Client d'Anyconnect à l'ASA avec l'utilisation du DHCP pour l'affectation d'adresses

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Produits connexes](#)
[Informations générales](#)
[Configurez](#)
[Diagramme du réseau](#)
[Configurez le Client à mobilité sécurisé Cisco AnyConnect](#)
[Configurez l'ASA avec l'utilisation du CLI](#)

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable de gamme Cisco 5500-X (ASA) pour inciter le serveur DHCP à fournir l'IP address de client à tous les clients d'Anyconnect avec l'utilisation d'Adaptive Security Device Manager (ASDM) ou du CLI.

Conditions préalables

Conditions requises

Ce document suppose que l´ASA est complètement opérationnel et configuré pour permettre au Cisco ASDM ou CLI d'apporter des modifications de configuration.

> **Note**: Référez-vous à l'ouvrage 1 : Guide de configuration général CLI d'exécutions de gamme de Cisco ASA, 9.2 pour permettre le périphérique à configurer à distance par l'ASDM ou Protocole Secure Shell (SSH).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 9.2(1) de Pare-feu de nouvelle génération de Cisco ASA 5500-X
- Version 7.1(6) d'Adaptive Security Device Manager
- Client à mobilité sécurisé Cisco AnyConnect 3.1.05152

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x et ultérieures de gamme 5500 d'appareils de Sécurité de Cisco ASA.

Informations générales

Les VPN d'accès à distance adressent la condition requise du collaborateur mobile pour se connecter en toute sécurité au réseau de l'entreprise. Les utilisateurs nomades peuvent installer une connexion sécurisée utilisant le logiciel de Client à mobilité sécurisé Cisco AnyConnect. Le Client à mobilité sécurisé Cisco AnyConnect initie une connexion à un lieu d'exploitation principal périphérique configuré pour recevoir ces demandes. Dans cet exemple, le périphérique de lieu d'exploitation principal est une appliance de sécurité adaptable de gamme 5500-X ASA qui utilise des crypto-cartes dynamiques.

En gestion d'adresses de dispositifs de sécurité, vous devez configurer les adresses IP qui connectent un client à une ressource sur le réseau privé, par le tunnel, et permettent le client de fonctionner comme si il ont été directement connectés au réseau privé.

En outre, vous traitez seulement les adresses IP privées qui sont assignées aux clients. Les adresses IP assignées à d'autres ressources sur votre réseau privé font partie de vos responsabilités d'administration réseau, pas une partie de Gestion VPN. Par conséquent, quand des adresses IP sont discutées ici, Cisco signifie ces adresses IP disponibles dans votre système d'adressage du réseau privé ce a permis la fonction de client comme périphérique du tunnel.

