AnyConnect Client إلى ASA باستخدام DHCP لتعيين العناوين

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل ال cisco 5500-X sery أمن أداة (ASA) أن يجعل ال DHCP نادل يزود الزبون عنوان إلى all the AnyConnect زبون مع الإستعمالمن (Adaptive Security Device Manager (ASDM أو CLI.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM أو CLI بإجراء تغييرات التكوين.

ملاحظة: ارجع إلى الكتاب 1: دليل تكوين واجهة سطر الأوامر لعمليات Cisco ASA Series General Operations، الإصدار 9.2 للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو SSH (Secure Shell).

المكونات المستخدمة

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

- جدار الحماية Cisco ASA 5500-X من الجيل التالي، الإصدار 9.2(1)
- Adaptive Security Device Manager، الإصدار 7.1(6)

- Cisco AnyConnect Secure Mobility Client 3.1.05152

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco ASA Security Appliance 5500 Series، الإصدار x.7 والإصدارات الأحدث.

معلومات أساسية

تلبي شبكات VPN الخاصة بالوصول عن بعد متطلبات الموظفين كثيري التنقل للاتصال بأمان بشبكة المؤسسة. يمكن للمستخدمين كثيري التنقل إعداد اتصال آمن باستخدام برنامج Cisco AnyConnect Secure Mobility Client. يقوم Cisco AnyConnect Secure Mobility Client ببدء اتصال بجهاز موقع مركزي تم تكوينه لقبول هذه الطلبات. في هذا المثال، جهاز الموقع المركزي هو جهاز الأمان القابل للتكيف ASA 5500-X Series الذي يستخدم خرائط التشفير الديناميكية.

في إدارة عنوان جهاز الأمان، يجب تكوين عناوين IP التي توصل عميلا بمورد على الشبكة الخاصة، عبر النفق، والسماح للعميل بالعمل كما لو كان متصلا مباشرة بالشبكة الخاصة.

علاوة على ذلك، فأنت تتعامل فقط مع عناوين IP الخاصة التي يتم تعيينها للعملاء. تعد عناوين IP التي تم تعيينها لموارد أخرى على الشبكة الخاصة الخاصة بك جزءا من مسؤوليات إدارة الشبكة الخاصة بك، وليس جزءا من إدارة VPN. لذلك، عندما تتم مناقشة عناوين IP هنا، تعني Cisco عناوين IP تلك المتاحة في مخطط عنونة الشبكة الخاصة لديك التي تتيح للعميل العمل كنقطة نهاية نفق.

