

ASA 7.2(2):스틱 컨피그레이션의 공용 인터넷 VPN용 SSL VPN 클라이언트(SVC) 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[ASDM 5.2\(2\)를 사용하는 ASA 7.2\(2\) 구성](#)

[ASA 7.2\(2\) CLI 컨피그레이션](#)

[SVC와 SSL VPN 연결 설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 ASA(Adaptive Security Appliance) 7.2.2을 설정하여 스틱에서 SSL VPN을 수행하는 방법에 대해 설명합니다. 이 설정은 ASA에서 스플릿 터널링을 허용하지 않고 사용자가 인터넷으로 이동하기 전에 ASA에 직접 연결하는 특정 경우에 적용됩니다.

참고: ASA 버전 7.2.2에서 `same-security-traffic permit configuration mode` 명령의 `intra-interface` 키워드는 모든 트래픽이 동일한 인터페이스(IPsec 트래픽뿐 아니라)에 들어오고 나갈 수 있도록 합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 허브 ASA Security Appliance는 버전 7.2.2을 실행해야 합니다.
- Cisco SSL VPN Client(SVC) 1.x**참고:** [Cisco 소프트웨어 다운로드\(등록된 고객만 해당\)](#)에서 SSL VPN 클라이언트 패키지(sslclient-win*.pkg)를 다운로드합니다. ASA의 플래시 메모리에 SVC를 복사합니다.ASA와의 SSL VPN 연결을 설정하기 위해 SVC를 원격 사용자 컴퓨터로 다운로드합니다.자세한 내용은 [Cisco Security Appliance 명령줄 구성 설명서 버전 7.2의 SVC 소프트웨어 설치](#) 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 7.2(2)를 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- Windows 1.1.4.179용 Cisco SSL VPN Client 버전
- Windows 2000 Professional 또는 Windows XP를 실행하는 PC
- Cisco ASDM(Adaptive Security Device Manager) 버전 5.2(2)

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

배경 정보

SVC(SSL VPN Client)는 원격 사용자에게 IPsec VPN 클라이언트를 설치 및 구성할 필요 없이 IPsec VPN 클라이언트의 이점을 제공하는 VPN 터널링 기술입니다. SVC는 원격 컴퓨터에 이미 있는 SSL 암호화와 보안 어플라이언스의 WebVPN 로그인 및 인증을 사용합니다.

SVC 세션을 설정하기 위해 원격 사용자는 브라우저에 보안 어플라이언스의 WebVPN 인터페이스의 IP 주소를 입력하고 브라우저가 해당 인터페이스에 연결하여 WebVPN 로그인 화면을 표시합니다. 사용자가 로그인 및 인증을 충족하고 보안 어플라이언스가 사용자를 SVC가 필요하다고 식별하면 보안 어플라이언스는 SVC를 원격 컴퓨터에 다운로드합니다. 보안 어플라이언스가 사용자에게 SVC를 사용할 수 있는 옵션이 있다고 확인하면 보안 어플라이언스는 사용자 화면에 링크를 제시하면서 원격 컴퓨터에 SVC를 다운로드하여 SVC 설치를 건너뛸니다.

다운로드 후 SVC는 자동으로 설치 및 구성되며, 연결이 종료되면 SVC는 구성에 따라 원격 컴퓨터에서 자체적으로 유지되거나 제거됩니다.

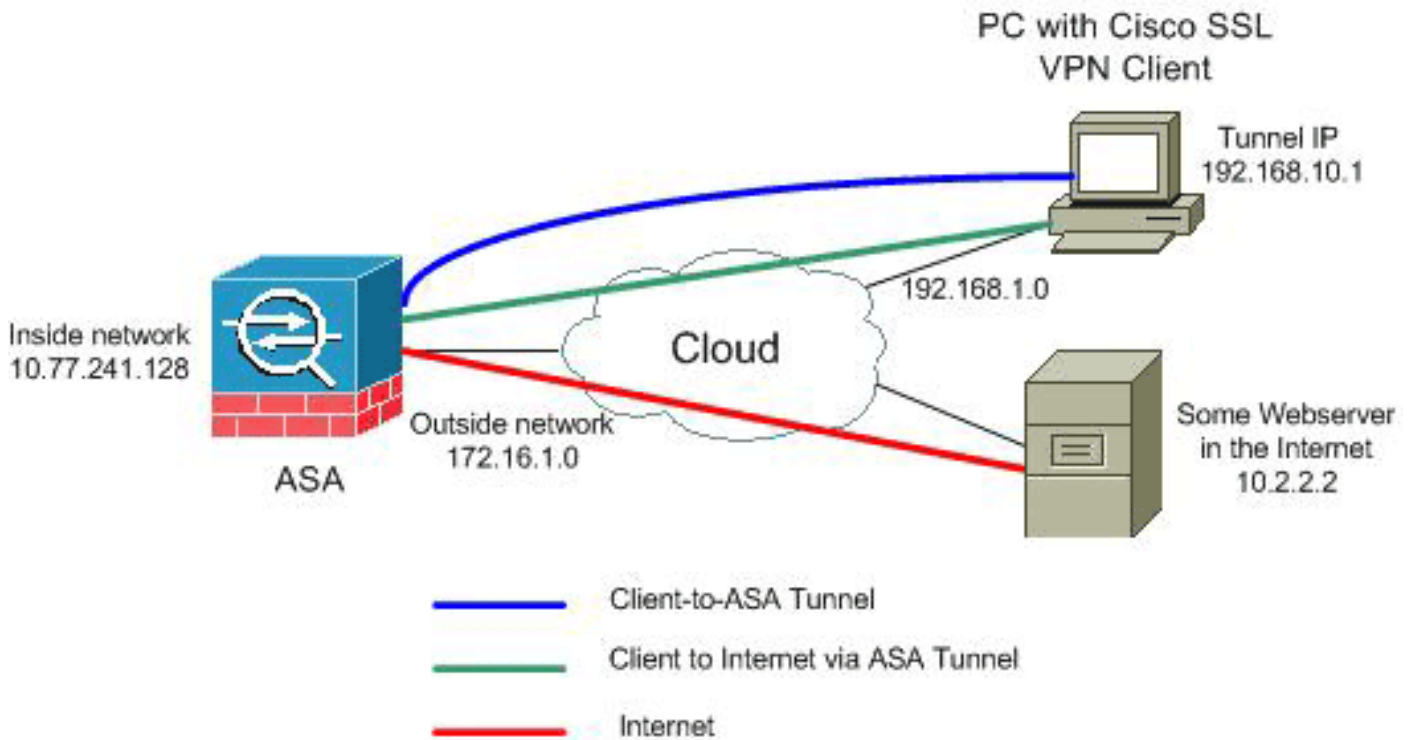
구성

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. 이는 [실습](#) 환경에서 사용된 RFC [1918](#) 주소입니다.

[ASDM 5.2\(2\)를 사용하는 ASA 7.2\(2\) 구성](#)

이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 이미 만들어졌으며 제대로 작동한다고 가정합니다.

참고: ASDM에서 ASA를 [구성할 수 있도록](#) 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

참고: 포트 번호를 변경하지 않으면 동일한 ASA 인터페이스에서 WebVPN 및 ASDM을 활성화할 수 없습니다. 자세한 내용은 [ASA의 동일한 인터페이스에서 ASDM 및 WebVPN 활성화](#)를 참조하십시오.

ASA의 스틱에서 SSL VPN을 구성하려면 다음 단계를 완료합니다.


1. Configuration > Interfaces를 선택하고 **Enable traffic between two or more hosts connected to the same interface** 확인란을 선택하여 SSL VPN 트래픽이 동일한 인터페이스에 들어오고 나가도록 허용합니다.
2. Apply를 클릭합니다

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask
Ethernet0/0	inside	Yes	100	10.77.241.142	255.255.255.192
Ethernet0/1	outside	Yes	0	172.16.1.1	255.255.255.0
Ethernet0/2		No			
Ethernet0/3		No			
Management0/0		No			

Please wait...

Please wait while ASDM is delivering the command(s) to the device...



Parsing running configuration...