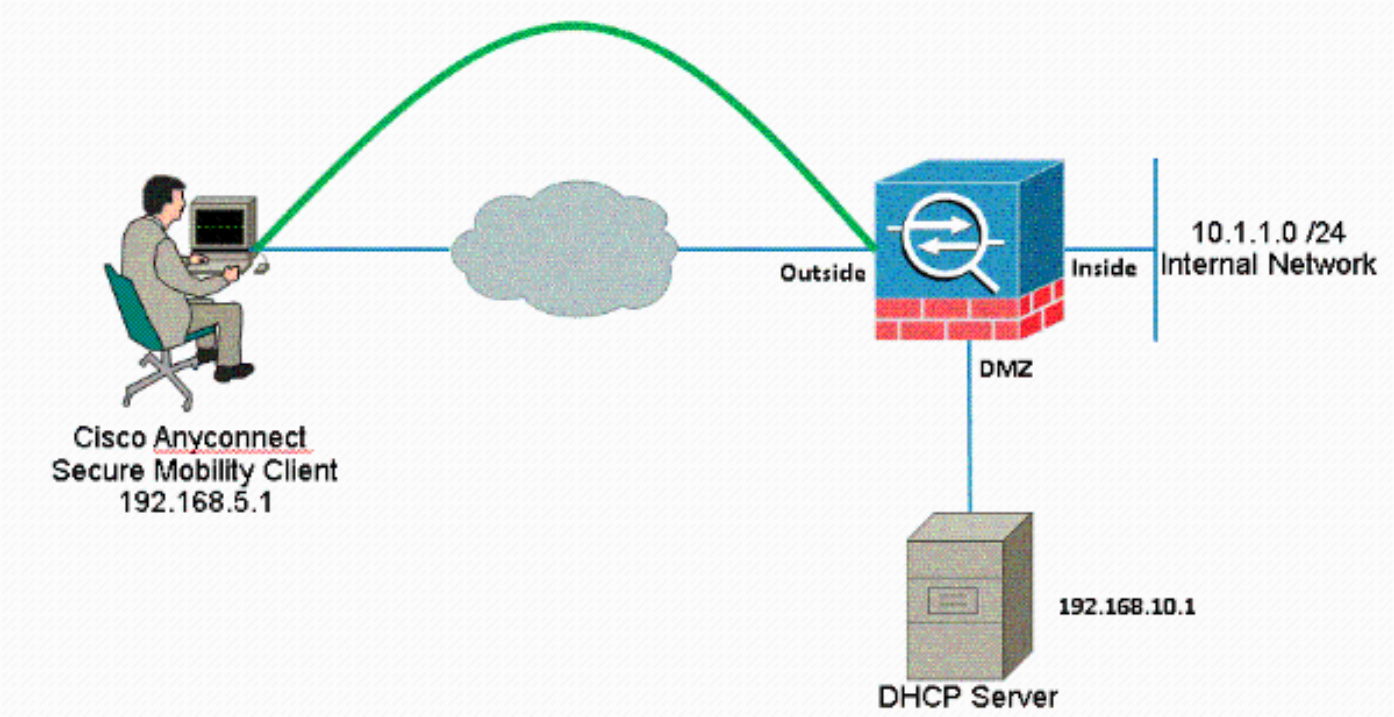
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Note: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

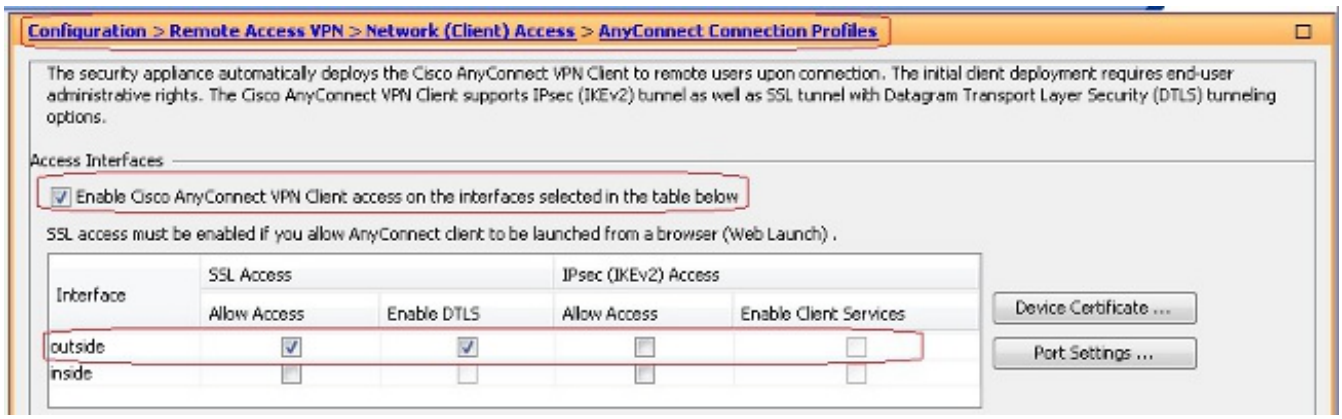
Configurez le Client à mobilité sécurisé Cisco AnyConnect

Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

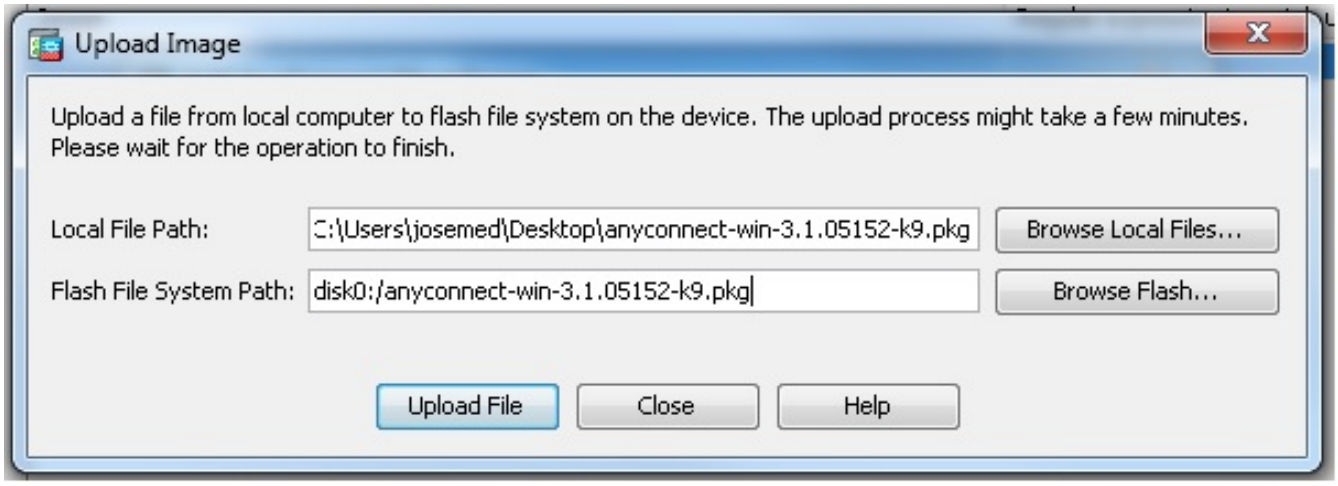
- Activez WebVPN.

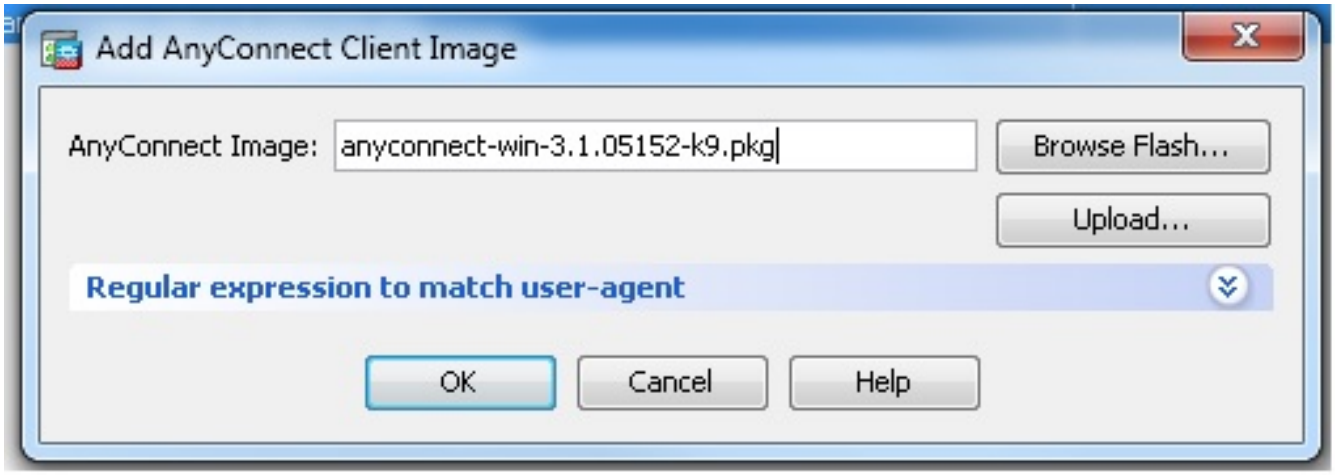
  Choisissez **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** et sous **Access Interfaces**, cliquez les cases à cocher **Allow Access** et **Enable DTLS** pour l'interface externe. En outre, cochez l'**accès client de VPN SSL de Cisco AnyConnect VPN Client ou de legs d'enable sur l'interface sélectionnée dans cette** case de **table** afin d'activer le VPN SSL sur l'interface extérieure.