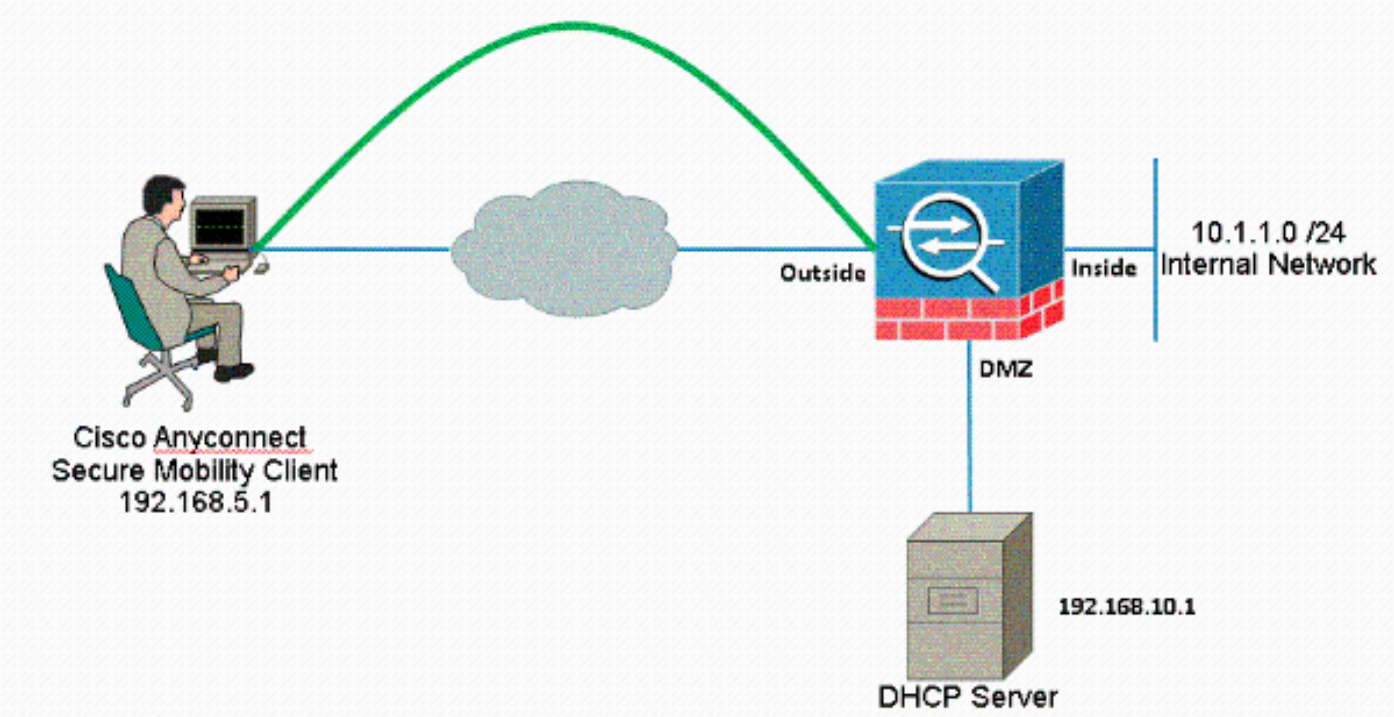
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



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

تكوين Cisco AnyConnect Secure Mobility Client

إجراء ASDM

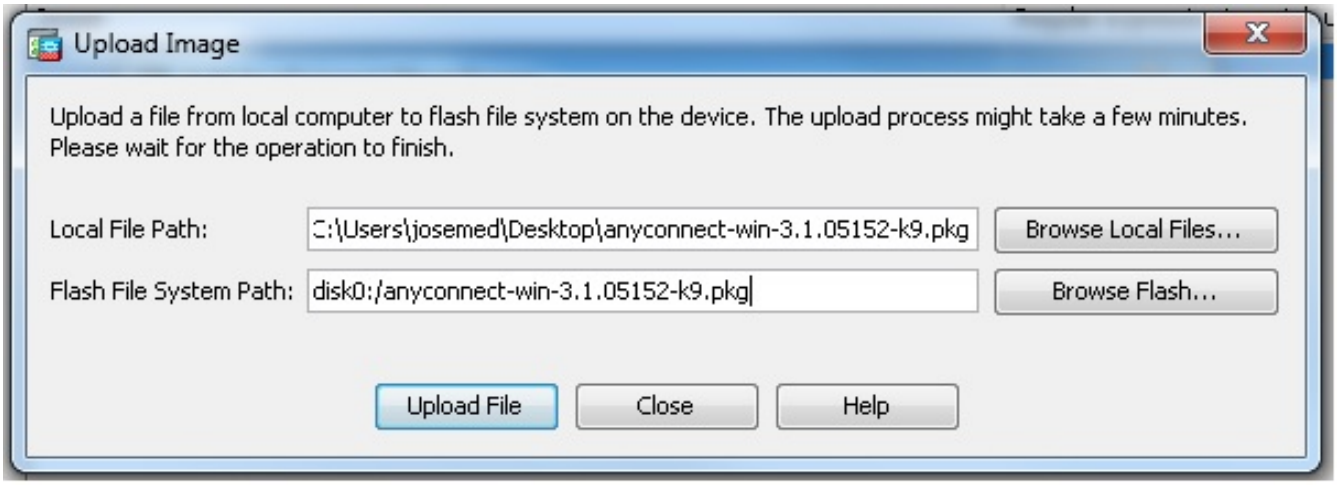
أتمت هذا steps in order to شكلت الوصول عن بعد VPN:

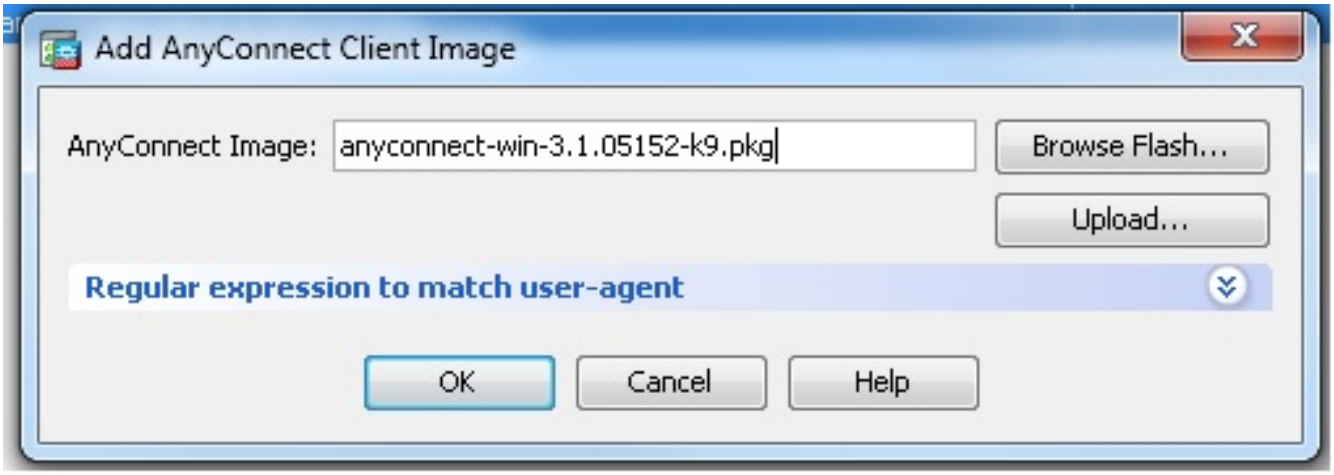
- تمكين WebVPN.

أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>SSL VPN توصيل** و**تحت منفذ قارن**، طقطقت ال **يسمح منفذ** و**يمكن DTLS** للقارن خارجي. تحقق أيضا من **تمكين وصول عميل AnyConnect VPN من Cisco أو وصول عميل SSL VPN القديم على الواجهة المحددة في** خانة الاختيار **هذا الجدول** لتمكين SSL VPN على الواجهة الخارجية.

طقطقة **يطبق**.

أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>AnyConnect زبون برمجية>إضافة** in order to أضفت ال cisco AnyConnect VPN زبون صورة من ال flash ذاكرة من ASA كما هو موضح.



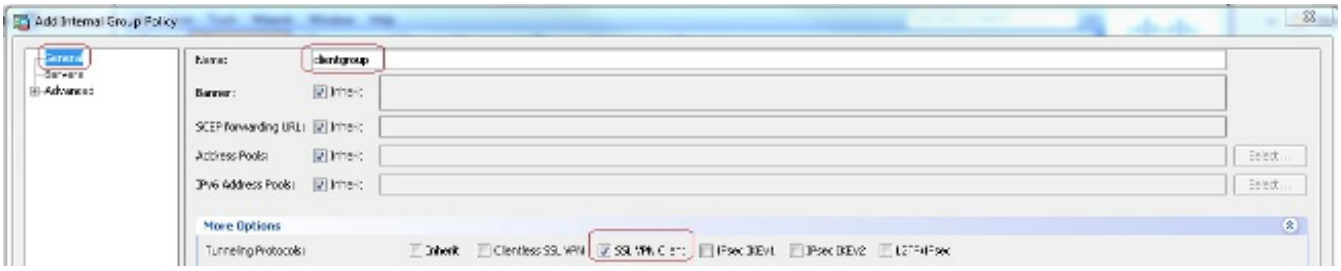


CLI تشكيل مكافئ:

```
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
```

- تكوين نهج المجموعة.