Enable traffic between two or more interfaces which are configured with same security levels
 Enable traffic between two or more hosts connected to the same interface

참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

3. vpnpool이라는 IP 주소 풀을 생성하려면 Configuration > VPN > IP Address Management > IP

Add IP Pool

Name:

Starting IP Address:

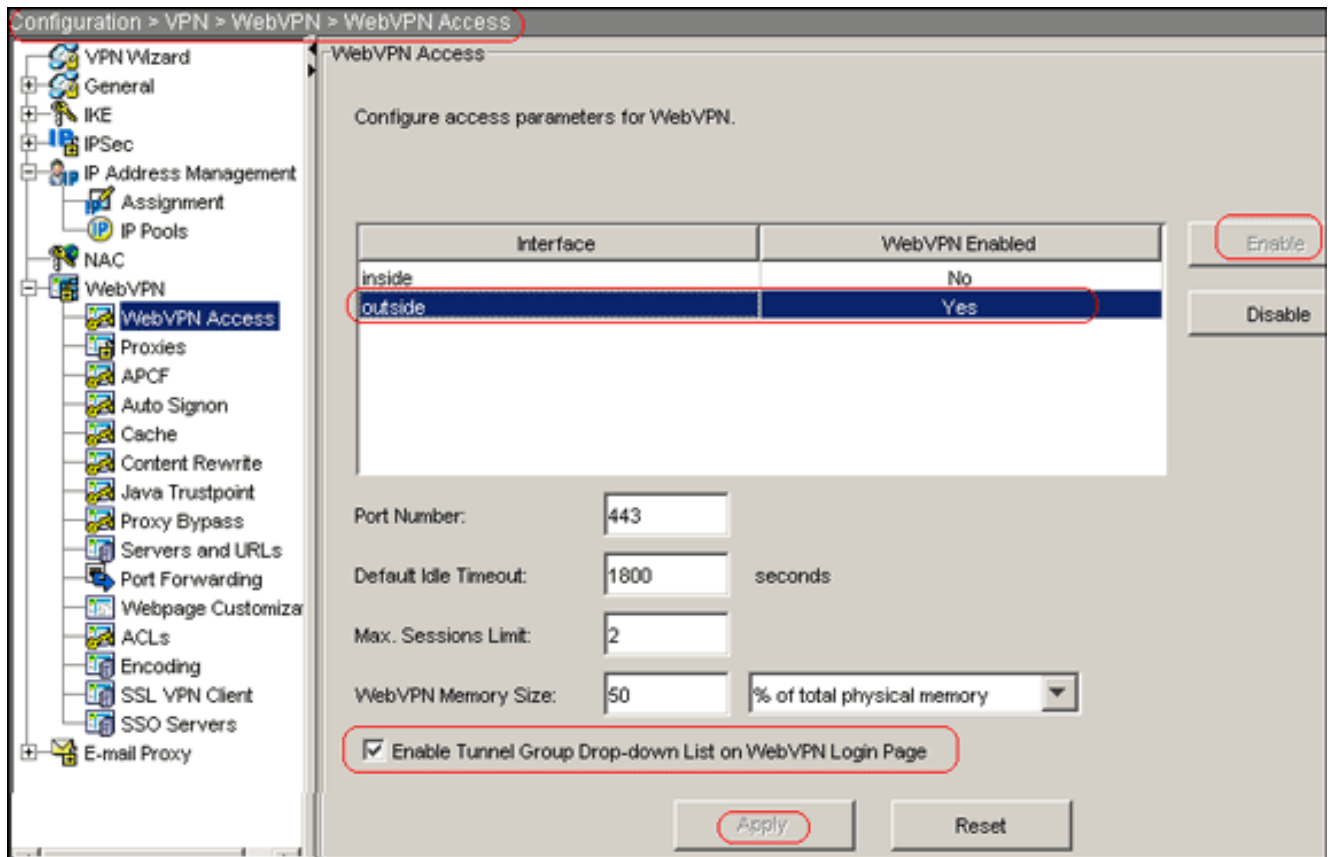
Ending IP Address:

Subnet Mask:

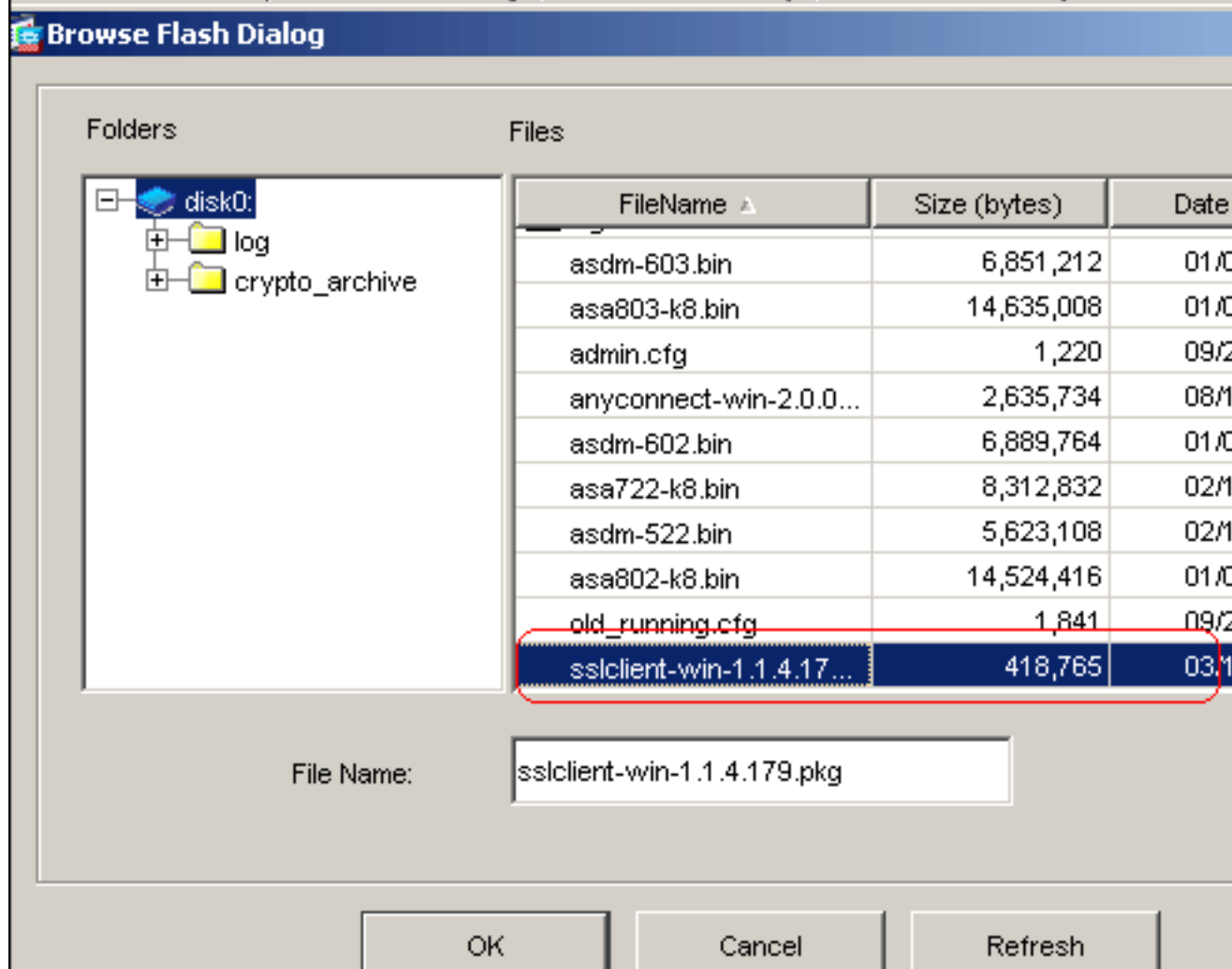
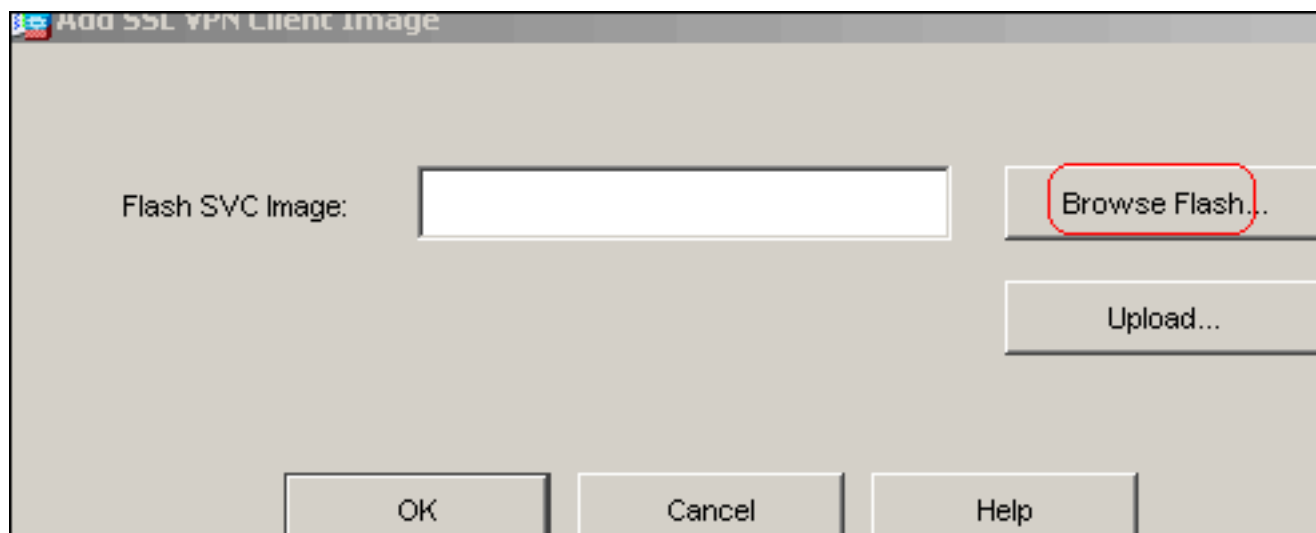
Pools > Add를 선택합니다.

