

로컬 LAN에 대한 AnyConnect 클라이언트 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[배경 정보](#)

[AnyConnect Secure Mobility Client에 대한 로컬 LAN 액세스 구성](#)

[ASDM을 통해 ASA 구성](#)

[CLI를 통해 ASA 구성](#)

[Cisco AnyConnect Secure Mobility Client 구성](#)

[사용자 기본 설정](#)

[XML 프로파일 예](#)

[다음을 확인합니다.](#)

[Cisco AnyConnect Secure Mobility Client](#)

[Ping으로 로컬 LAN 액세스 테스트](#)

[문제 해결](#)

[이름으로 인쇄 또는 검색할 수 없음](#)

[관련 정보](#)

소개

이 문서에서는 Cisco AnyConnect Secure Mobility Client가 Cisco ASA에 연결된 상태에서 로컬 LAN에 액세스하도록 허용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에 기능적 원격 액세스 VPN 컨피그레이션이 이미 있다고 가정합니다.

필요한 경우 [CLI Book 3: Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.17](#)에서 컨피그레이션 지원을 참조하십시오.

사용되는 구성 요소

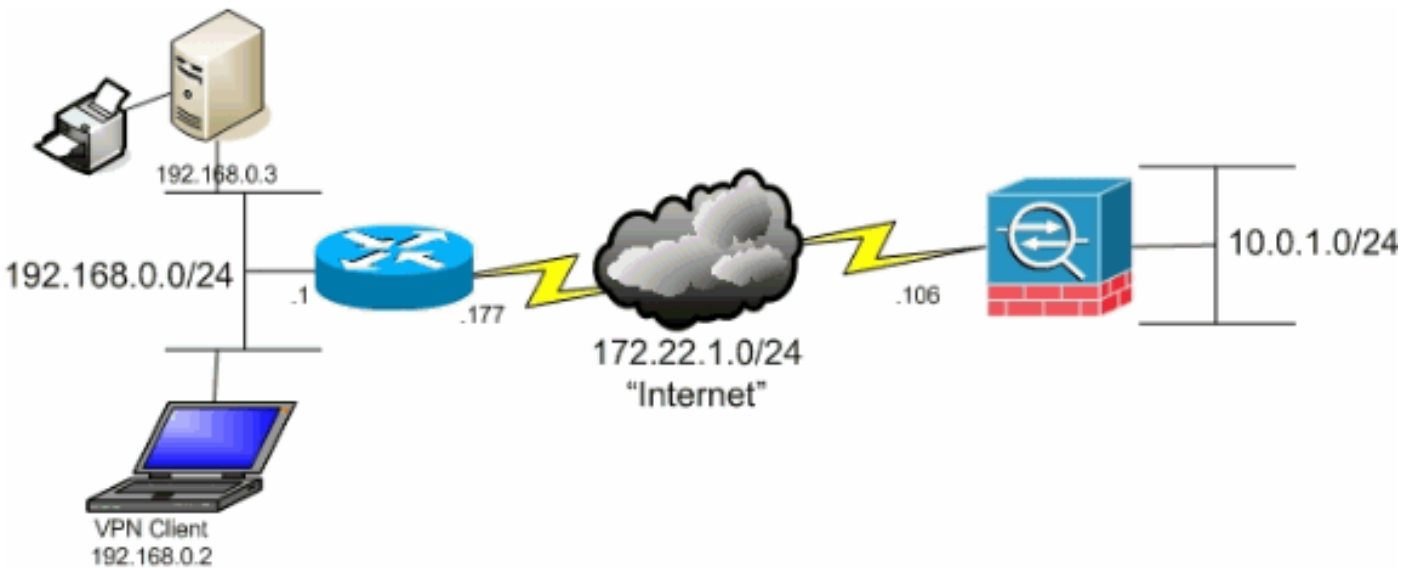
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500 Series 버전 9(2)1
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.1(6)
- Cisco AnyConnect Secure Mobility Client 버전 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

클라이언트는 일반적인 SOHO(Small Office/Home Office) 네트워크에 있으며 인터넷을 통해 본사에 연결됩니다.



배경 정보


이 컨피그레이션을 통해 Cisco AnyConnect Secure Mobility Client는 IPsec, SSL(Secure Sockets Layer) 또는 IKEv2(Internet Key Exchange Version 2)를 통해 기업 리소스에 안전하게 액세스할 수 있으며, 클라이언트가 있는 위치에 인쇄와 같은 작업을 수행할 수 있는 기능을 클라이언트에 제공합니다. 허용된 경우 인터넷으로 향하는 트래픽은 여전히 ASA로 터널링됩니다.

모든 인터넷 트래픽이 암호화되지 않은 상태로 전송되는 기존 스플릿 터널링 시나리오와 달리, VPN 클라이언트에 대해 로컬 LAN 액세스를 활성화하면 해당 클라이언트가 있는 네트워크의 디바이스만 사용하여 암호화되지 않은 상태로 통신할 수 있습니다. 예를 들어, 집에서 ASA에 연결되어 있는 동안 로컬 LAN 액세스가 허용된 클라이언트는 자체 프린터로 인쇄할 수 있지만 먼저 터널을 통해 트래픽을 전송하지 않으면 인터넷에 액세스할 수 없습니다.

액세스 목록은 ASA에서 스플릿 터널링이 구성된 것과 동일한 방식으로 로컬 LAN 액세스를 허용하기 위해 사용됩니다. 그러나 스플릿 터널링 시나리오와 달리 이 액세스 목록은 암호화해야 하는 네트워크를 정의하지는 않습니다. 그 대신, 어떤 네트워크를 암호화하지 않아야 할지를 정의합니다. 또한 스플릿 터널링 시나리오와 달리 목록의 실제 네트워크를 알 필요가 없습니다. 대신 ASA는 0.0.0.0/255.255.255.255의 기본 네트워크를 제공하며, 이는 클라이언트의 로컬 LAN을 의미하는 것으로 이해됩니다.



참고: 클라이언트가 ASA에 연결되어 있는 동안 인터넷에 암호화되지 않은 액세스 권한을 갖는 스플릿 터널링을 위한 컨피그레이션이 아닙니다. [ASA에서 스플릿 터널링을 구성하는 방법](#)에 대한 자세한 내용은 CLI Book 3: Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.17의 Set the Split-Tunneling Policy를 참조하십시오.

 참고: 클라이언트가 연결되어 있고 로컬 LAN 액세스를 위해 구성된 경우 로컬 LAN에서 이름으로 인쇄하거나 검색할 수 없습니다. 그러나 IP 주소별로 찾아보거나 인쇄할 수 있습니다. 이 [상황](#)의 해결 방법과 자세한 내용은 이 문서의 문제 해결 섹션을 참조하십시오.

