ASA: ASDM 컨피그레이션을 사용하는 스마트 터널 예

목차

소개

스마트 터널은 TCP 기반 애플리케이션과 개인 사이트 간의 연결로서 보안 어플라이언스를 통해 클라이언트리스(브라우저 기반) SSL VPN 세션을 사용하고 보안 어플라이언스를 프록시 서버로 사용합니다. 스마트 터널 액세스를 허용할 애플리케이션을 식별하고 각 애플리케이션에 대한 로컬 경로를 지정할 수 있습니다. Microsoft Windows에서 실행되는 애플리케이션의 경우 스마트 터널 액세스 권한을 부여하기 위한 조건으로 체크섬의 SHA-1 해시와 일치해야 할 수도 있습니다.

Lotus SameTime 및 *Microsoft Outlook Express*는 스마트 터널 액세스를 허용할 수 있는 응용 프로그램의 예입니다.

애플리케이션이 클라이언트인지 아니면 웹 지원 애플리케이션인지에 따라 스마트 터널 컨피그레이션에는 다음 절차 중 하나가 필요합니다.

- 클라이언트 애플리케이션의 스마트 터널 목록을 하나 이상 생성한 다음 스마트 터널 액세스를 제공하려는 그룹 정책 또는 로컬 사용자 정책에 목록을 할당합니다.
- 스마트 터널 액세스에 적합한 웹 지원 애플리케이션의 URL을 지정하는 하나 이상의 책갈피 목록 항목을 만든 다음 스마트 터널 액세스를 제공하려는 DAP, 그룹 정책 또는 로컬 사용자 정책에 목록을 할당합니다.클라이언트리스 SSL VPN 세션을 통해 스마트 터널 연결에서 로그인 자

격 증명 제출을 자동화할 웹 지원 애플리케이션을 나열할 수도 있습니다.

이 문서에서는 Cisco AnyConnect SSL VPN Client 컨피그레이션이 이미 작성되었으며, 스마트 터널 기능이 기존 컨피그레이션에서 구성될 수 있도록 올바르게 작동한다고 가정합니다. Cisco AnyConnect SSL VPN 클라이언트를 구성하는 방법에 대한 자세한 내용은 ASA 8.x: ASA 컨피그레이션 예에서 AnyConnect VPN 클라이언트에 대해 스플릿 터널링을 허용합니다.

참고: *ASA 8.x*의 ASDM 6.0(2) 섹션을 사용하여 ASA 컨피그레이션에 설명된 *4.b~4.l* 단계를 확인하십시오. *ASA 컨피그레이션 예제의 AnyConnect VPN 클라이언트에 대한 스플릿 터널링 허용*은 스마트 터널 기능을 구성하기 위해 수행되지 않습니다.

이 문서에서는 Cisco ASA 5500 Series Adaptive Security Appliance에서 스마트 터널을 구성하는 방법에 대해 설명합니다.

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 8.0(2)을 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Microsoft Vista, Windows XP SP2 또는 Windows 2000 Professional SP4(Microsoft Installer 버전 3.1 포함)를 실행하는 PC
- Cisco ASDM(Adaptive Security Device Manager) 버전 6.0(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 규칙을 참조하십시오.

배경 정보

스마트 터널 액세스 컨피그레이션

스마트 터널 테이블에는 스마트 터널 목록이 표시되며, 각 스마트 터널 액세스에 적합한 하나 이상의 애플리케이션 및 관련 OS(운영 체제)를 식별합니다. 각 그룹 정책 또는 로컬 사용자 정책은 하나의 스마트 터널 목록을 지원하므로, 지원되지 않는 브라우저 기반 애플리케이션을 스마트 터널 목록으로 그룹화해야 합니다. 목록의 컨피그레이션에 따라 하나 이상의 그룹 정책 또는 로컬 사용자 정책에 할당할 수 있습니다.

스마트 터널 창(Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN)** > **Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스)** > **Portal(포털)** > **Smart Tunnels(스마트 터널)**)을 사용하여 다음 절차를 완료할 수 있습니다.

- **스마트 터널 목록 추가 및 목록에 애플리케이션 추가**스마트 터널 목록을 추가하고 목록에 애플리케이션을 추가하려면 다음 단계를 완료합니다.Add(**추가)를 클릭합니다**.Add Smart Tunnel List 대화 상자가 나타납니다.목록의 이름을 입력하고 Add(추가)를 **클릭합니다**.스마트 터널의 특성을 목록에 할당할 수 있는 Add Smart Tunnel Entry 대화 상자가 열립니다.스마트 터널에 원하는 특성을 할당한 후 **OK**를 클릭합니다.ASDM은 목록에 해당 특성을 표시합니다.목록을 완성하기 위해 필요에 따라 이 단계를 반복한 다음 Add Smart Tunnel List 대화 상자에서 OK를 클릭합니다.
- **스마트 터널 목록 변경**스마트 터널 목록을 변경하려면 다음 단계를 완료하십시오.목록을 두 번 클릭하거나 테이블의 목록을 선택하고 편집을 **클릭합니다**.Add(**추가)**를 클릭하여 새 스마트 터널 특성 집합을 목록에 삽입하거나 목록에서 항목을 선택하고 Edit(편집) 또**는 Delete(삭제)**를 클릭합니다.
- **목록 제거**목록을 제거하려면 테이블의 목록을 선택하고 **삭제**를 클릭합니다.
- **책갈피 추가**스마트 터널 목록의 컨피그레이션 및 할당에 따라 서비스에 대한 책갈피를 추가하고 Add or Edit Bookmark 대화 상자에서 **Enable Smart Tunnel** 옵션을 클릭하여 스마트 터널을 쉽게 사용할 수 있습니다.

