ASA에서 스플릿 터널링으로 AnyConnect Secure Mobility Client 설정

목차

소개

이 문서에서는 소프트웨어 버전 9.3(2)을 실행하는 Cisco ASA(Adaptive Security Appliance)에서 Cisco ASDM(Adaptive Security Device Manager)을 통해 Cisco AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco AnyConnect Secure Mobility Client 웹 구축 패키지는 ASA에 대한 ASDM 액세스가 제공되는 로컬 데스크톱에 다운로드해야 합니다. 클라이언트 패키지를 다운로드하려면 Cisco AnyConnect Secure Mobility Client 웹 페이지를 참조하십시오. 다양한 OS(운영 체제)용 웹 구축 패키지를 ASA에 동시에 업로드할 수 있습니다.

다음은 다양한 OS의 웹 구축 파일 이름입니다.

- **Microsoft Windows OS** - *AnyConnect-win-<version>-k9.pkg*

- **Macintosh(MAC) OS** - *AnyConnect-macosx-i386-<version>-k9.pkg*
- **Linux OS** - *AnyConnect-linux-<version>-k9.pkg*

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 버전 9.3(2)
- ASDM 버전 7.3(1)101
- AnyConnect 버전 3.1

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.

배경 정보

이 문서에서는 ASDM을 통해 Cisco AnyConnect Configuration Wizard를 사용하여 AnyConnect 클라이언트를 구성하고 스플릿 터널링을 활성화하는 방법에 대한 단계별 세부 정보를 제공합니다.

스플릿 터널링은 특정 트래픽만 터널링해야 하는 시나리오에서 사용되며, 연결된 경우 모든 클라이언트 시스템에서 생성된 트래픽이 VPN을 통해 이동하는 시나리오와는 다릅니다. AnyConnect 컨피그레이션 마법사를 사용하면 기본적으로 ASA에서 *모든 터널* 컨피그레이션이 생성됩니다. 스플릿 터널링은 별도로 구성해야 합니다. 이 문서의 섹션에서 자세히 설명합니다.

이 컨피그레이션 예에서는 ASA 뒤에 있는 LAN 서브넷인 10.10.10.0/24 서브넷에 대한 트래픽을 VPN 터널을 통해 전송하고 클라이언트 머신의 다른 모든 트래픽은 자체 인터넷 회로를 통해 전달합니다.

AnyConnect 라이센스 정보

다음은 Cisco AnyConnect Secure Mobility Client 라이센스에 대한 유용한 정보로 연결되는 링크입니다.

- AnyConnect Secure Mobility Client에 필요한 라이센스 및 관련 기능을 결정하려면 AnyConnect Secure Mobility Client 기능, 라이센스 및 OS, 릴리스 3.1 문서를 참조하십시오.
- AnyConnect Apex 및 Plus 라이센스에 대한 자세한 내용은 Cisco AnyConnect 주문 가이드를 참조하십시오.
- IP Phone 및 모바일 VPN 연결에 필요한 ASA 라이센스를 참조하십시오. ip 전화 및 모바일 연결에 대한 추가 라이센스 요구 사항에 대한 자세한 내용은 을 참조하십시오.

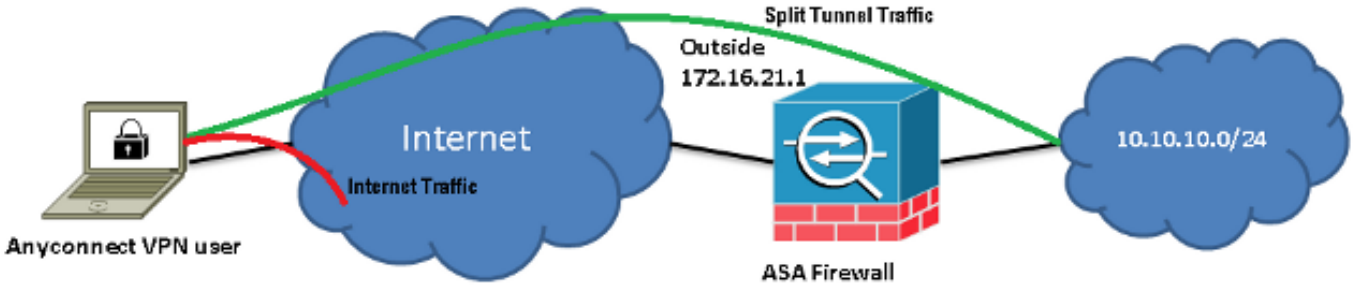
구성

이 섹션에서는 ASA에서 Cisco AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합

니다.

네트워크 다이어그램

다음은 이 문서의 예에 사용되는 토폴로지입니다.

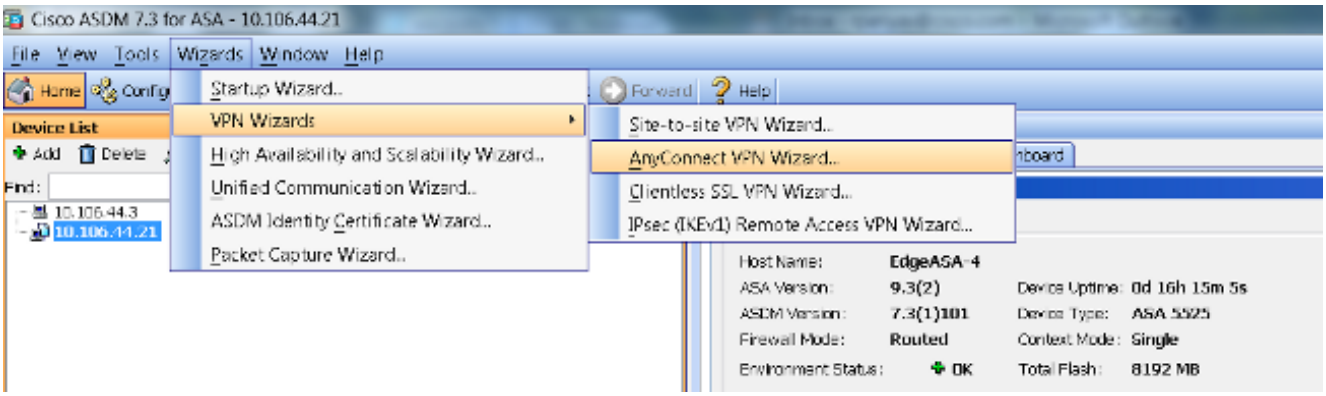


ASDM AnyConnect 컨피그레이션 마법사

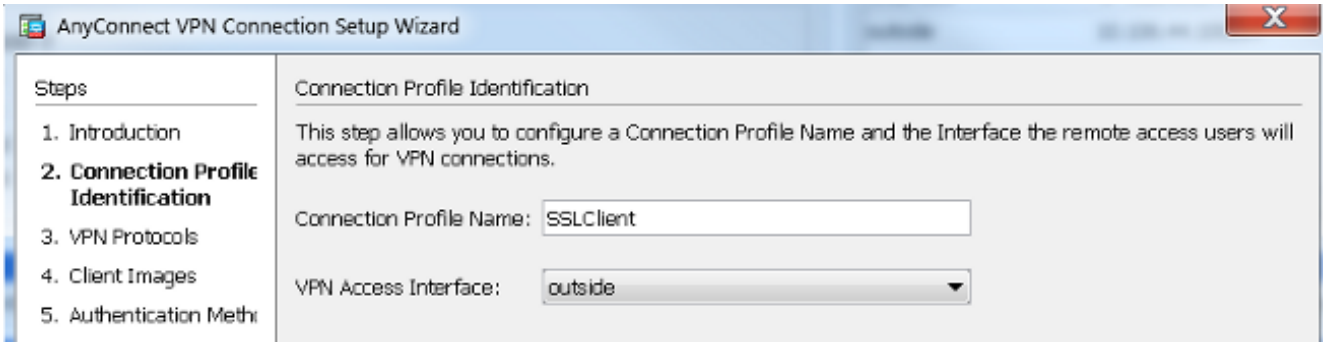
AnyConnect Secure Mobility Client를 구성하기 위해 AnyConnect 컨피그레이션 마법사를 사용할 수 있습니다. 계속하기 전에 AnyConnect 클라이언트 패키지가 ASA 방화벽의 플래시/디스크에 업로드되었는지 확인합니다.

컨피그레이션 마법사를 통해 AnyConnect Secure Mobility Client를 구성하려면 다음 단계를 완료하십시오.

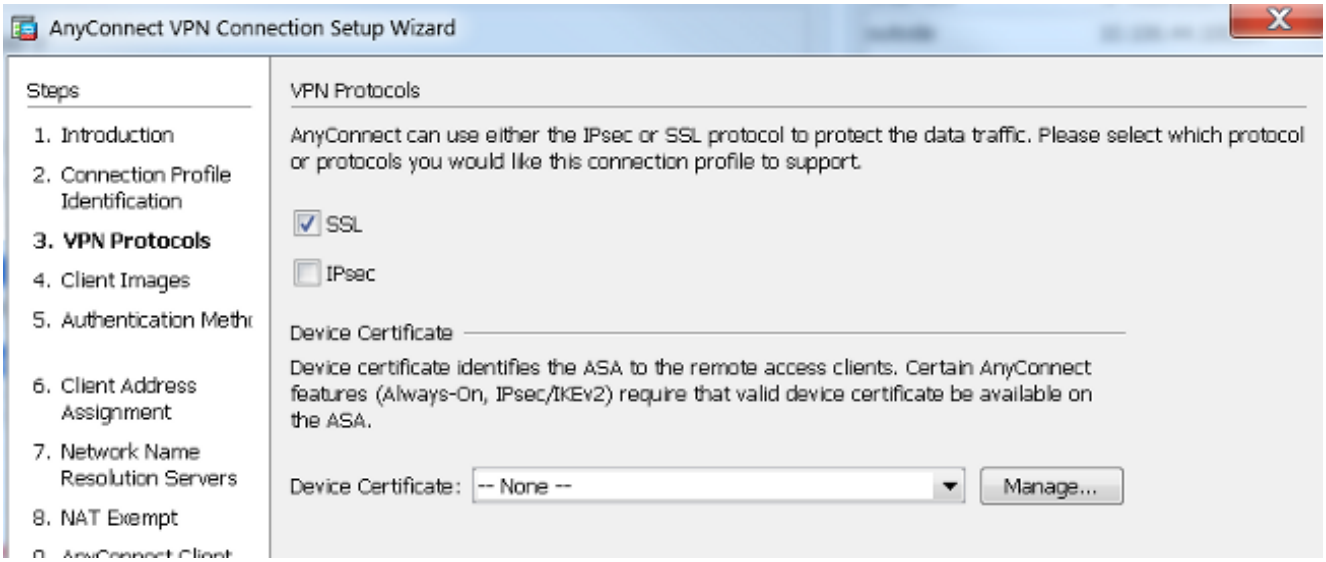
1. ASDM에 로그인하고 Configuration Wizard(컨피그레이션 마법사)를 **시작하고 Next(다음)**를 클릭합니다.



