ASA 8.X: 로그온 전 AnyConnect 시작 기능 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[배경 정보](#)
[로그온 전 시작 구성 요소 설치(Windows에만 해당)](#)
[Windows-Vista\Windows 7과 로그온 전 Vista 시작 사이의 차이점](#)
[SBL을 활성화하는 XML 설정](#)
[SBL 활성화](#)
[CLI를 사용하여 로그온 구성 전에 시작](#)
[ASDM을 사용하여 로그온 구성 전 시작](#)
[매니페스트 파일 사용](#)
[SBL 문제 해결](#)
[문제 1](#)
[솔루션 1](#)
[관련 정보](#)

소개

SBL(*Start Before Logon*)을 활성화하면 Windows® 로그온 대화 상자가 표시되기 전에 AnyConnect GUI 로그온 대화 상자가 표시됩니다. 이렇게 하면 먼저 VPN 연결이 설정됩니다. Windows 플랫폼에서만 사용 가능한 로그온 전 시작 을 사용하면 관리자가 로그인 스크립트 사용, 암호 캐싱, 로컬 드라이브에 네트워크 드라이브 매핑 등을 제어할 수 있습니다. SBL 기능을 사용하여 로그온 시퀀스의 일부로 VPN을 활성화할 수 있습니다. SBL은 기본적으로 비활성화되어 있습니다.

AnyConnect VPN 클라이언트 기능 구성에 대한 자세한 내용은 AnyConnect 클라이언트 기능 구성 절을 참조하십시오.

참고: AnyConnect 클라이언트 내에서 SBL에 대해 수행하는 유일한 컨피그레이션은 기능을 활성화하는 것입니다. 네트워크 관리자는 상황의 요구 사항에 따라 로그온 전에 수행되는 처리를 처리합니다. 로그온 스크립트는 도메인 또는 개별 사용자에게 할당할 수 있습니다. 일반적으로 도메인의 관리자는 배치 파일 또는 Active Directory의 사용자 또는 그룹과 함께 정의된 것과 같은 파일을 가지고 있습니다. 사용자가 로그온하면 로그인 스크립트가 실행됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco AnyConnect VPN 버전 2.0

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 규칙을 참조하십시오.

배경 정보

SBL의 핵심은 PC에 로그온하기 전에 원격 컴퓨터를 회사 인프라에 연결하는 것입니다. 예를 들어 사용자가 물리적 기업 네트워크 외부에 있을 수 있으며, PC가 기업 네트워크에 조인될 때까지 회사 리소스에 액세스할 수 없습니다. SBL이 활성화된 경우 AnyConnect 클라이언트는 사용자가 Microsoft 로그인 창을 보기 전에 연결됩니다. Microsoft 로그인 창이 나타나면 사용자는 Windows에 정상적으로 로그인해야 합니다.

다음은 SBL을 사용하는 몇 가지 이유입니다.

- 사용자의 PC가 Active Directory 인프라에 조인됩니다.
- 사용자는 PC에 캐시된 자격 증명을 가질 수 없습니다. 즉, 그룹 정책에서 캐시된 자격 증명을 허용하지 않는 경우.
- 사용자는 네트워크 리소스에서 실행되거나 네트워크 리소스에 대한 액세스가 필요한 로그인 스크립트를 실행해야 합니다.
- 사용자에게 Active Directory 인프라와의 인증이 필요한 네트워크 매핑 드라이브가 있습니다.
- MS NAP/CS NAC와 같은 네트워킹 구성 요소는 인프라에 연결해야 할 수 있습니다.

SBL은 로컬 기업 LAN에 포함되는 것과 동일한 네트워크를 생성합니다. SBL이 활성화된 경우 사용자가 로컬 인프라에 액세스할 수 있으므로 사무실의 사용자에 대해 일반적으로 실행되는 로그온 스크립트도 원격 사용자도 사용할 수 있습니다.

로그온 스크립트를 만드는 방법에 대한 자세한 내용은 이 Microsoft TechNet 문서를 참조하십시오 .

Windows XP에서 로컬 로그온 스크립트를 사용하는 방법에 대한 자세한 내용은 이 Microsoft 문서를 참조하십시오 .

또 다른 예에서는 PC에 로그온하기 위해 캐시된 자격 증명을 허용하지 않도록 시스템을 구성할 수 있습니다. 이 시나리오에서는 사용자가 PC에 액세스하기 전에 자격 증명을 검증하기 위해 회사 네트워크의 도메인 컨트롤러와 통신할 수 있어야 합니다. SBL을 호출하면 네트워크 연결이 있어야 합니다. 무선 연결이 무선 인프라에 연결하기 위해 사용자 자격 증명에 따라 달라질 수 있기 때문에 이 작업은 가능하지 않은 경우도 있습니다. SBL 모드는 로그인의 자격 증명 단계보다 우선하므로 이 시나리오에서는 연결을 사용할 수 없습니다. 이 경우 로그인 전체에서 자격 증명을 캐시하도록 무선 연결을 구성해야 하거나 SBL이 작동하도록 다른 무선 인증을 구성해야 합니다.

로그온 전 시작 구성 요소 설치(Windows에만 해당)

코어 클라이언트를 설치한 후 로그온 전 시작 구성 요소를 설치해야 합니다. 또한 AnyConnect 2.2 Start Before Logon 구성 요소에는 코어 AnyConnect 클라이언트 소프트웨어의 버전 2.2 이상이 설치되어 있어야 합니다. MSI 파일로 AnyConnect 클라이언트 및 로그온 전 시작 구성 요소를 사전 배포할 경우(예: 자체 소프트웨어 배포(Altiris, Active Directory 또는 SMS)가 있는 대기업의 경우 주문을 올바르게 받아야 합니다. AnyConnect가 웹 배포 및/또는 웹으로 업데이트된 경우 관리자가 AnyConnect를 로드하면 설치 순서가 자동으로 처리됩니다. 전체 설치 정보는 Cisco AnyConnect VPN Client 릴리스 정보, 릴리스 2.2를 참조하십시오.

Windows-Vista\Windows 7과 로그온 전 Vista 시작 사이의 차이점

SBL을 활성화하는 절차는 Windows Vista 및 Windows 7 시스템에서 약간 다릅니다. Vista 이전 시스템에서는 VPNGINA(Virtual Private Network Graphical Identification and Authentication)라는 구성 요소를 사용하여 SBL을 구현합니다. Vista 및 Windows 7 시스템은 PLAP라는 구성 요소를 사용하여 SBL을 구현합니다.