스마트 터널 액세스를 사용하면 클라이언트 TCP 기반 애플리케이션이 브라우저 기반 VPN 연결을 사용하여 서비스에 연결할 수 있습니다. 플러그인과 레거시 기술, 포트 포워딩에 비해 사용자에게 다음과 같은 이점을 제공합니다.

- 스마트 터널은 플러그인보다 우수한 성능을 제공합니다.
- 스마트 터널은 포트 전달과 달리 로컬 애플리케이션에 대한 사용자 연결이 필요하지 않으므로 사용자 환경을 간소화합니다.
- 포트 전달과 달리 스마트 터널은 사용자에게 관리자 권한이 필요하지 않습니다.

스마트 터널 요구 사항, 제한 사항 및 제한 사항

일반적인 요구 사항 및 제한 사항

스마트 터널에는 다음과 같은 일반적인 요구 사항과 제한이 있습니다.

- 스마트 터널을 시작하는 원격 호스트는 32비트 버전의 Microsoft Windows Vista, Windows XP 또는 Windows 2000을 실행해야 합니다. 또는 Mac OS 10.4 또는 10.5입니다.
- 스마트 터널 자동 로그온은 Windows에서 Microsoft Internet Explorer만 지원합니다.
- 브라우저가 Java, Microsoft ActiveX 또는 둘 모두로 활성화되어 있어야 합니다.
- 스마트 터널은 Microsoft Windows를 실행하는 컴퓨터와 보안 어플라이언스 사이에 배치된 프록시만 지원합니다. 스마트 터널은 Internet Explorer 컨피그레이션(즉, Windows에서 시스템 전체에 사용하기 위한 컨피그레이션)을 사용합니다. 원격 컴퓨터에 보안 어플라이언스에 도달하기 위해 프록시 서버가 필요한 경우, 연결 종료의 URL이 프록시 서비스에서 제외된 URL 목록에 있어야 합니다. 프록시 컨피그레이션에서 ASA로 향하는 트래픽이 프록시를 통과하도록 지정하면 모든 스마트 터널 트래픽이 프록시를 통과합니다.HTTP 기반 원격 액세스 시나리오에서 서브넷이 VPN 게이트웨이에 대한 사용자 액세스를 제공하지 않는 경우도 있습니다. 이 경우 웹과 최종 사용자의 위치 간에 트래픽을 라우팅하기 위해 ASA 앞에 배치된 프록시가 웹 액세스를 제공합니다. 그러나 VPN 사용자만 ASA 앞에 배치된 프록시를 구성할 수 있습니다. 이렇게 할 때 이러한 프록시가 CONNECT 방법을 지원하는지 확인해야 합니다. 인증이 필요한 프록시의 경우 스마트 터널은 기본 다이제스트 인증 유형만 지원합니다.
- 스마트 터널이 시작되면 보안 어플라이언스는 사용자가 클라이언트리스 세션을 시작하는 데 사용한 브라우저 프로세스의 모든 트래픽을 터널링합니다. 사용자가 브라우저 프로세스의 다

른 인스턴스를 시작하면 모든 트래픽을 터널로 전달합니다. 브라우저 프로세스가 동일하고 보안 어플라이언스가 지정된 URL에 대한 액세스를 제공하지 않는 경우 사용자는 브라우저 프로세스를 열 수 없습니다. 이를 해결하려면 클라이언트리스 세션을 설정하는 데 사용된 브라우저와 다른 브라우저를 사용할 수 있습니다.
- 스테이트풀 장애 조치는 스마트 터널 연결을 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.

Windows 요구 사항 및 제한 사항

다음 요구 사항 및 제한 사항은 Windows에만 적용됩니다.

- Winsock 2, TCP 기반 애플리케이션만 스마트 터널 액세스에 적합합니다.
- 보안 장치가 Microsoft MAPI(Outlook Exchange) 프록시를 지원하지 않습니다. 포트 전달과 스마트 터널이 모두 MAPI를 지원하지 않습니다. MAPI 프로토콜을 사용하는 Microsoft Outlook Exchange 통신의 경우 원격 사용자는 AnyConnect를 사용해야 합니다.
- 스마트 터널 또는 포트 전달을 사용하는 Microsoft Windows Vista 사용자는 ASA의 URL을 신뢰할 수 있는 사이트 영역에 추가해야 합니다. 신뢰할 수 있는 사이트 영역에 액세스하려면 Internet Explorer를 시작하고 **도구 > 인터넷 옵션**을 선택하고 **보안** 탭을 클릭합니다. Vista 사용자는 스마트 터널 액세스를 용이하게 하기 위해 보호 모드를 비활성화할 수도 있습니다. 그러나 Cisco에서는 이 방법이 공격의 취약성을 증가시키기 때문에 이를 권장하고 있습니다.

Mac OS 요구 사항 및 제한 사항

이러한 요구 사항 및 제한 사항은 Mac OS에만 적용됩니다.

- Safari 3.1.1 이상 또는 Firefox 3.0 이상
- Sun JRE 1.5 이상
- 포털 페이지에서 시작된 애플리케이션만 스마트 터널 연결을 설정할 수 있습니다. 이 요구 사항에는 Firefox에 대한 스마트 터널 지원이 포함됩니다. 스마트 터널을 처음 사용하는 동안 Firefox를 사용하여 다른 Firefox 인스턴스를 시작하려면 csco_st라는 사용자 프로필이 필요합니다. 이 사용자 프로필이 없는 경우, 세션에서 사용자에게 프로필을 생성하라는 메시지를 표시합니다.
- SSL 라이브러리에 동적으로 연결된 TCP를 사용하는 애플리케이션은 스마트 터널을 통해 작동할 수 있습니다.
- 스마트 터널은 Mac OS에서 다음 기능 및 애플리케이션을 지원하지 않습니다.프록시 서비스자동 로그온2단계 이름 공백을 사용하는 애플리케이션텔넷, SSH, cURL 등의 콘솔 기반 애플리케이션dlopen 또는 dlsym을 사용하여 libsocket 호출을 찾는 애플리케이션libsocket 호출을 찾기 위해 정적으로 연결된 애플리케이션

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

스마트 터널 목록 추가 또는 편집

Add Smart Tunnel List(스마트 터널 목록 추가) 대화 상자에서는 스마트 터널 항목 목록을 보안 어플라이언스 컨피그레이션에 추가할 수 있습니다. Edit Smart Tunnel List(스마트 터널 목록 수정) 대

화 상자에서는 목록의 내용을 수정할 수 있습니다.