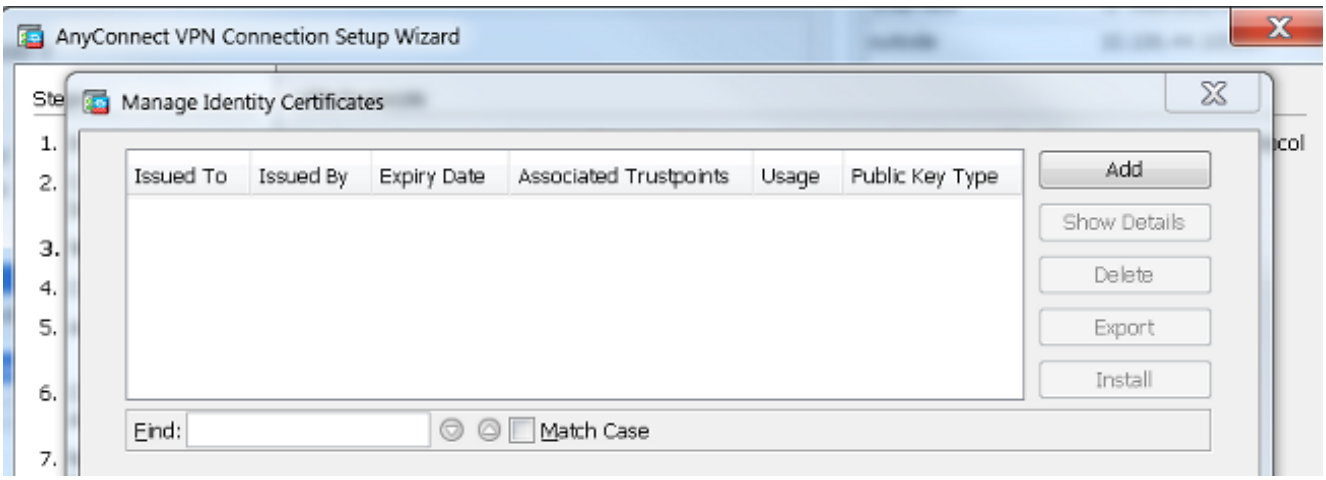
2. *Connection Profile Name(연결 프로파일 이름)*을 입력하고 VPN Access Interface(*VPN 액세스 인터페이스)* 드롭다운 메뉴에서 VPN이 종료될 인터페이스를 선택한 후 **Next(다음)**를 클릭합니다.



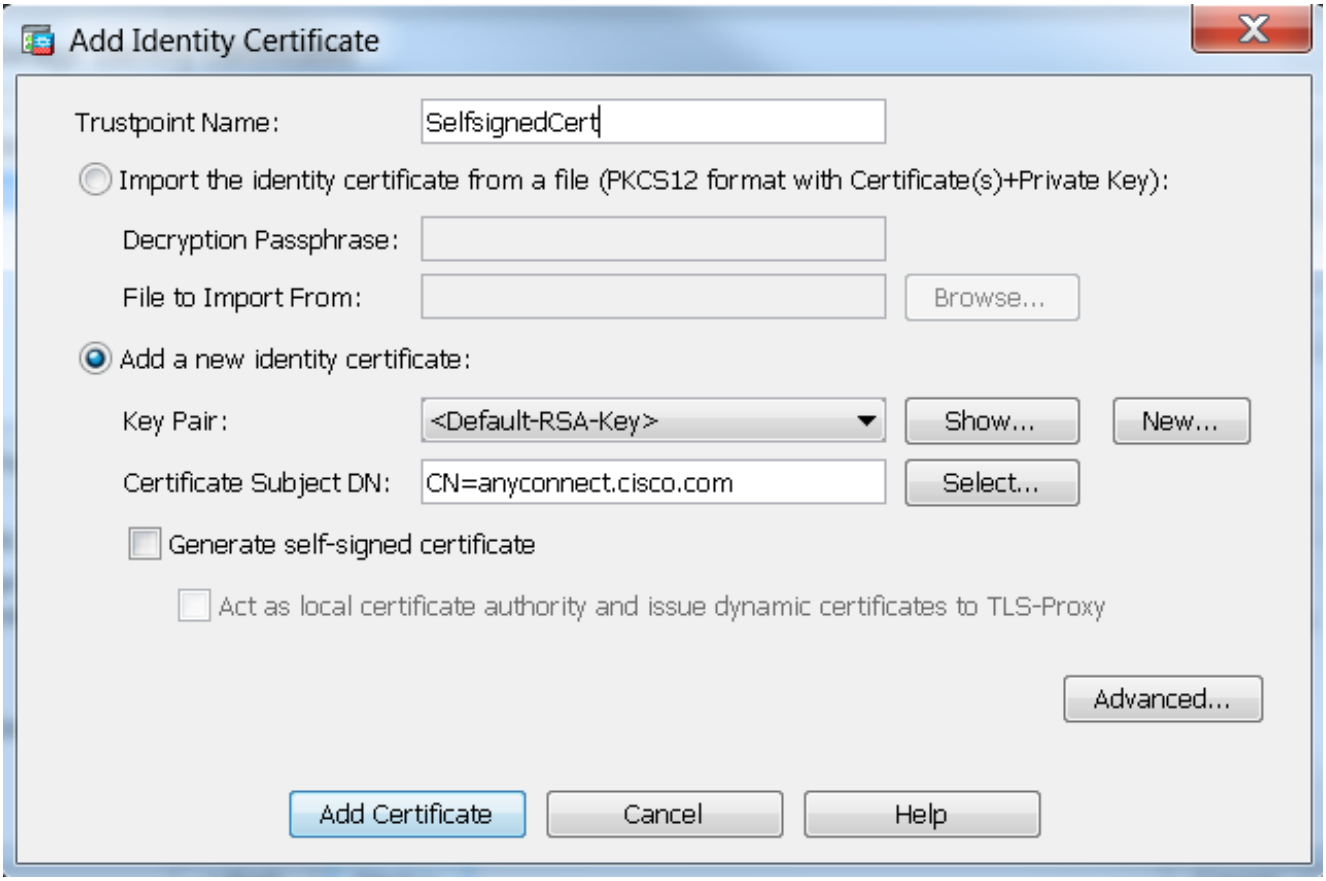
3. SSL(**Secure** Sockets Layer)을 활성화하려면 SSL 확인란을 선택합니다. *디바이스 인증서*는 신뢰할 수 있는 서드파티 CA(Certificate Authority) 발급 인증서(예: Verisign 또는 Entrust) 또는 자체 서명 인증서일 수 있습니다. 인증서가 ASA에 이미 설치되어 있는 경우 드롭다운 메뉴를 통해 선택할 수 있습니다. **참고:** 이 인증서는 제공될 서버측 인증서입니다. ASA에 현재 설치된 인증서가 없고 자체 서명 인증서를 생성해야 하는 경우 Manage(**관리**)를 클릭합니다.서드파티 인증서를 설치하려면 ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration 예 Cisco 문서에 설명된 단계를 완료합니다.



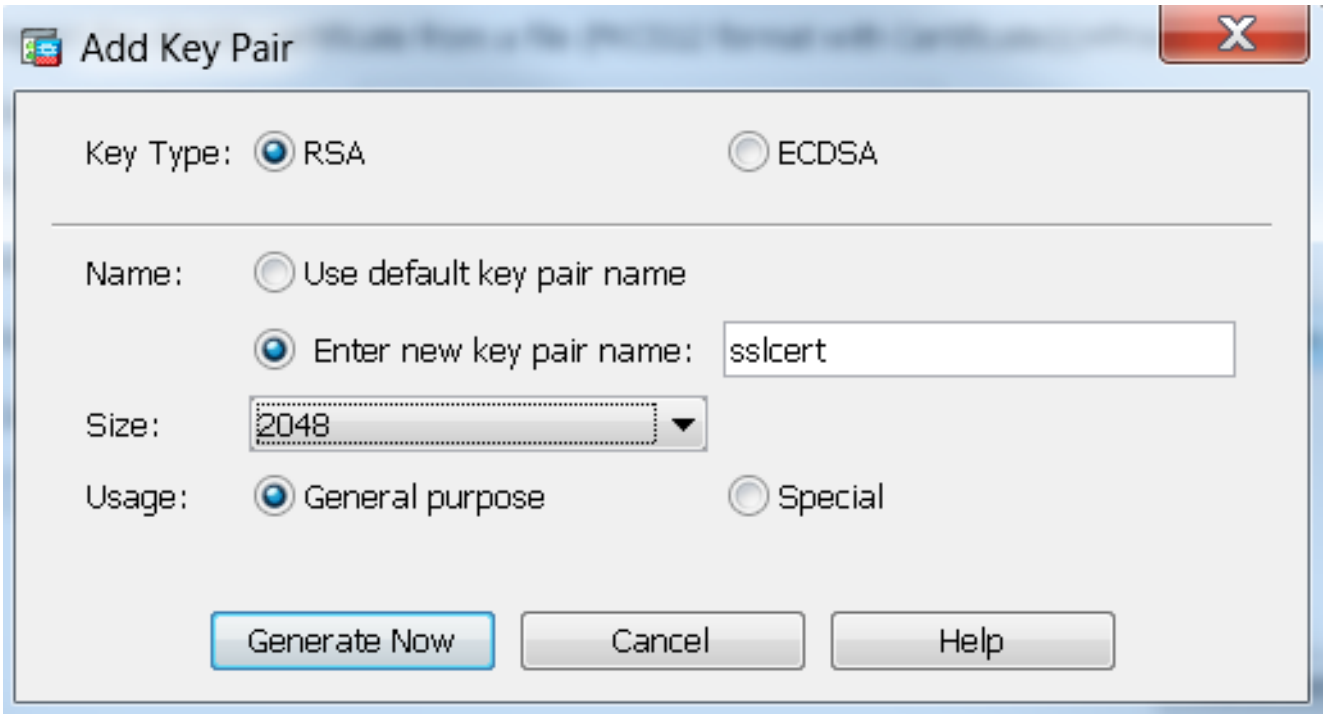
4. Add(추가)**를 클릭합니다**.



