AnyConnect-Client zu ASA mit Verwendung von DHCP für die Adresszuweisung

Inhalt

Einführung

Dieses Dokument beschreibt, wie die Cisco Adaptive Security Appliance (ASA) der Serie 5500-X so konfiguriert wird, dass der DHCP-Server mithilfe des ASDM (Adaptive Security Device Manager) oder der CLI allen AnyConnect-Clients die Client-IP-Adresse bereitstellt.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM oder die CLI Konfigurationsänderungen vornehmen können.

> **Hinweis**: Siehe Buch 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.2, um die Remote-Konfiguration des Geräts durch ASDM oder Secure Shell (SSH) zu ermöglichen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Firewall der nächsten Generation der Serie ASA 5500-X Version 9.2(1)
- Adaptive Security Device Manager Version 7.1(6)
- Cisco AnyConnect Secure Mobility Client 3.1.05152

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco ASA Security Appliance der Serie 5500, Version 7.x und höher, verwendet werden.

Hintergrundinformationen

VPNs für Remote-Zugriff erfüllen die Anforderung mobiler Mitarbeiter, eine sichere Verbindung zum Netzwerk des Unternehmens herzustellen. Mobile Benutzer können mithilfe der Cisco AnyConnect Secure Mobility Client-Software eine sichere Verbindung herstellen. Der Cisco AnyConnect Secure Mobility Client stellt eine Verbindung zu einem Gerät an einem zentralen Standort her, das für die Annahme dieser Anfragen konfiguriert ist. In diesem Beispiel ist das Gerät des zentralen Standorts eine Adaptive Security Appliance der Serie ASA 5500-X, die dynamische Crypto Maps verwendet.

Bei der Adressverwaltung der Sicherheitsappliance müssen Sie IP-Adressen konfigurieren, die einen Client mit einer Ressource im privaten Netzwerk über den Tunnel verbinden und den Client so funktionieren lassen, als ob er direkt mit dem privaten Netzwerk verbunden wäre.

Darüber hinaus handelt es sich nur um private IP-Adressen, die Clients zugewiesen sind. Die IP-Adressen, die anderen Ressourcen in Ihrem privaten Netzwerk zugewiesen werden, sind Teil Ihrer Netzwerkadministrationsaufgaben und nicht Teil des VPN-Managements. Wenn hier also IP-Adressen besprochen werden, bezieht sich Cisco auf die IP-Adressen, die in Ihrem privaten Netzwerkadressierungsschema verfügbar sind, sodass der Client als Tunnelendpunkt fungieren kann.