أخترت **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 SSL كبروتوكول نفق.



شكلت ال DHCP شبكة مجال في ال **نادل** تبويب، **يختار كثير خيار** in order to شكلت ال DHCP مجال للمستخدمين أن يكون عينت تلقائيا.

CLI تشكيل مكافئ:

```
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
```

- أخترت **تشكيل>Remote Access VPN وصول عن بعد>AAA/Local مستعمل>محلي>يضيف** in order to خلقت جديد مستعمل حساب **ssluser1**. طقطقت **ok** وبعد ذلك **يطبق**.

CLI تشكيل مكافئ:

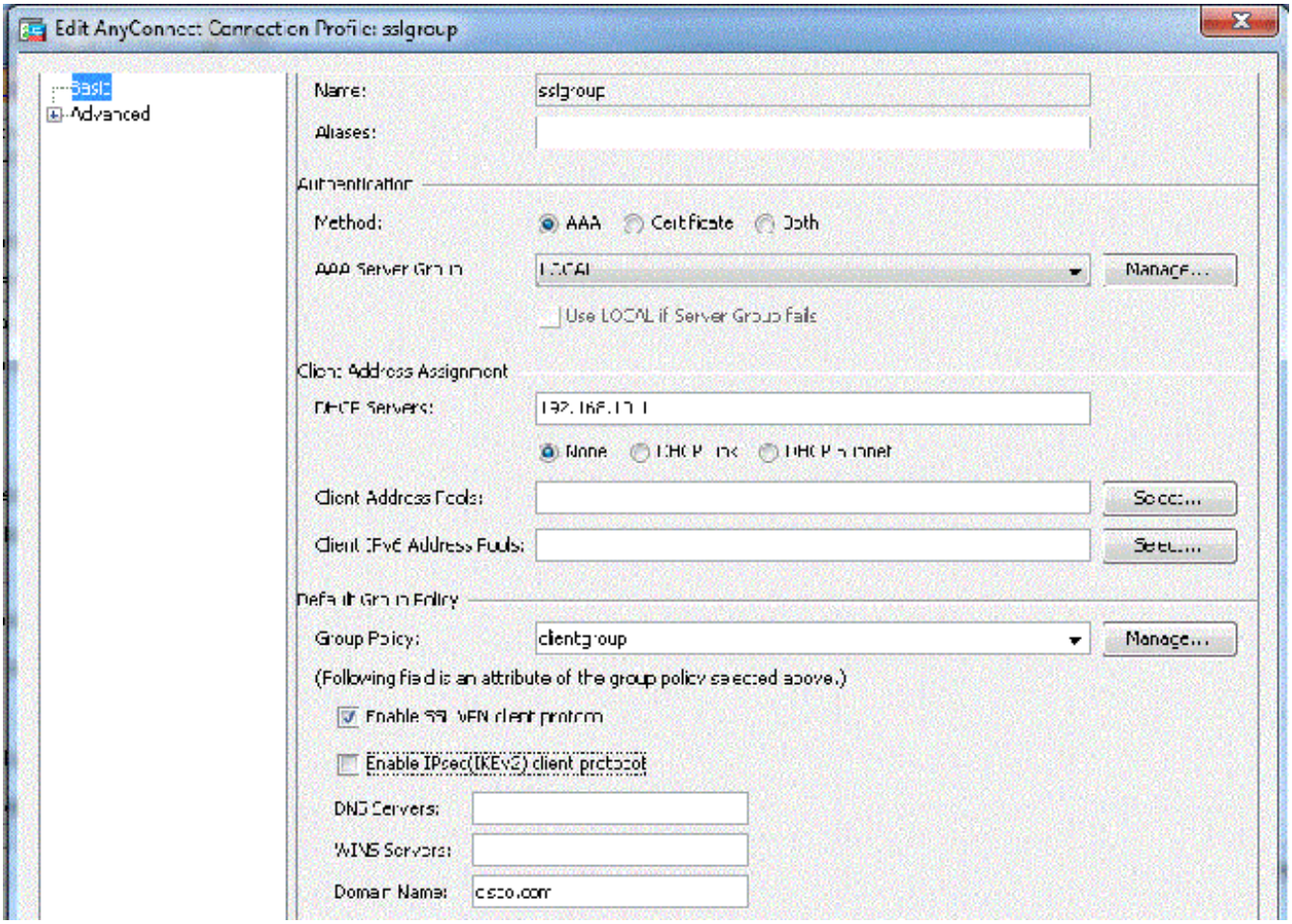
```
ciscoasa(config)#username ssluser1 password asdmASA
```

- تكوين مجموعة النفق.