AnyConnect Secure Mobility Client에 대한 로컬 LAN 액세스 구성

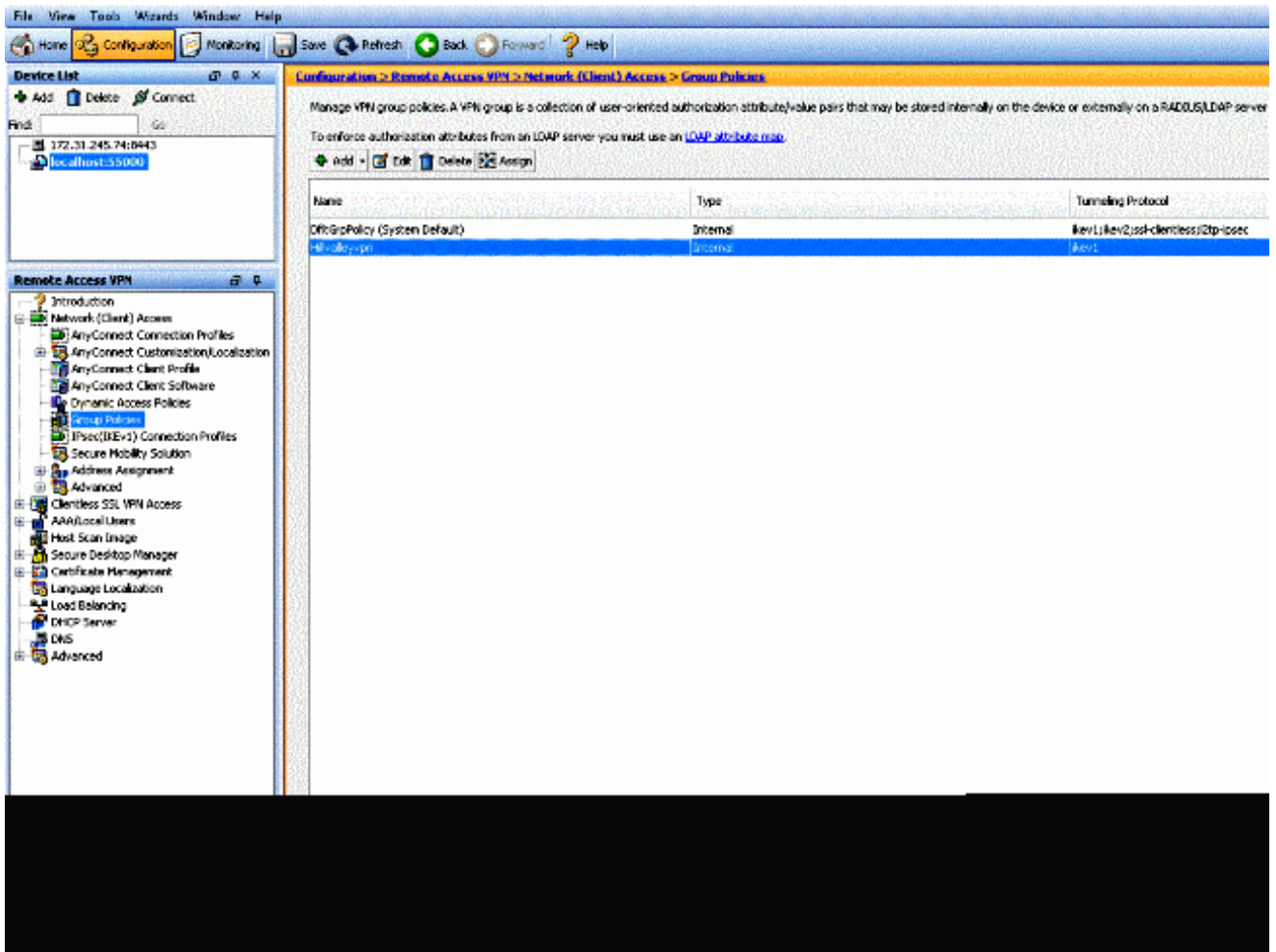
Cisco AnyConnect Secure Mobility Client가 ASA에 연결되어 있는 동안 로컬 LAN에 액세스할 수 있도록 하려면 다음 작업을 완료합니다.

- [ASDM을 통해 ASA를 구성하거나 CLI를 통해 ASA를 구성합니다](#)
- [Cisco AnyConnect Secure Mobility Client 구성](#)

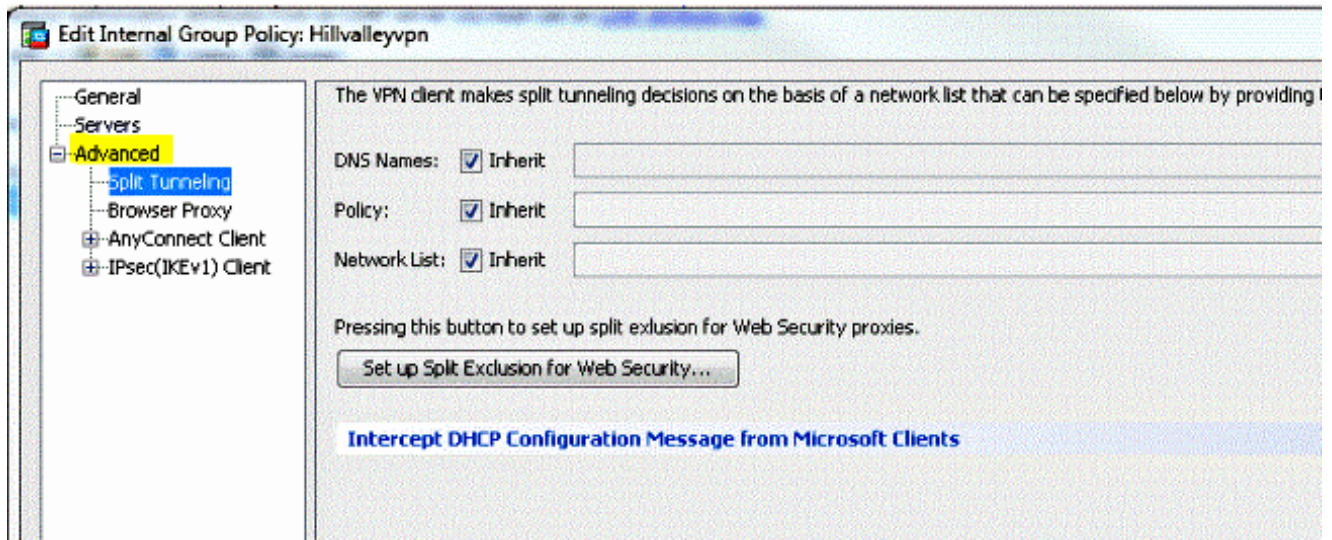
ASDM을 통해 ASA 구성

VPN 클라이언트가 ASA에 연결되어 있는 동안 로컬 LAN 액세스를 허용하려면 ASDM에서 다음 단계를 완료합니다.

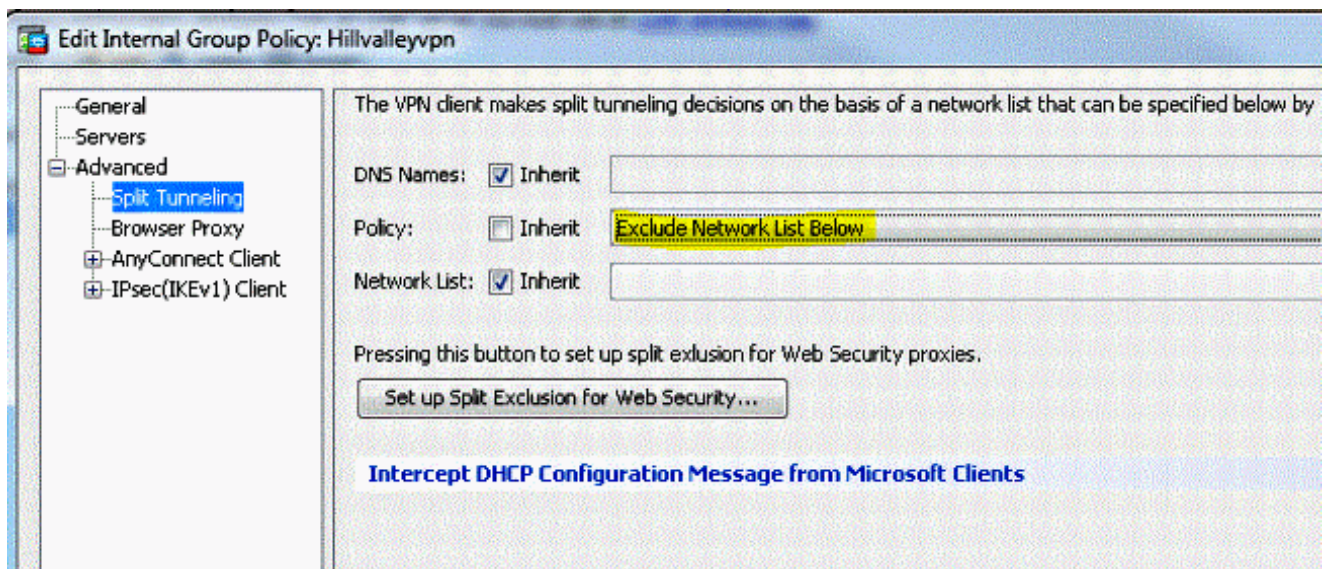
1. 로컬 LAN 액세스 Configuration > Remote Access VPN > Network (Client) Access > Group Policy 를 활성화하려는 그룹 정책을 선택하고 선택합니다. 그런 다음 을 Edit클릭합니다.



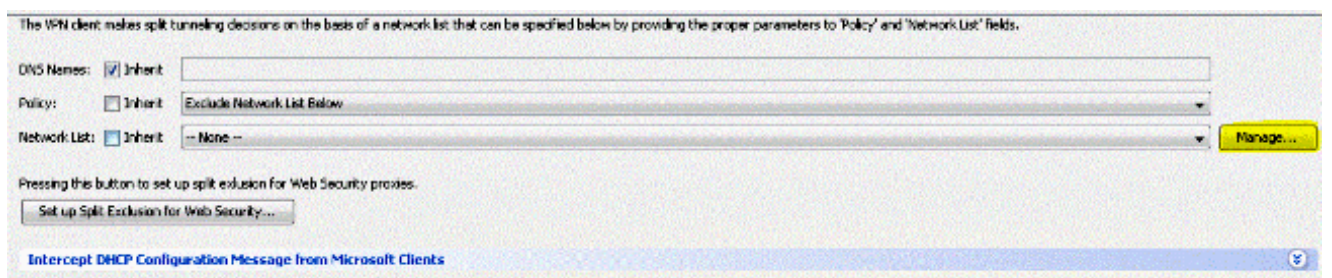
- 로 Advanced > Split Tunneling이동합니다.



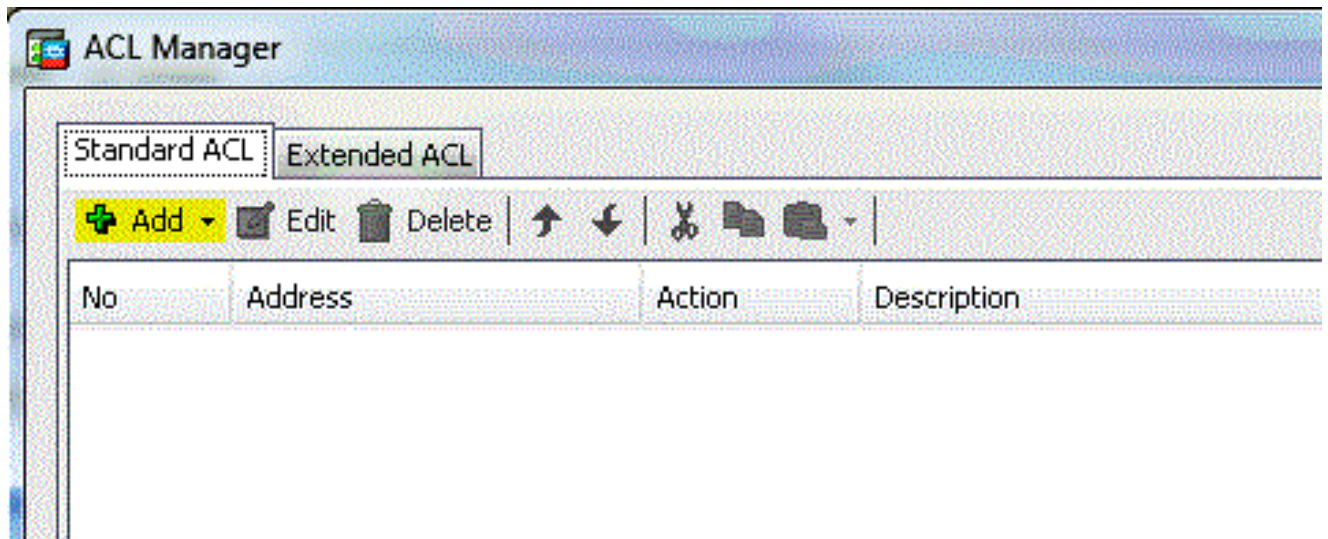
- Policy(정책) **Inherit** 확인란의 선택을 취소하고 **Exclude Network List Below** 선택합니다.



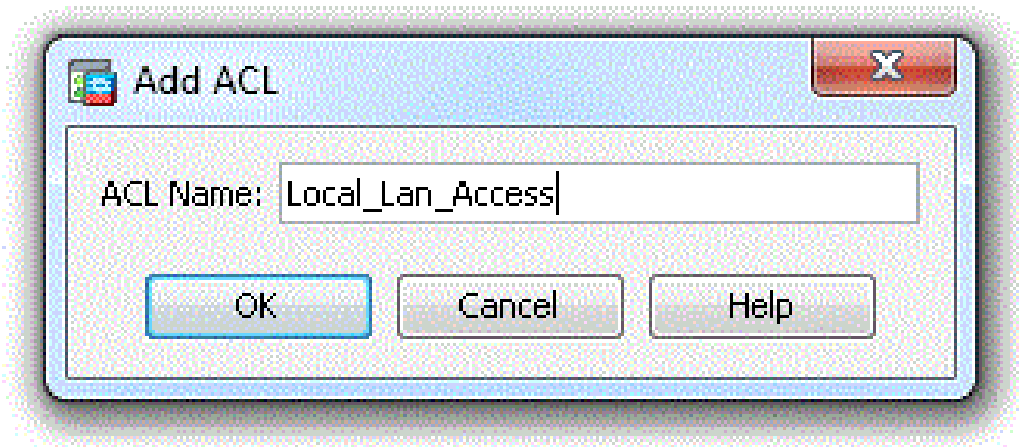
- Network List(**Inherit** 네트워크 목록) 확인란 **Manage** 의 선택을 취소한 다음 ACL(Access Control List) Manager를 실행하려면 을 클릭합니다.



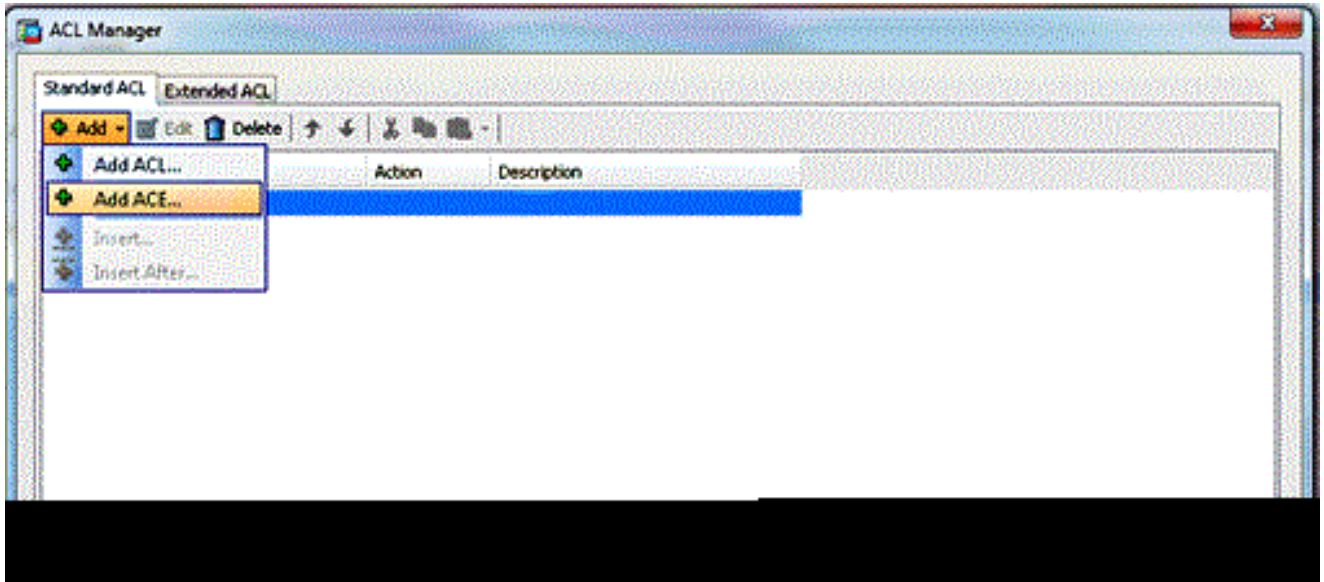
- ACL Manager(ACL 관리자) 내 **Add > Add ACL...** 에서 새 액세스 목록을 생성하려면 선택합니다.



- ACL의 이름을 입력하고 **OK**클릭합니다.



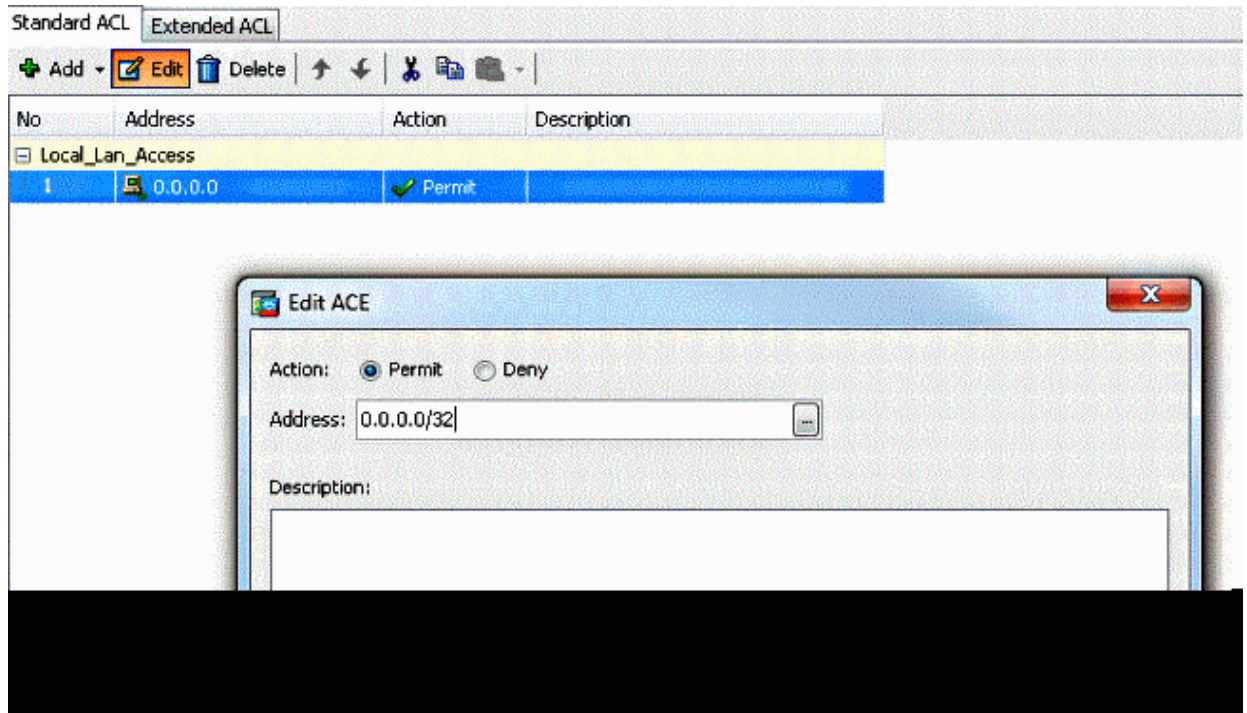
- ACL이 생성되면 ACE(Access Control Entry) **Add > Add ACE...** 를 추가하도록 선택합니다.



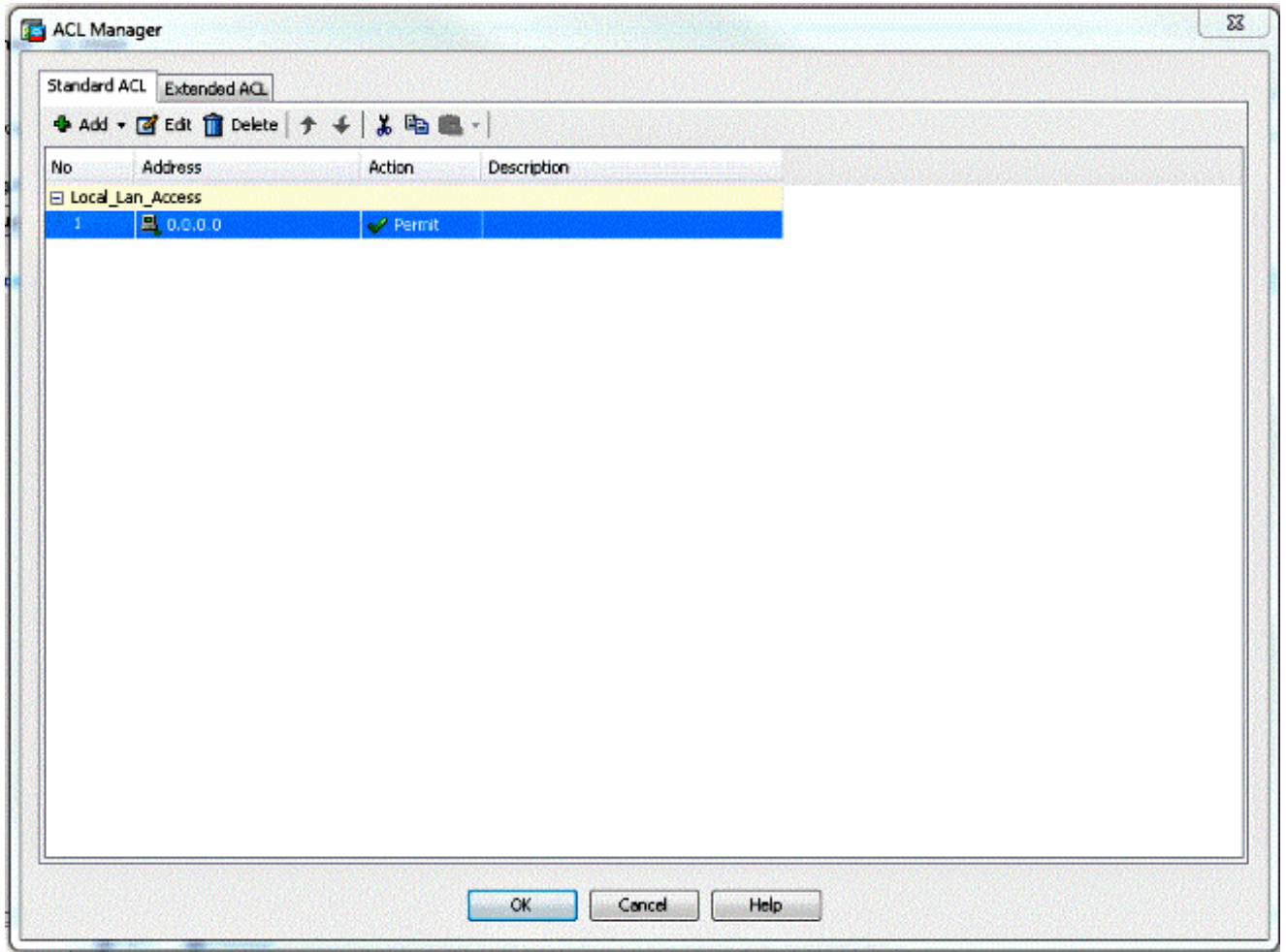
- 클라이언트의 로컬 LAN에 해당하는 ACE를 정의합니다.