필드

List Name(목록 이름) - 응용 프로그램 또는 프로그램 목록의 고유한 이름을 입력합니다. 이름의 문자 수는 제한되지 않습니다. 공백을 사용하지 마십시오. 스마트 터널 목록의 컨피그레이션에 따라 목록 이름이 클라이언트리스 SSL VPN 그룹 정책 및 로컬 사용자 정책의 스마트 터널 목록 특성 옆에 나타납니다. 구성하려는 다른 목록과 내용이나 용도를 구분하는 데 도움이 되는 이름을 할당합니다.

스마트 터널 항목 추가 또는 편집

Add or Edit Smart Tunnel Entry(스마트 터널 항목 추가 또는 수정) 대화 상자에서는 스마트 터널 목록에서 애플리케이션의 특성을 지정할 수 있습니다.

- **Application ID(애플리케이션 ID)** - 스마트 터널 목록의 항목 이름을 지정할 문자열을 입력합니다. 문자열은 OS에 대해 고유합니다. 일반적으로 스마트 터널 액세스를 허용할 애플리케이션의 이름을 지정합니다. 서로 다른 경로 또는 해시 값을 지정하도록 선택하는 응용 프로그램의 여러 버전을 지원하려면 이 속성을 사용하여 항목을 구별하고 각 목록 항목에서 지원되는 응용 프로그램의 이름과 버전을 지정할 수 있습니다. 문자열은 최대 64자까지 가능합니다.
- **Process Name(프로세스 이름)** - 응용 프로그램의 파일 이름 또는 경로를 입력합니다. 문자열은 최대 128자까지 가능합니다.Windows에서는 애플리케이션에 스마트 터널 액세스를 허용하려면 원격 호스트의 애플리케이션 경로 오른쪽에 이 값과 정확히 일치해야 합니다. Windows에 대한 파일 이름만 지정하면 SSL VPN은 스마트 터널 액세스를 위해 애플리케이션을 검증하기 위해 원격 호스트에 위치 제한을 적용하지 않습니다.경로를 지정하고 사용자가 애플리케이션을 다른 위치에 설치한 경우 해당 응용 프로그램은 적합하지 않습니다. 문자열의 오른쪽이 입력한 값과 일치하는 경우 응용 프로그램은 모든 경로에 상주할 수 있습니다.원격 호스트의 여러 경로 중 하나에 스마트 터널 액세스를 위한 애플리케이션이 있는 경우 이를 승인하려면 이 필드에 애플리케이션의 이름과 확장명만 지정하거나 각 경로에 대해 고유한 스마트 터널 항목을 생성합니다.Windows의 경우 명령 프롬프트에서 시작된 응용 프로그램에 스마트 터널 액세스를 추가하려면 스마트 터널 목록의 한 항목의 프로세스 이름에 "cmd.exe"를 지정하고 "cmd.exe"가 응용 프로그램의 부모이므로 다른 항목에서 응용 프로그램 자체의 경로를 지정해야 합니다.Mac OS는 프로세스에 대한 전체 경로를 필요로 하며 대/소문자를 구분합니다. 각 사용자 이름에 대한 경로를 지정하지 않으려면 부분 경로 앞에 물결표(~)를 삽입합니다(예: ~/bin/vnc).
- **OS** - 애플리케이션의 호스트 OS를 지정하려면 Windows 또는 Mac을 클릭합니다.
- **해시** - (*선택 사항이며 Windows에만 적용 가능*) 이 값을 얻으려면 SHA-1 알고리즘을 사용하여 해시를 계산하는 유틸리티에 실행 파일의 체크섬을 입력합니다. 이러한 유틸리티의 한 가지 예는 Microsoft FCIV(File Checksum Integrity Verifier)입니다. FCIV(Microsoft File Checksum Integrity Verifier)는 File Checksum Integrity Verifier 유틸리티의 가용성과 설명에 나와 있습니다. FCIV를 설치한 후 공백이 없는 경로(예: c:/fciv.exe)에 해시될 애플리케이션의 임시 복사본을 배치한 다음 명령줄에서 fciv.exe -sha1 애플리케이션(예: fciv.exe -sha1 c:\msimn.exe)을 입력하여 SHA-1 해시를 표시합니다.SHA-1 해시는 항상 16진수 40자입니다.스마트 터널 액세스에 대해 애플리케이션을 인증하기 전에 클라이언트리스 SSL VPN은 애플리케이션 ID와 일치하는 애플리케이션의 해시를 계산합니다. 결과가 해시 값과 일치하는 경우 스마트 터널 액세스를 위해 애플리케이션을 적격화합니다.해시를 입력하면 SSL VPN에서 애플리케이션 ID에 지정한 문자열과 일치하는 불법적인 파일을 정규화하지 않는다는 합당한 보증이 제공됩니다. 체크섬은 애플리케이션의 각 버전 또는 패치에 따라 다르기 때문에 입력하는 해시는 원격 호스트에서 하나의 버전 또는 패치만 매칭할 수 있습니다. 둘 이상의 애플리케이션 버전에 대해 해시를 지정하려면 각 해시 값에 대해 고유한 스마트 터널 항목을 생성합니다.**참고:** 해시 값을 입력

하고 스마트 터널 액세스를 통해 애플리케이션의 향후 버전 또는 패치를 지원하려는 경우 스마트 터널 목록을 나중에 업데이트해야 합니다. 스마트 터널 액세스의 갑작스러운 문제는 해시 값을 포함하는 애플리케이션이 애플리케이션 업그레이드에 최신 상태가 아니라는 의미일 수 있습니다. 해시를 입력하지 않으면 이 문제를 방지할 수 있습니다.