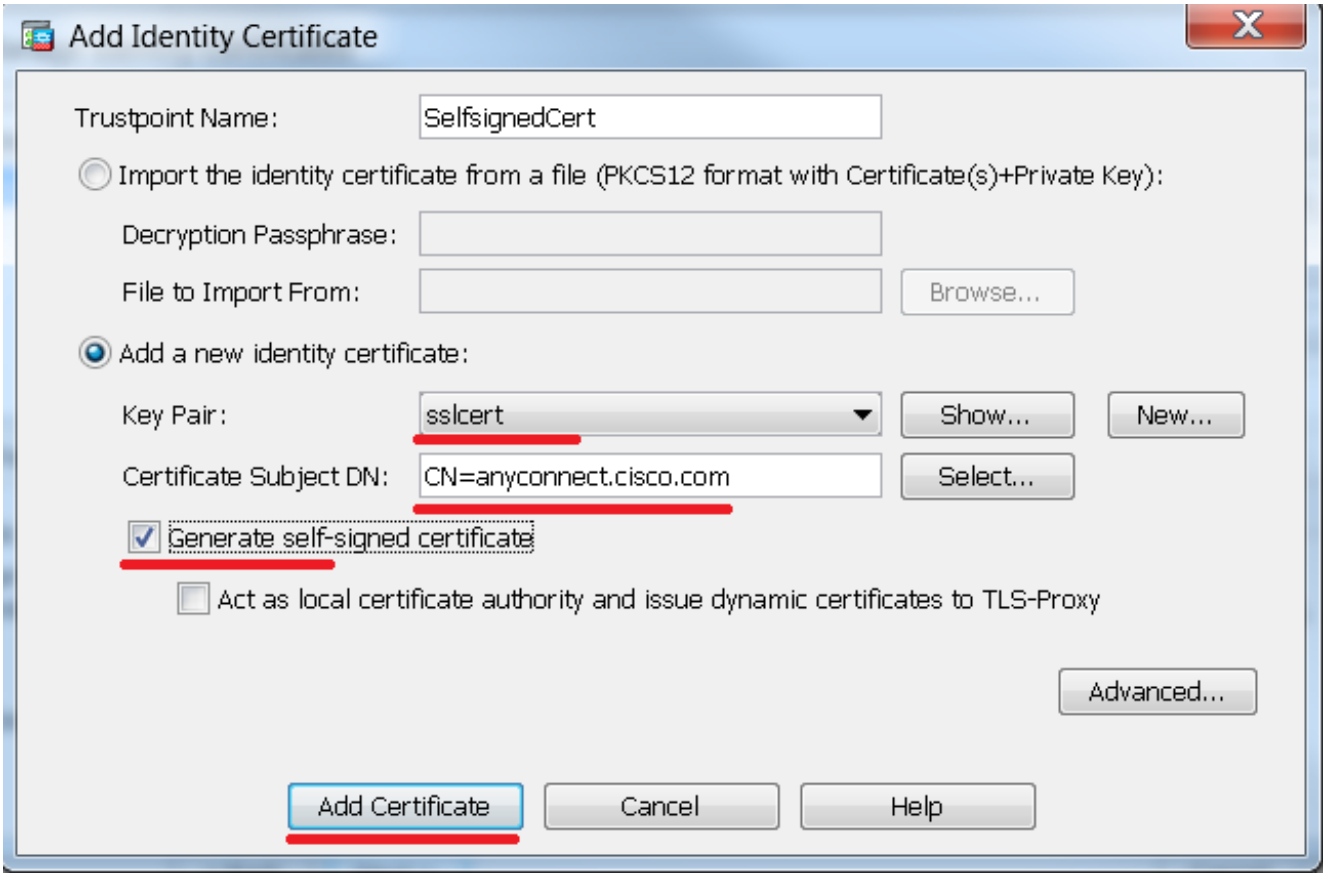
5. Trustpoint Name 필드에 적절한 *이름을* 입력하고 Add **a new identity certificate(새 ID 인증서 추가)** 라디오 버튼을 클릭합니다. 디바이스에 RSA(Rivest-Shamir-Addleman) 키 쌍이 없는 경우 **New**(새로 만들기)를 클릭하여 다음 중 하나를 생성합니다.



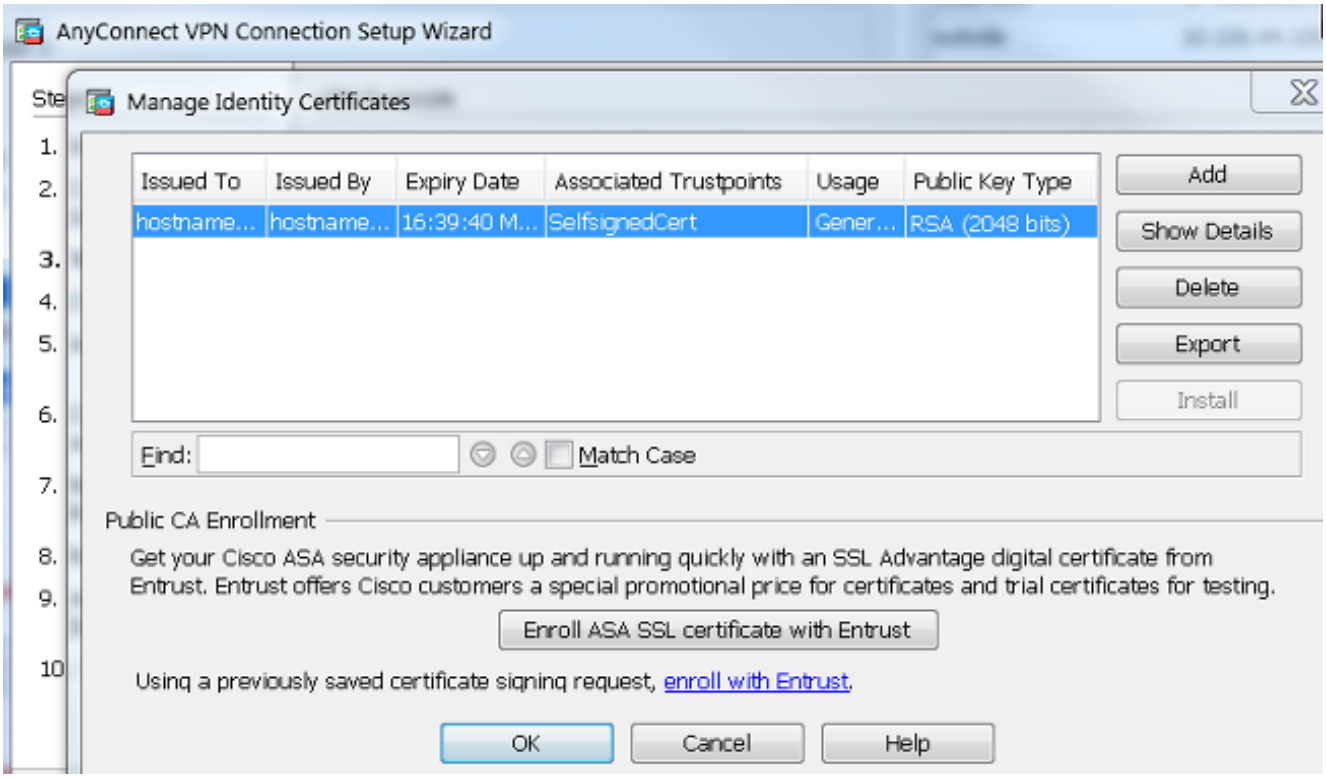
6. Use default **key pair name(기본 키 쌍 이름 사용)** 라디오 버튼을 클릭하거나 Enter **new key pair name(새 키 쌍 이름 입력)** 라디오 버튼을 클릭하고 새 이름을 입력합니다. 키의 크기를 선택한 다음 Generate **Now(지금 생성)**를 클릭합니다.



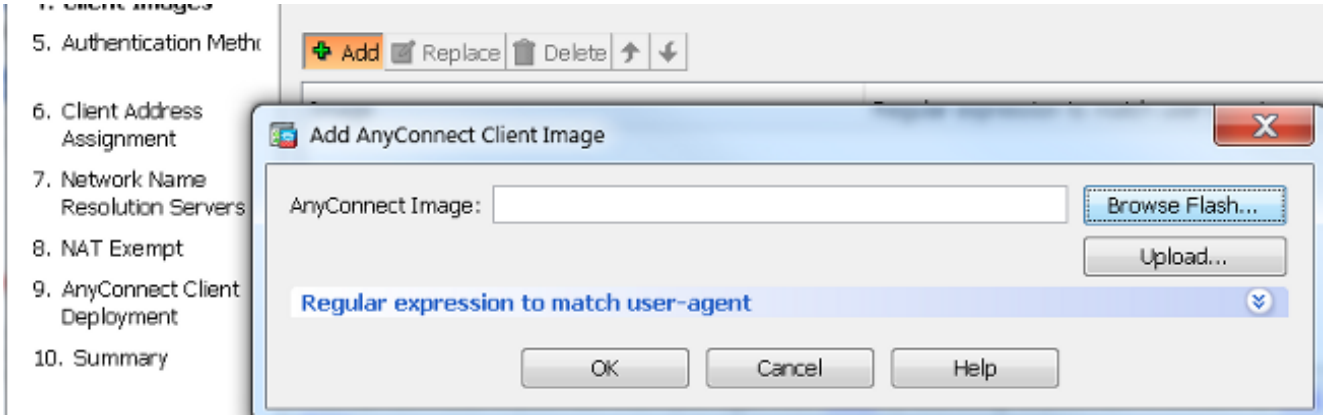
7. RSA 키 쌍이 생성된 후 키를 선택하고 Generate **self-signed certificate 확인란을** 선택합니다. Certificate Subject DN(*인증서 주체* DN) 필드에 원하는 *주체 DN*을 입력한 다음 Add **Certificate(인증서 추가)**를 클릭합니다.

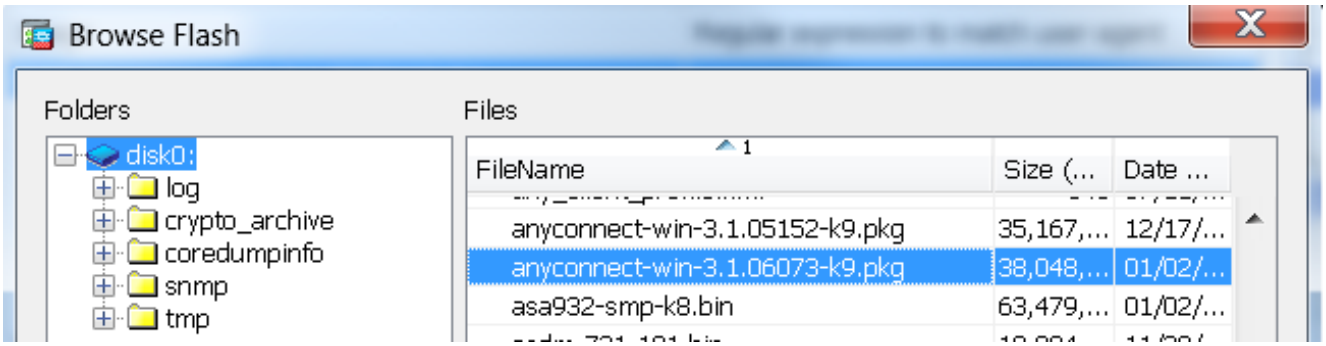


8. 등록이 완료되면 **OK(확인)**, **OK(확인)**, **Next(다음)**를 차례로 클릭합니다.