أخترت **تشكيل>Remote Access VPN>شبكة (زبون) منفذ>AnyConnect 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**.قم بتوفير عنوان IP لخادم DHCP في المساحة المتوفرة **لخوادم DHCP**.ضمن "نهج المجموعة الافتراضي"، أختر **مجموعة عملاء** نهج المجموعة من القائمة المنسدلة "نهج المجموعة".قم بتكوين إرتباط DHCP أو شبكة DHCP الفرعية.



تحت علامة التبويب **خيارات متقدمة > الاسم المستعار للمجموعة/مجموعة URL**، حدد اسم الاسم المستعار للمجموعة على هيئة **sslgroup_users** وانقر على **موافق**.

CLI تشكيل مكافئ:

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#dhcp-server 192.168.10.1
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
```

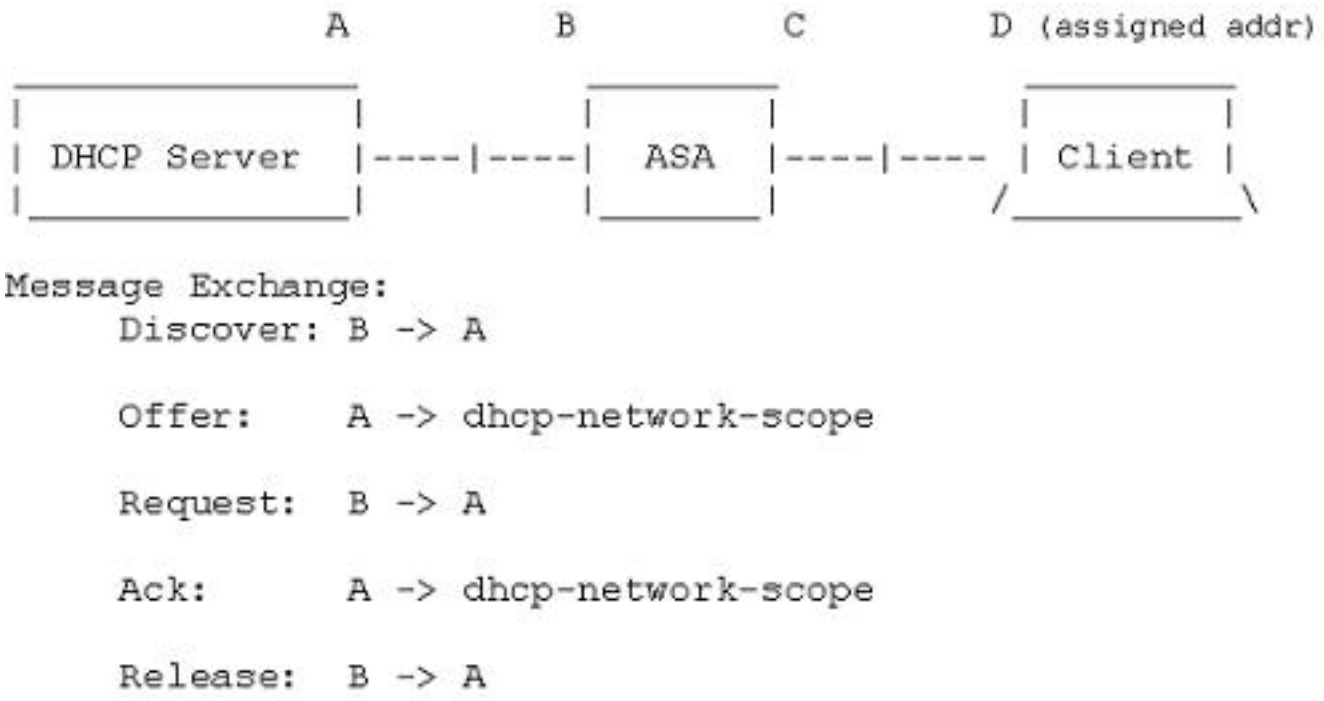
تحديد الشبكة الفرعية أو تحديد الارتباط

دعم وكيل بروتوكول DHCP ل RFC 3011 وRFC 3527 هو ميزة تم إدخالها في الإصدارين 8.0.5 و 8.2.2 وقد تم دعمها في الإصدارات التالية.

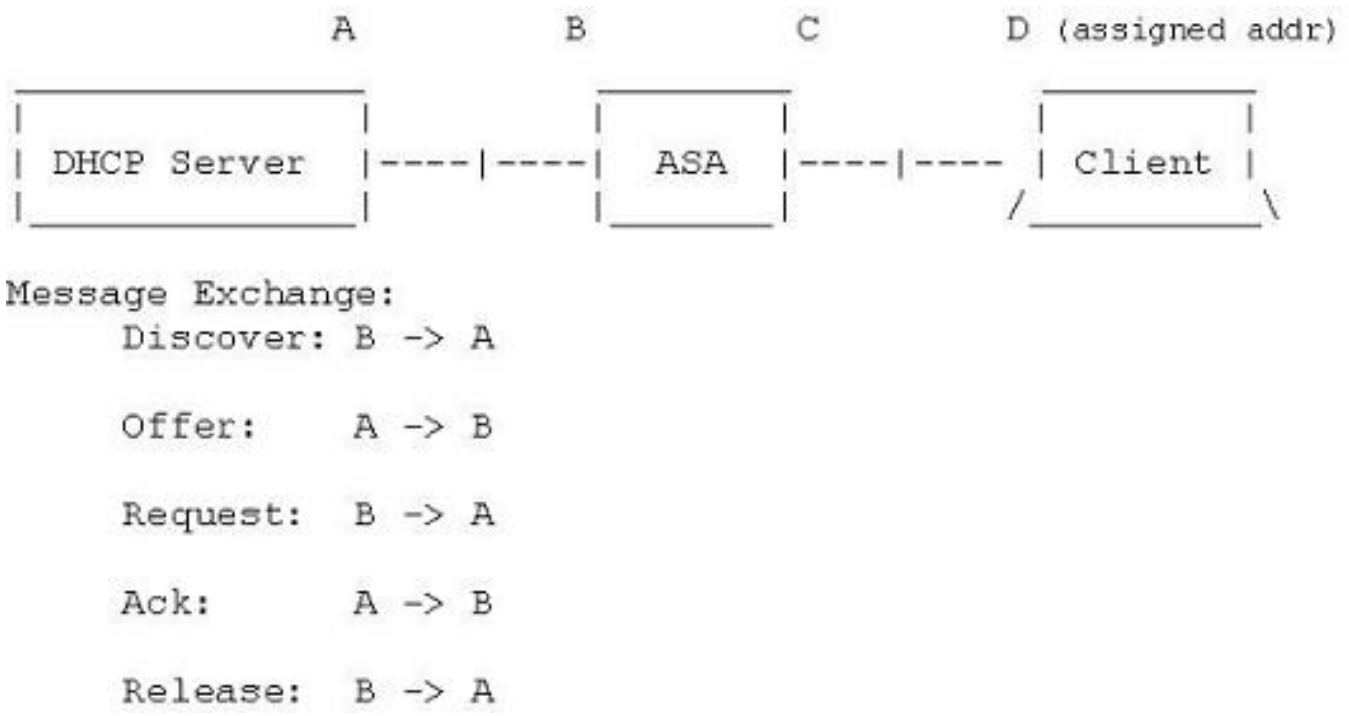
- يحدد RFC 3011 خيار DHCP جديد، خيار تحديد الشبكة الفرعية، الذي يسمح لعميل DHCP بتحديد الشبكة الفرعية التي سيتم تخصيص عنوان عليها. يعطي هذا الخيار الأولوية على الطريقة التي يستخدمها خادم DHCP لتحديد الشبكة الفرعية التي سيتم تحديد عنوان عليها.
- يحدد RFC 3527 خيار DHCP فرعي جديد، وهو الخيار الفرعي لتحديد الارتباط، الذي يسمح لعميل DHCP بتحديد العنوان الذي يجب أن يستجيب إليه خادم DHCP.

فيما يتعلق ب ASA، سيسمح RFCs هذا لمستخدم أن يعين DHCP-network-scope ل DHCP عنوان تنازل أن ليس محلي إلى ال ASA، وال DHCP نادل بعد يستطيع أن يرد مباشرة إلى القارن من ال ASA. ويجب ان تساعد الرسوم البيانية أدناه على ايضاح السلوك الجديد. سيتيح ذلك إستخدام النطاقات غير المحلية دون الحاجة إلى إنشاء مسار ثابت لذلك النطاق في شبكتهم.

عندما لا يتم تمكين RFC 3011 أو RFC 3527، يبدو تبادل وكيل DHCP مماثلا لهذا:



مع تمكين أي من نقاط الوصول عن بعد (RFCs) هذه، يبدو تبادل البيانات مشابها لهذا الإجراء بدلا من ذلك، ولا يزال عميل شبكة VPN معينا لعنوان في الشبكة الفرعية الصحيحة:



تكوين ASA باستخدام CLI

أتمت هذا steps in order to شكلت ال DHCP نادل أن يزود عنوان إلى ال VPN زبون من الأمر خط. راجع مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances للحصول على مزيد من المعلومات حول كل أمر يتم إستخدامه.