- 스마트 터널 목록을 구성한 후에는 다음과 같이 활성화되도록 그룹 정책 또는 로컬 사용자 정책에 이를 할당해야 합니다.그룹 정책에 목록을 할당하려면 **Config > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add or Edit > Portal을** 선택하고 Smart Tunnel List 특성 옆의 드롭다운 목록에서 스마트 터널 이름을 선택합니다.로컬 사용자 정책에 목록을 할당하려면 Config **> Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**을 선택하고 Smart Tunnel List 특성 옆의 드롭다운 목록에서 스마트 터널 이름을 선택합니다.

ASDM 6.0(2)을 사용하는 ASA 스마트 터널(Lotus 예) 컨피그레이션

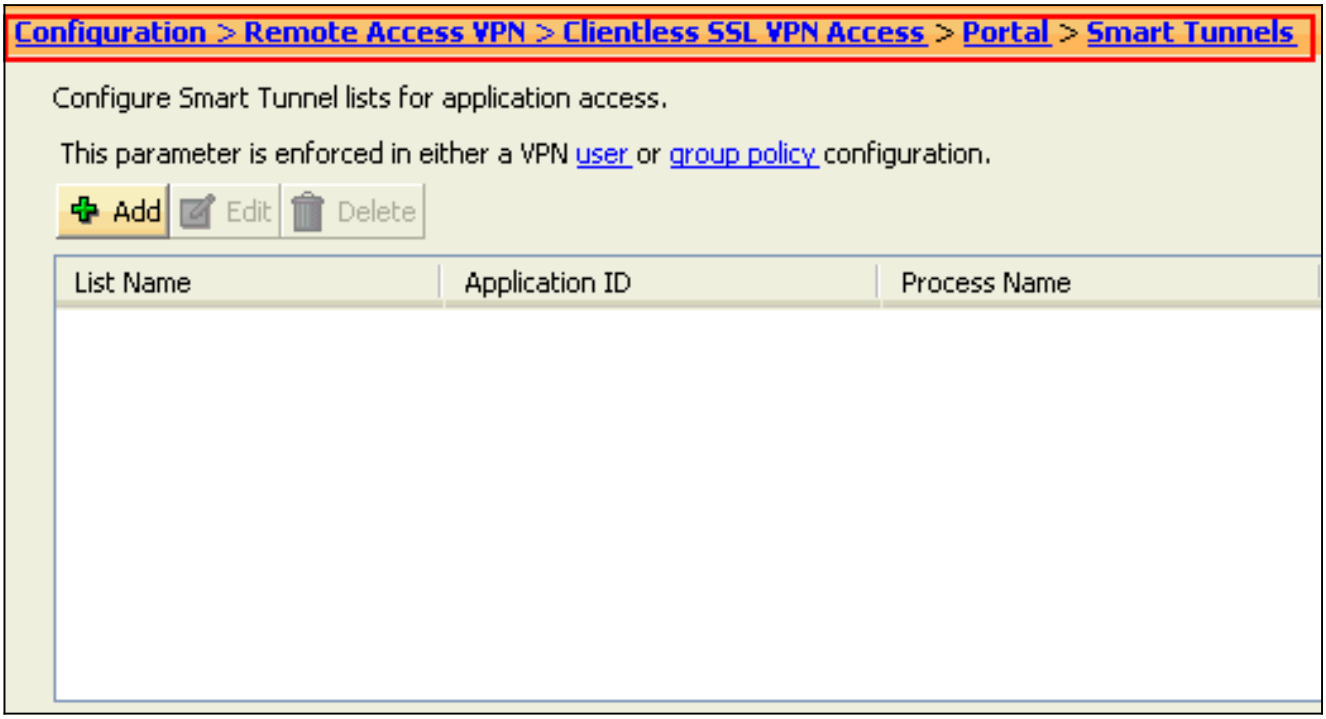
이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 완료되었으며 제대로 작동한다고 가정합니다.

스마트 터널을 구성하려면 다음 단계를 완료하십시오.

참고: 이 컨피그레이션 예에서는 Lotus 애플리케이션에 대해 스마트 터널이 구성됩니다.