AnyConnect 클라이언트에서 Windows Vista 로그온 전 시작 기능을 연결 가능한 자격 증명 공급자인 PLAP(Pre-Login Access Provider)라고 합니다. 이 기능을 사용하면 네트워크 관리자가 로그인 전에 자격 증명 모음 또는 네트워크 리소스에 대한 연결 등의 특정 작업을 수행할 수 있습니다. PLAP는 Windows Vista, Windows 7 및 Windows 2008 서버에서 로그온 전 시작 기능을 제공합니다. PLAP는 각각 vpnplap.dll 및 vpnplap64.dll을 사용하여 32비트 및 64비트 버전의 운영 체제를 지원합니다. PLAP 기능은 Windows Vista x86 및 x64 버전을 지원합니다.

참고: 이 섹션에서 VPNGINA는 Vista 이전 플랫폼의 로그온 전 시작 기능을 참조하고, PLAP는 Windows Vista 및 Windows 7 시스템의 로그온 전 시작 기능을 참조합니다.

Vista 이전 시스템에서 Start Before Logon(로그온 전 시작)은 VPN 그래픽 식별 및 인증 동적 링크 라이브러리(vpngina.dll)라는 구성 요소를 사용하여 로그온 전 시작 기능을 제공합니다. Windows Vista의 일부인 Windows PLAP 구성 요소는 Windows GINA 구성 요소를 대체합니다.

사용자가 Ctrl+Alt+Del 키 조합을 누르면 GINA가 활성화됩니다. PLAP를 사용하는 경우 Ctrl+Alt+Del 키 조합을 사용하면 사용자가 시스템에 로그인하거나 창의 오른쪽 아래 모서리에 있는 네트워크 연결 단추를 사용하여 네트워크 연결(PLAP 구성 요소)을 활성화할 수 있는 창이 열립니다 .

다음 섹션에서는 VPNGINA 및 PLAP SBL에 대한 설정 및 절차에 대해 설명합니다. Windows Vista 플랫폼에서 SBL 기능(PLAP)을 활성화하고 사용하는 방법에 대한 자세한 내용은 Windows Vista 시스템에서 PLAP(Start Before Logon) 구성을 참조하십시오.

SBL을 활성화하는 XML 설정

UseStartBeforeLogon의 요소 값을 사용하면 이 기능을 설정하거나 해제(false)할 수 있습니다. 프로파일에서 이 값을 **true로** 설정하면 로그온 시퀀스의 일부로 추가 처리가 발생합니다. 자세한 내용은 로그온 전 시작 설명을 참조하십시오. SBL을 활성화하려면 CiscoAnyConnect.xml 파일의 <UseStartBefore Logon> 값을 **true**로 설정합니다.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
```

```
</ClientInitialization>
```
SBL을 비활성화하려면 동일한 값을 **false로 설정합니다**.

사용자 제어 가능 기능을 활성화하려면 SBL을 활성화할 때 다음 문을 사용합니다.

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```
이 특성과 연결된 모든 사용자 설정은 다른 위치에 저장됩니다.

SBL 활성화

다운로드 시간을 최소화하기 위해 AnyConnect 클라이언트는 지원되는 각 기능에 필요한 핵심 모듈만 보안 어플라이언스에서 다운로드하도록 요청합니다. SBL과 같은 새 기능을 활성화하려면 그룹 정책 WebVPN 또는 사용자 이름 WebVPN 컨피그레이션 모드에서 svc **modules** 명령을 사용하여 모듈 이름을 지정해야 합니다.

```
[no] svc modules {none | value string}
```
SBL의 문자열 값은 **vpngina입니다**.

이 예에서는 네트워크 관리자가 그룹 정책 재택 근무자에 대해 그룹 정책 특성 모드를 시작합니다. 그룹 정책에 대한 WebVPN 컨피그레이션 모드를 시작합니다. 및 SBL을 활성화하기 위해 VPNGINA 문자열을 지정합니다.

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

또한 관리자는 AnyConnect <profile.xml> 파일(여기서 <profile.xml>은 네트워크 관리자가 XML 파일에 할당한 이름)에 <UseStartBeforeLogon> 문이 **true**로 설정되어 있는지 확인해야 합니다. 예:

```
UseStartBeforeLogon UserControllable="false">true
```

[로그온 전 시작]을 적용하려면 시스템을 재부팅해야 합니다. 또한 SBL을 허용할 보안 어플라이언스 또는 추가 기능을 위해 다른 모든 모듈을 지정해야 합니다. 자세한 내용은 추가 AnyConnect 기능에 대한 모듈 활성화, 2-5페이지(ASDM) 섹션 또는 추가 AnyConnect 기능에 대한 모듈 활성화, 3-4페이지(CLI)의 설명을 참조하십시오.

CLI를 사용하여 로그온 구성 전에 시작

이 시나리오에서는 CLI를 사용하여 XML 파일을 설정하는 방법을 보여줍니다.

1. 다음과 유사한 클라이언트 PC로 푸시할 프로파일을 만듭니다.
```
<?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>true</UseStartBeforeLogon>
```

```
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

2. 파일을 보안 어플라이언스의 플래시에 복사합니다.

