주소 할당을 위해 DHCP를 사용하는 AnyConnect Client to ASA

목차

소개

이 문서에서는 DHCP 서버가 ASDM(Adaptive Security Device Manager) 또는 CLI를 사용하여 모든 AnyConnect 클라이언트에 클라이언트 IP 주소를 제공하도록 Cisco 5500-X Series ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 ASA가 완전히 작동 중이고 Cisco ASDM 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

> **참고**: 1 장부 참조:Cisco ASA Series General Operations CLI Configuration Guide, 9.2 - ASDM 또는 SSH(Secure Shell)에서 디바이스를 원격으로 구성할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500-X Next Generation Firewall 버전 9.2(1)
- Adaptive Security Device Manager 버전 7.1(6)

- Cisco AnyConnect Secure Mobility Client 3.1.05152

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 Cisco ASA Security Appliance 5500 Series 버전 7.x 이상에서도 사용할 수 있습니다.

배경 정보

원격 액세스 VPN은 모바일 인력이 조직의 네트워크에 안전하게 연결해야 하는 요구 사항을 해결합니다.모바일 사용자는 Cisco Anyconnect Secure Mobility Client 소프트웨어를 사용하여 보안 연결을 설정할 수 있습니다.Cisco Anyconnect Secure Mobility Client는 이러한 요청을 수락하도록 구성된 중앙 사이트 디바이스에 대한 연결을 시작합니다.이 예에서 중앙 사이트 디바이스는 동적 암호화 맵을 사용하는 ASA 5500-X Series Adaptive Security Appliance입니다.

보안 어플라이언스 주소 관리에서는 터널을 통해 사설 네트워크의 리소스와 클라이언트를 연결하는 IP 주소를 구성하고 클라이언트가 사설 네트워크에 직접 연결된 것처럼 작동하도록 해야 합니다.

또한 클라이언트에 할당된 전용 IP 주소만 처리합니다.사설 네트워크의 다른 리소스에 할당된 IP 주소는 VPN 관리의 일부가 아니라 네트워크 관리 권한의 일부입니다.따라서 여기에서 IP 주소를 설명하는 경우 Cisco는 클라이언트가 터널 엔드포인트로 작동하도록 하는 사설 네트워크 주소 지정 체계에서 사용 가능한 IP 주소를 의미합니다.

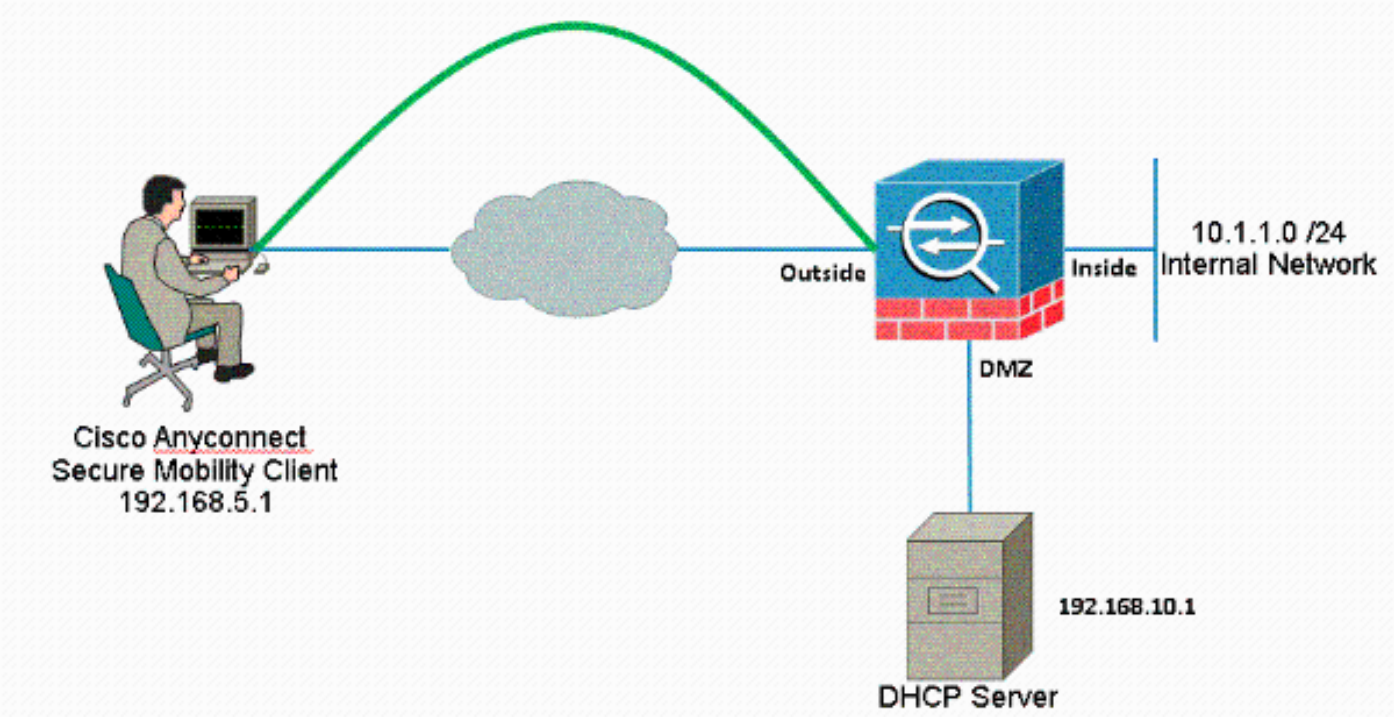
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

> **참고**: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

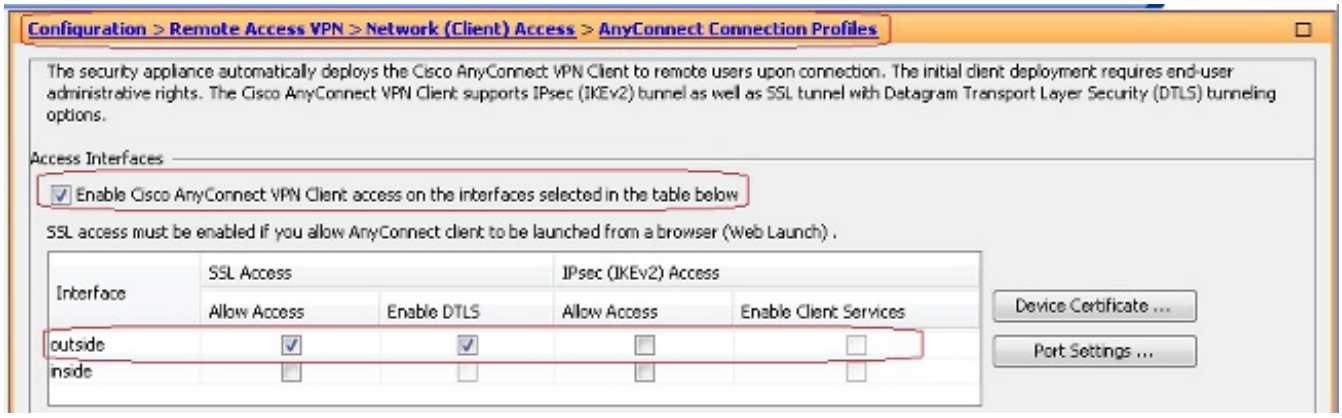
Cisco Anyconnect Secure Mobility Client 구성

ASDM 절차

원격 액세스 VPN을 구성하려면 다음 단계를 완료합니다.

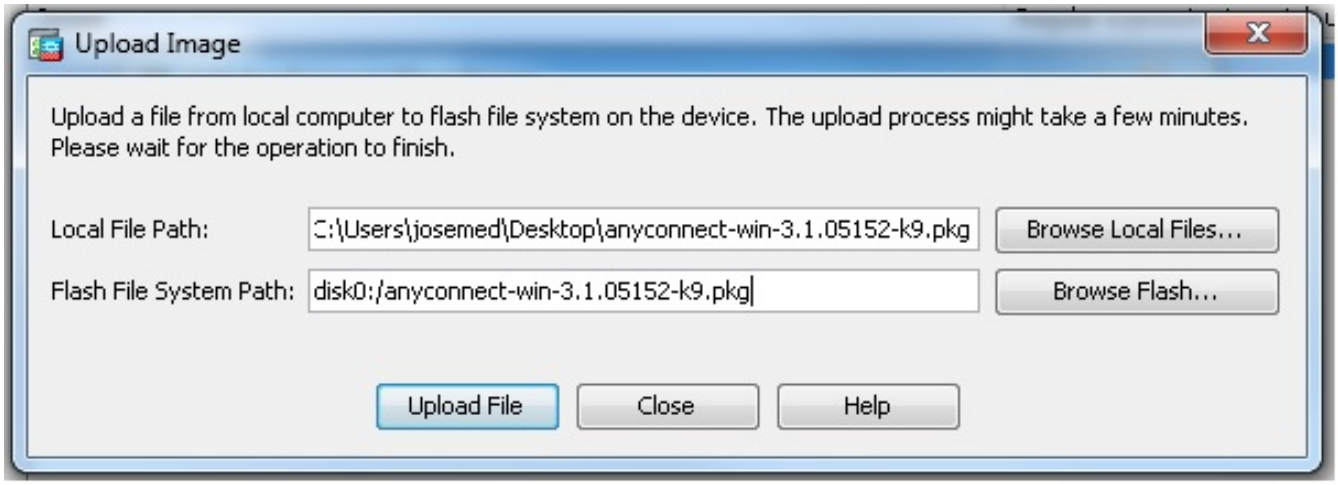
- WebVPN을 활성화합니다.

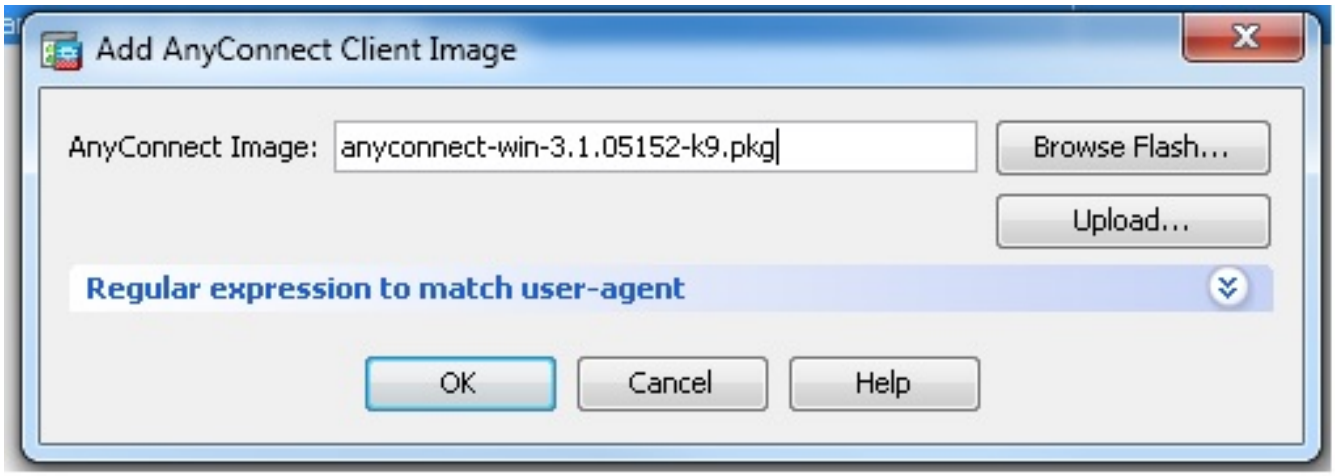
  Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > SSL VPN Connection Profiles(SSL VPN 연결 프로파일)를 선택하고 Access Interfaces(액세스 인터페이스**)에서 Allow Access(**액세스 허용**) 및 **Enable DTLS for the** outside interface(외부 인터페이스에 대해 DTLS 활성화)를 클릭합니다.또한 외부 인터페이스에서 SSL **VPN을 활성화하려면 Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface(이 표에서 선택한 인터페이스**에서 **Cisco AnyConnect VPN 클라이언트 또는 레거시 SSL VPN 클라이언트 액세스 활성화**) 확인란을 선택합니다.



Apply를 **클릭합니다**.

Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Anyconnect Client Software(Anyconnect 클라이언트 소프트웨어) > Add(추가)를 선택하여** ASA의 플래시 메모리에서 Cisco AnyConnect VPN 클라이언트 이미지를 추가합니다.



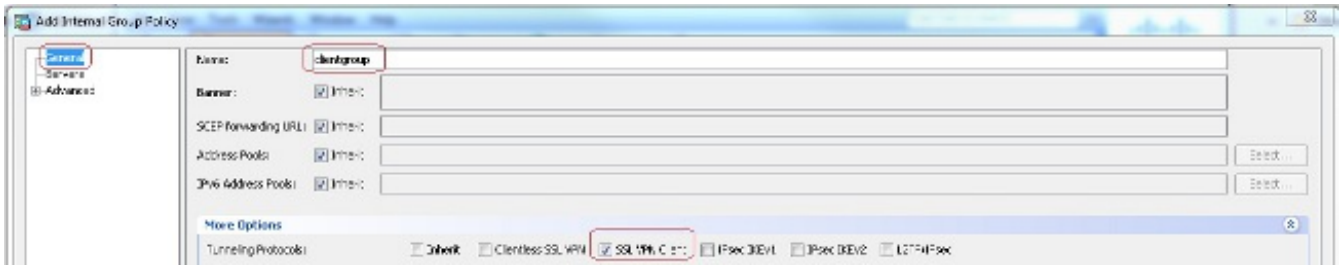


동일한 CLI 구성:

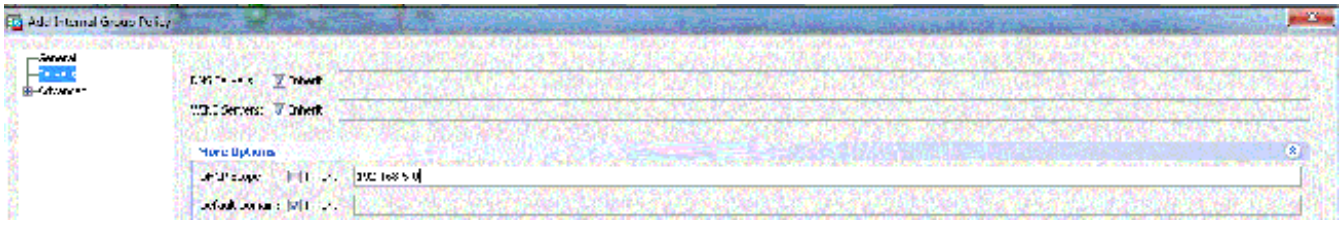
```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

- 그룹 정책을 구성합니다.

내부 그룹 정책 **클라이언트 그룹을** 생성하려면 Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책)를 선택합니다**.SSL을 터널링 프로토콜로 활성화하려면 **General** 탭에서 **SSL VPN Client** 확인란을 선택합니다.



Servers(**서버**) 탭에서 DHCP Network-Scope(DHCP 네트워크 범위)를 구성하고 **More Options(추가 옵션)**를 선택하여 사용자가 자동으로 할당되도록 DHCP 범위를 구성합니다.



동일한 CLI 구성:

```
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)#
```

- 새 사용자 계정 ssluser1**을** 생성하려면 **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add**를 선택합니다. **OK**를 클릭한 다음 **Apply를 클릭합니다**

.

동일한 CLI 구성:

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

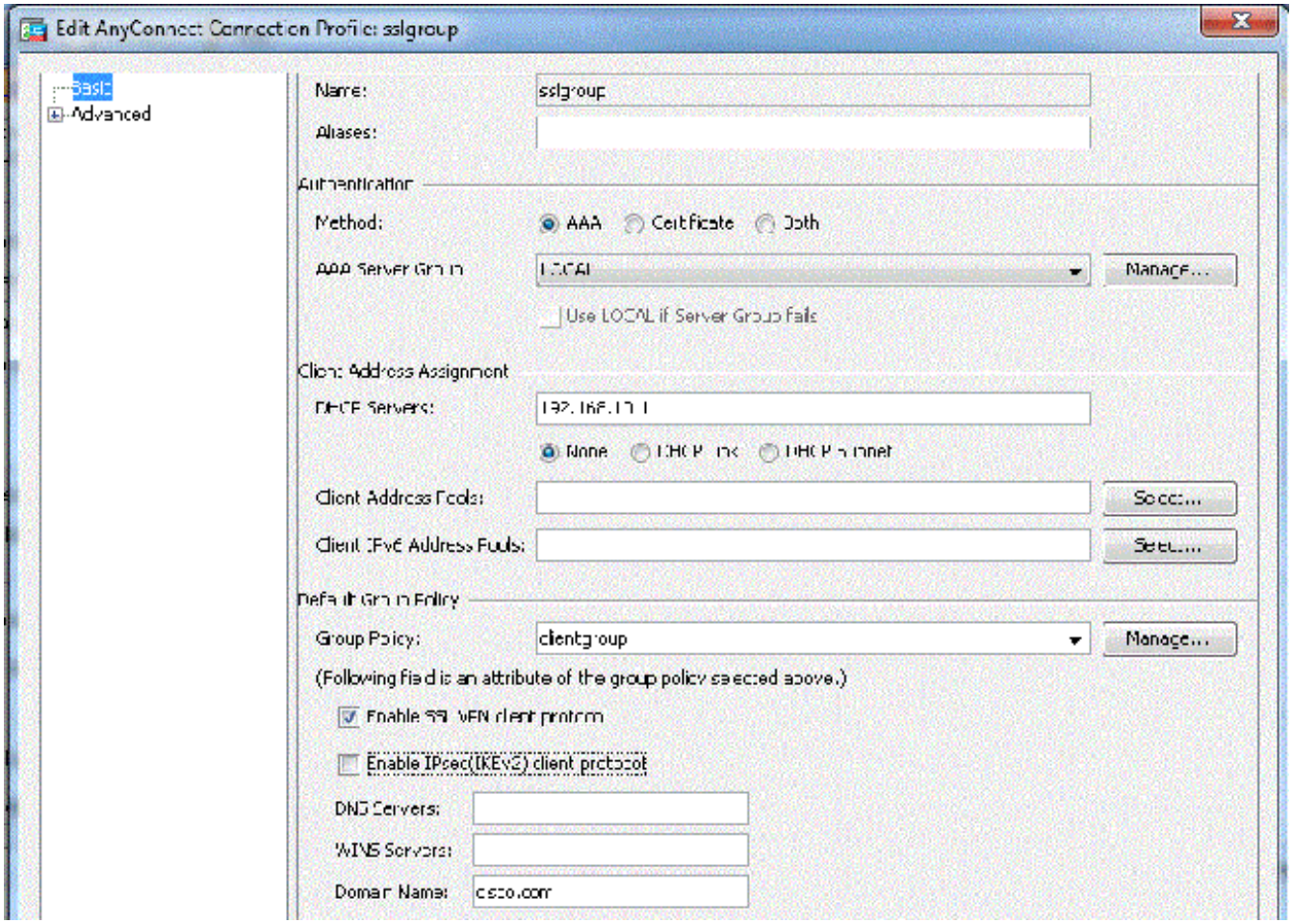
- 터널 그룹을 구성합니다.

새 터널 그룹 sslgroup을 생성하려면 **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add**를 **선택합니다**.

Basic(**기본**) 탭에서 다음과 같이 구성 목록을 수행할 수 있습니다.

터널 그룹의 이름을 sslgroup으로 **지정합니다**.DHCP 서버에 제공된 공간에 DHCP 서버 IP 주소를 **제공합니다**.Default Group Policy(기본 그룹 정책)의 Group **Policy(그룹 정책)** 드롭다운 목

록에서 그룹 정책 클라이언트 그룹을 선택합니다.DHCP 링크 또는 DHCP 서브넷을 구성합니다.



Advanced(**고급**) > **Group Alias/Group URL(그룹 별칭/그룹 URL**) 탭에서 그룹 별칭 이름을 sslgroup_**users**로 지정하고 **OK(확인)**를 클릭합니다.

동일한 CLI 구성:

```
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
```

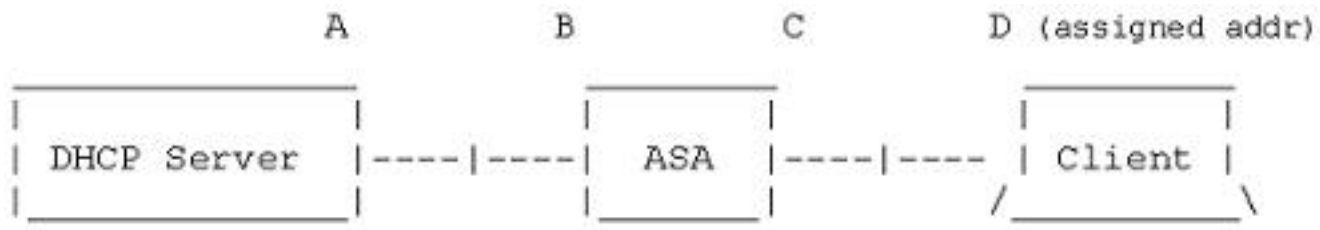
서브넷 선택 또는 링크 선택

RFC 3011 및 RFC 3527에 대한 DHCP 프록시 지원은 8.0.5 및 8.2.2에 도입된 기능이며 이후 릴리스에서 지원됩니다.

- RFC 3011은 DHCP 클라이언트가 주소를 할당할 서브넷을 지정할 수 있도록 하는 새로운 DHCP 옵션인 서브넷 선택 옵션을 정의합니다.이 옵션은 DHCP 서버가 주소를 선택할 서브넷을 결정하는 데 사용하는 방법보다 우선합니다.
- RFC 3527은 DHCP 클라이언트가 DHCP 서버가 응답할 주소를 지정할 수 있도록 하는 링크 선택 하위 옵션인 새 DHCP 하위 옵션을 정의합니다.

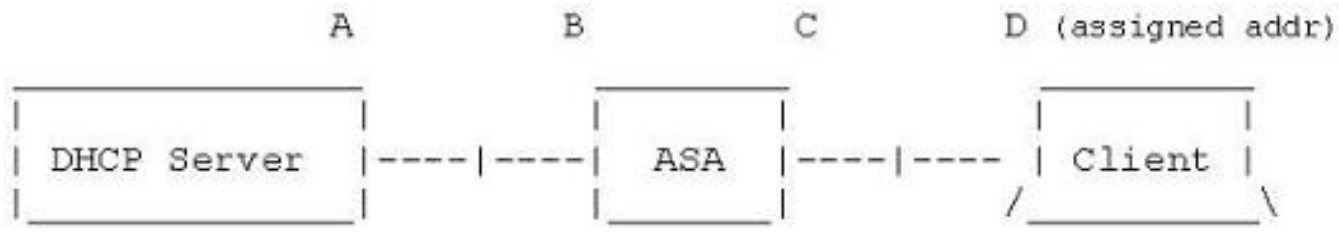
ASA의 관점에서 이러한 RFC를 통해 사용자는 ASA에 로컬이 아닌 DHCP 주소 할당을 위한 dhcp-network-scope를 지정할 수 있으며, DHCP 서버는 여전히 ASA의 인터페이스에 직접 응답할 수 있습니다.아래 다이어그램은 새 동작을 설명하는 데 도움이 됩니다.이렇게 하면 네트워크에서 해당 범위에 대한 고정 경로를 생성할 필요 없이 로컬이 아닌 범위를 사용할 수 있습니다.

RFC 3011 또는 RFC 3527이 활성화되지 않으면 DHCP 프록시 교환은 다음과 유사합니다.




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

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

이러한 RFC 중 하나를 활성화하면 교환이 이와 비슷하게 보이고 VPN 클라이언트에는 여전히 올바른 서브넷에 주소가 할당됩니다.




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

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

CLI를 사용하여 ASA 구성

명령행에서 VPN 클라이언트에 IP 주소를 제공하도록 DHCP 서버를 구성하려면 다음 단계를 완료합니다.사용되는 각 명령에 대한 자세한 내용은 Cisco ASA 5500 Series Adaptive Security Appliances-명령 참조를 참조하십시오.

```
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#
```