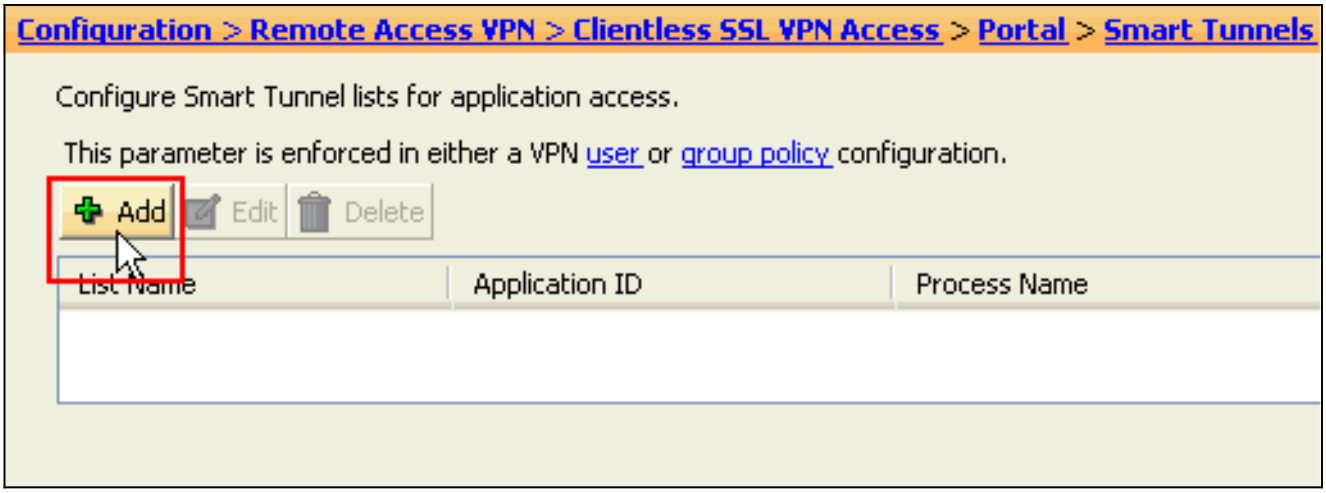
1. 스마트 터널 **컨피그레이션을** 시작하려면 Configuration(컨피그레이션) **> Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Smart Tunnels(스마트 터널)**를 선택합니다

.



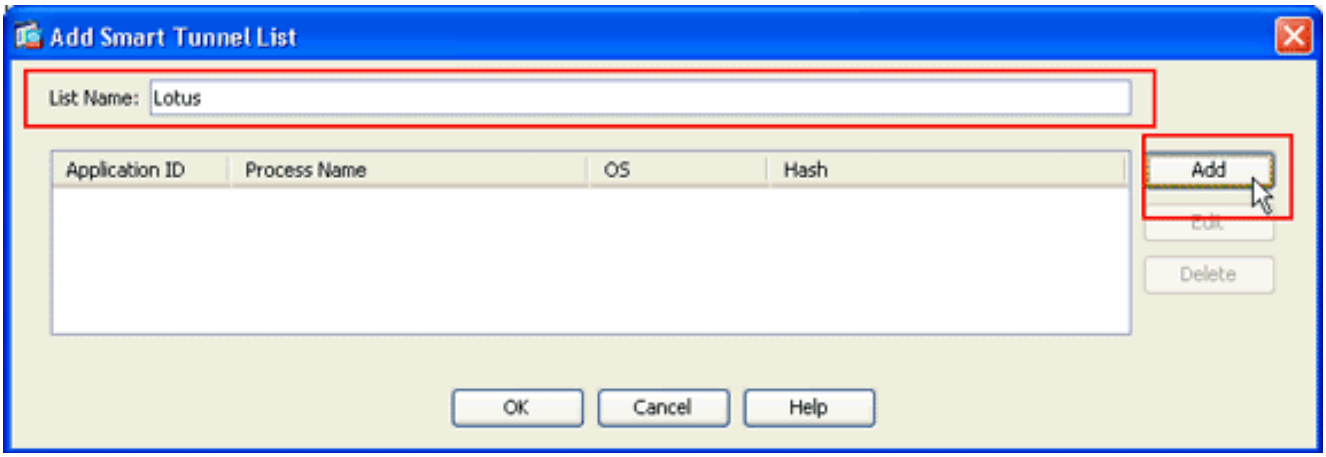
2. Add(**추가)를 클릭합니다**

.

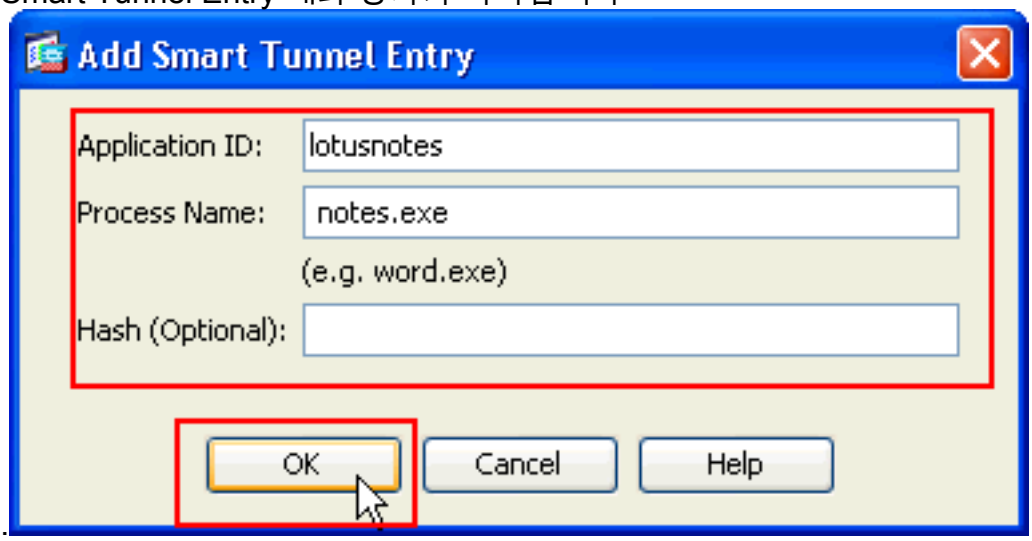


Add Smart Tunnel List 대화 상자가 나타납니다

.