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

3. AnyConnect 연결에 대해 다른 모든 것이 올바르게 설정된 경우 보안 어플라이언스에서 프로파일을 WebVPN 전역 섹션에 사용 가능한 프로필로 추가합니다.

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. 사용하는 그룹 정책을 수정하고 svc **모듈** 및 svc **profile** 명령을 추가합니다.

```
hostname(config)# group-policy GroupPolicy internal
hostname(config)# group-policy GroupPolicy attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

ASDM을 사용하여 로그온 구성 전 시작

ASDM을 사용하여 SBL을 구성하려면 다음 단계를 완료합니다.

1. 다음과 유사한 클라이언트 PC로 푸시할 프로파일을 만듭니다.

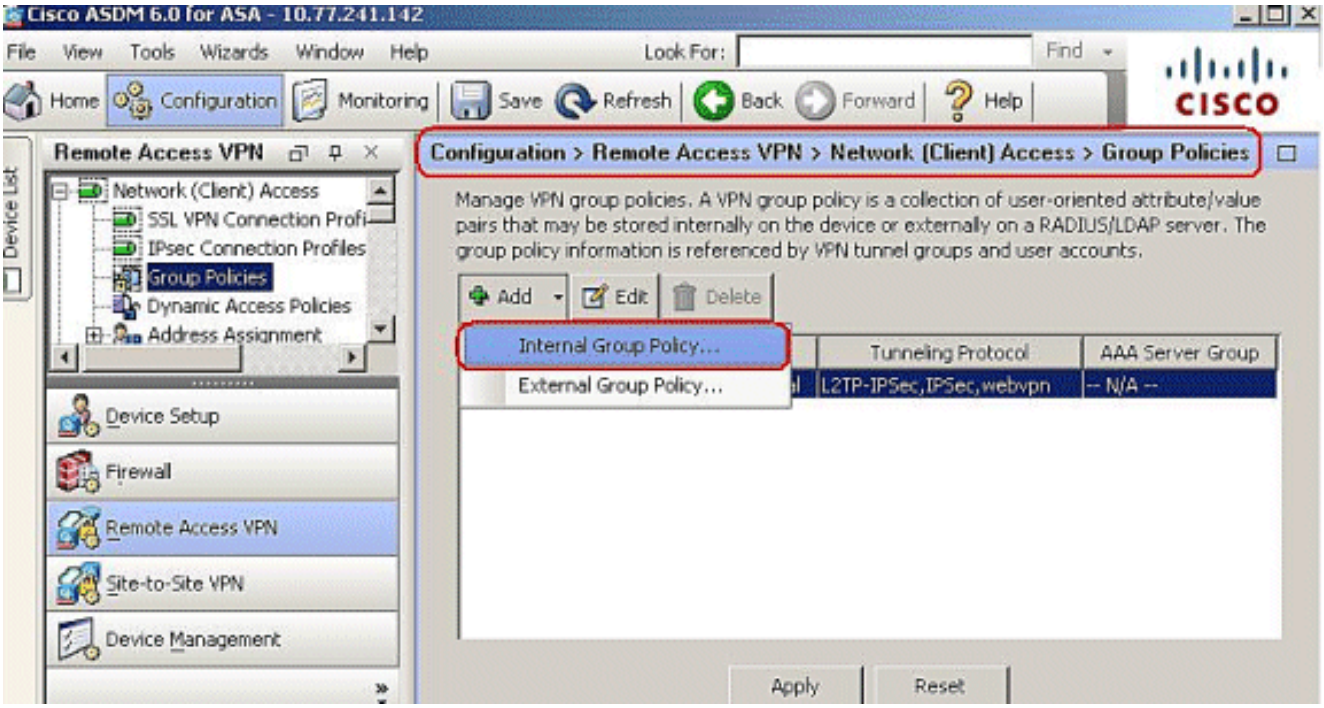
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
```