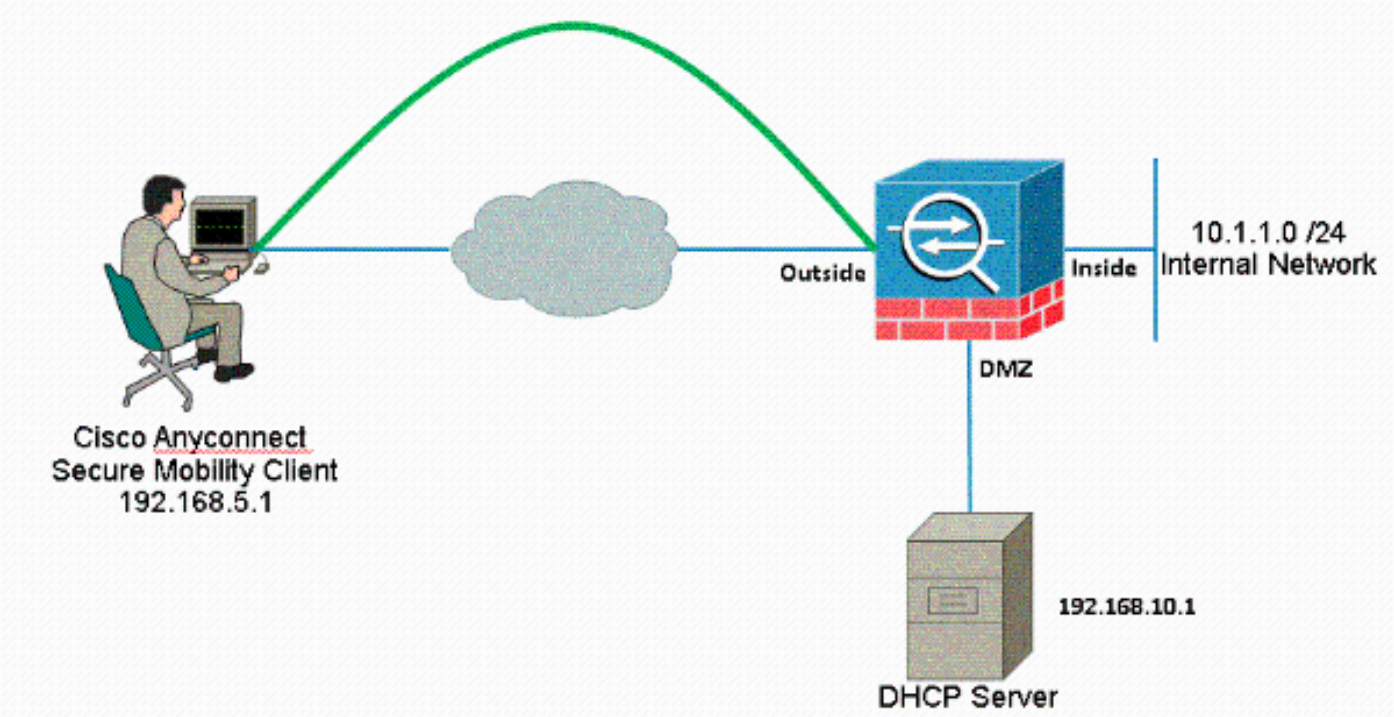
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht legal routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

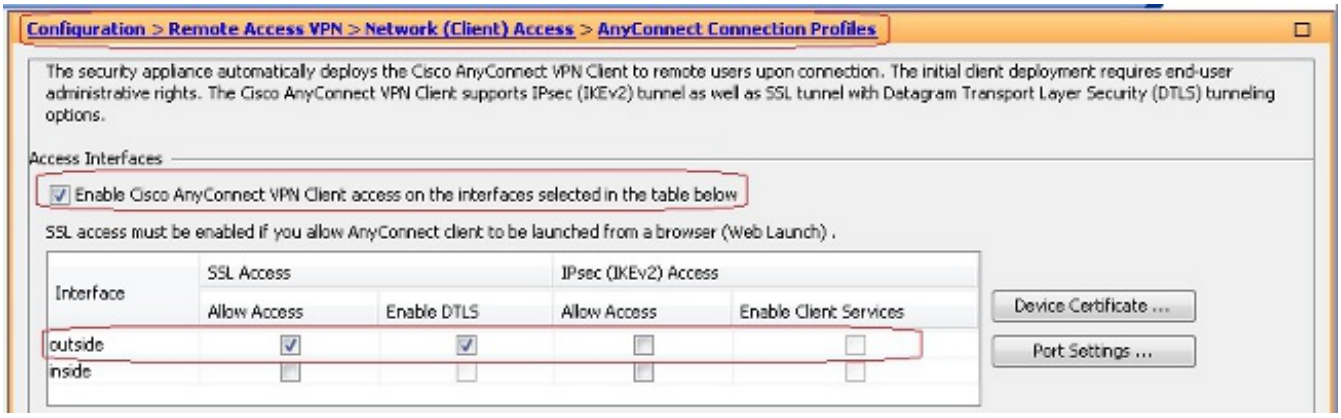
Konfigurieren des Cisco AnyConnect Secure Mobility Client

ASDM-Verfahren

Gehen Sie wie folgt vor, um das VPN für den Remote-Zugriff zu konfigurieren:

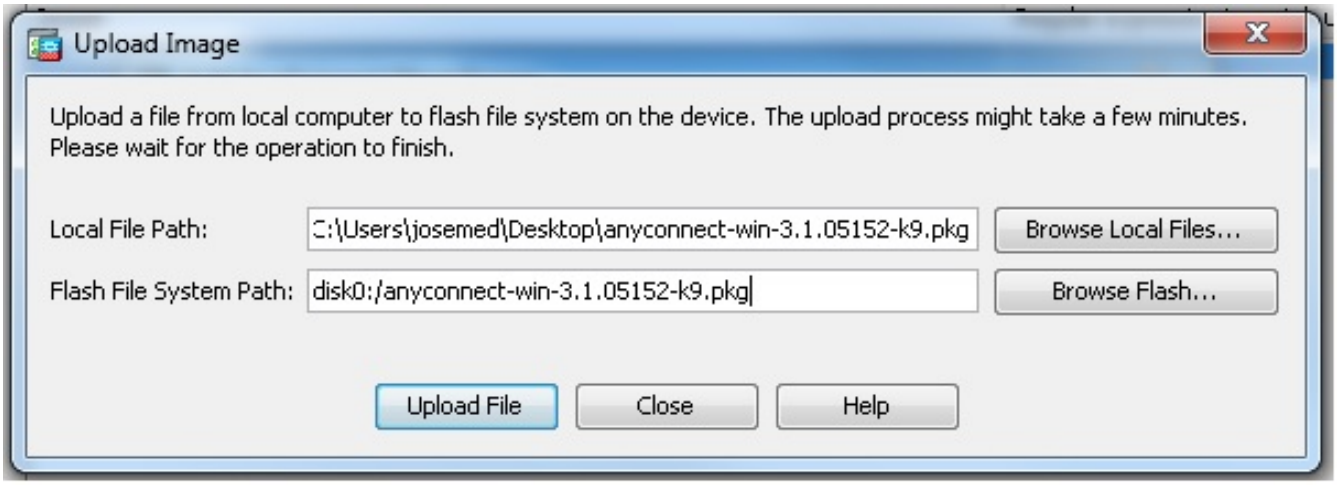
- Aktivieren Sie WebVPN.

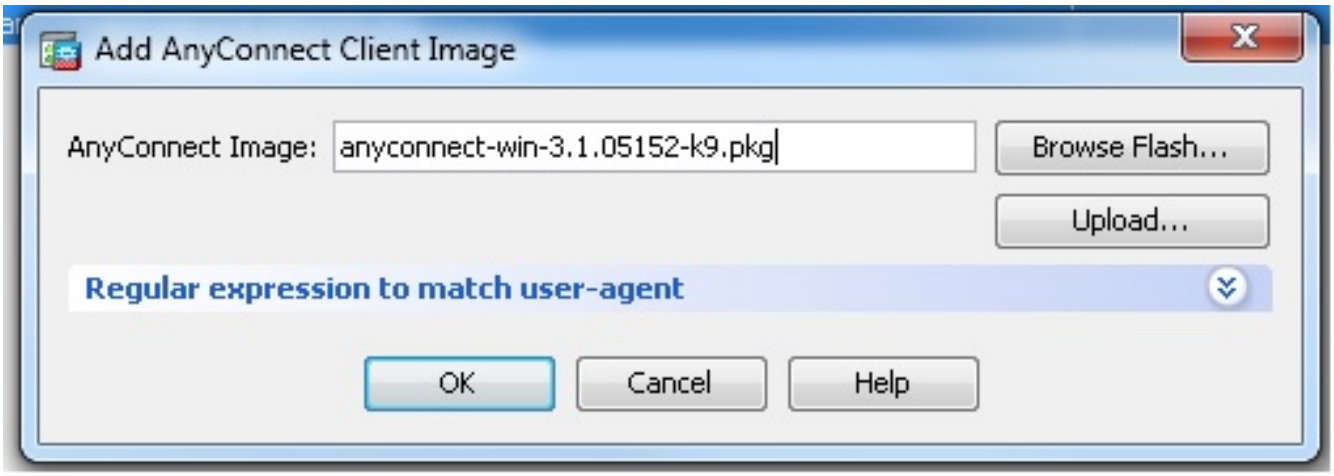
  Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** aus, und klicken Sie unter **Access Interfaces** auf die Kontrollkästchen **Allow Access** and **Enable DTLS** for the external interface. Aktivieren Sie außerdem das Kontrollkästchen **Enable Cisco AnyConnect VPN Client or Legacy SSL VPN Client access (Cisco AnyConnect VPN-Client oder Legacy-SSL VPN-Client-Zugriff aktivieren) in der in dieser Tabelle ausgewählten Schnittstelle**, um SSL VPN auf der externen Schnittstelle zu aktivieren.