```
ASA# show run
(ASA Version 9.2(1
!

.Specify the hostname for the Security Appliance ---!

hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!


.Configure the outside and inside interfaces ---!

interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 192.168.10.2 255.255.255.0


.Output is suppressed ---!


passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
object network obj-192.168.5.0
subnet 192.168.5.0 255.255.255.0

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1


Specify the location of the ASDM image for ASA to fetch the image ---!
.for ASDM access

asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
obj-192.168.5.0 obj-192.168.5.0
!
```

```
                                                    object network obj-10.1.1.0
                                                nat (inside,outside) dynamic interface
                                            route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
                                                            timeout xlate 3:00:00
                        timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
          timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
       timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
                                                    timeout uauth 0:05:00 absolute
                                        dynamic-access-policy-record DfltAccessPolicy
                                                            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
                                                            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
                                                                         !
                                    Enable webvpn and specify an Anyconnect image ---!

                                                                    webvpn
                                                                enable outside
                                anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
                                                            anyconnect enable
                                                        tunnel-group-list enable


                                                    group-policy clientgroup internal
                                                   group-policy clientgroup attributes


define the DHCP network scope in the group policy.This configuration is Optional ---!

                                                    dhcp-network-scope 192.168.5.0
```

```
,In order to identify remote access users to the Security Appliance ---!
      .you can also configure usernames and passwords on the device ---!

                              username ssluser1 password ffIRPGpDSOJh9YLq encrypted


                              Create a new tunnel group and set the connection ---!
                                                    .type to remote-access ---!

                                                tunnel-group sslgroup type remote-access


                                  .Define the DHCP server address to the tunnel group ---!

                                                tunnel-group sslgroup general-attributes
                                                        default-group-policy clientgroup
                                                                dhcp-server 192.168.10.1

If the use of RFC 3011 or RFC 3527 is required then the following command will ---!
                                                                enable support for them

                                                        tunnel-group sslgroup general-attributes
                                                (dhcp-server subnet-selection (server ip) (3011
                                                   (hcp-server link-selection (server ip) (3527

                                             Configure a group-alias for the tunnel-group ---!

                                                         tunnel-group sslgroup webvpn-attributes
                                                               group-alias sslgroup_users enable

                                                                        prompt hostname context
                                                 Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
                                                                                        end :
                                                                                         #ASA
```

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).