.

```
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

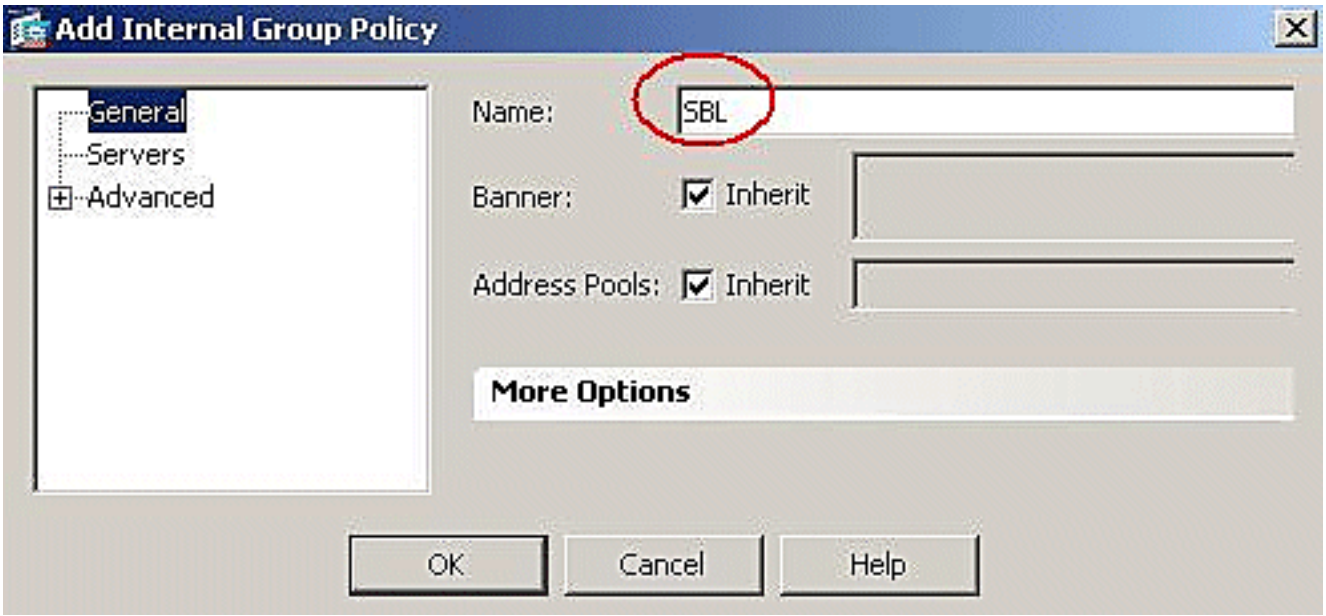
2. 프로파일을 로컬 컴퓨터에 **AnyConnectProfile.xml**로 저장합니다.
3. ASDM을 시작하고 홈 페이지로 이동합니다.
4. Configuration(컨피그레이션) **> Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Add(추가)로 이동하여 Internal Group Policy(내부 그룹 정책)**를 클릭합니다

.



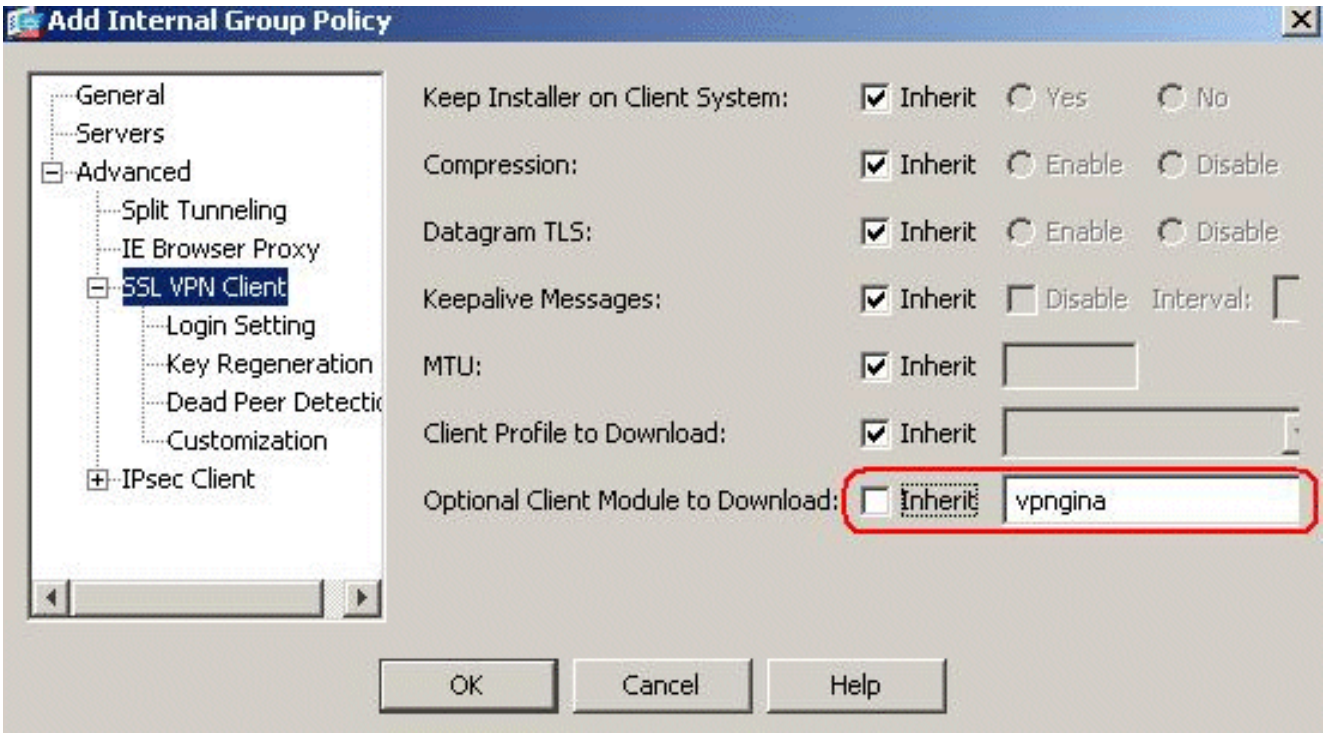
5. 그룹 정책의 이름(예: SBL)을 **입력합니다**

.



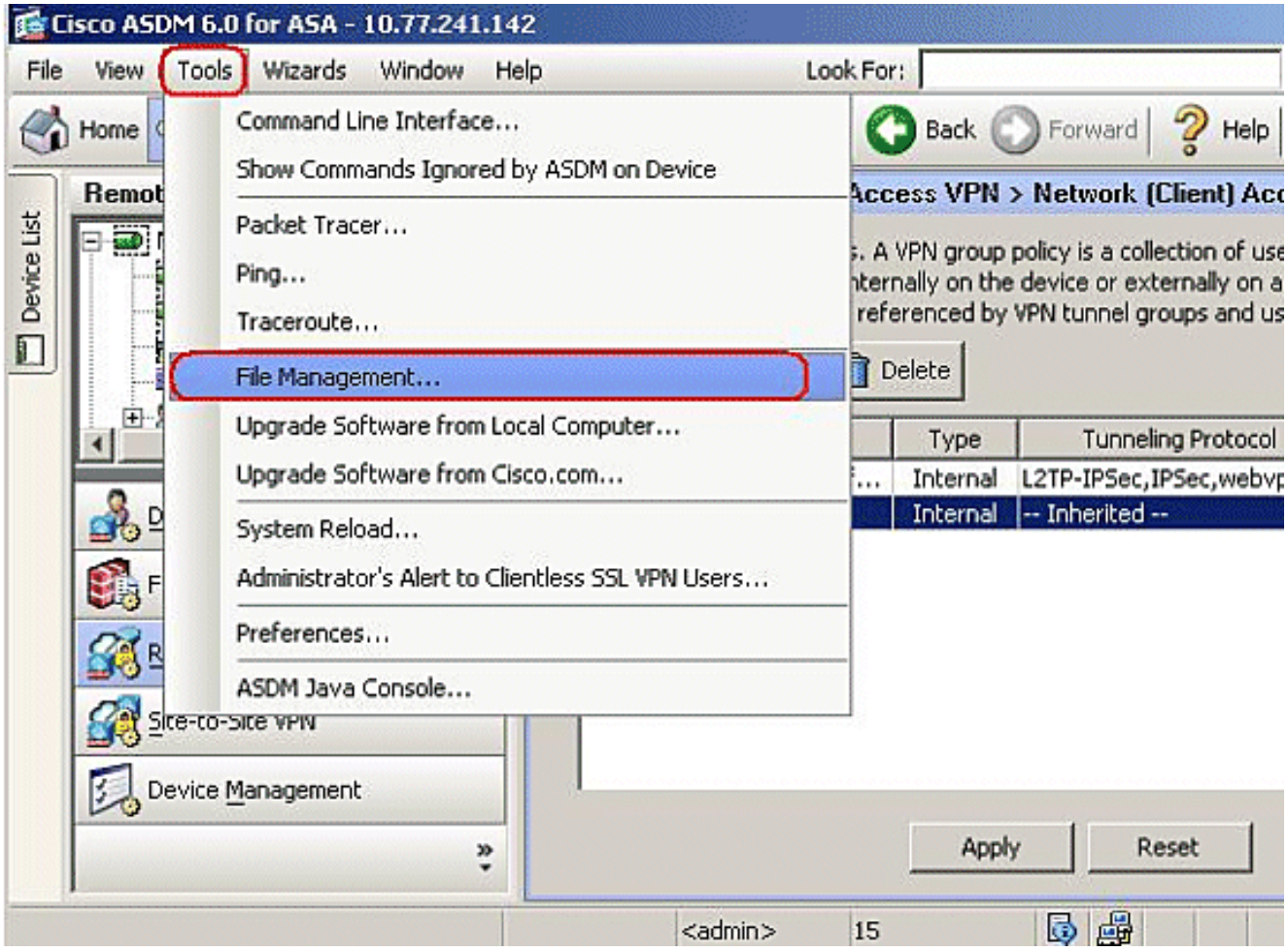
6. Advanced(**고급) > SSL VPN Client(SSL VPN 클라이언트)로 이동합니다**. Optional Client **Module to Download(다운로드할 선택적 클라이언트 모듈)**에서 Inherit(상속) 확인 표시를 제거하고 드롭다운 상자에서 vpngina를 선택합니다

.



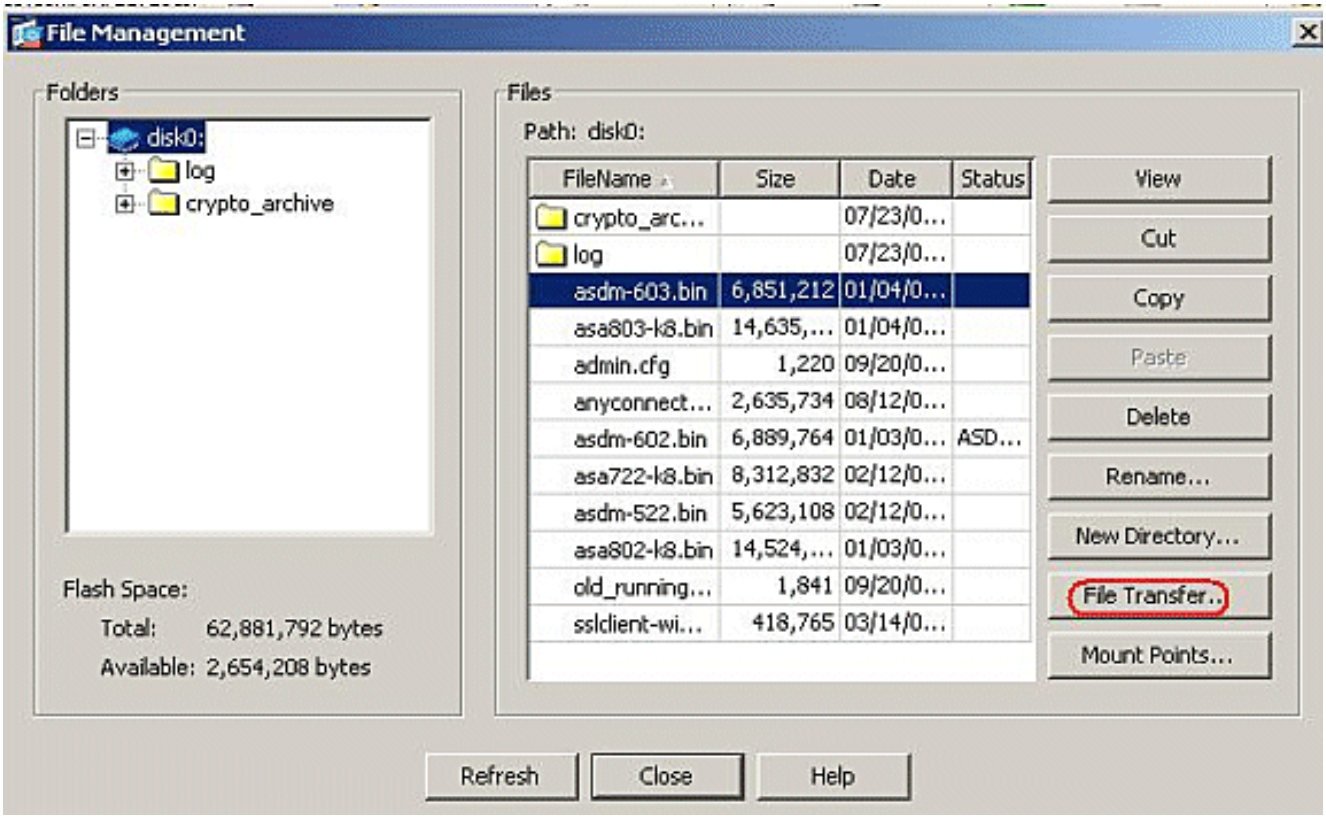
7. 프로파일 AnyConnectProfile.**xml을** 로컬 컴퓨터에서 플래시로 전송하려면 **도구**로 이동하고 **파일 관리**를 클릭합니다