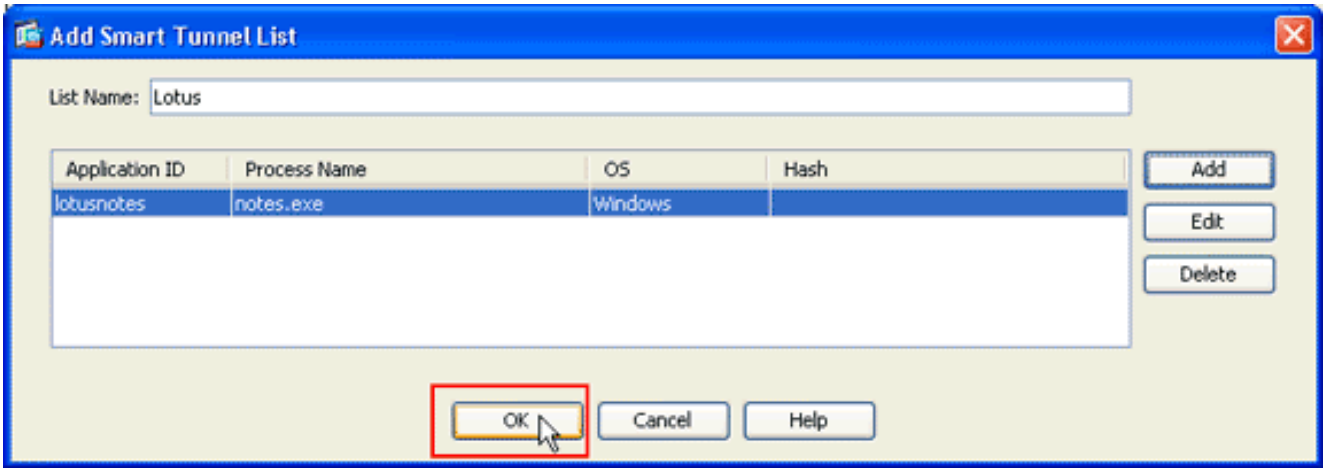
3. Add Smart Tunnel List(스마트 터널 목록 추가) 대화 상자에서 Add(추가)를 **클릭합니다**.Add Smart Tunnel Entry 대화 상자가 나타납니다



.

4. Application ID(애플리케이션 ID) 필드에 스마트 터널 목록 내의 항목을 식별할 문자열을 입력합니다.
5. 응용 프로그램의 파일 이름과 확장명을 입력하고 **확인**을 클릭합니다.
6. Add Smart Tunnel List(스마트 터널 목록 추가) 대화 상자에서 **OK**(확인)를 클릭합니다

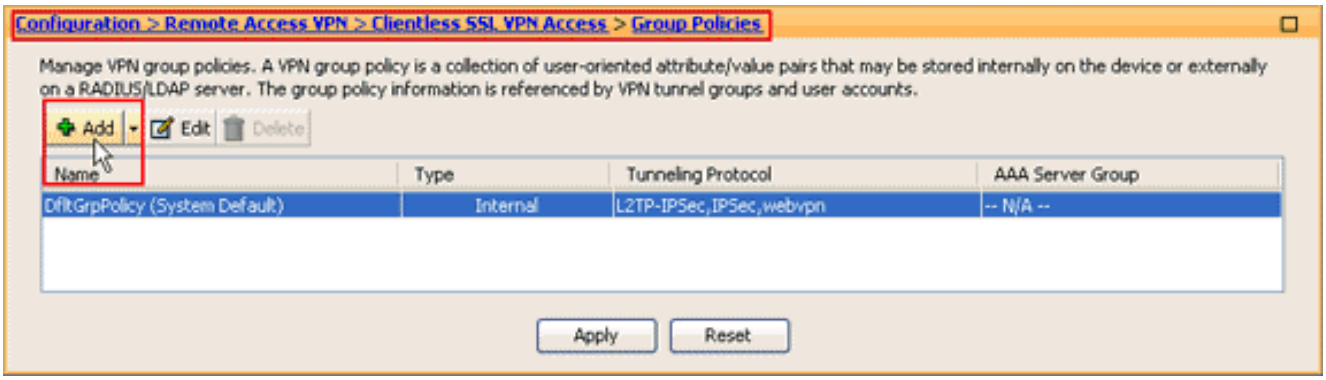
.



참고: 등가 CLI 컨피그레이션 명령은 다음과 같습니다.