Cliquez sur **Apply**.

Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > logiciel client d'Anyconnect > ajoutent** afin d'ajouter l'image de Cisco AnyConnect VPN Client de la mémoire flash de l'ASA comme affichée.



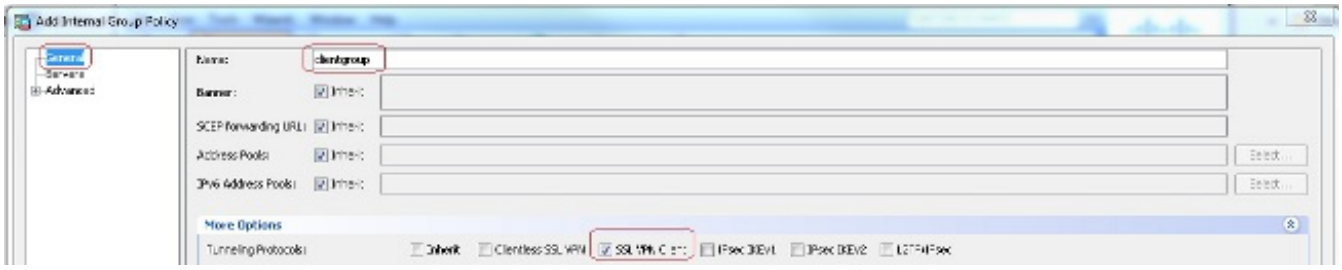


Configuration CLI équivalente :

```
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
```

- Configurez la stratégie de groupe.

Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** afin de créer une stratégie de groupe interne **clientgroup**. Sous l'**onglet Général**, sélectionnez la case de **client de VPN SSL** afin d'activer le SSL comme protocole de Tunnellisation.



Configurez la Réseau-portée DHCP dans l'onglet de **serveurs**, choisissez **plus d'options** afin de configurer la portée de DHCP pour que les utilisateurs soient assignés automatiquement.

Configuration CLI équivalente :

```
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
```

- Choisissez la **configuration > l'Accès à distance VPN > utilisateurs > utilisateurs locaux AAA/Local > ajoutent** afin de créer un nouveau compte utilisateur **ssluser1**. Cliquez sur **OK**, puis sur
Apply.

Configuration CLI équivalente :