.



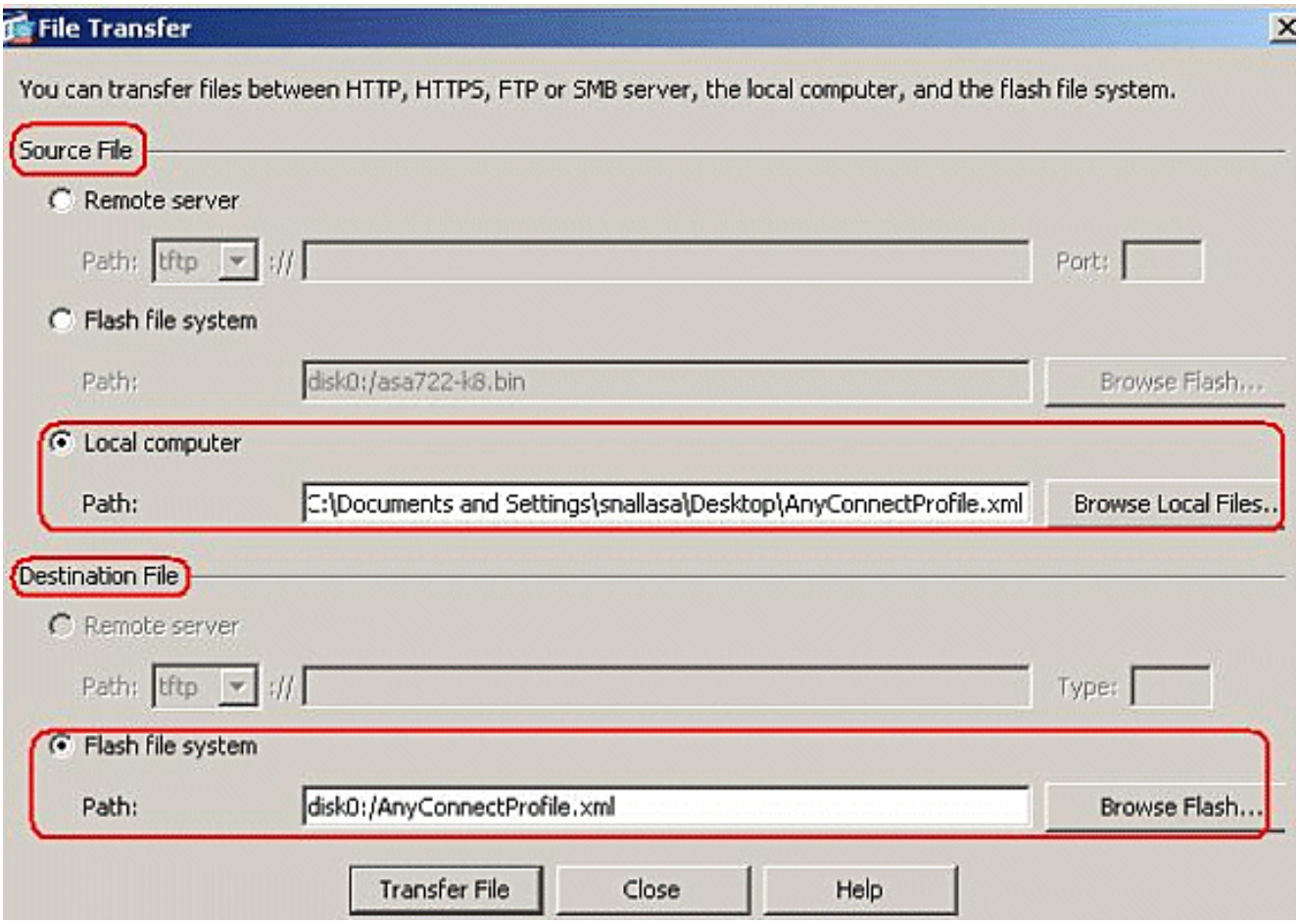
8. **파일 전송** 버튼을 클릭합니다

.



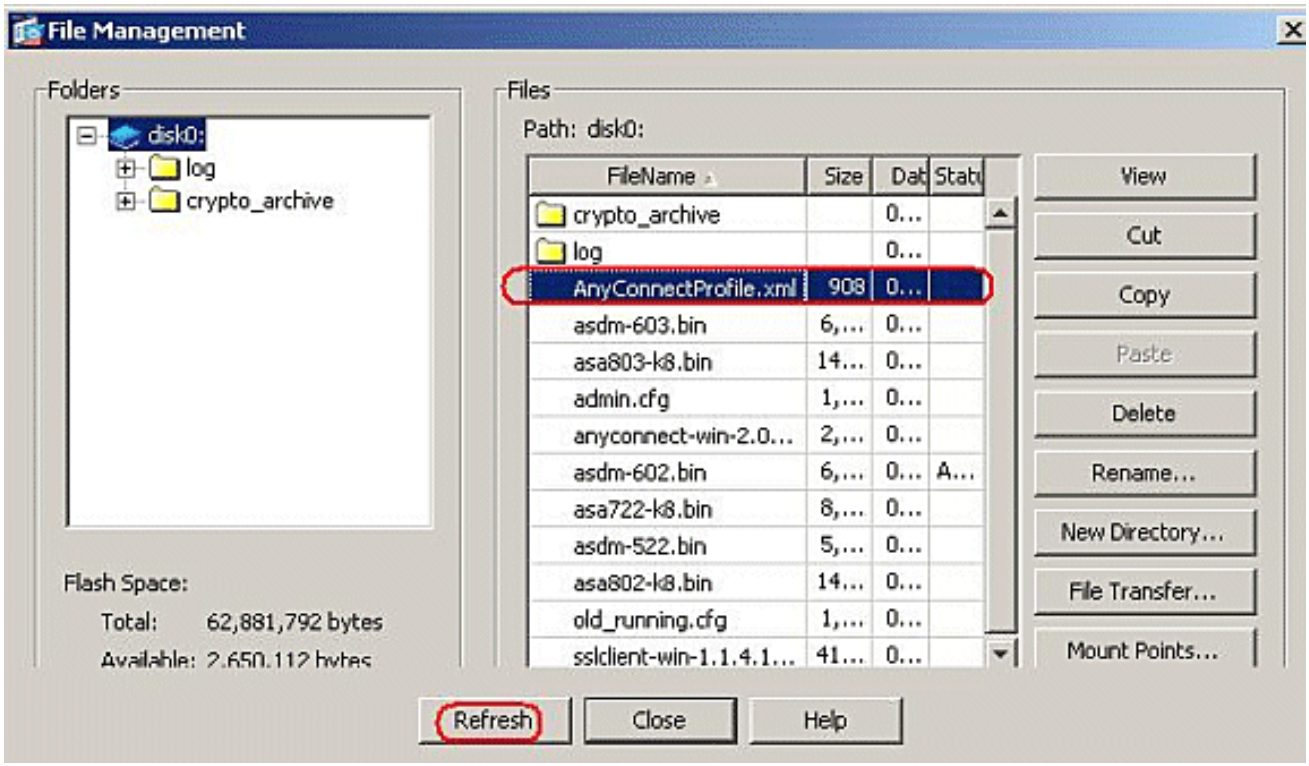
9. 로컬 컴퓨터에서 ASA 플래시 메모리로 프로필을 전송하려면 요구 사항에 따라 **소스 파일**, XML 파일 경로(로컬 컴퓨터) 및 **대상 파일** 경로를 선택합니다

.



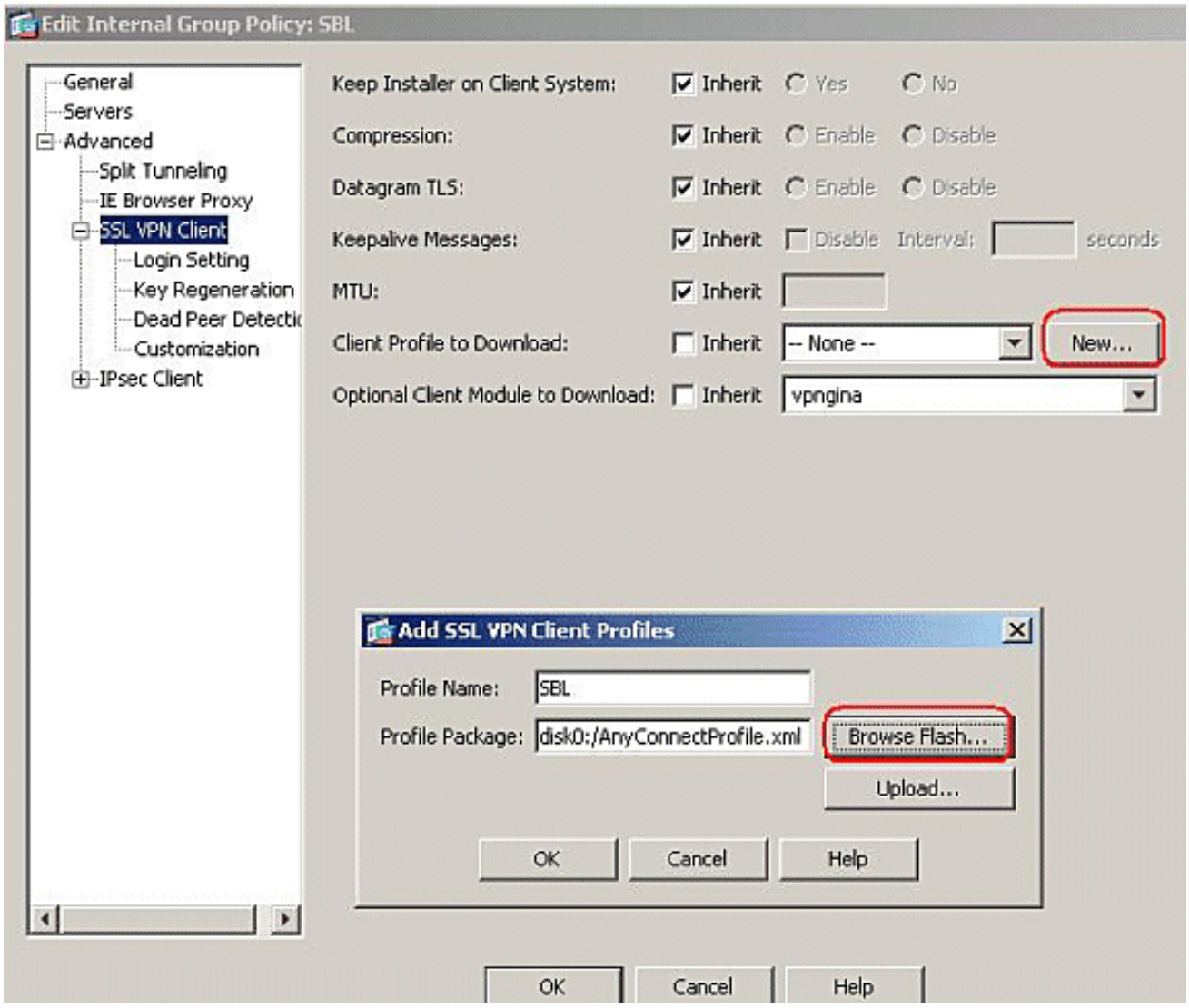
10. 전송 후 **Refresh**(새로 고침) 버튼을 클릭하여 프로파일 파일이 플래시 메모리에 있는지 확인합니다

.

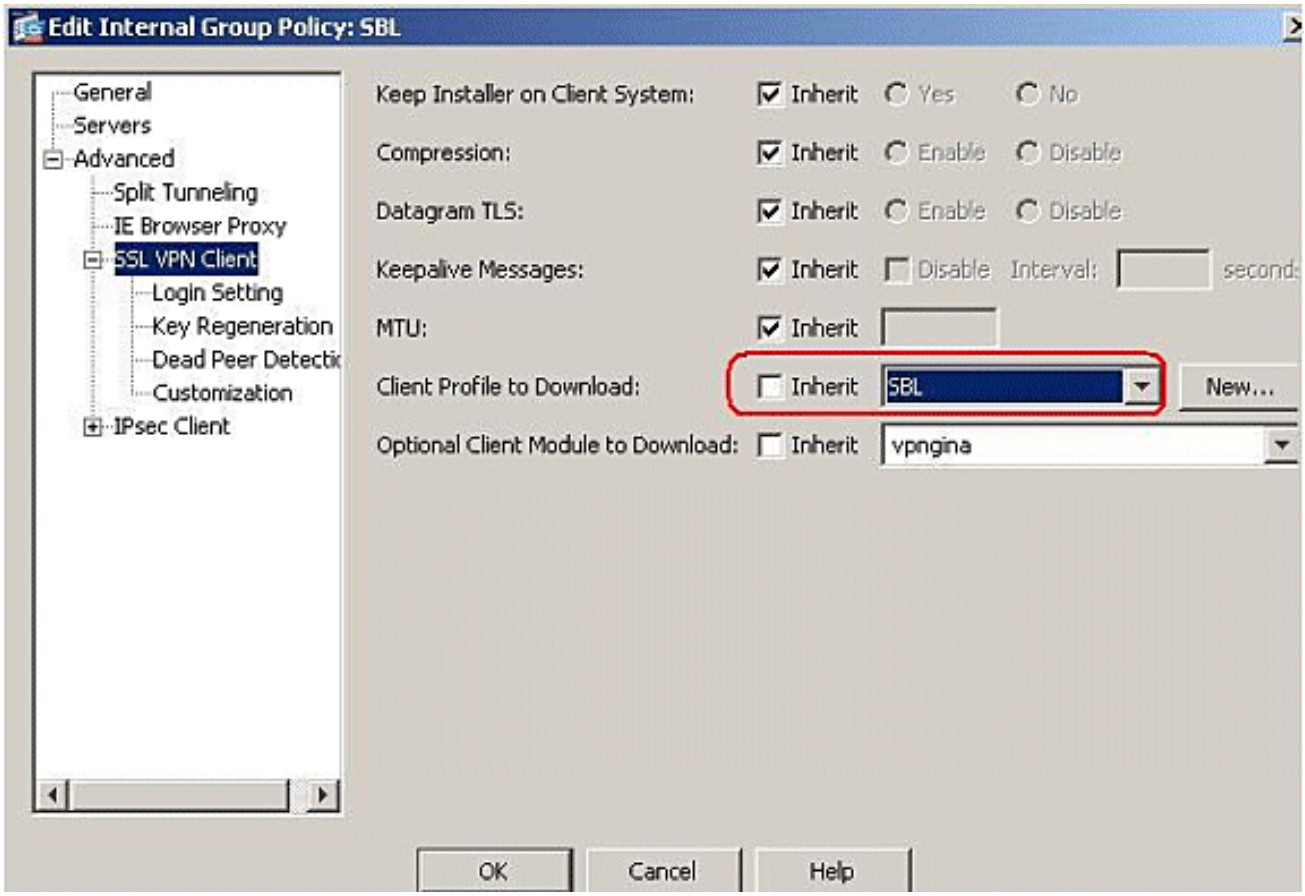


11. 프로파일을 내부 그룹 정책(SBL)에 **할당합니다**.이 경로를 따라 Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책) > Edit SBL (Internal Group Policy) > Advanced(고급) > SSL VPN Client(SSL VPN 클라이언트) > Client Profile to Download(다운로드할 클라이언트 프로파일)New(새로 만들기)** 버튼을 클릭합니다.Add **SSL VPN Client Profiles(SSL VPN 클라이언트 프로파일 추가)**에서 **Browse**(찾아보기) 버튼을 클릭하여 ASA 플래시 메모리에 저장된 프로파일(AnyConnectProfile.xml)의 위치를 선택합니다. 프로파일의 **이름**(예: SBL)을 **지정합니다**. OK(**확인**)를 클릭하여 완료합니다