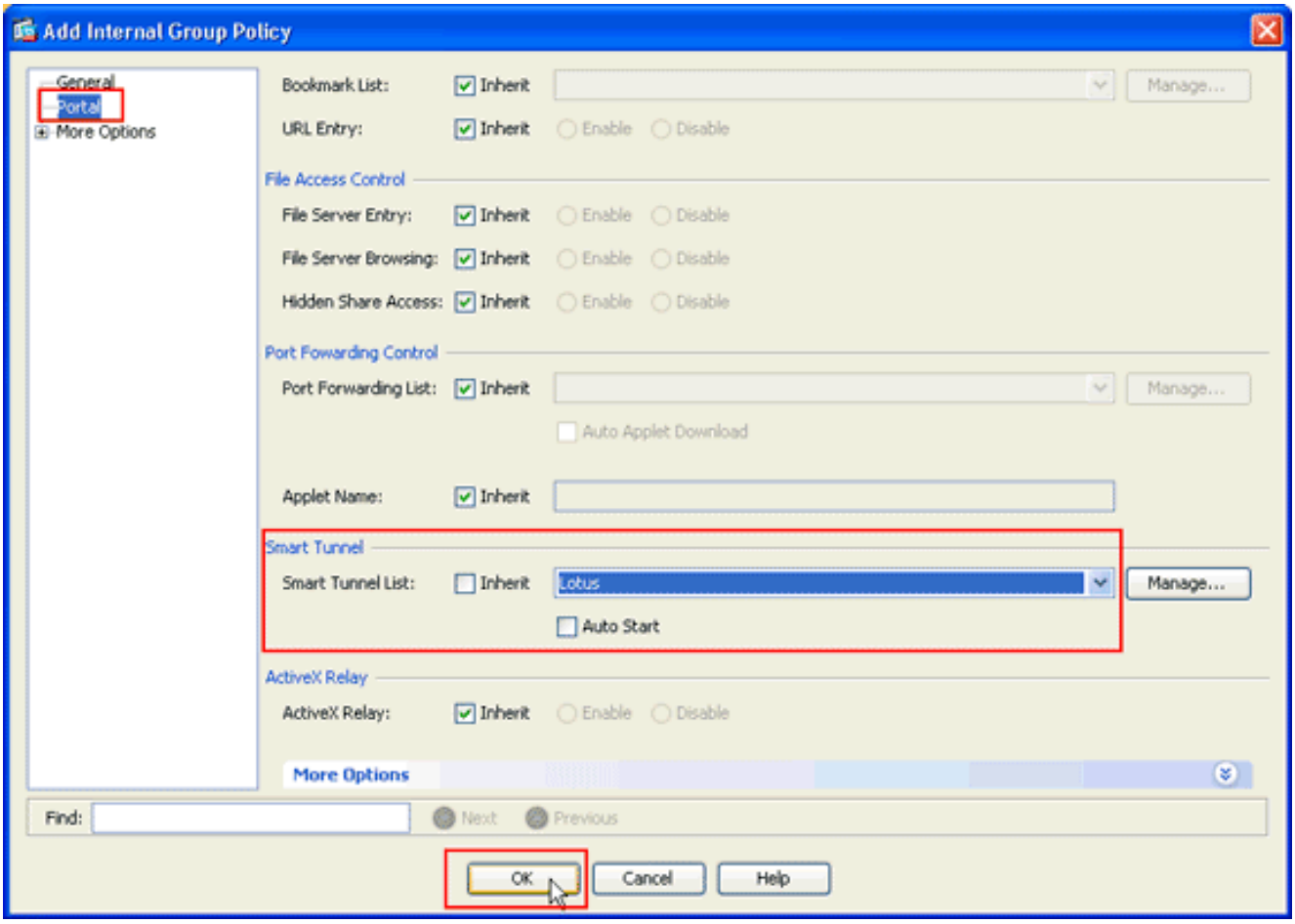
7. 다음과 같이 관련 애플리케이션에 스마트 터널 액세스를 제공하려는 그룹 정책 및 로컬 사용자 정책에 목록을 할당합니다.그룹 정책에 목록을 할당하려면 Configuration(컨피그레이션) **> Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Group Policies(그룹 정책)를** 선택하고 **Add(추가)** 또는 **Edit(편집)**를 클릭합니다

.



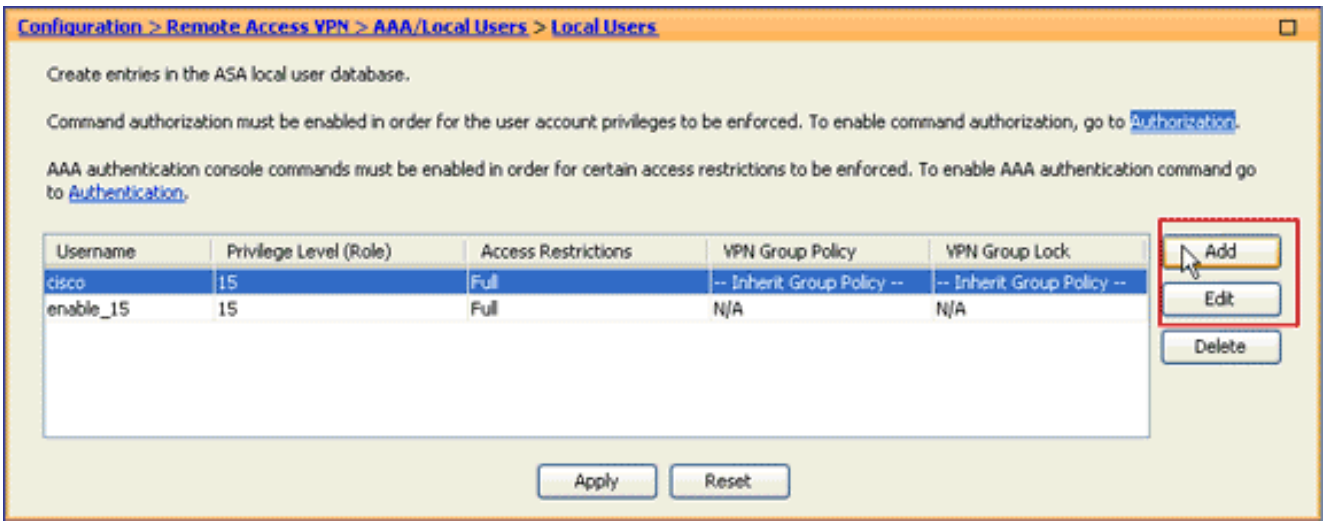
Add Internal Group Policy 대화 상자가 나타납니다

.