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

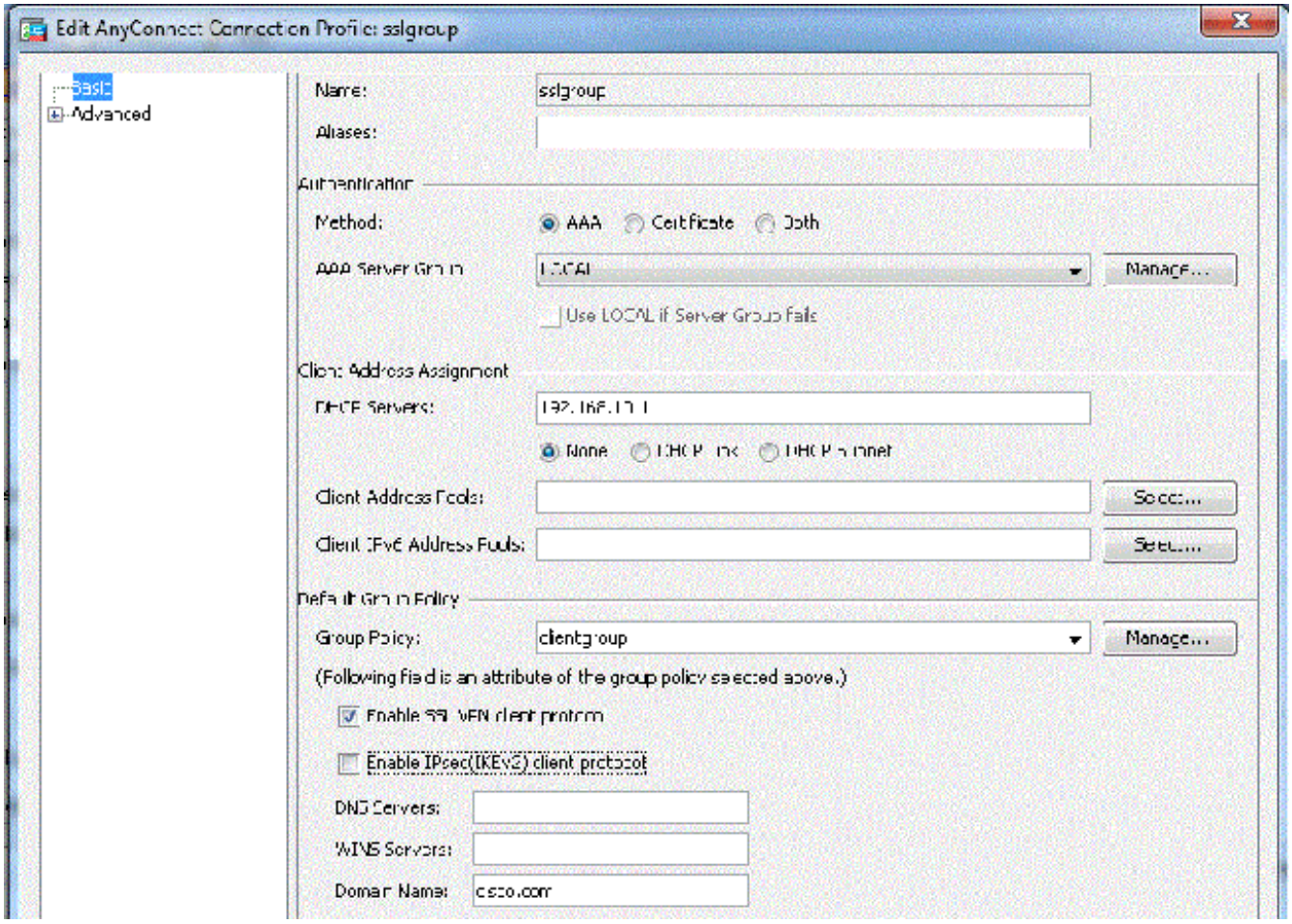
- Configurez le groupe de tunnels.

Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'Anyconnect > ajoutent** afin de créer un nouveau **sslgroup de** groupe de tunnel.

Dans l'onglet **Basic**, vous pouvez exécuter la liste des configurations indiquée :

Donnez au groupe de tunnels le nom **sslgroup**.Fournissez l'adresse IP de serveur DHCP dans

l'espace prévu pour des **serveurs DHCP**.Dans le cadre de la stratégie de groupe par défaut, choisissez le **clientgroup de** stratégie de groupe de la liste déroulante de stratégie de groupe.Configurez le lien DHCP ou le sous-réseau DHCP.



Sous l'**avancé > le groupe** onglet **URL alias/groupe**, spécifient le pseudonyme de groupe comme **sslgroup_users** et cliquent sur OK.

Configuration CLI équivalente :

```
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
```

Sous-réseau-sélection ou Lien-sélection

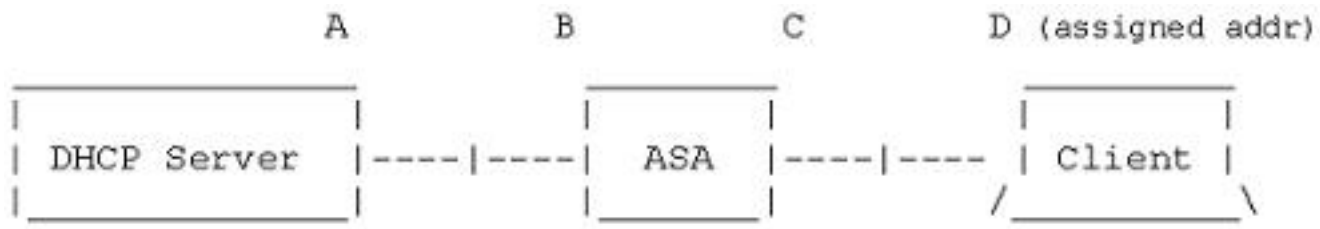
Le soutien de proxy DHCP de RFC 3011 et de RFC 3527 est une fonctionnalité introduite dans les 8.0.5 et les 8.2.2 et il a été pris en charge dans des releases en avant.

- RFC 3011 définit une nouvelle option DHCP, l'option de sélection de sous-réseau, qui permet au DHCP Client pour spécifier le sous-réseau sur lequel pour allouer une adresse. Cette option a la priorité au-dessus de la méthode que le serveur DHCP l'utilise pour déterminer le sous-réseau sur lequel pour sélectionner une adresse.

- RFC 3527 définit un nouveau suboption DHCP, le suboption de sélection de lien, qui permet au DHCP Client pour spécifier l'adresse à laquelle le serveur DHCP devrait répondre.

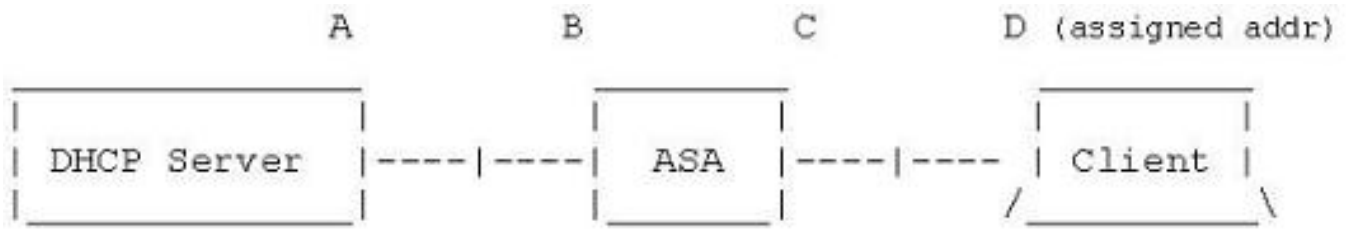
En termes d'ASA, ces RFC permettront à un utilisateur pour spécifier une DHCP-réseau-portée pour l'affectation d'adresses DHCP qui n'est pas locale à l'ASA, et le serveur DHCP pourra toujours répondre directement à l'interface de l'ASA. Les diagrammes ci-dessous devraient aider à montrer le nouveau comportement. Ceci permettra les portées de non-gens du pays d'utilisation sans devoir créer une artère statique pour cette portée dans leur réseau.

Quand RFC 3011 ou RFC 3527 n'est pas activé, l'échange de proxy DHCP semble semblable à ceci :




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

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

Avec l'un ou l'autre de ces RFC activés, l'échange semble semblable à ceci à la place, et le client vpn est encore assigné une adresse dans le sous-réseau correct :



Message Exchange:

Discover: B -> A

Offer: A -> B

Request: B -> A

Ack: A -> B

Release: B -> A

Configurez l'ASA avec l'utilisation du CLI

Terminez-vous ces étapes afin de configurer le serveur DHCP pour fournir l'adresse IP aux clients vpn de la ligne de commande. Référez-vous aux [références adaptatives d'Appliance-commande de Sécurité de gamme de Cisco ASA 5500](#) pour plus d'informations sur chaque commande qui est utilisée.

```
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#
```