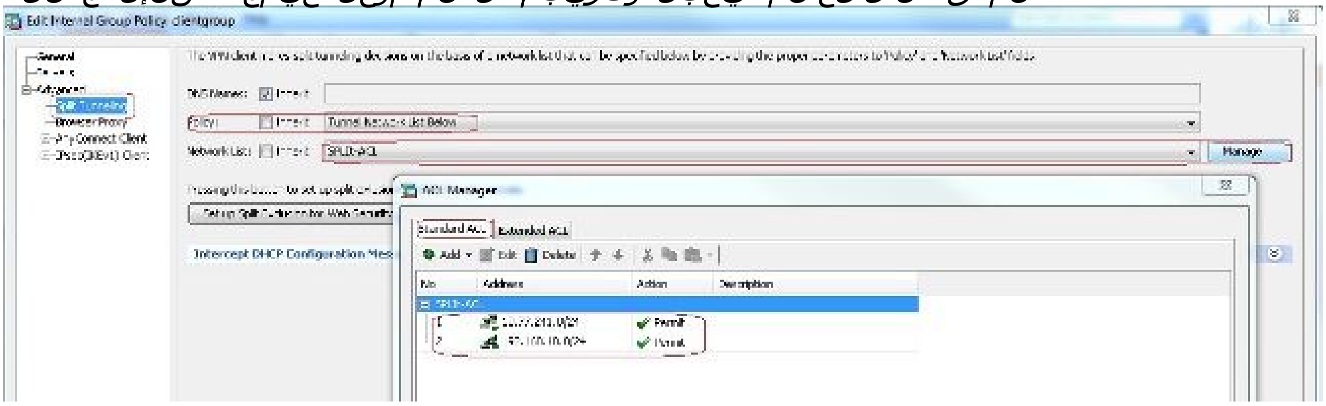
CLI تشكيل مكافئ:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

4. *تكوين نم ةعومجملا جهن. اتخن* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *ةيلخاد ةعومجم ةسايس ءاشنإل* **clientgroup**. *تحت* **General** *ةمئاقلا لتبويبلا، ددح* **SSL VPN Client** *ةناخ الاتخاي لتمكين WebVPN كبورتوكول نفق مسموح به.*



في **Advanced > Split Tunneling** جدولة، إختيار **Tunnel Network List Below** من القائمة المنسدلة "النهج" لإنشاء جميع الحزم من الكمبيوتر البعيد من خلال نفق آمن.



CLI تشكيل مكافئ:

