AnyConnect-client met ASA met DHCP voor adrestoewijzing

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco 5500-X Series adaptieve security applicatie (ASA) kunt configureren om de DHCP-server het IP-adres van de client te laten geven aan alle AnyConnect-clients met het gebruik van Adaptieve Security Devices Manager (ASDM) of CLI.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren.

> **Opmerking**: Raadpleeg boek 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.2 om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500-X next-generation firewall versie 9.2(1)

- Adaptieve Security Service Manager versie 7.1(6)
- Cisco AnyConnect beveiligde mobiliteit-client 3.1.05/152

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA security applicatie 5500 Series versie 7.x en hoger.

Achtergrondinformatie

VPN's voor externe toegang voldoen aan de vereisten van de mobiele medewerkers om zich veilig aan te sluiten op het netwerk van de organisatie. Mobiele gebruikers kunnen een beveiligde verbinding opzetten met behulp van de Cisco AnyConnect Secure Mobility Client-software. De Cisco AnyConnect Secure Mobility Client stelt een verbinding met een centraal siteapparaat in om deze verzoeken te aanvaarden. In dit voorbeeld is het centrale plaatsapparaat een ASA 5500-X Series Adaptieve security applicatie die dynamische crypto kaarten gebruikt.

In het beheer van het veiligheidsapparaat moet u IP adressen configureren die een client met een resource op het privénetwerk verbinden, door de tunnel en de client laten functioneren alsof deze direct verbonden is met het privénetwerk.

Bovendien heeft u alleen te maken met de privé IP-adressen die aan klanten zijn toegewezen. De IP-adressen die aan andere bronnen op uw privénetwerk zijn toegewezen, maken deel uit van uw netwerkbeheerverantwoordelijkheden en maken geen deel uit van VPN-beheer. Daarom, wanneer IP adressen hier worden besproken, betekent Cisco die IP adressen beschikbaar in uw privé netwerk adresseringsschema die de client als tunneleindpunt laten functioneren.

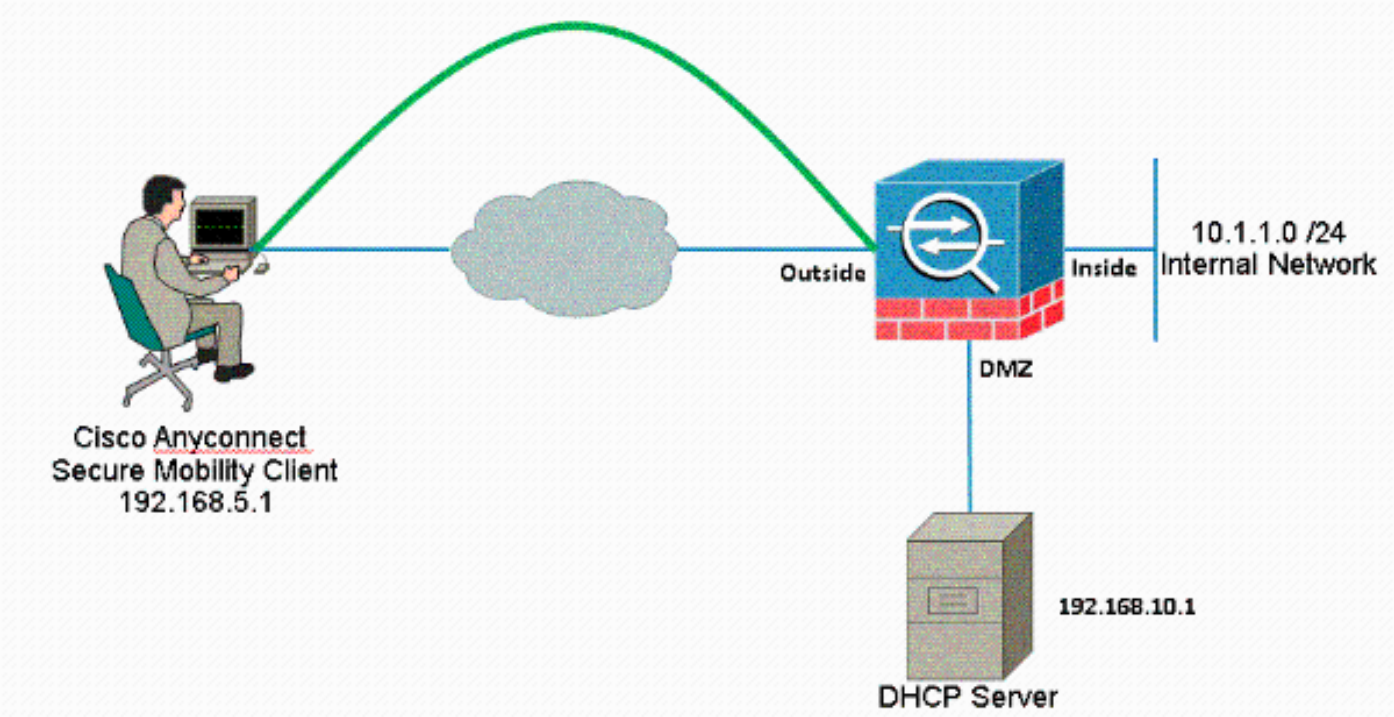
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