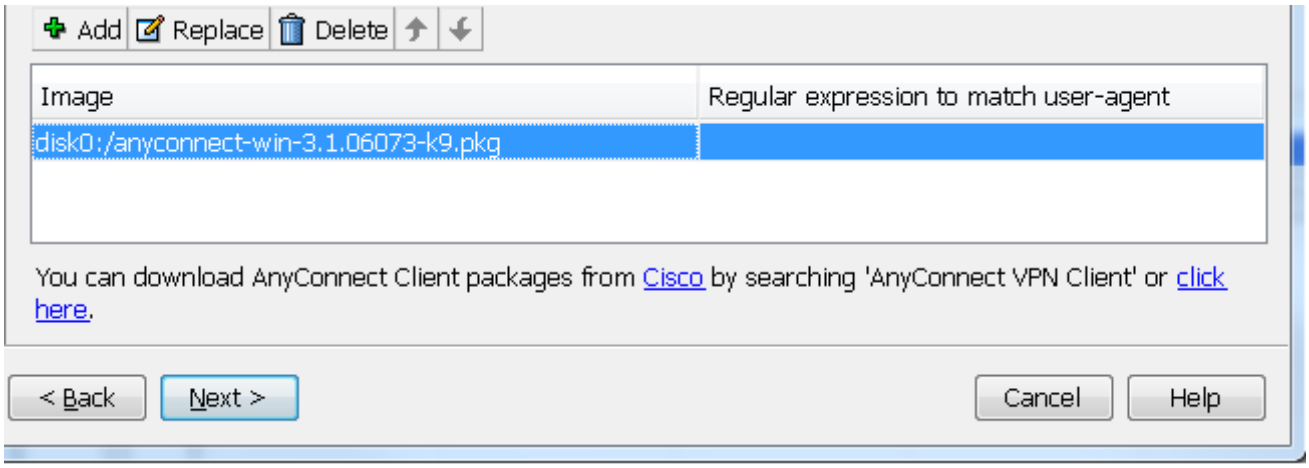


9. PC **또는** 플래시에서 AnyConnect 클라이언트 이미지(*.pkg* 파일)를 추가하려면 Add를 클릭합니다. 플래시 **드라이브**에서 이미지를 추가하려면 Browse Flash(플래시 찾아보기)를 클릭하고 호스트 시스템에서 직접 이미지를 추가하려면 **Upload(업로드)**를 클릭합니다.



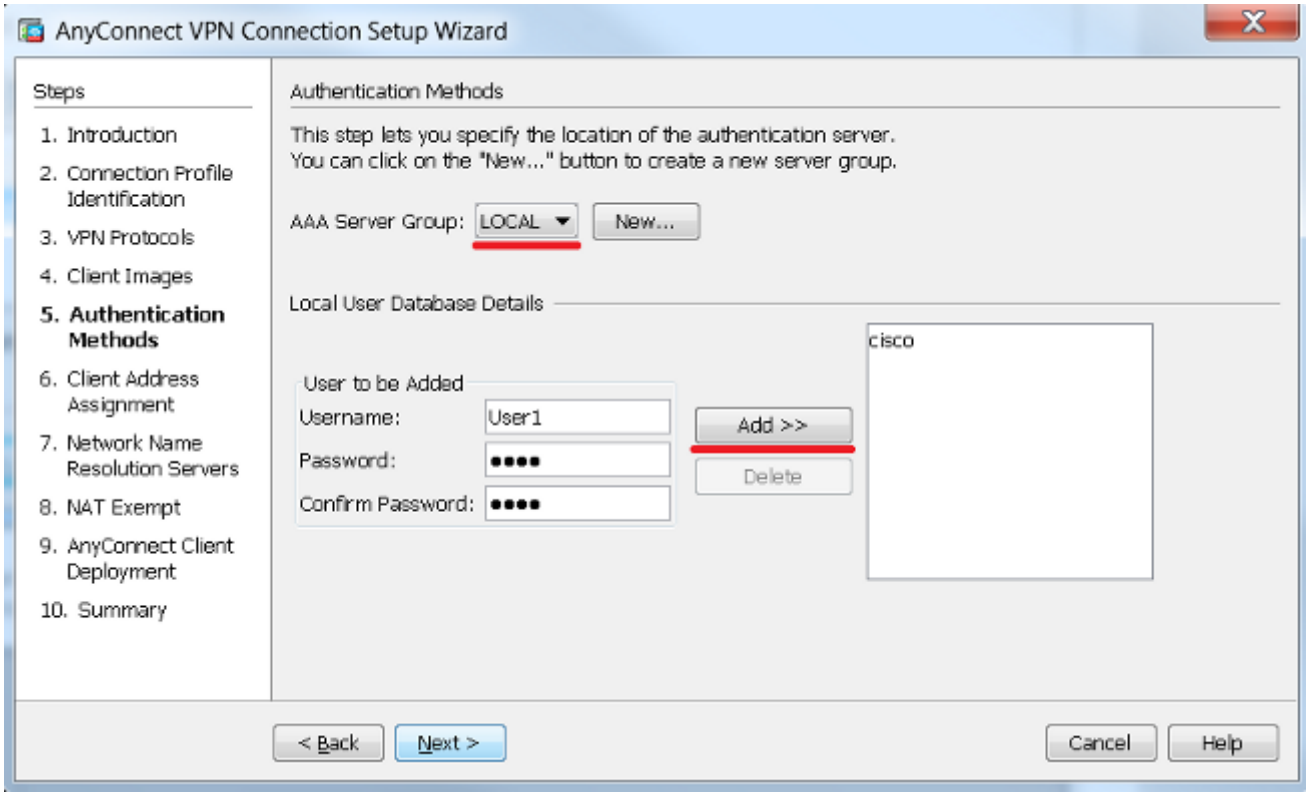


10. 이미지가 추가되면 다음을 **클릭합니다**.

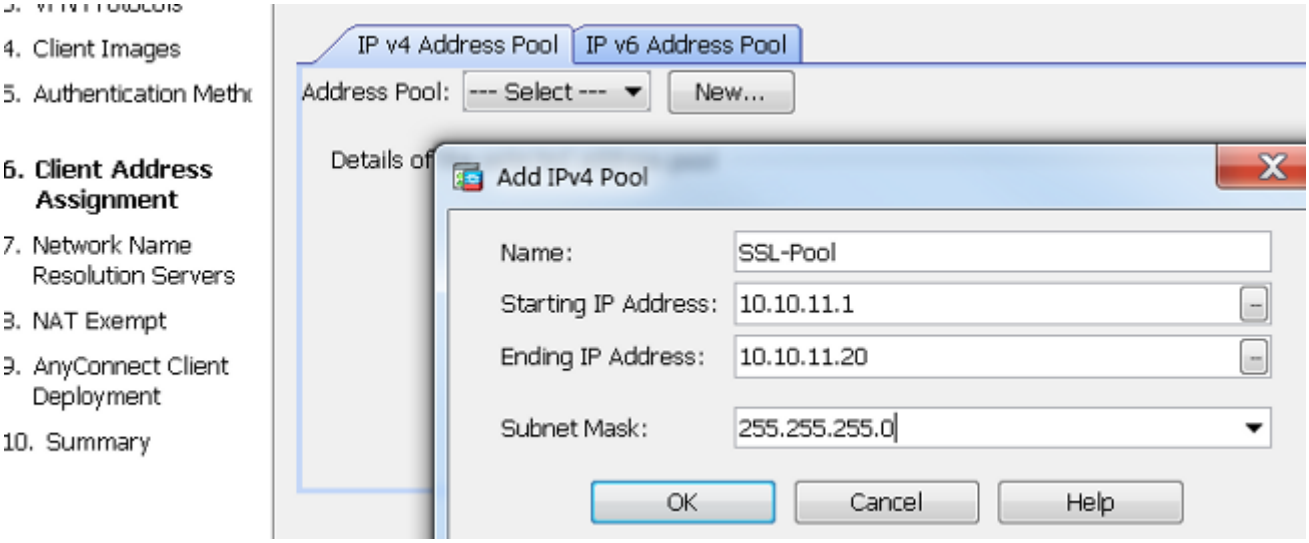


11. 사용자 인증은 AAA(Authentication, Authorization, and Accounting) 서버 그룹을 통해 완료할 수 있습니다. 사용자가 이미 구성된 경우 LOCA를 선택하고 **Next(다음)**를 클릭합니다. **참고:** 이 예에서는 **LOCAL** 인증이 구성되므로 ASA의 로컬 사용자 데이터베이스가 인증에 사용됩니다

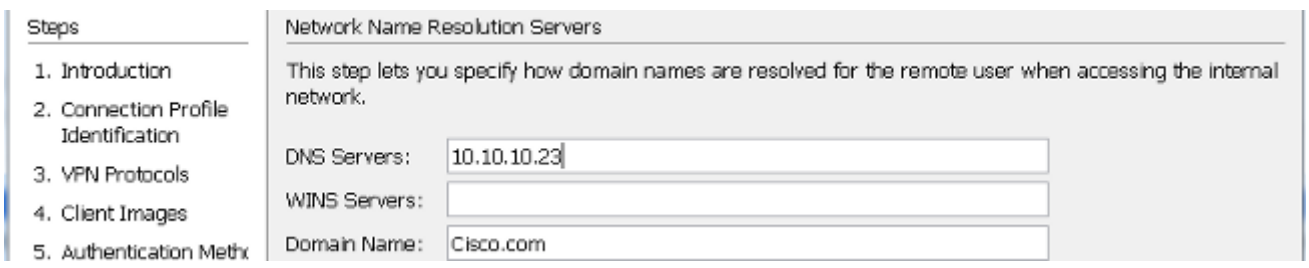
.



12. VPN 클라이언트의 주소 풀을 구성해야 합니다. 이미 구성된 경우 드롭다운 메뉴에서 선택합니다. 그렇지 않은 경우 **New(새로** 만들기)를 클릭하여 새 파일을 구성합니다. 완료되면 다음을 **클릭합니다**.

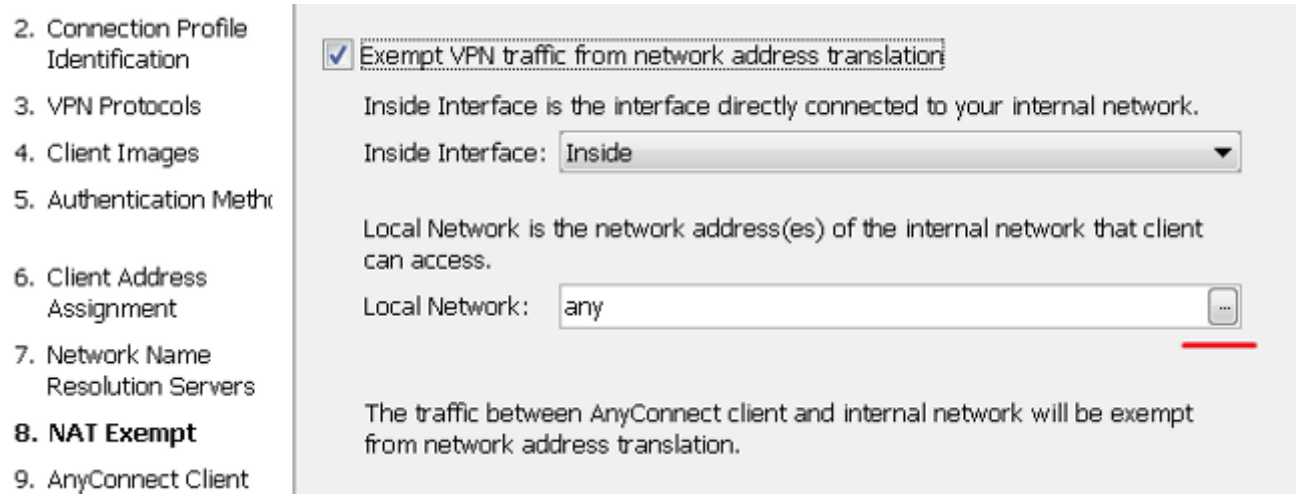


13. DNS(Domain Name System) 서버 및 DN을 *DNS* 및 *Domain Name* 필드에 적절히 입력한 후 **Next(다음)를 클릭합니다**.

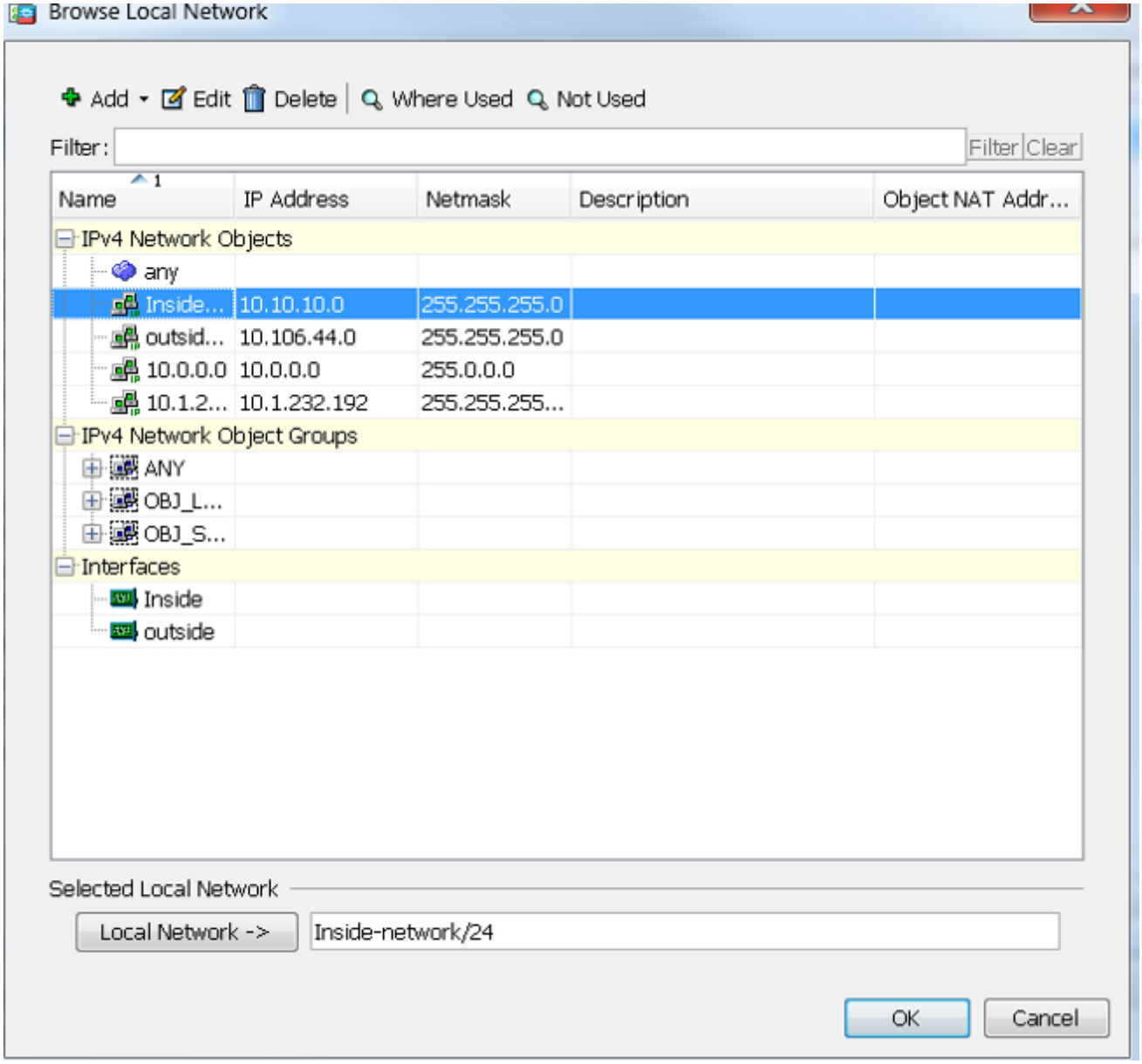


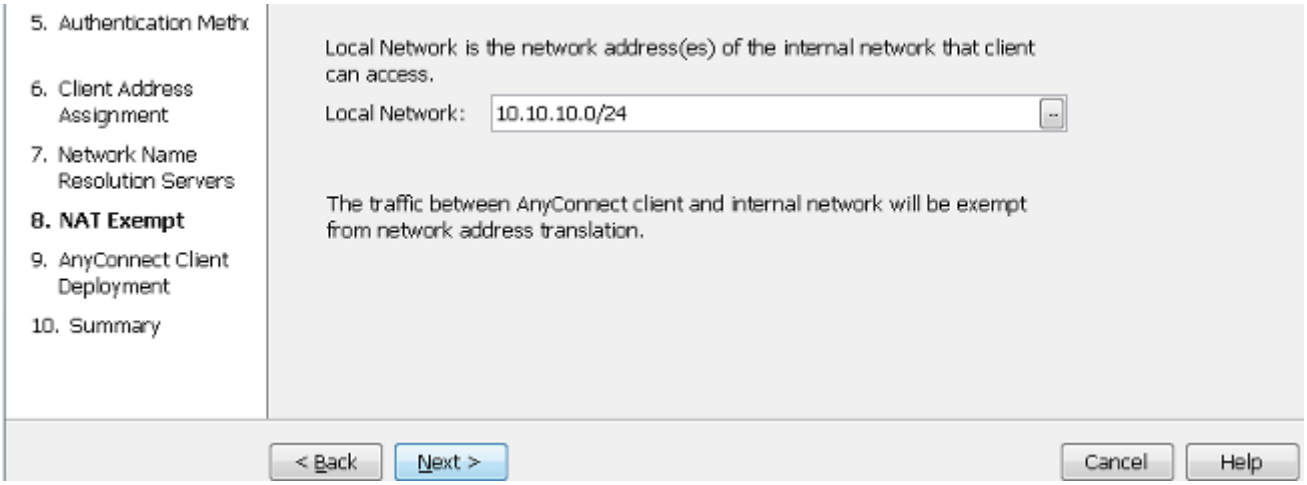
14. 이 시나리오에서는 VPN을 통한 액세스를 ASA 뒤의 *내부*(또는 LAN) 서브넷으로 구성된 **10.10.10.0/24** 네트워크로 제한하는 것을 목적으로 합니다. 클라이언트와 내부 서브넷 간의 트래픽은 동적 NAT(Network Address Translation)에서 제외되어야 합니다.

    Exempt **VPN traffic from network address translation(네트워크 주소 변환에서 VPN 트래픽 제외)** 확인란을 선택하고 제외에 사용할 LAN 및 WAN 인터페이스를 구성합니다.



15. 제외해야 하는 로컬 네트워크를 선택합니다.





16. **다음**, **다음**, 마침을 **클릭합니다**.

이제 AnyConnect 클라이언트 컨피그레이션이 완료되었습니다. 그러나 컨피그레이션 마법사를 통해 AnyConnect를 구성할 때 기본적으로 *스플릿 터널 정책*을 터널**로** 구성합니다. 특정 트래픽만 터널링하려면 *스플릿 터널링을* 구현해야 합니다.

참고: 스플릿 터널링이 구성되지 않은 경우 스플릿 터널 정책은 기본 그룹 정책

(DfltGrpPolicy)에서 상속됩니다. 이 정책은 기본적으로 Tunnelall로 **설정됩니다.** 즉, 클라이언트가 VPN을 통해 연결되면 (웹에 대한 트래픽을 포함하기 위해) 모든 트래픽이 터널을 통해 전송됩니다.

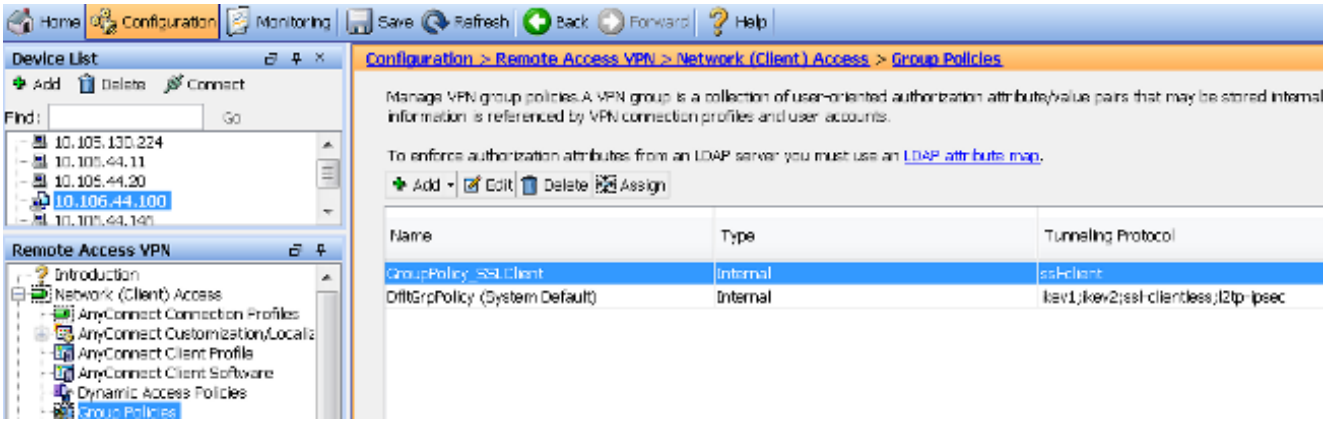
ASA WAN(또는 *외부*) IP 주소로 향하는 트래픽만 클라이언트 머신에서 터널링을 우회합니다. 이는 Microsoft Windows 시스템의 route print **명령** 출력에서 확인할 수 있습니다.

스플릿 터널 컨피그레이션

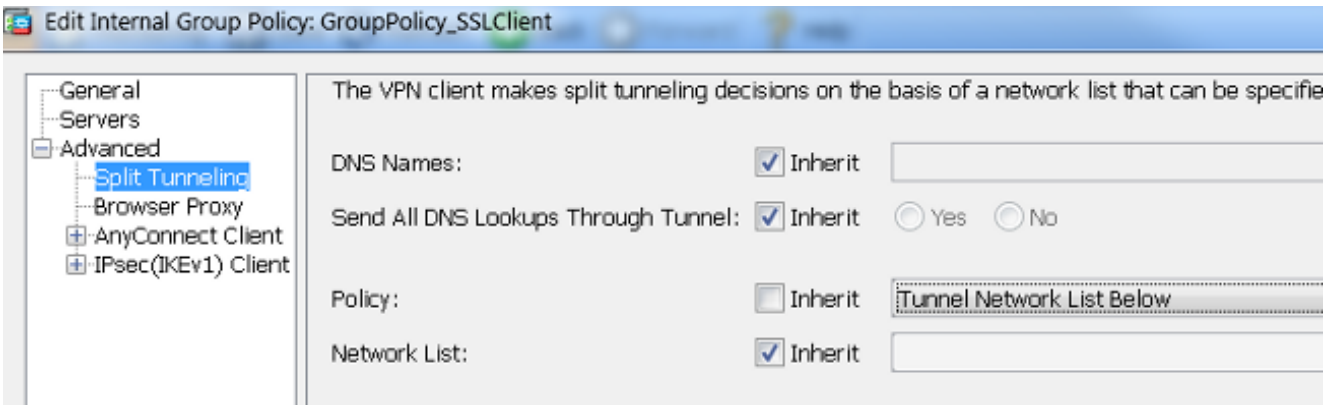
스플릿 터널링은 암호화해야 하는 서브넷 또는 호스트의 트래픽을 정의하기 위해 사용할 수 있는 기능입니다. 여기에는 이 기능과 연결될 ACL(Access Control List) 컨피그레이션이 포함됩니다. 이 ACL에 정의된 서브넷 또는 호스트의 트래픽은 클라이언트 엔드로부터 터널을 통해 암호화되며 이러한 서브넷의 경로는 PC 라우팅 테이블에 설치됩니다.

Tunnel-all 컨피그레이션에서 Split-*tunnel 컨피그레이션*으로 이동하려면 *다음 단계를* 완료합니다.

1. Configuration(컨피그레이션) **> Remote Access VPN(원격 액세스 VPN) > Group Policies(그룹 정책)로 이동합니다**.

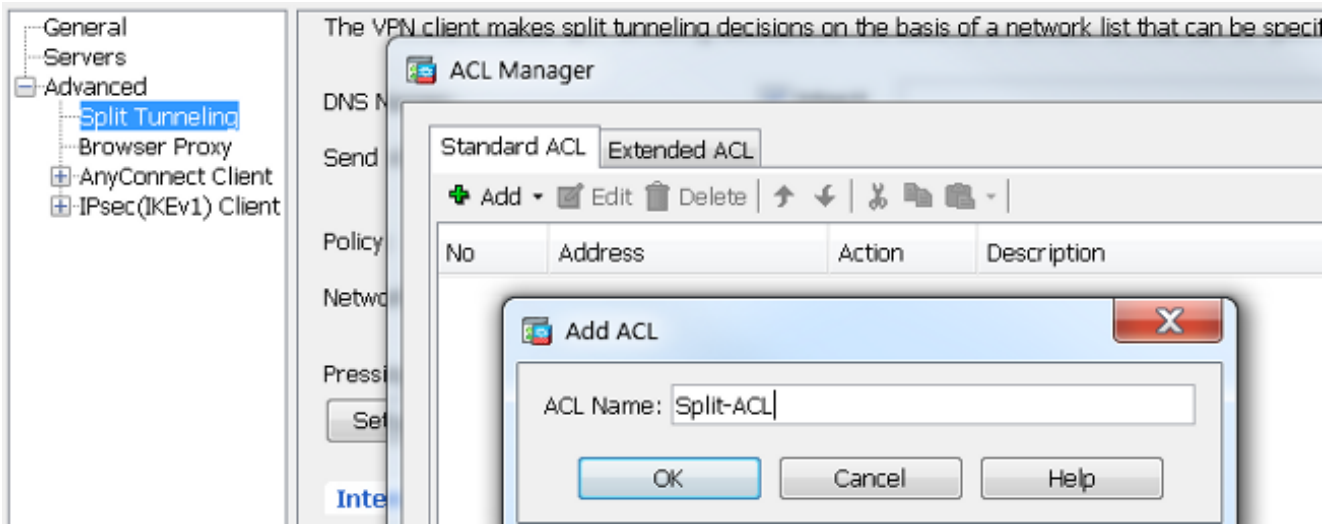


2. Edit(**편집**)를 클릭하고 탐색 트리를 사용하여 Advanced(고급) **> Split Tunneling(스플릿 터널링)**으로 이동합니다. Inherit(**상속**) 확인란의 선택을 *취소하고*, 드롭다운 메뉴에서 **Tunnel Network List Below(아래**의 **터널 네트워크 목록)를** 선택합니다.

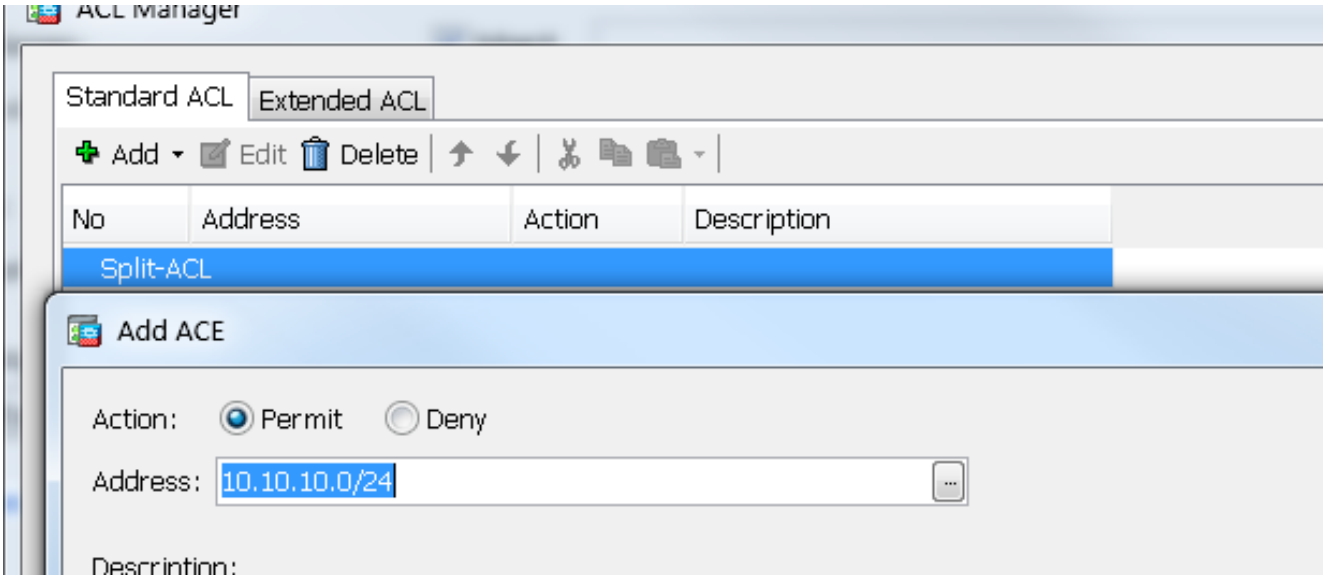


3. 클라이언트가 **액세스해야 하는** LAN 네트워크를 지정하는 ACL을 선택하려면 *Network List(네트워크 목록) 섹션*에서 Inherit(상속) 확인란의 선택을 취소하고 Manage(**관리)**를 클릭합니다.

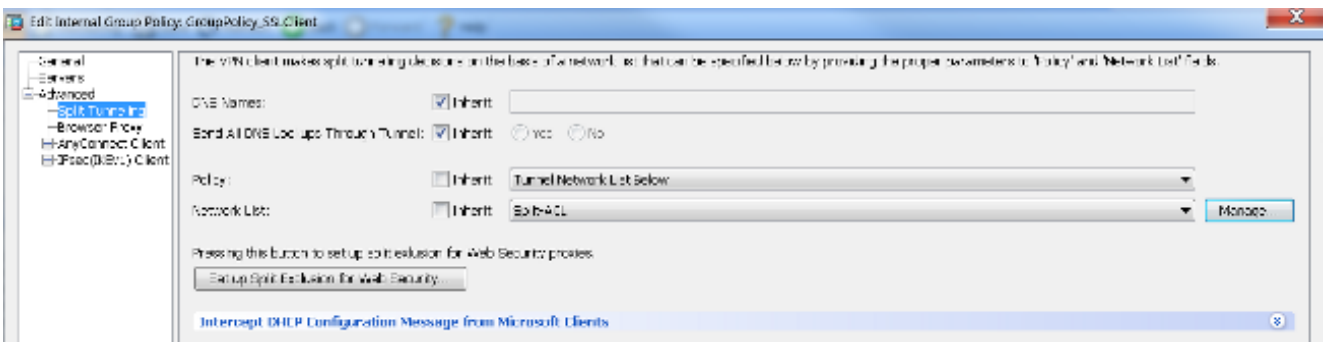
4. Standard ACL(표준 **ACL), Add(추가**), Add **ACL(ACL 추가)**을 클릭한 다음 **ACL 이름을 클릭합니다.**



5. 규칙을 **추가하려면 Add** ACE(ACE 추가)를 클릭합니다.



6. **OK(확인)**를 클릭합니다.



7. Apply를 **클릭합니다**.

일단 연결되면 스플릿 ACL의 서브넷 또는 호스트에 대한 경로가 클라이언트 시스템의 라우팅 테이블에 추가됩니다. Microsoft Windows 시스템의 경우 route print 명령의 출력에서 이를 볼 **수** 있습니다. 이러한 경로의 다음 홉은 클라이언트 IP 풀 서브넷의 IP 주소(일반적으로 서브넷의 첫 번째 IP 주소)입니다.

```
C:\Users\admin>route print
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0      255.255.255.0    10.10.11.2  10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1    255.255.255.255     On-link    10.106.44.243  6

!! This is the route for the ASA Public IP Address.
```

MAC OS 컴퓨터에서 PC 라우팅 **테이블을** 보려면 netstat -r 명령을 입력합니다.

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

AnyConnect 클라이언트 다운로드 및 설치

사용자 시스템에 Cisco AnyConnect Secure Mobility Client를 구축하기 위해 사용할 수 있는 두 가지 방법이 있습니다.

- 웹 구축
- 독립형 구축

이 두 방법은 다음 섹션에서 자세히 설명합니다.

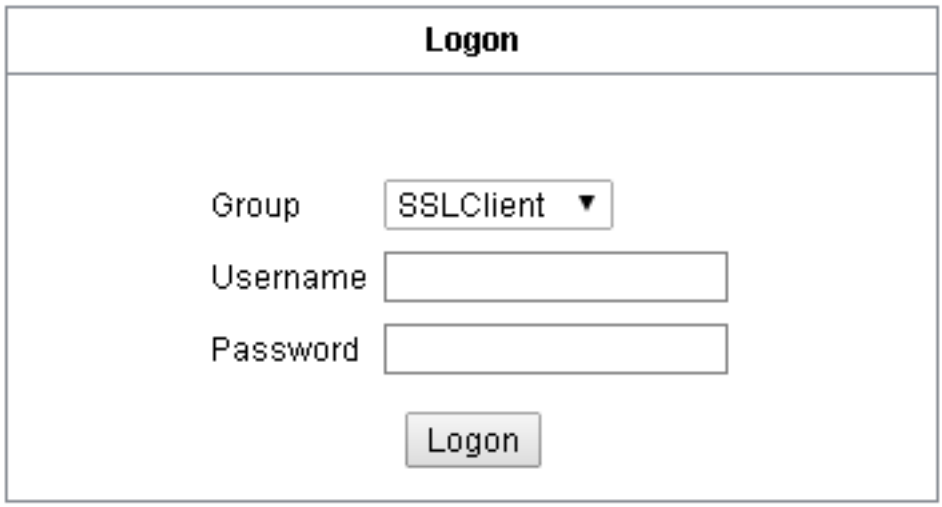
웹 구축

웹 구축 방법을 사용하려면 클라이언트 시스템의 브라우저에 https://**<ASA의 FQDN> 또는<ASA의 IP>** URL을 입력하여 *WebVPN* 포털 페이지로 이동합니다.

> **참고:** Internet Explorer(IE)를 사용하는 경우 Java를 강제로 사용하지 않는 한 대부분 ActiveX를 통해 설치가 완료됩니다. 다른 모든 브라우저에서는 Java를 사용합니다.

페이지에 로그인한 후 클라이언트 시스템에서 설치가 시작되고 설치가 완료된 후 클라이언트가 ASA에 연결되어야 합니다.

> **참고:** ActiveX 또는 Java를 실행할 수 있는 권한을 묻는 메시지가 표시될 수 있습니다. 설치를 계속하려면 이를 허용해야 합니다.



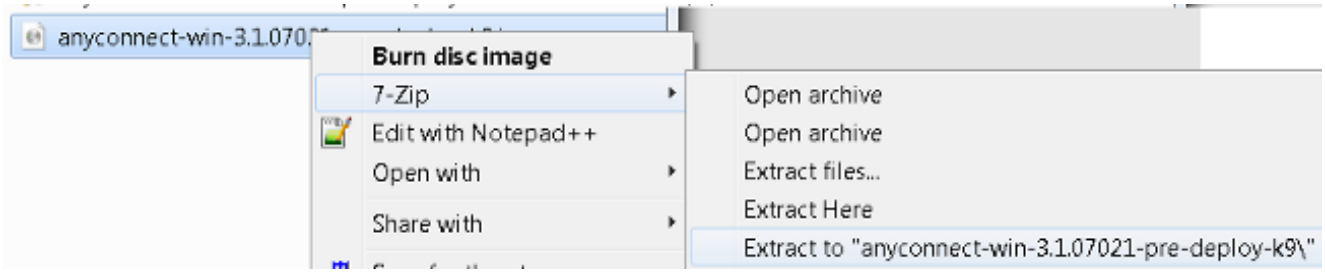
독립형 구축

독립형 구축 방법을 사용하려면 다음 단계를 완료하십시오.

1. Cisco 웹 사이트에서 AnyConnect 클라이언트 이미지를 다운로드합니다. 다운로드할 올바른 이미지를 선택하려면 Cisco AnyConnect Secure Mobility Client 웹 페이지를 참조하십시오. 다운로드 링크는 이 페이지에 제공됩니다. 다운로드 페이지로 이동하여 적절한 버전을 선택합니다. **전체 설치 패키지 - 창/독립형 설치 프로그램(ISO) 검색을 수행합니다. 참고:** 그런 다음 ISO

설치 프로그램 이미지(예: *anyconnect-win-3.1.06073-pre-deploy-k9.iso*)를 다운로드합니다.

2. WinRar *또는 7-Zip*을 사용하여 ISO 패키지의 내용을 추출합니다.



3. 콘텐츠가 추출되면 Setup.**exe 파일**을 실행하고 Cisco AnyConnect Secure Mobility Client와 함께 설치해야 하는 모듈을 선택합니다.

팁: VPN에 대한 추가 설정을 구성하려면 *Cisco ASA 5500 Series Configuration Guide*의 CLI, *8.4 및 8.6을 사용하여 Configuring AnyConnect VPN Client Connections 섹션을 참조하십시오*.

CLI 컨피그레이션

이 섹션에서는 참조를 위해 Cisco AnyConnect Secure Mobility Client의 CLI 컨피그레이션을 제공합니다.

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!**********Split ACL configuration**********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
```

```
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate***********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
```

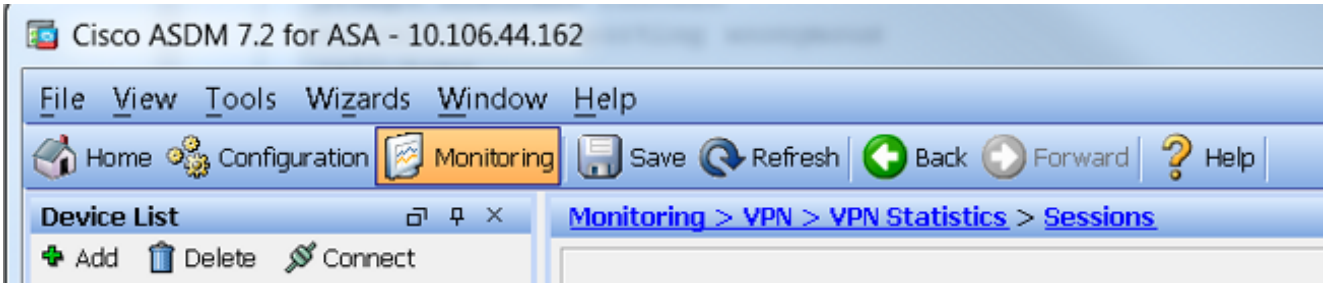
```
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
```

```
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

다음을 확인합니다.

클라이언트 연결 및 해당 연결과 연결된 다양한 매개변수를 확인하려면 다음 단계를 완료하십시오.

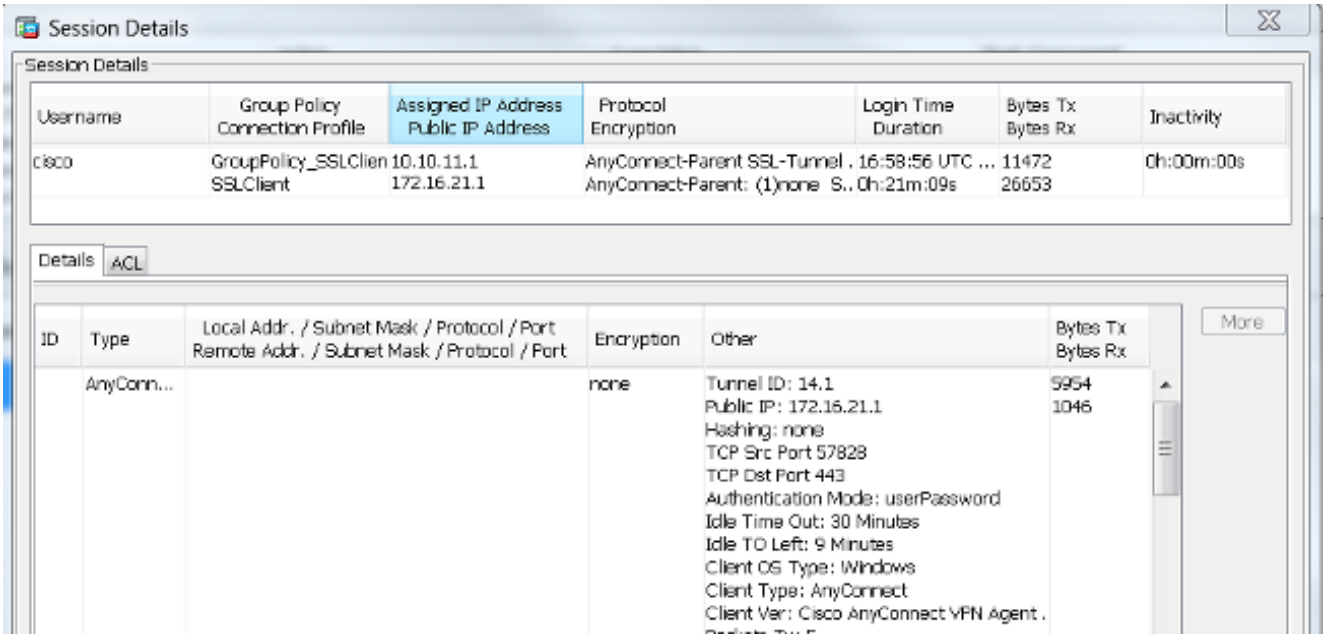
1. ASDM에서 **Monitoring > VPN**으로 이동합니다.



2. VPN 유형을 **필터링하려면 Filter** By 옵션을 사용할 수 있습니다. 드롭다운 **메뉴**와 모든 AnyConnect 클라이언트 세션에서 AnyConnect 클라이언트를 선택합니다. **팁:** 세션은 Username(사용자 이름) 및 *IP address(IP 주소)*와 같은 다른 기준으로 추가로 필터링할 수 있습니다

.

3. 특정 세션에 대한 자세한 내용을 보려면 해당 세션을 두 번 클릭합니다.



4. 세션 세부사항을 **가져오려면 CLI**에 show vpn-sessiondb anyconnect 명령을 입력합니다.

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. 다른 필터 옵션을 사용하여 결과를 세분화할 수 있습니다.

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

문제 해결

AnyConnect 설치 및 연결 문제를 해결하는 데 유용한 데이터를 수집하기 위해 AnyConnect 진단 및 보고 도구(DART)를 사용할 수 있습니다. DART 마법사는 AnyConnect를 실행하는 컴퓨터에서 사용됩니다. DART는 Cisco TAC(Technical Assistance Center) 분석을 위해 로그, 상태 및 진단 정보를 취합하며 클라이언트 시스템에서 실행하는 데 관리자 권한이 필요하지 않습니다.

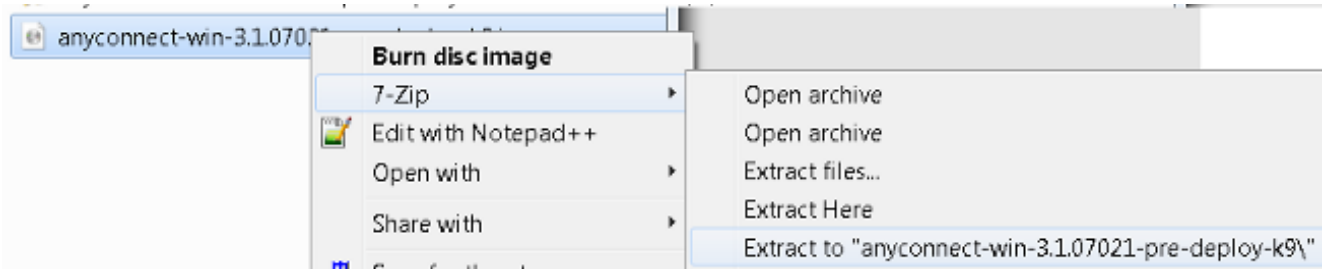
DART 설치

DART를 설치하려면 다음 단계를 완료하십시오.