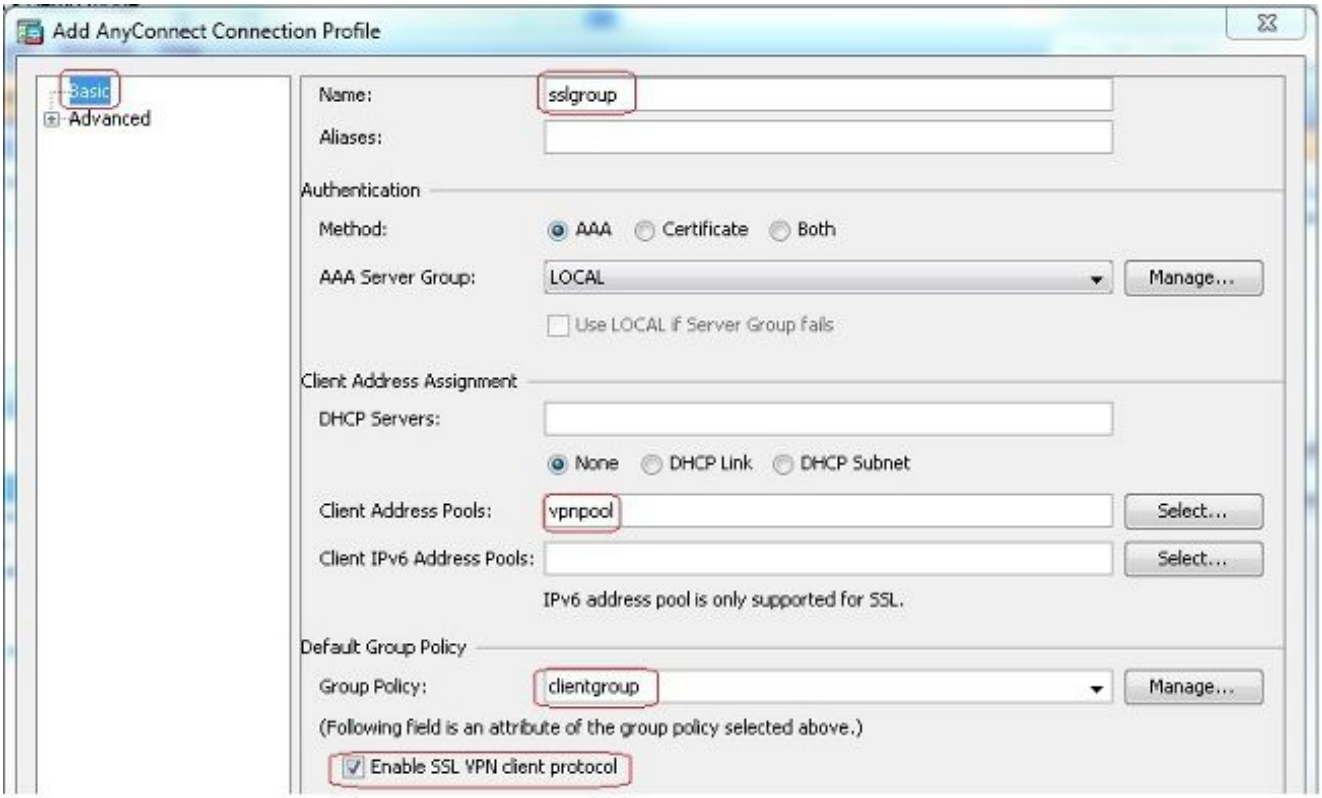
```
ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policy clientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL
```

5. نختار **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** لإنشاء حساب مستخدم جديد **ssluser1**. انقر **OK** ومن ثم **Apply**.

CLI تشكيل مكافئ:

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

6. تكوين مجموعة النفق. نختار **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** لإنشاء مجموعة نفق جديدة **sslgroup**.في **Basic** علامة التبويب، يمكنك تنفيذ قائمة التكوينات كما هو موضح: تسمية مجموعة النفق باسم **sslgroup**.تحت **Client Address Assignment**، أختر تجمع العناوين **vpnpool** من **Client Address Pools** القائمة المنسدلة.تحت **Default Group Policy**، أختر نهج المجموعة **clientgroup** من **Group Policy** القائمة المنسدلة.



تحت **Advanced > Group Alias/Group URL** عالمة التبويب، قم بتعيين اسم المجموعة المستعار ك **sslgroup_users** وانقر فوق **OK**. *CLI تشكيل مكافئ:*

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

ASA الإصدار 9.1(2) تشكيل في CLI

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the
Anyconnect tunnel.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when
going to the Anyconnect Pool

object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol
```

```
split-tunnel-policy tunnelspecified

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL
VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