> **Opmerking**: gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn juridisch niet routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

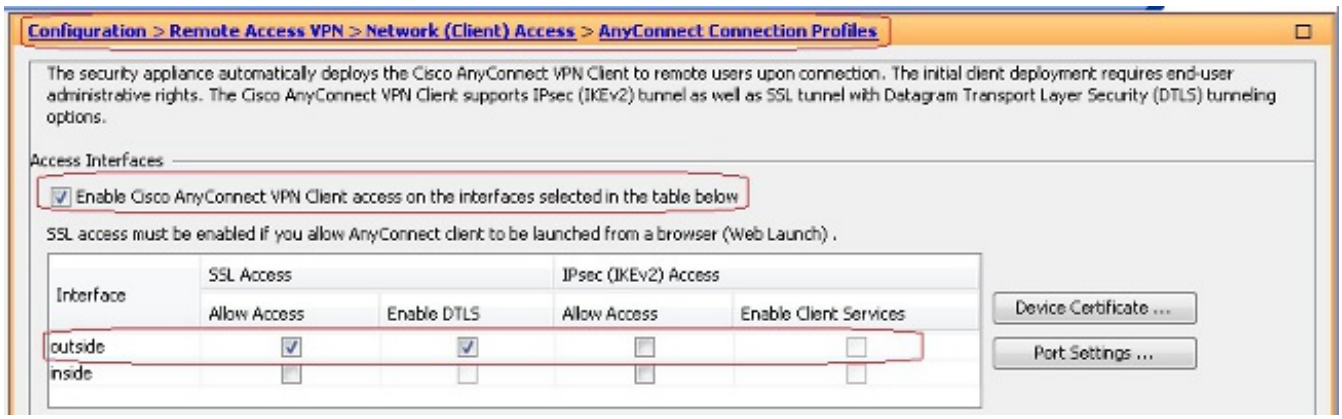
Cisco AnyConnect Secure Mobility Client configureren

ASDM-procedure

Voltooi deze stappen om de externe VPN-toegang te configureren:

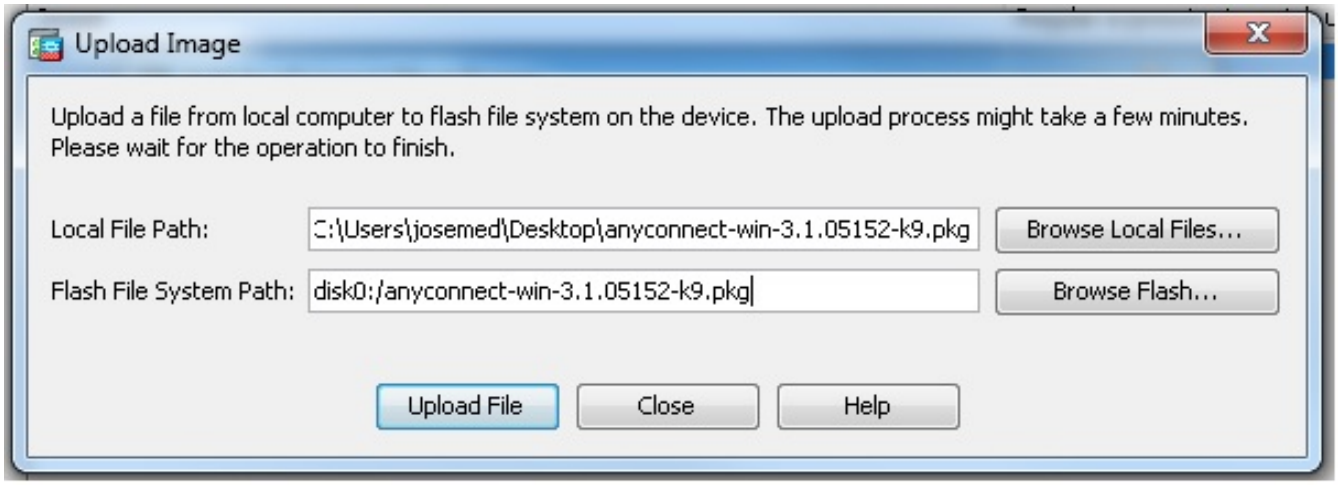
- Webex inschakelen.

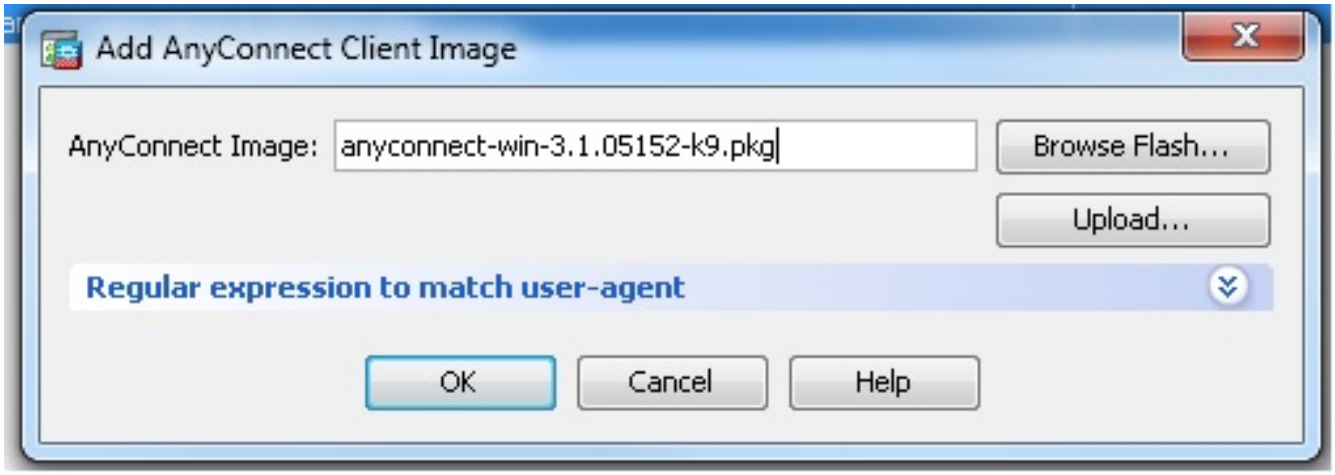
  Kies **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN-verbindingsprofielen** en klik **onder Access-interfaces** op de vinkjes **Toegang toestaan** en **DTLS** inschakelen voor de externe interface. Controleer ook de **toegang tot Cisco AnyConnect VPN-client of oudere SSL VPN-client op de interface die in dit** venster **van tabel is geselecteerd** om SSL VPN op de externe interface mogelijk te maken.