4. Apply를 클릭합니다.참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

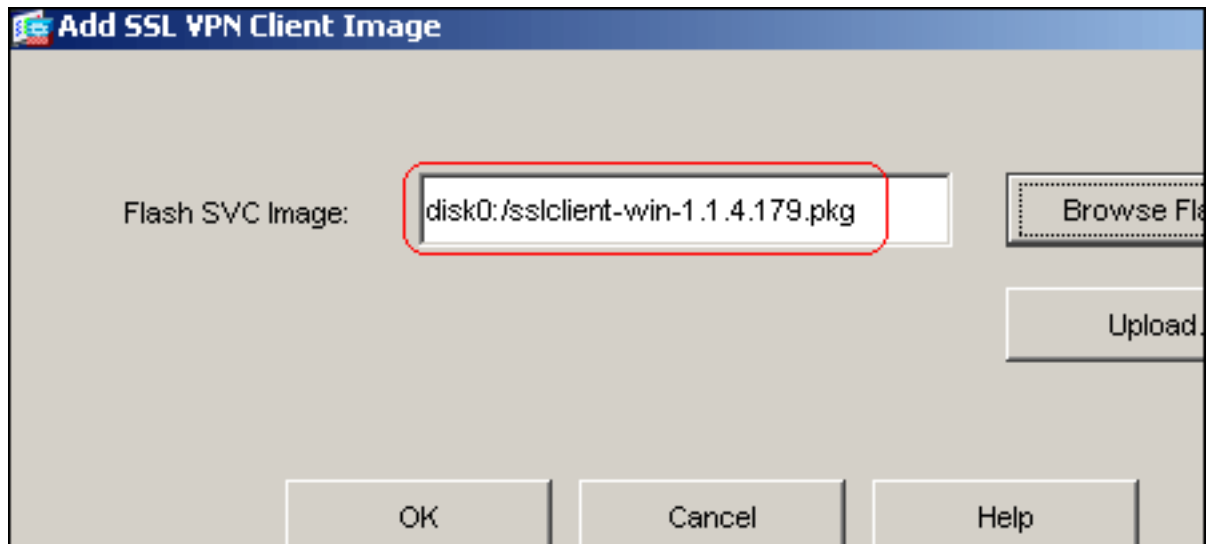
5. WebVPN 사용:Configuration(구성) > VPN > WebVPN > WebVPN Access(WebVPN 액세스)를 선택하고 외부 인터페이스를 선택합니다.Enable을 클릭합니다.사용자가 Login 페이지에서 각 그룹을 선택할 수 있도록 하려면 **Enable Tunnel Group Drop-down List on WebVPN Login Page** 확인란을 선택합니다



Apply를 클릭합니다.ASA의 플래시 메모리에서 SSL VPN 클라이언트 이미지를 추가하려면 Configuration(컨피그레이션) > VPN > WebVPN > SSL VPN Client(SSL VPN 클라이언트) > Add(추가)를 선택합니다