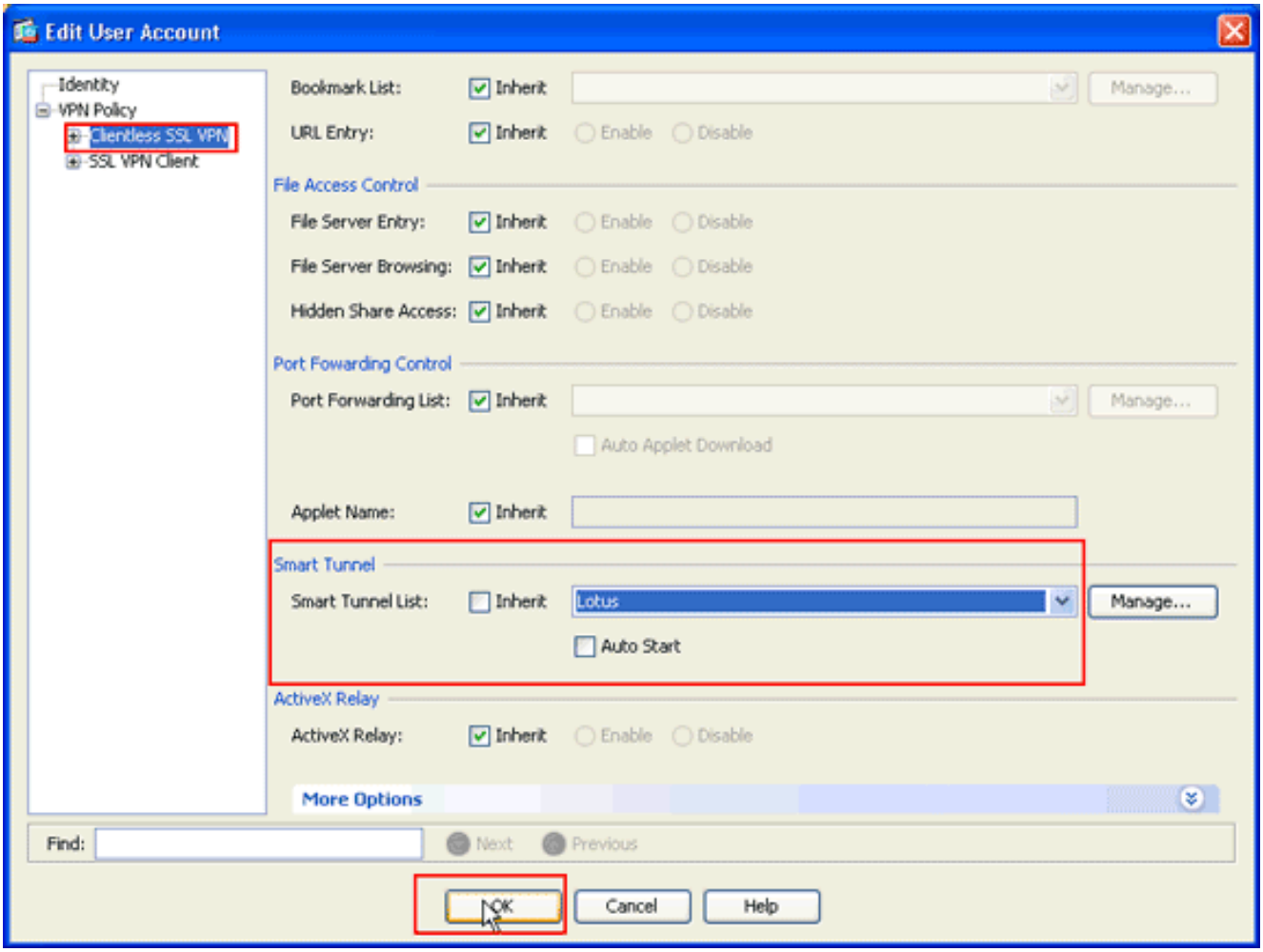
8. Add Internal Group Policy(내부 그룹 정책 추가) 대화 상자에서 **Portal(포털)**을 클릭하고 Smart Tunnel List(스마트 터널 목록) 드롭다운 목록에서 스마트 터널 이름을 선택한 다음 **OK**(확인)를 클릭합니다.**참고:** 이 예에서는 *Lotus*를 스마트 터널 목록 이름으로 사용합니다.
9. 로컬 사용자 정책에 목록을 할당하려면 Configuration(구성) **> Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > Local Users(로컬 사용자)를** 선택하고 **Add(추가)를** 클릭하여 새 사용자를 구성하거나 Edit(편집)를 클릭하여 기존 사용자를 수정합니다

.



Edit User Account 대화 상자가 나타납니다

.



10. Edit User Account(사용자 계정 수정) 대화 상자에서 Clientless **SSL VPN**을 클릭하고 Smart Tunnel List(스마트 터널 목록) 드롭다운 목록에서 스마트 터널 이름을 선택한 다음 **OK**(확인)를 클릭합니다.**참고:** 이 예에서는 *Lotus*를 스마트 터널 목록 이름으로 사용합니다.

스마트 터널 구성이 완료되었습니다.

문제 해결

클라이언트리스 포털에서 즐겨찾기에 추가된 스마트 터널 URL을 사용하여 연결할 수 없습니다. 이 문제는 왜 발생하며 어떻게 해결할 수 있습니까?

이 문제는 Cisco Bug ID CSCsx05766에 설명된 문제로 인해 발생합니다(**등록된 고객만 해당**). 이 문제를 해결하려면 Java Runtime 플러그인을 이전 버전으로 다운그레이드합니다.

WebVPN에 구성된 스마트 터널 링크의 URL을 연결할 수 있습니까?

ASA에서 스마트 터널이 사용되는 경우 URL을 왜곡하거나 브라우저의 주소 표시줄을 숨길 수 없습니다. 사용자는 스마트 터널을 사용하는 WebVPN에 구성된 링크의 URL을 볼 수 있습니다. 따라서 포트를 변경하고 다른 서비스를 위해 서버에 액세스할 수 있습니다.

이 문제를 해결하려면 WebType ACL을 사용합니다. 자세한 내용은 웹 타입 액세스 제어 목록을 참조하십시오.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- ASA의 SVC(SSL VPN Client) with ASDM 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems