ASA 9.X에서 AnyConnect VPN 클라이언트 U-turn 트래픽 구성

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) Release 9.X를 설정하여 VPN 트래픽을 u-turn할 수 있도록 하는 방법에 대해 설명합니다. 이 구성 시나리오를 다룹니다. 원격 액세스 클라이언트에서 트래픽을 U턴합니다.

> **참고:** 네트워크에서 IP 주소가 중복되지 않도록 하려면 VPN 클라이언트에 완전히 다른 IP 주소 풀(예: 10.x.x.x, 172.16.x.x 및 192.168.x.x)을 할당합니다. 이 IP 주소 체계는 네트워크 문제를 해결하는 데 유용합니다.

헤어핀 또는 U-턴

이 기능은 인터페이스로 들어가지만 동일한 인터페이스에서 라우팅되는 VPN 트래픽에 유용합니다. 예를 들어, 보안 어플라이언스가 허브이고 원격 VPN 네트워크가 스포크인 허브 앤 스포크 VPN 네트워크가 있는 경우 한 스포크가 다른 스포크 트래픽과 통신하려면 보안 어플라이언스로 이동한 다음 다시 다른 스포크로 나가야 합니다.

다음을 입력합니다. **same-security-traffic** 명령을 사용하여 트래픽이 동일한 인터페이스로 들어오고 나가도록 허용합니다.

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요건을 충족하는 것이 좋습니다.

- 허브 ASA Security Appliance는 Release 9.x를 실행해야 합니다.
- Cisco AnyConnect VPN Client 3.x**참고:** AnyConnect VPN 클라이언트 패키지 다운로드 (anyconnect-win*.pkg) Cisco 소프트웨어 다운로드(등록된 고객만 해당) AnyConnect VPN 클라이언트를 Cisco ASA 플래시 메모리에 복사합니다. 이 플래시 메모리는 ASA와 SSL VPN 연결을 설정하기 위해 원격 사용자 컴퓨터에 다운로드됩니다. 자세한 내용은 ASA 컨피그레이션 가이드의 AnyConnect VPN 클라이언트 연결 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.1(2)을 실행하는 Cisco 5500 Series ASA
- Windows 3.1.05152용 Cisco AnyConnect SSL VPN 클라이언트 버전
- 지원되는 VPN 플랫폼인 Cisco ASA Series에 따라 지원되는 OS를 실행하는 PC.
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.1(6)

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

배경 정보

Cisco AnyConnect VPN Client는 원격 사용자를 위해 보안 어플라이언스에 대한 보안 SSL 연결을 제공합니다. 이전에 설치된 클라이언트가 없으면 원격 사용자는 SSL VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. 보안 어플라이언스가 리디렉션하도록 구성되지 않은 경우 **http://** 요청 **https://**, 사용자는 양식에 URL을 입력해야 합니다. **https://**

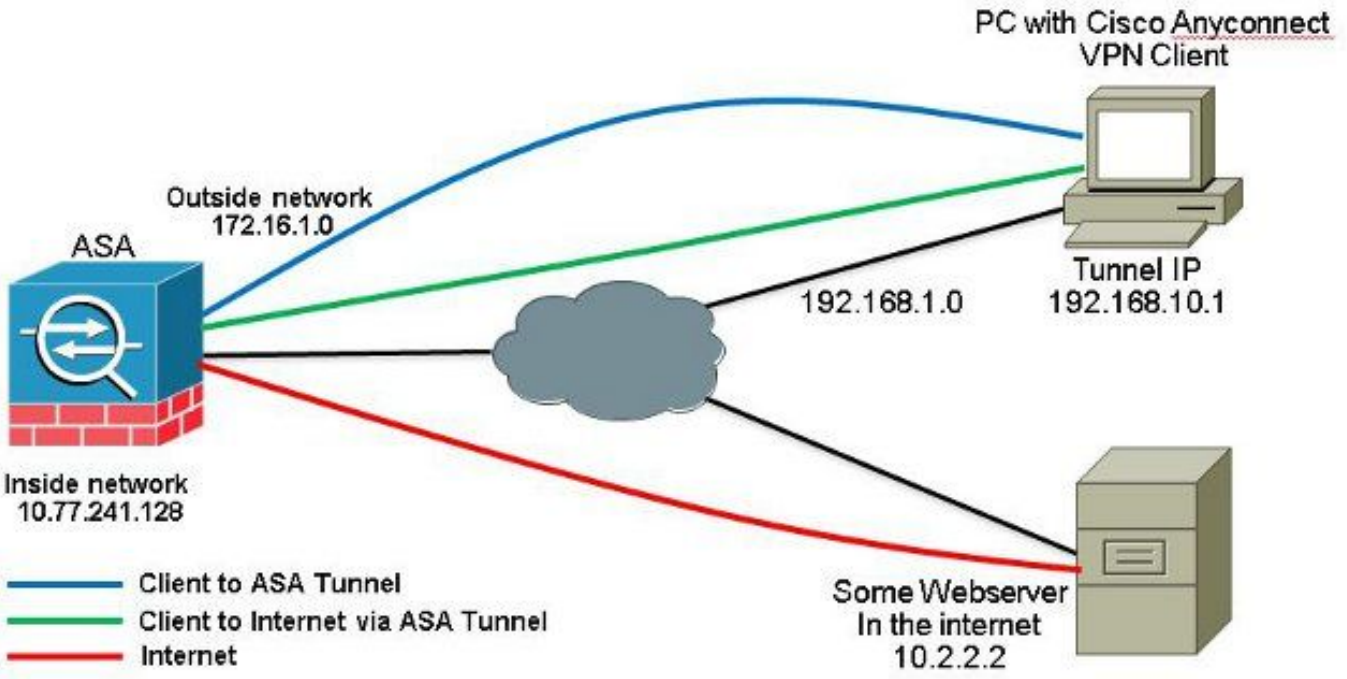
.URL을 입력하면 브라우저가 해당 인터페이스에 연결되고 로그인 화면이 표시됩니다. 사용자가 로그인 및 인증을 충족하고 보안 어플라이언스가 클라이언트가 필요한 사용자를 식별하면 원격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드 후 클라이언트는 자신을 설치하고 구성하며 보안 SSL 연결을 설정하고 연결이 종료되면 그대로 유지되거나 자동으로 제거됩니다(보안 어플라이언스 구성에 따라 다름).이전에 설치된 클라이언트의 경우 사용자가 인증하면 보안 어플라이언스는 클라이언트의 수정 버전을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.클라이언트가 보안 어플라이언스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security)에 연결하고 DTLS(Datagram Transport Layer Security)도 사용합니다. DTLS는 일부 SSL 연결과 관련된 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 향상시킵니다.AnyConnect 클라이언트는 보안 어플라이언스에서 다운로드할 수도 있고 시스템 관리자가 원격 PC에 수동으로 설치할 수도 있습니다. 클라이언트를 수동으로 설치하는 방법에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 설명서를 참조하십시오.보안

*어플라이언스는 연결을 설정하는 사용자의 그룹 정책 또는 사용자 이름 특성에 따라 클라이언트를 다운로드합니다. 클라이언트를 자동으로 다운로드하도록 보안 어플라이언스를 구성하거나, 원격 사용자에게 클라이언트 다운로드 여부를 묻는 메시지를 표시하도록 구성할 수 있습니다. 후자의 경우 사용자가 응답하지 않을 경우 시간 초과 기간 후에 클라이언트를 다운로드하거나 로그인 페이지를 표시하도록 보안 어플라이언스를 구성할 수 있습니다.**참고:** 이 문서에 사용된 예는 IPv4를 사용합니다. IPv6 U-turn 트래픽의 경우 단계는 동일하지만 IPv4 대신 IPv6 주소를 사용합니다.*

U-turn 원격 액세스 트래픽 구성

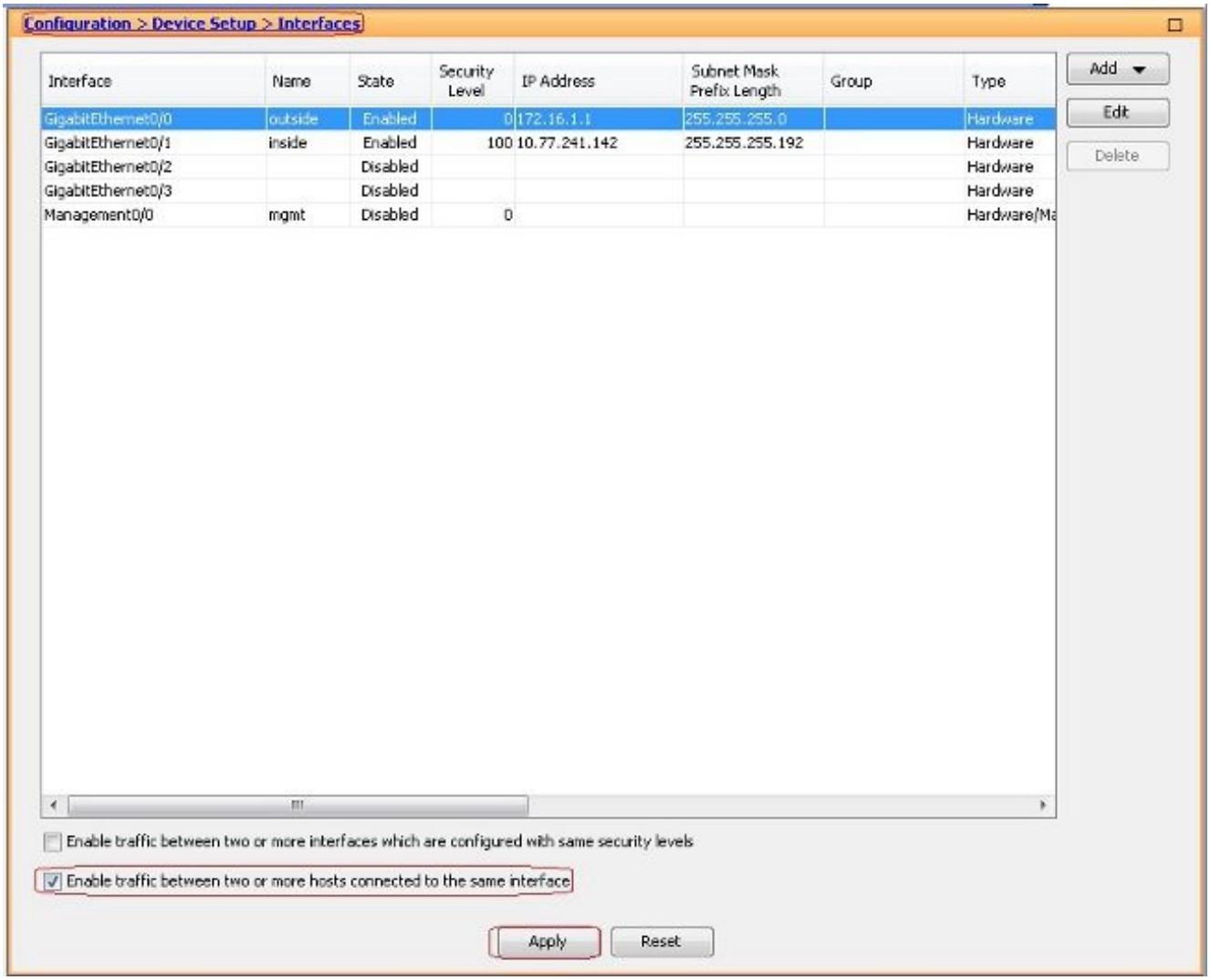
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.참고: 이 섹션에서 사용되는 명령에 대한 자세한 내용을 보려면 명령 참조 안내서를 사용하십시오.Stick 컨피그레이션의 공용 인터넷 VPN용 AnyConnect VPN 클라이언트 예네트워크 다이어그램이 문서에서는 이 네트워크 설정을 사용합니다

.



ASDM 릴리스 7.1(6)을 사용하는 ASA 릴리스 9.1(2) 컨피그레이션이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 이미 완료되었으며 제대로 작동한다고 가정합니다.참고: ASDM에서 ASA를 구성할 수 있도록 하려면 관리 액세스 구성을 참조하십시오.참고: 릴리스 8.0(2) 이상에서 ASA는 외부 인터페이스의 포트 443에서 클라이언트리스 SSL VPN(WebVPN) 세션 및 ASDM 관리 세션을 동시에 지원합니다. 릴리스 8.0(2) 이전 버전에서는 포트 번호를 변경하지 않는 한 동일한 ASA 인터페이스에서 WebVPN 및 ASDM을 활성화할 수 없습니다. 자세한 내용은 ASA의 동일한 인터페이스에서 활성화된 ASDM 및 WebVPN을 참조하십시오.ASA에서 스틱에 SSL VPN을 구성하려면 다음 단계를 완료하십시오.

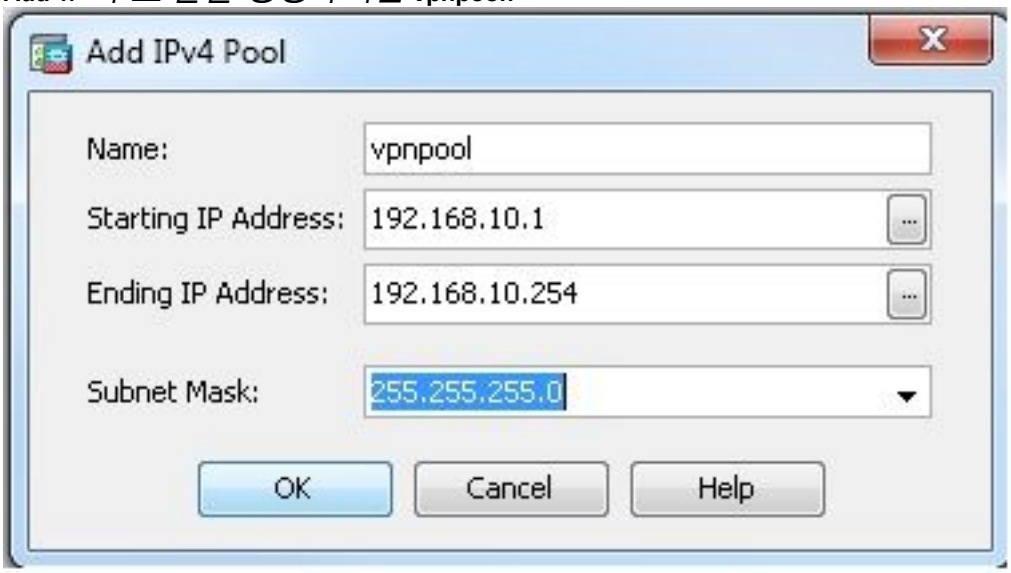
1. *선택* **Configuration > Device Setup > Interfaces** *및* **Enable traffic between two or more hosts connected to the same interface** *SSL VPN 트래픽이 동일한 인터페이스로 들어오고 나가도록 허용하려면 확인란을 선택합니다. 클릭* **Apply**.



동등한 CLI 컨피그레이션:

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

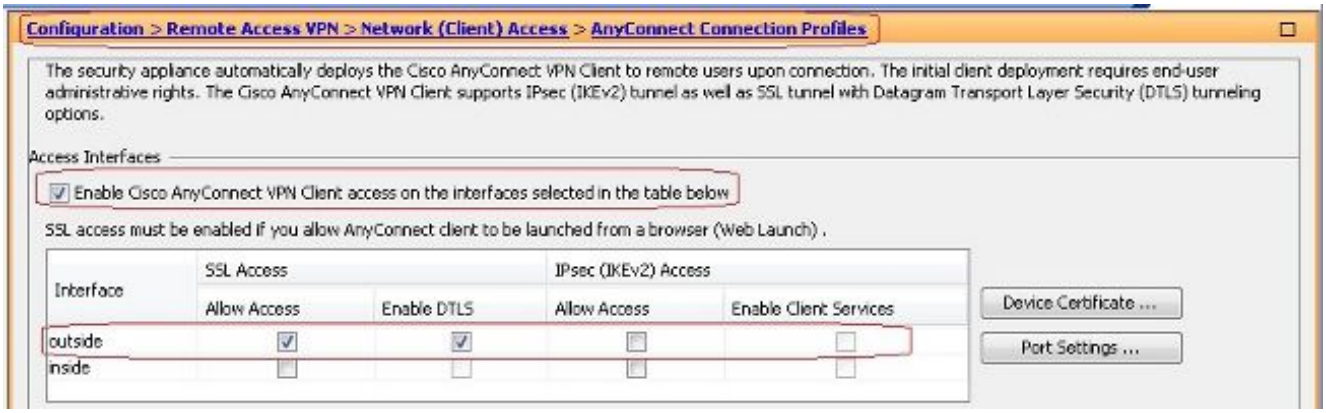
2. *선택* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *IP 주소 풀을 생성하려면* **vpnpool**.



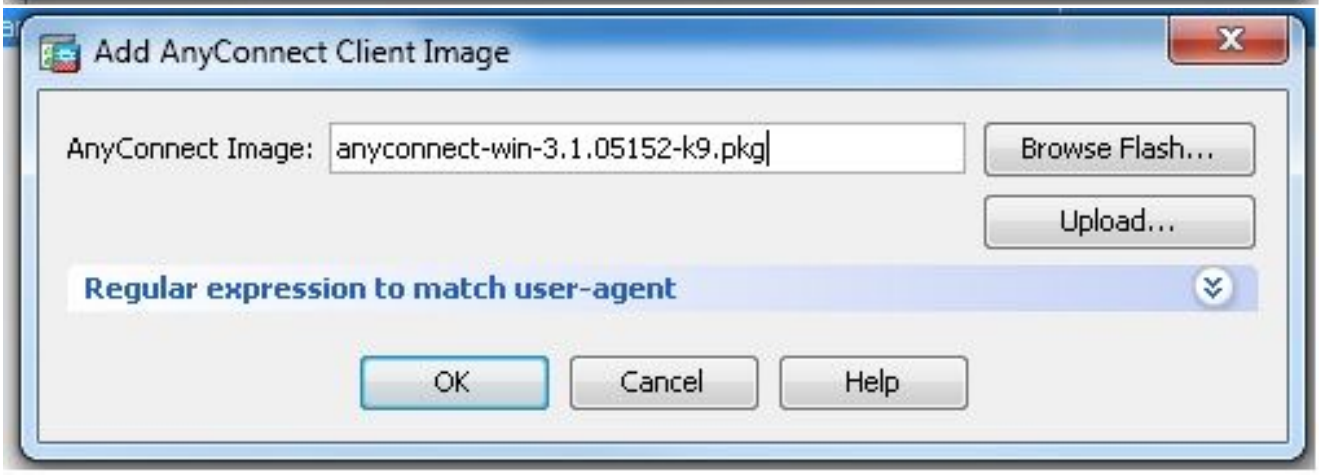
3. *클릭* **Apply**. ***동등한 CLI 컨피그레이션:***

```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

4. *WebVPN을 활성화합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *및 아래에* **Access Interfaces**, *확인란을 클릭합니다* **Allow Access** *및* **Enable DTLS** *외부 인터페이스용입니다. 또한* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *외부 인터페이스에서 SSL VPN을 활성화하려면 확인란을 선택합니다.*



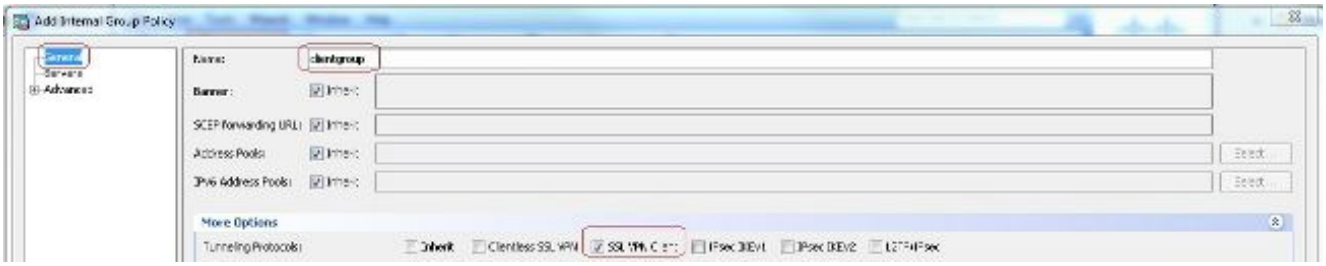
클릭 **Apply**. *선택* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *그림과 같이 ASA의 플래시 메모리에서 Cisco AnyConnect VPN 클라이언트 이미지를 추가합니다.*



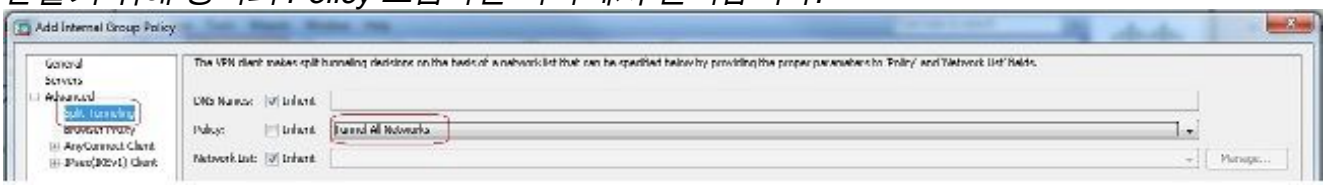
동등한 CLI 컨피그레이션:

```
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
```

5. *그룹 정책을 구성합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *내부 그룹 정책을 생성하려면* **clientgroup**. *아래* **General** *탭에서* **SSL VPN Client** *터널 프로토콜로 WebVPN을 활성화하려면 확인란을 선택합니다.*



의 **Advanced > Split Tunneling** *탭, 선택* **Tunnel All Networks** *보안 터널을 통해 원격 PC의 모든 패킷을 만들기 위해 정책의 Policy 드롭다운 목록에서 선택합니다.*



동등한 CLI 컨피그레이션:

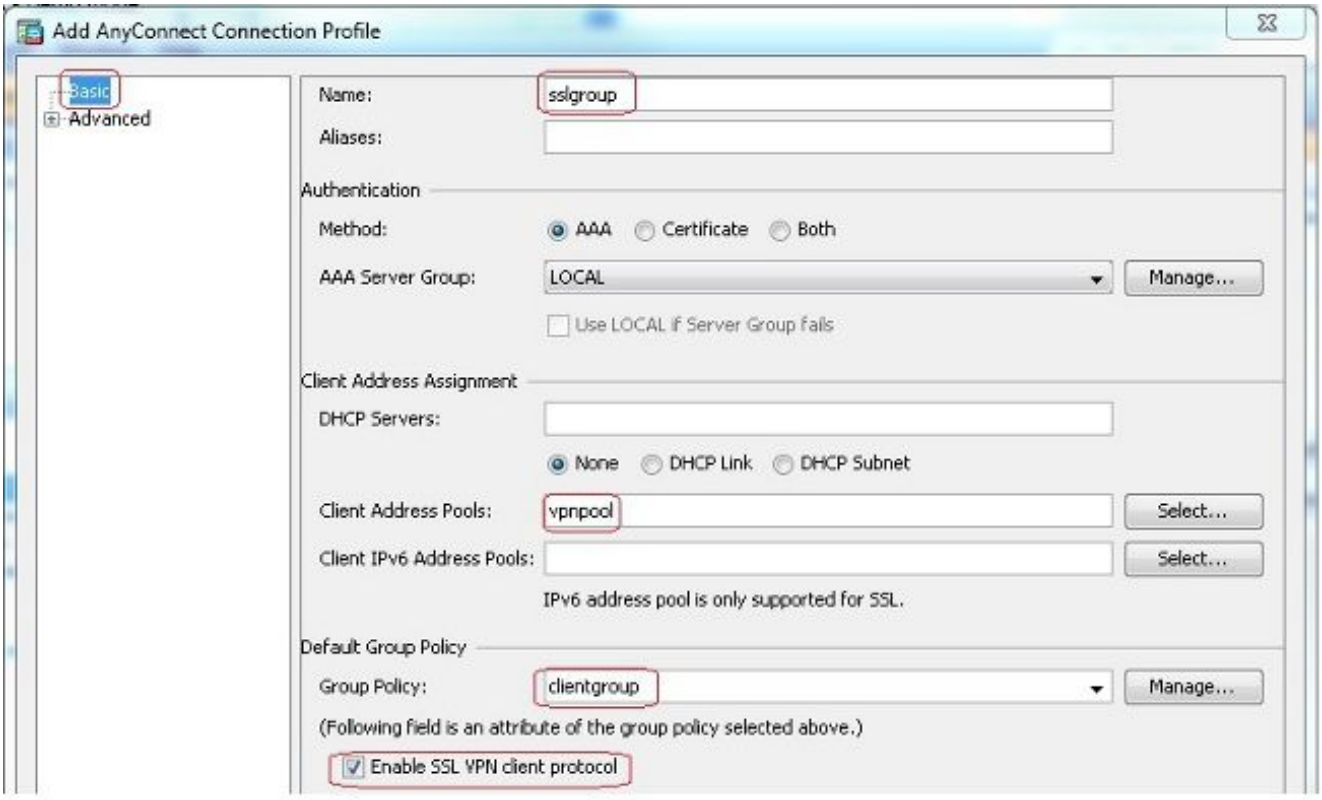
```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policyclientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelall
```

6. *선택* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *새 사용자 계정을 생성하려면* **ssluser1**. *클릭* **OK** *그리고* **Apply**.

동등한 CLI 컨피그레이션:

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

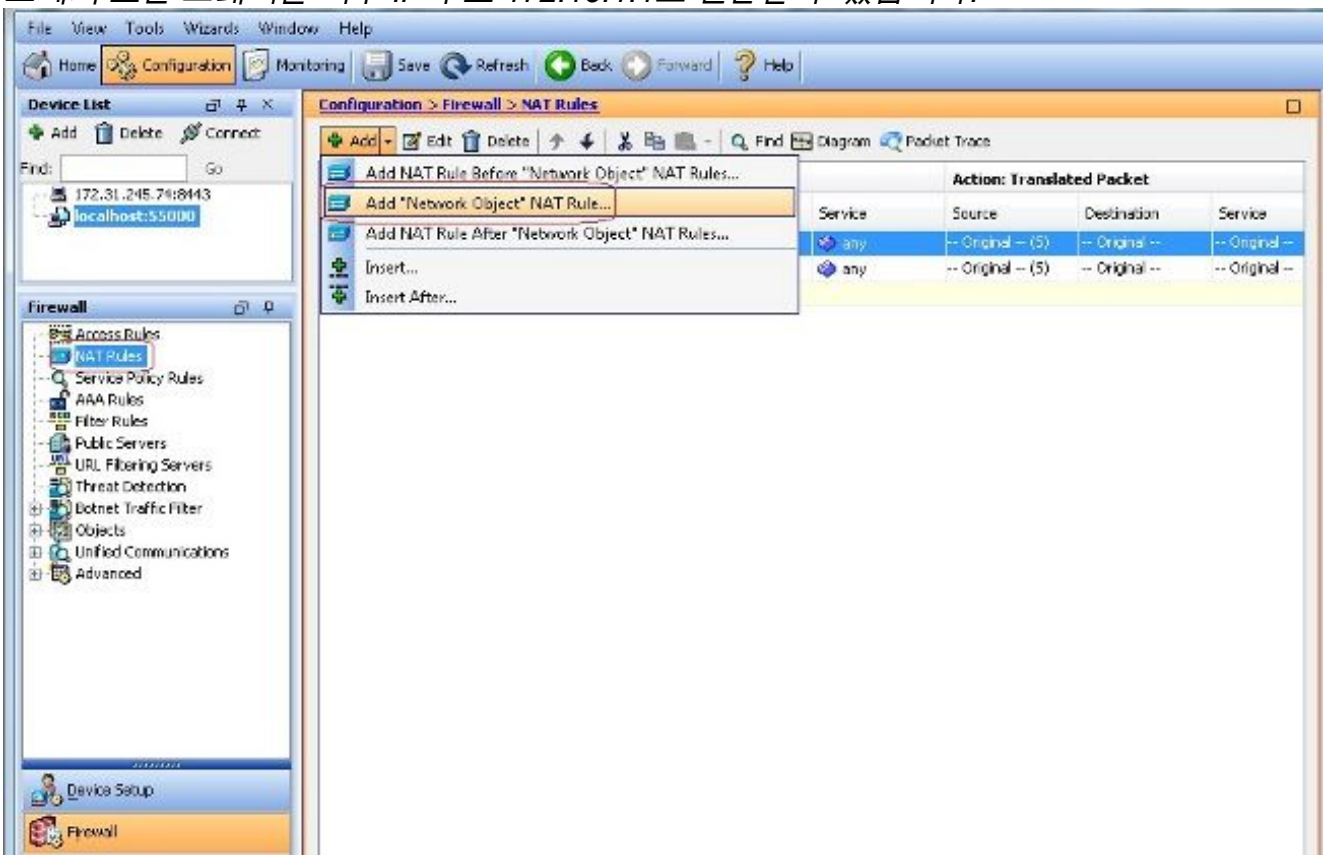
7. *터널 그룹을 구성합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *새 터널 그룹을 생성하려면* **sslgroup**.*의* **Basic** *탭에서는 다음과 같은 컨피그레이션 목록을 수행할 수 있습니다. 터널 그룹의 이름을* **sslgroup**.*아래* **Client Address Assignment***주소 풀을 선택합니다.* **vpnpool** *에서* **Client Address Pools** *드롭다운 목록입니다.아래* **Default Group Policy**, *그룹 정책을 선택합니다* **clientgroup** *에서* **Group Policy** *드롭다운 목록입니다.*

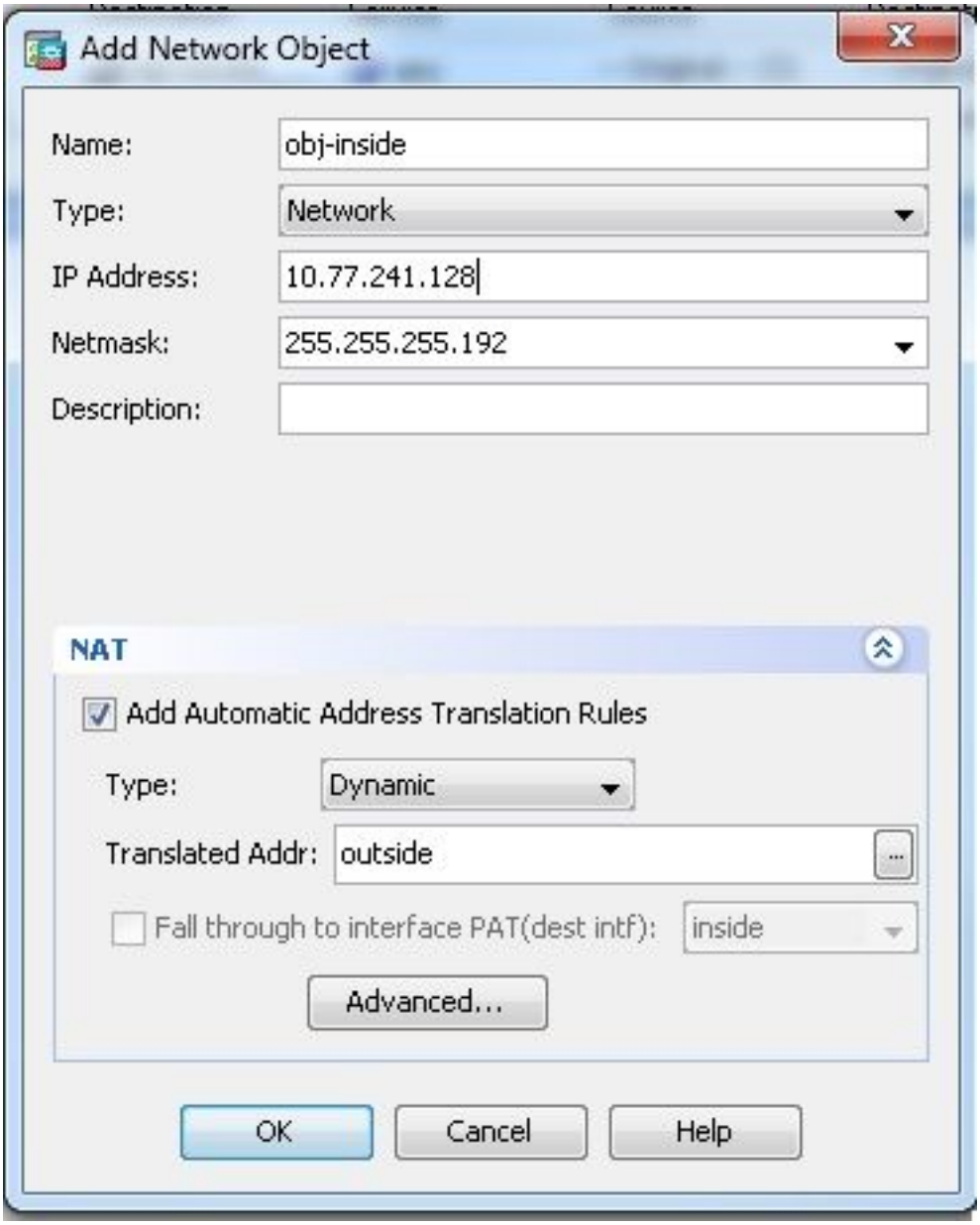


아래 **Advanced > Group Alias/Group URL** *탭에서 그룹 별칭 이름을 다음으로 지정합니다.* **sslgroup_users** *및* **OK**. ***동등한 CLI 컨피그레이션:***

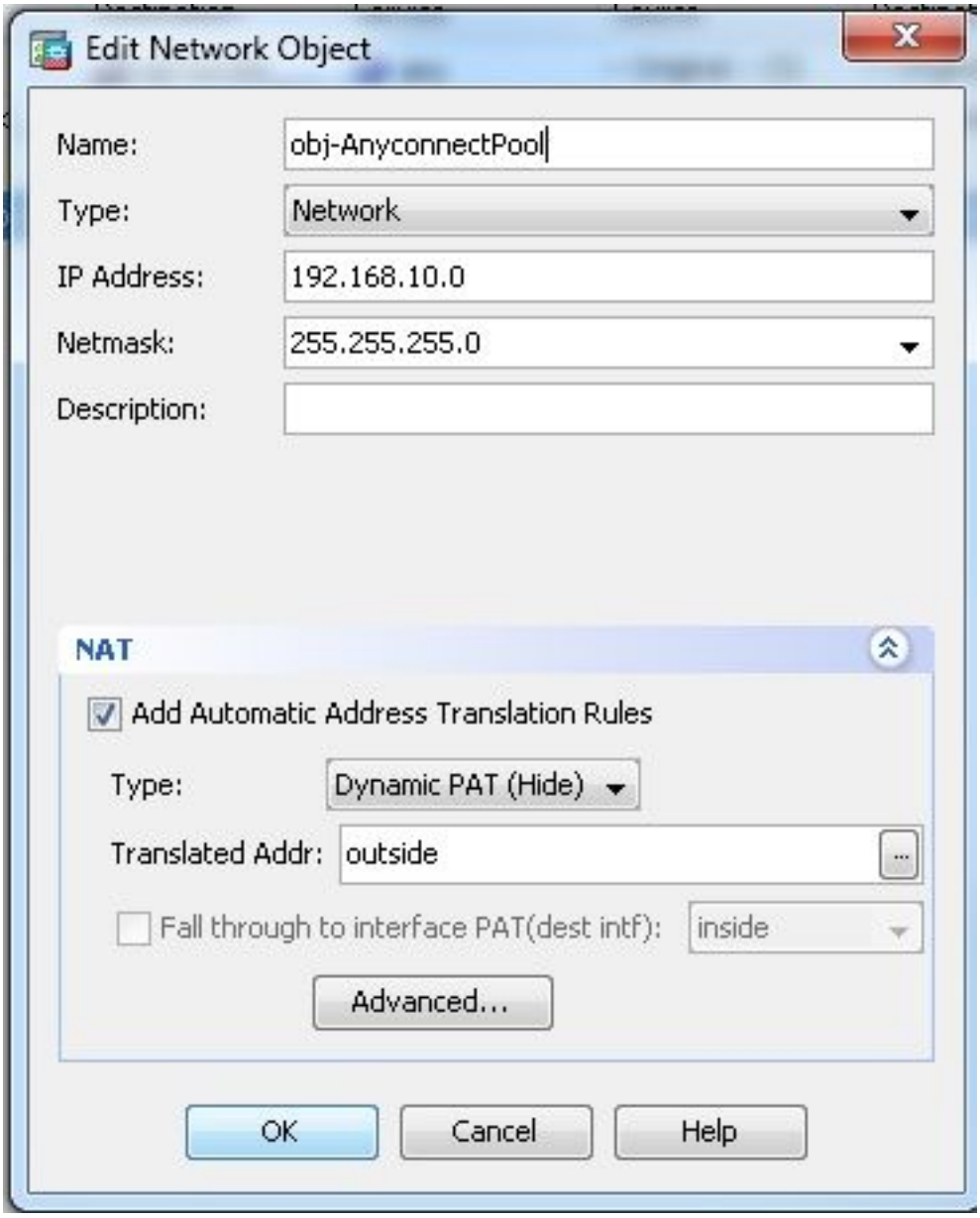
```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

8. *NAT 구성 선택* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *따라서 내부 네트워크에서 오는 트래픽을 외부 IP 주소 172.16.1.1로 변환할 수 있습니다.*





선택 **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *따라서 외부 네트워크에서 오는 VPN 트래픽이 외부 IP 주소 172.16.1.1로 변환될 수 있습니다.*



동등한 CLI 컨피그레이션:

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

CLI의 ASA 릴리스 9.1(2) 컨피그레이션

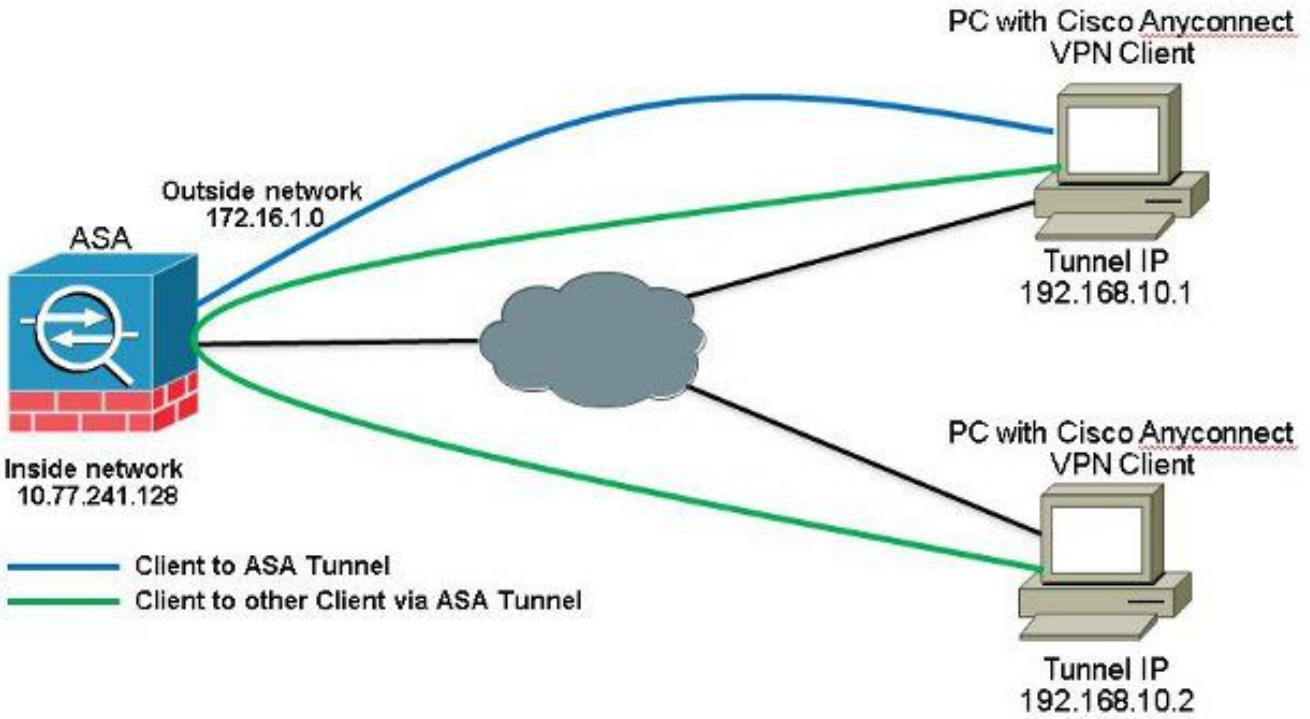
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
```

```
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0


!--- The address pool for the Cisco AnyConnect SSL VPN Clients


no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated
when going to the Anyconnect Pool.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
no crypto isakmp nat-traversal
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
webvpn
enable outside


!--- Enable WebVPN on the outside interface


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable


!--- Enable the display of the tunnel-group list on the WebVPN Login page
```

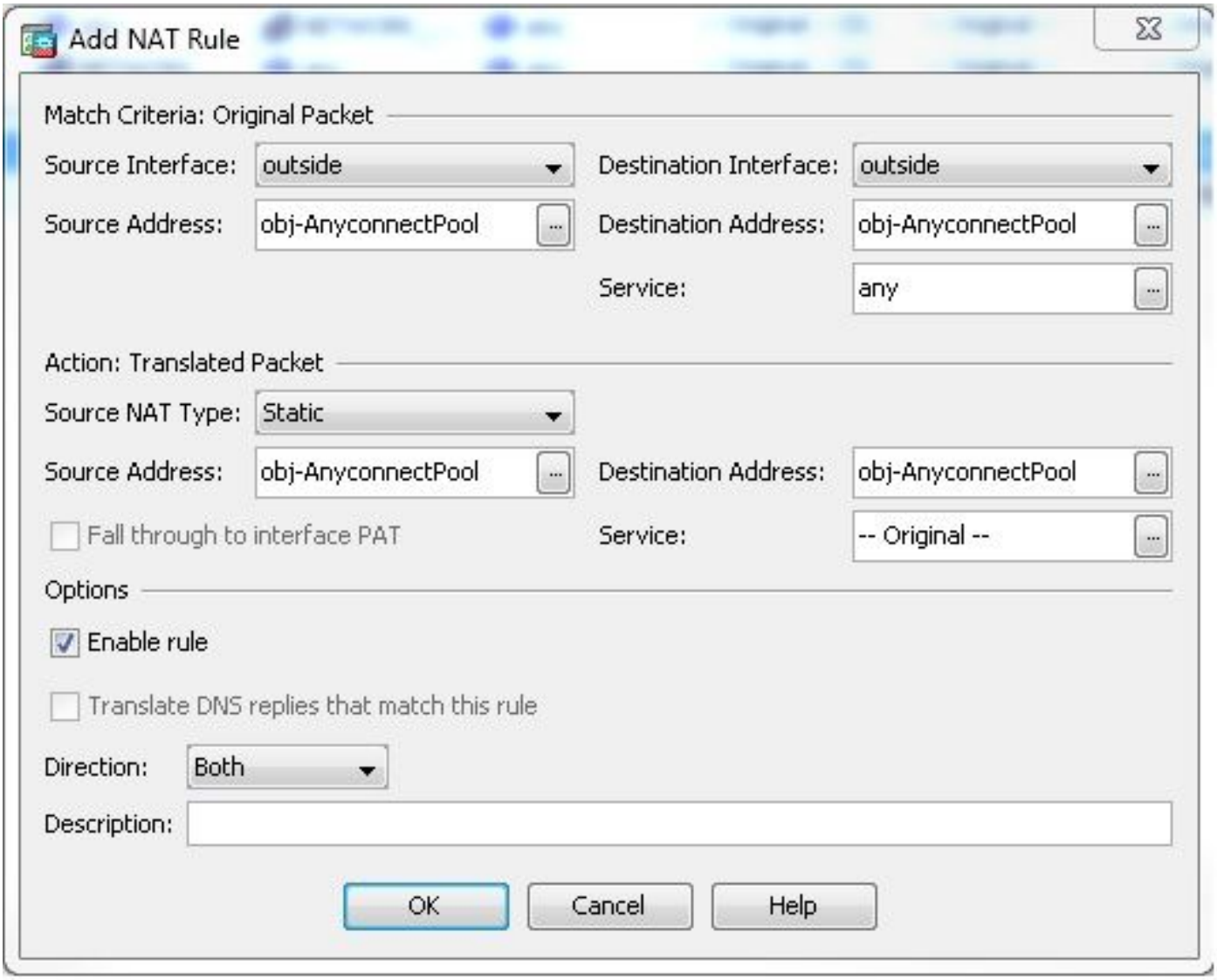
```
group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted


!--- Create a user account "ssluser1"


tunnel-group sslgroup type remote-access


!--- Create a tunnel group "sslgroup" with type as remote access


tunnel-group sslgroup general-attributes
address-pool vpnpool


!--- Associate the address pool vpnpool created


default-group-policy clientgroup


!--- Associate the group policy "clientgroup" created


tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable


!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

TunnelAll 컨피그레이션이 있는 AnyConnect VPN 클라이언트 간의 통신 허용네트워크 다이어그램



Anyconnect 클라이언트 간 통신이 필요하고 Stick의 공용 인터넷용 NAT가 있는 경우 양방향 통신을 허용하기 위해 수동 NAT도 필요합니다.이는 Anyconnect 클라이언트가 전화 서비스를 사용하고 서로 통화할 수 있어야 하는 일반적인 시나리오입니다.ASDM 릴리스 7.1(6)을 사용하는 ASA 릴리스 9.1(2) 컨피그레이션선택 Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules 따라서 외부 네트워크(Anyconnect 풀)에서 들어오고 동일한 풀에서 다른 Anyconnect 클라이언트로 향하는 트래픽은 외부 IP 주소 172.16.1.1로 변환되지 않습니다

.



동등한 CLI 컨피그레이션:

```
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
```

CLI의 ASA 릴리스 9.1(2) 컨피그레이션

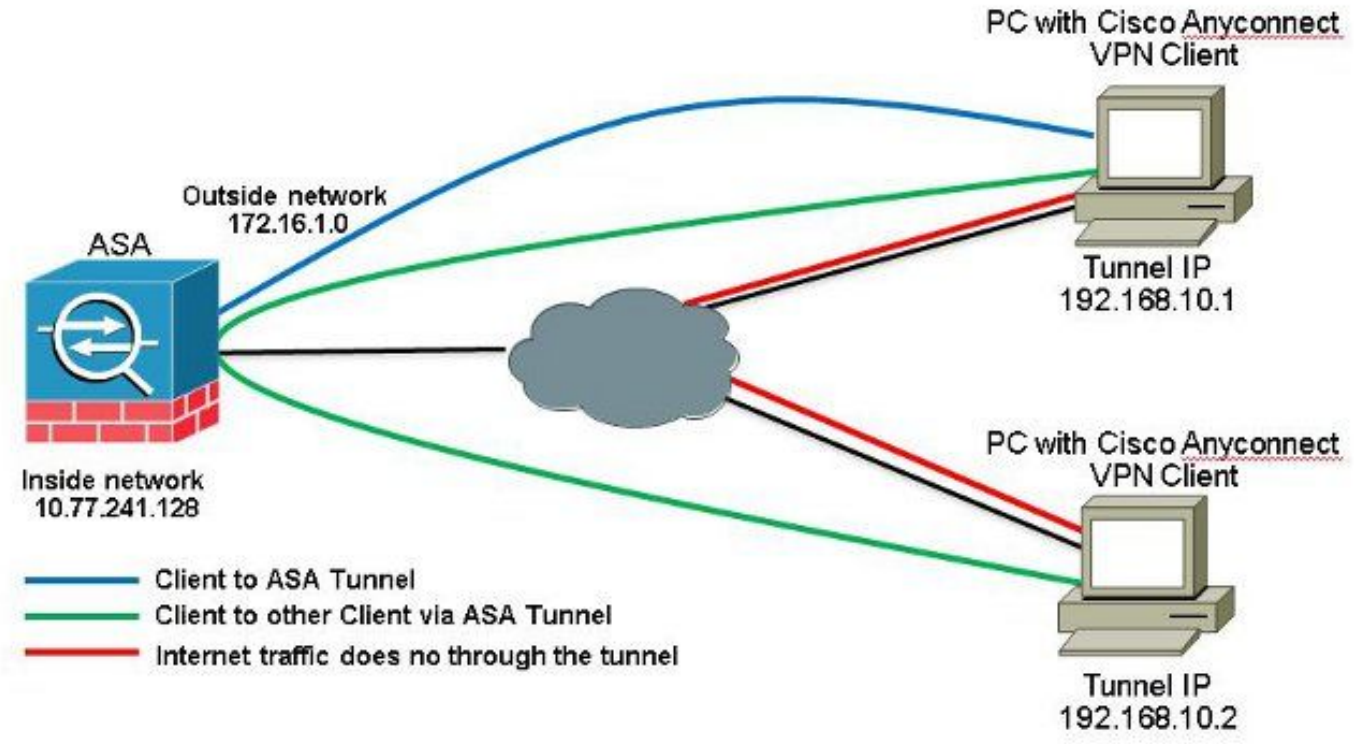
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
```

```
no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0


!--- The address pool for the Cisco AnyConnect SSL VPN Clients


no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool
destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network
destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined
to another Client within the same pool does not get translated.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
no crypto isakmp nat-traversal
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
webvpn
enable outside


!--- Enable WebVPN on the outside interface


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable


!--- Enable the display of the tunnel-group list on the WebVPN Login page


group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"
```

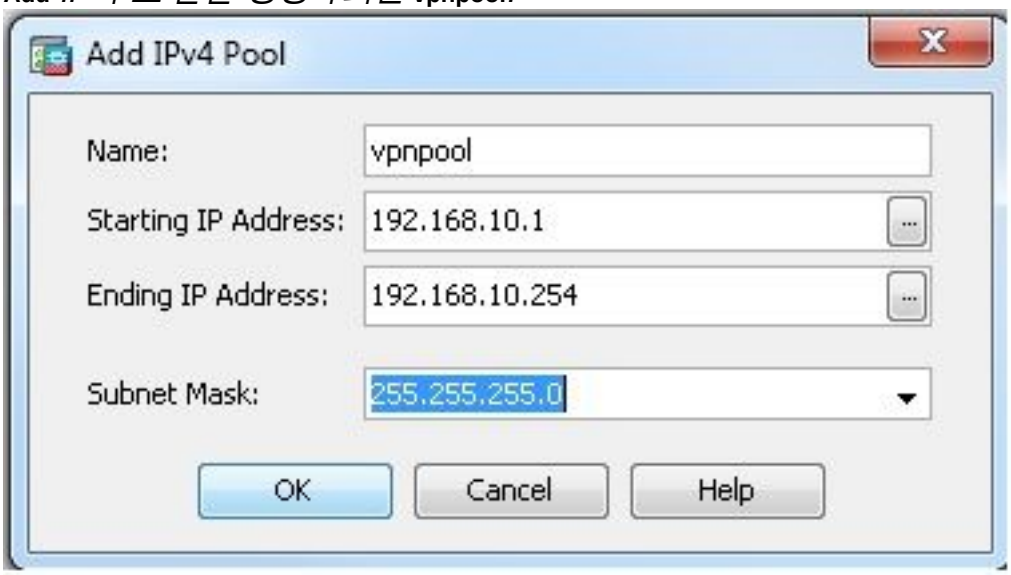
```
group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

tunnel-group sslgroup general-attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created

default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

스플릿 터널로 AnyConnect VPN 클라이언트 간 통신 허용네트워크 다이어그램



Anyconnect 클라이언트 간의 통신이 필요하고 스플릿 터널이 사용되는 경우 구성된 이 트래픽에 영향을 주는 NAT 규칙이 없는 한 양방향 통신을 허용하기 위해 수동 NAT는 필요하지 않습니다. 그러나 Anyconnect VPN 풀은 스플릿 터널 ACL에 포함되어야 합니다.이는 Anyconnect 클라이언트가 전화 서비스를 사용하고 서로 통화할 수 있어야 하는 일반적인 시나리오입니다.ASDM 릴리스 7.1(6)을 사용하는 ASA 릴리스 9.1(2) 컨피그레이션

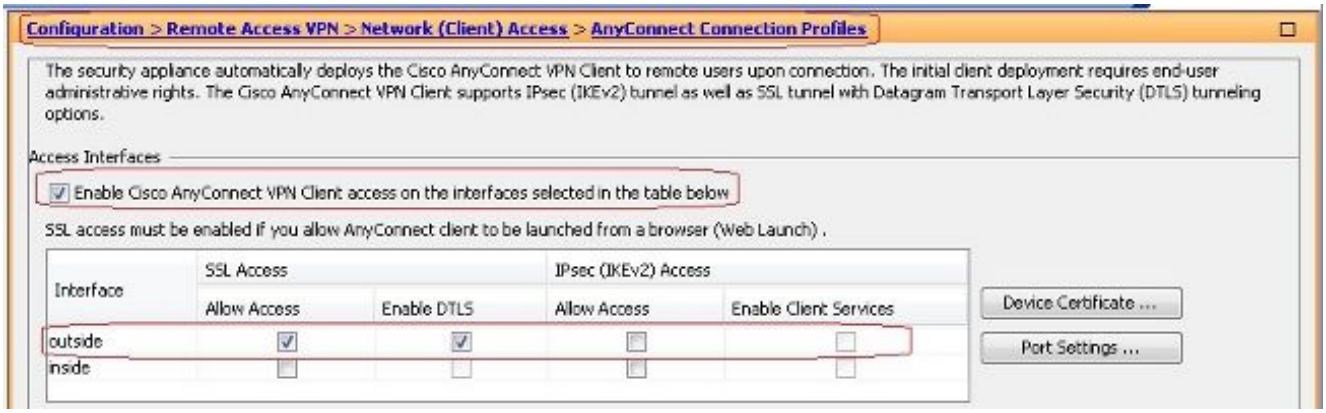
1. *선택* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *IP 주소 풀을 생성하려면* **vpnpool**.



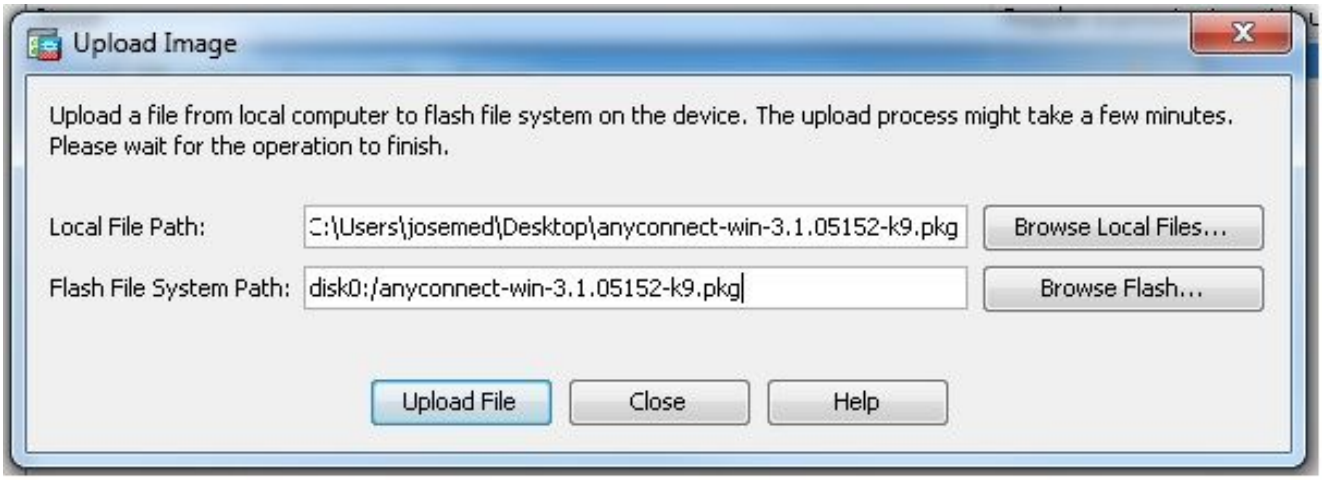
2. *클릭* **Apply**. ***동등한 CLI 컨피그레이션:***

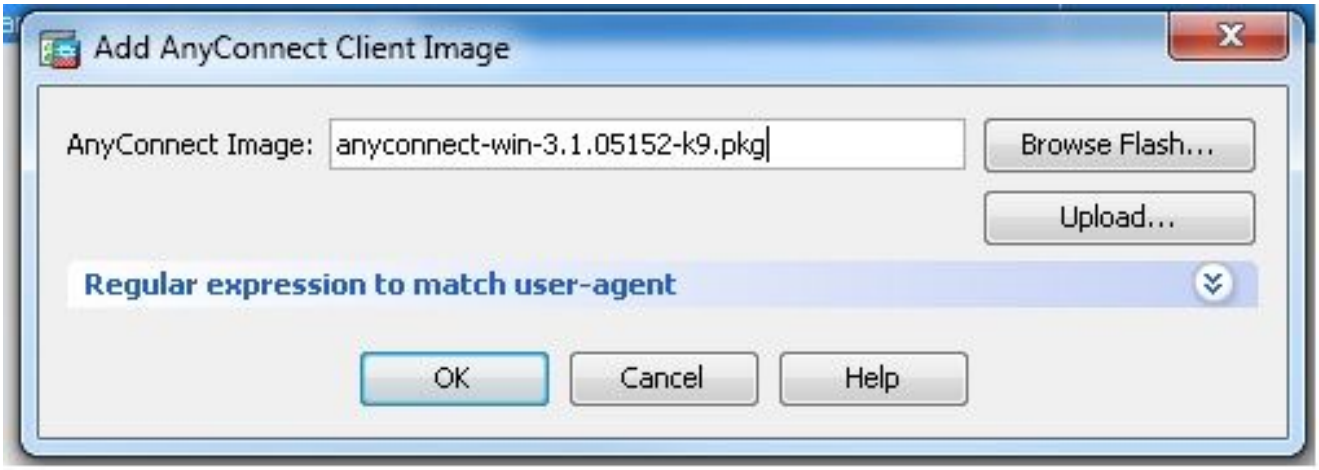
```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

3. *WebVPN을 활성화합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *및 아래에* **Access Interfaces**, *확인란을 클릭합니다* **Allow Access** *및* **Enable DTLS** *외부 인터페이스용입니다. 또한* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *외부 인터페이스에서 SSL VPN을 활성화하려면 확인란을 선택합니다.*



클릭 **Apply**. *선택* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *그림과 같이 ASA의 플래시 메모리에서 Cisco AnyConnect VPN 클라이언트 이미지를 추가합니다.*

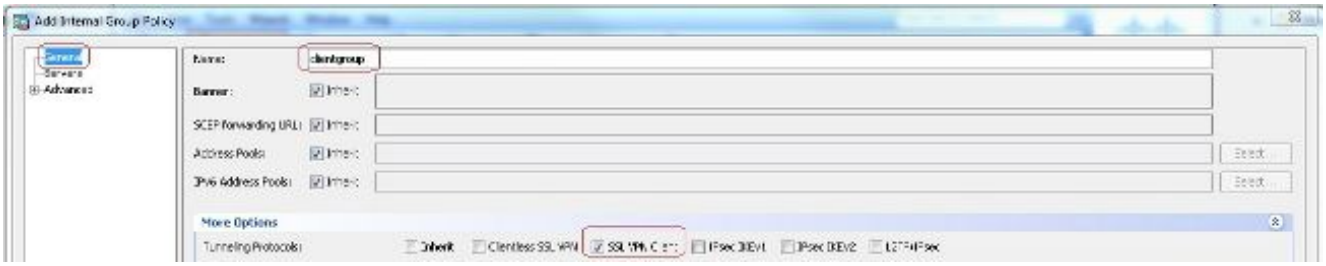




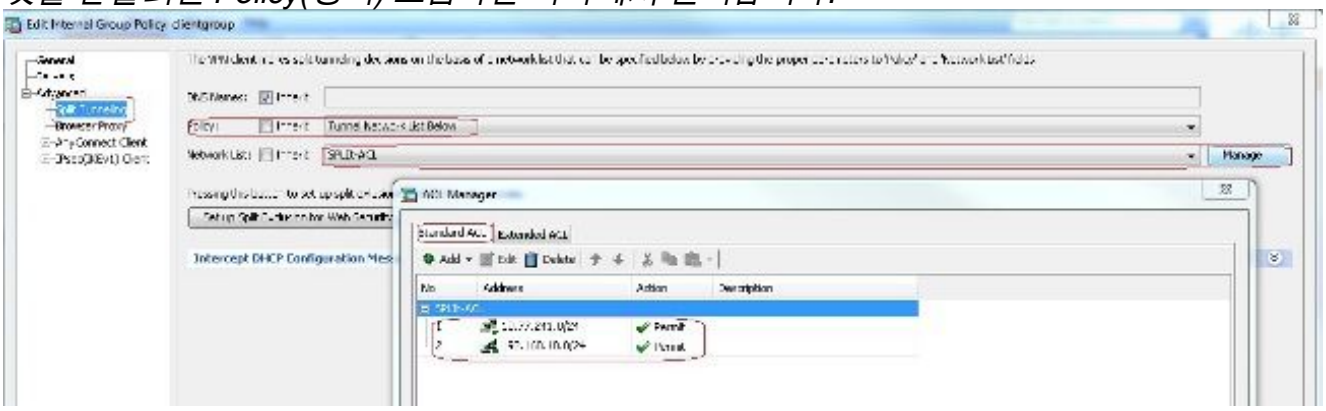
동등한 CLI 컨피그레이션:

```
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
```

4. *그룹 정책을 구성합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *내부 그룹 정책을 생성하려면* **clientgroup**. *아래* **General** *탭에서* **SSL VPN Client** *허용되는 터널 프로토콜로 WebVPN을 활성화하려면 확인란을 선택합니다.*



의 **Advanced > Split Tunneling** *탭, 선택* **Tunnel Network List Below** *보안 터널을 통해 원격 PC의 모든 패킷을 만들려면 Policy(정책) 드롭다운 목록에서 선택합니다.*



동등한 CLI 컨피그레이션:

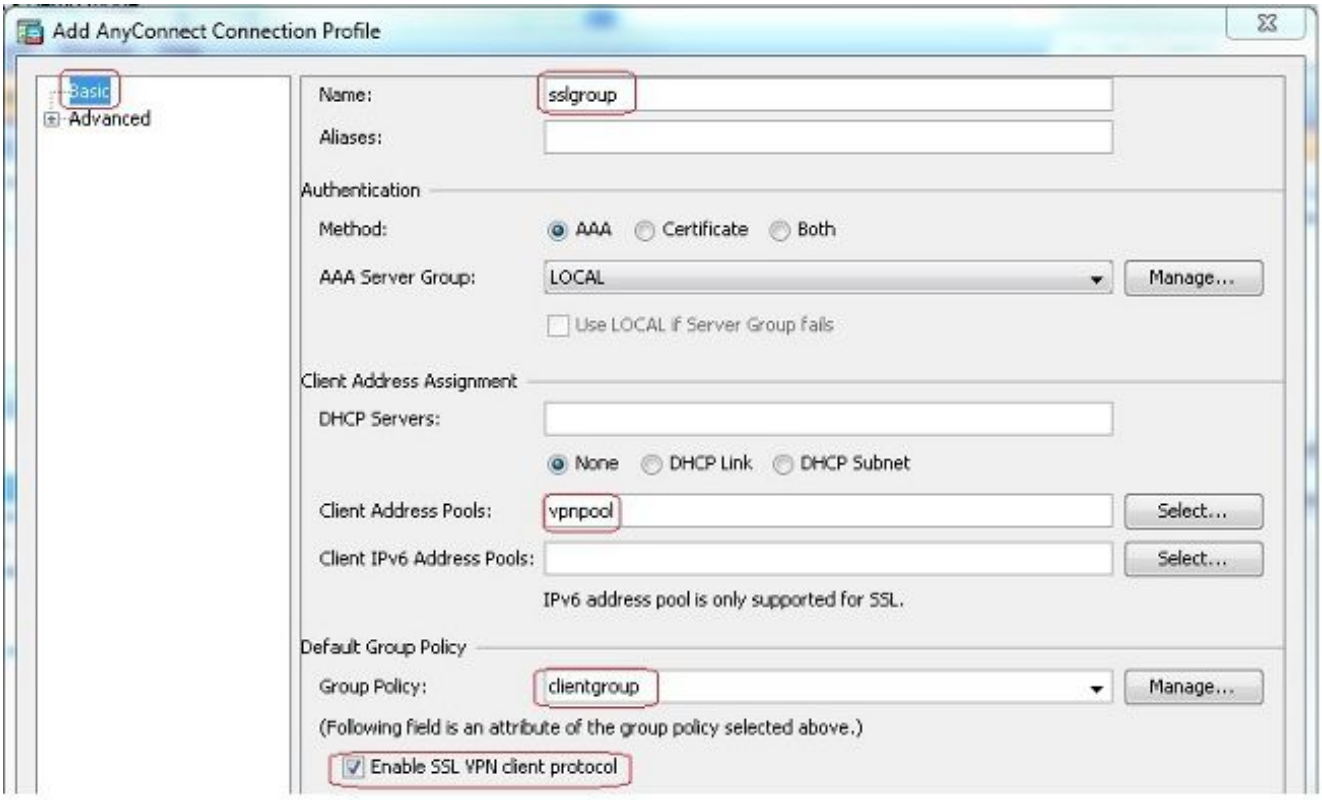
```
ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

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)#split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL
```

5. *선택* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *새 사용자 계정을 생성하려면* **ssluser1**. *클릭* **OK** *그리고* **Apply**.

동등한 CLI 컨피그레이션:

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

6. *터널 그룹을 구성합니다. 선택* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *새 터널 그룹을 생성하려면* **sslgroup**.*의* **Basic** *탭에서는 다음과 같은 컨피그레이션 목록을 수행할 수 있습니다. 터널 그룹의 이름을* **sslgroup**.*아래* **Client Address Assignment***주소 풀을 선택합니다.* **vpnpool** *에서* **Client Address Pools** *드롭다운 목록입니다.아래* **Default Group Policy**, *그룹 정책을 선택합니다* **clientgroup** *에서* **Group Policy** *드롭다운 목록입니다.*



아래 **Advanced > Group Alias/Group URL** *탭에서 그룹 별칭 이름을 다음으로 지정합니다.* **sslgroup_users** *및* **OK**. ***동등한 CLI 컨피그레이션:***

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
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
```

CLI의 ASA 릴리스 9.1(2) 컨피그레이션

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

!
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
domain-name default.domain.invalid
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the
Anyconnect tunnel.

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when
going to the Anyconnect Pool

object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
no crypto isakmp nat-traversal
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
webvpn
enable outside


!--- Enable WebVPN on the outside interface


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect enable


!--- Enable the security appliance to download SVC images to remote computers


tunnel-group-list enable


!--- Enable the display of the tunnel-group list on the WebVPN Login page


group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol
```

```
split-tunnel-policy tunnelspecified

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL
VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

tunnel-group sslgroup general-attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created

default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

다음을 확인합니다. 설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

- **show vpn-sessiondb svc** - 현재 SSL 연결에 대한 정보를 표시합니다.

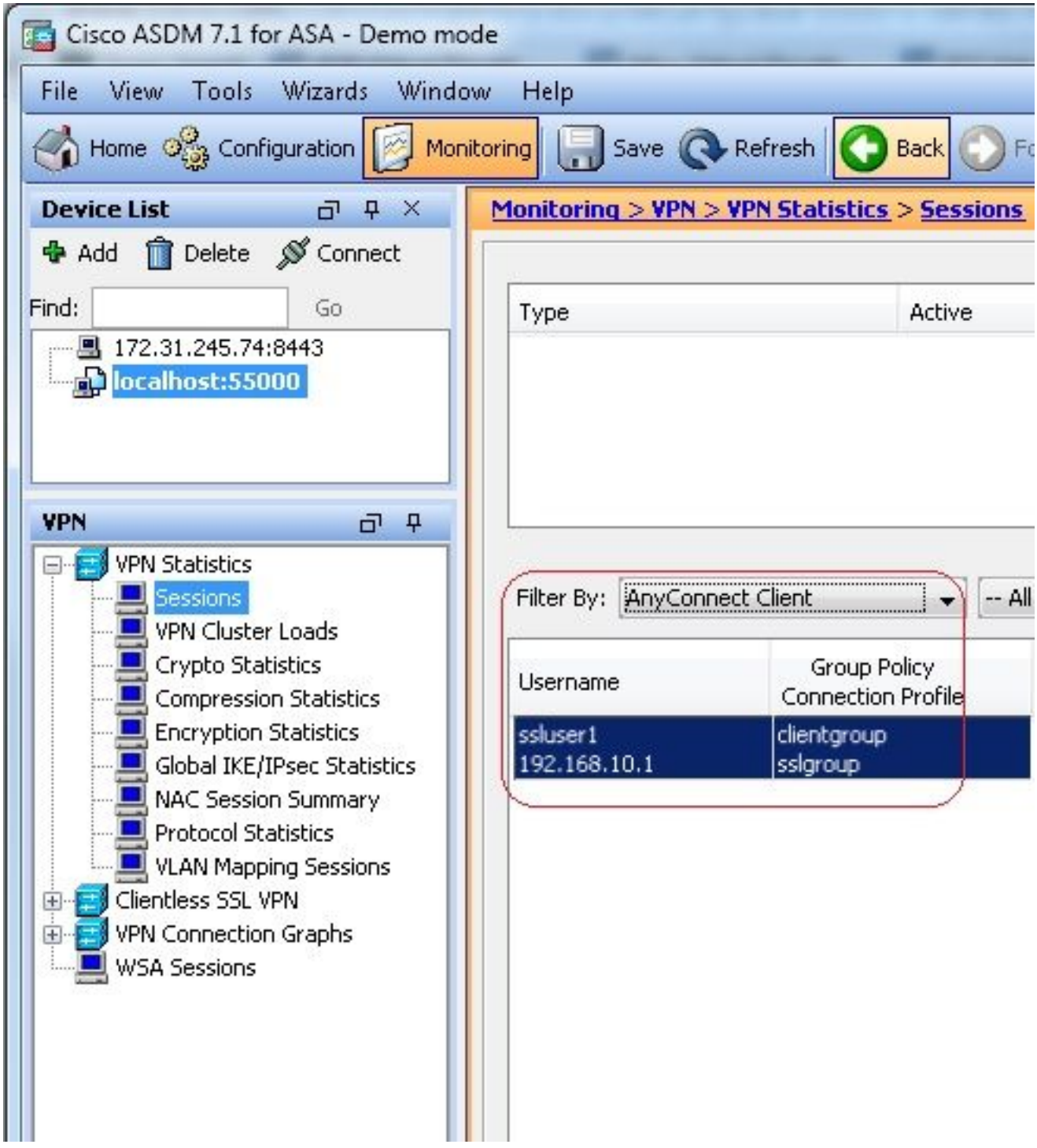
```
ciscoasa#show vpn-sessiondb anyconnect

Session Type: SVC

Username : ssluser1                Index        : 12
Assigned IP : 192.168.10.1           Public IP    : 192.168.1.1
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
Encryption : RC4 AES128              Hashing      : SHA1
Bytes Tx : 194118 Bytes Rx : 197448
Group Policy : clientgroup           Tunnel Group : sslgroup
Login Time : 17:12:23 IST Mon Mar 24 2008
Duration : 0h:12m:00s
```

```
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

- **show webvpn group-alias** - *다양한 그룹에 대해 구성된 별칭을 표시합니다.*

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- *ASDM에서* **Monitoring > VPN > VPN Statistics > Sessions** *를 클릭하면 ASA의 현재 세션을 알 수 있습니다.*



문제 해결이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

- **vpn-sessiondb logoff name** - *특정 사용자 이름에 대한 SSL VPN 세션을 로그오프하는 명령입니다.*

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
```

np_svc_destroy_session(0xB000)

마찬가지로 **vpn-sessiondb logoff anyconnect** *명령을 사용하여 모든 AnyConnect 세션을 종료합니다.*

- **debug webvpn anyconnect <1-255>** - *세션을 설정하기 위해 실시간 webvpn 이벤트를 제공합니다.*

```
Ciscoasa#debug webvpn anyconnect 7

CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
```

```
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
No SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260(mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt

Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

- *ASDM에서* **Monitoring > Logging > Real-time Log Viewer > View** *실시간 이벤트를 볼 수 있습니다. 이 예에서는 ASA 172.16.1.1을 통한 인터넷의 AnyConnect 192.168.10.1과 텔넷 서버 10.2.2.2 간의 세션 정보를 보여 줍니다*

.

관련 정보

- *Cisco ASA 5500-X Series 방화벽*
- *Stick 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 및 VPN 클라이언트 예*
- *ASDM을 사용하는 ASA의 SVC(SSL VPN Client) 컨피그레이션 예*
- *기술 지원 및 문서 – Cisco Systems*

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.