a. 를 **Permit** 선택합니다.

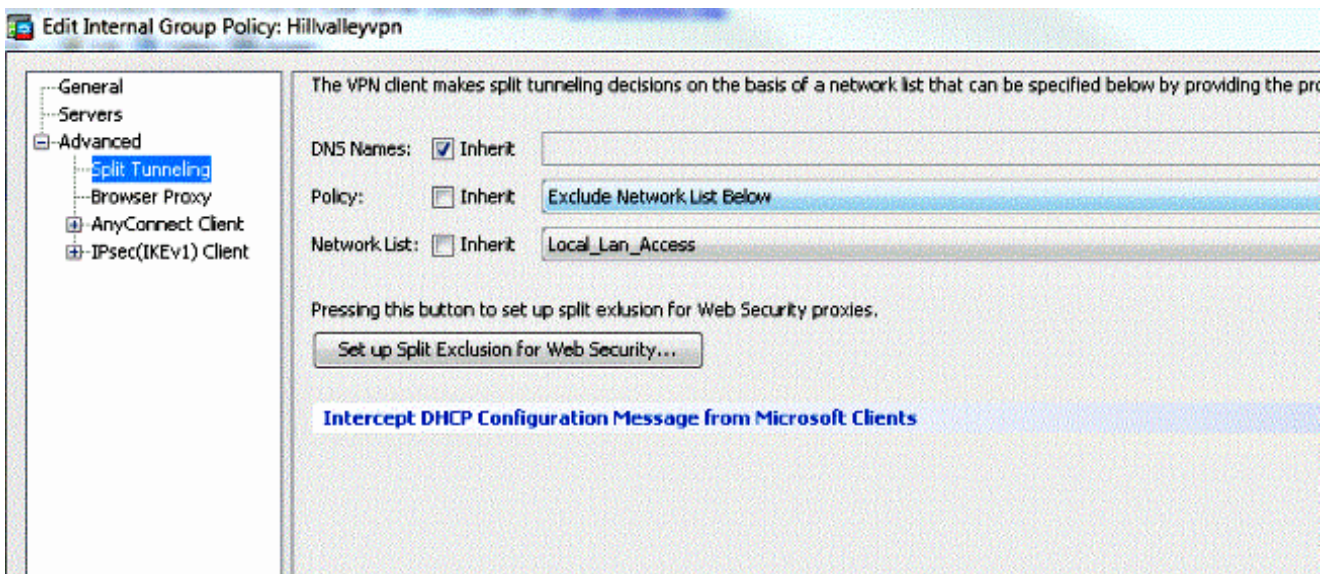
- 0.0.0.0의 IP 주소 선택
- /32의 넷마스크를 선택합니다.
- (선택 사항) 설명을 제공합니다.
- 를 **OK** 클릭합니다.



- ACL 관리자 OK 를 종료하려면 를 클릭합니다.



- 방금 생성한 ACL이 스플릿 터널 네트워크 목록에 대해 선택되었는지 확인합니다.



- 그룹 정책 컨피그레이션 **OK** 으로 돌아가려면 을 클릭합니다.

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameter

DNS Names: Inherit

Policy: Inherit Exclude Network List Below

Network List: Inherit Local_Lan_Access

Pressing this button to set up split exclusion for Web Security proxies.

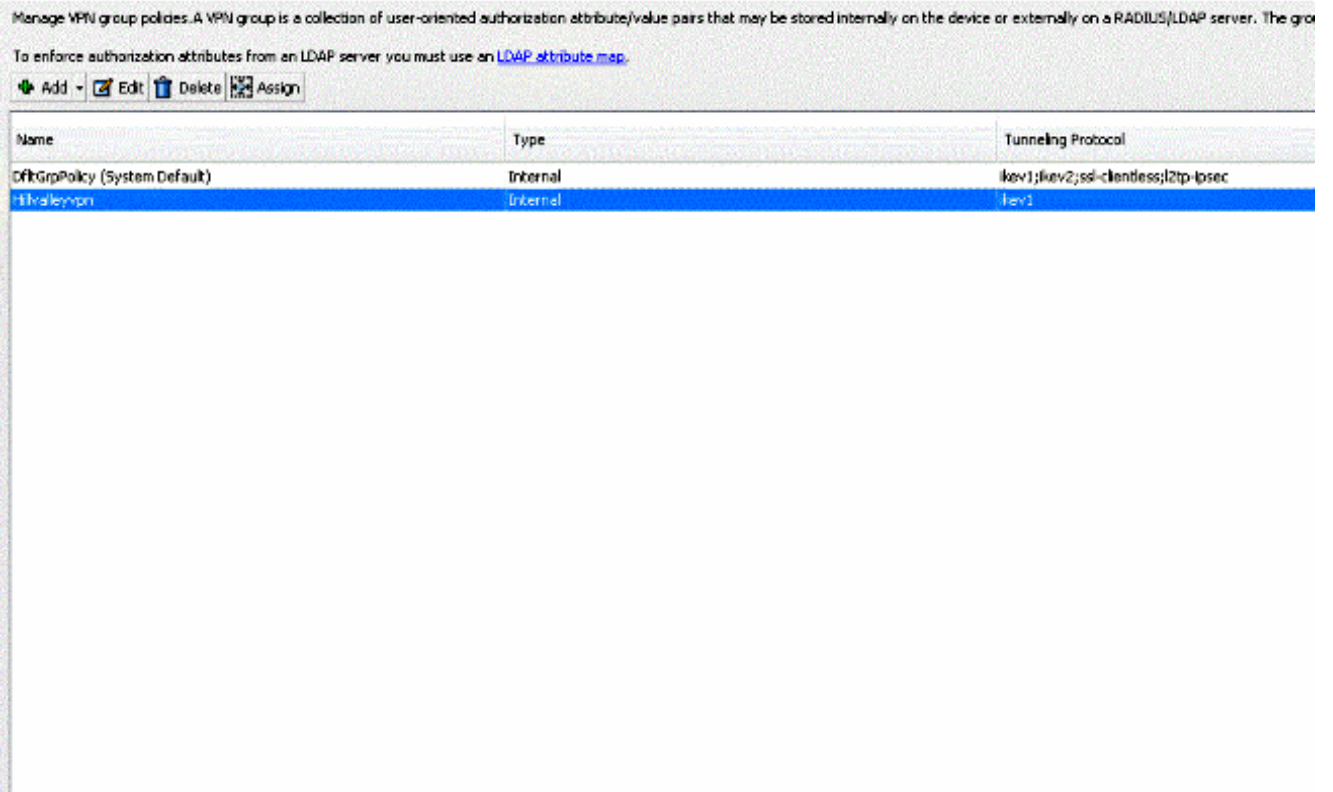
Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

Next Previous

OK Cancel Help

- ASA Apply 에 **Send** 명령을 보내려면 을 클릭한 다음 (필요한 경우) 를 클릭합니다.



CLI를 통해 ASA 구성

ASDM을 사용하지 않고 ASA에 연결하는 동안 VPN 클라이언트에서 로컬 LAN 액세스를 허용하도록 ASA CLI에서 다음 단계를 완료할 수 있습니다.

- 컨피그레이션 모드로 들어갑니다.

```
<#root>
```

```
ciscoasa>
```

`enable`

Password:
`ciscoasa#`

`configure terminal`

`ciscoasa(config)#`

- 로컬 LAN 액세스를 허용하기 위해 액세스 목록을 생성합니다.

<#root>

`ciscoasa(config)#`

`access-list Local_LAN_Access remark Client Local LAN Access`

`ciscoasa(config)#`

`access-list Local_LAN_Access standard permit host 0.0.0.0`

- 수정하려는 정책에 대한 그룹 정책 컨피그레이션 모드로 들어갑니다.

<#root>

`ciscoasa(config)#`


```
group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

- 스플릿 터널 정책을 지정합니다. 이 경우 정책은 다음과 excludespecified같습니다.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-policy excludespecified
```

- 스플릿 터널 액세스 목록을 지정합니다. 이 경우 목록은 Local_LAN_Access입니다.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-network-list value Local_LAN_Access
```

- 다음 명령을 실행합니다.

```
<#root>
```

```
ciscoasa(config)#
```

```
tunnel-group hillvalleyvpn general-attributes
```

- 그룹 정책을 터널 그룹과 연결합니다.

```
<#root>
```

```
ciscoasa(config-tunnel-ipsec)#
```

```
default-group-policy hillvalleyvpn
```

- 두 가지 컨피그레이션 모드를 종료합니다.

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
exit
```

```
ciscoasa(config)#
```

```
exit
```

```
ciscoasa#
```

- **컨피그레이션**을 비휘발성 RAM(NVRAM)에 저장하고 소스 파일 이름을 지정하라는 메시지가 **Enter** 나타나면 키를 누릅니다.

```
<#root>
```

```
ciscoasa#
```

```
copy running-config startup-config
```

```
Source filename [running-config]?  
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a  
  
3847 bytes copied in 3.470 secs (1282 bytes/sec)  
ciscoasa#
```

Cisco AnyConnect Secure Mobility Client 구성

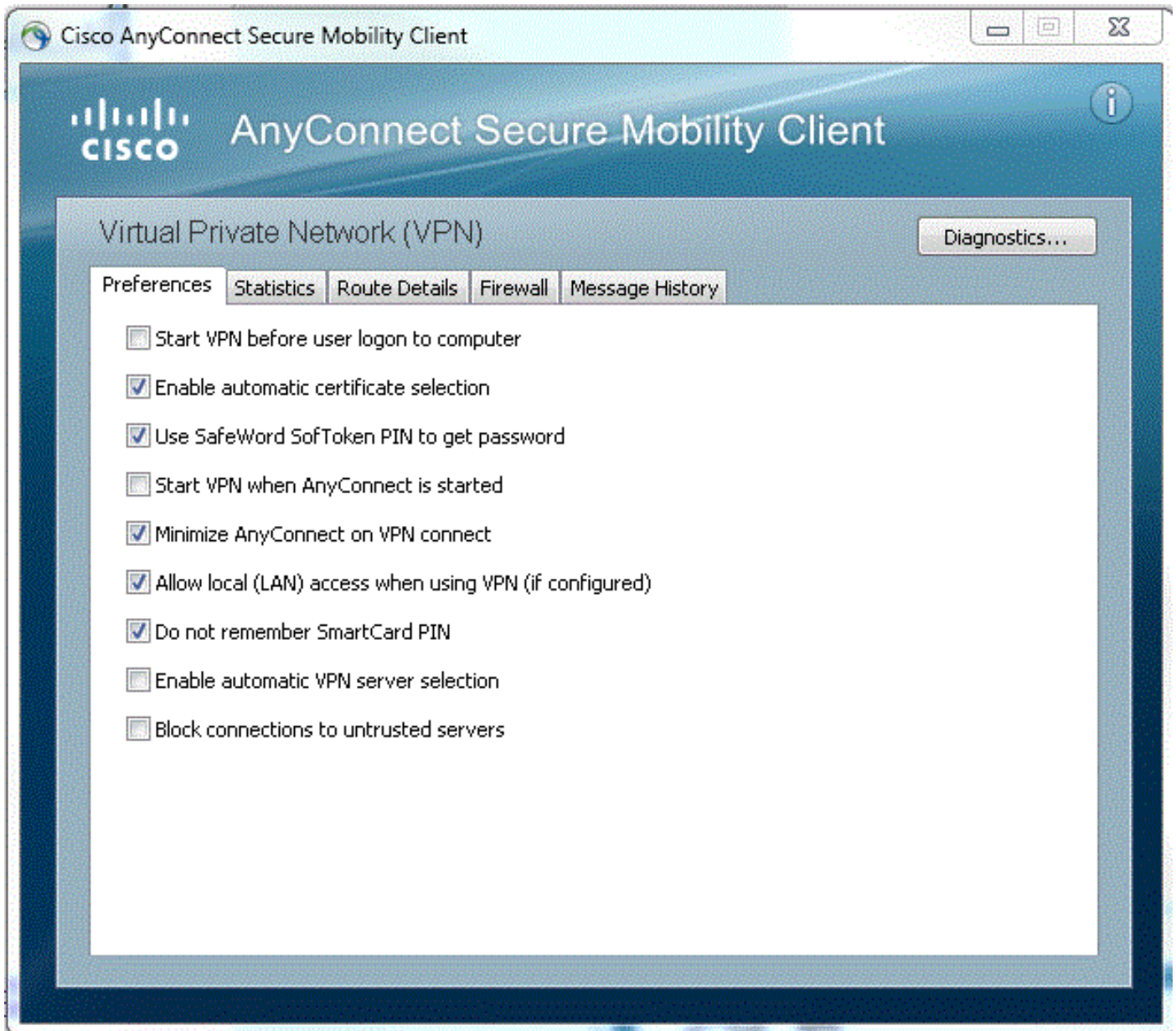
Cisco AnyConnect Secure Mobility Client를 구성하려면 *CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17*의 Configure AnyConnect [Connections](#) 섹션을 참조하십시오.

스플릿 제외 터널링을 사용하려면 AnyConnect 클라이언트 **AllowLocalLanAccess** 에서 활성화해야 합니다. 모든 스플릿 제외 터널링은 로컬 LAN 액세스로 간주됩니다. 스플릿 터널링의 제외 기능을 사용하려면 AnyConnect VPN 클라이언트 기본 **AllowLocalLanAccess** 설정에서 기본 설정을 활성화해야 합니다. 기본적으로 로컬 LAN 액세스는 비활성화되어 있습니다.

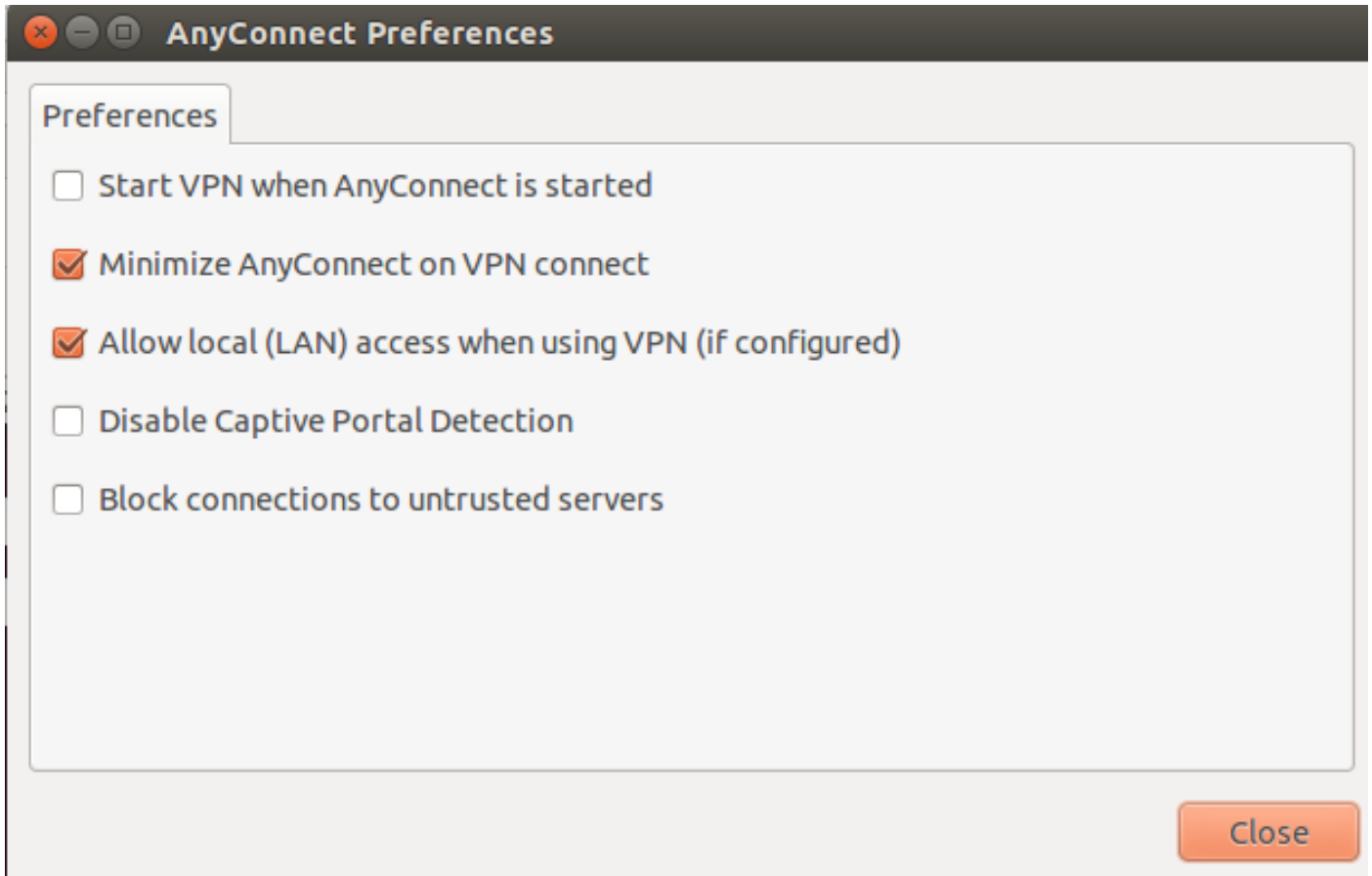
로컬 LAN 액세스, 즉 스플릿 제외 터널링을 허용하려면 네트워크 관리자가 프로파일에서 활성화하거나 사용자가 기본 설정 설정에서 활성화할 수 있습니다(다음 섹션의 이미지 참조). 사용자는 로컬 LAN 액세스를 허용하기 위해 보안 게이트웨이에서 스플릿 터널링이 활성화되어 있고 정책으로 구성된 **Allow Local LAN access** 경우 확인란을 split-tunnel-policy exclude specified 선택합니다. 또한 로컬 LAN 액세스가 허용되는 경우 VPN 클라이언트 프로파일을 구성할 수 있습니다 <**LocalLanAccess** **UserControllable="true">true</LocalLanAccess>**.

사용자 기본 설정

로컬 LAN 액세스를 허용하려면 Cisco AnyConnect Secure Mobility Client의 Preferences(환경 설정) 탭에서 선택해야 하는 항목을 선택하십시오.



Linux에서



XML 프로파일 예

다음은 XML을 사용하여 VPN 클라이언트 프로파일을 구성하는 방법의 예입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">Automatic
```

```

</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>

```

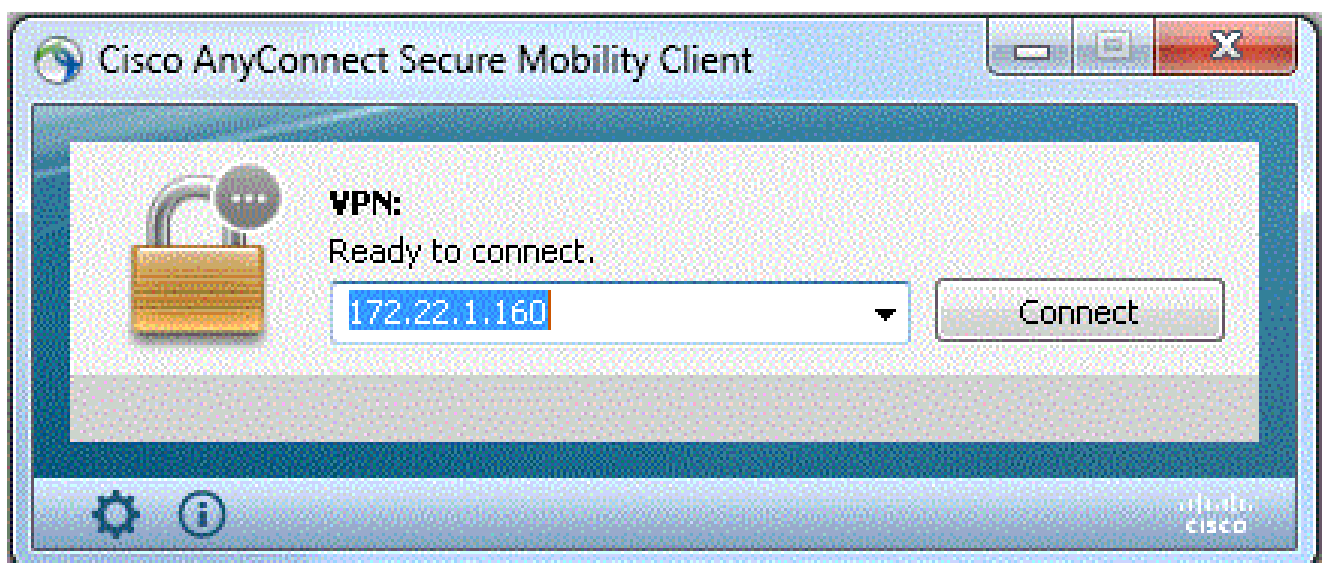
다음을 확인합니다.

컨피그레이션을 확인하려면 다음 절의 단계를 완료하십시오.

- [DART 보기](#)
- [Ping으로 로컬 LAN 액세스 테스트](#)

컨피그레이션을 확인하기 위해 Cisco AnyConnect Secure Mobility Client를 ASA에 연결합니다.

- 서버 목록에서 연결 항목을 선택하고 **Connect**클릭합니다.



- 터널 모드 Advanced Window for All Components > Statistics... 를 표시하려면 선택합니다.

Virtual Private Network (VPN)

Statistics | Route Details | Firewall | Message History


Connection Information		Address Information	
State:	Connected	Client (IPv4):	192.168.11.1
Tunnel Mode (IPv4):	Split Exclude	Client (IPv6):	Not Available
Tunnel Mode (IPv6):	Drop All Traffic	Server:	64.102.156.87
Duration:	00:01:11	Transport Information	
Bytes		Protocol:	DTLS
Sent:	49749	Cipher:	RSA_3DES_168_SHA1
Received:	9298	Compression:	LZS
Frames		Proxy Address:	No Proxy
Sent:	710	Feature Configuration	
Received:	3	FIPS Mode:	Disabled
Control Frames		Trusted Network Detection:	Disabled
Sent:	7	Always On:	Disabled
Received:	5	Secure Mobility Solution	
Client Management		Status:	Unconfirmed
Profile Name:	pro_locallan.xml	Appliance:	Not Available
Administrative Domain:	Undefined		

Reset Export Stats...

Linux에서

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | Route Details



Connection Information		Address Information	
State:	Connected	Client (IPv4):	20.20.20.1
Connection Mode (IPv4):	Split Exclude	Server:	10.48.67.223
Connection Mode (IPv6):	Drop All Traffic	Client (IPv6):	Not Available
Duration:	00:16:22		
Session Disconnect:	None		
Bytes		Transport Information	
Sent:	0	Protocol:	DTLS
Received:	20550	Cipher:	RSA_AES_256_SHA1
		Compression:	None
		Proxy Address:	No Proxy
Frames		Feature Configuration	
Sent:	0	FIPS Mode:	Disabled
Received:	5	Trusted Network Detection:	Disabled
Control Frames			
Sent:	132		
Received:	65		

- Cisco **Route Details** AnyConnect Secure Mobility Client가 여전히 로컬 액세스 권한을 가지고 있는 경로를 확인하려면 탭을 클릭합니다.


이 예에서 클라이언트는 10.150.52.0/22 및 169.254.0.0/16에 대한 로컬 LAN 액세스를 허용하지만 다른 모든 트래픽은 암호화되어 터널을 통해 전송됩니다.



Linux에서

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | **Route Details**



Non-Secured Routes	
Destination	Subnet Mask
192.168.171.0	24

Secured Routes	
Destination	Subnet Mask
0.0.0.0	0

Cisco AnyConnect Secure Mobility Client

DART(Diagnostics and Reporting Tool) 번들에서 AnyConnect 로그를 검토할 때 로컬 LAN 액세스를 허용하는 매개변수가 설정되었는지 여부를 결정할 수 있습니다.

Date : 11/25/2011
 Time : 13:01:48
 Type : Information
 Source : acvpndownloader

Description : Current Preference Settings:
 ServiceDisable: false
 CertificateStoreOverride: false
 CertificateStore: All
 ShowPreConnectMessage: false
 AutoConnectOnStart: false
 MinimizeOnConnect: true
 LocalLanAccess: true
 AutoReconnect: true
 AutoReconnectBehavior: DisconnectOnSuspend
 UseStartBeforeLogon: false
 AutoUpdate: true
 RSA SecurID Integration: Automatic
 Windows Logon Enforcement: SingleLocalLogon
 Windows VPN Establishment: LocalUsersOnly
 Proxy Settings: Native
 AllowLocalProxyConnections: true

PPPEExclusion: Disable
PPPEExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSoftTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true

Ping으로 로컬 LAN 액세스 테스트

VPN 헤드엔드로 터널링되는 동안 VPN 클라이언트에 로컬 LAN 액세스가 있는지 테스트하는 또 다른 방법은 Microsoft Windows 명령줄에서 **ping** 명령을 사용하는 것입니다. 다음은 클라이언트의 로컬 LAN이 192.168.0.0/24이고 IP 주소가 192.168.0.3인 다른 호스트가 네트워크에 있는 예입니다.

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

```
malhyari@ubuntu:~$ ping 192.168.171.131
PING 192.168.171.131 (192.168.171.131) 56(84) bytes of data.
64 bytes from 192.168.171.131: icmp_seq=1 ttl=128 time=0.474 ms
64 bytes from 192.168.171.131: icmp_seq=2 ttl=128 time=0.315 ms
64 bytes from 192.168.171.131: icmp_seq=3 ttl=128 time=0.336 ms
64 bytes from 192.168.171.131: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.171.131: icmp_seq=5 ttl=128 time=0.337 ms
64 bytes from 192.168.171.131: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.171.131: icmp_seq=7 ttl=128 time=0.252 ms
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

이름으로 인쇄 또는 검색할 수 없음

VPN 클라이언트가 연결되어 있고 로컬 LAN 액세스를 위해 구성된 경우 로컬 LAN에서 이름으로 인쇄하거나 검색할 수 없습니다. 이 상황을 해결하기 위해 두 가지 옵션을 사용할 수 있습니다.

- IP 주소로 검색하거나 인쇄합니다.
 - 구문 대신 `\\x.x.x.x` 구문을 `\\sharename` 사용하여 찾아봅니다. 여기서 `x.x.x.x`는 호스트 컴퓨터의 IP 주소입니다.
 - 인쇄하려면 이름 대신 IP 주소를 사용하려면 네트워크 프린터의 속성을 변경하십시오. 예를 들어 구문 대신 `\\sharename\printername`를 사용합니다. `\\x.x.x.x\printername` 여기서 `x.x.x`는 IP 주소입니다.
- VPN 클라이언트 LMHOSTS 파일을 만들거나 수정합니다. Microsoft Windows PC의 LMHOSTS 파일을 사용하면 호스트 이름과 IP 주소 간에 정적 매핑을 만들 수 있습니다. 예를 들어 LMHOSTS 파일은 다음과 같이 표시될 수 있습니다.

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```

Microsoft Windows XP Professional Edition에서 LMHOSTS 파일은에 있습니다 `%SystemRoot%\System32\Drivers\Etc`. 자세한 내용은 Microsoft 설명서를 참조하십시오.

관련 정보

- [CLI Book 3: Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.17](#)
- [Cisco ASA 5500-X Series 방화벽](#)
- [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.