.

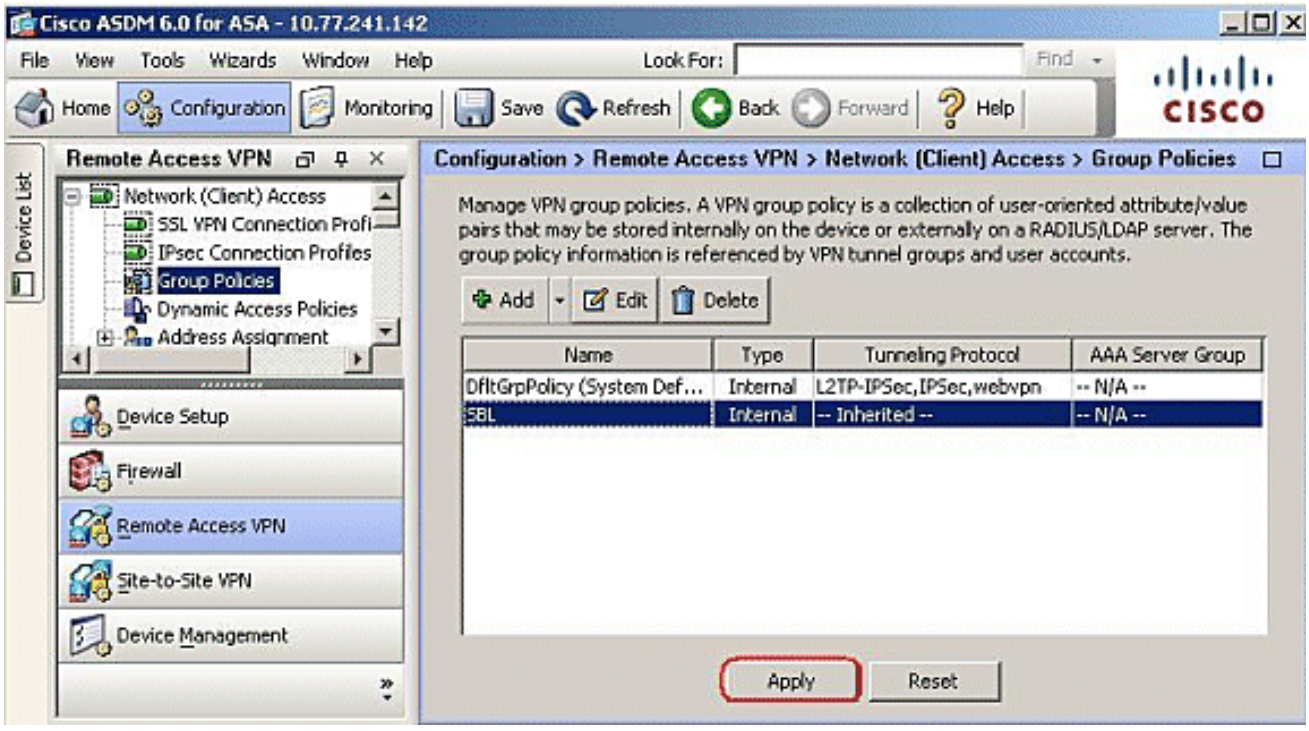


12. Inherit(상속) 확인란을 제거하고 Client Profile to Download(다운로드할 **클라이언트 프로파일**) 필드에서 **SBL을** 선택합니다. **확인을 클릭합니다**
.



13. Apply(**적용**)를 클릭하여 완료합니다

.



매니페스트 파일 사용

보안 어플라이언스에 업로드되는 AnyConnect 패키지에는 VPNManifest.xml이라는 파일이 포함되어 있습니다. 다음 예에서는 이 파일의 샘플 내용을 보여 줍니다.

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
```

```
    is_core="yes" type="exe" action="install">
    <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
  </file>
  <file version="2.1.0150" id="gina"
    is_core="yes" type="exe" action="install" module="vpngina">
    <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
  </file>
</vpn>
```