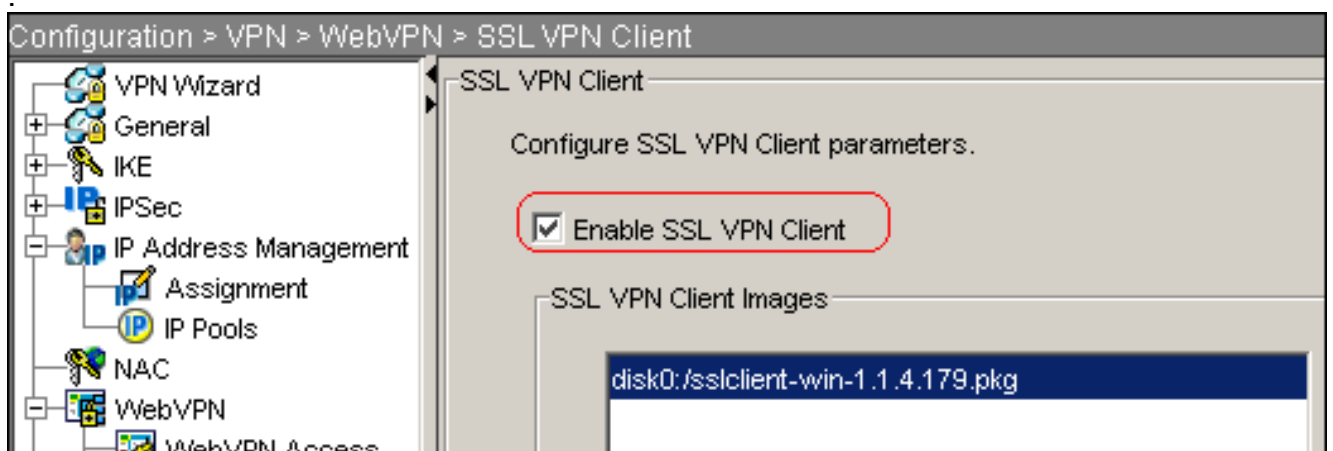


확인을 클릭합니다



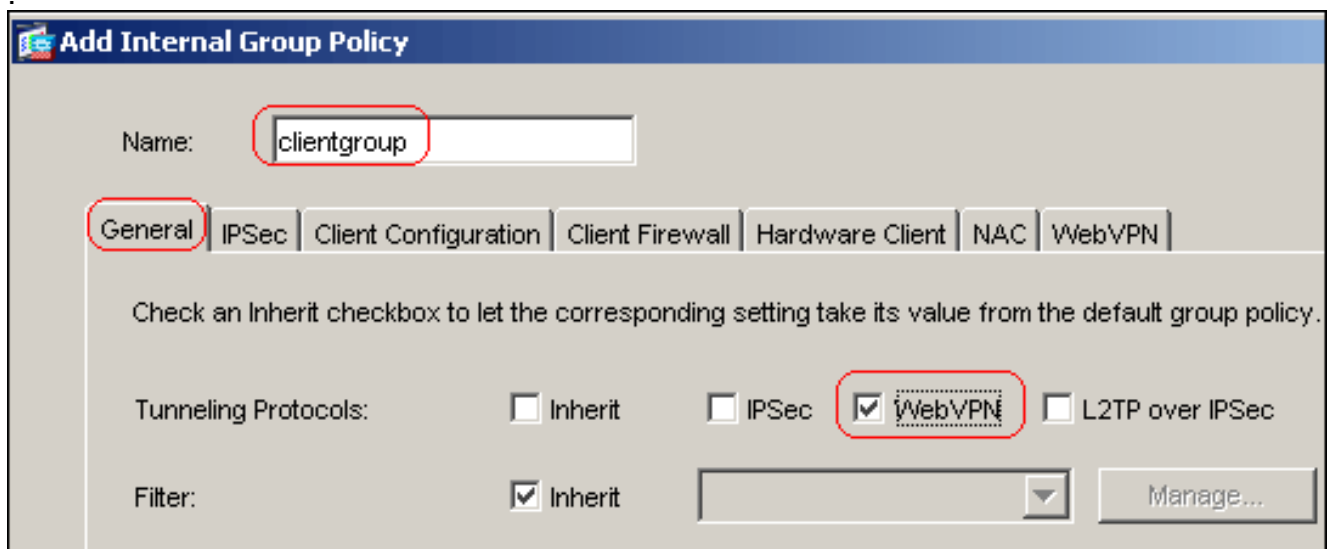
확인

클릭합니다.SSL VPN Client 확인란을 클릭합니다



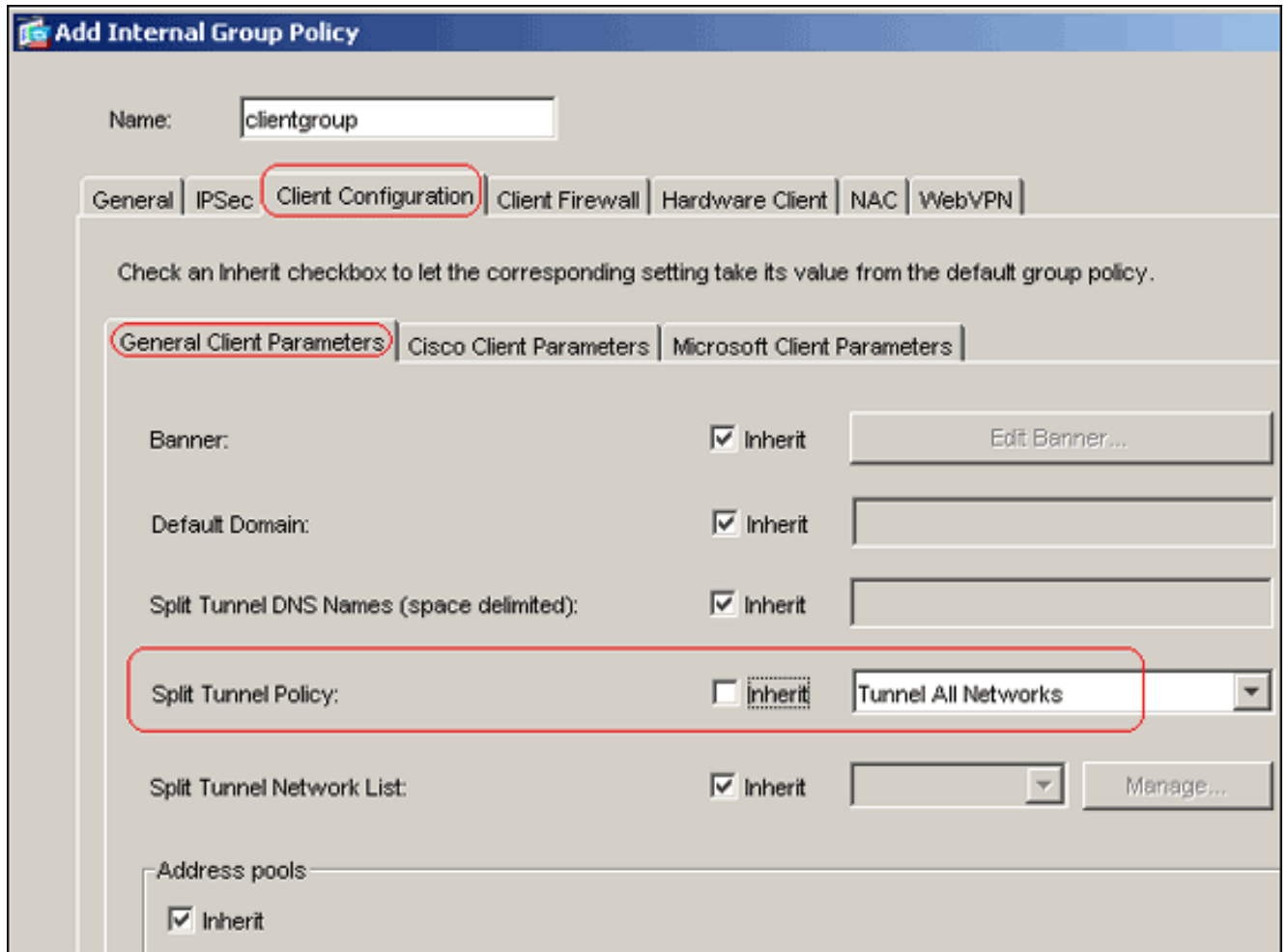
참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

6. 그룹 정책을 구성합니다.Configuration(컨피그레이션) > VPN > General(일반) > Group Policy(그룹 정책) > Add (Internal Group Policy)를 선택하여 이름이 clientgroup인 내부 그룹 정책을 생성합니다.WebVPN을 터널링 프로토콜으로 활성화하려면 General(일반) 탭을 클릭하고 WebVPN 확인란을 선택합니다

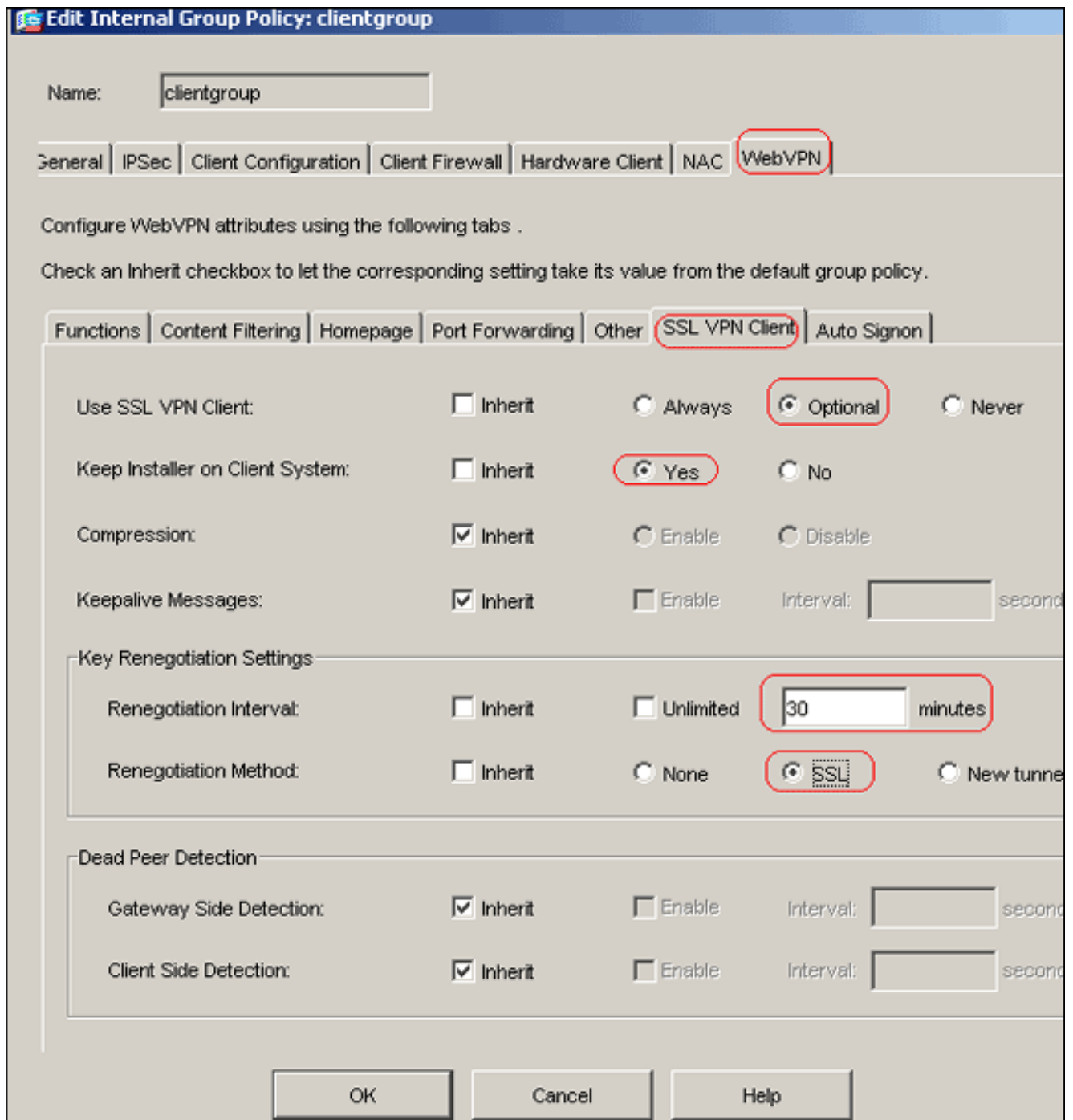


Client Configuration(클라이언트 컨피그레이션) 탭을 클릭한 다음 General Client Parameters(일반 클라이언트 매개변수) 탭을 클릭합니다.Split Tunnel Policy(터널 정책 분할) 드롭다운 목록에서 Tunnel All Networks(모든 네트워크 터널링)를 선택하여 모든 패킷이 보안

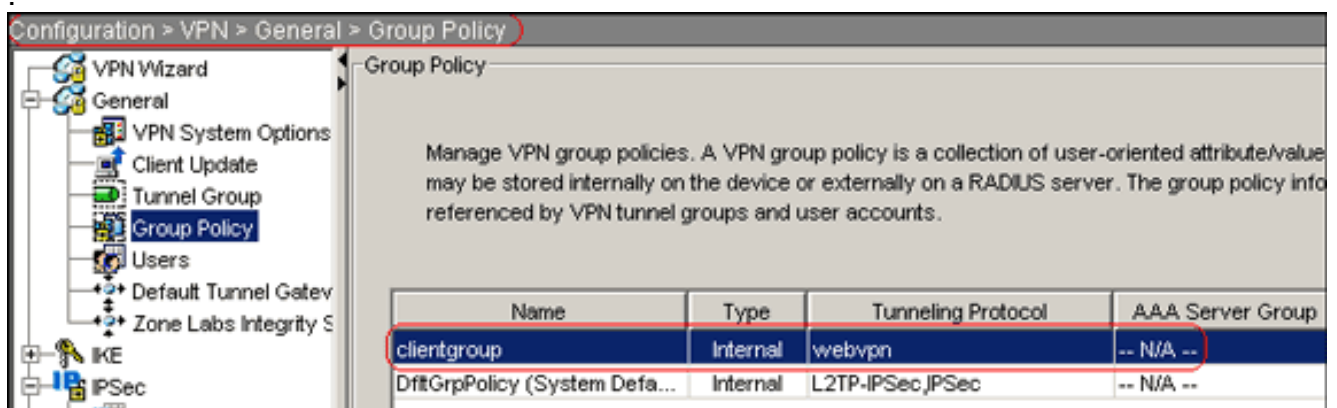
터널을 통해 원격 PC에서 이동하도록 합니다



WebVPN > **SSLVPN Client** 탭을 클릭하고 다음 옵션을 선택합니다. Use SSL VPN Client(SSL VPN 클라이언트 사용) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 Optional(선택) 라디오 버튼을 클릭합니다. 이 옵션을 사용하면 원격 클라이언트가 SVC를 다운로드할지 여부를 선택할 수 있습니다. Always(항상 선택) 옵션을 선택하면 각 SSL VPN 연결 중에 SVC가 원격 워크스테이션에 다운로드됩니다. Keep Installer on Client System(클라이언트 시스템에서 설치 프로그램 유지) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 Yes(예) 라디오 버튼을 클릭합니다. 이 옵션을 사용하면 SVC 소프트웨어가 클라이언트 시스템에 남아 있을 수 있습니다. 따라서 연결이 이루어질 때마다 SVC 소프트웨어를 클라이언트에 다운로드할 필요가 없습니다. 이 옵션은 기업 네트워크에 자주 액세스하는 원격 사용자에게 적합합니다. Renegotiation Interval(재협상 간격) 옵션에서 Inherit(상속) 상자의 선택을 취소하고 Unlimited(무제한) 확인란의 선택을 취소하고 다시 키를 누를 때까지 분 수를 입력합니다. 참고: 키가 유효한 시간에 대한 제한을 설정하여 보안이 강화됩니다. Renegotiation Method(재협상 방법) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 SSL 라디오 버튼을 클릭합니다. 참고: 재협상은 재협상으로 특별히 생성된 현재 SSL 터널 또는 새 터널을 사용할 수 있습니다. 다음 이미지에 표시된 대로 SSL VPN 클라이언트 특성을 구성해야 합니다



OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다



참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

7. 새 사용자 계정 `ssluser1`을 생성하려면 Configuration > VPN > General > Users > Add를 선택합니다.

8. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다

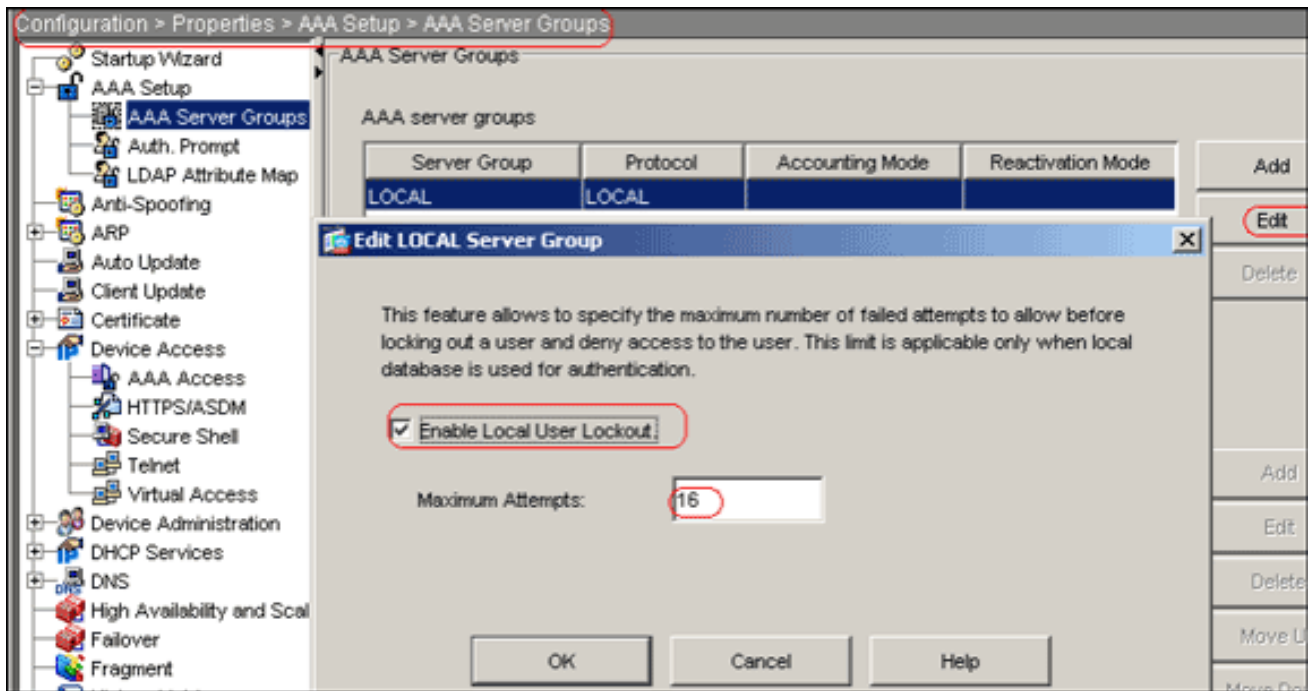
The screenshot shows the 'Add User Account' dialog box with the following fields and values:

- Identity** (selected tab)
- Username:** ssluser1
- Password:** *****
- Confirm Password:** *****
- User authenticated using MSCHAP
- Privilege level is used with command authorization.
- Privilege Level:** 2

Buttons: OK, Cancel, Help

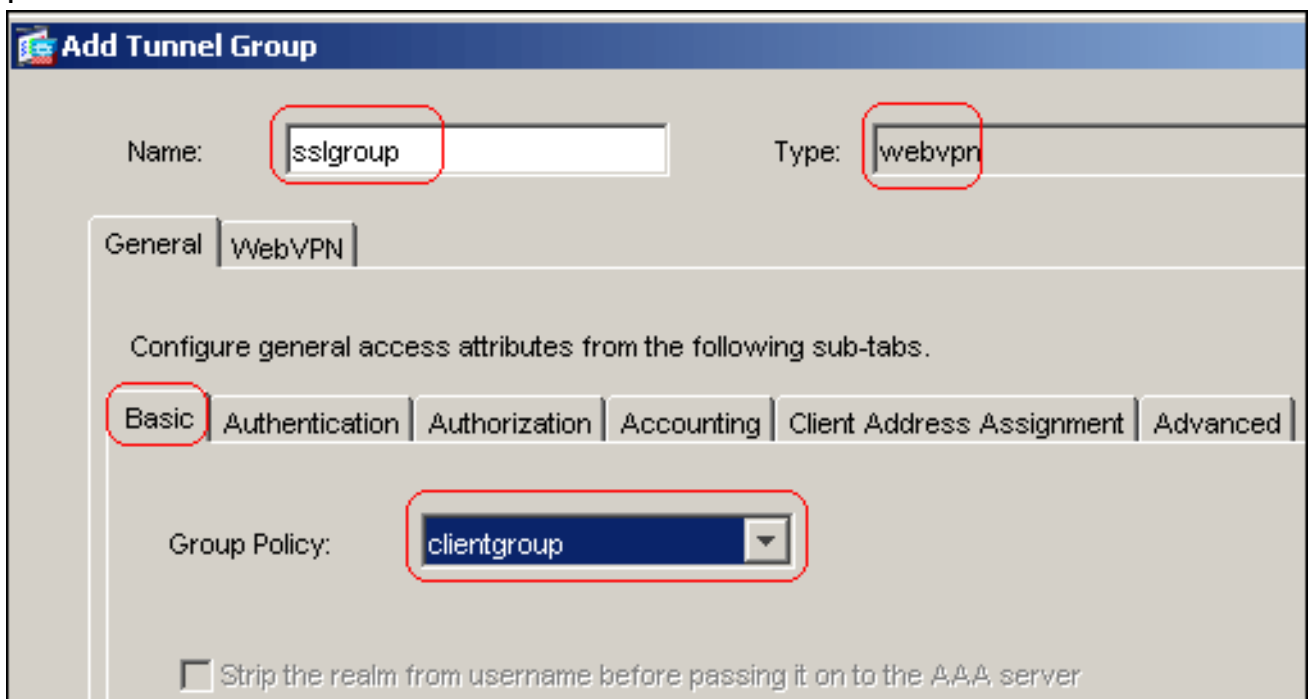
참고: 등가 CLI 명령은 다음과 같습니다.

9. Configuration > Properties > AAA Setup > AAA Servers Groups > Edit를 선택합니다.
10. 기본 서버 그룹 LOCAL을 선택하고 Edit를 클릭합니다.
11. Edit LOCAL Server Group(LOCAL 서버 그룹 편집) 대화 상자에서 **Enable Local User Lockout(로컬 사용자 잠금 활성화)** 확인란을 클릭하고 Maximum Attempts(최대 시도) 텍스트 상자에 16을 입력합니다.
12. 확인을 클릭합니다



참고: 등가 CLI 명령은 다음과 같습니다.

- 터널 그룹을 구성합니다. `sslgroup`이라는 새 터널 그룹을 생성하려면 Configuration > VPN > General > Tunnel Group > Add(WebVPN 액세스)를 선택합니다. 일반 탭을 클릭한 다음 기본 탭을 클릭합니다. Group Policy 드롭다운 목록에서 `clientgroup`을 선택합니다



Client Address Assignment(클라이언트 주소 할당) 탭을 클릭한 다음 Add(추가)를 클릭하여 사용 가능한 주소 풀 vpnpool을 할당합니다

Add Tunnel Group

Name: Type:

General | WebVPN

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | **Client Address Assignment** | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

Available Pools

Assigned pools

vpnpool

WebVPN 탭을 클릭한 다음 **Group Aliases and URLs** 탭을 클릭합니다. 매개변수 상자에 별칭 이름을 입력하고 **추가**를 클릭하여 로그인 페이지의 그룹 이름 목록에 추가합니다

General | **WebVPN**

Configure WebVPN access attributes from the following sub-tabs.

