Cliente de Anyconnect al ASA con el uso del DHCP para la asignación de dirección

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de las Cisco 5500-X Series (ASA) para hacer que el servidor DHCP proporciona el dirección IP del cliente a todos los clientes de Anyconnect con el uso del Administrador de dispositivos de seguridad adaptante (ASDM) o del CLI.

Prerequisites

Requisitos

Este documento asume que el ASA está completamente operativo y está configurado para permitir que el ASDM de Cisco o el CLI realice los cambios de configuración.

> **Note**: Refiera al [libro 1: Guía de configuración CLI de los funcionamientos generales de la serie de Cisco ASA, 9.2](#) para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión del Firewall de la última generación de Cisco ASA 5500-X 9.2(1)
- Versión 7.1(6) adaptante del Administrador de dispositivos de seguridad
- Cliente de movilidad Cisco AnyConnect Secure 3.1.05152

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.x y posterior de las 5500 Series del dispositivo de seguridad de Cisco ASA.

Antecedentes

Los VPN de accesos remotos dirigen el requisito del equipo de trabajo móvil de conectar con seguridad con la red de la organización. Los usuarios ambulantes pueden configurar una conexión segura usando el software del Cliente de movilidad Cisco AnyConnect Secure. El Cliente de movilidad Cisco AnyConnect Secure inicia una conexión a un dispositivo del sitio central configurado para validar estas peticiones. En este ejemplo, el dispositivo del sitio central es un dispositivo de seguridad adaptante de las 5500-X Series ASA que utiliza las correspondencias cifradas dinámicas.

En administración de direcciones del dispositivo de seguridad, usted tiene que configurar los IP Addresses que conecta a un cliente con un recurso en la red privada, a través del túnel, y deja al cliente funcionar como si fuera conectado directamente con la red privada.

Además, usted se está ocupando solamente de los IP Address privados que se asignan a los clientes. Los IP Addresses asignados a otros recursos en su red privada son parte de sus responsabilidades de la Administración de red, no Administración de VPN de la parte de. Por lo tanto, cuando los IP Addresses se discuten aquí, Cisco significa esos IP Addresses disponibles en su esquema de direccionamiento de la red privada que deje al cliente funcionar como un punto final del túnel.

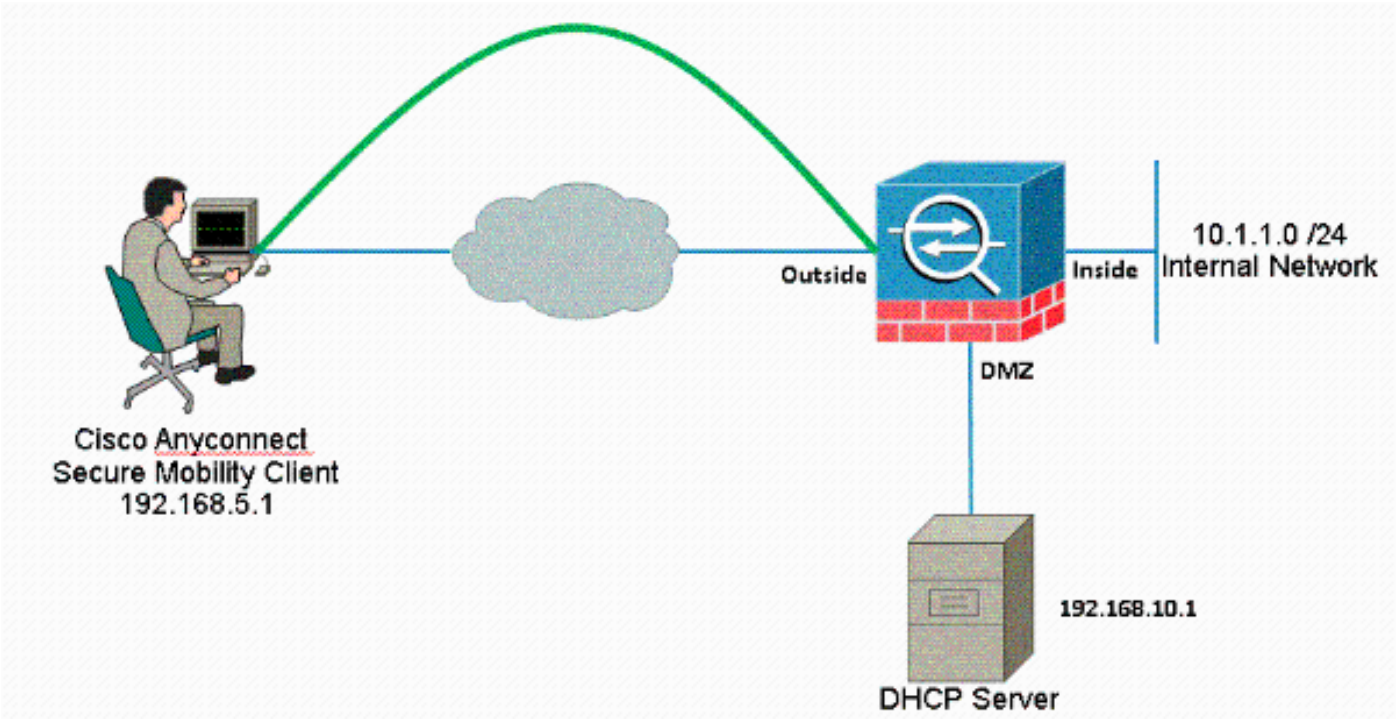
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Note: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que fueron utilizadas en un entorno de laboratorio.