보안 어플라이언스는 1단계에서 설명한 대로 구성된 프로파일에 저장했으며, AnyConnect 클라이언트 자체, 다운로더 유틸리티, 매니페스트 파일 및 기타 선택적 모듈이나 지원 파일이 포함된 하나 이상의 AnyConnect 패키지를 저장합니다.

원격 사용자가 WebLaunch 또는 현재 독립형 클라이언트를 사용하여 보안 어플라이언스에 연결하면 다운로더가 먼저 다운로드되고 실행됩니다. 매니페스트 파일을 사용하여 원격 사용자 PC에 업그레이드해야 하는 현재 클라이언트가 있는지 또는 새로 설치해야 하는지 여부를 확인합니다. 매니페스트 파일에는 VPNGINA를 다운로드하여 설치해야 하는 선택적 모듈이 있는지 여부에 대한 정보도 들어 있습니다. 클라이언트 프로파일은 보안 어플라이언스에서 푸시됩니다. VPNGINA의 설치는 4단계에서 설명한 대로 **그룹 정책(webvpn)** 명령 모드에 구성된 svc **모듈 값 vpngina에** 의해 활성화됩니다. AnyConnect 클라이언트와 VPNGINA가 설치되며 사용자는 Windows 도메인 로그온 전에 다음 재부팅 시 AnyConnect 클라이언트를 확인합니다.

사용자가 연결되면 클라이언트 및 프로파일이 사용자 PC에 전달됩니다. 클라이언트 및 VPNGINA가 설치되어 있습니다. 사용자가 로그온하기 전에 다음 재부팅 시 AnyConnect 클라이언트를 확인합니다.

AnyConnect가 설치된 경우 클라이언트 PC에 샘플 프로파일이 제공됩니다. **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

SBL 문제 해결

SBL에 문제가 있는 경우 다음 절차를 사용합니다.

1. 프로파일이 푸시되었는지 확인합니다.
2. 이전 프로필 삭제; 하드 드라이브에서 해당 위치를 찾기 위해 검색합니다. *.xml
3. 프로그램 추가/제거로 이동할 때 AnyConnect 설치 및 AnyConnect VPNGINA가 모두 설치되어 있습니까?
4. AnyConnect 클라이언트를 제거합니다.
5. 이벤트 뷰어에서 사용자의 AnyConnect 로그를 지우고 다시 테스트합니다.
6. 웹 브라우저에서 보안 어플라이언스로 다시 이동하여 클라이언트를 다시 설치합니다.
7. 프로필도 나타나는지 확인합니다.
8. 한 번 재부팅합니다. 다음 재부팅 시 로그온 전 시작 프롬프트가 표시됩니다.
9. AnyConnect 이벤트 로그를 .evt 형식으로 Cisco에 전송합니다.
10. 이 오류가 표시되면 사용자 프로필을 삭제하고 기본 프로필을 사용합니다.

```
Description: Unable to parse the profile
C:\Documents and Settings\All Users\Application Data\Cisco
\Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available.
```

문제 1

AnyConnect 프로파일을 업로드하는 동안 다음 오류 메시지가 표시됩니다. XML . 이 오류는 어떻게 해결됩니까?

솔루션 1

이 오류 메시지는 대부분 AnyConnect 프로파일의 구문 또는 컨피그레이션 문제로 인해 발생합니다 . 이 문제를 해결하려면 구성된 AnyConnect 프로파일이 Cisco AnyConnect VPN Client Administrator Guide의 Sample AnyConnect Profile and XML Schema 섹션에 있는 샘플 AnyConnect 프로파일과 유사한지 확인합니다.

관련 정보

- Cisco AnyConnect VPN 클라이언트 관리자 가이드, 버전 2.0
- 로그온 스크립트 만들기 - Windows TechNet
- Windows Vista 시스템에서 로그온 전 시작(PLAP) 구성
- AnyConnect SSL VPN 클라이언트 구성을 통한 ASA 8.x VPN 액세스 예
- Cisco AnyConnect VPN 클라이언트
- Cisco ASA 5500 Series Adaptive Security Appliance
- 기술 지원 및 문서 – Cisco Systems