Klik op **Toepassen**.

Kies **Configuration > Remote Access VPN > Network (Client) Access > Any-clientsoftware > Add** om de Cisco AnyConnect VPN-clientafbeelding uit het flash-geheugen van ASA toe te voegen zoals weergegeven.



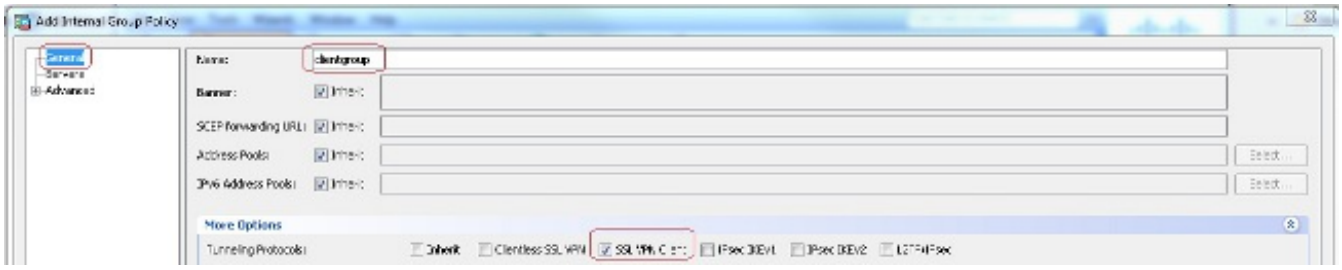


Compatibele CLI-configuratie:

```
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
```

- Groepsbeleid configureren

Kies **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** om een interne **clientgroep** voor groepsbeleid te maken. Selecteer onder het tabblad **General** het dialoogvenster **SSL VPN-client** om SSL als tunneling-protocol in te schakelen.



Configureer de DHCP-netwerkscope in het tabblad **servers**, kies **Meer opties** om het DHCP-werkgebied te configureren zodat de gebruikers automatisch worden toegewezen.

Compatibele CLI-configuratie:

```
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)#
```

- Kies **Configuration > Remote Access VPN > AAA/Local Gebruikers > Local Gebruikers > Add** om een nieuwe **gebruiker-gebruiker1** te maken**. Klik op OK** en **Toepassen**.

Compatibele CLI-configuratie:

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

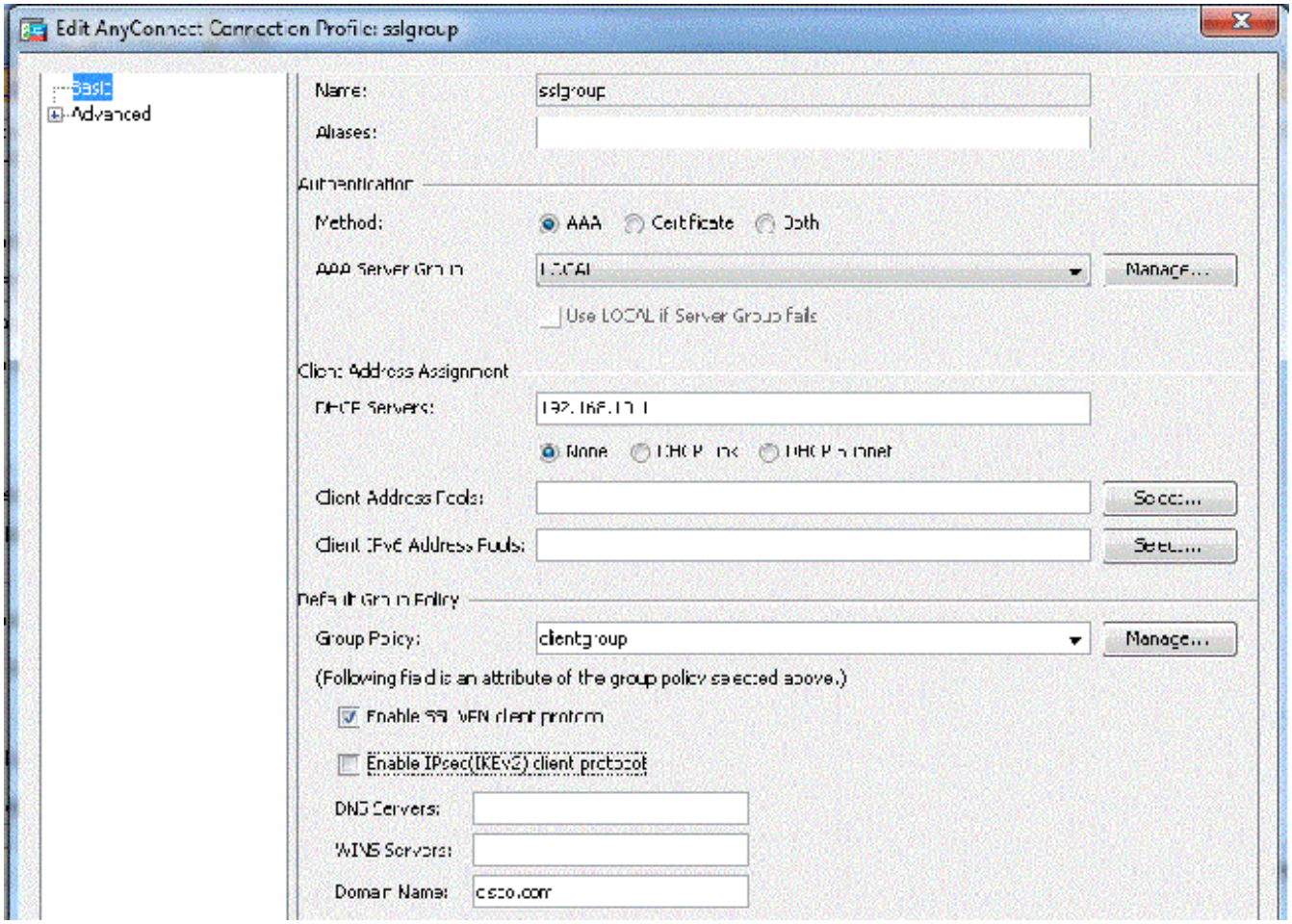
- Tunnelgroep configureren

Kies **Configuration > Remote Access VPN > Network (Client) Access > Any** Connect **Connection-profielen > Add** om een nieuwe **groep** tunnelgroepen te maken.

In het tabblad **Basic** kunt u de lijst met configuraties uitvoeren zoals wordt weergegeven:

Geef de tunnelgroep een naam als **groep**.Geef het IP-adres van de DHCP-server op in de ruimte die voor **DHCP-servers** is meegeleverd.Selecteer onder Standaardgroepsbeleid de

clientgroep voor groepsbeleid uit de vervolgkeuzelijst Groepsbeleid.Configuratie DHCP-link of DHCP-subnet.



Onder het tabblad **Geavanceerd > Group Alias/Group URL** specificeert u de naam van de groep alias als **sslgroup_user** en klikt u op **OK**.

Compatibele CLI-configuratie:

```
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
```

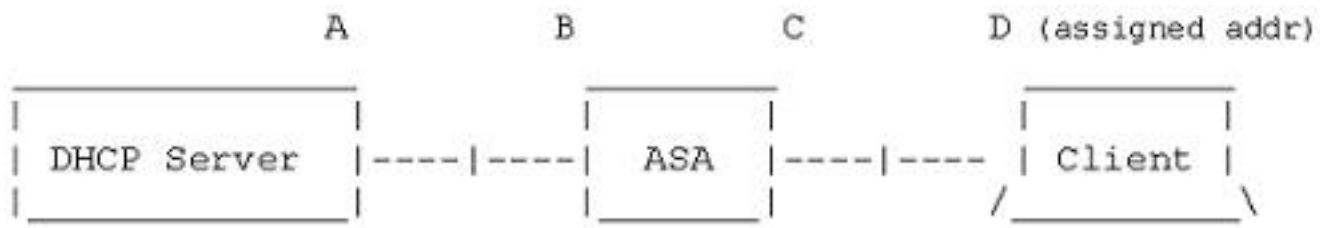
Subnet-selectie of linkselectie

Ondersteuning van DHCP-proxy voor RFC 3011 en RFC 3527 is een optie die in de 8.0.5 en 8.2.2 is geïntroduceerd en deze is ondersteund door verdere releases.

- RFC 3011 definieert een nieuwe DHCP-optie, de subnetselectie optie, die de DHCP-client toestaat om het subsysteem te specificeren waarop u een adres wilt toewijzen. Deze optie heeft voorrang op de methode die de server van DHCP gebruikt om het net te bepalen waarop om een adres te selecteren.
- RFC 3527 definieert een nieuwe DHCP-suboptie, de suboptie voor link Selectie, waarbij de

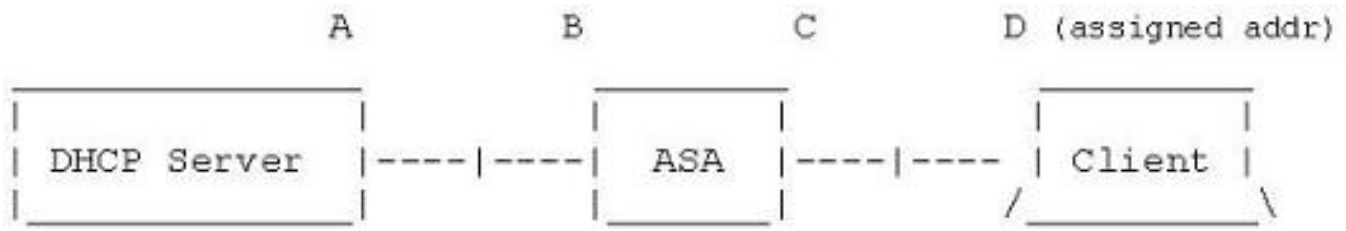
DHCP-client het adres kan specificeren waarop de DHCP-server moet reageren.
In termen van de ASA, zullen deze RFCs een gebruiker in staat stellen om een dhcp-netwerk-scope voor DHCP-adrestoewijzing te specificeren die niet lokaal is voor de ASA, en de DHCP-server zal nog steeds in staat zijn om rechtstreeks te antwoorden op de interface van de ASA. De onderstaande diagrammen moeten helpen het nieuwe gedrag te illustreren. Dit zal het gebruik van niet-lokale scopen mogelijk maken zonder een statische route voor dat toepassingsgebied in hun netwerk te hoeven creëren.

Wanneer RFC 3011 of RFC 3527 niet is ingeschakeld, lijkt de DHCP-proxyuitwisseling er precies op:




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

Met één van deze RFCs die werd geactiveerd, lijkt de uitwisseling in plaats daarvan op dit, en de VPN client wordt nog steeds een adres in de juiste vorm van netwerk toegewezen:




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

De ASA met Gebruik van de CLI configureren

Voltooi deze stappen om de DHCP-server te configureren om IP-adres aan de VPN-clients te geven vanuit de opdrachtregel. Raadpleeg Cisco ASA 5500 Series adaptieve security applicaties-commando referenties voor meer informatie over elke opdracht die gebruikt wordt.

```
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#