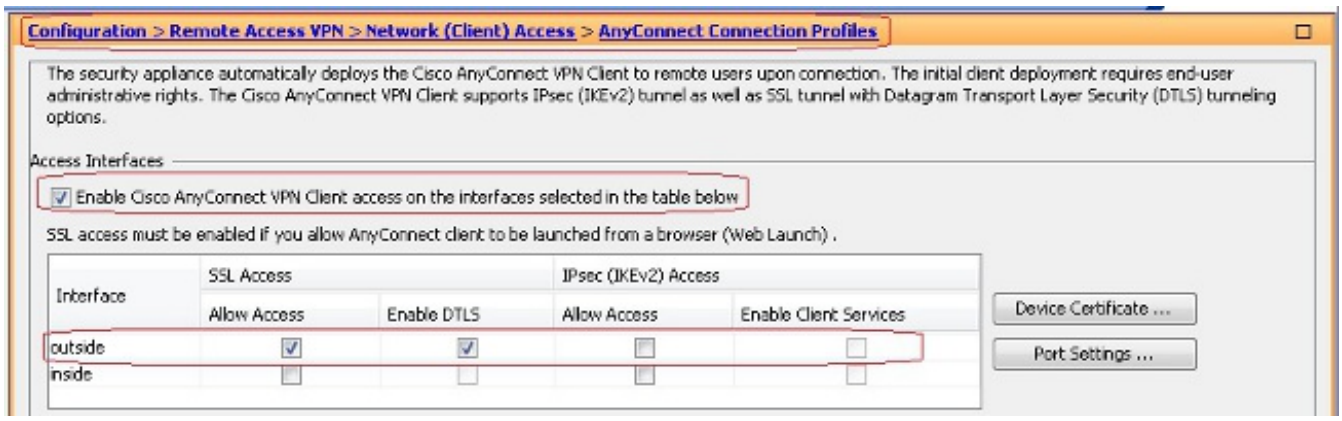
Cliente de movilidad Cisco AnyConnect Secure de la configuración

Procedimiento del ASDM

Complete estos pasos para configurar el VPN de acceso remoto:

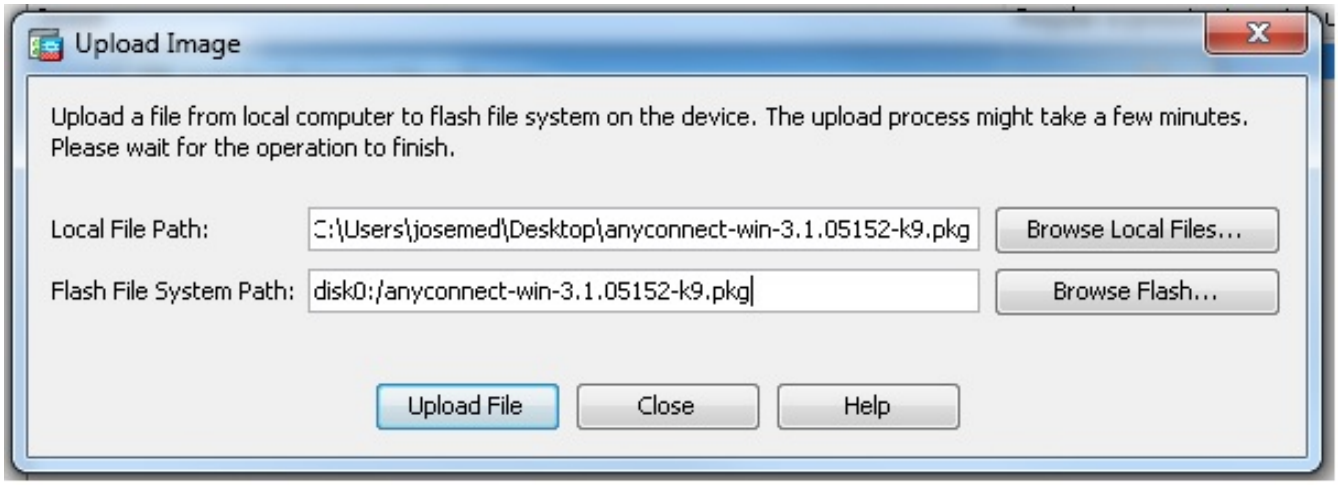
- Habilite WebVPN.

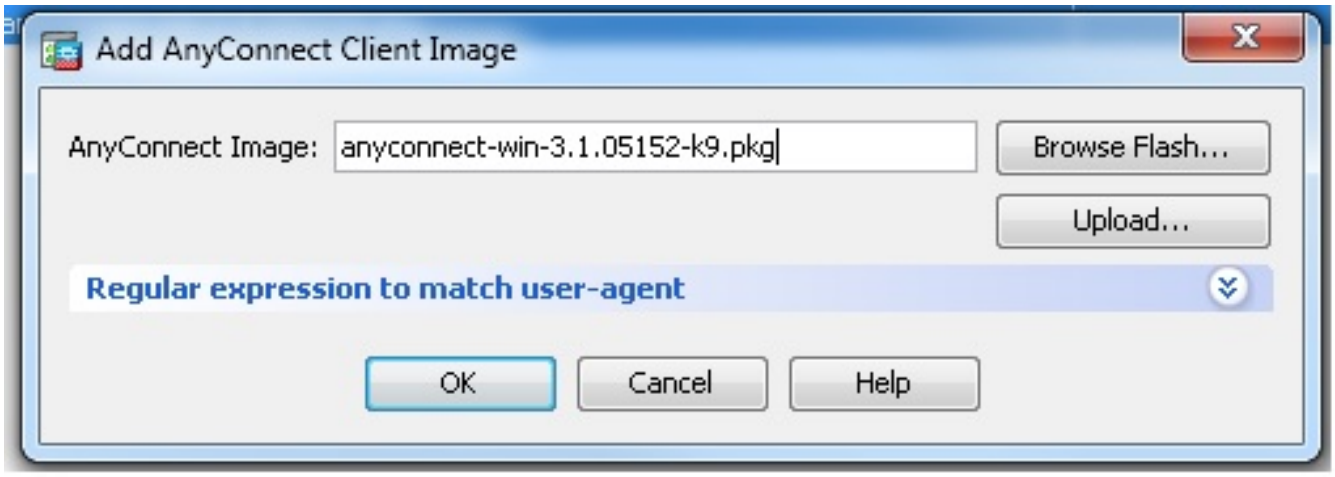
  Elija **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** y, debajo de **Access Interfaces**, haga clic en los cuadros de verificación **Allow Access** and **Enable DTLS** para la interfaz externa. También, marque el **acceso del Cliente Cisco AnyConnect VPN del permiso o de cliente VPN de la herencia SSL en la interfaz seleccionada en esta** casilla de verificación de la **tabla** para habilitar SSL VPN en la interfaz exterior.



Haga clic en Apply (Aplicar).

Elija la **configuración > el acceso del VPN de acceso remoto > de la red (cliente) > el software de cliente de Anyconnect > Add** para agregar la imagen del Cliente Cisco AnyConnect VPN de memoria flash del ASA como se muestra.



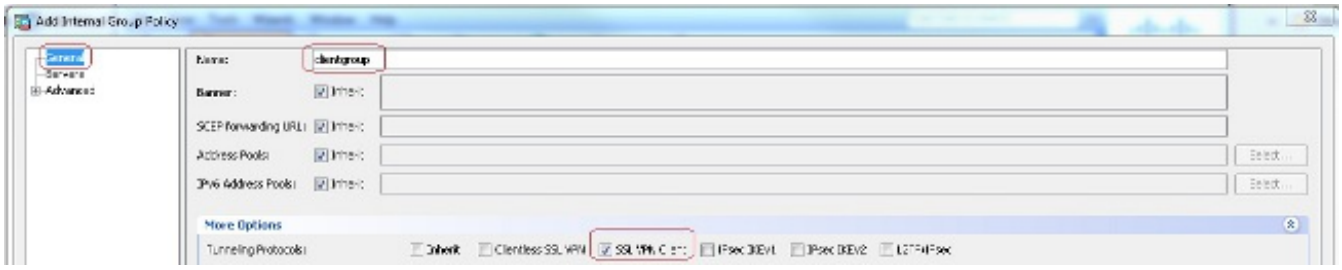


Configuración CLI Equivalente:

```
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
```

- Configure la Política de Grupo.

Elija **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** para crear una política de grupo interna **clientgroup**. Conforme a la **ficha general**, seleccione la casilla de verificación del **cliente VPN SSL** para habilitar el SSL como Tunneling Protocol.



Configure el Alcance de la red DHCP en la lengueta de los **servidores**, elija **más opciones** para configurar el alcance de DHCP para que los usuarios sean asignados automáticamente.

Configuración CLI Equivalente:

```
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
```

- Elija la **configuración > el VPN de acceso remoto > los usuarios > a los usuarios locales AAA/Local > Add** para crear una cuenta de usuario nuevo **ssluser1**. Haga clic en OK y en **Apply**.

Configuración CLI Equivalente:

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

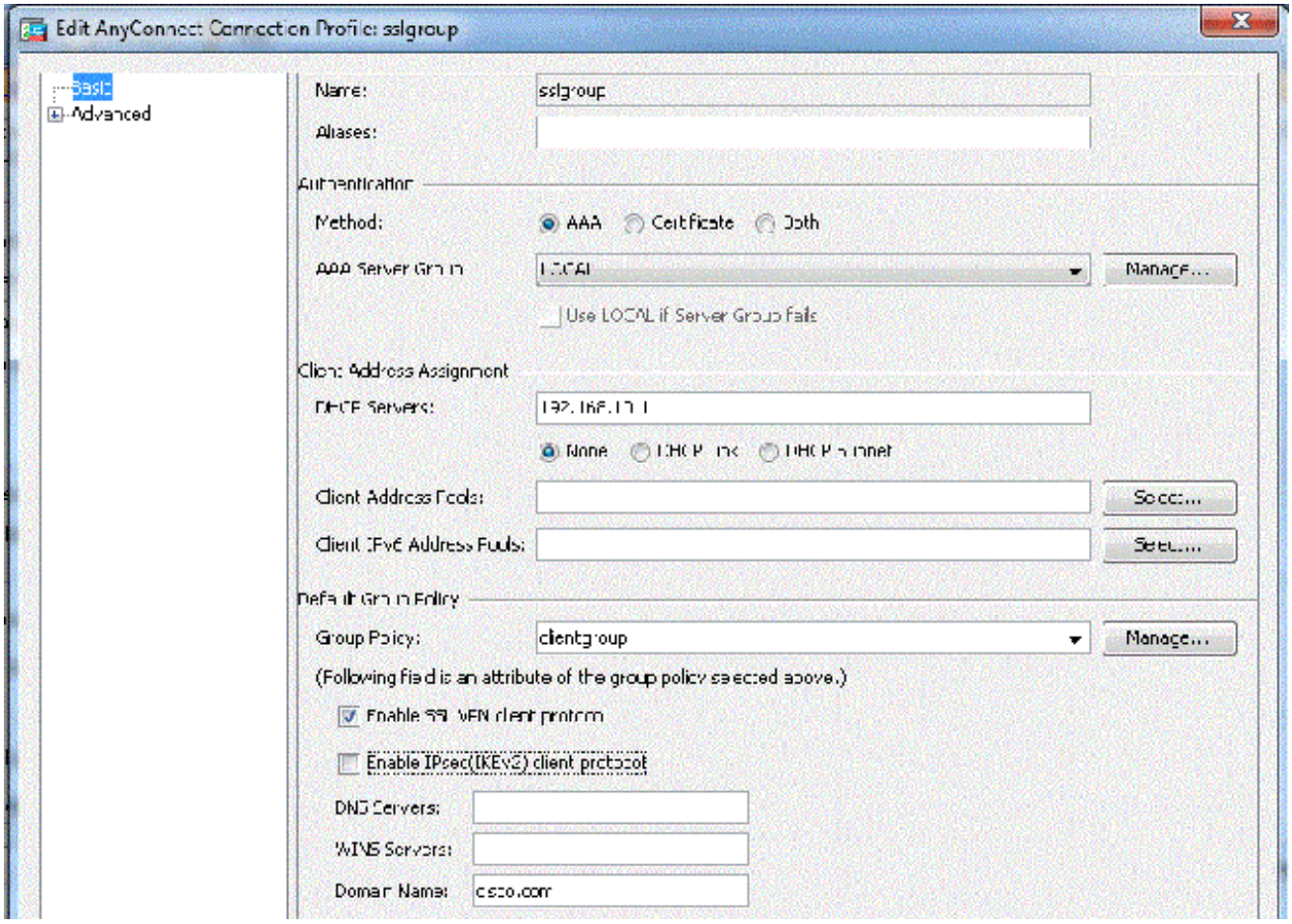
- Configure el Grupo de Túnel.

Elija la **configuración > el acceso del VPN de acceso remoto > de la red (cliente) > los perfiles de la conexión de Anyconnect > Add** para crear un nuevo **sslgroup del** grupo de túnel.

En la pestaña **Basic**, puede confeccionar la lista de configuraciones como se muestra:

Asigne el grupo de Túnel como **sslgroup**.Proporcione el IP Address del servidor DHCP en el

espacio proporcionado para los **servidores DHCP**.Bajo directiva del grupo predeterminado, elija el **clientgroup de la** directiva del grupo de la lista desplegable de la directiva del grupo.Configure el link del DHCP o la subred del DHCP.



Bajo el **avanzado > el grupo** lengueta **alias/del grupo URL**, especifica el nombre de alias del grupo como **sslgroup_users** y hace clic la **AUTORIZACIÓN**.

Configuración CLI Equivalente:

```
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
```

Subred-selección o Link-selección

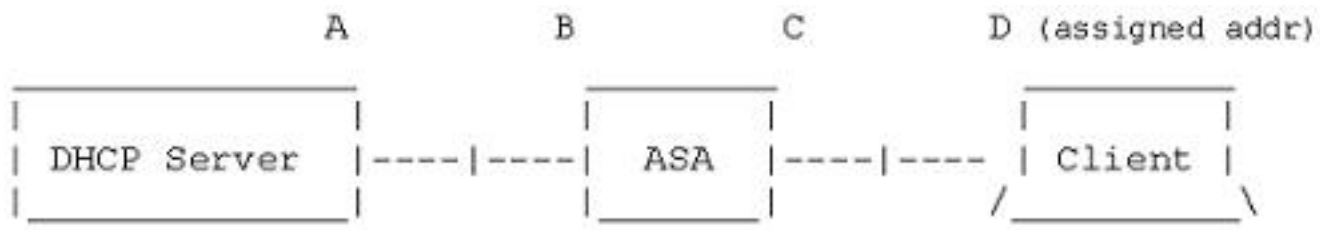
El Soporte de proxy del DHCP para el RFC 3011 y el RFC 3527 es una característica introducida en los 8.0.5 y los 8.2.2 y se ha soportado en las versiones hacia adelante.

- El RFC 3011 define una nueva opción DHCP, la opción de la selección de la subred, que permite que el Cliente de DHCP especifique la subred en la cual afectar un aparato un direccionamiento. Esta opción toma la precedencia sobre el método que el servidor DHCP utiliza para determinar la subred en la cual seleccionar un direccionamiento.

- El RFC 3527 define un nuevo suboption del DHCP, el suboption de la selección del link, que permite que el Cliente de DHCP especifique el direccionamiento al cual el servidor DHCP debe responder.

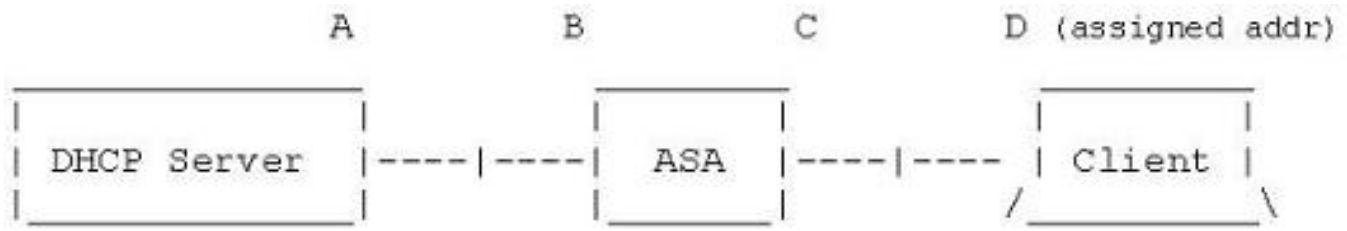
En términos de ASA, estos RFC permitirán que un usuario especifique un DHCP-red-alcance para la asignación de DHCP Address que no es local al ASA, y el servidor DHCP todavía podrá contestar directamente a la interfaz del ASA. Los diagramas a continuación deben ayudar a ilustrar el nuevo comportamiento. Esto no prohibirá a uso los alcances NON-locales sin tener que crear una Static ruta para ese alcance en su red.

Cuando el RFC 3011 o el RFC 3527 no se habilita, el intercambio del proxy del DHCP parece similar a esto:




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

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

Con cualquiera de estos RFC habilitados, el intercambio parece similar a esto en lugar de otro, y todavía asignan el cliente VPN un direccionamiento en la subred correcta:



Message Exchange:

Discover: B -> A

Offer: A -> B

Request: B -> A

Ack: A -> B

Release: B -> A

Configure el ASA con el uso del CLI

Complete estos pasos para configurar al servidor DHCP para proporcionar la dirección IP a los clientes VPN de la línea de comando. Refiera a las referencias adaptantes del Dispositivo-comando de la Seguridad de las 5500 Series de Cisco ASA para más información sobre cada comando se utilice que.

```
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#
```