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)#
```

التحقق من الصحة استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

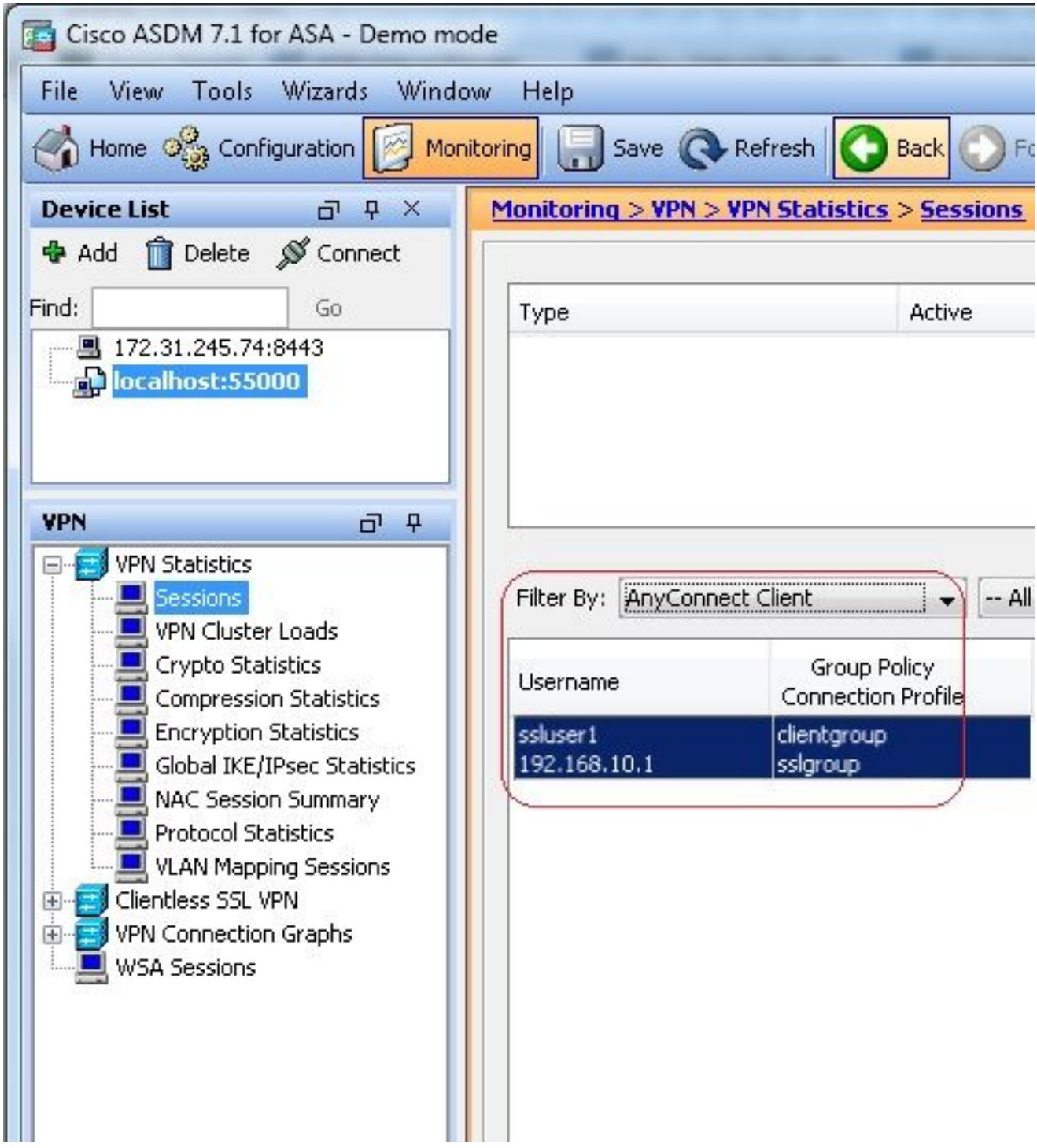
```
ciscoasa#show vpn-sessiondb anyconnect

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، أختر **Monitoring > VPN > VPN Statistics > Sessions** *in order to* عرفت الحالي جلسة في ال *ASA.*



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- **vpn-sessiondb logoff name** - أمر تسجيل الخروج من ال SSL VPN جلسة ل ال يعين username.

```
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)
```

وبالمثل، يمكنك إستخدام **vpn-sessiondb logoff anyconnect** *أمر in order to أنهيت all the AnyConnect جلسة.*

- **debug webvpn anyconnect <1-255>** - *يوفر أحداث WebVPN في الوقت الفعلي من أجل إنشاء الجلسة.*

```
Ciscoasa#debug webvpn anyconnect 7

CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
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: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
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'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
No SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260(mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt

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
```

- في ASDM، أختر **Monitoring > Logging > Real-time Log Viewer > View** عشان اشوف الاحداث السابقه. وضح اذه المثال معلومات الجلسة بين AnyConnect 192.168.10.1 و Telnet Server10.2.2.2 عبر ASA في الإنترنت 172.16.1.1.

معلومات ذات صلة

- دردان الحماية من الجيل التالي Cisco ASA 5500-X Series
- عميل PIX/ASA و VPN لشبكة VPN العامة 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).