Klicken Sie auf **Übernehmen**.

Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software > Add** aus, um das Cisco AnyConnect VPN Client-Image aus dem Flash-Speicher der ASA hinzuzufügen, wie gezeigt.



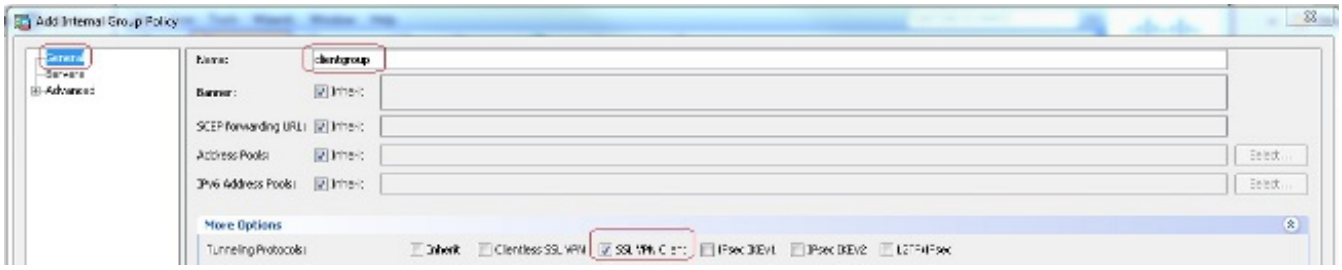


Entsprechende CLI-Konfiguration:

```
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
```

- Konfigurieren Sie die Gruppenrichtlinie.

  Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policies (Konfigurationsrichtlinien)**, um eine interne Gruppenrichtlinien-**Clientgruppe** zu erstellen. Aktivieren Sie auf der Registerkarte **Allgemein das** Kontrollkästchen **SSL VPN Client**, um SSL als Tunneling-Protokoll zu aktivieren.



  Konfigurieren Sie den DHCP-Netzwerkbereich auf der Registerkarte **Server**, und wählen Sie **More Options (Weitere Optionen) aus**, um den DHCP-Bereich für die automatisch zuzuweisenden Benutzer zu konfigurieren.

  Entsprechende CLI-Konfiguration:

```
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)#
```

- Wählen Sie **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add (Konfiguration > Remote-Access-VPN > AAA/Lokale Benutzer > Lokale Benutzer > Hinzufügen**, um ein neues Benutzerkonto **ssluser1** zu erstellen. Klicken Sie auf **OK** und dann auf
Übernehmen.

Entsprechende CLI-Konfiguration:

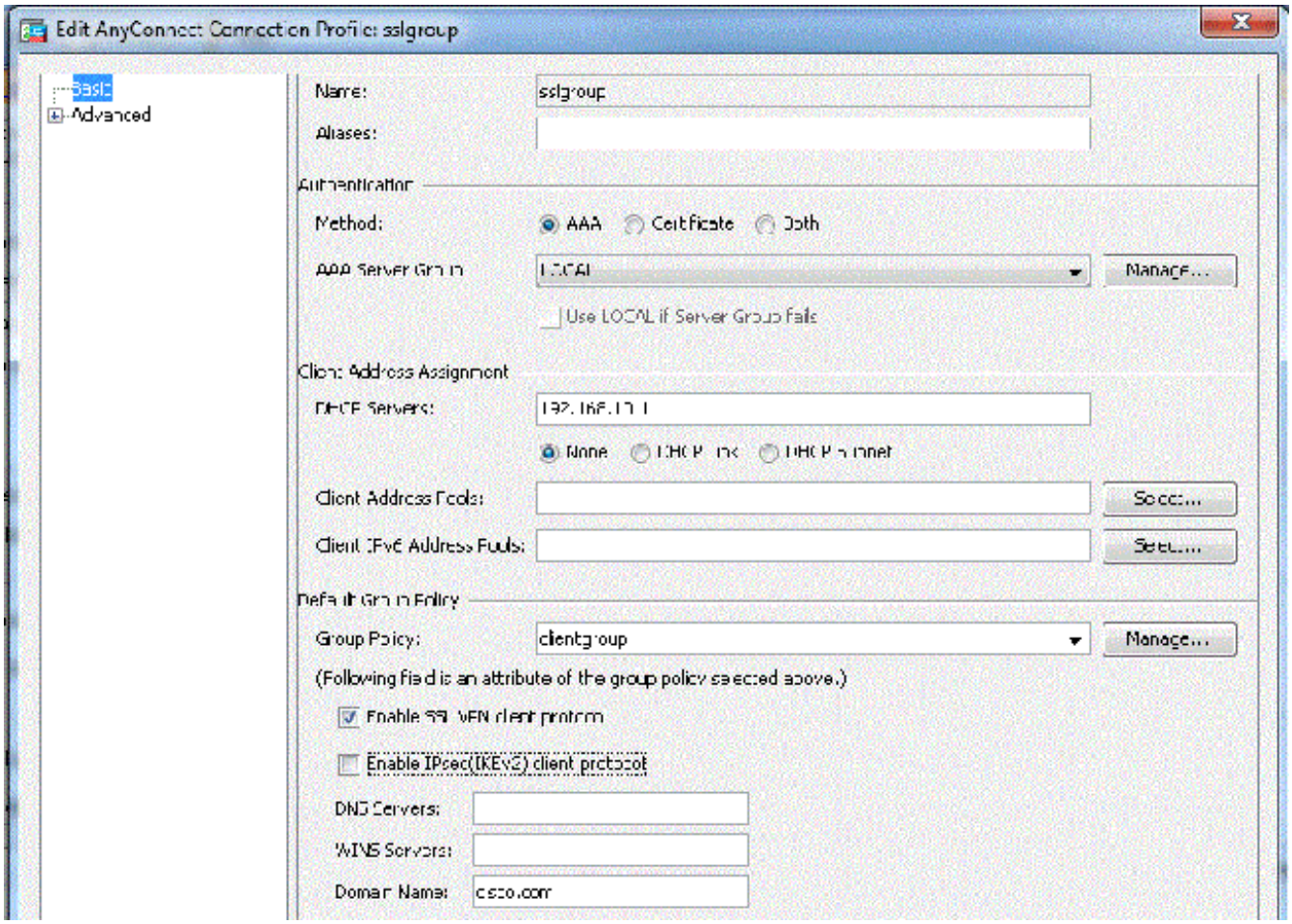
```
ciscoasa(config)#username ssluser1 password asdmASA
```

- Konfigurieren Sie die Tunnelgruppe.

Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** aus, um eine neue Tunnelgruppen-**SSL-Gruppe** zu erstellen.

Auf der Registerkarte **Basic** (Grundlegende) können Sie die folgende Konfigurationsliste ausführen:

Geben Sie der Tunnelgruppe den Namen **sslgroup**.Geben Sie die IP-Adresse des DHCP-Servers im für die **DHCP-Server** vorgesehenen Bereich ein.Wählen Sie unter Default Group Policy (Gruppenrichtlinie) die Gruppenrichtlinien-**Clientgruppe** aus der Dropdown-Liste Group Policy (Gruppenrichtlinie) aus.DHCP-Link oder DHCP-Subnetz konfigurieren



Geben Sie auf der Registerkarte **Erweitert > Gruppen-Alias/Gruppen-URL** den Namen des Gruppen-Alias als **sslgroup_users** an, und klicken Sie auf **OK**.

Entsprechende CLI-Konfiguration:

```
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
```

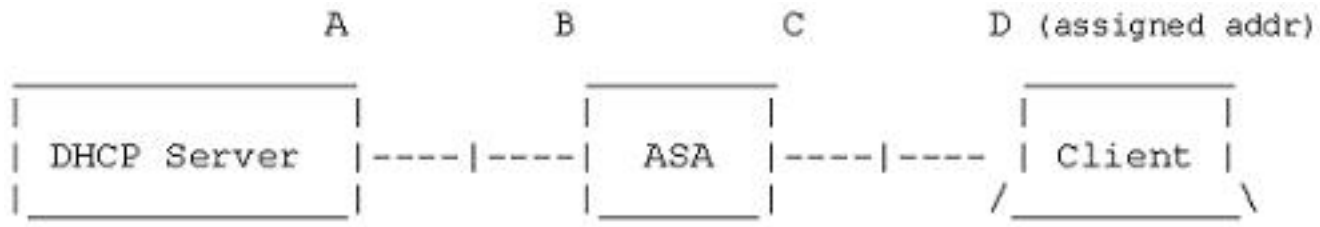
Subnetzauswahl oder Verbindungsauswahl

Die DHCP-Proxy-Unterstützung für RFC 3011 und RFC 3527 ist eine Funktion, die in den Versionen 8.0.5 und 8.2.2 eingeführt wurde und in späteren Versionen unterstützt wurde.

- RFC 3011 definiert eine neue DHCP-Option, die Subnetzauswahloption, mit der der DHCP-Client das Subnetz angeben kann, auf dem eine Adresse zugewiesen werden soll. Diese Option hat Vorrang vor der Methode, die der DHCP-Server zum Bestimmen des Subnetzes verwendet, in dem eine Adresse ausgewählt werden soll.
- RFC 3527 definiert eine neue DHCP-Unteroption, die Unteroption für die Verbindungsauswahl, mit der der DHCP-Client die Adresse angeben kann, auf die der DHCP-Server reagieren soll.

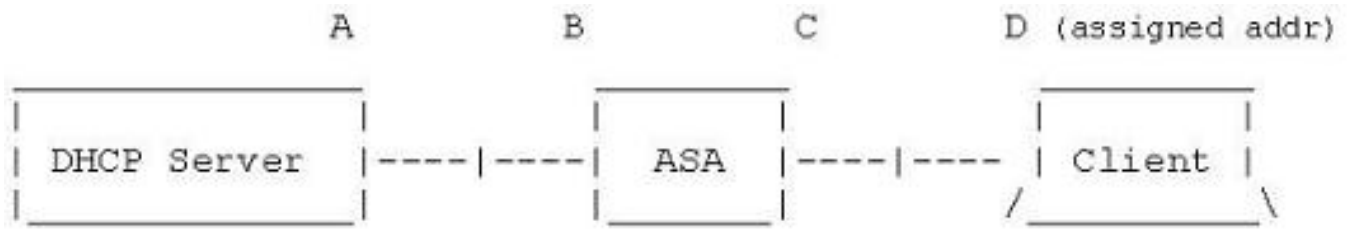
In Bezug auf die ASA ermöglichen diese RFCs einem Benutzer, einen DHCP-Netzwerkbereich für die DHCP-Adressenzuweisung anzugeben, der nicht lokal für die ASA ist, und der DHCP-Server kann weiterhin direkt auf die ASA-Schnittstelle antworten. Die folgenden Diagramme sollen helfen, das neue Verhalten zu veranschaulichen. Dadurch können nicht lokale Bereiche verwendet werden, ohne dass eine statische Route für diesen Bereich im Netzwerk erstellt werden muss.

Wenn RFC 3011 oder RFC 3527 nicht aktiviert ist, sieht der DHCP-Proxy-Austausch ähnlich aus wie folgt:




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

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

Wenn eine dieser RFCs aktiviert ist, sieht der Austausch ähnlich wie diese aus, und dem VPN-Client wird immer noch eine Adresse im richtigen Subnetz zugewiesen:




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

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

Konfigurieren der ASA mithilfe der CLI

Führen Sie diese Schritte aus, um den DHCP-Server so zu konfigurieren, dass den VPN-Clients über die Befehlszeile IP-Adressen bereitgestellt werden. Weitere Informationen zu den jeweils verwendeten Befehlen finden Sie unter Cisco Adaptive Security Appliances - Command References der Serie ASA 5500.

```
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#
```