Basic | NetBIOS Servers | **Group Aliases and URLs** | Web Page

Group Aliases

Alias:

Enable

Alias	Status
sslgroun_users	enable

OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

14. NAT 구성:Configuration(컨피그레이션) > NAT > Add(추가) > Add Dynamic NAT Rule(동적 NAT 규칙 추가)을 선택하여 내부 네트워크에서 오는 트래픽이 외부 IP 주소 172.16.1.5을 사

용하여 변환되도록 합니다

Real Address

Interface: inside

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Dynamic Translation

Interface: outside

+ Add Edit Delete

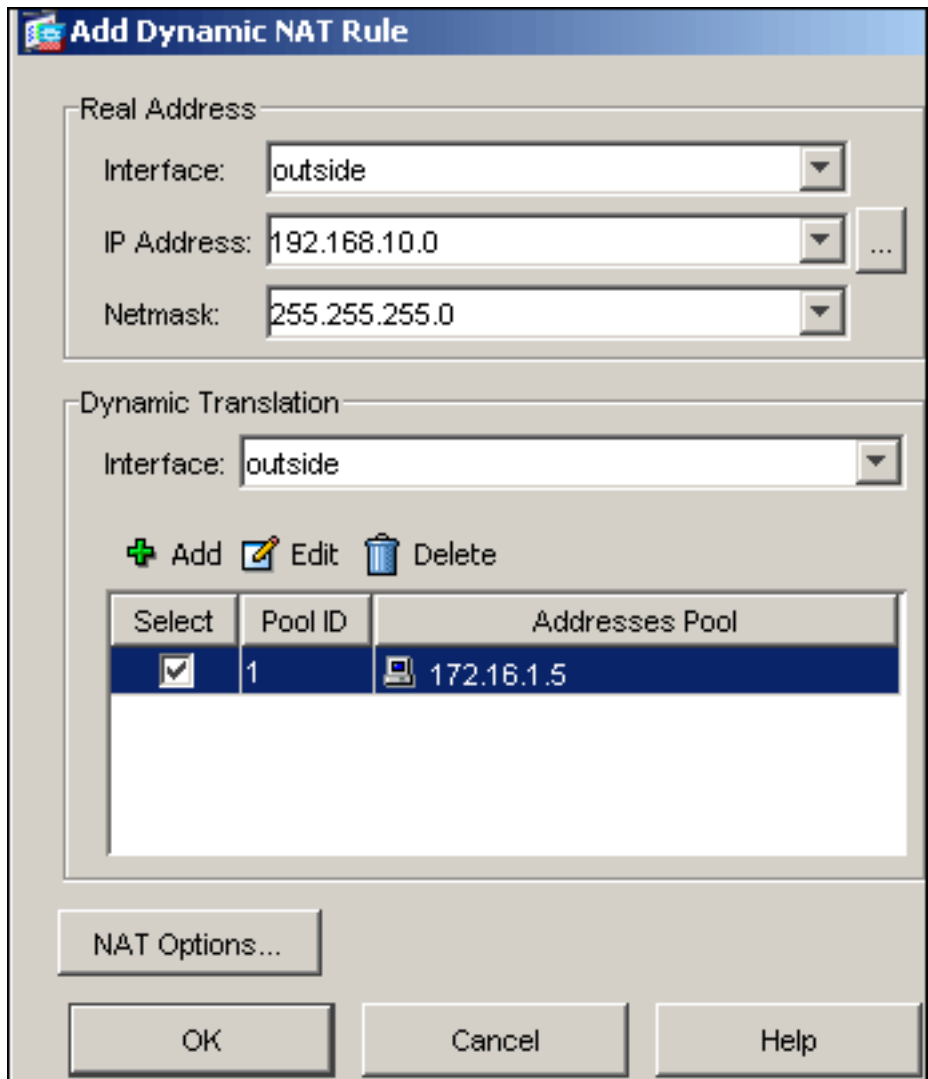
Select	Pool ID	Addresses Pool
<input checked="" type="checkbox"/>	1	172.16.1.5

NAT Options...

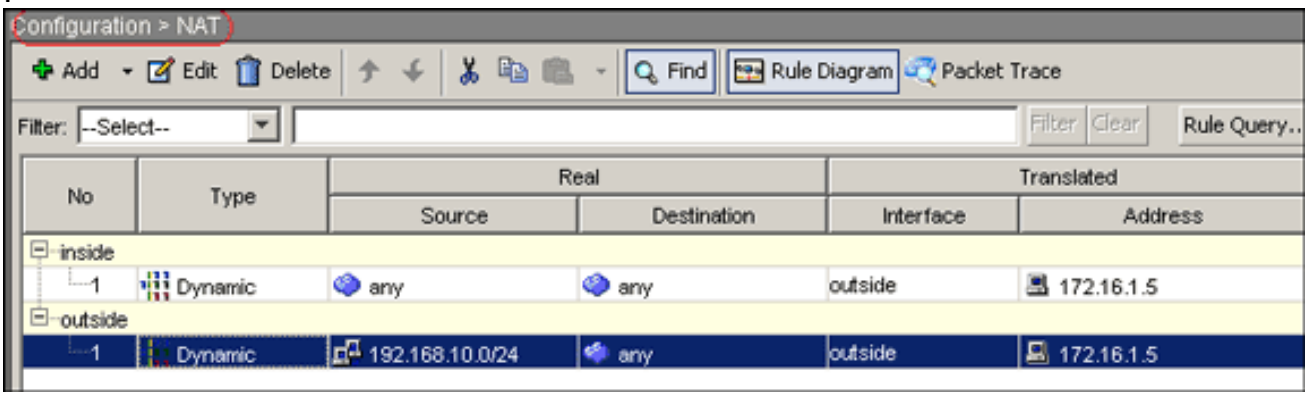
OK Cancel Help

확인을 클릭합니다

.Configuration > NAT > Add > Add Dynamic NAT Rule을 선택하여 외부 네트워크 192.168.10.0 들어오는 트래픽을 외부 IP 주소 172.16.1.5을 사용하여 변환할 수 있습니다



확인을 클릭합니다



Apply를 클릭합니다.참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

ASA 7.2(2) CLI 컨피그레이션

```

Cisco ASA 7.2(2)

ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
  
```

```
!  
interface Ethernet0/0  
  nameif inside  
  security-level 100  
  ip address 10.77.241.142 255.255.255.192  
!  
interface Ethernet0/1  
  nameif outside  
  security-level 0  
  ip address 172.16.1.1 255.255.255.0  
!  
interface Ethernet0/2  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Ethernet0/3  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Management0/0  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
ftp mode passive  
same-security-traffic permit intra-interface  
  
!--- Command that permits the SSL VPN traffic to enter  
!--- and exit the same interface. access-list 100  
extended permit icmp any any pager lines 24 mtu inside  
1500 mtu outside 1500 ip local pool vpnpool  
192.168.10.1-192.168.10.254  
  
!--- The address pool for the SSL VPN Clients. no  
failover icmp unreachable rate-limit 1 burst-size 1 asdm  
image disk0:/asdm-522.bin no asdm history enable arp  
timeout 14400 global (outside) 1 172.16.1.5  
  
!--- The global address for Internet access used by VPN  
Clients. !--- Note: Uses an RFC 1918 range for lab  
setup. !--- Apply an address from your public range  
provided by your ISP. nat (inside) 1 0.0.0.0 0.0.0.0  
  
!--- The NAT statement to define what to encrypt !---  
(the addresses from vpn-pool). nat (outside) 1  
192.168.10.0 255.255.255.0  
  
access-group 100 in interface outside  
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:  
timeout uauth 0:05:00 absolute  
group-policy clientgroup internal
```

```
!--- Create an internal group policy "clientgroup."  
group-policy clientgroup attributes  
  vpn-tunnel-protocol webvpn  
  
!--- Enable webvpn as tunneling protocol. split-tunnel-  
policy tunnelall  
  
!--- Encrypt all the traffic coming from the SSL VPN  
Clients. webvpn  
  svc required  
  
!--- Activate the SVC under webvpn mode svc keep-  
installer installed  
  
!--- When the security appliance and the SVC perform a  
rekey, they renegotiate !--- the crypto keys and  
initialization vectors, increasing the security of !---  
the connection. svc rekey time 30  
  
--- Command that specifies the number of minutes from  
the start of the !--- session until the rekey takes  
place, from 1 to 10080 (1 week). svc rekey method ssl  
  
!--- Command that specifies that SSL renegotiation takes  
place during SVC rekey. username ssluser1 password  
ZRhW85jZqEaVd5P. encrypted  
  
!--- Create an user account "ssluser1." aaa local  
authentication attempts max-fail 16  
  
!--- Enable the AAA local authentication. 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 tunnel-  
group sslgroup type webvpn  
  
!--- Create a tunnel group "sslgroup" with type as  
WebVPN. 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. telnet  
timeout 5 ssh timeout 5 console timeout 0 ! 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  
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect  
sip inspect xdmcp ! service-policy global_policy global  
webvpn  
  enable outside  
  
!--- Enable WebVPN on the outside interface. svc image  
disk0:/sslclient-win-1.1.4.179.pkg 1
```



```

!--- Assign an order to the SVC image. svc 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. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#

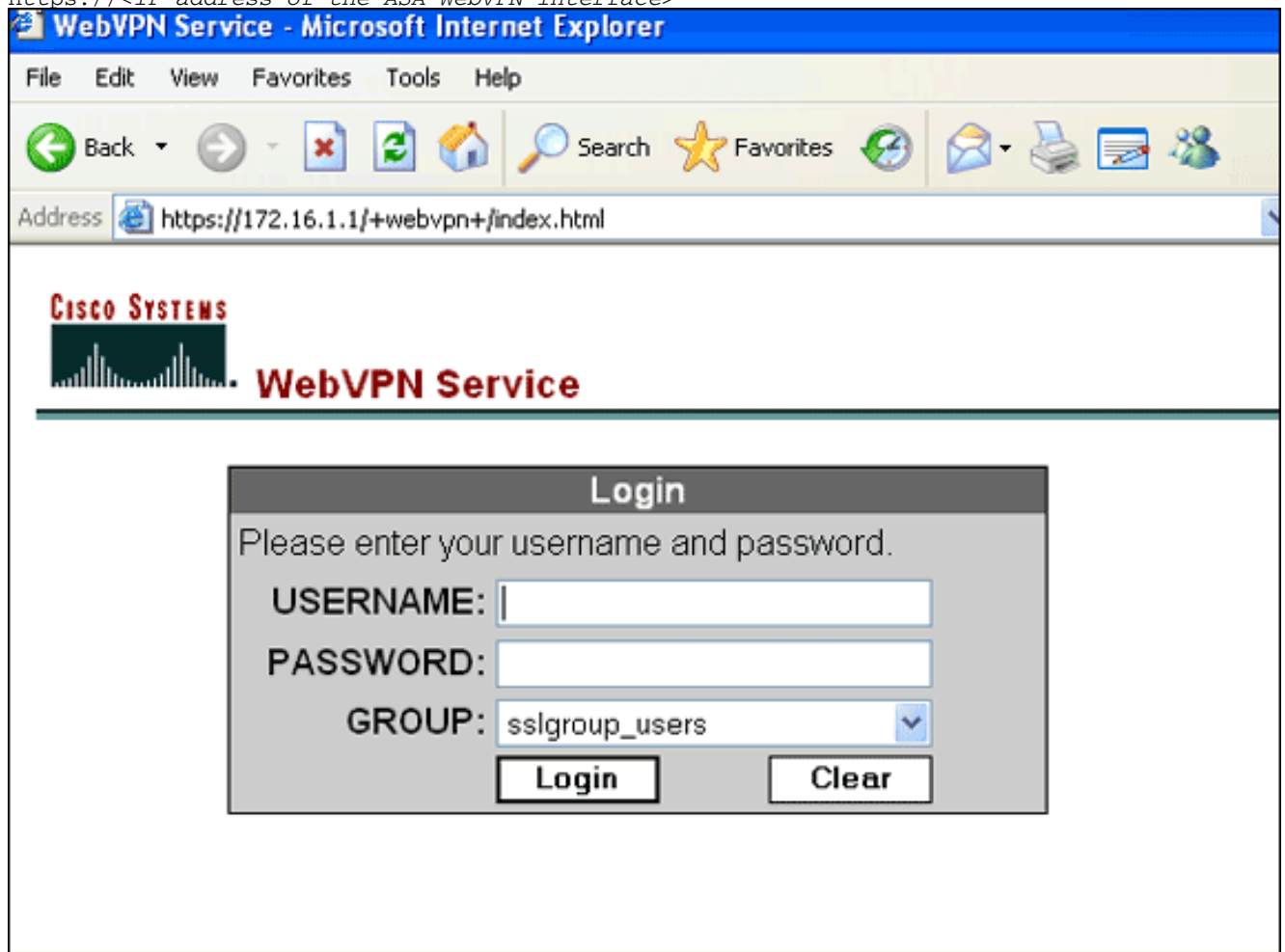
```

SVC와 SSL VPN 연결 설정

ASA와 SSL VPN 연결을 설정하려면 다음 단계를 완료하십시오.

1. 웹 브라우저의 Address 필드에 ASA의 WebVPN 인터페이스에 대한 URL 또는 IP 주소를 입력합니다.예:

`https://<IP address of the ASA WebVPN interface>`



2. 사용자 이름과 암호를 입력한 다음 그룹 드롭다운 목록에서 해당 그룹을 선택합니다

Login

Please enter your username and password.

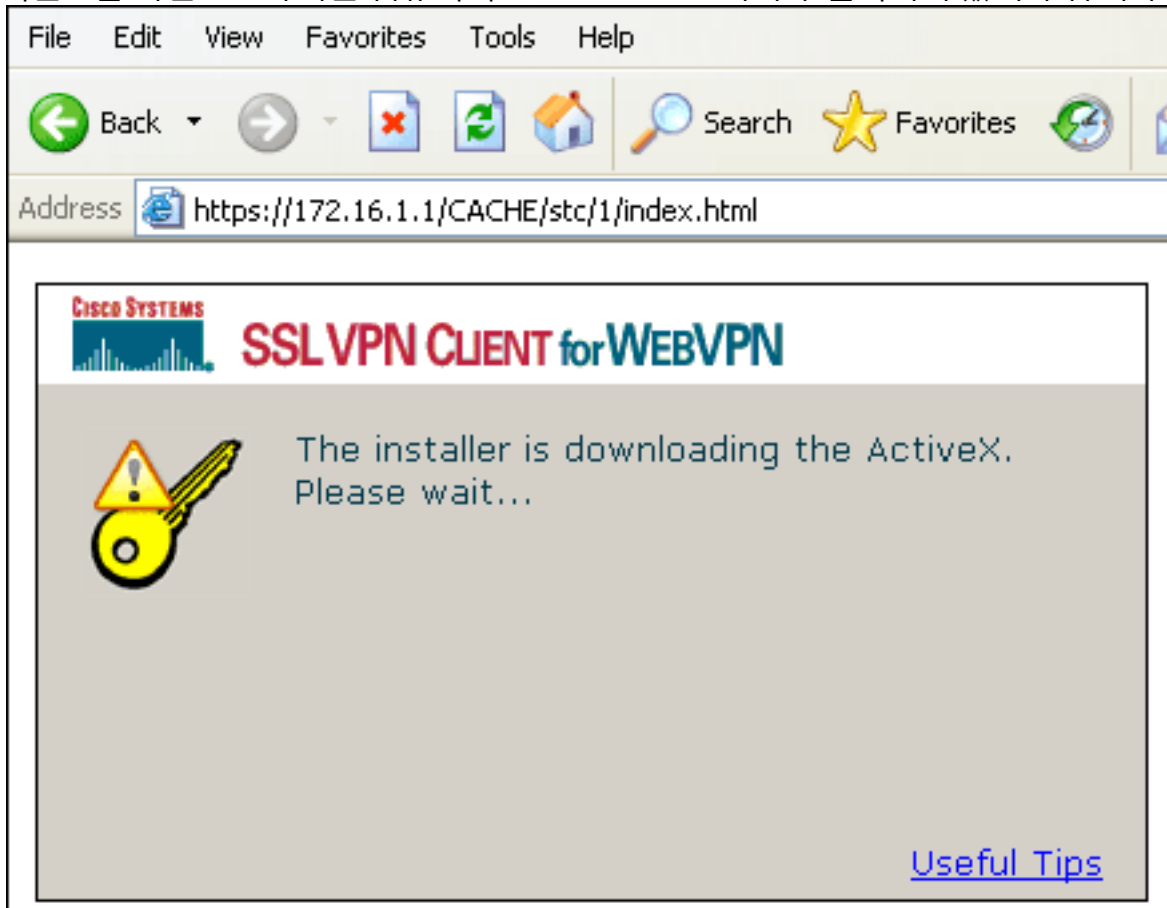
USERNAME:

PASSWORD:

GROUP: ▼

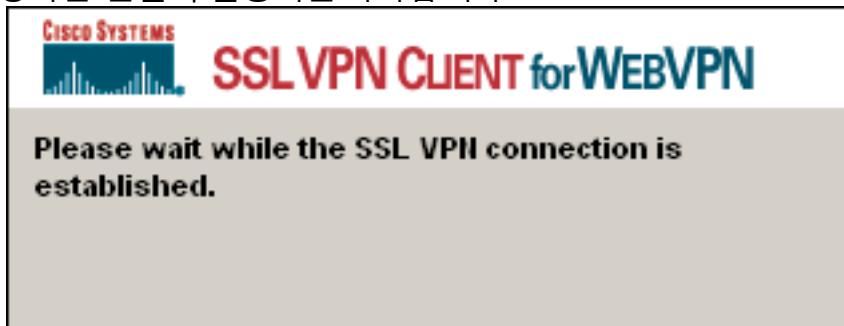
참고: SSL VPN 클라

이언트를 다운로드하려면 컴퓨터에 ActiveX 소프트웨어가 설치되어 있어야 합니다



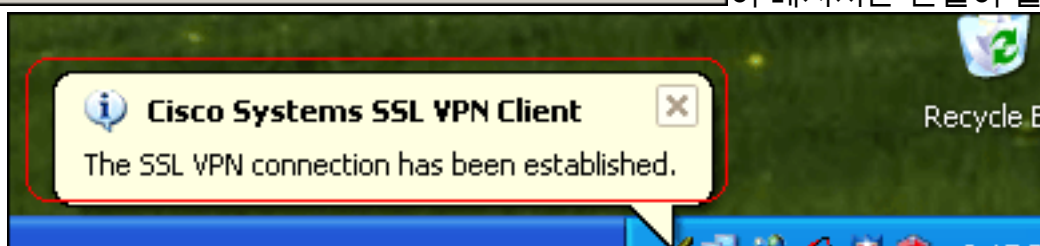
이 대화

상자는 연결이 설정되면 나타납니다



이 메시지는 연결이 설정되면 나

타납니다.