1. Cisco 웹 사이트에서 AnyConnect 클라이언트 이미지를 다운로드합니다. 다운로드할 올바른 이미지를 선택하려면 Cisco AnyConnect Secure Mobility Client 웹 페이지를 참조하십시오. 다운로드 링크는 이 페이지에 제공됩니다. 다운로드 페이지로 이동하여 적절한 버전을 선택합니다. **전체 설치 패키지 - 창/독립형 설치 프로그램(ISO) 검색을 수행합니다**. **참고:** 그런 다음 ISO

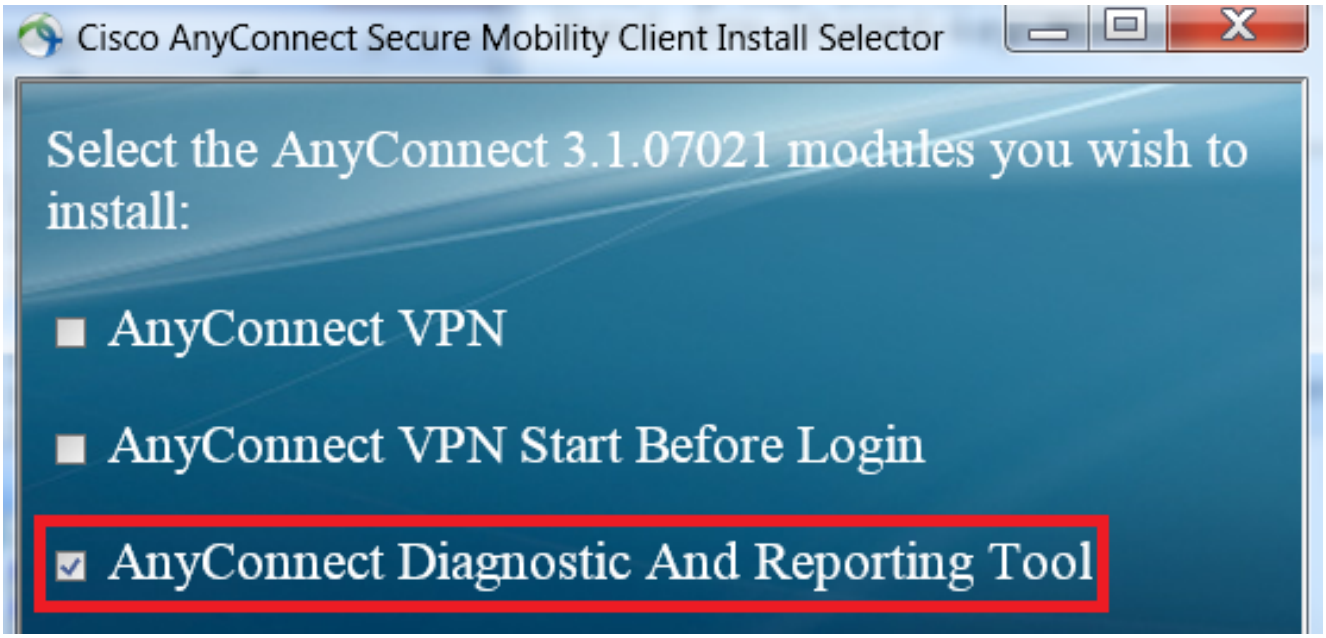
설치 프로그램 이미지(예: *anyconnect-win-3.1.06073-pre-deploy-k9.iso*)를 다운로드합니다.

2. WinRar *또는 7-Zip*을 사용하여 ISO 패키지의 내용을 추출합니다.



3. 내용을 추출한 폴더를 찾습니다.

4. Setup.**exe 파일**을 실행하고 Anyconnect **진단 및 보고 도구만 선택합니다**.



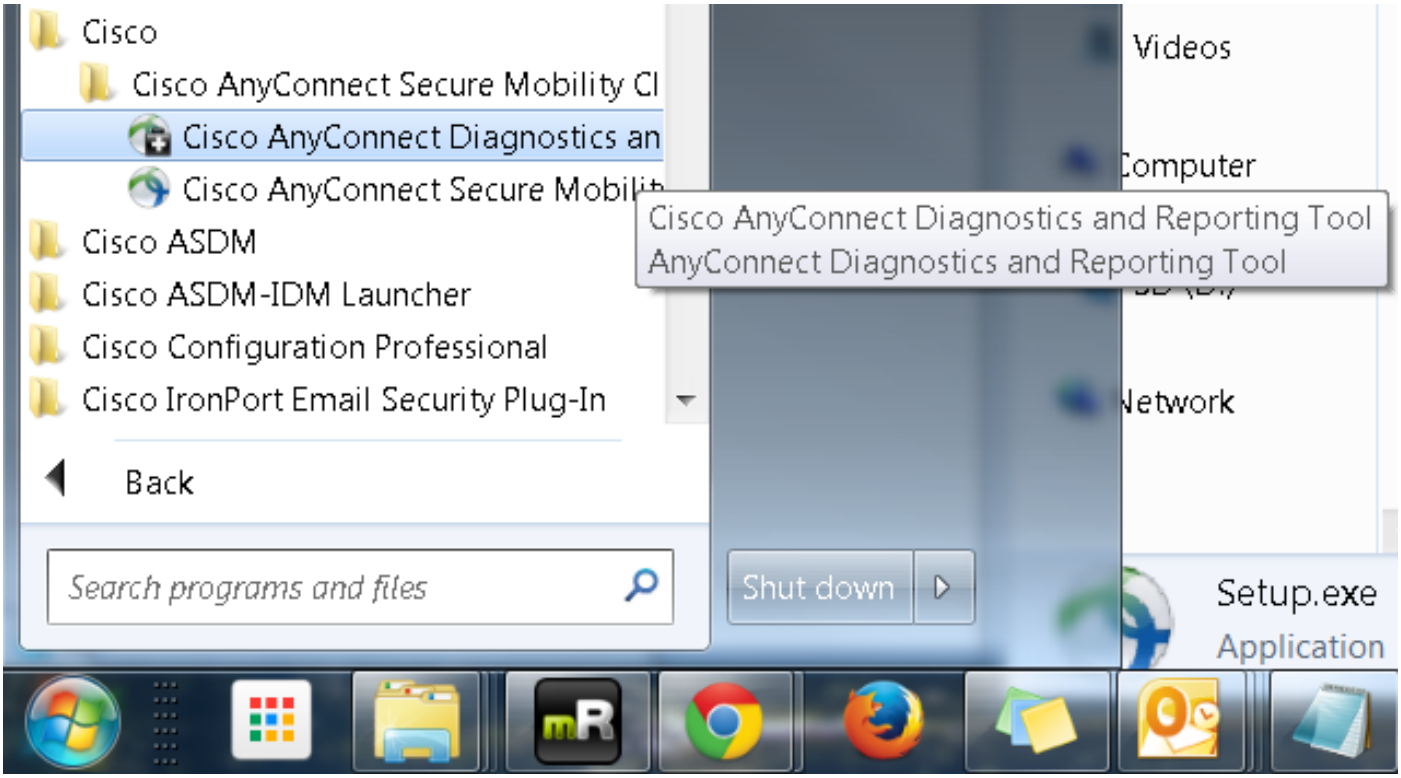
DART 실행

DART를 실행하기 전에 고려해야 할 몇 가지 중요한 정보는 다음과 같습니다.

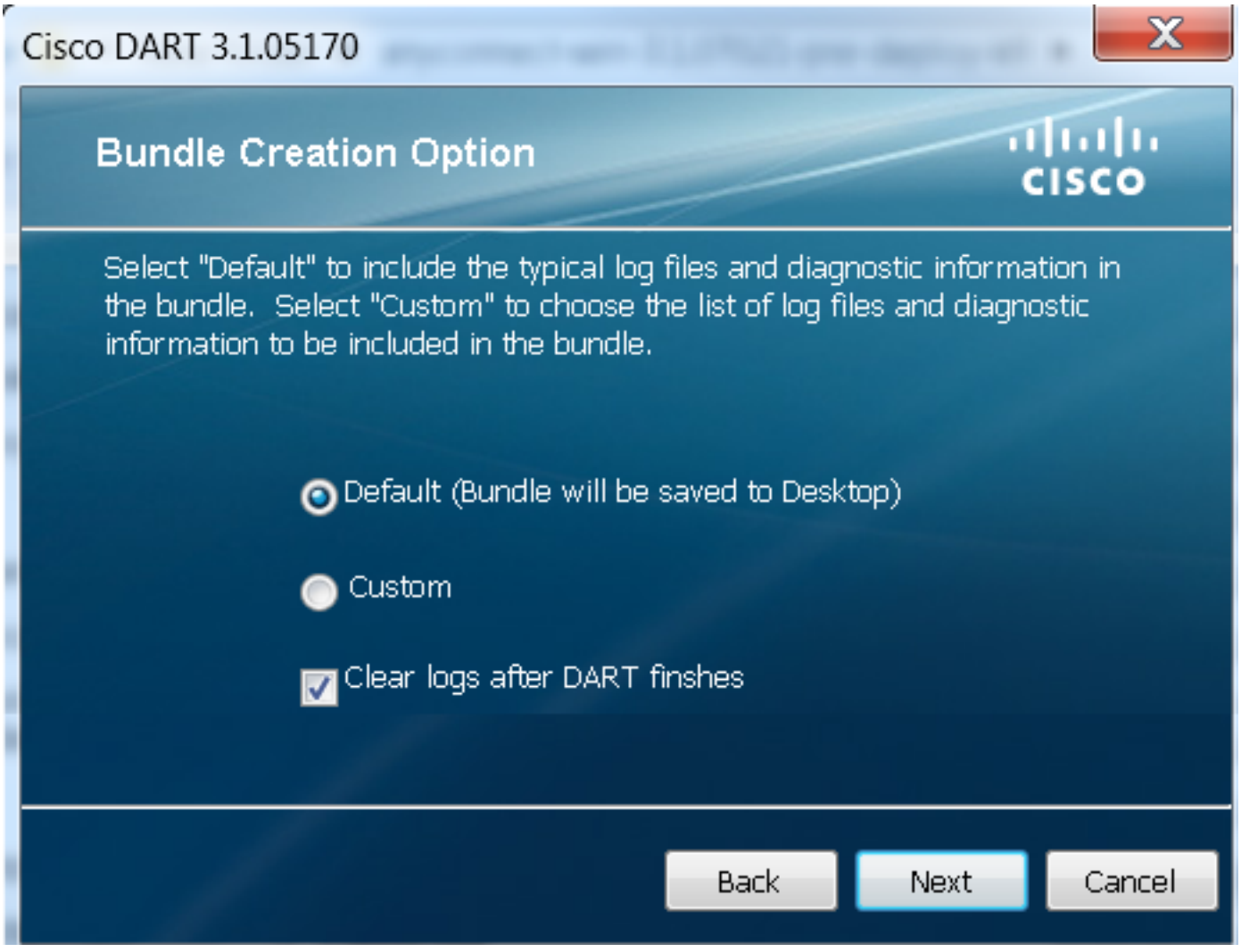
- DART를 실행하기 전에 문제를 한 번 이상 다시 생성해야 합니다.

- 문제가 다시 생성될 때 사용자 시스템의 날짜 및 시간을 기록해야 합니다.

클라이언트 시스템의 *시작 메뉴*에서 DART를 실행합니다.



기본 *또는 사용자 지정* 모드를 선택할 수 있습니다. 모든 정보를 한 번에 캡처할 수 있도록 기본 모드에서 DART를 실행하는 것이 좋습니다.



완료되면 툴은 DART bundle *.zip* 파일을 클라이언트 데스크톱에 저장합니다. 그런 다음 추가 분석

을 위해 (TAC 케이스를 연 후) 번들을 TAC에 이메일로 보낼 수 있습니다.

관련 정보

- AnyConnect VPN 클라이언트 트러블슈팅 가이드 - 일반적인 문제
- Java 7 Issues with AnyConnect, CSD/Hostscan 및 WebVPN - 문제 해결 설명서
- 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.