3. 연결이 설정되면 컴퓨터의 작업 표시줄에 나타나는 노란색 키 아이콘을 두 번 클릭합니다

.Cisco Systems SSL VPN Client 대화 상자에는 SSL 연결에 대한 정보가 표시됩니다

The screenshot shows the 'Statistics' tab of the Cisco Systems SSL VPN Client. It displays connection details such as server and client IP addresses, cipher and version information, transport settings, and connection duration. A 'Reset' button is located at the bottom of the statistics area.

Address Information	
Server:	172.16.1.1
Client:	192.168.10.1

Bytes	
Sent:	5471
Received:	884

Frames	
Sent:	75
Received:	12

SSL Information	
Cipher:	3DES SHA-1
Version:	TLSv1

Transport Information	
Local LAN:	Disabled
Split Tunneling:	Disabled

Connection Information	
Time:	00:00:35

Buttons: Close, Disconnect, Reset

The screenshot shows the 'Route Details' tab of the Cisco Systems SSL VPN Client. It displays two tables: 'Local LAN Routes' and 'Secure Routes'. The 'Secure Routes' table shows a single entry with Network 0.0.0.0 and Subnet Mask 0.0.0.0.

Local LAN Routes	
Network	Subnet Mask

Secure Routes	
Network	Subnet Mask
0.0.0.0	0.0.0.0

Buttons: Close, Disconnect



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구](#)([등록된](#) 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show webvpn svc** - ASA 플래시 메모리에 저장된 SVC 이미지를 표시합니다.

```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
   CISCO STC win2k+ 1.0.0
   1,1,4,179
   Fri 01/18/2008 15:19:49.43
```

```
1 SSL VPN Client(s) installed
```

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

```
ciscoasa#show vpn-sessiondb svc
```

```
Session Type: SVC
```

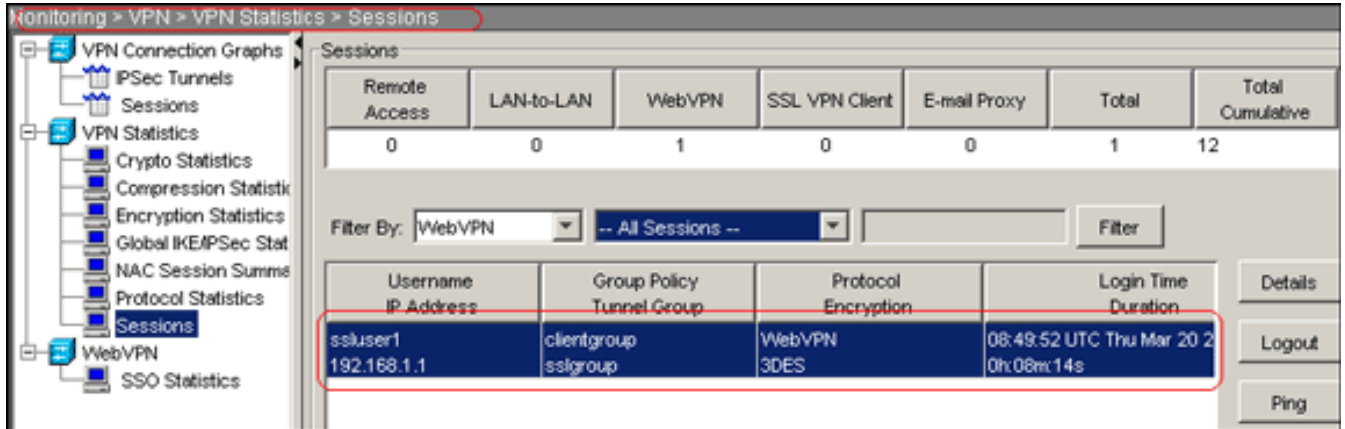
```
Username      : ssluser1
Index         : 1
Assigned IP   : 192.168.10.1      Public IP    : 192.168.1.1
Protocol      : SVC              Encryption   : 3DES
Hashing       : SHA1
Bytes Tx      : 131813           Bytes Rx     : 5082
Client Type   : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver    : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy  : clientgroup
```

```
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration    : 0h:00m:53s
Filter Name  :
```

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

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

- ASA의 현재 WebVPN 세션에 대한 정보를 보려면 ASDM에서 **Monitoring > VPN > VPN Statistics > Sessions**를 선택합니다



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- **vpn-sessiondb logoff name <username>** - 지정된 사용자 이름에 대한 SSL VPN 세션을 로그오프할 수 있습니다.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

마찬가지로 **vpn-sessiondb logoff svc** 명령을 사용하여 모든 SVC 세션을 종료할 수 있습니다.
참고: PC가 대기 모드 또는 최대 절전 모드로 전환되면 SSL VPN 연결을 종료할 수 있습니다.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

- **Debug webvpn svc <1-255>** - 세션을 설정하기 위해 실시간 WebVPN 이벤트를 제공합니다.

```
Ciscoasa#debug webvpn svc 7

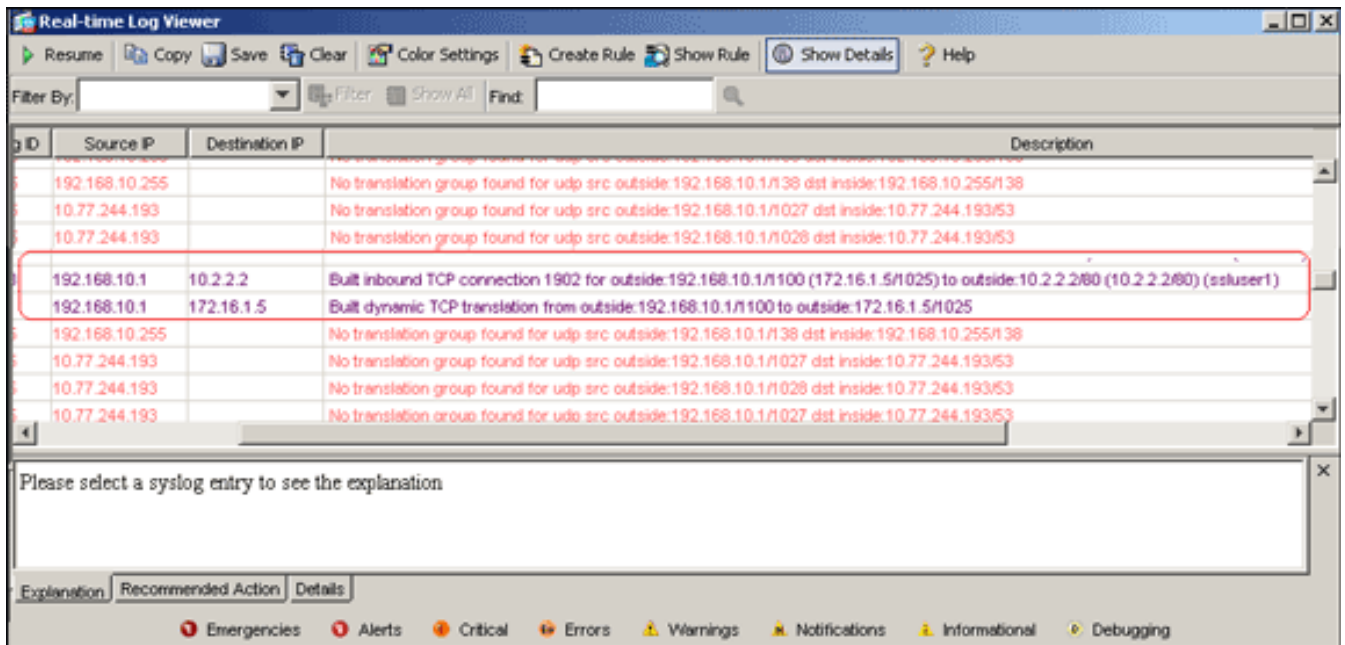
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
```

```

webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
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: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED

```

- ASDM에서 실시간 이벤트를 보려면 **Monitoring > Logging > Real-time Log Viewer > View**를 선택합니다. 다음 예에서는 ASA 172.16.1.5을 통해 인터넷에서 SVC 192.168.10.1과 Webserver 10.2.2.2 간의 세션 정보를 보여 줍니다



관련 정보

- [Cisco 5500 Series Adaptive Security Appliance 지원 페이지](#)
- [스틱 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 7.x 및 VPN 클라이언트 예](#)
- [ASA의 SVC\(SSL VPN Client\) with ASDM 컨피그레이션 예](#)
- [기술 지원 및 문서 - Cisco Systems](#)